FlexPod Lösungen

FlexPod

NetApp
November 04, 2025

Inhalt

FlexPod Lösungen

FlexPod-Definition

Technische Spezifikationen zu FlexPod Express

TR-4293: Technische Spezifikationen von FlexPod Express

Kardick Radhakrishnan, Arvind Ramakrishnan, Lindsey Street, Savita Kumari, NetApp

FlexPod Express ist eine vorkonfigurierte Best Practice-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS) und den Switches der Cisco Nexus Familie aufbaut. Die Storage-Ebene basiert auf dem NetApp FAS oder auf dem NetApp E-Series Storage. FlexPod Express ist eine geeignete Plattform zur Ausführung verschiedener Virtualisierungshypervisoren sowie Bare Metal-Betriebssysteme (Betriebssysteme) und Enterprise Workloads.

FlexPod Express ist nicht nur eine Basiskonfiguration, sondern auch die Flexibilität, sich an die Vielzahl von Anwendungsfällen und Anforderungen anpassen zu lassen. Dieses Dokument kategorisiert die Konfigurationen von FlexPod Express basierend auf dem verwendeten Storage-System, FlexPod Express mit NetApp FAS und FlexPod Express mit der E-Series.

FlexPod Plattformen

Es gibt drei FlexPod Plattformen:

- **FlexPod Datacenter.** Diese Plattform ist eine äußerst skalierbare virtuelle Datacenter-Infrastruktur, die sich für Workloads von Enterprise-Applikationen, Virtualisierung, VDI sowie Public und Private Clouds eignet. FlexPod Datacenter verfügt über eigene Spezifikationen, die in dokumentiert sind "TR-4036: Technische Spezifikationen zu FlexPod Datacenter".
- **FlexPod Express.** Diese Plattform ist eine kompakte konvergente Infrastruktur, die sich für Anwendungsfälle in Remote-Zweigstellen und Edge eignet.

Dieses Dokument enthält die technischen Spezifikationen der FlexPod Express Plattform.

FlexPod Regeln

Das FlexPod Design ermöglicht eine flexible Infrastruktur, die viele verschiedene Komponenten und Softwareversionen umfasst.

Verwenden Sie die Regelsätze als Leitfaden zum Erstellen oder Zusammenbauen einer gültigen FlexPod-Konfiguration. Die in diesem Dokument aufgeführten Zahlen und Regeln stellen die Mindestanforderungen für FlexPod dar und können in den enthaltenen Produktfamilien erweitert werden, so wie es für unterschiedliche Umgebungen und Anwendungsfälle erforderlich ist.

Unterstützte und validierte FlexPod Konfigurationen

Die FlexPod-Architektur wird durch den in diesem Dokument beschriebenen Regelsatz definiert. Die Hardwarekomponenten und Software-Konfigurationen müssen von der Cisco Hardware Compatibility List (HCL) und der unterstützt werden "NetApp Interoperabilitäts-Matrix-Tool (IMT)".

Jedes Cisco Validated Design (CVD) oder jede NetApp Verified Architecture (NVA) ist eine mögliche FlexPod-Konfiguration. Cisco und NetApp dokumentieren diese Konfigurationskombinationen und validieren sie in umfangreichen End-to-End-Tests. Die von diesen Konfigurationen abweichenden FlexPod-Einsätze werden vollständig unterstützt, wenn sie den Richtlinien in diesem Dokument entsprechen und alle Komponenten in der Cisco HCL und NetApp als kompatibel aufgeführt sind "IMT".

Beispielsweise werden zusätzliche Storage-Controller oder Cisco UCS Server hinzugefügt und Software-Upgrades auf neuere Versionen durchgeführt, wenn die Software, Hardware und Konfigurationen den in diesem Dokument definierten Richtlinien entsprechen.

Storage Software

FlexPod Express unterstützt Storage-Systeme mit NetApp ONTAP oder SANtricity Betriebssystemen.

NetApp ONTAP

Die NetApp ONTAP Software ist das Betriebssystem, das auf AFF und FAS Storage-Systemen ausgeführt wird. ONTAP bietet eine hochskalierbare Storage-Architektur, die unterbrechungsfreien Betrieb, unterbrechungsfreie Upgrades und eine agile Dateninfrastruktur ermöglicht.

Weitere Informationen zu ONTAP finden Sie im "ONTAP Produktseite".

E-Series SANtricity Software

Die E-Series SANtricity Software ist das Betriebssystem, das auf Storage-Systemen der E-Series ausgeführt wird. SANtricity bietet ein hochflexibles System, das verschiedene Applikationsanforderungen erfüllt und integrierte Hochverfügbarkeit sowie zahlreiche Datensicherungsfunktionen bietet.

Weitere Informationen finden Sie im "SANtricity Produktseite".

Mindestanforderungen an die Hardware

In diesem Abschnitt werden die Mindestanforderungen an die Hardware für die verschiedenen Versionen von FlexPod Express beschrieben.

FlexPod Express mit NetApp FAS

Zu den Hardwareanforderungen für FlexPod Express Lösungen, die NetApp FAS Controller für zugrunde liegenden Storage verwenden, gehören die in diesem Abschnitt beschriebenen Konfigurationen.

CIMC-basierte Konfiguration (Standalone Rack Server)

Die Konfiguration des Cisco Integrated Management Controller (CIMC) umfasst die folgenden Hardwarekomponenten:

- Zwei 10 Gbit/s-Standard-Ethernet-Switches in einer redundanten Konfiguration (Cisco Nexus 31108 wird empfohlen, mit Unterstützung der Cisco Nexus 3000- und 9000-Modelle)
- Standalone-Rack-Server der Cisco UCS C-Serie
- Zwei AFF Controller der C190, AFF A250, FAS2600 oder FAS 2700 Serie in einer HA-Paar-Konfiguration, die als Cluster mit zwei Nodes implementiert wird

Von Cisco UCS gemanagte Konfiguration

Die Bestätigung, die durch Cisco UCS gemanagt wird, umfasst die folgenden Hardwarekomponenten:

- Zwei 10 Gbit/s Standard-Ethernet-Switches in einer redundanten Konfiguration (Cisco Nexus 3524 wird empfohlen)
- Ein Cisco UCS 5108 Wechselstrom-Blade-Server-Chassis (AC
- Zwei Cisco UCS 6324 Fabric Interconnects
- Cisco UCS B-Series Server (mindestens vier Cisco UCS B200 M5 Blade Server)
- Zwei AFF C190, AFF A250, FAS2750 oder FAS2720 Controller in einer HA-Paar-Konfiguration (erfordert zwei verfügbare Unified Target Adapter 2 [UTA2]-Ports pro Controller)

FlexPod Express mit E-Series

Zu den Hardwareanforderungen für die FlexPod Express Konfiguration mit E-Series Starter gehören:

- Zwei Cisco UCS 6324 Fabric Interconnects
- Ein Cisco UCS Mini-Chassis 5108 AC2 oder DC2 (die Cisco UCS 6324 Fabric Interconnects werden nur in den AC2- und DC2-Gehäusen unterstützt)
- Cisco UCS B-Series Server (mindestens zwei Cisco UCS B200 M4 Blade Server)
- Eine HA-Paar-Konfiguration eines E-Series E2824 Storage-Systems mit mindestens 12 Festplattenlaufwerken
- Zwei 10 Gbit/s Standard-Ethernet-Switches in einer redundanten Konfiguration (vorhandene Switches im Datacenter können verwendet werden)

Diese Hardwarekomponenten sind erforderlich, um eine Einstiegkonfiguration der Lösung zu erstellen; bei Bedarf können zusätzliche Blade Server und Festplatten hinzugefügt werden. Das E2824 Storage-System der E-Series kann durch eine höhere Plattform ersetzt werden und kann auch als All-Flash-System ausgeführt werden.

Mindestanforderungen An Die Software

In diesem Abschnitt werden die Mindestanforderungen für Software für die verschiedenen Versionen von FlexPod Express beschrieben.

Softwareanforderungen für FlexPod Express mit NetApp AFF oder FAS

Zu den Softwareanforderungen für FlexPod Express mit NetApp FAS gehören:

- ONTAP 9.1 oder höher
- Cisco NX-OS Version 7.0(3)I6(1) oder höher
- In der von Cisco UCS verwalteten Konfiguration entspricht Cisco UCS Manager UCS 4.0(1b)

Alle Software muss in aufgeführt und unterstützt sein "NetApp IMT". Bestimmte Softwarefunktionen erfordern möglicherweise mehr aktuelle Code-Versionen als die in vorherigen Architekturen aufgeführten Mindestwerte.

Softwareanforderungen für FlexPod Express mit E-Series

Zu den Softwareanforderungen für FlexPod Express mit der E-Series gehören:

- E-Series SANtricity Software 11.30 oder höher
- Cisco UCS Manager 4.0(1b):

Alle Software muss in aufgeführt und unterstützt sein "NetApp IMT".

Konnektivitätsanforderungen erfüllen

In diesem Abschnitt werden die Konnektivitätsanforderungen für die verschiedenen Versionen von FlexPod Express beschrieben.

Konnektivitätsanforderungen für FlexPod Express mit NetApp FAS

Die Konnektivitätsanforderungen für FlexPod Express mit NetApp FAS umfassen:

- NetApp FAS Storage Controller müssen direkt mit den Cisco Nexus Switches verbunden sein. Ausnahmen bilden die von Cisco UCS gemanagte Konfiguration, bei der Storage Controller mit Fabric Interconnects verbunden werden.
- Es können keine zusätzlichen Geräte zwischen den Kern-FlexPod-Komponenten inline platziert werden.
- Virtuelle Port-Kanäle (vPCs) sind erforderlich, um die Switches der Cisco Nexus 3000/9000 Serie mit den NetApp Storage Controllern zu verbinden.
- Dies ist zwar nicht erforderlich, jedoch wird die Unterstützung für Jumbo Frames in der gesamten Umgebung empfohlen.

Konnektivitätsanforderungen für FlexPod Express mit NetApp E-Series

Die Konnektivitätsanforderungen für FlexPod Express mit der E-Series umfassen:

- Die Storage Controller der E-Series müssen direkt mit den Fabric Interconnects verbunden sein.
- Es sollten keine zusätzlichen Geräte zwischen den Kern-FlexPod-Komponenten inline platziert werden.
- Zwischen Fabric Interconnects und Ethernet Switches sind vPCs erforderlich.

Konnektivitätsanforderungen für FlexPod Express mit NetApp AFF

Die Konnektivitätsanforderungen für FlexPod Express mit NetApp AFF umfassen:

- NetApp AFF Storage-Controller müssen direkt mit den Cisco Nexus Switches verbunden sein. Ausnahmen bilden die von Cisco UCS gemanagte Konfiguration, in der Storage-Controller mit dem Fabric verbunden werden. Interconnects:
- Es können keine zusätzlichen Geräte zwischen den Kern-FlexPod-Komponenten inline platziert werden.
- Virtuelle Port-Kanäle (vPCs) sind erforderlich, um die Switches der Cisco Nexus 3000/9000 Serie mit den NetApp Storage Controllern zu verbinden.
- Dies ist zwar nicht erforderlich, jedoch wird die Unterstützung für Jumbo Frames in der gesamten Umgebung empfohlen.

Andere Anforderungen

Zusätzliche Anforderungen für FlexPod Express sind:

- Für alle Geräte sind gültige Support-Verträge erforderlich, darunter:

- SMARTnet-Support für Cisco-Geräte
- SupportEdge Advisor oder SupportEdge Premium Support für NetApp Systeme

- Alle Softwarekomponenten müssen in aufgeführt und unterstützt werden "NetApp IMT".
- Alle Hardwarekomponenten von NetApp müssen auf aufgeführt und unterstützt werden "NetApp Hardware Universe".
- Alle Hardwarekomponenten von Cisco müssen auf aufgeführt und unterstützt werden "Cisco HCL".

Altgeräte

In der folgenden Tabelle werden die Optionen für ältere Storage Controller von NetApp aufgeführt.

Storage Controller	FAS Teilenummer	Technische Spezifikationen
FAS2520	Basierend auf den ausgewählten Optionen	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	Basierend auf den ausgewählten Optionen	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	Basierend auf den ausgewählten Optionen	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	Basierend auf den ausgewählten Optionen	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

In der folgenden Tabelle werden die Optionen für alte NetApp Platten-Shelfs für NetApp FAS aufgeführt.

Festplatten-Shelf	Teilenummer	Technische Spezifikationen
DE1600	E-X5682A-DM-0E-R6-C	"Technische Spezifikationen zu Festplatten-Shelfs auf NetApp Hardware Universe"
DE5600	E-X4041A-12-R6	"Technische Spezifikationen zu Festplatten-Shelfs auf NetApp Hardware Universe"
DE6600	X-48564-00-R6	"Technische Spezifikationen zu Festplatten-Shelfs auf NetApp Hardware Universe"

Ältere NetApp FAS Controller

In der folgenden Tabelle werden die Optionen für veraltete NetApp FAS Controller aufgeführt.

Aktuelle Komponente	FAS2554	FAS2552	FAS2520
Konfiguration	2 Controller in einem 4-HE-Gehäuse	2 Controller in einem 2-HE-Gehäuse	2 Controller in einem 2-HE-Gehäuse

Aktuelle Komponente	FAS2554	FAS2552	FAS2520
Maximale Rohkapazität	576 TB	509 TB	336 TB
Interne Laufwerke	24	24	12
Maximale Anzahl an Laufwerken (intern und extern)	144	144	84
Maximale Volume-Größe	60 TB		
Maximale Aggregatgröße	120 TB		
Maximale Anzahl an LUNs	2,048 pro Controller		
Unterstützte Storage-Netzwerke	ISCSI, FC, FCoE, NFS und CIFS		ISCSI, NFS und CIFS
Maximale Anzahl an NetApp FlexVol-Volumes	1,000 pro Controller		
Die maximale Anzahl an NetApp Snapshot Kopien	255,000 pro Controller		

Weitere NetApp FAS Modelle finden Sie im "Bereich „FAS-Modelle“" Im Hardware Universe.

Weitere Informationen

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten und auf den folgenden Websites:

- AFF und FAS System Documentation Center

  "https://docs.netapp.com/platstor/index.jsp"

- AFF Dokumentationsmaterialien

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- Dokumentations-Seite zu FAS Storage-Systemen

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- NetApp Dokumentation

  "https://docs.netapp.com"

Technische Spezifikationen für FlexPod Datacenter

TR-4036: Technische Spezifikationen zu FlexPod Datacenter

Arvind Ramakrishnan und Jyh-Sing Chen, NetApp

Die FlexPod Plattform ist eine vorkonfigurierte, Best Practice Datacenter-Architektur, die auf Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switch-Produktfamilie und NetApp Storage Controllern (AFF, ASA oder FAS Systeme) basiert.

FlexPod ist eine geeignete Plattform für die Ausführung einer Vielzahl von Virtualisierungs-Hypervisoren sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads. FlexPod bietet nicht nur eine Basiskonfiguration, sondern auch die Flexibilität, gemäß den Anforderungen vieler verschiedener Anwendungsfälle und Anwendungsfälle dimensioniert zu werden.

Informationen zur Bestellung einer vollständigen FlexPod-Konfiguration finden Sie im "Konvergente FlexPod Infrastruktur" Seite auf netapp.com für die aktuelle Version dieser technischen Spezifikationen.

"Als Nächstes: FlexPod Plattformen."

FlexPod Plattformen

Es gibt zwei FlexPod Plattformen:

- **FlexPod Datacenter.** Diese Plattform ist eine äußerst skalierbare virtuelle Datacenter-Infrastruktur, die sich für Enterprise-Workloads, Virtualisierung, Virtual Desktop Infrastructure (VDI) sowie Public, Private und Hybrid Cloud-Workloads eignet.
- * FlexPod Express.* Bei dieser Plattform handelt es sich um eine kompakte konvergente Infrastruktur für Anwendungsfälle in Remote-Zweigstellen und an Edge-Standorten. FlexPod Express verfügt über eigene Spezifikationen, die im dokumentiert sind "Technische Spezifikationen zu FlexPod Express"

Dieses Dokument enthält die technischen Spezifikationen zur FlexPod Datacenter-Plattform.

FlexPod Regeln

Das FlexPod Design ermöglicht eine flexible Infrastruktur, die viele verschiedene Komponenten und Softwareversionen umfasst.

Verwenden Sie die Regelsätze als Leitfaden zum Erstellen oder Zusammenbauen einer gültigen FlexPod-Konfiguration. Die in diesem Dokument aufgeführten Zahlen und Regeln stellen die Mindestanforderungen für eine FlexPod-Konfiguration dar. Sie können je nach Bedarf in verschiedenen Umgebungen und Anwendungsfällen in den enthaltenen Produktfamilien erweitert werden.

NetApp ONTAP

Die NetApp ONTAP Software wird auf allen NetApp FAS, AFF und AFF All SAN Array (ASA) Systemen installiert. FlexPod wurde mit der ONTAP Software validiert und bietet eine hochskalierbare Storage-Architektur, die unterbrechungsfreien Betrieb, unterbrechungsfreie Upgrades und eine Agile Data Infrastructure ermöglicht.

Weitere Informationen zu ONTAP finden Sie im "ONTAP Data Management-Software" Produktseite.

Cisco Nexus Switching Betriebsmodi

Als Switching-Komponente bei einer bestimmten FlexPod Implementierung können mehrere Cisco Nexus Produkte verwendet werden. Die meisten dieser Optionen nutzen das herkömmliche Cisco Nexus Betriebssystem oder die NX-OS Software. Die Cisco Nexus Switches bieten in ihren Produktlinien unterschiedliche Funktionen. Diese Funktionen werden im weiteren Verlauf dieses Dokuments genauer beschrieben.

Das Angebot von Cisco im Bereich der softwaredefinierten Netzwerke heißt Application Centric Infrastructure (ACI). Die Cisco Nexus Produktreihe, die den ACI Modus unterstützt, auch als Fabric-Modus bezeichnet, ist die Cisco Nexus 9300 Serie. Diese Switches können auch im NX-OS- oder Standalone-Modus implementiert werden.

Cisco ACI wurde für die Implementierungen in Datacentern entwickelt, die die Anforderungen einer spezifischen Applikation erfüllen. Applikationen werden durch eine Reihe von Profilen und Verträgen instanziiert, die die Konnektivität vom Host oder der Virtual Machine (VM) über das Netzwerk zum Storage ermöglichen.

FlexPod wurde mit beiden Betriebsmodi des Cisco Nexus Switches validiert. Weitere Informationen zur ACI und zum NX-OS-Modus finden Sie auf den folgenden Cisco Seiten:

- "Cisco Application Centric Infrastructure"
- "Cisco NX-OS Software"

Mindestanforderungen an die Hardware

Eine FlexPod Datacenter Konfiguration verfügt über ein Minimum an Hardware-Anforderungen, einschließlich Switches, Fabric Interconnects, Servern und NetApp Storage Controllern.

Sie müssen Cisco UCS Server verwenden. Sowohl C-Series als auch B-Series Server wurden in den validierten Designs zum Einsatz kommen. Cisco Nexus Fabric Extender (FEXs) sind optional mit Servern der C-Serie erhältlich.

Eine FlexPod-Konfiguration umfasst die folgenden Mindestanforderungen an die Hardware:

- Zwei Cisco Nexus Switches in einer redundanten Konfiguration. Diese Konfiguration kann aus zwei redundanten Switches der Cisco Nexus 5000, 7000 oder 9000 Serie bestehen. Die beiden Switches sollten vom gleichen Modell sein und im gleichen Betriebsmodus konfiguriert sein.

  Bei der Implementierung einer ACI Architektur müssen folgende zusätzliche Anforderungen erfüllt werden:

  - Implementieren Sie Switches der Cisco Nexus 9000 Serie in einer Leaf-Spine-Topologie.
  - Verwendung von drei Cisco Application Policy Infrastructure Controllern (APICs)
- Zwei Cisco UCS 6200, 6300 oder 6400 Series Fabric Interconnects in einer redundanten Konfiguration.
- Cisco UCS-Server:
  - Wenn die Lösung Server der B-Serie verwendet, gibt es ein Cisco UCS 5108 Blade Server-Gehäuse der B-Serie sowie zwei Cisco UCS Blade Server der B-Serie plus zwei 2104, 2204/8, 2408 oder 2304 I/O-Module (IOMs).
  - Wenn die Lösung Server der C-Serie verwendet, werden zwei Cisco UCS C-Series Rack Server

verwendet.

Für größere Implementierungen von Cisco UCS C-Series Rack Servern können Sie ein Paar 2232PP FEX-Module wählen. Die 2232PP ist jedoch keine Hardware-Anforderung.

- Zwei NetApp Storage-Controller in einer HA-Paar-Konfiguration (High Availability, Hochverfügbarkeit):

  Diese Konfiguration kann aus allen unterstützten NetApp FAS-, AFF- oder ASA-Storage Controllern bestehen. Siehe "NetApp Hardware Universe" Applikation für eine aktuelle Liste der unterstützten Controller-Modelle FAS, AFF und ASA.

  - Für den Datenzugriff benötigt die HA-Konfiguration zwei redundante Schnittstellen pro Controller. Als Schnittstellen können FCoE, FC oder 10/25 GB-Ethernet (GbE) verwendet werden.
  - Wenn in der Lösung NetApp ONTAP verwendet wird, ist eine von NetApp genehmigte Cluster-Interconnect-Topologie erforderlich. Weitere Informationen finden Sie im "Schalter" Registerkarte im NetApp Hardware Universe.
  - Bei Nutzung von ONTAP sind mindestens zwei zusätzliche 10/25/100-GbE-Ports pro Controller für den Datenzugriff erforderlich.
  - Bei ONTAP Clustern mit zwei Nodes können Sie ein 2-Node-Cluster ohne Switches konfigurieren.
  - Bei ONTAP Clustern mit mehr als zwei Nodes sind Cluster-Interconnect-Switches erforderlich.
- Ein NetApp-Festplatten-Shelf mit jeder unterstützten Festplattenart Siehe die Registerkarte Shelfs des "NetApp Hardware Universe" Erhalten Sie eine aktuelle Liste der unterstützten Platten-Shelf-Modelle.

Mindestanforderungen an Software

Eine FlexPod-Konfiguration erfüllt die folgenden Mindestanforderungen für Software:

- NetApp ONTAP:
  - Für die ONTAP Softwareversion ist ONTAP 9.1 oder höher erforderlich
- Versionen von Cisco UCS Manager:
  - Fabric Interconnect der Cisco UCS 6200-Serie – 2.2(8a)
  - Fabric Interconnect der Cisco UCS 6300-Serie – 3.1(1e)
  - Fabric Interconnect der Cisco UCS 6400-Serie – 4.0(1)
- Cisco Intersight Managed Mode:
  - Fabric Interconnect der Cisco UCS 6400-Serie – 4.1(2)
- Für Switches der Cisco Nexus 5000-Serie, Cisco NX-OS-Softwareversion 5.0(3)N1(1c) oder höher, einschließlich NX-OS 5.1.x
- Für Switches Der Cisco Nexus 7000 Serie:
  - Für das 4-Steckplatz-Chassis ist die Cisco NX-OS Software Version 6.1(2) oder höher erforderlich
  - Für das 9-Steckplatz-Chassis ist die Cisco NX-OS Software Version 5.2 oder höher erforderlich
  - Für das 10-Steckplatz-Chassis ist die Cisco NX-OS Software Version 4.0 oder höher erforderlich
  - Für das 18-Steckplatz-Chassis ist die Cisco NX-OS Software Version 4.1 oder höher erforderlich
- Für Switches der Cisco Nexus 9000 Serie, Cisco NX-OS Software Version 6.1(2) oder höher

Die Software, die in einer FlexPod-Konfiguration verwendet wird, muss im NetApp aufgeführt und unterstützt werden "IMT". Bei einigen Funktionen sind möglicherweise aktuellere Versionen der Software erforderlich als die aufgeführten.

Konnektivitätsanforderungen erfüllen

Eine FlexPod-Konfiguration erfüllt die folgenden Konnektivitätsanforderungen:

- Für alle Komponenten ist ein separates Ethernet-/1 GB/s-Ethernet-Out-of-Band-Managementnetzwerk erforderlich.
- NetApp empfiehlt, die Jumbo Frame-Unterstützung in der gesamten Umgebung zu aktivieren, ist jedoch nicht erforderlich.
- Die Ports der Cisco UCS Fabric Interconnect Appliance werden nur für iSCSI- und NAS-Verbindungen empfohlen.
- Es können keine zusätzlichen Geräte zwischen den Kern-FlexPod-Komponenten angeordnet werden.

Uplink-Verbindungen:

- Die Ports auf den NetApp Storage Controllern müssen mit den Switches der Cisco Nexus 5000, 7000 oder 9000 Serie verbunden sein, um virtuelle Port-Kanäle (vPCs) zu unterstützen.
- VPCs sind von den Cisco Switches der Serie Nexus 5000, 7000 oder 9000 zu den NetApp Storage Controllern erforderlich.
- VPCs sind erforderlich für Cisco Switches der Nexus 5000, 7000 oder 9000 Serie zu Fabric Interconnects.
- Für einen vPC sind mindestens zwei Verbindungen erforderlich. Die Anzahl der Verbindungen innerhalb eines vPC kann abhängig von der Applikationslast und den Performance-Anforderungen erhöht werden.

Direkte Verbindungen:

- NetApp Storage Controller Ports, die direkt mit Fabric Interconnects verbunden sind, können gruppiert werden, um einen Port Channel zu unterstützen. VPC wird für diese Konfiguration nicht unterstützt.
- Für End-to-End FCoE-Designs werden FCoE-Port-Channel empfohlen.

SAN Booting:

- FlexPod Lösungen wurden auf eine SAN Boot-Architektur mit iSCSI-, FC- oder FCoE-Protokollen ausgerichtet. Durch die Verwendung von Boot-from-SAN-Technologien wird die flexibelste Konfiguration für die Datacenter-Infrastruktur erzielt, sodass die umfassenden Funktionen, die innerhalb jeder Infrastrukturkomponente zur Verfügung stehen, ermöglicht werden. Obwohl das Booten über SAN die effizienteste Konfiguration ist, ist das Booten über lokalen Server Storage eine gültige und unterstützte Konfiguration.
- SAN-Boot über FC-NVME wird nicht unterstützt.

Andere Anforderungen

Eine FlexPod Architektur verfügt über die folgenden zusätzlichen Anforderungen bezüglich Interoperabilität und Support:

- Alle Hardware- und Software-Komponenten müssen auf der NetApp aufgeführt und unterstützt werden "IMT", Das "Cisco UCS Hardware- und Software-Kompatibilitätsliste"Und das Cisco UCS Hardware and

Software Interoperability Matrix Tool.

- Für alle Geräte sind gültige Support-Verträge erforderlich, darunter:
  - Smart Net Total Care (SmartNet)-Support für Cisco-Geräte
  - SupportEdge Advisor oder SupportEdge Premium Support für NetApp Systeme
- Relevante Verkaufsmerkmale des Verkaufsauftrags zur Unterstützung:
  - FlexPod Berechtigungen
  - FlexPod Lösungs-Supportberechtigungen

Weitere Informationen finden Sie im NetApp "IMT".

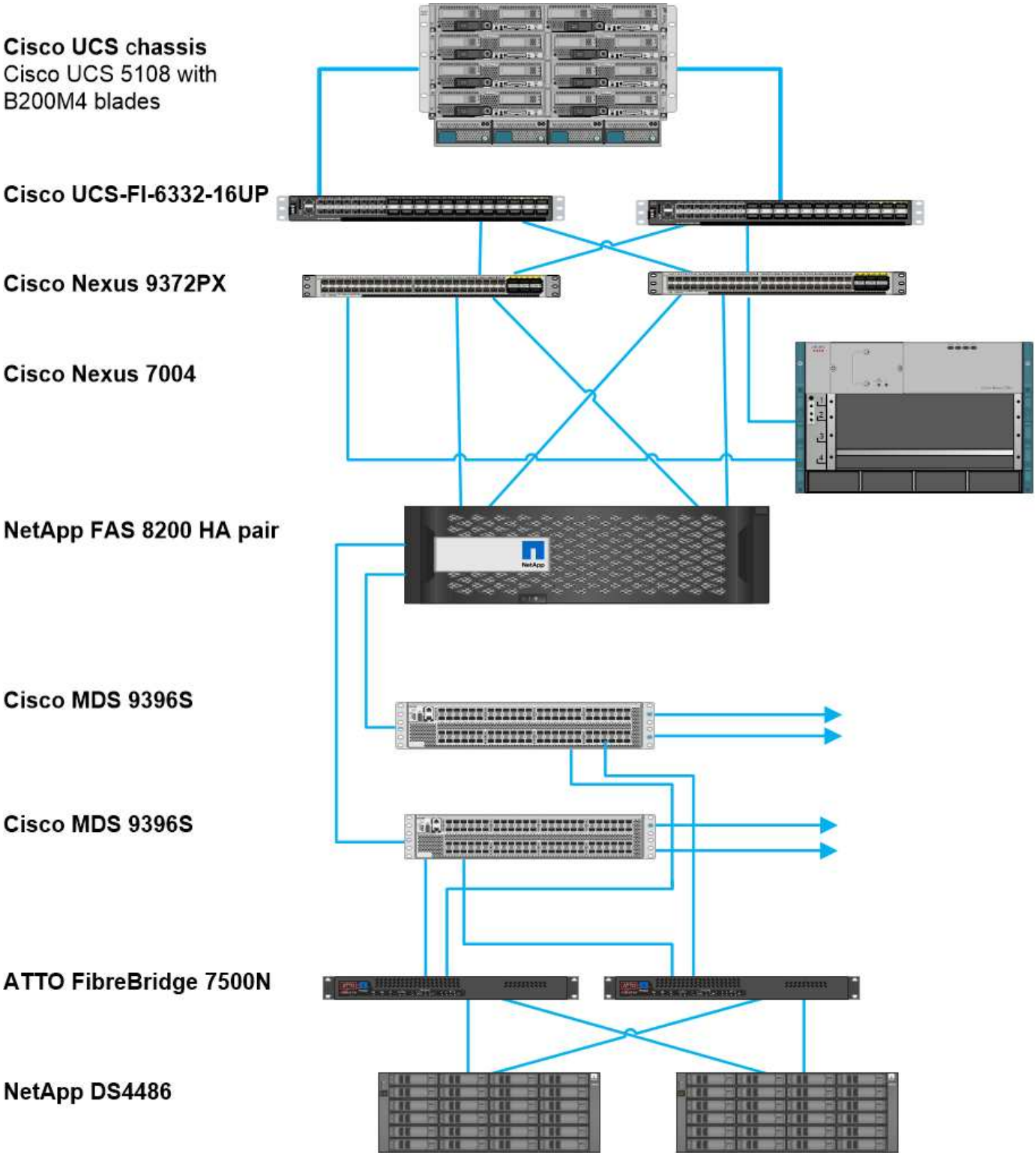
Optionale Funktionen

NetApp unterstützt mehrere optionale Komponenten, um FlexPod Datacenter-Architekturen noch weiter zu verbessern. Optionale Komponenten werden in den folgenden Abschnitten beschrieben.

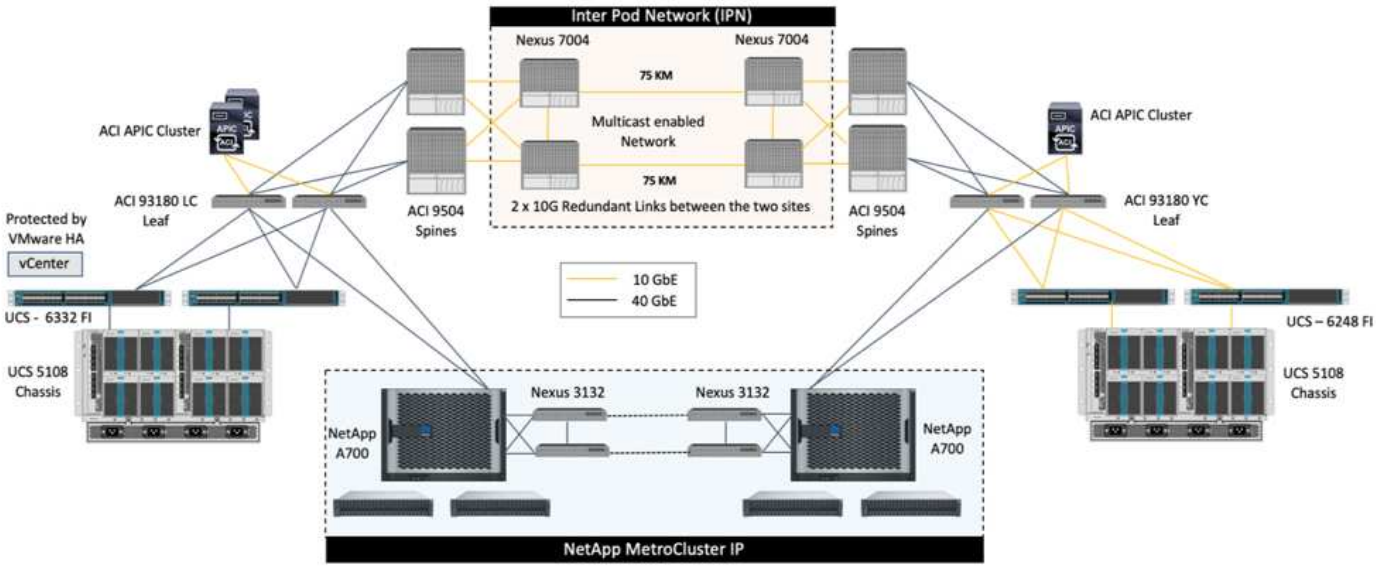
MetroCluster

FlexPod unterstützt beide Varianten der NetApp MetroCluster Software für durchgängige Verfügbarkeit in Cluster-Konfigurationen mit zwei oder vier Nodes. MetroCluster bietet synchrone Replizierung für kritische Workloads. Es ist eine Konfiguration mit zwei Standorten erforderlich, die mit Cisco Switching verbunden ist. Die maximal unterstützte Entfernung zwischen den Standorten beträgt etwa 186 km für MetroCluster FC und beträgt für MetroCluster IP ca. 435 km. Die folgenden Abbildungen veranschaulichen ein FlexPod Datacenter mit NetApp MetroCluster Architektur und FlexPod Datacenter mit NetApp MetroCluster IP Architektur.

Die folgende Abbildung zeigt die Architektur von FlexPod Datacenter mit NetApp MetroCluster.

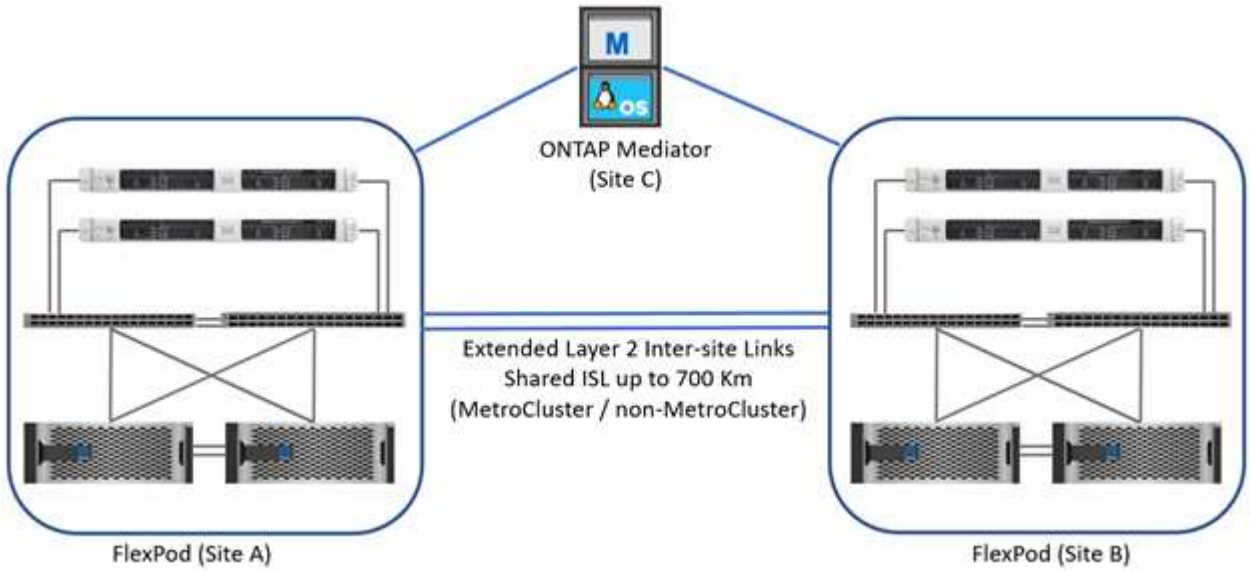


Folgende Abbildung zeigt die FlexPod Datacenter mit NetApp MetroCluster IP Architektur:



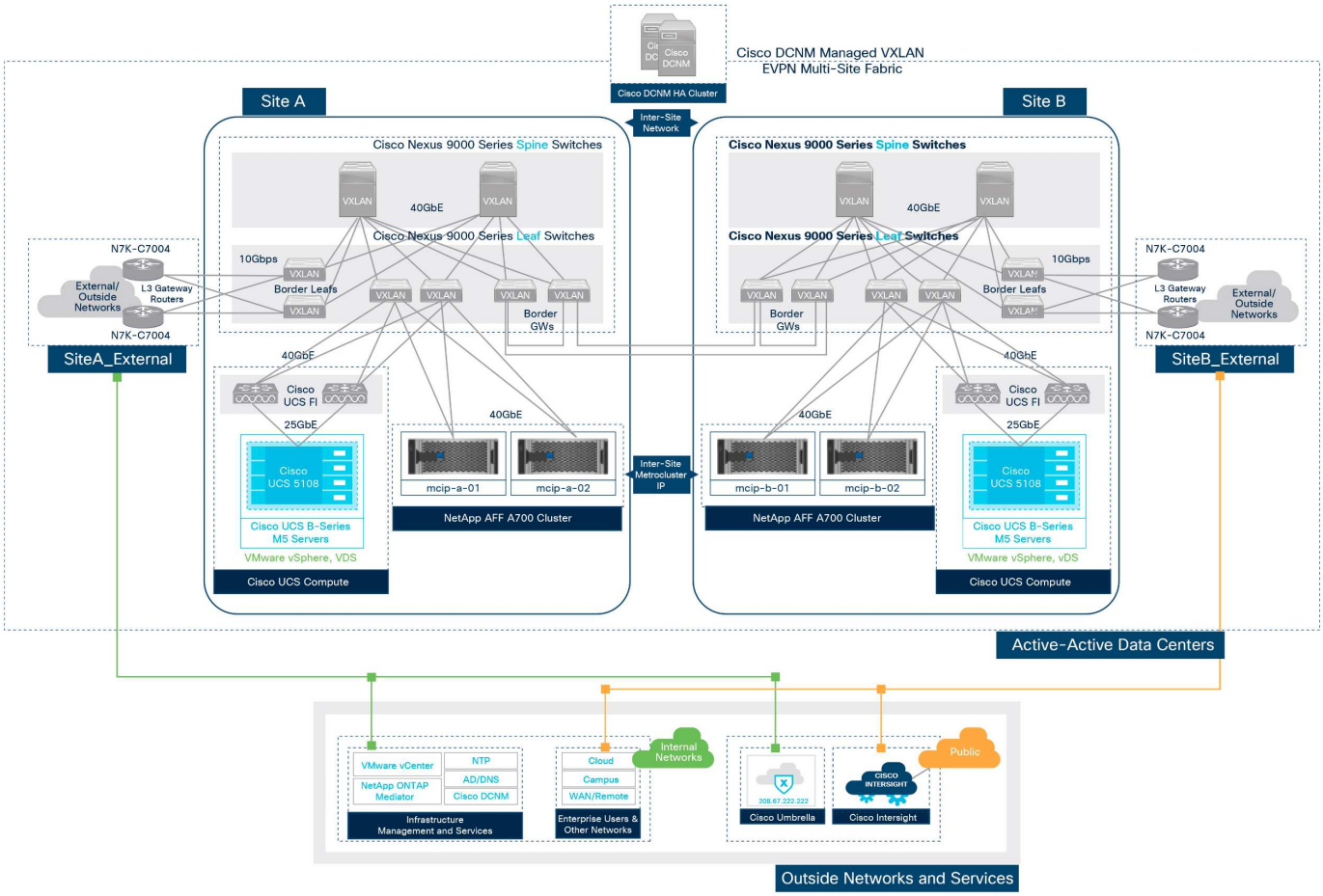
Ab ONTAP 9.8 kann ONTAP Mediator an einem dritten Standort implementiert werden, um die MetroCluster IP Lösung zu überwachen und bei einem Standortausfall eine automatisierte ungeplante Umschaltung zu ermöglichen.

Bei der Implementierung einer FlexPod MetroCluster IP-Lösung mit einer erweiterten Site-to-Site-Konnektivität zwischen Schicht und 2 können Sie Kosteneinsparungen erzielen, indem Sie ISL freigeben und FlexPod Switches als MetroCluster-konforme IP-Switches verwenden, wenn die Netzwerkbandbreite und die Switches den in der folgenden Abbildung dargestellten Anforderungen entsprechen. Zeigt die FlexPod MetroCluster IP-Lösung mit ISL-Freigabe und konformen Switches.

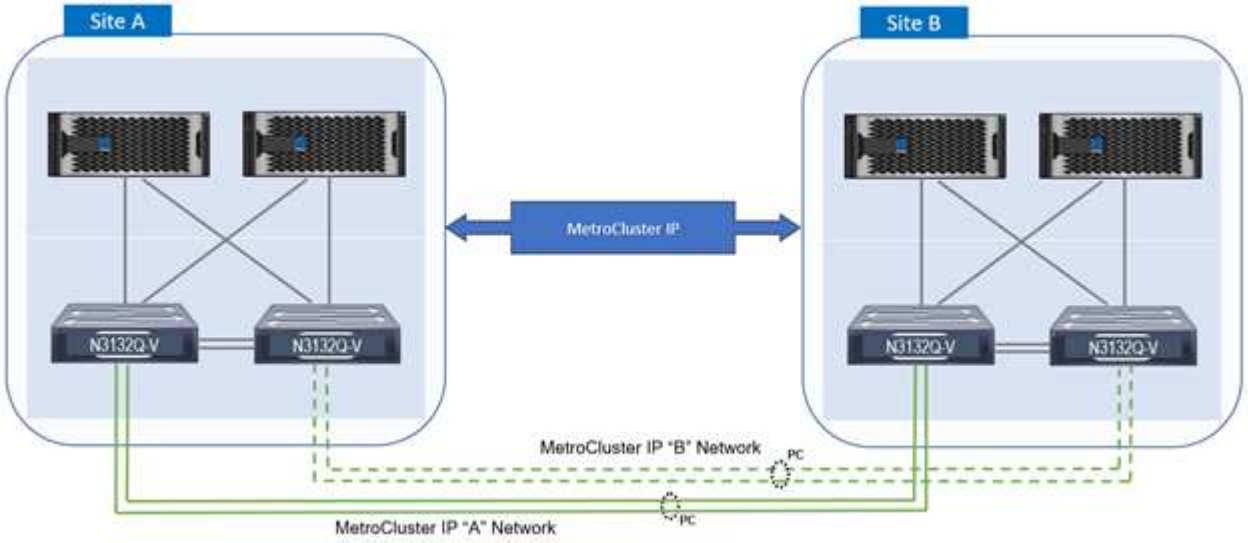


In den folgenden beiden Abbildungen wird das VXLAN Multi-Site Fabric und das MetroCluster IP Storage Fabric für eine FlexPod MetroCluster IP-Lösung mit VXLAN Multi-Site Fabric-Implementierung dargestellt.

- VXLAN-Multi-Site Fabric für FlexPod MetroCluster IP-Lösung



- MetroCluster IP Storage Fabric für FlexPod MetroCluster IP-Lösung



End-to-End FC-NVMe

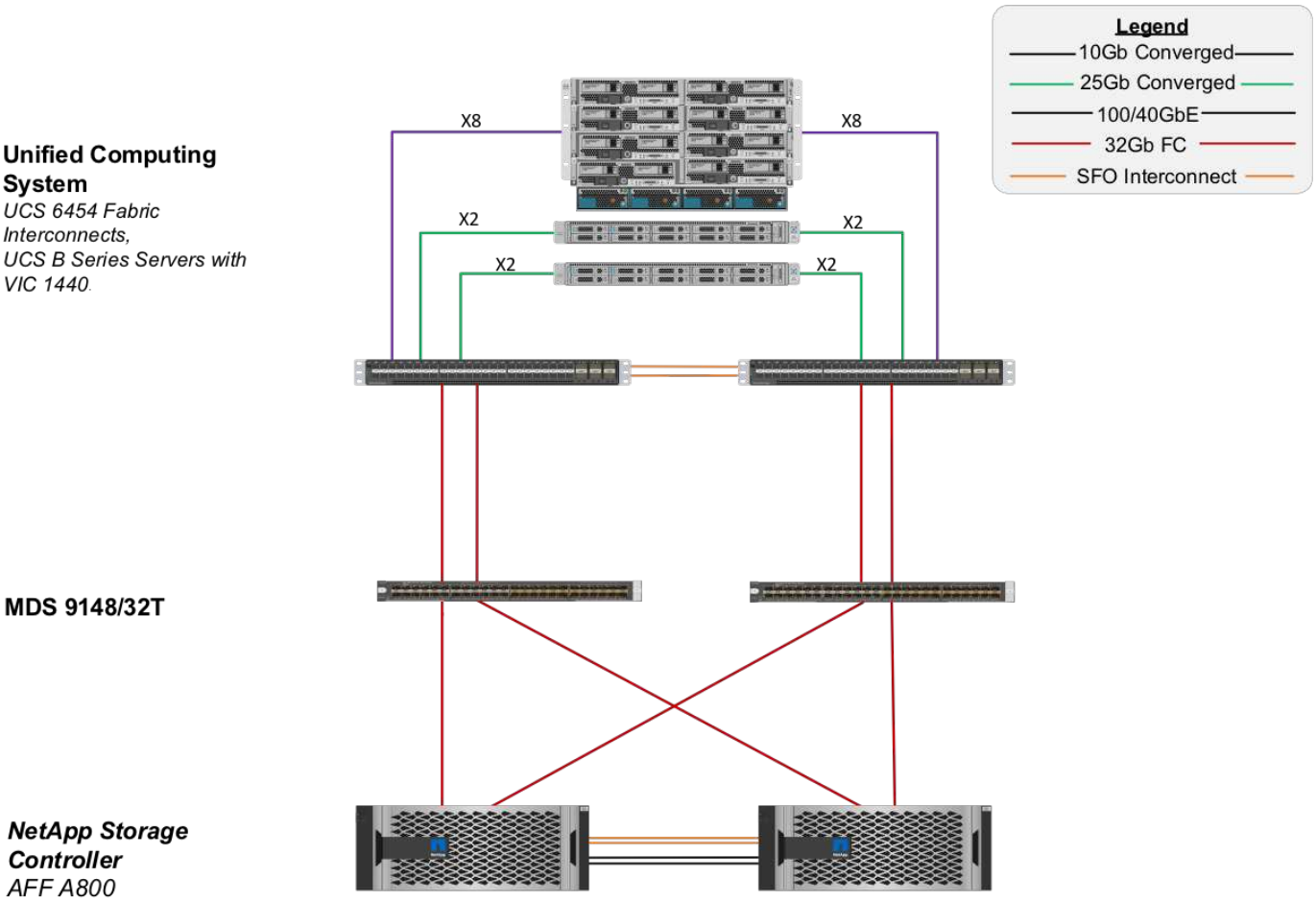
Mit einem umfassenden FC-NVMe wird die vorhandene SAN-Infrastruktur eines Kunden für Echtzeitapplikationen nahtlos erweitert und gleichzeitig höhere IOPS-Werte und einen höheren Durchsatz bei niedrigerer Latenz bereitgestellt.

Eine vorhandene 32-Gbit-FC-SAN-Übertragung kann zur gleichzeitigen Übertragung von NVMe und SCSI-Workloads verwendet werden.

Die folgende Abbildung zeigt das FlexPod Datacenter für FC mit Cisco MDS.

Weitere Informationen über die FlexPod Konfigurationen und Performance-Vorteile finden Sie unter "Whitepaper: End-to-End-NVMe für FlexPod"

Weitere Informationen zur ONTAP-Implementierung finden Sie unter "TR-4684: Implementieren und Konfigurieren moderner SANs mit NVMe".



FC SAN-Boot über Cisco MDS

Zur Erhöhung der Skalierbarkeit durch ein dediziertes SAN-Netzwerk unterstützt FlexPod FC über Cisco MDS Switches und Nexus Switches mit FC-Unterstützung, wie beispielsweise Cisco Nexus 93108TC-FX. Die FC-SAN-Boot-Option über Cisco MDS hat folgende Lizenzierungs- und Hardwareanforderungen:

- Mindestens zwei FC-Ports pro NetApp Storage Controller, ein Port pro SAN-Fabric
- Eine FC-Lizenz auf jedem NetApp Storage Controller
- Cisco MDS-Switches und Firmware-Versionen, die von NetApp unterstützt werden "IMT"

Weitere Anleitungen zu einem MDS-basierten Design finden Sie im CVD "FlexPod Datacenter mit VMware vSphere 6.7U1 Fibre Channel und iSCSI Deployment Guide".

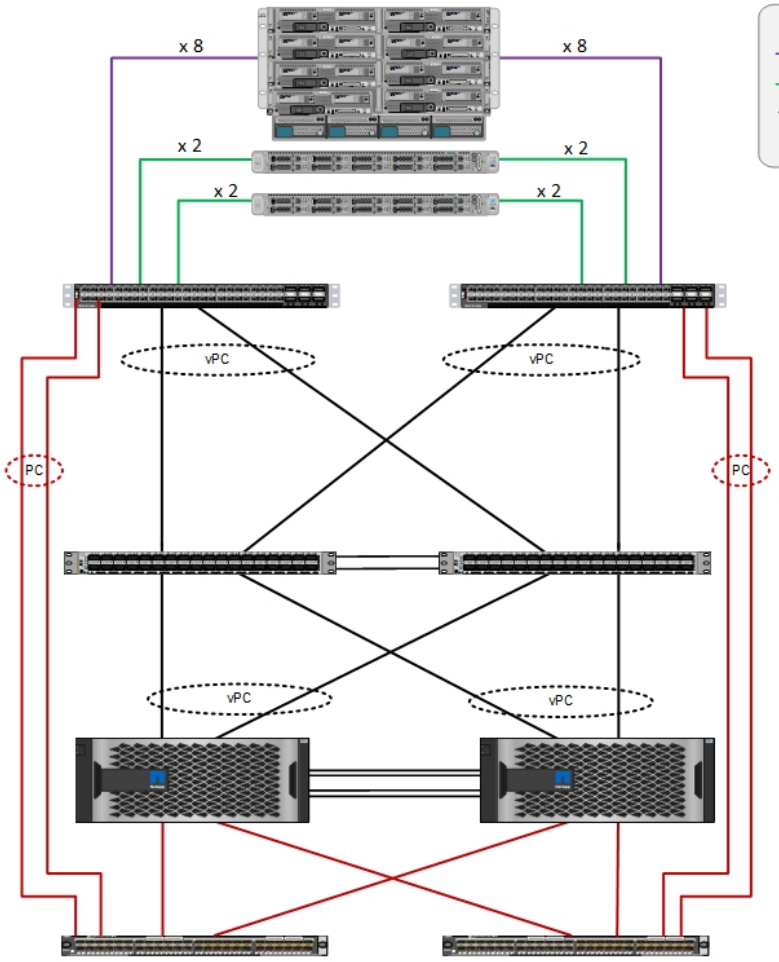
Die folgenden Abbildungen zeigen ein Beispiel für das FlexPod Datacenter für FC mit MDS-Konnektivität und das FlexPod Datacenter für FC mit Cisco Nexus 93180YC-FX.

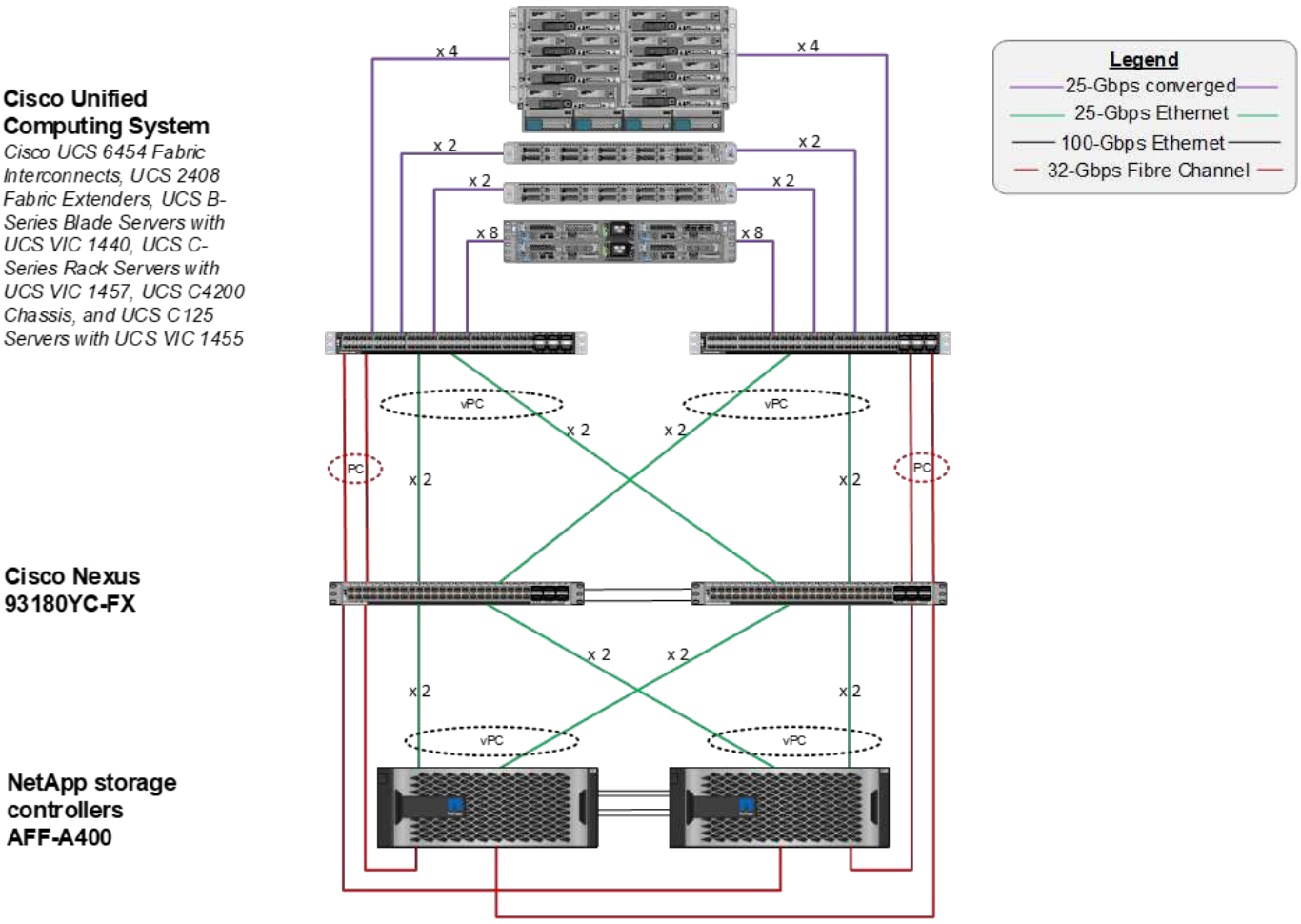
Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457

Cisco Nexus 9336C-FX2

NetApp storage controllers AFF-A800

Cisco MDS 9148T or 9132T switch





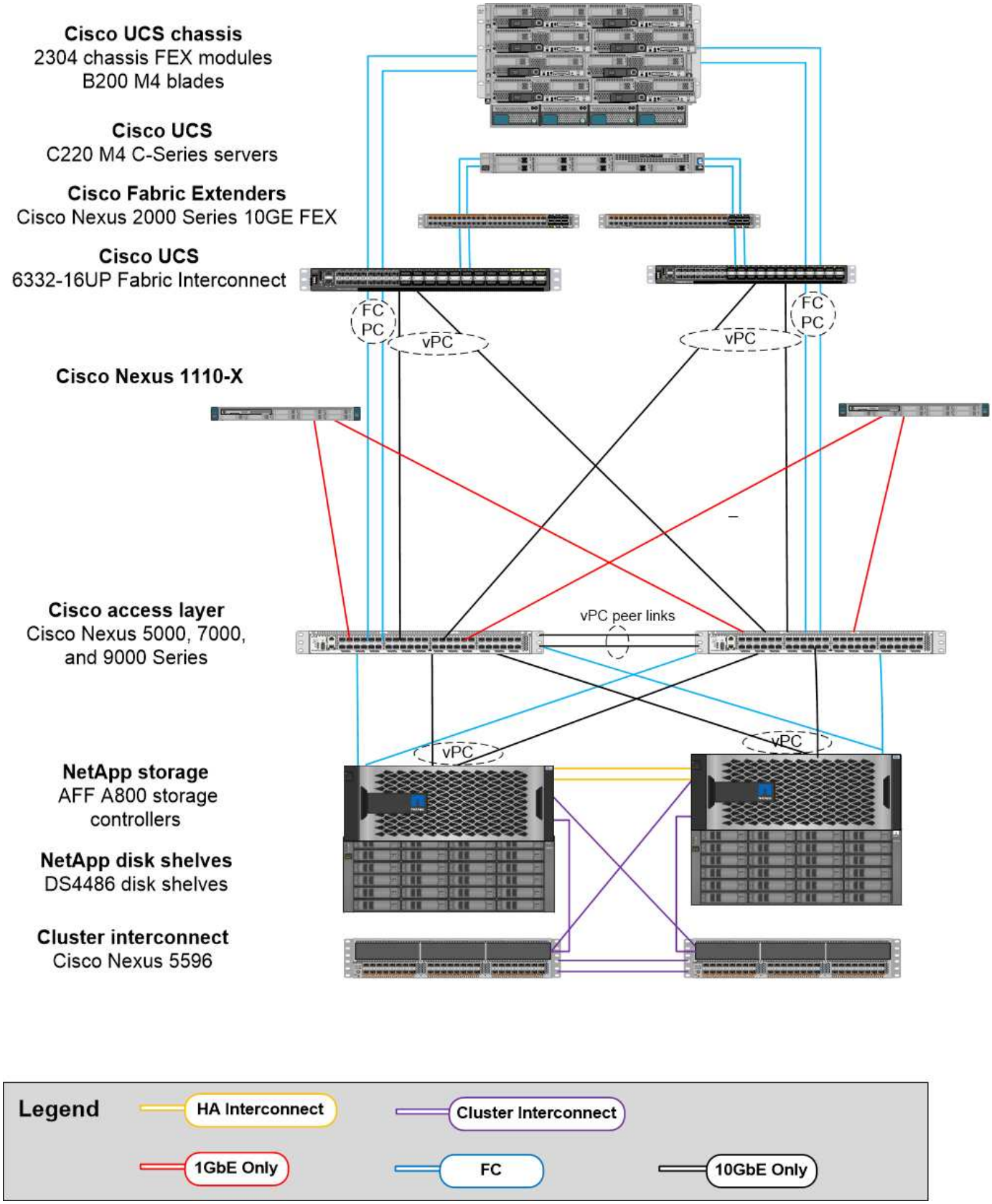
FC SAN booten mit Cisco Nexus

Der klassische FC-SAN-Boot-Service erfüllt folgende Lizenzierungs- und Hardwareanforderungen:

- Wenn FC-Zoning auf dem Cisco Nexus 5000 Series Switch ausgeführt wird, ist eine Lizenz für das Storage Protocols Service Package für die Switches der Cisco Nexus 5000 Serie (FC_FEATURES_PKG) erforderlich.
- Wenn FC Zoning auf dem Cisco Nexus 5000 Series Switch ausgeführt wird, sind SAN-Links zwischen dem Fabric Interconnect und dem Cisco Nexus 5000 Series Switch erforderlich. Für zusätzliche Redundanz werden SAN-Port-Kanäle zwischen den Links empfohlen.
- Für die Cisco Nexus 5010, 5020 und 5548P Switches ist ein separates FC- oder Universal Port-Modul (UP) erforderlich, um mit dem Cisco UCS Fabric Interconnect und mit dem NetApp Storage Controller verbunden zu werden.
- Für die Cisco Nexus 93180YC-FX ist eine FC-Funktionslizenz erforderlich, die die FC-Aktivierung ermöglicht.
- Jeder NetApp Storage-Controller benötigt für Konnektivität mindestens zwei 8/16/32-GB-FC-Ports.
- Auf dem NetApp Storage Controller ist eine FC-Lizenz erforderlich.

Die Verwendung der Switches der Cisco Nexus 7000 oder 9000 Familie schließt die Verwendung des herkömmlichen FC aus, es sei denn, FC Zoning wird im Fabric Interconnect ausgeführt. In diesem Fall werden SAN-Uplinks zum Switch nicht unterstützt.

In der folgenden Abbildung ist eine Konfiguration der FC-Konnektivität dargestellt.



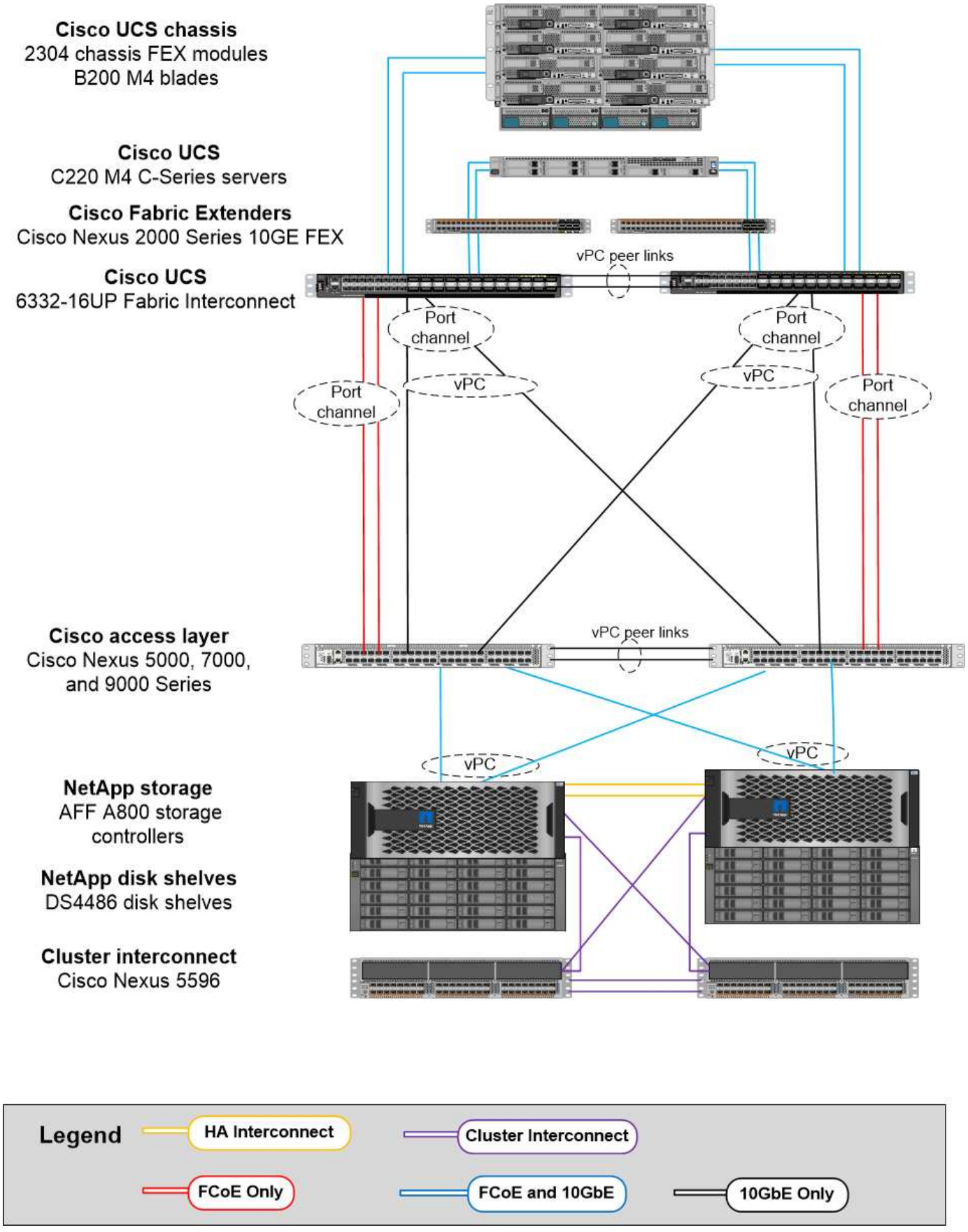
Bootsoption für FCoE SAN

Das Booten der FCoE SAN-Option umfasst die folgenden Lizenzierungs- und Hardwareanforderungen:

- Wenn das FC Zoning auf dem Switch ausgeführt wird, ist eine Lizenz für das Storage Protocols Service Package für die Switches der Cisco Nexus 5000 oder 7000 Serie (`FC_FEATURES_PKG`) Ist erforderlich.
- Wenn auf dem Switch FC-Zoning durchgeführt wird, sind FCoE-Uplinks zwischen dem Fabric Interconnect und den Switches der Cisco Nexus 5000 oder 7000 Serie erforderlich. Für zusätzliche Redundanz werden FCoE-Port-Kanäle zwischen den Links ebenfalls empfohlen.
- Jeder NetApp Storage Controller benötigt mindestens eine UTA-Zusatzkarte (Dual Port Unified Target Adapter) für FCoE-Konnektivität, es sei denn, integrierte UTA2-Ports (Unified Target Adapter 2) sind vorhanden.
- Für diese Option ist eine FC-Lizenz auf dem NetApp Storage Controller erforderlich.
- Wenn Sie die Switches der Cisco Nexus 7000 Serie und FC Zoning auf dem Switch verwenden, ist eine Karte erforderlich, die FCoE unterstützt.

> Durch die Verwendung der Switches der Cisco Nexus 9000 Serie ist FCoE ausgeschlossen, es sei denn, FC Zoning wird im Fabric Interconnect ausgeführt und der Storage ist mit den Fabric Interconnects mit Appliance-Ports verbunden. In diesem Fall werden FCoE-Uplinks zum Switch nicht unterstützt.

Die folgende Abbildung zeigt ein Szenario des FCoE-Startens.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
Port channel
Port channel
vPC
vPC
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

ISCSI-Boot-Option

Die iSCSI-Startoption umfasst die folgenden Lizenzierungs- und Hardwareanforderungen:

- Es ist eine iSCSI-Lizenz auf dem NetApp Storage Controller erforderlich.
- Im Cisco UCS Server, der iSCSI-Boot kann, ist ein Adapter erforderlich.
- Es ist ein 2-Port 10 Gbit/s Ethernet Adapter auf dem NetApp Storage Controller erforderlich.

Die folgende Abbildung zeigt eine reine Ethernet-Konfiguration, die über iSCSI gestartet wird.

Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades

Cisco UCS
C220 M4 C-Series servers

Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX

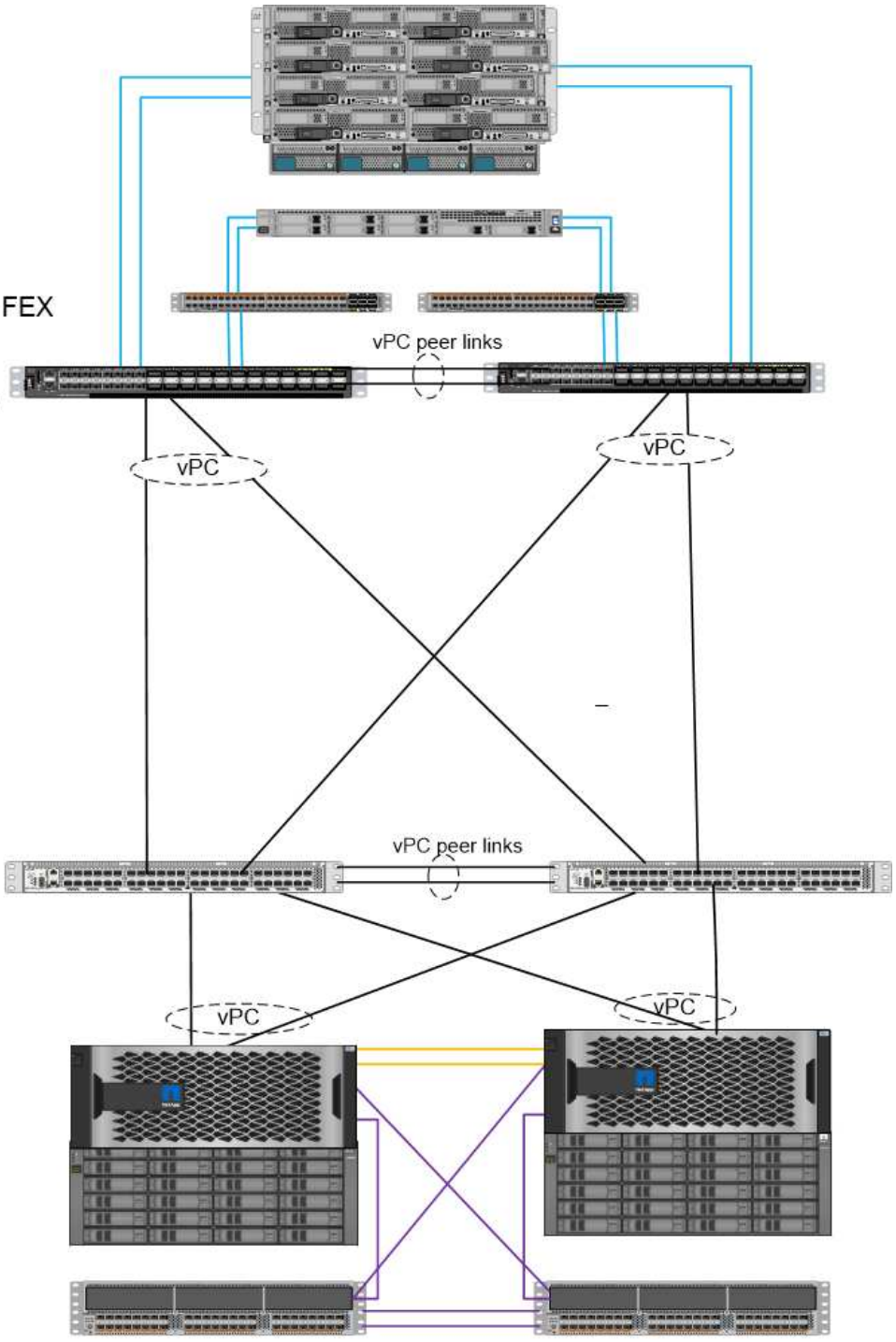
Cisco UCS
6332-16UP Fabric Interconnect

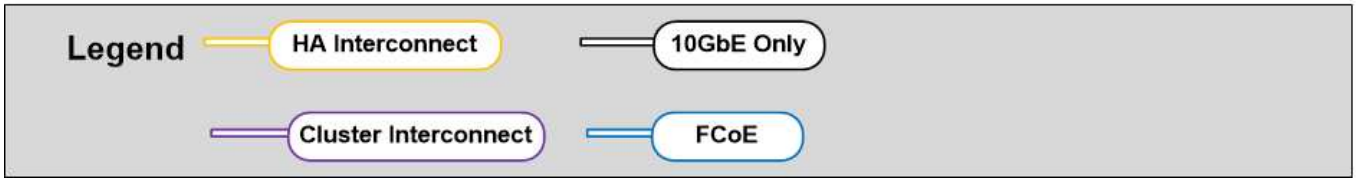
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series

NetApp storage
AFF A800 storage controllers

NetApp disk shelves
DS4486 Disk shelves

Cluster Interconnect
Cisco Nexus 5596





Cisco UCS Direktverbindung zu NetApp Storage

NetApp AFF und FAS Controller können ohne Upstream SAN Switch direkt mit den Cisco UCS Fabric Interconnects verbunden werden.

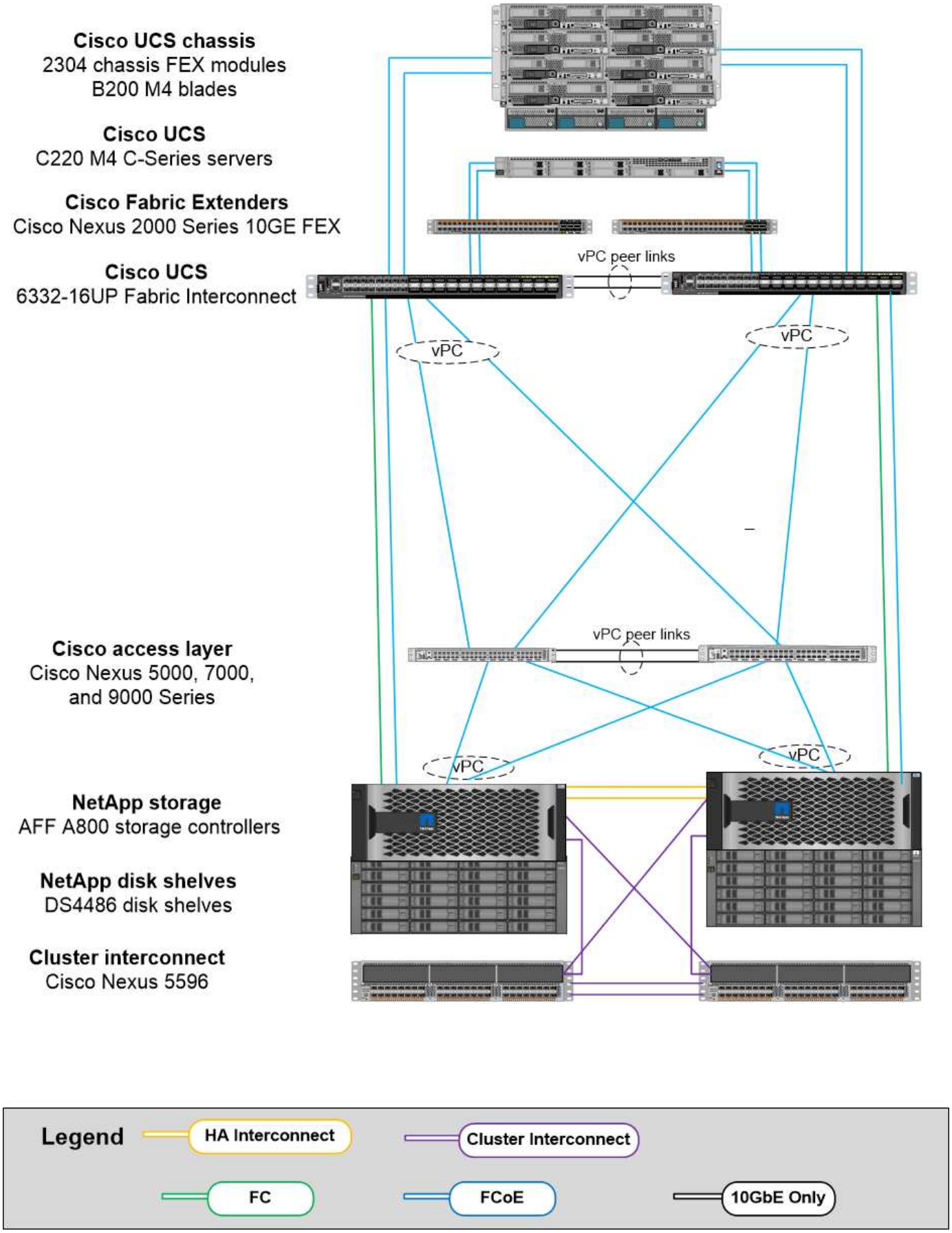
Vier Cisco UCS Port-Typen können zur direkten Verbindung zu NetApp Storage verwendet werden:

- **Storage FC-Port.** Verbinden Sie diesen Port direkt mit einem FC-Port auf NetApp Storage.
- **Storage-FCoE-Port.** Verbinden Sie diesen Port direkt mit einem FCoE-Port auf NetApp Storage.
- **Appliance-Port.** Verbinden Sie diesen Port direkt mit einem 10-GbE-Port auf NetApp Storage.
- **Unified Storage Port.** diesen Port direkt mit einer NetApp UTA verbinden.

Die Lizenz- und Hardwareanforderungen lauten wie folgt:

- Auf dem NetApp Storage Controller ist eine Protokolllizenz erforderlich.
- Auf dem Server ist ein Cisco UCS Adapter (Initiator) erforderlich. Eine Liste der unterstützten Cisco UCS-Adapter finden Sie im NetApp "IMT".
- Auf dem NetApp Storage Controller ist ein Target-Adapter erforderlich.

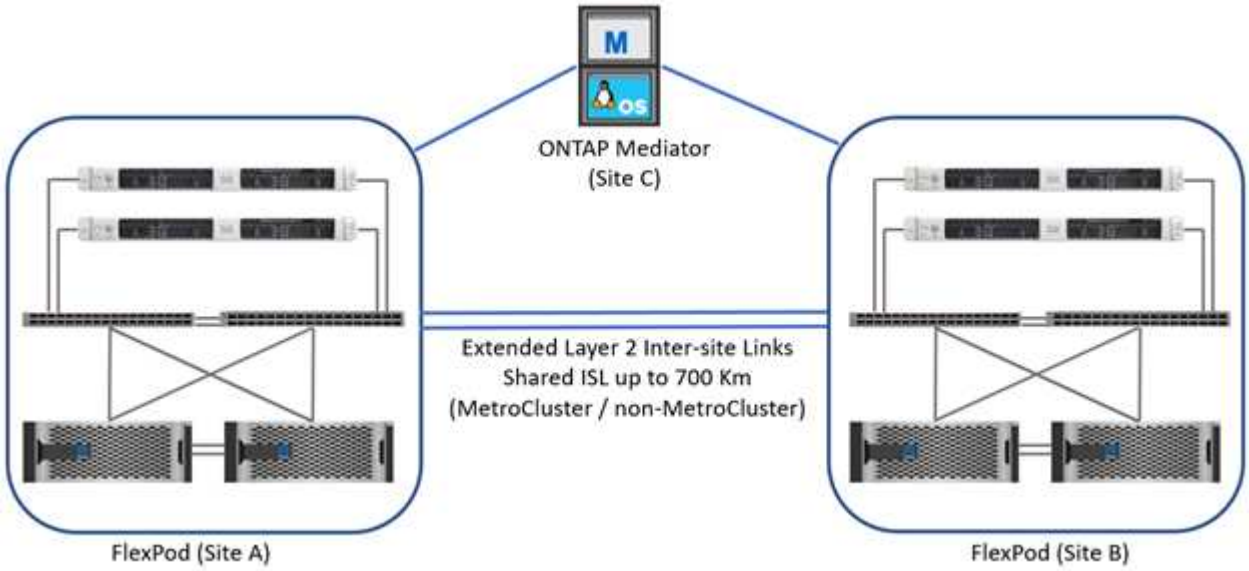
In der folgenden Abbildung ist eine Konfiguration für die Direktverbindung per FC dargestellt.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

Hinweise:

- Cisco UCS ist im FC-Switching-Modus konfiguriert.
- Die FCoE-Ports vom Ziel bis zu Fabric Interconnects werden als FCoE-Storage-Ports konfiguriert.
- FC-Ports vom Ziel bis zu Fabric Interconnects werden als FC-Storage-Ports konfiguriert.

Die folgende Abbildung zeigt eine iSCSI/Unified IP Direct-Connect-Konfiguration.



Hinweise:

- Cisco UCS ist im Ethernet Switching-Modus konfiguriert.
- ISCSI-Ports vom Ziel bis zu Fabric Interconnects werden als Ethernet Storage-Ports für iSCSI-Daten konfiguriert.
- Ethernet-Ports vom Ziel bis hin zu Fabric Interconnects werden als Ethernet Storage Ports für CIFS-/NFS-Daten konfiguriert.

Komponenten von Cisco

Cisco hat entscheidend zum Design und der Architektur von FlexPod beigetragen, die sowohl die Computing- als auch die Netzwerkebenen der Lösung abdeckt. In diesem Abschnitt werden die Optionen von Cisco UCS und Cisco Nexus für FlexPod beschrieben. FlexPod unterstützt sowohl Cisco Server der UCS B-Serie als auch C-Serie.

Cisco UCS Fabric Interconnect-Optionen

In der FlexPod Architektur sind redundante Fabric Interconnects erforderlich. Wenn Sie einem Paar Fabric Interconnects mehrere Cisco UCS Gehäuse hinzufügen, beachten Sie, dass die maximale Anzahl an Gehäusen in einer Umgebung von einer Architektur und einem Port-Limit abhängig ist.

Die in der folgenden Tabelle aufgeführten Teilenummern gelten für die Basis-Fabric-Interconnects. Sie umfassen nicht die Netzteileinheit (PSU), SFP+, QSFP+ oder Erweiterungsmodule. Weitere Fabric Interconnects werden unterstützt, siehe "NetApp IMT" Für eine komplette Liste.

Cisco UCS Fabric Interconnect	Teilenummer	Technische Spezifikationen
Cisco UCS 6332UP	UCS-FI-6332-UP	"Cisco UCS 6332 Fabric Interconnect"
Cisco UCS 6454	UCS-FI-6454-U	"Cisco UCS 6454 Fabric Interconnect"

Cisco UCS 6454

Die Cisco UCS 6454 Serie bietet verlustfreie, latenzarme 10/25/40/100-GbE-Ethernet- und FCoE-Konnektivität sowie Unified Ports, die einen Ethernet- oder FC-Betrieb ermöglichen. Die 44 10/25-Gbit/s-Ports können als 10-Gbit/s- oder 25-Gbit/s-konvergentes Ethernet betrieben werden. 8 Ports sind einheitliche Ports, die bei FC mit 8/16/32 Gbit/s. betrieben werden können. Vier Ports arbeiten bei 1/10/25 Gbit/s für ältere Konnektivität, und sechs QSFP-Ports dienen als Uplink-Ports mit 40/100 Gbit/s oder Breakout-Ports. Mit NetApp Storage Controllern, die 100-Gbit/s-Adapter unterstützen, können Sie eine vollständige Netzwerkkonnektivität mit 100 Gbit/s herstellen. Informationen zu Adaptern und Plattformunterstützung finden Sie im "NetApp Hardware Universe".

Informationen zu Ports finden Sie im "Cisco UCS 6454 Fabric Interconnect" Datenblatt.

Technische Spezifikationen zu den 100-GB-QSFP-Datenmodulen finden Sie im "Datenblatt zu Cisco 100GBASE QSFP Modulen".

Cisco UCS B-Series Gehäuse-Option

Zur Verwendung von Cisco UCS B-Series Blades müssen Sie über ein Cisco UCS B-Series Gehäuse verfügen. In der folgenden Tabelle wird die Gehäuseoption Cisco UCS BSeries beschrieben.

Gehäuse der Cisco UCS B-Serie	Teilenummer	Technische Spezifikationen
Cisco UCS 5108	N20-C6508	"Blade Server-Chassis der Cisco UCS 5100-Serie"

Jedes Cisco UCS 5108 Blade Chassis muss über zwei IOMs der Cisco UCS 2200/2300/2400 Serie verfügen, um redundante Konnektivität zu den Fabric Interconnects bereitzustellen.

Blade Server-Optionen der Cisco UCS B-Serie

Cisco UCS Blade Server der B-Serie sind in verschiedenen Varianten mit halber Breite und voller Breite verfügbar, wobei verschiedene CPU-, Arbeitsspeicher- und I/O-Optionen verfügbar sind. Die in der folgenden Tabelle aufgeführten Teilenummern beziehen sich auf den Basisserver. Sie enthalten keine CPU, Arbeitsspeicher, Laufwerke oder Mezzanine-Adapterkarten. Es sind mehrere Konfigurationsoptionen verfügbar, die in der FlexPod-Architektur unterstützt werden.

Cisco UCS Blade der B-Serie	Teilenummer	Technische Spezifikationen
CISCO UCS B200 M6	UCSB-B200-M6	"Cisco UCS B200 M6 Blade Server"

Ältere Generationen von Blades der Cisco UCS B-Serie können in der FlexPod Architektur verwendet werden, sofern sie auf dem unterstützt werden "Cisco UCS Hardware- und Software-Kompatibilitätsliste". Die Cisco UCS Blade Server der B-Serie müssen zudem über einen gültigen SmartNet-Supportvertrag verfügen.

Cisco UCS X-Serie: Gehäuseoption

Zur Verwendung der Computing-Nodes der Cisco UCS X-Serie müssen Sie ein Chassis der Cisco UCS X-Serie haben. In der folgenden Tabelle wird die Gehäuseoption des Cisco UCS X-Series beschrieben.

Cisco UCS X-Serie Blade	Teilenummer	Technische Spezifikationen
Cisco UCS 9508 M6	UCSD-9508	"Cisco UCX9508 Gehäuse der X-Serie"

Jedes Cisco UCS 9508 Chassis muss über zwei Cisco UCS 9108 Intelligent Fabric Modules (IFMS) verfügen, um redundante Konnektivität zu den Fabric Interconnects bereitzustellen.

Optionen für Cisco UCS X-Series Geräte

Cisco UCS X-Series Computing-Nodes stehen mit unterschiedlichen CPU-, Speicher- und I/O-Optionen zur Verfügung. Die in der folgenden Tabelle aufgeführten Teilenummern gelten für den Basis-Node. Sie enthalten keine CPU, Arbeitsspeicher, Laufwerke oder Mezzanine-Adapterkarten. Es sind mehrere Konfigurationsoptionen verfügbar, die in der FlexPod-Architektur unterstützt werden.

Cisco UCS X-Serie Computing-Nodes	Teilenummer	Technische Spezifikationen
Cisco UCS X210c M6	UCSD-210C-M6	"Cisco UCS X210c M6 Computing-Node"

Rack Server-Optionen für Cisco UCS C-Serie

Cisco UCS C-Series Rack Server sind in einer und zwei Höheneinheiten (HE) erhältlich und bieten verschiedene CPU-, Arbeitsspeicher- und I/O-Optionen. Die Teilenummern, die in der zweiten Tabelle unten aufgeführt sind, beziehen sich auf den Basisserver. Sie umfassen keine CPUs, Arbeitsspeicher, Laufwerke, PCIe-Karten (Peripheral Component Interconnect Express) oder den Cisco Fabric Extender. Es sind mehrere Konfigurationsoptionen verfügbar, die in der FlexPod-Architektur unterstützt werden.

In der folgenden Tabelle werden die Optionen für Cisco UCS Rack Server der C-Serie aufgeführt.

Rack Server der Cisco UCS C-Serie	Teilenummer	Technische Spezifikationen
CISCO UCS C220 M6	UCSC-C220-M6	"Cisco UCS C220 M6 Rack Server"
CISCO UCS C225 M6	UCSC-C225-M6	"Cisco UCS C225 M6 Rack Server"
CISCO UCS C240 M6	UCSC-C240-M6	"Cisco UCS C240 M6 Rack Server"
CISCO UCS C245 M6	UCSC-C245-M6	"Cisco UCS C245 M6 Rack Server"

Ältere Generationen von Cisco UCS C-Series Servern können in der FlexPod Architektur verwendet werden, sofern sie auf der unterstützt werden "Cisco UCS Hardware- und Software-Kompatibilitätsliste". Die Cisco Server der UCS C-Serie müssen zudem über einen gültigen SmartNet-Supportvertrag verfügen.

Switch-Optionen für die Cisco Nexus 5000 Serie

In der FlexPod Architektur sind redundante Switches der Cisco Nexus 5000, 7000 oder 9000 Serie erforderlich. Die in der nachstehenden Tabelle aufgeführten Teilenummern gelten für die Gehäuse der Cisco Nexus 5000 Serie. Dabei sind keine SFP-Module, kein Add-on FC- oder Ethernet-Module enthalten.

Switch der Cisco Nexus 5000-Serie	Teilenummer	Technische Spezifikationen
Cisco Nexus 56128P	N5K-C56128P	"Switches Der Cisco Nexus 5600 Plattform"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Cisco Nexus 5548 und 5596 Switches"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Switch-Optionen für die Cisco Nexus 7000 Serie

In der FlexPod Architektur sind redundante Switches der Cisco Nexus 5000, 7000 oder 9000 Serie erforderlich. Die in der nachstehenden Tabelle aufgeführten Teilenummern gelten für die Gehäuse der Cisco Nexus 7000 Serie. SFP-Module, Line Cards und Netzteile sind nicht enthalten, aber Lüftereinschübe.

Switch Der Cisco Nexus 7000-Serie	Teilenummer	Technische Spezifikationen
Cisco Nexus 7004	N7K-C7004	"Cisco Nexus Switch Mit 7000 4 Steckplätzen"
Cisco Nexus 7009	N7K-C7009	"Cisco Nexus Switch Mit 7000 9 Steckplätzen"
Cisco Nexus 7702	N7K-C7702	"Cisco Nexus 7700 Switch Mit 2 Steckplätzen"
Cisco Nexus 7706	N77-C7706	"Cisco Nexus Switch Mit 7700 6 Steckplätzen"

Switch-Optionen für die Cisco Nexus 9000 Serie

In der FlexPod Architektur sind redundante Switches der Cisco Nexus 5000, 7000 oder 9000 Serie erforderlich. Die in der unten stehenden Tabelle aufgeführten Teilenummern gelten für Gehäuse der Cisco Nexus 9000 Serie. SFP-Module und Ethernet-Module sind nicht enthalten.

Switch Der Cisco Nexus 9000-Serie	Teilenummer	Technische Spezifikationen
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Switches Der Cisco Nexus 9300-Serie"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ ACI Wirbelsäule	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	
Cisco Nexus 92304QC	N9K-C92304QC	"Switches Der Cisco Nexus 9200-Serie"
Cisco Nexus 9236C	N9K-9236C	

Einige Switches der Cisco Nexus 9000-Serie verfügen über zusätzliche Varianten. Diese Varianten werden im Rahmen der FlexPod Lösung unterstützt. Die vollständige Liste der Switches der Cisco Nexus 9000-Serie finden Sie unter "Switches Der Cisco Nexus 9000-Serie" Auf der Cisco Website zu finden.

Cisco APIC-Optionen

Bei der Implementierung von Cisco ACI müssen zusätzlich zu den Elementen im Abschnitt die drei Cisco APICs konfiguriert werden "Switches Der Cisco Nexus 9000-Serie". Weitere Informationen zu den Cisco APIC-Größen finden Sie im "Datenblatt Zu Cisco Application Centric Infrastructure."

Weitere Informationen zu APIC-Produktspezifikationen finden Sie in Tabelle 1 bis Tabelle 3 auf der "Datenblatt Zum Cisco Application Policy Infrastructure Controller".

Cisco Nexus Fabric Extender Optionen

Für große FlexPod-Architekturen, die Server der C-Serie nutzen, werden redundante rackmontierte FEXs der Cisco Nexus 2000-Serie empfohlen. In der folgenden Tabelle werden einige Cisco Nexus FEX-Optionen beschrieben. Alternative FEX-Modelle werden ebenfalls unterstützt. Weitere Informationen finden Sie im "Cisco UCS Hardware- und Software-Kompatibilitätsliste".

Cisco Nexus rackmontierter FEX	Teilenummer	Technische Spezifikationen
Cisco Nexus 2232PP	N2K-C2232PP	"Cisco Nexus 2000 Series Fabric Extender"
Cisco Nexus 2232TM-E	N2K-C2232TM-E	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Cisco Nexus 2300 Platform Fabric Extender"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E	N2K-C2348TQN2K-C2348TQ-E	

Cisco MDS Optionen

Cisco MDS Switches sind optionale Komponente in der FlexPod Architektur. Bei der Implementierung des Cisco MDS Switches für FC SAN sind redundante SAN Switch Fabrics erforderlich. In der folgenden Tabelle sind die Teilenummern und Details für einen Teil der unterstützten Cisco MDS-Switches aufgeführt. Siehe "NetApp IMT" Und "Cisco Hardware- und Software-Kompatibilitätsliste" Erhalten Sie eine vollständige Liste der unterstützten SAN Switches.

Switch der Cisco MDS 9000 Serie	Teilenummer	Beschreibung
Cisco MDS 9148T	DS-C9148T-24IK	"Switches der Cisco MDS 9100 Serie"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Switches der Cisco MDS 9300 Serie"

Cisco Software-Lizenzoptionen

Für die Aktivierung von Storage-Protokollen auf den Cisco Nexus Switches sind Lizenzen erforderlich. Die Switches der Cisco Nexus Serien 5000 und 7000 erfordern alle eine Storage-Services-Lizenz, um das FC- oder FCoE-Protokoll für SAN-Boot-Implementierungen zu aktivieren. Die Switches der Cisco Nexus 9000 Serie unterstützen momentan keine FC oder FCoE.

Die erforderlichen Lizenzen und die Teilenummern dieser Lizenzen variieren je nach den Optionen für die jeweilige Komponente der FlexPod Lösung. Beispielsweise variieren die Teilenummern für Softwarelizenzen je nach Anzahl der Ports und den Switches der Cisco Nexus 5000- oder 7000-Serie. Genaue Teilenummern können von Ihrem Vertriebsmitarbeiter angegeben werden. In der folgenden Tabelle sind die Cisco Software-Lizenzoptionen aufgeführt.

Cisco Softwarelizenzen	Teilenummer	Lizenzinformationen
Cisco Nexus 5500 Storage-Lizenz für 8, 48 und 96 Ports	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Lizenzierung der Cisco NX-OS-Softwarefunktionen"
Lizenz Für Cisco Nexus 5010/5020 Storage-Protokolle	N5010-SSK9/N5020-SSK9	
Lizenz Für Cisco Nexus 5600 Storage-Protokolle	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Cisco Nexus 7000 Storage Enterprise-Lizenz	N7K-SAN1K9	
Cisco Nexus 9000 Enterprise Services-Lizenz	N95-LAN1K9/N93-LAN1K9	

Cisco Support-Lizenzoptionen

Für alle Cisco Geräte in der FlexPod Architektur sind gültige SmartNet Support-Verträge erforderlich.

Die erforderlichen Lizenzen und die Teilenummern für diese Lizenzen müssen von Ihrem Vertriebsvertreter überprüft werden, da diese für verschiedene Produkte variieren können. In der folgenden Tabelle sind die Lizenzoptionen für den Cisco Support aufgeführt.

Cisco Support-Lizenzierung	Lizenzhandbuch
Smart Net Total Care Vor Ort Premium	"Cisco Smart Net Total Care Service"

Komponenten von NetApp

NetApp Storage-Controller bilden die Storage-Grundlage in der FlexPod-Architektur für Boot- und Applikationsdaten-Storage. NetApp Komponenten umfassen Storage Controller, Cluster Interconnect Switches, Laufwerke und Festplatten-Shelfs sowie Lizenzoptionen.

Optionen für NetApp Storage Controller

In der FlexPod Architektur sind redundante NetApp FAS-, AFF- oder AFF ASA-Controller erforderlich. Die Controller verwenden ONTAP Software. Wenn die Speicher-Controller bestellt werden, kann die bevorzugte Softwareversion auf die Controller vorgeladen werden. Für ONTAP wird ein komplettes Cluster bestellt. Ein vollständiger Cluster umfasst zwei Storage Controller-Paare und einen Cluster Interconnect (Switch oder ohne Switch).

Abhängig von der ausgewählten Storage-Plattform stehen verschiedene Optionen und Konfigurationen zur Verfügung. Details zu diesen zusätzlichen Komponenten finden Sie von Ihrem Ansprechpartner.

Die in der nachstehenden Tabelle aufgeführten Controller-Familien eignen sich für die Verwendung in einer FlexPod Datacenter-Lösung, da ihre Verbindung zu den Cisco Nexus-Switches nahtlos ist. Siehe "NetApp

Hardware Universe" Für bestimmte Kompatibilitätsdetails zu jedem Controller-Modell.

Storage Controller-Produktfamilie	Technische Spezifikationen
AFF A-Serie	"AFF A-Series - Dokumentation"
AFF ASA A-SERIES	"AFF ASA A-Series - Dokumentation"
FAS Serie	"Dokumentation der FAS Serie"

Optionen für Cluster-Interconnect-Switches

In der folgenden Tabelle werden die verfügbaren Nexus Cluster Interconnect Switches für FlexPod Architekturen aufgeführt. Darüber hinaus unterstützt FlexPod alle von ONTAP unterstützten Cluster-Switches auch ohne Cisco Switches, sofern diese mit der zu implementierenden ONTAP Version kompatibel sind. Siehe "NetApp Hardware Universe" Weitere Kompatibilitätsangaben für bestimmte Switch-Modelle.

Cluster-Interconnect-Switch	Technische Spezifikationen
Cisco Nexus 3132Q-V	"NetApp Dokumentation: Cisco Nexus 3132Q-V Switches"
Cisco Nexus 9336C-FX2	"NetApp Dokumentation: Cisco Nexus 9336C-FX2 Switches"

NetApp Platten-Shelf- und Laufwerksoptionen

Für alle Storage Controller ist mindestens ein NetApp Platten-Shelf erforderlich.

Der ausgewählte NetApp Shelf-Typ bestimmt, welche Laufwerkstypen in diesem Shelf verfügbar sind.

Alle Festplatten-Shelfs und Festplatten-Teilenummern können bei Ihrem Vertriebsmitarbeiter angegeben werden.

Weitere Informationen zu den unterstützten Laufwerken erhalten Sie über den Link NetApp Hardware Universe in der folgenden Tabelle, und wählen Sie dann unterstützte Laufwerke aus.

Festplatten-Shelf	Technische Spezifikationen
DS224C	"Festplatten-Shelfs und unterstützte Storage-Medien auf NetApp Hardware Universe"
DS212C	
DS460C	
NS224	

NetApp Software-Lizenzoptionen

In der folgenden Tabelle sind die NetApp Software-Lizenzoptionen für die FlexPod Datacenter-Architektur aufgeführt. NetApp Software ist auf Controller-Ebene des FAS und AFF lizenziert.

NetApp Softwarelizenzen	Teilenummer	Technische Spezifikationen
SW, komplette BNDL (Controller), -C	SW-8XXX-COMP-BNDL-C	"Produktbibliothek Von A–Z"
SW, ONTAP Essentials (Controller), -C	SW-8XXX-ONTAP9-C	

NetApp Support-Lizenzoptionen

Für die FlexPod Architektur sind NetApp SupportEdge Premium Lizenzen erforderlich. Die Teilenummern dieser Lizenzen variieren jedoch je nach den Optionen im FlexPod-Design. Beispielsweise unterscheiden sich die Teilenummern für die Software-Lizenzen, je nachdem, welchen FAS-Controller Sie wählen. Wenden Sie sich an Ihren Vertriebsmitarbeiter, um Informationen zu den genauen Teilenummern für einzelne Support-Lizenzen zu erhalten. Die folgende Tabelle zeigt ein Beispiel für eine SupportEdge-Lizenz.

NetApp Support-Lizenzierung	Teilenummer	Technische Spezifikationen
SupportEdge Premium 4 Stunden vor Ort – Monate: 36	CS-O2-4HR	"NetApp SupportEdge Premium"

Strom- und Verkabelungsanforderungen

Ein FlexPod Design erfüllt die Mindestanforderungen für Strom und Verkabelung.

Stromversorgung

Die Stromanforderungen für das FlexPod Datacenter unterscheiden sich je nach Installationsort der FlexPod Datacenter Konfiguration.

Weitere Informationen über die maximale Leistung, die benötigt wird, und weitere detaillierte Informationen zur Stromversorgung finden Sie in den technischen Spezifikationen für jede im Abschnitt aufgeführte Hardware-Komponente "Technische Spezifikationen und Referenzen: Hardware-Komponenten".

Detaillierte Informationen zur Stromversorgung von Cisco UCS finden Sie im "Cisco UCS – Stromversorgungsrechner".

Informationen zum Einschalten des NetApp Storage Controllers finden Sie im "NetApp Hardware Universe". Wählen Sie unter Plattformen die Storage-Plattform aus, die Sie für die Konfiguration verwenden möchten (FAS/V-Series oder AFF). Wählen Sie die ONTAP-Version und den Speicher-Controller aus, und klicken Sie dann auf die Schaltfläche Ergebnisse anzeigen.

Mindestanforderungen an die Kabel

Die Anzahl und der Typ der erforderlichen Kabel und Adapter variiert je nach Implementierung des FlexPod Datacenter. Der Kabeltyp, der Transceiver-Typ und die Nummer werden während des Entwurfsprozesses anhand Ihrer Anforderungen ermittelt. In der folgenden Tabelle ist die Mindestanzahl der erforderlichen Kabel aufgeführt.

Trennt	Modellnummer	Kabel erforderlich
Cisco UCS-Gehäuse	Cisco UCS 5108	Mindestens zwei Twinaxialkabel pro Cisco UCS 2104XP, 2204XP oder 2208XP Modul

Trennt	Modellnummer	Kabel erforderlich
Cisco UCS Fabric Interconnects	Cisco UCS 6248UP	• Zwei Cat5e-Kabel für Management-Ports • Zwei Cat5e-Kabel für L1, L2-Interconnects pro Fabric-Paar • Mindestens vier Twinaxialkabel pro Fabric Interconnect • Mindestens vier FC-Kabel pro Fabric Interconnect
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• Zwei Cat5e-Kabel für Management-Ports • Zwei Cat5e-Kabel für L1, L2-Interconnects pro Fabric-Paar • Mindestens vier Twinaxialkabel pro Fabric Interconnect	Cisco UCS 6324
	• Zwei 10/100/1000 MBit/s-Management-Ports • Mindestens zwei Twinaxialkabel pro Fabric Interconnect	Switches der Cisco Nexus 5000 und 7000 Serie
	Cisco Nexus 5000 Serie	
• Mindestens zwei 10-GbE-Glasfaserkabel oder Twinaxialkabel pro Switch • Mindestens zwei FC-Kabel pro Switch (bei FC/FCoE-Konnektivität)	Cisco Nexus 7000 Serie	Switches Der Cisco Nexus 9000-Serie

Trennt	Modellnummer	Kabel erforderlich
Cisco Nexus 9000 Serie	Mindestens zwei 10-GbE-Kabel pro Switch	NetApp FAS Controller
AFF A-Serie	• Ein SAS- oder SATA-Kabel pro Storage Controller • Mindestens zwei FC-Kabel pro Controller, wenn ältere FC-Ressourcen verwendet werden • Mindestens zwei 10-GbE-Kabel pro Controller • Mindestens ein GbE-Kabel für Management pro Controller • Für ONTAP werden pro Paar Cluster-Interconnect-Switches acht kurze Twinaxialkabel benötigt	
FAS Serie	NetApp Platten-Shelves	DS212C
Zwei SAS-, SATA- oder FC-Kabel pro Festplatten-Shelf		DS224C
		DS460C
		NS224

Technische Spezifikationen und Referenzen

Technische Spezifikationen enthalten Details zu den Hardwarekomponenten einer FlexPod-Lösung, z. B. Chassis, FEXs, Server, Switches, Und Storage Controllern.

Blade Server-Chassis der Cisco UCS B-Serie

Die technischen Spezifikationen für das Blade Server-Chassis der Cisco UCS B-Serie, wie in der folgenden Tabelle dargestellt, umfassen die folgenden Komponenten:

- Anzahl der Höheneinheiten
- Maximale Anzahl an Blades
- Unified Fabric Funktionalität
- Midplane-I/O-Bandbreite pro Server
- Anzahl der E/A-Schächte für FEXs

Komponente	Blade Server-Chassis der Cisco UCS 5100-Serie
Höheneinheiten	6
Maximale Rotorblätter in voller Breite	4
Maximale Rotorblätter in halber Breite	8
Der sogenannten Unified Fabric	Ja.

Komponente	Blade Server-Chassis der Cisco UCS 5100-Serie
Midplane-I/O	Bis zu 80 GBit/s I/O-Bandbreite pro Server
E/A-Schächte für FEXs	Zwei Einschübe für Cisco UCS 2104XP, 2204/8XP, 2408XP und 2304 FEXs

Weitere Informationen finden Sie im "Blade Server-Chassis der Cisco UCS 5100-Serie – Datenblatt".

Cisco UCS Blade Server der B-Serie

Die technischen Spezifikationen für Cisco UCS Blade Server der B-Serie, wie in der nachfolgenden Tabelle dargestellt, umfassen die folgenden Komponenten:

- Anzahl der Prozessorsockeln
- Prozessorunterstützung
- Speicherkapazität
- Größe und Geschwindigkeit
- SAN Boot-Unterstützung
- Anzahl der Mezzanine-Adaptersteckplätze
- Maximaler I/O-Durchsatz
- Formfaktor
- Maximale Anzahl an Servern pro Chassis

Komponente	Cisco UCS Datenblatt
CISCO UCS B200 M6	"Cisco UCS B200 M6 Blade Server"

Rack-Server der Cisco UCS C-Serie

Die technischen Spezifikationen für die Rack-Server der Cisco UCS C-Serie umfassen Prozessorunterstützung, maximale Speicherkapazität, die Anzahl der PCIe-Steckplätze und die Größe des Formfaktors. Weitere Informationen zu kompatiblen UCS Servermodellen finden Sie im "Cisco Hardware-Kompatibilität" Liste. In den folgenden Tabellen sind jeweils die Datenblätter für den C-Series Rack Server und die Gehäuseoption Cisco UCS C-Series dargestellt.

Komponente	Cisco UCS Datenblatt
CISCO UCS C220 M6	"Cisco UCS C220 M6 Rack Server"
CISCO UCS C225 M6	"Cisco UCS C225 M6 Rack Server"
CISCO UCS C240 M6	"Cisco UCS C240 M6 Rack Server"
CISCO UCS C245 M6	"Cisco UCS C245 M6 Rack Server"

Gehäuse der Cisco UCS X-Serie

Die technischen Spezifikationen für Gehäuse der Cisco UCS X-Serie, wie in der nachfolgenden Tabelle dargestellt, umfassen die folgenden Komponenten:

- Anzahl der Höheneinheiten

- Maximale Anzahl an Nodes
- Unified Fabric Funktionalität
- Anzahl der I/O-Einschübe für IFMS

Komponente	Cisco UCS 9508 Computing-Node-Chassis der X-Serie
Höheneinheiten	7
Maximale Anzahl an Nodes	8
Der sogenannten Unified Fabric	Ja.
I/O-Einschübe für IFMS	Zwei Einschübe für Cisco UCS 9108 Intelligent Fabric Module (IFMS)

Weitere Informationen finden Sie im "Datenblatt zum Cisco UCS X9508 X-Series Gehäuse".

Computing-Node der Cisco UCS X-Serie

Die technischen Spezifikationen für den Computing-Node der Cisco UCS X-Serie, wie in der folgenden Tabelle dargestellt, umfassen die folgenden Komponenten:

- Anzahl der Prozessorsockeln
- Prozessorunterstützung
- Speicherkapazität
- Größe und Geschwindigkeit
- SAN Boot-Unterstützung
- Anzahl der Mezzanine-Adaptersteckplätze
- Maximaler I/O-Durchsatz
- Formfaktor
- Maximale Anzahl der Computing-Nodes pro Chassis

Komponente	Cisco UCS Datenblatt
Cisco UCS X210c M6	"Cisco UCS X210c M6 Computing-Node"

GPU-Empfehlung für FlexPod AI, ML und DL

Die in der nachstehenden Tabelle aufgeführten Cisco UCS C-Series Rack Server können in einer FlexPod-Architektur zum Hosten von KI-, ML- und DL-Workloads verwendet werden. Die Cisco UCS C480 ML M5 Server wurden speziell für KI-, ML- und DL-Workloads entwickelt und verwenden NVIDIA SXM2-basierte GPUs, während die anderen Server PCIe-basierte GPUs verwenden.

In der folgenden Tabelle sind auch die empfohlenen GPUs aufgeführt, die mit diesen Servern verwendet werden können.

Server	GPUs
CISCO UCS C220 M6	NVIDIA T4

Server	GPUs
CISCO UCS C225 M6	NVIDIA T4
CISCO UCS C240 M6	NVIDIA TESLA A10, A100
CISCO UCS C245 M6	NVIDIA TESLA A10, A100

Cisco UCS VIC Adapter für Cisco UCS B-Series Blade Server

Die technischen Spezifikationen für die Cisco UCS Virtual Interface Card (VIC) Adapter für Cisco UCS B-Series Blade Server umfassen die folgenden Komponenten:

- Anzahl der Uplink-Ports
- Performance pro Port (IOPS)
- Strom
- Anzahl der Blade Ports
- Hardware-Entlastung
- Unterstützung für Virtualisierung der ein-/Ausgabe-Einzelroot-Eingabe (SR-IOV

Alle derzeit validierten FlexPod Architekturen nutzen einen Cisco UCS VIC. Wenn diese im NetApp aufgeführt sind, werden auch andere Adapter unterstützt "IMT" Sie sind mit Ihrer Implementierung von FlexPod kompatibel, bieten jedoch möglicherweise nicht alle Funktionen, die in der entsprechenden Referenzarchitektur beschrieben werden. Die folgende Tabelle zeigt die Datenblätter zum Cisco UCS VIC Adapter.

Komponente	Cisco UCS Datenblatt
Cisco UCS Virtual Interface Adapter	"Cisco UCS VIC – Datenblätter"

Cisco UCS Fabric Interconnects

Die technischen Spezifikationen für Cisco UCS Fabric Interconnects beinhalten Formfaktor Größe, Gesamtanzahl der Ports und Erweiterungssteckplätze sowie Durchsatzkapazität. Die folgende Tabelle zeigt die Cisco UCS Fabric Interconnect Datenblätter.

Komponente	Cisco UCS Datenblatt
Cisco UCS 6248UP	"Fabric Interconnects der Cisco UCS 6200-Serie"
Cisco UCS 6296UP	
Cisco UCS 6324	"Cisco UCS 6324 Fabric Interconnect"
Cisco UCS 6300	"Fabric Interconnects der Cisco UCS 6300-Serie"
Cisco UCS 6454	"Fabric Interconnects der Cisco UCS 6400-Serie"

Switches der Cisco Nexus 5000 Serie

Die technischen Spezifikationen für Switches der Cisco Nexus 5000 Serie, einschließlich Formfaktor-Größe, Gesamtanzahl der Ports und Unterstützung für Layer-3-Module und Tochterkarten, sind im Datenblatt für jede Modellfamilie enthalten. Diese Datenblätter sind in der folgenden Tabelle zu finden.

Komponente	Cisco Nexus Datenblatt
Cisco Nexus 5548UP	"Cisco Nexus 5548UP Switch"
Cisco Nexus 5596UP (2 HE)	"Cisco Nexus 5596UP Switch"
Cisco Nexus 56128P	"Cisco Nexus 56128P-Switch"
Cisco Nexus 5672UP	"Cisco Nexus 5672UP Switch"

Switches der Cisco Nexus 7000 Serie

Die technischen Spezifikationen für Switches der Cisco Nexus 7000 Serie, einschließlich der Formfaktor-Größe und maximale Anzahl der Ports, sind im Datenblatt für jede Modellfamilie enthalten. Diese Datenblätter sind in der folgenden Tabelle zu finden.

Komponente	Cisco Nexus Datenblatt
Cisco Nexus 7004	"Switches Der Cisco Nexus 7000-Serie"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Switches Der Cisco Nexus 7700-Serie"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Switches der Cisco Nexus 9000 Serie

Die technischen Spezifikationen für Switches der Cisco Nexus 9000 Serie sind bei jedem Modell im Datenblatt enthalten. Die Spezifikationen umfassen die Größe des Formfaktors, die Anzahl der Supervisoren, das Fabric-Modul und die Linienkartensteckplätze sowie die maximale Anzahl der Ports. Diese Datenblätter sind in der folgenden Tabelle zu finden.

Komponente	Cisco Nexus Datenblatt
Cisco Nexus 9000 Serie	"Switches Der Cisco Nexus 9000-Serie"
Cisco Nexus 9500 Serie	"Switches Der Cisco Nexus 9500-Serie"
Cisco Nexus 9300 Serie	"Switches Der Cisco Nexus 9300-Serie"
Cisco Nexus 9336PQ ACI Wirbelsäulenschalter	"Cisco Nexus 9336PQ ACI Wirbelsäulenschalter"
Cisco Nexus 9200 Serie	"Switches Der Cisco Nexus 9200 Plattform"

Cisco Application Policy Infrastructure Controller

Bei der Implementierung von Cisco ACI zusätzlich zu den Elementen im Abschnitt "Switches Der Cisco Nexus 9000-Serie", Sie müssen drei Cisco APICs konfigurieren. In der folgenden Tabelle ist das Cisco APIC Datenblatt aufgeführt.

Komponente	Cisco Application Policy Infrastructure – Datenblatt
Cisco Application Policy Infrastructure Controller	"Datenblatt zu Cisco APIC"

Details des Cisco Nexus Fabric Extender

Die technischen Spezifikationen für den Cisco Nexus FEX umfassen Geschwindigkeit, die Anzahl der festen Ports und Verbindungen sowie die Größe des Formfaktors.

In der folgenden Tabelle ist das Datenblatt zur FEX-Serie Cisco Nexus 2000 aufgeführt.

Komponente	Cisco Nexus Fabric Extender Datenblatt
Cisco Nexus 2000 Series Fabric Extender	"FEX-Datenblatt für die Nexus 2000-Serie"

SFP-Module

Weitere Informationen zu den SFP-Modulen finden Sie in den folgenden Ressourcen:

- Weitere Informationen zum Cisco 10-Gbit-SFP finden Sie unter "Cisco 10-Gigabit-Module".
- Informationen zum Cisco 25GB SFP finden Sie unter "Cisco 25-Gigabit-Module".
- Informationen zum Cisco QSFP-Modul finden Sie im "Datenblatt zu Cisco 40GBASE QSFP Modulen".
- Informationen zum Cisco 100-GB-SFP finden Sie unter "Cisco 100-Gigabit-Module".
- Informationen zum Cisco FC SFP-Modul finden Sie im "Datenblatt zu Cisco MDS 9000-Produktreihe Pluggable Transceivern".
- Informationen zu allen unterstützten Cisco SFP- und Transceiver-Modulen finden Sie unter "Hinweise zur Installation des Cisco SFP- und SFP+-Transceivermoduls" Und "Cisco Transceiver-Module".

NetApp Storage Controller

Die technischen Spezifikationen für NetApp Storage Controller umfassen die folgenden Komponenten:

- Chassis-Konfiguration
- Anzahl der Höheneinheiten
- Speichermenge
- NetApp Flash Cache Caching
- Aggregatgröße
- Volume-Größe
- Anzahl LUNs
- Unterstützter Netzwerkspeicher
- Maximale Anzahl an NetApp FlexVol-Volumes
- Maximale Anzahl der unterstützten SAN-Hosts
- Die maximale Anzahl von Snapshot Kopien

FAS Serie

Alle verfügbaren Modelle von FAS Storage Controllern werden zur Verwendung in einem FlexPod-Datacenter unterstützt. Detaillierte Spezifikationen für alle Storage Controller der FAS Serie finden Sie im "NetApp Hardware Universe". Ausführliche Informationen zu einem bestimmten FAS-Modell finden Sie in der plattformspezifischen Dokumentation in der folgenden Tabelle.

Komponente	Dokumentation der Controller-Plattform der FAS Serie
FAS9000 Serie	"Datenblatt zur FAS9000 Serie"
FAS8700 Serie	"Datenblatt zur FAS8700 Serie"
FAS8300 Serie	"Datenblatt zur FAS8300 Serie"
FAS500f Serie	"Datenblatt zur FAS500f Serie"
FAS2700 Serie	"Datenblatt: FAS2700 Serie"

AFF A-Serie

Alle aktuellen Modelle der NetApp AFF A-Series Storage Controller werden zur Verwendung in FlexPod unterstützt. Weitere Informationen finden Sie im "Technische Spezifikationen der AFF" Datenblatt und im "NetApp Hardware Universe" . Ausführliche Informationen zu einem bestimmten AFF-Modell finden Sie in der in der folgenden Tabelle aufgeführten plattformspezifischen Dokumentation.

Komponente	Dokumentation der Controller-Plattform der AFF A-Series
NetApp AFF A800	"Dokumentation der AFF A800 Plattform"
NetApp AFF A700	"Dokumentation der AFF A700 Plattform"
NetApp AFF A700s	"AFF A700s Plattform-Dokumentation"
NetApp AFF A400	"Dokumentation der AFF A400 Plattform"
NetApp AFF A250	"Dokumentation der AFF A250-Plattform"

AFF ASA A-SERIES

Alle aktuellen Modelle der NetApp AFF ASA A-Series Storage Controller werden zur Verwendung in FlexPod unterstützt. Weitere Informationen finden Sie in der Dokumentation zu All-SAN-Arrays, im technischen Bericht zu ONTAP AFF All-SAN-Systemen und im NetApp Hardware Universe. Ausführliche Informationen zu einem bestimmten AFF-Modell finden Sie in der plattformspezifischen Dokumentation, die in der folgenden Tabelle aufgeführt ist.

Komponente	Dokumentation der Controller-Plattform der AFF A-Series
NETAPP AFF ASA A800	"Dokumentation der AFF ASA A800 Plattform"
NETAPP AFF ASA A700	"Dokumentation der AFF ASA A700 Plattform"
NETAPP AFF ASA A400	"Dokumentation der AFF ASA A400 Plattform"
NETAPP AFF ASA A250	"Dokumentation der AFF ASA A250-Plattform"
NETAPP AFF ASA A220	"Dokumentation der AFF ASA A220 Plattform"

NetApp Platten-Shelves

Die technischen Spezifikationen für NetApp Platten-Shelves umfassen die Größe des Formfaktor, die Anzahl der Laufwerke pro Gehäuse und die Shelf-I/O-Module. Diese Dokumentation finden Sie in der folgenden Tabelle. Weitere Informationen finden Sie im "Technische Spezifikationen zu NetApp Platten-Shelfs und Storage-Medien" Und das "NetApp Hardware Universe".

Komponente	Dokumentation des NetApp FAS/AFF Festplatten-Shelf
NetApp DS212C Festplatten-Shelf	"DS212C Disk Shelf-Dokumentation"
NetApp DS224C Festplatten-Shelf	"DS224C Festplatten-Shelf-Dokumentation"
NetApp DS460C Festplatten-Shelf	"DS460C Festplatten-Shelf-Dokumentation"
NetApp NS224 NVMe-SSD Festplatten-Shelf	"NS224 Disk Shelf-Dokumentation"

NetApp Laufwerke

Die technischen Spezifikationen für NetApp Laufwerke umfassen Formfaktor Größe, Festplattenkapazität, Festplatten-U/min, unterstützende Controller und ONTAP Versionsanforderungen. Diese Spezifikationen finden Sie im Abschnitt Laufwerke des "NetApp Hardware Universe".

Altgeräte

FlexPod ist eine flexible Lösung, mit der Sie Ihre vorhandenen Systeme und neue Systeme, die derzeit von Cisco und NetApp verkauft werden, nutzen können. Gelegentlich werden bestimmte Modelle von Geräten von Cisco und NetApp als End-of-Life (EOL) bezeichnet.

Auch wenn diese Modelle nicht mehr verfügbar sind, wenn Sie vor dem Datum der Einstellung der Verfügbarkeit (EOA) eines dieser Modelle gekauft haben, können Sie diese Systeme in einer FlexPod Konfiguration verwenden. Auf der finden Sie eine vollständige Liste der älteren Modelle, die in FlexPod unterstützt werden und die nicht mehr verkauft werden können "NetApp Service und Support Produktprogramme, deren Ende der Verfügbarkeit Index erreicht ist".

Weitere Informationen zu älteren Cisco Systemen finden Sie in den Cisco EOL- und EOA-Mitteilungen für "Cisco UCS C-Serie Rack Server", "Blade Server der Cisco UCS B-Serie", und "Nexus Switches".

Unterstützung für ältere FC-Fabric-Systeme umfasst:

- 2 GB Fabric
- 4 GB Fabric

Ältere Software umfasst Folgendes:

- NetApp Data ONTAP in 7-Mode, 7.3.5 und höher
- ONTAP 8.1.x bis 9.0.x
- Cisco UCS Manager 1.3 und höher
- Cisco UCS Manager 2.1 bis 2.2.7

Weitere Informationen

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

- NetApp Produktdokumentation

  "https://docs.netapp.com/"

- NetApp Support Communications

  "https://mysupport.netapp.com/info/communications/index.html"

- NetApp Interoperabilitäts-Matrix-Tool (IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe

  "https://hwu.netapp.com/"

- NetApp Support

  "https://mysupport.netapp.com/"

FlexPod Datacenter

FlexPod Datacenter mit NetApp SnapMirror Business Continuity und ONTAP 9.10

TR-4920: FlexPod Datacenter mit NetApp SnapMirror Business Continuity und ONTAP 9.10

Jyh-shing Chen, NetApp

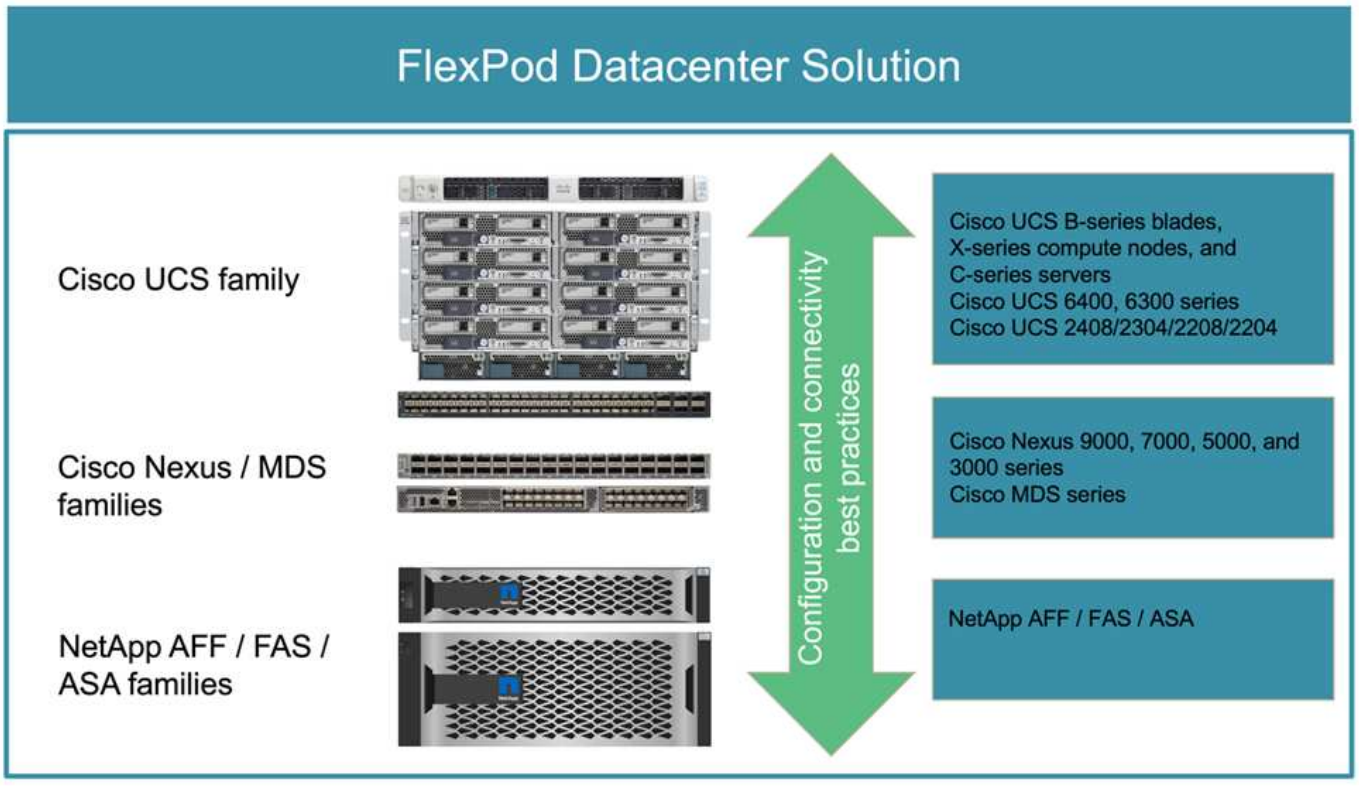
Einführung

Die FlexPod Lösung

FlexPod ist eine Best-Practice-Architektur für konvergente Infrastrukturen, die die folgenden Komponenten von Cisco und NetApp umfasst:

- Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus und MDS Switches-Familien
- NetApp FAS, NetApp AFF und NetApp All SAN Array (ASA) Systeme

Die folgende Abbildung zeigt einige der zum Erstellen von FlexPod Lösungen verwendeten Komponenten. Diese Komponenten sind sowohl von Cisco als auch von NetApp entsprechend den Best Practices miteinander verbunden und konfiguriert, sodass eine ideale Plattform für eine Vielzahl von Enterprise Workloads ohne Bedenken eingesetzt werden kann.



Es ist ein großes Portfolio von Cisco Validated Designs (CVDs) und NetApp Verified Architectures (NVAs)

erhältlich. Diese CVDs und NVAs decken alle größeren Datacenter-Workloads ab und sind das Ergebnis der kontinuierlichen Zusammenarbeit und Innovationen zwischen NetApp und Cisco auf den FlexPod-Lösungen.

FlexPod CVDs und NVAs enthalten umfangreiche Tests und Validierungen im Erstellungsprozess. Außerdem bieten sie Referenzarchitekturen-Designs sowie Schritt-für-Schritt-Anleitungen für die Implementierung von FlexPod Lösungen für Partner und Kunden. Wenn Unternehmen diese CVDs und NVAs als Leitfäden für Design und Implementierung einsetzen, können sie Risiken verringern, das Ausfallzeiten der Lösung verringern und die Verfügbarkeit, Skalierbarkeit, Flexibilität und Sicherheit der implementierten FlexPod Lösungen erhöhen.

Jede der gezeigten FlexPod-Komponentenfamilien (Cisco UCS, Cisco Nexus/MDS Switches und NetApp Storage) bietet Plattform- und Ressourcenoptionen für die vertikale und horizontale Skalierung der Infrastruktur. Gleichzeitig werden die Funktionen unterstützt, die unter den Best Practices für Konfiguration und Konnektivität von FlexPod erforderlich sind. FlexPod kann auch horizontal für Umgebungen skaliert werden, in denen mehrere konsistente Implementierungen durch die Bereitstellung weiterer FlexPod-Stacks erforderlich sind.

Disaster Recovery und Business Continuity

Unternehmen können auf verschiedene Weise sicherstellen, dass sie ihre Applikations- und Datenservices nach Ausfällen schnell wiederherstellen können. Mit einem Disaster Recovery- (DR-) und Business Continuity-Plan (BC), der Implementierung einer Lösung, die die Geschäftsziele erfüllt, und durch regelmäßige Tests der Disaster-Szenarien können Unternehmen die Wiederherstellung nach einem Notfall durchführen und wichtige Business Services nach einem Notfall aufrechterhalten.

Für verschiedene Applikations- und Datenservices können Unternehmen unterschiedliche DR- und BC-Anforderungen haben. Einige Applikationen und Daten sind möglicherweise nicht in Notfällen oder Notfallsituationen notwendig, während andere Unternehmen möglicherweise kontinuierlich zur Verfügung stehen müssen, um geschäftliche Anforderungen zu unterstützen.

Für geschäftskritische Applikations- und Datenservices, die den Betrieb stören könnten, wenn diese nicht verfügbar sind, ist eine sorgfältige Evaluierung erforderlich, um Fragen wie Wartungsarbeiten und Ausfallszenarien zu beantworten, die Ihr Unternehmen in Betracht ziehen sollte, Wie viele Daten das Unternehmen bei einem Ausfall verkraften kann und wie schnell die Recovery erfolgen kann und sollte.

Für Unternehmen, die Datenservices zur Umsatzgenerierung nutzen, müssen die Datenservices möglicherweise durch eine Lösung geschützt werden, die nicht nur verschiedenen Single-Point-of-Failure-Szenarien, sondern auch einem Ausfallszenario am Standort standhält, um den unterbrechungsfreien Geschäftsbetrieb zu gewährleisten.

Recovery-Zeitpunkt und Recovery-Zeitvorgabe

Der Recovery-Zeitpunkt (Recovery Point Objective, RPO) bezeichnet die Menge an Daten im Hinblick auf die Zeit, die Sie sich leisten können, oder den Zeitpunkt, an dem Sie Ihre Daten wiederherstellen können. Mit einem täglichen Backup-Plan kann ein Unternehmen einen Tag an Daten verlieren, weil die Änderungen an den Daten seit dem letzten Backup in einem Notfall verloren gehen könnte. Für geschäftskritische und geschäftskritische Datenservices sind unter Umständen ein RPO von Null sowie ein Plan und eine zugehörige Infrastruktur zum Schutz von Daten ohne Datenverluste erforderlich.

Die Recovery-Zeitvorgabe (Recovery Time Objective, RTO) beschreibt, wie lange Sie sich leisten können, ohne die Daten verfügbar zu haben oder wie schnell Datenservices gesichert werden müssen. So kann ein Unternehmen beispielsweise über eine Backup- und Recovery-Implementierung verfügen, bei der aufgrund seiner Größe herkömmliche Tapes für bestimmte Datensätze verwendet werden. Das Ergebnis: Die Wiederherstellung der Daten von den Backup-Tapes kann es im Falle eines Infrastruktur-Ausfalls mehrere Stunden oder gar Tage dauern. Überlegungen zur Zeit müssen außerdem die Zeit beinhalten, die erforderlich

ist, um die Infrastruktur zusätzlich zum Wiederherstellen der Daten zu sichern. Für geschäftskritische Datenservices benötigen Sie unter Umständen ein sehr niedriges RTO und können daher für Business Continuity nur eine Failover-Zeit von Sekunden oder Minuten tolerieren, um die Datenservices schnell wieder online zu bringen.

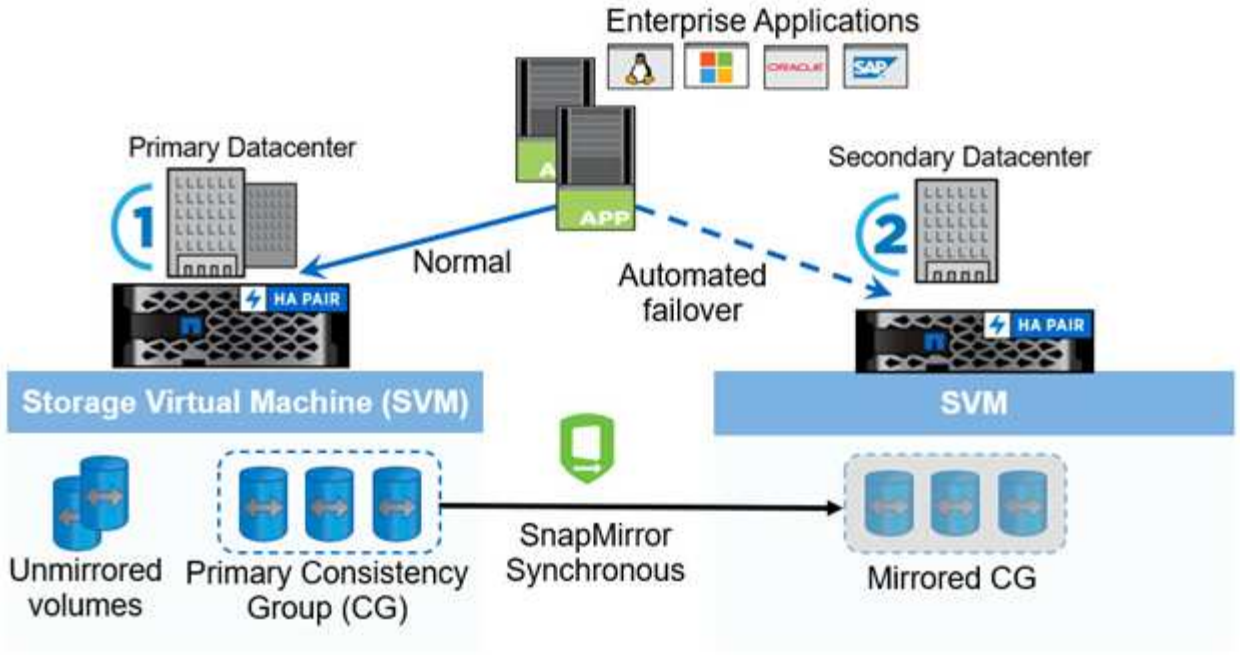
SM-BC

Ab ONTAP 9.8 können Sie SAN-Workloads für transparentes Applikations-Failover mit NetApp SM-BC sichern. Sie können Konsistenzgruppen zwischen zwei AFF Clustern oder zwei ASA Clustern erstellen, um Daten zu replizieren, damit ein Recovery Point Objective von null und ein Recovery Time Objective von fast null erreicht wird.

Die SM-BC Lösung repliziert Daten mithilfe der SnapMirror Synchronous Technologie über ein IP-Netzwerk. Die Lösung bietet Granularität auf Applikationsebene und automatisches Failover zur Sicherung geschäftskritischer Daten-Services wie Microsoft SQL Server, Oracle usw. mit iSCSI oder FC protokollbasierten SAN LUNs. Ein an einem dritten Standort bereitgestellter ONTAP Mediator überwacht die SM-BC-Lösung und ermöglicht ein automatisches Failover bei einem Standortausfall.

Eine Konsistenzgruppe (CG) ist eine Sammlung von FlexVol-Volumes, die eine konsistente Schreibreihenfolge für den Applikations-Workload gewährleistet, der zur Gewährleistung der Business Continuity geschützt werden muss. Es ermöglicht gleichzeitige, absturzkonsistente Snapshot-Kopien einer Sammlung von Volumes zu einem bestimmten Zeitpunkt. Eine SnapMirror-Beziehung, auch als CG-Beziehung bekannt, wird zwischen einer Quell-CG und einer Ziel-CG eingerichtet. Die Gruppe der Volumes, die als Teil einer CG ausgewählt wurden, kann einer Applikationsinstanz, einer Gruppe von Applikationsinstanzen oder für eine komplette Lösung zugeordnet werden. Darüber hinaus können auf der Grundlage von Geschäftsanforderungen und Änderungen die Beziehungen der SM-BC Consistency Group nach Bedarf erstellt oder gelöscht werden.

Wie in der folgenden Abbildung dargestellt, werden die Daten in der Konsistenzgruppe für Disaster Recovery und Business Continuity in einen zweiten ONTAP Cluster repliziert. Die Anwendungen haben Konnektivität zu den LUNs in beiden ONTAP-Clustern. I/O wird normalerweise vom primären Cluster bereitgestellt und setzt diesen automatisch vom sekundären Cluster fort, falls auf dem primären Cluster ein Notfall auftritt. Beim Design einer SM-BC-Lösung muss die unterstützte Objektanzahl für die CG-Beziehungen (z. B. maximal 20 CGS und maximal 200 Endpunkte) beachtet werden, um zu vermeiden, dass die unterstützten Grenzwerte überschritten werden.



"Weiter: FlexPod SM-BC Lösung."

FlexPod SM-BC Lösung

"Zurück: Einführung."

Lösungsüberblick

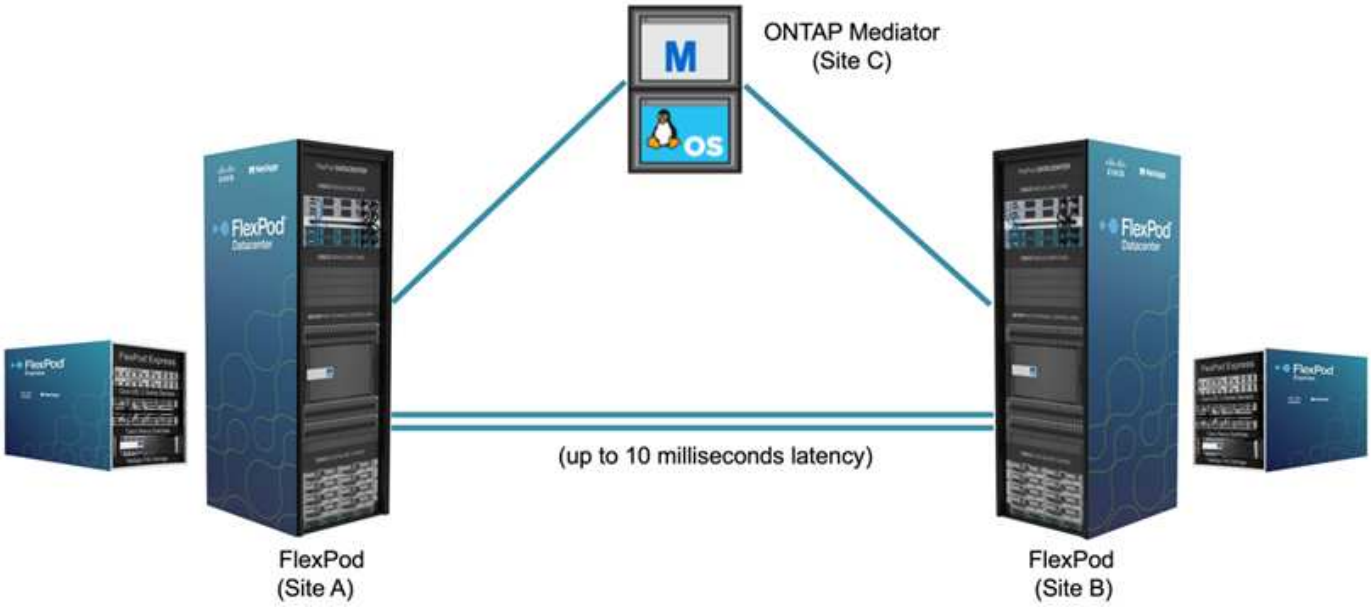
Eine FlexPod SM-BC Lösung besteht im Wesentlichen aus zwei FlexPod Systemen, die sich an zwei Standorten trennen und in Verbindung setzen, um eine hochverfügbare, äußerst flexible und hochgradig zuverlässige Datacenter-Lösung bereitzustellen, die trotz eines Standortausfalls Business Continuity bietet.

Neben der Implementierung von zwei neuen FlexPod-Infrastrukturen zur Erstellung einer FlexPod SM-BC Lösung kann die Lösung auch auf zwei vorhandenen FlexPod-Infrastrukturen implementiert werden, die mit SM-BC kompatibel sind, oder indem ein neues FlexPod hinzugefügt wird, um eine bestehende FlexPod zu nutzen.

Die beiden FlexPod Systeme in einer FlexPod SM-BC Lösung müssen in Konfigurationen nicht identisch sein. Die zwei ONTAP Cluster müssen jedoch aus den gleichen Storage-Familien stammen, entweder zwei AFF oder zwei ASA Systeme, jedoch nicht unbedingt das gleiche Hardware-Modell. Die SM-BC Lösung unterstützt keine FAS Systeme.

Die beiden FlexPod Standorte benötigen Netzwerkkonnektivität, was der Bandbreite der Lösung und den Quality of Service-Anforderungen entspricht und zwischen den Standorten weniger als 10 Millisekunden (10 ms) Latenz für Umlaufzeit hat, wie von der ONTAP SM-BC Lösung benötigt. Für diese FlexPod SM-BC Lösungsvalidierung werden die beiden FlexPod-Standorte über ein erweitertes Layer-2-Netzwerk im selben Lab miteinander verbunden.

Die NetApp ONTAP SM-BC Lösung bietet synchrone Replizierung zwischen den beiden NetApp Storage-Clustern und sorgt so für Hochverfügbarkeit und Disaster Recovery an Standorten bzw. Großraumgebieten. Der an einem dritten Standort implementierte ONTAP Mediator überwacht die Lösung und ermöglicht ein automatisiertes Failover im Falle eines Standortausfalls. Die folgende Abbildung bietet einen allgemeinen Überblick über die Komponenten der Lösung.



Mit der FlexPod SM-BC Lösung können Sie eine Private Cloud auf Basis von VMware vSphere auf Basis einer verteilten und doch integrierten Infrastruktur implementieren. Die integrierte Lösung ermöglicht die Koordinierung mehrerer Standorte als eine einheitliche Lösungsinfrastruktur, um Datenservices vor einer Vielzahl von Single Point-of-Failure und einem kompletten Standortausfall zu schützen.

In diesem technischen Bericht werden einige der End-to-End-Designüberlegungen der FlexPod SM-BC-Lösung hervorgehoben. Die Fachleute sollten Informationen in den verschiedenen FlexPod CVDs und NVAs verwenden, um weitere Einzelheiten zur Implementierung von FlexPod Lösungen zu erhalten.

Die Lösung wurde zwar durch die Implementierung von zwei FlexPod Systemen auf der Basis von Best Practices von FlexPod validiert, wie in CVDs dokumentiert. Dennoch werden die Anforderungen für die SM-BC Lösung berücksichtigt. Die in diesem Bericht vorgestellten FlexPod SM-BC Lösung wurde für Ausfallsicherheit und Fehlertoleranz während verschiedener Fehlerszenarien und in einem simulierten Standortfehler validiert.

Anforderungen der Lösung erfüllen

Die FlexPod SM-BC Lösung ist auf folgende wichtige Anforderungen ausgerichtet:

- Business Continuity für geschäftskritische Applikationen und Datenservices bei einem vollständigen Datacenter-Ausfall
- Flexible, verteilte Workload-Platzierung mit Workload-Mobilität über mehrere Datacenter hinweg
- Standortaffinität, bei der während des normalen Betriebs lokal auf Virtual Machine-Daten vom selben Datacenter-Standort zugegriffen wird
- Schnelles Recovery ohne Datenverlust bei Standortausfall

Lösungskomponenten

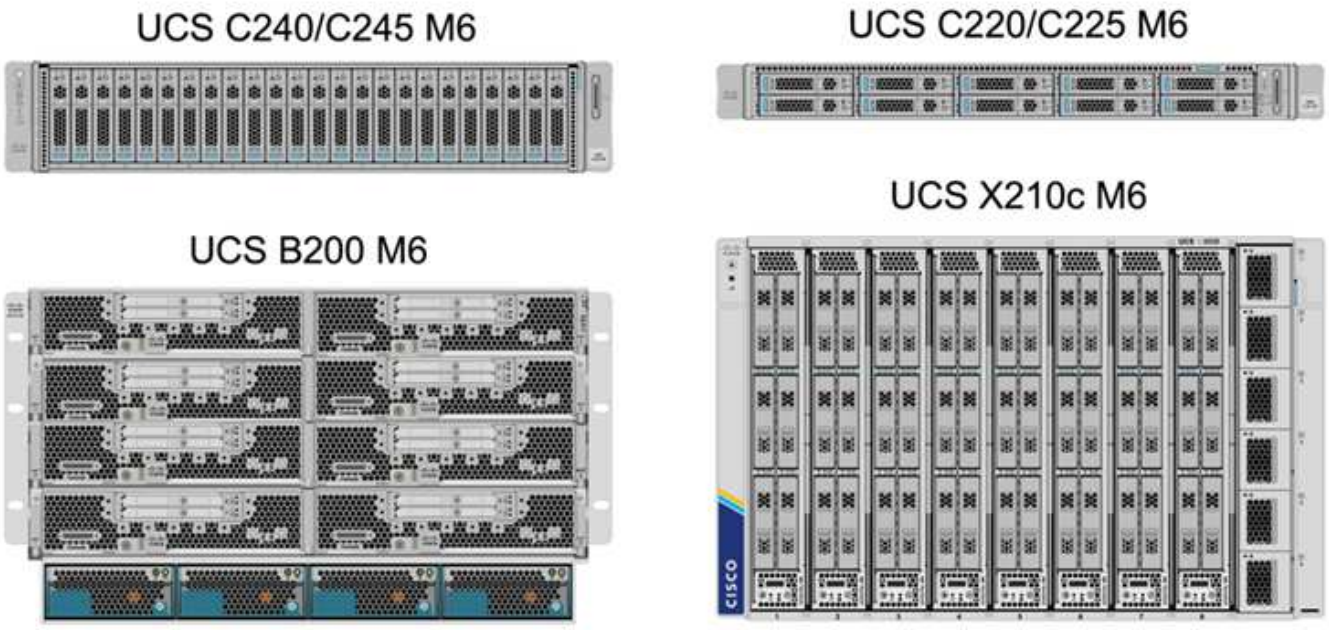
Cisco Computing-Komponenten

Cisco UCS ist eine integrierte Computing-Infrastruktur für einheitliche Computing-Ressourcen, Unified Fabric und einheitliches Management. Damit können Unternehmen den Einsatz von Applikationen, einschließlich Virtualisierung und Bare Metal Workloads, automatisieren und beschleunigen. Das Cisco UCS unterstützt eine Vielzahl von Implementierungsanwendungsfällen, einschließlich Remote-Standorten und Zweigstellen, Datacenter und Hybrid-Cloud-Anwendungsfälle. Je nach den spezifischen Lösungsanforderungen kann die

FlexPod Cisco Computing-Implementierung eine Vielzahl von Komponenten in unterschiedlichen Maßstäben verwenden. Die folgenden Abschnitte enthalten zusätzliche Informationen zu einigen der UCS Komponenten.

UCS Server und Compute-Node

Die folgende Abbildung zeigt einige Beispiele für die UCS Server-Komponenten: Rack Server der UCS C-Serie, UCS 5108 Chassis mit Blade Servern der B-Serie und das neue UCS X9508 Chassis mit Computing-Nodes der X-Serie. Die Cisco UCS C-Series Rack Server sind in einem und zwei Rack-Einheiten (RU)-Formfaktor, Intel und AMD CPU-basierten Modellen sowie mit verschiedenen CPU-Geschwindigkeiten und -Kernen, Arbeitsspeicher und I/O-Optionen verfügbar. Die Cisco UCS Blade Server der B-Serie und die neuen Computing-Nodes der X-Serie sind auch mit verschiedenen CPU-, Arbeitsspeicher- und I/O-Optionen verfügbar. Zur Erfüllung der unterschiedlichen geschäftlichen Anforderungen werden sie alle in der FlexPod Architektur unterstützt.



Neben den in der Abbildung gezeigten Rack-Servern C220/C225/C240/C245 M6, B200 M6 Blade Servern und X210c Computing-Nodes können auch ältere Rack- und Blade-Server-Generationen genutzt werden, wenn sie weiterhin unterstützt werden.

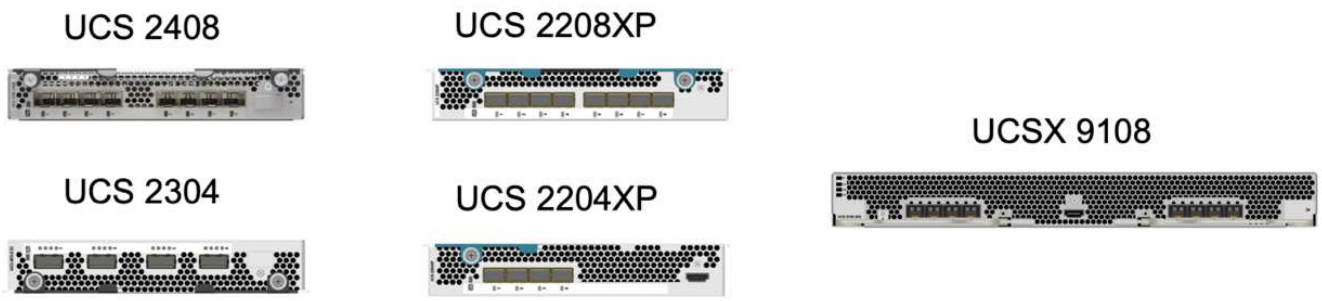
I/O-Modul und Intelligent Fabric Module

Das I/O-Modul (IOM)/Fabric Extender und das Intelligent Fabric Module (IFM) bieten eine einheitliche Fabric-Konnektivität für das Cisco UCS 5108 Blade-Server-Chassis und das Cisco UCS X9508 X-Series Gehäuse.

Die vierte Generation des UCS IOM 2408 verfügt über acht 25-G Unified Ethernet-Ports für die Verbindung des UCS 5108-Gehäuses mit Fabric Interconnects (FI). Jeder 2408 verfügt über vier 10-G-Rückwandplatine zur Ethernet-Verbindung über die Midplane zu jedem Blade-Server im Gehäuse.

Der UCSD 9108 25G IFM verfügt über acht 25-G Unified Ethernet Ports für die Verbindung der Blade Server im UCS X9508 Chassis mit Fabric Interconnects. Jeder 9108 verfügt über vier 25-G-Verbindungen zu jedem UCS X210c Computing-Node im X9108-Gehäuse. Das 9108 IFM arbeitet auch in Verbindung mit dem Fabric Interconnect für das Management der Gehäuseumgebung.

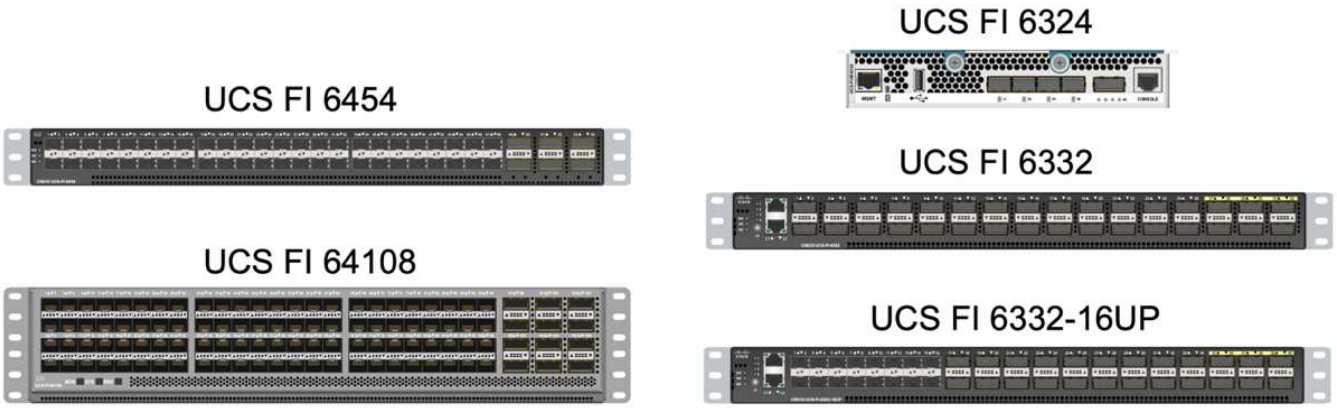
Die folgende Abbildung zeigt die UCS 2408 und früheren IOM Generationen für das UCS 5108 Chassis und den 9108 IFM für das X9508 Chassis.



UCS Fabric Interconnects

Die Cisco UCS Fabric Interconnects (FIS) sorgen für Konnektivität und Management für das gesamte Cisco UCS. Das FIS des Systems wird in der Regel als aktiv/aktiv-Paar bereitgestellt und integriert alle Komponenten in eine einzige, hochverfügbare Management-Domäne, die vom Cisco UCS Manager oder Cisco Intersight gesteuert wird. Cisco UCS FIS bieten ein einzelnes Unified Fabric für das System mit latenzarmem und verlustfreiem, Cut-Through-Switching, das LAN-, SAN- und Management-Datenverkehr über ein einziges Kabelset unterstützt.

Für den Cisco UCS FIS der vierten Generation gibt es zwei Varianten: UCS FI 6454 und 64108. Zu den Merkmalen gehören Unterstützung für 10/25 Gbps Ethernet-Ports, 1/10/25-Gbps-Ethernet-Up-Link-Ports, 40/100-Gbps-Ports und Unified Ports, die 10/25-Gigabit-Ethernet oder 8/16/32-Gbps-Fibre Channel unterstützen. Die folgende Abbildung zeigt den Cisco UCS FIS der vierten Generation zusammen mit den ebenfalls unterstützten Modellen der dritten Generation.



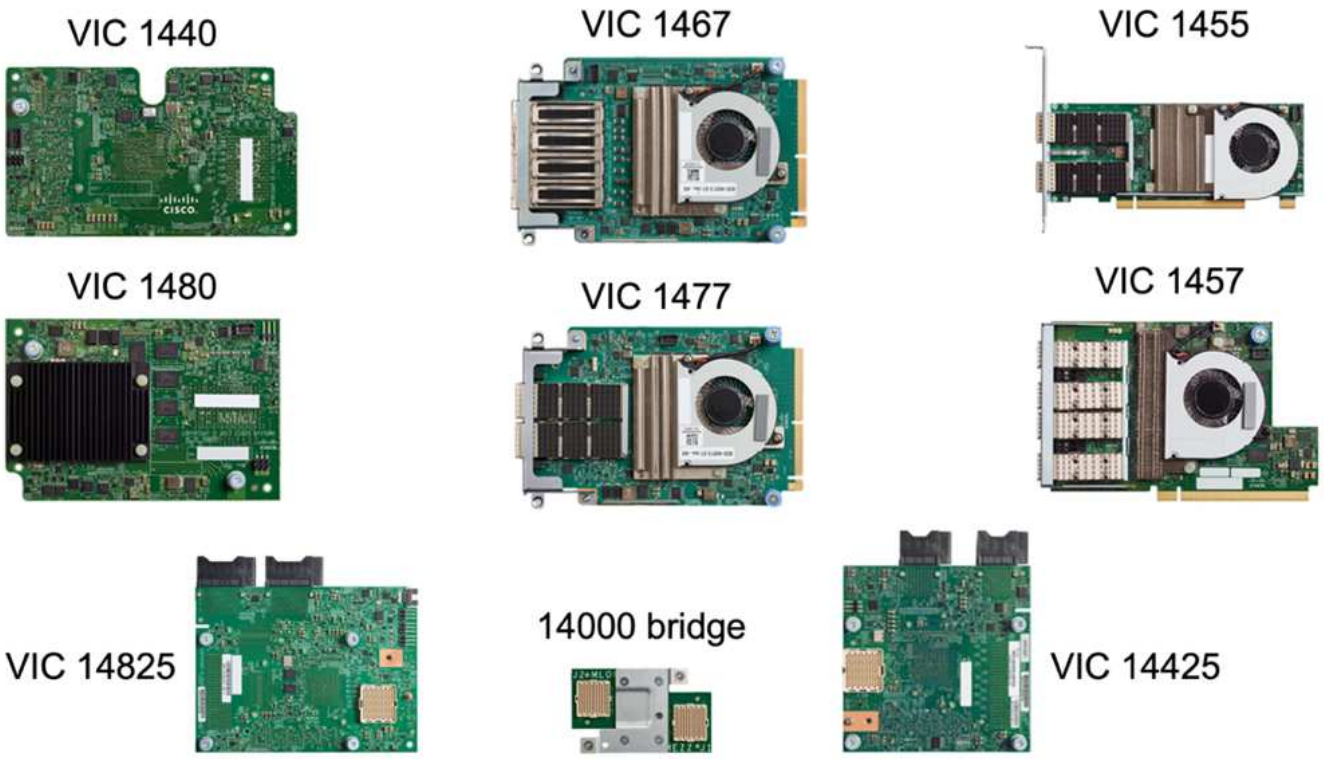
Zur Unterstützung des Cisco UCS X-Series Gehäuses sind Fabric Interconnects der vierten Generation erforderlich, die im Intersight Managed Mode (IMM) konfiguriert sind. Das Cisco UCS 5108 Gehäuse der B-Serie kann jedoch sowohl im IMM-Modus als auch im UCSM-Managed-Modus unterstützt werden.

Das UCS FI 6324 nutzt den IOM-Formfaktor und ist in ein UCS Mini-Chassis für Implementierungen eingebettet, die nur eine kleine UCS-Domäne erfordern.

UCS Virtual Interface-Karten

Cisco UCS Virtual Interface Cards (VIC) sorgen für einheitliches Systemmanagement und LAN- und SAN-Konnektivität für Rack- und Blade Server. Es unterstützt bis zu 256 virtuelle Geräte, entweder als virtuelle Netzwerkschnittstellenkarten (vNICs) oder als virtuelle Host Bus Adapter (vHBAs) mit der Cisco SingleConnect

Technologie. Durch die Virtualisierung vereinfachen VIC Karten die Netzwerk-Konnektivität erheblich und reduzieren die Anzahl der für die Lösungsimplementierung benötigten Netzwerkadapter, Kabel und Switch Ports. Die folgende Abbildung zeigt einige Cisco UCS VIC für Server der B-Serie und C-Serie und die Computing-Nodes der X-Serie.



Die verschiedenen Adaptermodelle unterstützen verschiedene Blade- und Rack-Server mit unterschiedlichen Port-Anzahlen, Port-Geschwindigkeiten und Formfaktoren für modulare LAN on Motherboard (mLOM), Mezzanine-Karten und PCIe-Schnittstellen. Die Adapter unterstützen einige Kombinationen aus 10/25/40/100-G Ethernet und Fibre Channel over Ethernet (FCoE). Sie integrieren die Cisco Converged Network Adapter (CNA)-Technologie, unterstützen ein umfassendes Funktionsset und vereinfachen das Adaptermanagement und die Bereitstellung von Anwendungen. Der VIC unterstützt beispielsweise die VM-FEX-Technologie (Data Center Virtual Machine Fabric Extender) von Cisco, die die Cisco UCS Fabric Interconnect Ports auf Virtual Machines erweitert und somit die Implementierung der Server-Virtualisierung vereinfacht.

Mit einer Kombination aus Cisco VIC in Konfigurationen für mLOM, Mezzanine und Port Expander und Bridge-Karten können Sie die Bandbreite und Konnektivität der Blade Server voll ausschöpfen. Beispielsweise besteht die kombinierte VIC-Bandbreite 2 x 50-G + 2 x 50-G, indem die beiden 25-G-Links auf dem VIC 14825 (mLOM) und 14425 (Mezzanine) sowie die 14000 (Bridge Card) für den X210c Computing-Node genutzt werden. Oder 100 GB pro Fabric/IFM und 200 G insgesamt pro Server bei dualer IFM-Konfiguration.

Details zu den Cisco UCS-Produktfamilien, technischen Spezifikationen und Dokumentationen finden Sie im "Cisco UCS" Website für Informationen.

Cisco Switching-Komponenten

Nexus Switches

FlexPod verwendet Switches der Cisco Nexus Serie, um ein Ethernet Switching Fabric für die Kommunikation zwischen Cisco UCS und NetApp Storage Controllern bereitzustellen. Für die FlexPod Implementierung werden alle derzeit unterstützten Cisco Nexus Switch Modelle, einschließlich der Cisco Nexus 3000, 5000, 7000 und 9000 Serien, unterstützt.

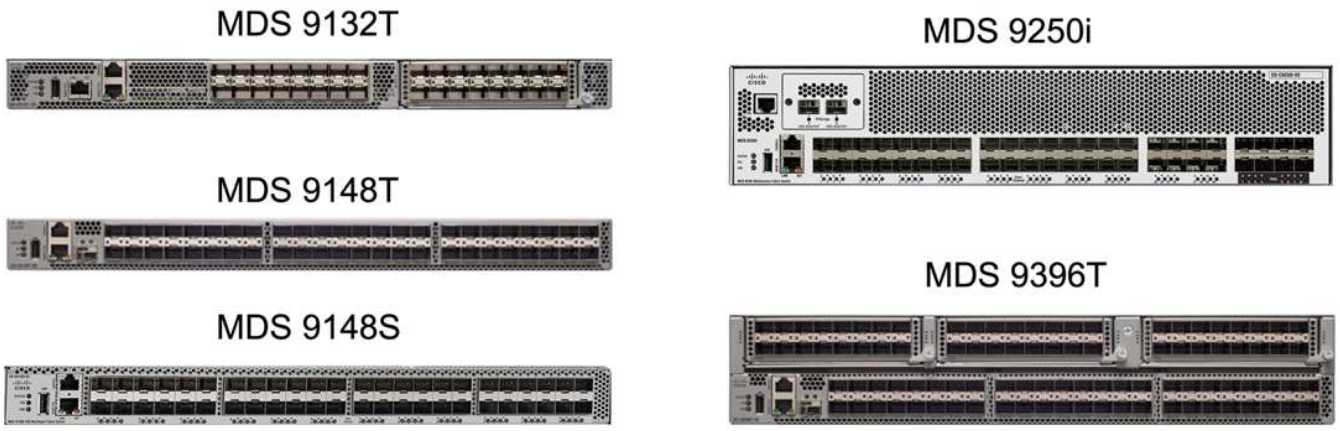
Bei der Auswahl eines Switch-Modells für FlexPod-Implementierungen müssen viele Faktoren berücksichtigt werden, beispielsweise Performance, Port-Geschwindigkeit, Port-Dichte, Switching-Latenz. Und Protokolle wie ACI und VXLAN Unterstützung, für Ihre Designziele sowie für die Unterstützung von Switches.

In der Validierung vieler aktueller FlexPod CVDs werden Switches der Cisco Nexus 9000 Serie wie Nexus 9336C-FX2 und Nexus 93180YC-FX3 verwendet, die eine hohe Performance von 40/100G- und 10/25G-Ports, eine niedrige Latenz und eine außergewöhnliche Energieeffizienz in einem kompakten 1U-Formfaktor bieten. Zusätzliche Geschwindigkeiten werden über Uplink-Ports und Breakout-Kabel unterstützt. Die folgende Abbildung zeigt einige Cisco Nexus 9k- und 3K-Switches, einschließlich des Nexus 9336C-FX2 und des Nexus 3232C-Systems für diese Validierung.

Siehe "Cisco Data Center Switches" Weitere Informationen zu den verfügbaren Nexus Switches und ihren Spezifikationen und Dokumentationen.

MDS-Switches

Die Fabric Switches der Cisco MDS 9100/9200/9300 Serie sind optional Bestandteil der FlexPod Architektur. Diese Switches sind äußerst zuverlässig, hochflexibel und sicher und bieten Sichtbarkeit des Datenflusses in der Fabric. Die folgende Abbildung zeigt einige Beispiele für MDS-Switches, die zum Aufbau redundanter FC-SAN-Fabrics für eine FlexPod-Lösung zur Erfüllung von Applikations- und Geschäftsanforderungen verwendet werden können.



Cisco MDS 9132T/9148T/9396T Hochleistungs-32G-Multilayer-Fabric-Switches sind kostengünstig und extrem zuverlässig, flexibel und skalierbar. Die erweiterten Funktionen für Speichernetzwerke sind leicht zu managen und für eine zuverlässige SAN-Implementierung mit dem gesamten Portfolio der Cisco MDS 9000-Familie kompatibel.

In diese Hardware-Plattform der nächsten Generation sind hochmoderne SAN-Analyse- und

Telemetrierungsfunktionen integriert. Die aus der Überprüfung der Frame-Header extrahierten Telemetriedaten können auf eine Analysevisualisierungsplattform wie den Cisco Data Center Network Manager gestreamt werden. Auch die MDS-Switches unterstützen 16-Gbit-FC, beispielsweise den MDS 9148S, werden in FlexPod unterstützt. Darüber hinaus sind auch Multiservice-MDS-Switches, wie beispielsweise MDS 9250i mit Unterstützung für FCoE- und FCIP-Protokolle neben FC-Protokoll, Teil des FlexPod Lösungsportfolios.

Bei semi-modularen MDS-Switches wie 9132T und 9396T können zusätzliche Port-Erweiterungsmodule und Port-Lizenzen hinzugefügt werden, um zusätzliche Gerätekonnektivität zu unterstützen. Auf den festen Switches wie 9148T können je nach Bedarf weitere Portlizenzen hinzugefügt werden. Diese Flexibilität beim „Pay-as-you-grow"-Modell stellt eine Komponente für Betriebskosten zur Verfügung, mit der sich die Investitionskosten für die Implementierung und den Betrieb einer Switch-basierten MDS-SAN-Infrastruktur verringern lassen.

Siehe "Cisco MDS Fabric Switches" Weitere Informationen zu den verfügbaren MDS Fabric Switches finden Sie im "NetApp IMT" Und "Cisco Hardware- und Software-Kompatibilitätsliste" Erhalten Sie eine vollständige Liste der unterstützten SAN Switches.

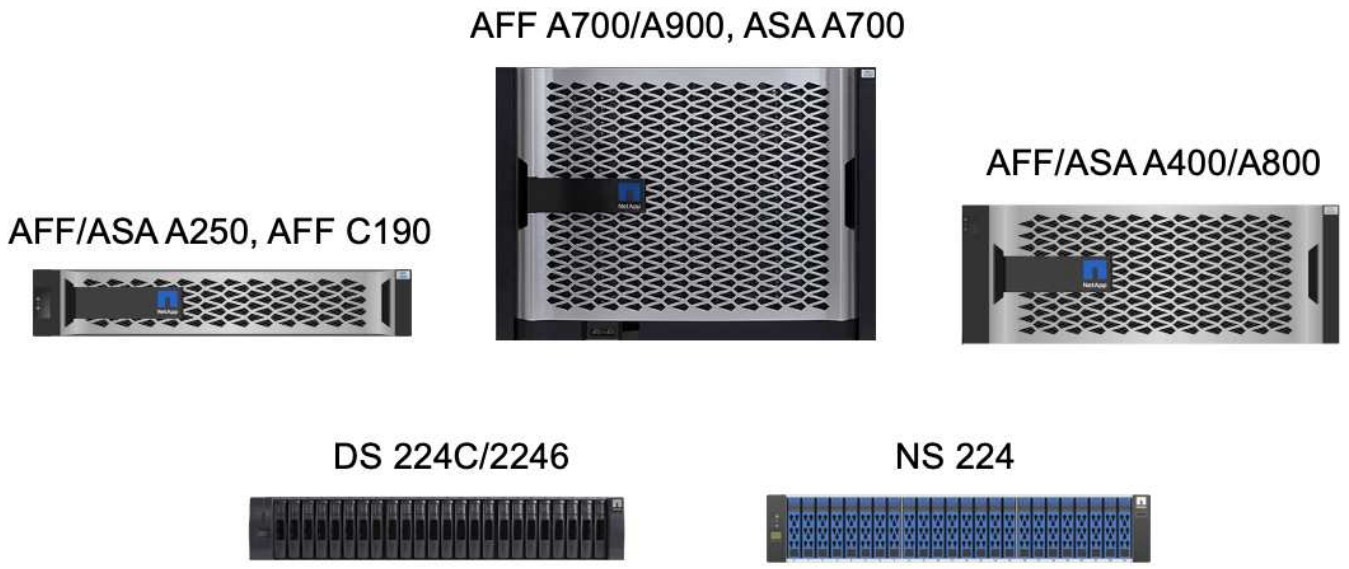
Komponenten von NetApp

Zur Erstellung einer FlexPod SM-BC Lösung sind redundante NetApp AFF oder ASA Controller mit ONTAP Software 9.8 oder neuere Versionen erforderlich. Das aktuelle ONTAP-Release, derzeit 9.10.1, wird für die SM-BC-Implementierung empfohlen, um von den kontinuierlichen ONTAP-Innovationen, Performance- und Qualitätsverbesserungen und der höheren maximalen Anzahl von Objekten für den SM-BC-Support zu profitieren.

NetApp AFF und ASA Controller bieten branchenführende Performance und Innovationen für Datensicherung der Enterprise-Klasse sowie vielseitige Datenmanagementfunktionen. Die AFF und ASA Systeme unterstützen End-to-End-NVMe-Technologien, einschließlich NVMe-Attached SSDs und NVMe over Fibre Channel (NVMe/FC) Front-End-Host-Konnektivität. Mit einer NVMe/FC-basierten SAN-Infrastruktur können Sie den Workload-Durchsatz verbessern und die I/O-Latenz verringern. NVMe/FC-basierte Datastores können jedoch derzeit nur für Workloads genutzt werden, die nicht durch SM-BC geschützt sind, da die SM-BC Lösung derzeit nur iSCSI- und FC-Protokolle unterstützt.

NetApp AFF und ASA Storage-Controller bieten Kunden auch eine Hybrid-Cloud-Grundlage, um von den Vorteilen der nahtlosen Datenmobilität mithilfe der NetApp Data-Fabric-Architektur zu profitieren. Mit Data Fabric lassen sich Daten einfach vom Edge-Bereich in den Core-Bereich verschieben, wo sie verwendet werden, und in die Cloud. So profitieren Sie von den flexiblen On-Demand-Computing- sowie KI- und ML-Funktionen und können damit schneller geschäftliche Einblicke gewinnen.

Wie in der folgenden Abbildung dargestellt, bietet NetApp verschiedene Storage Controller und Festplatten-Shelfs, um Ihre Performance- und Kapazitätsanforderungen zu erfüllen. In der folgenden Tabelle finden Sie Links zu Produktseiten für Informationen zu den Funktionen und Spezifikationen des NetApp AFF und ASA Controllers.

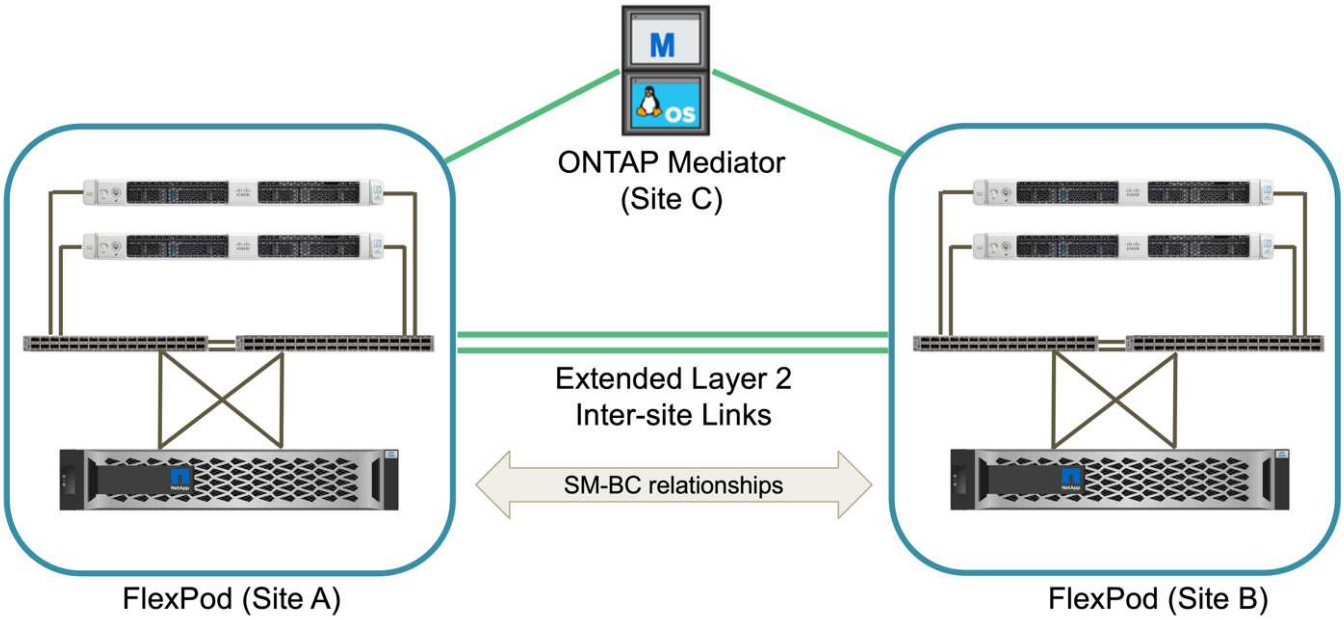


Produktfamilie	Technische Spezifikationen
AFF Serie	"Dokumentation der AFF Serie"
ASA Serie	"Dokumentation der ASA Serie"

Konsultieren Sie die "Dokumentation der Platten-Shelfs und Storage-Medien von NetApp" Und "NetApp Hardware Universe" Weitere Informationen zu den Festplatten-Shelfs und zu unterstützten Platten-Shelfs für jedes Storage-Controller-Modell

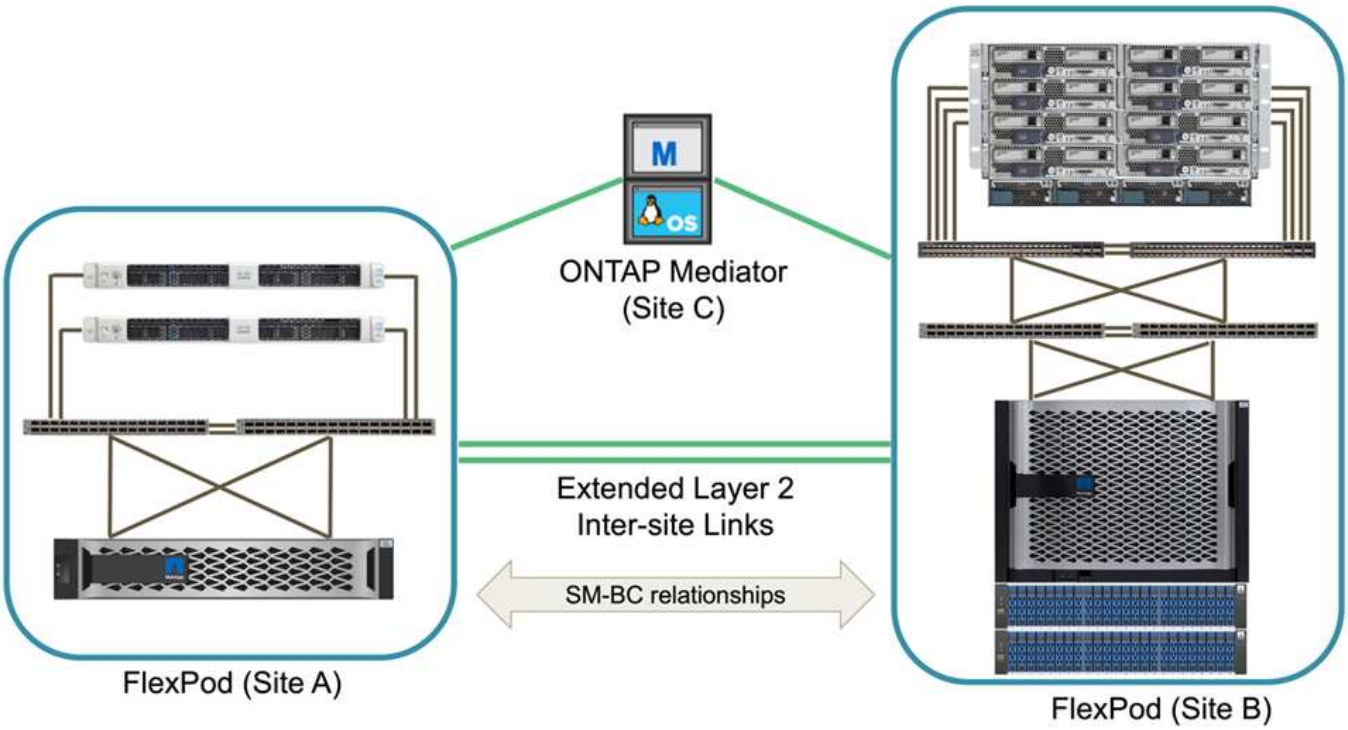
Lösungstopologien

FlexPod Lösungen sind flexibel in der Topologie und lassen sich je nach Anforderungen vertikal oder horizontal skalieren. Eine Lösung, die Business Continuity-Sicherheit erfordert und nur minimale Computing- und Storage-Ressourcen erfordert, kann eine einfache Topologie der Lösung verwenden, wie in der folgenden Abbildung dargestellt. Diese einfache Topologie verwendet Rack-Server der UCS C-Serie und AFF/ASA Controller mit SSDs im Controller ohne zusätzliche Festplatten-Shelfs.



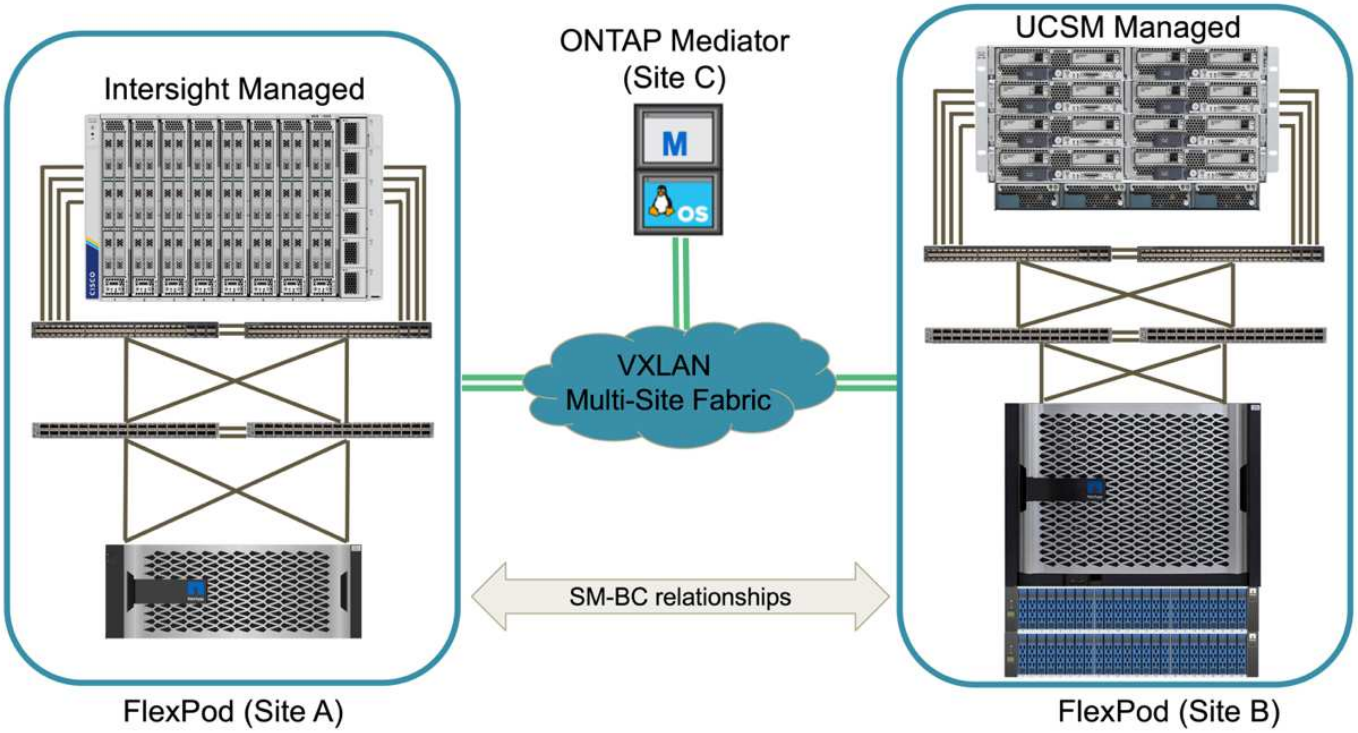
Die redundanten Computing-, Netzwerk- und Storage-Komponenten sind durch die redundante Konnektivität zwischen den Komponenten miteinander verbunden. Dieses hochverfügbare Design bietet eine zuverlässige Lösung, die sich gegen Single Point of Failure-Szenarien aushält. Trotz des standortübergreifenden Designs und der synchronen ONTAP SM-BC Datenreplizierung können geschäftskritische Daten-Services genutzt werden, selbst wenn ein Storage-Ausfall an einem einzigen Standort möglich ist.

Eine asymmetrische Implementierungstopologie, die in Unternehmen zwischen einem Datacenter und einer Niederlassung in einem Großraumgebiet eingesetzt werden kann, könnte wie folgt aussehen: Für dieses asymmetrische Design erfordert das Datacenter ein FlexPod mit höherer Performance und mehr Computing- und Storage-Ressourcen. Die Anforderungen an die Remote-Zweigstelle sind jedoch weniger und können durch eine viel kleinere FlexPod erfüllt werden.

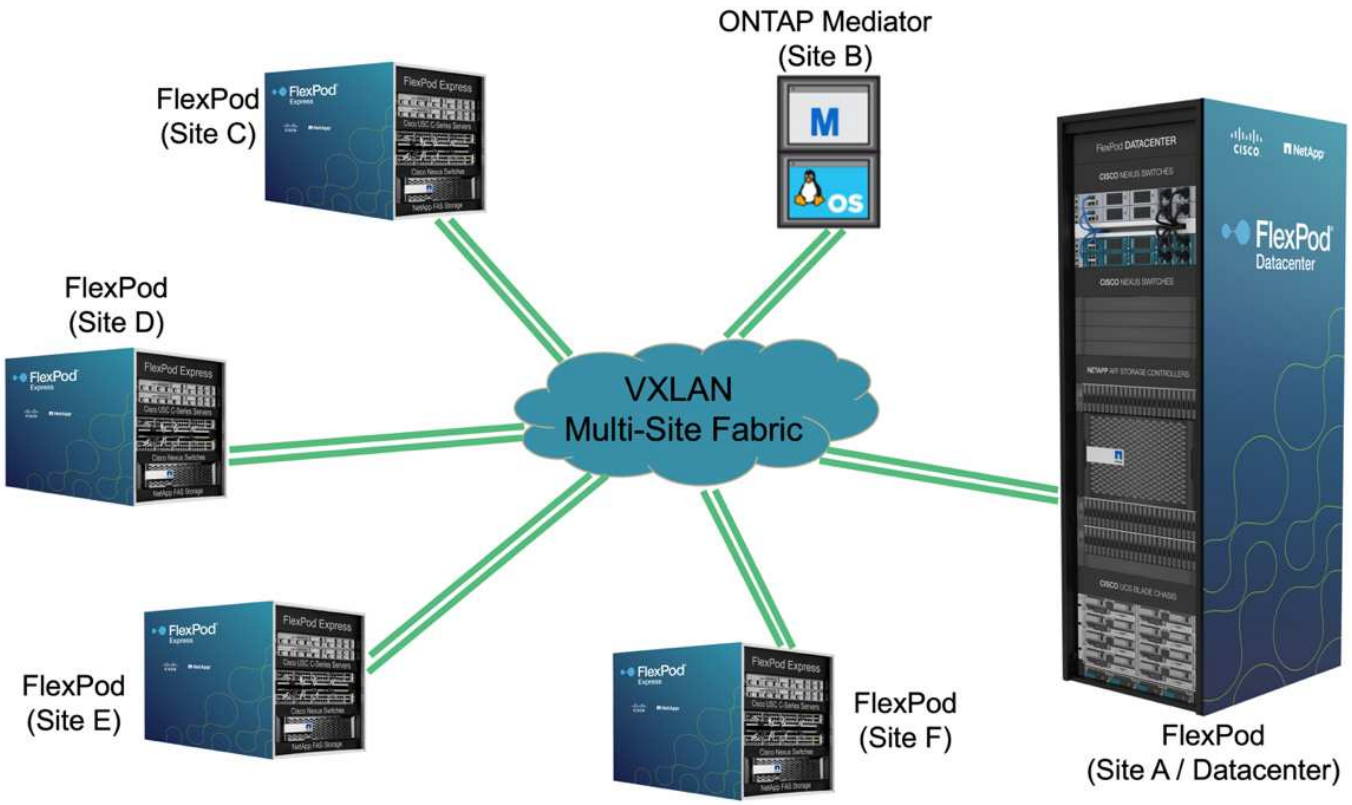


Für Unternehmen mit höheren Anforderungen an Computing- und Storage-Ressourcen und mehreren Standorten verfügt eine VXLAN-basierte Multi-Site-Fabric über eine nahtlose Netzwerk-Fabric-Infrastruktur, die die Applikationsmobilität vereinfacht, sodass eine Applikation von jedem Standort aus bedient werden kann.

Möglicherweise gibt es eine vorhandene FlexPod Lösung mit dem Cisco UCS 5108 Chassis und Blade Servern der B-Serie, die durch eine neue FlexPod Instanz geschützt werden müssen. Die neue FlexPod Instanz nutzt das neueste UCS X9508 Chassis mit X210c Computing Nodes, die von Cisco Intersight gemanagt werden, wie in der folgenden Abbildung dargestellt. In diesem Fall sind die FlexPod Systeme an jedem Standort mit einer größeren Datacenter-Fabric verbunden. Die Standorte sind über ein Interconnect-Netzwerk verbunden und bilden so eine VXLAN Multi-Site Fabric.



Für Unternehmen mit einem Datacenter und mehreren Niederlassungen in einem Großraumgebiet, die alle gesichert werden müssen, um Business Continuity sicherzustellen, Die in der folgenden Abbildung dargestellte FlexPod SM-BC Implementierungstopologie kann implementiert werden, um kritische Applikations- und Datenservices zu sichern und so ein Recovery Point Objective von null und ein Recovery Time Objective von fast null für alle Zweigstellen zu erreichen.



Bei diesem Implementierungsmodell richtet jede Niederlassung die SM-BC-Beziehungen und Consistency Groups ein, die sie für das Datacenter benötigen. Sie müssen die unterstützten SM-BC-Objektgrenzwerte berücksichtigen, sodass die Gesamtwerte für Consistency Group-Beziehungen und Endpunkte die im Datacenter unterstützten Maximalwerte nicht überschreiten.

"Weiter: Übersicht zur Lösungsvalidierung"

Lösungsvalidierung

Lösungsvalidierung – Überblick

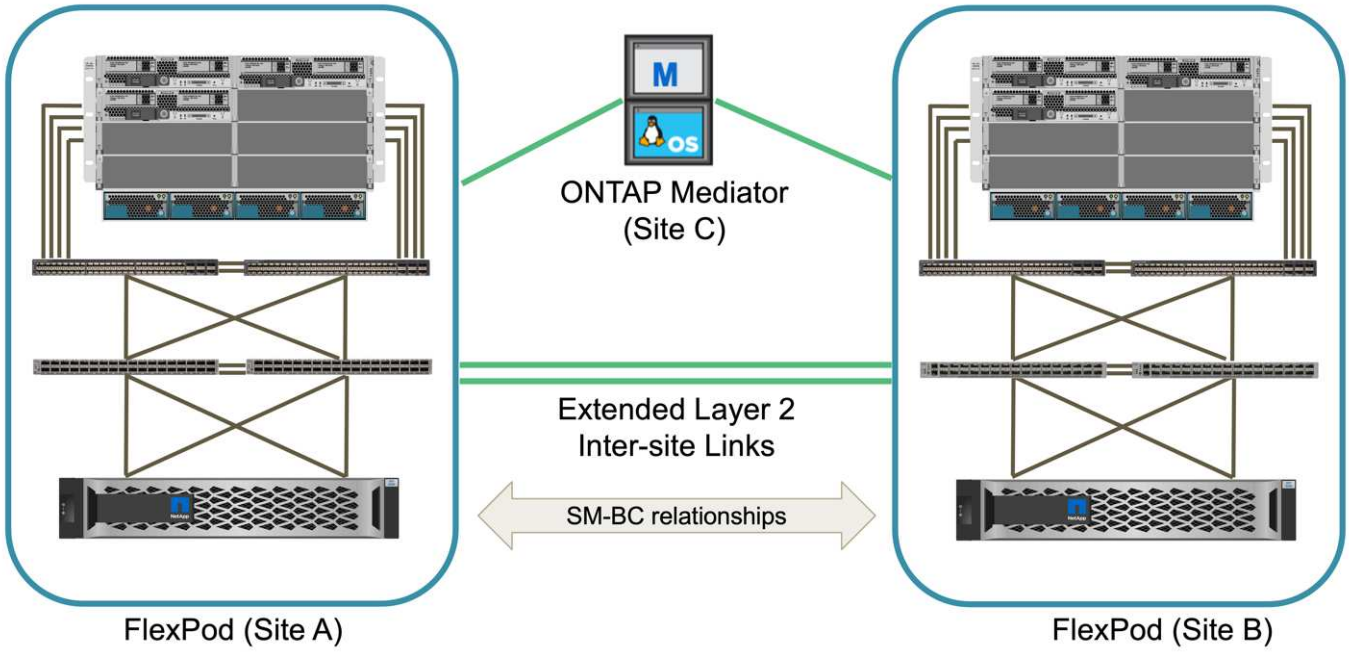
"Früher: FlexPod SM-BC Lösung."

Die Details zum Design und der Implementierung der FlexPod SM-BC Lösung hängen von der jeweiligen Konfiguration der FlexPod-Situation und den jeweiligen Lösungszielen ab. Nach Definition der allgemeinen Business Continuity-Anforderungen kann die FlexPod SM-BC Lösung erstellt werden. Dazu wird eine vollständig neue Lösung mit zwei neuen FlexPod Systemen implementiert, ein neues FlexPod an einem anderen Standort hinzugefügt und mit einem vorhandenen FlexPod gekoppelt oder zwei bestehende FlexPod Systeme verbunden.

Da FlexPod Lösungen in seinen Konfigurationen flexibel sind, können alle unterstützten FlexPod Konfigurationen und Komponenten verwendet werden. Der restliche Abschnitt enthält Informationen zu den Implementierungsprüfungen, die bei einer VMware-basierten virtuellen Infrastrukturlösung durchgeführt werden. Mit Ausnahme der SM-BC bezogenen Aspekte folgt die Implementierung den Standardprozessen des FlexPod Implementierungsauftrages. In den verfügbaren FlexPod CVDs und NVAs finden Sie die jeweiligen Konfigurationen für allgemeine FlexPod-Implementierungsdetails.

Validierungstopologie

Zur Validierung der FlexPod SM-BC Lösung kommen unterstützte Technologiekomponenten von NetApp, Cisco und VMware zum Einsatz. Die Lösung umfasst NetApp AFF A250 HA-Paare mit ONTAP 9.10.1, duale Cisco Nexus 9336C-FX2 Switches an Standort A und duale Cisco Nexus 3232C-Switches am Standort B, Cisco UCS 6454 FIS an beiden Standorten, Und drei Cisco UCS B200 M5 Server an jedem Standort mit VMware vSphere 7.0u2. Sie werden durch UCS Manager und VMware vCenter Server gemanagt. Die folgende Abbildung zeigt die Lösungstopologie auf Komponentenebene mit zwei FlexPod-Systemen, die an Standort A und Standort B ausgeführt werden. Sie sind über erweiterte Layer-2-Verbindungen zwischen Standorten und ONTAP Mediator verbunden, der an Standort C ausgeführt wird



Hardware- und Software-Suite von NetApp

In der folgenden Tabelle sind die für die Lösungsvalidierung verwendete Hardware und Software aufgeführt. Es ist wichtig zu beachten, dass Cisco, NetApp und VMware über Interoperabilitätsmatrixe verfügen, die zur Bestimmung des Supports für jede spezifische Implementierung von FlexPod eingesetzt werden:

- "http://support.netapp.com/matrix/"
- "Cisco UCS Hardware and Software Interoperability Tool"
- "http://www.vmware.com/resources/compatibility/search.php"

Kategorie	Komponente	Softwareversion	Menge
Computing	Cisco UCS Fabric Interconnect 6454	4.2 (1f)	4 (2 pro Standort)
	Cisco UCS B200 M5 Server	4.2 (1f)	6 (3 pro Standort)
	CISCO UCS IOM 2204XP	4.2 (1f)	4 (2 pro Standort)
	CISCO VIC 1440 (PID: UCSB-MLOM-40G-04)	5.2 (1a)	2 (1 pro Standort)

Kategorie	Komponente	Softwareversion	Menge
	CISCO VIC 1340 (PID: UCSB-MLOM-40G-03)	4.5 (1a)	4 (2 pro Standort)
Netzwerk	Cisco Nexus 9336C-FX2	9.3 (6)	2 (Standort A)
	Cisco Nexus 3232C	9.3 (6)	2 (Standort B)
Storage	NetApp AFF A250	9.10.1	4 (2 pro Standort)
	NetApp System Manager	9.10.1	2 (1 pro Standort)
	NetApp Active IQ Unified Manager	9.10	1
	NetApp ONTAP Tools für VMware vSphere	9.10	1
	NetApp SnapCenter Plug-in für VMware vSphere	4.6	1
	NetApp ONTAP Mediator	1.3	1
	NAbox	3.0.2	1
	NetApp Harvest	21.11.1-1	1
Einheitliche	VMware ESXi	7,0U2	6 (3 pro Standort)
	VMware ESXi Nenic Ethernet-Treiber	1.0.35.0	6 (3 pro Standort)
	VMware vCenter	7,0U2	1
	NetApp NFS Plug-in für VMware VAAI	2.0	6 (3 pro Standort)
Tests	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 pro Standort)
	Iometer	1.1.0	6 (3 pro Standort)

"Als Nächstes: Lösungsvalidierung – Computing."

Lösungsvalidierung – Computing

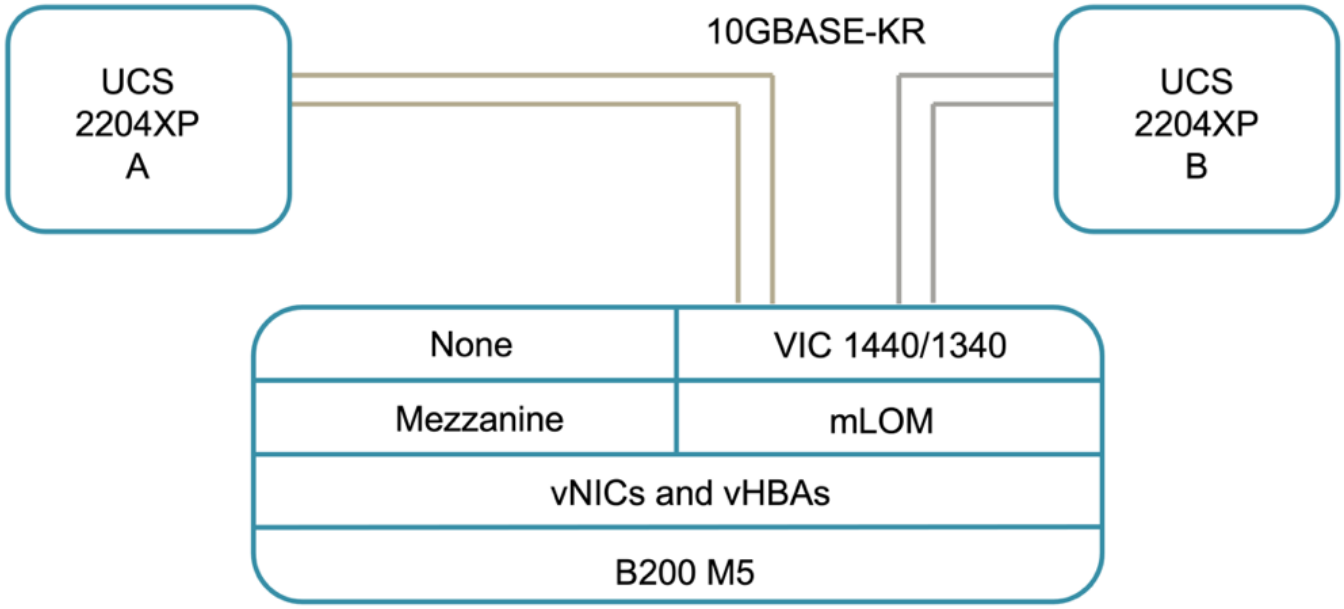
"Preiiwous: Lösungsvalidierung – Überblick."

Die Computing-Konfiguration für die FlexPod SM-BC-Lösung folgt den typischen Best Practices der FlexPod Lösung. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt. Einige Punkte, die im Zusammenhang mit SM-BC zu berücksichtigen sind, geben auch

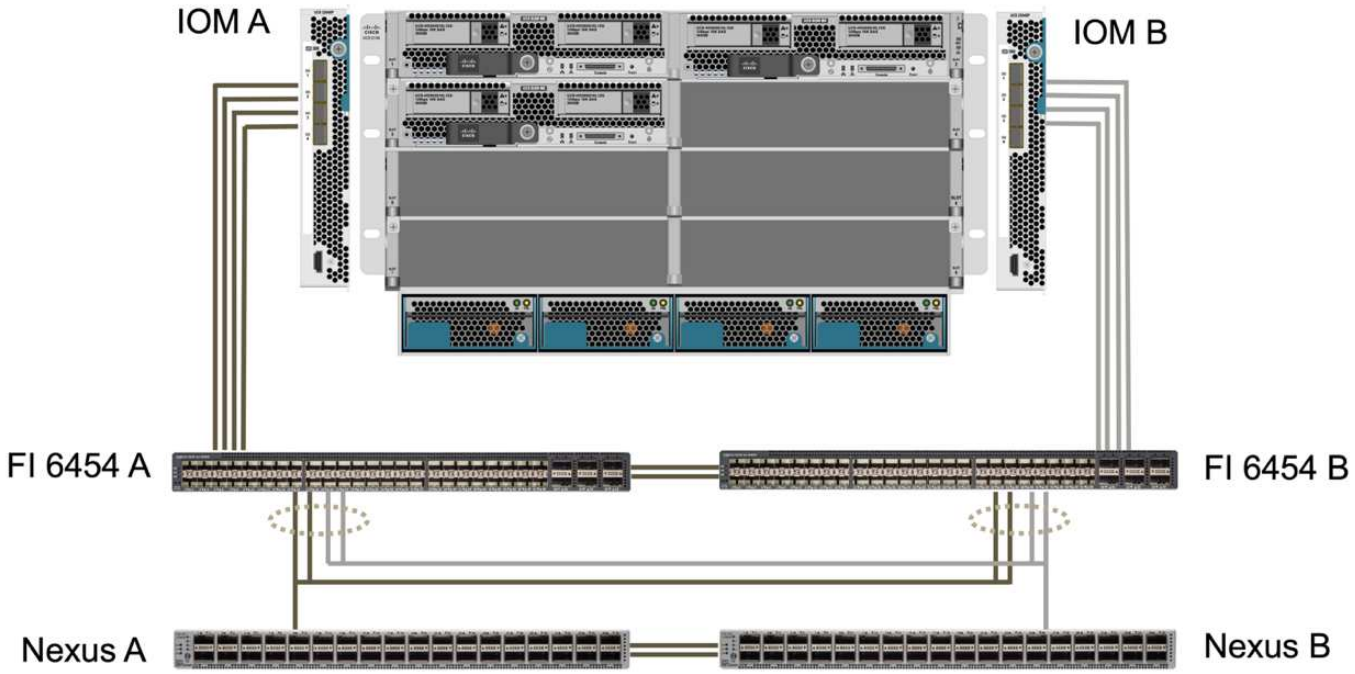
Implementierungsreferenzen und -Anleitungen an.

Konnektivität

Die Konnektivität zwischen den UCS B200 Blade Servern und den IOMs wird durch die UCS VIC-Karte über die UCS 5108 Gehäuse-Backplane-Verbindungen bereitgestellt. Die für die Validierung verwendeten UCS 2204XP Fabric Extender verfügen über sechzehn 10G-Ports, um sich mit den acht Blade Servern mit halber Breite zu verbinden, z. B. zwei für jeden Server. Zur Erhöhung der Server-Konnektivitätsbandbreite kann ein zusätzlicher Mezzanine-basierter VIC hinzugefügt werden, um den Server mit dem alternativen UCS 2408 IOM zu verbinden, das vier 10G-Verbindungen zu jedem Server bietet.



Die Konnektivität zwischen dem UCS 5108 Gehäuse und dem für die Validierung verwendeten UCS 6454 FIS wird durch das IOM 2204XP bereitgestellt, welches vier 10G-Verbindungen verwendet. Die FI-Ports 1 bis 4 sind als Serveranschlüsse für diese Verbindungen konfiguriert. Die FI-Ports 25 bis 28 sind als Netzwerk-Uplink-Ports zum Nexus-Switch A und B am lokalen Standort konfiguriert. Die folgende Abbildung und Tabelle enthalten das Konnektivitätsdiagramm und die Details zur Port-Verbindung, mit denen UCS 6454 FIS eine Verbindung zum UCS 5108-Chassis und den Nexus-Switches herstellen kann.



Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
UCS 6454 FI A	1	IOM A	1
	2		2
	3		3
	4		4
	25	Nexus A	1/13/1
	26		1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus A	1/13/3
	26		1/13/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
	L2		L2

Die obigen Verbindungen sind für beide Standorte A und B ähnlich, trotz Standort A mit Nexus 9336C-FX2Switches und Standort B mit Nexus 3232C-Switches. Breakout-Kabel von 40G bis 4X10G werden für den Nexus für FI-Verbindungen verwendet. Die FI-Verbindungen zu Nexus nutzen Port-Channel und virtuelle Port-Kanäle sind auf den Nexus-Switches konfiguriert, um die Verbindungen zu jedem FI aggregieren.

Wenn Sie eine andere Kombination aus IOM, FI und Nexus Switch-Komponenten verwenden, achten Sie bei der Kombination der Umgebung auf die entsprechenden Kabel und die Port-Geschwindigkeit.

Zusätzliche Bandbreite lässt sich durch Komponenten erreichen, die Verbindungen mit höherer Geschwindigkeit oder mehr Verbindungen unterstützen. Zusätzliche Redundanz lässt sich durch Hinzufügen weiterer Verbindungen mit Komponenten erreichen, die diese unterstützen.

Serviceprofile

Ein Blade Server Chassis mit Fabric Interconnects, das von UCS Manager (UCSM) oder Cisco Intersight gemanagt wird, kann die Server durch Nutzung von Service-Profilen abstrahieren, die in UCSM und Server-Profilen in Intersight verfügbar sind. Diese Validierung nutzt UCSM und Serviceprofile, um das Server Management zu vereinfachen. Mithilfe von Serviceprofilen können Sie einen Server einfach durch die Verknüpfung des ursprünglichen Serviceprofils mit der neuen Hardware ersetzen oder aktualisieren.

Die erstellten Serviceprofile unterstützen für VMware ESXi Hosts Folgendes:

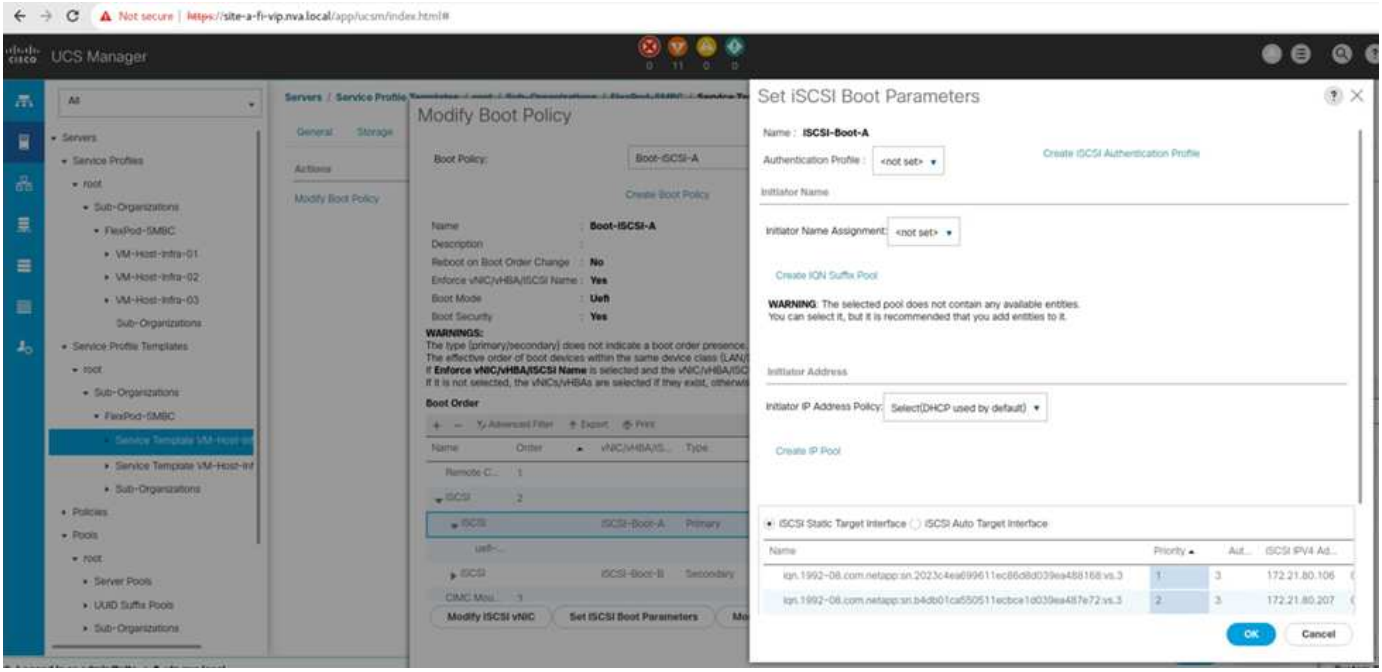
- SAN startet über den AFF A250-Storage an beiden Standorten mit iSCSI-Protokoll.
- Sechs vNICs werden für die Server erstellt, in denen:
  - Zwei redundante vNICs (vSwitch0-A und vSwitch0-B) tragen den in-Band-Management-Traffic. Optional können diese vNICs auch mit NFS-Protokolldaten verwendet werden, die nicht durch SM-BC geschützt sind.
  - Zwei redundante vNICs (VdS-A und VdS-B) werden vom vSphere Distributed Switch verwendet, um VMware vMotion und anderen Applikationsdatenverkehr zu transportieren.
  - ISCSI-A vNIC verwendet von iSCSI-A vSwitch, um Zugriff auf iSCSI-A-Pfad zu bieten.
  - ISCSI-B vNIC, die von iSCSI-B vSwitch verwendet wird, um Zugriff auf den iSCSI-B-Pfad zu ermöglichen.

SAN Booting

Für die iSCSI-SAN-Startkonfiguration sind die iSCSI-Startparameter so eingestellt, dass iSCSI von beiden iSCSI-Fabrics aus gestartet werden kann. Um das SM-BC Failover-Szenario unterzubringen, in dem ein iSCSI SAN Boot LUN vom sekundären Cluster bereitgestellt wird, wenn das primäre Cluster nicht verfügbar ist, sollte die statische iSCSI-Zielkonfiguration Ziele sowohl von Standort A als auch von Standort B umfassen Um die Boot-LUN-Verfügbarkeit zu maximieren, konfigurieren Sie darüber hinaus die iSCSI-Boot-Parameter-Einstellungen, damit sie von allen Storage Controllern gebootet werden können.

Das statische iSCSI-Ziel kann in der Boot-Policy der Service-Profile-Vorlagen unter dem Dialogfeld Set iSCSI Boot Parameter konfiguriert werden, wie in der folgenden Abbildung dargestellt. Die empfohlene Konfiguration für den iSCSI-Boot-Parameter ist in der folgenden Tabelle dargestellt, welche die oben beschriebene Boot-

Strategie implementiert, um eine hohe Verfügbarkeit zu erreichen.



ISCSI Fabric	Priorität	ISCSI-Ziel	ISCSI LIF
ISCSI A	1	ISCSI-Ziel Standort A	Standort A Controller 1 iSCSI A LIF
	2	ISCSI-Ziel Standort B	Standort B Controller 2 iSCSI A LIF
ISCSI B	1	ISCSI-Ziel Standort B	Standort B Controller 1 iSCSI B LIF
	2	ISCSI-Ziel Standort A	Standort A Controller 2 iSCSI B LIF

"Weiter: Lösungsvalidierung – Netzwerk."

Lösungsvalidierung – Netzwerk

"Früher: Lösungsvalidierung – Computing."

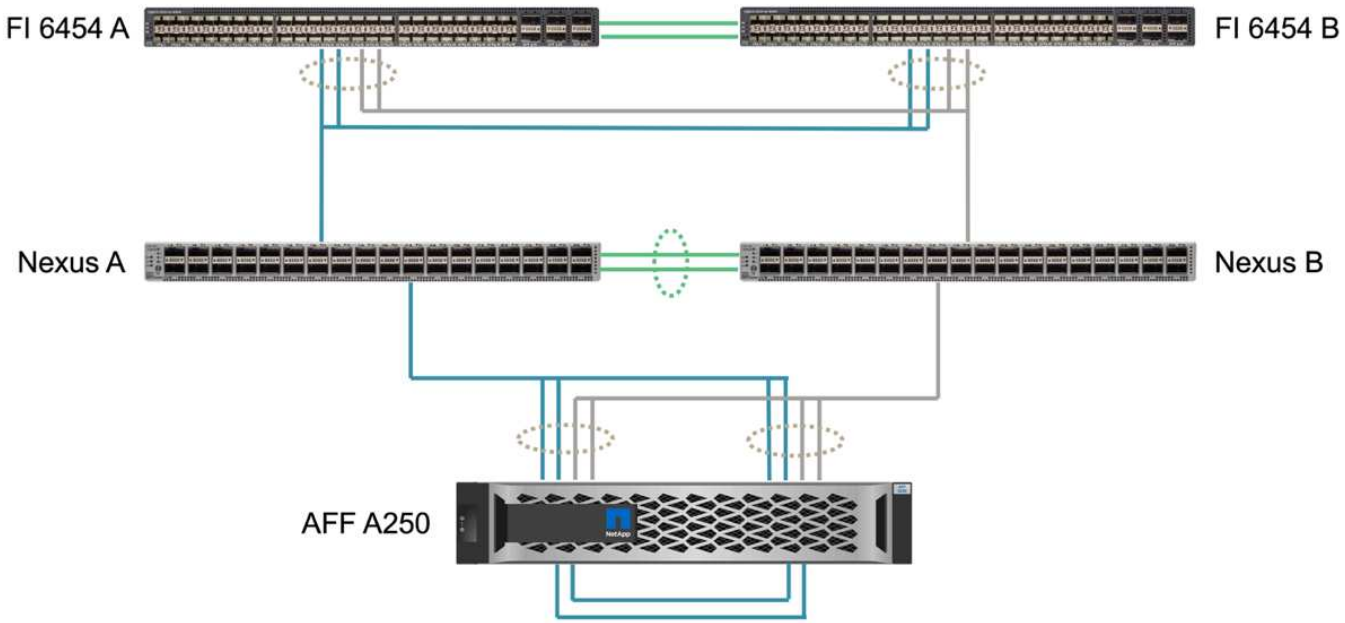
Die Netzwerkkonfiguration für die FlexPod SM-BC Lösung folgt an jedem Standort den typischen Best Practices der FlexPod Lösung. Für die Konnektivität zwischen Standorten werden die FlexPod Nexus Switches an beiden Standorten über die Lösungsvalidierung miteinander verbunden. So wird für Verbindungen zwischen den Standorten zwischen den beiden Standorten hergestellt, was die VLANs zwischen den beiden Standorten erweitert. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt.

Konnektivität

Die FlexPod Nexus Switches an jedem Standort sorgen in einer hochverfügbaren Konfiguration für die lokale Konnektivität zwischen UCS Computing und ONTAP Storage. Die redundanten Komponenten und die

redundante Konnektivität bieten die Ausfallsicherheit bei Single-Point-of-Failure-Szenarien.

Das folgende Diagramm zeigt die lokale Konnektivität von Nexus Switch an den einzelnen Standorten. Neben den im Diagramm dargestellten Informationen gibt es für jede Komponente auch Konsolen- und Management-Netzwerkverbindungen. Die 40G bis 4 x 10G-Breakout-Kabel werden zur Verbindung der Nexus-Switches mit dem UCS FIS und den ONTAP AFF A250 Storage Controllern verwendet. Alternativ können Sie mit den 100 G bis 4 x 25 G Breakout Kabeln die Kommunikationsgeschwindigkeit zwischen den Nexus Switches und den AFF A250 Storage Controllern erhöhen. Zur Vereinfachung werden die beiden AFF A250-Controller zur Verkabelungsabbildung logisch nebeneinander dargestellt. Dank der beiden Verbindungen zwischen den beiden Storage Controllern kann der Storage ein Cluster ohne Switches bilden.

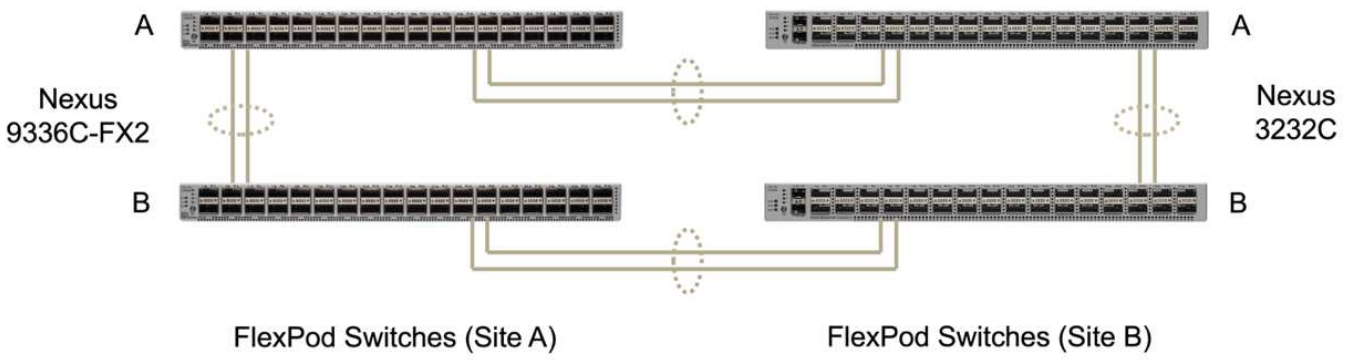


Die folgende Tabelle zeigt die Konnektivität zwischen Nexus Switches und AFF A250 Storage-Controllern an jedem Standort.

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Nexus A	1/10/1	AFF A250 A	e1a
	1/10/2		e1b
	1/10/3	AFF A250 B	e1a
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B	e1c
	1/10/4		e1d

Die Konnektivität zwischen den FlexPod-Switches an Standort A und Standort B ist in der folgenden Abbildung dargestellt. Die entsprechende Verkabelung ist in der Tabelle aufgeführt. Die Verbindungen zwischen den beiden Switches an jedem Standort gelten für die vPC-Peer-Links. Auf der anderen Seite stellen die Verbindungen zwischen den Switches über die Standorte hinweg die Verbindungen zwischen den Standorten dar. Die Links erweitern die VLANs auf mehrere Standorte für Cluster-übergreifende Kommunikation, SM-BC

Datenreplizierung, in-Band-Management und Datenzugriff für die Ressourcen des Remote-Standorts.



Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Standort A Schalter A	33	Schalter A Standort B	31
	34		32
	25	Standort A Schalter B	25
	26		26
Standort A Schalter B	33	Schalter B an Standort B	31
	34		32
	25	Standort A Schalter A	25
	26		26
Schalter A Standort B	31	Standort A Schalter A	33
	32		34
	25	Schalter B an Standort B	25
	26		26
Schalter B an Standort B	31	Standort A Schalter B	33
	32		34
	25	Schalter A Standort B	25
	26		26

In der Tabelle oben ist die Konnektivität aus der Perspektive jedes FlexPod Switches aufgeführt. Die Tabelle enthält daher doppelte Informationen zur Lesbarkeit.

Port Channel und virtueller Port Channel

Port Channel ermöglicht die Link-Aggregation mithilfe des Link Aggregation Control Protocol (LACP) für Bandbreitenaggregation und Ausfallsicherheit bei Link-Ausfällen. Über den virtuellen Port-Kanal (vPC) können die Port-Channel-Verbindungen zwischen zwei Nexus-Switches logisch als eine angezeigt werden. Dadurch wird die Ausfallsicherheit bei Szenarien wie dem Ausfall einer einzelnen Verbindung oder eines Single Switch noch weiter verbessert.

Der UCS Server-Datenverkehr zum Storage nimmt Pfade Von IOM A zu FI A und IOM B zu FI B vor dem Erreichen der Nexus-Switches. Da DIE FI-Verbindungen zu Nexus Switches auf DER FI-Seite Port Channel und der virtuelle Port Channel auf der Nexus Switch-Seite nutzen, kann der UCS Server Pfade über beide Nexus Switches effektiv nutzen und gegen Single Point-of-Failure-Szenarien überleben. Zwischen den beiden Standorten sind die Nexus Switches miteinander verbunden, wie in der vorherigen Abbildung dargestellt. Je zwei Links können die Switch-Paare zwischen den Standorten verbunden werden, und sie verwenden zudem eine Port-Channel-Konfiguration.

Die Konnektivität zwischen in-Band-Management, Clustern und iSCSI/NFS Daten-Storage-Protokollen wird bereitgestellt, indem die Storage-Controller an jedem Standort in einer redundanten Konfiguration mit den lokalen Nexus-Switches verbunden werden. Jeder Storage-Controller ist mit zwei Nexus-Switches verbunden. Die vier Verbindungen werden als Teil einer Schnittstellengruppe auf dem Storage konfiguriert, um die Ausfallsicherheit zu erhöhen. Beim Nexus Switch sind diese Ports auch Teil eines vPC zwischen den Switches.

In der folgenden Tabelle sind die Port-Channel-ID und die Port-Nutzung an jedem Standort aufgeführt.

Port-Kanal-ID	Zu Verwenden
10	Lokale Nexus Peer-Verbindung
15	Fabric Interconnect A-Links
16	Fabric Interconnect B-Links
27	Storage Controller A-Links
28	Storage Controller B-Links
100	Wechseln Sie zwischen den Standorten A-Links
200	Switch B-Links zwischen Standorten

VLANs

In der folgenden Tabelle sind für das Einrichten der Validierungsumgebung der FlexPod SM-BC-Lösung und ihrer Verwendung konfigurierte VLANs aufgeführt.

Name	VLAN-ID	Zu Verwenden
Natives VLAN	2	VLAN 2 wird als natives VLAN statt Standard-VLAN verwendet (1)
OOB-MGMT-VLAN	3333	Out-of-Band-Management-VLAN für Geräte
IB-MGMT-VLAN	3334	In-Band-Management-VLAN für ESXi Hosts, VM Management usw.
NFS-VLAN	3335	Optionales NFS VLAN für NFS-Verkehr
ISCSI-A-VLAN	3336	ISCSI-A Fabric-VLAN für iSCSI-Datenverkehr
ISCSI-B-VLAN	3337	ISCSI-B Fabric-VLAN für iSCSI-Datenverkehr
VMotion-VLAN	3338	VMware vMotion Traffic VLAN
VM-Traffic – VLAN	3339	VMware VM Traffic VLAN

Name	VLAN-ID	Zu Verwenden
Intercluster-VLAN	3340	Intercluster-VLAN für ONTAP Cluster Peer Communications

SM-BC unterstützt zwar keine NFS- oder CIFS-Protokolle für Business Continuity, Sie können diese jedoch auch für Workloads einsetzen, die nicht zur Gewährleistung der Business Continuity gesichert werden müssen. NFS-Datastores wurden für diese Validierung nicht erstellt.

"Weiter: Lösungsvalidierung – Storage."

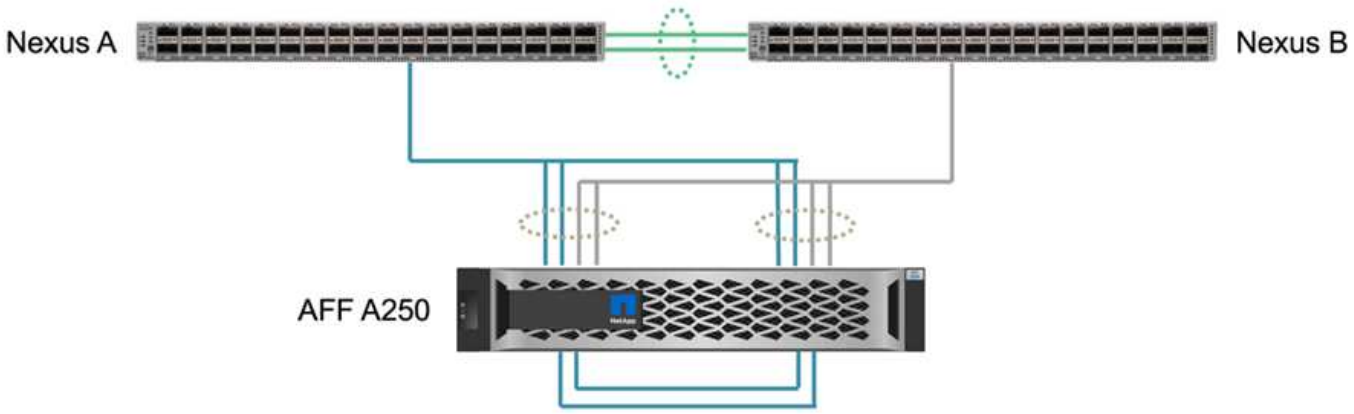
Lösungsvalidierung: Storage

"Zurück: Lösungsvalidierung - Netzwerk."

Die Storage-Konfiguration für die FlexPod SM-BC Lösung folgt den typischen Best Practices der FlexPod Lösung an jedem Standort. Für SM-BC Cluster-Peering und Datenreplizierung verwenden sie die Verbindungen zwischen den Standorten, die zwischen den FlexPod Switches an beiden Standorten hergestellt wurden. In den folgenden Abschnitten werden einige der für die Validierung verwendeten Konnektivität und Konfigurationen vorgestellt.

Konnektivität

Die Storage-Konnektivität mit den lokalen UCS FIS- und Blade-Servern wird von den Nexus Switches am lokalen Standort bereitgestellt. Durch die Nexus Switch-Konnektivität zwischen Standorten kann auch von den Remote UCS Blade Servern auf den Storage zugegriffen werden. Die folgende Abbildung und Tabelle zeigen das Storage-Konnektivitätsdiagramm und eine Liste der Verbindungen für die Storage-Controller an jedem Standort.



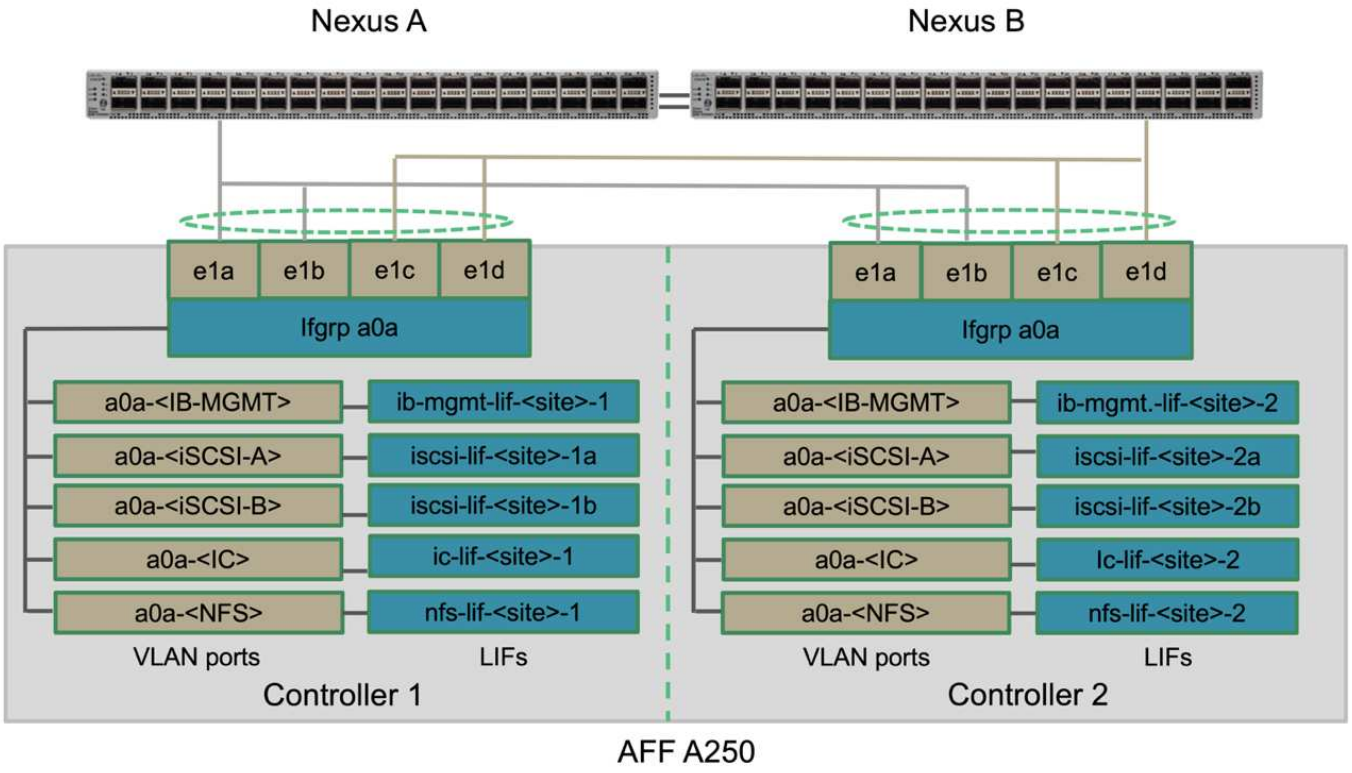
Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
AFF A250 A	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A	1/10/1
	e1b		1/10/2

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B	e0c	AFF A250 A	e0c
	e0d		e0d
	e1a	Nexus A	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

Verbindungen und Schnittstellen

Zwei physische Ports an jedem Storage-Controller sind für diese Validierung mit jedem Nexus-Switch verbunden, um die Bandbreitenaggregation und Redundanz zu gewährleisten. Diese vier Verbindungen nehmen an einer Schnittstellengruppenkonfiguration auf dem Speicher Teil. Die entsprechenden Ports auf den Nexus Switches teilen sich für die Link-Aggregation und Ausfallsicherheit in einem vPC.

Die Storage-Protokolle für das in-Band-Management, Cluster-übergreifende und NFS/iSCSI-Daten verwenden VLANs. VLAN-Ports werden auf der Interface Group erstellt, um die verschiedenen Arten von Datenverkehr zu trennen. Logische Schnittstellen (LIFs) für die jeweiligen Funktionen werden auf den entsprechenden VLAN-Ports erstellt. Die folgende Abbildung zeigt die Beziehung zwischen den physischen Verbindungen, Schnittstellengruppen, VLAN-Ports und logischen Schnittstellen.

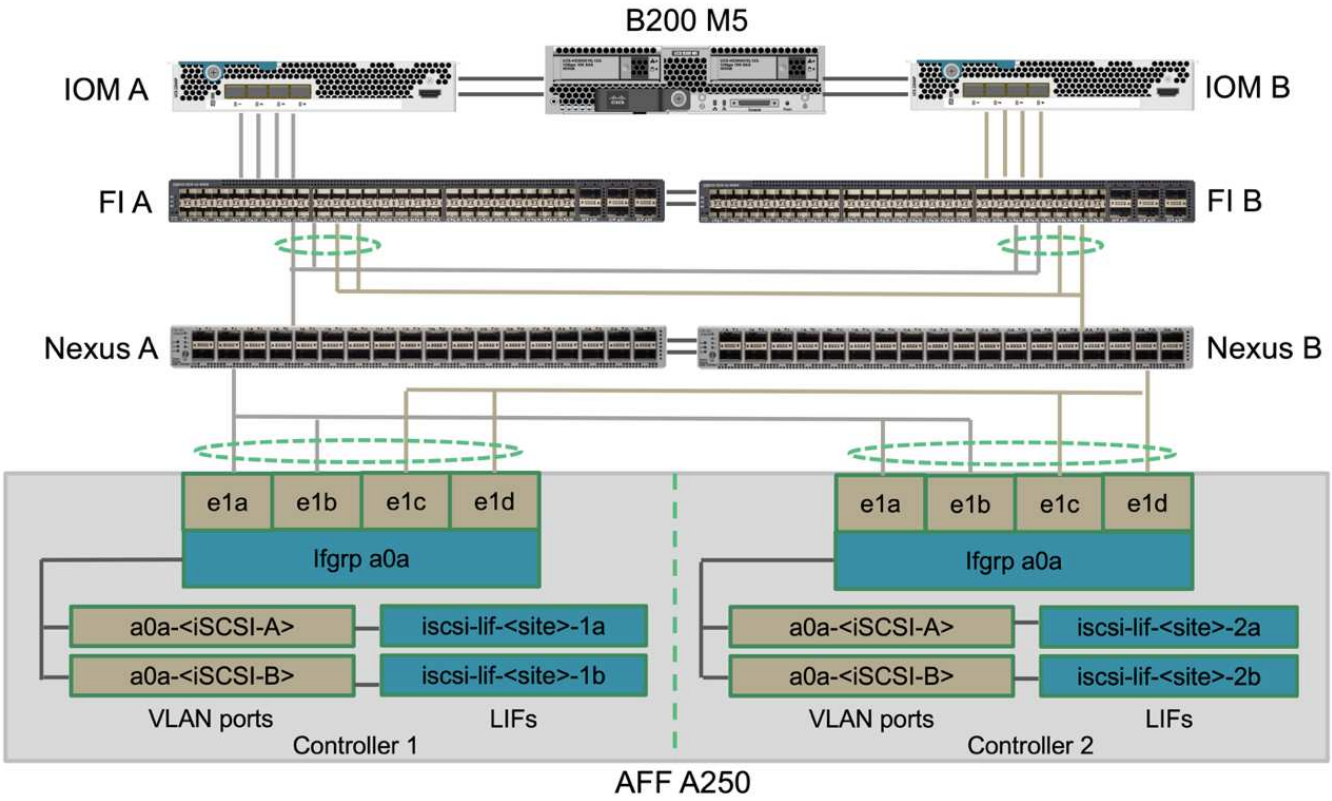


SAN Booting

NetApp empfiehlt, SAN-Boot für die Cisco UCS Server in der FlexPod Lösung zu implementieren. Die Implementierung von SAN Boot ermöglicht die sichere Sicherung des Betriebssystems im NetApp Storage-System und bietet höhere Performance und Flexibilität. Für diese Lösung wurde iSCSI SAN-Boot validiert.

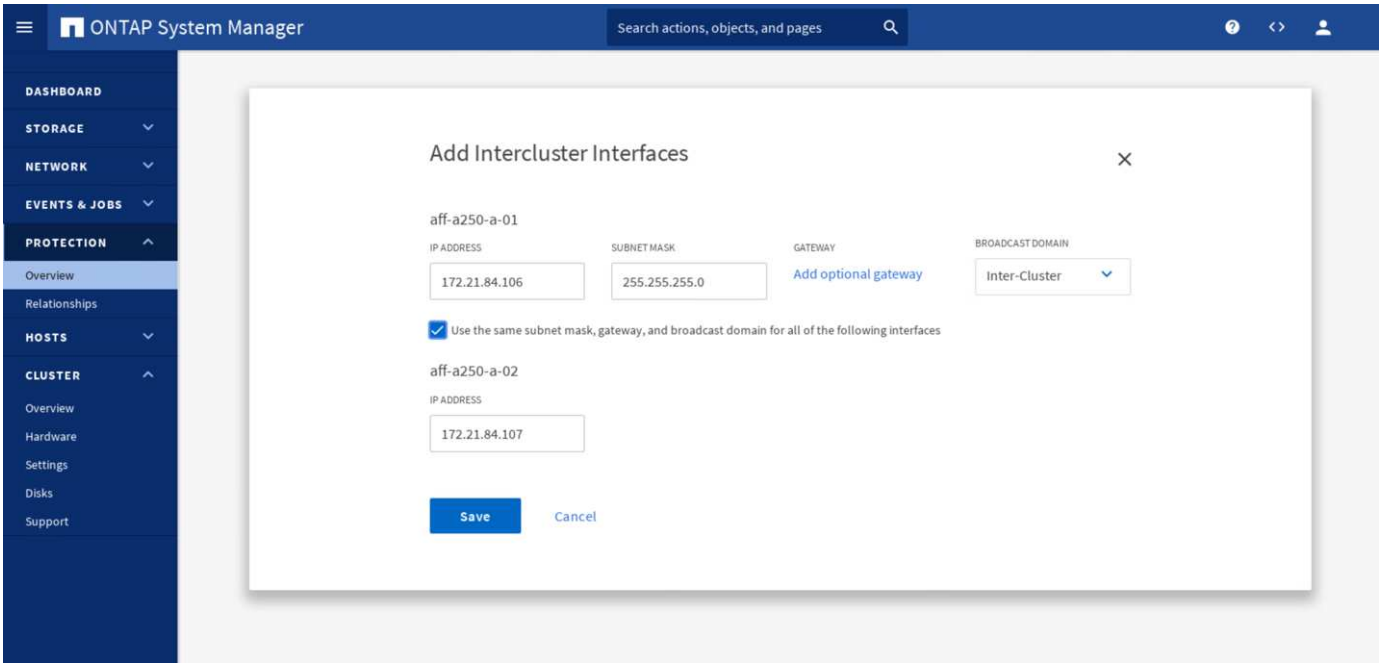
Die folgende Abbildung zeigt die Konnektivität für das iSCSI-SAN-Booten des Cisco UCS Servers aus NetApp Storage. Bei iSCSI SAN Boot wird jedem Cisco UCS Server zwei iSCSI vNICs zugewiesen (einer für jede SAN-Fabric), die redundante Konnektivität vom Server bis zum Storage bieten. Die 10/25-G Ethernet Storage Ports, die mit den Nexus Switches verbunden sind (in diesem Beispiel e1a, e1b, e1c und e1d), werden zu einer Interface Group (ifgrp) (in diesem Beispiel, a0a) gruppiert. Die iSCSI VLAN-Ports werden auf dem ifgrp erstellt, und die iSCSI LIFs werden auf den iSCSI VLAN-Ports erstellt.

Jede iSCSI-Boot-LUN wird dem Server zugeordnet, der von ihm über die iSCSI-LIFs bootet, indem die Boot-LUN mit den iSCSI-qualifizierten Namen (IQNs) des Servers in seiner Boot-Initiatorgruppe verknüpft wird. Die Boot-iGroup des Servers enthält zwei IQNs, eine für jede vNIC / SAN-Fabric. Mit dieser Funktion kann nur der autorisierte Server auf die speziell für diesen Server erstellte Boot-LUN zugreifen.



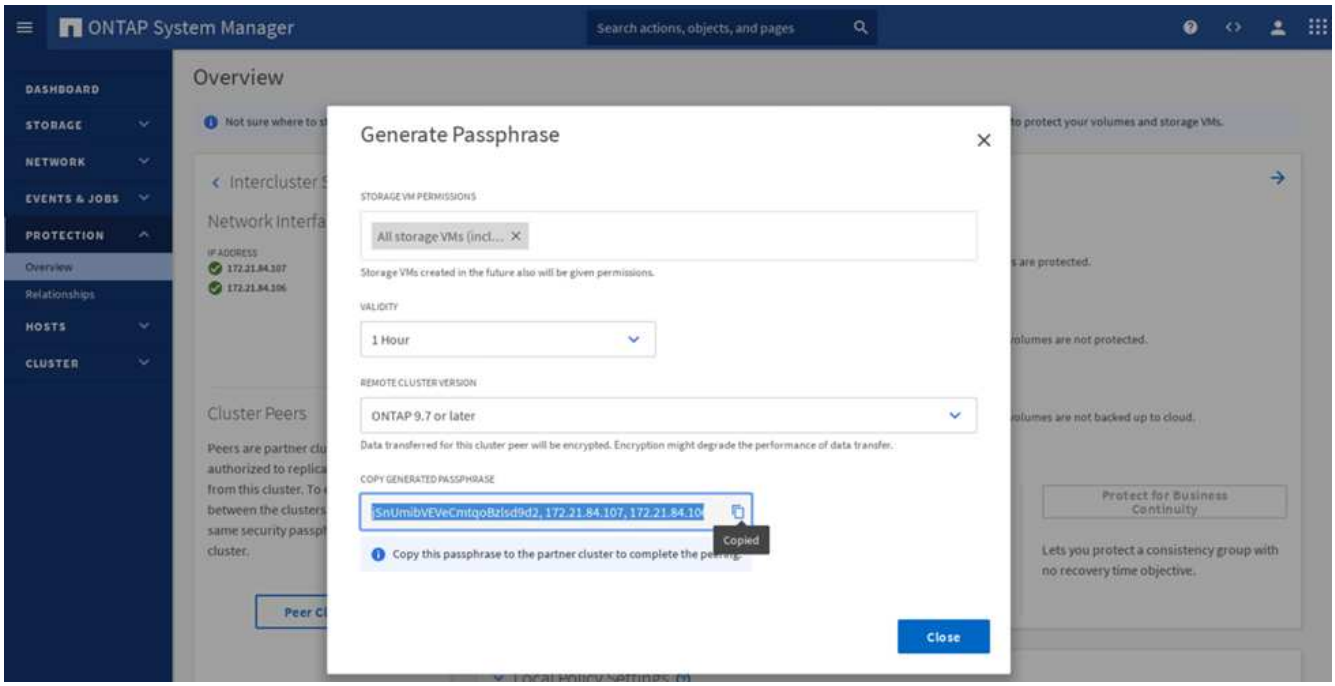
Cluster-Peering

ONTAP Cluster Peers kommunizieren über die Intercluster LIFs. Mit ONTAP System Manager für die beiden Cluster können Sie im Teilfenster „Schutz“ > „Übersicht“ die erforderlichen Intercluster-LIFs erstellen.

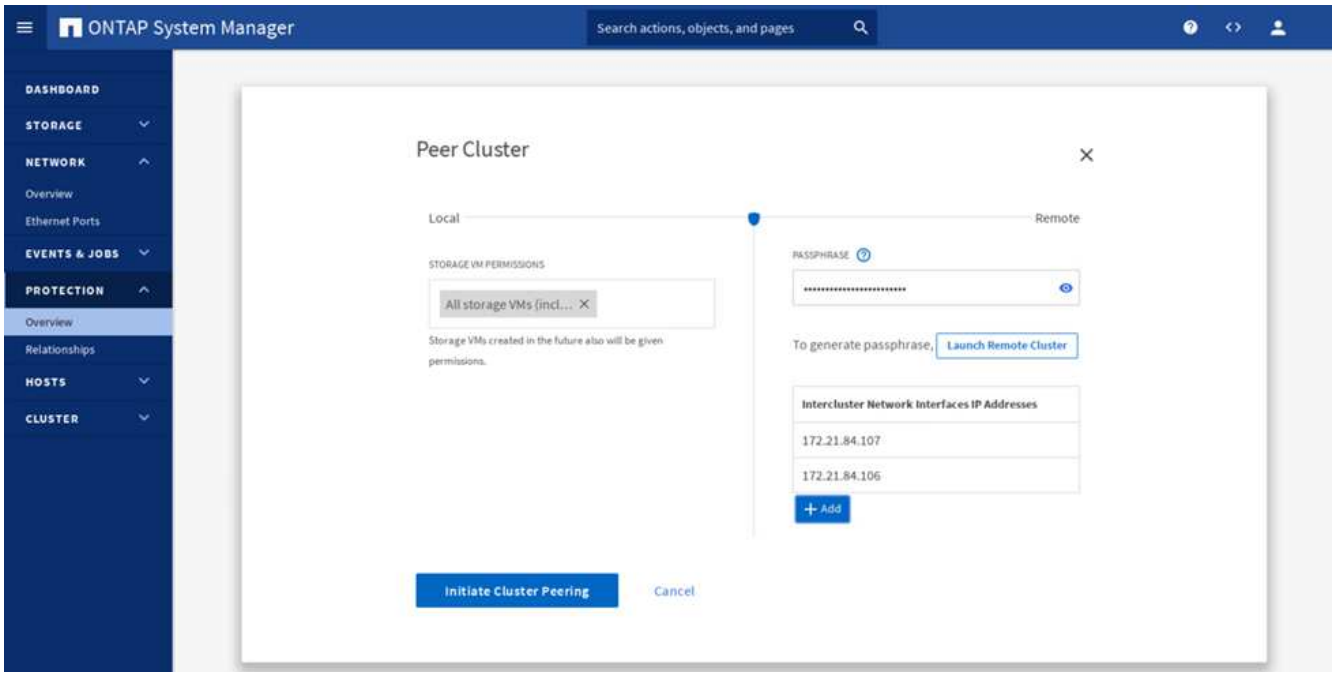


Gehen Sie wie folgt vor, um die beiden Cluster miteinander zu verbinden:

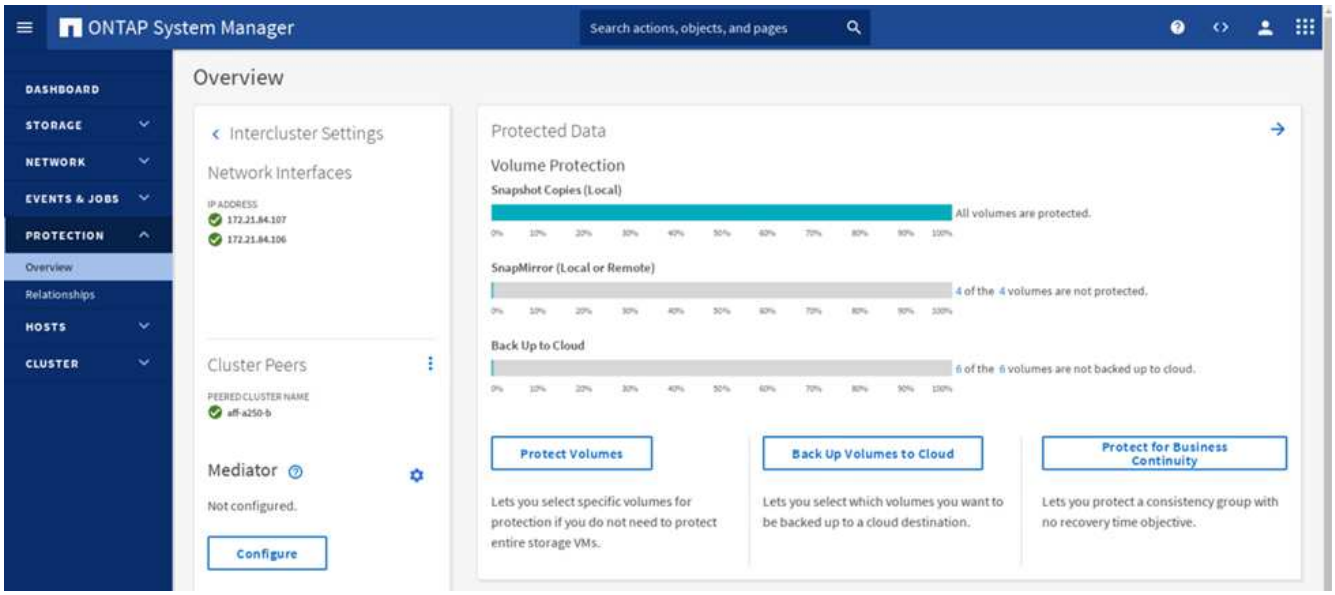
1. Erzeugen einer Cluster-Peering-Passphrase im ersten Cluster



2. Rufen Sie die Peer Cluster-Option im zweiten Cluster auf und stellen Sie die LIF-Informationen für Passphrase und Intercluster bereit.



3. Im Teilfenster System Manager Protection > Overview werden Cluster-Peer-Informationen angezeigt.

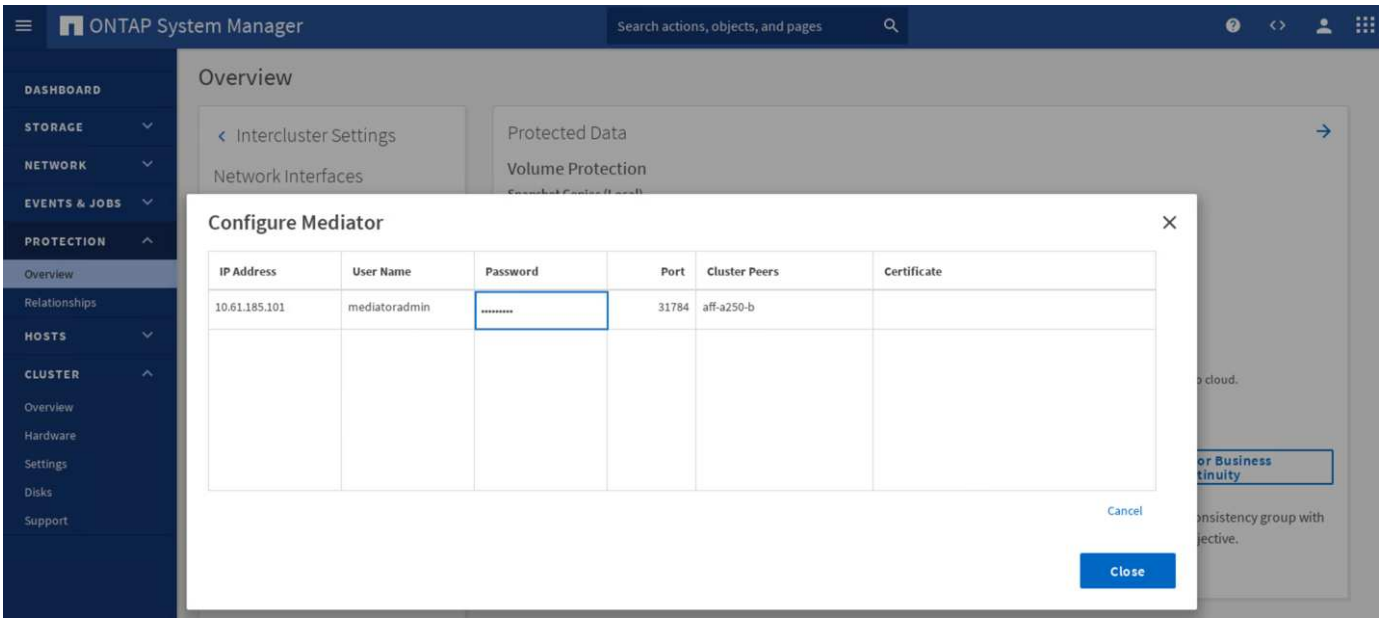


Installation und Konfiguration des ONTAP Mediators

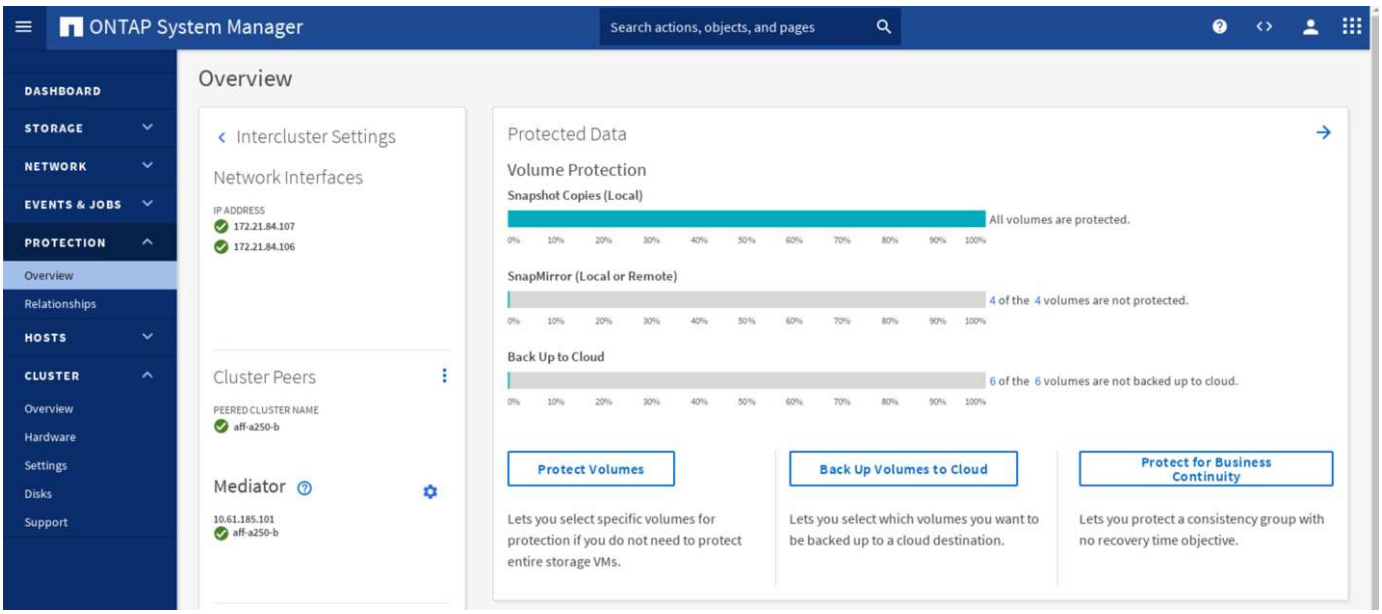
Der ONTAP Mediator stellt ein Quorum für die ONTAP Cluster in einer SM-BC Beziehung her. Es koordiniert das automatisierte Failover, wenn ein Fehler erkannt wird, und vermeidet Split-Brain-Szenarien, wenn jedes Cluster gleichzeitig versucht, die Kontrolle als primäres Cluster zu etablieren.

Bevor Sie den ONTAP Mediator installieren, überprüfen Sie den "Installieren oder aktualisieren Sie den ONTAP Mediator-Dienst" Seite für Voraussetzungen, unterstützte Linux-Versionen und die Verfahren für die Installation auf den verschiedenen unterstützten Linux-Betriebssystemen.

Nach der Installation des ONTAP Mediators können Sie das Sicherheitszertifikat des ONTAP Mediators zu den ONTAP Clustern hinzufügen und dann den ONTAP Mediator im Fenster System Manager Protection > Overview konfigurieren. Der folgende Screenshot zeigt die ONTAP Mediator Konfiguration GUI.



Nachdem Sie die erforderlichen Informationen bereitgestellt haben, wird der konfigurierte ONTAP-Mediator im Fenster System Manager-Schutz > Übersicht angezeigt.



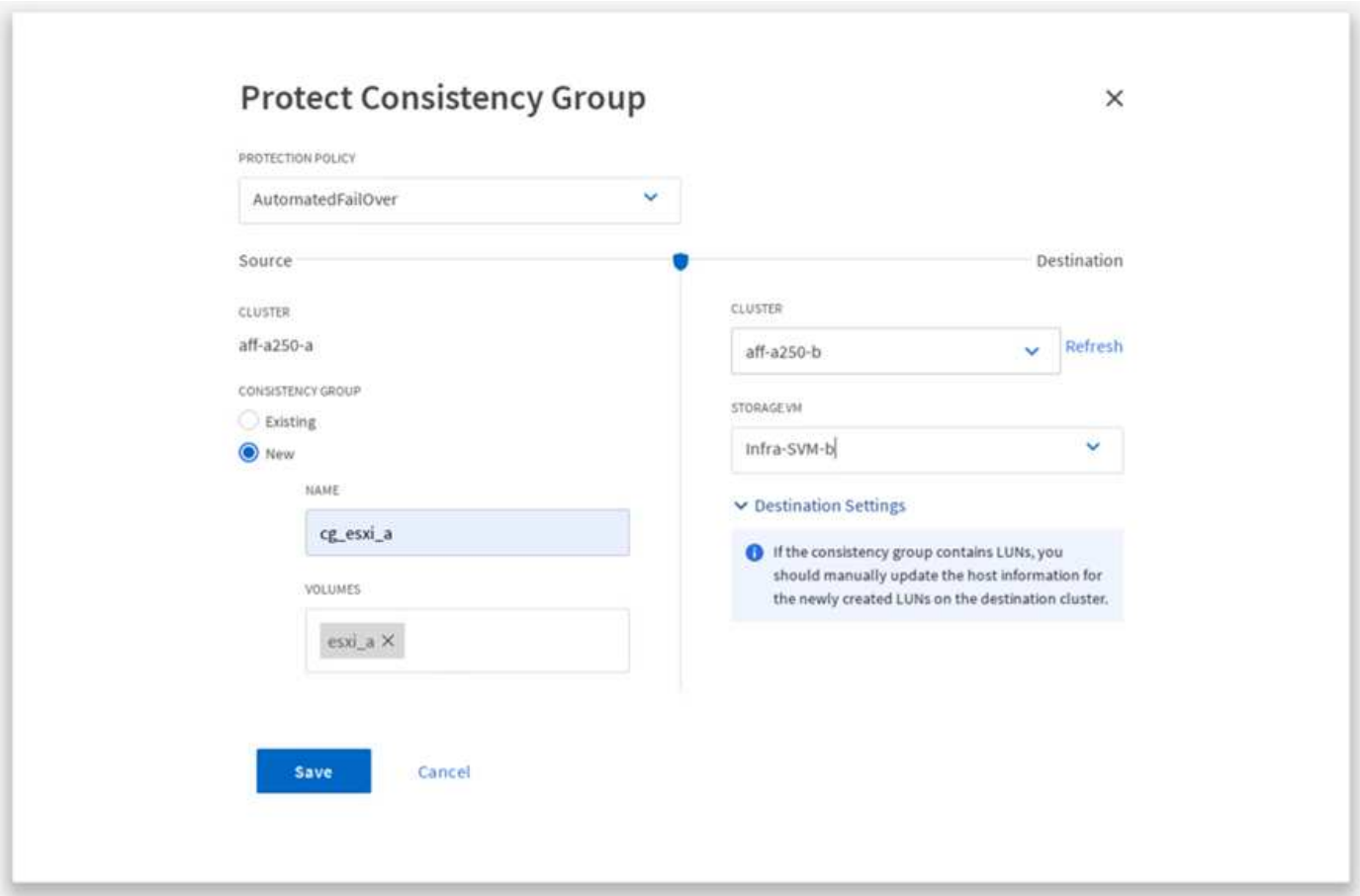
SM-BC Konsistenzgruppe

Eine Konsistenzgruppe bietet eine Schreibreihenfolge-Konsistenzgarantie für einen Applikations-Workload, der eine Sammlung angegebener Volumes umfasst. Für ONTAP 9.10.1 sind hier einige der wichtigen Einschränkungen und Grenzen zu sehen.

- Die maximale Anzahl von SM-BC-Konsistenzgruppenbeziehungen in einem Cluster ist 20.
- Die maximale Anzahl von unterstützten Volumen pro SM-BC-Beziehung ist 16.
- Die maximale Anzahl von Quell- und Ziel-Endpunkten in einem Cluster beträgt 200.

Weitere Informationen finden Sie in der Dokumentation zu ONTAP SM-BC auf der "Einschränkungen und Einschränkungen".

Für die Validierungskonfiguration wurde ONTAP System Manager verwendet, um die Konsistenzgruppen zu erstellen, um sowohl die ESXi Boot-LUNs als auch die gemeinsam genutzten Datenspeicher-LUNs für beide Standorte zu schützen. Auf das Dialogfeld zur Erstellung von Konsistenzgruppen kann unter „Protection“ > „Overview“ > „Protect for Business Continuity“ > „Protect Consistency Group“ zugegriffen werden. Zum Erstellen einer Konsistenzgruppe geben Sie die erforderlichen Quell-Volumes, Ziel-Cluster und Ziel-Storage Virtual Machine-Informationen für die Erstellung ein.

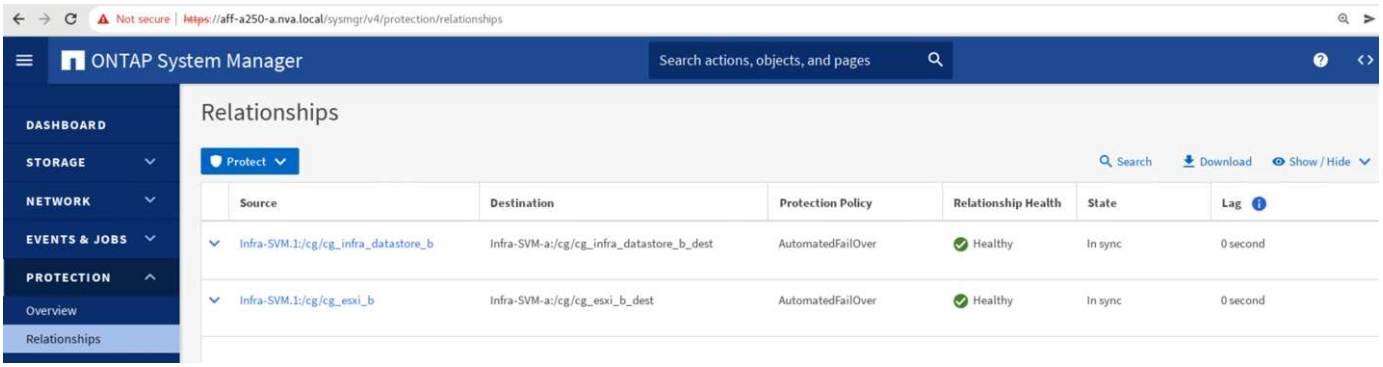


In der folgenden Tabelle werden die vier erstellten Konsistenzgruppen und die Volumes aufgeführt, die in jeder Konsistenzgruppe für die Validierungstests enthalten sind.

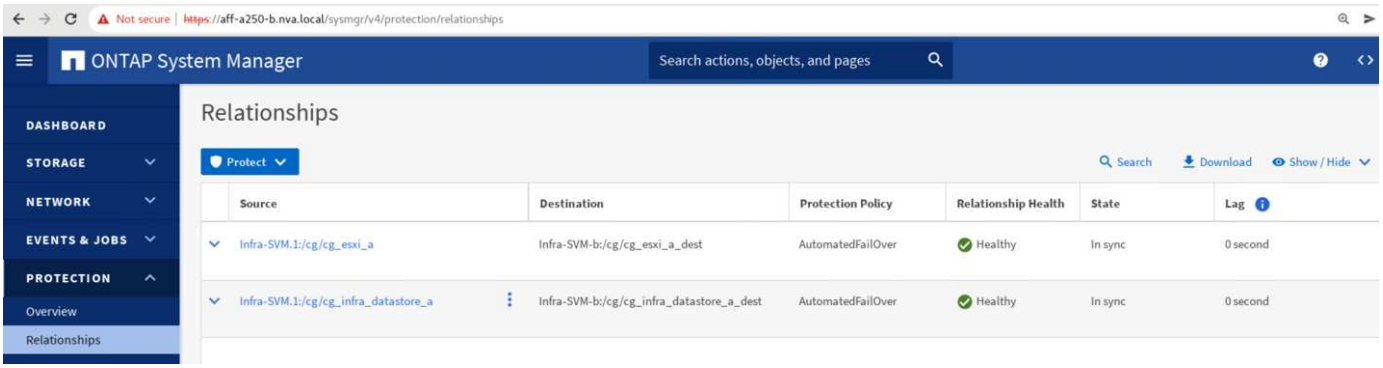
System Manager	Konsistenzgruppe	Volumes
Standort A	cg_esxi_A	esxi_A
Standort A	cg_Infra_Datastore_A	Infra_Datastore_A_01 Infra_Datastore_A_02
Standort B	cg_esxi_b	esxi_b
Standort B	cg_Infra_Datastore_b	Infra_Datastore_b_01 Infra_Datastore_b_02

Nach dem Erstellen der Konsistenzgruppen werden sie unter den jeweiligen Schutzbeziehungen an Standort A und Standort B angezeigt

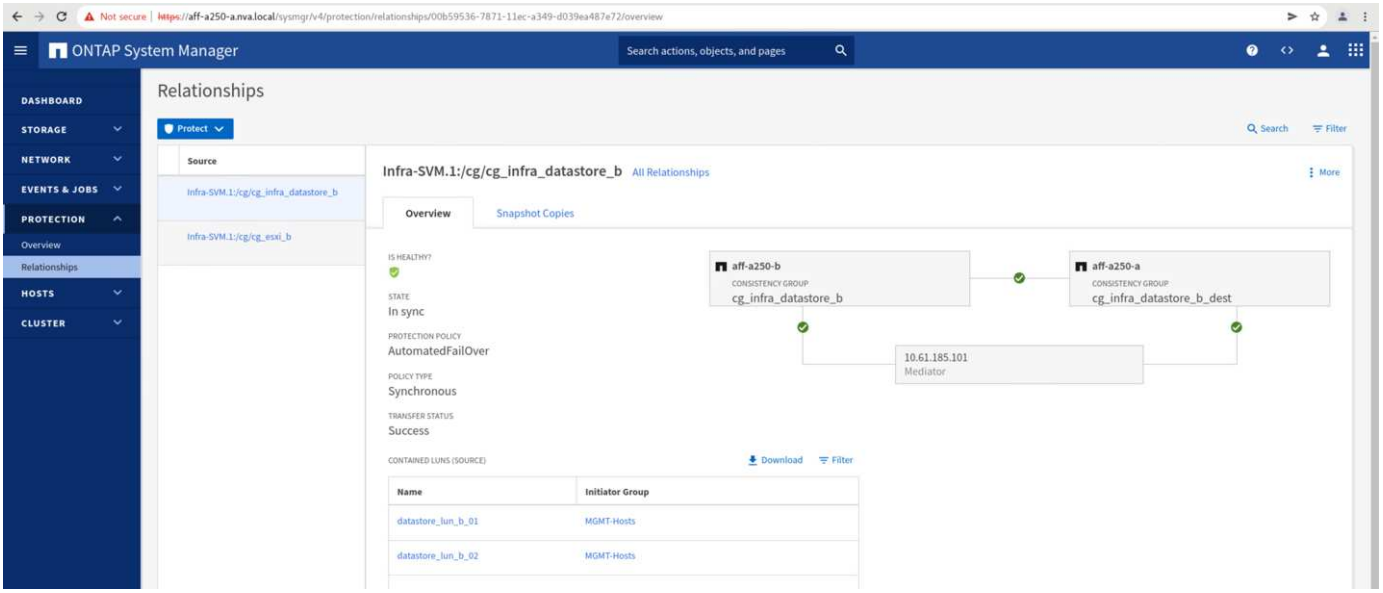
In diesem Screenshot werden die Beziehungen zu Konsistenzgruppen an Standort A angezeigt



In diesem Screenshot werden die Beziehungen zu Konsistenzgruppen an Standort B. angezeigt



In diesem Screenshot werden die Details zur Consistency Group-Beziehung für die cg_Infra_Datastore_b-Gruppe angezeigt.



Volumes, LUNs und Host-Zuordnungen

Nach der Erstellung der Konsistenzgruppen synchronisiert SnapMirror die Quell- und Ziel-Volumes, damit die Daten immer synchron sind. Die Ziel-Volumes am Remote-Standort tragen die Volume-Namen mit dem _dest-Ende. Zum Beispiel gibt es für das esxi_A-Volume in Standort-Cluster ein entsprechendes esxi_A_dest Data Protection (DP)-Volume in Standort B.

In diesem Screenshot werden die Volume-Informationen für Standort A angezeigt

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Dieser Screenshot zeigt die Volume-Informationen für Standort B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Um ein transparentes Applikations-Failover zu ermöglichen, müssen die gespiegelten SM-BC LUNs auch den Hosts aus dem Ziel-Cluster zugeordnet werden. Dadurch können die Hosts Pfade zu den LUNs sowohl von den Quell- als auch von den Ziel-Clustern ordnungsgemäß sehen. Der `igroup show` Und `lun show` Die Ausgänge für Standort A und Standort B werden in den folgenden beiden Screenshots erfasst. Mit den erstellten Zuordnungen sehen jeder ESXi Host im Cluster seine eigene Boot-LUN als ID 0 und alle vier gemeinsamen iSCSI-Datenspeicher-LUNs.

In diesem Screenshot werden die Host-Initiatorgruppen und die LUN-Zuordnung für Standort-Ein-Cluster angezeigt.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01          VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02          VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03          VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                  MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01     VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02     VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03     VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b             MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

In diesem Screenshot werden die Host-Initiatorgruppen und die LUN-Zuordnung für Standort B-Cluster angezeigt.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Weiter: Lösungsvalidierung – Virtualisierung."

Lösungsvalidierung – Virtualisierung

"Früher: Lösungsvalidierung – Storage."

In der FlexPod SM-BC Lösung an mehreren Standorten managt ein einzelnes VMware vCenter die Ressourcen der virtuellen Infrastruktur für die gesamte Lösung. Die Hosts in beiden Datacentern Teil des einzelnen VMware HA Clusters, der beide Datacenter umfasst. Die Hosts haben Zugriff auf die NetApp SM-BC Lösung, bei der auf Storage mit definierten SM-BC-Beziehungen von beiden Standorten aus zugegriffen werden kann.

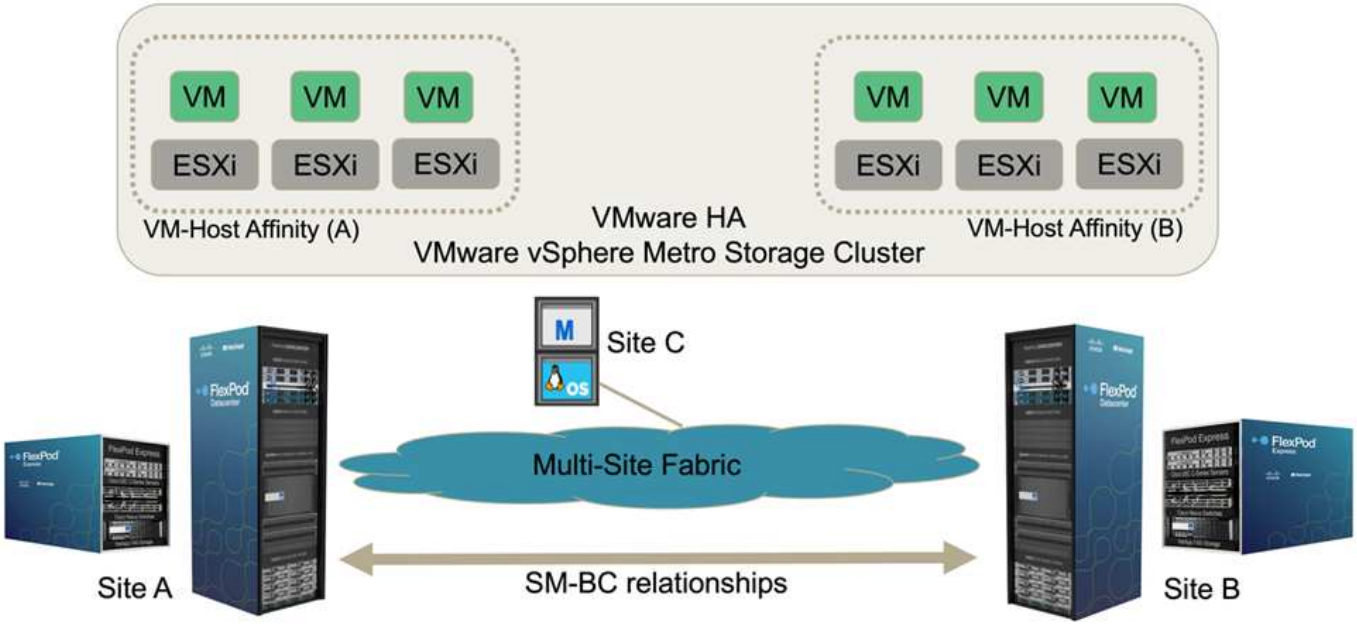
Der Storage für SM-BC Lösung entspricht dem einheitlichen Zugriffsmodell in der VMware vSphere Metro Storage Cluster (vMSC) Funktion zur Vermeidung von Ausfällen und Ausfallzeiten. Für eine optimale Performance der Virtual Machines sollten die Virtual-Machine-Festplatten auf den lokalen NetApp AFF A250 Systemen gehostet werden, um die Latenz und den Datenverkehr über WAN-Links im normalen Betrieb zu minimieren.

Im Rahmen der Design-Implementierung muss die Verteilung der Virtual Machines auf die beiden Standorte ermittelt werden. Sie können die Standortaffinität dieser Virtual Machine und die Applikationsverteilung über die beiden Standorte entsprechend den Vorlieben Ihres Standorts und den Applikationsanforderungen festlegen. Die VMware Cluster VM/Host Groups und VM/Host Rules werden verwendet, um die VM/Host-Affinität zu konfigurieren, um sicherzustellen, dass die VMs auf den Hosts am gewünschten Standort

ausgeführt werden.

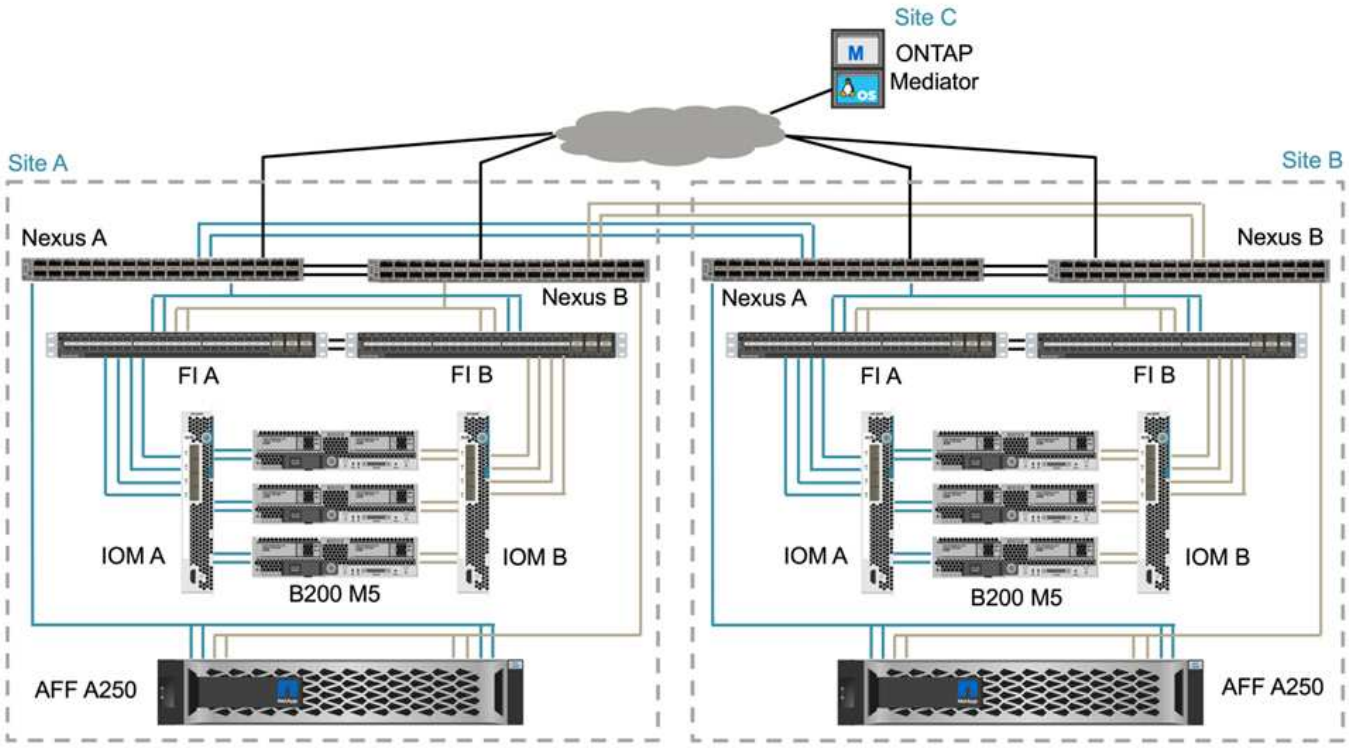
Konfigurationen, mit denen die VMs an beiden Standorten ausgeführt werden können, stellen jedoch sicher, dass VMs durch VMware HA an den Remote-Hosts neu gestartet werden können, um die Stabilität der Lösung zu gewährleisten. Damit die Virtual Machines auf beiden Seiten ausgeführt werden können, müssen alle gemeinsam genutzten iSCSI-Datenspeicher auf allen ESXi Hosts eingebunden werden, um einen reibungslosen vMotion Betrieb der Virtual Machines zwischen den Standorten sicherzustellen.

Die folgende Abbildung zeigt eine allgemeine Virtualisierungsansicht einer FlexPod SM-BC Lösung mit VMware HA- und vMSC-Funktionen für eine hohe Verfügbarkeit von Computing- und Storage-Services. Die aktiv/aktiv-Architektur für Datacenter-Lösungen ermöglicht Workload-Mobilität zwischen Standorten und bietet DR/BC-Schutz.



Umfassende Netzwerkkonnektivität

Die FlexPod SM-BC Lösung umfasst FlexPod-Infrastrukturen an jedem Standort, Netzwerkkonnektivität zwischen Standorten und den ONTAP Mediator, der an einem dritten Standort implementiert wird, um die erforderlichen RPO- und RTO-Vorgaben zu erfüllen. Die folgende Abbildung zeigt die End-to-End-Netzwerkkonnektivität zwischen den Cisco UCS B200M5 Servern an jedem Standort und dem NetApp Storage mit SM-BC Funktionen innerhalb eines Standorts und über mehrere Standorte hinweg.



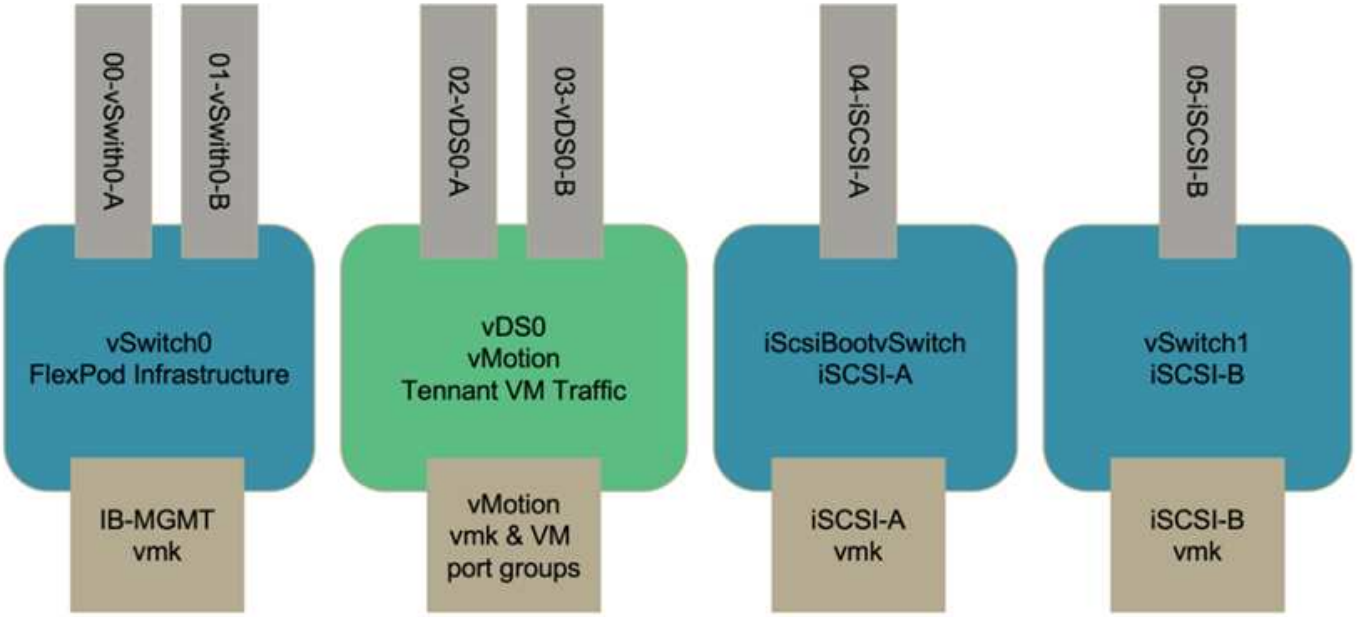
Die FlexPod Implementierungsarchitektur ist bei dieser Lösungsvalidierung an jedem Standort identisch. Die Lösung unterstützt jedoch asymmetrische Implementierungen und kann, wenn sie die Anforderungen erfüllen, auch zu vorhandenen FlexPod Lösungen hinzugefügt werden.

Die erweiterte Layer-2-Architektur dient einer nahtlosen Multi-Site-Data-Fabric-Architektur, die eine Konnektivität zwischen dem Port-gechannelten Cisco UCS-Computing und NetApp Storage in jedem Datacenter sowie Konnektivität zwischen Datacentern bietet. Die Port-Channel-Konfiguration und gegebenenfalls die Konfiguration des virtuellen Port-Kanals werden für die Bandbreitenaggregation und Fehlertoleranz zwischen den Computing-, Netzwerk- und Storage-Ebenen sowie für die standortübergreifenden Links verwendet. Das Ergebnis: Konnektivität und Multipath-Zugriff auf lokalen und Remote NetApp Storage sind die UCS Blade Server.

Virtuelle Netzwerke

Jeder Host im Cluster wird unabhängig vom Speicherort für identische virtuelle Netzwerke bereitgestellt. Das Design trennt die verschiedenen Traffic-Typen mit VMware Virtual Switches (vSwitch) und VMware Virtual Distributed Switches (VdS). Der VMware vSwitch wird hauptsächlich für die FlexPod-Infrastrukturnetzwerke und VdS für Applikationsnetzwerke verwendet, ist aber nicht erforderlich.

Die virtuellen Switches (vSwitch, VdS) werden mit zwei Uplinks pro virtuellen Switch bereitgestellt; die Uplinks auf der ESXi Hypervisor-Ebene werden als VMkernel und virtuelle NICs (vNICs) auf der Cisco UCS Software bezeichnet. Die vNICs werden auf dem Cisco UCS VIC Adapter in jedem Server mit Cisco UCS Service-Profilen erstellt. Sechs vNICs sind definiert, zwei für vSwitch0, zwei für vDS0, zwei für vSwitch1 und zwei für die iSCSI-Uplinks wie in der folgenden Abbildung dargestellt.



VSwitch0 wird während der VMware ESXi Host-Konfiguration definiert. Es enthält das FlexPod Infrastruktur-Management-VLAN und die ESXi Host VMkernel (VMK)-Ports für das Management. Für alle erforderlichen kritischen Virtual Machines für das Infrastrukturmanagement wird zudem eine VM-Portgruppe für vSwitch0 hinzugefügt.

Es ist wichtig, solche Management-Infrastruktur-Virtual Machines auf vSwitch0 statt auf den VdS zu platzieren, da wenn die FlexPod-Infrastruktur heruntergefahren oder aus- und wieder eingeschaltet wird und Sie versuchen, diese Management-Virtual Machine auf einem anderen Host als dem Host zu aktivieren, auf dem sie ursprünglich ausgeführt wurde, Es startet gut im Netzwerk auf vSwitch0. Dieser Prozess ist besonders wichtig, wenn VMware vCenter die Management-Virtual Machine ist. Wenn vCenter auf dem VdS wäre und zu einem anderen Host verschoben und dann gestartet wurde, wäre es nicht mit dem Netzwerk nach dem Booten verbunden.

In diesem Design werden zwei iSCSI Boot vSwitches verwendet. Beim Booten von Cisco UCS iSCSI sind separate vNICs für iSCSI erforderlich. Diese vNICs verwenden das iSCSI-VLAN des entsprechenden Fabric als natives VLAN und sind an den entsprechenden iSCSI-Boot-vSwitch angeschlossen. Optional können Sie auch iSCSI-Netzwerke auf VdS bereitstellen, indem Sie einen neuen VdS oder eine vorhandene einsetzen.

VM-Host-Gruppen und Regeln

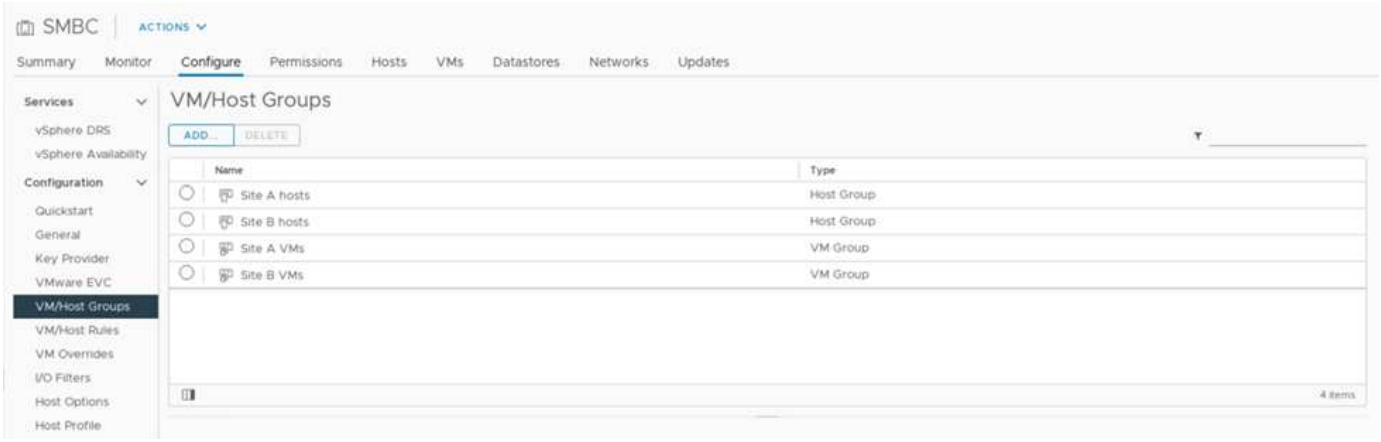
Damit Virtual Machines auf jedem ESXi Host an beiden SM-BC-Sites ausgeführt werden können, müssen alle ESXi Hosts die iSCSI-Datenspeicher von beiden Standorten aus mounten. Wenn die Datastores von beiden Standorten ordnungsgemäß von allen ESXi Hosts eingebunden werden, können Sie eine Virtual Machine zwischen beliebigen Hosts mit vMotion migrieren, und die VM bleibt weiterhin Zugriff auf alle ihre virtuellen Festplatten, die aus diesen Datastores erstellt wurden.

Bei einer virtuellen Maschine, die lokale Datenspeicher verwendet, wird der Zugriff auf virtuelle Festplatten Remote, wenn sie zu einem Host am Remote-Standort migriert wird und somit die Verzögerung beim Lesevorgang aufgrund der physischen Entfernung zwischen den Standorten erhöht. Daher empfiehlt es sich, die Virtual Machines auf lokalen Hosts aufzubewahren und den lokalen Storage am Standort zu nutzen.

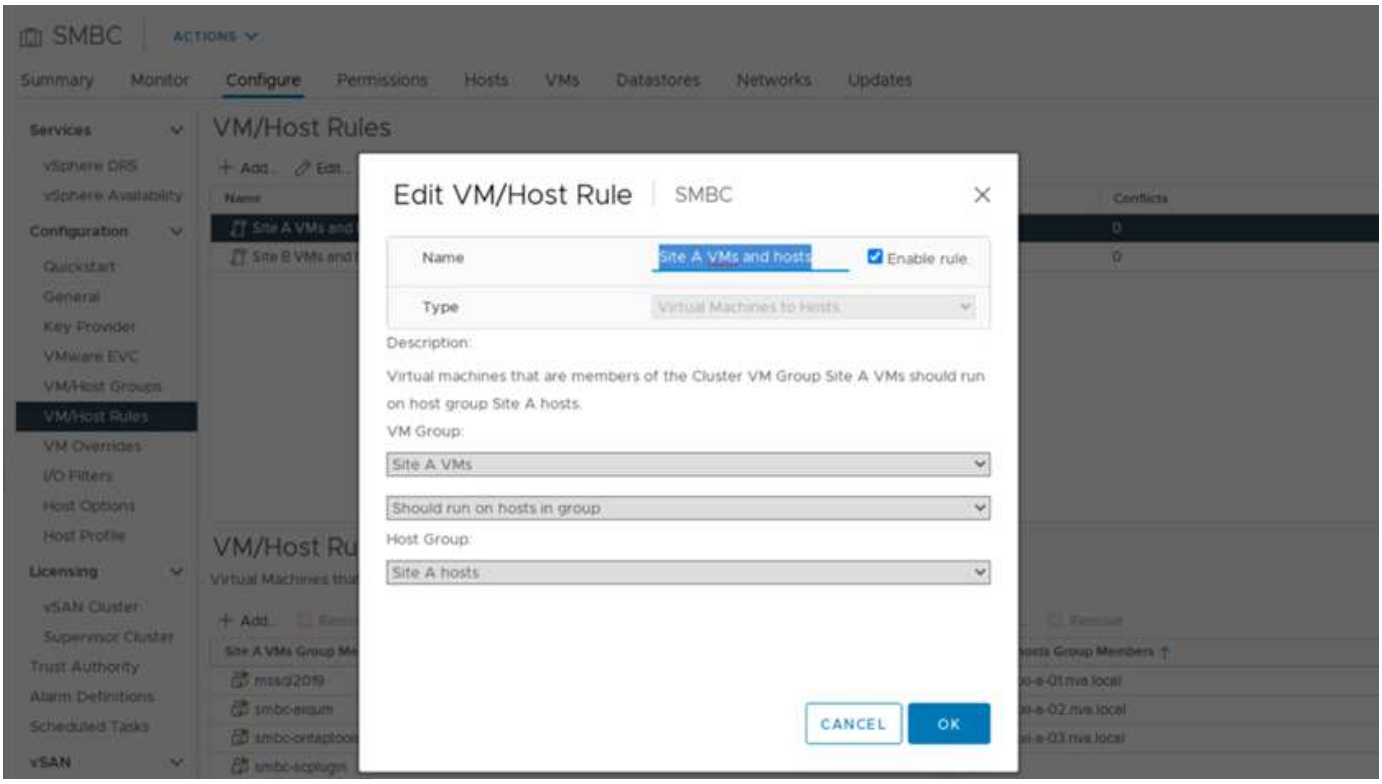
Mithilfe eines Mechanismus zur VM-/Hostorientierung können Sie VM-/Host-Gruppen verwenden, um eine VM-Gruppe und eine Host-Gruppe für Virtual Machines und Hosts zu erstellen, die sich an einem bestimmten Standort befinden. Mithilfe von VM-/Host-Regeln können Sie die Richtlinie für die folgenden VMs und Hosts festlegen. Um eine standortübergreifende Migration virtueller Maschinen während einer Standortwartung oder

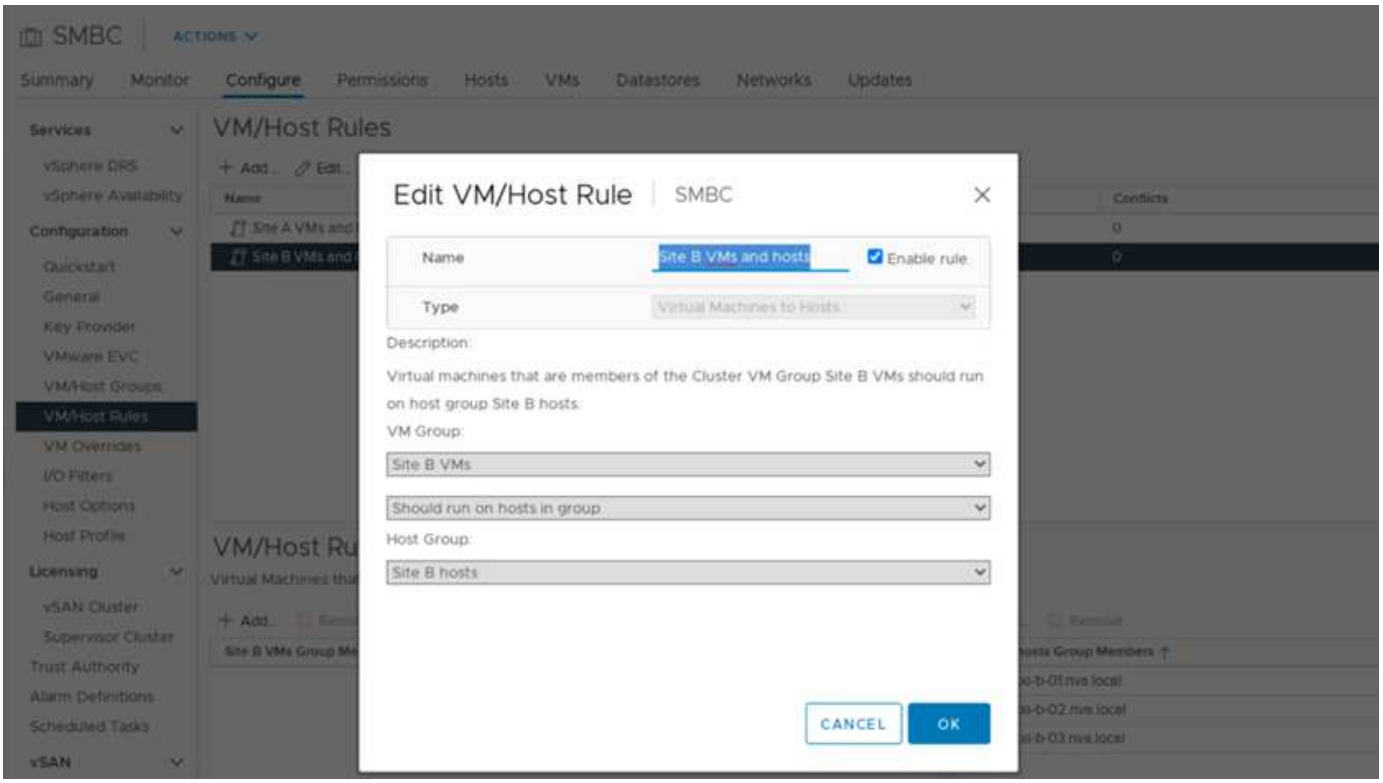
eines Notfallszenarios zu ermöglichen, verwenden Sie die Richtlinienspezifikation „sollte auf Hosts in der Gruppe ausgeführt werden“, um diese Flexibilität zu gewährleisten.

Der folgende Screenshot zeigt, dass zwei Host-Gruppen und zwei VM-Gruppen für Hosts und VMs an Standort A und Standort B erstellt werden



Zusätzlich zeigen die folgenden beiden Abbildungen die VM/Host Regeln, die für Standort A und Standort B VMs erstellt werden, um auf den Hosts auf ihren jeweiligen Seiten mit der "sollte auf Hosts in der Gruppe laufen"-Politik zu laufen.

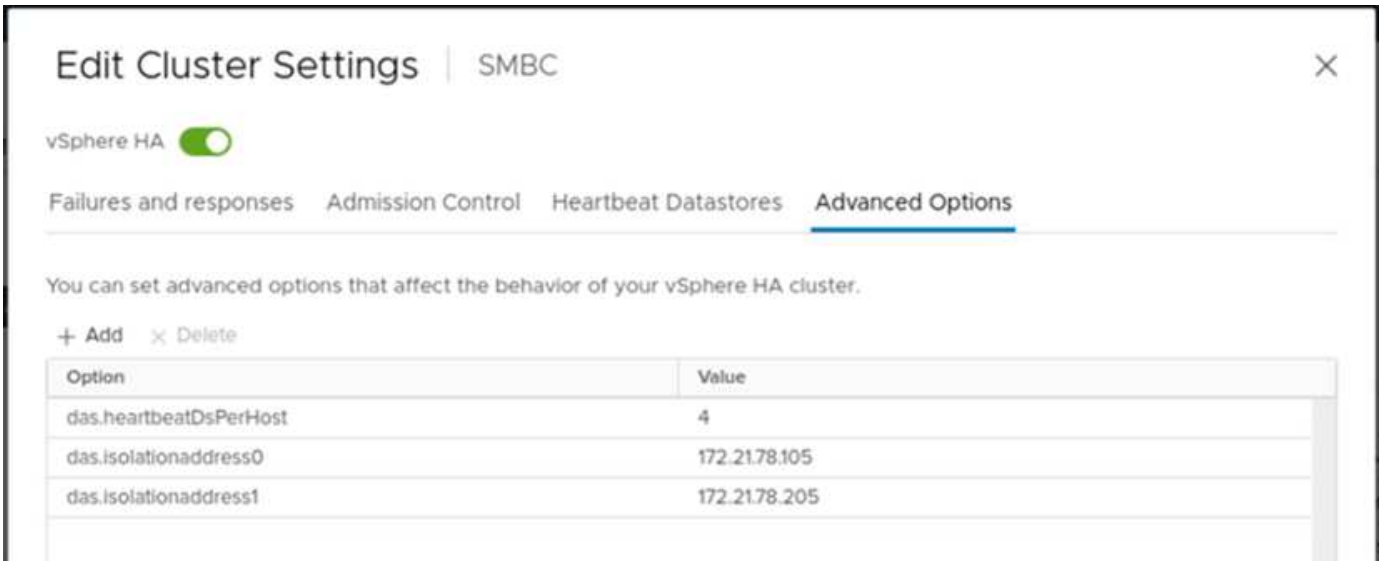




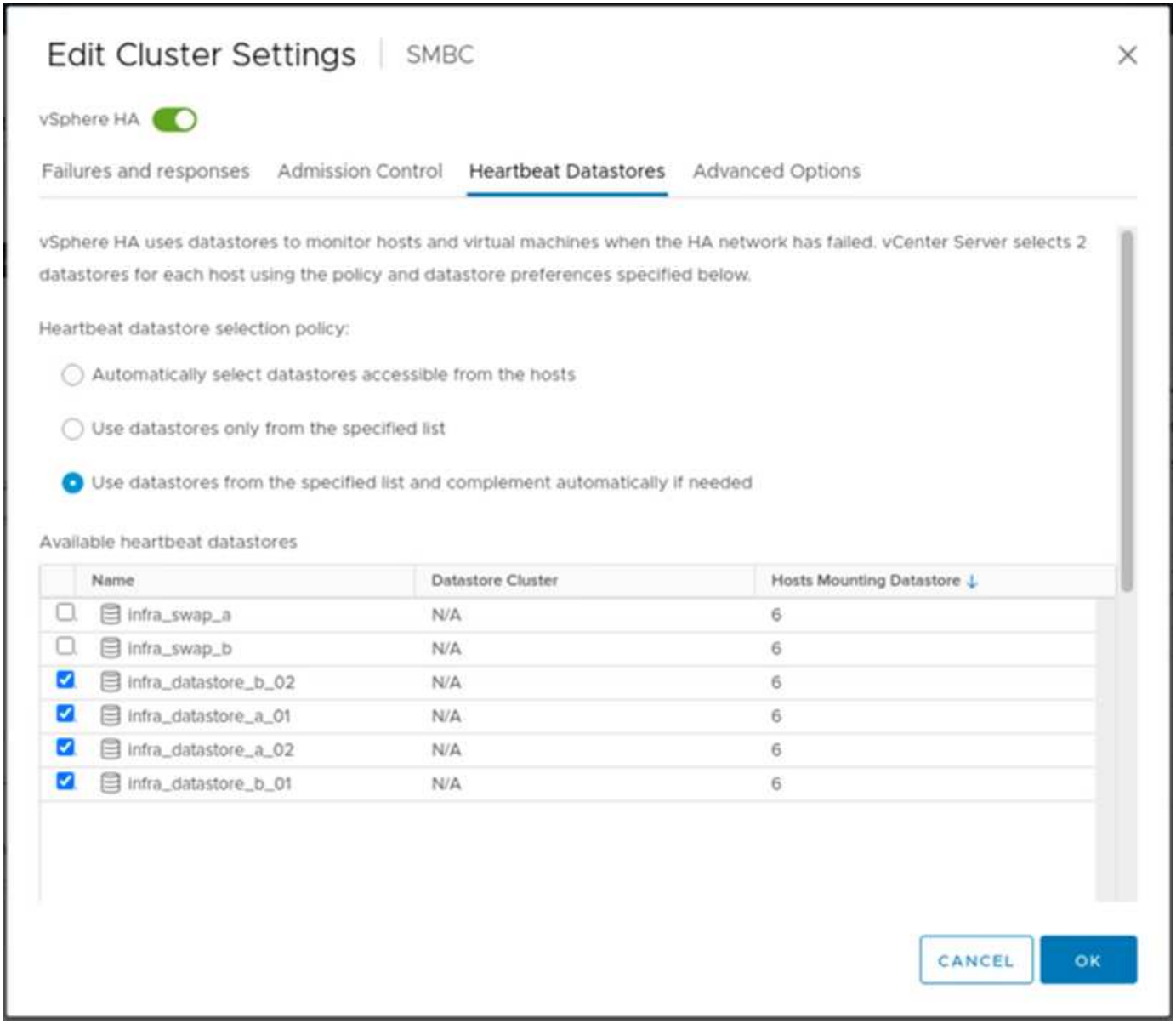
Ha-Herzschlag von vSphere

VMware vSphere HA verfügt über einen Heartbeat-Mechanismus zur Validierung des Hoststatus. Der primäre Heartbeat-Mechanismus wird über das Netzwerk durchgeführt. Der sekundäre Heartbeat-Mechanismus erfolgt über den Datenspeicher. Wenn keine Herzschläge empfangen werden, entscheidet sie dann, ob sie vom Netzwerk isoliert wird, indem sie das Standard-Gateway oder die manuell konfigurierten Isolationsadressen pingen. Beim Herzschlag des Datenspeichers empfiehlt VMware, die Heartbeat-Datenspeicher für ein dehnbares Cluster von mindestens zwei auf vier zu erhöhen.

Für die Lösungsvalidierung werden die beiden ONTAP-Cluster-Management-IP-Adressen als Isolationsadresse verwendet. Darüber hinaus die empfohlene vSphere HA Advanced Option `ds.heartbeatDsPerHost` Mit einem Wert von 4 wurde hinzugefügt, wie in der folgenden Abbildung dargestellt.



Geben Sie für den Heartbeat-Datenspeicher die vier gemeinsam genutzten Datenspeicher aus dem Cluster an und ergänzen Sie sie automatisch, wie in der folgenden Abbildung dargestellt.



Weitere Best Practices und Konfigurationen für VMware HA Cluster und VMware vSphere Metro Storage Cluster finden Sie unter "Erstellen und Verwenden von vSphere HA-Clustern", "VMware vSphere Metro Storage-Cluster (vMSC)" Und der VMware KB für "NetApp ONTAP mit NetApp SnapMirror Business Continuity (SM-BC) und VMware vSphere Metro Storage Cluster (vMSC)".

"Weiter: Lösungsvalidierung – validierte Szenarien."

Lösungsvalidierung – validierte Szenarien

"Zurück: Lösungsvalidierung – Virtualisierung."

Die FlexPod Lösung für SM-BC von Datacenter schützt Datenservices für verschiedene Single-Point-of-Failure-Szenarien und für einen Standortausfall. Das an jedem Standort implementierte redundante Design sorgt für Hochverfügbarkeit. Die SM-BC Implementierung mit synchroner Datenreplizierung an allen Standorten schützt

Datenservices vor einem standortweiten Ausfall. Die implementierte Lösung wurde für die gewünschte Funktionalität der Lösung sowie für verschiedene Ausfallszenarien validiert, bei denen die Lösung zum Schutz entwickelt wurde.

Validierung der Funktionen der Lösung

In verschiedenen Testfällen werden die Funktionen der Lösung überprüft und teilweise oder vollständige Ausfallszenarien am Standort simuliert. Um die Duplizierung durch die bereits in den vorhandenen FlexPod Datacenter-Lösungen im Rahmen des Cisco Validated Design Programms durchgeführten Tests zu minimieren, liegt der Schwerpunkt dieses Berichts auf den SM-BC-bezogenen Aspekten der Lösung. Einige allgemeine FlexPod-Validierungen sind enthalten, damit die Praktizierenden für ihre Umsetzung Validierungen gehen.

Für die Lösungsvalidierung wurde ein Virtual Machine unter Windows 10 pro ESXi Host auf allen ESXi Hosts an beiden Standorten erstellt. Das IOMeter Tool wurde installiert und zur Generierung von I/O-Vorgängen zu zwei virtuellen Datenfestplatten verwendet, die aus den gemeinsam genutzten lokalen iSCSI-Datenspeichern zugeordnet werden. Die konfigurierten IOMeter Workload-Parameter waren 8-KB I/O, 75 % Lesezugriffe und 50 % zufällige Zugriffe, mit 8 ausstehenden I/O-Befehlen für jede Datenfestplatte. Die Fortsetzung der IOMeter I/O-Vorgänge liefert bei den meisten durchgeführten Testszenarien an, dass ein Szenario keinen Ausfall des Datenservice verursacht hat.

Da SM-BC für Business-Applikationen wie Datenbankserver wichtig ist, Die Microsoft SQL Server 2019 Instanz auf einer Windows Server 2022 Virtual Machine wurde auch als Teil der Tests eingeschlossen, um zu bestätigen, dass die Applikation weiter ausgeführt wird, wenn Storage am lokalen Standort nicht verfügbar ist und der Datenservice ohne Applikation am Remote-Standort fortgesetzt wird Unterbrechungen.

Bootstest für ESXi Host iSCSI SAN

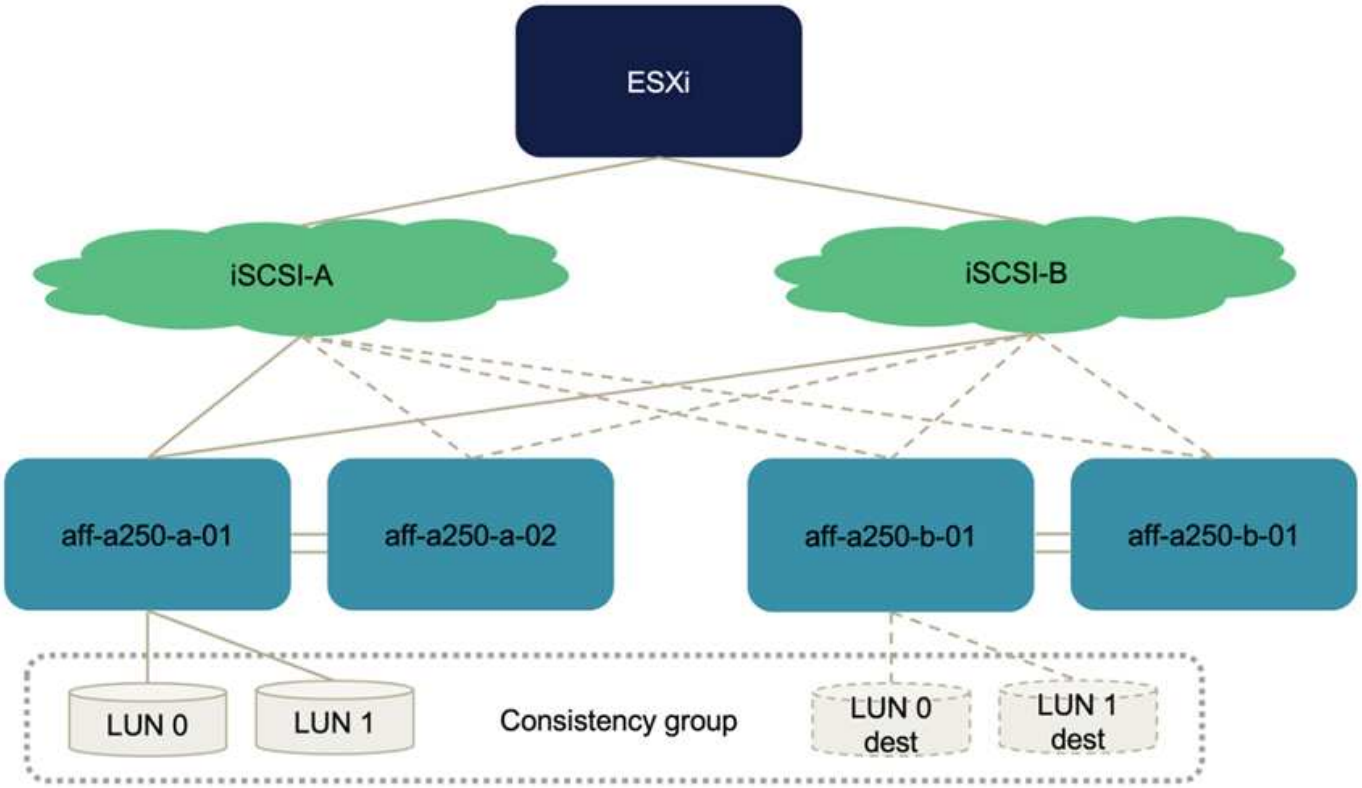
Die ESXi-Hosts in der Lösung sind für das Booten über das iSCSI-SAN konfiguriert. Die Verwendung von SAN-Boot vereinfacht das Servermanagement beim Austausch eines Servers, da das Serviceprofil des Servers einem neuen Server zugewiesen werden kann, damit der IT-Server ohne zusätzliche Konfigurationsänderungen gestartet werden kann.

Zusätzlich zum Booten eines ESXi Hosts an einem Standort von seiner lokalen iSCSI-Boot-LUN wurden Tests zum Booten des ESXi Hosts durchgeführt, wenn sich der lokale Storage-Controller im Übernahmemodus befindet oder dessen lokaler Storage-Cluster vollständig nicht verfügbar ist. Mithilfe dieser Validierungsszenarien wird sichergestellt, dass die ESXi Hosts je Design ordnungsgemäß konfiguriert sind und während einer Storage-Wartung oder eines Disaster Recovery-Szenarios hochgefahren werden können, um Business Continuity zu gewährleisten.

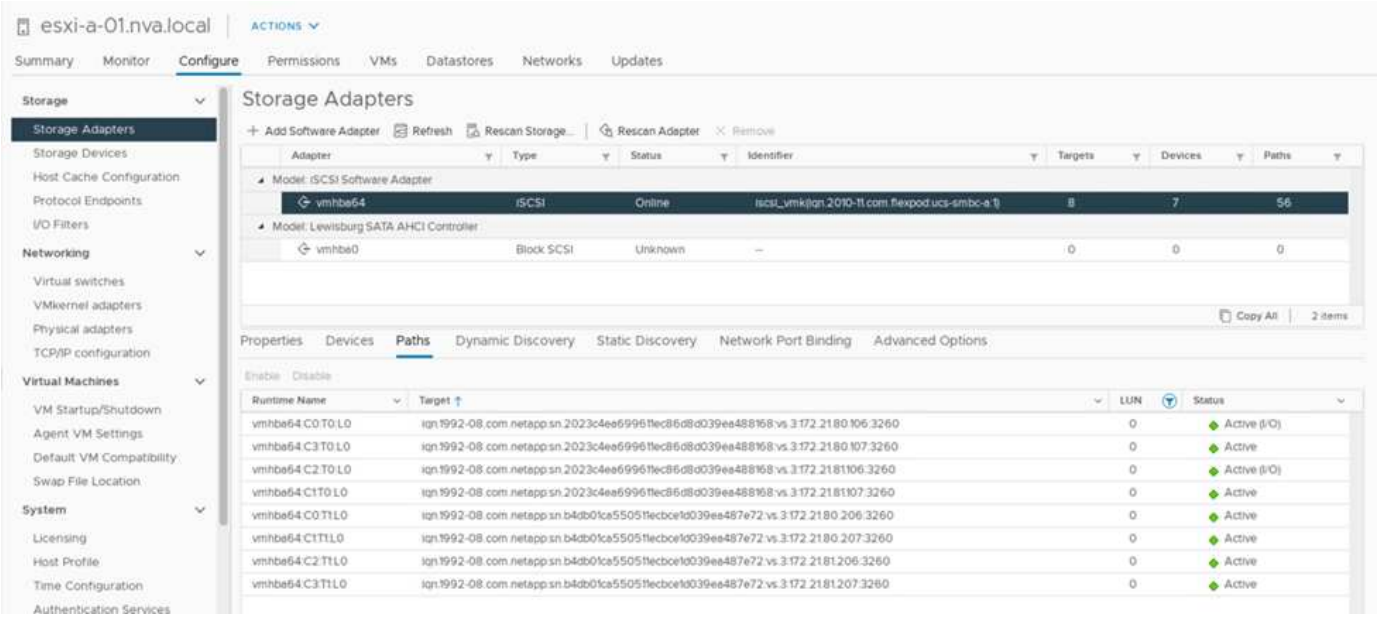
Bevor die SM-BC Konsistenzgruppenbeziehung konfiguriert ist, verfügt ein iSCSI-LUN, das von einem Storage Controller HA-Paar gehostet wird, über vier Pfade, zwei über jede iSCSI-Fabric, basierend auf der Implementierung von Best Practices. Ein Host kann über die zwei iSCSI-VLANs/Fabrics zum LUN-Hosting Controller gelangen und über den hochverfügbaren Partner des Controllers zur LUN gelangen.

Nachdem die SM-BC Konsistenzgruppe-Beziehung konfiguriert ist und die gespiegelten LUNs den Initiatoren ordnungsgemäß zugeordnet sind, verdoppelt sich die Pfadanzahl für die LUN. Für diese Implementierung reicht es von zwei aktiven/optimierten Pfaden und zwei aktiv/nicht-optimierte Pfade bis hin zu zwei aktiv/optimierten Pfaden und sechs aktiv/nicht optimierte Pfade.

In der folgenden Abbildung werden die Pfade dargestellt, die ein ESXi Host für den Zugriff auf eine LUN nutzen kann, beispielsweise LUN 0. Da die LUN an den Standort A Controller 01 angeschlossen ist, sind nur die beiden Pfade, die direkt über diesen Controller auf die LUN zugreifen, aktiv/optimiert und alle verbleibenden sechs Pfade sind aktiv/nicht optimiert.



Der folgende Screenshot mit den Informationen zum Pfad für das Storage-Gerät zeigt, wie der ESXi Host die zwei Typen von Gerätepfaden sieht. Die beiden aktiven/optimierten Pfade werden als haben angezeigt `active (I/O)` Pfadstatus, während die sechs aktiven/nicht optimierten Pfade nur als angezeigt werden `active`. Beachten Sie außerdem, dass in der Spalte Ziel die beiden iSCSI-Ziele und die entsprechenden iSCSI-LIF-IP-Adressen angezeigt werden, um die Ziele zu erreichen.



Wenn einer der Storage Controller für Wartungsarbeiten oder Upgrades ausfällt, stehen die beiden Pfade zum Erreichen des heruntergekommen Controllers nicht mehr zur Verfügung und zeigen den Pfadstatus von an `dead` Stattdessen.

Wenn ein Failover der Konsistenzgruppe auf dem primären Storage Cluster erfolgt, entweder aufgrund von

manuellen Failover-Tests oder aufgrund von automatischem Disaster Failover, stellt das sekundäre Storage-Cluster weiterhin Datenservices für die LUNs in der SM-BC-Konsistenzgruppe bereit. Da die LUN-Identitäten erhalten bleiben und die Daten synchron repliziert werden, bleiben alle durch SM-BC-Konsistenzgruppen geschützten ESXi Host-Boot-LUNs über das Remote-Storage-Cluster verfügbar.

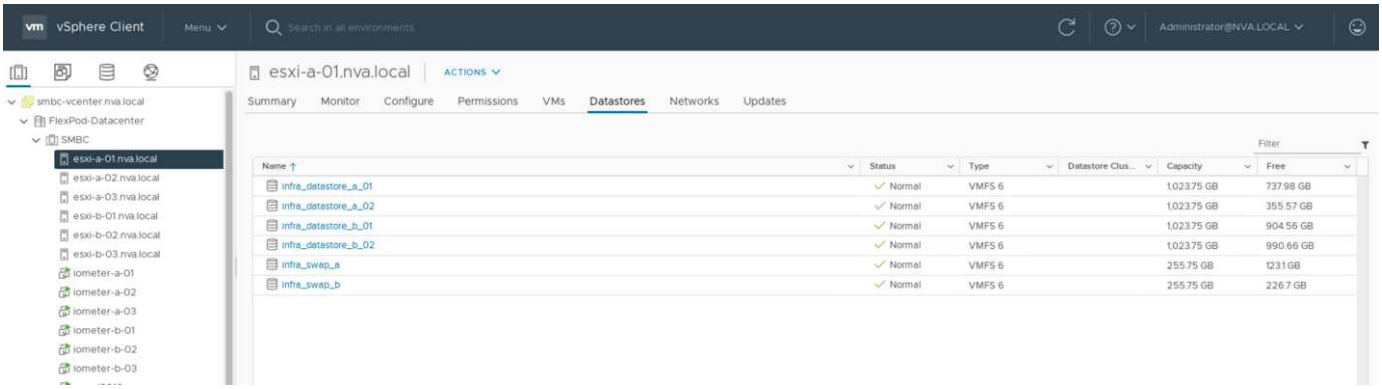
VMware vMotion und VM/Host-Affinitätstest

Obwohl eine allgemeine FlexPod VMware Datacenter Lösung Multi-Protokolle wie FC, iSCSI, NVMe und NFS unterstützt, unterstützt die FlexPod SM-BC Lösungsfunktion FC und iSCSI SAN-Protokolle, die üblicherweise für geschäftskritische Lösungen verwendet werden. Diese Validierung verwendet nur iSCSI-protokollbasierte Datenspeicher und iSCSI SAN Boot.

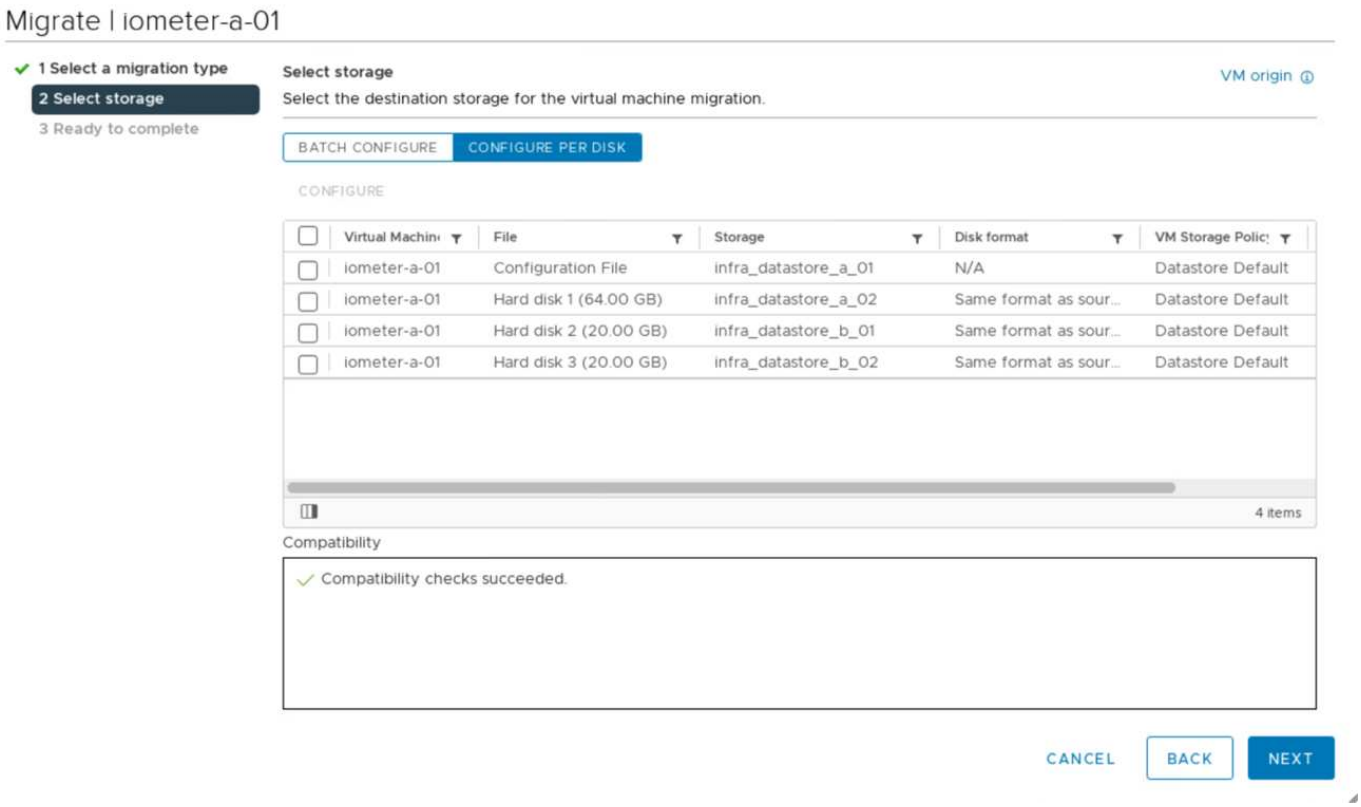
Damit Virtual Machines Storage-Services von einem SM-BC-Standort aus verwenden können, müssen die iSCSI-Datenspeicher beider Standorte von allen Hosts im Cluster gemountet werden, um die Migration von Virtual Machines zwischen beiden Standorten und für Disaster Failover-Szenarien zu ermöglichen.

Für Applikationen, die auf der virtuellen Infrastruktur ausgeführt werden, die über Standorte hinweg keinen SM-BC-Konsistenzgruppenschutz benötigen, können auch NFS-Protokoll und NFS-Datenspeicher verwendet werden. In diesem Fall ist Vorsicht zu beachten, wenn Storage für VMs zugewiesen wird, damit geschäftskritische Applikationen die durch SM-BC Consistency Group geschützten SAN-Datenspeicher ordnungsgemäß verwenden, um Business Continuity zu gewährleisten.

Der folgende Screenshot zeigt, dass Hosts konfiguriert sind, um iSCSI-Datenspeicher von beiden Seiten einzubinden.



Sie haben die Möglichkeit, Laufwerke von Virtual Machines zwischen verfügbaren iSCSI-Datenspeichern beider Standorte zu migrieren, wie in der folgenden Abbildung dargestellt. Bei Performance-Überlegungen ist es optimal, Virtual Machines zu nutzen, die Storage aus dem lokalen Storage-Cluster verwenden, um die Festplatten-I/O-Latenzen zu verringern. Dies gilt insbesondere, wenn sich beide Standorte aufgrund der physischen Latenz für die hin- und Rückfahrt von ca. 1 ms pro 100 km Entfernung in einigen Entfernungen voneinander unterscheiden.



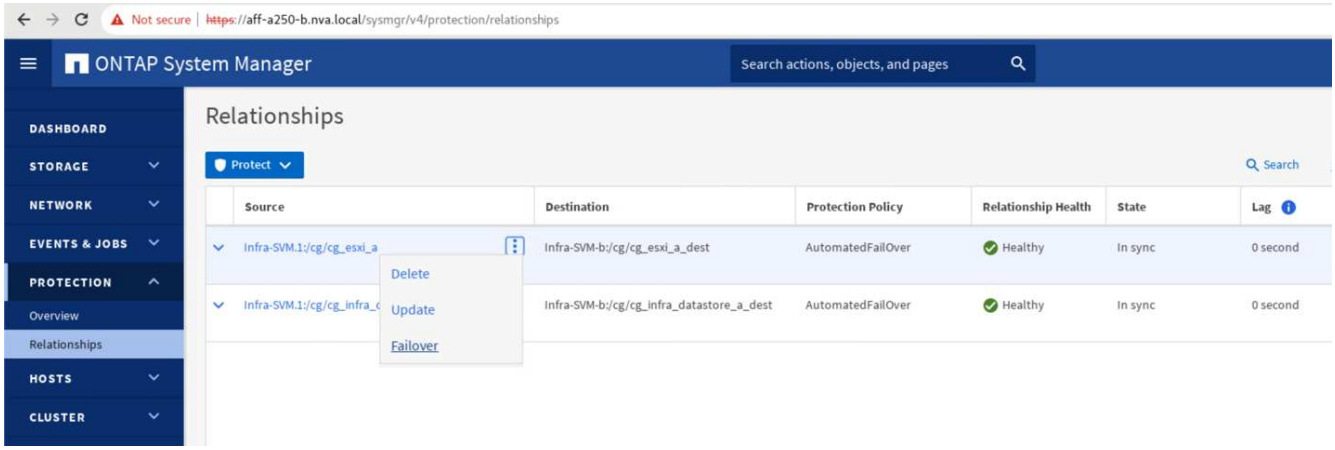
Tests von vMotion von Virtual Machines auf einem anderen Host an demselben Standort und über mehrere Standorte hinweg wurden durchgeführt und erfolgreich durchgeführt. Nach der manuellen Migration einer virtuellen Maschine über Standorte hinweg wird die Regel für die VM/Hostaffinität aktiviert und die virtuelle Maschine zurück zur Gruppe migriert, in der sie unter dem normalen Zustand gehört.

Geplantes Storage-Failover

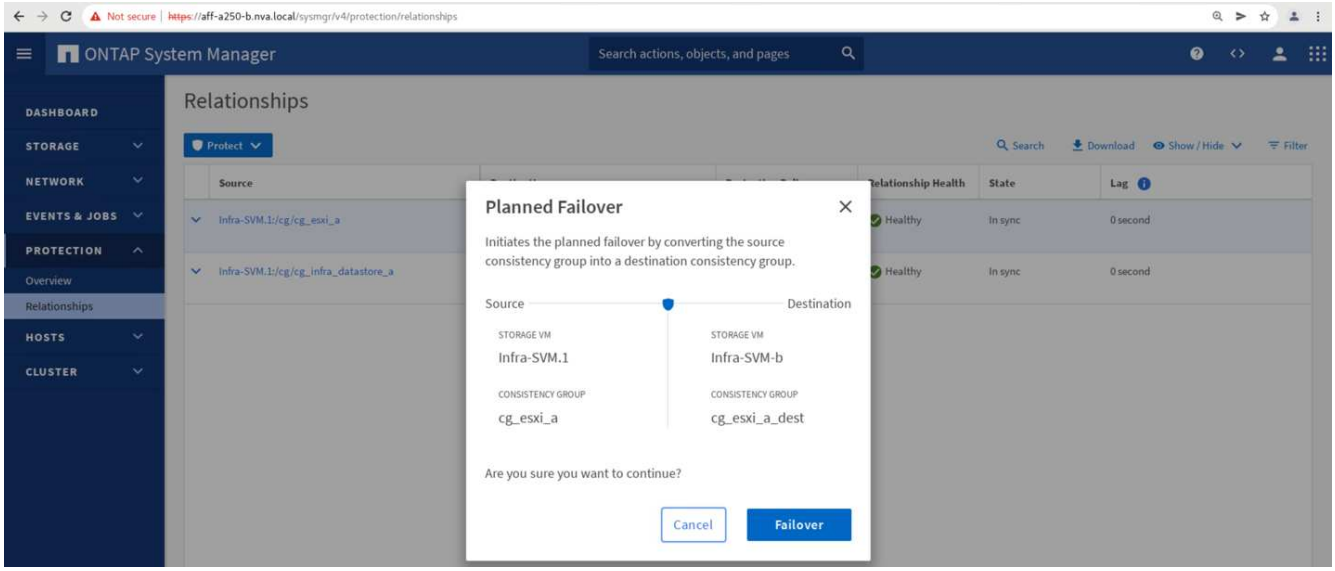
Geplante Storage Failover-Vorgänge sollten nach der Erstkonfiguration der Lösung ausgeführt werden, um festzustellen, ob die Lösung nach dem Storage Failover ordnungsgemäß funktioniert. Der Test kann dabei helfen, alle Verbindungs- oder Konfigurationsprobleme zu identifizieren, die zu I/O-Unterbrechungen führen können. Durch regelmäßige Tests und Behebung von Verbindungs- oder Konfigurationsproblemen können im Falle eines wirklichen Standortausfalls unterbrechungsfreie Datenservices bereitgestellt werden. Geplante Storage-Failovers können auch vor geplanten Aktivitäten zur Storage-Wartung verwendet werden, damit Datenservices vom nicht betroffenen Standort bedient werden können.

Um einen manuellen Failover von Standort-A-Speicherdatendiensten an Standort B zu initiieren, können Sie die Aktion mithilfe des Standort B ONTAP-System Managers durchführen.

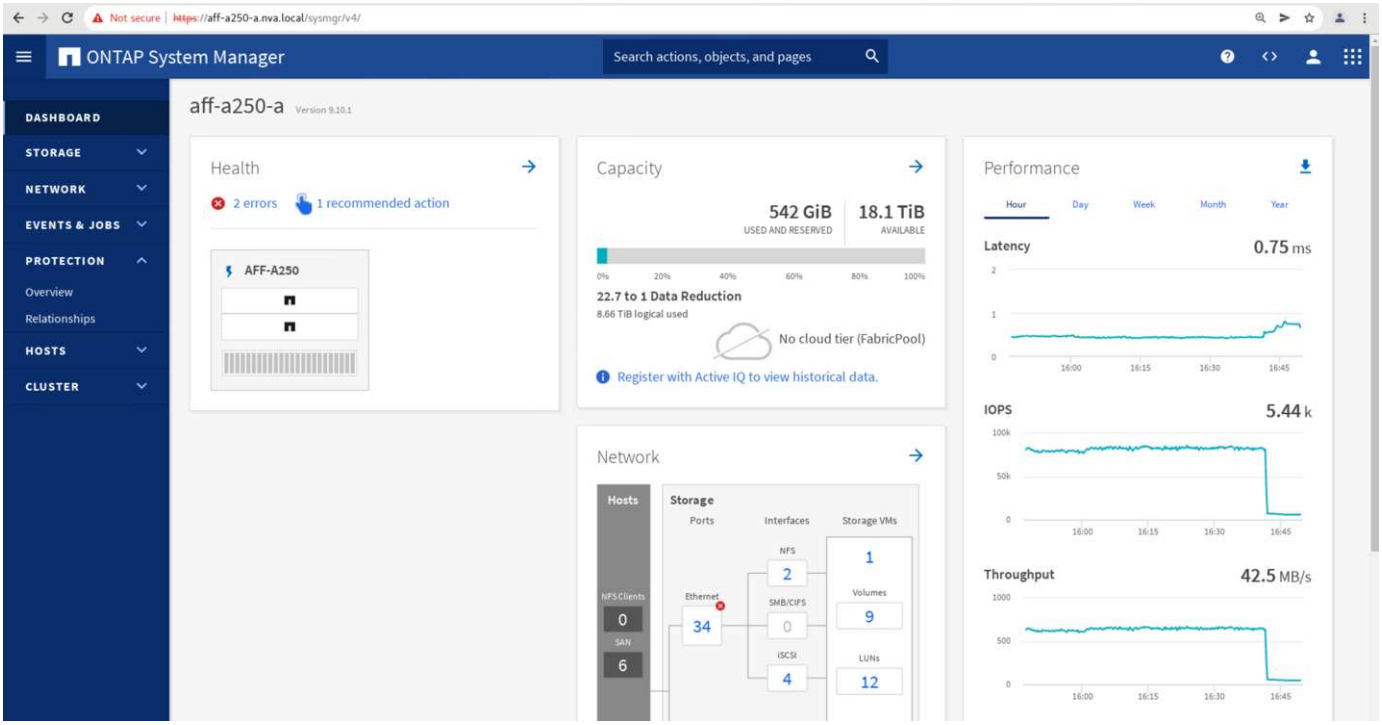
1. Wechseln Sie zum Bildschirm Schutz > Beziehungen, um zu bestätigen, dass der Status der Beziehungen zu Konsistenzgruppen lautet `In Sync`. Wenn es noch im ist `Synchronizing` Status: Warten Sie, bis der Status in lautet `In Sync` Vor dem Durchführen eines Failover.
2. Erweitern Sie die Punkte neben dem Quellnamen, und klicken Sie auf Failover.



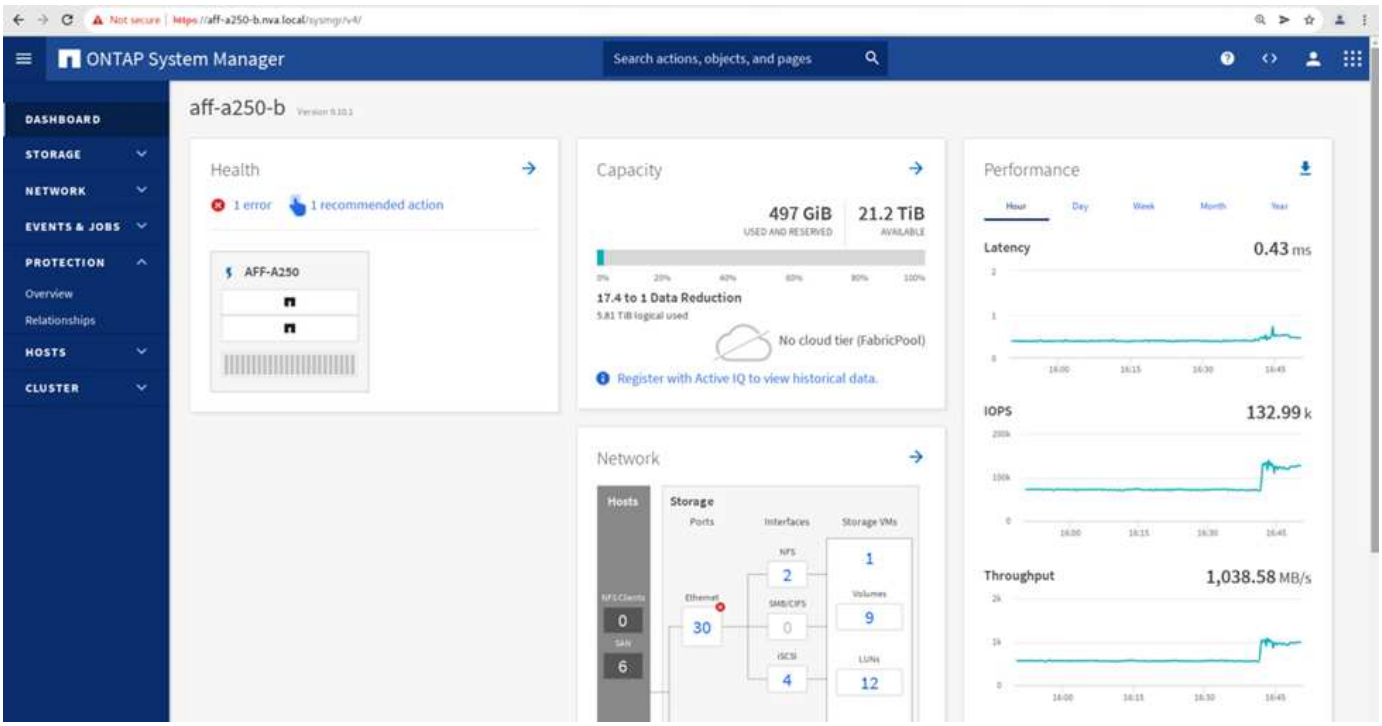
3. Bestätigen Sie das Failover für den Start der Aktion.



Kurz nach dem Start des Failover der beiden Konsistenzgruppen, `cg_esxi_a` Und `cg_infra_datastore_a`, Auf der Website B System Manager GUI ist der Standort A I/O, der die beiden Konsistenzgruppen bereitstellt, auf Standort B. verschoben Dadurch wird die I/O an Standort Erheblich reduziert, wie am Standort Das Performance-Teilfenster „System Manager“ dargestellt.

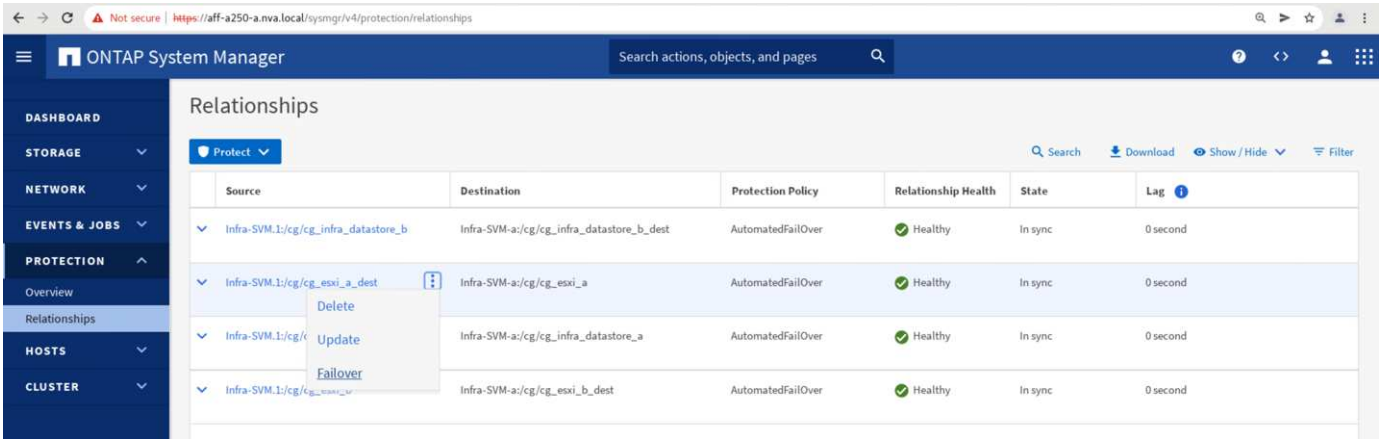


Auf der anderen Seite zeigt das Teilfenster „Performance“ des Dashboards von Standort B System Manager einen deutlich höheren IOPS-Wert, da zusätzliche I/O-Vorgänge von Standort A auf ca. 130.000 IOPS verschoben werden. Und erreichte einen Durchsatz von etwa 1 GB/s bei einer I/O-Latenz von unter 1 Millisekunde.



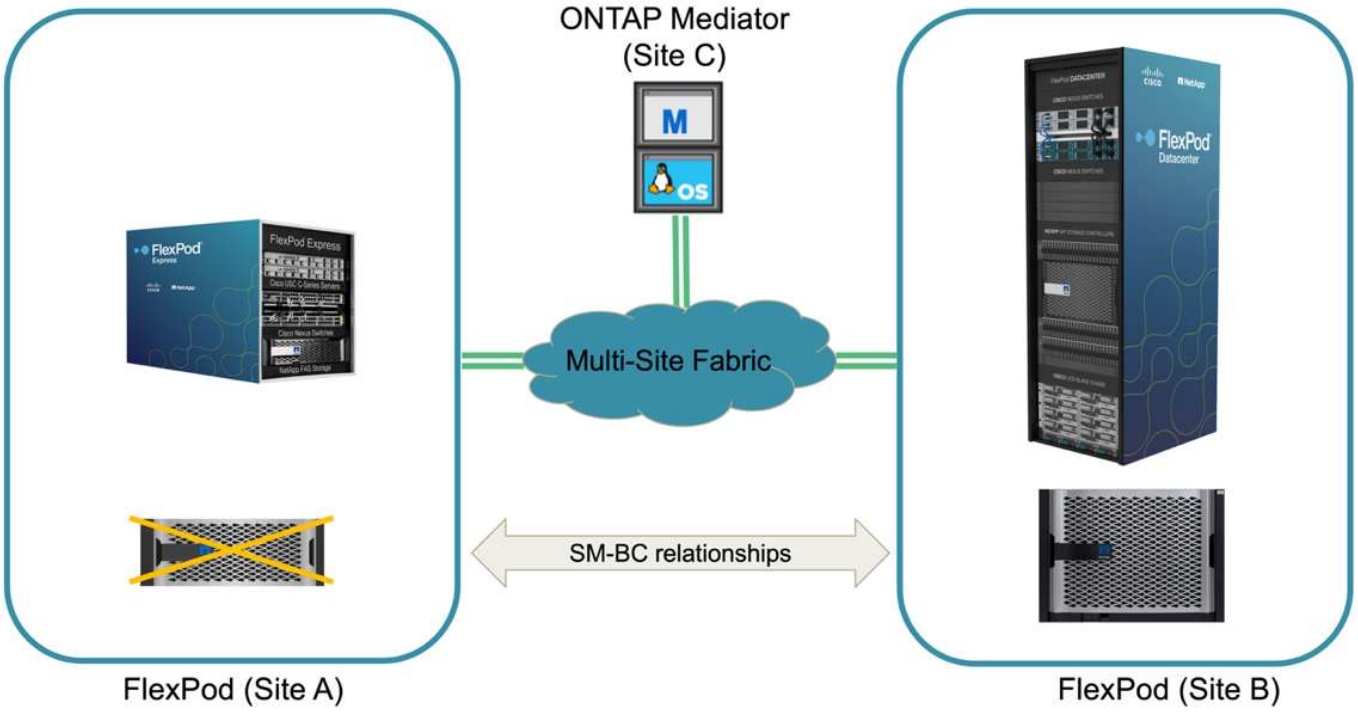
Wenn die I/O-Vorgänge transparent von Standort A nach Standort B migriert werden, können Storage-Controller an Standort A zu geplanten Wartungsarbeiten heruntergefahren werden. Nachdem die Wartungsarbeiten oder Tests abgeschlossen und ein Storage Cluster wieder betriebsbereit gemacht wurde, prüfen und warten Sie, bis sich der Sicherungsstatus der Konsistenzgruppe wieder in ändert `In sync` Bevor Sie ein Failover durchführen, um die Failover-I/O von Standort B zurück zu Standort A zurückzugeben Beachten Sie bitte, dass je länger ein Standort zu Wartungszwecken oder für das Testen ausfällt, desto länger

dauert es, bis die Daten synchronisiert und die Konsistenzgruppe wieder an den zurückgesendet wird `In sync` Bundesland.



Ungeplantes Storage-Failover

Wenn ein echter Notfall eintritt oder während einer Disaster Simulation auftritt, kann ein ungeplantes Storage-Failover erfolgen. Die folgende Abbildung zeigt beispielsweise, in der das Storage-System an Standort A einen Stromausfall hat, ein ungeplantes Storage-Failover ausgelöst wird und die Datenservices für Standort A LUNs, die durch die SM-BC-Beziehungen gesichert sind, von Standort B fortgesetzt werden



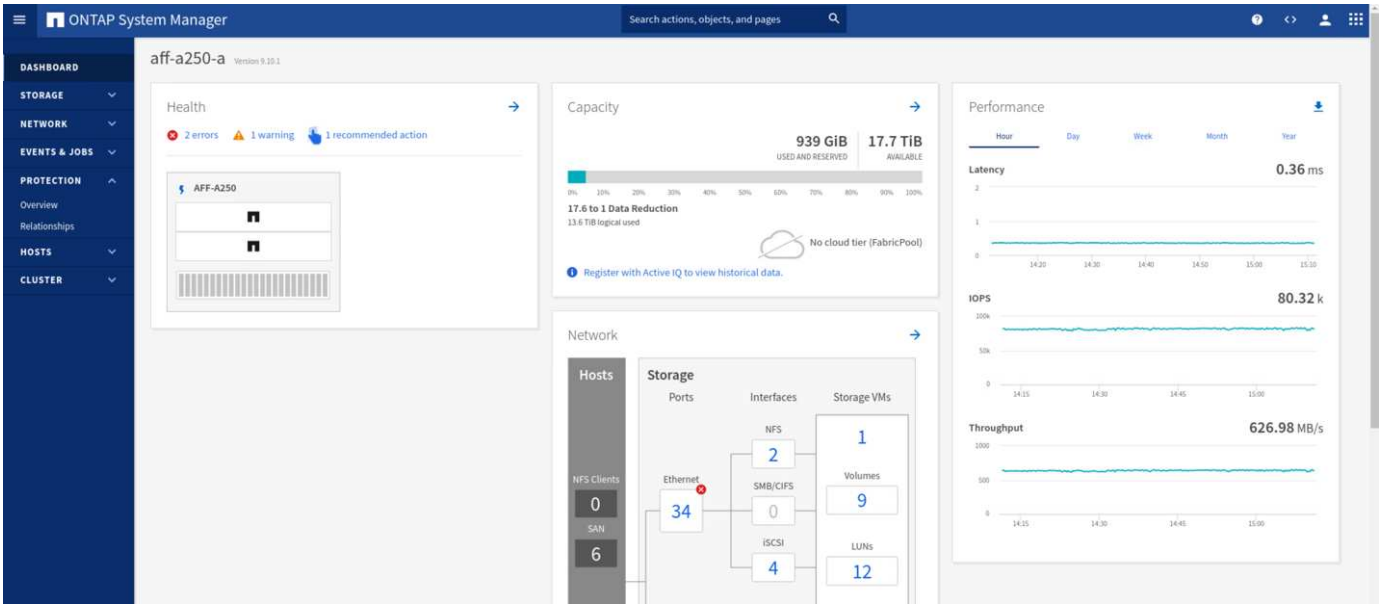
Um einen Storage-Ausfall an Standort A zu simulieren, können beide Storage Controller an Standort A ausgeschaltet werden, indem der Netzschalter deaktiviert wird, um die Stromversorgung der Controller einzustellen, Oder mit dem System Power Management Befehl der Speichercontroller-Prozessoren zum Ausschalten der Controller.

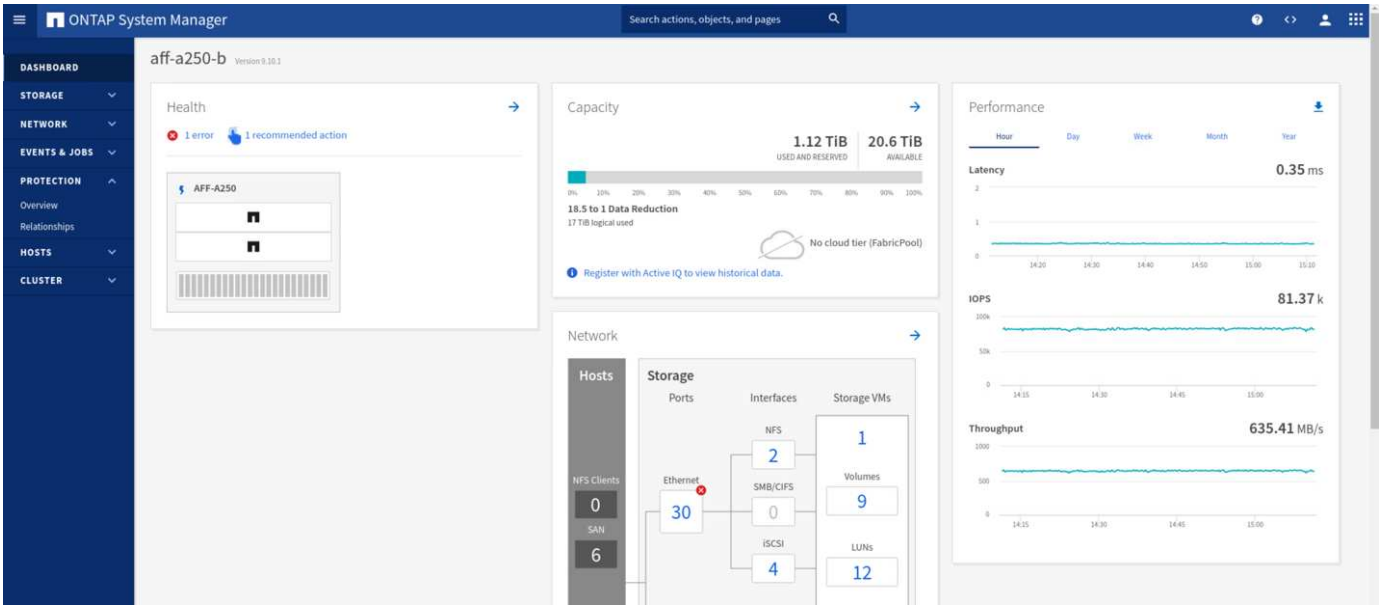
Wenn der Storage Cluster an Standort Mit Strom versorgt wird, findet ein plötzlicher Stopp der Datenservices statt, die von Standort A Storage-Cluster bereitgestellt werden. Anschließend erkennt der ONTAP Mediator, der die SM-BC-Lösung von einem dritten Standort aus überwacht, den Standort Als Storage-Ausfall und ermöglicht der SM-BC-Lösung ein automatisiertes ungeplantes Failover. Dadurch können Standort B Storage

Controller Datenservices für die LUNs fortsetzen, die in den SM-BC-Konsistenzgruppenbeziehungen mit Standort A konfiguriert sind

Aus der Applikationsperspektive stehen die Datenservices kurz vor der Pause, während das Betriebssystem den Pfadstatus der LUNs überprüft und mit den verfügbaren Pfaden zu den verbleibenden Storage Controllern am Standort B fortfahren.

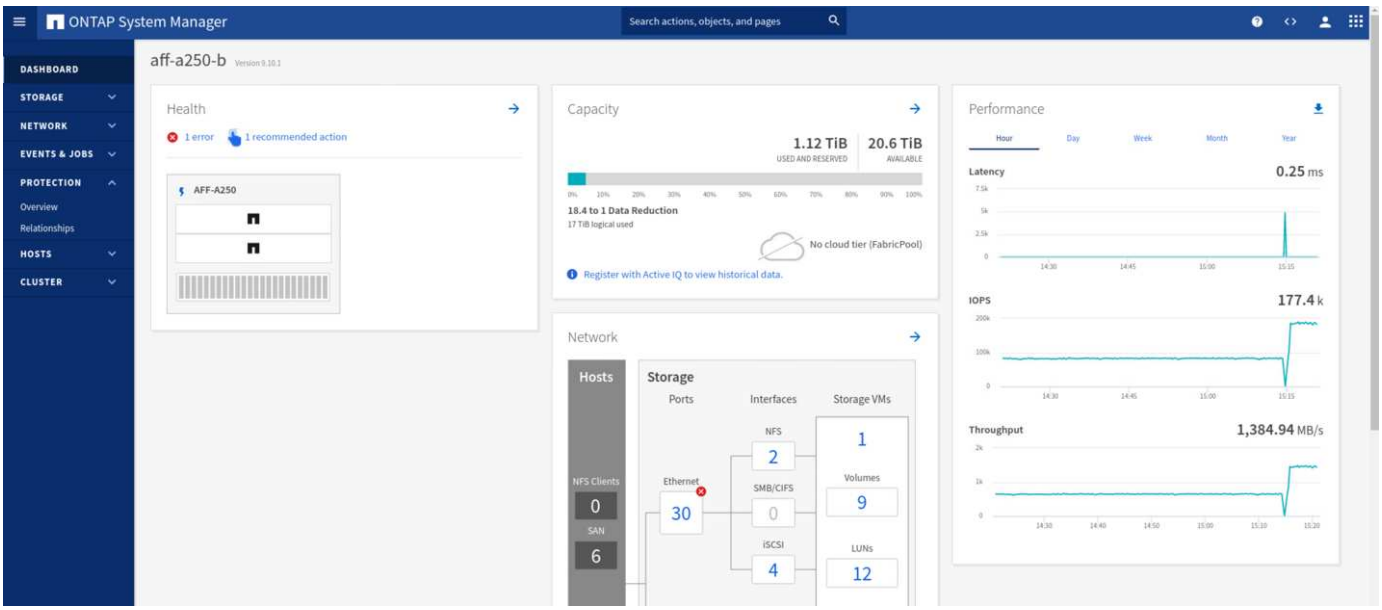
Während der Validierungstests generiert das IOMeter Tool auf den VMs an beiden Standorten I/O-Vorgänge für die lokalen Datenspeicher. Nachdem der Standort Ein Cluster ausgeschaltet war, wurden die I/O-Vorgänge kurz angehalten und danach wieder aufgenommen. In den folgenden beiden Abbildungen sind die Dashboards des Storage-Clusters an Standort A und Standort B bzw. vor dem Desaster dargestellt, die rund 80.000 IOPS und einen Durchsatz von 600 MB/s an jedem Standort zeigen.



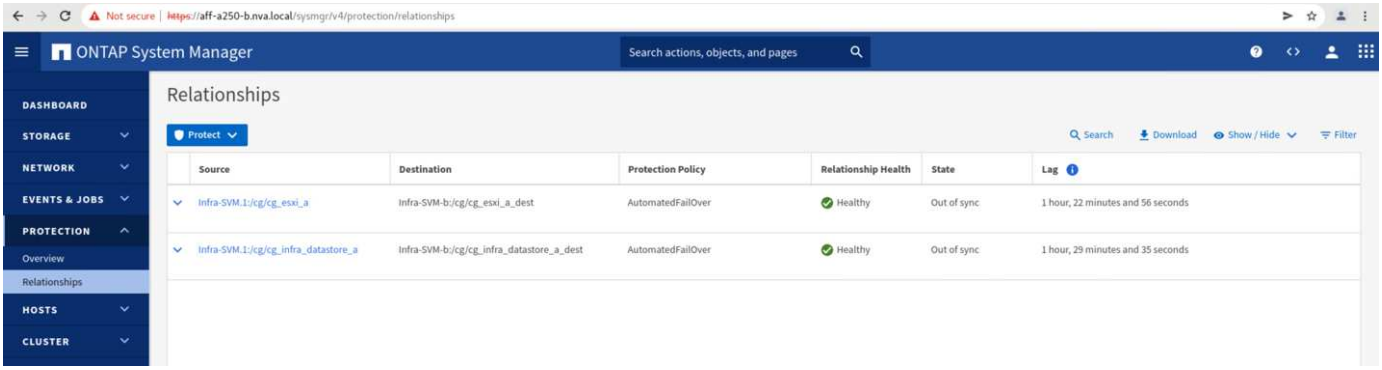


Nach dem Ausschalten der Storage-Controller an Standort A können wir visuell validieren, dass der I/O-Wert des Standort B Storage-Controllers stark erhöht wird, um zusätzliche Datenservices für Standort A bereitzustellen (siehe folgende Abbildung). Darüber hinaus zeigte die GUI der IOMeter VMs außerdem, dass die I/O-Vorgänge trotz eines Ausfalls des Standorts Im Storage-Cluster fortgesetzt wurden. Beachten Sie bitte, dass bei einem Storage-Ausfall zusätzliche Datastores, die von LUNs nicht durch SM-BC-Beziehungen

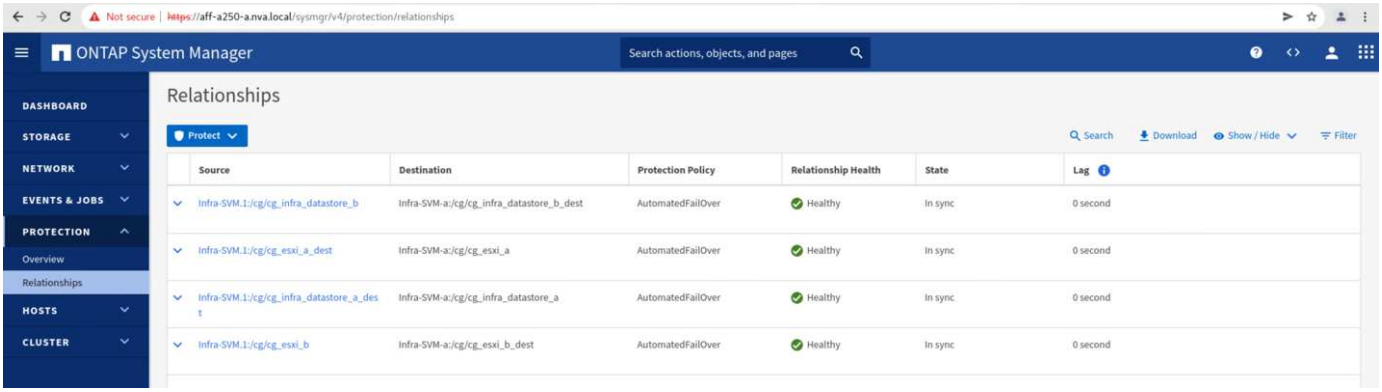
gesichert werden, nicht mehr zugänglich sind. Daher ist es wichtig, die geschäftlichen Anforderungen der verschiedenen Applikationsdaten zu bewerten und sie ordnungsgemäß in durch SM-BC-Beziehungen gesicherten Datenspeichern abzulegen, um Business Continuity zu gewährleisten.



Während der Standort Ein Cluster ausfällt, werden die Beziehungen der konsistenten Gruppen angezeigt `Out of sync` Status wie in der folgenden Abbildung dargestellt. Nachdem die Stromversorgung für die Storage-Controller an Standort A wieder eingeschaltet ist, startet das Storage-Cluster und die Datensynchronisierung zwischen Standort A und Standort B erfolgt automatisch.



Bevor Sie die Datenservices von Standort B zurück an Standort A zurücksenden, müssen Sie Standort A System Manager überprüfen und sicherstellen, dass die SM-BC-Beziehungen erfasst werden und der Status wieder synchron ist. Nachdem Sie bestätigt haben, dass die Konsistenzgruppen synchron sind, kann ein manueller Failover-Vorgang gestartet werden, um Datendienste in den Beziehungen der Konsistenzgruppen zurück an Standort A zurückzugeben



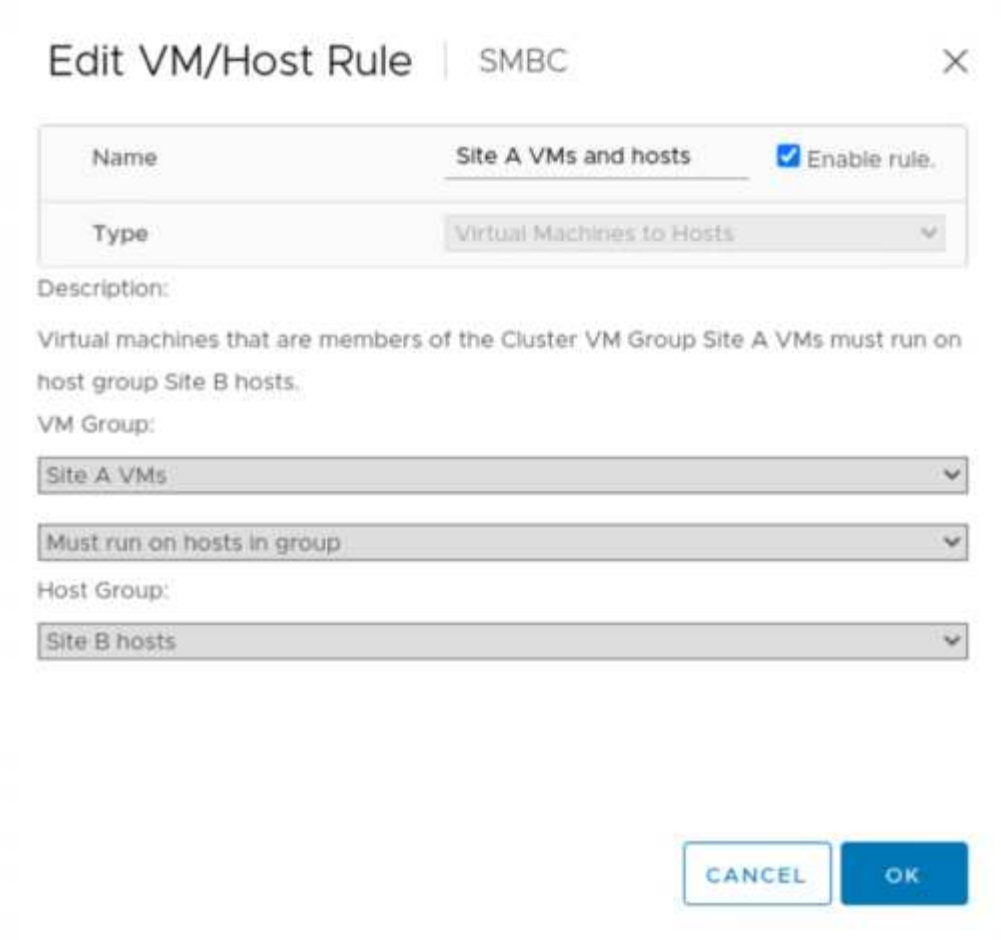
Komplette Wartung des Standorts oder des Standorts

Möglicherweise müssen Standortwartungsarbeiten durchgeführt, Stromverluste oder Naturkatastrophen wie Hurrikan oder Erdbeben ihre Auswirkungen haben. Daher ist es von entscheidender Bedeutung, dass geplante und ungeplante Standortausfälle angewendet werden, um sicherzustellen, dass Ihre FlexPod SM-BC Lösung richtig konfiguriert ist, damit diese Ausfälle all Ihrer geschäftskritischen Applikationen und Datenservices überleben können. Die folgenden standortbezogenen Szenarien wurden validiert.

- Geplantes Szenario für die Standortwartung durch Migration von Virtual Machines und wichtigen Datenservices zu einem anderen Standort
- Szenario mit ungeplanten Standortausfällen durch Ausschalten von Servern und Storage Controllern zur Disaster Simulation

Um einen Standort für die geplante Standortwartung vorbereitet zu sein, sind eine Kombination aus der Migration der betroffenen Virtual Machines vom Standort mit vMotion und ein manuelles Failover der SM-BC Consistency Group-Beziehungen erforderlich, um Virtual Machines und wichtige Datenservices auf einen alternativen Standort zu migrieren. Die Tests wurden in zwei verschiedenen Bestellungen durchgeführt: VMotion, zuerst gefolgt von SM-BC Failover und SM-BC Failover, gefolgt von vMotion, um sicherzustellen, dass die Virtual Machines weiterhin ausgeführt werden und die Datenservices nicht unterbrochen werden.

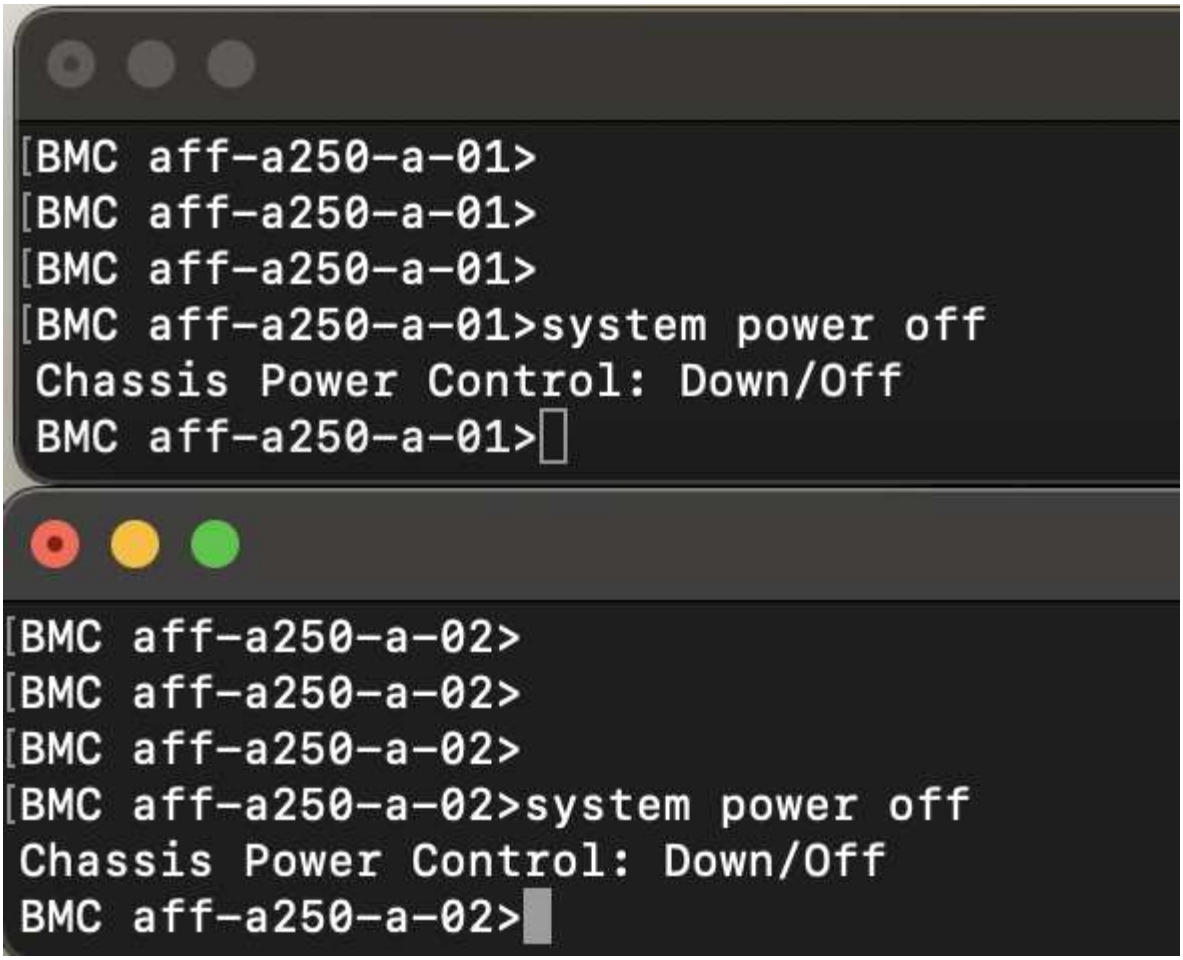
Aktualisieren Sie vor Durchführung der geplanten Migration die VM-/Host-Affinitätsregel, damit die VMs, die aktuell am Standort ausgeführt werden, automatisch von dem Wartungsort migriert werden. Der folgende Screenshot zeigt ein Beispiel für die Änderung der Regel für eine VM/Host-Affinität, die von VMs automatisch von Standort A nach Standort B migriert werden soll. Sie müssen nicht angeben, dass die VMs nun auf Standort B ausgeführt werden müssen, sondern können die Affinitätsregel vorübergehend deaktivieren, sodass die VMs manuell migriert werden können.



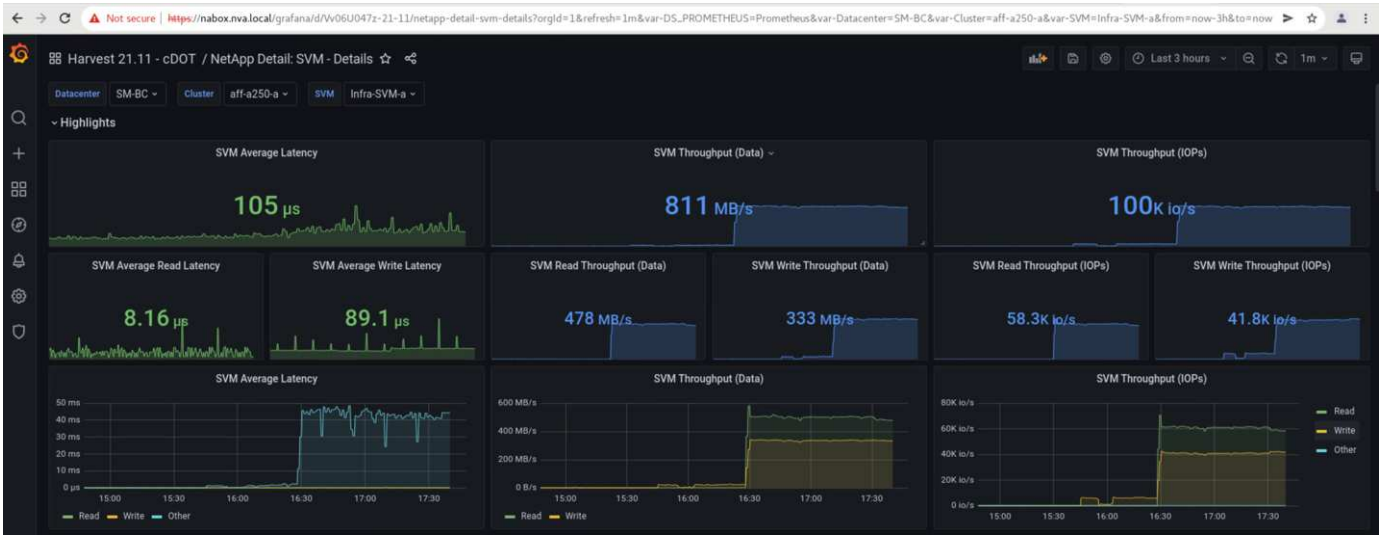
Nach der Migration von Virtual Machines und Storage Services können Sie Server, Storage Controller, Platten-Shelves und Switches ausschalten und die erforderlichen Wartungsarbeiten am Standort durchführen. Wenn die Standortwartung abgeschlossen ist und die FlexPod Instanz wieder aufgenommen wird, können Sie die Host-Gruppenaffinität für die VMs ändern, um wieder an den ursprünglichen Standort zurückzukehren. Danach sollten Sie die Regel „muss auf Hosts in Gruppe laufen“ VM/Host Site Affinity zurück zu „sollte auf Hosts in der Gruppe laufen“ ändern, so dass virtuelle Maschinen auf Hosts an dem anderen Standort ausgeführt werden dürfen, sollte eine Katastrophe stattfinden. Für die Validierungstests wurden alle Virtual Machines erfolgreich an den anderen Standort migriert, und die Datenservices werden nach dem Failover für die SM-BC-Beziehungen ohne Probleme fortgesetzt.

Bei der ungeplanten Disaster-Simulation am Standort wurden die Server und Storage Controller ausgeschaltet, um einen Standortausfall zu simulieren. Die VMware HA-Funktion erkennt die heruntergefahrenen Virtual Machines und startet die Virtual Machines am noch intakten Standort neu. Zudem erkennt der ONTAP Mediator, der an einem dritten Standort ausgeführt wird, den Standortausfall und der überlebende Standort initiiert einen Failover und beginnt mit der Bereitstellung von Datenservices für den Down-Standort wie erwartet.

Der folgende Screenshot zeigt, dass die Speicher-Controller Service-Prozessor-CLI verwendet wurden, um den Standort Ein Cluster abrupt auszuschalten, um eine Speicherkatastrophe zu simulieren.



Die Storage Virtual Machine Dashboards von Storage-Clustern, die vom NetApp Harvest Datenerfassungs-Tool erfasst und in Grafana Dashboard im NABox-Monitoring-Tool angezeigt werden, sind in den folgenden zwei Screenshots dargestellt. Wie auf der rechten Seite der IOPS- und Durchsatzdiagramme zu sehen ist, wählt der Cluster B sofort einen Storage-Workload aus, nachdem Standort Ein Cluster ausfällt.

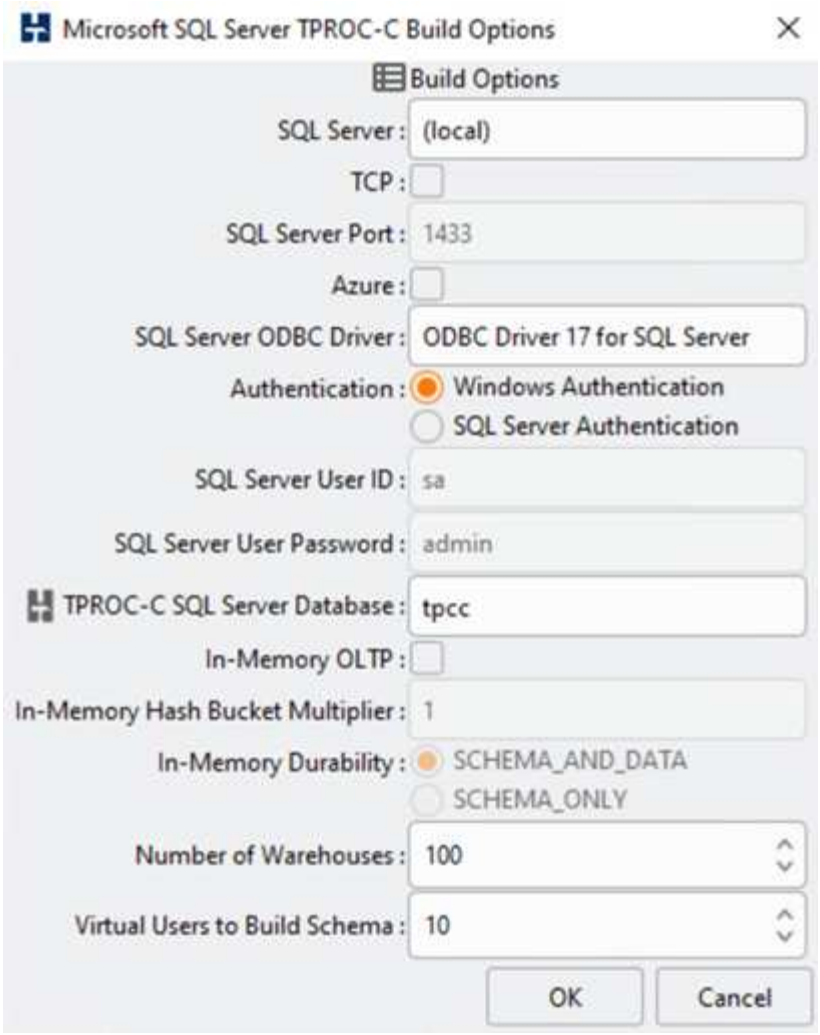


Microsoft SQL Server

Microsoft SQL Server ist eine weit verbreitete und implementierte Datenbankplattform für DIE IT in Unternehmen. Die Version Microsoft SQL Server 2019 enthält zahlreiche neue Funktionen und Verbesserungen für seine relationalen und analytischen Engines. Sie unterstützt Workloads bei Applikationen, die lokal, in der Cloud und bei hybriden Umgebungen über eine Kombination dieser Applikationen ausgeführt werden. Darüber hinaus kann die Lösung auf diversen Plattformen implementiert werden, darunter Windows, Linux und Container.

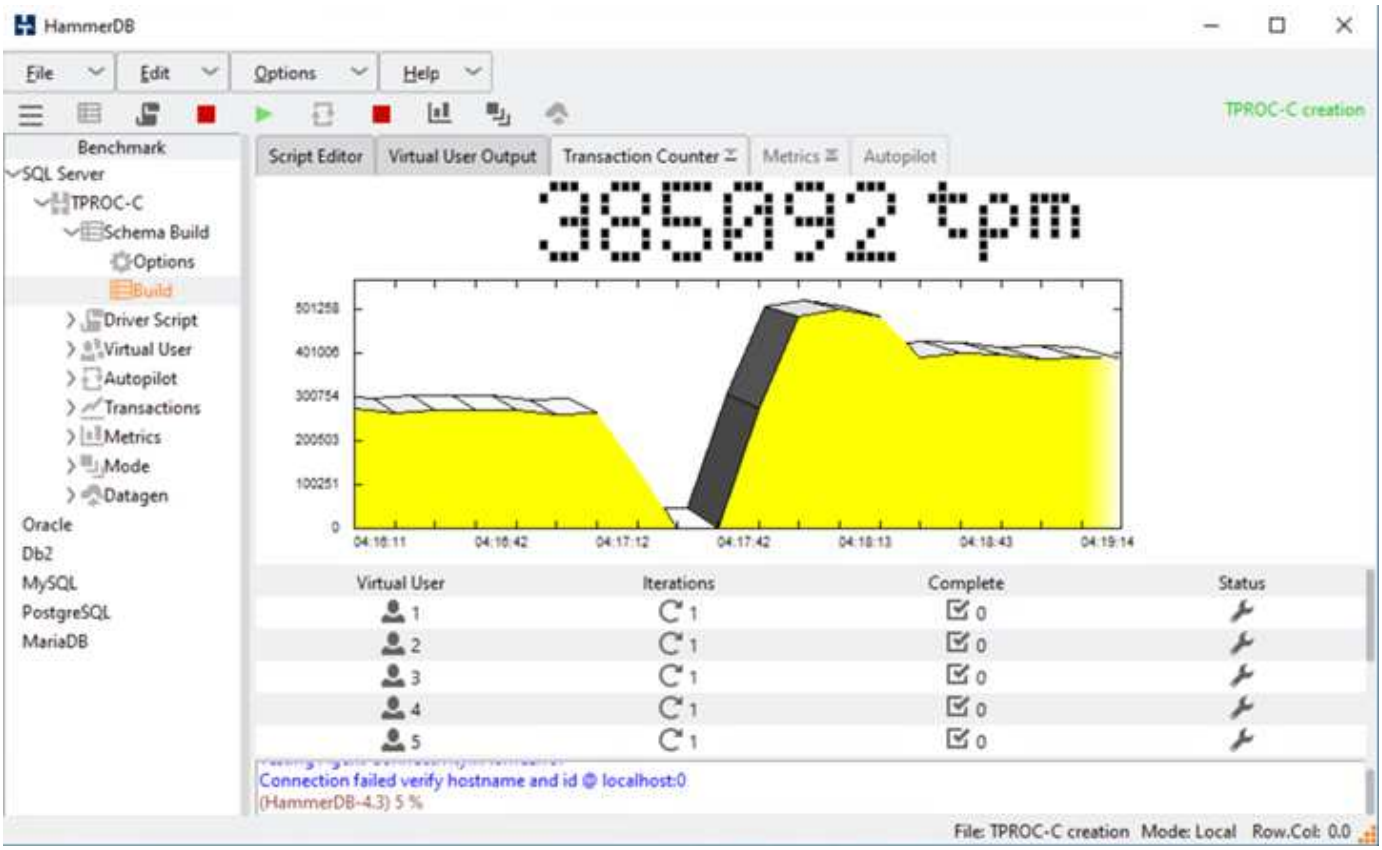
Im Rahmen der geschäftskritischen Workload-Validierung für die FlexPod SM-BC Lösung wird Microsoft SQL Server 2019 auf einer Windows Server 2022 VM installiert. Außerdem sind die IOMeter VMs für geplante und ungeplante Storage Failover-Tests enthalten. Auf der Windows Server 2022 VM wird SQL Server Management Studio installiert, um den SQL Server zu verwalten. Das Datenbanktool HammerDB wird für Tests zur Generierung von Datenbanktransaktionen eingesetzt.

Das HammerDB Datenbank-Testtool wurde für die Prüfung mit dem Microsoft SQL Server TPROC-C Workload konfiguriert. Für die Schemakonfigurationen wurden die Optionen aktualisiert, um 100 Lagerhäuser mit 10 virtuellen Benutzern zu verwenden, wie im folgenden Screenshot dargestellt.



Nachdem die Optionen zum Erstellen des Schemas aktualisiert wurden, wurde der Prozess zum Erstellen des Schemas gestartet. Einige Minuten später wurde ein ungeplanter Storage-Cluster an Standort B durch das gleichzeitige Herunterfahren beider Nodes des AFF A250 Storage-Clusters mit zwei Nodes mithilfe von CLI-Befehlen eingeleitet.

Nach einer kurzen Pause von Datenbanktransaktionen trat das automatisierte Failover zur Disaster-Korrektur ein und die Transaktionen wurden wieder aufgenommen. Der folgende Screenshot zeigt den HammerDB Transaction Counter Screenshot um diese Zeit. Da sich die Datenbank für den Microsoft SQL Server normalerweise im Storage-Cluster vor Ort B befindet, pausierte die Transaktion kurz, als der Storage an Standort B ausfällt und nach dem automatisierten Failover wieder aufgenommen wurde.



Die Storage Cluster-Kennzahlen wurden mithilfe des NAbox Tools mit dem installierten NetApp Harvest Monitoring Tool erfasst. Die Ergebnisse werden in den vordefinierten Grafana Dashboards für die Storage Virtual Machine und andere Speicherobjekte angezeigt. Das Dashboard bietet Matrizen für Latenz, Durchsatz, IOPS und zusätzliche Details mit Lese- und Schreibstatistiken, die sowohl für Standort B als auch Standort A getrennt sind

Dieser Screenshot zeigt das NAbox Grafana Performance-Dashboard für Storage-Cluster an Standort B.

Die IOPS für das Storage-Cluster am Standort B wiesen circa 100.000 IOPS auf, bevor der Ausfall einführte. Anschließend zeigte die Performance-Metriken einen deutlichen Rückgang auf Null auf der rechten Seite der Diagramme aufgrund des Ausfalls. Da der Storage-Cluster Standort B ausgefallen war, konnte nach der Katastrophe kein Storage-Cluster am Standort B gesammelt werden.

Andererseits nahmen die IOPS für den Standort Ein Storage-Cluster die zusätzlichen Workloads von Standort B nach dem automatisierten Failover ab. Der zusätzliche Workload kann im folgenden Screenshot auf der rechten Seite der IOPS- und Durchsatzdiagramme angezeigt werden. Darin wird das NAbox Grafana Performance-Dashboard für Standort A Storage-Cluster angezeigt.

Das oben aufgeführte Szenario für das Storage-Disaster-Test bestätigte, dass der Microsoft SQL Server Workload einen vollständigen Ausfall des Storage-Clusters an Standort B überleben kann, wo sich die Datenbank befindet. Die Applikation verwendete die von dem Standort Einem Storage-Cluster bereitgestellten Datenservices transparent, nachdem ein Ausfall erkannt und der Failover stattgefunden hat.

Wenn auf der Rechenebene die VMs, die an einem bestimmten Standort ausgeführt werden, ein Host-Ausfall auftreten, werden die VMs so konzipiert, dass sie automatisch durch die VMware HA-Funktion neu gestartet werden. Für einen vollständigen Ausfall des Standorts ermöglicht es die VM-/Host-Affinitätsregeln, VMs am noch intakten Standort neu zu starten. Damit eine geschäftskritische Applikation unterbrechungsfreie Services bereitstellen kann, ist jedoch ein applikationsbasiertes Clustering wie Microsoft Failover Cluster oder Container-basierte Applikationsarchitektur für Kubernetes erforderlich, um Ausfallzeiten bei Applikationen zu vermeiden. Bitte lesen Sie das entsprechende Dokument zur Implementierung des applikationsbasierten Clustering. Dieses Dokument übersteigt den Rahmen dieses technischen Berichts.

"Weiter: Fazit."

Schlussfolgerung

"Zurück: Lösungsvalidierung - validierte Szenarien."

Das FlexPod Datacenter mit SM-BC beruht auf einem aktiv/aktiv-Datacenter-Design, das Business Continuity und Disaster Recovery für geschäftskritische Workloads bietet. Mit der Lösung sind normalerweise zwei Datacenter verknüpft, die an separaten, geografisch verteilten Standorten in einem Großraumgebiet bereitgestellt werden. Die NetApp SM-BC Lösung verwendet synchrone Replizierung, um geschäftskritische Datenservices gegen einen Standortausfall zu schützen. Voraussetzung für die Lösung ist, dass die beiden FlexPod-Bereitstellungsstandorte eine Netzwerklatenz von weniger als 10 Millisekunden pro Jahr nutzen.

Der NetApp ONTAP Mediator, der an einem dritten Standort implementiert wird, überwacht die SM-BC-Lösung und ermöglicht ein automatisiertes Failover bei einem Standortausfall. VMware vCenter mit VMware HA und

Stretched VMware vSphere Metro Storage Cluster Konfiguration funktionieren nahtlos mit NetApp SM-BC, damit die Lösung die gewünschten RPO von null und RTO von fast null erfüllt.

Die FlexPod SM-BC Lösung kann auch in vorhandenen FlexPod Infrastrukturen implementiert werden, wenn sie die Anforderungen erfüllen, oder wenn eine zusätzliche FlexPod Lösung zu einem vorhandenen FlexPod hinzugefügt wird, um die Business Continuity-Ziele zu erreichen. Zusätzliche Management-, Monitoring- und Automatisierungs-Tools wie Cisco Intersight, Ansible und HashiCorp Terraform- basierte Automatisierung stehen von NetApp und Cisco zur Verfügung, damit Sie die Lösung einfach überwachen, Einblicke in ihren Betrieb erhalten und die Implementierung und den Betrieb automatisieren können.

Aus Sicht einer geschäftskritischen Applikation wie Microsoft SQL Server ist eine Datenbank, die sich auf einem VMware Datastore befindet und durch eine ONTAP SM-BC CG-Beziehung geschützt ist, trotz eines Standort-Storage-Ausfalls weiterhin verfügbar. Wie während der Validierungstests verifiziert, wird nach einem Stromausfall im Storage Cluster, in dem sich die Datenbank befindet, ein Failover der SM-BC CG-Beziehung durchgeführt und die Microsoft SQL Server Transaktionen ohne Applikationsunterbrechung fortgesetzt.

Dank der granularen Datensicherung für Applikationen können ONTAP SM-BC CG-Beziehungen für geschäftskritische Applikationen erstellt werden, um RPO-Anforderungen von null und RTO von nahezu null zu erfüllen. Damit das VMware Cluster, auf dem die Microsoft SQL Server Applikation ausgeführt wird, einen Storage-Ausfall vor Ort überleben kann, sind die Boot-LUNs der ESXi Hosts an jedem Standort ebenfalls durch eine SM-BC CG-Beziehung geschützt.

Dank der Flexibilität und Skalierbarkeit von FlexPod können Sie mit einer geeigneten Infrastruktur beginnen, die sich Ihren wachsenden Geschäftsanforderungen anpassen lässt. Dieses validierte Design ermöglicht es Ihnen, zuverlässig eine auf VMware vSphere basierende Private Cloud in einer verteilten und integrierten Infrastruktur zu implementieren. Dadurch erhalten Sie eine Lösung, die sich gegen viele Single-Point-of-Failure-Szenarien sowie einen Standortausfall schützen kann, sodass wichtige Business-Datenservices geschützt sind.

"Weiter: Wo finden Sie zusätzliche Informationen und Versionsverlauf."

Wo finden Sie weitere Informationen und Versionsverlauf

"Zurück: Schlussfolgerung."

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

FlexPod

- 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"

- Cisco Server – Unified Computing System (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- NetApp Produktdokumentation

"https://www.netapp.com/support-and-training/documentation/"

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

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

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

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

- FlexPod Datacenter mit Cisco UCS X-Serie, VMware 7.0 U2 und NetApp ONTAP 9.9 Design Guide

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

- FlexPod Datacenter mit Cisco UCS X-Serie, VMware 7.0 U2 und NetApp ONTAP 9.9 Deployment Guide

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp All Flash FAS/FAS NVA Design-Leitfaden

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- FlexPod Express for VMware vSphere 7.0 with Cisco UCS Mini and NetApp AFF/FAS NVA Deployment Guide

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP mit VXLAN-Frontend für mehrere Standorte

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox

  "https://nabox.org"

- NetApp Harvest

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

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

- TR-4878: SnapMirror Business Continuity (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Wie eine SnapMirror Beziehung ONTAP 9 richtig gelöscht wird

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Grundlagen von SnapMirror Synchronous Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Grundlagen der asynchronen SnapMirror Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Datensicherung und Disaster Recovery

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Installieren oder aktualisieren Sie den ONTAP Mediator-Dienst

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

VMware vSphere HA und vSphere Metro Storage Cluster

- Erstellen und Verwenden von vSphere HA-Clustern

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage-Cluster (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Empfohlene Practices für VMware vSphere Metro Storage-Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP mit NetApp SnapMirror Business Continuity (SM-BC) mit VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Schutz von Tier-1-Applikationen und -Datenbanken mit VMware vSphere Metro Storage-Cluster und ONTAP

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL und HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Architecting Microsoft SQL Server on VMware vSphere Best Practices Guide

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- HammerDB-Website

  "https://www.hammerdb.com"

Kompatibilitätsmatrix

- Cisco UCS Hardware Compatibility Matrix

  "https://ucshcltool.cloudapps.cisco.com/public/"

- NetApp Interoperabilitäts-Matrix-Tool

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

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- VMware Compatibility Guide

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

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2022	Erste Version.

FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 – Bereitstellung

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt das Cisco und NetApp FlexPod-Datacenter mit NetApp ONTAP 9.7 auf NetApp AFF A400 All-Flash-Storage-System, die Unified Software-Version 4.1(2) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation und VMware vSphere 7.0. Cisco UCS Manager (UCSM) 4.1(2) bietet konsolidierten Support für Folgendes:

- Alle aktuellen Cisco UCS Fabric Interconnect-Modelle: 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- IOM der Serie 2200/2300/2400
- Cisco UCS B-Serie
- Cisco UCS C-Serie

Darüber hinaus sind die Cisco Intersight- und NetApp Active IQ-SaaS-Managementplattformen enthalten.

FlexPod-Datacenter mit NetApp ONTAP 9.7, Cisco UCS Unified Software Release 4.1(2) und VMware vSphere 7.0 umfassen eine vorab entwickelte Best-Practice Datacenter-Architektur auf Basis des Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switches, MDS 9000 Multilayer Fabric Switches, Und den NetApp Storage-Arrays der AFF A-Serie mit der Datenmanagement-Software ONTAP 9.7.

"FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 – Bereitstellung"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, einen validierten Ansatz zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere, der beliebtesten Virtualisierungsplattform der Enterprise-Klasse für Datacenter auf FlexPod.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 – Deployment

John George, Cisco Scott Kovacs, NetApp

Der aktuelle Trend in der Datacenter-Branche geht hin zu Shared IT Infrastructures. Durch die Virtualisierung und vorab validierte IT-Plattformen begeben sich Enterprise-Kunden auf den Weg zur Cloud. Sie verlassen sich dabei auf Applikationssilos und nutzen eine schnell implementierbare Shared IT-Infrastruktur, wodurch sich die Flexibilität erhöht und die Kosten sinken. Cisco und NetApp haben gemeinsam FlexPod entwickelt. Diese Technologie verwendet branchenführende Storage-, Server- und Netzwerkkomponenten, um als Grundlage für eine Vielzahl von Workloads zu dienen. So können effiziente Architekturdesigns bereitgestellt werden, die schnell und sicher implementiert werden können.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 – Deployment"

FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt eine validierte Lösung zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere,

der beliebtesten Virtualisierungsplattform der Enterprise-Klasse für Datacenter auf FlexPod.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und Anwendungsfällen unterstützt. Mit dieser Lösung können Kunden schnell und zuverlässig eine auf VMware vSphere basierende Private Cloud in einer integrierten Infrastruktur implementieren.

"FlexPod-Datacenter mit Cisco Intersight und NetApp ONTAP 9.7 - Design"

FlexPod-Datacenter mit VMware vSphere 6.7 U2, Cisco UCS – Fabric-Infrastruktur der Forth-Generation und NetApp ONTAP 9.6

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt das FlexPod-Datacenter von Cisco und NetApp mit NetApp ONTAP 9.6, die Unified Software Release 4.0(4) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation und VMware vSphere 6.7 U2. Cisco UCS Manager (UCSM) 4.0(4) bietet konsolidierten Support für Folgendes:

- Alle aktuellen Cisco UCS Fabric Interconnect-Modelle: 6200, 6300, 6324 (Cisco UCS Mini)
- 6454
- IOM der Serie 2200/2300/2400
- Cisco UCS B-Serie
- Cisco UCS C-Serie:

FlexPod-Datacenter mit NetApp ONTAP 9.6, Cisco UCS Unified Software Release 4.0(4) und VMware vSphere 6.7 U2 ist eine vorab entwickelte Best-Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switch-Familie, MDS 9000 Multilayer Fabric Switches, NetApp AFF Storage-Arrays Der A-Serie mit ONTAP 9.

"FlexPod-Datacenter mit VMware vSphere 6.7 U2, Cisco UCS Fabric der vierten Generation und NetApp ONTAP 9.6"

FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series – Design

John George, Cisco Sree Lakshmi Lanka, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, einen validierten Ansatz zur Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur. Das validierte Design liefert die Rahmenbedingungen für die Implementierung von VMware vSphere, der beliebtesten Virtualisierungsplattform der Enterprise-Klasse von Datacentern auf FlexPod.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und

Anwendungsfällen unterstützt. Mit dieser Lösung können Kunden eine auf VMware vSphere basierende Private Cloud schnell und zuverlässig in einer integrierten Infrastruktur implementieren.

Die empfohlene Lösungsarchitektur basiert auf Cisco Unified Computing System (Cisco UCS) und verwendet die einheitliche Softwareversion zur Unterstützung der Cisco UCS Hardware-Plattformen, einschließlich Cisco UCS B-Series Blade- und C-Series Rack-Servern, Cisco UCS 6454 Fabric Interconnects, Switches der Cisco Nexus 9000 Serie, Cisco MDS Fibre Channel Switches, NetApp All-Flash-Storage-Arrays vorgestellt. Darüber hinaus enthält es VMware vSphere 6.7 Update 1, das eine Reihe neuer Funktionen zur Optimierung der Storage-Auslastung und zur Einrichtung einer privaten Cloud bietet.

"FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series – Design"

FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series

John George, Cisco Scott Kovacs, NetApp

Dieses Dokument beschreibt das FlexPod-Datacenter von Cisco und NetApp mit der einheitlichen Softwareversion 4.0(2) von Cisco UCS Manager und VMware vSphere 6.7 U1. Cisco UCS Manager (UCSM) 4.0(2) bietet konsolidierten Support für alle aktuellen Cisco UCS Fabric Interconnect Modelle (6200, 6300, 6324 (Cisco UCS Mini)), IOM der Serie 6454,2200/2300, Cisco UCS B-Serie und Cisco UCS C-Serie. FlexPod Datacenter mit Cisco UCS Unified Software Release 4.0(2) und VMware vSphere 6.7 U1 ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (UCS), der Cisco Nexus 9000 Switch-Familie und MDS 9000 Multilayer Fabric Switches basiert. Und NetApp Storage-Arrays der AFF A-Serie mit dem Storage-Betriebssystem ONTAP 9.

"FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS Fabric der vierten Generation und NetApp AFF A-Series"

Design von FlexPod Datacenter mit Cisco ACI Multi-Pod, NetApp MetroCluster IP und VMware vSphere 6.7

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Dieses Dokument beschreibt die Integration der Cisco ACI Multi-Pod und NetApp MetroCluster IP Lösung in das FlexPod Datacenter, um eine hochverfügbare Multi-Datacenter-Lösung anzubieten. Die Multi-Datacenter-Architektur bietet die Möglichkeit, Workloads zwischen zwei Datacentern auszubalancieren, indem unterbrechungsfreie Workload-Mobilität genutzt wird. Auf diese Weise können Services ohne Unterbrechung eines Ausfalls zwischen den Standorten migriert werden.

Die FlexPod mit ACI Multi-Pod und NetApp MetroCluster IP Lösung bietet folgende Vorteile:

- Nahtlose Workload-Mobilität über mehrere Datacenter hinweg
- Einheitliche Richtlinien an allen Standorten

- Layer-2-Erweiterung über geografisch verteilte Datacenter hinweg
- Verbesserte Vermeidung von Ausfallzeiten während der Wartung
- Vermeidung von Ausfällen und Recovery

"Design von FlexPod Datacenter mit Cisco ACI Multi-Pod, NetApp MetroCluster IP und VMware vSphere 6.7"

FlexPod Datacenter mit Cisco ACI Multi-Pod mit NetApp MetroCluster IP und VMware vSphere 6.7 – Implementierung

Haseeb Niazi, Cisco Ramesh Issac, Cisco Arvind Ramakrishnan, NetApp

Cisco und NetApp haben gemeinsam eine Reihe von FlexPod Lösungen zur Unterstützung strategischer Datacenter-Plattformen entwickelt. Die FlexPod Lösung bietet eine integrierte Architektur, die Best Practices für das Design von Computing, Storage und Netzwerken umfasst. Dadurch werden IT-Risiken minimiert, indem die integrierte Architektur validiert wird, um die Kompatibilität verschiedener Komponenten sicherzustellen. Die Lösung löst auch IT-Problempunkte durch dokumentierte Designanleitungen, Implementierungsanleitungen und Support, die in verschiedenen Phasen (Planung, Entwurf und Implementierung) einer Bereitstellung verwendet werden können.

"FlexPod Datacenter mit Cisco ACI Multi-Pod mit NetApp MetroCluster IP und VMware vSphere 6.7 – Implementierung"

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.

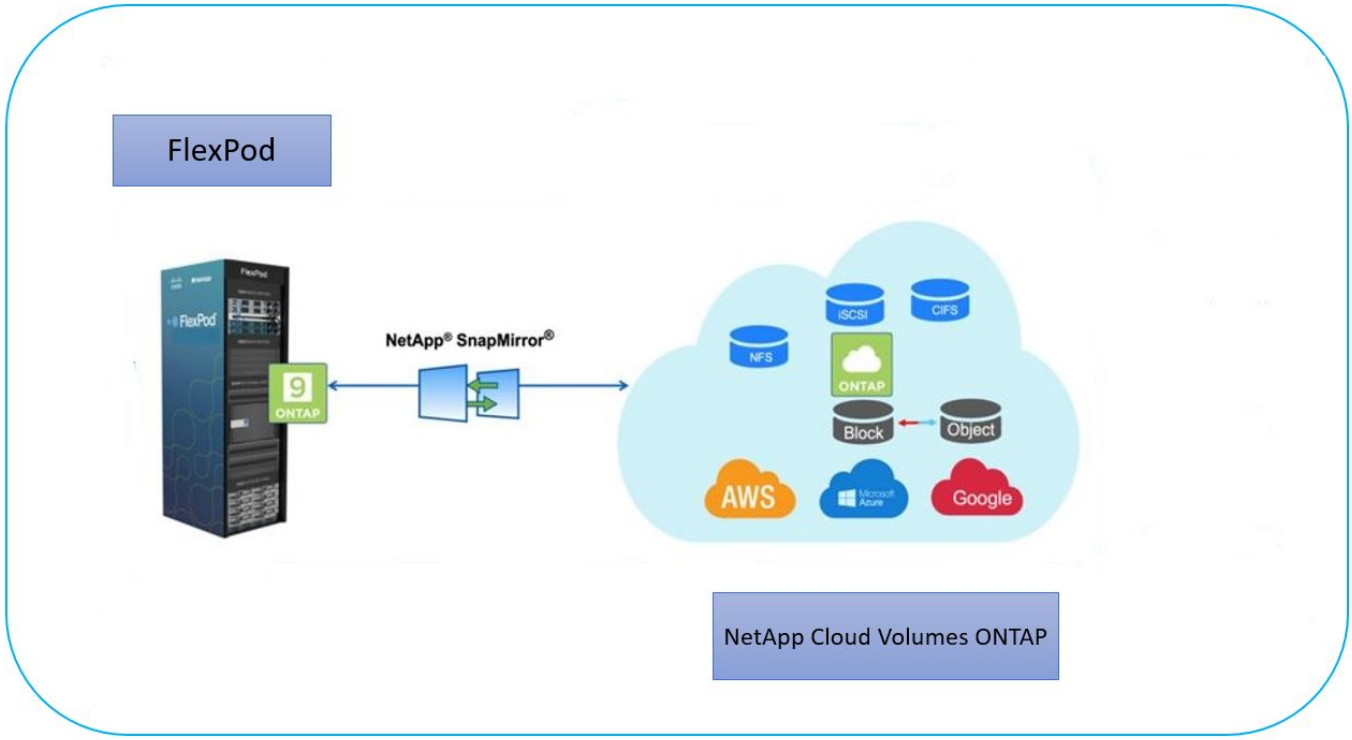
Durch die stetig wachsende Datenmenge im Gesundheitswesen und die wertvollen Einblicke, die diese Daten bieten, werden Datenservices und Datensicherung im Gesundheitswesen zu einer wichtigen und schwierigen Herausforderung. Erstens müssen Daten im Gesundheitswesen sowohl verfügbar als auch geschützt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

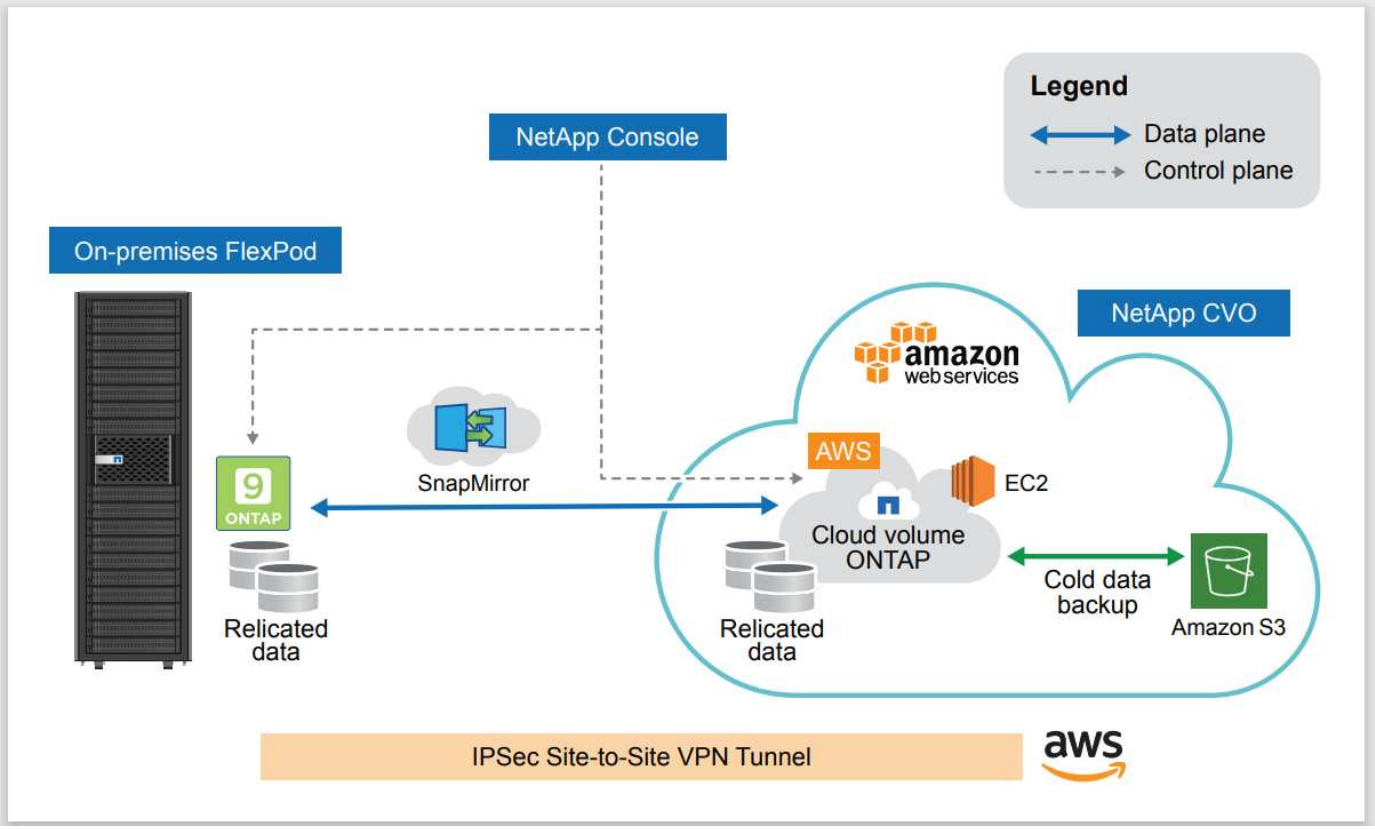
Eine Integration von FlexPod Datacenter mit NetApp Cloud Volumes ONTAP bietet folgende Vorteile für Workloads im Gesundheitswesen:

- **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.

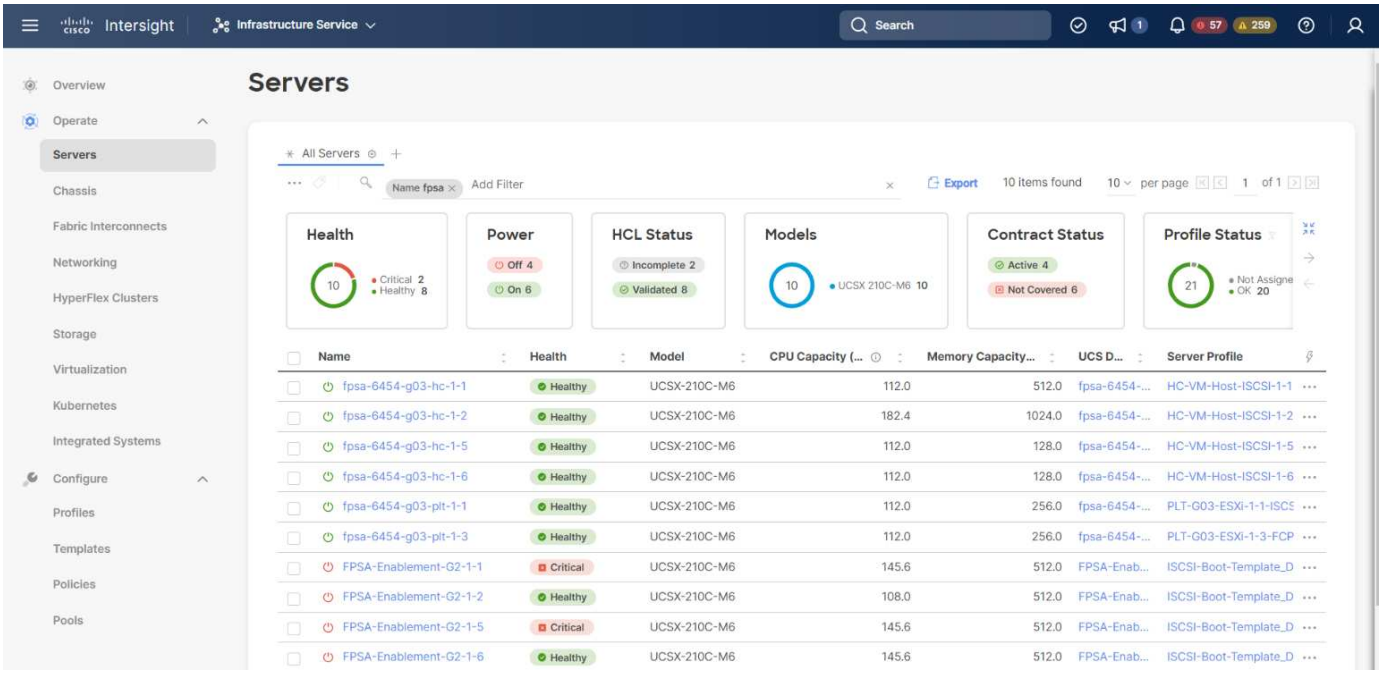
Weitere Informationen finden Sie unter "Active IQ Unified Manager".

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.

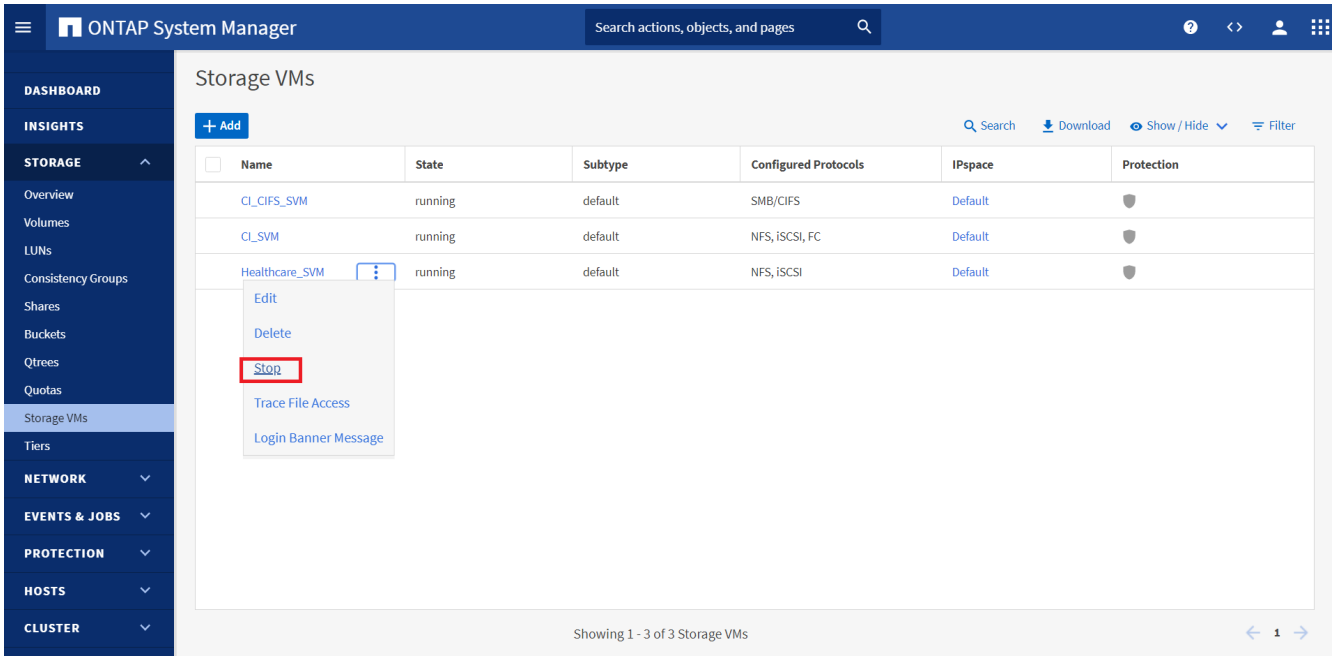
Disaster Recovery

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.

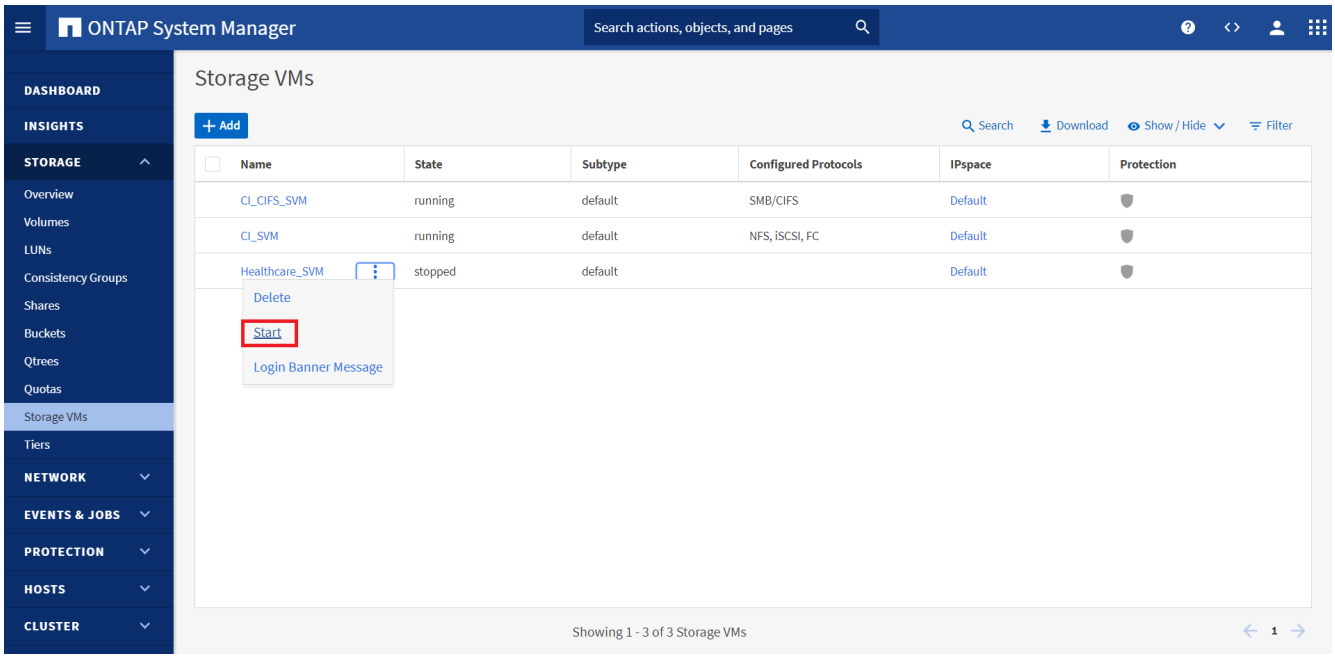
Verifizierung der Daten am Produktionsstandort

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).

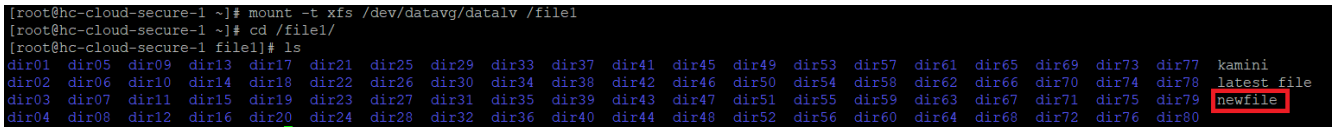
```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver        volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

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

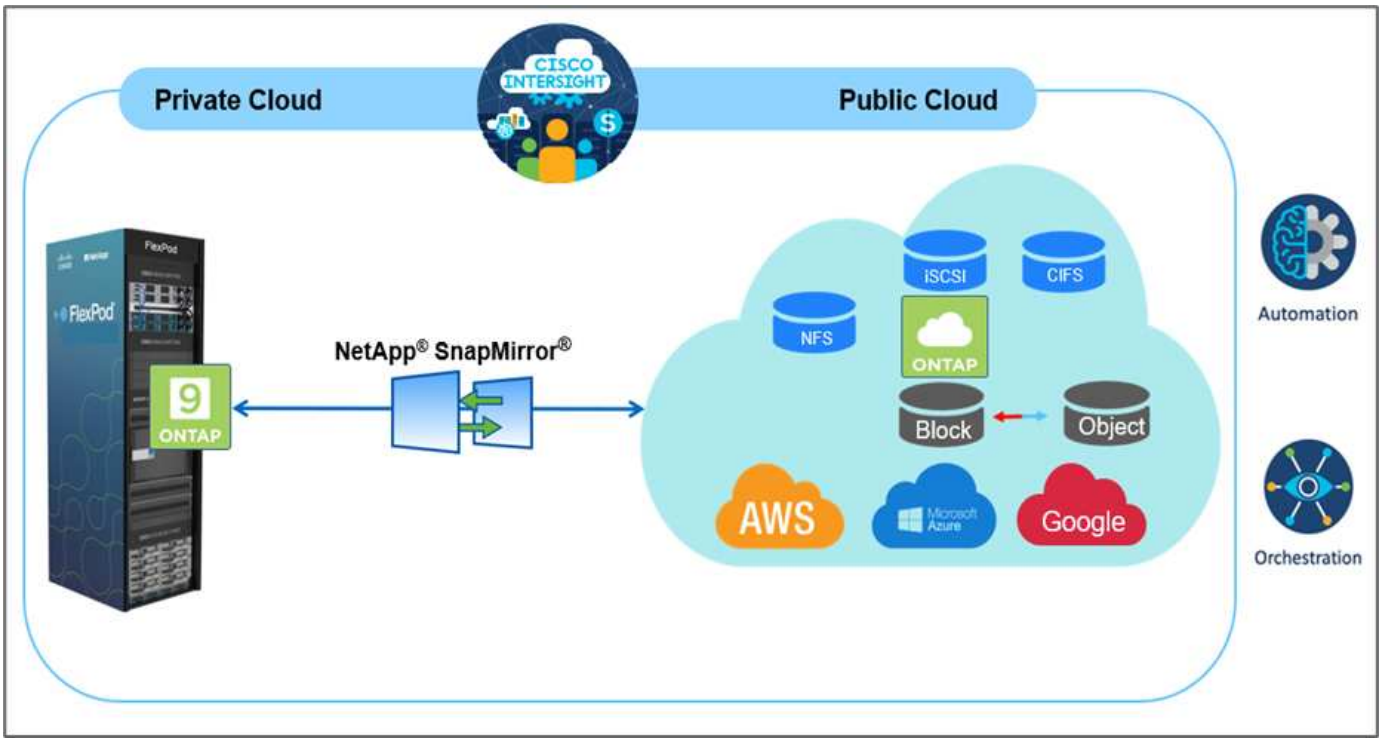
Der Schutz von Daten mit Disaster Recovery (DR) ist ein wichtiges Ziel für die Aufrechterhaltung von Unternehmenskontinuität. DR ermöglicht Unternehmen ein Failover ihrer Betriebsabläufe an einem sekundären Standort und Recovery und Failback effizient und zuverlässig zum primären Standort. Aufgrund diverser 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:

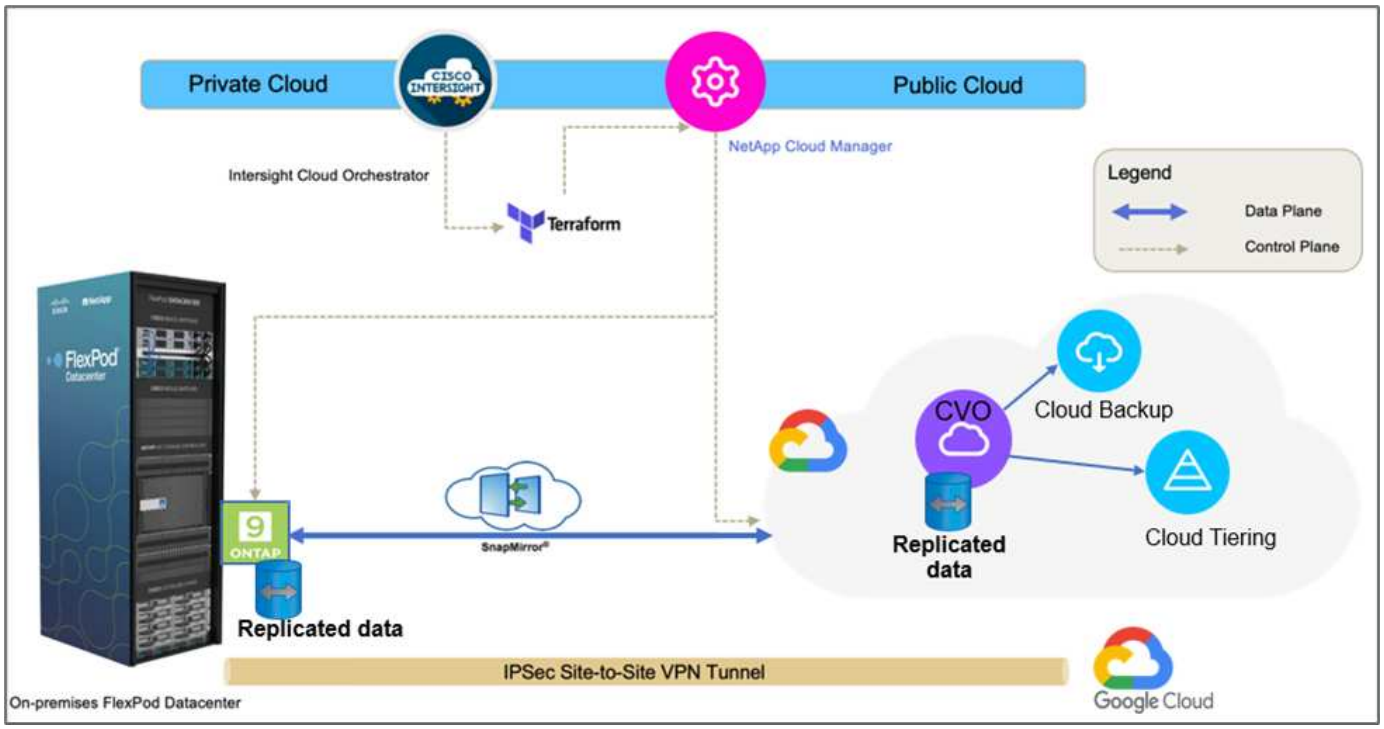
- **Orchestrierung und Automatisierung.** Cisco Intersight vereinfacht den täglichen Betrieb einer FlexPod Hybrid-Cloud-Infrastruktur durch Bereitstellung konsistenter Orchestrierungs-Frameworks, die über Automatisierung bereitgestellt werden.
- **Customized Protection.** Cloud Volumes ONTAP bietet Daten 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".

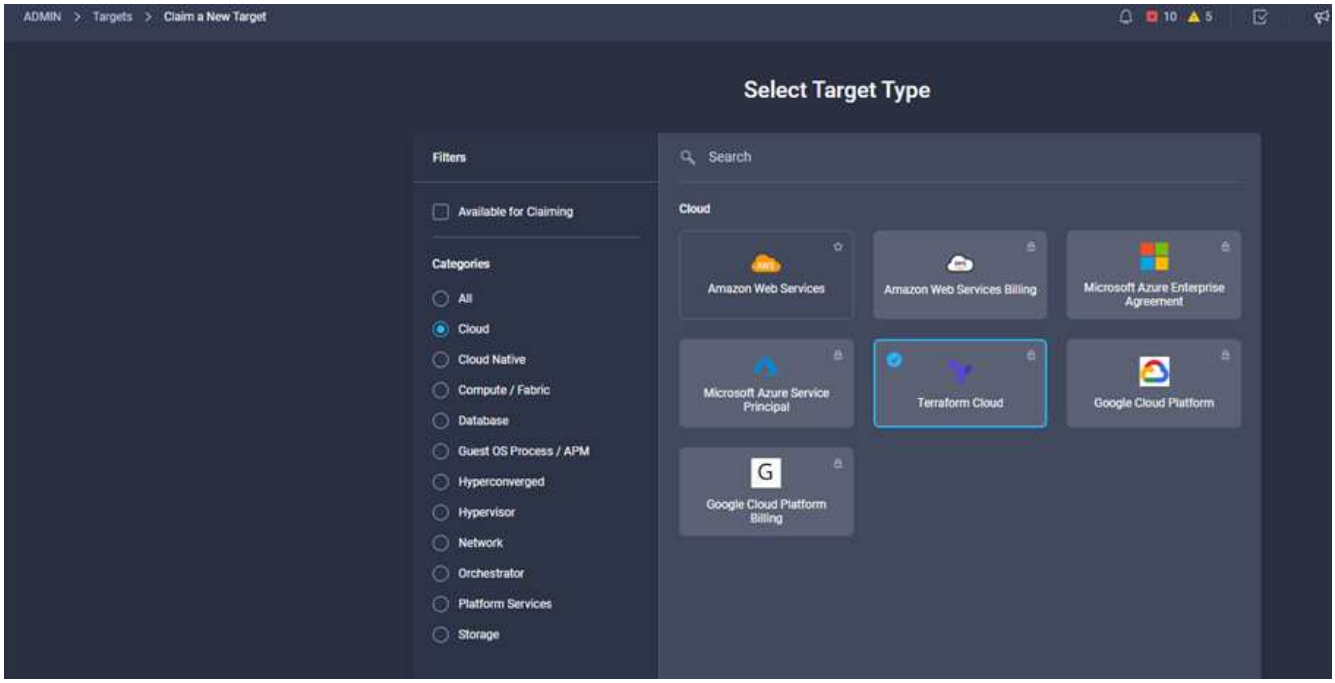
Verfahren 2: Benutzer-Token generieren

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

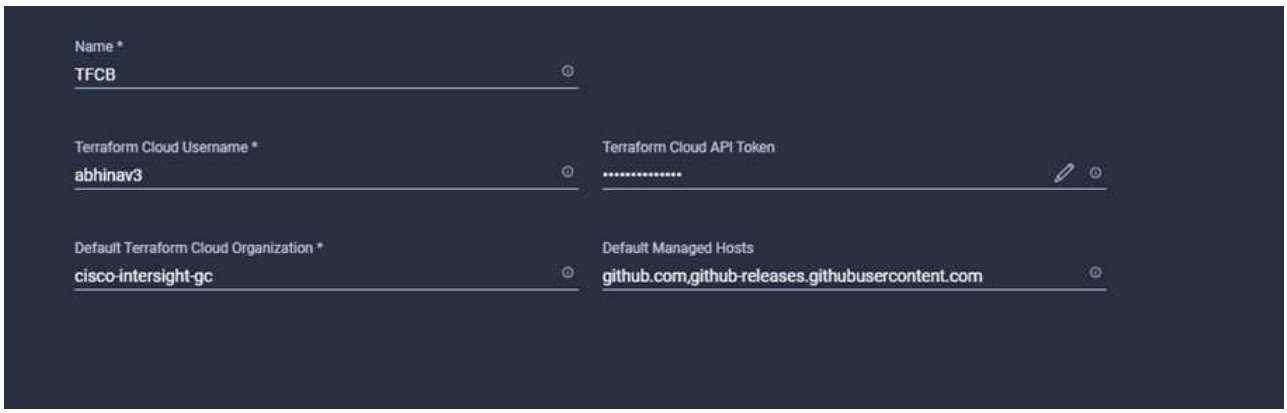
1. Melden Sie sich bei Terraform Cloud an und gehen Sie zu **Benutzer-Token**: "https://app.terraform.io/app/settings/tokens".
2. Klicken Sie auf **Erstellen Sie ein neues API-Token**.
3. Weisen Sie einen Namen zu merken und speichern Sie das Token an einem sicheren Ort.

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

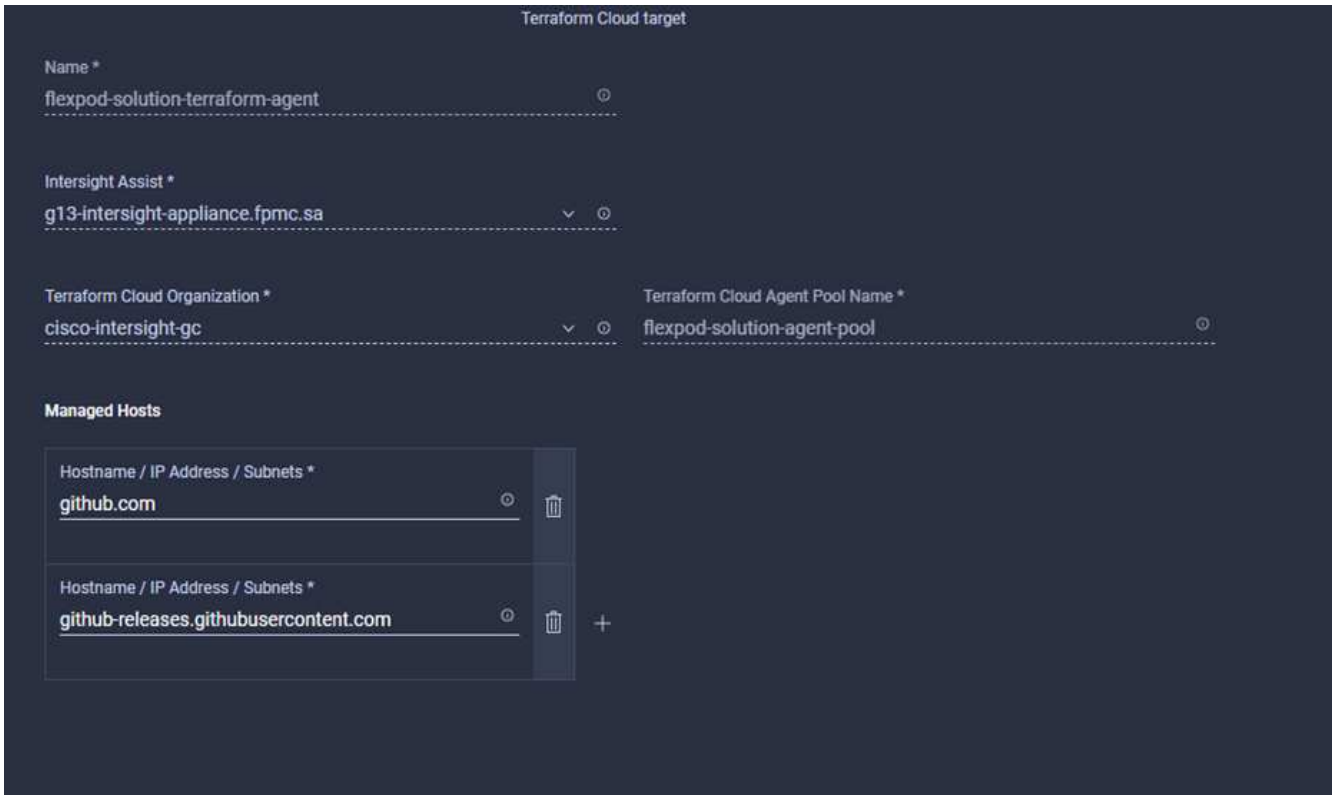
Voraussetzungen:

- 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.

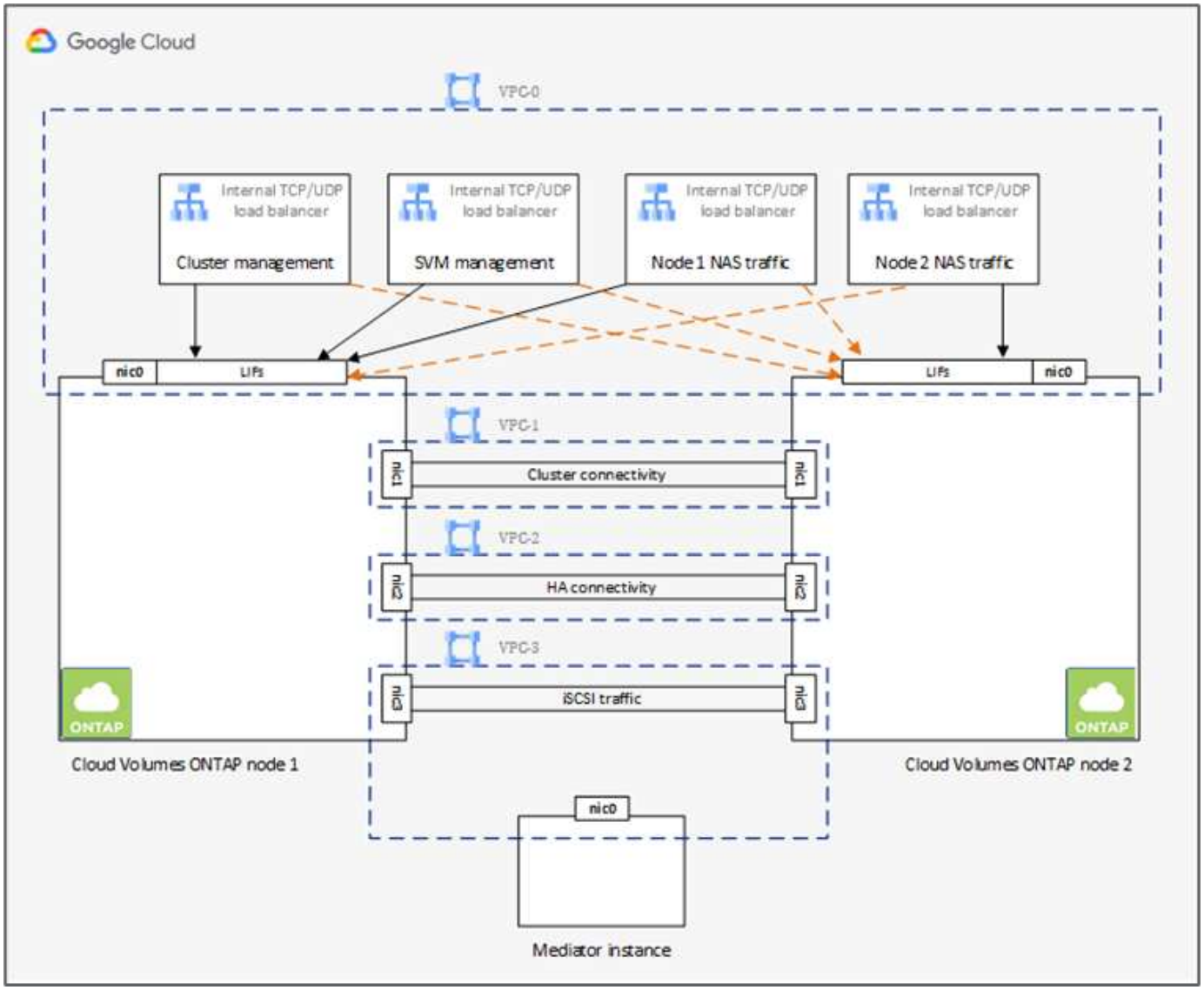
Hochverfügbare Cloud Volumes ONTAP in Google Cloud

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:

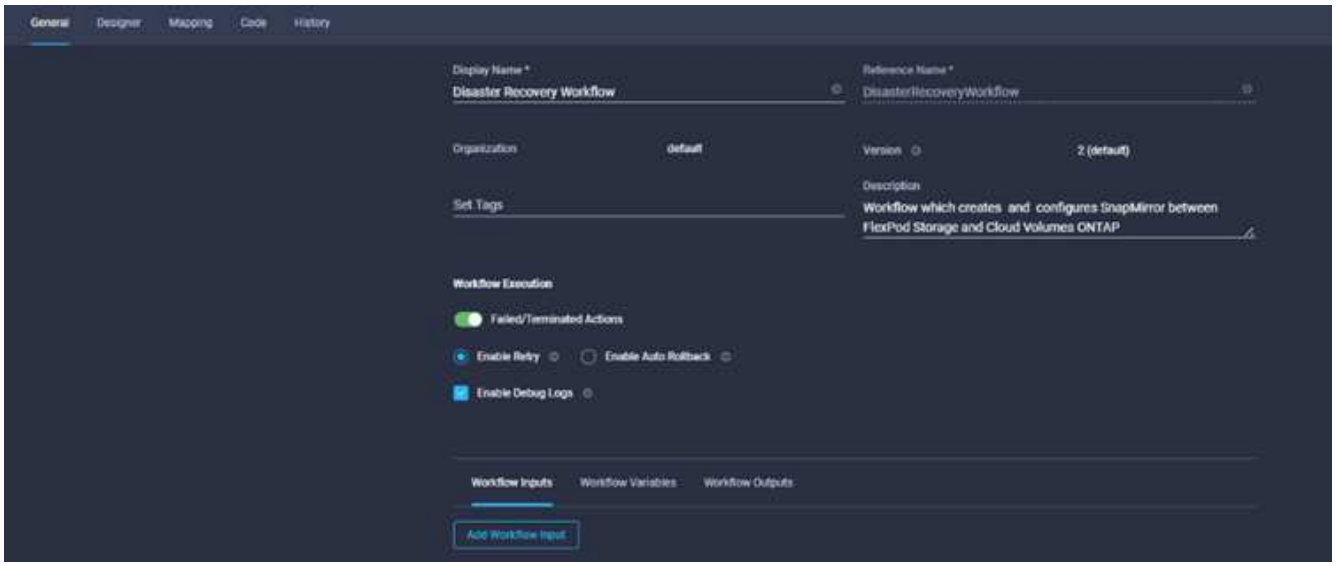
    - Terraform-Workspace hinzufügen
    - Terraform-Variablen hinzufügen
    - Terraform-sensible Variablen hinzufügen
    - Starten Sie den neuen Terraform-Plan

- Terraform-Lauf bestätigen

4. Validieren Sie den Workflow.

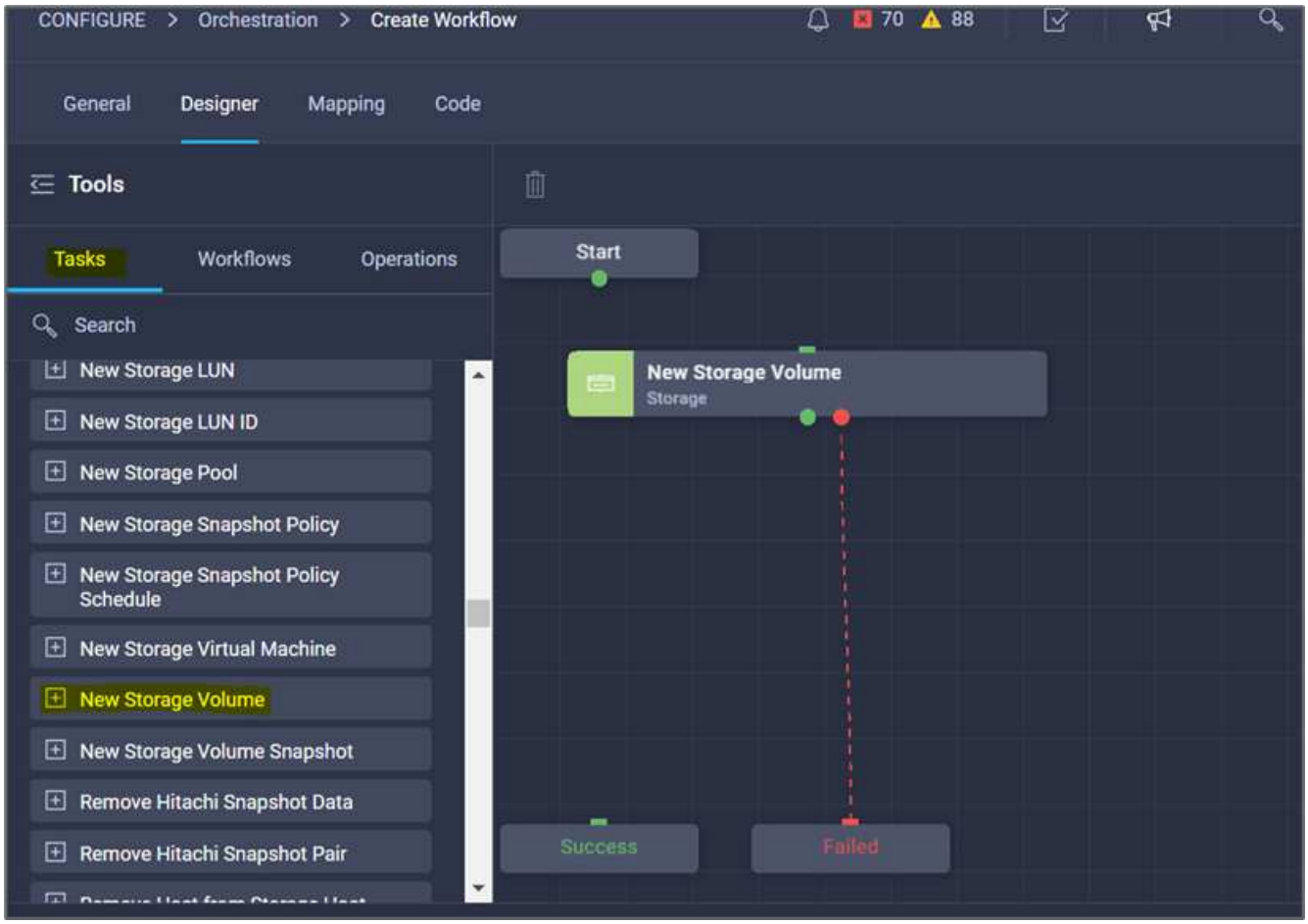
Verfahren 1: Erstellen Sie den Workflow

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 .

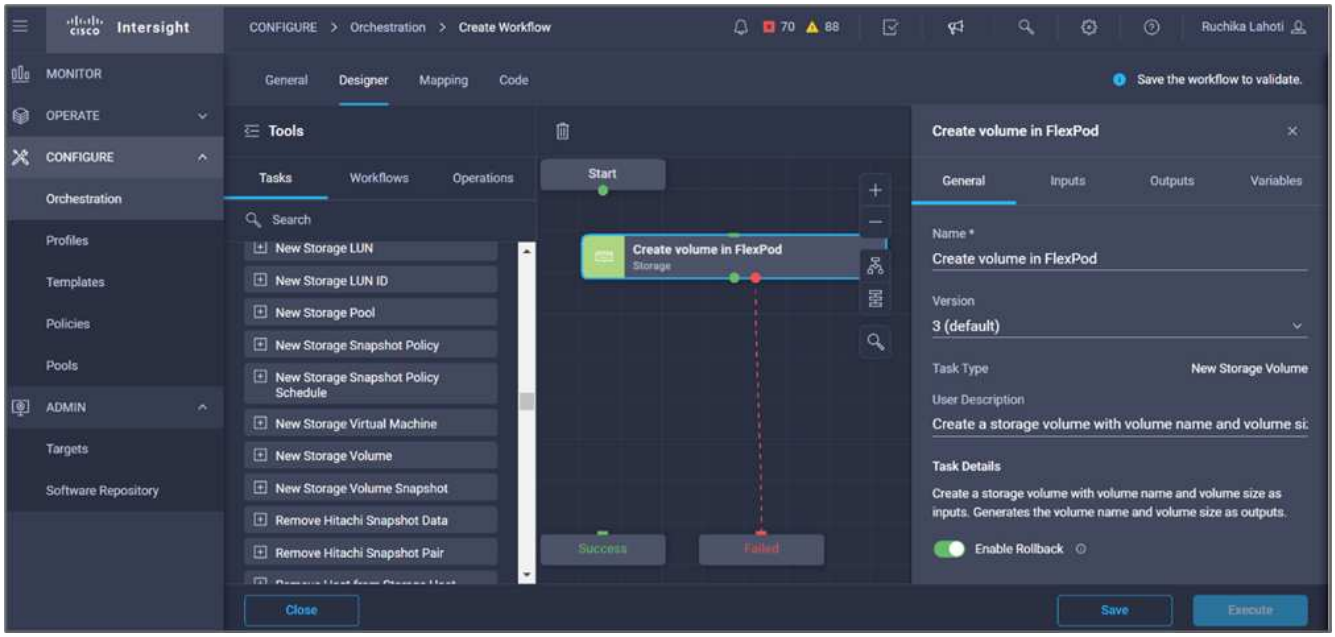


Verfahren 2. Erstellen Sie in FlexPod ein neues Volume

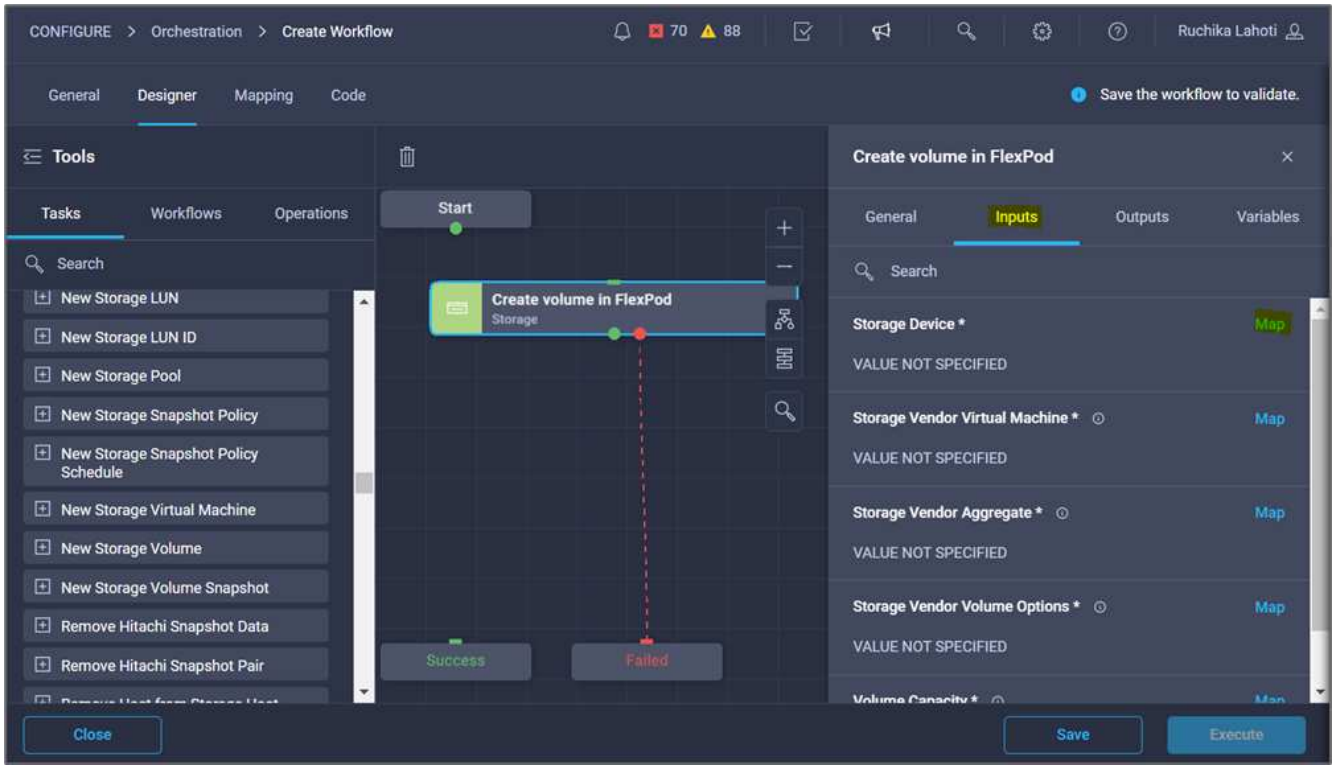
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Storage > New Storage Volume** aus dem Abschnitt **Tools** in den Bereich **Design**.
3. Klicken Sie Auf **Neues Speichervolume**.



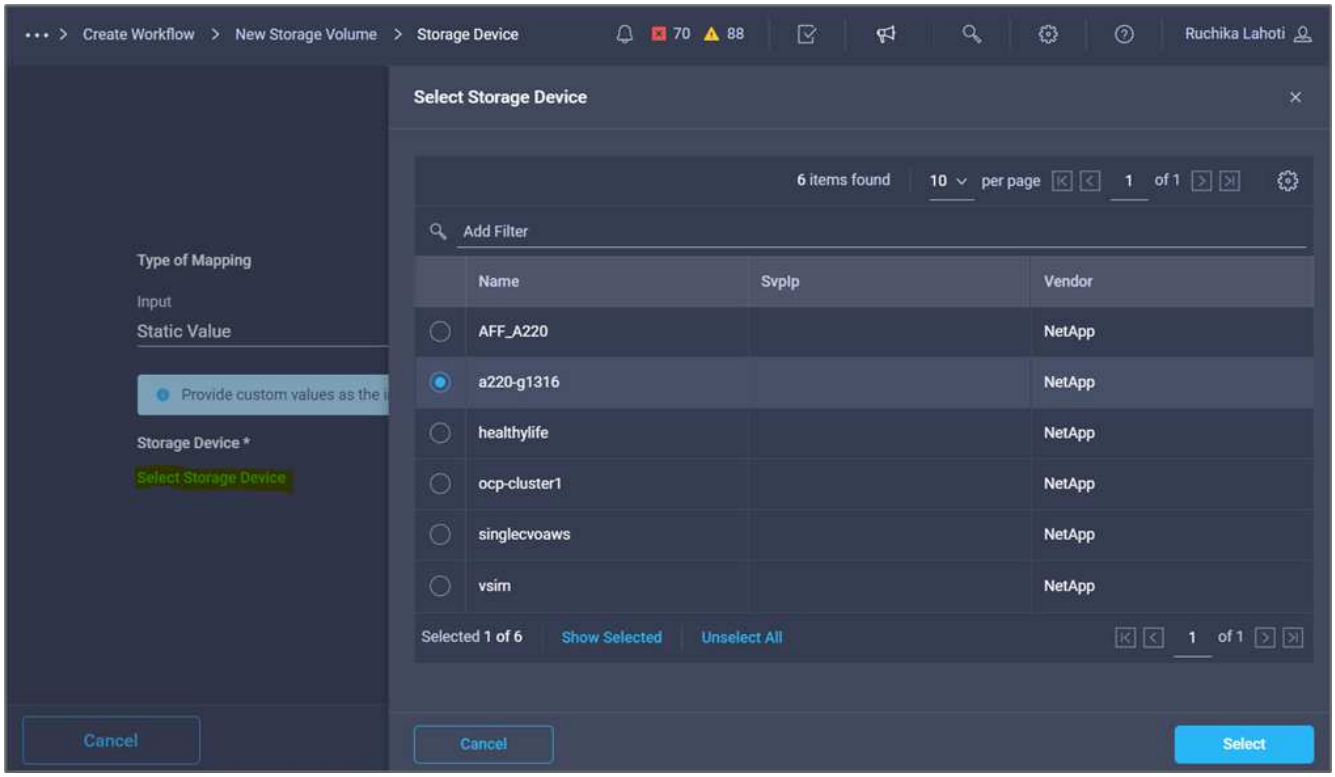
4. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe **Volumen in FlexPod erstellen**.



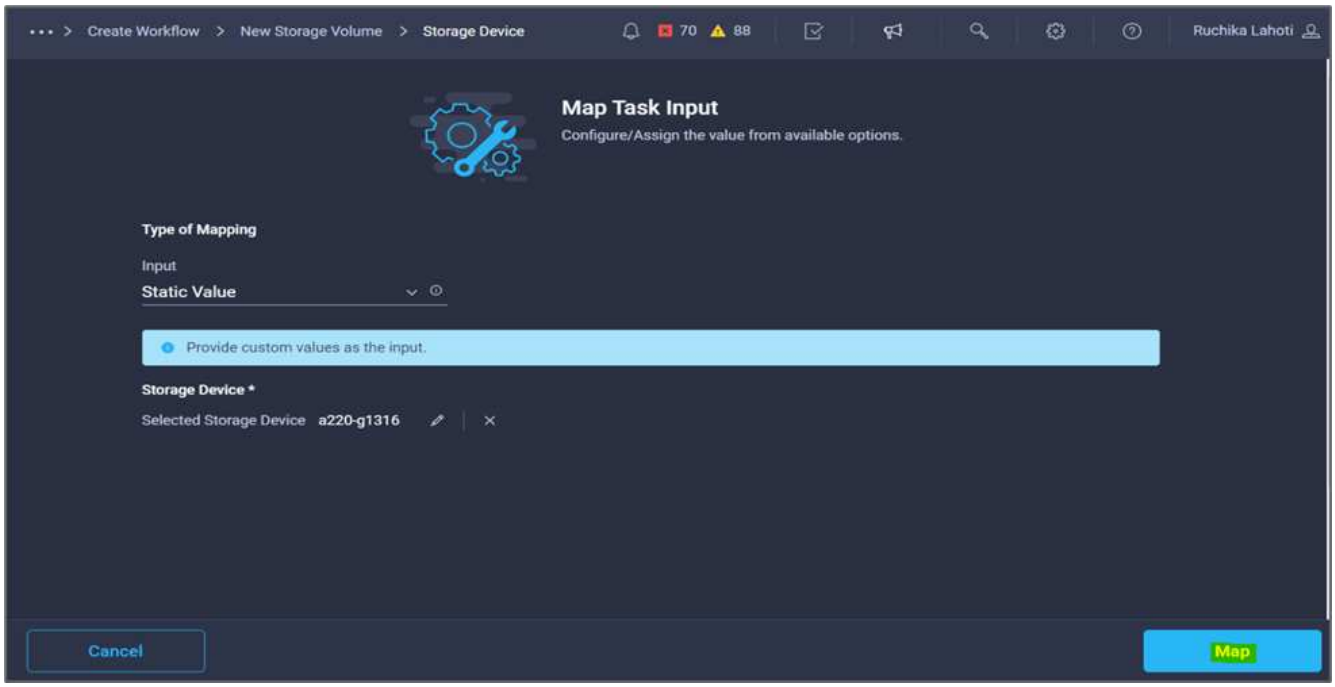
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Speichergerät** auf **Karte**.



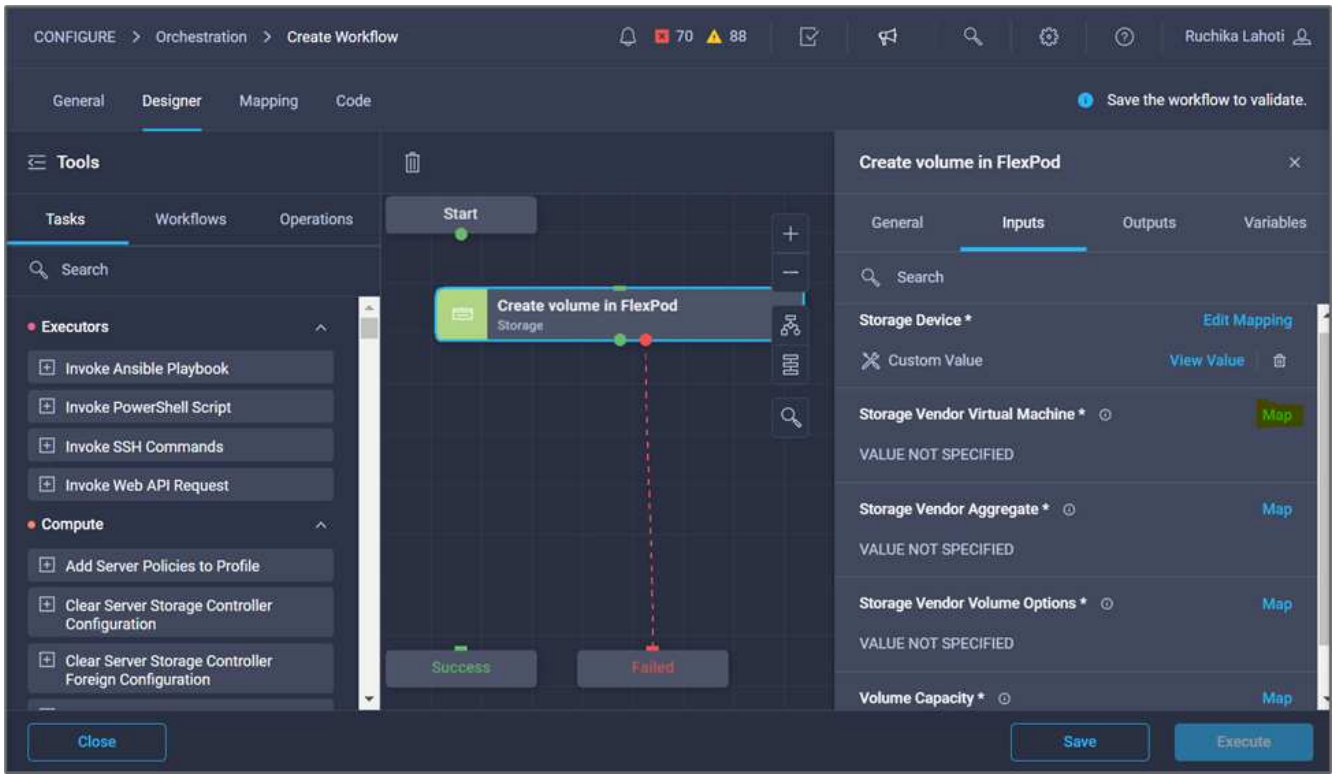
7. Wählen Sie **statischer Wert** und klicken Sie auf **Speichergerät auswählen**.
8. Klicken Sie auf das hinzugefügte Speicherziel und klicken Sie auf **Auswählen**.



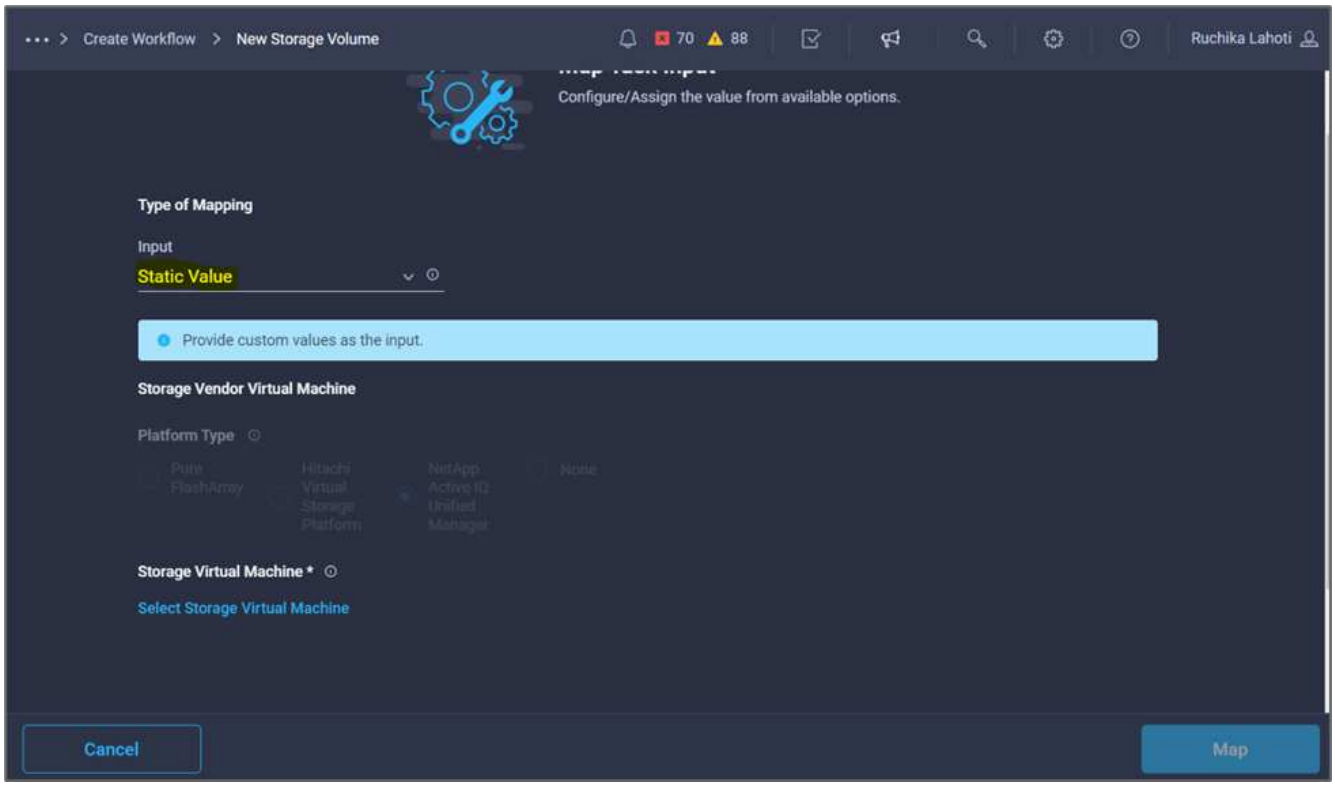
9. Klicken Sie Auf **Karte**.



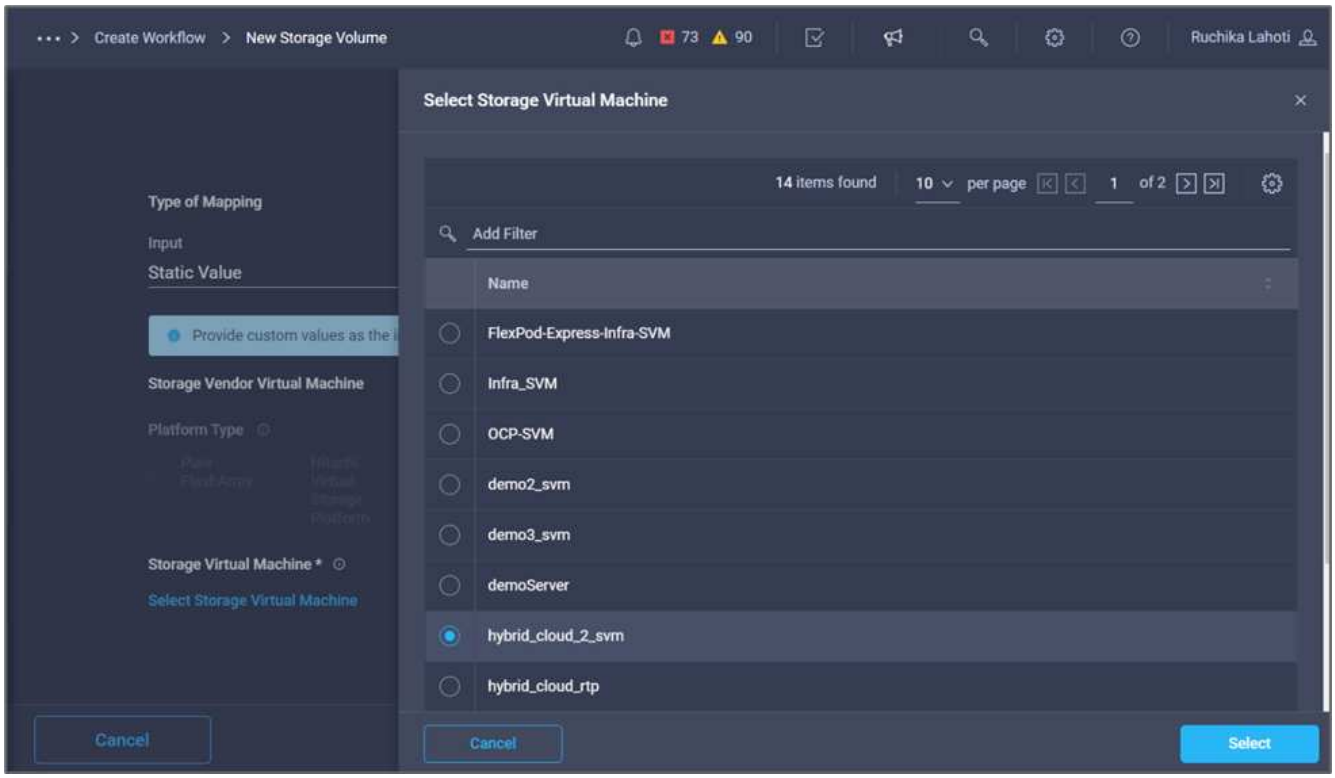
10. Klicken Sie im Feld **Storage Vendor Virtual Machine** auf **Map**.



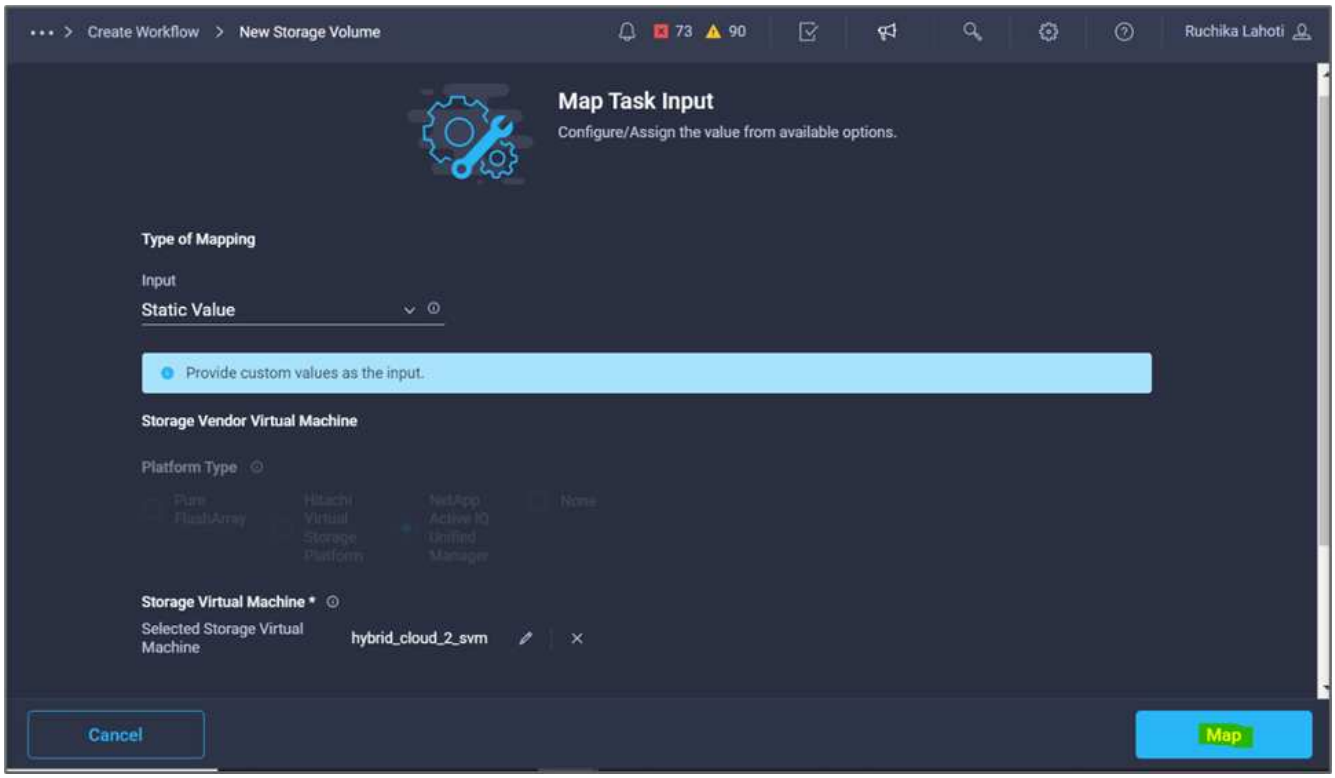
11. Wählen Sie **statischer Wert** und klicken Sie auf **Storage Virtual Machine auswählen**.



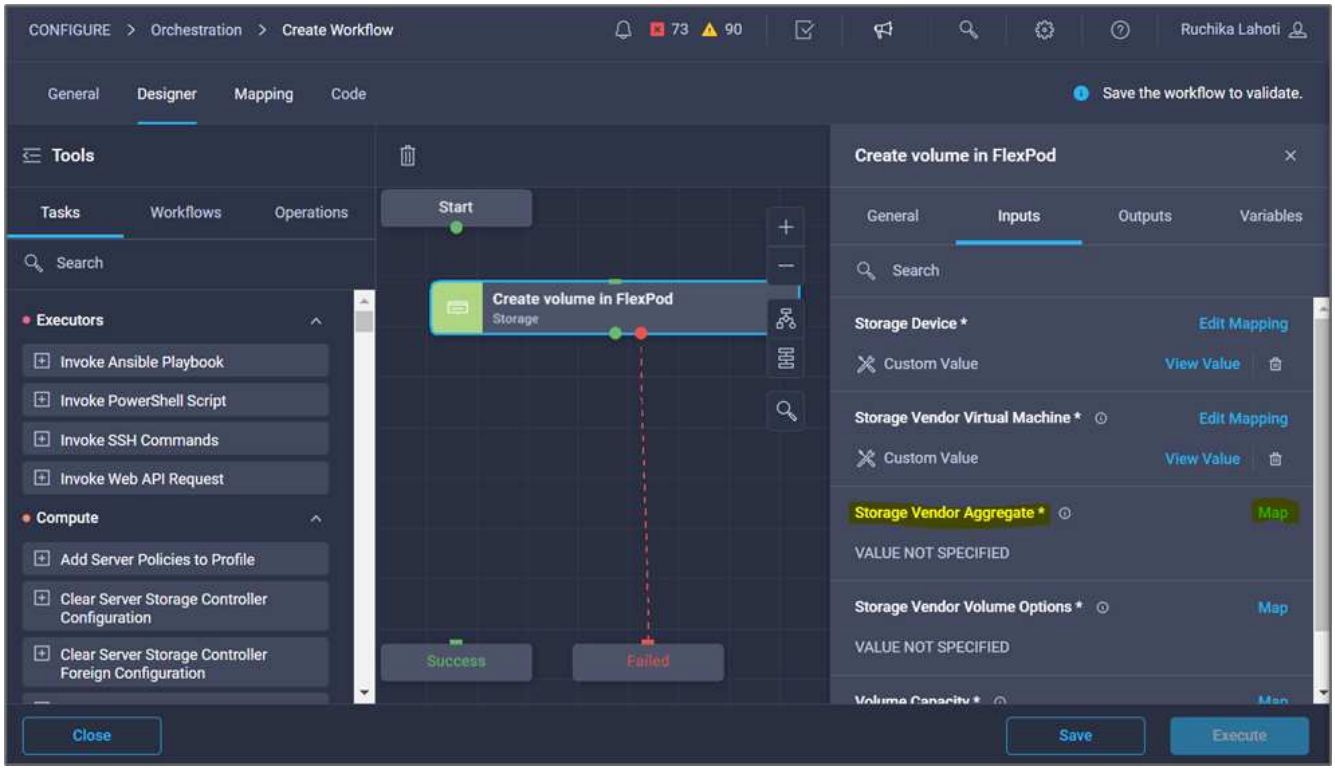
12. Wählen Sie die virtuelle Speichermaschine aus, auf der das Volume erstellt werden soll, und klicken Sie auf **Auswählen**.



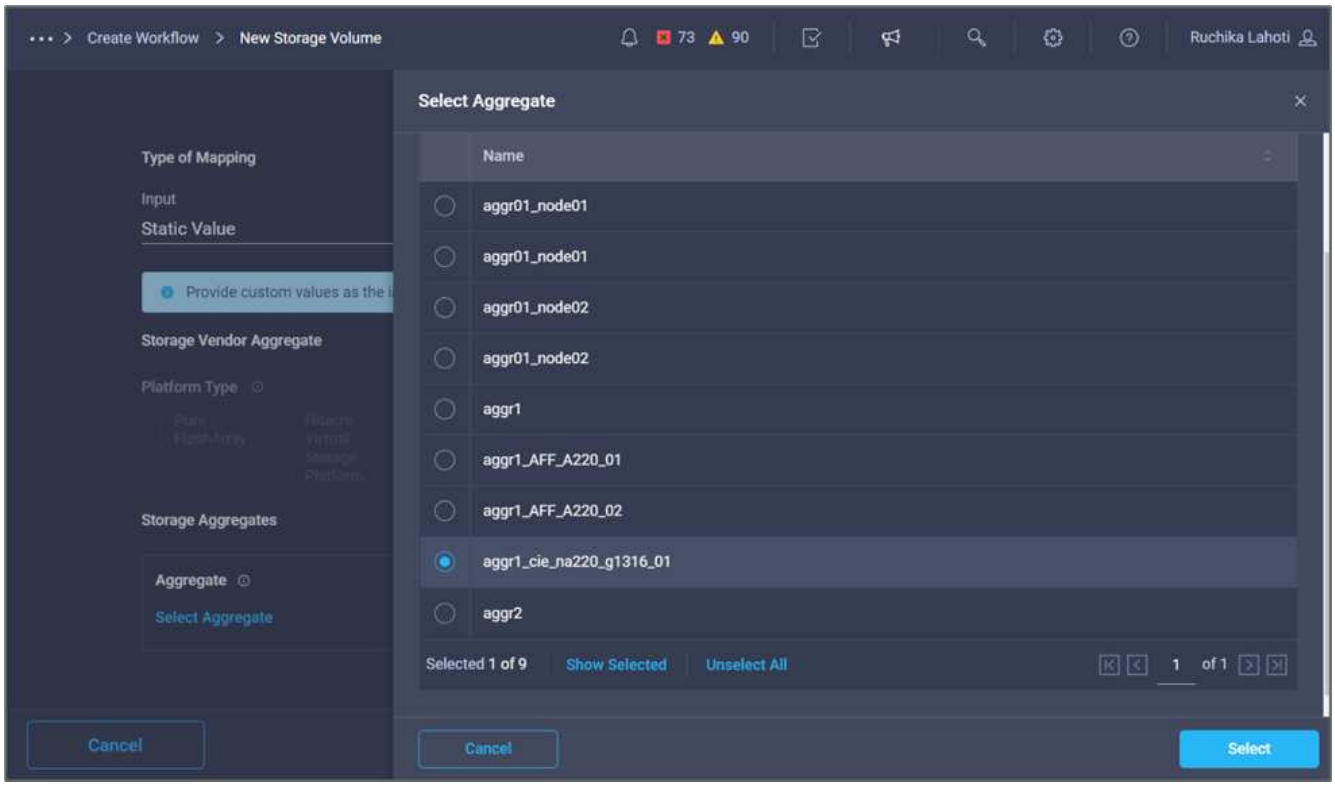
13. Klicken Sie Auf **Karte**.



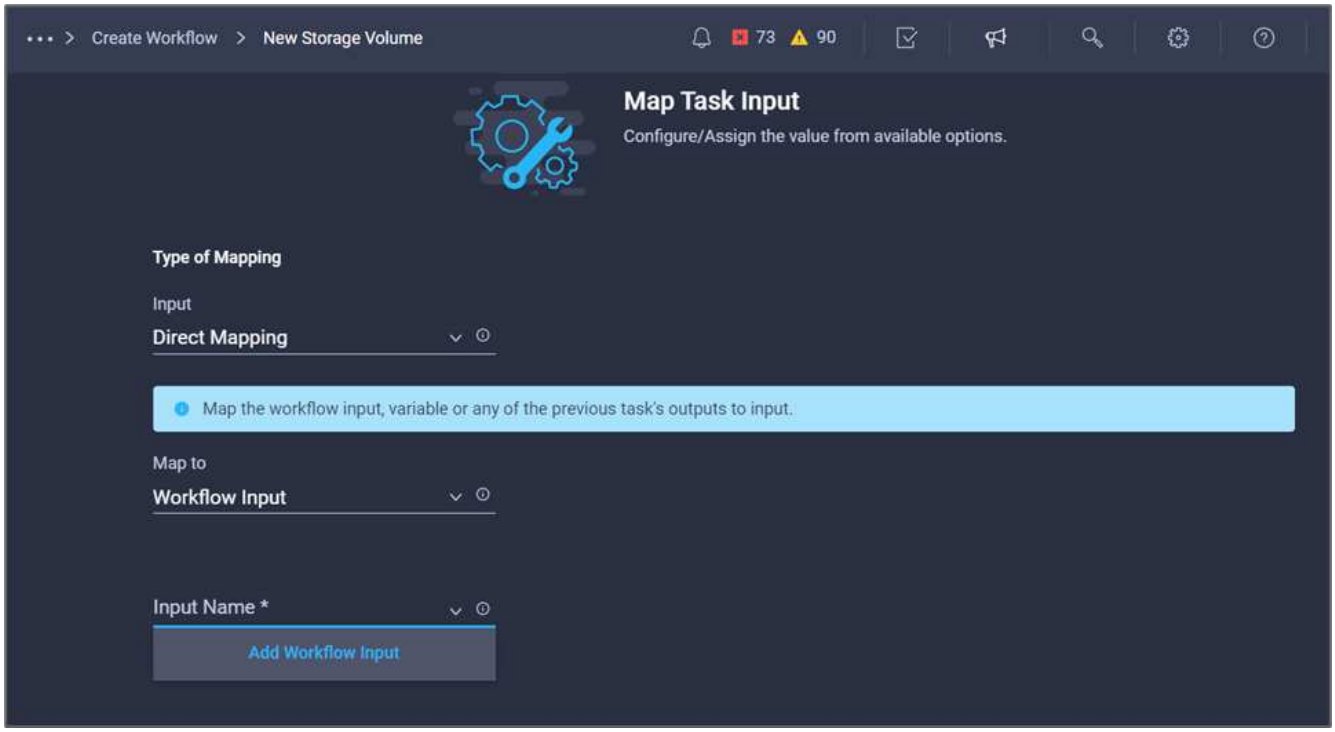
14. Klicken Sie im Feld **Storage Vendor Aggregate** auf **Map**.



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**.

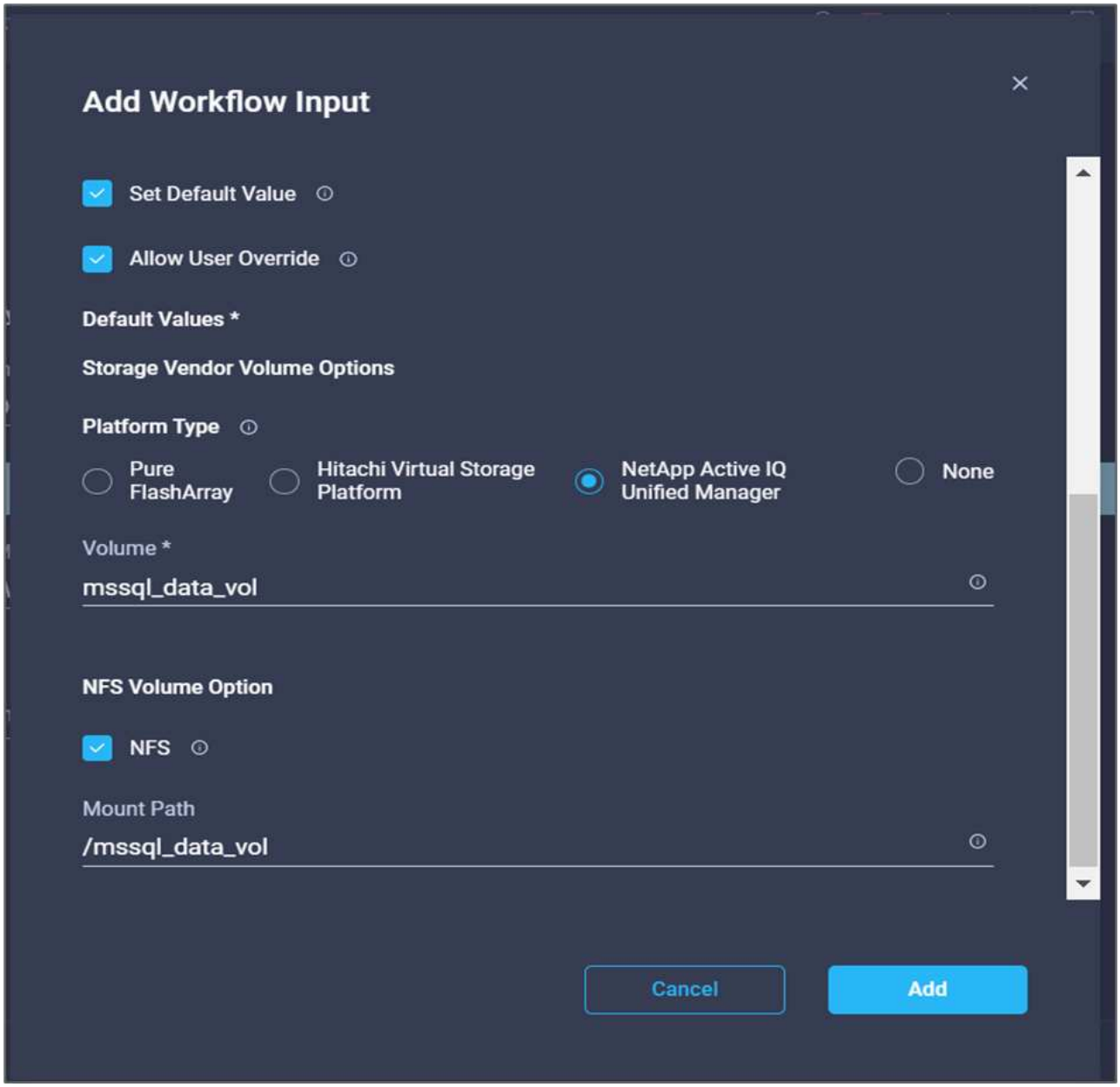
d. Klicken Sie Auf * Erforderlich*.

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

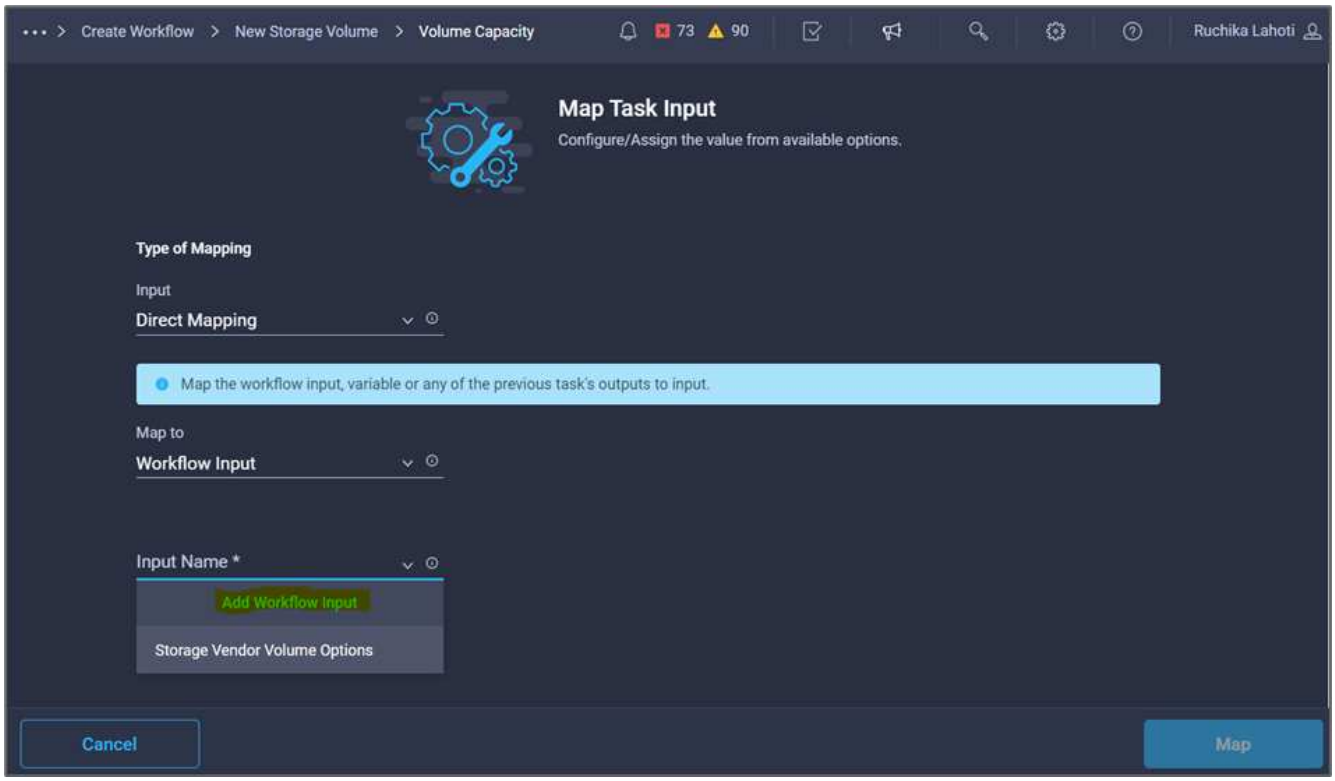
f. Geben Sie einen Standardwert für das erstellte Volume unter **Volume** an.

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.

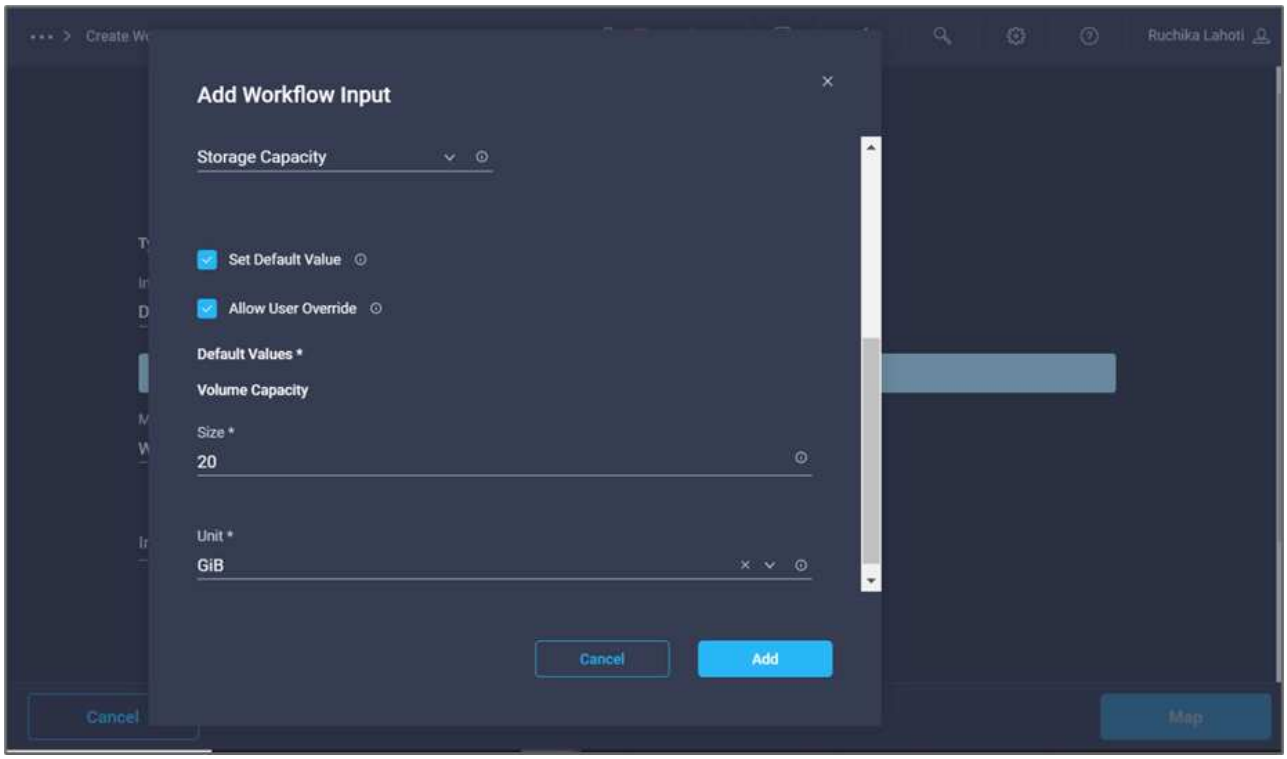
h. Geben Sie einen Mount-Pfad an und klicken Sie auf **Hinzufügen**.



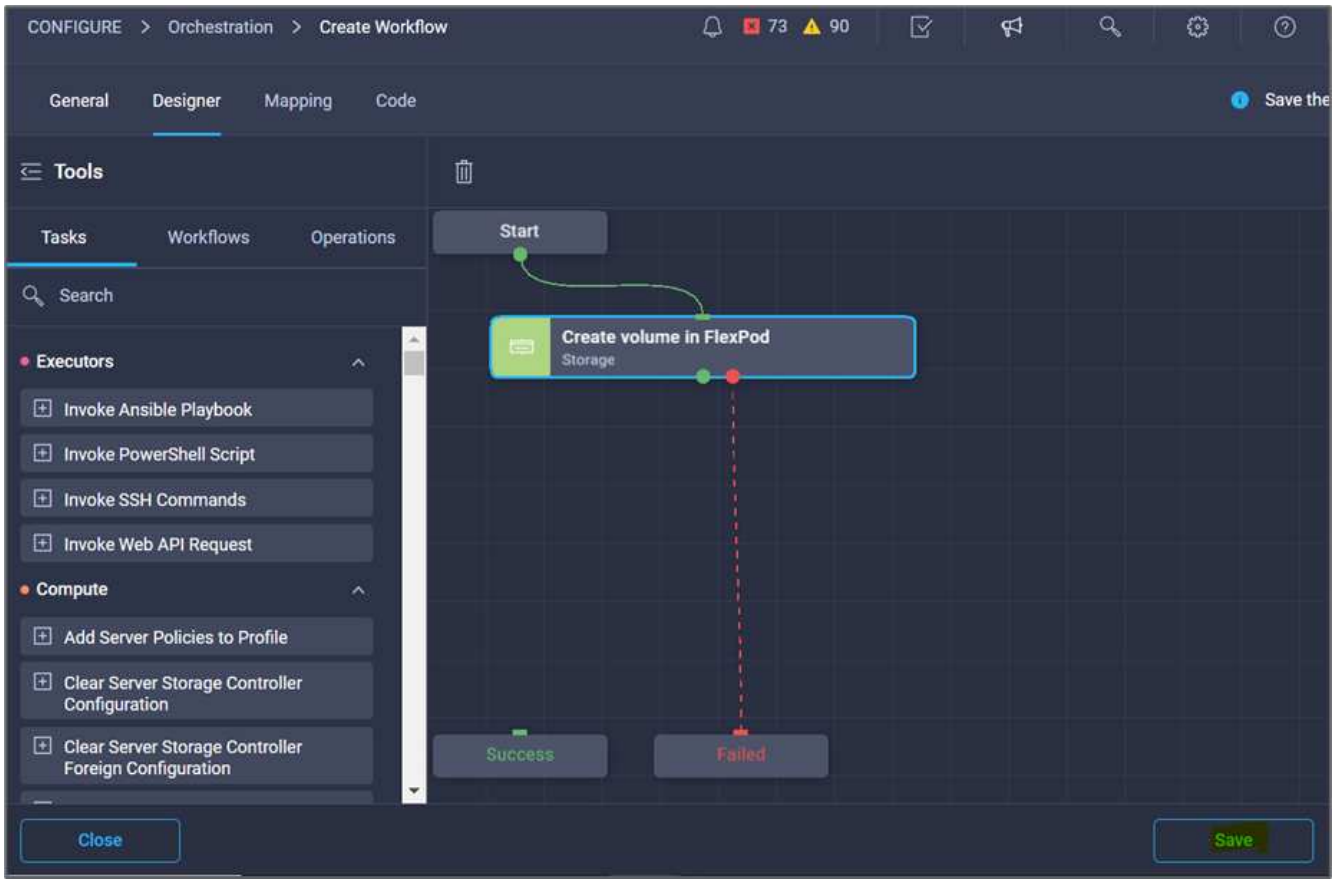
20. Klicken Sie Auf **Karte**.
21. Klicken Sie im Feld **Volume Capacity** auf **Map**.
22. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
23. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



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**.



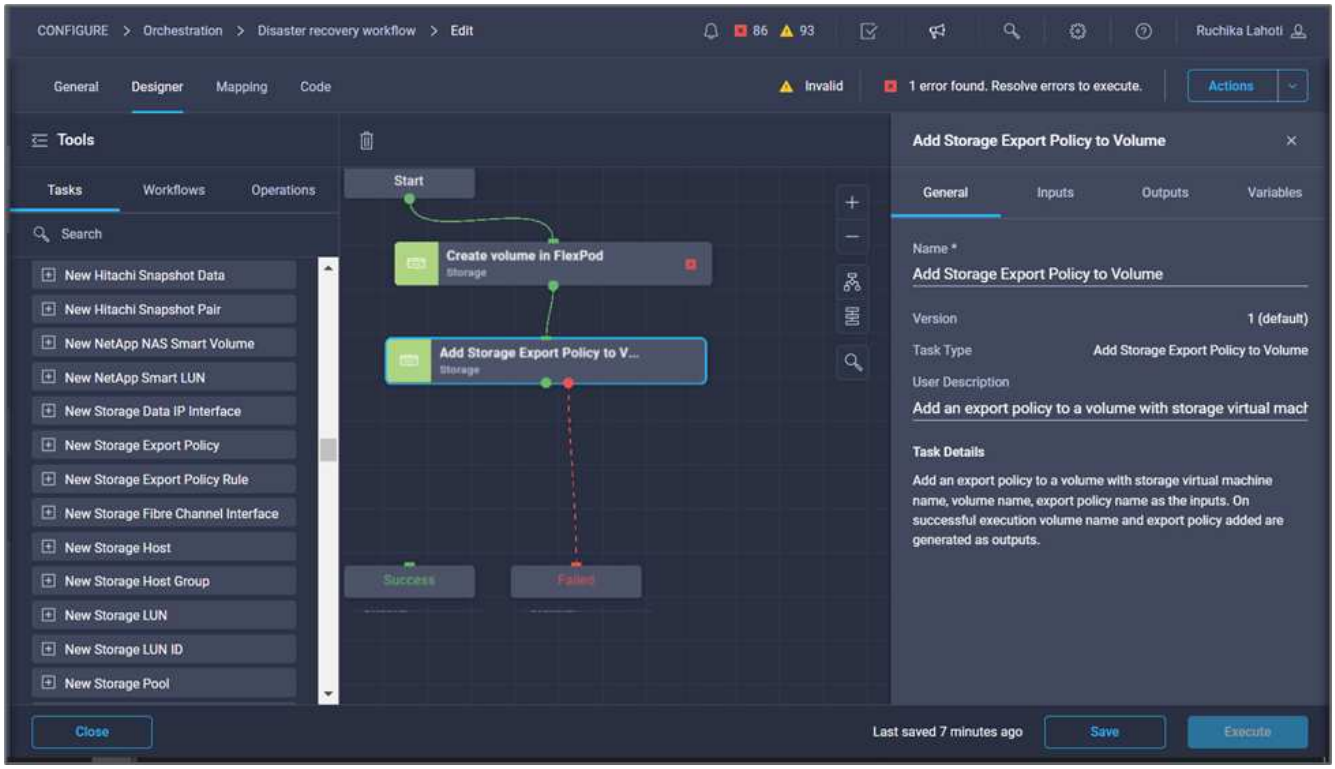
25. Klicken Sie Auf **Karte**.
26. Erstellen Sie mit Connector eine Verbindung zwischen den Aufgaben **Start** und **Lautstärke in FlexPod** erstellen, und klicken Sie auf **Speichern**.



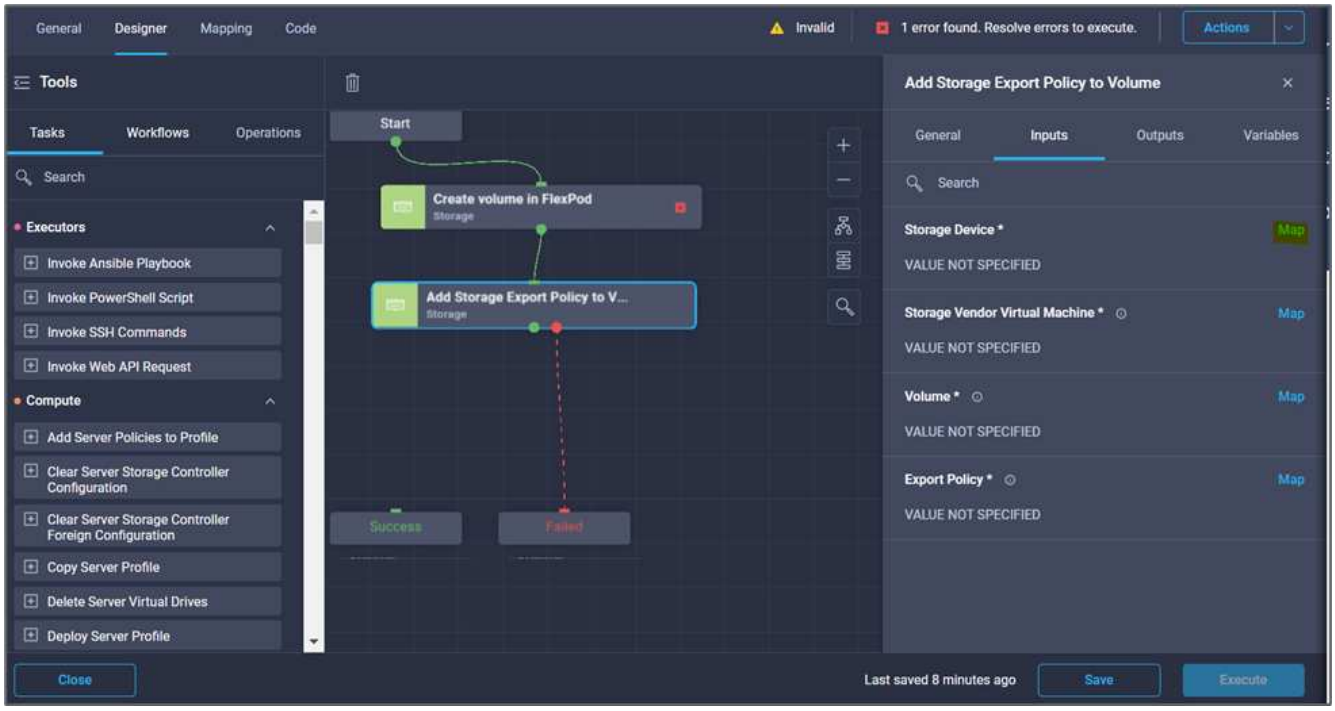
Ignorieren Sie den Fehler jetzt. Dieser Fehler wird angezeigt, weil es keine Verbindung zwischen den Tasks **Create Volume in FlexPod** und **success** gibt, die erforderlich ist, um den erfolgreichen Übergang festzulegen.

Verfahren 3: Add Storage Export Policy

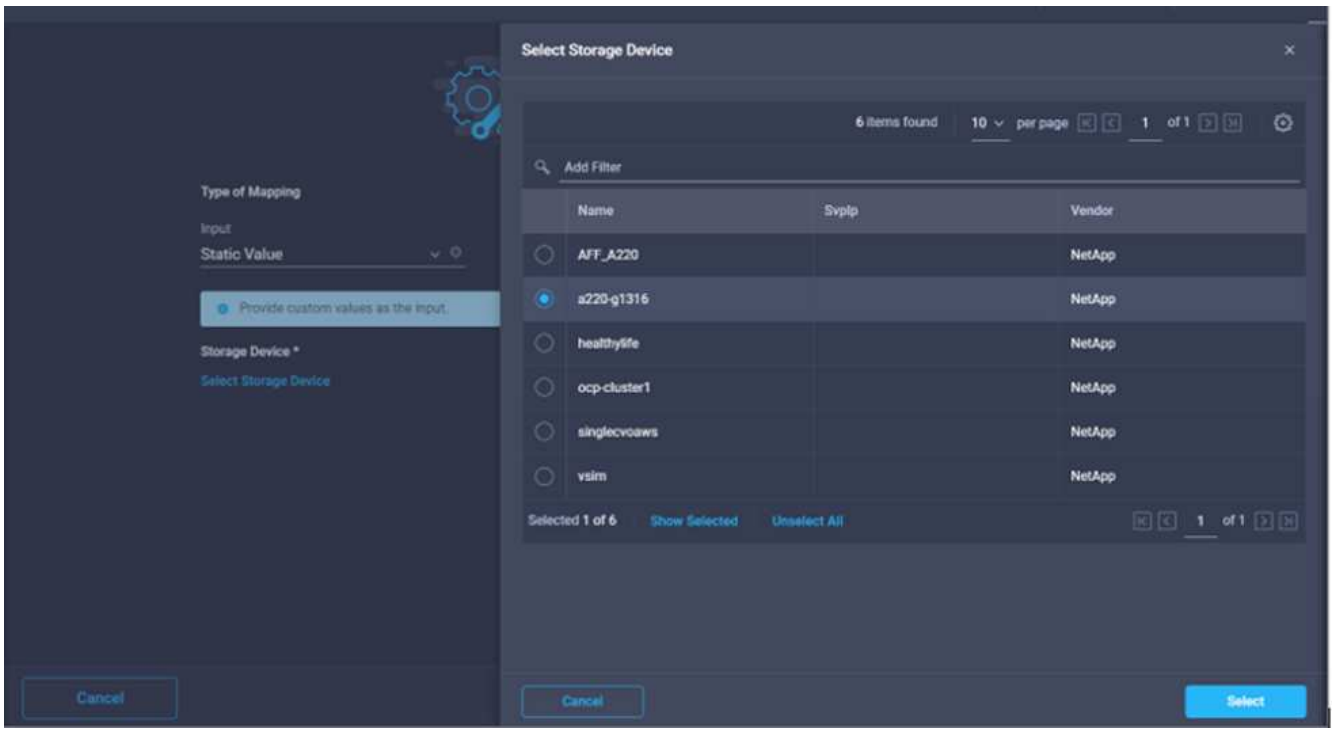
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Speicherung > Speicherexport Policy in Volume** hinzufügen aus dem Abschnitt **Tools** im Bereich **Design**.
3. Klicken Sie auf **Storage Export Policy zum Volume hinzufügen**. 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**.



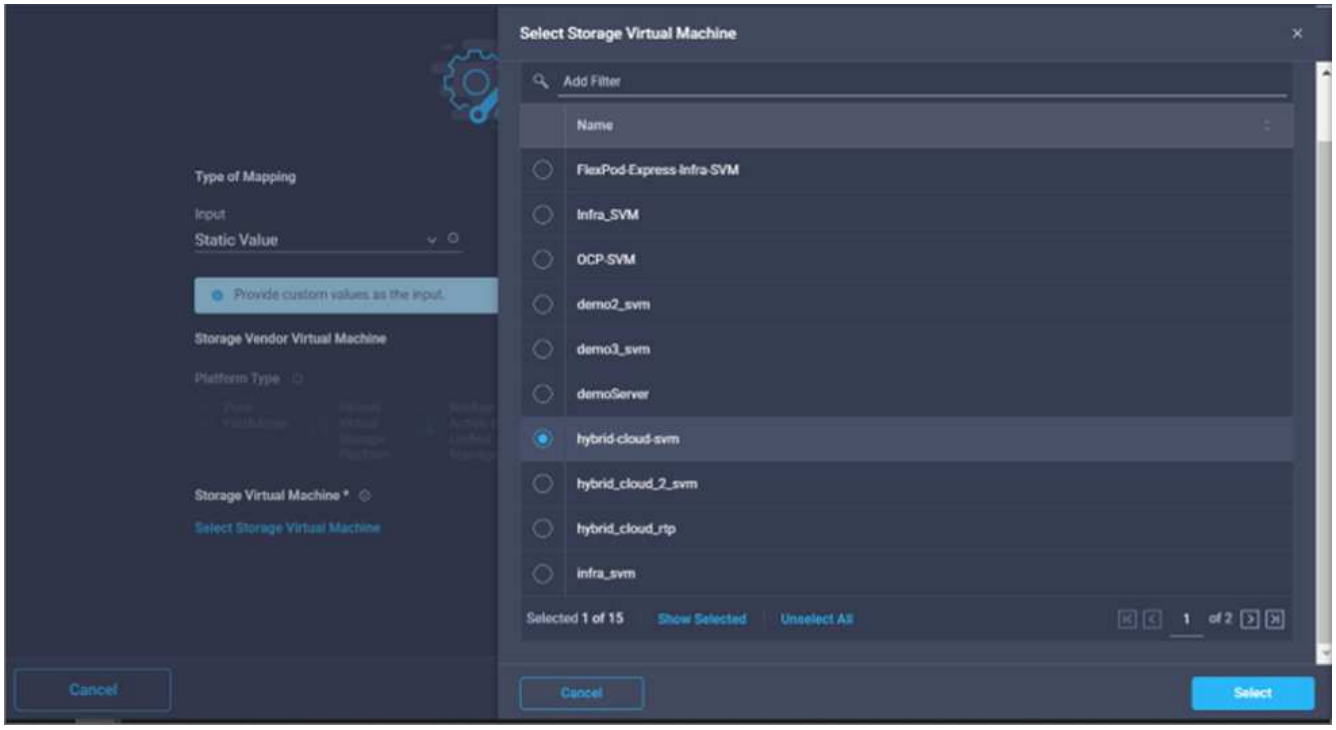
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Speichergerät** auf **Karte**.



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**.

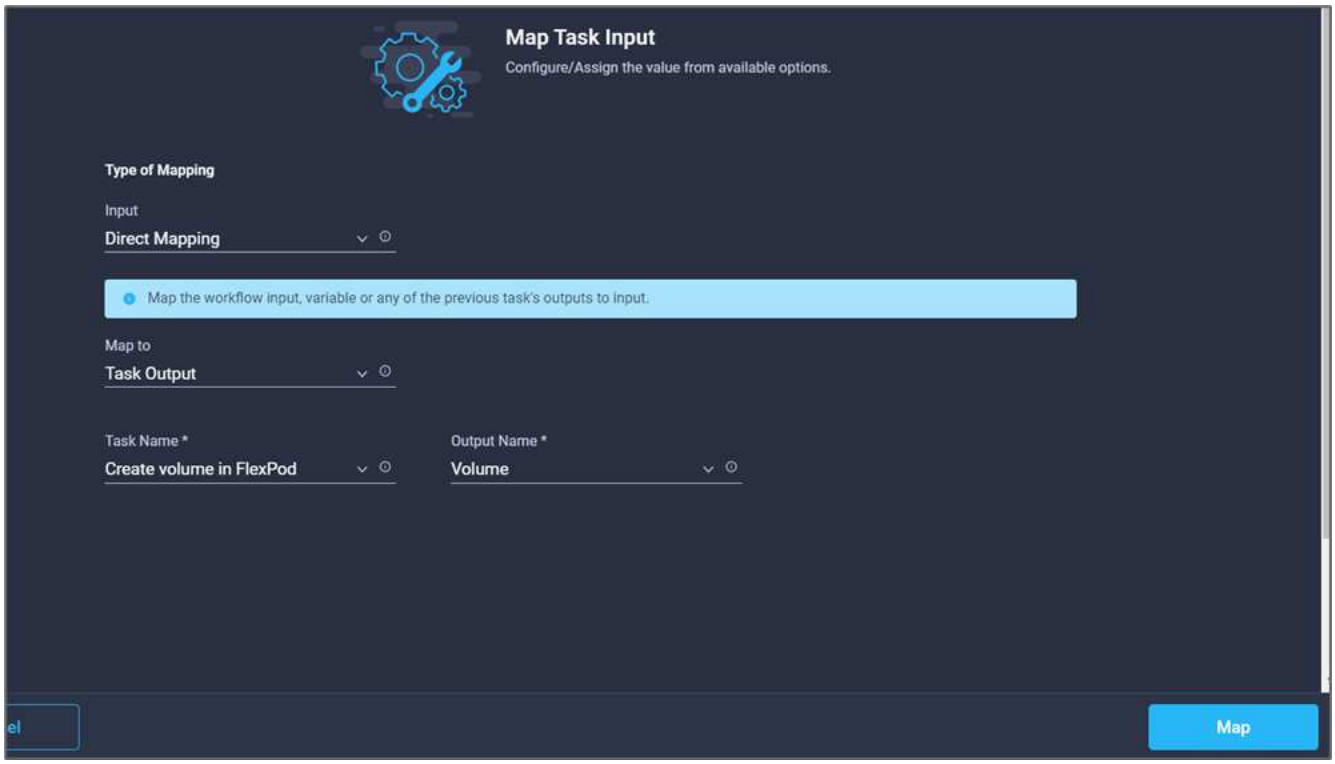


9. Klicken Sie im Feld **Storage Vendor Virtual Machine** auf **Map**.
10. Wählen Sie **statischer Wert** und klicken Sie auf **Storage Virtual Machine auswählen**. Wählen Sie dieselbe virtuelle Speichermaschine aus, die beim Erstellen der vorherigen Aufgabe zur Erstellung eines neuen Speichervolumes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

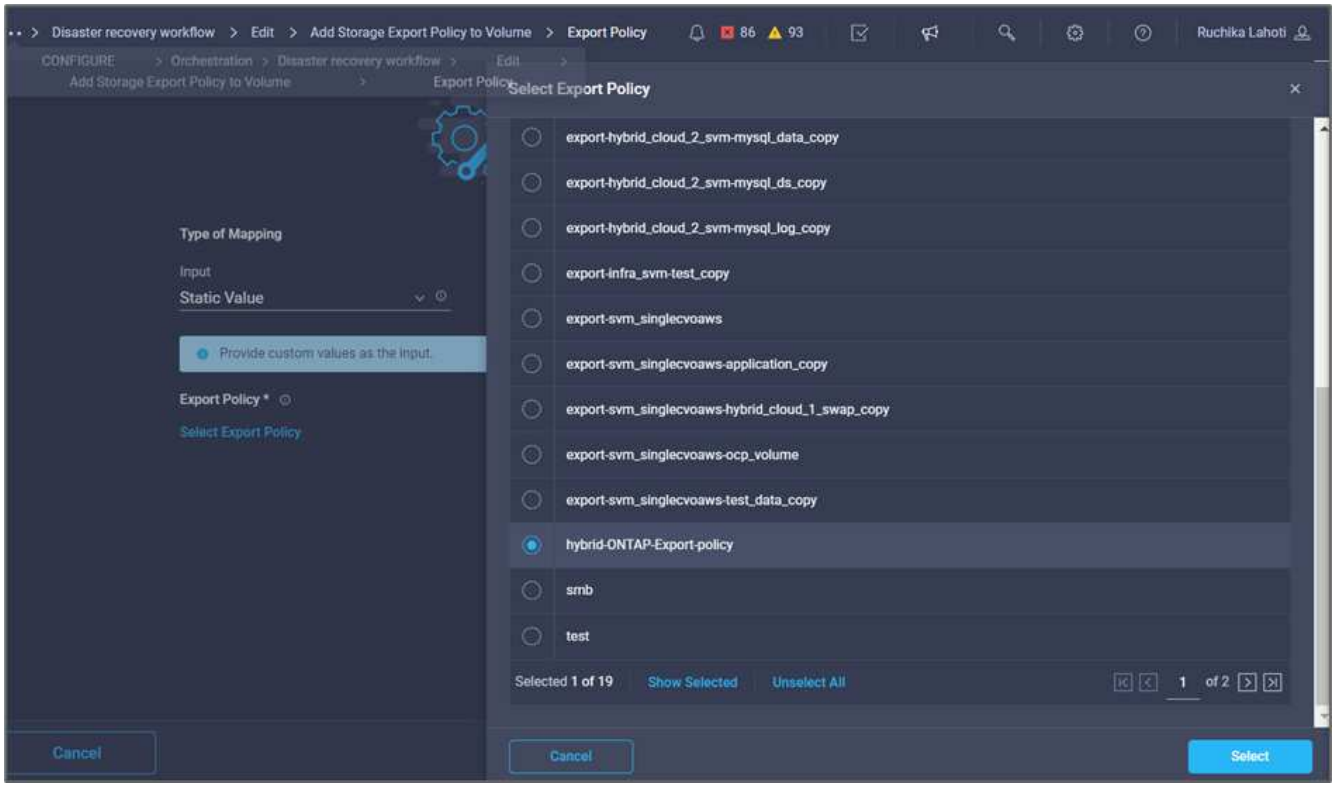


11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld **Volumen** auf **Karte**.
13. Klicken Sie auf **Aufgabenname** und dann auf **Volumen in FlexPod erstellen**. Klicken Sie auf **Ausgabename** und dann auf **Volumen**.

> 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.

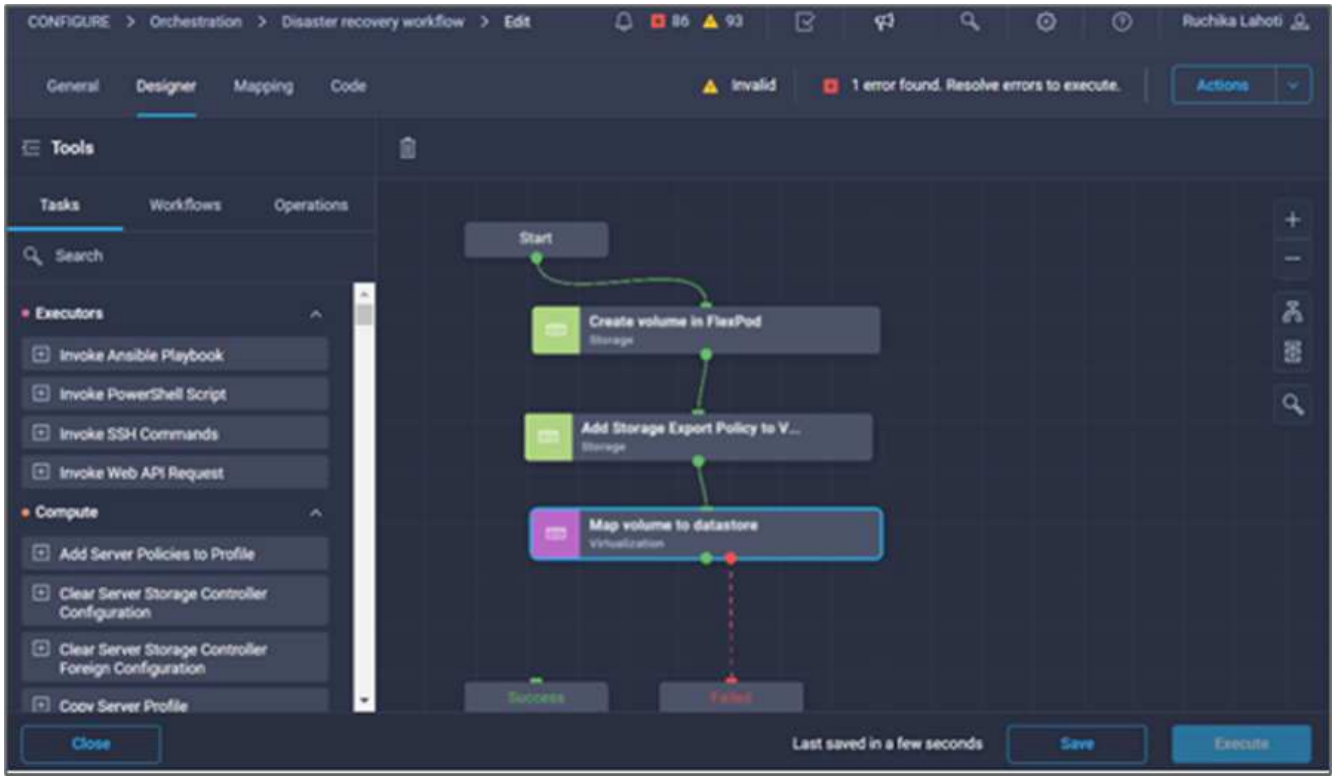


17. Klicken Sie auf **Karte** und dann auf **Speichern**.

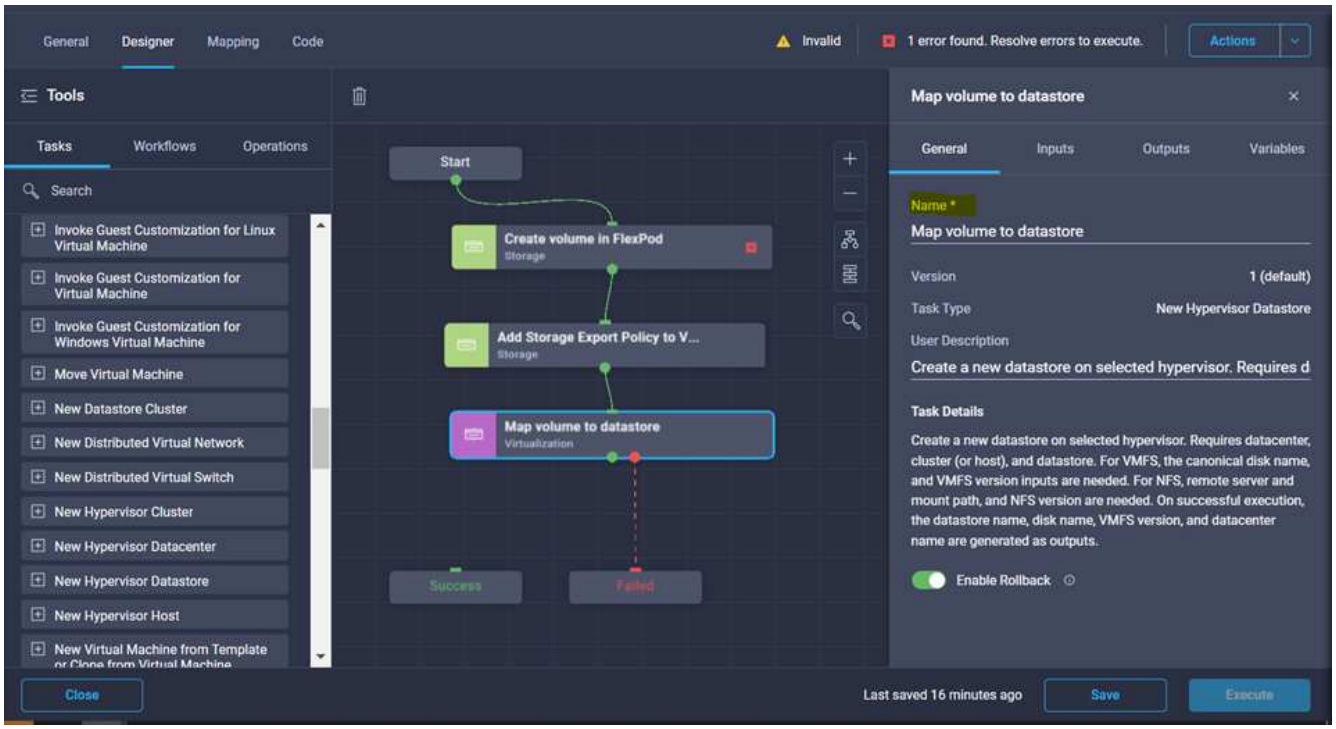
Damit ist das Hinzufügen einer Exportrichtlinie zum Volume abgeschlossen. Als Nächstes erstellen Sie einen neuen Datenspeicher, der das erstellte Volume zugeordnet.

Prozedur 4: FlexPod Volume zu Datastore zuordnen

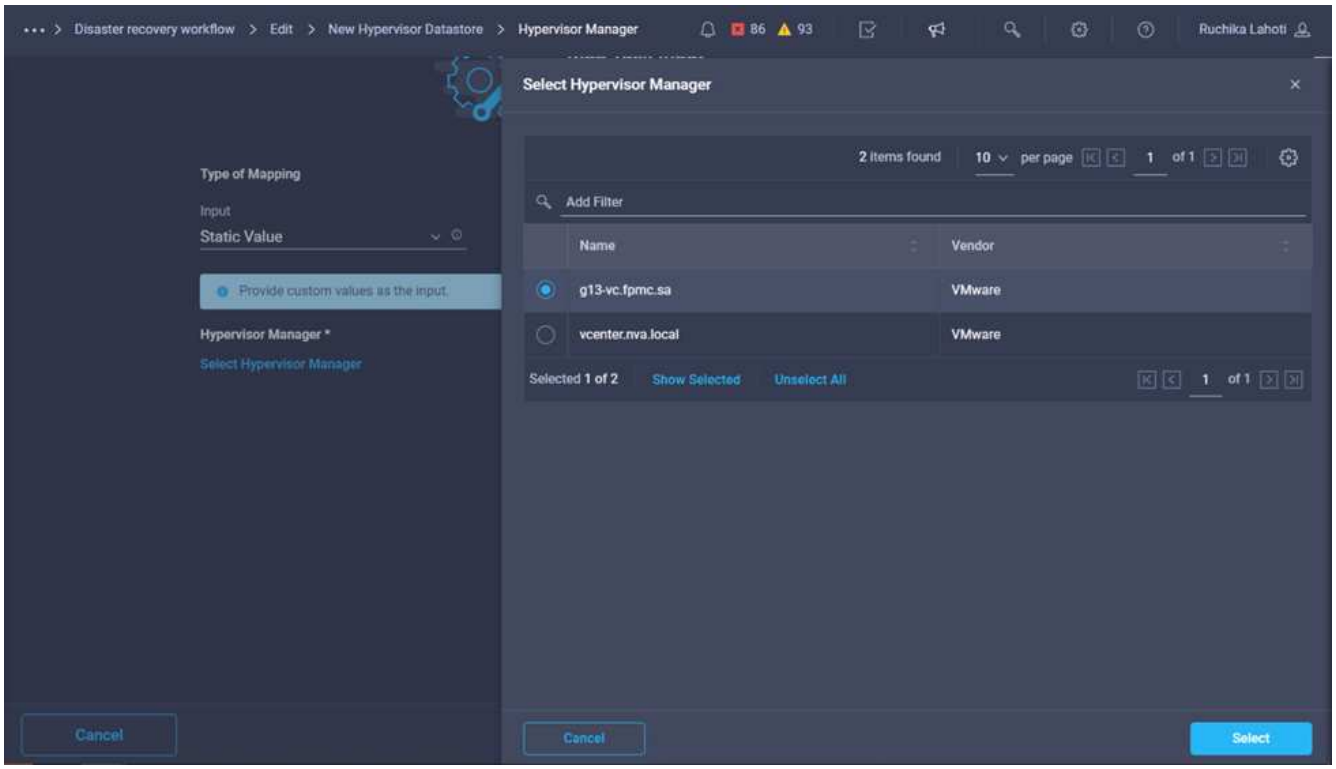
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Virtualisierung > Neuer Hypervisor Datastore** aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie Connector, um eine Verbindung zwischen den Aufgaben **Add Storage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



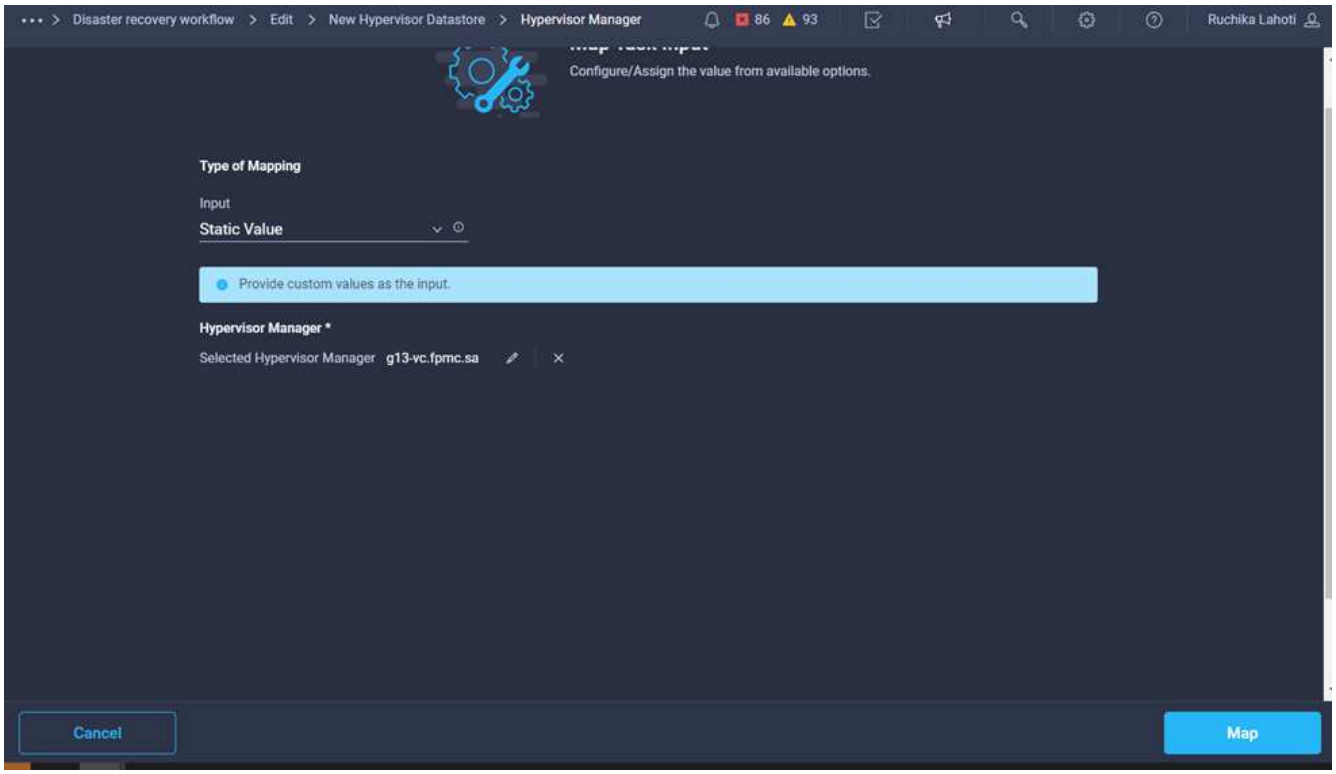
4. Klicken Sie Auf **Neuer Hypervisor Datastore**. Klicken Sie im Bereich **Aufgabeneigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern. In diesem Beispiel lautet der Name der Aufgabe **Datenträger in Datastore** zuordnen.



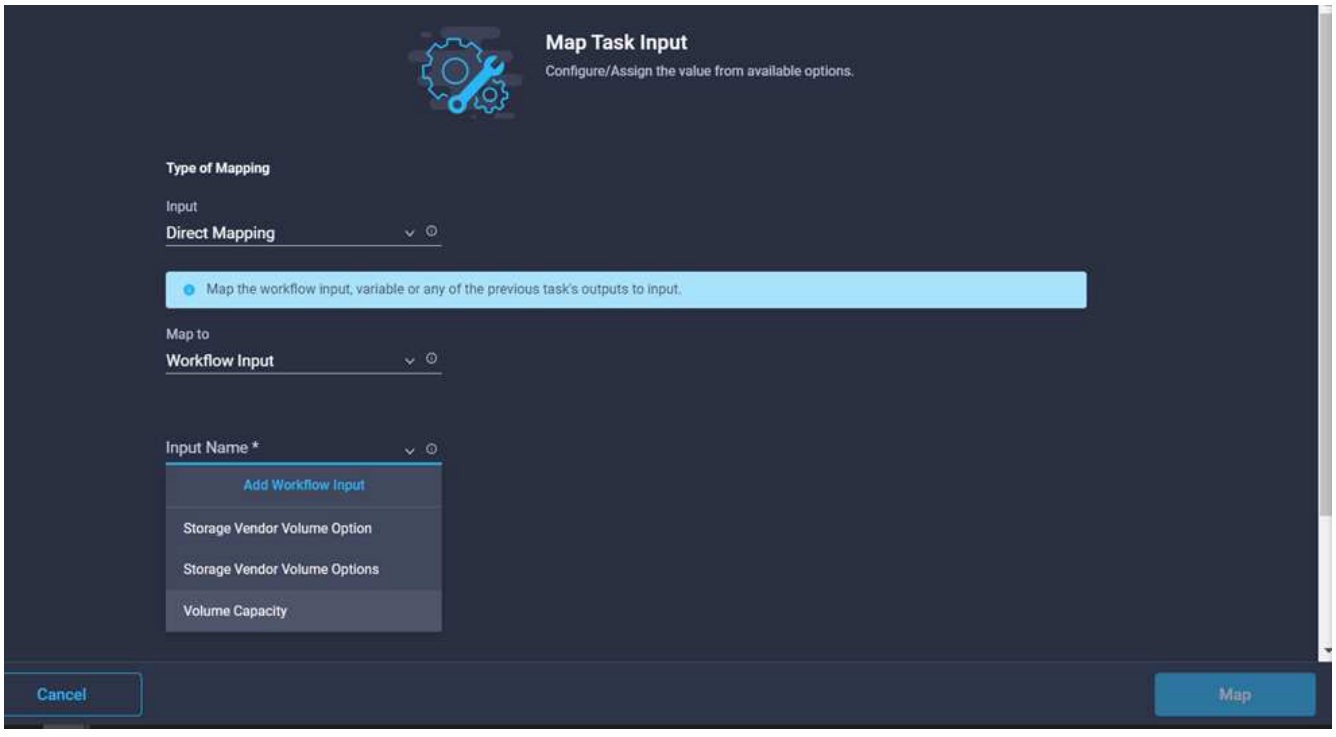
5. Klicken Sie im Bereich **Aufgabeneigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Hypervisor Manager** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Hypervisor Manager auswählen**. Klicken Sie auf das VMware vCenter Ziel.



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**.



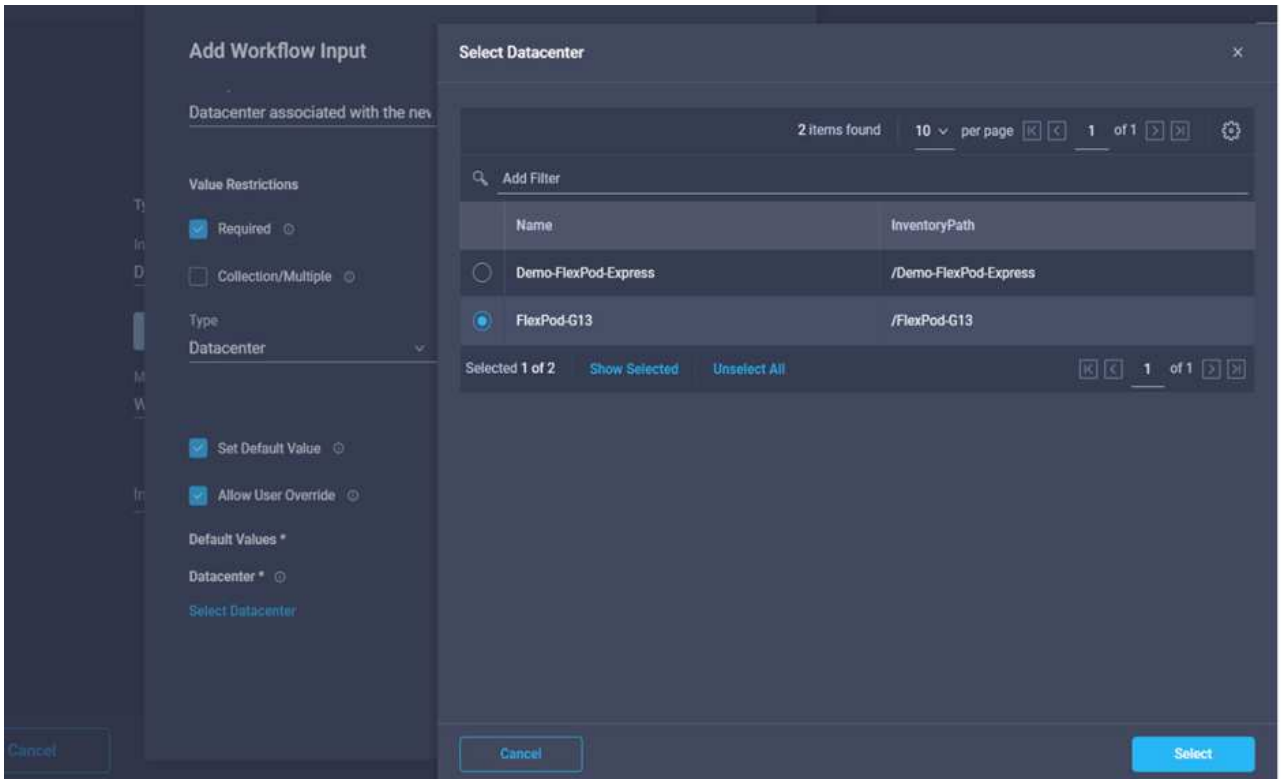
12. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).

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

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

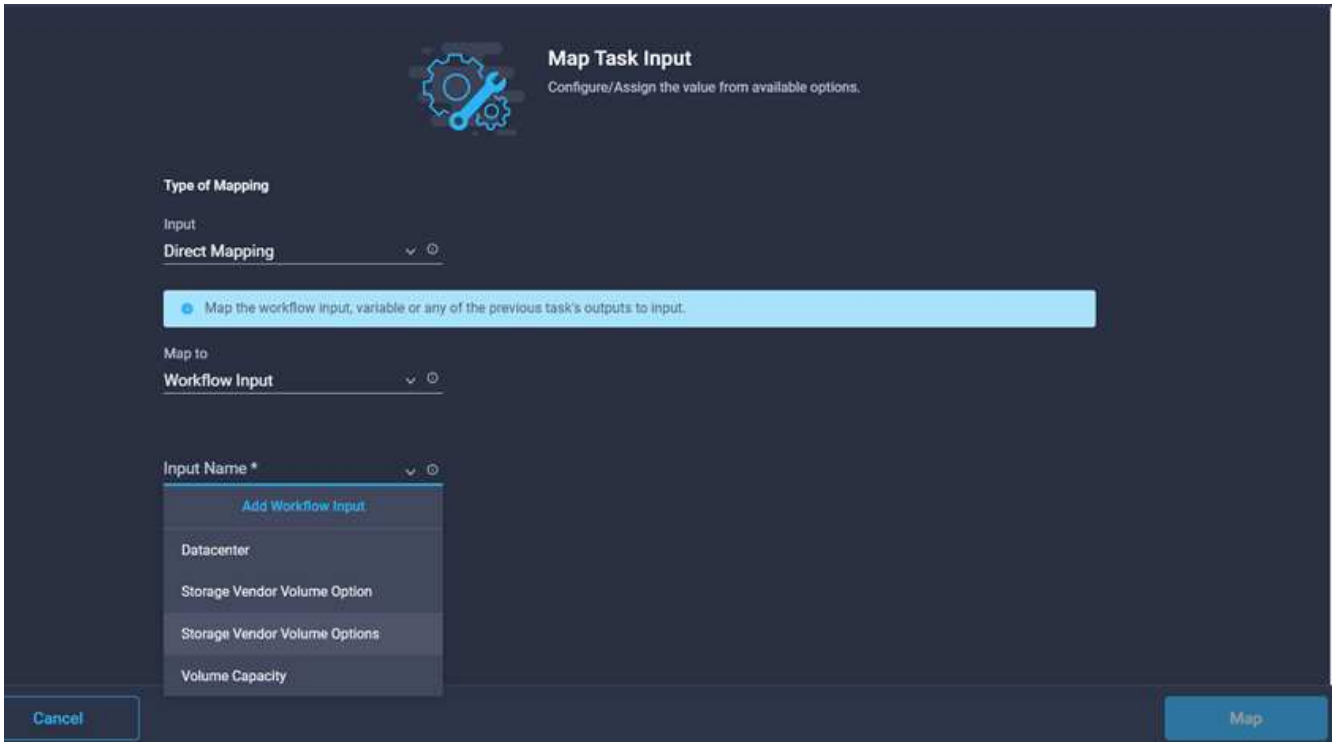
d. Klicken Sie Auf **Datacenter Auswählen**.

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

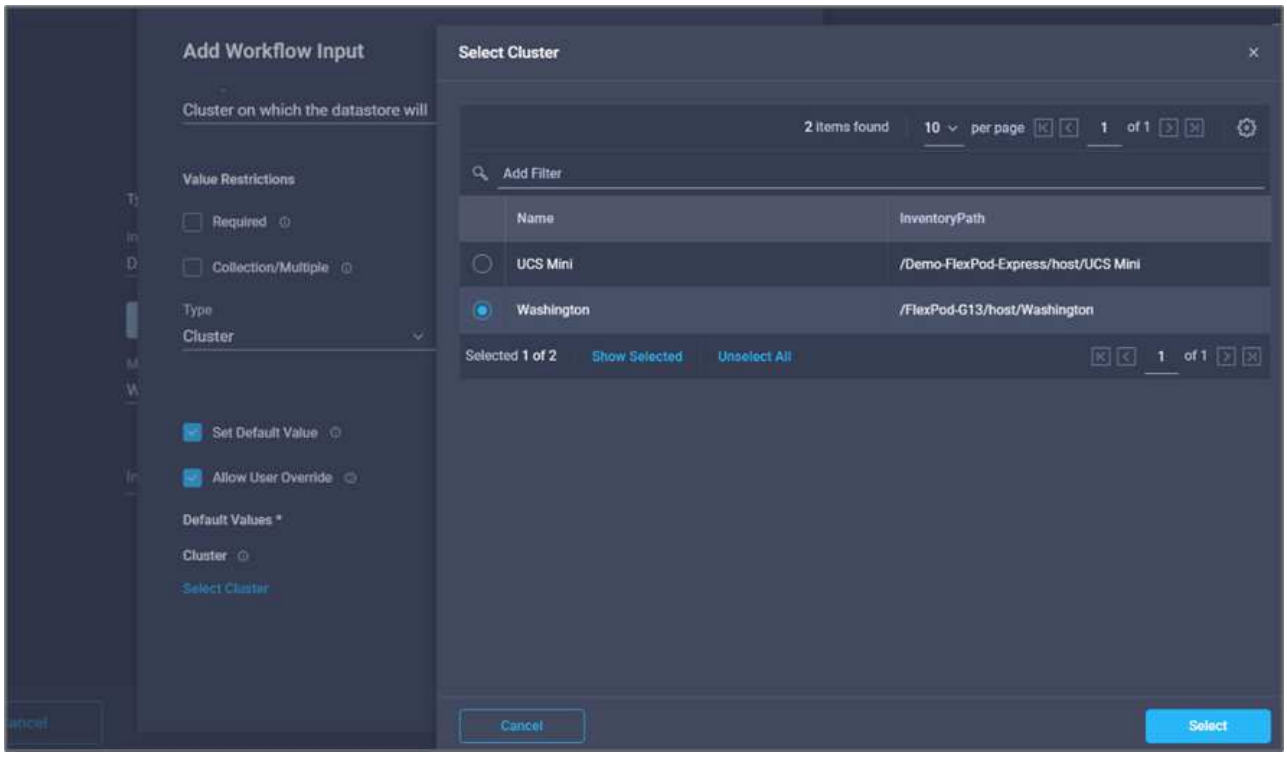


- Klicken Sie Auf **Hinzufügen**.

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

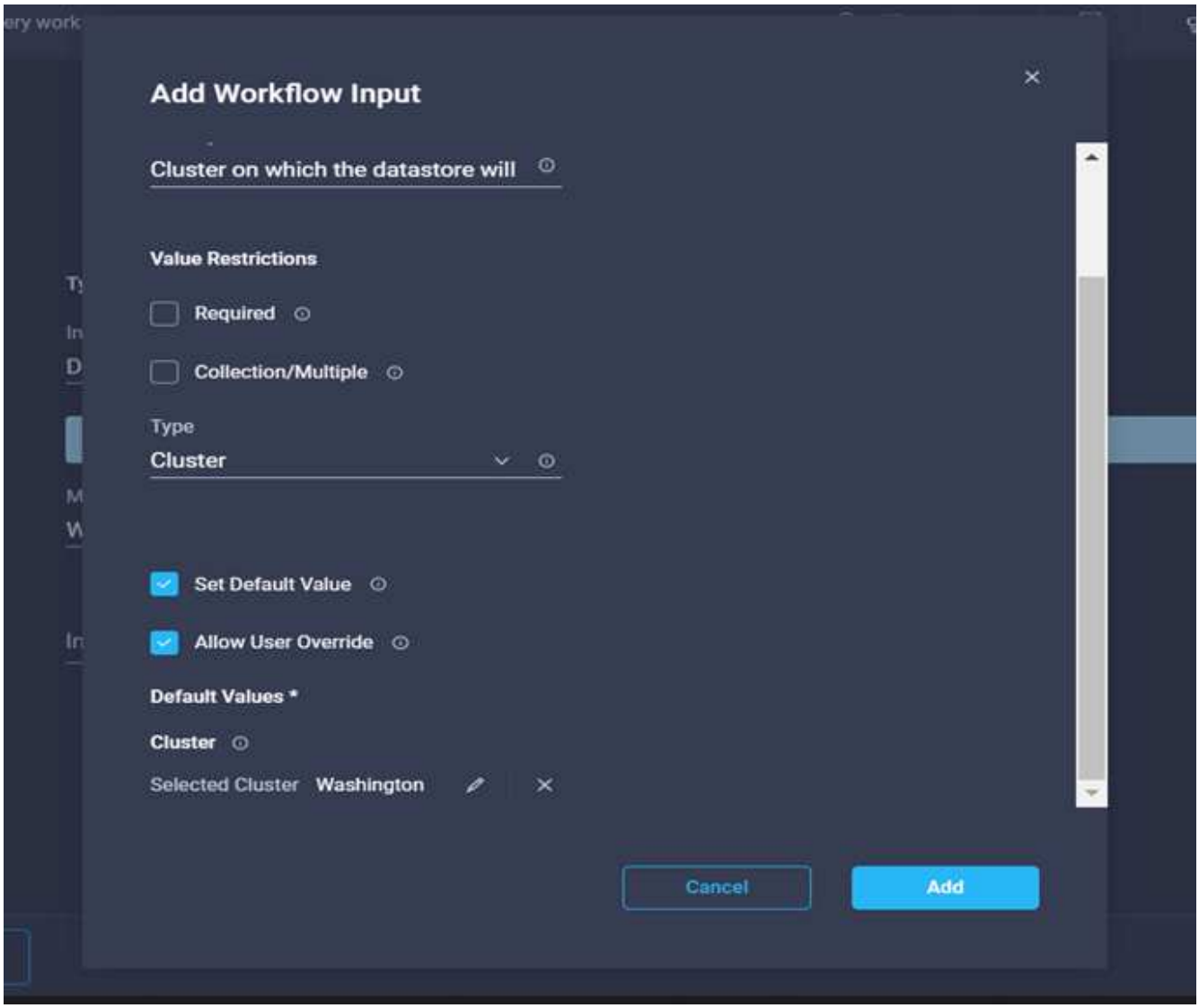


16. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Wählen Sie als Typ Cluster aus.
    d. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    e. Klicken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

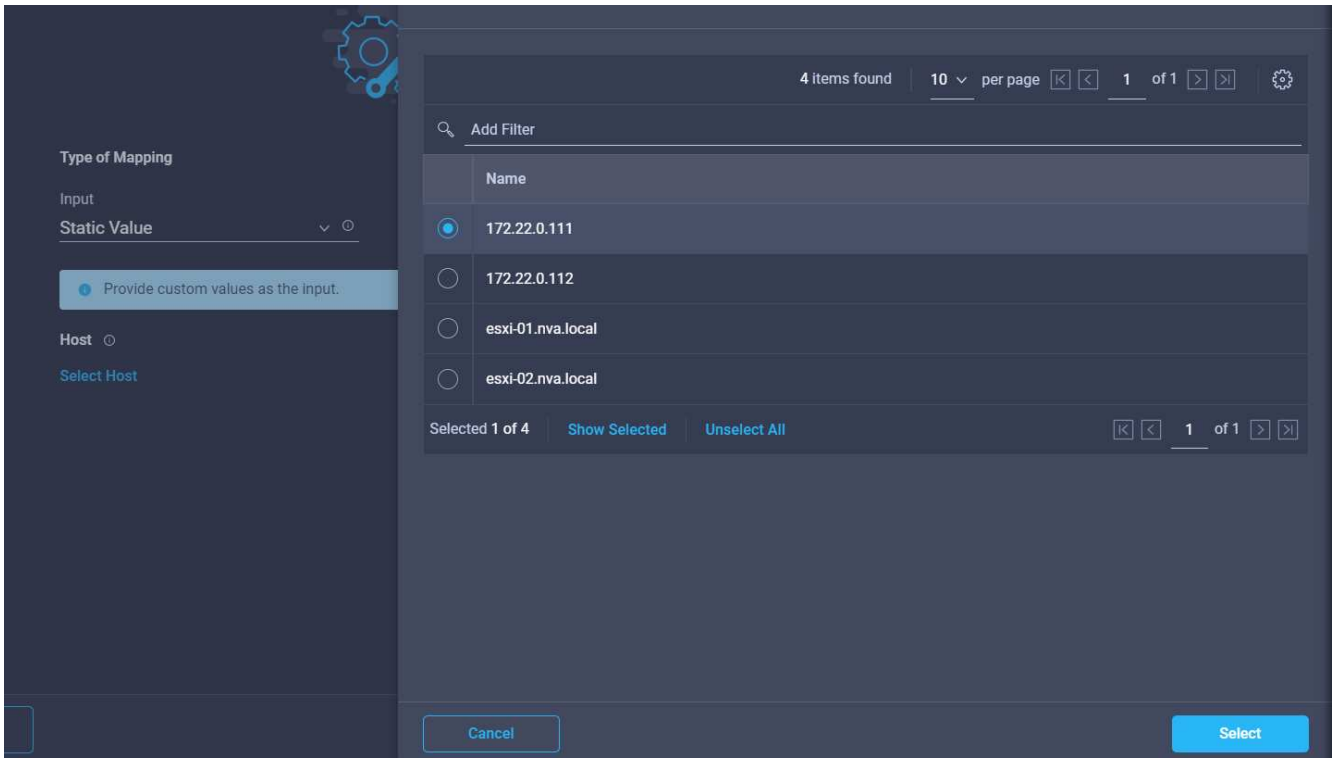


h. Klicken Sie Auf **Hinzufügen**.

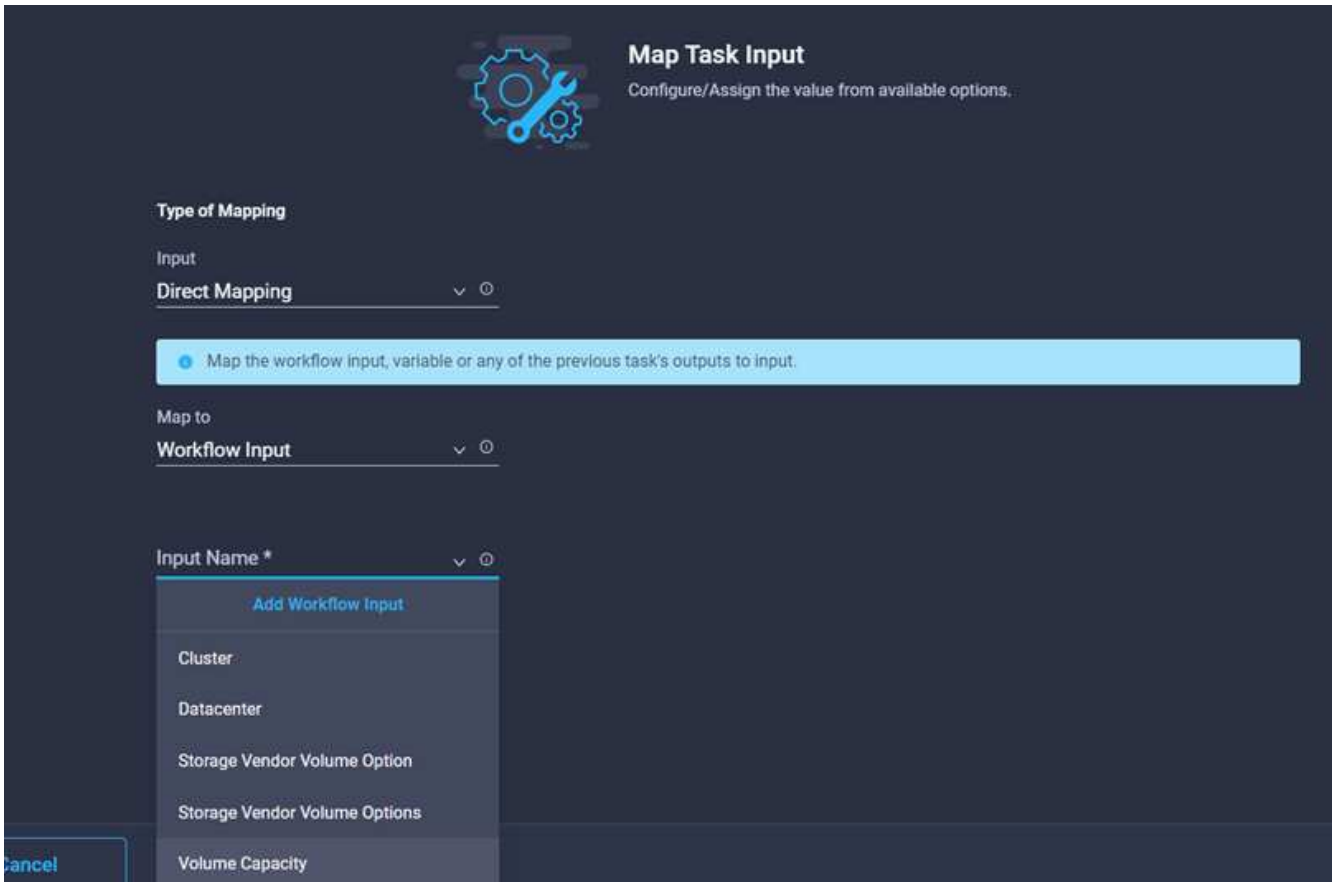
17. Klicken Sie Auf **Karte**.
18. Klicken Sie im Feld **Host** auf **Karte**.



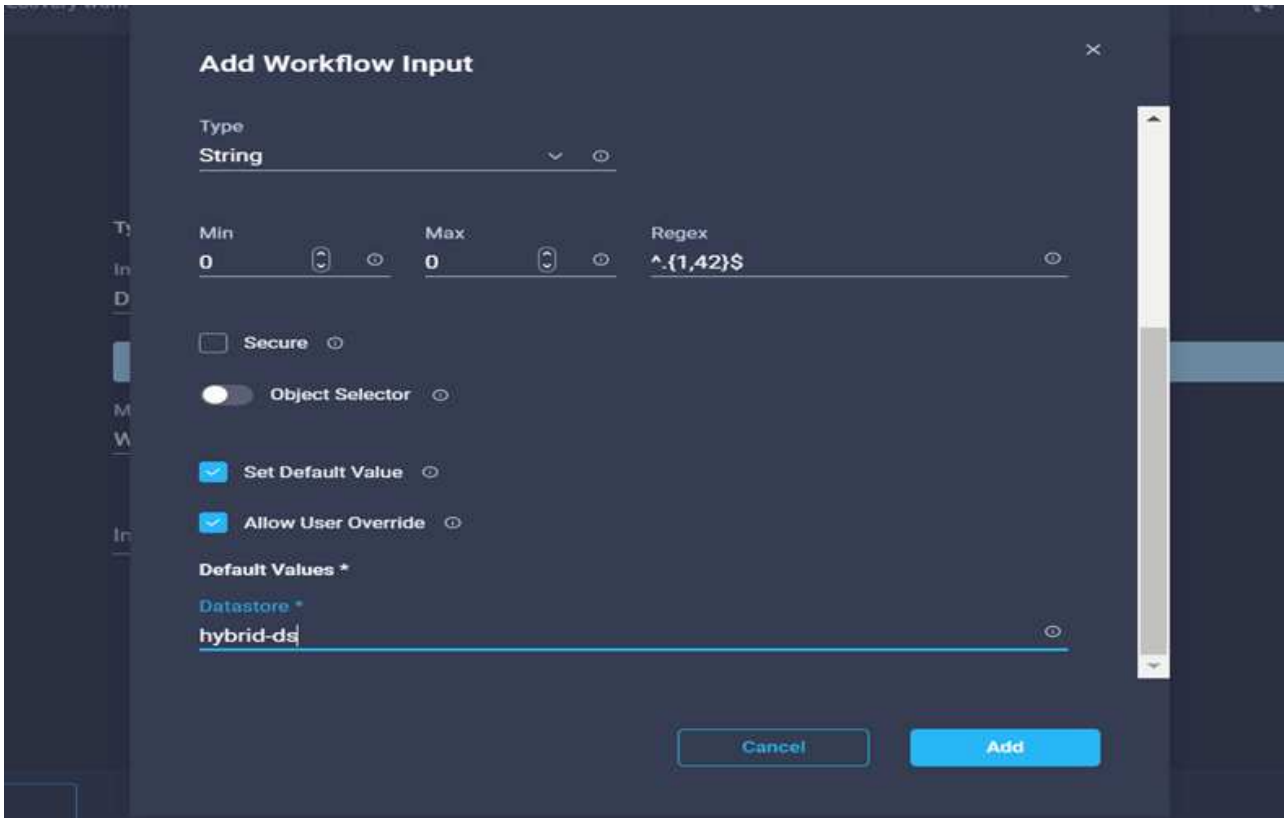
19. Wählen Sie **statischer Wert** und klicken Sie auf den Host, auf dem der Datenspeicher gehostet werden soll. Wenn ein Cluster angegeben wird, wird der Host ignoriert.



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**.

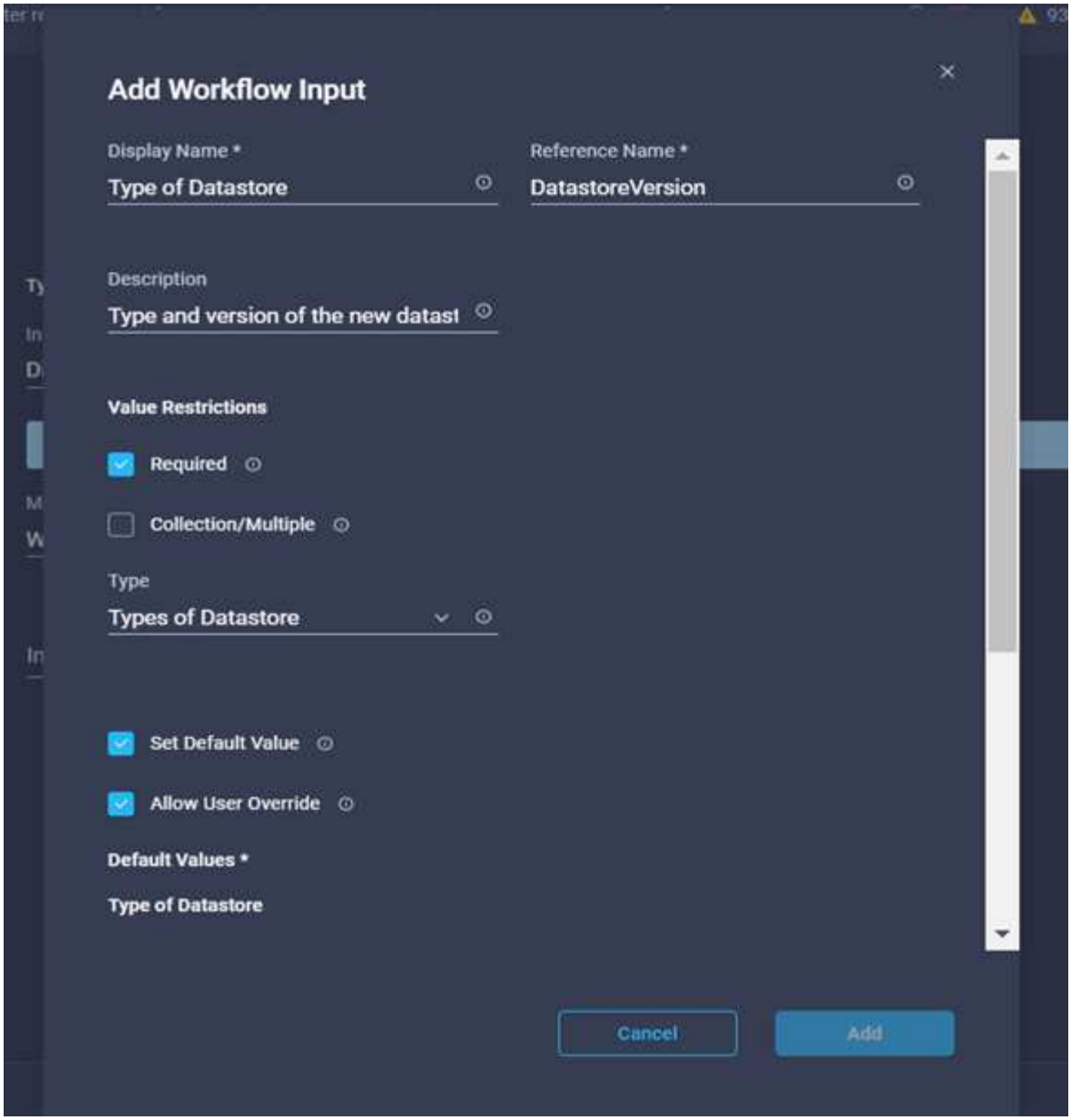


24. Im Add Input Wizard:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Klicken Sie auf **Standardwert festlegen und überschreiben**.
    d. Geben Sie einen Standardwert für den Datastore ein und klicken Sie auf **Hinzufügen**.



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**.

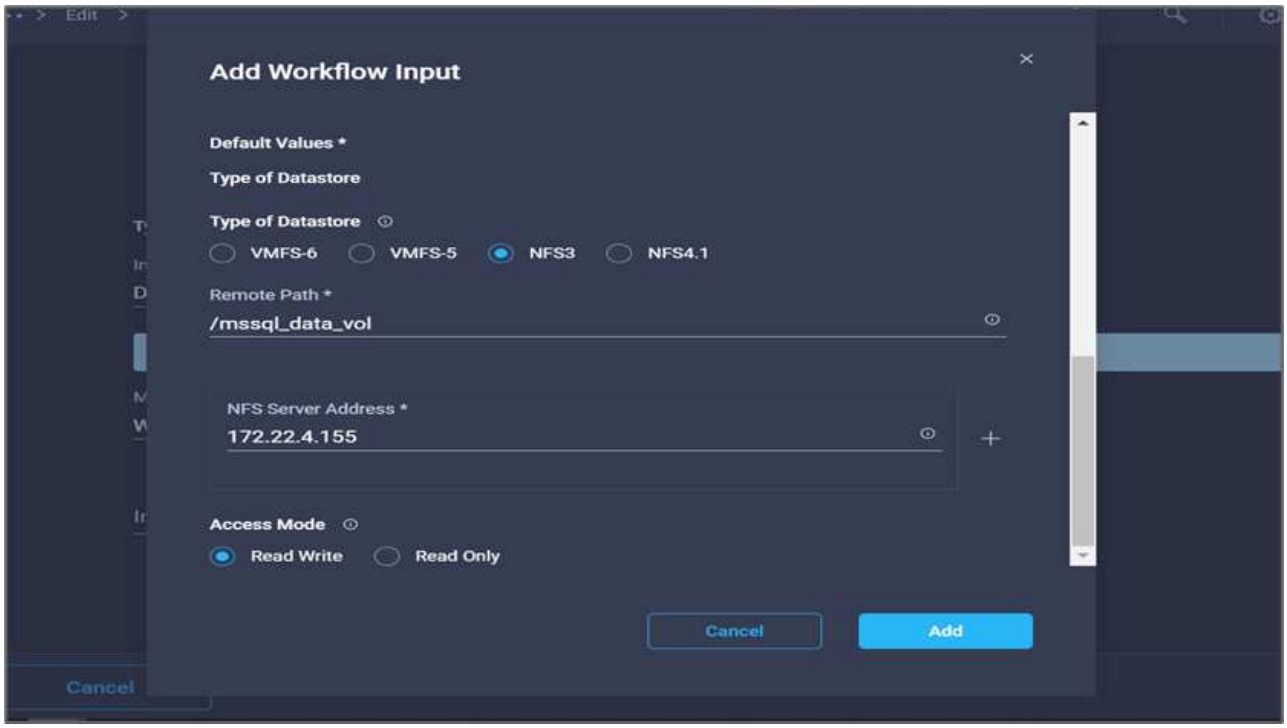
29. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional) und klicken Sie auf **erforderlich**.
    b. Stellen Sie sicher, dass Sie den Typ **Types of Datastore** auswählen und auf **Standardwert festlegen und überschreiben**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



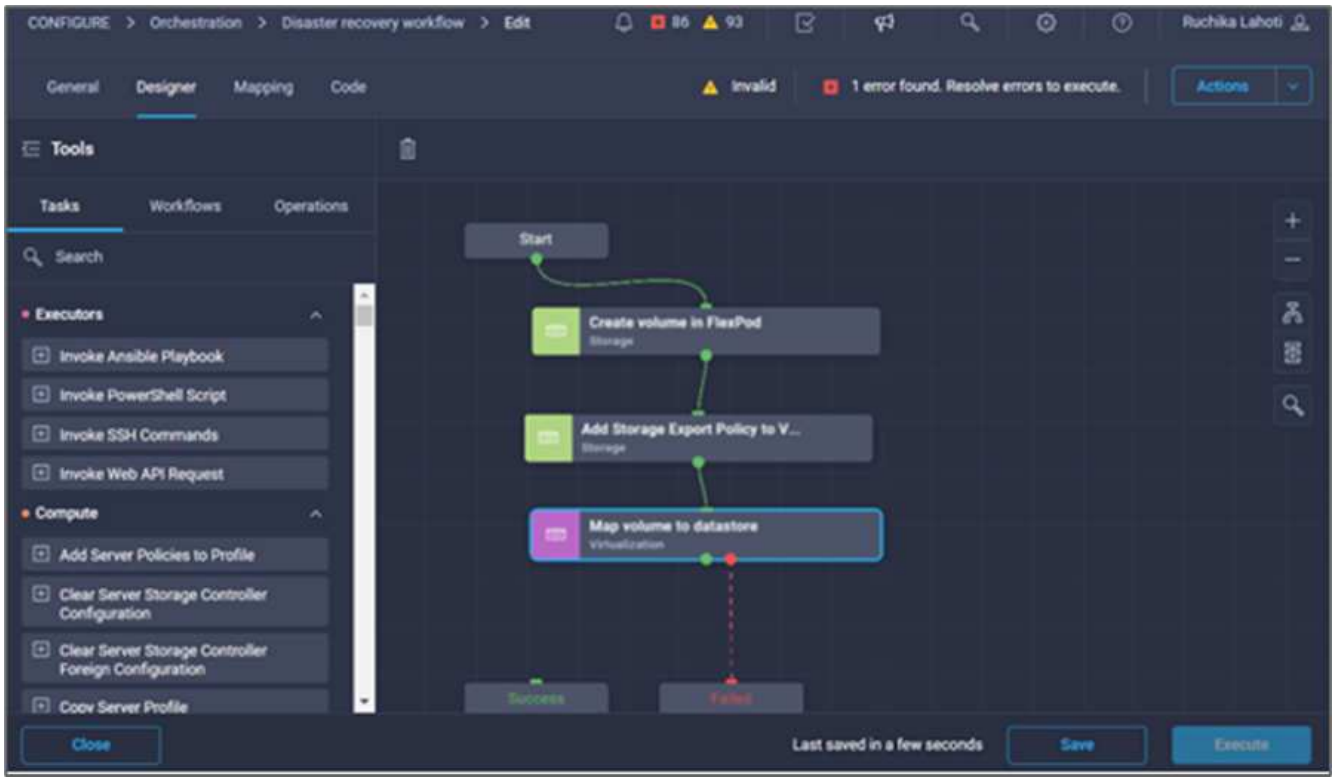
c. Geben Sie den Remote-Pfad an. Dies ist der Remote-Pfad des NFS Mount-Punkts.

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

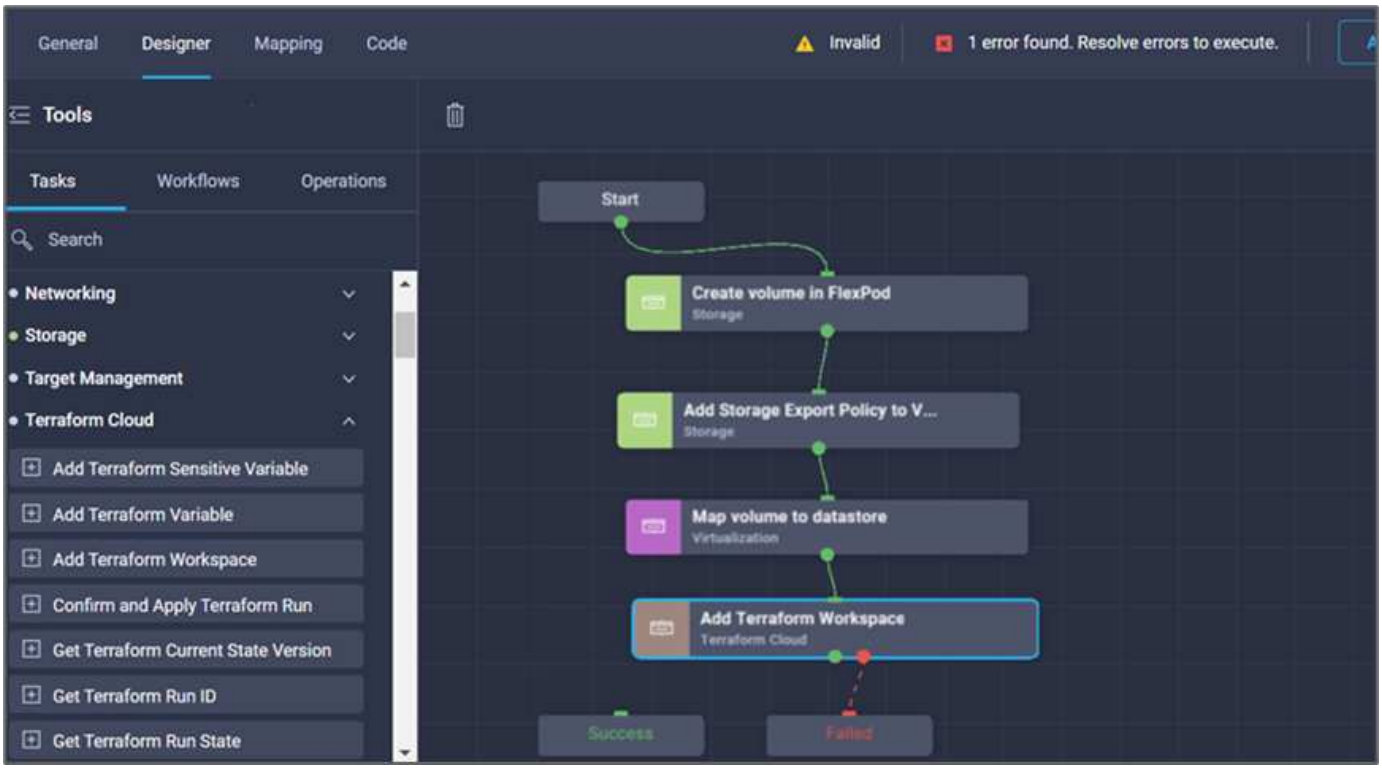
e. Klicken Sie auf den **Zugriffsmodus**. Der Zugriffsmodus gilt für den NFS-Server. Klicken Sie auf schreibgeschützt, wenn Volumes als schreibgeschützt exportiert werden. Klicken Sie Auf **Hinzufügen**.



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

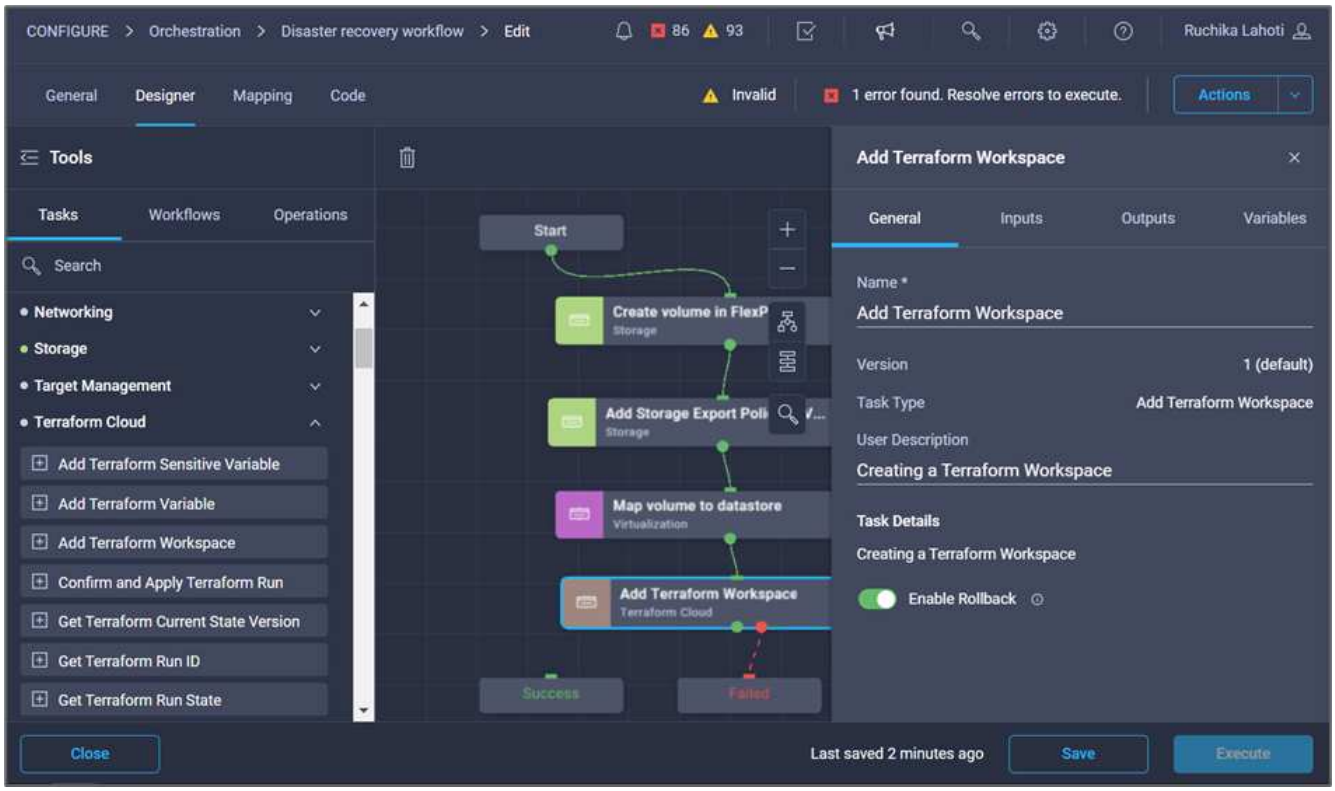


Damit ist die Erstellung des Datastores abgeschlossen. Alle im On- Premises-FlexPod-Datacenter ausgeführten Aufgaben werden abgeschlossen.

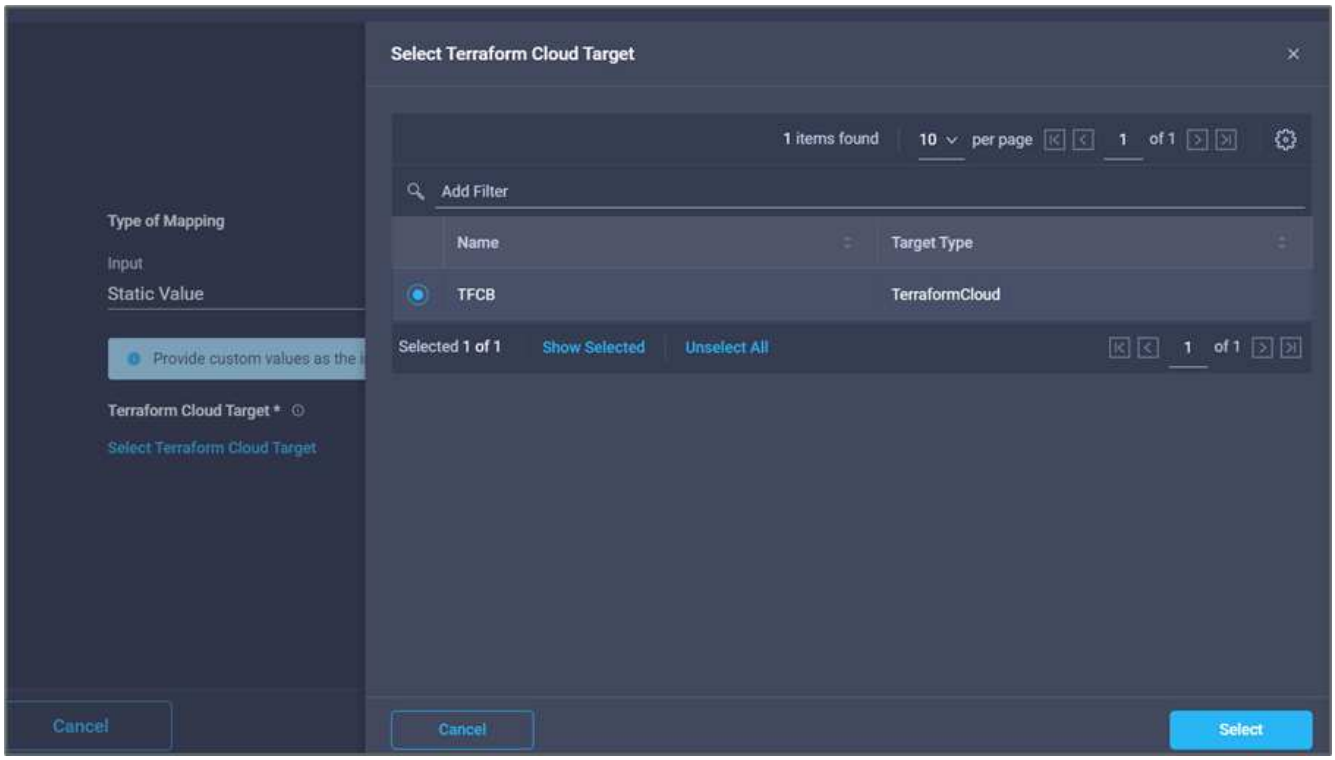


Prozedur 5: Fügen Sie einen neuen Terraform-Arbeitsbereich hinzu

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.

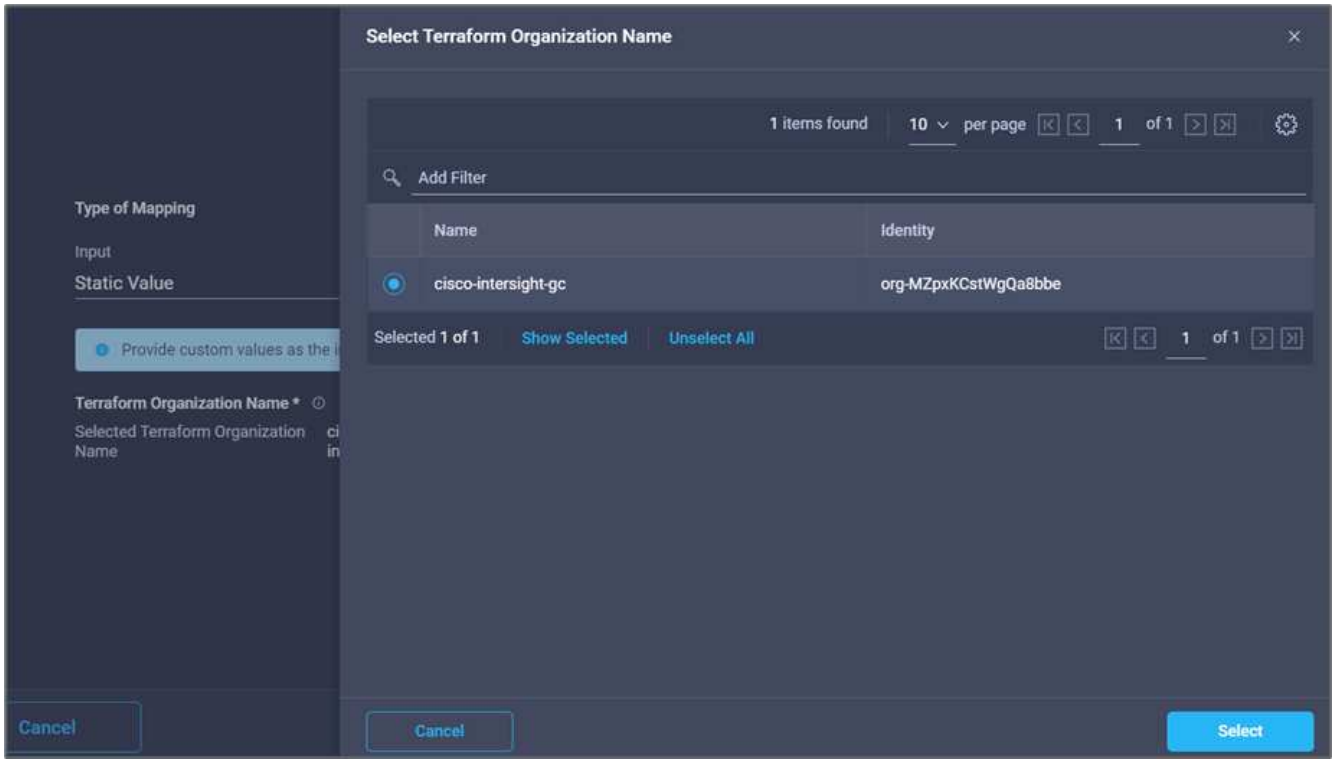


5. Klicken Sie im Bereich Aufgabeneigenschaften auf **Eingaben**.
6. Klicken Sie im Eingabefeld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das wie in erläutert hinzugefügt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

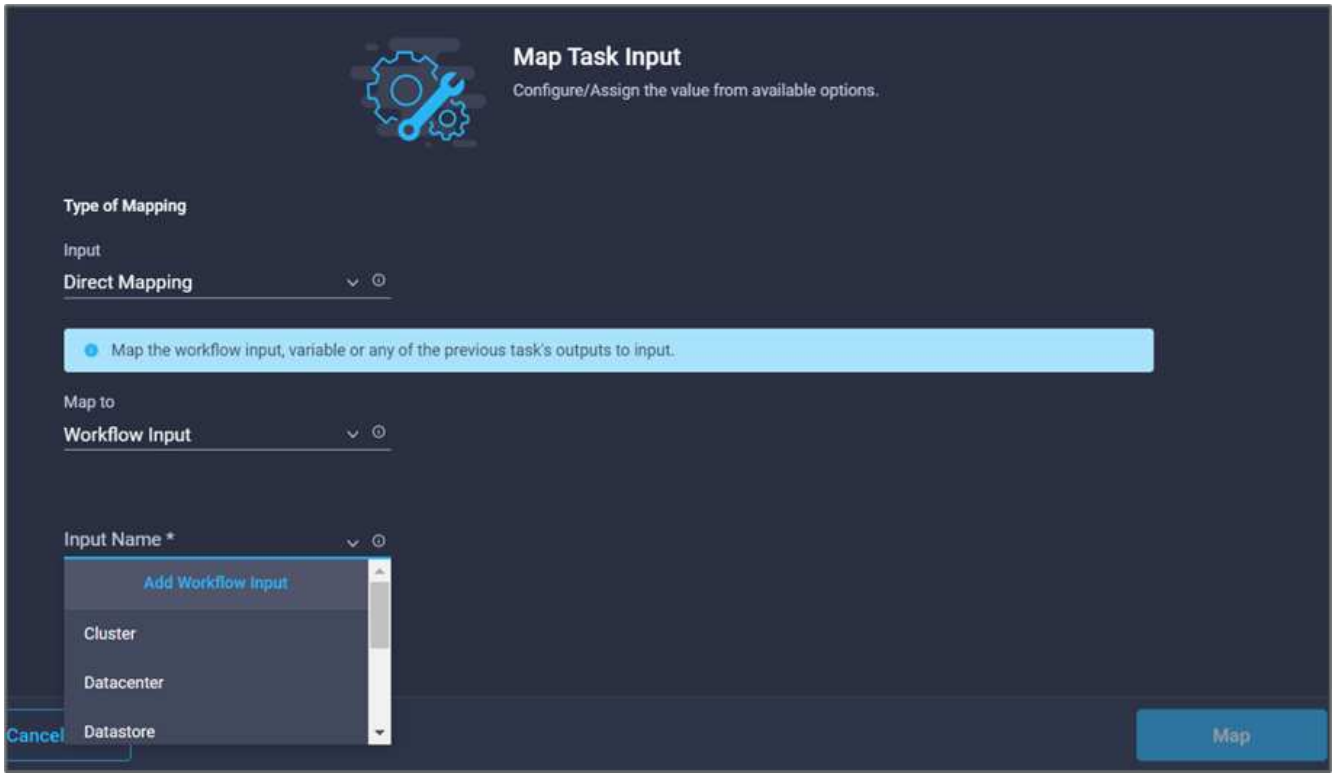


8. Klicken Sie Auf **Karte**.

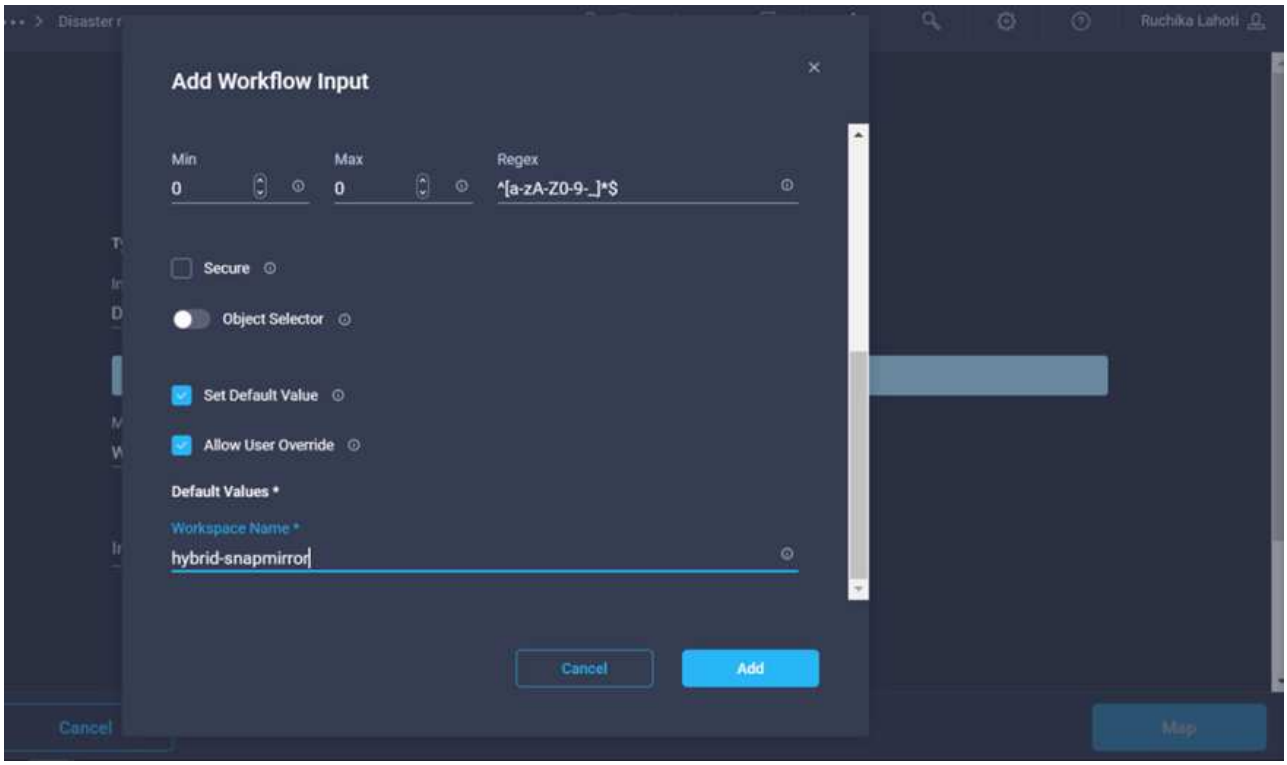
9. Klicken Sie im Eingabefeld **Terraform Organisationsname** auf **Karte**.
10. Wählen Sie **statischer Wert** und klicken Sie dann auf **Terraform-Organisation auswählen**. Wählen Sie den Namen der Terraform-Organisation aus, der Sie in Ihrem Terraform Cloud for Business-Account gehören.



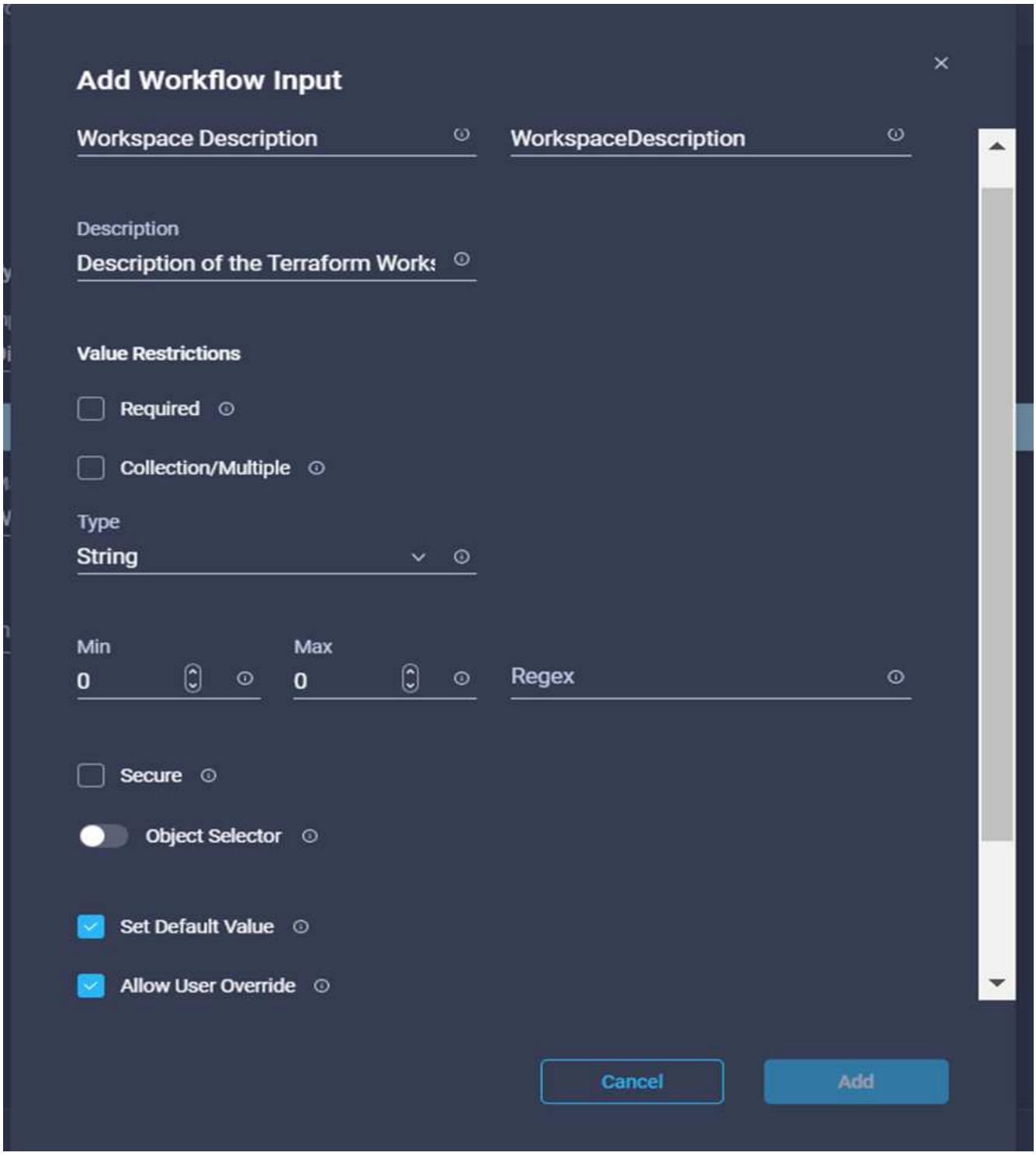
11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**. Dies ist der neue Workspace im Terraform Cloud for Business Account.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
14. Klicken Sie auf **Eingabename** und **Workflow-Eingabe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



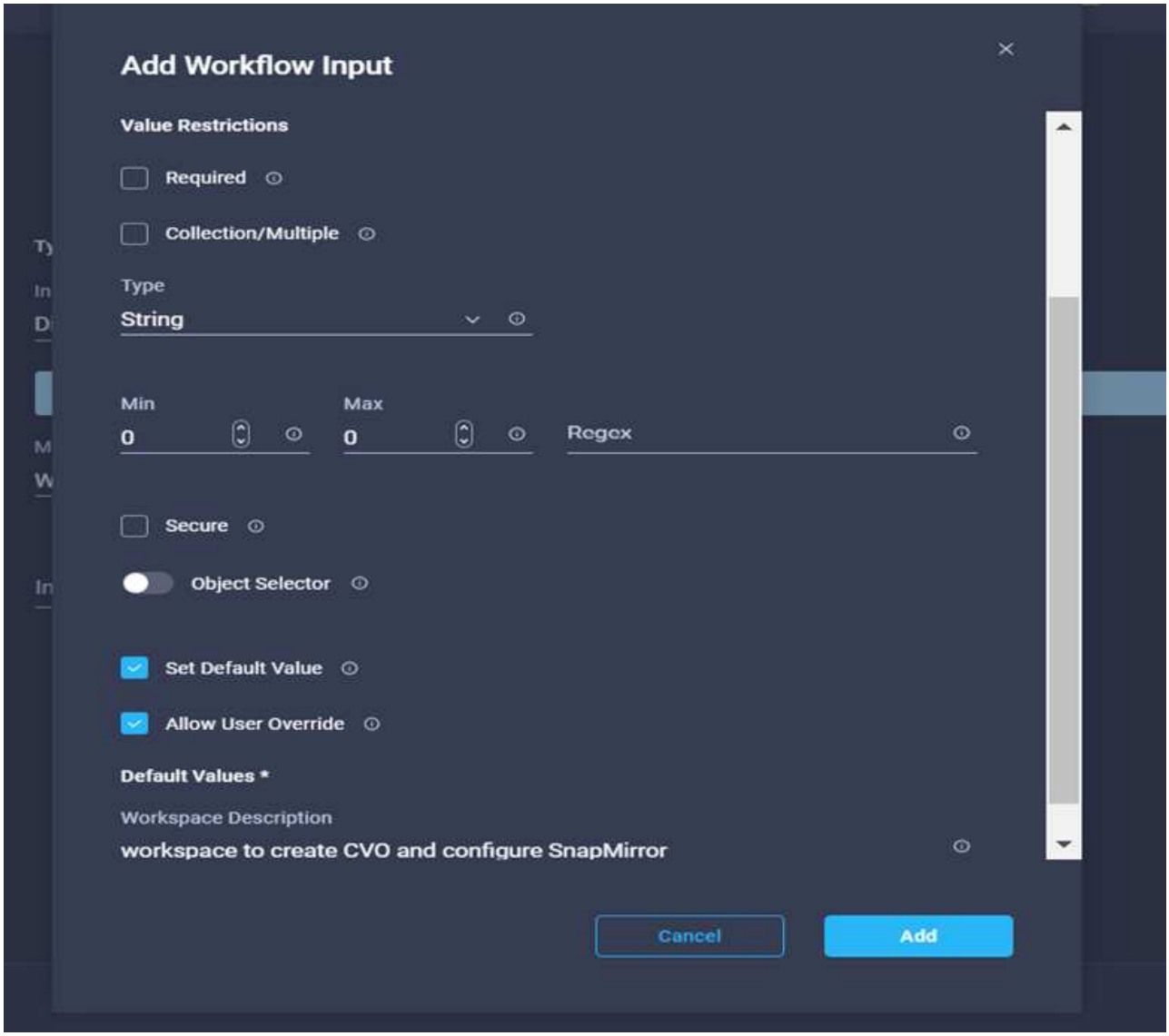
15. Führen Sie im Add Input Wizard die folgenden Schritte aus:
    a. Geben Sie einen Anzeigenamen und einen Referenznamen an (optional).
    b. Klicken Sie Auf * Erforderlich*.
    c. Achten Sie darauf, **String** für **Typ** auszuwählen.
    d. Klicken Sie auf **Standardwert festlegen und überschreiben**.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



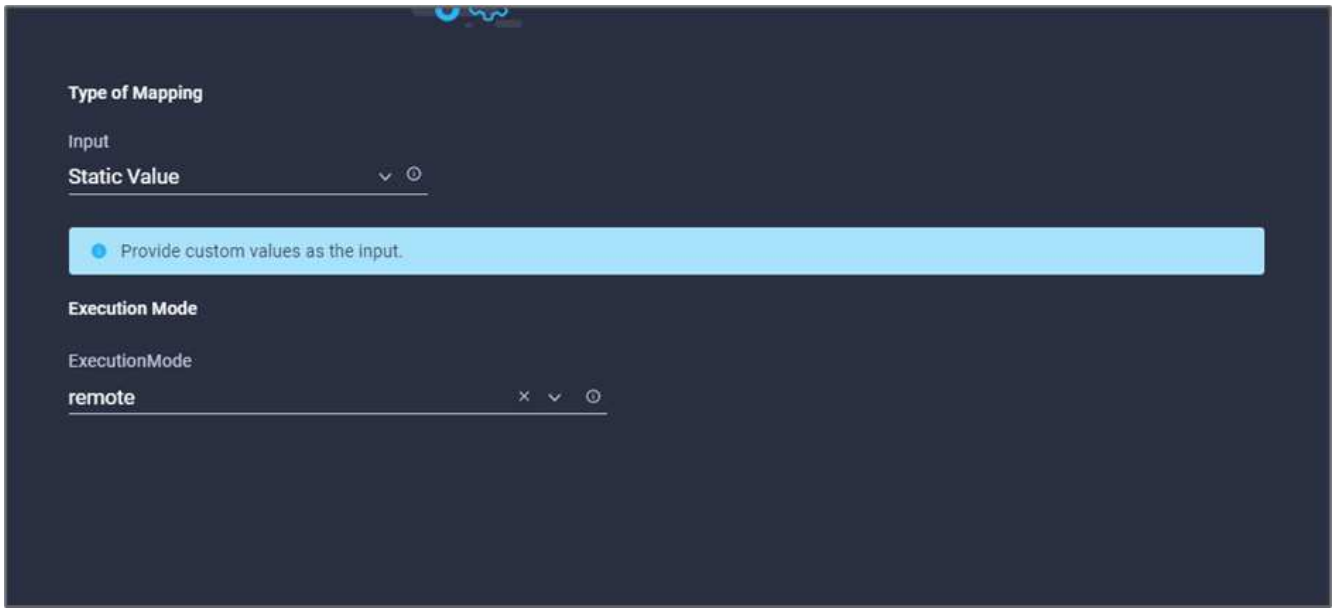
16. Klicken Sie Auf **Karte**.
17. Klicken Sie im Feld **Workspace Beschreibung** auf **Karte**.
18. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Workflow-Eingabe**.
19. Klicken Sie auf **Eingabename** und **Workflow-Eingabe erstellen**.



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**.



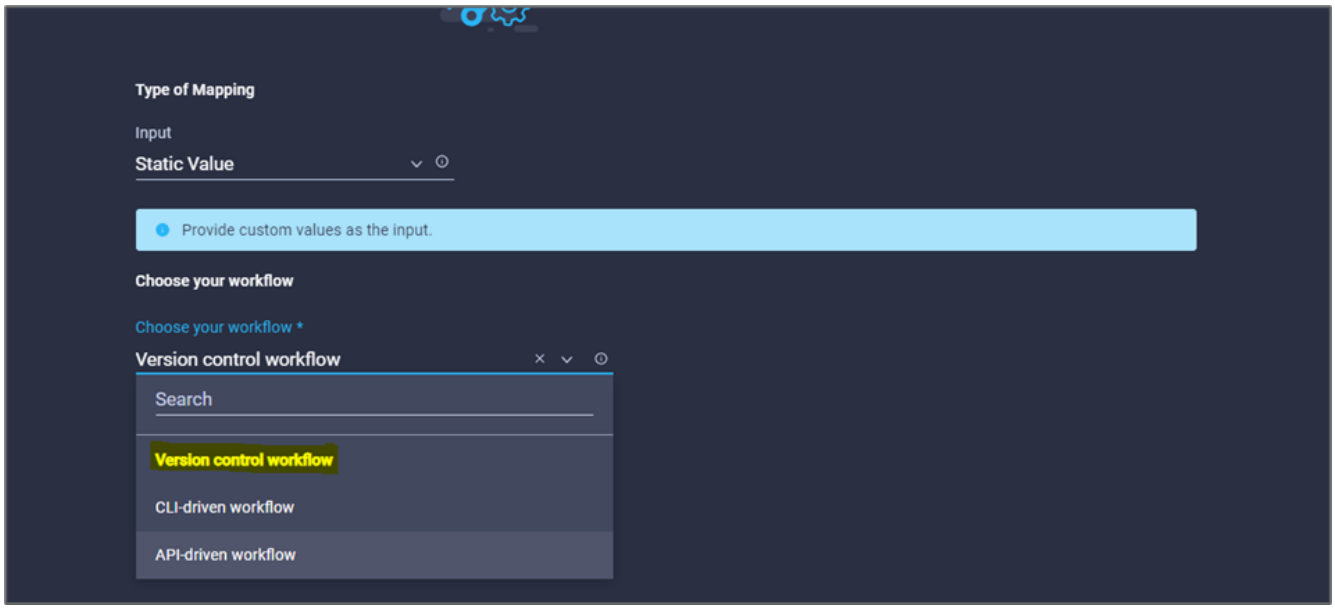
21. Klicken Sie Auf **Karte**.
22. Klicken Sie im Feld **Ausführungsmodus** auf **Karte**.
23. Wählen Sie **statischer Wert**, klicken Sie auf **Ausführungsmodus** und dann auf **Remote**.



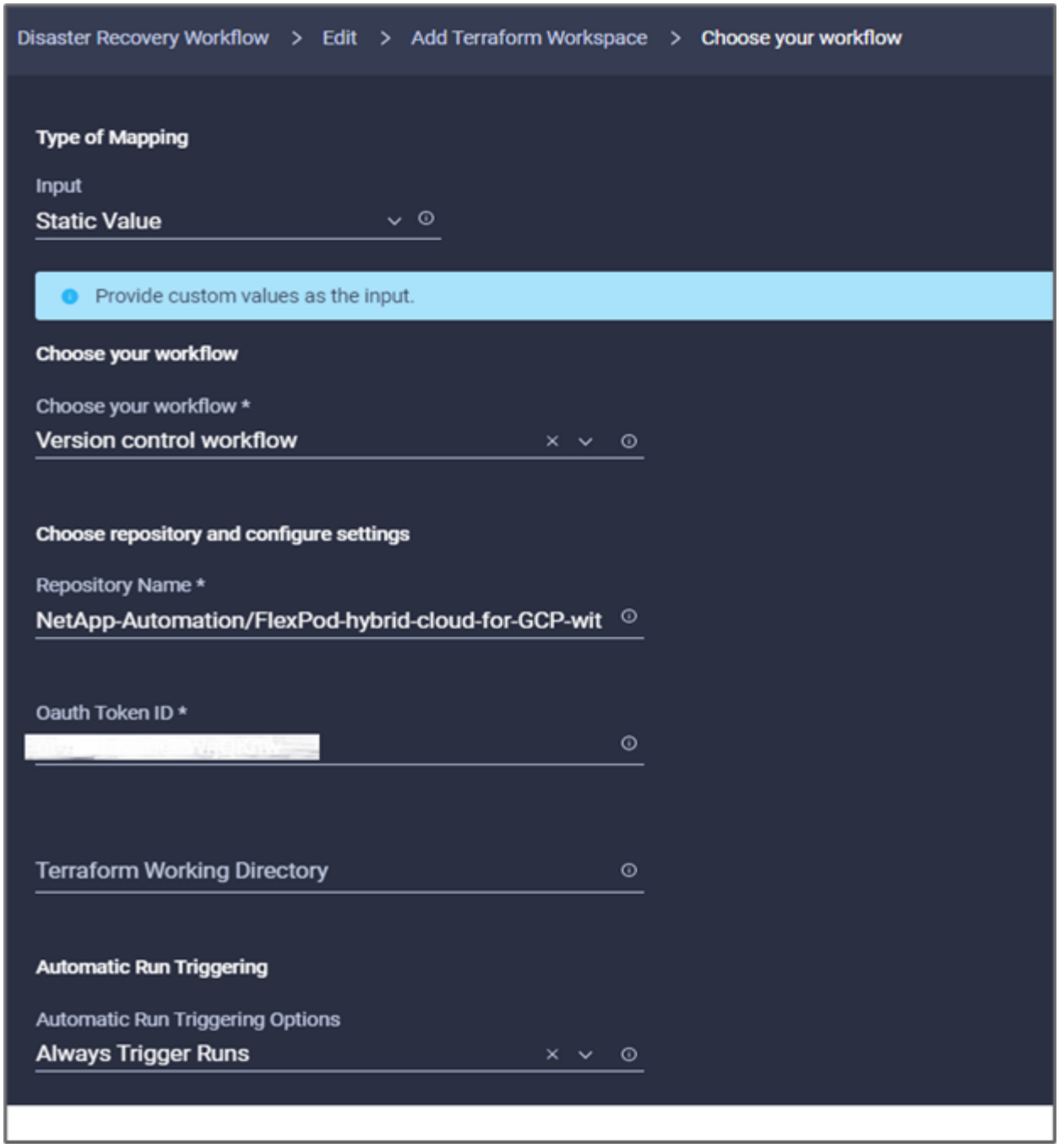
24. Klicken Sie Auf **Karte**.
25. Klicken Sie im Feld **Methode anwenden** auf **Karte**.
26. Wählen Sie **statischer Wert** und klicken Sie auf **Methode anwenden**. Klicken Sie Auf **Manuelle Anwendung**.

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.



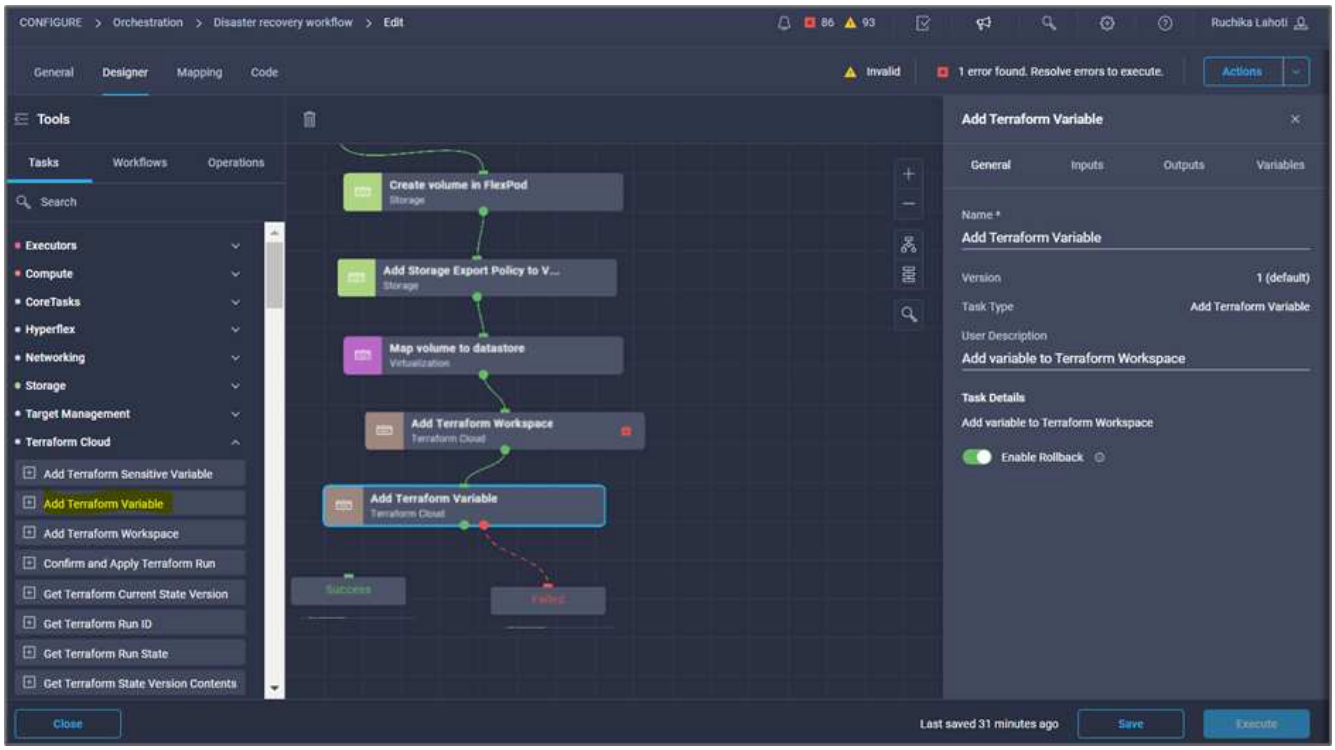
34. Klicken Sie Auf **Karte**.
35. Klicken Sie Auf **Speichern**.

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

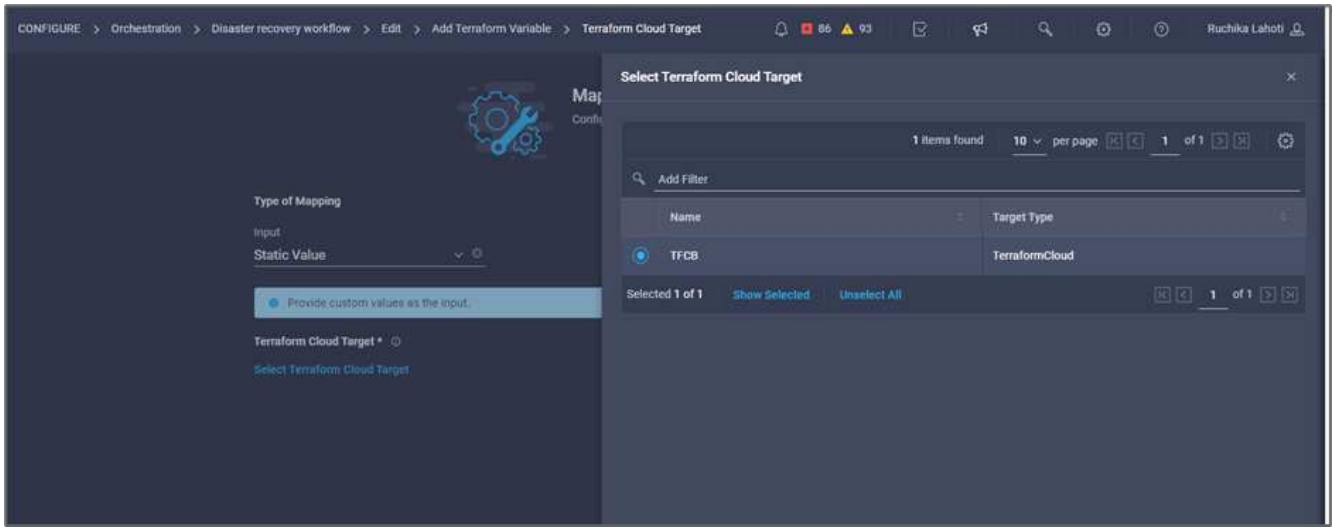
Prozedur 6: Fügen Sie dem Arbeitsbereich nicht-sensible Variablen hinzu

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**.

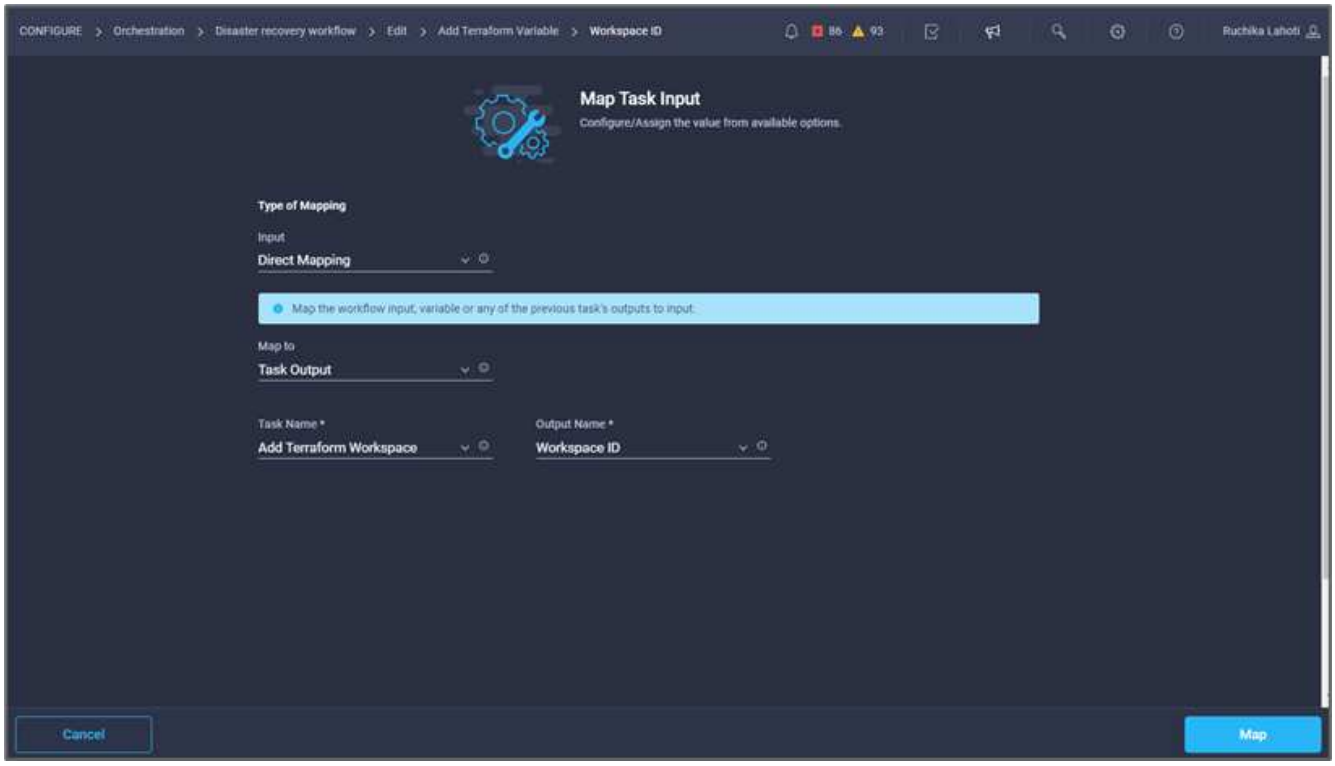
4. Klicken Sie Auf **Terraform-Variablen Hinzufügen**. Klicken Sie im Bereich **Workflow-Eigenschaften** auf die Registerkarte **Allgemein**. Optional können Sie den Namen und die Beschreibung für diese Aufgabe ändern.



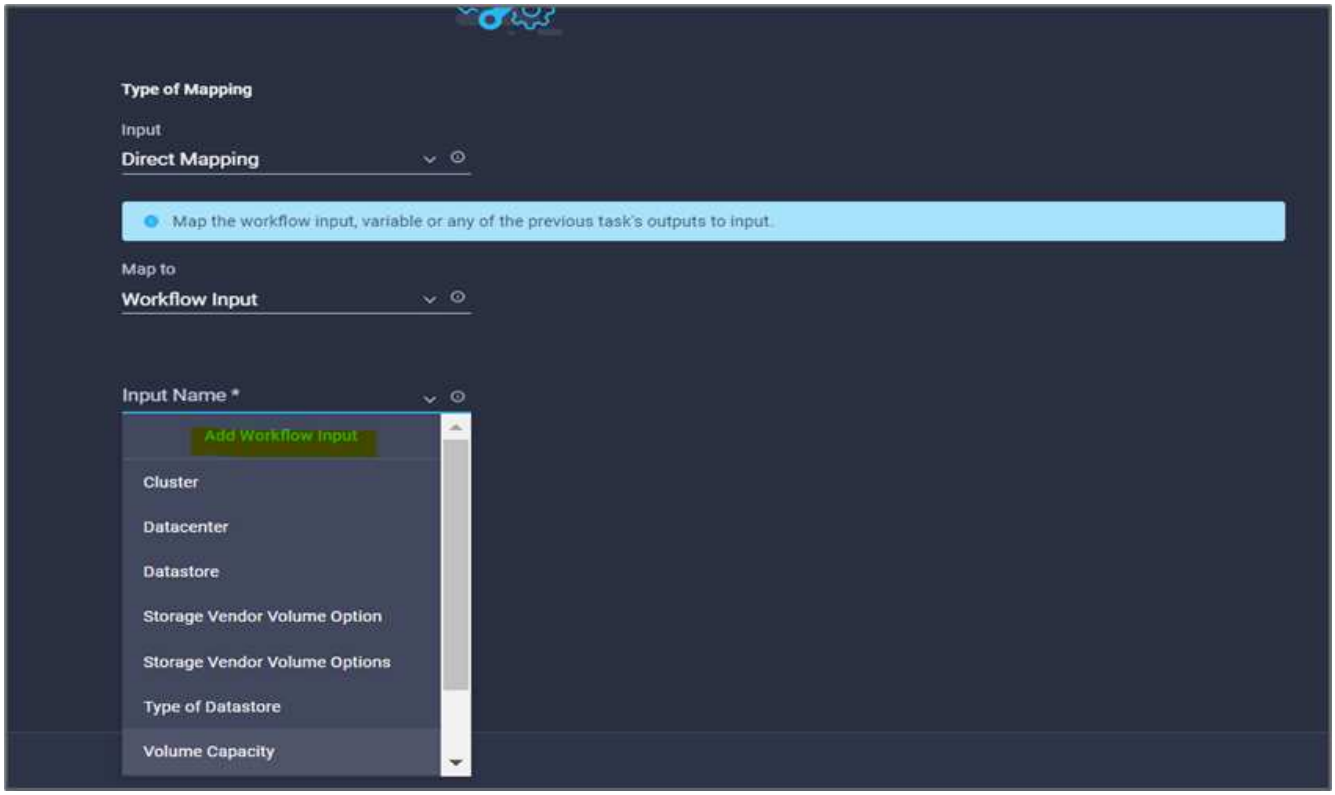
5. Klicken Sie im Bereich **Workflow-Eigenschaften** auf **Eingaben**.
6. Klicken Sie im Feld **Terraform Cloud Target** auf **Karte**.
7. Wählen Sie **statischer Wert** und klicken Sie auf **Terraform Cloud Target**. Wählen Sie das Terraform Cloud for Business-Konto aus, das wie in erläutert hinzugefügt 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.

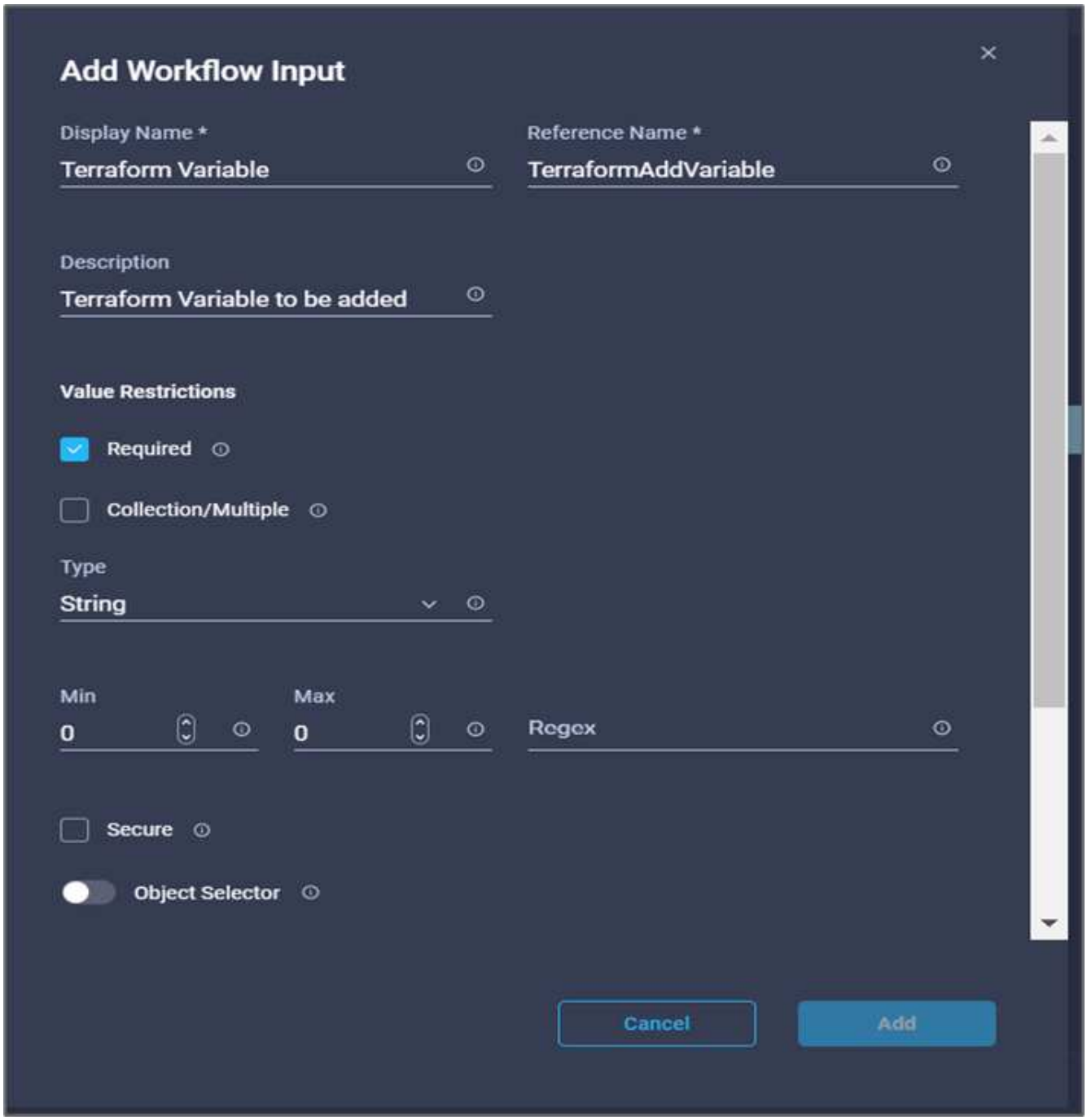


11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
14. Klicken Sie auf **Aufgabenname** und klicken Sie auf **Terraform Workspace hinzufügen**.



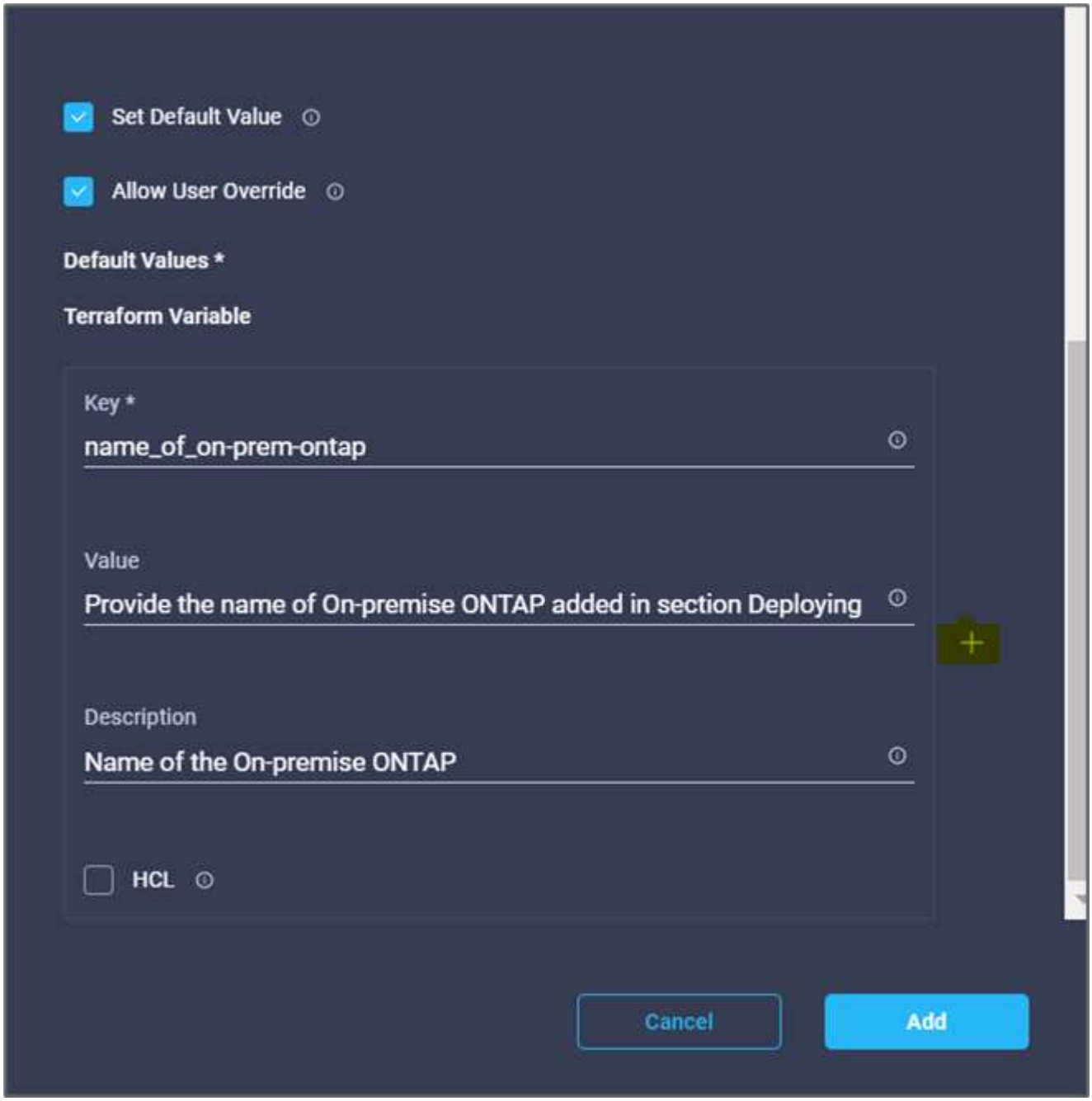
15. Klicken Sie auf **Ausgabename** und dann auf **Workspace Name**.

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.

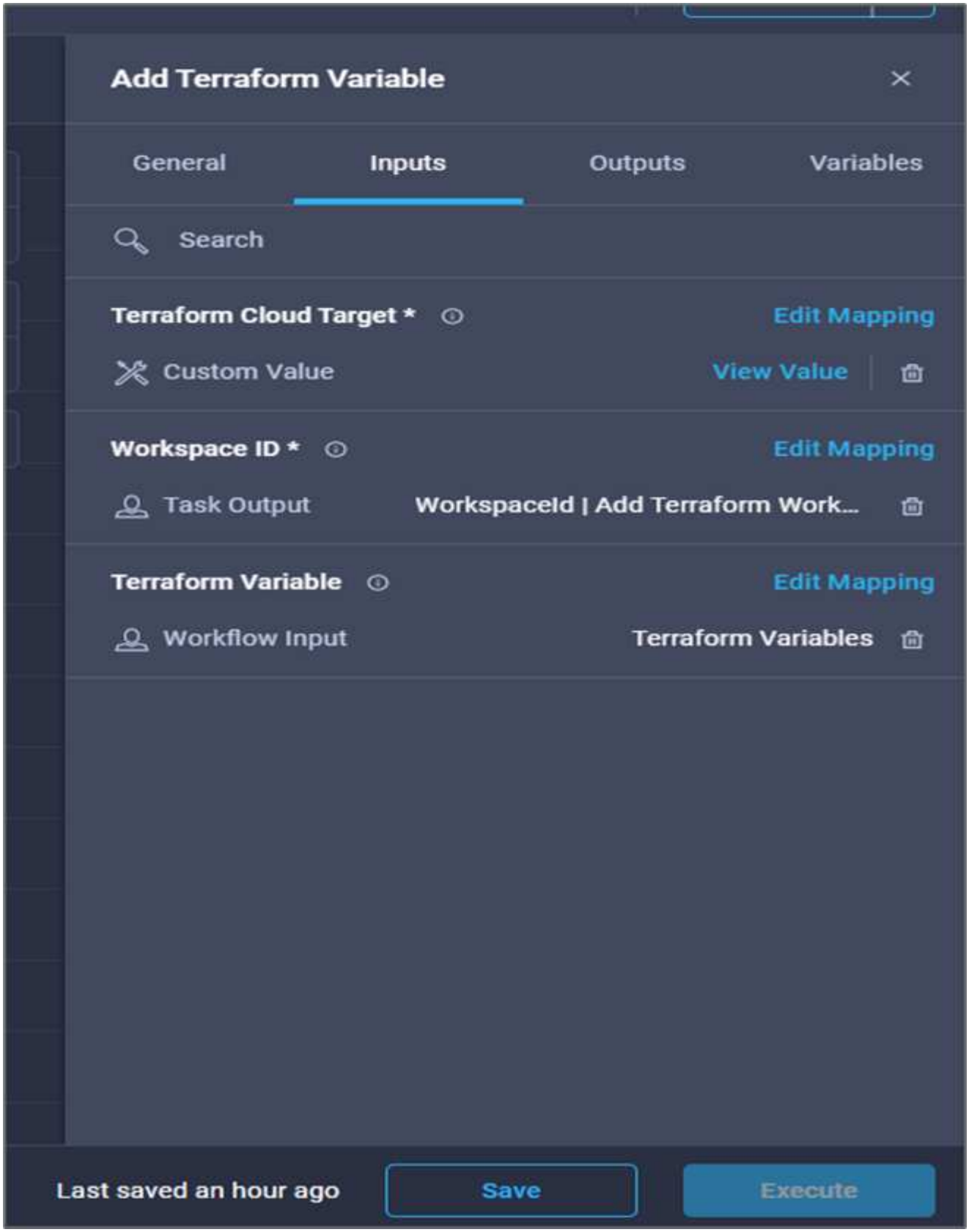


23. Fügen Sie alle Terraform-Variablen wie in der folgenden Tabelle dargestellt hinzu. Sie können auch einen Standardwert angeben.

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**.



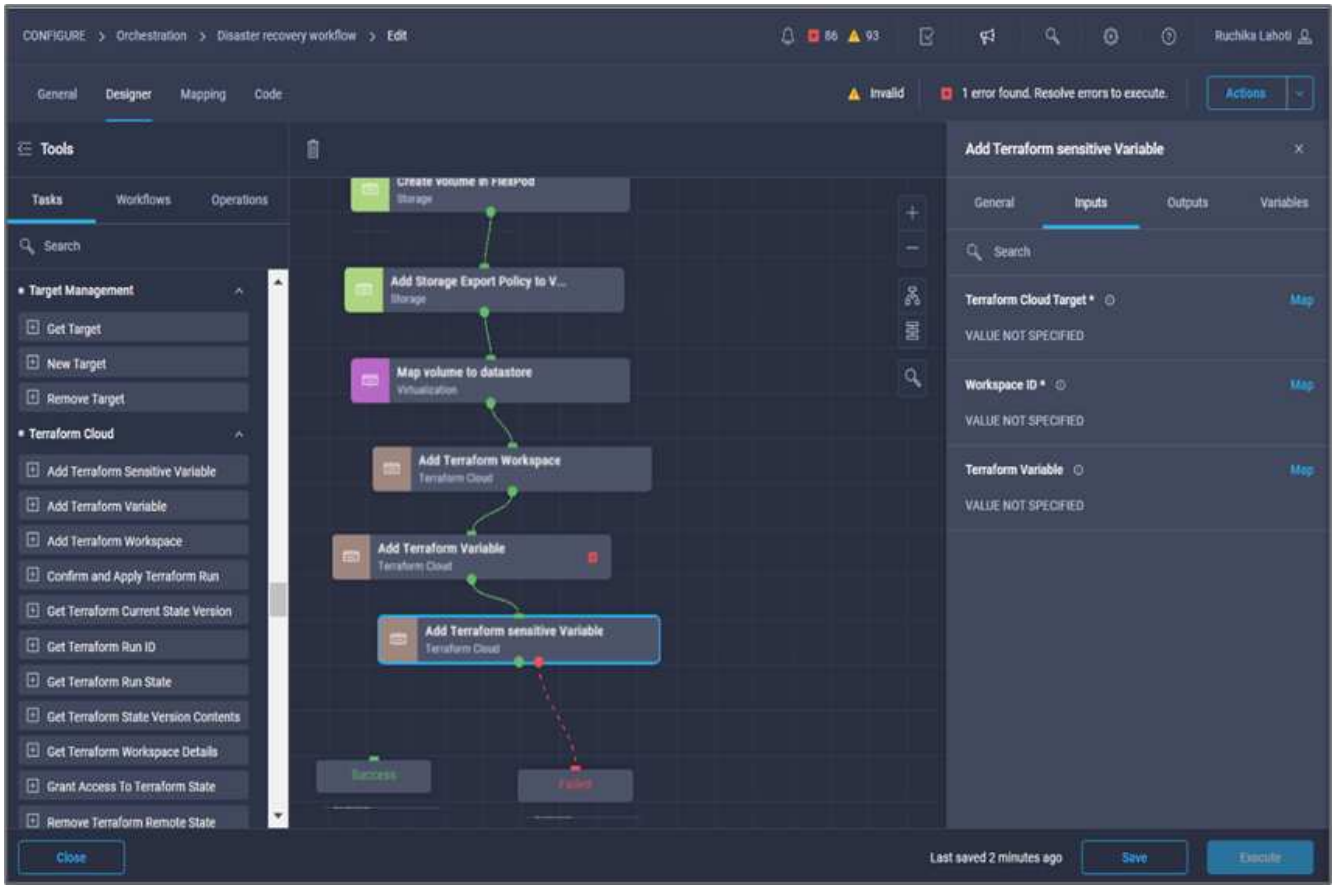
Damit ist das Hinzufügen der erforderlichen Terraform-Variablen zum Arbeitsbereich abgeschlossen. Fügen Sie anschließend die erforderlichen sensiblen Terraform-Variablen zum Arbeitsbereich hinzu. Sie können beide auch zu einer einzigen Aufgabe kombinieren.

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**.

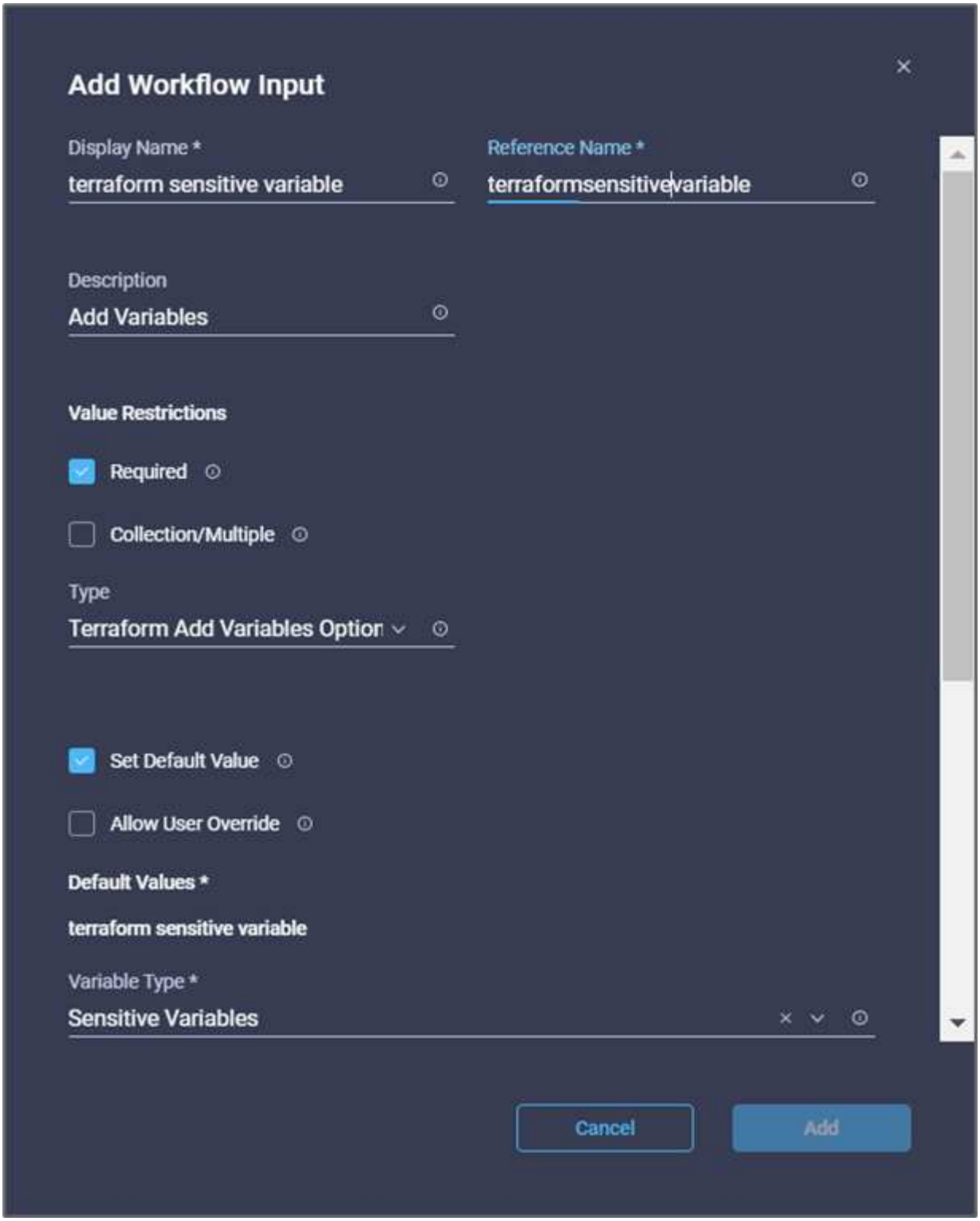
> Es wird eine Warnung angezeigt, die angibt, dass die beiden Aufgaben denselben Namen haben. Ignorieren Sie den Fehler für jetzt, da Sie den Aufgabennamen im nächsten Schritt ändern.

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.

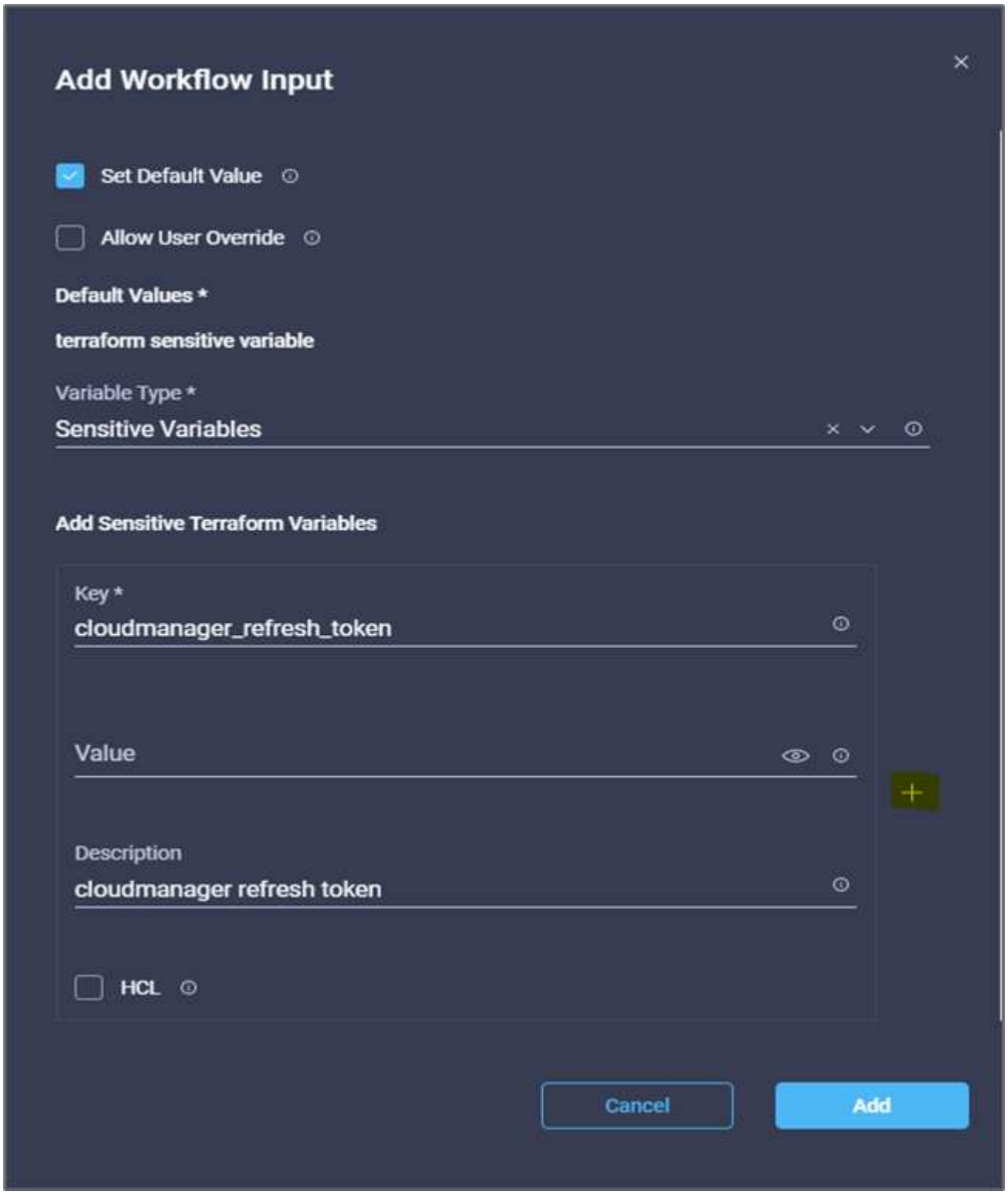
11. Klicken Sie Auf **Karte**.
12. Klicken Sie im Feld * Terraform Workspace Name* auf **Karte**.
13. Wählen Sie **direkte Zuordnung** und klicken Sie auf **Aufgabenausgabe**.
14. Klicken Sie auf **Aufgabenname** und dann auf **Terraform Workspace hinzufügen**.
15. Klicken Sie auf **Ausgabename** und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



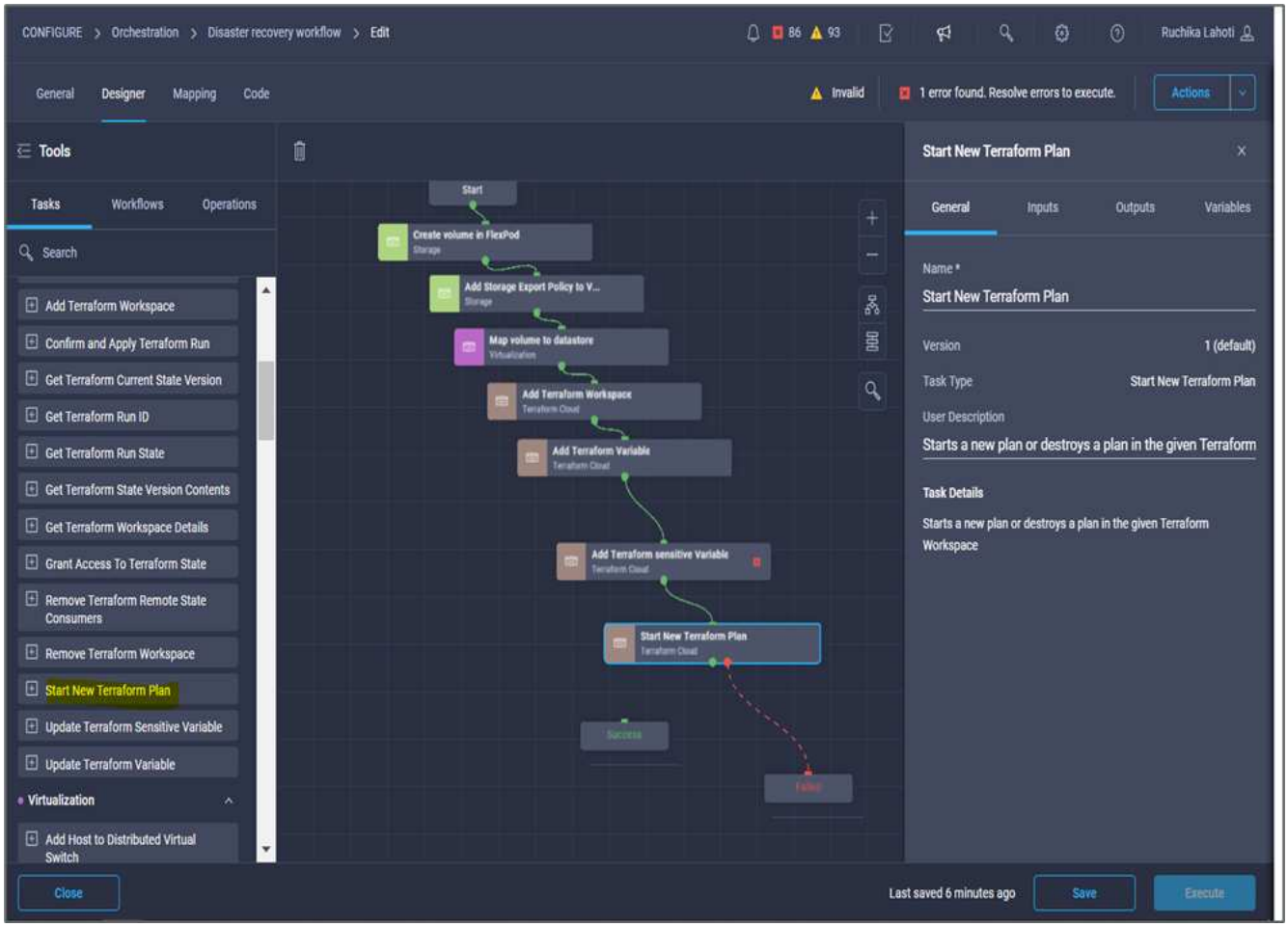
22. Fügen Sie alle Terraform-empfindlichen Variablen hinzu, wie in der nachstehenden Tabelle dargestellt. Sie können auch einen Standardwert angeben.

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

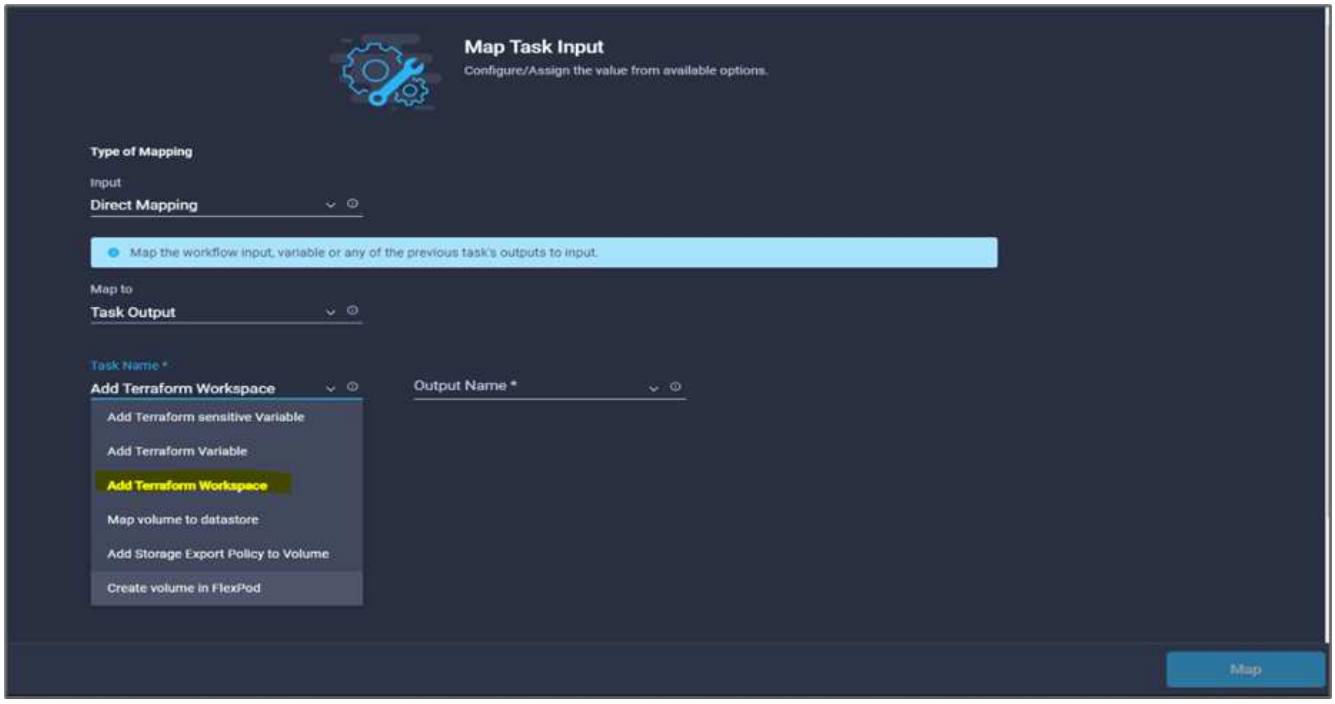
23. Klicken Sie auf **Karte**.damit ist die Aufgabe abgeschlossen, dem Arbeitsbereich die erforderlichen Terraform-empfindlichen Variablen hinzuzufügen. Starten Sie dann einen neuen Terraform-Plan im konfigurierten Arbeitsbereich.

Verfahren 8: Starten Sie einen neuen Terraform-Plan

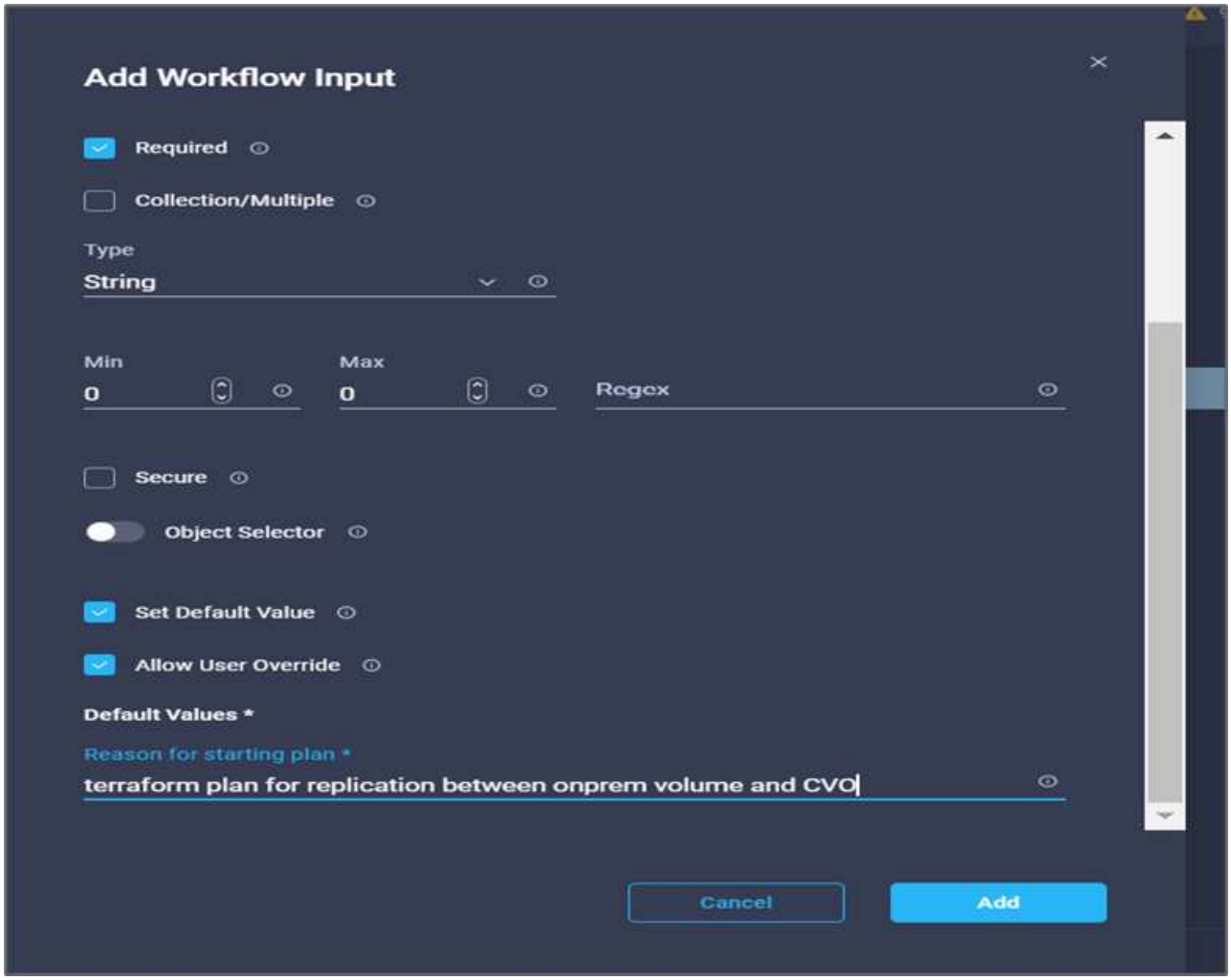
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe **Terraform Cloud > Neue Terraform Plan** aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Connector, um zwischen den Aufgaben zu verbinden **Terraform sensible 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**.

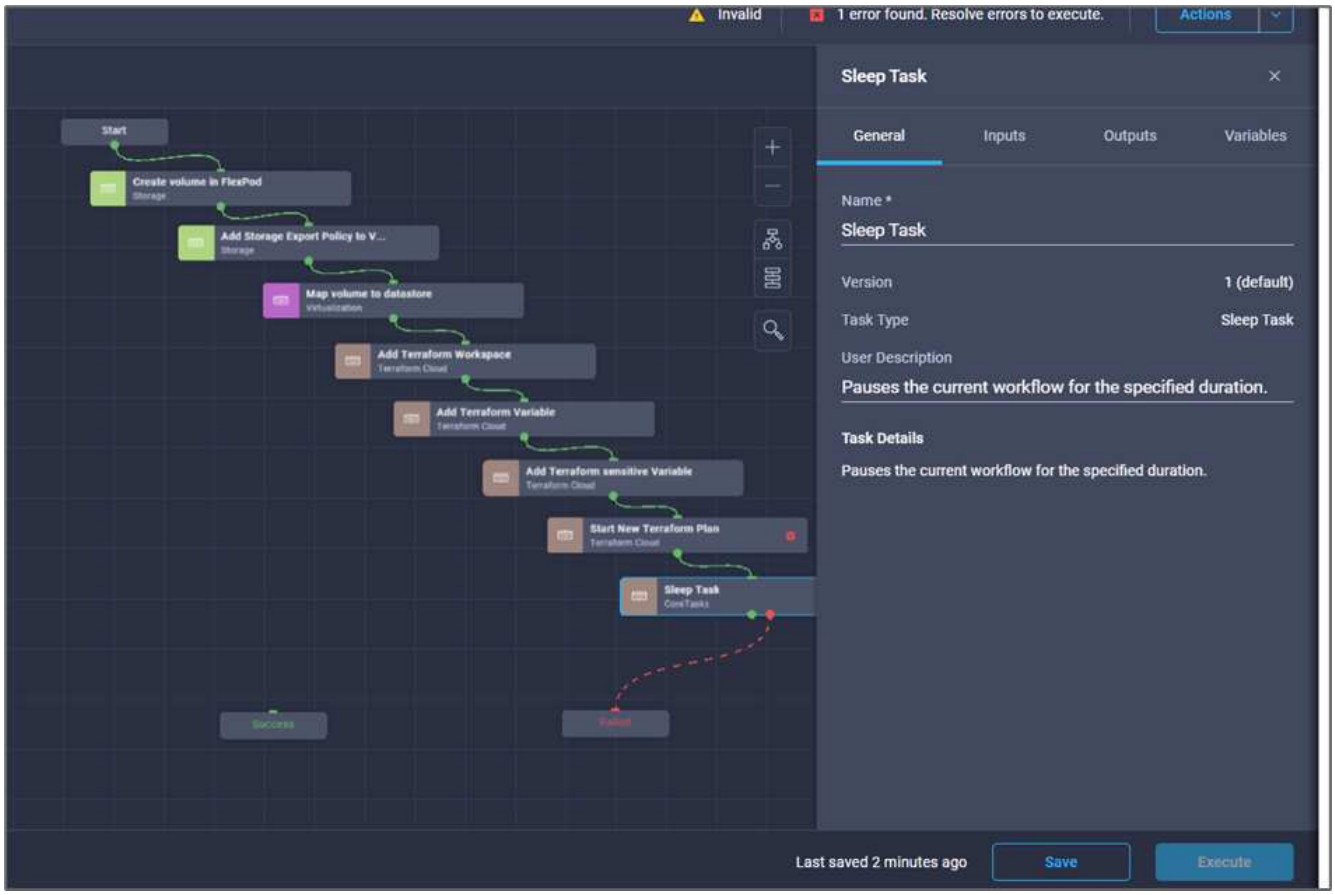
20. Klicken Sie Auf **Karte**.
21. Klicken Sie Auf **Speichern**.

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

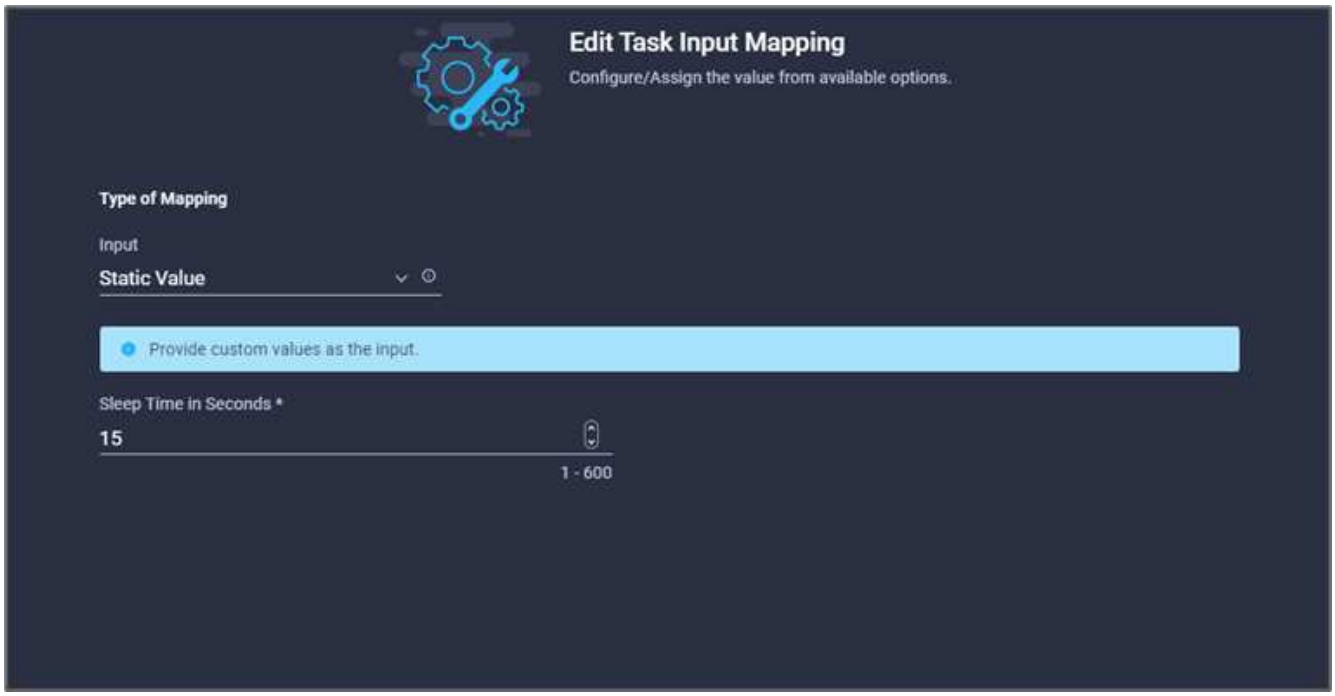
Prozedur 9: Sleep-Task für die Synchronisation

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.

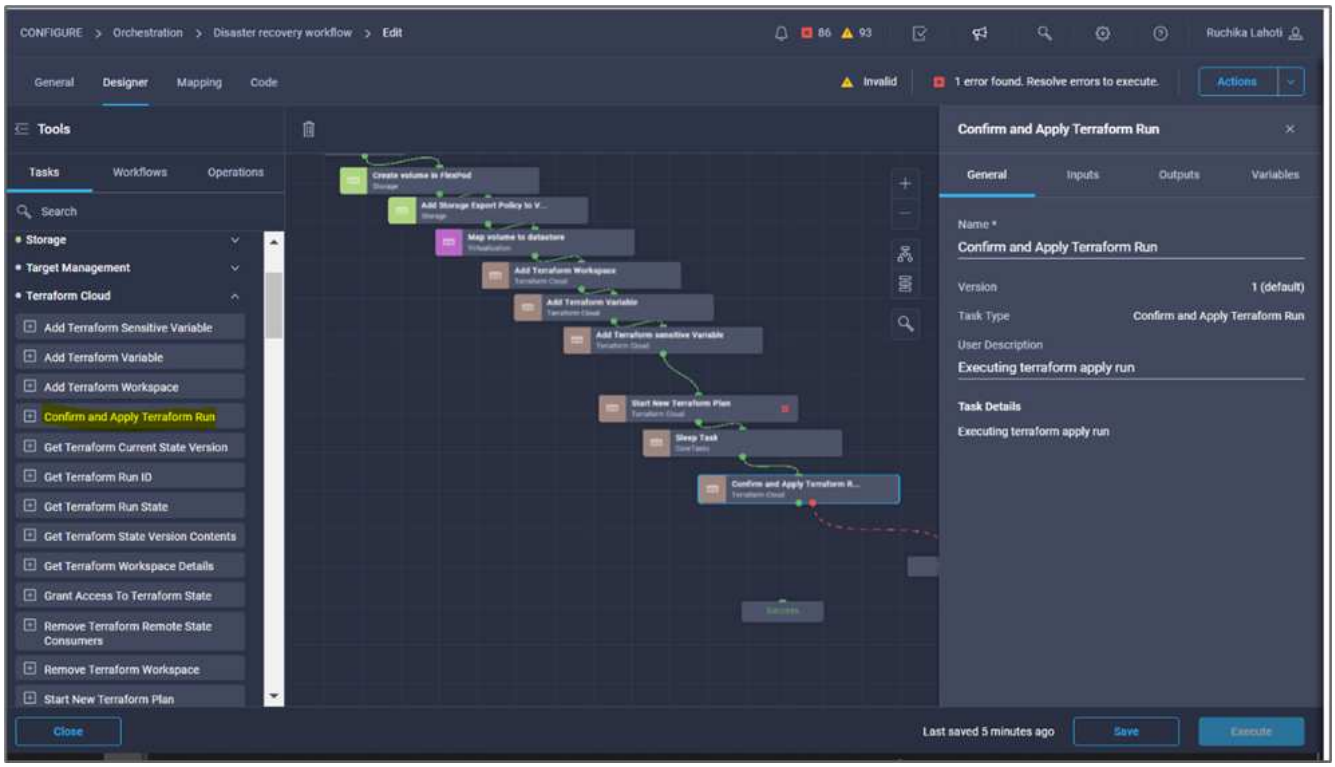


8. Klicken Sie Auf **Karte**.
9. Klicken Sie Auf **Speichern**.

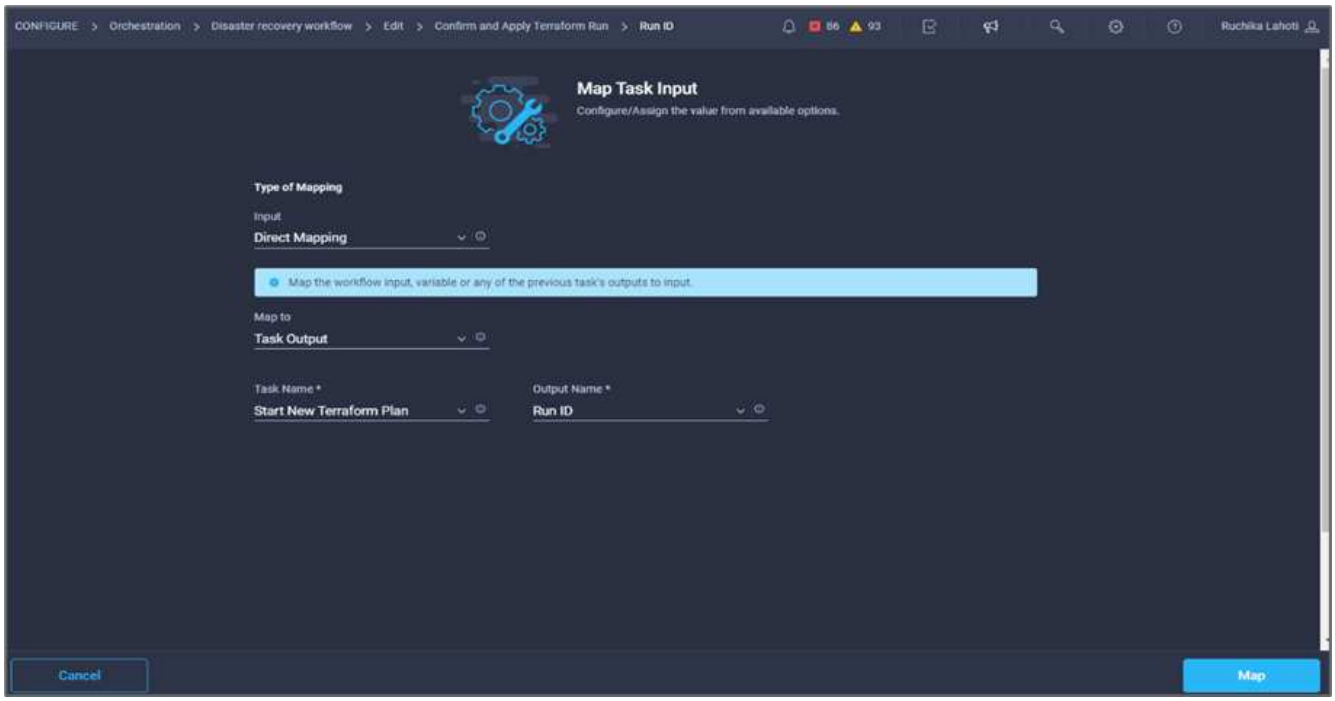
Damit ist die Schlafaufgabe abgeschlossen. Erstellen Sie als Nächstes die letzte Aufgabe dieses Workflows, indem Sie den Terraform-Lauf bestätigen und anwenden.

Prozedur 10: Terraform Run bestätigen und anwenden

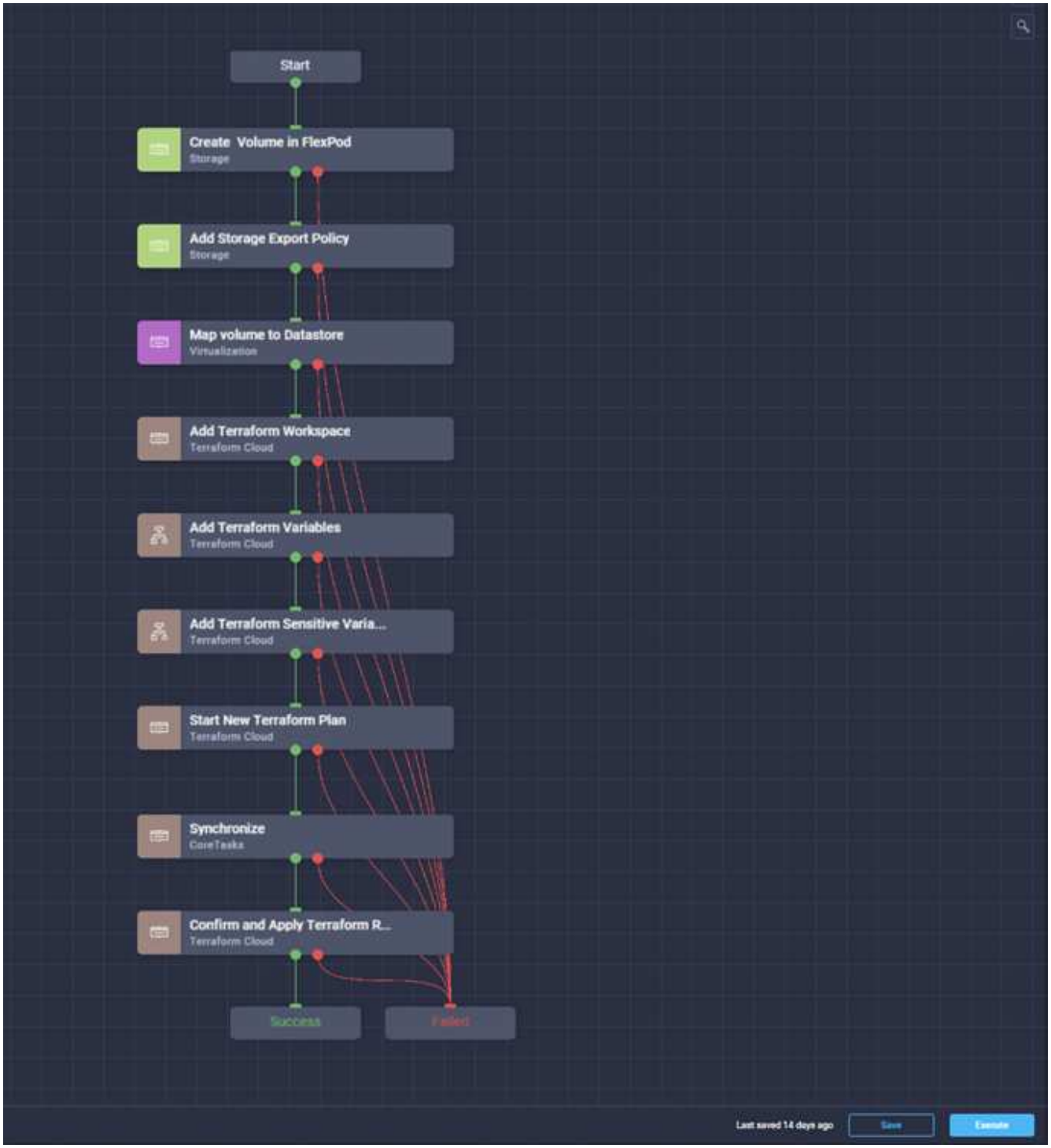
1. Gehen Sie zur Registerkarte **Designer** und klicken Sie im Abschnitt **Tools** auf **Tasks**.
2. Ziehen Sie die Aufgabe * Terraform Cloud > Bestätigen und anwenden Sie Terraform Run* aus dem Abschnitt **Tools** im Bereich **Design**.
3. Verwenden Sie den Anschluss, um die Aufgaben zu verbinden **Synchronisieren** 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.

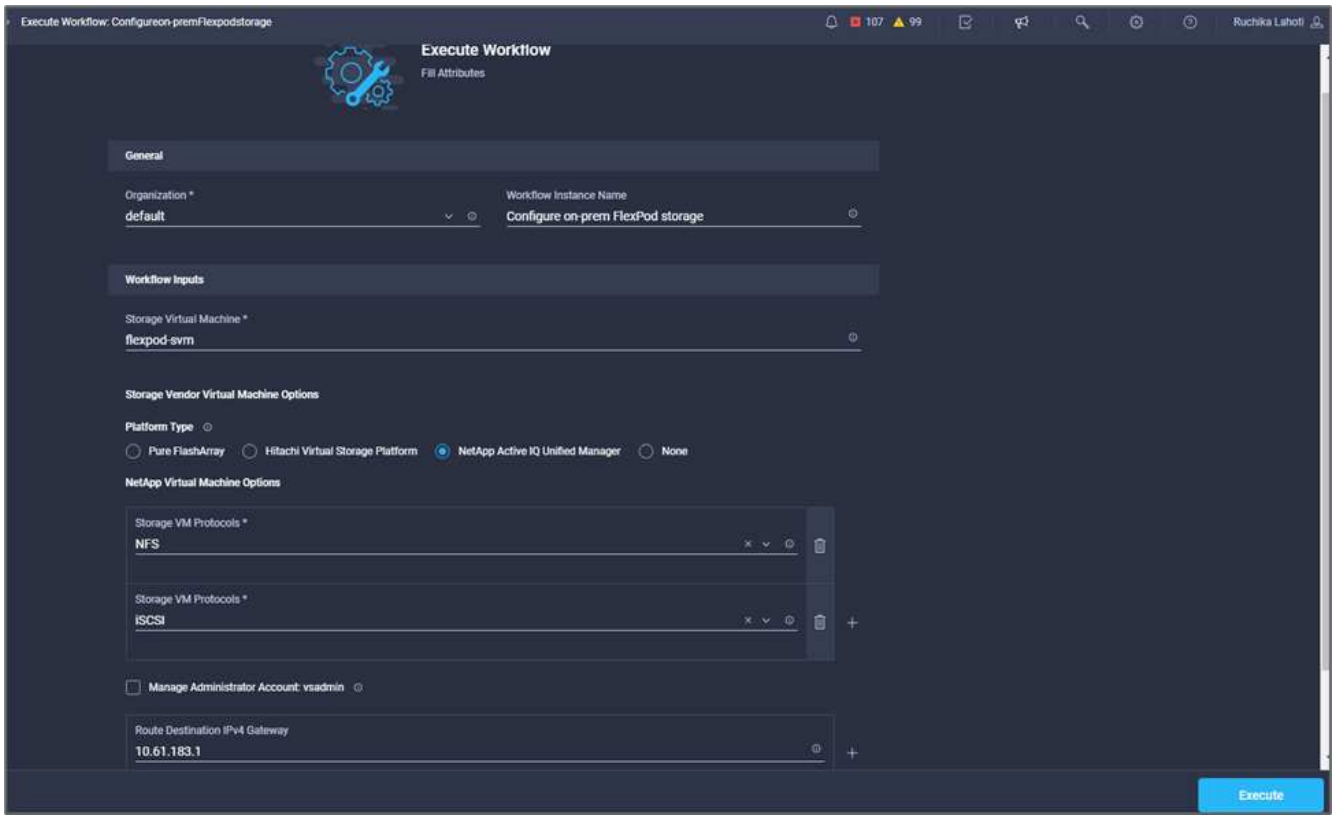
Die folgenden grundlegenden Schritte werden zur Überprüfung der Erfolgskriterien dieser Lösung herangezogen:

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.

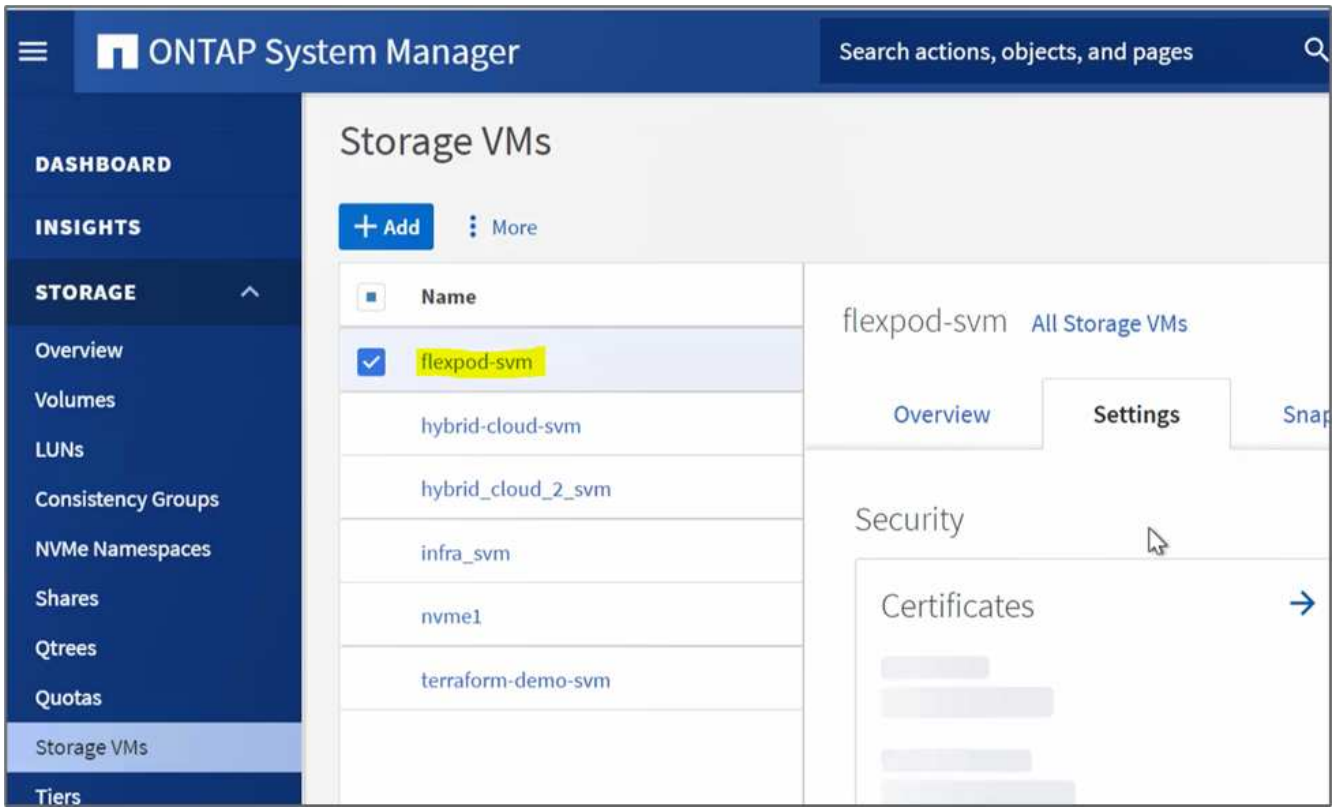
Um den lokalen Workflow auszuführen, gehen Sie wie folgt vor:

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

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

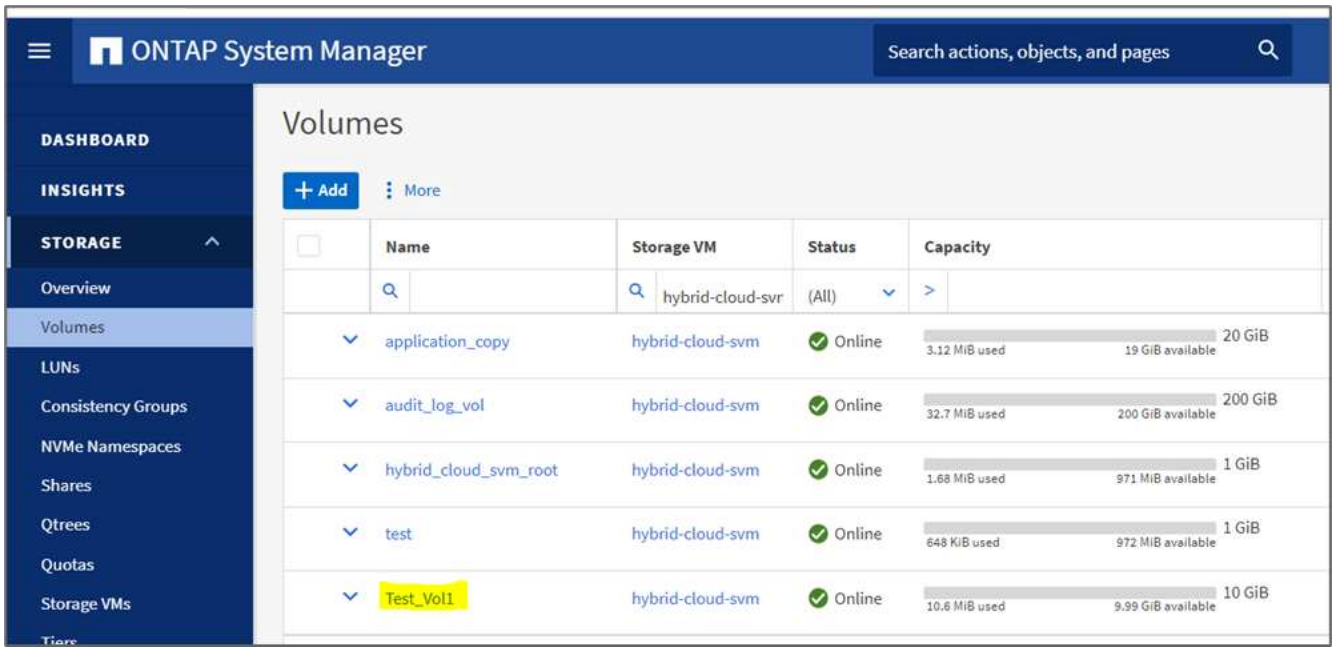


3. Überprüfen Sie die neu erstellte SVM im System Manager.



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.

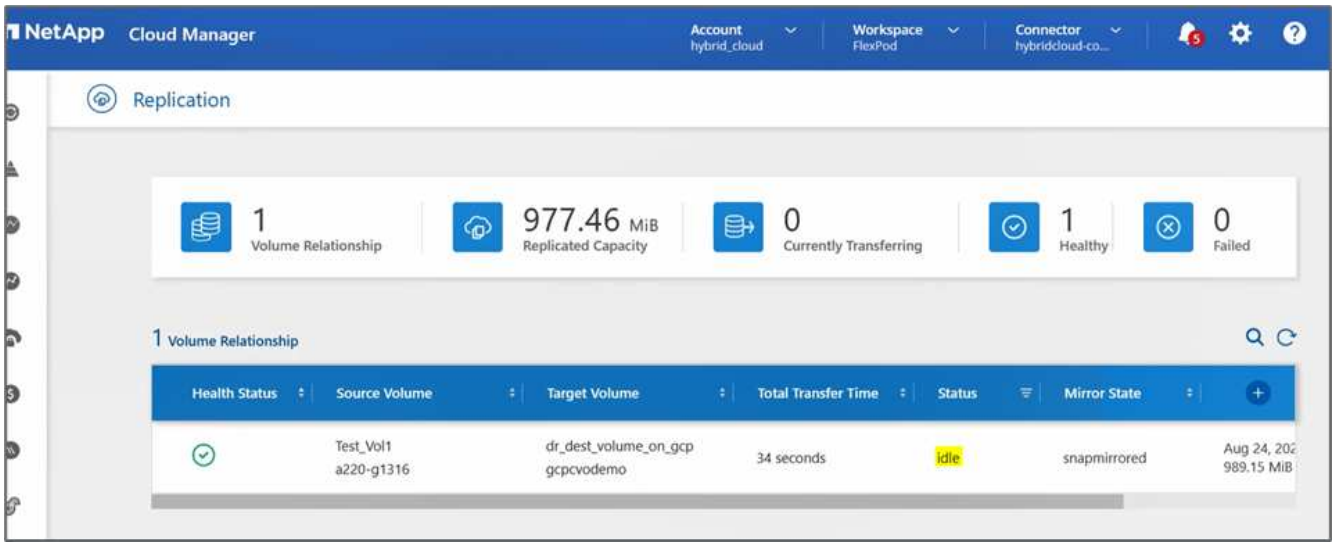


6. Mounten Sie dasselbe NFS-Volume auf eine lokale Virtual Machine, kopieren Sie dann den Beispieldatensatz und führen Sie die Prüfsumme durch.

```
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#
```

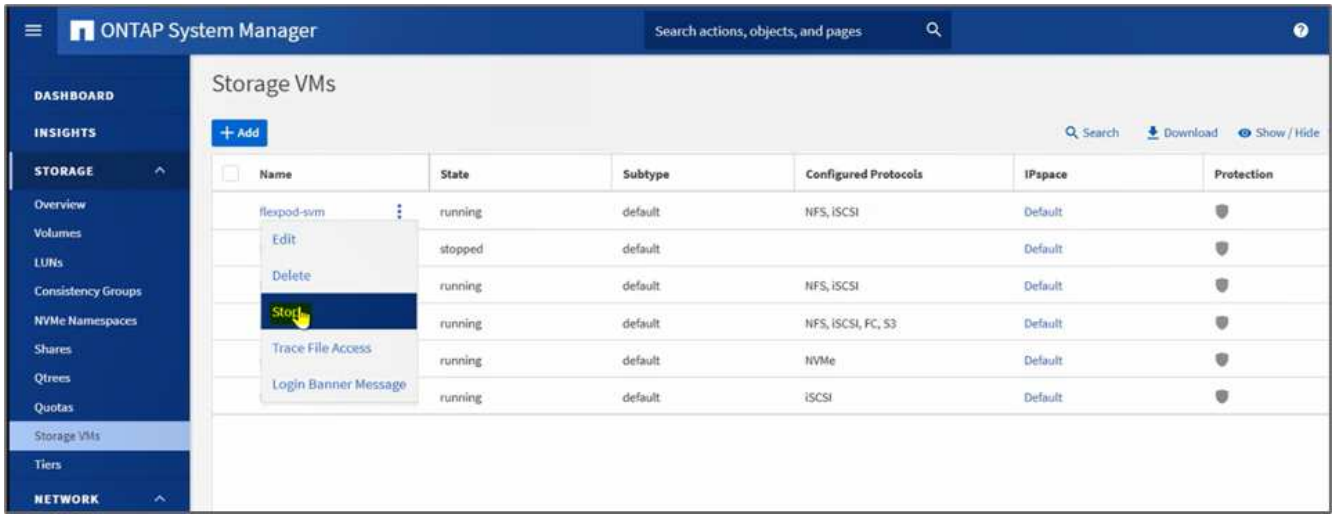
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

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.

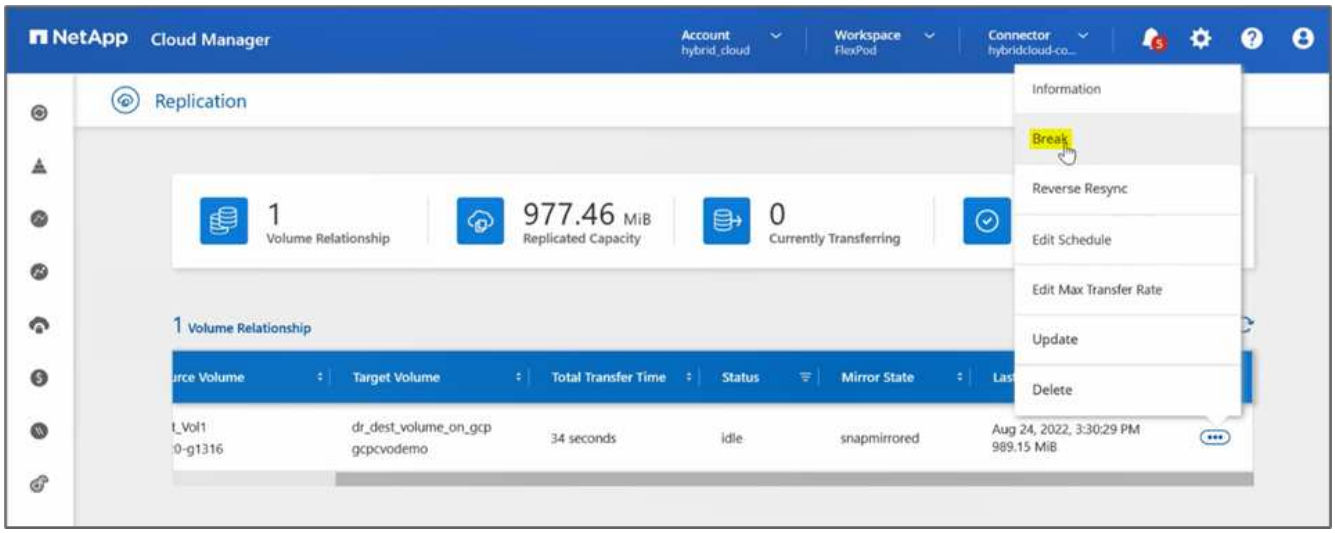


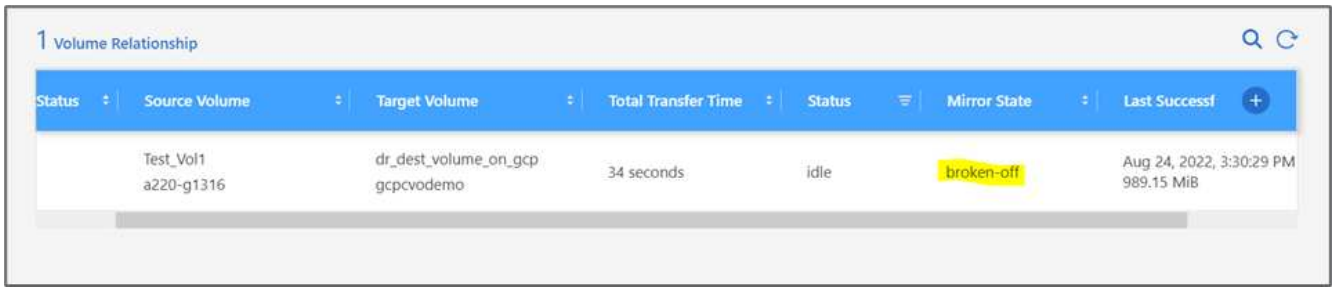
8. Wenn der Datentransfer abgeschlossen ist, simulieren Sie einen Notfall auf der Quellseite, indem Sie die SVM, die den hostet, anhalten `Test_vol1` Datenmenge:

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

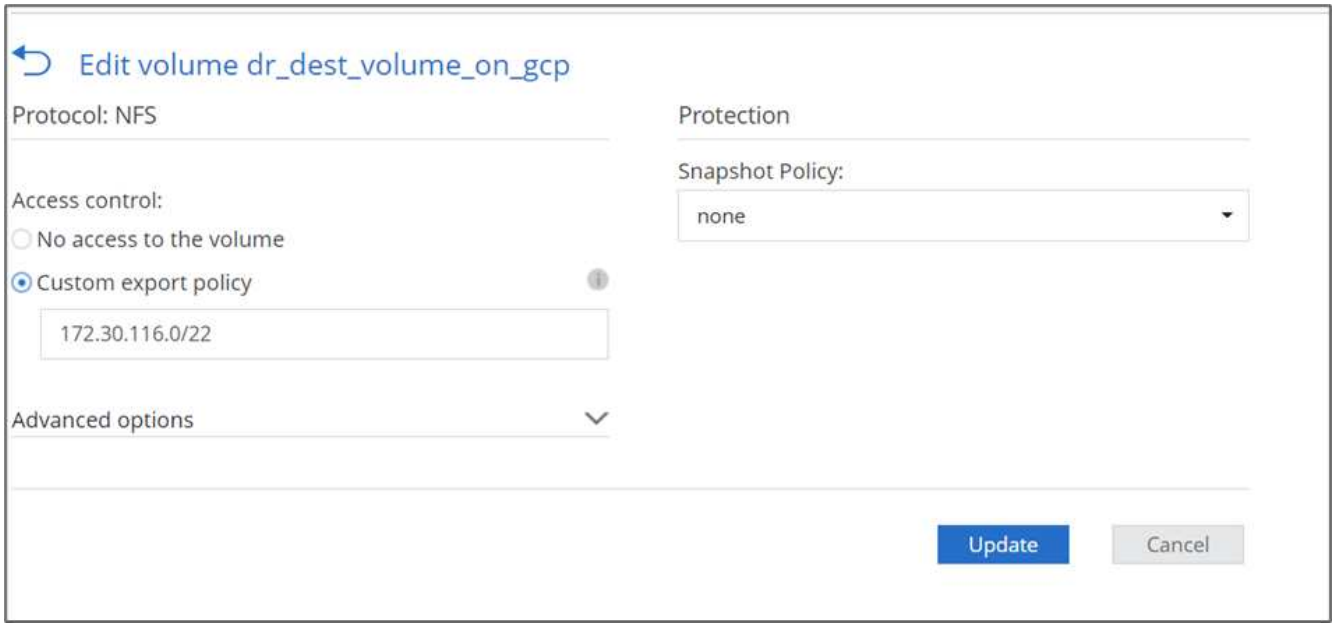


9. Replizierungsbeziehung wird zerbrechen und das Cloud Volumes ONTAP Ziel-Volume zur Produktion heraufstufen.

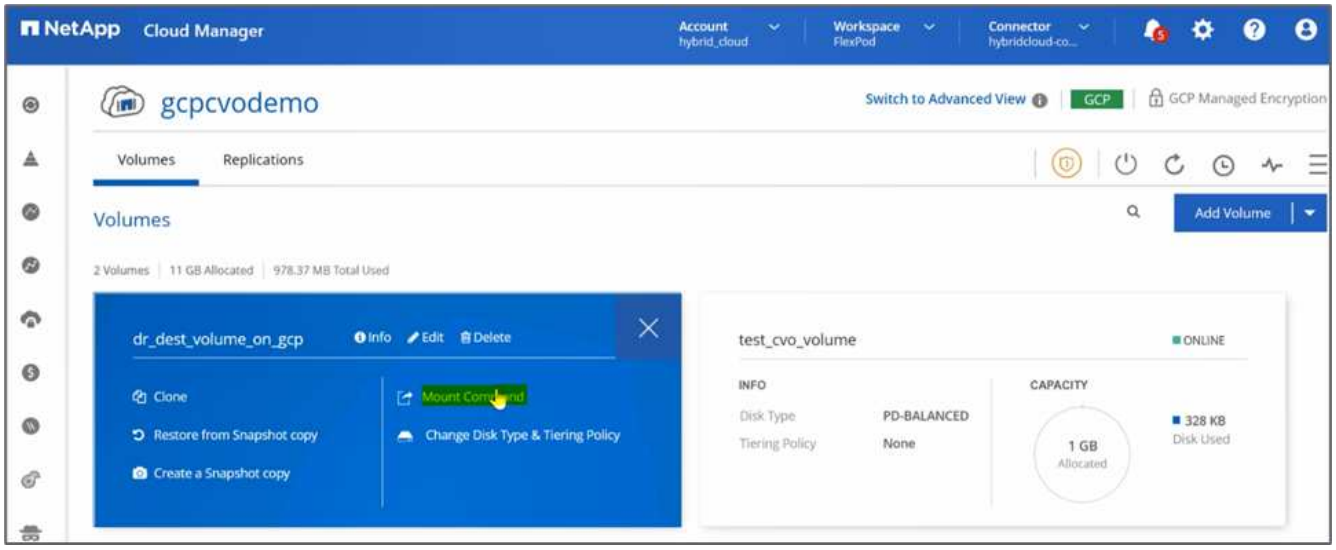




10. Bearbeiten Sie das Volume, und aktivieren Sie den Client-Zugriff, indem Sie es mit einer Exportrichtlinie verknüpfen.



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

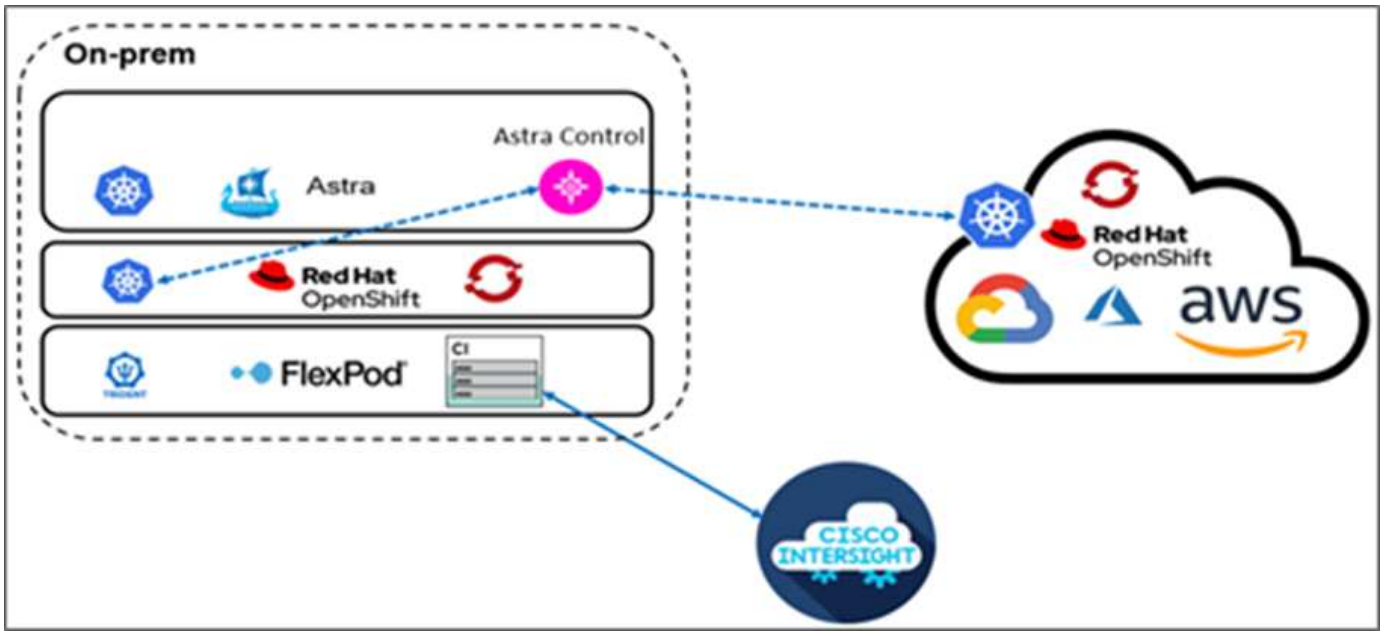
Abhinav Singh

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

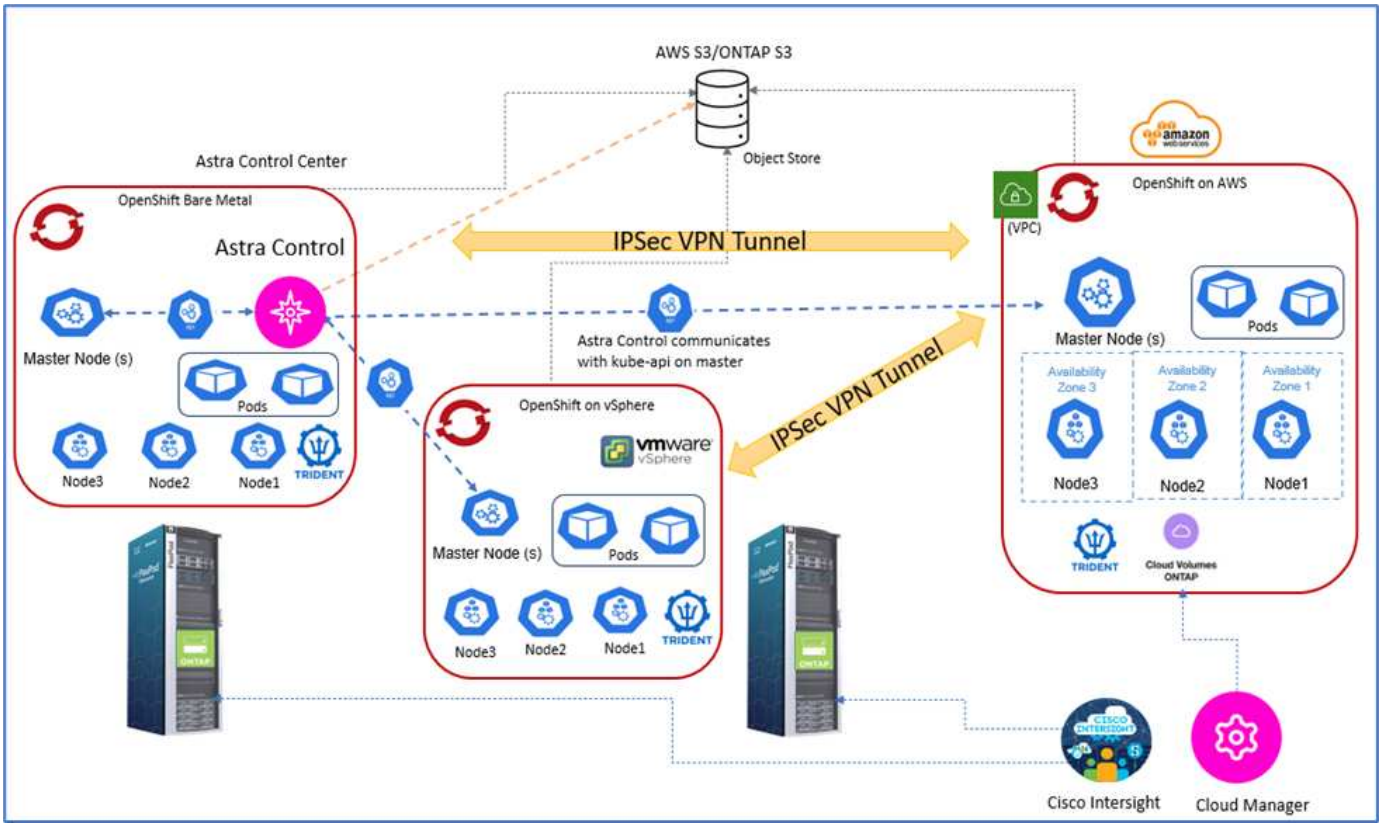
NetApp Astra Control möchte Kunden, die sich mit Cloud-nativen Microservices befassen, die Datensicherung vereinfachen:

- **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.

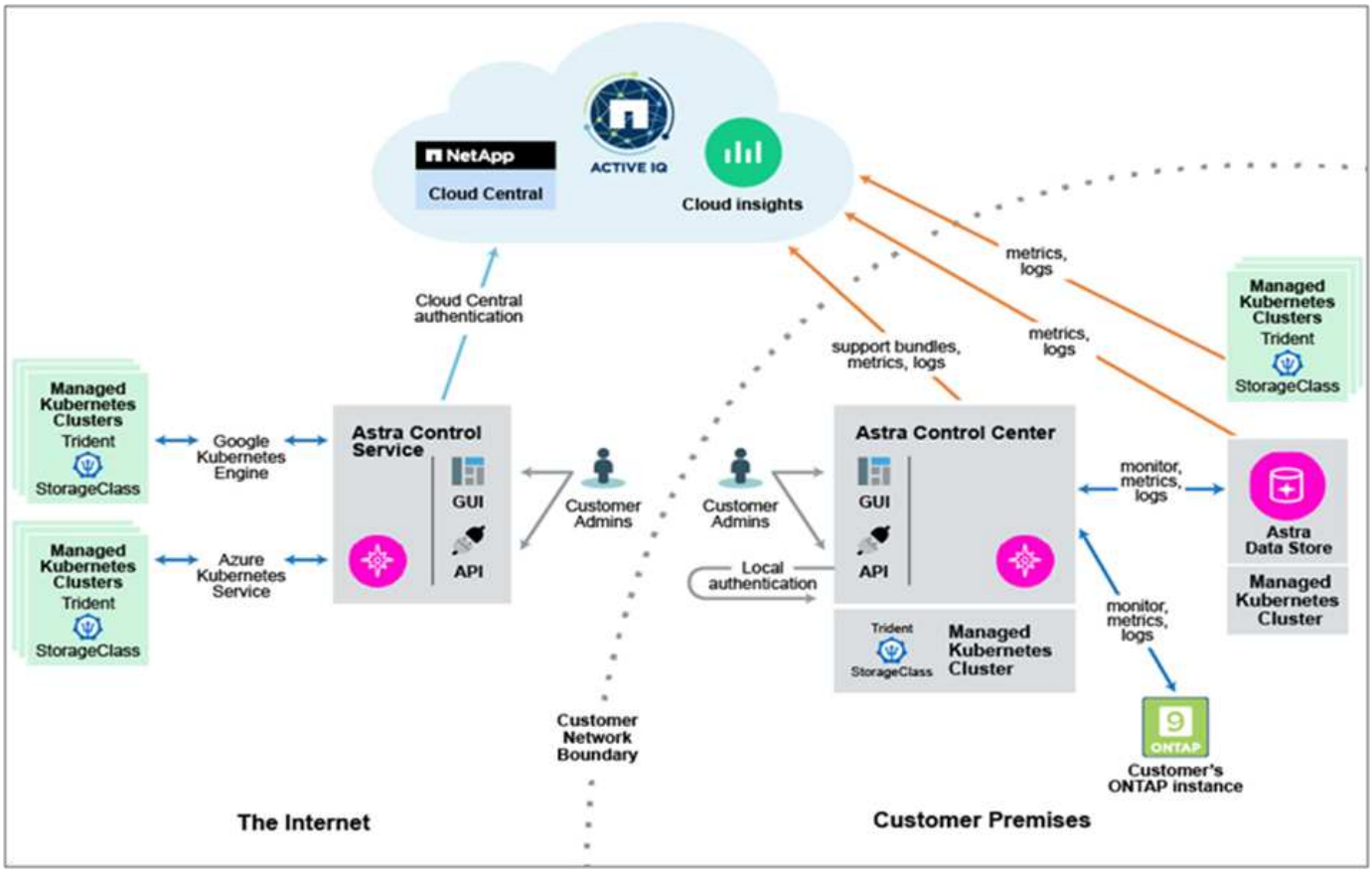
Astra Control Nutzungsmodelle

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:

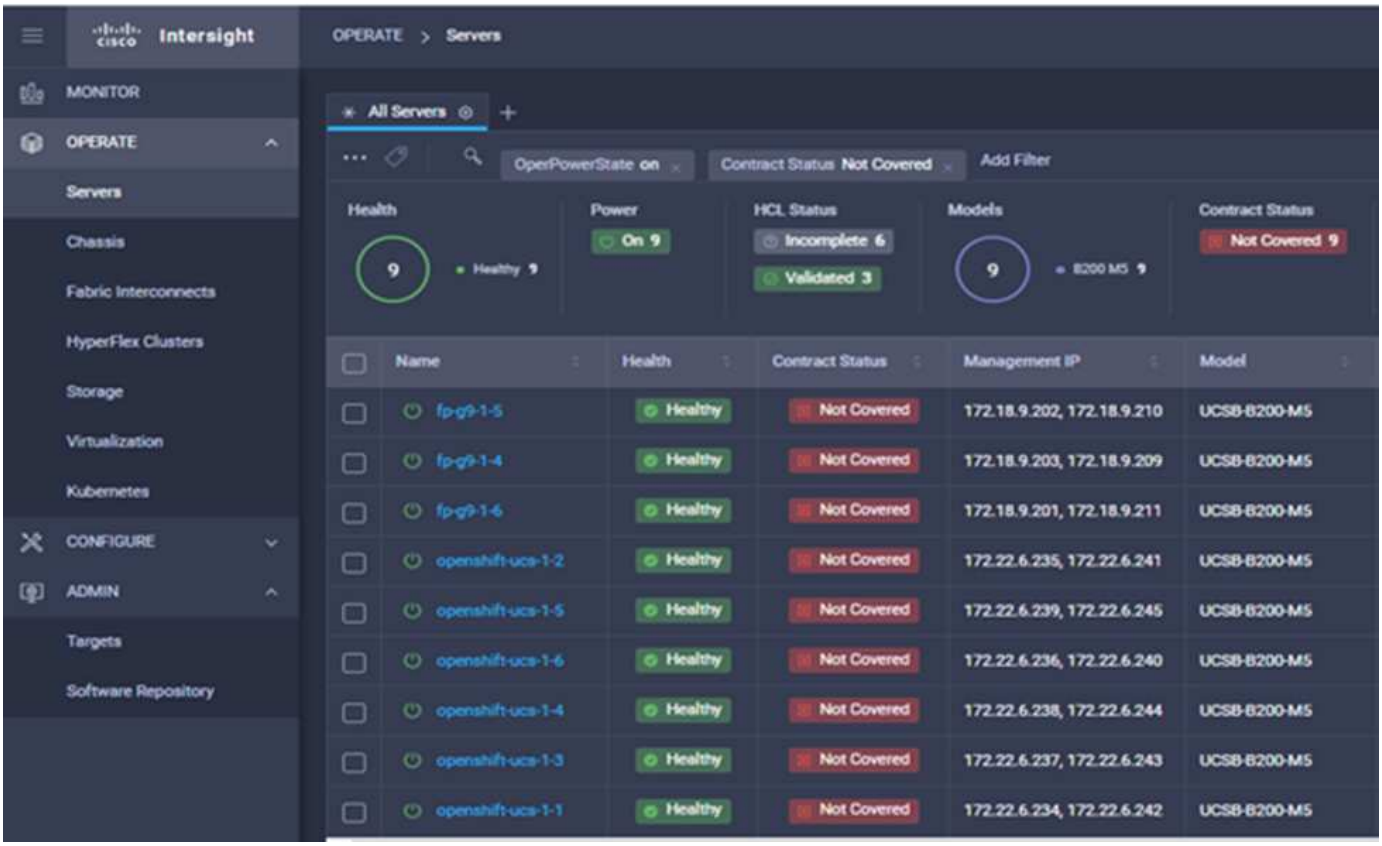
- **Schnellere Lieferung.** als Service aus der Cloud oder im Rechenzentrum des Kunden mit häufigen Updates und fortgesetzten Innovationen durch ein agiles, auf Software basierendes Entwicklungsmodell geliefert. So kann sich der Kunde ganz einfach darauf konzentrieren, die Bereitstellung für den Geschäftsbereich 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.



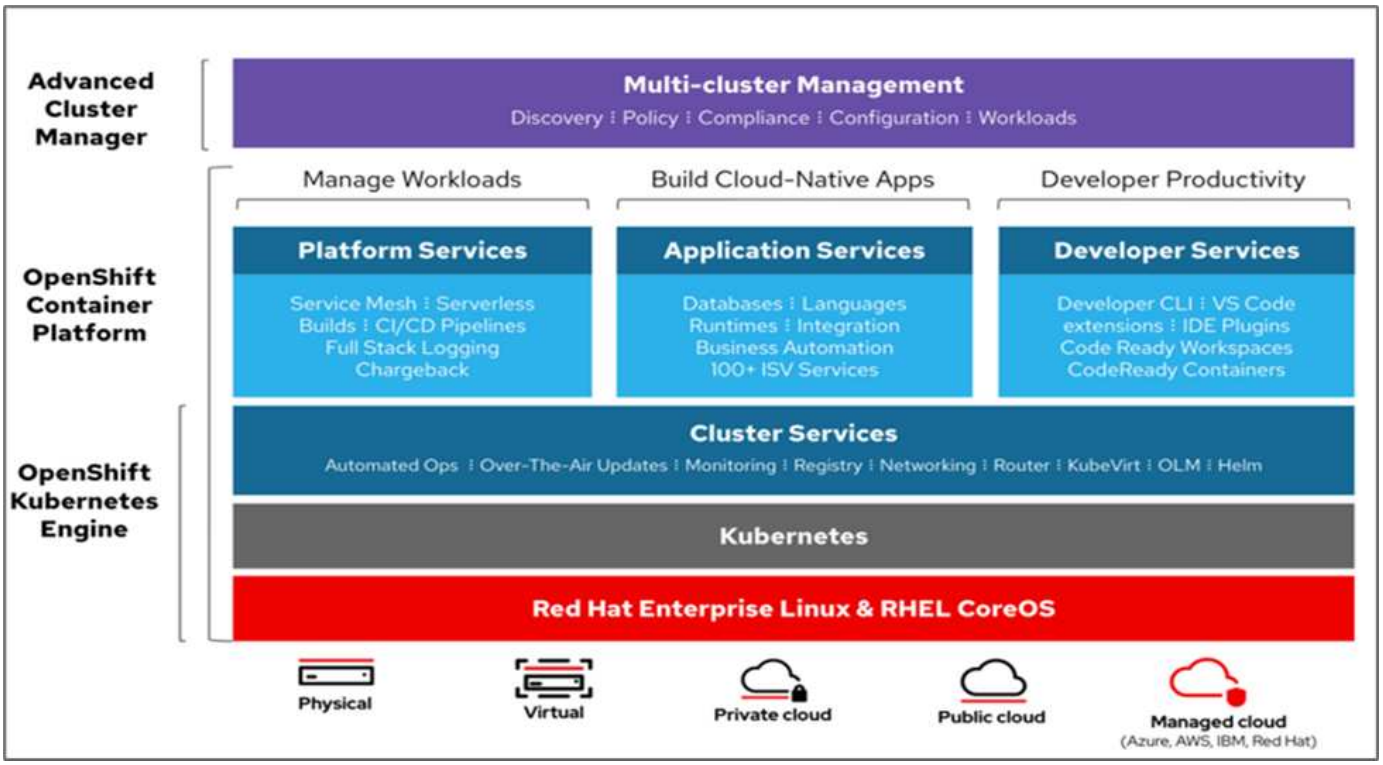
Red hat OpenShift Container Platform

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."

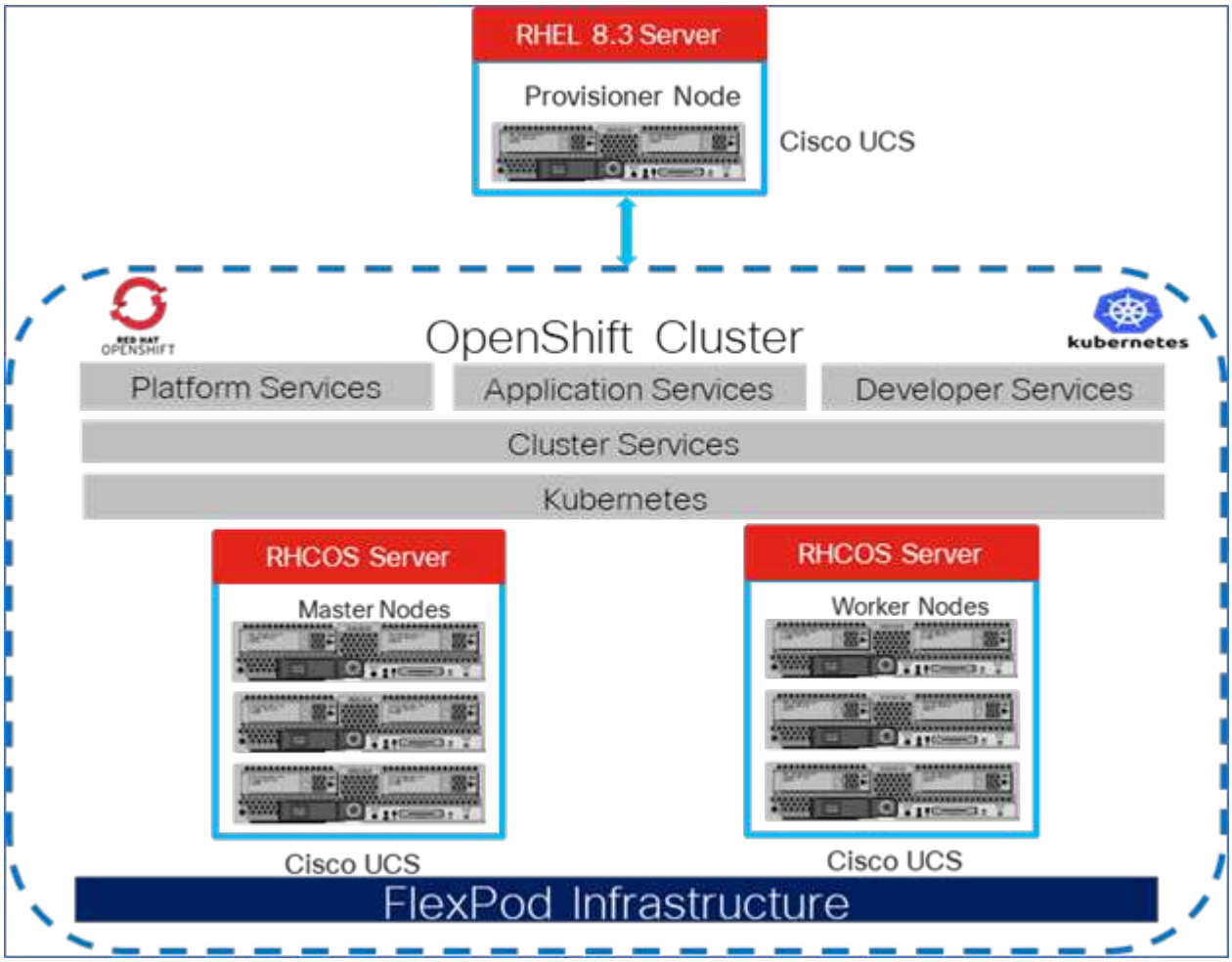
Installation und Konfiguration

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

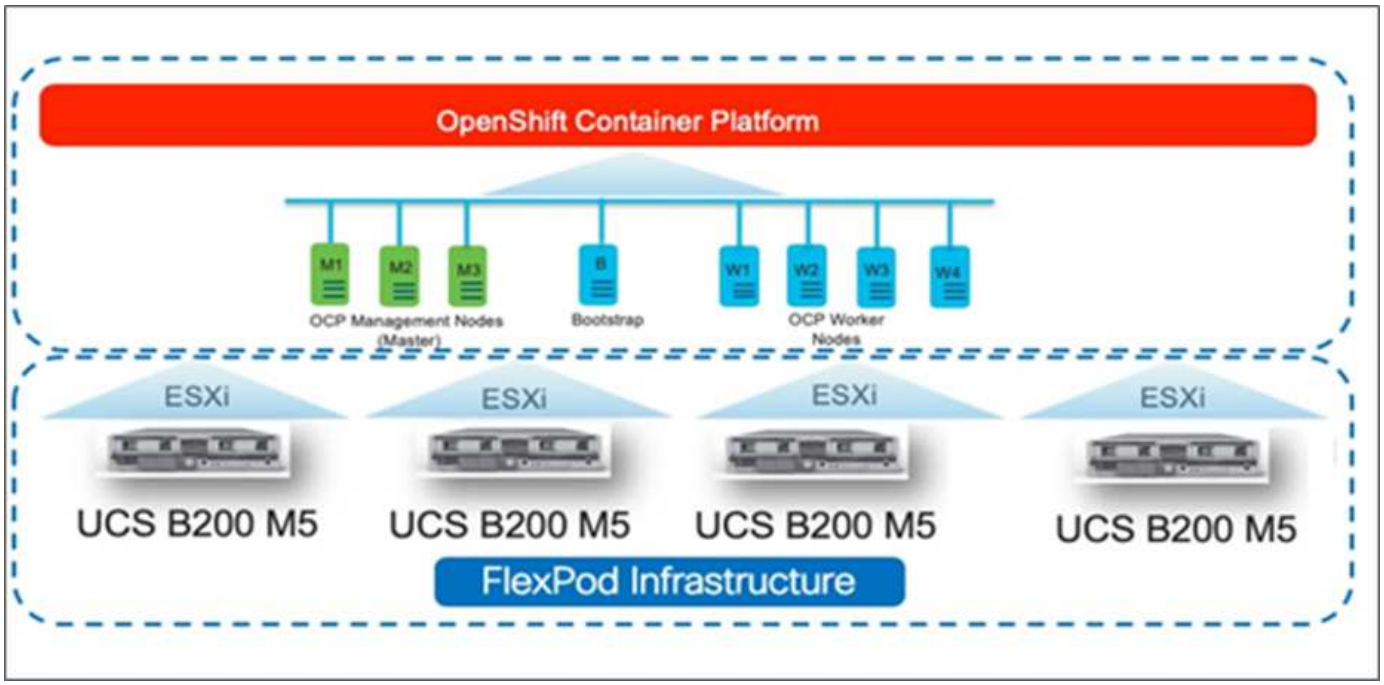
Die folgende Abbildung zeigt OpenShift Container Platform 4 Bare Metal auf FlexPod.



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.

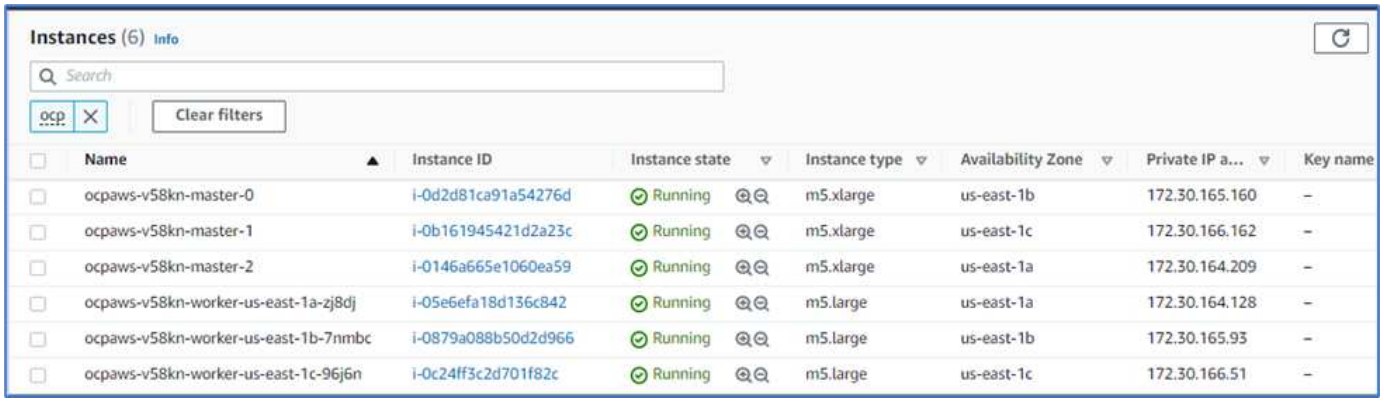


"Nächste Frage: Red hat OpenShift auf AWS"

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.

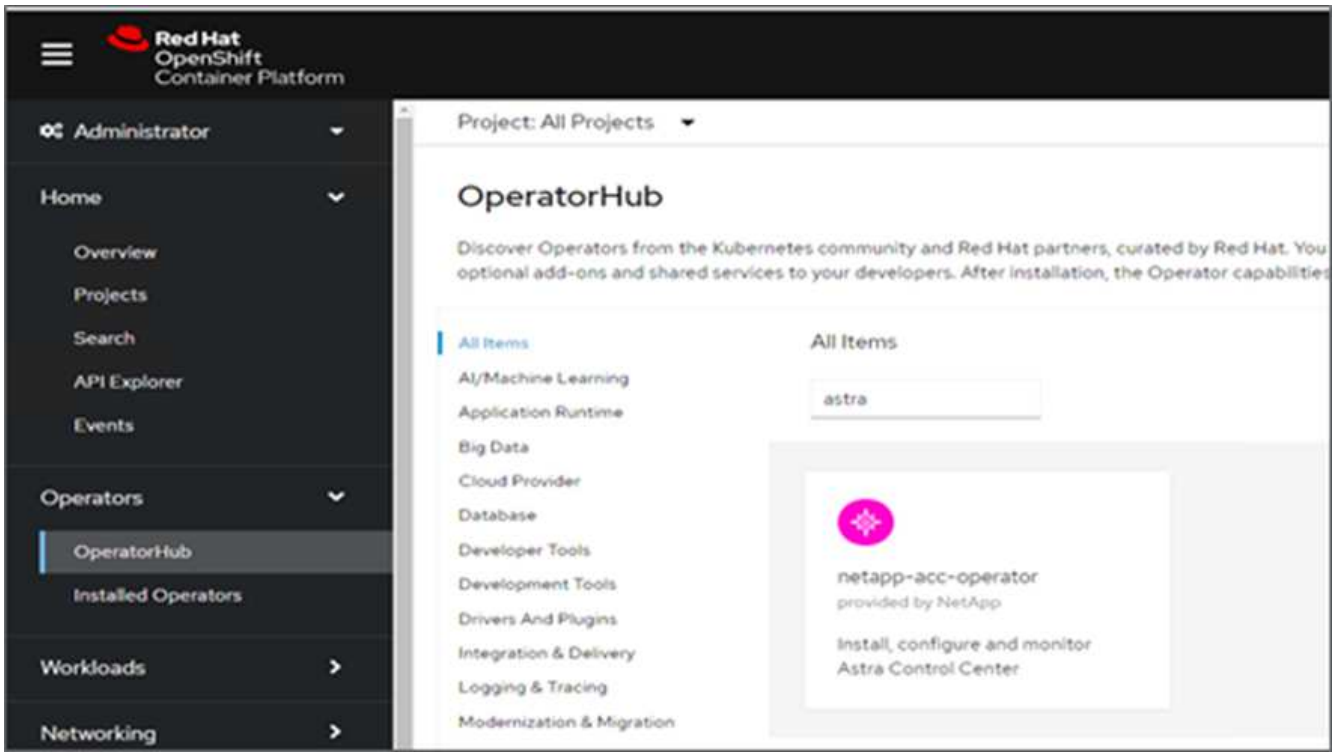
   Für Docker:

```
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:

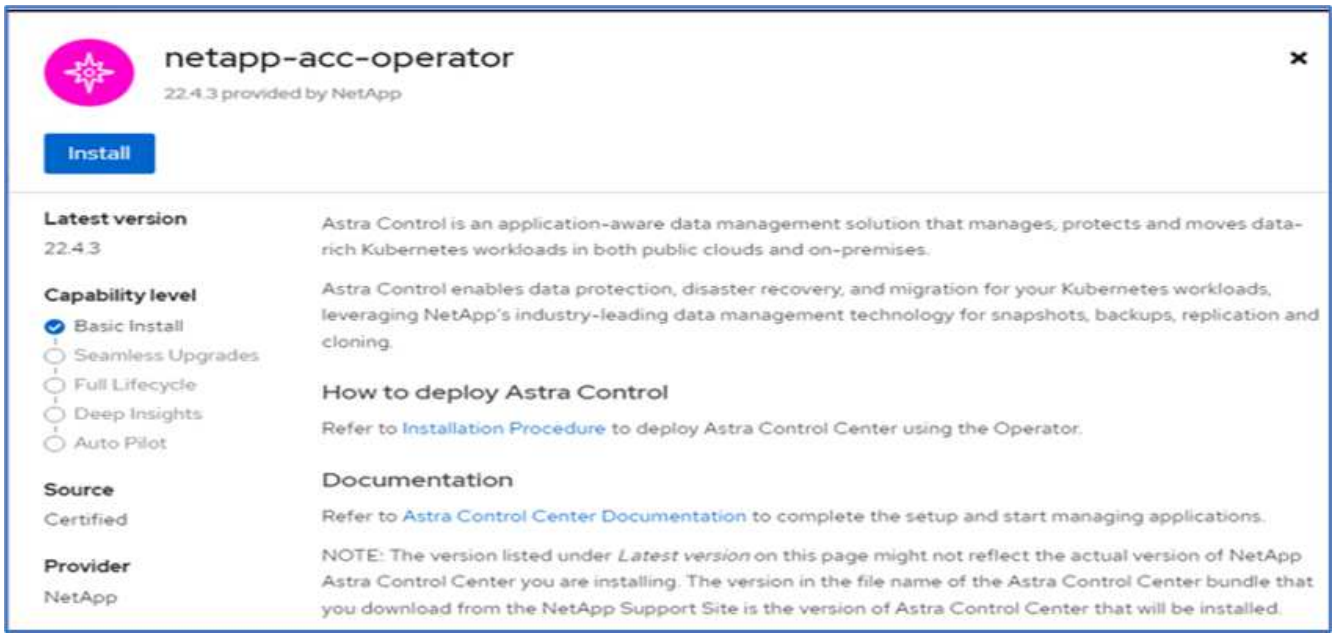
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed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

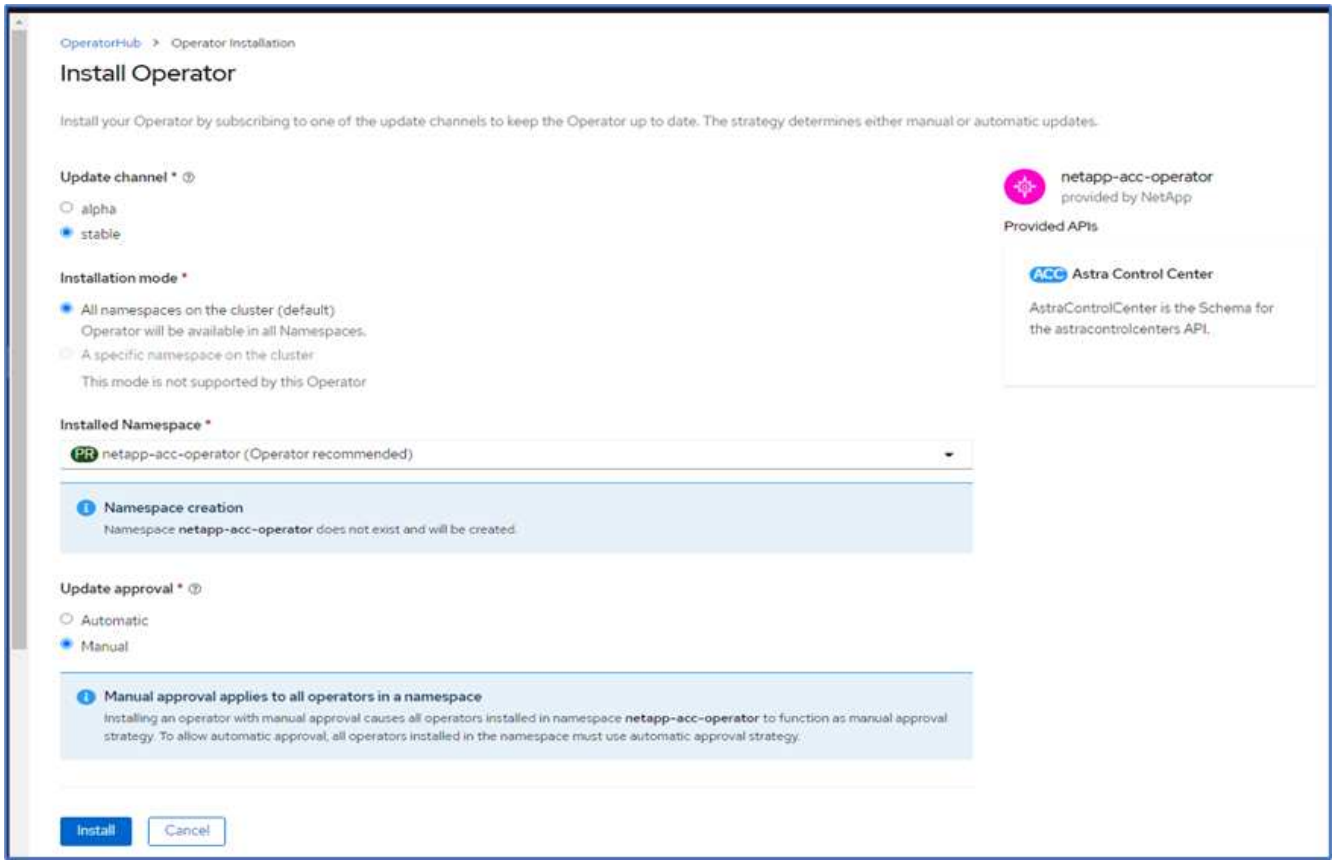


`netapp-acc-operator` Ist ein zertifizierter Red hat OpenShift Operator und ist im OperatorHub-Katalog aufgeführt.

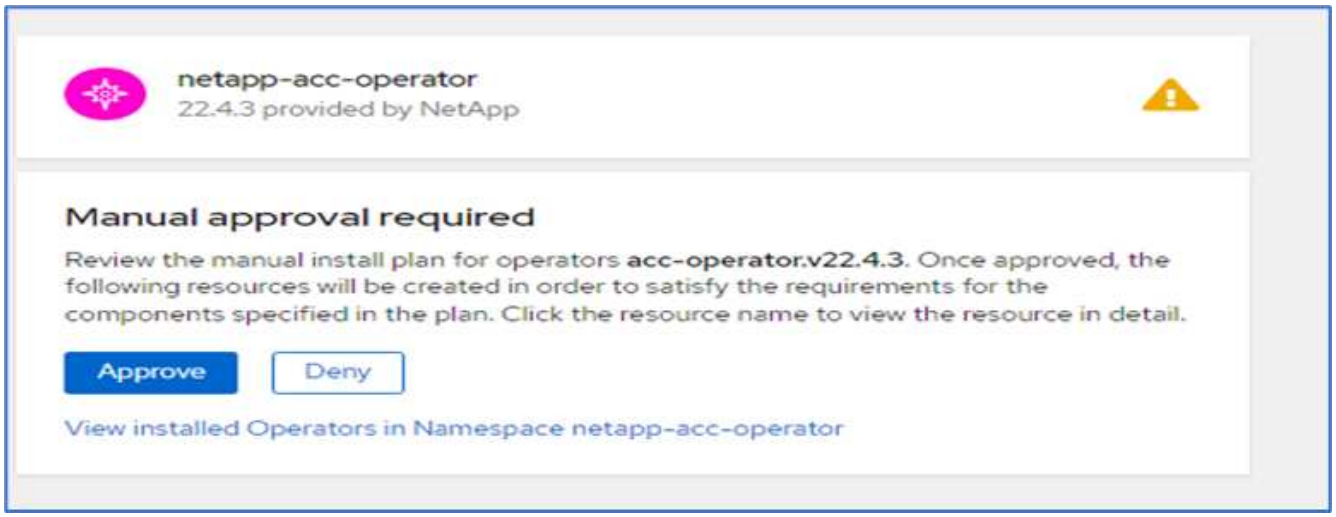
9. Wählen Sie `netapp-acc-operator` Und klicken Sie auf Installieren.



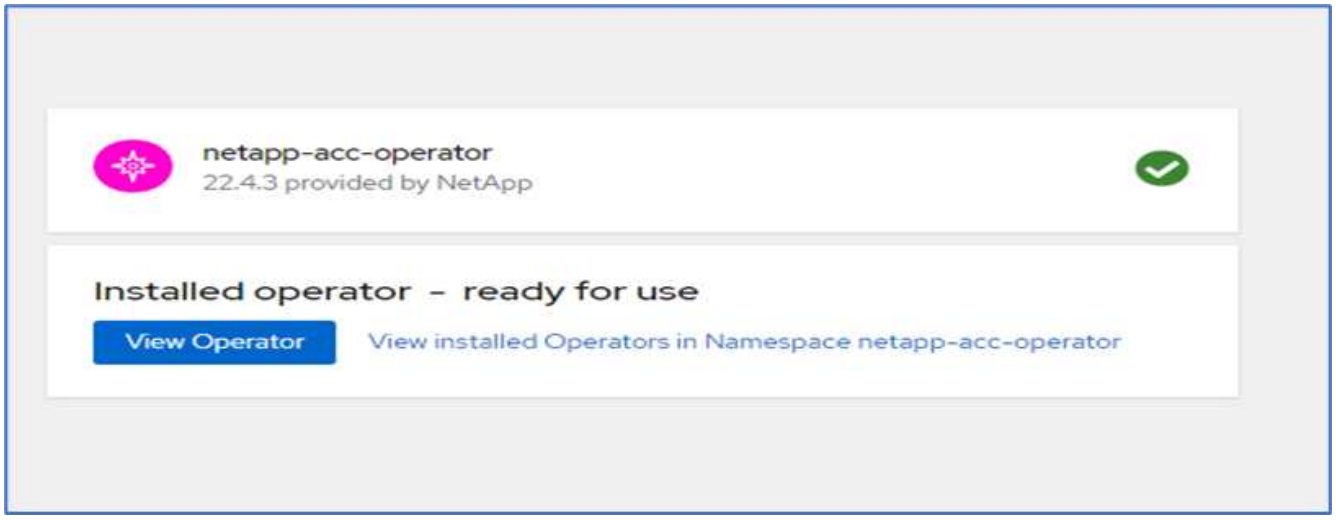
10. Wählen Sie die entsprechenden Optionen aus, und klicken Sie auf Installieren.



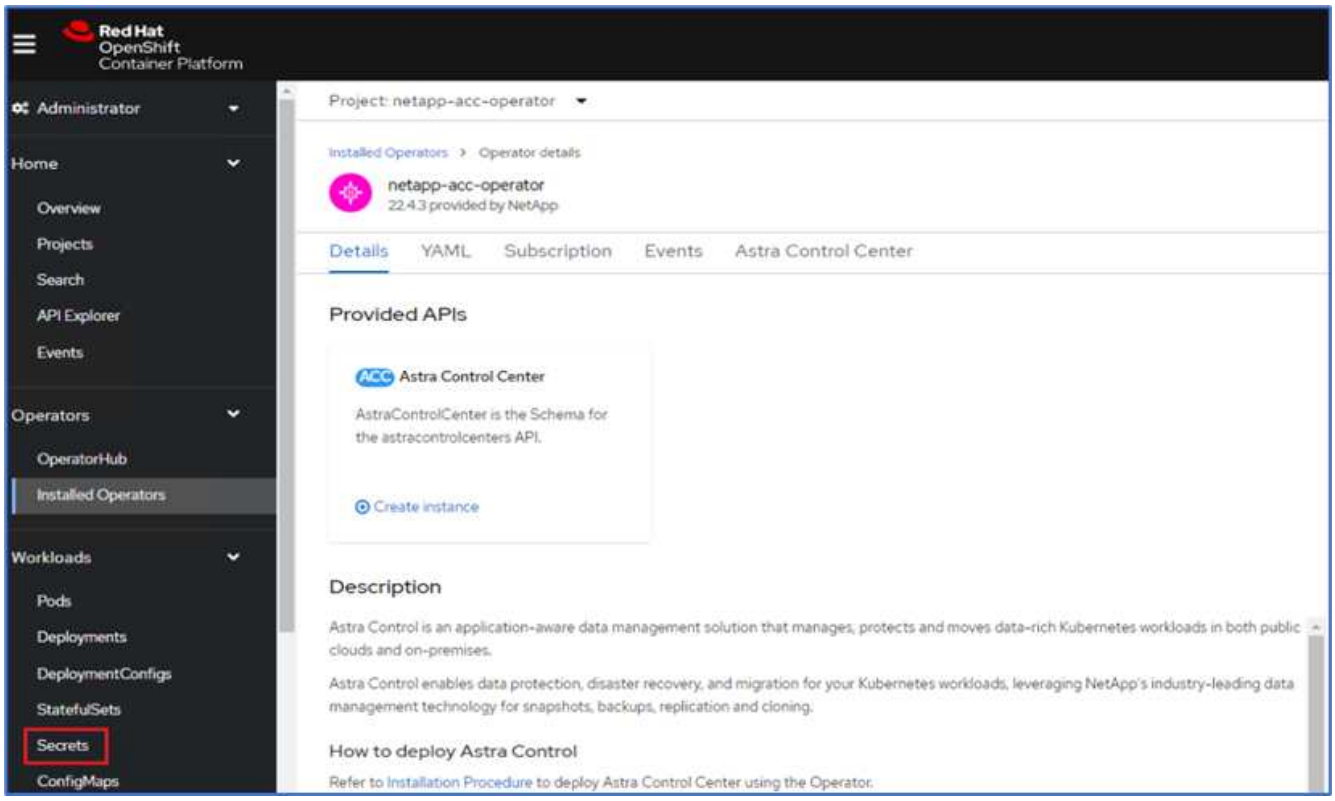
11. Genehmigen Sie die Installation, und warten Sie, bis der Bediener installiert ist.



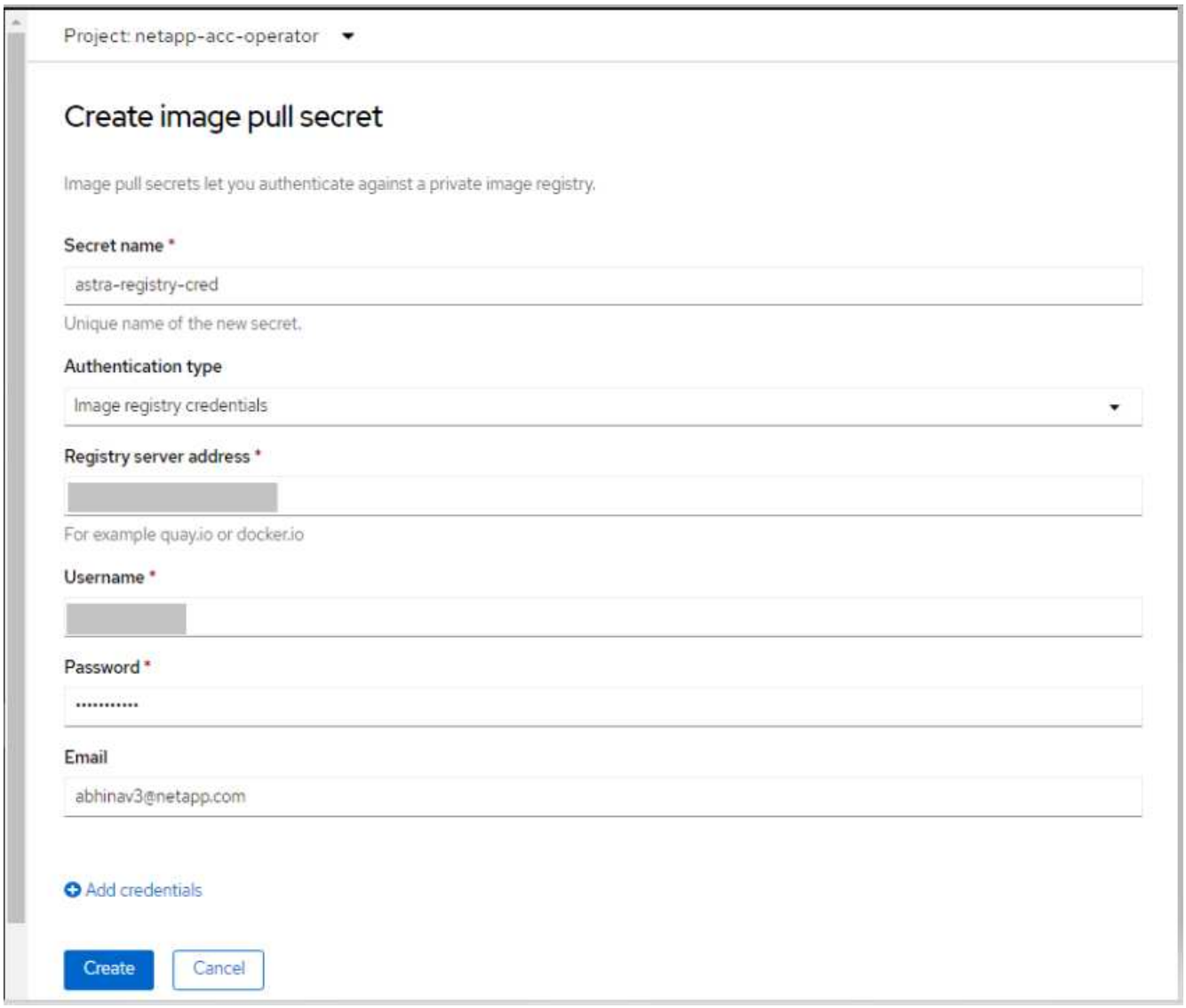
12. In dieser Phase ist der Bediener erfolgreich installiert und betriebsbereit. Klicken Sie auf Ansichtsverwalter, um die Installation des Astra Control Centers zu starten.



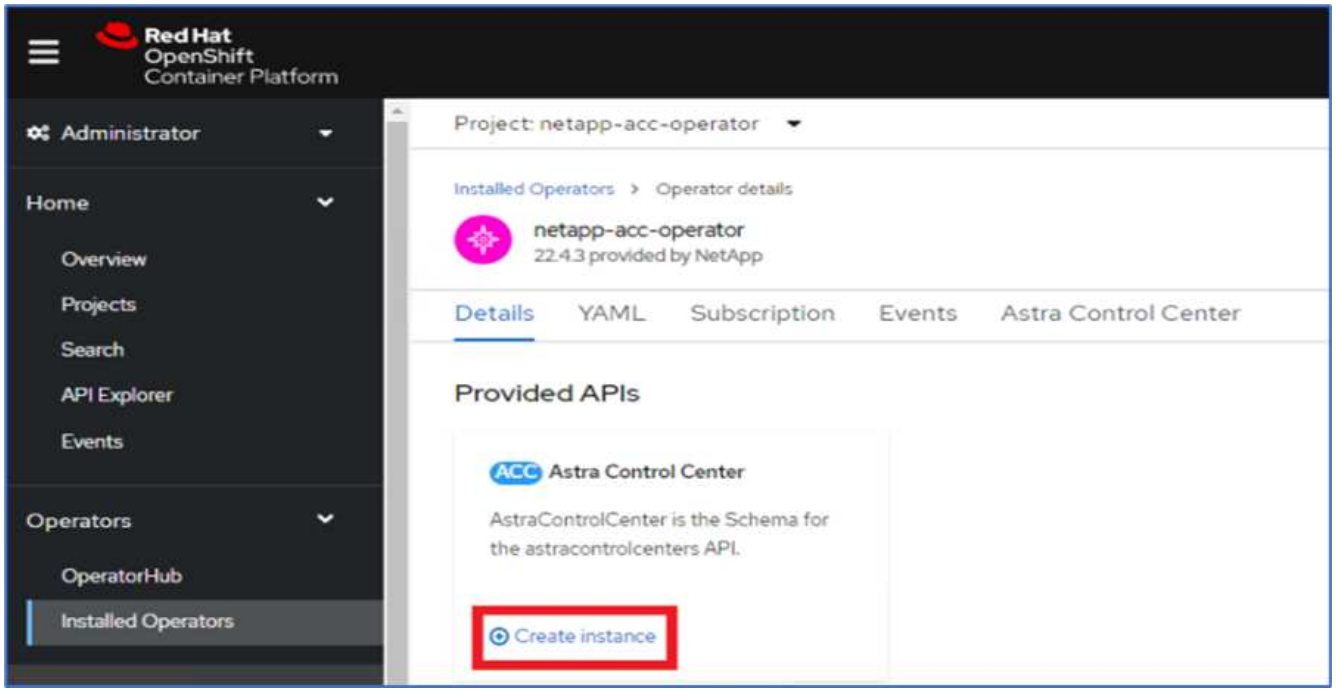
13. Erstellen Sie vor der Installation von Astra Control Center das Pull Secret, um Astra-Bilder aus der Docker-Registry, die Sie früher verschoben haben, herunterzuladen.



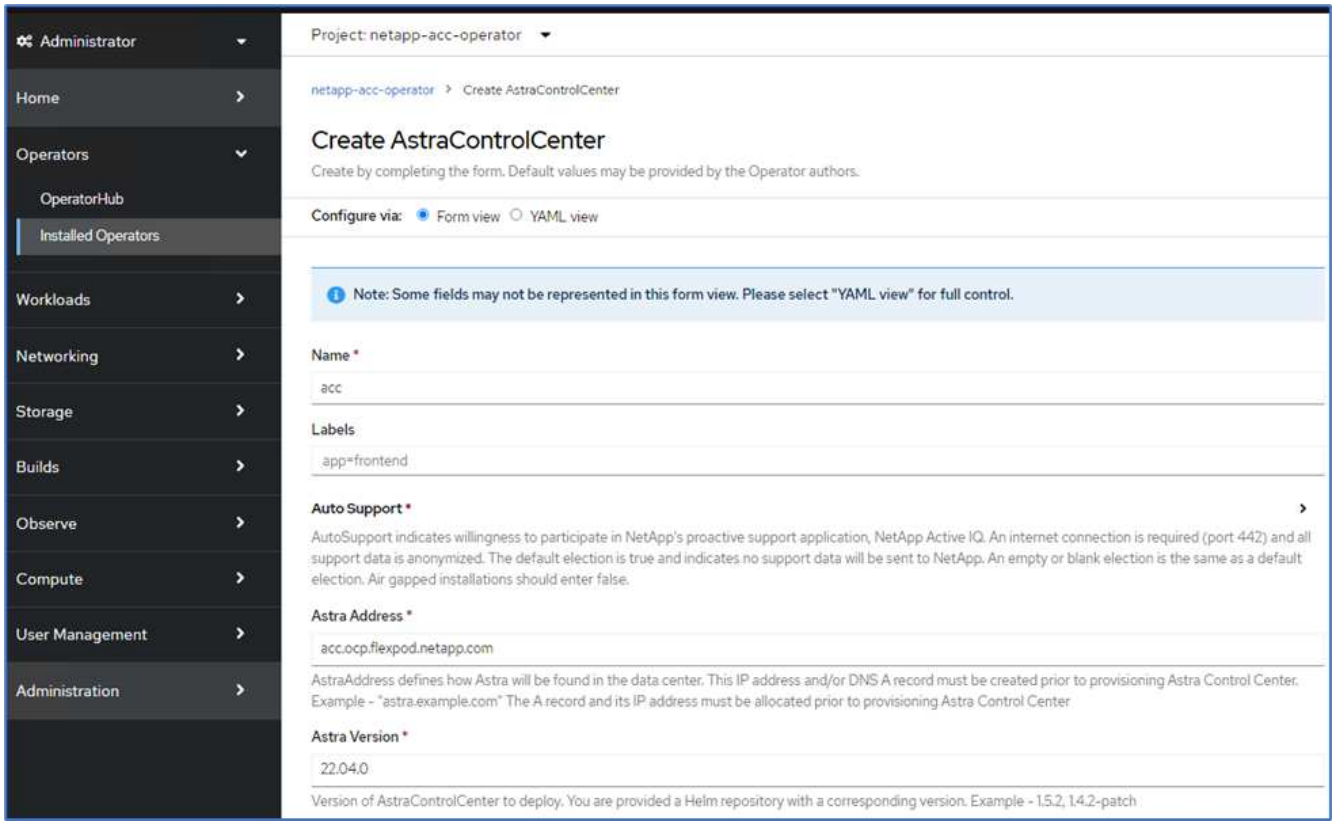
14. Damit Sie die Astra Control Center-Bilder von Ihrer privaten Docker-Repo abrufen können, sollten Sie im ein Geheimnis schaffen `netapp-acc-operator` Namespace. Dieser geheime Name wird in einem späteren Schritt im Astra Control Center YAML-Manifest angegeben.



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



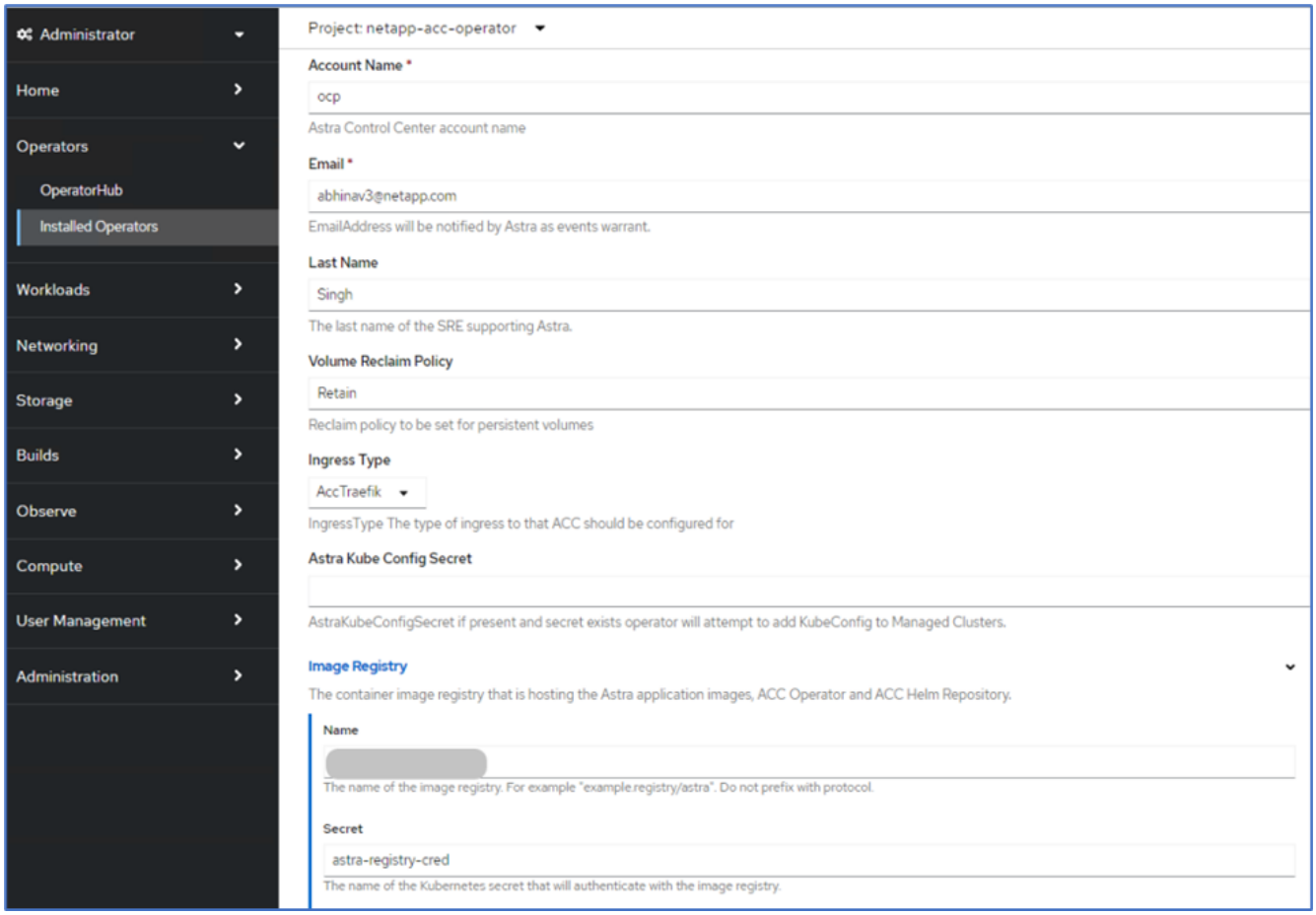
16. Füllen Sie das Formular AstraControlCenter erstellen aus. Geben Sie den Namen, die Astra-Adresse und die Astra-Version an.



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.

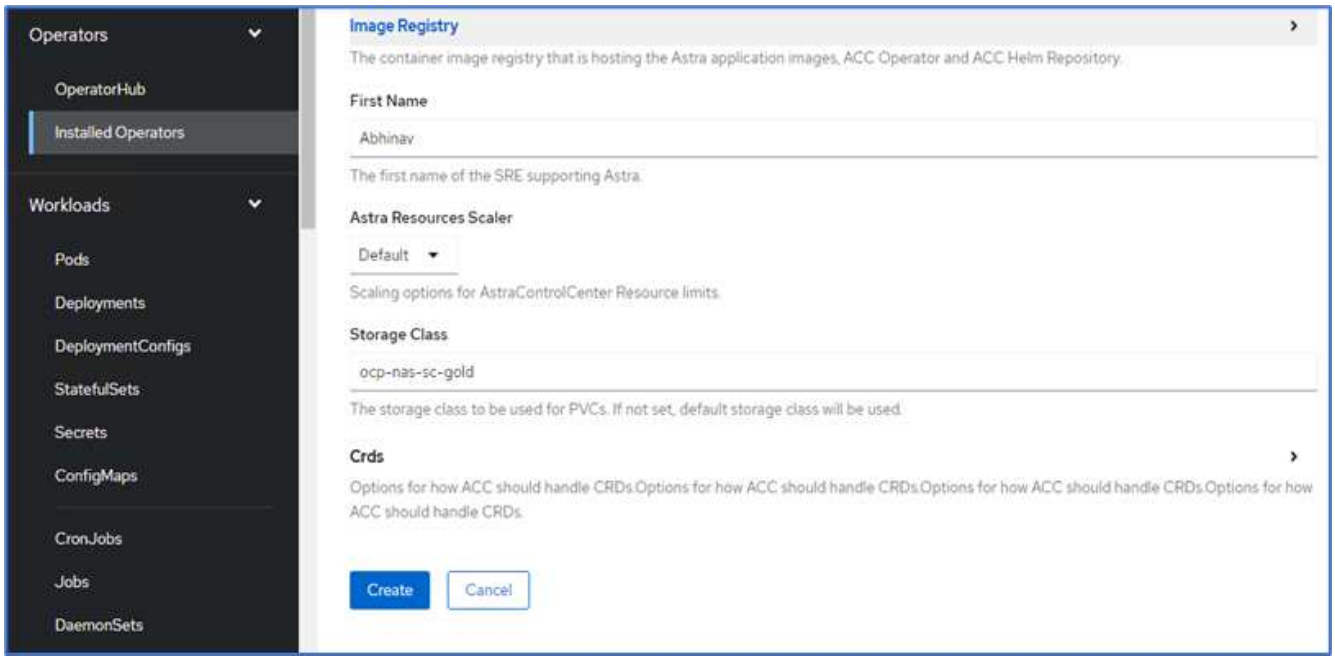
17. Geben Sie einen Kontonamen, eine E-Mail-Adresse, einen Administrator-Nachnamen ein, und behalten

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.

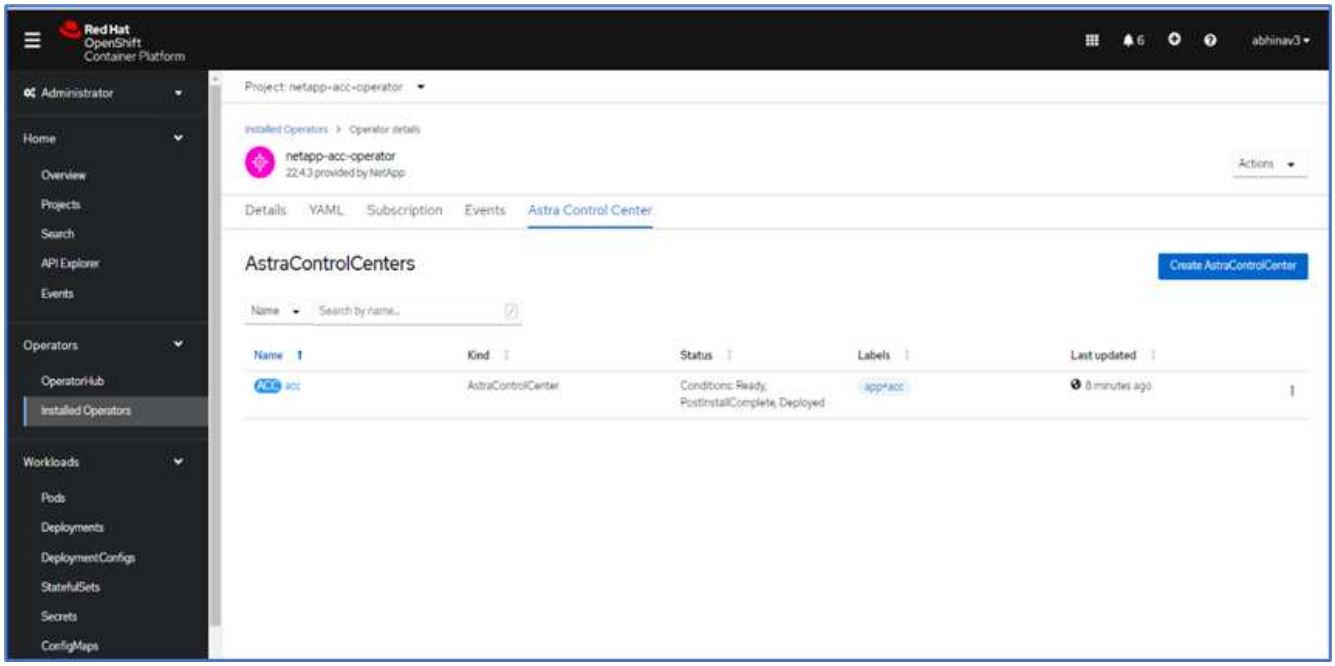


In dieser Lösung wird der Metallb Load Balancer eingesetzt. Daher ist der Eingangstyp AccTraefik. Das Astra Control Center Trafik Gateway wird damit als Kubernetes Service des Typ Load Balancer bereitgestellt.

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
```

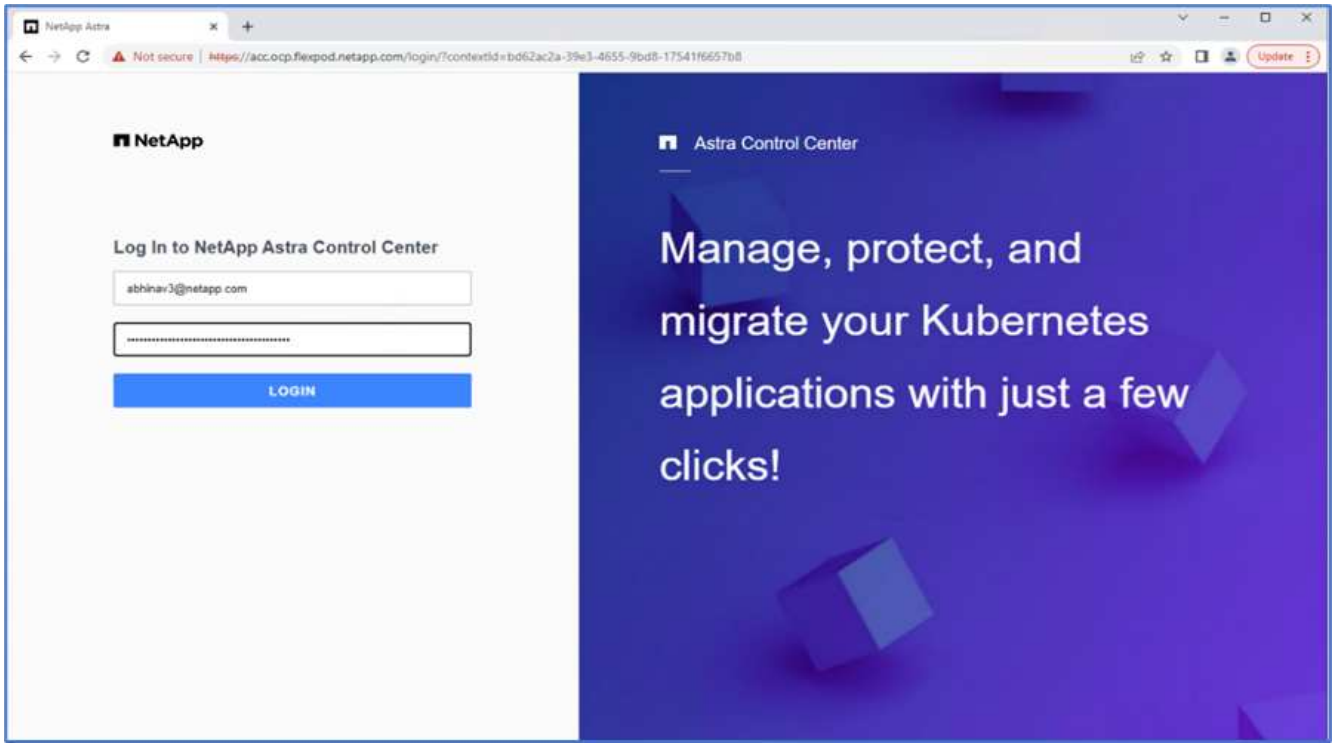
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
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]).

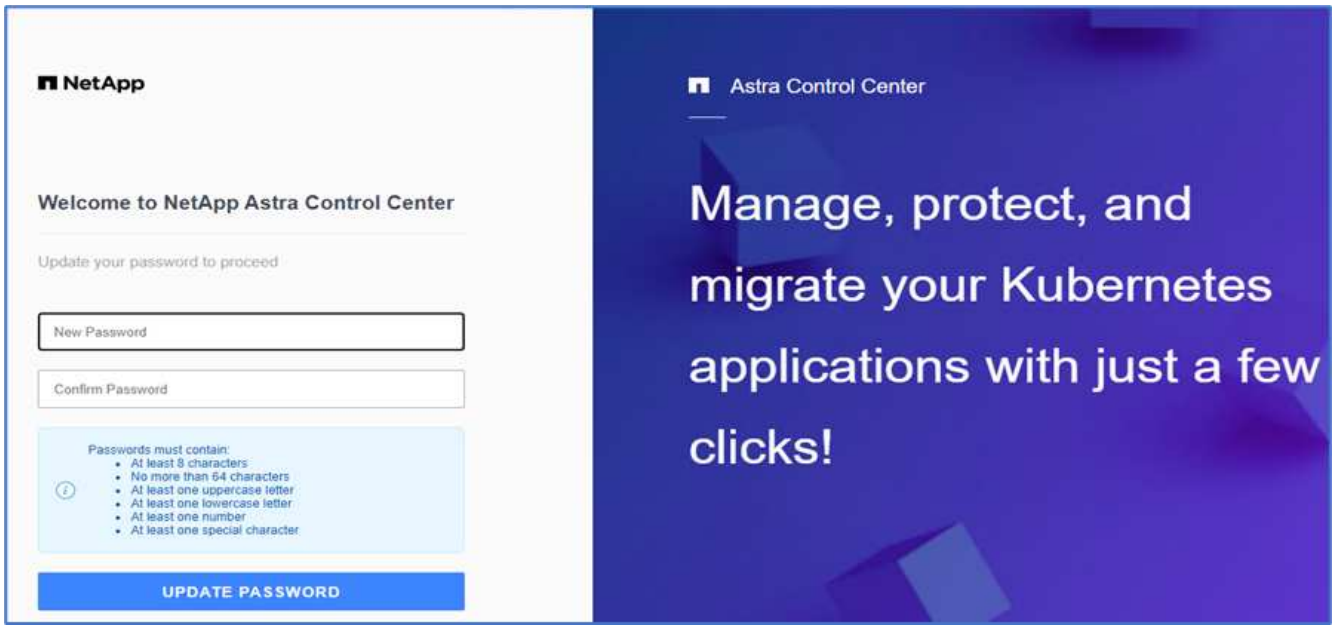
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

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.

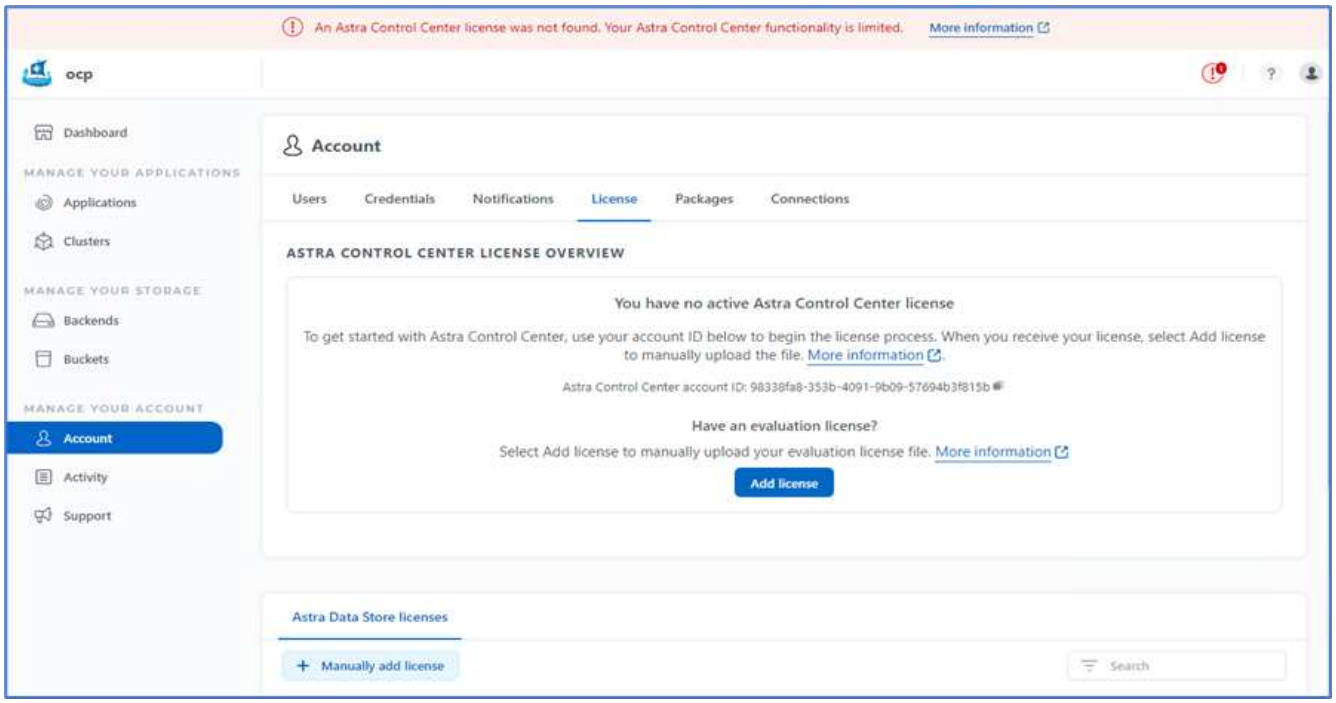


Weitere Informationen zur Installation des Astra Control Center finden Sie im "Astra Control Center – Übersicht über die Installation" Seite.

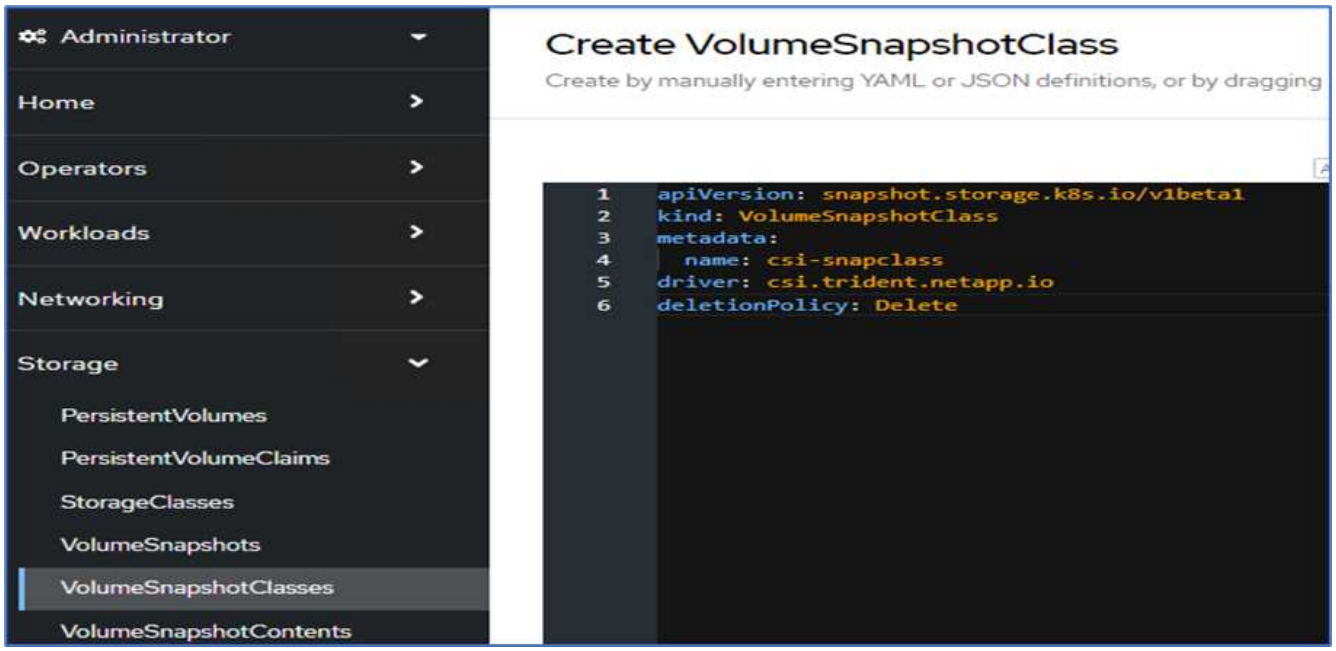
Einrichten des Astra Control Center

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.

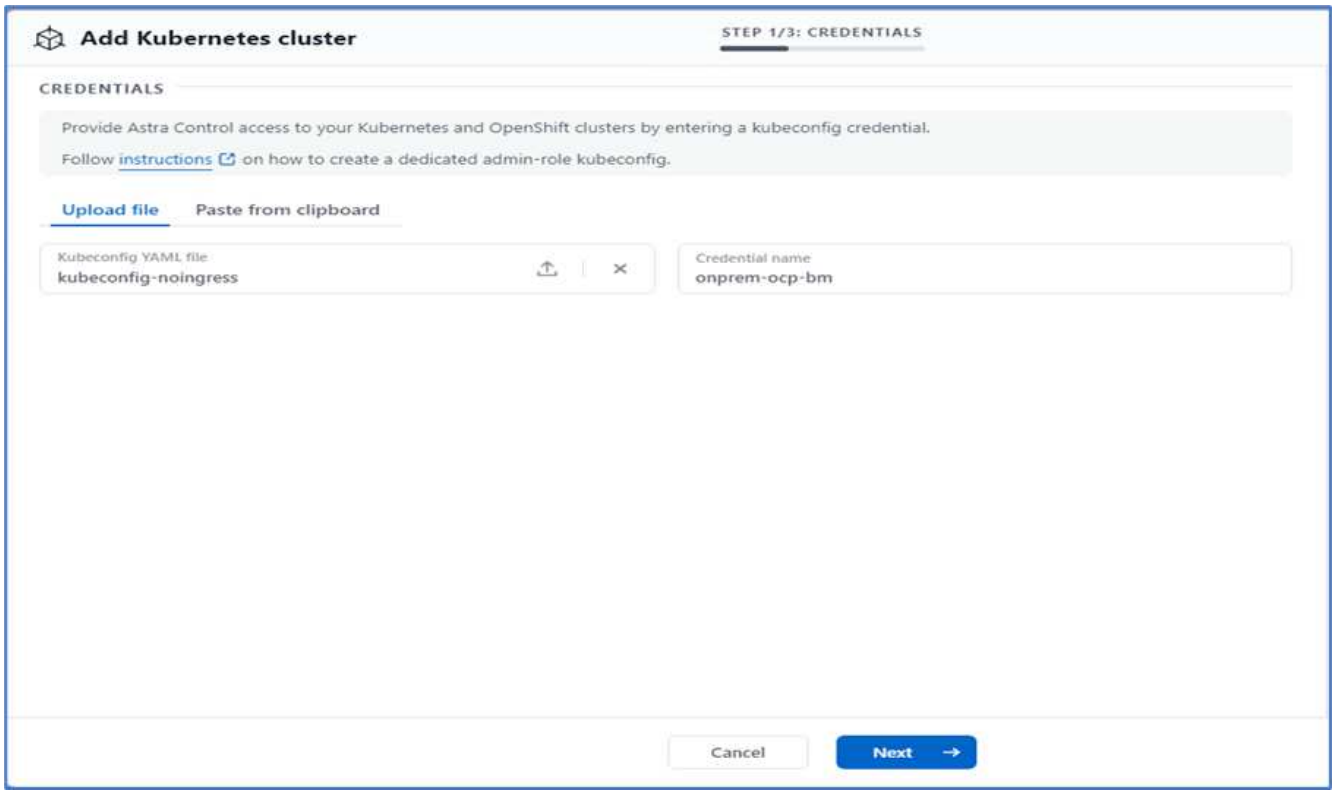
1. Gehen Sie auf der Homepage unter Konto auf die Registerkarte Lizenz und wählen Sie Lizenz hinzufügen, um die Astra-Lizenz hochzuladen.



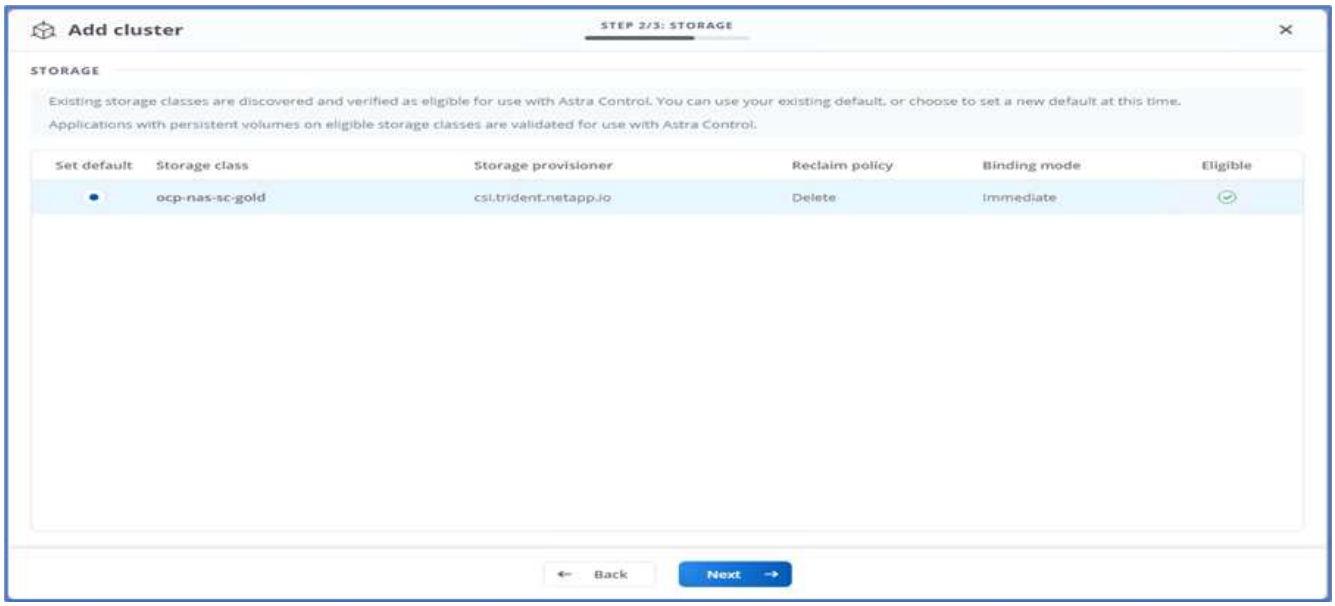
2. Erstellen Sie vor dem Hinzufügen des OpenShift-Clusters über die OpenShift-Webkonsole einen Astra Trident Volume Snapshot. Die Klasse Volume Snapshot wird mit dem konfiguriert `csi.trident.netapp.io` Treiber.



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.



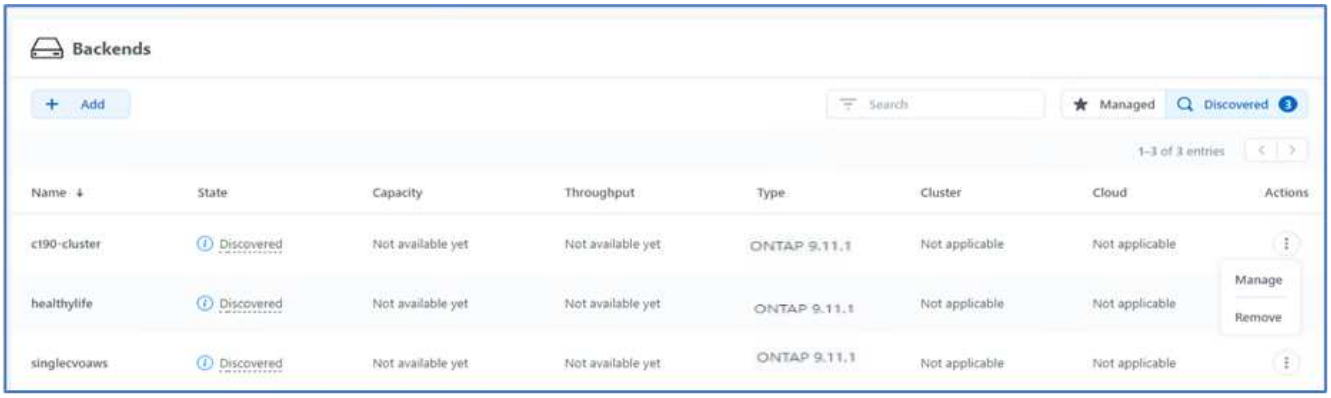
4. Die vorhandenen Speicherklassen werden automatisch erkannt. Wählen Sie die Standard-Storage-Klasse aus, klicken Sie auf Weiter und klicken Sie dann auf Cluster hinzufügen.



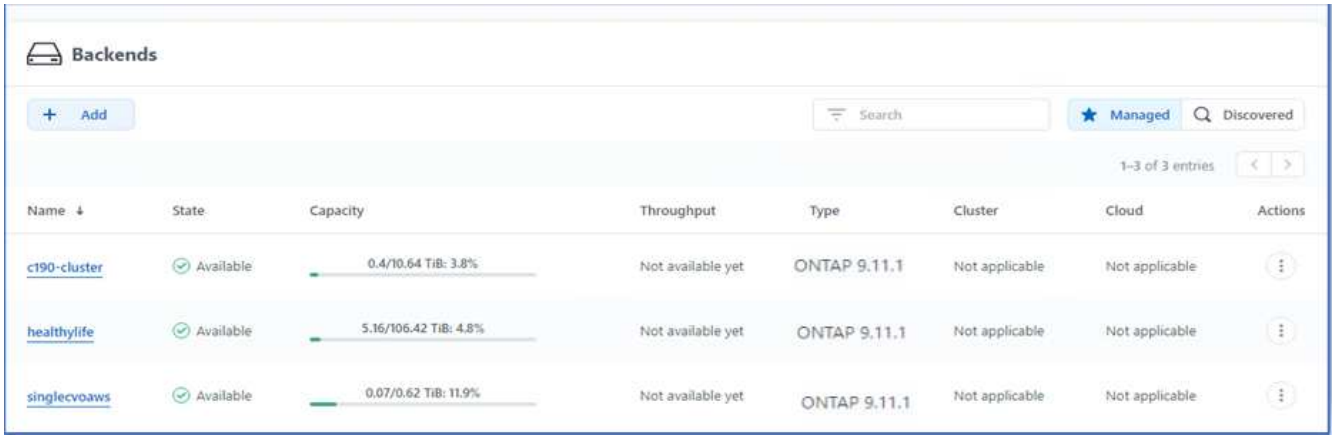
5. Der Cluster wird in wenigen Minuten hinzugefügt. Um weitere Cluster der OpenShift Container Platform hinzuzufügen, wiederholen Sie die Schritte 1 bis 4.

> 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.

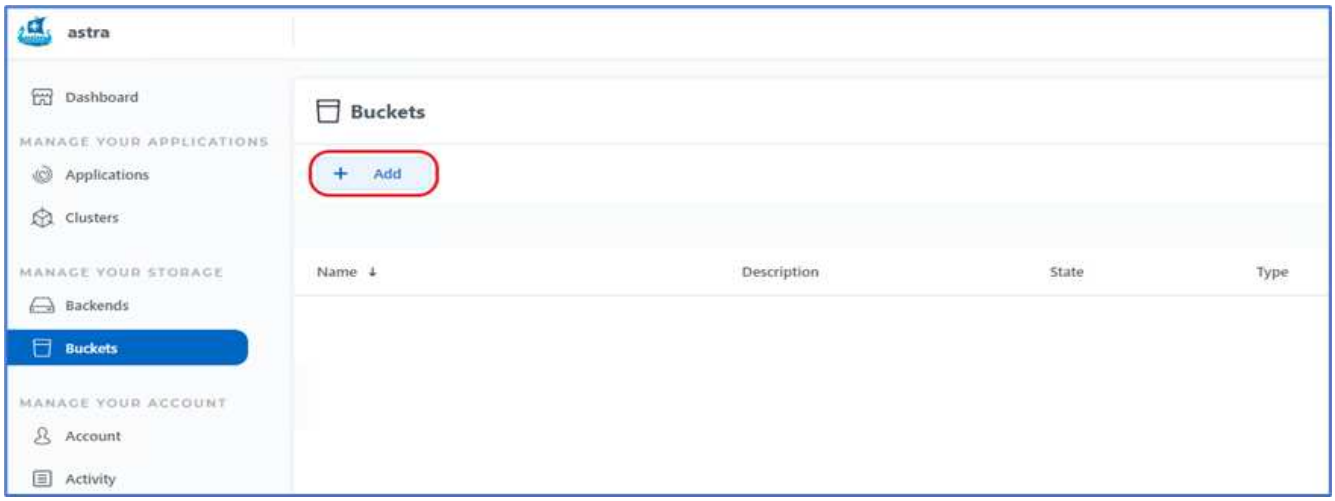
6. Um den Speicher zu verwalten, gehen Sie zu Backend, klicken Sie auf die drei Punkte unter Aktionen gegen das Backend, das Sie verwalten möchten. Klicken Sie Auf Verwalten.



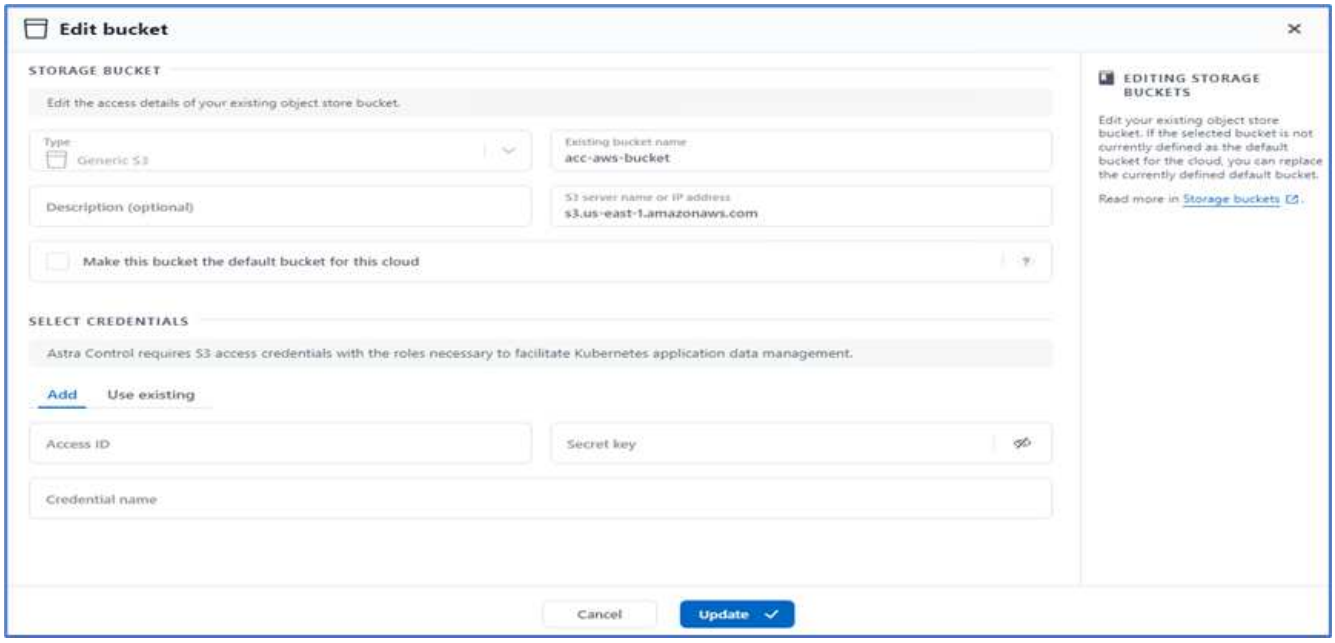
7. Geben Sie die ONTAP Zugangsdaten ein und klicken Sie auf Weiter. Überprüfen Sie die Informationen, und klicken Sie auf verwaltet. Die Back-Ends sollten wie im folgenden Beispiel aussehen.



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

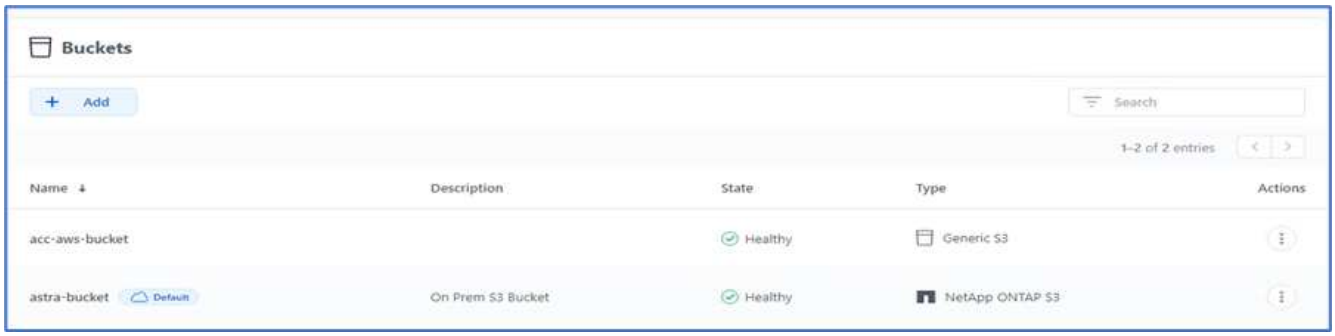


9. Wählen Sie den Bucket-Typ aus und geben Sie den Bucket-Namen, den S3-Servernamen oder die IP-Adresse und S3-Zugangsdaten an. Klicken Sie Auf Aktualisieren.



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"

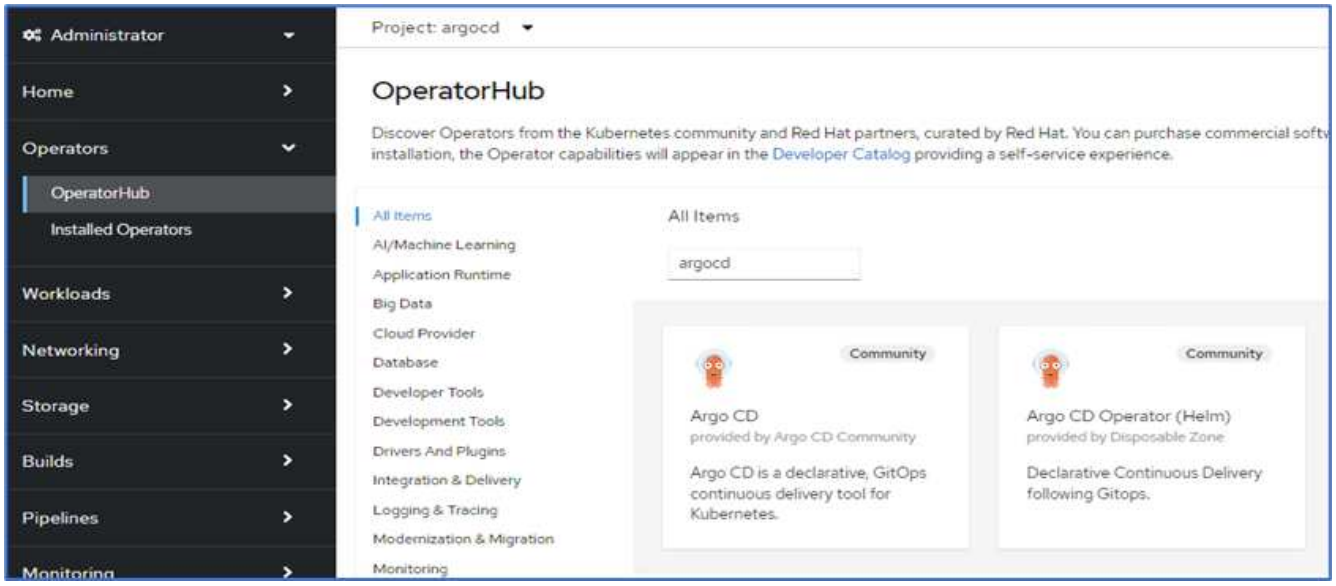
Mit Astra können Sie ein vollständiges und applikationskonsistentes Backup erstellen, mit dem Ihre Applikation ihre Daten auf einem anderen Kubernetes-Cluster wiederherstellen kann, der in einem On-Premises-Datacenter oder in einer Public Cloud ausgeführt wird.

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.

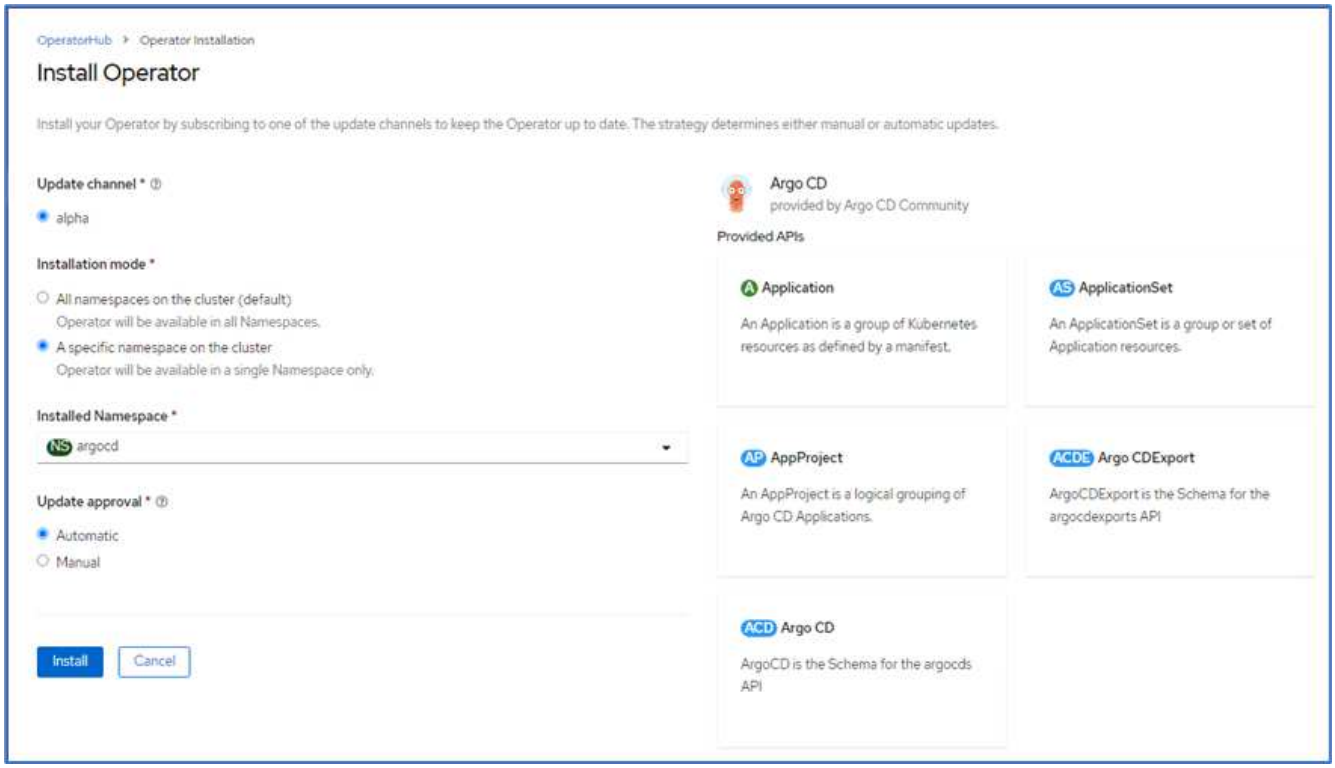
Die Beispielanwendung ist eine Anwendung der Preisliste, die MySQL für die Datenbank verwendet. Zur Automatisierung der Implementierung verwendeten wir das "Argo-CD" Werkzeug. Argo CD ist ein deklaratives GitOps, Continuous Delivery Tool für Kubernetes.

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

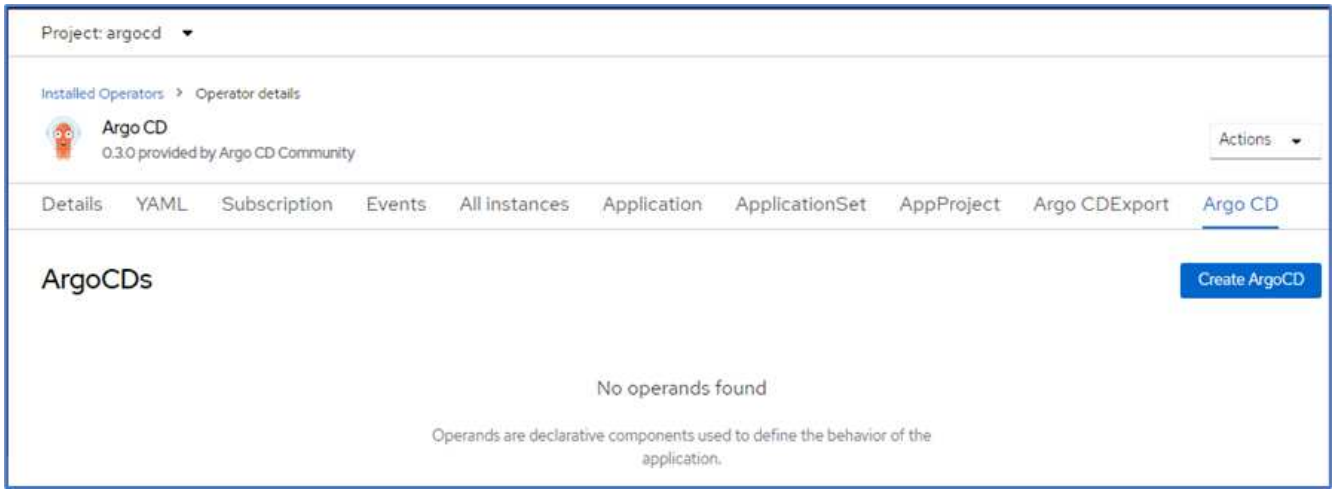
2. Suchen Sie im OperatorHub nach `argocd` Und wählen Sie Argo CD Operator.



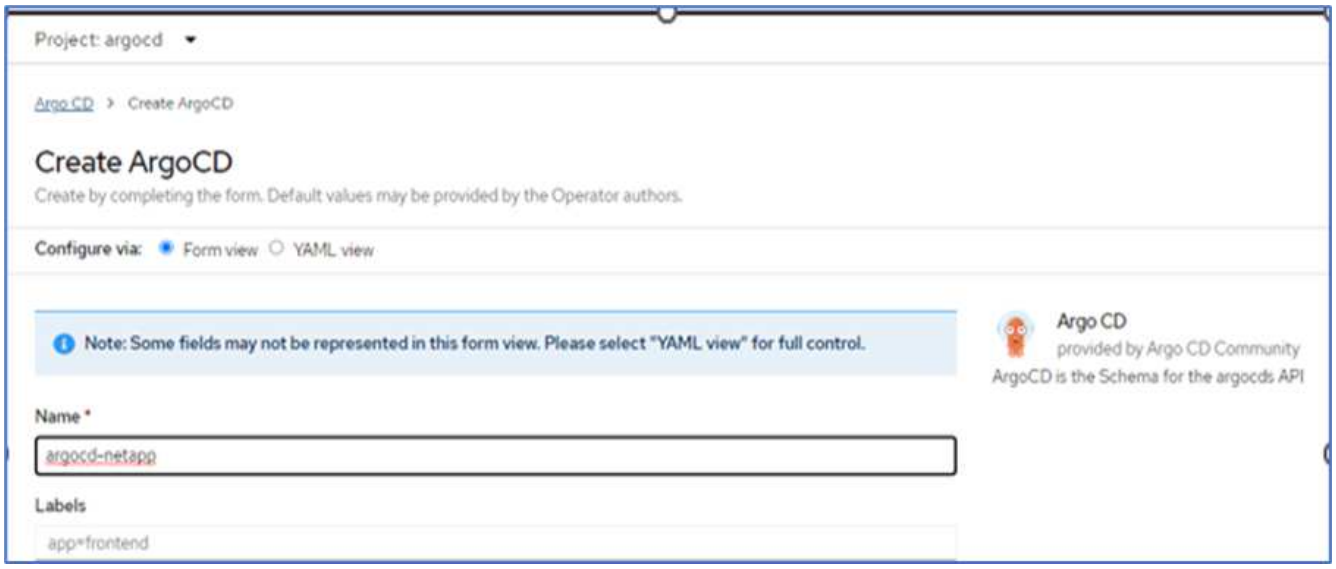
3. Installieren Sie den Operator in das `argocd` Namespace.



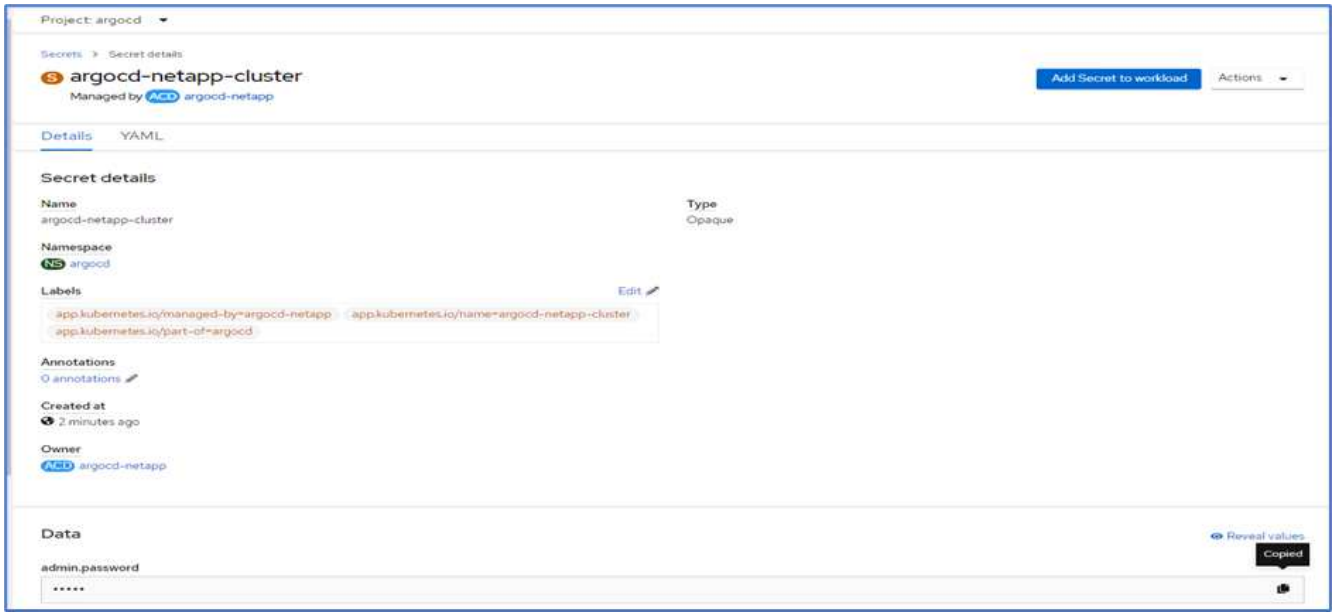
4. Gehen Sie zum Operator und klicken Sie auf ArgoCD erstellen.



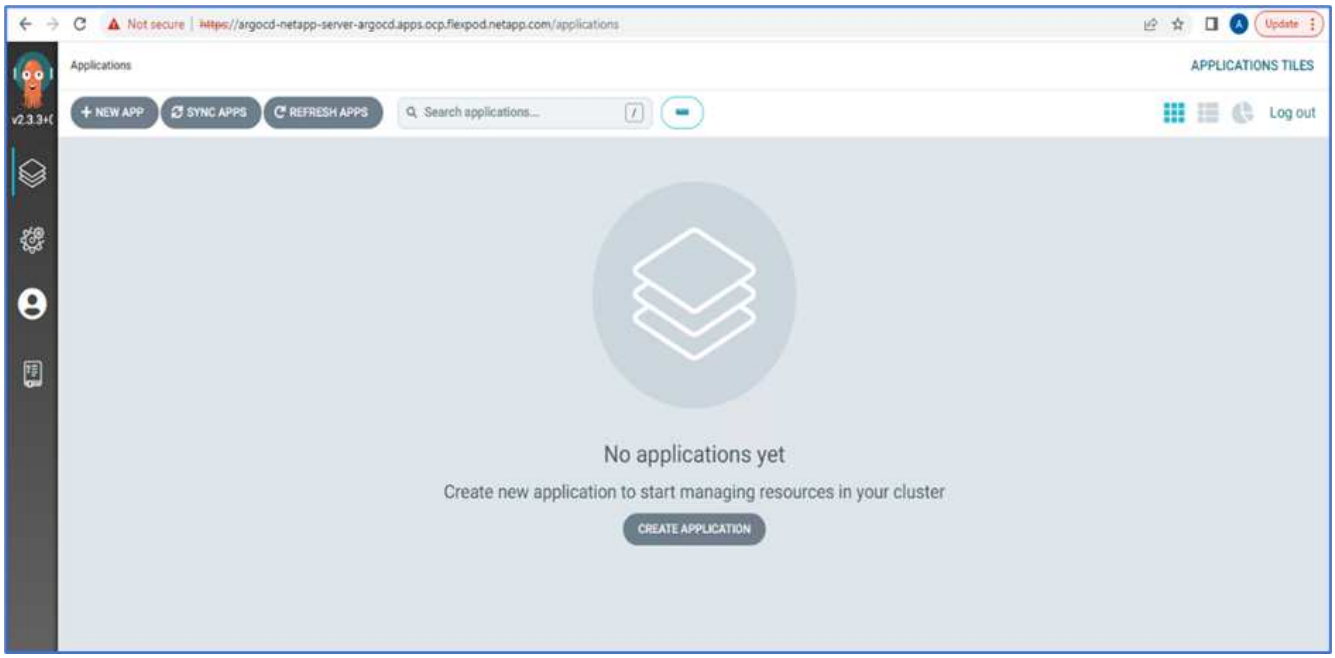
5. So stellen Sie die Argo-CD-Instanz im bereit `argocd` Geben Sie einen Namen ein, und klicken Sie auf Erstellen.



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`.



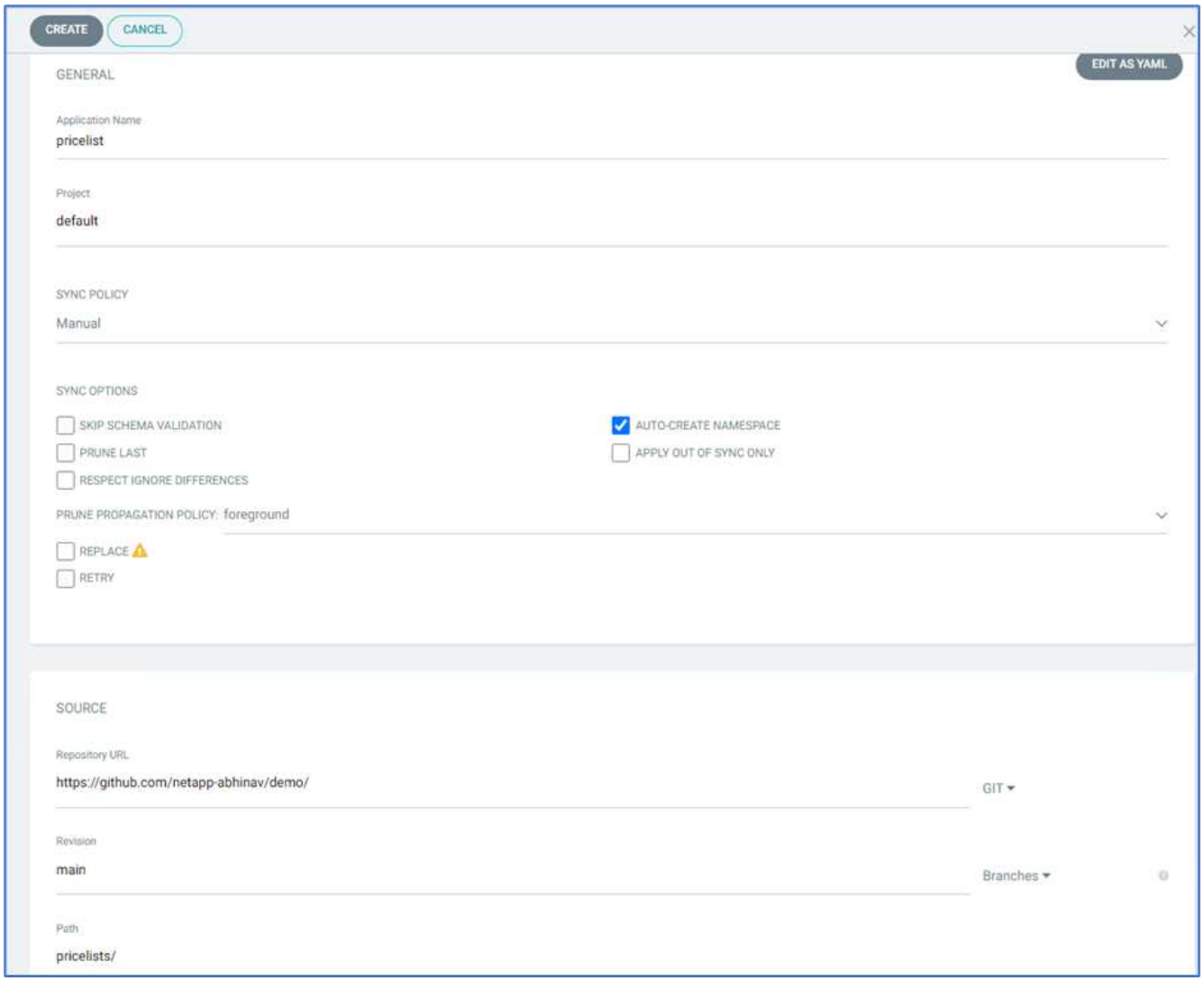
7. Wählen Sie im Seitenmenü Routen > Standort aus, und klicken Sie auf die URL für das `argocd` Routen. Geben Sie den Benutzernamen und das Kennwort ein.



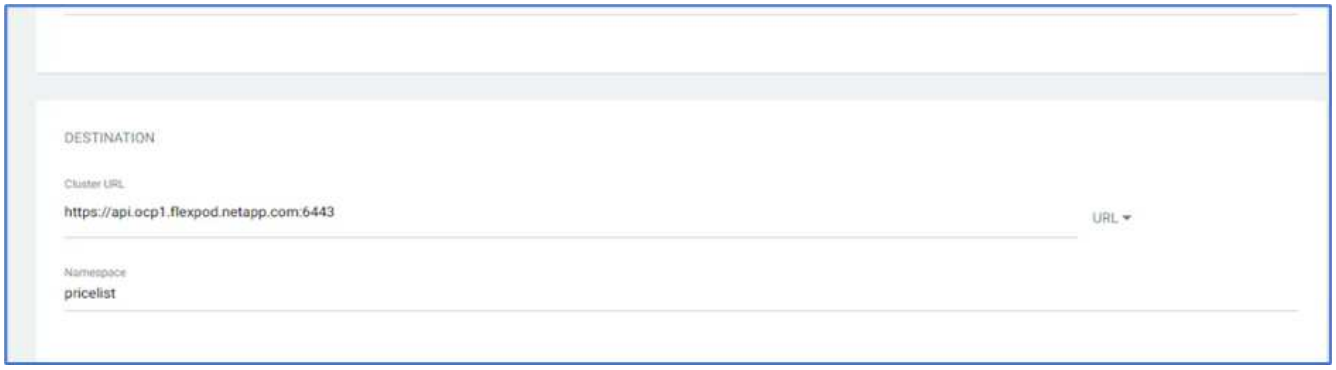
8. Fügen Sie den lokalen OpenShift-Cluster über die CLI zur Argo-CD hinzu.

```
####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
```

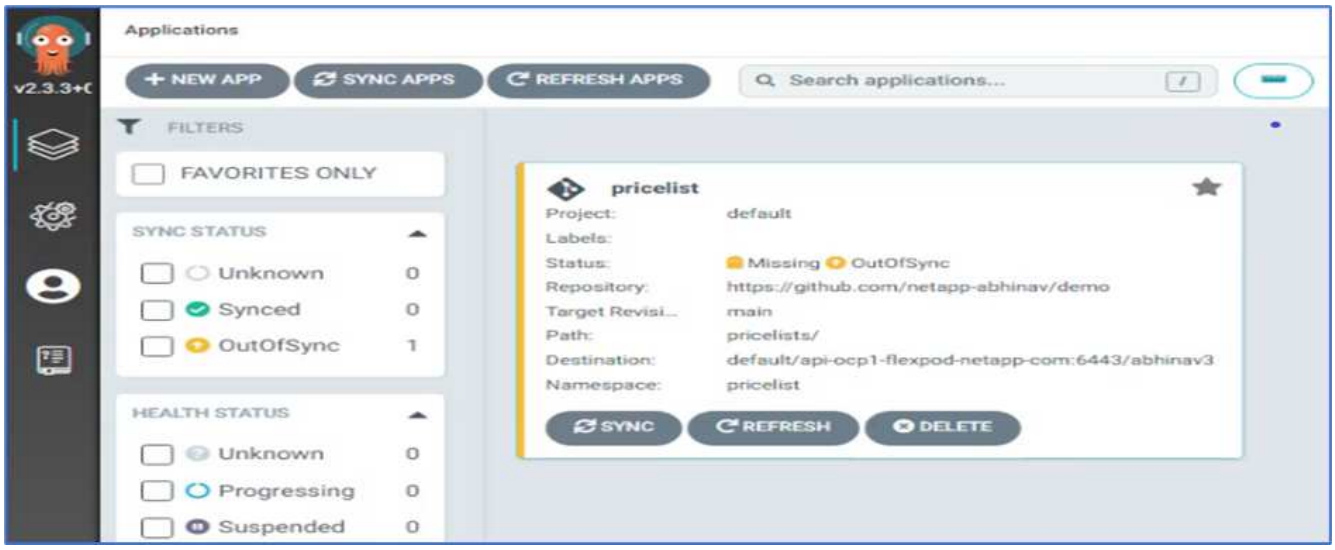
9. Klicken Sie in der ArgoCD-Benutzeroberfläche AUF DIE NEUE APP, und geben Sie die Details zum App-Namen und Code-Repository ein.



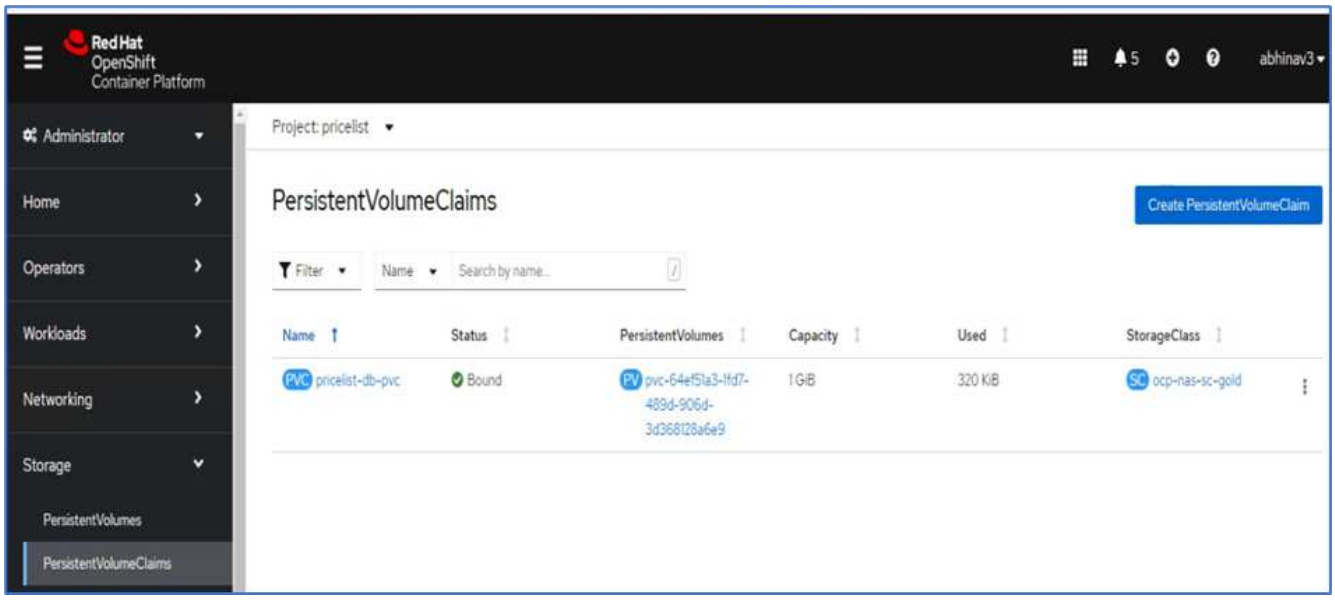
10. Geben Sie den OpenShift-Cluster ein, in dem die App zusammen mit dem Namespace bereitgestellt wird.



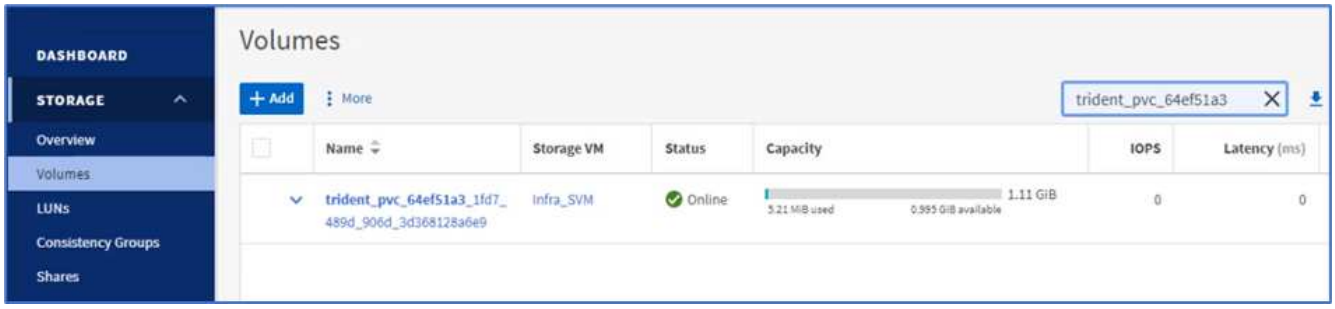
11. Klicken SIE ZUM Bereitstellen der App auf dem lokalen OpenShift-Cluster auf „SYNC“.



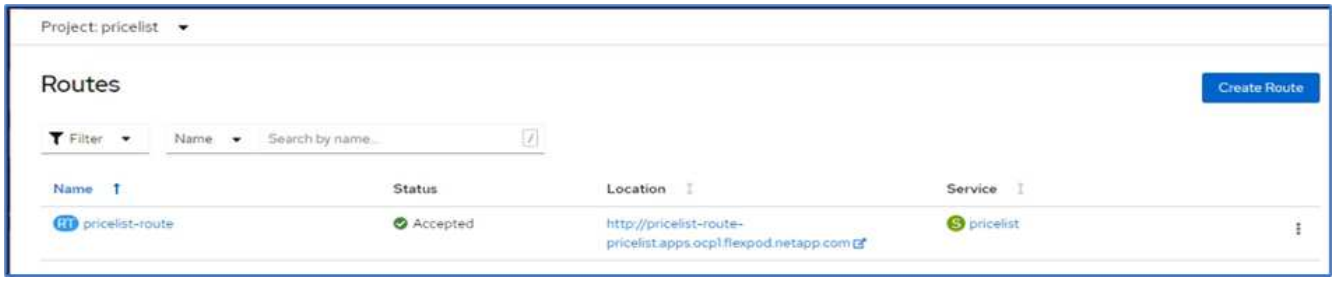
12. Wechseln Sie in der Konsole der OpenShift Container Platform zur Project Pricliste, und überprüfen Sie unter Storage den Namen und die Größe des PVC.



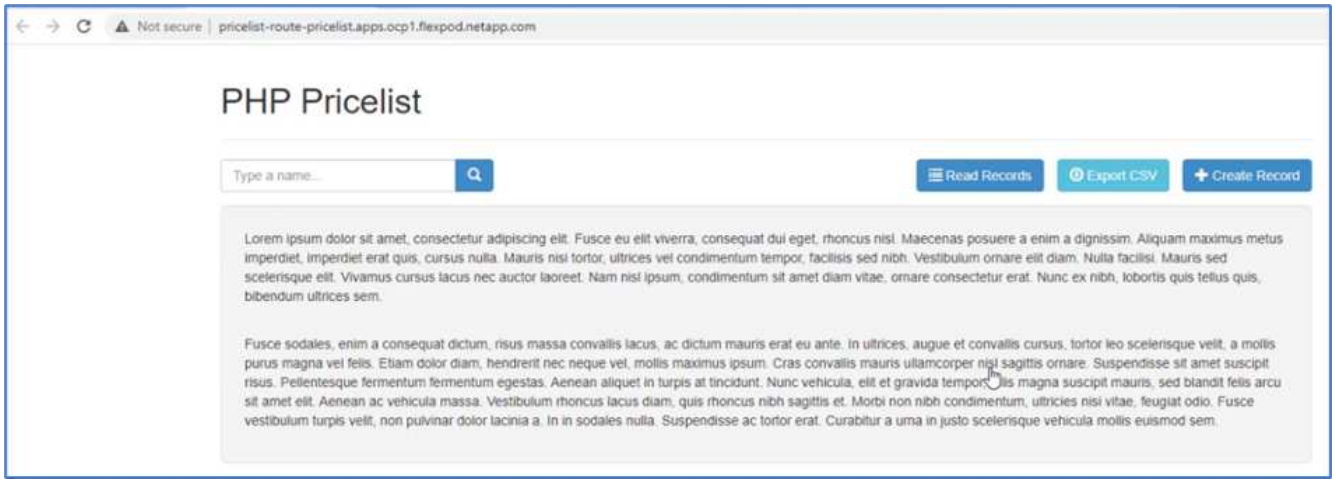
13. Melden Sie sich bei System Manager an und überprüfen Sie die PVC.



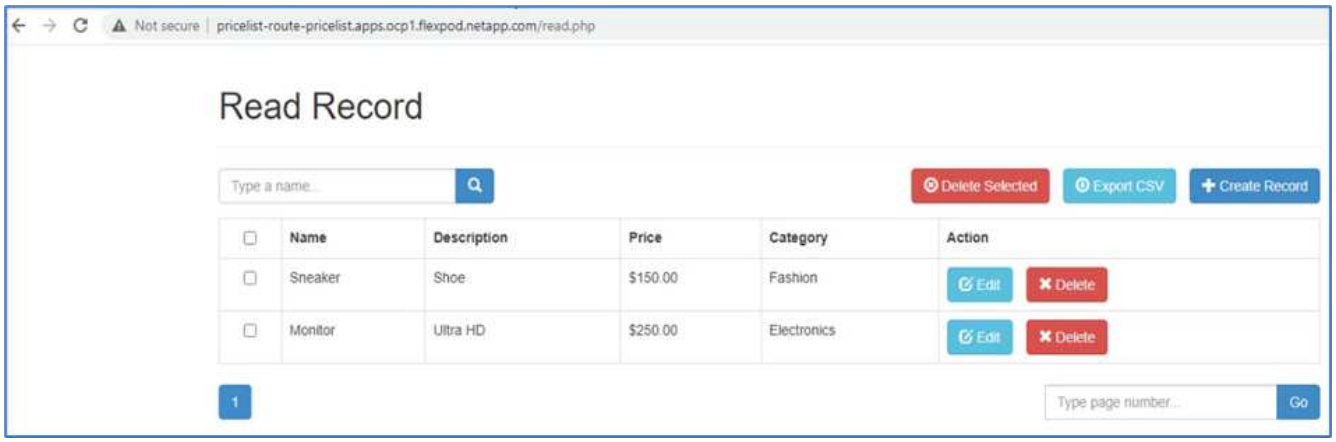
14. Wählen Sie nach dem Ausführen der Pods im Seitenmenü Netzwerk > Routen aus, und klicken Sie unter Speicherort auf die URL.



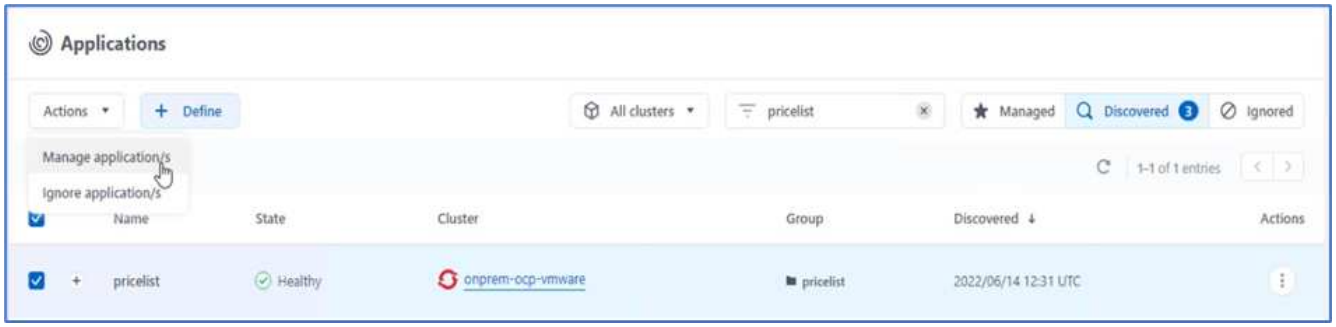
15. Die Homepage der Preisliste wird angezeigt.



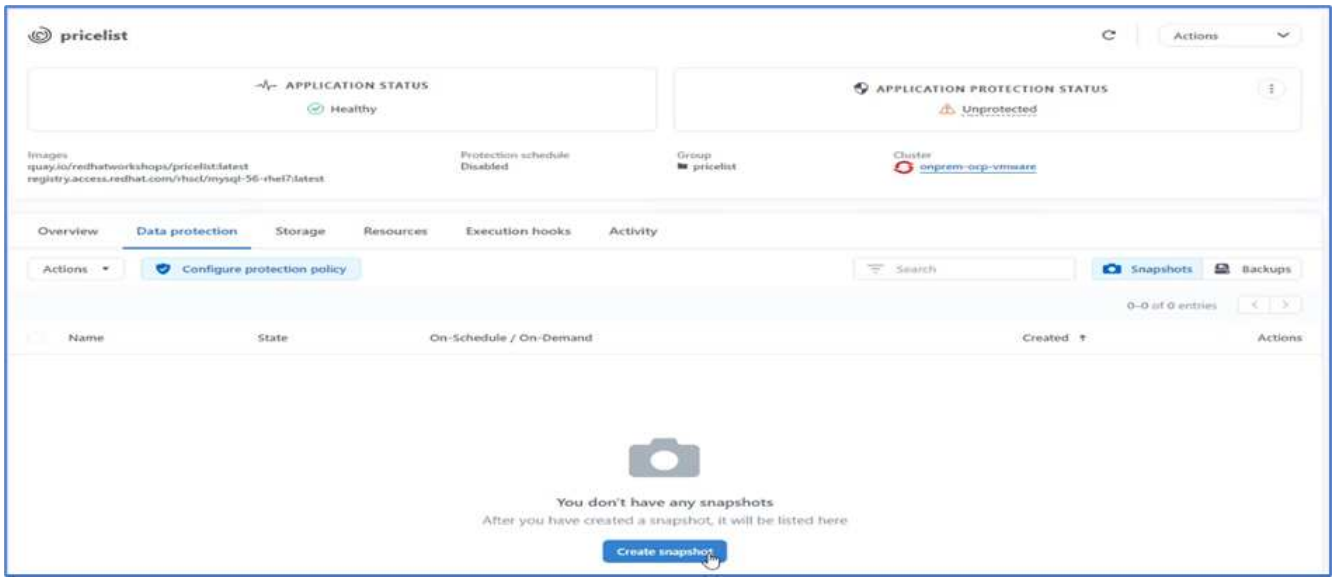
16. Erstellen Sie ein paar Datensätze auf der Webseite.



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.

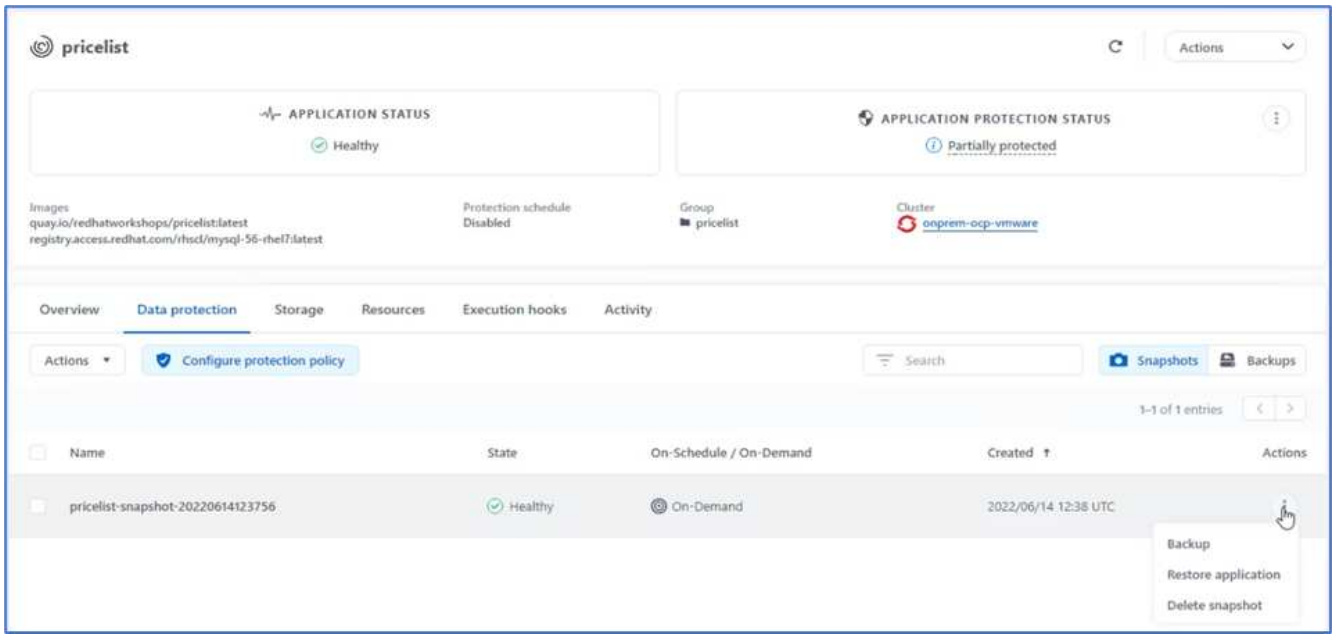


18. Klicken Sie auf die Preisliste-App und wählen Sie Datenschutz aus. Zu diesem Zeitpunkt sollten keine Snapshots oder Backups vorhanden sein. Klicken Sie auf Snapshot erstellen, um einen On-Demand-Snapshot zu erstellen.

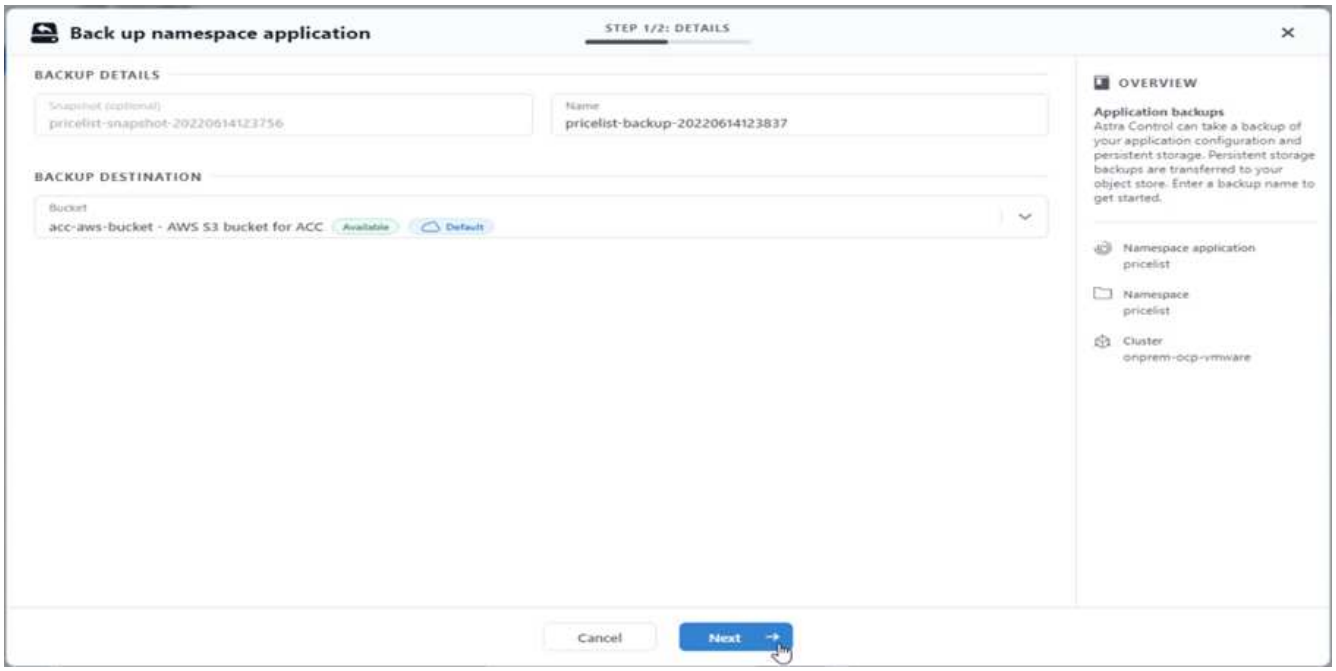


Das NetApp Astra Control Center unterstützt sowohl On-Demand als auch geplante Snapshots und Backups.

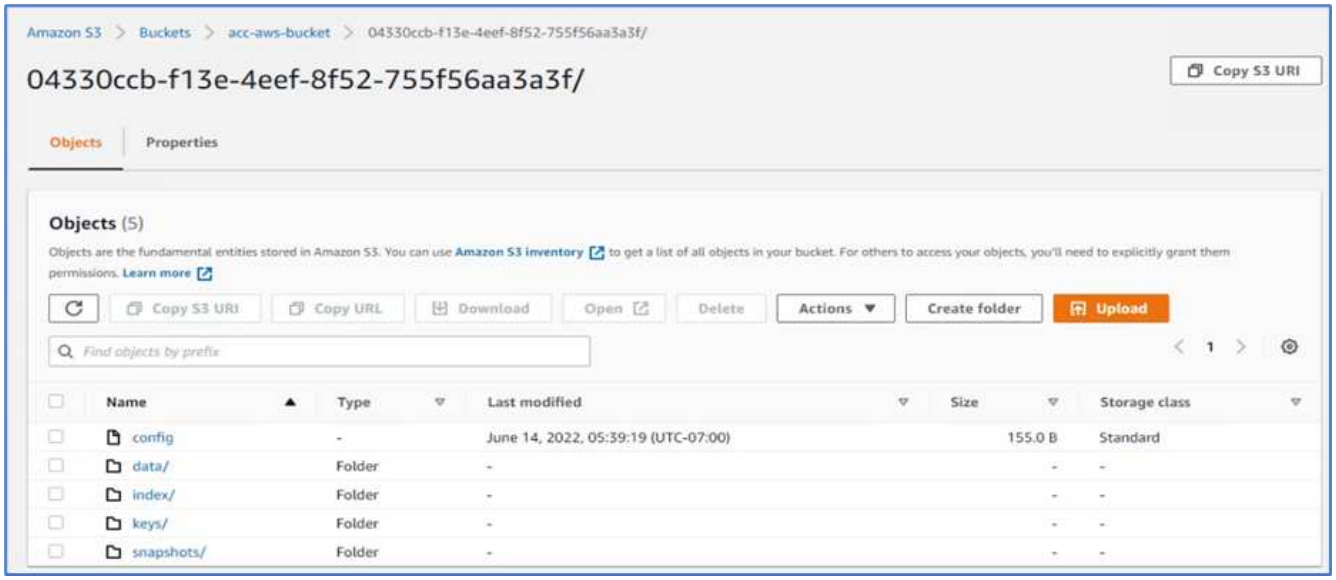
19. Nachdem der Snapshot erstellt wurde und der Status sich in einem ordnungsgemäßen Zustand befindet, erstellen Sie mithilfe dieses Snapshots eine Remote-Sicherung. Dieses Backup wird im S3-Bucket gespeichert.



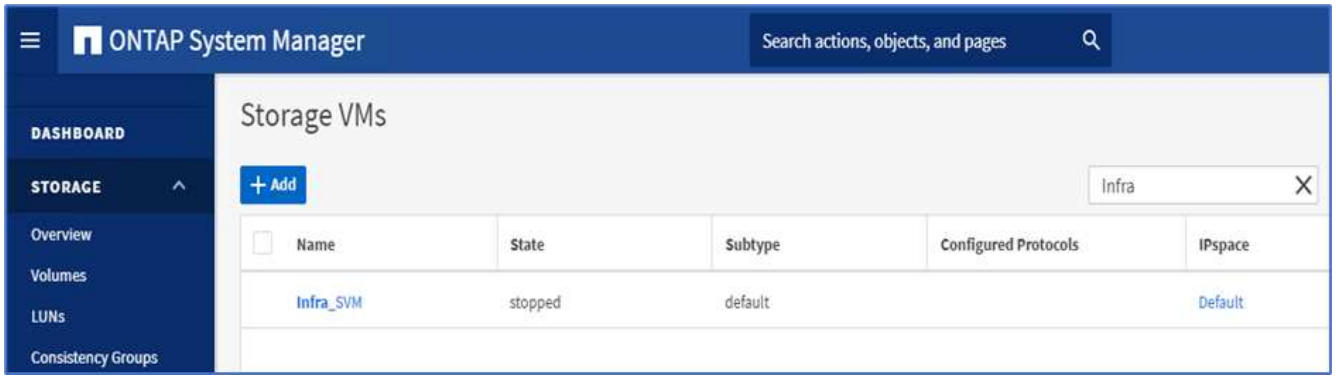
20. Wählen Sie den AWS S3-Bucket aus und initiieren Sie den Backup-Vorgang.



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



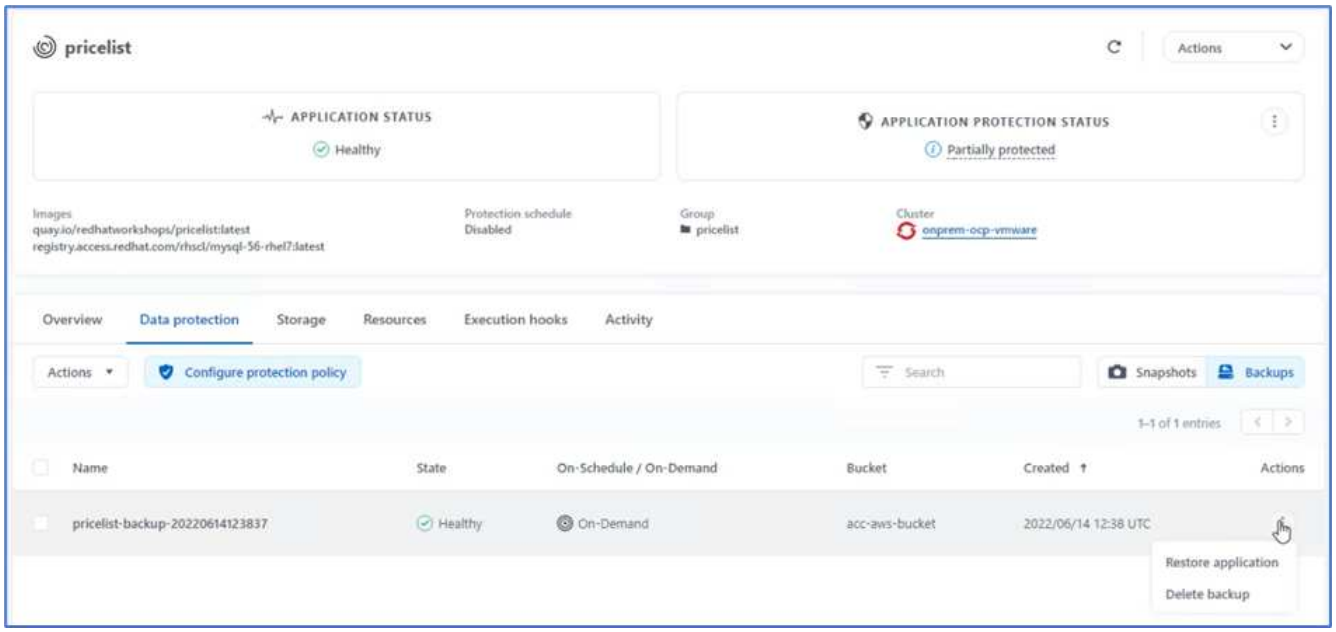
22. Nach Abschluss des Remote Backups simulieren Sie eine Katastrophe im lokalen Datacenter, indem Sie die Storage Virtual Machine (SVM) stoppen, die das zugrunde liegende Volume für das PV hostet.



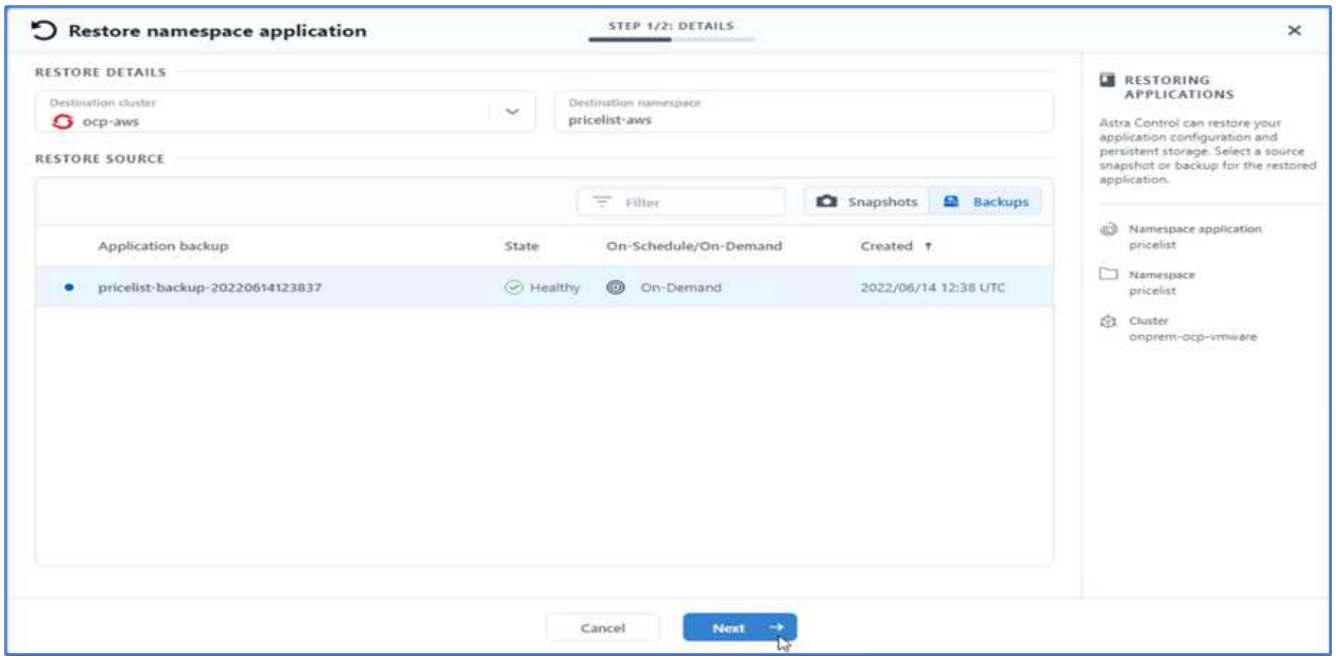
23. Aktualisieren Sie die Website, um den Ausfall zu bestätigen. Die Webseite ist nicht verfügbar.

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.

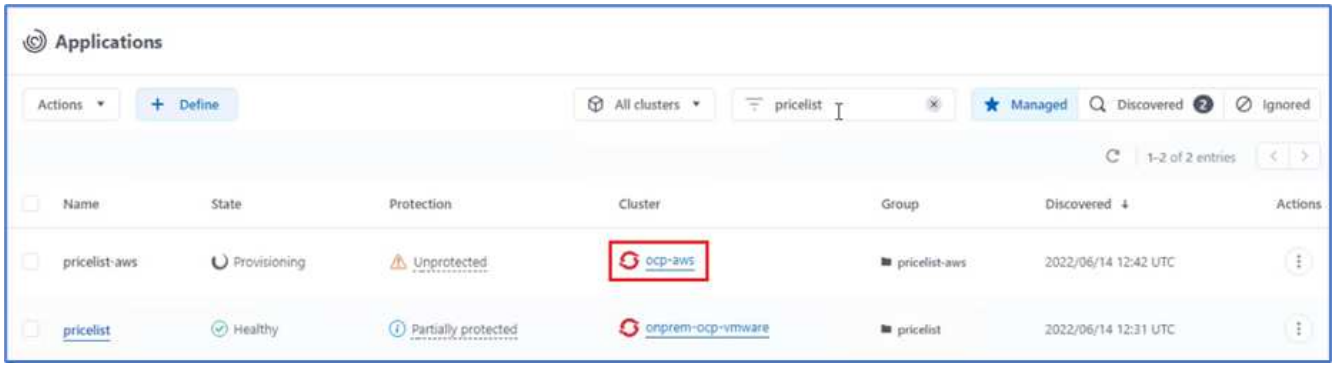
24. Klicken Sie im Astra Control Center auf die Preisliste und wählen Sie Datensicherheit > Backups. Wählen Sie das Backup aus, und klicken Sie unter Aktion auf Anwendung wiederherstellen.



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.

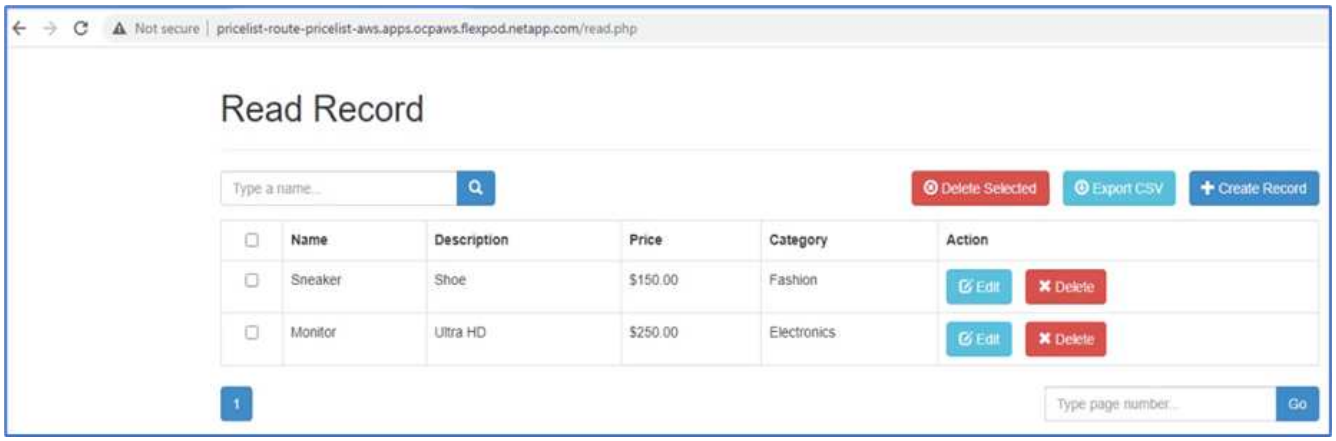


26. Eine neue App mit dem Namen `pricelist-app` Wird auf dem OpenShift-Cluster in AWS beschrieben.



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

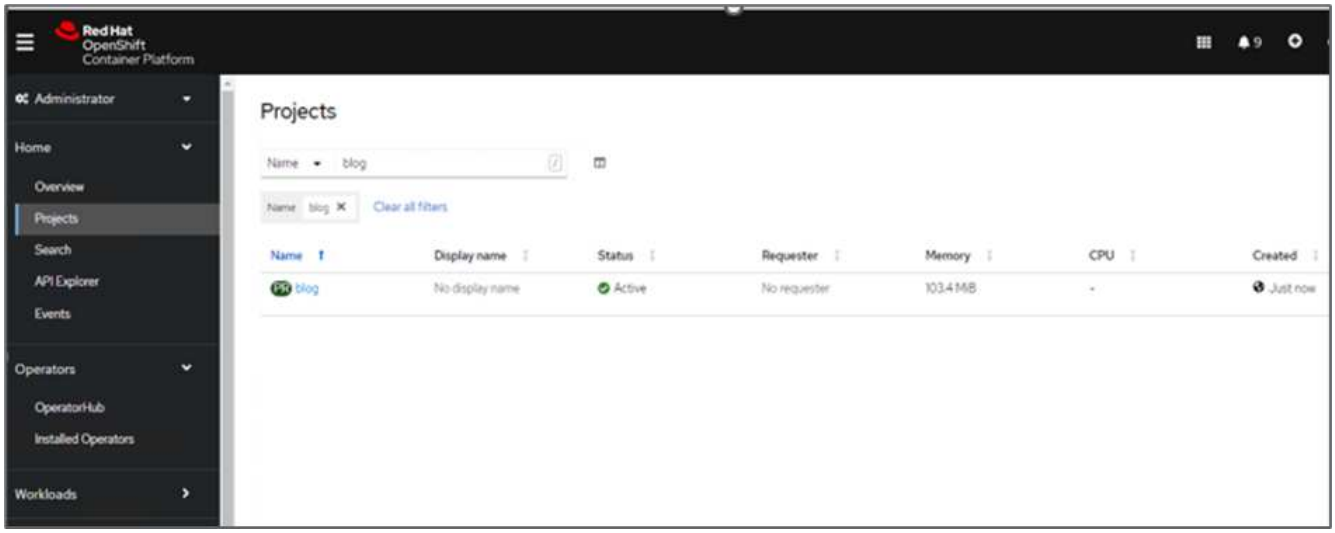
Mit Astra Control Center können Sie applikationsgerechte Snapshots für die lokale Datensicherung erstellen. Wenn Sie Ihre Daten versehentlich löschen oder beschädigt haben, können Sie Ihre Anwendungen und zugehörigen Daten mithilfe eines zuvor aufgenommenen Snapshots in einen bekannten fehlerfreien Zustand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

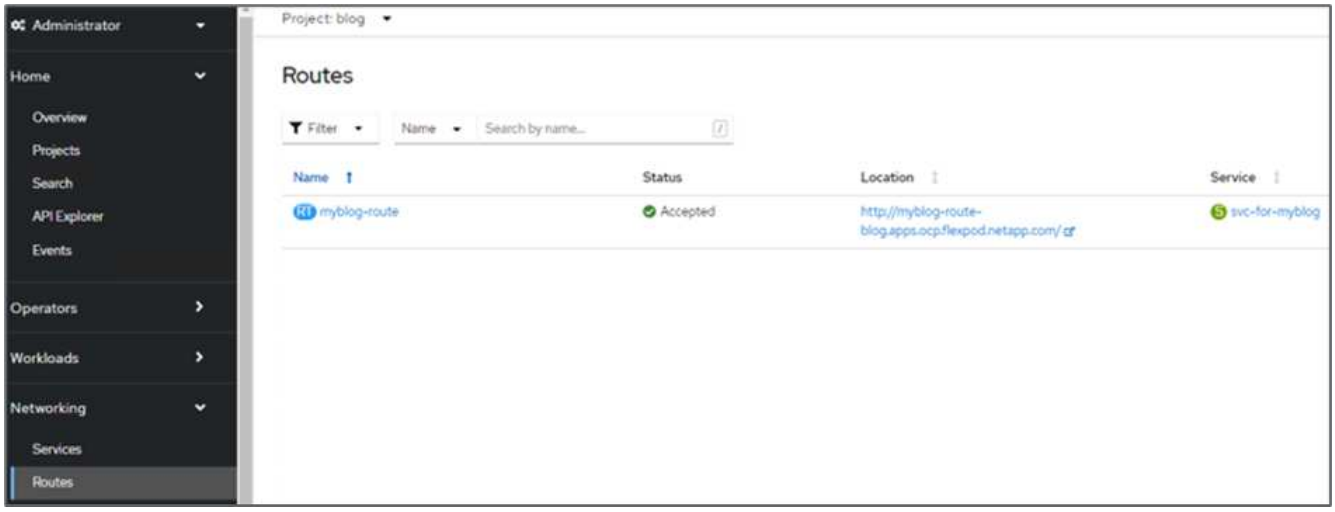
1. Stellen Sie die Beispiel-Blogging-App bereit und synchronisieren Sie sie von ArgoCD.

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

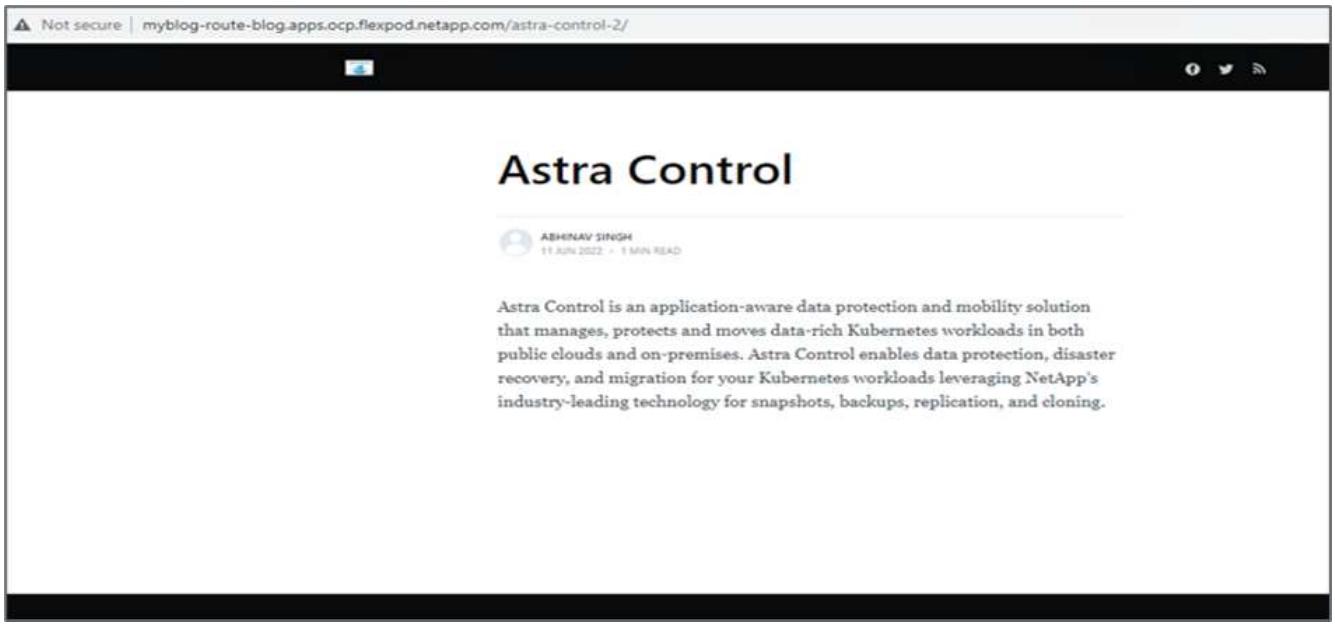
den Blog ein.



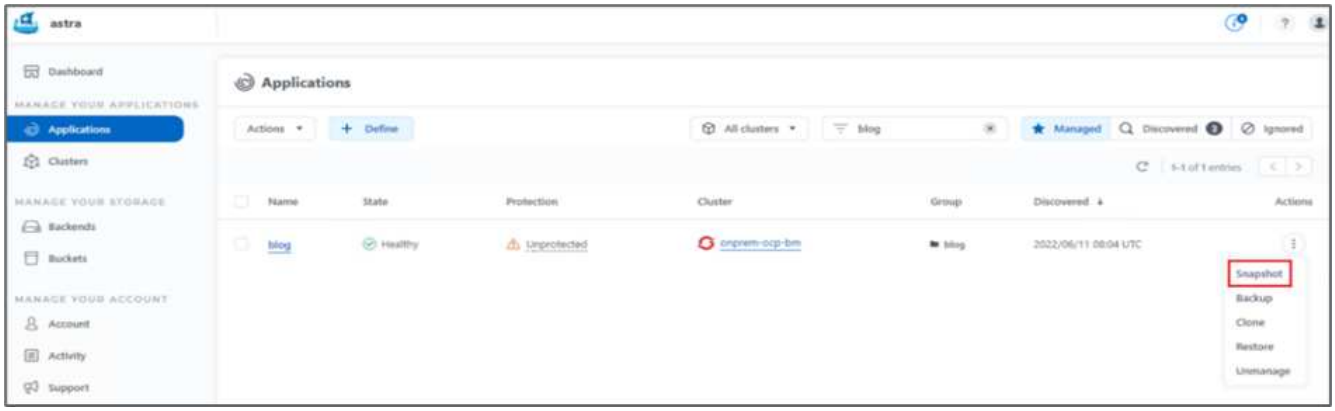
3. Wählen Sie im seitlichen Menü die Option Netzwerk > Routen, und klicken Sie auf die URL.



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.

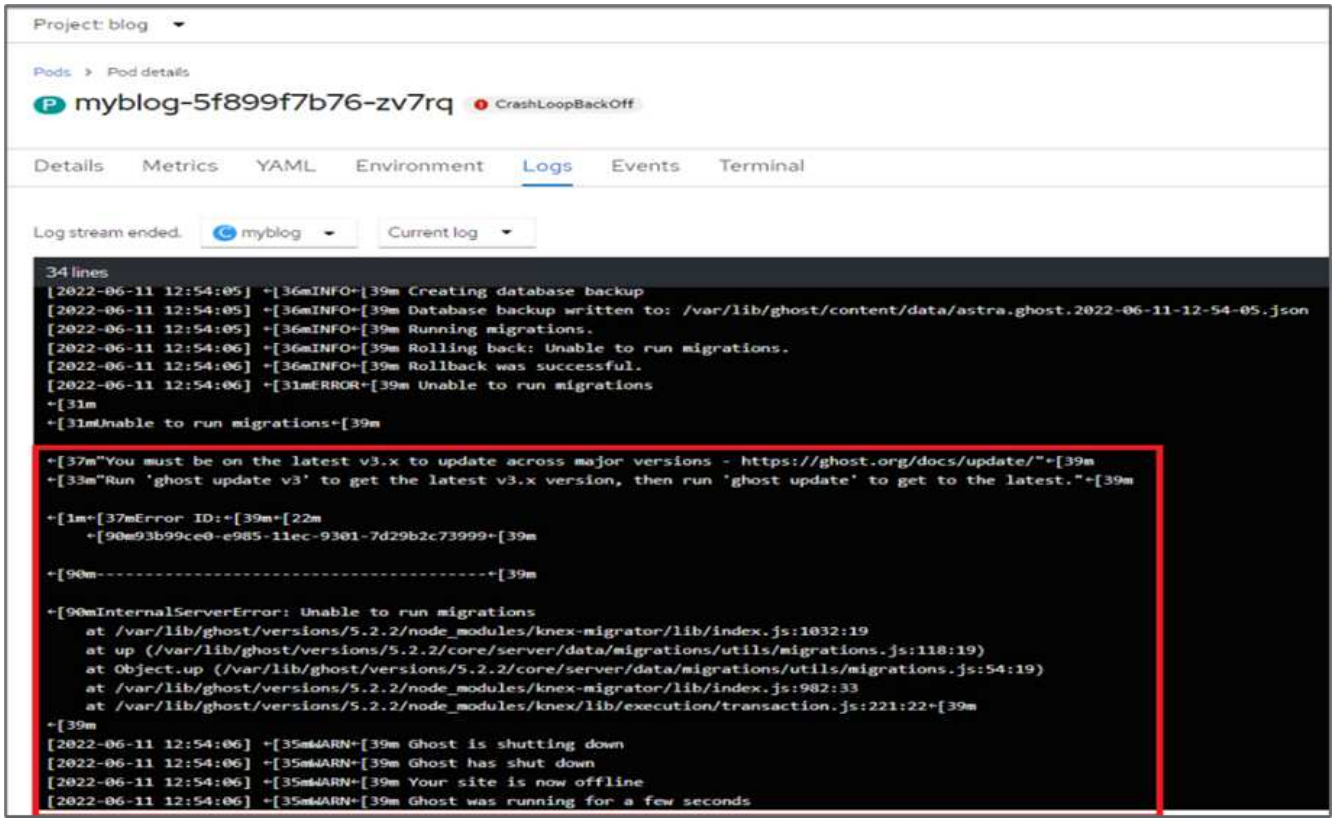


Sie können auch Ihre Applikationen schützen, indem Sie Snapshots, Backups oder beides nach einem definierten Zeitplan erstellen. Weitere Informationen finden Sie unter "Sichern von Applikationen durch Snapshots und Backups".

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.

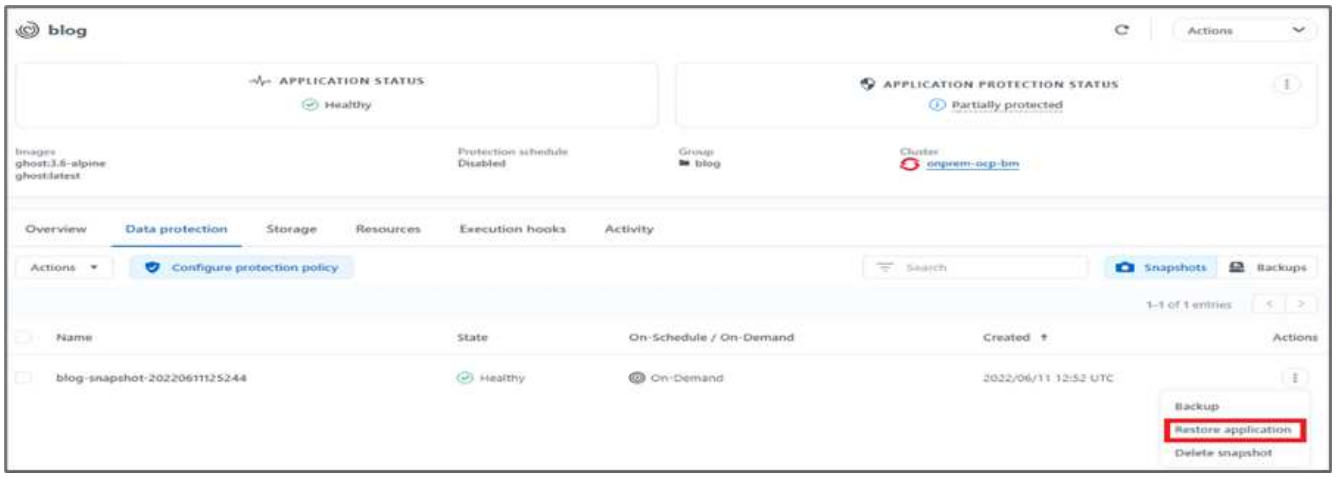
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

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.

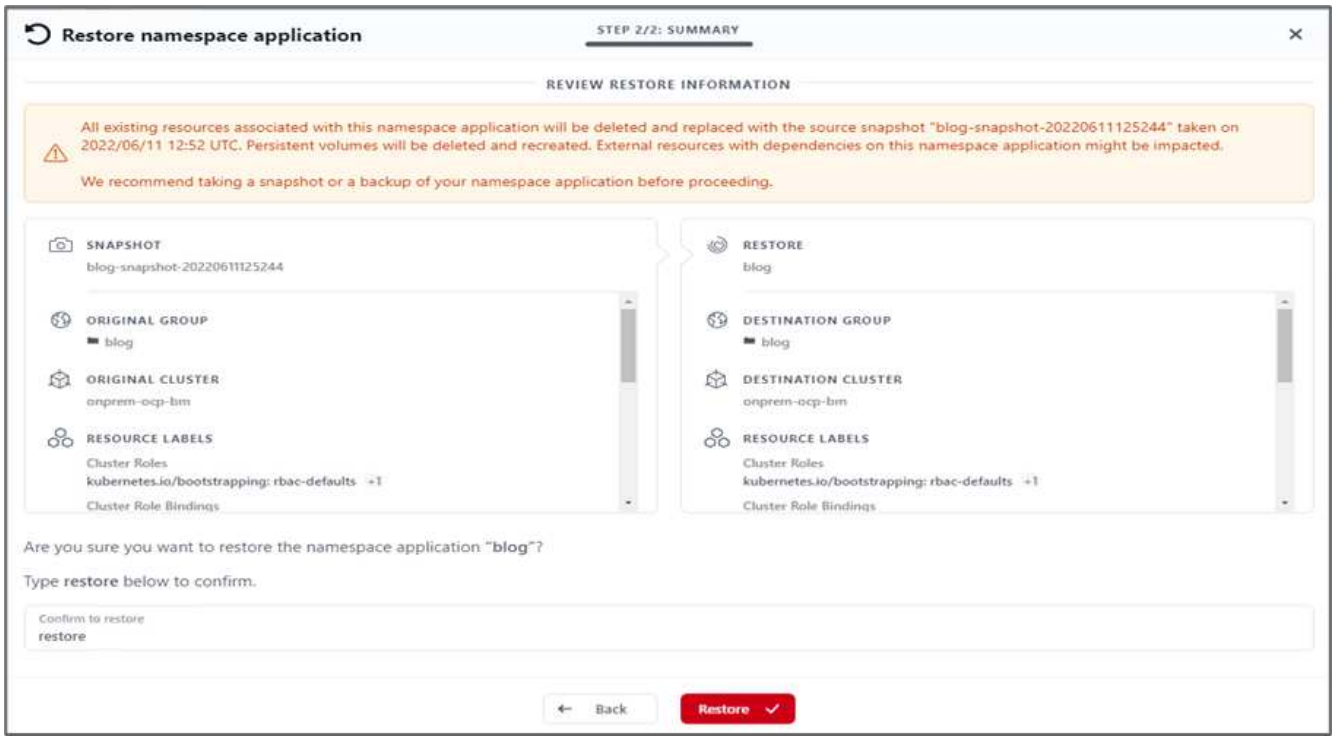


8. Aktualisieren Sie die URL, um die Nichtverfügbarkeit der Blog-Site zu bestätigen.

9. Die Anwendung aus dem Snapshot wiederherstellen.



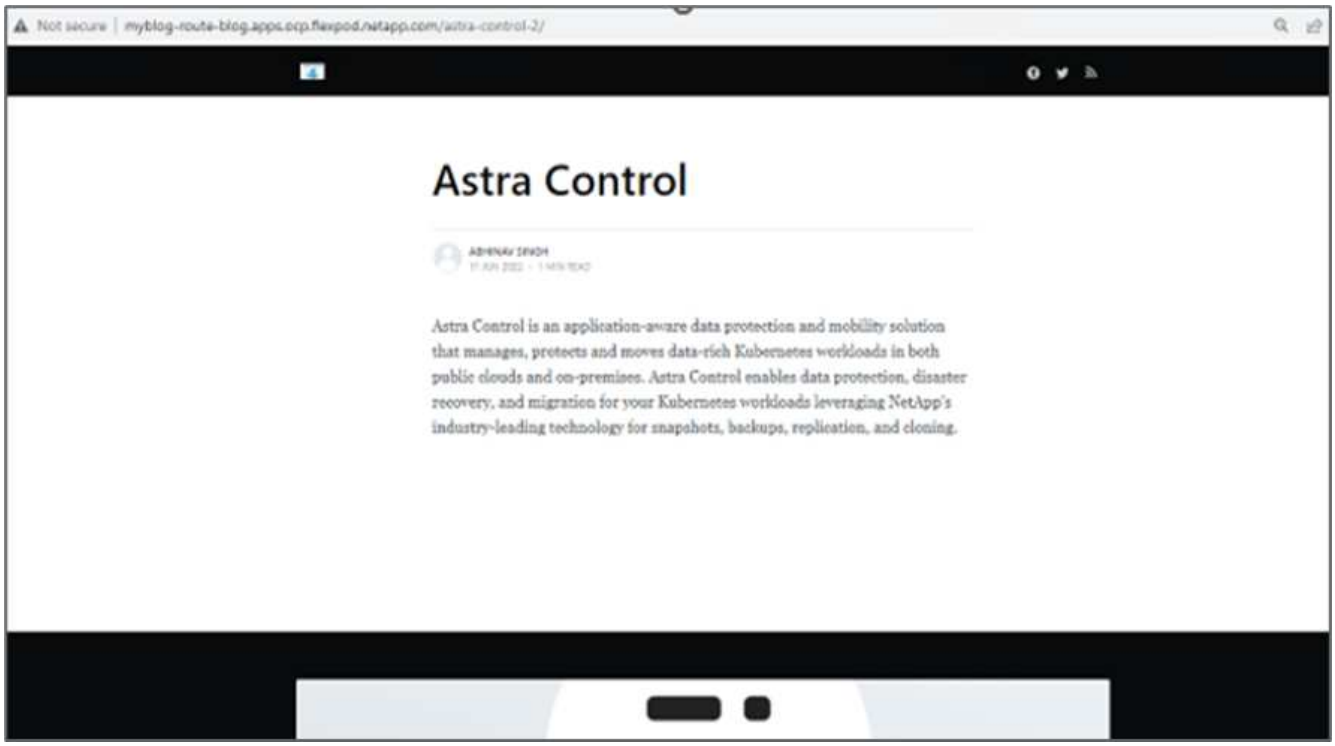
10. Die App wird auf demselben OpenShift-Cluster wiederhergestellt.



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.

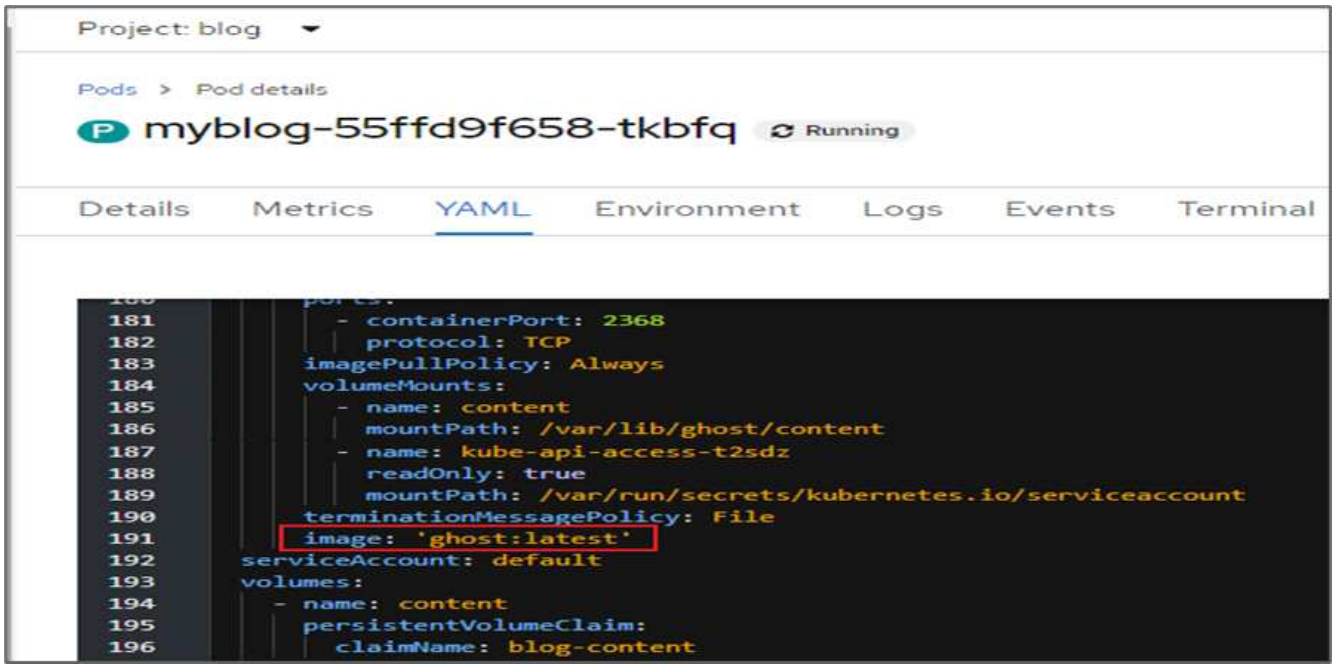


Mithilfe des Astra Control Center kann ein DevTest-Team mithilfe des Snapshots eine Blog-Site-App und die damit verbundenen Daten erfolgreich wiederherstellen.

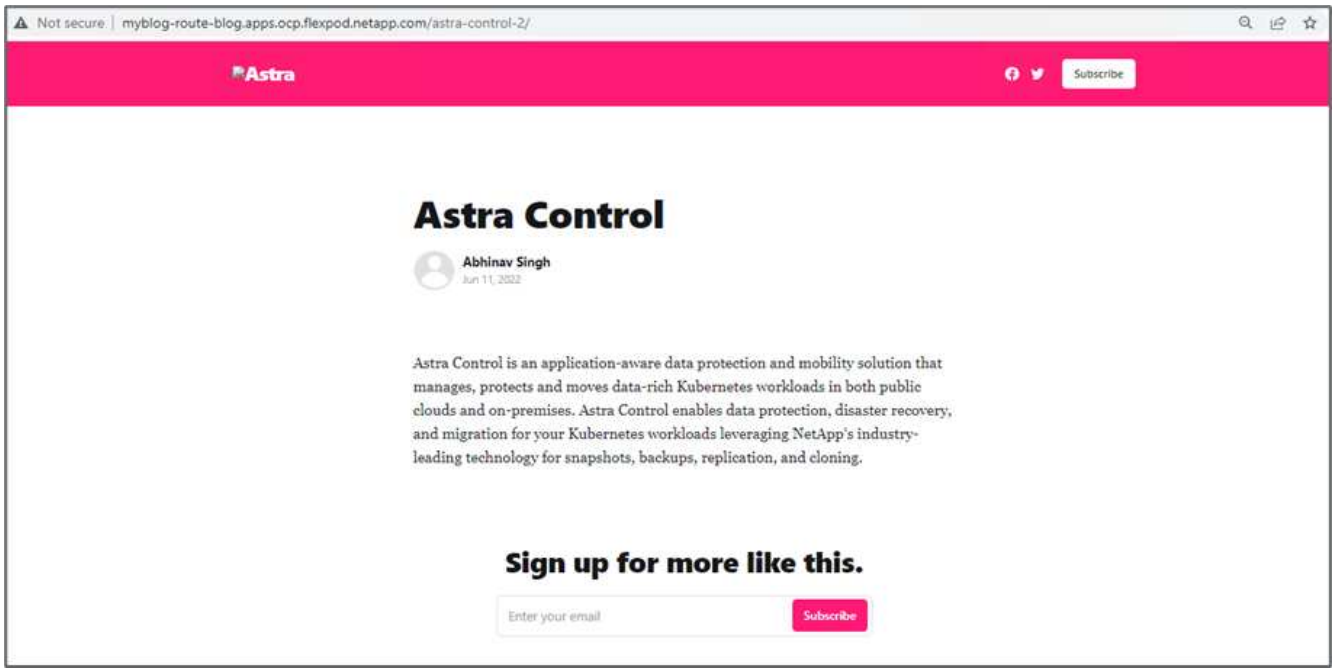
Teil 2

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).

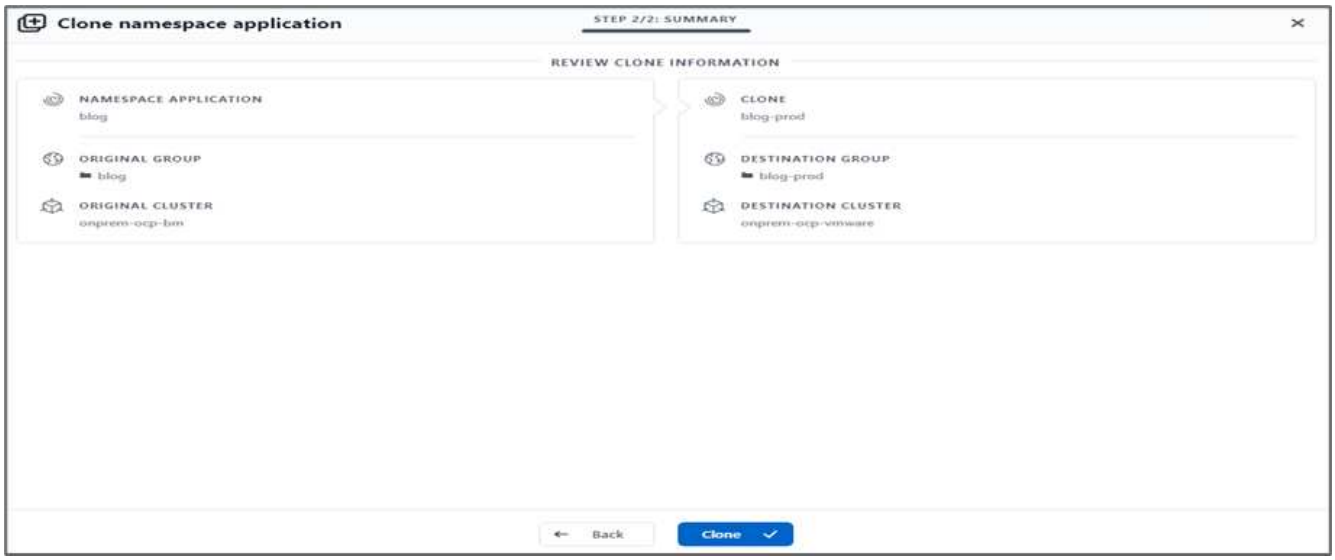
1. Das DevTest-Team aktualisiert zunächst die App auf die unterstützte Version (`ghost-4.6-alpine`) Vor dem Upgrade auf die endgültige Version (`ghost-latest`) Um die Produktion bereit zu machen. Anschließend wird ein Upgrade der App veröffentlicht, die in den OpenShift-Cluster in der Produktion geklont 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.



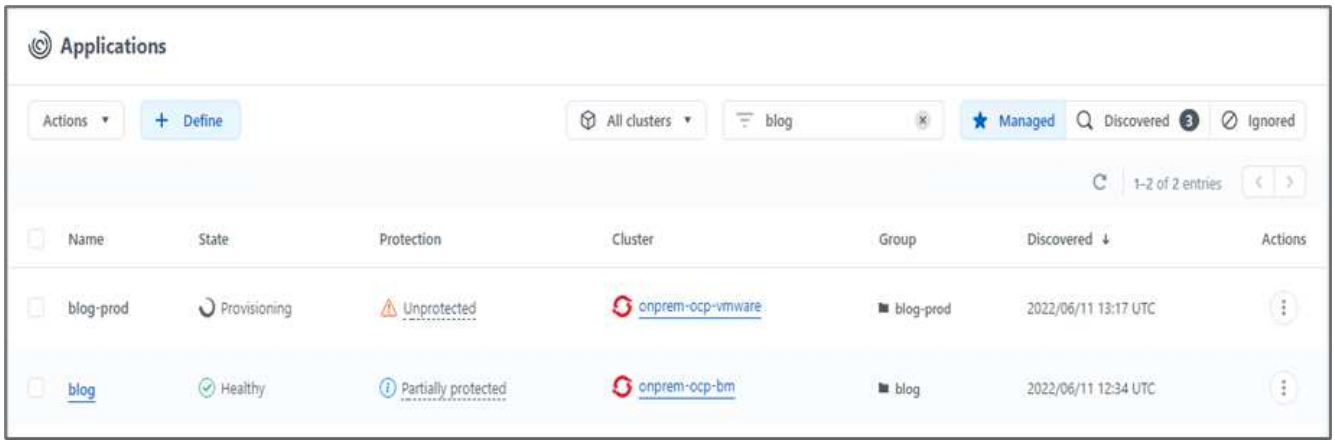
3. Um das neue Thema zu überprüfen, aktualisieren Sie die Blog-Site.



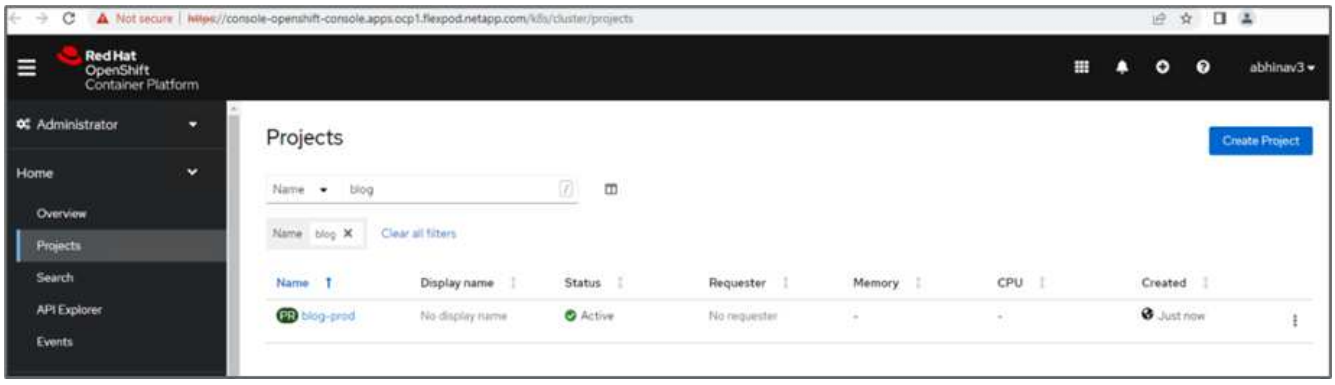
4. Vom Astra Control Center können Sie die App auf den anderen OpenShift-Cluster in der Produktion klonen, der auf VMware vSphere ausgeführt wird.



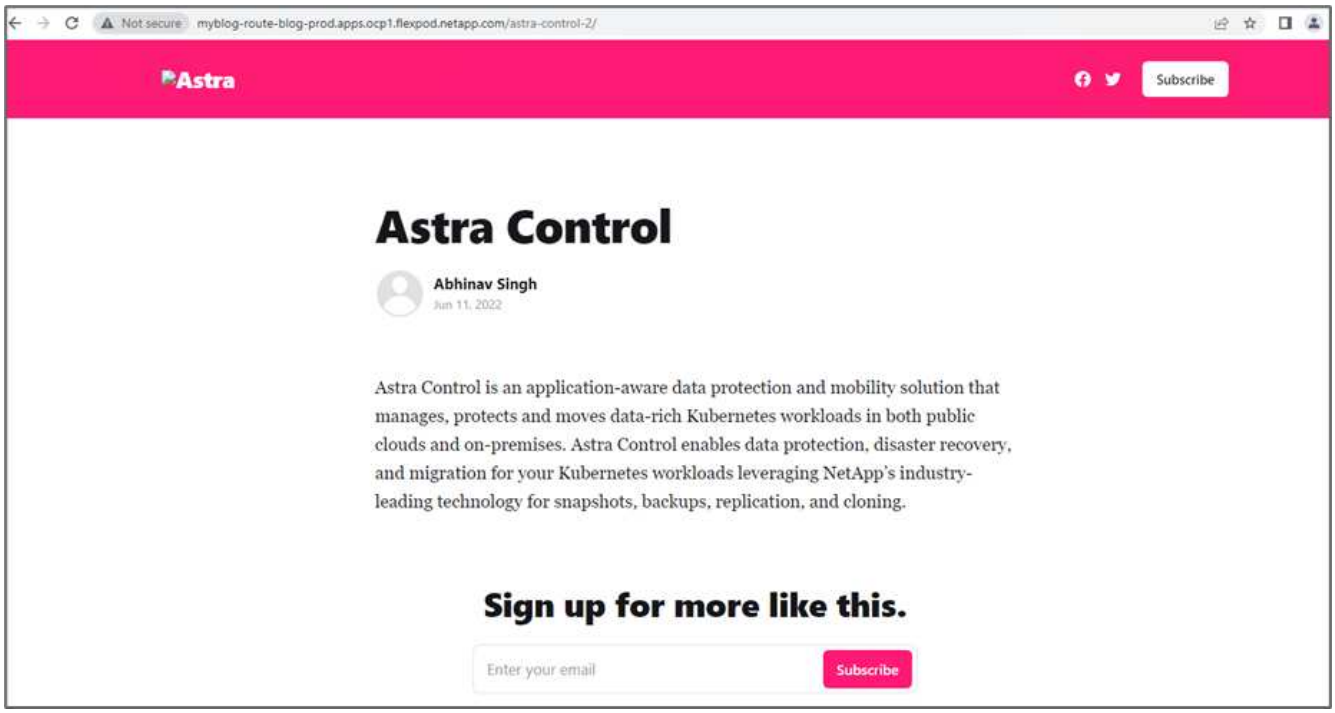
Im OpenShift-Cluster in der Produktion wird nun ein neuer Applikationsklon bereitgestellt.



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

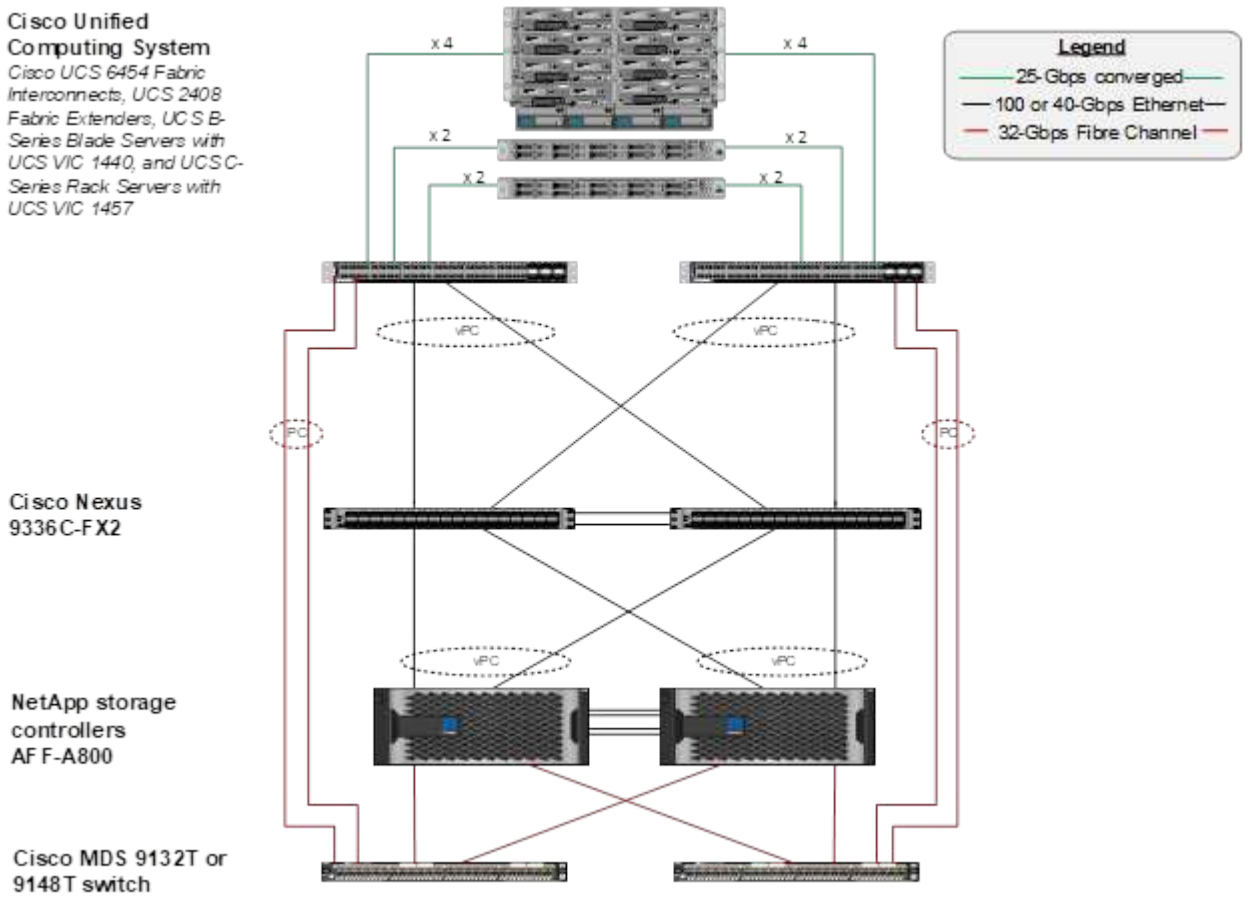
Damit Cloud Insights Daten sammeln kann, muss ein Unternehmen eine Erfassungseinheit als virtuelle oder physische Maschine entweder innerhalb seiner FlexPod-Datacenter-Umgebung oder an einem Ort bereitstellen, an dem die IT-Abteilung die Komponenten kontaktieren kann, von denen sie Daten erfassen. Sie 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

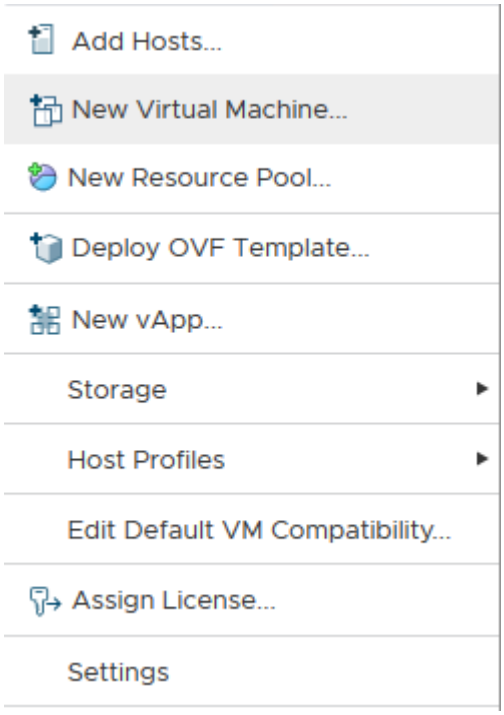
So melden Sie sich für den NetApp Cloud Insights Service an:

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

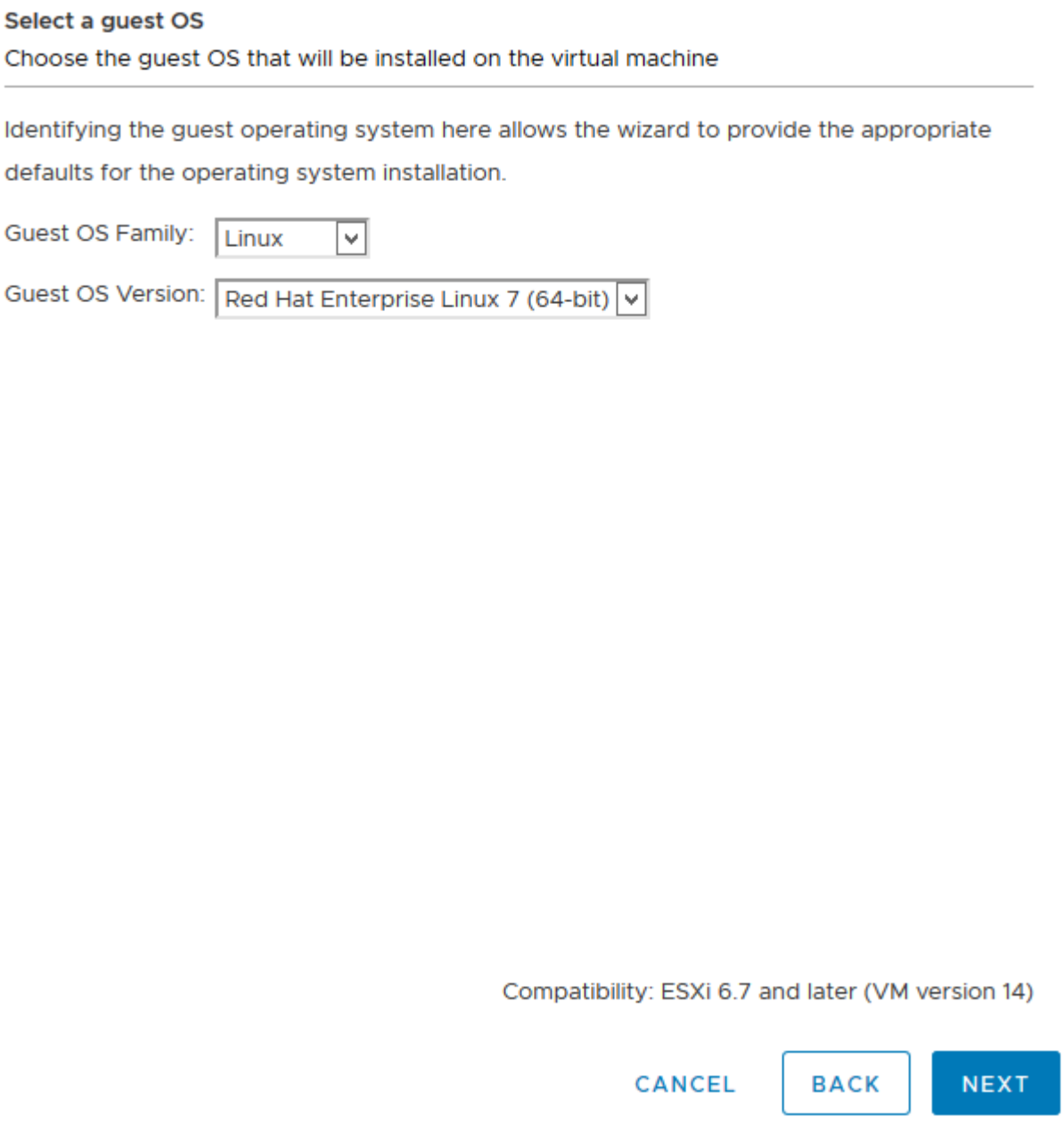
Gehen Sie wie folgt vor, um eine VMware VM zu erstellen, die als Erfassungseinheit konfiguriert werden soll:

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).



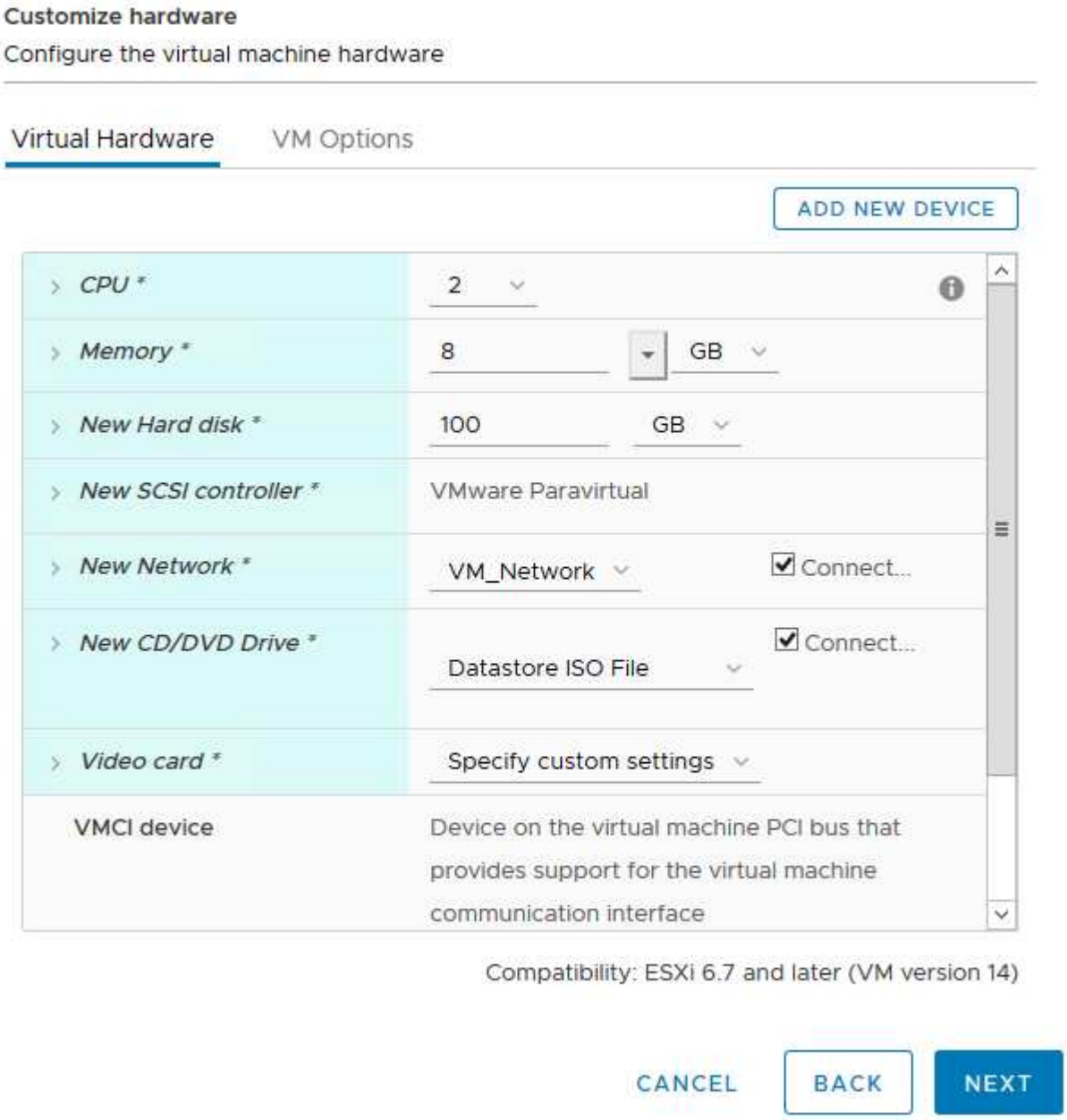
9. Die nächste Seite ermöglicht die Anpassung der Hardwareressourcen auf der VM. Für die Cloud Insights-Erfassungseinheit sind die folgenden Ressourcen erforderlich: Klicken Sie nach Auswahl der Ressourcen auf Weiter:
   a. Zwei CPUs

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.

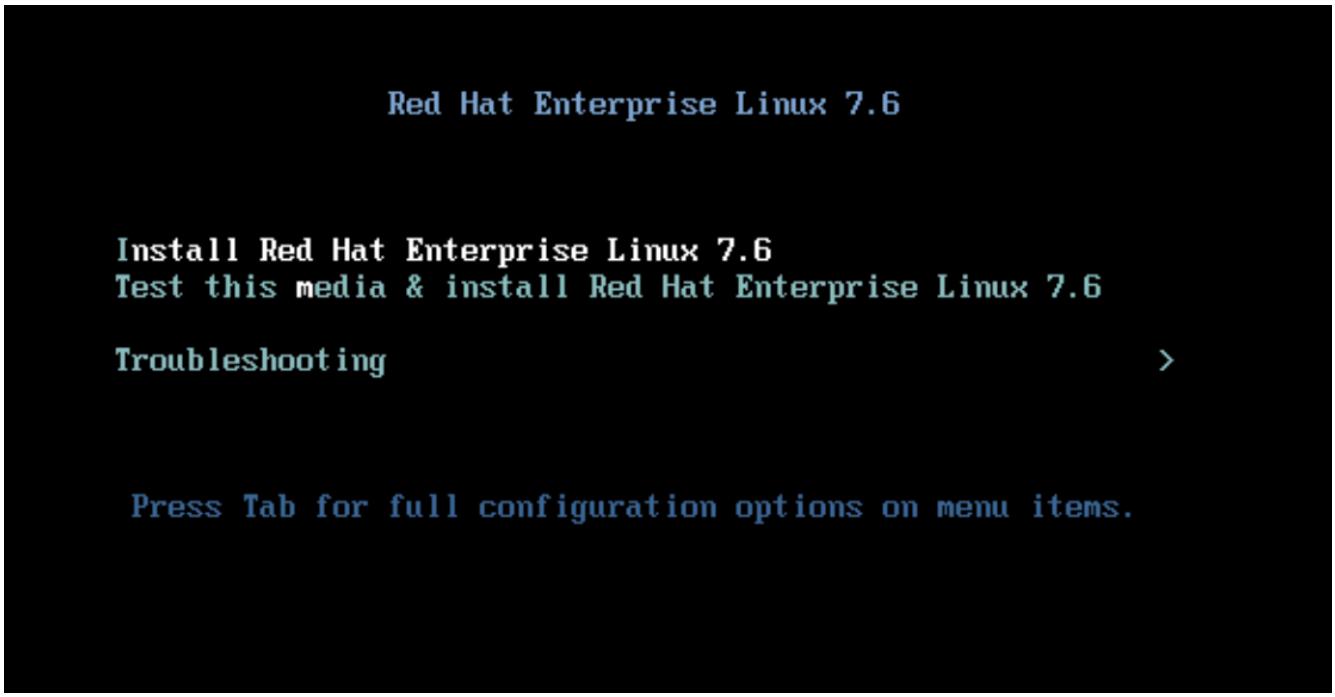


10. Überprüfen Sie zum Erstellen der VM auf der Seite bereit zum Abschließen die Einstellungen, und klicken Sie auf Fertig stellen.

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.



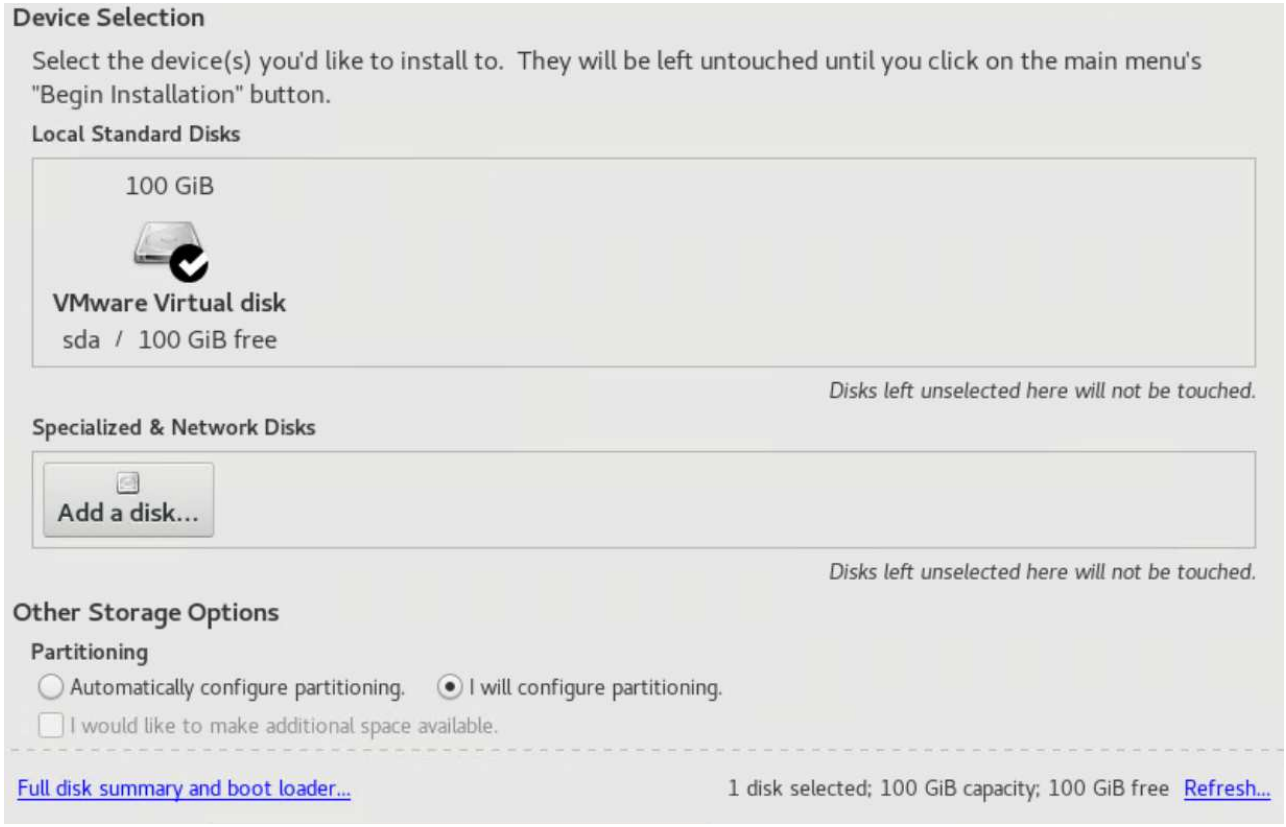
2. Wählen Sie die gewünschte Sprache aus, und klicken Sie auf Weiter.

   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:

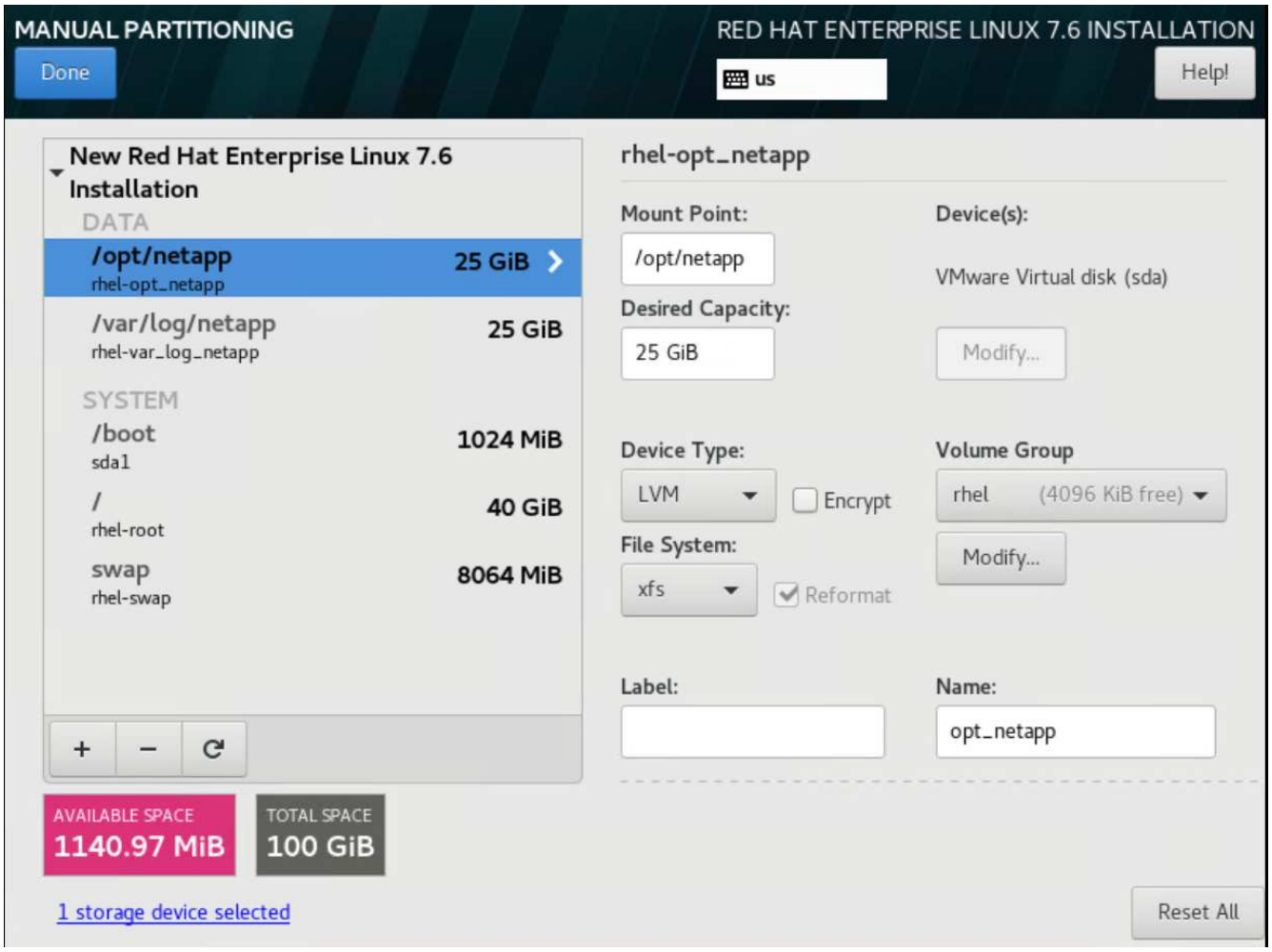
   a. Um die Partitionierung für den Server anzupassen, klicken Sie auf Installationsziel.

   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.



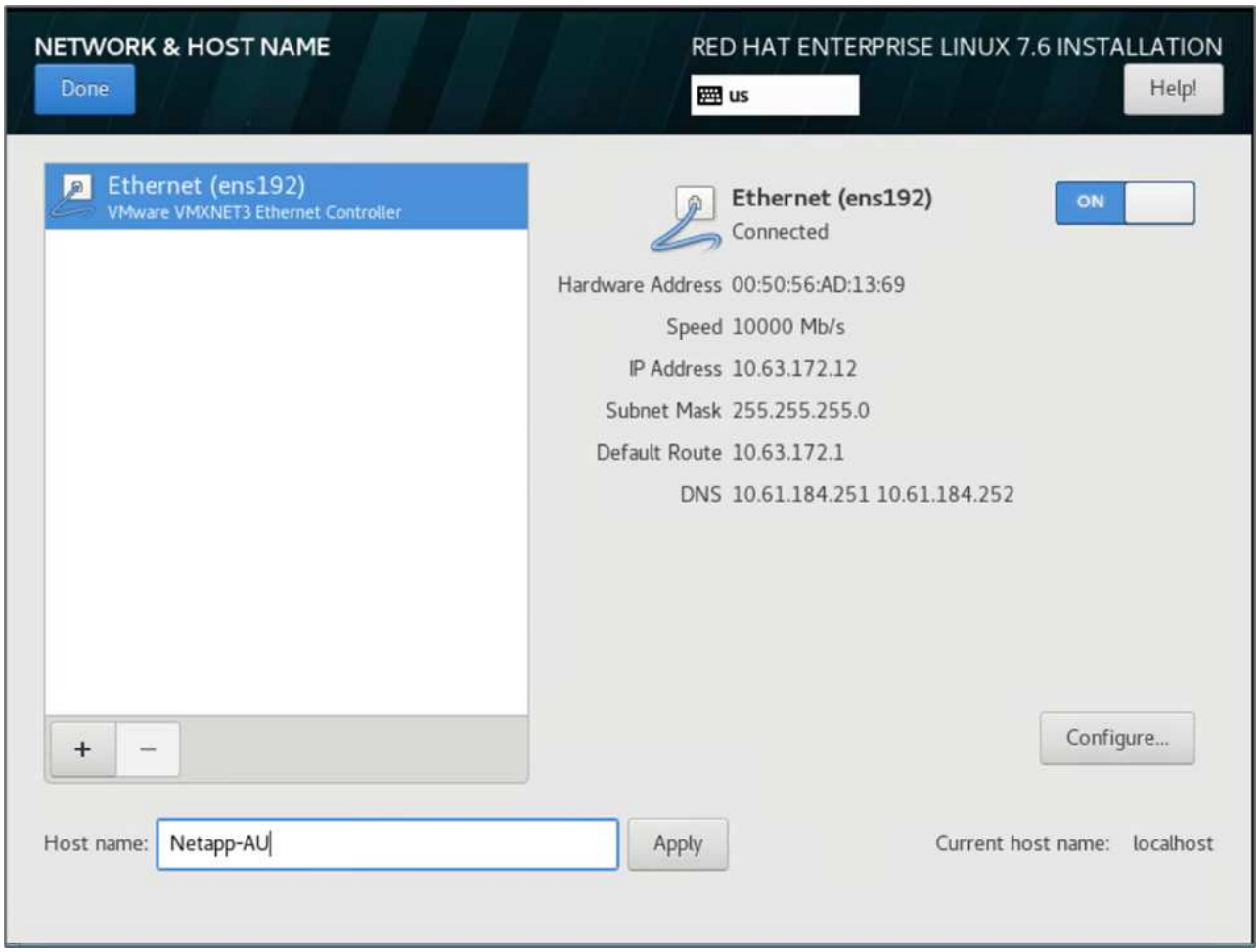
c. Klicken Sie Auf Fertig.

   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.



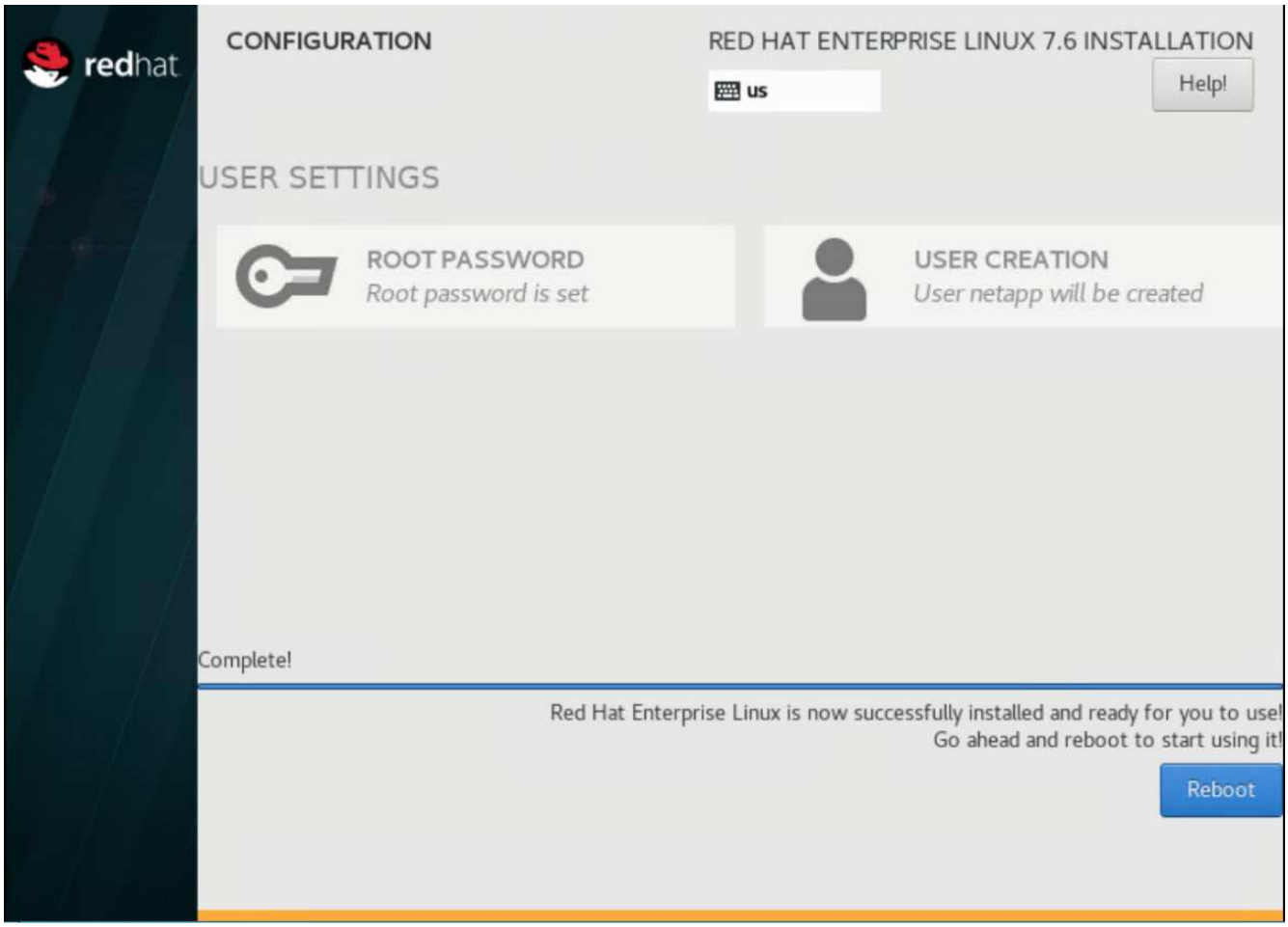
a. Um zur Installationsübersicht zurückzukehren, klicken Sie auf „Fertig“.

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 ~]#
```

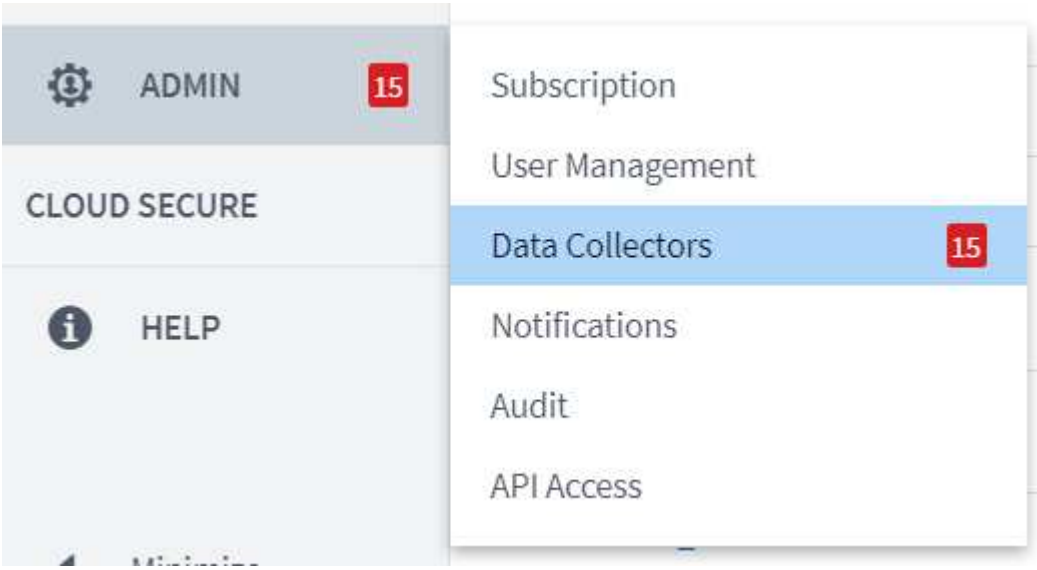
8. Fügen Sie ein verfügbares Abonnement für Red hat Enterprise Linux bei.

```
[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.

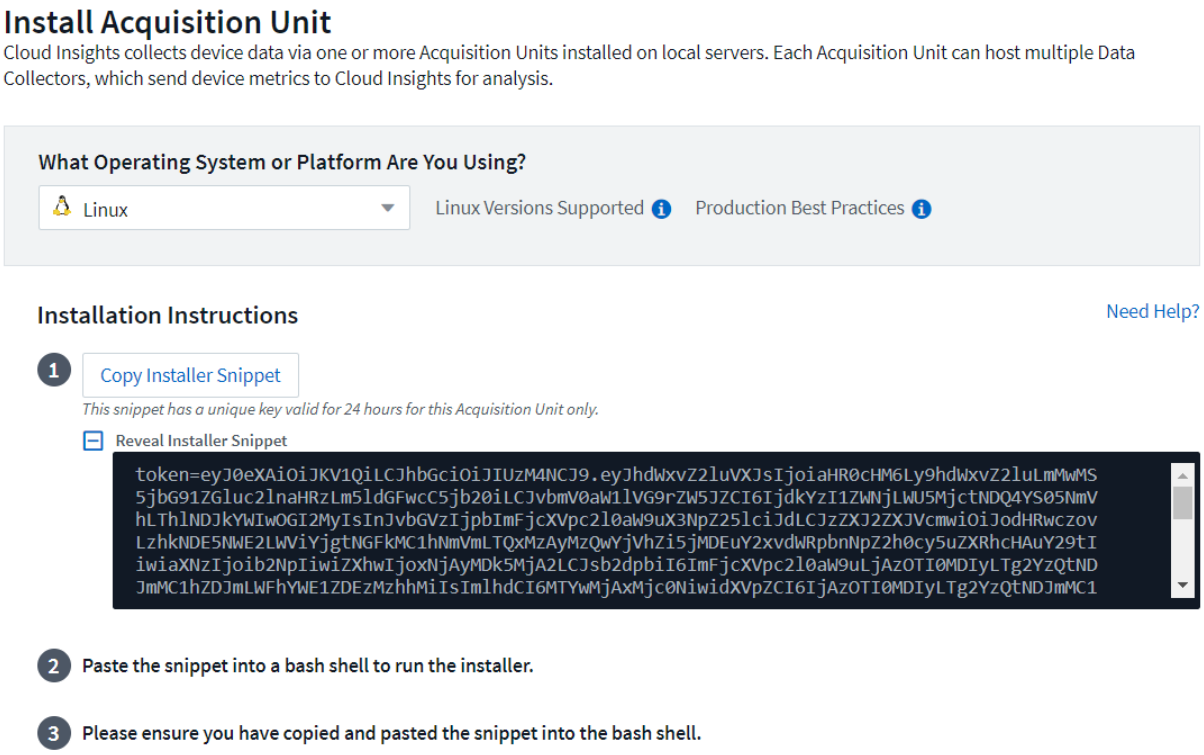


2. Klicken Sie in der oberen Mitte der Seite Data Collectors auf den Link für Acquisition Units.

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.

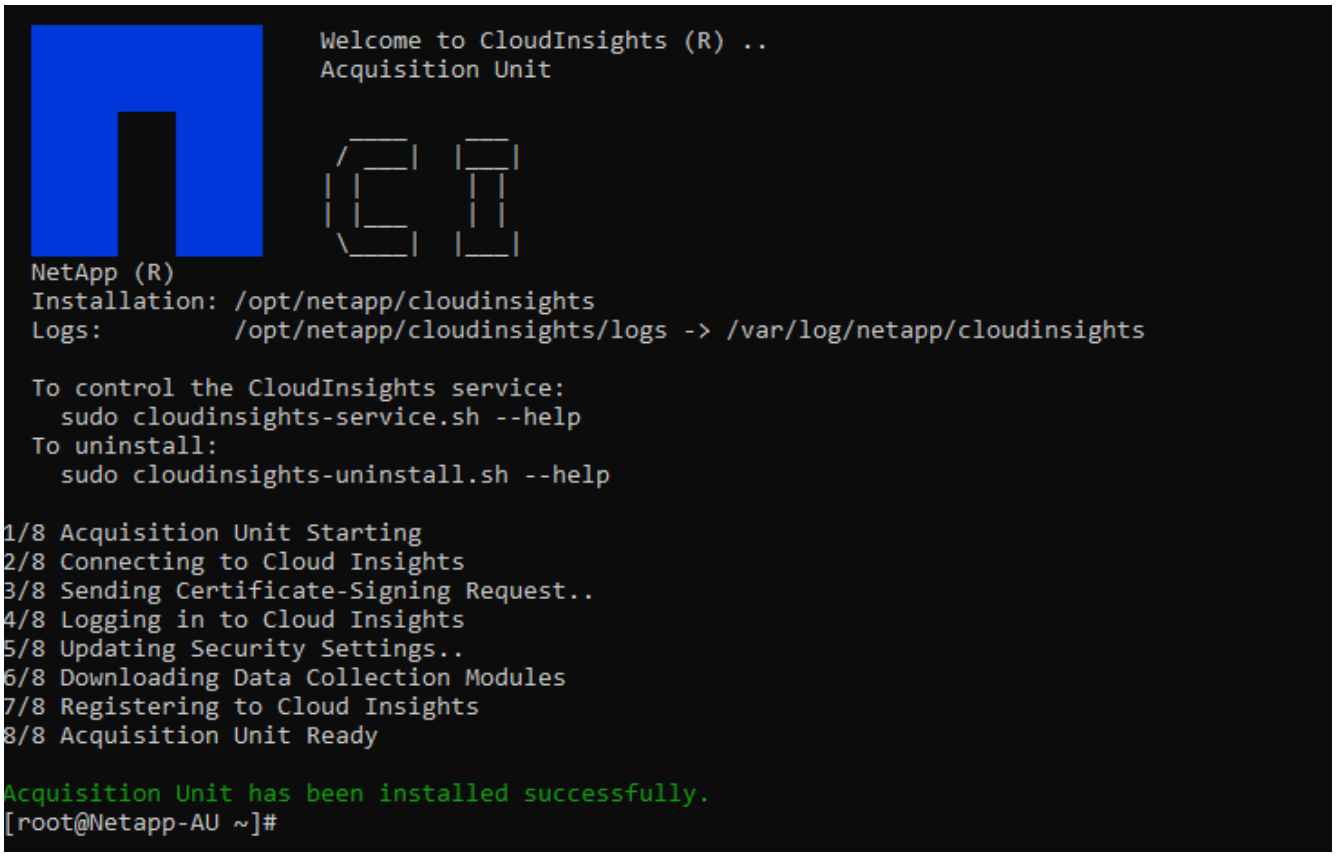
   In diesem Beispiel handelt es sich um einen Linux-Server, der ein Snippet und ein Token zum Einfügen in die CLI auf unserem Host bereitstellt. Auf der Webseite wird darauf gewartet, dass die Erfassungseinheit eine Verbindung herstellt.



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"
```

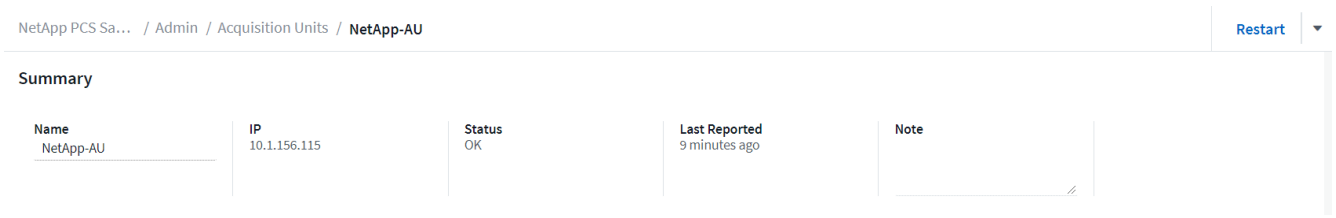
Das Installationsprogramm lädt ein komprimiertes Paket herunter und beginnt mit der Installation. Nach Abschluss der Installation erhalten Sie eine Nachricht, die besagt, dass die Erwerbseinheit bei NetApp Cloud Insights registriert wurde.



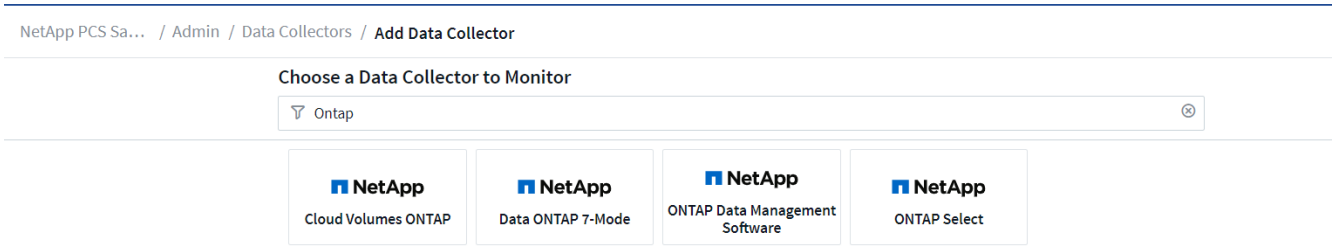
Fügen Sie das überwachte Storage-System vom FlexPod Datacenter zu Cloud Insights hinzu

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.

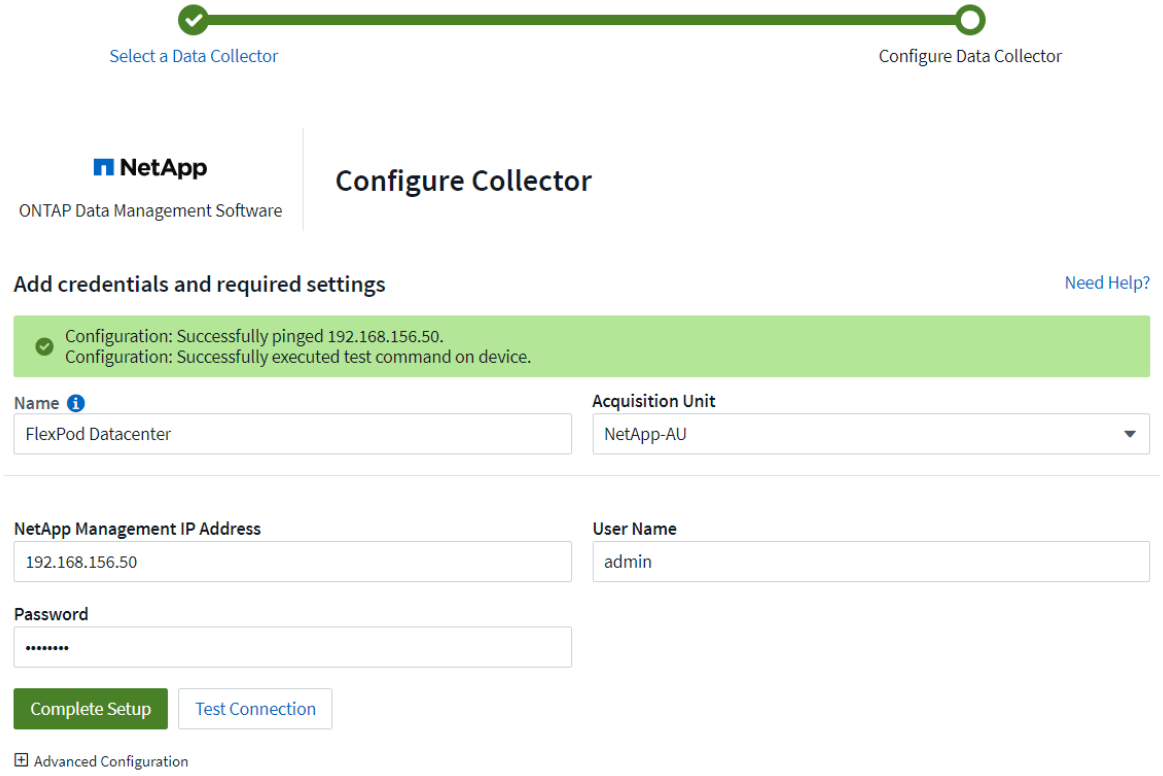


2. Um einen Assistenten zum Hinzufügen des Speichersystems zu starten, klicken Sie auf der Seite Zusammenfassung auf die Schaltfläche zum Erstellen eines Datensammlers. Auf der ersten Seite werden alle Systeme angezeigt, aus denen Daten erfasst werden können. Verwenden Sie die Suchleiste, um nach ONTAP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



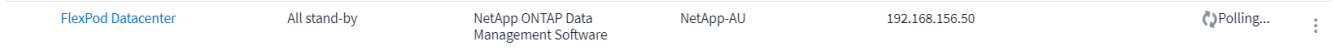
3. Wählen Sie ONTAP Datenmanagement-Software.

   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

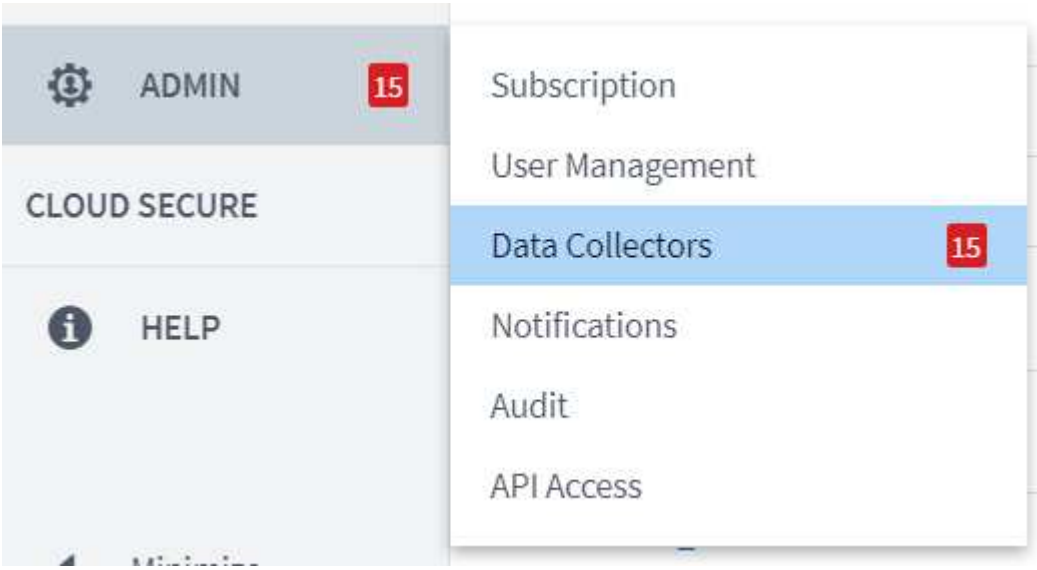
Active IQ Integration

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.

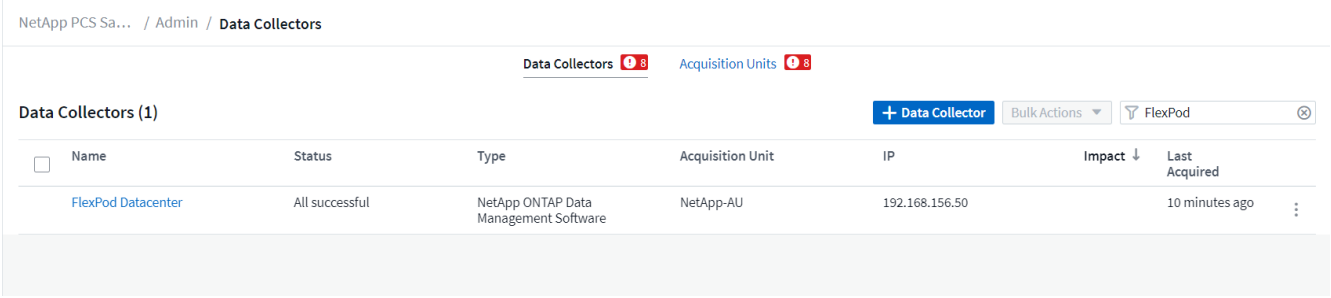
Greifen Sie über das Cloud Insights Dashboard auf Active IQ-Informationen zu

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

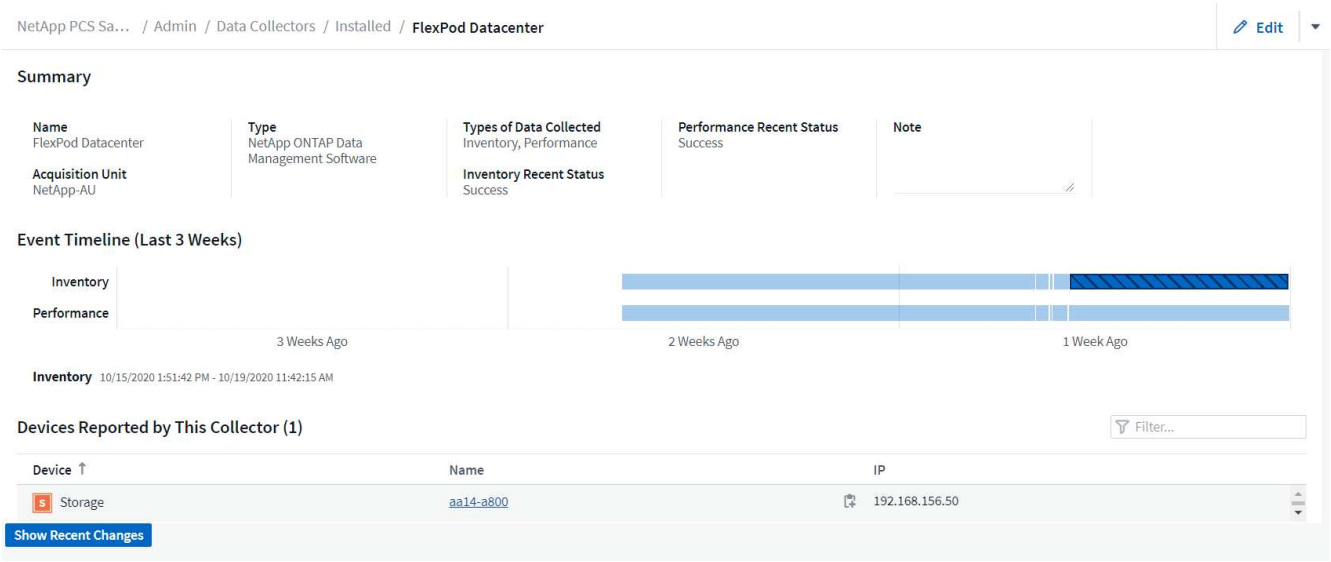
1. Klicken Sie auf die Option Data Collector im Menü Admin auf der linken Seite.



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

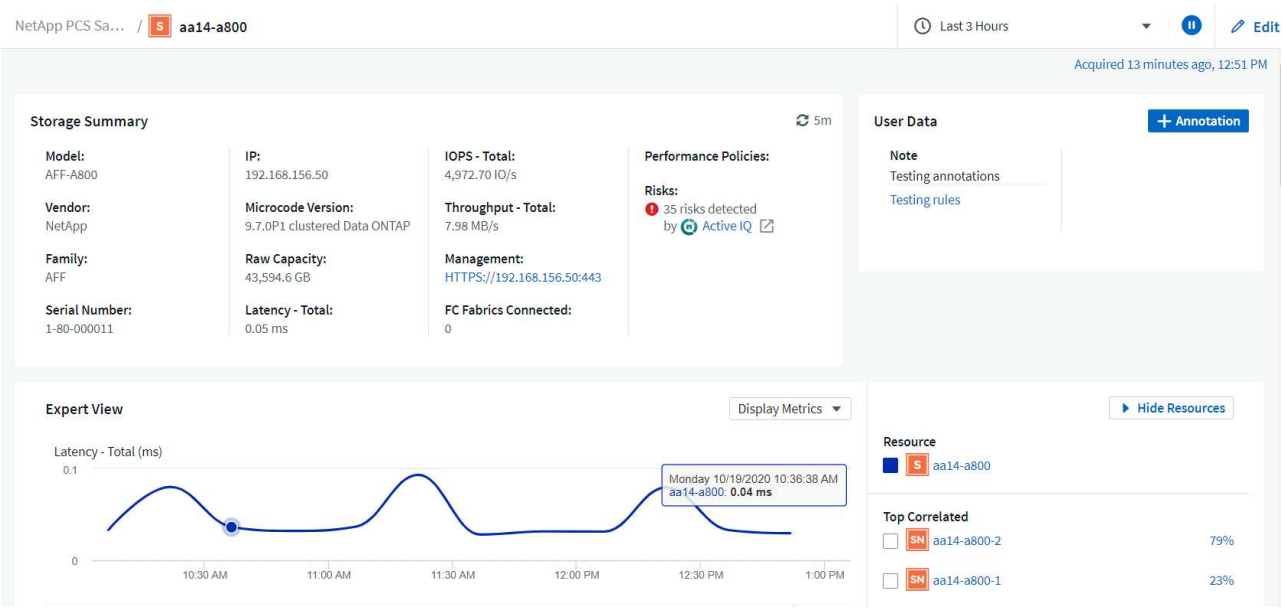


3. Klicken Sie auf den Data Collector, um eine Übersicht über die Umgebung und die Geräte zu erhalten, die von diesem Collector überwacht werden.

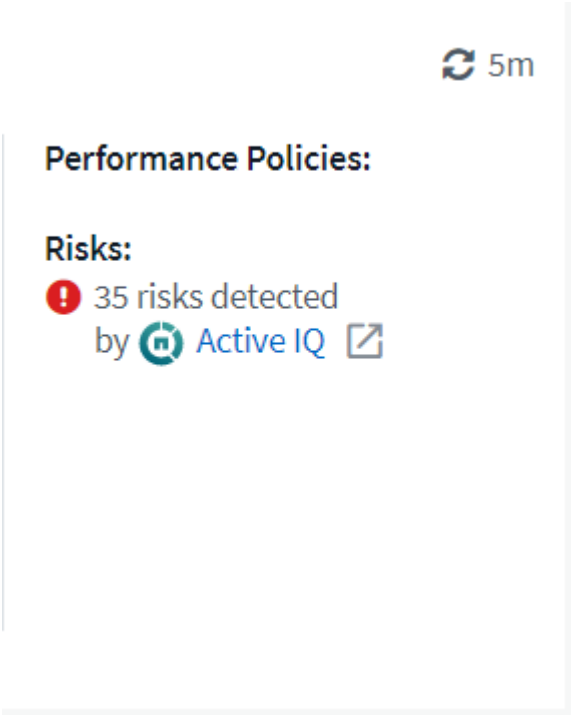


Klicken Sie unter der Geräteliste unten auf den Namen des überwachten ONTAP Storage-Systems. Auf diese Weise wird ein Dashboard mit Informationen angezeigt, die über das System erfasst wurden. Dazu gehören folgende Details:

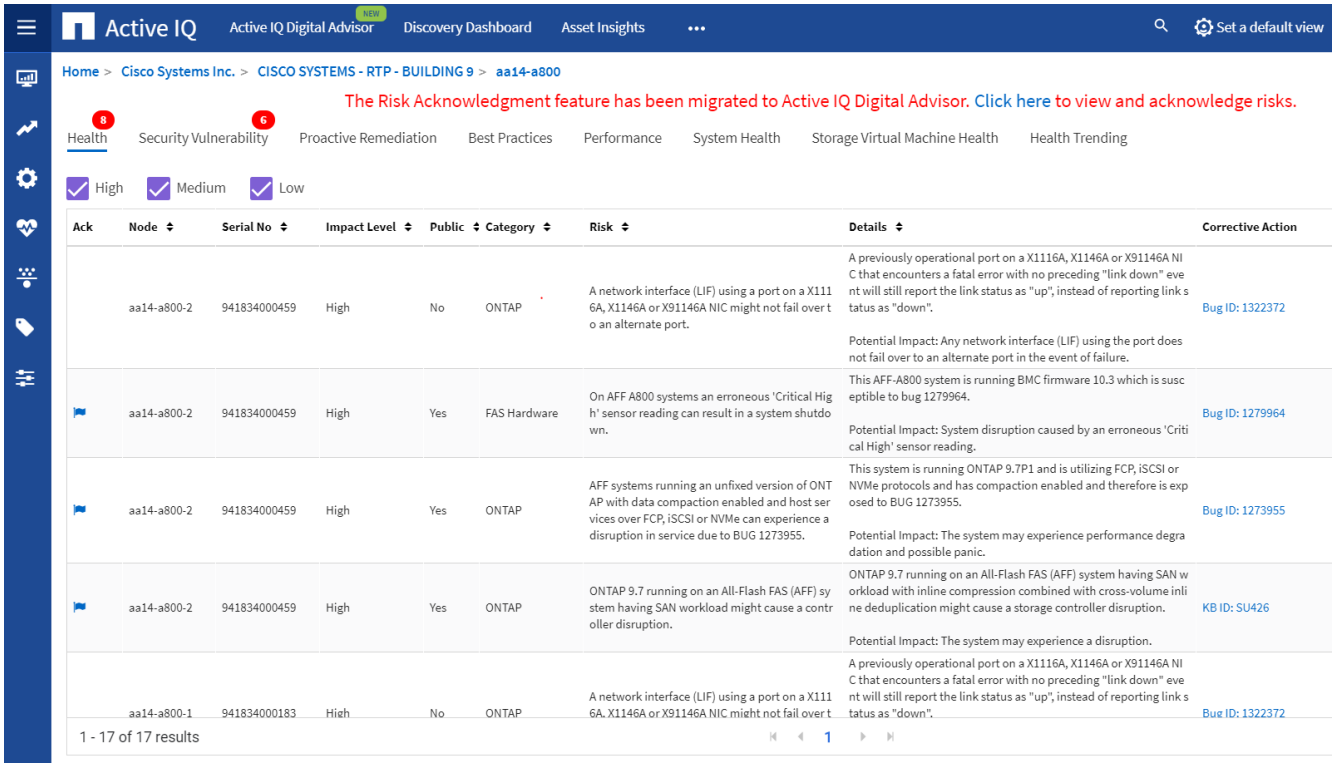
- Modell
- Familie
- ONTAP-Version
- Bruttokapazität
- IOPS-Durchschnitt
- Durchschnittliche Latenz
- Durchschnittlicher Durchsatz



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.

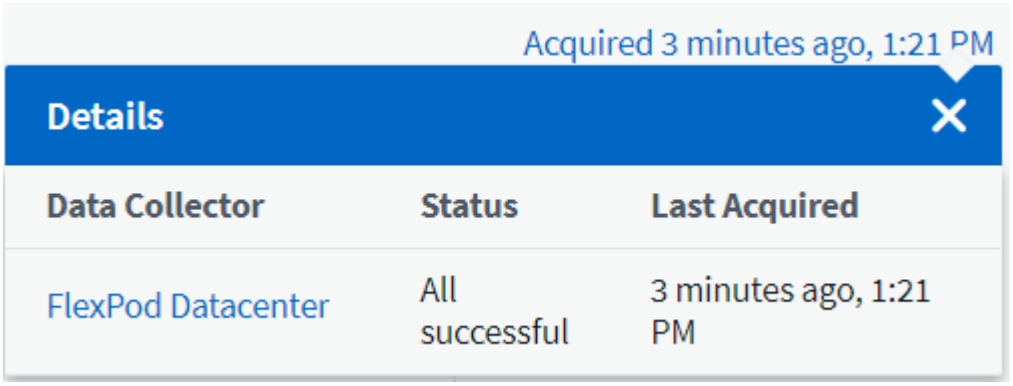


Dashboards in Echtzeit

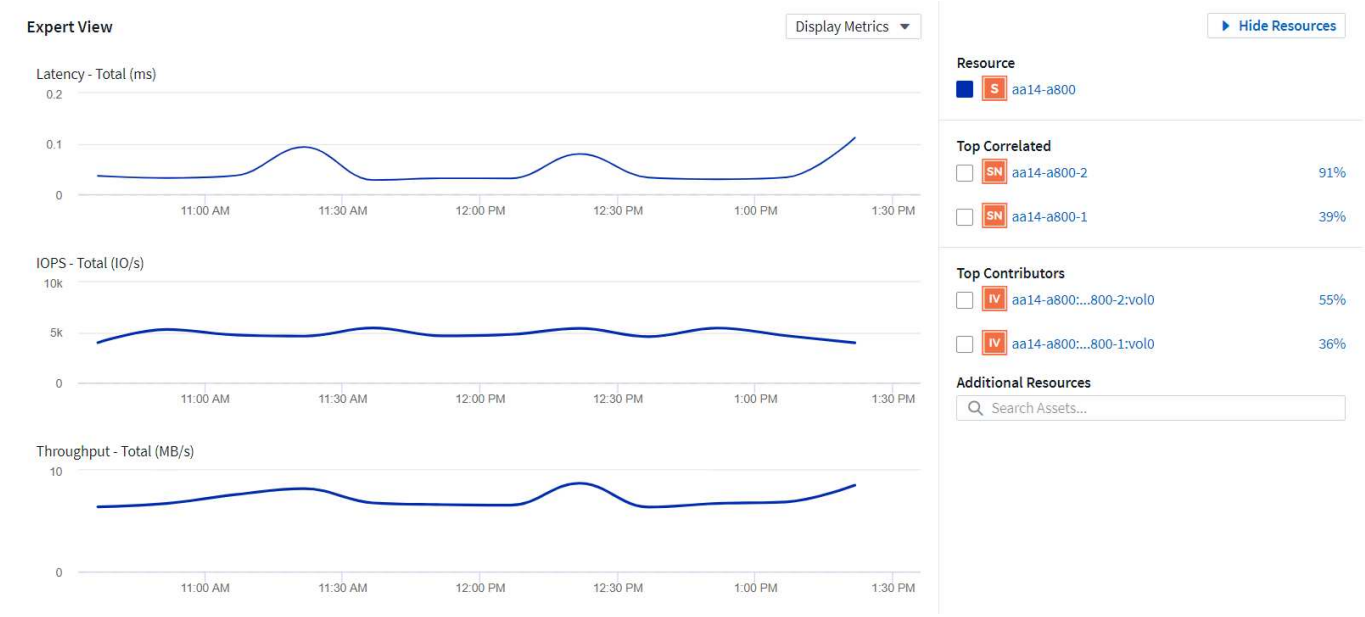
Cloud Insights bietet Echtzeit-Dashboards mit Informationen, die von dem in einer FlexPod Datacenter-Lösung implementierten ONTAP Storage-System abgefragt wurden. Die Cloud Insights-Erfassungseinheit erfasst Daten in regelmäßigen Abständen und füllt das Standard-Storage-System-Dashboard mit den erfassten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

Zugriff auf Echtzeitdiagramme über das Cloud Insights Dashboard

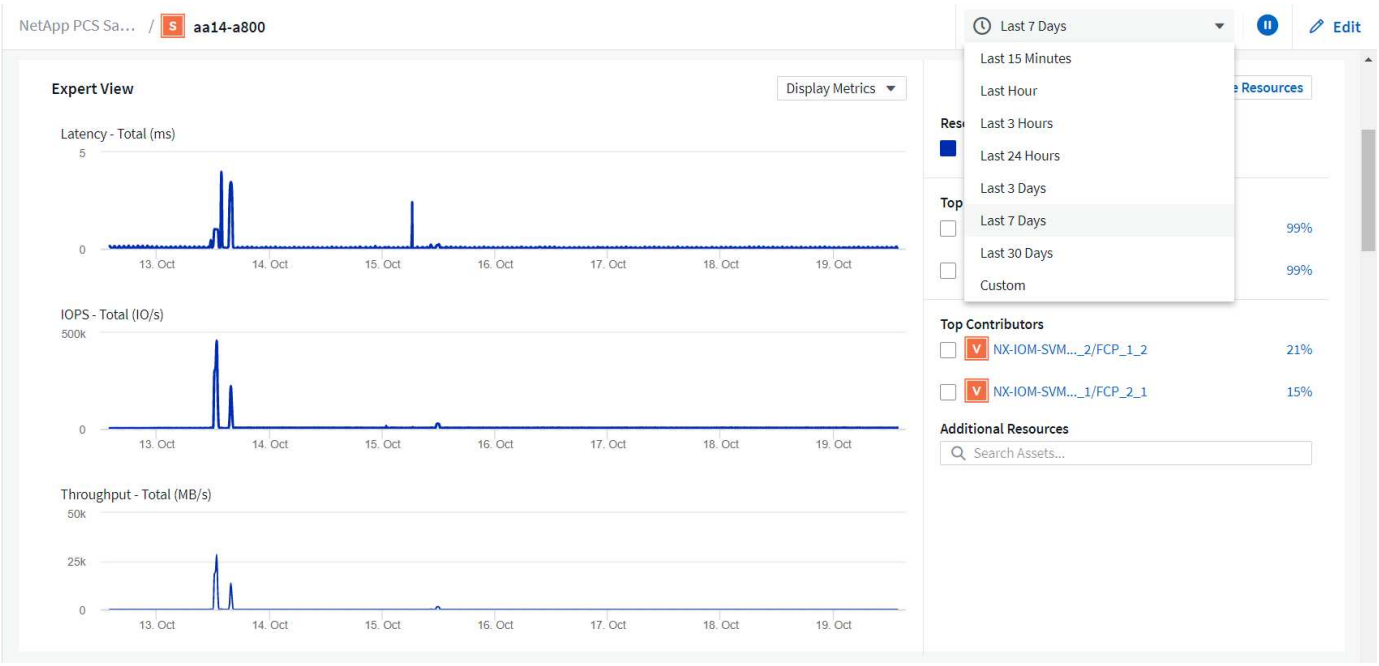
Im Dashboard des Speichersystems wird angezeigt, wenn der Data Collector die Informationen zuletzt aktualisiert hat. Ein Beispiel hierfür ist in der Abbildung unten dargestellt.



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.



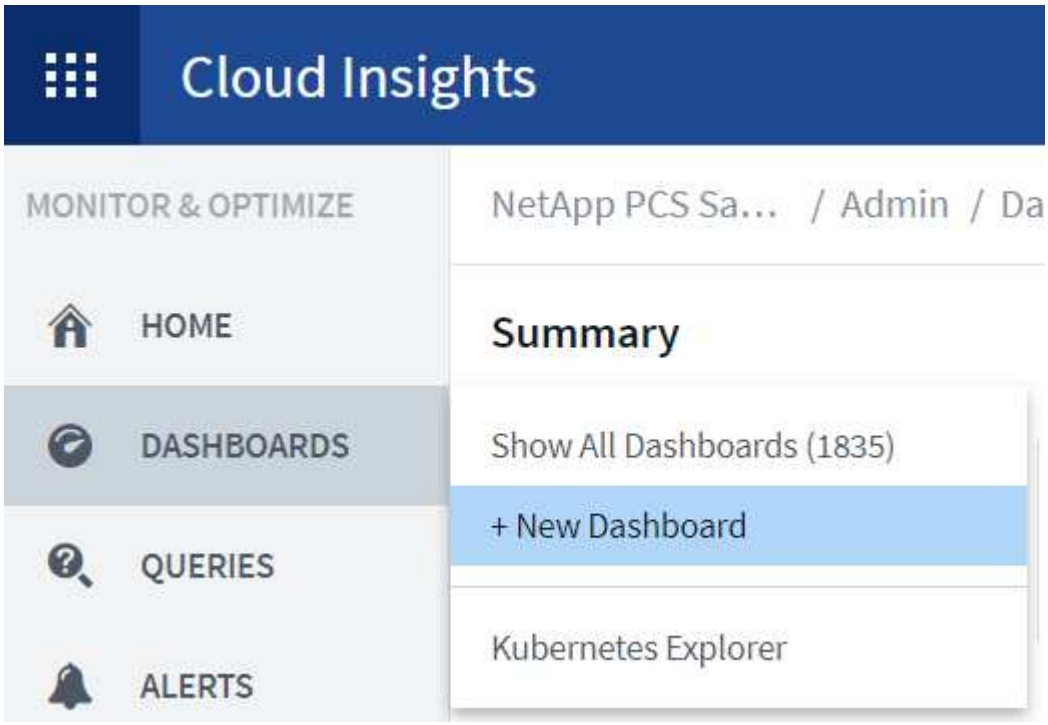
Erstellen benutzerdefinierter Dashboards

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

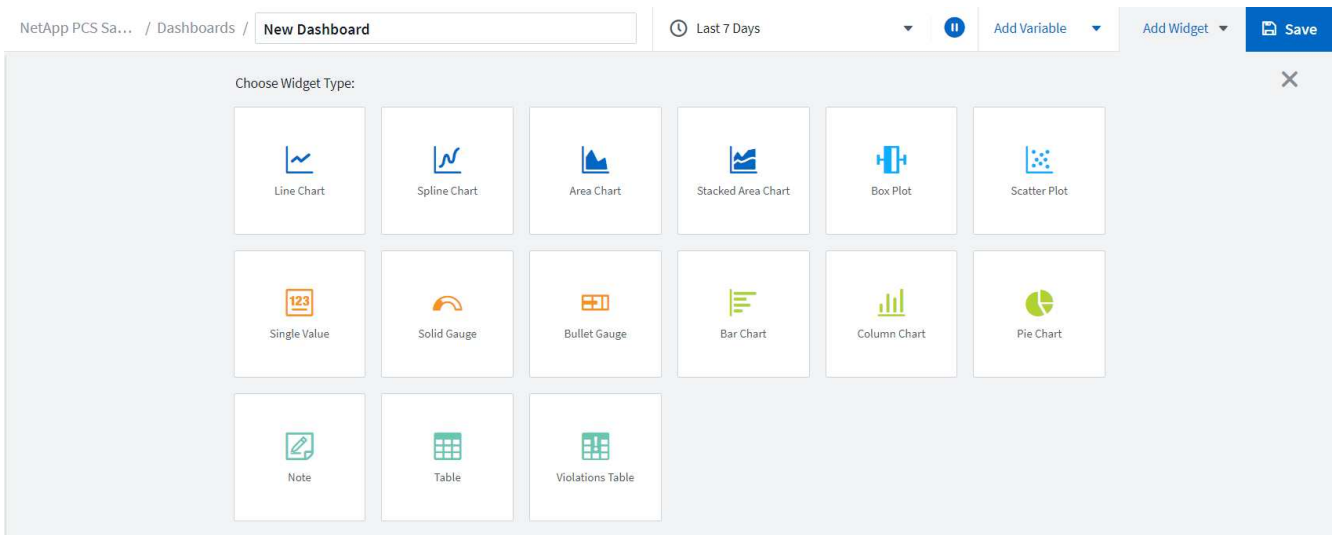
Gehen Sie wie folgt vor, um ein angepasstes Dashboard zur Bewertung von Storage-Ressourcen zu erstellen:

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.



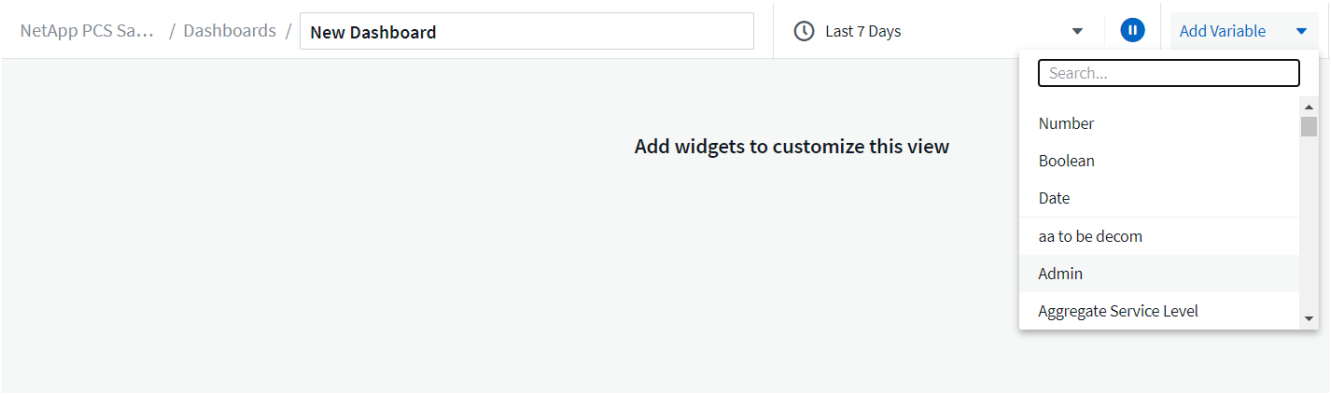
   Das Fenster Neues Dashboard wird geöffnet.

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.

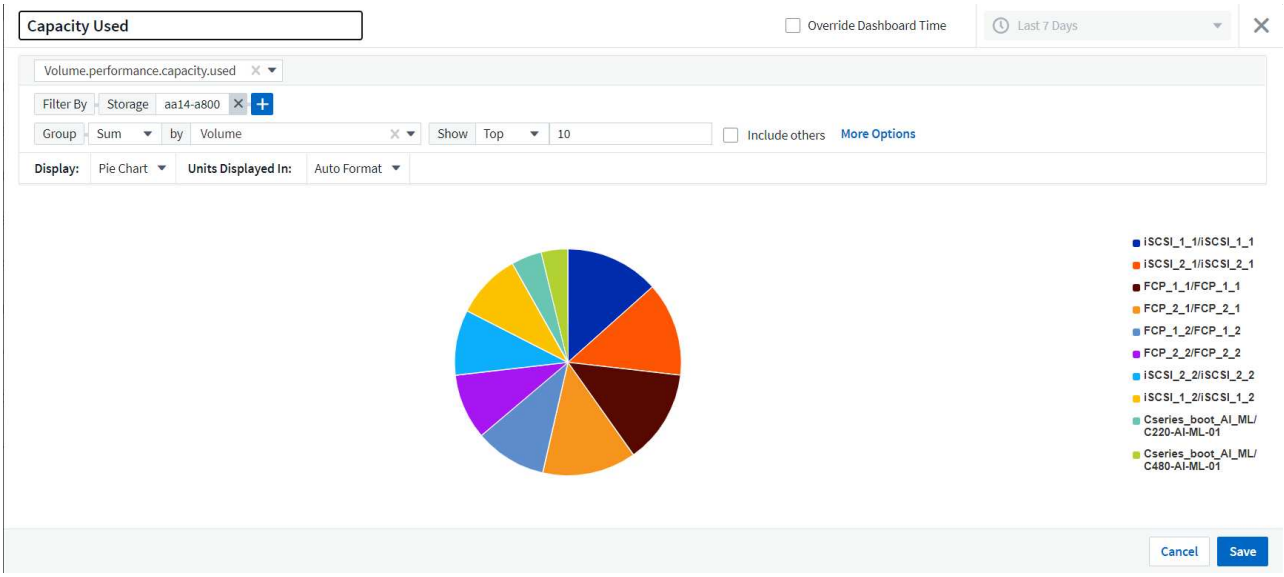
   b. Benennen Sie das Widget mit einer beschreibenden Kennung, z. B. `Capacity Used`.

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

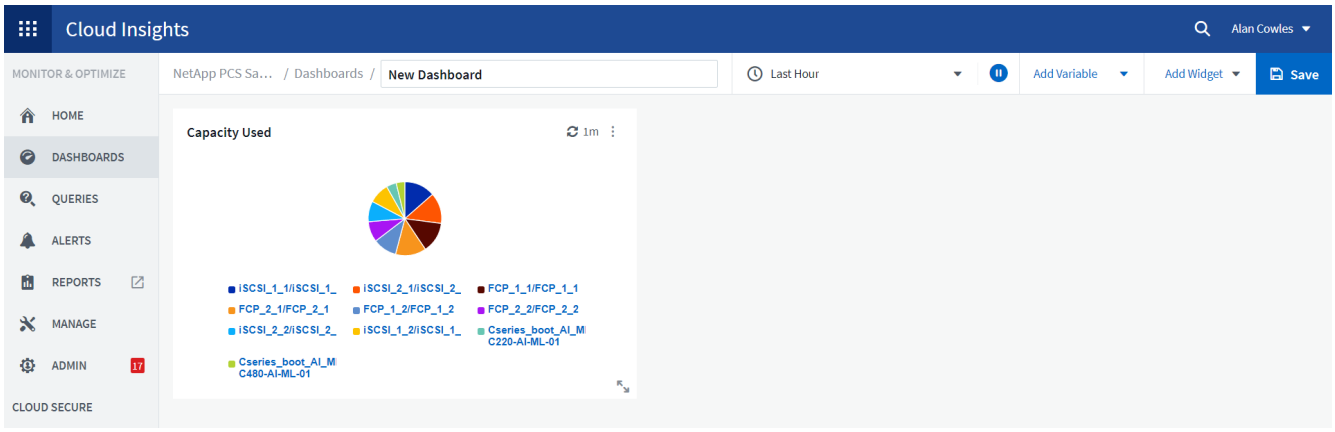
   d. Um nach Storage-Systemen zu filtern, verwenden Sie den Filter, und geben Sie den Namen des Storage-Systems in der FlexPod Datacenter Lösung ein.

   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.

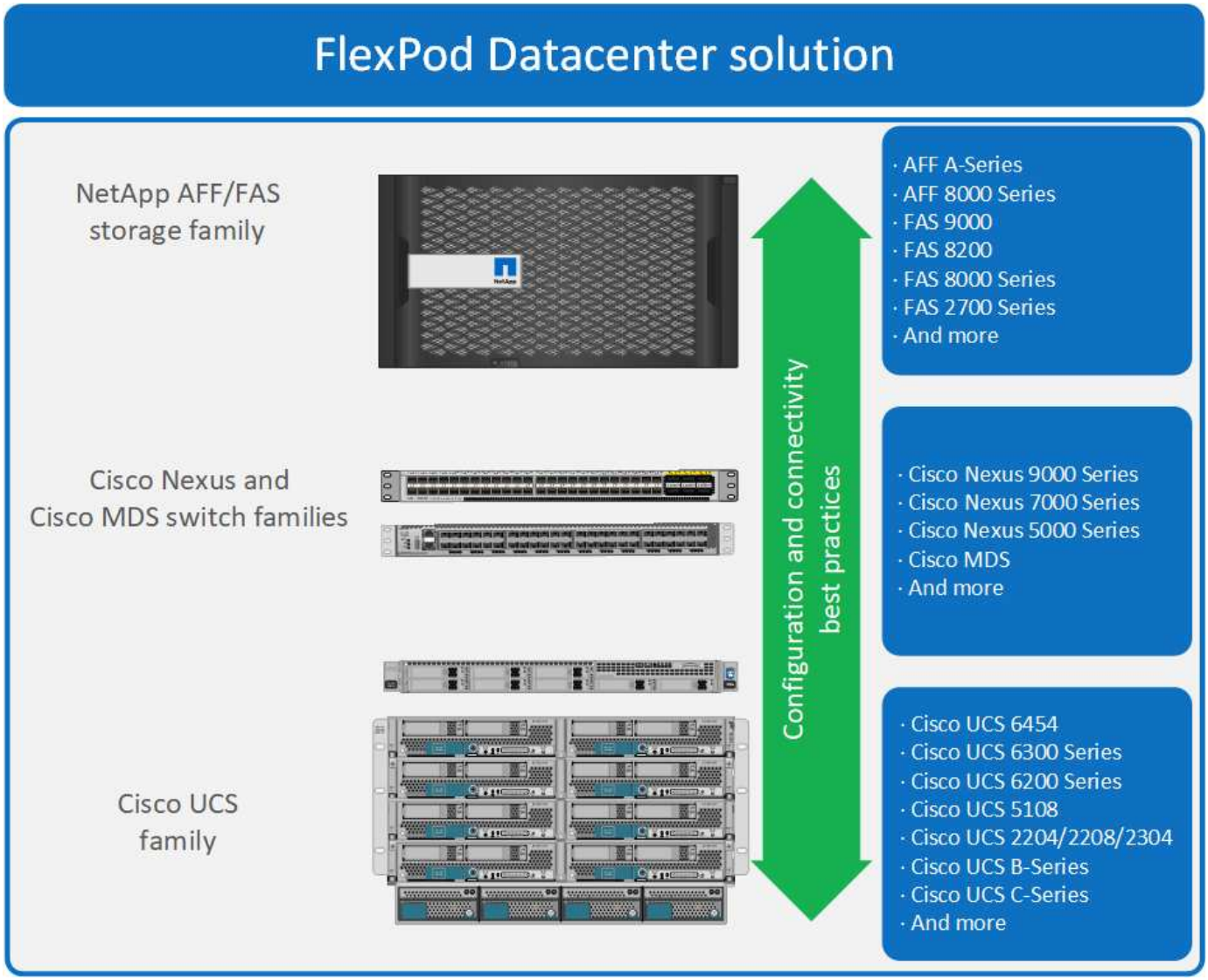
Weitere Informationen zu FlexPod finden Sie in "TR-4036 FlexPod Datacenter – Technische Spezifikationen".

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.

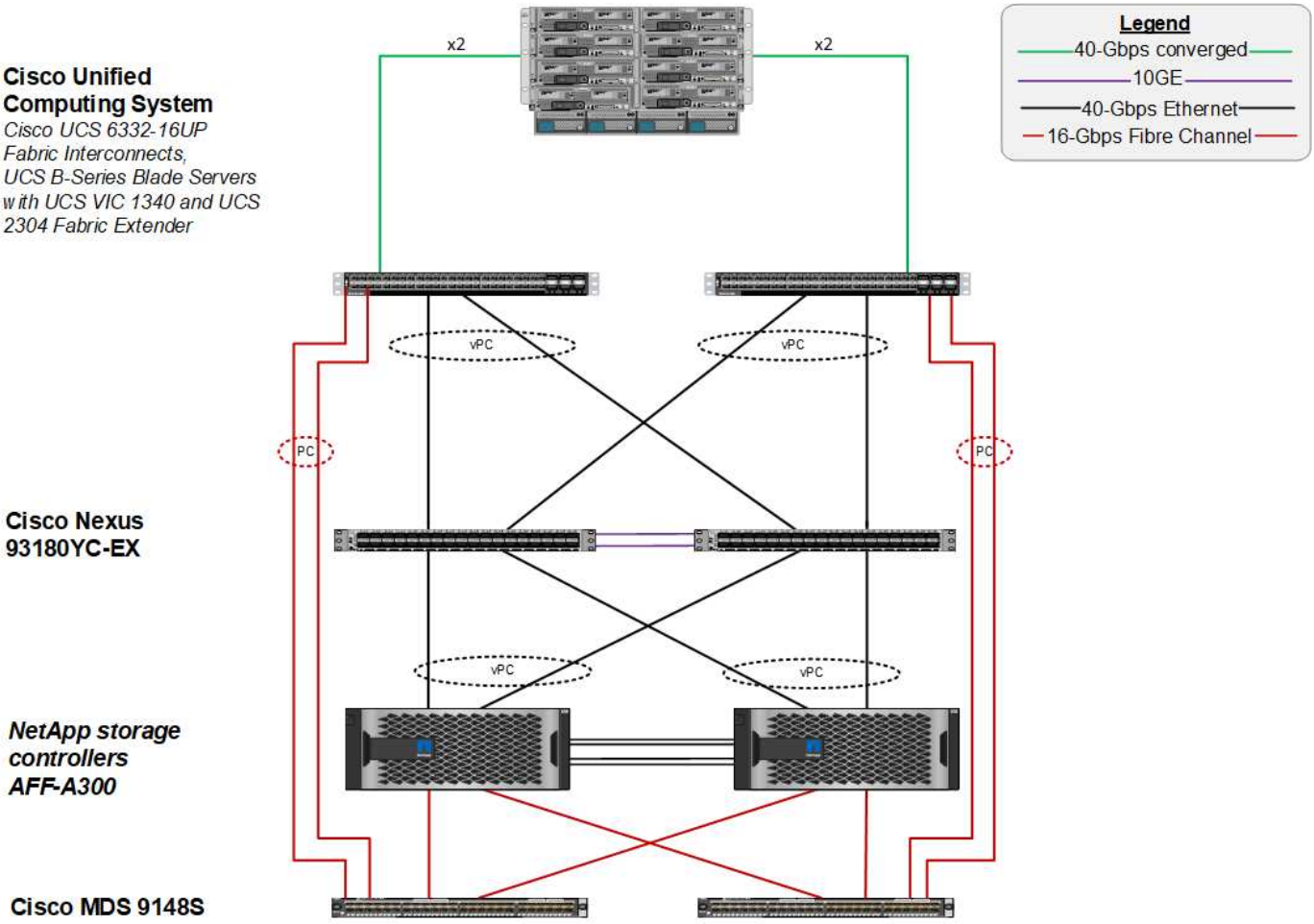


Architektur von FlexPod

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.

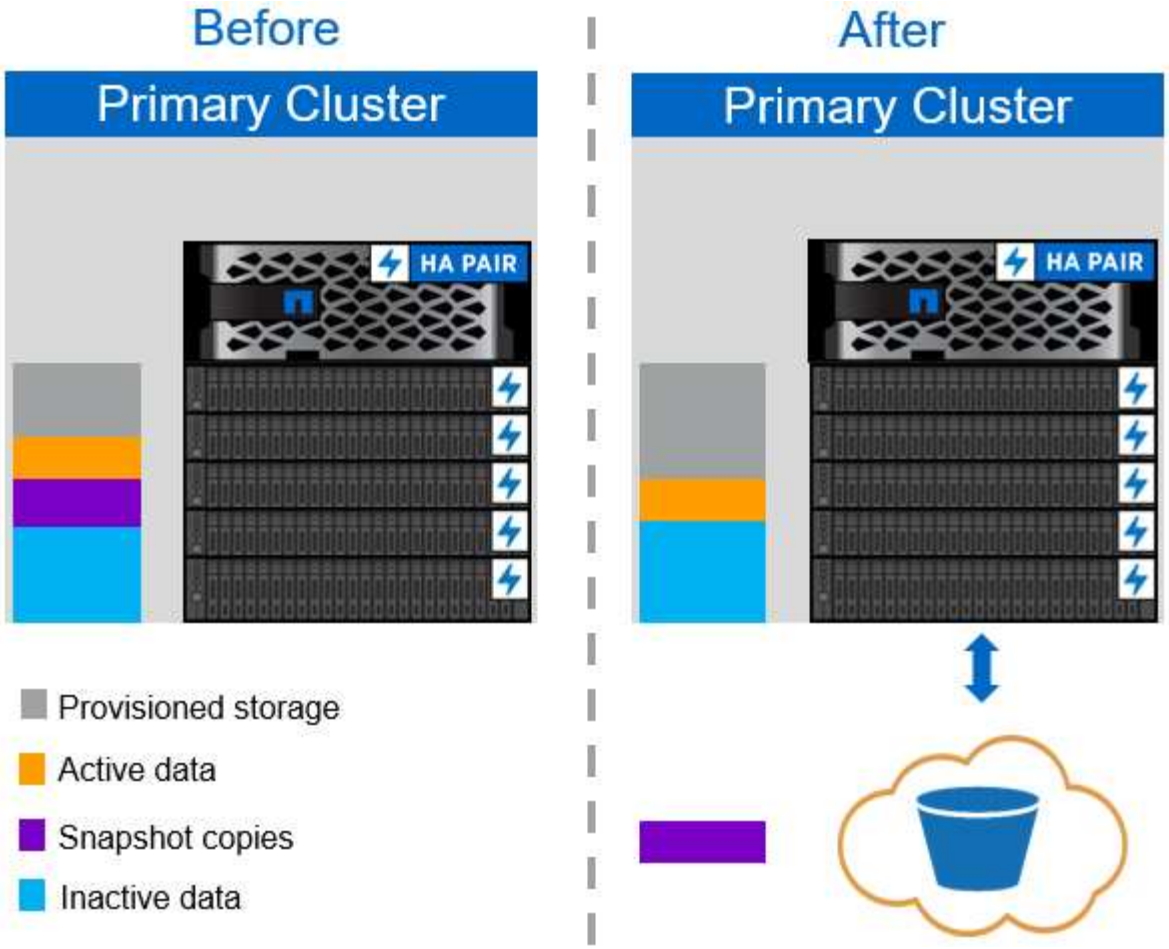
Wenn die Performance-Tier-Auslastung bei einer Kapazität von mehr als 70 % liegt, werden kalte Daten direkt aus der Cloud-Tier gelesen, ohne zurück in die Performance-Tier geschrieben zu werden. Durch Verhinderung von Datenschreibbacks auf stark ausgelasteten Aggregaten erhält FabricPool das Aggregat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

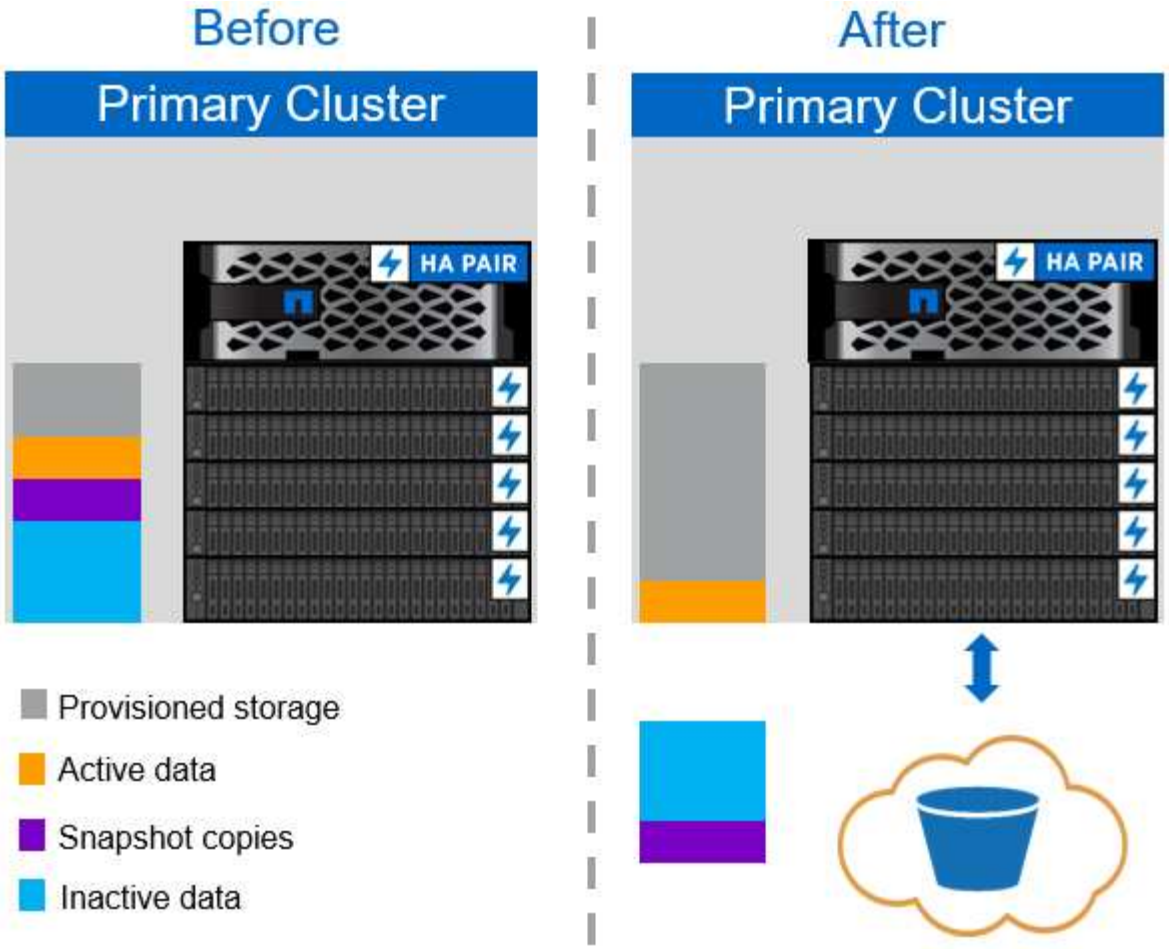


Automatisches Tiering

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.

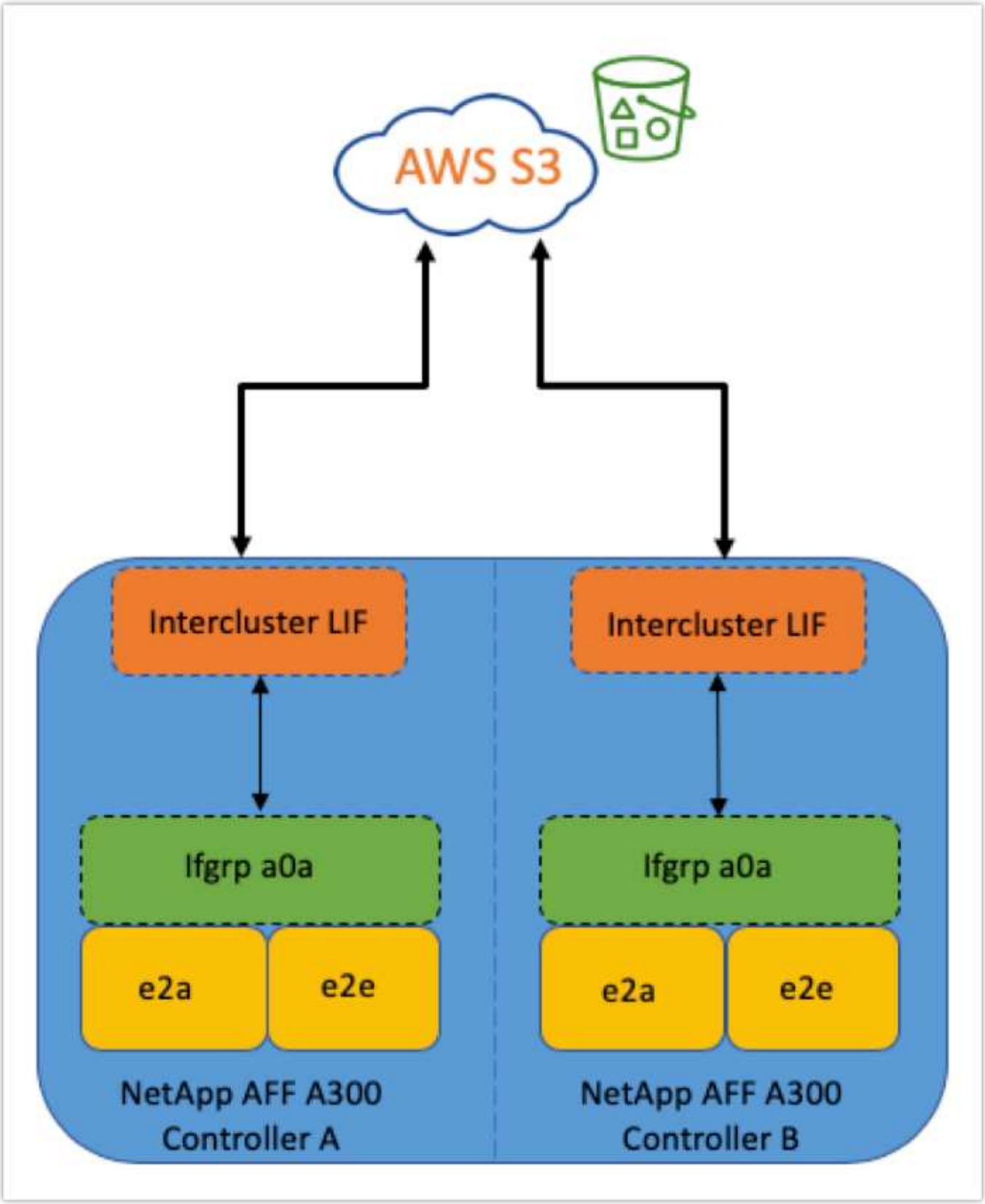
Wenn mehr als eine Intercluser LIF auf einem Node mit unterschiedlichem Routing verwendet wird, empfiehlt NetApp, sie in verschiedenen IPspaces zu platzieren. Während der Konfiguration kann FabricPool aus mehreren IPspaces auswählen, es ist jedoch nicht in der Lage, bestimmte Intercluster LIFs innerhalb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

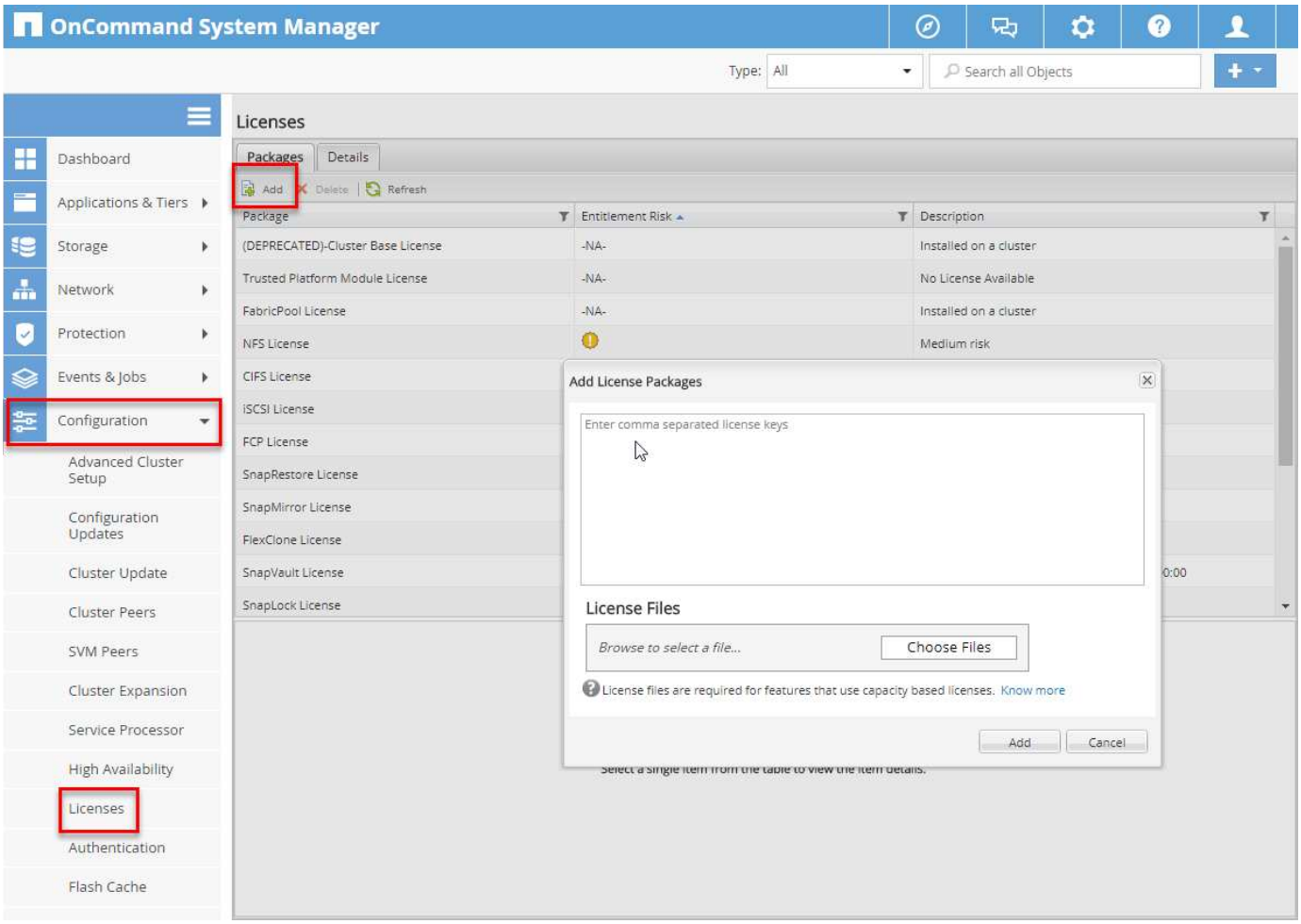
1. Installieren Sie eine FabricPool Lizenz.
2. Erstellen eines AWS S3-Objektspeicher-Buckets
3. Hinzufügen einer Cloud-Tier zu ONTAP
4. Verbinden Sie die Cloud-Tier mit einem Aggregat.
5. Legen Sie die Tiering-Richtlinie für Volumes fest.

"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.



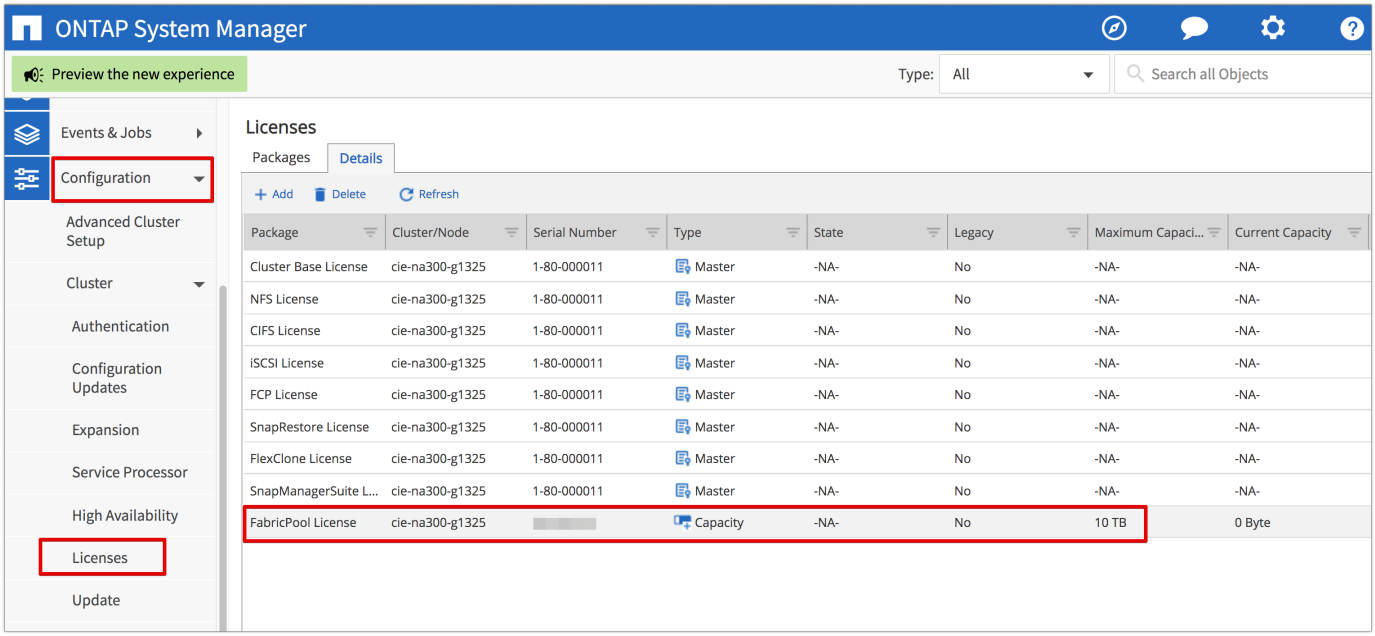
Lizenzkapazität

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"

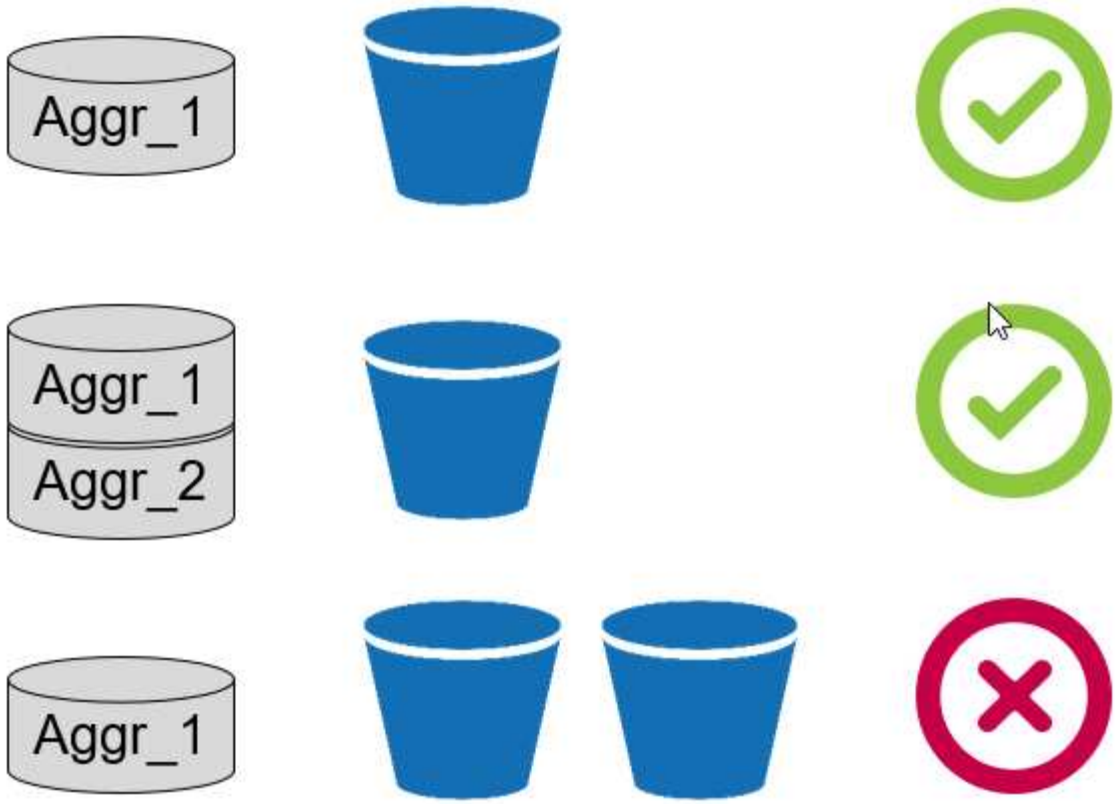
AWS S3 Bucket erstellen

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.

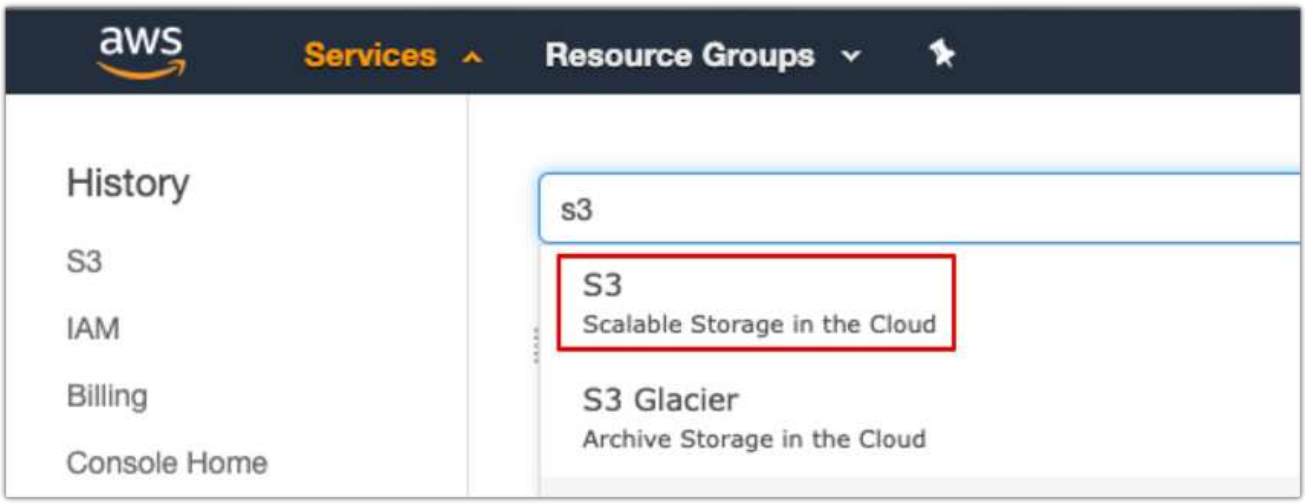
FabricPool unterstützt den Anhang eines Buckets pro Aggregat, wie in der folgenden Abbildung dargestellt. Ein einzelner Bucket kann mit einem einzelnen Aggregat verbunden werden, und ein einzelner Bucket kann mit mehreren Aggregaten verbunden werden. Jedoch kann ein einzelnes Aggregat nicht an mehrere 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.

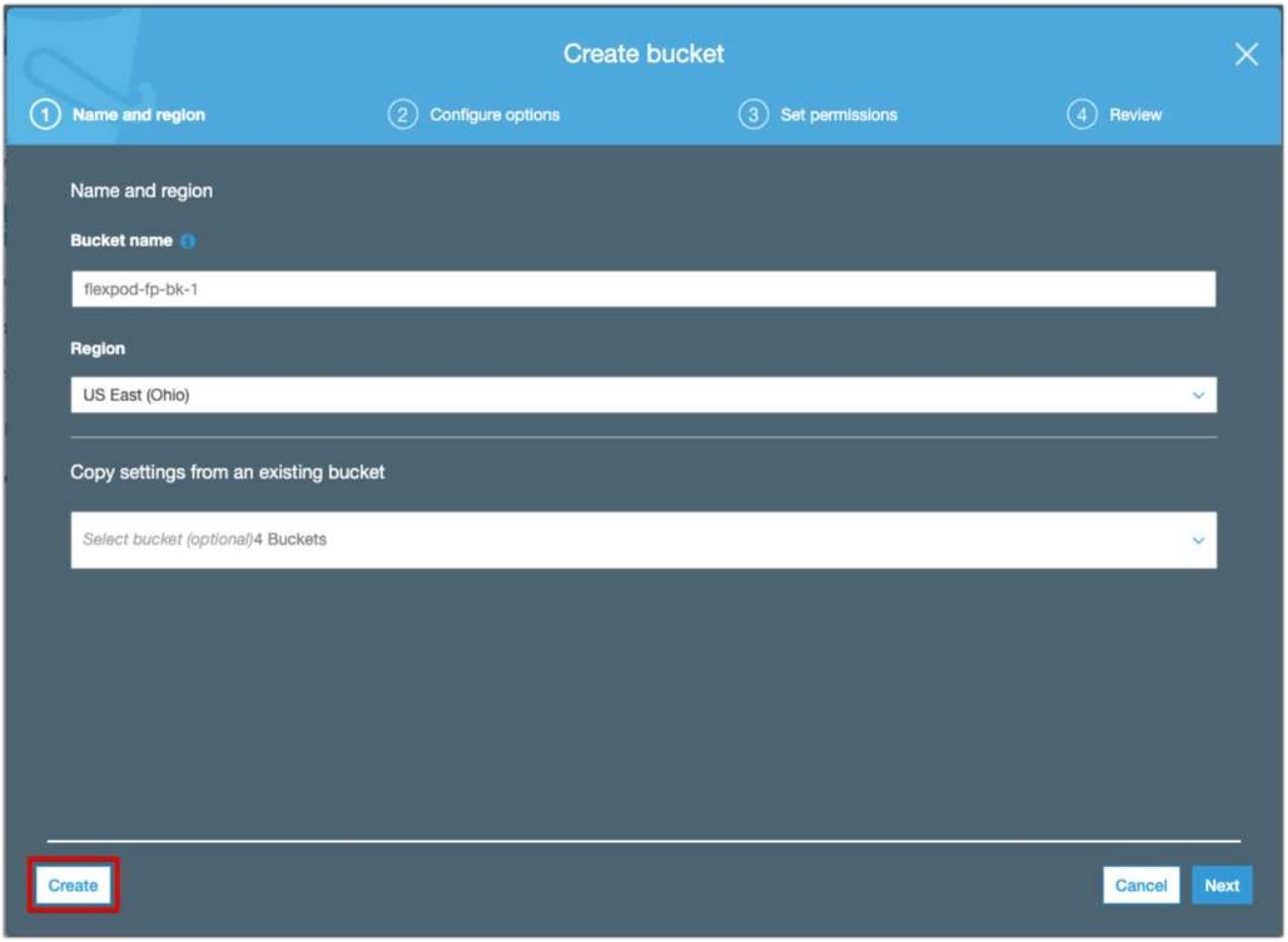


Erstellen eines S3-Buckets

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:

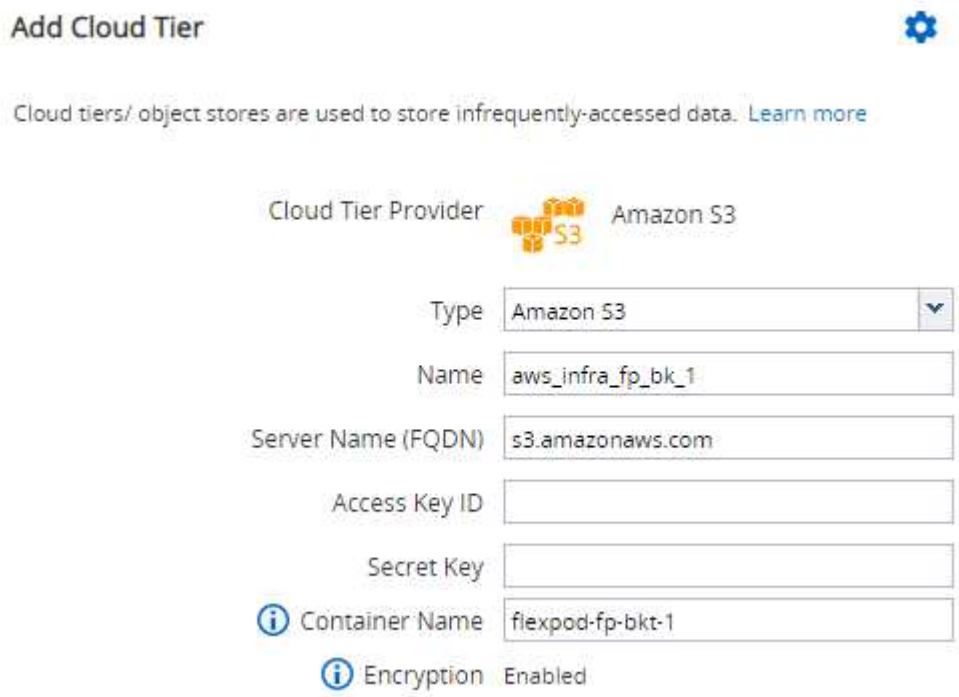
- Servername (FQDN), z. B. `s3.amazonaws.com`
- Zugriffsschlüssel-ID
- Geheimer Schlüssel
- Container-Name (Bucket-Name)

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.

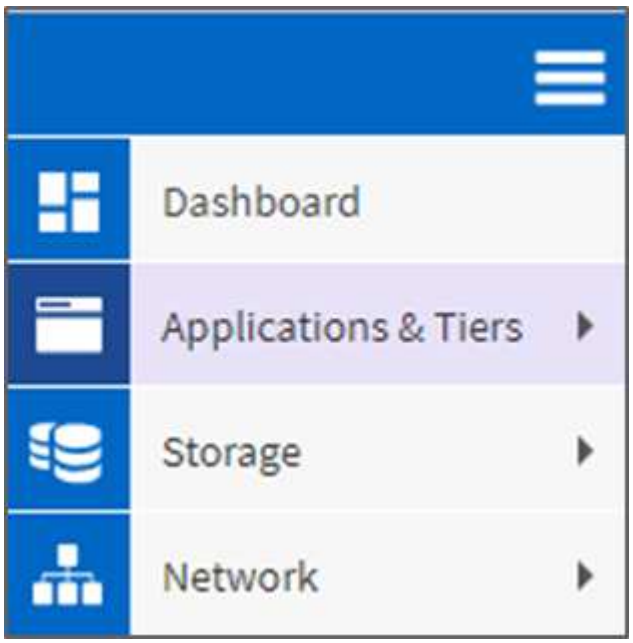
Mit einem Cluster kann mehrere Objektspeichertypen verbunden werden. Mit jedem Aggregat kann jedoch nur ein Objektspeichertyp verbunden werden. So kann beispielsweise ein Aggregat Google Cloud verwenden, ein anderes Aggregat Amazon S3 verwenden, aber an beide kann kein Aggregat angeschlossen werden.

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.

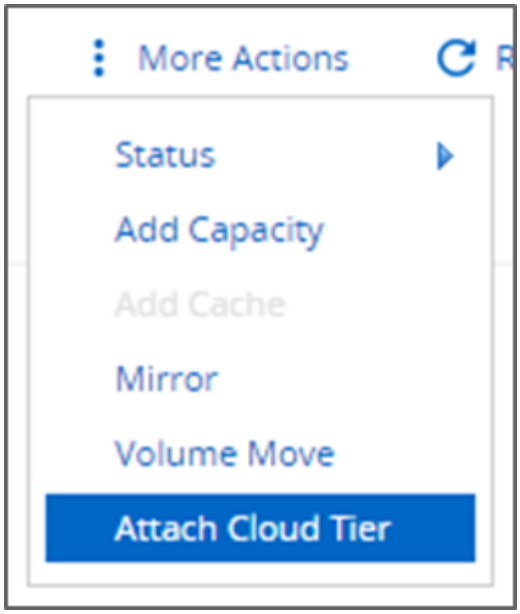
OnCommand System Manager

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.

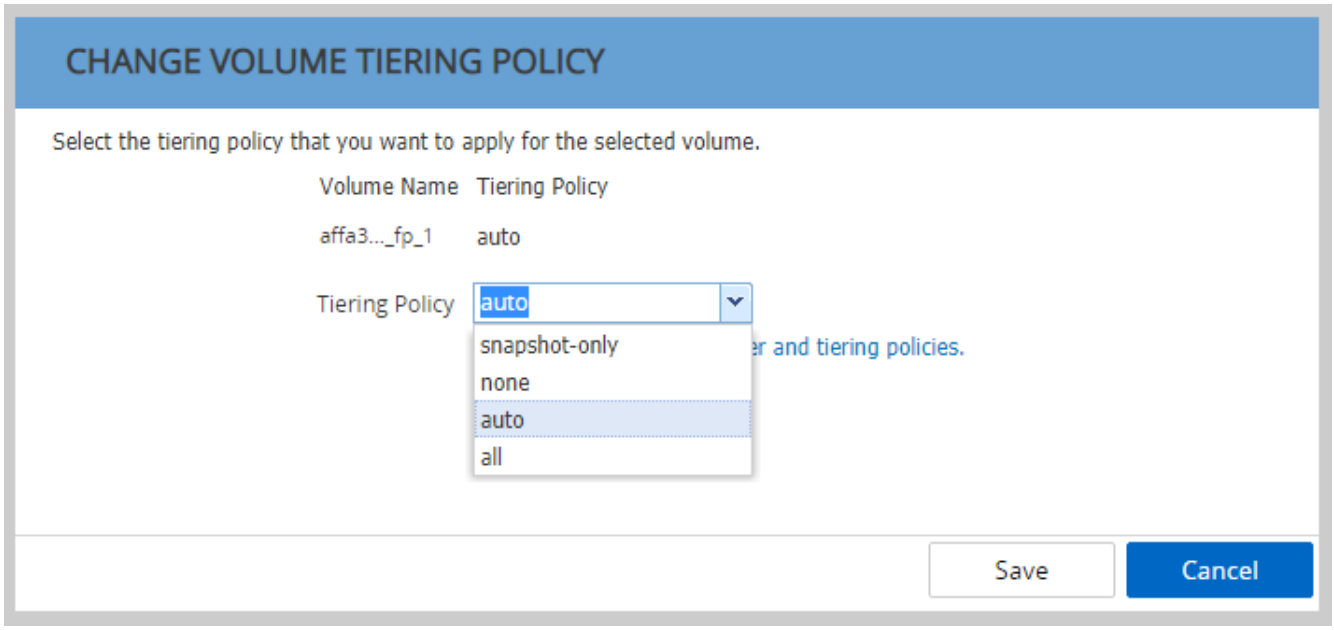
In Verbindung mit FlexPod bietet FabricPool drei Volume Tiering-Richtlinien: Automatisch, nur Snapshot und keine.

- **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"

Enterprise-Datenbanken

SAP

Einführung in SAP auf FlexPod

Die FlexPod Plattform ist eine vorkonfigurierte Datacenter-Architektur mit Best Practices, die auf Cisco Unified Computing System (Cisco UCS), den Cisco Nexus Switches und NetApp Storage Controllern basiert.

FlexPod ist eine geeignete Plattform für die Ausführung von SAP-Anwendungen. Mit den hier angebotenen Lösungen können Sie SAP HANA mit einem Modell der maßgeschneiderten Datacenter-Integration schnell und zuverlässig implementieren. FlexPod bietet nicht nur eine Basiskonfiguration, sondern auch die Flexibilität, gemäß den Anforderungen vieler verschiedener Anwendungsfälle und Anwendungsfälle dimensioniert zu werden.

FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt das Cisco und NetApp FlexPod-Datacenter mit NetApp ONTAP 9.7 auf NetApp AFF A400 Storage und die Unified Software-Version 4.1(1) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation speziell für SAP HANA.

FlexPod-Datacenter mit NetApp ONTAP 9.7 und Cisco UCS Unified Software Release 4.1(1) ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switch-Familie und MDS 9000 Multilayer Fabric Switches basiert. Und NetApp Storage-Arrays der AFF A-Serie mit dem Storage-Betriebssystem ONTAP 9.7.

"FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7"

SAP Non-HANA with SQL Whitepaper – Design

In der aktuellen IT-Branche erlebt eine drastische Transformation bei Datacenter-Lösungen. In den letzten Jahren war das Interesse an vorab validierten und ausgereiften Datacenter-Lösungen groß. Die Einführung der Virtualisierungstechnologie in kritische Bereiche hat große Auswirkungen auf die Designprinzipien und die Architektur dieser Lösungen. Viele Applikationen, die auf Bare-Metal-Systemen ausgeführt werden, können nun zu neuen virtualisierten, integrierten Lösungen migriert werden. FlexPod ist eine solche vorab validierte und entwickelte Datacenter-Lösung, die auf die sich schnell ändernden Anforderungen VON IT-Abteilungen zugeschnitten ist. Cisco und NetApp stellen gemeinsam FlexPod bereit, die auf erstklassigen Computing-, Netzwerk- und Storage-Komponenten als Grundlage für eine Vielzahl von Enterprise Workloads wie Datenbanken, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) und Web-Applikationen basiert.

Die Konsolidierung VON IT-Anwendungen, insbesondere Datenbanken, hat in den letzten Jahren großes

Interesse hervorgerufen. Die am weitesten verbreitete Datenbankplattform der letzten Jahre ist Microsoft SQL Server. SQL Server-Datenbanken unterliegen häufig der unkontrollierten Zunahme von Datenbanken. Dies bringt IT-Herausforderungen wie nicht ausgelastete Server, falsche Lizenzierungen, Sicherheitsbedenken, Managementprobleme und hohe Betriebskosten mit sich. Daher eignen sich SQL Server Datenbanken gut für die Konsolidierung auf einer robusteren, flexibleren und stabileren Plattform. Dieses Dokument beschreibt eine FlexPod Referenzarchitektur für die Implementierung und Konsolidierung von SQL Server Datenbanken.

"SAP Non-HANA with SQL Whitepaper – Design"

FlexPod Datacenter for SAP Solution mit Cisco UCS Fabric der dritten Generation und der NetApp AFF A-Serie

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt die Implementierungsmethodik von Cisco und NetApp FlexPod-Datacenter für SAP HANA auf der Basis der zweiten Generation von skalierbaren Intel Xeon Prozessoren, die das Cisco UCS Computing System (Cisco UCS) unterstützen.

Cisco UCS Manager (UCSM) 4.0(4) bietet konsolidierten Support für alle aktuellen Cisco UCS Fabric Interconnect Modelle (6200, 6300, 6324 und 6454), IOM der Serie 2200/2300, Cisco UCS Blade der B-Serie und Cisco UCS Rack Formfactor Server der C-Serie. FlexPod Datacenter mit der Cisco UCS Unified Software Release 4.0(4d) und NetApp ONTAP 9.6 ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco UCS, der Cisco Nexus 9000 Switch-Familie und den Storage Arrays der AFF A-Serie basiert.

"FlexPod Datacenter for SAP Solution mit Cisco UCS Fabric der dritten Generation und der NetApp AFF A-Serie"

FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7: Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Cisco und NetApp haben gemeinsam eine Reihe von FlexPod Lösungen zur Unterstützung strategischer Datacenter-Plattformen entwickelt. Die FlexPod Lösung bietet eine integrierte Architektur, in der Best Practices für Computing, Storage und Netzwerkdesign enthalten sind. Dadurch werden IT-Risiken minimiert, indem die integrierte Architektur validiert wird, um die Kompatibilität verschiedener Komponenten sicherzustellen. Die Lösung behebt auch IT-Probleme durch dokumentierte Designanleitungen, Implementierungsanleitungen und Support, die in verschiedenen Phasen (Planung, Entwurf und Implementierung) einer Bereitstellung verwendet werden können.

"FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7: Design"

FlexPod Datacenter for SAP Solution with Cisco ACI, Cisco UCS Manager 4.0 und NetApp AFF A-Series – Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

In diesem Dokument wird die in Cisco ACI integrierte FlexPod Lösung als validierter Ansatz für die Implementierung von SAP HANA Tailored Datacenter Integration (TDI) Umgebungen beschrieben. Dieses validierte Design enthält Richtlinien und ein Framework zur Implementierung von SAP HANA mit Best Practices von Cisco und NetApp.

Die empfohlene Lösungsarchitektur basiert auf dem Cisco Unified Computing System (Cisco UCS) und verwendet eine einheitliche Softwareversion zur Unterstützung von Cisco UCS Hardwareplattformen, die folgende Komponenten umfassen:

- Cisco UCS Blade-Server der B-Serie und Cisco UCS Rack-Server der C-Serie, konfigurierbar mit der Option Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnects der Cisco UCS 6400 Serie
- Leaf- und Wirbelsäulenschalter der Cisco Nexus 9000-Serie
- NetApp All-Flash-Storage-Arrays

Darüber hinaus bietet dieses Dokument Validierungen sowohl für Red hat Enterprise Linux als auch für SUSE Linux Enterprise Server for SAP HANA.

"FlexPod Datacenter for SAP Solution with Cisco ACI, Cisco UCS Manager 4.0 und NetApp AFF A-Series – Design"

FlexPod Datacenter for SAP with Cisco ACI, Cisco UCS Manager 4.0, and NetApp AFF A-Series – Implementierung

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

In diesem Dokument werden die Architektur und Bereitstellungsverfahren für die SAP HANA Tailored DataCenter Integration Option auf FlexPod Infrastruktur beschrieben. Diese besteht aus:

- Cisco UCS Computing System (Cisco UCS) unterstützt durch skalierbare Intel Xeon Prozessoren der zweiten Generation.
- Switching-Produkte, die die Cisco Application Centric Infrastructure (ACI) nutzen
- NetApp AFF Arrays Der A-Series

Ziel dieses Dokuments ist es, die detaillierten Konfigurationsschritte für die SAP HANA-Bereitstellung aufzuzeigen

"FlexPod Datacenter for SAP with Cisco ACI, Cisco UCS Manager 4.0, and NetApp AFF A-Series – Implementierung"

FlexPod Datacenter for SAP Solution with Cisco UCS Manager 4.0 and NetApp AFF A-Series – Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, bei der es sich um einen validierten Ansatz für die Implementierung von SAP HANA Tailored Datacenter Integration (TDI) Umgebungen handelt. Dieses validierte Design enthält Richtlinien und

ein Framework zur Implementierung von SAP HANA mit Best Practices von Cisco und NetApp.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und Anwendungsfällen unterstützt. Diese Lösung ermöglicht Ihnen die schnelle und zuverlässige Implementierung von SAP HANA mit einem Modell eines maßgeschneiderten Datacenter-Integrationsmodus.

"FlexPod Datacenter for SAP Solution with Cisco UCS Manager 4.0 and NetApp AFF A-Series – Design"

FlexPod Datacenter for SAP Solution with Cisco ACI on Cisco UCS M5 Servers with SLES 12 SP3 and RHEL 7.4

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

In diesem Dokument werden die Architektur und Implementierungsverfahren für die SAP HANA Tailored DataCenter Integration Option auf einer FlexPod Infrastruktur beschrieben. Sie besteht aus Cisco Computing- und Switching-Produkten, die die branchenführende softwaredefinierte Netzwerklösung (SDN) Cisco Application Centric Infrastructure (ACI) nutzen, und NetApp AFF Arrays Der A-Series. Ziel dieses Dokuments ist es, die Designprinzipien mit den detaillierten Konfigurationsschritten für die SAP HANA-Bereitstellung aufzuzeigen.

"FlexPod Datacenter for SAP Solution with Cisco ACI on Cisco UCS M5 Servers with SLES 12 SP3 and RHEL 7.4"

FlexPod Datacenter für SAP mit IP-basiertem Storage mit der NetApp AFF A-Serie und Cisco UCS Manager 3.2

Shailendra Mcruunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

Die in diesem Dokument detailliert erläutere Referenzarchitektur verdeutlicht die Ausfallsicherheit, die Kostenvorteile und die einfache Implementierung einer IP-basierten Storage-Lösung. Ein Storage-System, das mehrere Protokolle über eine einzige Schnittstelle unterstützen kann, sorgt für die freie Wahl der Kunden und schützt ihre Investitionen, da es sich wirklich um eine einmalige Kabelarchitektur handelt. Die Lösung wurde zum Hosten skalierbarer SAP HANA Workloads entwickelt.

"FlexPod Datacenter für SAP mit IP-basiertem Storage mit der NetApp AFF A-Serie und Cisco UCS Manager 3.2"

FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt das Cisco und NetApp FlexPod-Datacenter mit NetApp ONTAP 9.7 auf NetApp AFF A400 Storage und die Unified Software-Version 4.1(1) von Cisco UCS Manager mit skalierbaren Intel Xeon Prozessoren der zweiten Generation speziell für SAP HANA.

FlexPod-Datacenter mit NetApp ONTAP 9.7 und Cisco UCS Unified Software Release 4.1(1) ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS), der Cisco Nexus 9000 Switch-Familie und MDS 9000 Multilayer Fabric Switches basiert. Und NetApp Storage-Arrays der AFF A-Serie mit dem Storage-Betriebssystem ONTAP 9.7.

"FlexPod Datacenter für SAP Lösung mit FibreChannel SAN mit Cisco UCS Manager 4.0 und NetApp ONTAP 9.7"

SAP Applikations-Server auf FlexPod mit SQL implementieren

FlexPod ist eine vorab validierte und entwickelte Datacenter-Lösung, die auf die sich schnell ändernden Anforderungen VON IT-Abteilungen zugeschnitten ist. Cisco und NetApp arbeiten gemeinsam an der Bereitstellung von FlexPod, die als Grundlage für eine Vielzahl von Enterprise Workloads erstklassige Computing-, Netzwerk- und Storage-Komponenten verwendet. Hierzu zählen Datenbanken, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM) und Web-Applikationen. Die Konsolidierung VON IT-Anwendungen, insbesondere Datenbanken, hat in den letzten Jahren großes Interesse hervorgerufen. Die am weitesten verbreitete Datenbankplattform der letzten Jahre ist Microsoft SQL Server. SQL Server-Datenbanken unterliegen häufig der unkontrollierten Zunahme von Datenbanken. Dies bringt IT-Herausforderungen wie nicht ausgelastete Server, falsche Lizenzierungen, Sicherheitsbedenken, Managementprobleme und hohe Betriebskosten mit sich. Daher eignen sich SQL Server Datenbanken gut für die Konsolidierung auf einer robusteren, flexibleren und stabileren Plattform. Dieses Dokument beschreibt eine FlexPod Referenzarchitektur für die Implementierung und Konsolidierung von SQL Server Datenbanken.

"SAP Applikations-Server auf FlexPod mit SQL implementieren"

FlexPod Datacenter for SAP with Cisco ACI, Cisco UCS Manager 4.0, and NetApp AFF A-Series

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

In diesem Dokument werden die Architektur und Bereitstellungsverfahren für die SAP HANA Tailored DataCenter Integration Option auf FlexPod Infrastruktur beschrieben. Diese besteht aus:

- Cisco UCS Computing System (Cisco UCS) unterstützt durch skalierbare Intel Xeon Prozessoren der zweiten Generation.
- Switching-Produkte, die die Cisco Application Centric Infrastructure (ACI) nutzen
- NetApp AFF Arrays Der A-Series

"FlexPod Datacenter for SAP with Cisco ACI, Cisco UCS Manager 4.0, and NetApp AFF A-Series"

FlexPod Datacenter for SAP Solution with Cisco ACI, Cisco UCS Manager 4.0 und NetApp AFF A-Series – Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

In diesem Dokument wird die in Cisco ACI integrierte FlexPod Lösung als validierter Ansatz für die Implementierung von SAP HANA Tailored Datacenter Integration (TDI) Umgebungen beschrieben. Dieses validierte Design enthält Richtlinien und ein Framework zur Implementierung von SAP HANA mit Best Practices von Cisco und NetApp.

Die empfohlene Lösungsarchitektur basiert auf dem Cisco Unified Computing System (Cisco UCS) und verwendet eine einheitliche Softwareversion zur Unterstützung von Cisco UCS Hardwareplattformen, die folgende Komponenten umfassen:

- Cisco UCS Blade-Server der B-Serie und Cisco UCS Rack-Server der C-Serie, konfigurierbar mit der Option Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnects der Cisco UCS 6400 Serie
- Leaf- und Wirbelsäulenschalter der Cisco Nexus 9000-Serie
- NetApp All-Flash-Storage-Arrays

Darüber hinaus bietet dieses Dokument Validierungen sowohl für Red hat Enterprise Linux als auch für SUSE Linux Enterprise Server for SAP HANA.

"FlexPod Datacenter for SAP Solution with Cisco ACI, Cisco UCS Manager 4.0 und NetApp AFF A-Series – Design"

FlexPod Datacenter for SAP Solution mit Cisco UCS Fabric der dritten Generation und der NetApp AFF A-Serie

Shailendra Mcruunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt die Implementierungsmethodik von Cisco und NetApp FlexPod-Datacenter für SAP HANA auf der Grundlage des Cisco UCS Computing Systems (Cisco UCS), das durch skalierbare Intel Xeon Prozessoren der zweiten Generation unterstützt wird.

Cisco UCS Manager (UCSM) 4.0(4) bietet konsolidierten Support für alle aktuellen Cisco UCS Fabric Interconnect Modelle (6200, 6300, 6324 und 6454), IOM der Serie 2200/2300, Cisco UCS Blade der B-Serie und Cisco UCS Rack Formfactor Server der C-Serie. FlexPod Datacenter mit der Cisco UCS Unified Software Release 4.0(4d) und NetApp ONTAP 9.6 ist eine vorab entwickelte, Best Practice Datacenter-Architektur, die auf dem Cisco UCS, der Cisco Nexus 9000 Switch-Produktfamilie und den NetApp AFF Storage Arrays Der A-Serie basiert.

"FlexPod Datacenter for SAP Solution mit Cisco UCS Fabric der dritten Generation und der NetApp AFF A-Serie"

FlexPod Datacenter for SAP Solution with Cisco UCS Manager 4.0 and NetApp AFF A-Series – Design

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Dieses Dokument beschreibt die FlexPod Lösung von Cisco und NetApp, bei der es sich um einen validierten Ansatz für die Implementierung von SAP HANA Tailored Datacenter Integration (TDI) Umgebungen handelt. Dieses validierte Design enthält Richtlinien und

ein Framework zur Implementierung von SAP HANA mit Best Practices von Cisco und NetApp.

FlexPod ist eine führende integrierte Infrastruktur, die eine Vielzahl von Enterprise-Workloads und Anwendungsfällen unterstützt. Diese Lösung ermöglicht Ihnen die schnelle und zuverlässige Implementierung von SAP HANA mit einem Modell eines maßgeschneiderten Datacenter-Integrationsmodus.

Die empfohlene Lösungsarchitektur basiert auf dem Cisco Unified Computing System (Cisco UCS) und verwendet eine einheitliche Softwareversion zur Unterstützung von Cisco UCS Hardwareplattformen, die folgende Komponenten umfassen:

- Cisco UCS Blade-Server der B-Serie und Cisco UCS Rack-Server der C-Serie, konfigurierbar mit der Option Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnects der Cisco UCS 6300 Serie
- Switches der Cisco Nexus 9000 Serie
- NetApp All-Flash-Storage-Arrays

Darüber hinaus bietet dieses Dokument Validierungen sowohl für Red hat Enterprise Linux als auch für SUSE Linux Enterprise Server for SAP HANA.

"FlexPod Datacenter for SAP Solution with Cisco UCS Manager 4.0 and NetApp AFF A-Series – Design"

Oracle

FlexPod Datacenter mit Oracle RAC Datenbanken auf Cisco UCS und NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Cisco Validated Designs umfassen Systeme und Lösungen, die entwickelt, getestet und dokumentiert wurden, um Kundenimplementierungen zu vereinfachen und zu verbessern. Bei diesen Designs wird ein breites Spektrum an Technologien und Produkten in ein Portfolio von Lösungen integriert, das speziell für die Geschäftsanforderungen der Kunden entwickelt wurde. Gemeinsam entwickeln Cisco und NetApp FlexPod, das als Grundlage für eine Vielzahl an Workloads dient und effiziente Architekturdesigns ermöglicht, die auf den Kundenanforderungen basieren. Eine FlexPod Lösung ist ein validierter Ansatz für die Implementierung von Technologien von Cisco und NetApp als Shared Cloud-Infrastruktur.

Das FlexPod Datacenter mit NetApp All Flash AFF System ist eine konvergente Infrastrukturplattform, die erstklassige Technologien von Cisco und NetApp in einer leistungsstarken, konvergenten Plattform für Enterprise-Applikationen vereint. Cisco und NetApp arbeiten eng mit Oracle zusammen, um die anspruchsvollsten transaktionsorientierten und reaktionszeitabhängigen Datenbanken zu unterstützen, die moderne Unternehmen benötigen.

Dieses Cisco Validated Design (CVD) beschreibt die Referenzarchitektur von FlexPod Datacenter unter Verwendung von Cisco UCS und NetApp All Flash AFF Storage zur Implementierung einer hochverfügbaren Oracle RAC Datenbankumgebung. In diesem Dokument werden die Hardware- und Softwarekonfiguration der involvierten Komponenten sowie die Ergebnisse verschiedener Tests dargestellt. Dieses Dokument bietet darüber hinaus Implementierungs- und Best Practices-Anleitungen für Cisco UCS Compute Server, Cisco

Fabric Interconnect Switches, Cisco MDS Switches, Cisco Nexus Switches, NetApp AFF Storage und Oracle RAC Datenbanken.

"FlexPod Datacenter mit Oracle RAC Datenbanken auf Cisco UCS und NetApp AFF A-Series"

FlexPod Datacenter mit Oracle RAC auf Oracle Linux

Tushar Patel, Cisco Niranjan Mohapatra, Cisco John Elliott, NetApp

Das Cisco Unified Computing System (Cisco UCS) ist eine zukunftsweisende Datacenter-Plattform, die Computing, Netzwerk, Storage-Zugriff und Virtualisierung in einem einzigen geschlossenen System vereint. Cisco UCS ist die ideale Plattform für die Architektur geschäftskritischer Datenbank-Workloads. Die Kombination aus Cisco UCS Plattform, NetApp Storage und Oracle Real Application Cluster (RAC) Architektur beschleunigt Ihre IT-Transformation, indem sie schnellere Bereitstellungen, größere Flexibilität bei der Auswahl, Effizienz und weniger Risiken ermöglicht. Dieses Cisco Validated Design (CVD) legt den Schwerpunkt auf eine flexible, mandantenfähige, hochperformante und robuste FlexPod Referenzarchitektur, die die Oracle 12c RAC Database umfasst.

Die von NetApp und Cisco entwickelte FlexPod Plattform ist eine flexible, integrierte Infrastrukturlösung, die vorab validierte Storage-, Netzwerk- und Servertechnologien bereitstellt. Sie wurde mit dem Ziel konzipiert, die Reaktionsfähigkeit DER IT auf geschäftliche Anforderungen zu verbessern und gleichzeitig die Computing-Gesamtkosten zu senken. Denken Sie an maximale Verfügbarkeit, minimales Risiko. Die Komponenten von FlexPod sind integriert und standardisiert, um Ihnen dabei zu helfen, eine zeitnahe, wiederholbare und konsistente Implementierung zu erreichen. Sie können Leistung, Platzbedarf, nutzbare Kapazität, Performance und Kosten der einzelnen FlexPod Implementierungen genau planen.

FlexPod setzt auf neueste Technologie und vereinfacht auf effiziente Weise die Datacenter-Workloads, die die Wertschöpfung DER IT neu definieren:

- Nutzen Sie die Funktionen von NetApp FAS Hybrid-Arrays mit Flash Pool. So können Sie für Ihre spezifische Applikation oder Umgebung den genauen Anteil an Flash für rotierende Medien bereitstellen.
- Nutzen Sie eine vorab validierte Plattform, um Geschäftsunterbrechungen zu minimieren, DIE IT-Flexibilität zu verbessern und die Implementierungszeit von Monaten auf Wochen zu verkürzen.
- Verringern Sie den Administrationsaufwand und die TCO um 50 Prozent.
- Erfüllen oder übertreffen Sie die stetig wachsenden Hardware-Performance-Anforderungen für Datacenter-Workloads.

"FlexPod Datacenter mit Oracle RAC auf Oracle Linux"

FlexPod Datacenter mit Oracle RAC Datenbanken auf Cisco UCS und NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Das FlexPod Datacenter mit NetApp All Flash AFF System ist eine konvergente Infrastrukturplattform, die erstklassige Technologien von Cisco und NetApp in einer leistungsstarken, konvergenten Plattform für Enterprise-Applikationen vereint. Cisco und NetApp arbeiten eng mit Oracle zusammen, um die anspruchsvollsten

transaktionsorientierten und reaktionszeitabhängigen Datenbanken zu unterstützen, die moderne Unternehmen benötigen.

Dieses Cisco Validated Design (CVD) beschreibt die Referenzarchitektur von FlexPod Datacenter unter Verwendung von Cisco UCS und NetApp All Flash AFF Storage zur Implementierung einer hochverfügbaren Oracle RAC Datenbankumgebung. Dieses Dokument zeigt die Hardware- und Softwarekonfiguration der involvierten Komponenten sowie die Ergebnisse verschiedener Tests. Dieses Dokument bietet darüber hinaus Implementierungs- und Best Practices-Anleitungen für Cisco UCS Compute Server, Cisco Fabric Interconnect Switches, Cisco MDS Switches, Cisco Nexus Switches, NetApp AFF Storage und Oracle RAC Datenbanken.

"FlexPod Datacenter mit Oracle RAC Datenbanken auf Cisco UCS und NetApp AFF A-Series"

Microsoft SQL Server

FlexPod Datacenter für Microsoft SQL Server 2019 und VMware vSphere 6.7

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Dieses Dokument beschreibt eine FlexPod Referenzarchitektur mit den neuesten Hardware- und Softwareprodukten und bietet Implementierungsempfehlungen für das Hosting von Microsoft SQL Server 2019-Datenbanken in virtualisierten VMware ESXi-Umgebungen. Diese Lösung verwendet darüber hinaus Cisco Workload Optimization Manager (CWOM), der automatisierte Empfehlungen für eine optimale und effiziente Ressourcenauslastung von SQL-Workloads und Infrastruktur bietet.

Die Lösung basiert auf dem Cisco Unified Computing System (Cisco UCS) und verwendet die einheitliche Software-Version 4.1.1c zur Unterstützung der Cisco UCS Hardware-Plattformen, darunter Cisco UCS B-Series Blade Server, Cisco UCS 6400 Fabric Interconnects, Switches der Cisco Nexus 9000 Serie und NetApp Storage-Arrays der AFF Serie.

"FlexPod Datacenter für Microsoft SQL Server 2019 und VMware vSphere 6.7"

FlexPod Datacenter with Microsoft SQL Server 2016 and VMware vSphere 6.5

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco David Arnette, NetApp

Dieses Dokument behandelt eine FlexPod Referenzarchitektur mit aktuellen Hardware- und Softwareprodukten und enthält Konfigurationsempfehlungen für die Implementierung von Microsoft SQL Server-Datenbanken in einer virtualisierten Umgebung.

Die empfohlene Lösungsarchitektur basiert auf Cisco Unified Computing System (Cisco UCS). Dabei wird mithilfe der einheitlichen Softwareversion die Cisco UCS Hardware-Plattformen unterstützt, darunter Cisco UCS B-Series Blade Server, Cisco UCS 6300 Fabric Interconnects, Cisco Switches der Nexus 9000 Serie und NetApp All-Flash-Storage-Arrays. Darüber hinaus umfasst diese Lösung VMware vSphere 6.5 und vSphere 6.5 mit zahlreichen neuen Funktionen zur Optimierung der Storage-Auslastung und zur Unterstützung einer Private Cloud.

"FlexPod Datacenter with Microsoft SQL Server 2016 and VMware vSphere 6.5"

FlexPod-Datacenter mit Microsoft SQL Server 2017 auf Linux VM unter VMware und Hyper-V

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Dieses Dokument erläutert eine FlexPod Referenzarchitektur mit den neuesten Hardware- und Softwareprodukten und enthält Implementierungsempfehlungen für das Hosting von Microsoft SQL Server Datenbanken in virtualisierten VMware ESXi- und Microsoft Windows Hyper-V-Umgebungen mit Linux-Unterstützung von Microsoft für SQL Server-Implementierungen.

Die empfohlene Lösungsarchitektur basiert auf Cisco Unified Computing System (Cisco UCS) und verwendet die einheitliche Software-Version 4.0.1c zur Unterstützung der Cisco UCS Hardware-Plattformen wie Cisco UCS B-Series Blade Server, Cisco UCS 6300 Fabric Interconnects, Switches der Cisco Nexus 9000 Serie und NetApp Storage-Arrays der AFF Serie.

"FlexPod-Datacenter mit Microsoft SQL Server 2017 auf Linux VM unter VMware und Hyper-V"

FlexPod-Datacenter mit Microsoft SQL Server 2017 auf Linux VM unter VMware und Hyper-V

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Dieses Dokument erläutert eine FlexPod Referenzarchitektur mit den neuesten Hardware- und Softwareprodukten und enthält Implementierungsempfehlungen für das Hosting von Microsoft SQL Server Datenbanken in virtualisierten VMware ESXi- und Microsoft Windows Hyper-V-Umgebungen mit Linux-Unterstützung von Microsoft für SQL Server-Implementierungen.

Die empfohlene Lösungsarchitektur basiert auf Cisco Unified Computing System (Cisco UCS) und verwendet die einheitliche Software-Version 4.0.1c zur Unterstützung der Cisco UCS Hardware-Plattformen, einschließlich Cisco UCS B-Serie Blade Server, Cisco UCS 6300 Fabric Interconnects, Switches der Cisco Nexus 9000 Serie und NetApp Storage-Arrays der AFF Serie.

"FlexPod-Datacenter mit Microsoft SQL Server 2017 auf Linux VM unter VMware und Hyper-V"

Gesundheitswesen

FlexPod für die Genomik

TR-4911: FlexPod Genomics

JayaKishore Esanakula, NetApp

In der Medizin gibt es nur wenige Gebiete, die für das Gesundheitswesen und die Biowissenschaften wichtiger sind als Genomik. Genomik wird für Ärzte und Krankenschwestern schnell zu einem wichtigen klinischen Werkzeug. Genomik hilft uns in Kombination mit medizinischer Bildgebung und digitaler Pathologie zu verstehen, wie die Gene eines Patienten durch Behandlungsprotokolle beeinflusst werden können. Der Erfolg von Genomik im Gesundheitswesen hängt zunehmend von Dateninteroperabilität nach Maß ab. Ziel ist es, die enormen Mengen an genetischen Daten zu erkennen und klinisch relevante Zusammenhänge und Varianten zu identifizieren, die die Diagnose verbessern und die Präzisionsmedizin zur Realität machen. Genomik hilft uns dabei zu verstehen, woher Krankheiten kommen, wie sich Krankheiten entwickeln und welche Behandlungen und Strategien effektiv sein können. Die Genomik bietet offensichtlich viele Vorteile, die nicht nur Prävention, sondern auch Diagnostik und Behandlung umfassen. Gesundheitseinrichtungen haben verschiedene Herausforderungen mit sich:

- Bessere Versorgungsqualität
- Wertbasierte Versorgung
- Datenexplosion
- Präzisionsmedizin
- Pandemien
- Wearables, Fernüberwachung und Pflege
- Cyber-Sicherheit

Standardisierte klinische Behandlungspfade und klinische Protokolle sind eine der kritischen Komponenten der modernen Medizin. Einer der wichtigsten Aspekte der Standardisierung ist die Interoperabilität zwischen Gesundheitsanbietern: Nicht nur bei medizinischen Unterlagen, sondern auch bei Genomdaten. Die große Frage lautet: Werden Gesundheitseinrichtungen sich anstelle der Patienteneigentum an ihren persönlichen Genomdaten und den damit verbundenen medizinischen Unterlagen auf Genomdaten verzichten?

Interoperable Patientendaten sind der Schlüssel zu Präzisionsmedizin, eine der ausschlaggebenden Faktoren bei der kürzlich explosionsartigen Zunahme des Datenwachstums. Das Ziel der Präzisionsmedizin ist es, die Gesundheitsvorsorge, die Prävention, die Diagnose und die Behandlungslösungen effektiver und genauer zu gestalten.

Das Datenwachstum war exponentiell. Anfang Februar 2021 wurden in den USA ca. 8,000 COVID-19 Stämme pro Woche sequenziert. Die Anzahl der sequenzierten Genome war bis April 2021 auf 29,000 pro Woche erhöht. Jedes vollständig sequenzierte menschliche Genom ist etwa 125GB groß. Daher würde die gesamte Genomspeicherung im Ruhezustand mit einer Rate von 29,000 Genomen pro Woche mehr als 180 Petabyte pro Jahr betragen. Verschiedene Länder haben sich für die Genomepidemiologie engagiert, um die genomische Überwachung zu verbessern und sich auf die nächste Welle globaler Herausforderungen im

Gesundheitswesen vorzubereiten.

Die reduzierten Kosten für die Genomforschung führen zu nie da gewesenen Gentests und Forschungen. Die drei PS befinden sich an einem Wendepunkt: Computerleistung, Datenschutz und Personalisierung der Medizin. Bis 2025 schätzen Forscher, dass 100 Millionen bis 2 Milliarden menschliche Genome sequenziert werden. Damit Genomik effektiv und wertvoll sein kann, müssen Genomik-Funktionen einen nahtlosen Teil der Pflegungsprozesse sein. Er sollte leicht zugänglich sein und bei einem Patientenbesuch umsetzbar sein. Ebenso wichtig ist es, dass Patientendaten der elektronischen Krankenakten in die Genomik-Daten des Patienten integriert werden. Mit der Einführung hochmoderner konvergenter Infrastrukturen wie FlexPod können Unternehmen ihre Genomfunktionen in die alltäglichen Workflows von Ärzten, Pflegepersonal und Klinikmanagern integrieren. Aktuelle Informationen zur FlexPod Plattform finden Sie in dieser "FlexPod Datacenter with Cisco UCS X-Series Whitepaper".

Der wahre Nutzen der Genomforschung besteht für Ärzte darin, Präzisionsmedizin zu bieten und personalisierte Behandlungspläne zu entwickeln, die auf den genomischen Daten eines Patienten basieren. In der Vergangenheit gab es noch nie derartige Synergien zwischen Klinikpersonal und Datenanalysten, und die Genomik profitiert von den technologischen Innovationen der jüngsten Vergangenheit sowie von echten Partnerschaften zwischen Einrichtungen im Gesundheitswesen und Technologieführern der Branche.

Akademische medizinische Zentren und andere Organisationen im Gesundheitswesen und Life Science sind auf dem besten Weg, um in der Genomforschung das Kompetenzzentrum (COE) aufzubauen. Laut Dr. Charlie Gersbach, Dr. Greg Crawford und Dr. Tim E Reddy von der Duke University: „Wir wissen, dass Gene nicht durch einen einfachen binären Schalter ein- oder ausgeschaltet werden, sondern dass es ein Ergebnis mehrerer genregulatorischer Schalter ist, die zusammen arbeiten. Sie haben auch festgestellt, dass „keiner dieser Teile des Genoms isoliert arbeitet. Das Genom ist ein sehr kompliziertes Netz, das Evolution gewebt hat" ("ref").

NetApp und Cisco arbeiten bereits seit über 10 Jahren intensiv an der Implementierung inkrementeller Verbesserungen in der FlexPod Plattform. Das gesamte Kundenfeedback wird gehört, bewertet und an die Value Streams und Funktionen von FlexPod gebunden. Es ist diese kontinuierliche Schleife, Zusammenarbeit, Verbesserungen und Feier, die FlexPod als vertrauenswürdige konvergente Infrastrukturplattform auf der ganzen Welt auszeichnet. Die Lösung wurde von Grund auf vereinfacht und als die zuverlässigste, robusteste, vielseitigste und agilste Plattform für Unternehmen im Gesundheitswesen konzipiert.

Umfang

Mit der konvergenten Infrastrukturplattform von FlexPod können Gesundheitseinrichtungen einen oder mehrere Genomapplikationen und andere klinische und nicht klinische Applikationen im Gesundheitswesen hosten. Dieser technische Bericht verwendet ein Open-Source-Tool für die branchenübliche Genomik mit dem Namen GATK während der Plattformvalidierung von FlexPod. Eine umfassendere Diskussion über Genomik oder GATK ist jedoch nicht im Rahmen dieses Dokuments enthalten.

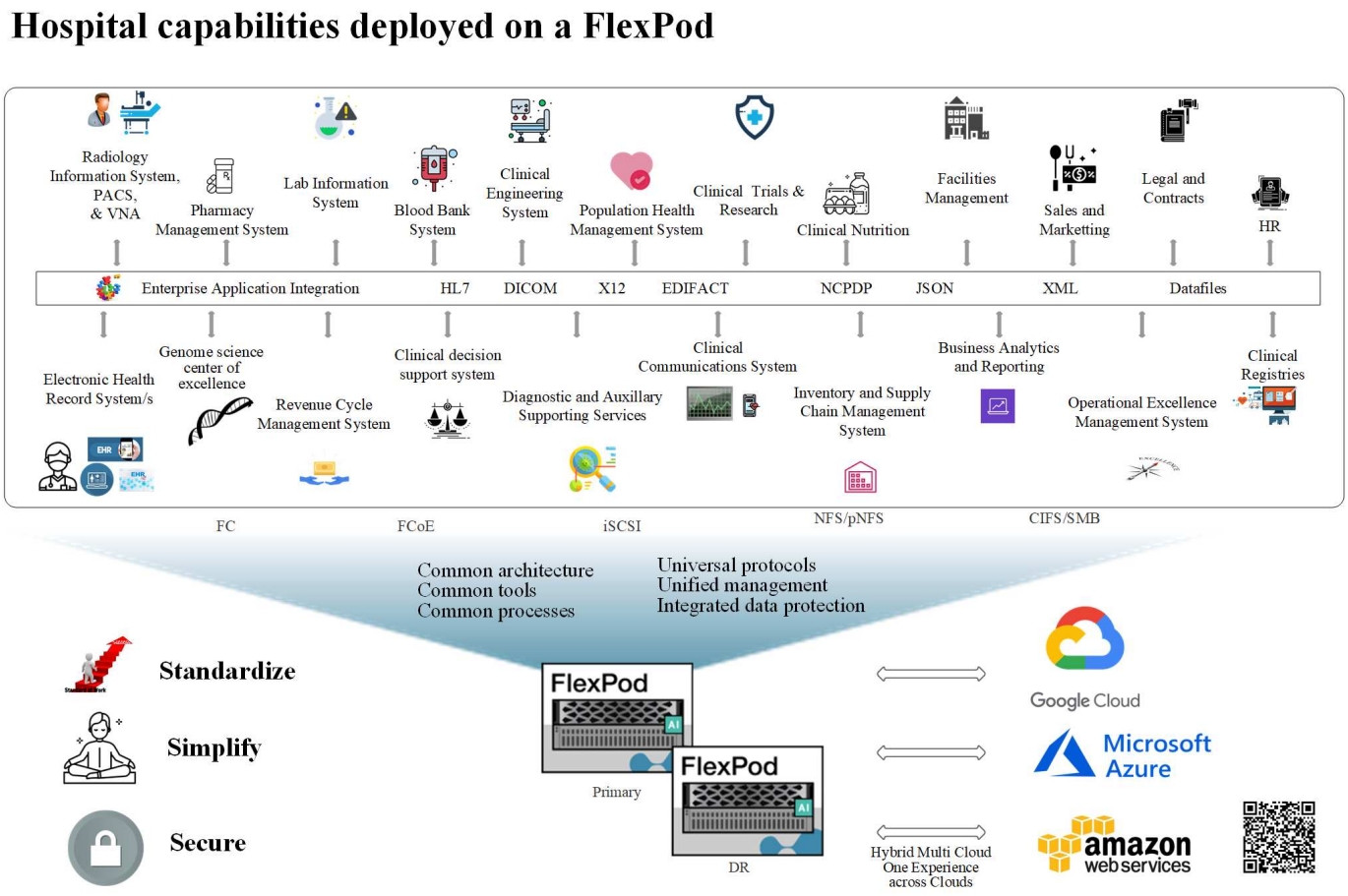
Zielgruppe

Dieses Dokument richtet sich an technische Leiter im Gesundheitswesen sowie an Lösungstechniker von Cisco und NetApp Partnern und Professional Services-Mitarbeiter. NetApp geht davon aus, dass der Leser gute Kenntnisse der Konzepte zur Berechnung der Storage- und Computing-Größenbemessung sowie der technischen Vertrautheit mit Bedrohungen für das Gesundheitswesen, mit der Sicherheit im Gesundheitswesen, MIT IT-Systemen im Gesundheitswesen, mit Cisco UCS und NetApp Storage-Systemen hat.

Auf FlexPod implementierte Krankenhausfunktionen

Ein typisches Krankenhaus verfügt über eine Reihe an IT-Systemen. Der Großteil solcher Systeme wird bei einem Anbieter gekauft, während nur sehr wenige von dem Krankenhaussystem im Haus gebaut werden. Aus

diesem Grund muss das Kliniksystem eine diverse Infrastrukturumgebung in seinen Datacentern managen. Wenn Krankenhäuser ihre Systeme in einer konvergenten Infrastrukturplattform wie FlexPod zusammenführen, können Unternehmen ihren Datacenter-Betrieb standardisieren. Mit FlexPod können Gesundheitseinrichtungen klinische und nicht klinische Systeme auf derselben Plattform implementieren und so den Datacenter-Betrieb vereinheitlichen.



"Der nächste Schritt: Vorteile der Implementierung genomischer Workloads auf FlexPod."

Vorteile der Implementierung genomischer Workloads auf FlexPod

"Zurück: Einführung."

Dieser Abschnitt bietet eine kurze Übersicht über die Vorteile, die zum Ausführen eines Genomik-Workloads auf einer konvergenten FlexPod Infrastrukturplattform erzielt werden können. Lassen Sie uns kurz die Möglichkeiten eines Krankenhauses beschreiben. Die folgende Ansicht der Unternehmensarchitektur zeigt die Funktionen eines Krankenhauses, die auf einer konvergenten, Hybrid-Cloud-fähigen FlexPod Infrastrukturplattform bereitgestellt werden.

- **Vermeiden von Silos im Gesundheitswesen.** Silos im Gesundheitswesen sind ein sehr echtes Anliegen. Abteilungen sind häufig Silos in ihrer eigenen Hardware und Software, nicht nach ihrer Wahl, sondern organisch. Beispielsweise Radiologie, Kardiologie, EHR, Genomik analysen, Umsatzzyklen und andere Abteilungen enthalten jeweils einen individuellen Satz an dedizierter Software und Hardware. Einrichtungen im Gesundheitswesen haben nur wenige IT-Fachkräfte für das Management ihrer Hardware- und Software-Ressourcen. Der Wendepunkt folgt, wenn zu erwarten ist, dass diese Gruppe von

Einzelpersonen ein sehr vielseitiges Spektrum an Hardware und Software managen wird. Die Heterogenität wird durch eine unkongruente Reihe von Prozessen, die von Anbietern in die Gesundheitsorganisation eingebracht werden, noch verschlimmert.

- **Start Small and Grow.** das GATK Tool Kit ist auf die CPU-Ausführung abgestimmt, die besten Suites Plattformen wie FlexPod. FlexPod ermöglicht eine unabhängige Skalierbarkeit von Netzwerk, Computing und Storage. Klein beginnen und mit der Zeit wachsen, wenn die Genomfunktionen und die Umgebung wachsen. Unternehmen im Gesundheitswesen müssen nicht in spezialisierte Plattformen investieren, um genomische Workloads auszuführen. Stattdessen können Unternehmen vielseitige Plattformen wie FlexPod nutzen, um Genomik- und nicht-genomikfreie Workloads auf derselben Plattform auszuführen. Wenn beispielsweise die Abteilung für Pädiatrie Genomfunktionen implementieren möchte, kann die IT-Leitung Computing, Storage und Networking auf einer vorhandenen FlexPod Instanz bereitstellen. Mit dem Wachstum der Geschäftsbereiche zur Genomik können Unternehmen im Gesundheitswesen ihre FlexPod Plattform nach Bedarf skalieren.
- **Eine einzige Kontrollscheibe und unübertroffene Flexibilität.** Cisco Intersight vereinfacht den IT-Betrieb erheblich, indem Anwendungen mit Infrastruktur überbrückt werden. Dadurch werden Transparenz und Management von Bare-Metal-Servern und -Hypervisoren zu serverlosen Anwendungen ermöglicht, wodurch Kosten gesenkt und Risiken gemindert werden. Diese einheitliche SaaS-Plattform verwendet ein einheitliches Open API-Design, das sich nativ in Plattformen und Tools von Drittanbietern integrieren lässt. Außerdem kann das Betriebsteam des Datacenters direkt oder von einem beliebigen Ort aus über eine mobile App heraus managen.

  Die Benutzer schöpfen in ihrer Umgebung schnell greifbaren Wert aus, indem sie Intersight als Managementplattform nutzen. Durch die Möglichkeit der Automatisierung vieler täglicher manueller Aufgaben beseitigt Intersight Fehler und vereinfacht Ihre täglichen Abläufe. Dank der erweiterten Support-Funktionen von Intersight können Anwender zudem Probleme voraus bleiben und die Problembehebung beschleunigen. Gemeinsam geben Unternehmen deutlich weniger Zeit und Geld für ihre Applikationsinfrastruktur aus und gewinnen mehr Zeit für die eigentliche Geschäftsentwicklung.

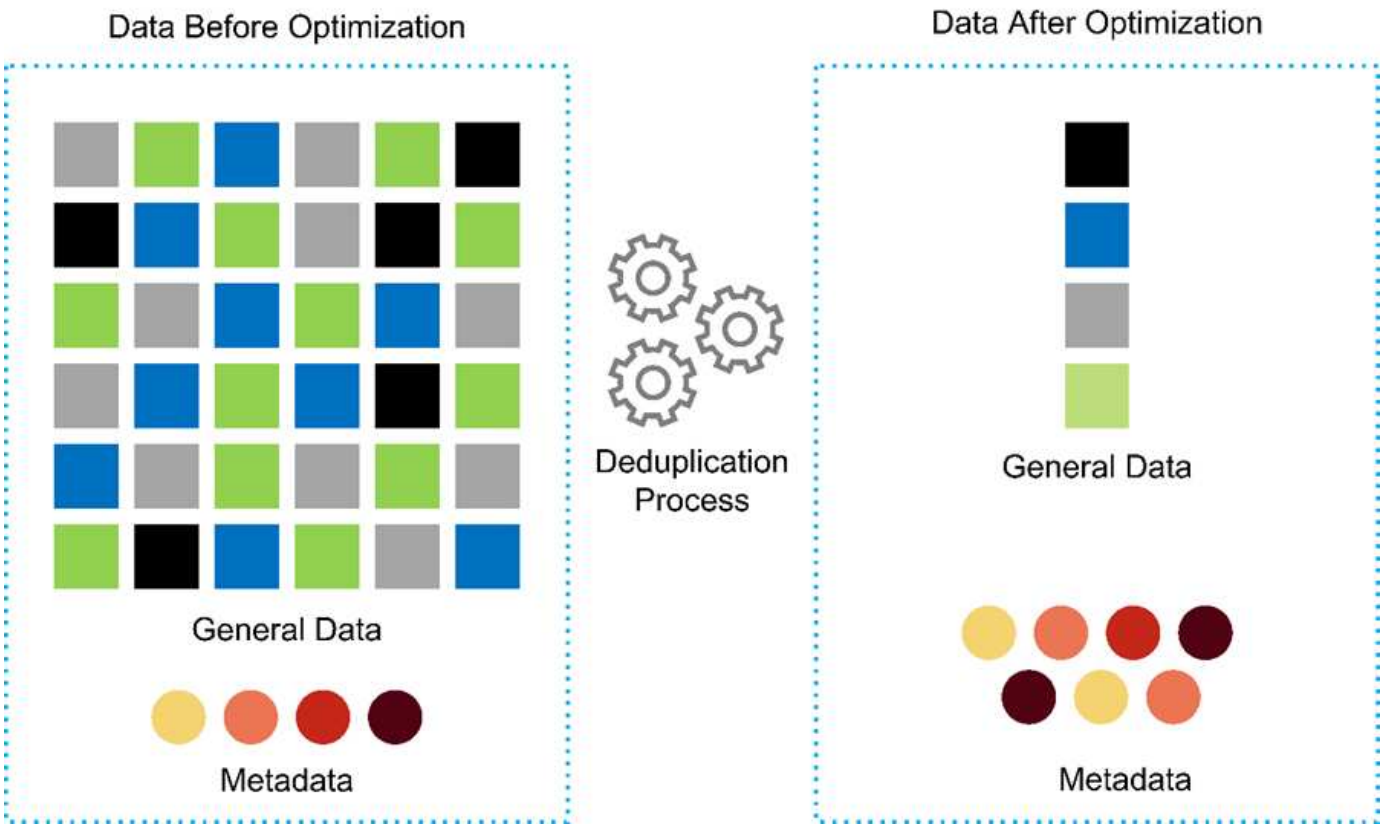
  Durch die Nutzung von Intersight Management und der leicht skalierbaren Architektur von FlexPod können Unternehmen mehrere Genom-Workloads auf einer einzigen FlexPod Plattform ausführen. Dies steigert die Auslastung und senkt die Gesamtbetriebskosten (TCO). FlexPod ermöglicht die flexible Dimensionierung. Dabei stehen Ihnen die Wahl, beginnend mit unserem kleinen FlexPod Express, und die Skalierung zu großen FlexPod Datacenter-Implementierungen. Dank der in Cisco Intersight integrierten Funktionen zur rollenbasierten Zugriffssteuerung können Organisationen im Gesundheitswesen robuste Zugriffskontrollmechanismen implementieren, sodass keine separaten Infrastruktur-Stacks erforderlich sind. Mehrere Geschäftseinheiten im Gesundheitswesen können Genomik als wichtigste Kernkompetenzen nutzen.

  FlexPod vereinfacht den IT-Betrieb und senkt die Betriebskosten. IT-Infrastrukturadministratoren können sich auf Aufgaben konzentrieren, die Klinikpersonal Innovationen ermöglichen, anstatt nur auf den Betrieb zu zugreifen.

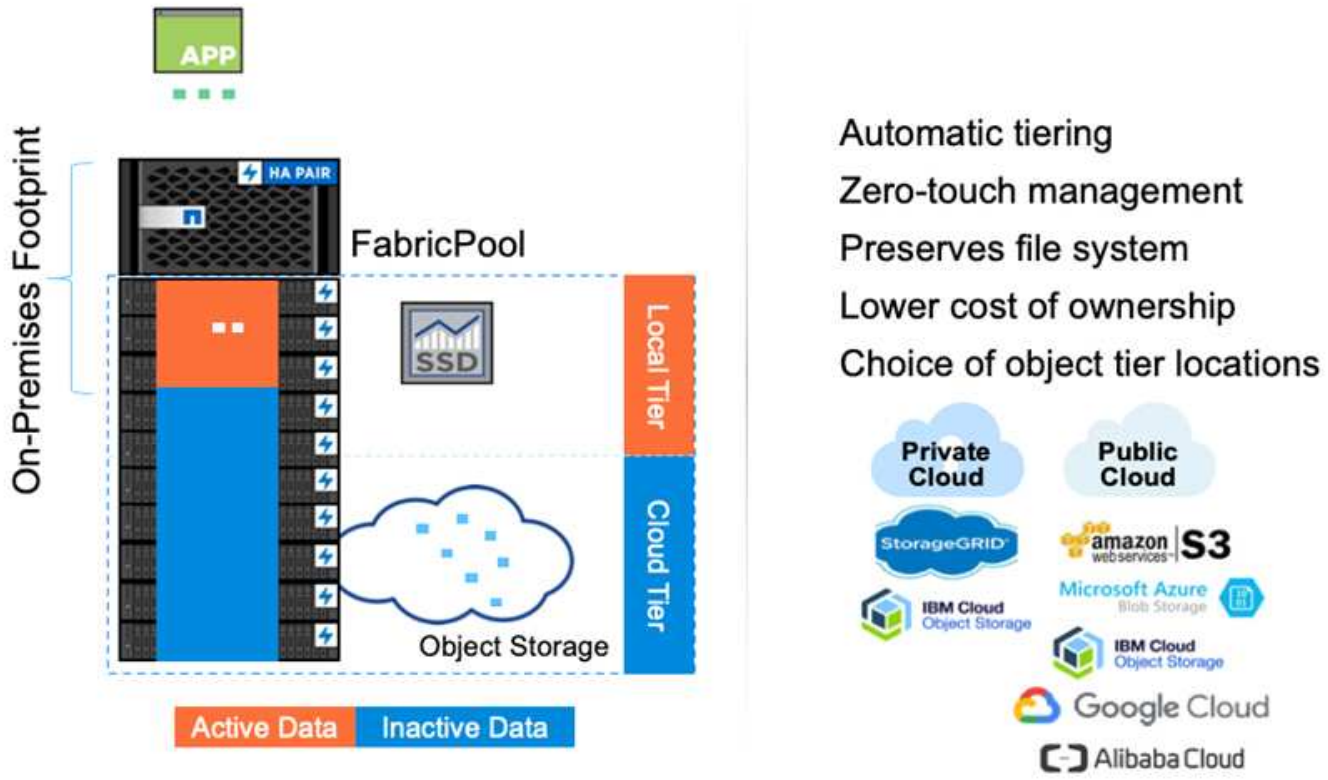
- **Validiertes Design und garantierte Ergebnisse.** Design- und Implementierungsleitfäden für FlexPod werden wiederholbar validiert. Sie umfassen umfassende Konfigurationsdetails und branchenspezifische Best Practices, die erforderlich sind, um ein FlexPod zuverlässig zu implementieren. Validierte Designrichtlinien, Implementierungsleitfäden und Architekturen von Cisco und NetApp helfen Ihrem Unternehmen im Gesundheitswesen oder Life Science, bei der Implementierung einer validierten und bewährten Plattform von Anfang an keine Unsicherheiten mehr zu mehr zu machen. Mit FlexPod können Sie Implementierungszeiten verkürzen und Kosten, Komplexität und Risiken senken. Durch validierte Designs und Implementierungsleitfäden von FlexPod wird FlexPod als ideale Plattform für eine Vielzahl von Genomik-Workloads etabliert.
- **Innovation und Agilität.** FlexPod wird als ideale Plattform von EHRs wie Epic, Cerner, Meditech und Imaging Systemen wie Agfa, GE, Philips empfohlen. Finden Sie weitere Informationen zu "Epische

Ehrenrolle" Und Zielplattform-Architektur finden Sie im Epic userweb. Genomik auf Basis "FlexPod" Ermöglicht es Organisationen im Gesundheitswesen, den Weg der Innovationen flexibel fortzusetzen. Mit FlexPod kommt es auf die natürliche Weise, Veränderungen im Unternehmen umzusetzen. Wenn Unternehmen eine FlexPod-Plattform nutzen, können IT-Experten im Gesundheitswesen Zeit, Aufwand und Ressourcen für Innovationen bereitstellen und so agil sein wie die Anforderungen des Ökosystems.

- **Data befreit.** mit der konvergenten Infrastrukturplattform FlexPod und einem NetApp ONTAP Storage-System können Genomikdaten über eine einzige Plattform zur Verfügung gestellt und zugänglich gemacht werden. FlexPod mit NetApp ONTAP bietet eine einfache, intuitive und leistungsstarke Hybrid-Cloud-Plattform. Die Data Fabric von NetApp ONTAP verknüpft Daten über Standorte, physische Grenzen und Applikationen hinweg. Ihre Data Fabric wurde für Unternehmen in einer datenorientierten Welt entwickelt. Daten werden an zahlreichen Orten erstellt und verwendet. Oft werden sie auch an mehreren Orten sowie in mehreren Applikationen und Infrastrukturen gleichzeitig genutzt. Daher benötigen Sie eine einheitliche und integrierte Lösung für das Management. Mit FlexPod hat Ihr IT-Team die Kontrolle und vereinfacht die ständig zunehmende Komplexität IM IT-BEREICH.
- **Sichere Mandantenfähigkeit.** FlexPod verwendet FIPS 140-2-2-konforme Kryptografiemodule, die es Unternehmen ermöglichen, Sicherheit als Grundelement und nicht als Nachdenken zu implementieren. FlexPod ermöglicht es Unternehmen, sichere Mandantenfähigkeit von einer einzigen konvergenten Infrastrukturplattform aus zu implementieren, unabhängig von der Größe der Plattform. FlexPod mit sicherer Mandantenfähigkeit und QoS unterstützt die Trennung von Workloads und maximiert die Auslastung. Dadurch vermeiden Sie, dass Investitionen in spezialisierte Plattformen gebunden sind, die möglicherweise nicht ausgelastet sind und über spezielle Fachkenntnisse für das Management erforderlich sind.
- **Storage-Effizienz.** Genomics erfordert, dass der zugrunde liegende Storage über branchenführende Storage-Effizienz-Funktionen verfügt. NetApp Storage-Effizienzfunktionen wie Deduplizierung (inline und On-Demand), Datenkomprimierung und Data-Compaction (senken die Storage-Kosten "ref"). NetApp Deduplizierung bietet Deduplizierung auf Blockebene in einem FlexVol Volume. Im Wesentlichen werden durch Deduplizierung Blockduplikate entfernt und somit nur eindeutige Blöcke im FlexVol Volume gespeichert. Die Deduplizierung arbeitet mit einer hohen Granularität und wird auf dem aktiven File-System des FlexVol Volume betrieben. Die folgende Abbildung zeigt die Funktionsweise der NetApp Deduplizierung. Deduplizierung ist applikationsunabhängig. Somit können auch Daten von beliebigen Applikationen dedupliziert werden, die das NetApp System nutzen. Sie können die Volume-Deduplizierung als Inline-Prozess und als Hintergrundprozess ausführen. Sie können die Funktion so konfigurieren, dass sie automatisch ausgeführt, geplant oder manuell über die CLI, den NetApp ONTAP System Manager oder NetApp Active IQ Unified Manager gestartet wird.



- **Genomik-Interoperabilität ermöglichen.** ONTAP FlexCache ist eine Remote-Caching-Funktion, die Dateiverteilung vereinfacht, WAN-Latenz reduziert und die Kosten für die WAN-Bandbreite senkt ("ref"). Eine der wichtigsten Aktivitäten bei der Identifizierung von Genomvariationen und bei der Annotation ist die Zusammenarbeit zwischen Ärzten. Die ONTAP FlexCache-Technologie erhöht den Datendurchsatz, selbst wenn mehrere Kliniker an verschiedenen geografischen Standorten zusammenarbeiten. Angesichts der typischen Größe einer *.BAM-Datei (1 GB bis 100 GB) ist es von großer Bedeutung, dass die zugrunde liegende Plattform Dateien für Kliniker an verschiedenen geografischen Standorten verfügbar machen kann. Mit FlexPod mit ONTAP FlexCache sind genomische Daten und Applikationen vollständig auf mehrere Standorte vorbereitet. Somit wird die Zusammenarbeit zwischen den weltweiten Forschern nahtlos ermöglicht, da sie eine geringe Latenz und einen hohen Durchsatz bieten. Medizinische Einrichtungen, die Genomapplikationen auf mehreren Standorten ausführen, können mit der Data-Fabric-Architektur horizontal skaliert werden, um das Management zu einem ausgewogenen Verhältnis zwischen Kosten und Geschwindigkeit zu halten.
- **Intelligente Nutzung der Speicherplattform.** FlexPod mit ONTAP Auto-Tiering und NetApp Fabric Pool Technologie vereinfacht das Datenmanagement. FabricPool senkt die Storage-Kosten, ohne dabei Einbußen bei Performance, Effizienz, Sicherheit oder Sicherung hinnehmen zu müssen. FabricPool ist transparent für Enterprise-Applikationen und nutzt die Cloud-Effizienz weiter, indem die Storage-TCO gesenkt werden, ohne dass die Applikationsinfrastruktur umgestaltet werden muss. FlexPod bietet die Storage Tiering-Funktionen von FabricPool für eine effizientere Nutzung von ONTAP Flash Storage. Weitere Informationen finden Sie unter "FlexPod mit FabricPool". Das folgende Diagramm bietet einen allgemeinen Überblick über FabricPool und seine Vorteile.



- **Schnellere Variantenanalyse und -Annotation.** die FlexPod-Plattform ist schneller bereitzustellen und zu operationalisieren. Die FlexPod Plattform ermöglicht klinische Zusammenarbeit, da die Daten in großen Umgebungen mit niedriger Latenz und höherem Durchsatz verfügbar sind. Eine bessere Interoperabilität ermöglicht Innovationen. Medizinische Einrichtungen können nebeneinander ihre genomischen und nicht genomischen Workloads ausführen. Das bedeutet, dass Unternehmen für den Übergang zur Genomik keine speziellen Plattformen benötigen.

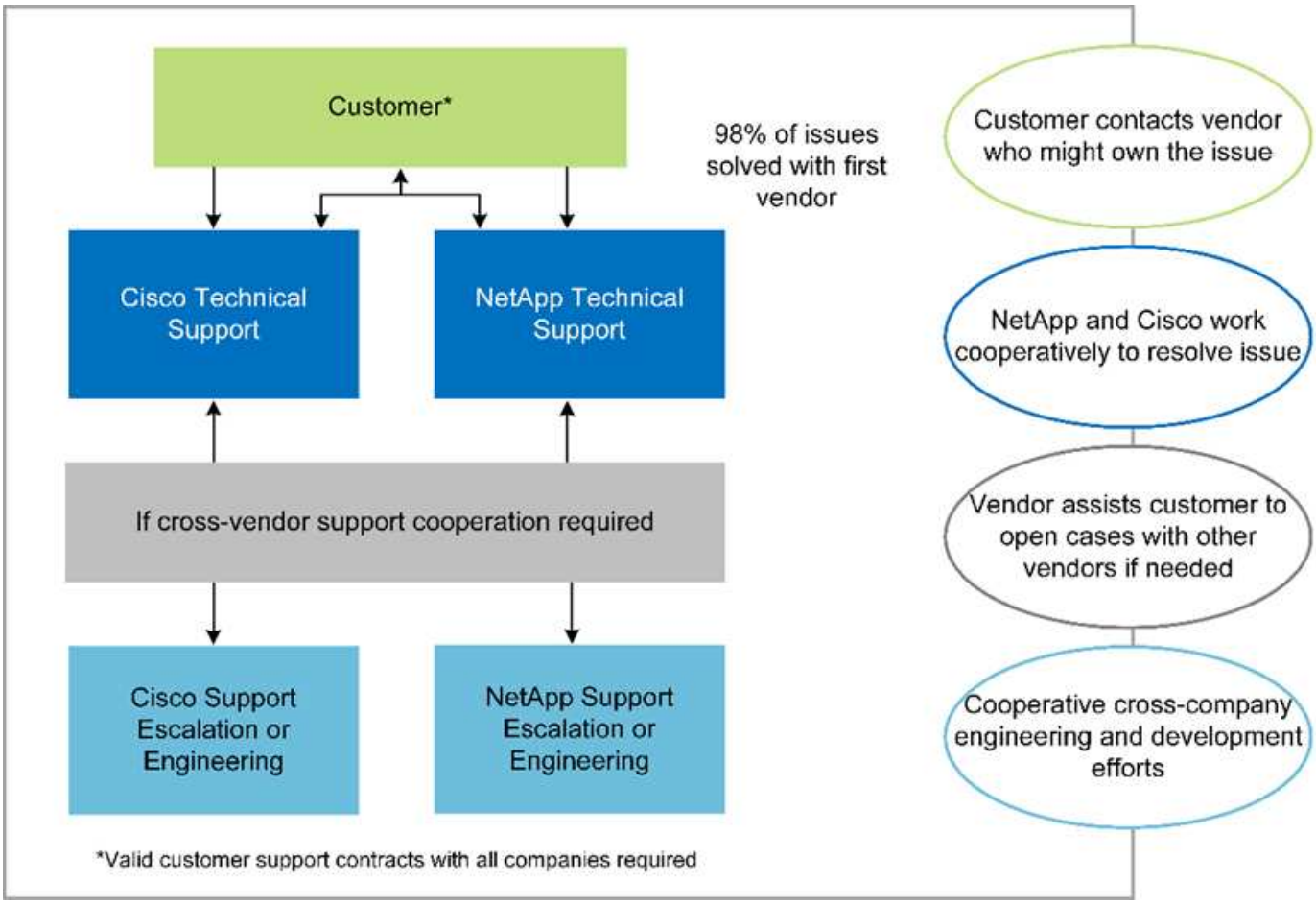
  FlexPod ONTAP erweitert die Storage-Plattform routinemäßig auf die neuesten Funktionen. FlexPod Datacenter ist die optimale Grundlage für die Implementierung von FC- NVMe-Storage für hochperformanten Storage-Zugriff auf Applikationen, die sie benötigen. Da FC- NVMe mit hoher Verfügbarkeit, Multipathing und zusätzlicher Unterstützung von Betriebssystemen einhergeht, eignet sich FlexPod hervorragend als bevorzugte Plattform und bietet die Skalierbarkeit und Zuverlässigkeit, die zur Unterstützung dieser Funktionen erforderlich sind. ONTAP mit schnelleren I/O-Vorgängen und End-to-End-NVMe ermöglicht Analysen der Genomik schneller ("ref").

  Die sequenzierten RAW-Genomdaten erzeugen große Dateigrößen, und es ist wichtig, dass diese Dateien den Variantenanalysatoren zur Verfügung gestellt werden, um die Gesamtzeit von der Probensammlung bis zur Variantenbeschriftung zu reduzieren. Wenn NVMe (Nonvolatile Memory Express) als Storage-Zugriffs- und Datenübertragungsprotokoll verwendet wird, bietet das Unternehmen einen beispiellosen Durchsatz und die schnellsten Reaktionszeiten. FlexPod implementiert das NVMe-Protokoll und greift über den PCI Express Bus (PCIe) auf Flash-Storage zu. PCIe ermöglicht die Implementierung von Zehntausenden von Befehlswarteschlangen, wodurch sich die Parallelisierung und der Durchsatz erhöhen. Ein einziges Protokoll von der Storage- bis zum Speicher sorgt für schnellen Datenzugriff.

- **Agilität für die klinische Forschung von Grund auf.** Dank flexibler, erweiterbarer Speicherkapazität und Performance können Forschungsunternehmen im Gesundheitswesen die Umgebung flexibel oder just-in-time (JIT) optimieren. Durch die Entkopplung der Storage-Systeme von der Computing- und Netzwerkinfrastruktur lässt sich die FlexPod Plattform unterbrechungsfrei vertikal und horizontal skalieren. Mithilfe von Cisco Intersight lässt sich die FlexPod Plattform sowohl mit integrierten als auch mit

benutzerdefinierten automatisierten Workflows managen. Durch die Cisco Intersight Workflows können Organisationen im Gesundheitswesen die Lebenszyklusmanagement-Zeiten von Anwendungen reduzieren. Wenn ein akademisches medizinisches Zentrum verlangt, dass Patientendaten anonymisiert und ihrem Zentrum für Forschungsinformatik bzw. Datacenter in Bezug auf Qualität zur Verfügung gestellt werden, kann die IT-Abteilung Cisco Intersight FlexPod Workflows nutzen, um sichere Daten-Backups, Klone und die Wiederherstellung in nur wenigen Sekunden statt Stunden durchzuführen. Mit NetApp Trident und Kubernetes können IT-Abteilungen neue Data Scientists bereitstellen und klinische Daten für die Modellentwicklung in wenigen Minuten – manchmal sogar in Sekunden – zur Verfügung stellen.

- **Schutz von Genomdaten.** NetApp SnapLock bietet ein speziell zu Zweck geuniversell einsetzbares Volume, in dem Dateien gespeichert und in einen nicht löschbaren, nicht wiederbeschreibbaren Zustand versetzt werden können. Die Produktionsdaten des Benutzers, die sich in einem FlexVol Volume befinden, können mithilfe von NetApp SnapMirror oder SnapVault gespiegelt oder in ein SnapLock Volume archiviert werden. Die Dateien im SnapLock Volume, das Volume selbst und das Hosting-Aggregat können bis zum Ende der Aufbewahrungsdauer nicht gelöscht werden. ONTAP FPolicy Software verhindert Ransomware-Angriffe, indem sie auf Dateien mit bestimmten Erweiterungen distanten. Ein FPolicy-Ereignis kann für bestimmte Dateivorgänge ausgelöst werden. Das Ereignis ist mit einer Richtlinie verknüpft, die die Engine aufruft, die es verwenden muss. Sie können eine Richtlinie mit einer Reihe von Dateierweiterungen konfigurieren, die möglicherweise Ransomware enthalten könnten. Wenn eine Datei mit einer nicht zulässigen Erweiterung versucht, einen nicht autorisierten Vorgang auszuführen, verhindert FPolicy die Ausführung dieses Vorgangs ("ref").
- **Kooperativer Support für FlexPod** NetApp und Cisco haben ein solides, skalierbares und flexibles Support-Modell für den FlexPod entwickelt, das die individuellen Support-Anforderungen der konvergenten FlexPod Infrastruktur erfüllt. Dieses Modell greift auf die Erfahrungswerte, Ressourcen und das Know-how des technischen Supports von NetApp und Cisco zurück, um unabhängig von der Ursache des Problems einen optimierten Prozess der Identifizierung und Behebung von FlexPod Support-Problemen zu bieten. Die folgende Abbildung bietet einen Überblick über das kooperative Support-Modell für FlexPod. Der Kunde kontaktiert den Anbieter, der möglicherweise für das Problem zuständig ist, und Cisco und NetApp arbeiten gemeinsam an einer Lösung. Cisco und NetApp verfügen über unternehmensübergreifende Engineering- und Entwicklungsteams, die Hand in Hand arbeiten, um Probleme zu lösen. Dieses Support-Modell reduziert den Verlust von Informationen während der Übersetzung, sorgt für Vertrauen und reduziert Ausfallzeiten.

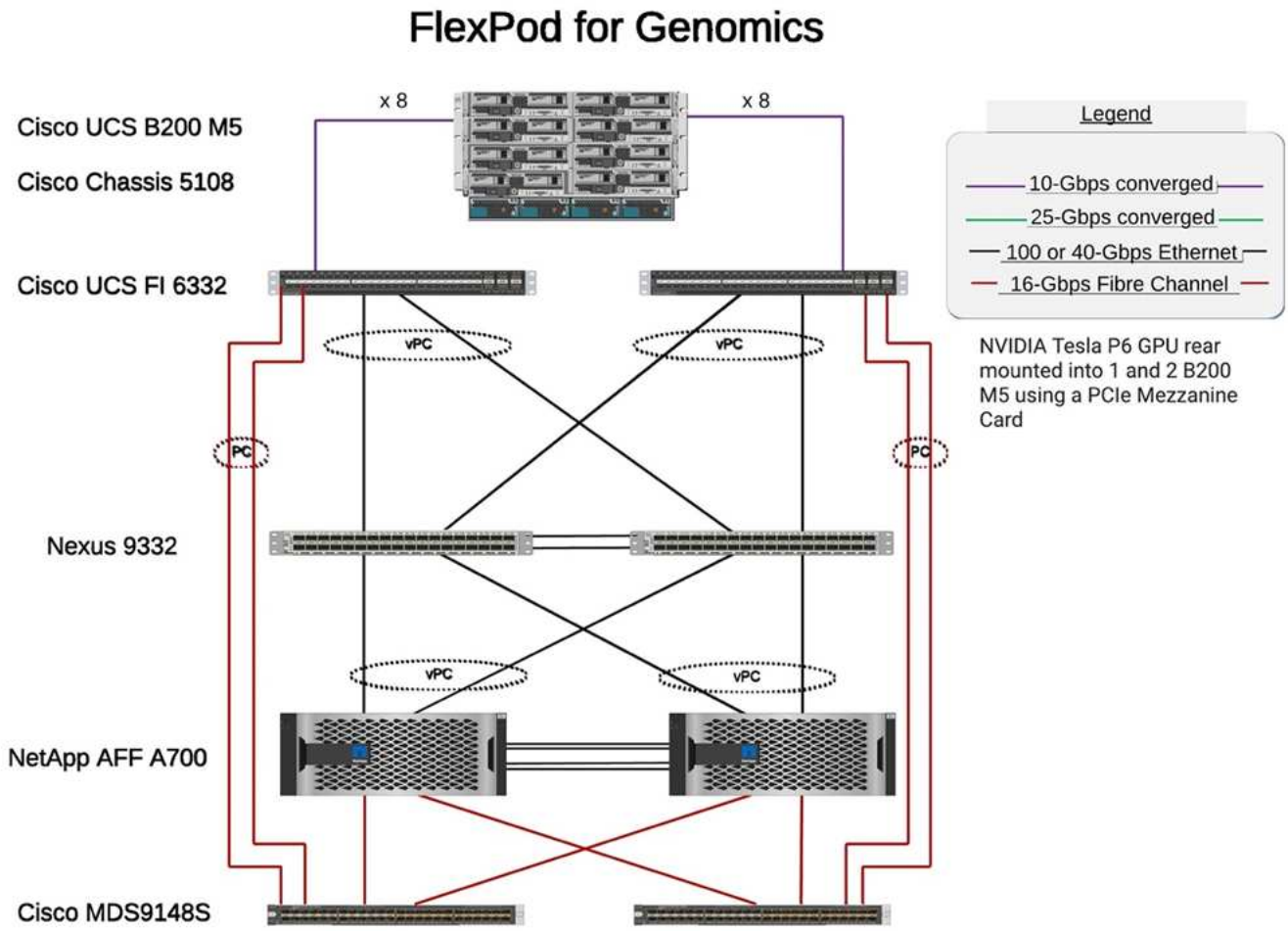


"Als Nächstes: Hardware- und Softwarekomponenten in der Lösungsinfrastruktur."

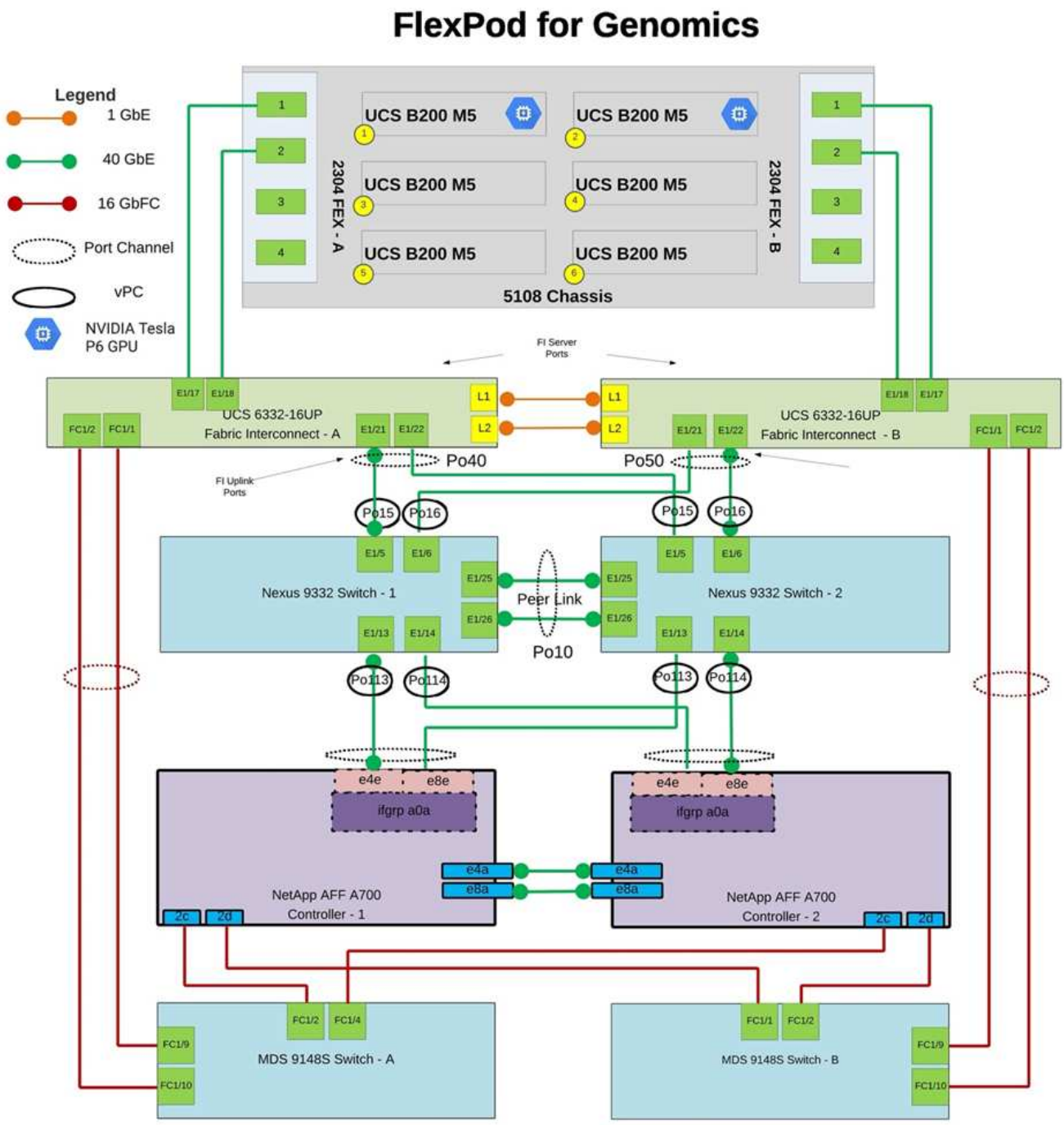
Hardware- und Softwarekomponenten der Lösungsinfrastruktur

"Previous: Vorteile der Implementierung genomische Workloads auf FlexPod."

Die folgende Abbildung zeigt das FlexPod-System, das für die Einrichtung und Validierung von GATK verwendet wird. Wir haben genutzt "FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 Cisco Validated Design (CVD)" Während des Setups.



Im folgenden Diagramm sind die Details zur FlexPod-Verkabelung dargestellt.



In der folgenden Tabelle sind die während der GATK-Tests verwendeten Hardwarekomponenten auf einem FlexPod aufgeführt. Hier ist der "NetApp Interoperabilitäts-Matrix-Tool" (IMT) und "Cisco Hardware Compatibility List (HCL)".

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1 oder 2	
	Cisco UCS Blade Server	6 B200 M5	Jeweils mit 2x 20 Cores, 2,7 GHz und 128 bis 384 GB RAM

Schicht	Produktfamilie	Menge und Modell	Details
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Siehe
	2 Cisco UCS Fabric Interconnects	6332	-
Netzwerk	Cisco Nexus Switches	2 x Cisco Nexus 9332	-
Datennetzwerk Storage-Netzwerk	IP-Netzwerk für Storage-Zugriff über SMB-/CIFS-, NFS- oder iSCSI-Protokolle	Gleiche Netzwerk-Switches wie oben	-
	Storage-Zugriff über FC	2 x Cisco MDS 9148S	-
Storage	NetApp AFF A700 All-Flash-Storage-System	1 Cluster	Cluster mit zwei Nodes
	Festplatten-Shelf	Ein DS224C oder NS224 Festplatten-Shelf	Vollständig mit 24 Laufwerken bestückt
	SSD	24, 1,2 TB oder höhere Kapazität	-

In dieser Tabelle ist die Infrastruktursoftware aufgeführt.

Software	Produktfamilie	Version/Release	Details
Verschiedene	Linux	RHEL 8.3	-
	Windows	Windows Server 2012 R2 (64-Bit)	-
	NetApp ONTAP	ONTAP 9.8 oder höher	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 oder höher	-
	Cisco Switches der Ethernet-Serie 3000 oder 9000	Für 9000-Serie, 7.0(3)I7(7) oder höher für 3000-Serie, 9.2(4) oder höher	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) oder höher	-
	Hypervisor	VMware vSphere ESXi 7.0	-
Storage	Hypervisor-Managementsystem	VMware vCenter Server 7.0 (vCSA) oder höher	-
Netzwerk	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	-
	NetApp SnapCenter	SnapCenter 4.3 oder höher	-
	Cisco UCS Manager	4.1(3c) oder höher	

Software	Produktfamilie	Version/Release	Details
Hypervisor	ESXi		
Vereinfachtes	Hypervisor-ManagementsystemVMware vCenter Server 7.0 (vCSA) oder höher		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	
	NetApp SnapCenter	SnapCenter 4.3 oder höher	
	Cisco UCS Manager	4.1(3c) oder höher	

"Weiter: Genomik - GATK Einrichtung und Ausführung."

Genomik - GATK Einrichtung und Ausführung

"Früher: Hardware- und Softwarekomponenten der Lösungsinfrastruktur."

Laut dem National Human Genome Research Institute ("NHGRI"„Genomics ist die Untersuchung aller Gene einer Person (das Genom), einschließlich der Wechselwirkungen dieser Gene miteinander und mit der Umwelt einer Person. „

Laut dem "NHGRI", "Deoxyribonukleinsäure (DNA) ist die chemische Verbindung, die die notwendigen Anweisungen enthält, um die Aktivitäten von fast allen lebenden Organismen zu entwickeln und zu leiten. DNA-Moleküle bestehen aus zwei verdrehenden, paarweise angeordneten Strängen, die oft als Doppelhelix bezeichnet werden.“ „Der gesamte DNA-Satz eines Organismus wird sein Genom genannt.“

Sequenzierung ist der Prozess der Bestimmung der genauen Reihenfolge der Basen in einem Strang der DNA. Eine der häufigsten Sequenzierungsarten, die heute verwendet werden, nennt man Sequenzierung durch Synthese. Diese Technik verwendet die Emission von fluoreszierenden Signalen, um die Grundlagen zu bestellen. Forscher können mit Hilfe der DNA-Sequenzierung nach genetischen Variationen und Mutationen suchen, die bei der Entwicklung oder dem Fortschreiten einer Krankheit eine Rolle spielen könnten, während sich eine Person noch im embryonalen Stadium befindet.

Von der Probe bis zur Variantenidentifikation, Anmerkung und Vorhersage

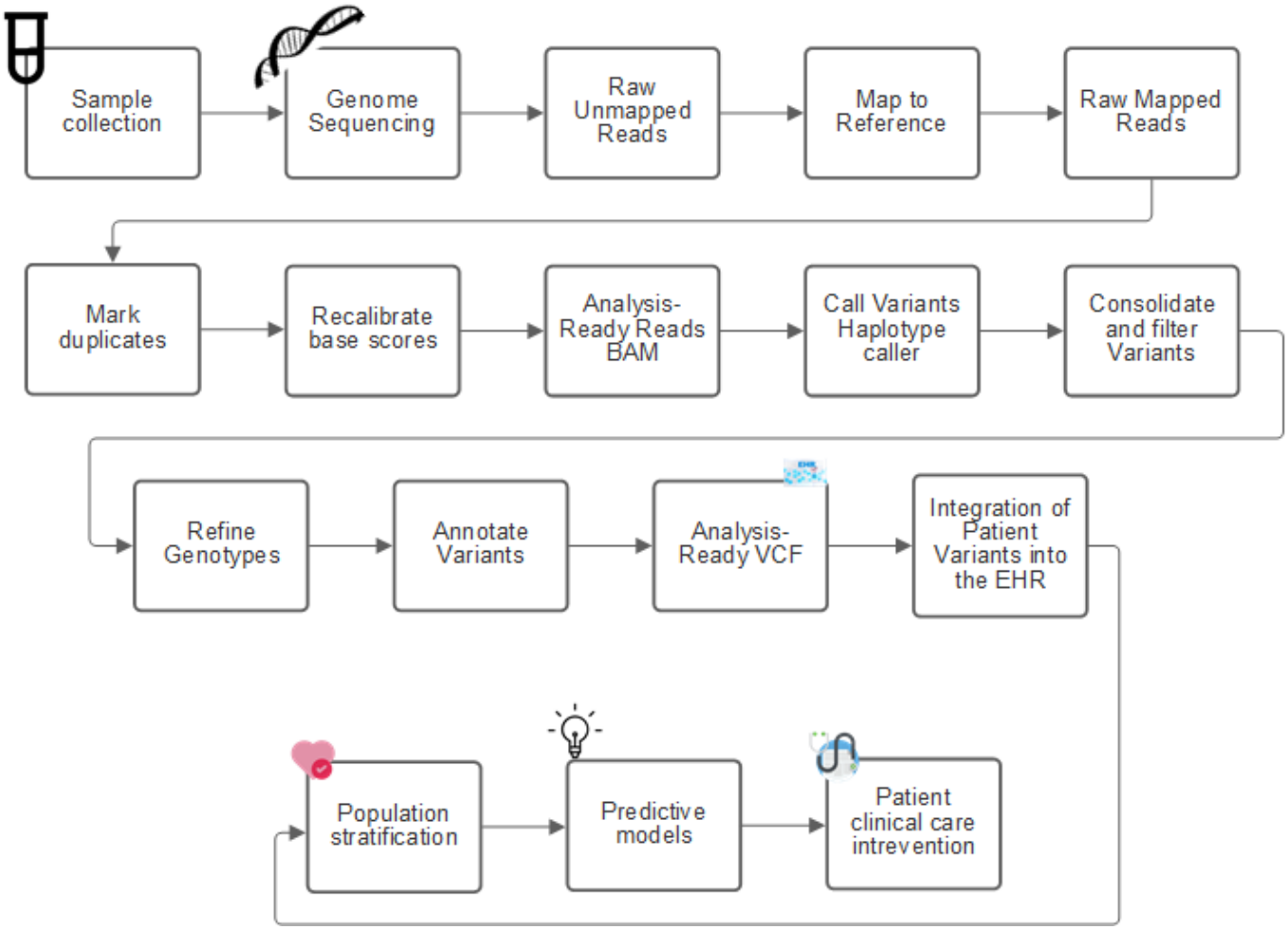
Genomik kann im allgemeinen zu den folgenden Schritten eingeteilt werden. Dies ist keine umfassende Liste:

1. Probenentnahme.
2. "Genom-Sequenzierung" Verwenden eines Sequenzers zum Generieren der Rohdaten.
3. Vorverarbeitung: Beispiel: "Deduplizierung" Wird verwendet "Picard".
4. Genomanalyse:
   a. Wird einem Referenzgenom zugeordnet.
   b. "Variante" Identifizierung und Beschriftung, die in der Regel mit GATK und ähnlichen Tools durchgeführt werden.
5. Integration in das Electronic Health Record-System (EHR).
6. "Bevölkerungsstratifizierung" Und Identifizierung der genetischen Variation über geografische Lage und

ethnische Herkunft.

7. "Prädiktive Modelle" Verwendung von signifikanter Single-Nukleotid-Polymorphismus.
8. "Validierung".

Die folgende Abbildung zeigt den Prozess von der Probenahme bis zur Variantenidentifikation, Anmerkung und Vorhersage.



Das Human Genome Projekt wurde im April 2003 abgeschlossen und das Projekt stellte eine sehr hochwertige Simulation der menschlichen Genom-Sequenz dar, die in der Öffentlichkeit zur Verfügung stand. Das Referenzgenom initiierte eine Explosion der Forschung und Entwicklung von Genomfunktionen. Praktisch jede menschliche Krankheit hat eine Signatur in den Genen des Menschen. Bis vor kurzem nutzen Ärzte Gene, um Geburtsfehler wie Sichelzellenanämie vorherzusagen und zu bestimmen, die durch ein bestimmtes Erbmuster verursacht wird, das durch eine Änderung in einem einzelnen Gen verursacht wird. Die Schatzkammer der Daten, die das Humangenom-Projekt zur Verfügung gestellt wurde, führte zu dem Beginn des aktuellen Status der Genomfunktionen.

Die Genomik bietet zahlreiche Vorteile. Hier ein kleiner Satz von Vorteilen in den Bereichen Gesundheitswesen und Life Sciences:

- Bessere Diagnose am Point of Care
- Bessere Prognose
- Präzisionsmedizin

- Personalisierte Behandlungspläne
- Bessere Krankheitsüberwachung
- Verringerung unerwünschter Ereignisse
- Besserer Zugang zu Therapien
- Verbesserte Krankheitsüberwachung
- Effektive Teilnahme an klinischen Studien und bessere Auswahl von Patienten für klinische Studien auf Basis von Genotypen.

Genomik ist eine "Vierköpfige," Aufgrund der Computing-Anforderungen für den gesamten Lebenszyklus eines Datensatzes, zu Erfassung, Storage, Verteilung und Analyse

Genom Analysis Toolkit (GATK)

GATK wurde als Datenwissenschaftsplattform am entwickelt "Broad Institute". GATK ist eine Reihe von Open-Source-Tools, die Genomanalysen ermöglichen, insbesondere Variantenerkennung, Identifizierung, Annotation und Genotyping. Einer der Vorteile von GATK besteht darin, dass der Satz von Tools und Befehlen zu einem kompletten Workflow gekettet werden kann. Die Hauptprobleme, mit denen sich das breite Institut befasst, sind:

- Die Ursachen und biologischen Mechanismen von Krankheiten verstehen.
- Identifizieren Sie therapeutische Interventionen, die auf die grundlegende Ursache einer Krankheit wirken.
- Verstehen Sie die Sichtlinie von Varianten bis zur Funktion in der menschlichen Physiologie.
- Standards und Richtlinien erstellen "Frameworks" Für die Darstellung von Genomdaten, Speicherung, Analysen, Sicherheit usw.
- Standardisieren und Sozialisieren interoperabler Genom Aggregation Datenbanken (gnomAD).
- Genom-basierte Überwachung, Diagnose und Behandlung von Patienten mit größerer Präzision.
- Helfen Sie bei der Implementierung von Tools, mit denen Krankheiten schon lange vorhergesagt werden, bevor Symptome auftreten.
- Schaffen und stärken Sie eine Gemeinschaft von interdisziplinären Mitarbeitern, um die schwierigsten und wichtigsten Probleme in der Biomedizin zu lösen.

Nach Angaben des GATK und des breiten Instituts sollte die Genomsequenzierung in einem Pathologielabor als Protokoll behandelt werden; jede Aufgabe ist gut dokumentiert, optimiert, reproduzierbar und konsistent über Proben und Experimente hinweg. Im Folgenden finden Sie eine Reihe von Schritten, die vom Broad Institute empfohlen werden. Weitere Informationen finden Sie im "GATK-Website".

Einrichtung von FlexPod

Für Genomik-Workloads wurde eine FlexPod Infrastrukturplattform von Grund auf neu eingerichtet. Die FlexPod Plattform ist hochverfügbar und lässt sich unabhängig skalieren, beispielsweise Netzwerk, Storage und Compute unabhängig voneinander skalieren. Wir verwendeten den folgenden Cisco Validated Design Leitfaden als Referenzarchitekturdokument zur Einrichtung der FlexPod Umgebung: "FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7". Sehen Sie sich die folgenden FlexPod Plattform-Highlights an:

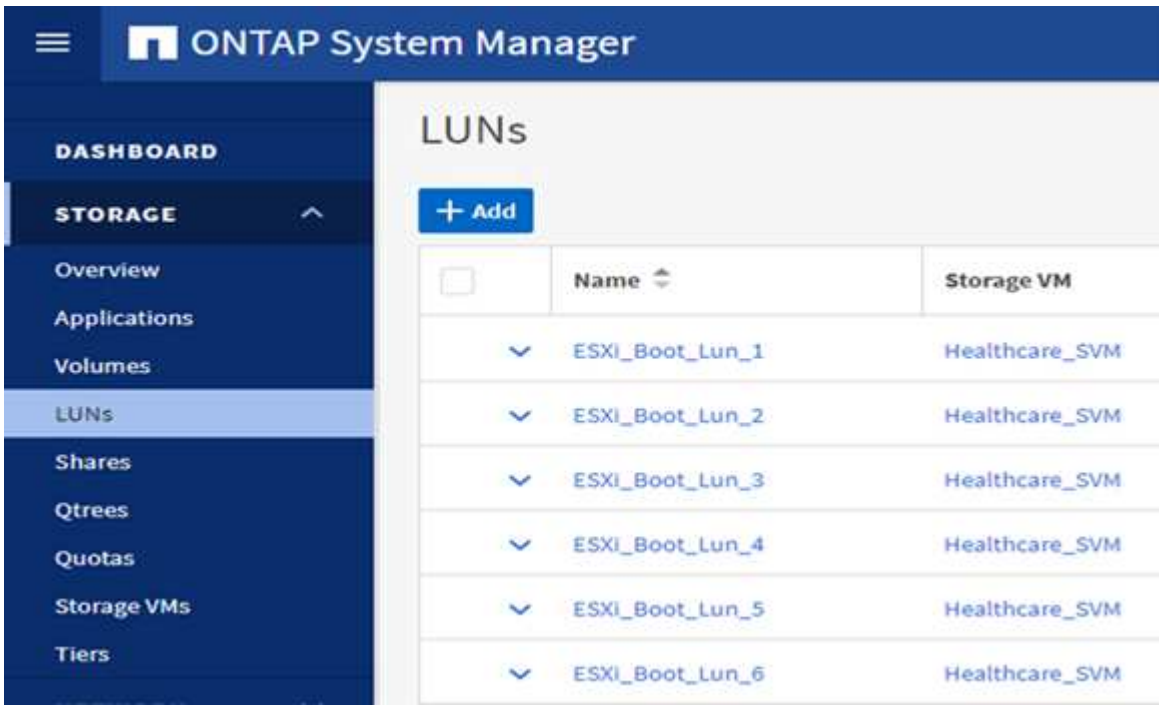
Um die FlexPod Lab-Einrichtung durchzuführen, gehen Sie wie folgt vor:

1. Zur Einrichtung und Validierung von FlexPod kommen die folgenden IP4-Reservierungen und -VLANs zum Einsatz.

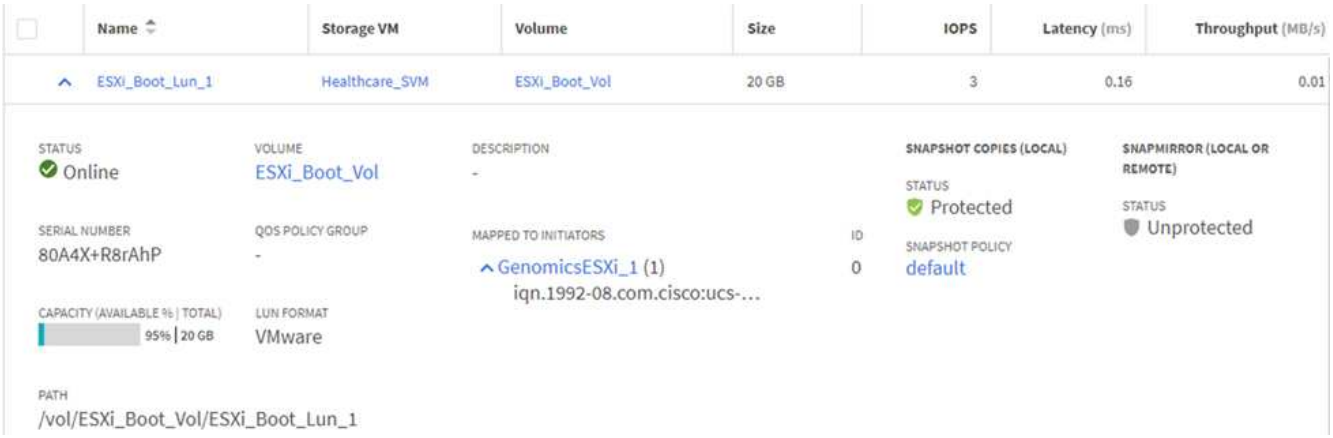
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. Konfigurieren Sie iSCSI-basierte Boot-LUNs auf der ONTAP SVM.

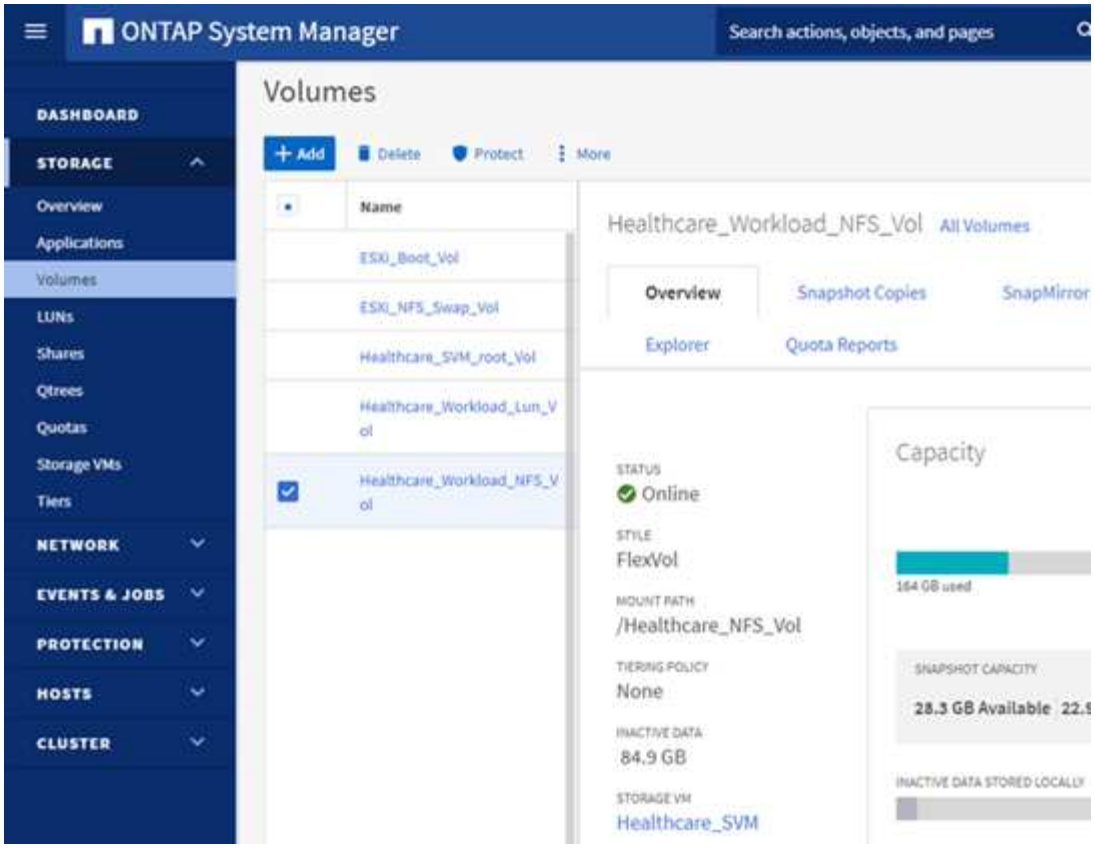


3. Zuordnen von LUNs zu iSCSI-Initiatorgruppen

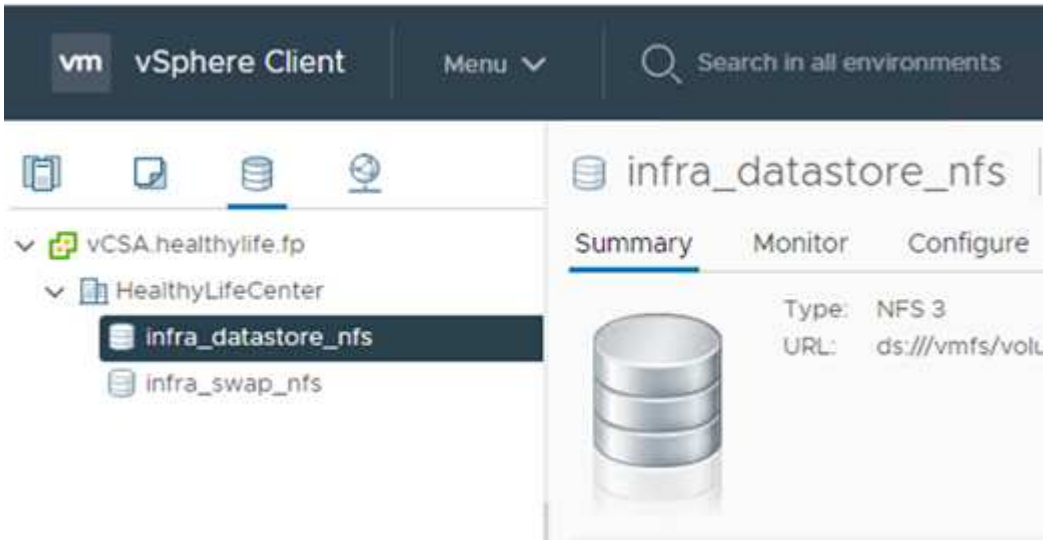


4. Installation von vSphere 7.0 mit iSCSI Boot
5. Registrieren Sie ESXi-Hosts mit vCenter.

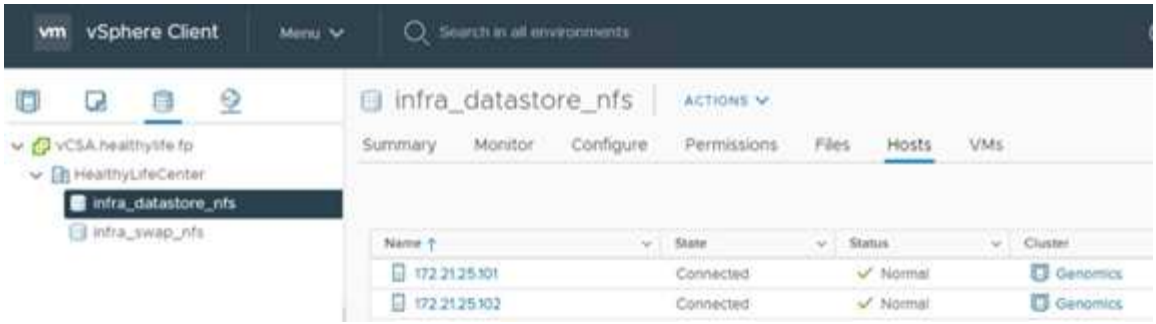
6. Bereitstellung eines NFS-Datenspeichers `infra_datastore_nfs` Auf dem ONTAP Storage.



7. Fügen Sie den Datastore zum vCenter hinzu.



8. Fügen Sie mithilfe von vCenter einen NFS-Datenspeicher zu den ESXi Hosts hinzu.



9. Erstellen Sie mithilfe von vCenter eine VM mit Red hat Enterprise Linux (RHEL) 8.3 zur Ausführung von GATK.
10. Ein NFS-Datastore wird der VM präsentiert und bei gemountet `/mnt/genomics`, Die zum Speichern von ausführbaren GATK-Dateien, Skripten, BAM-Dateien (Binary Alignment Map), Referenzdateien, Indexdateien, Wörterbuchdateien und Ausrufdateien für Variantenaufrufe verwendet wird.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb                308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

GATK-Einrichtung und -Ausführung

Installieren Sie die folgenden Voraussetzungen auf der RedHat Enterprise 8.3 Linux VM:

- Java 8 oder SDK 1.8 oder höher
- GATK 4.2.0.0 vom Broad Institute herunterladen "GitHub-Website". Genom-Sequenzdaten werden in der Regel in Form einer Reihe von tabulatorgetrennte ASCII-Spalten gespeichert. ASCII beansprucht jedoch zu viel Platz zum Speichern. Daher wurde ein neuer Standard entwickelt, der als BAM (*.bam)-Datei bezeichnet wird. Eine BAM-Datei speichert die Sequenzdaten in komprimierter, indizierter und binärer Form. Wir "Heruntergeladen" Eine Reihe öffentlich verfügbarer BAM-Dateien für die GATK-Ausführung vom "Öffentliche Domäne". Wir haben auch Indexdateien (*.bai), Wörterbuchdateien (*) heruntergeladen. Dict) und Referenzdatendateien (*. fasta) von der gleichen öffentlichen Domäne.

Nach dem Download verfügt das GATK-Tool-Kit über eine JAR-Datei und eine Reihe von Supportskripten.

- `gatk-package-4.2.0.0-local.jar` Ausführbar
- `gatk` Skriptdatei.

Wir haben die BAM-Dateien und die entsprechenden Index-, Wörterbuch- und Referenzgenom-Dateien für eine Familie heruntergeladen, die aus Vater-, Mutter- und Son *.bam-Dateien bestand.

Cromwell-Motor

Cromwell ist eine Open-Source-Engine, die auf wissenschaftliche Workflows ausgerichtet ist und Workflow-Management ermöglicht. Der Cromwell Motor kann in zwei laufen "Modi", Servermodus oder ein Einzelworkflowmodus. Das Verhalten des Cromwell-Motors kann mit dem gesteuert werden "Cromwell Engine-Konfigurationsdatei".

- **Servermodus.** aktiviert "Rest-konforme" Ausführung von Workflows in Cromwell Engine.
- **Run-Modus.** der Run-Modus eignet sich am besten zur Ausführung einzelner Workflows in Cromwell, "ref" Für einen vollständigen Satz verfügbarer Optionen im Run-Modus.

Wir nutzen die Cromwell Engine, um die Workflows und Pipelines nach Bedarf auszuführen. Die Cromwell Engine verwendet eine benutzerfreundliche "Sprache für die Workflow-Beschreibung" (WDL)-basierte Skriptsprache. Cromwell unterstützt auch einen zweiten Workflow-Skriptstandard, der als Common Workflow Language (CWL) bezeichnet wird. In diesem technischen Bericht wurde WDL verwendet. WDL wurde ursprünglich vom Broad Institute for Genome Analysis Pipelines entwickelt. Mithilfe der WDL-Workflows können verschiedene Strategien implementiert werden, darunter:

- **Linear Chaining.** wie der Name schon sagt, wird die Ausgabe von Task#1 als Eingabe an Task #2 gesendet.
- **Multi-in/out.** Dies ist ähnlich wie bei linearer Verkettung, da jede Aufgabe mehrere Ausgänge als Eingang zu nachfolgenden Aufgaben haben kann.
- **Scatter-Gather.** Dies ist eine der leistungsstärksten EAI-Strategien (Enterprise Application Integration), die zur Verfügung stehen, insbesondere bei ereignisgesteuerter Architektur. Jede Aufgabe wird entkoppelt ausgeführt, und die Ausgabe für jede Aufgabe wird in die Endausgabe konsolidiert.

Es gibt drei Schritte, wenn WDL zum Ausführen von GATK im Standalone-Modus verwendet wird:

1. Syntax validieren mit `womtool.jar`.

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. Eingabe JSON generieren.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Führen Sie den Workflow mit der Cromwell Engine und aus `Cromwell.jar`.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

Das GATK kann mit mehreren Methoden ausgeführt werden; dieses Dokument untersucht drei dieser Methoden.

Ausführung von GATK mit der JAR-Datei

Schauen wir uns eine einzelne Variante Call Pipeline-Ausführung unter Verwendung des haplotypype Variant Caller an.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

Bei dieser Methode der Ausführung verwenden wir die lokale GATK-Ausführungs-JAR-Datei, wir verwenden einen einzigen java-Befehl, um die JAR-Datei aufzurufen, und wir übergeben mehrere Parameter an den Befehl.

1. Dieser Parameter gibt an, dass wir den aufrufen `HaplotypeCaller` Variant Caller Pipeline.
2. `-- input` Gibt die Eingabe-BAM-Datei an.
3. `--output` Gibt die Variant-Ausgabedatei im Variantenaufrufformat (*.vcf) an ("ref").
4. Mit dem `--reference` Parameter, geben wir ein Referenzgenom weiter.

Nach der Ausführung sind die Ausgabendetails im Abschnitt zu finden "Ausgabe zur Ausführung des GATK unter Verwendung der JAR-Datei."

Ausführung von GATK mit ./gatk-Skript

Das GATK-Werkzeugkit kann mit dem ausgeführt werden `./gatk` Skript: Untersuchen wir nun den folgenden Befehl:

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

Wir übergeben mehrere Parameter an den Befehl.

- Dieser Parameter gibt an, dass wir den aufrufen `HaplotypeCaller` Variant Caller Pipeline.
- `-I` Gibt die Eingabe-BAM-Datei an.
- `-O` Gibt die Variant-Ausgabedatei im Variantenaufrufformat (*.vcf) an ("ref").
- Mit dem `-R` Parameter, geben wir ein Referenzgenom weiter.

Nach der Ausführung sind die Ausgabendetails im Abschnitt zu finden

Ausführung von GATK mit Cromwell Engine

Wir verwenden die Cromwell-Engine, um die Ausführung des GATK zu verwalten. Schauen wir uns die Kommandozeile und ihre Parameter an.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

Hier rufen wir den Java-Befehl auf, indem wir den übergeben `-jar` Parameter, um anzugeben, dass wir eine JAR-Datei ausführen möchten, z. B. `Cromwell-65.jar`. Der nächste Parameter wurde übergeben (`run`) Zeigt an, dass die Cromwell-Engine im Run-Modus läuft, die andere mögliche Option ist der Server-Modus. Der nächste Parameter lautet `*.wdl` Dass der Run-Modus zum Ausführen der Pipelines verwendet werden soll. Der nächste Parameter ist der Satz von Eingabeparametern für die ausgeführten Workflows.

Hier ist der Inhalt der `ghplo.wdl` Datei wie folgt aussehen:

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

Hier ist die entsprechende JSON-Datei mit den Eingaben zur Cromwell Engine.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Bitte beachten Sie, dass Cromwell für die Ausführung eine in-Memory-Datenbank verwendet. Nach der Ausführung ist das Ausgabungsprotokoll im Abschnitt zu sehen "Ausgabe zur Ausführung von GATK mit Cromwell Engine."

Eine umfassende Reihe von Schritten zur Ausführung des GATK finden Sie im "GATK-Dokumentation".

"Weiter: Ausgabe für die Ausführung von GATK mit der JAR-Datei."

Ausgabe zur Ausführung des GATK unter Verwendung der JAR-Datei

"Früher: Genomik - GATK Einrichtung und Ausführung."

Die Ausführung von GATK unter Verwendung der JAR-Datei hat folgende Probenausgabe erzeugt.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
```

```
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
```

```
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

Beachten Sie, dass sich die Ausgabedatei an dem nach der Ausführung angegebenen Speicherort befindet.

Ausgabe zur Ausführung des GATK mit dem Skript ./gatk

"Zurück: Ausgabe für die Ausführung von GATK mit der JAR-Datei."

Die Ausführung des GATK unter Verwendung des `./gatk` Skript hat die folgende Musterausgabe erzeugt.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
```

```
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
```

```
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

Beachten Sie, dass sich die Ausgabedatei an dem nach der Ausführung angegebenen Speicherort befindet.

"Weiter: Ausgabe für die Ausführung von GATK mit der Cromwell-Engine."

Ausgabe zur Ausführung von GATK mit Cromwell Engine

Die Ausführung von GATK mit der Cromwell-Engine hat die folgende Probenausgabe erzeugt.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
```

```
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
```

```
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
```

```
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
```

```
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"Als Nächstes: GPU-Setup."

GPU-Einrichtung

"Zurück: Ausgabe für die Ausführung von GATK mit der Cromwell-Engine."

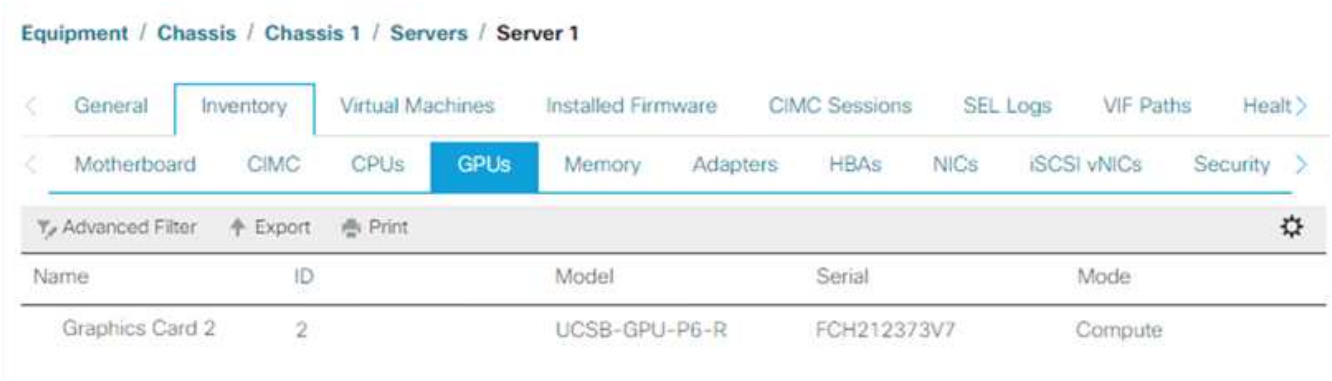
Zum Zeitpunkt der Veröffentlichung bietet das GATK-Tool keine native Unterstützung für die GPU-basierte Ausführung vor Ort. Die folgende Einrichtung und Anleitung werden bereitgestellt, damit die Leser verstehen können, wie einfach es ist, FlexPod mit einer an der Rückseite montierten NVIDIA Tesla P6 GPU mit einer PCIe Mezzanine-Karte für GATK zu verwenden.

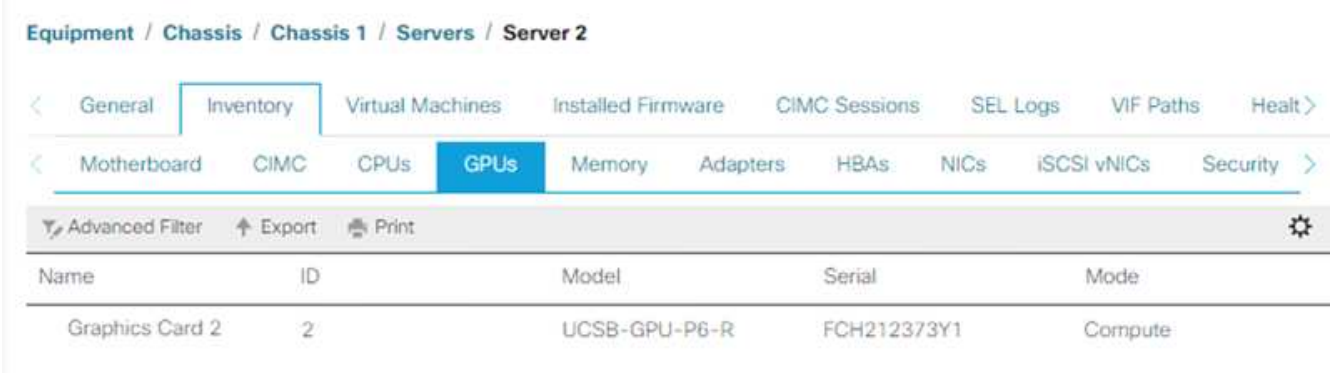
Zur Einrichtung der FlexPod Umgebung haben wir folgendes Cisco Validated Design (CVD) als Referenzarchitektur und Best Practice Guide verwendet. Damit können wir Applikationen ausführen, die GPUs verwenden.

- "FlexPod Datacenter for AI/ML with Cisco UCS 480 ML for Deep Learning"

Kernpunkte dieses Setups:

1. Wir haben eine PCIe NVIDIA Tesla P6 GPU in einem Mezzanine-Steckplatz in den UCS B200 M5 Servern verwendet.





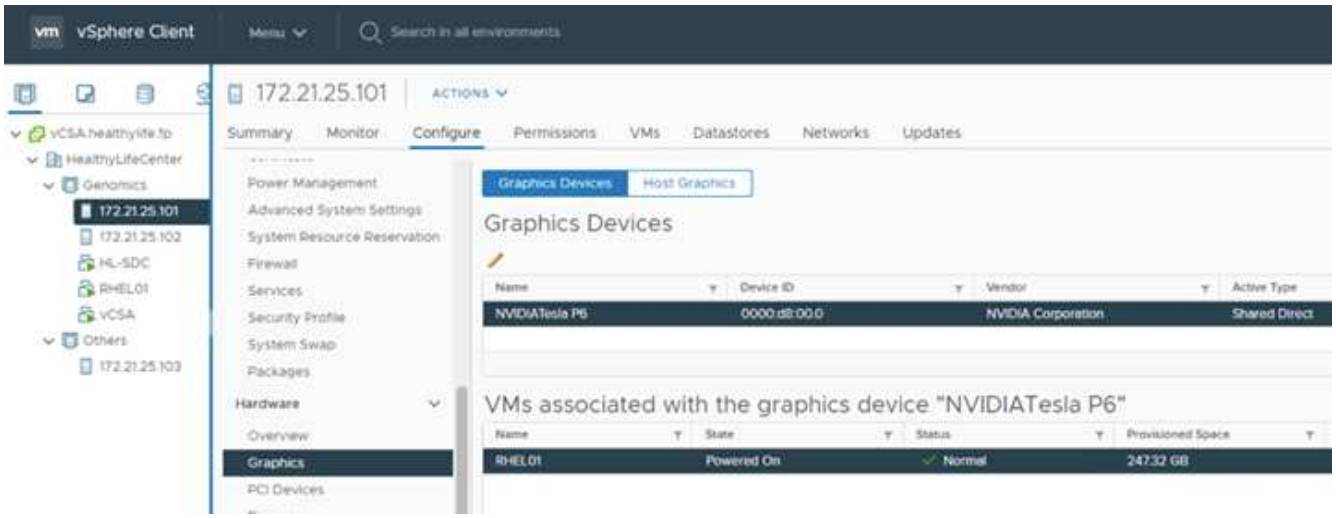
2. Wir haben uns für dieses Setup im NVIDIA Partner-Portal registriert und eine Evaluierungslizenz (auch als Berechtigung bekannt) erhalten, die GPUs im Compute-Modus verwenden kann.
3. Wir haben die erforderliche NVIDIA vGPU-Software von der NVIDIA-Partner-Website heruntergeladen.
4. Wir haben die Berechtigung heruntergeladen `*.bin` Datei von der NVIDIA-Partner-Website.
5. Wir installierten einen NVIDIA vGPU-Lizenzserver und fügten die Berechtigungen unter Verwendung von dem auf dem Lizenzserver hinzu `*.bin` Datei wird von der NVIDIA-Partnerwebsite heruntergeladen.
6. Stellen Sie sicher, dass Sie die richtige NVIDIA vGPU-Softwareversion für Ihre Implementierung im NVIDIA-Partnerportal auswählen. Für dieses Setup haben wir Treiberversion 460.73.02 verwendet.
7. Mit diesem Befehl wird der installiert "NVIDIA vGPU Manager" In ESXi.

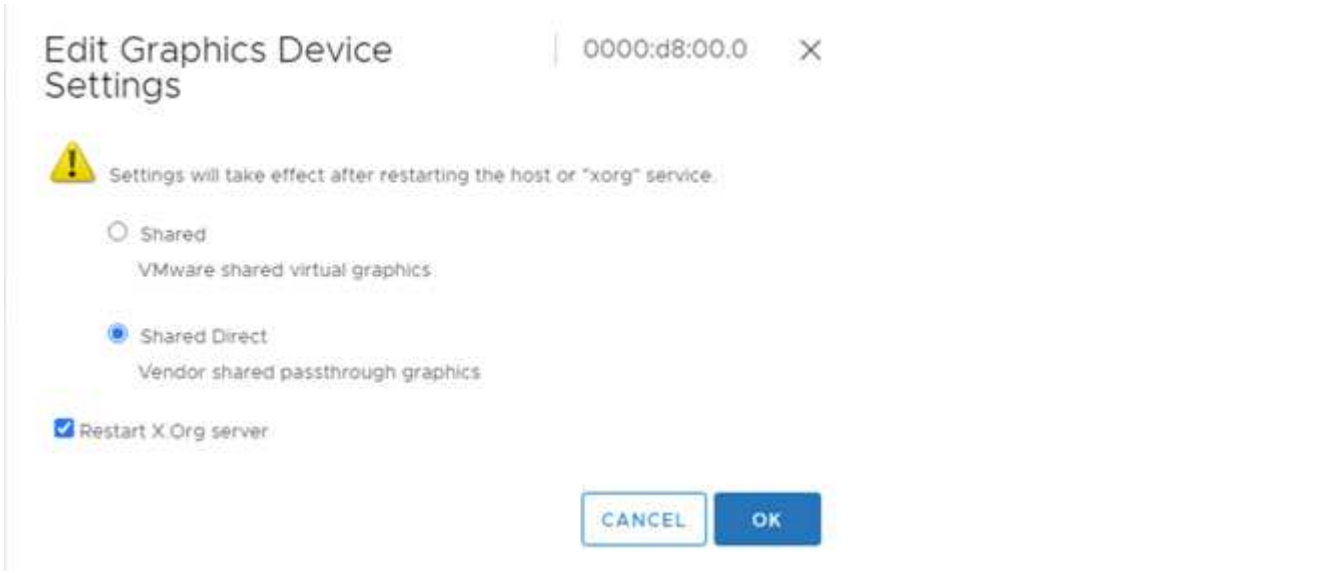
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. Führen Sie nach dem Neubooten des ESXi-Servers den folgenden Befehl aus, um die Installation zu validieren und den Zustand der GPUs zu überprüfen.

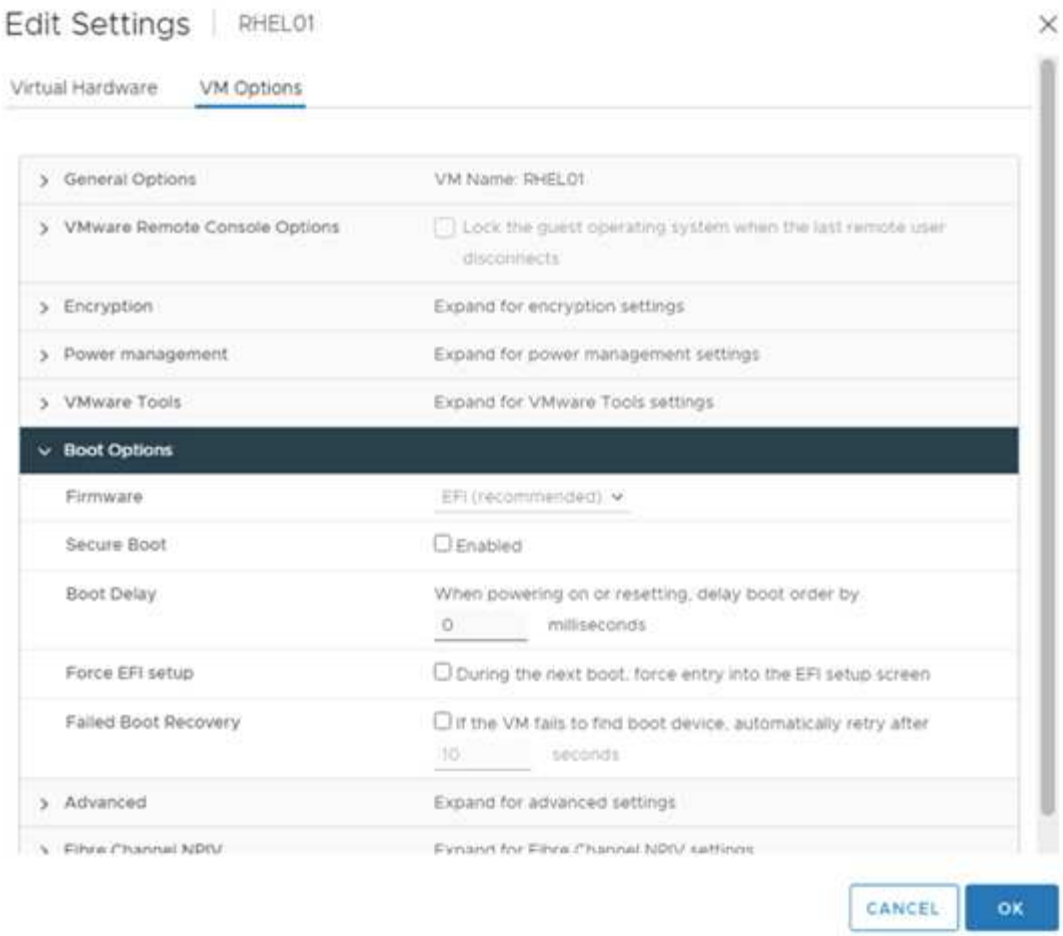
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. Mit vCenter "Konfigurieren" Die Einstellungen des Grafikgeräts auf „Shared Direct“.





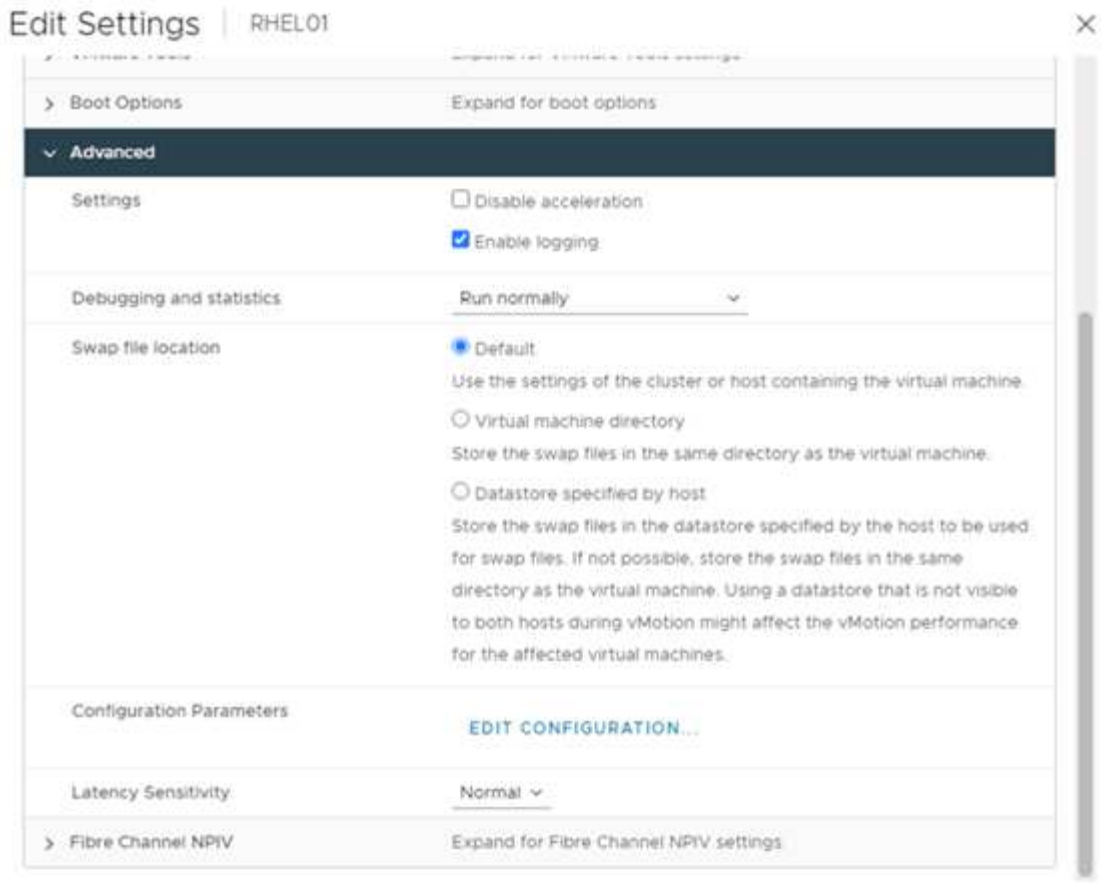
10. Vergewissern Sie sich, dass der sichere Boot für die RedHat-VM deaktiviert ist.
11. Stellen Sie sicher, dass die Firmware für VM-Startoptionen auf EFI (gesetzt ist "ref").

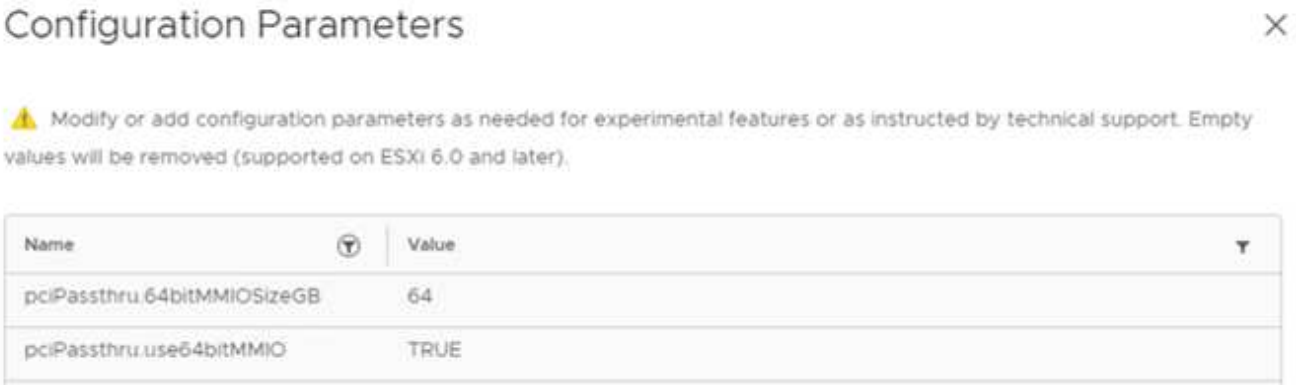


12. Stellen Sie sicher, dass die folgenden PARAMS zur erweiterten Konfiguration der VM-Optionen hinzugefügt werden. Der Wert des `pciPassthru.64bitMMIOSizeGB` Parameter hängt vom GPU-Speicher und der Anzahl der der der VM zugewiesenen GPUs ab. Beispiel:

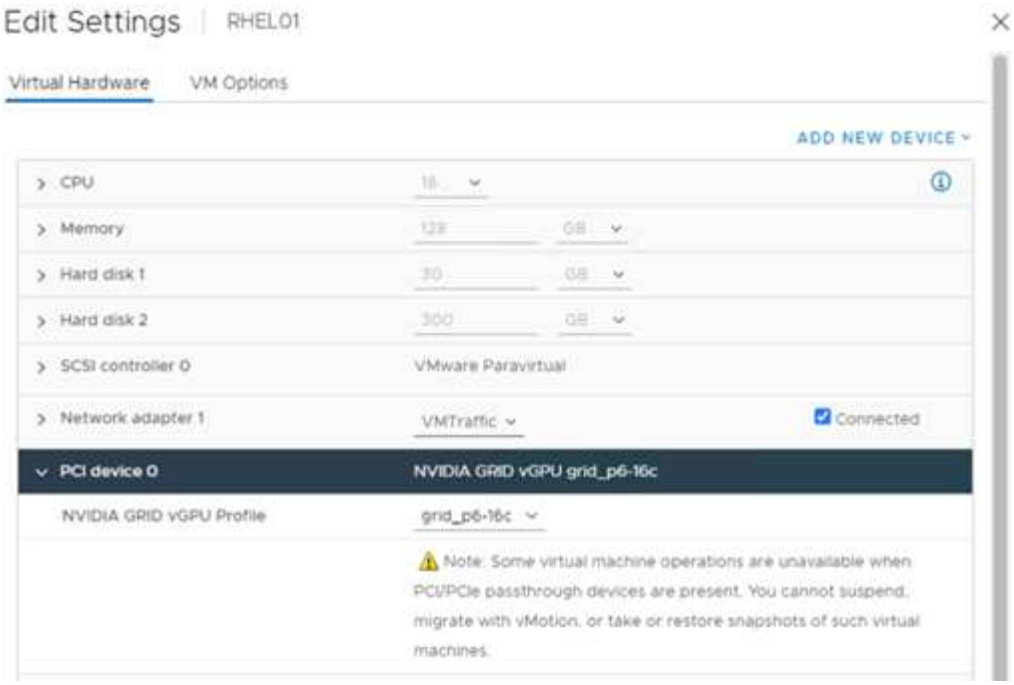
    a. Wenn einer VM 4 x 32-GB-V100-GPUs zugewiesen sind, sollte dieser Wert 128 sein.

    b. Wenn einer VM 4 x 16-GB-P6-GPUs zugewiesen sind, sollte dieser Wert 64 sein.





13. Wenn Sie der virtuellen Maschine in vCenter vGPUs als neues PCI-Gerät hinzufügen, stellen Sie sicher, dass Sie NVIDIA GRID vGPU als PCI-Gerätetyp auswählen.
14. Wählen Sie das richtige GPU-Profil aus, das die verwendete GPU, den GPU-Speicher und den Nutzungszweck anführt, z. B. Grafik oder Rechner.



15. Auf der RedHat Linux VM können NVIDIA-Treiber installiert werden, indem Sie den folgenden Befehl ausführen:

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. Überprüfen Sie, ob das richtige vGPU-Profil angegeben wird, indem Sie den folgenden Befehl ausführen:

```
[root@genomics1 genomics]# nvidia-smi –query-gpu=gpu_name
–format=csv,noheader –id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. Überprüfen Sie nach dem Neubooten, ob die richtigen NVIDIA vGPU-Versionen zusammen mit den Treiberversionen gemeldet werden.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. Stellen Sie sicher, dass die IP-Adresse des Lizenzservers auf der VM in der vGPU-Grid-Konfigurationsdatei konfiguriert ist.
    a. Kopieren Sie die Vorlage.

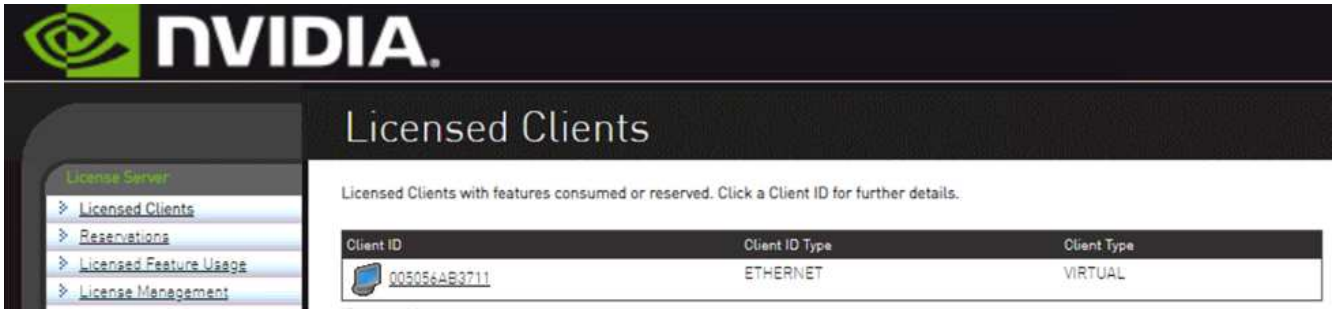
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. Bearbeiten Sie die Datei `/etc/nvidia/rid.conf`, Fügen Sie die IP-Adresse des Lizenzservers hinzu und setzen Sie den Funktionstyp auf 1.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. Nach dem Neustart der VM sollten Sie einen Eintrag unter lizenzierte Clients im Lizenzserver sehen, wie unten gezeigt.



20. Weitere Informationen zum Herunterladen der Software GATK und Cromwell finden Sie im Abschnitt Solutions Setup.
21. Nachdem GATK GPUs vor Ort, die Workflow-Beschreibungssprache, verwenden kann `*. wdl` Enthält die Laufzeitattribute wie unten dargestellt.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"Weiter: Fazit."

Schlussfolgerung

"Zurück: GPU-Setup."

Viele Gesundheitseinrichtungen auf der ganzen Welt haben FlexPod als gemeinsame Plattform standardisiert. Mit FlexPod können Sie Funktionen im Gesundheitswesen zuverlässig implementieren. FlexPod mit NetApp ONTAP wird standardmäßig mit der Möglichkeit geliefert, eine sofort einsatzbereite Reihe branchenführender Protokolle zu implementieren. Unabhängig vom Ursprung der Anforderung, Genomik eines Patienten zu betreiben, verfügen Interoperabilität, Zugänglichkeit, Verfügbarkeit und Skalierbarkeit

standardmäßig über eine FlexPod-Plattform. Wenn sie auf einer FlexPod-Plattform standardisiert ist, wird die Innovationskultur ansteckend.

Wo Sie weitere Informationen finden

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

- FlexPod Datacenter for AI/ML with Cisco UCS 480 ML for Deep Learning

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- FlexPod Datacenter with VMware vSphere 7.0 and NetApp ONTAP 9.7

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- ONTAP 9 Dokumentationszentrum

  "http://docs.netapp.com"

- Agil und effizient – wie FlexPod die Modernisierung des Datacenters fördert

  "https://www.flexpod.com/idc-white-paper/"

- KI im Gesundheitswesen

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod für das Gesundheitswesen vereinfachen den Wandel

  "https://flexpod.com/solutions/verticals/healthcare/"

- FlexPod von Cisco und NetApp

  "https://flexpod.com/"

- KI- und Analyselösungen für das Gesundheitswesen (NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- KI im Gesundheitswesen Intelligente Infrastrukturauswahlen führen zum Erfolg

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- FlexPod Datacenter with ONTAP 9.8, ONTAP Storage Connector for Cisco Intersight und Cisco Intersight Managed Mode.

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- FlexPod-Datacenter mit Red hat Enterprise Linux OpenStack Platform

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	November 2021	Erste Version.

FlexPod for MEDITECH Directional Sizing Guide

TR-4774: FlexPod for MEDITECH Directional Sizing

Brandon Agee, John Duignan, NetApp Mike Brennan, Jon Ebmeir, Cisco

In Zusammenarbeit mit: 

Dieser Bericht enthält Hinweise zur Größenbestimmung von FlexPod für eine MEDITECH EHR-Applikationsumgebung.

Zweck

FlexPod-Systeme können für das Hosting von MEDITECH EXPENSE, 6.x, 5.x und MAGIC Services bereitgestellt werden. FlexPod-Server, die die MEDITECH-Anwendungsschicht hosten, bieten eine integrierte Plattform für eine zuverlässige, leistungsstarke Infrastruktur. Die integrierte FlexPod Plattform wird schnell von qualifizierten FlexPod Channel Partnern implementiert und wird durch Technical Assistance Center von Cisco und NetApp unterstützt.

Die Größenbemessung basiert auf Informationen in MEDITECH's Hardware-Konfigurationsvorschlag und dem MEDITECH Task-Dokument. So wird die optimale Größe für Computing-, Netzwerk- und Storage-Infrastrukturkomponenten ermittelt.

Der "MEDITECH Workload – Übersicht" In diesem Abschnitt werden die Arten von Computing- und Speicher-Workloads beschrieben, die in MEDITECH-Umgebungen zu finden sind.

Der "Technische Spezifikationen für kleine, mittlere und große Architekturen" Abschnitt enthält eine Beispielrechnung der Materialien für die verschiedenen Storage-Architekturen, die im Abschnitt beschrieben werden. Die angegebenen Konfigurationen sind nur allgemeine Richtlinien. Dimensionierung der Systeme mit Dimensionierungstools immer abhängig vom Workload und passen die Konfigurationen entsprechend an.

Gesamtvorteile der Lösung

Das Auflaufen einer MEDITECH-Umgebung auf dem Architekturfundament von FlexPod kann Organisationen im Gesundheitswesen dabei helfen, die Produktivität zu steigern und ihre Kapital- und Betriebsausgaben zu senken. FlexPod bietet eine vorab validierte, umfassend getestete und konvergente Infrastruktur aus der strategischen Partnerschaft von Cisco und NetApp. Er wurde speziell für vorhersehbare System-Performance mit niedriger Latenz und Hochverfügbarkeit konzipiert. Dieser Ansatz führt zu schnelleren Reaktionszeiten für die Nutzer des MEDITECH EHR-Systems.

Die FlexPod Lösung von Cisco und NetApp erfüllt die MEDITECH-Systemanforderungen mit einem leistungsstarken, modularen, vorab validierten, konvergierten, virtualisierten Effiziente, skalierbare und kostengünstige Plattform: Ein Datacenter in FlexPod mit MEDITECH bietet verschiedene Vorteile, die speziell für das Gesundheitswesen entwickelt wurden:

- **Modulare Architektur**. FlexPod erfüllt die unterschiedlichen Anforderungen der modularen MEDITECH-Architektur mit individuell angepassten FlexPod-Systemen für jeden einzelnen Workload. Alle Komponenten sind über eine Clustered Server- und Storage-Managementstruktur verbunden und verwenden ein zusammenhängendes Management-Toolset.
- **Vereinfachter Betrieb und niedrigere Kosten**. Sie können die Kosten und die Komplexität älterer Plattformen eliminieren, indem Sie diese durch eine effizientere und skalierbarere Shared-Ressource ersetzen, die das Klinikpersonal überall unterstützen kann. Diese Lösung bietet eine bessere Ressourcenauslastung und damit einen höheren ROI.
- **Schnellere Implementierung der Infrastruktur**. Das integrierte Design des FlexPod Datacenter in Kombination mit MEDITECH sorgt dafür, dass die neue Infrastruktur für einen schnellen und einfachen Betrieb sowohl von Datacentern vor Ort als auch von externen Datacentern bereit ist.
- **Scale-out-Architektur**. Sie können SAN und NAS von Terabyte auf Petabyte im zweistelligen Bereich skalieren, ohne laufende Applikationen neu zu konfigurieren.
- **Unterbrechungsfreier Betrieb**. Sie können Storage-Wartungen, Hardware-Lebenszyklusoperationen und Software-Upgrades ohne Unterbrechung des Geschäftsbetriebs durchführen.
- **Sichere Mandantenfähigkeit**. Diese Vorteile unterstützen die gestiegenen Anforderungen an virtualisierte Server- und Shared Storage-Infrastrukturen und ermöglichen so eine sichere Mandantenfähigkeit für spezifische Informationen. Dieser Vorteil ist wichtig, wenn Sie mehrere Instanzen von Datenbanken und Software hosten.
- **Ressourcenoptimierung in Pools**. Dadurch können Sie die Anzahl physischer Server und Storage-Controller reduzieren, die Workload-Anforderungen ausgleichen, die Auslastung steigern und gleichzeitig die Performance verbessern.
- * Quality of Service (QoS).* FlexPod bietet Quality of Service (QoS) auf dem gesamten Stack. Branchenführende QoS-Storage-Richtlinien ermöglichen differenzierte Service-Level in einer Shared IT-Umgebung. Diese Richtlinien ermöglichen optimale Performance für Workloads und helfen, unkontrollierte Applikationen zu isolieren und zu kontrollieren.
- * Storage-Effizienz*. Mit der NetApp Storage-Effizienz von 7:1 senken Sie Ihre Storage-Kosten.
- **Agilität**. Mit den branchenführenden Workflow-Automatisierungs-, Orchestrierungs- und Management Tools von FlexPod Systemen KANN DIE IT wesentlich schneller auf geschäftliche Anforderungen reagieren. Diese Geschäftsanforderungen können von MEDITECH-Backups und Bereitstellungen von mehr Test- und Schulungsumgebungen bis zu Analytics-Datenbank-Replikationen für Population Health Management Initiativen reichen.
- * Produktivität*. Sie können die Lösung schnell implementieren und skalieren und damit für eine optimale Benutzererfahrung sorgen.
- * Data Fabric*. Die NetApp Data-Fabric-Architektur verknüpft Daten über Standorte, physische Grenzen und Applikationen hinweg. NetApp Data Fabric wurde für Unternehmen in einer datenorientierten Welt entwickelt. Daten werden an diversen Orten erstellt und verwendet und werden oft auch mit Applikationen und Infrastrukturen gemeinsam genutzt. Data Fabric ermöglicht konsistentes und integriertes Datenmanagement. Die IT hat darüber hinaus mehr Kontrolle über die Daten und vereinfacht die ständig zunehmende Komplexität IM IT-BEREICH.

Umfang

Dieses Dokument behandelt Umgebungen, in denen Cisco UCS und NetApp ONTAP Storage zum Einsatz kommen. Es bietet Beispiele für Referenzarchitekturen für das Hosting von MEDITECH.

Er deckt nicht ab:

- Detaillierte Anleitung zur Dimensionierung mit NetApp System Performance Modeler (SPM) oder anderen

NetApp Dimensionierungstools.

- Dimensionierung für nicht produktive Workloads.

Zielgruppe

Dieses Dokument richtet sich an Systems Engineers von NetApp und Partnern sowie an Mitarbeiter der NetApp Professional Services. NetApp geht davon aus, dass der Leser gute Kenntnisse der Konzepte zur Computing- und Storage-Größenbemessung sowie der technischen Vertrautheit mit Cisco UCS und NetApp Storage-Systemen hat.

Relevante Dokumente

Die folgenden technischen Berichte und sonstigen Dokumente sind für diesen technischen Bericht relevant und bilden eine komplette Reihe von Dokumenten, die für die Dimensionierung, Gestaltung und Bereitstellung von MEDITECH auf FlexPod-Infrastruktur erforderlich sind.

- "TR-4753: FlexPod-Datacenter for MEDITECH Deployment Guide"
- "TR-4190: NetApp Sizing Guidelines for MEDITECH Environments"
- "TR-4319: NetApp Deployment Guidelines for MEDITECH Environments"

Für den Zugriff auf einige dieser Berichte sind Anmeldeinformationen für das NetApp Field Portal erforderlich.

MEDITECH Workload – Übersicht

In diesem Abschnitt werden die Arten von Computing- und Speicher-Workloads beschrieben, die in MEDITECH-Umgebungen zu finden sind.

MEDITECH und Backup-Workloads

Wenn Sie NetApp Storage-Systeme für MEDITECH-Umgebungen dimensionieren, müssen Sie sowohl den MEDITECH-Produktions-Workload als auch den Backup-Workload in Betracht ziehen.

MEDITECH-Host
Ein MEDITECH-Host ist ein Datenbankserver. Dieser Host wird auch als MEDITECH-Dateiserver (für DIE EXPENSE, 6.x oder C/S 5.x-Plattform) oder ALS ZAUBERMASCHINE (für DIE MAGIC-Plattform) bezeichnet. Dieses Dokument verwendet den Begriff MEDITECH Host, um auf einen MEDITECH-Dateiserver und EINEN ZAUBERCOMPUTER zu verweisen.

In den folgenden Abschnitten werden die I/O-Merkmale und Performance-Anforderungen dieser beiden Workloads beschrieben.

MEDITECH-Workload

In einer MEDITECH-Umgebung führen mehrere Server, auf denen MEDITECH-Software ausgeführt wird, verschiedene Aufgaben als integriertes System, das als MEDITECH-System bekannt ist, aus. Weitere Informationen zum MEDITECH-System finden Sie in der MEDITECH-Dokumentation:

- In Produktionsumgebungen für MEDITECH-Umgebungen finden Sie die entsprechende MEDITECH-Dokumentation, um die Anzahl der MEDITECH-Hosts und die Speicherkapazität zu bestimmen, die im Rahmen der Größenanpassung des NetApp Storage-Systems enthalten sein muss.

- Informationen zu neuen MEDITECH-Umgebungen finden Sie im Dokument mit dem Vorschlag zur Hardwarekonfiguration. Informationen zu vorhandenen MEDITECH-Umgebungen finden Sie in dem Dokument für die Hardwarebewertung. Die Hardwarebewertungaufgabe ist ein MEDITECH Ticket zugeordnet. Kunden können eines dieser Dokumente von MEDITECH anfordern.

Sie können das MEDITECH-System skalieren, um eine erhöhte Kapazität und Leistung durch Hinzufügen von Hosts bereitzustellen. Jeder Host benötigt für seine Datenbank und Applikationsdateien Storage-Kapazität. Der für jeden MEDITECH-Host verfügbare Speicher muss auch die vom Host erzeugten I/O unterstützen. In einer MEDITECH-Umgebung ist für jeden Host eine LUN verfügbar, um die Datenbank- und Anwendungsspeicheranforderungen des Hosts zu unterstützen. Die Art der MEDITECH-Kategorie und die Art der Plattform, die Sie bereitstellen, bestimmt die Workload-Eigenschaften der einzelnen MEDITECH-Hosts und damit des gesamten Systems.

MEDITECH-Kategorien

MEDITECH ordnet die Bereitstellungsgröße einer Kategorienummer zwischen 1 und 6 zu. Kategorie 1 stellt die kleinsten MEDITECH-Bereitstellungen dar; die Kategorie 6 ist die größte. Beispiele für die MEDITECH-Anwendungsspezifikationen, die jeder Kategorie zugeordnet sind, sind Metriken wie z. B.:

- Anzahl der Krankenhausbetten
- Patienten pro Jahr
- Patienten pro Jahr
- Notaufnahme pro Jahr
- Prüfungen pro Jahr
- Patienten-Rezepte pro Tag
- Ambulante Rezepte pro Tag

Weitere Informationen zu den MEDITECH-Kategorien finden Sie im Referenzblatt zur MEDITECH-Kategorie. Sie können dieses Datenblatt von MEDITECH über den Kunden oder über den MEDITECH-Systeminstallateur beziehen.

MEDITECH-Plattformen

MEDITECH verfügt über vier Plattformen:

- EXPANSIV
- MEDITECH 6.x
- Client/Server 5.x (C/S 5.x)
- ZAUBERN KANN

Für die Plattformen MEDITECH EXPLISE, 6.x und C/S 5.x werden die I/O-Eigenschaften jedes Hosts als 100% zufällig mit einer Anfragegröße von 4,000 definiert. Für die MEDITECH MAGIC Platform werden die I/O-Eigenschaften jedes Hosts als 100% zufällig mit einer Anfragegröße von entweder 8,000 oder 16,000 definiert. Nach Angaben von MEDITECH beträgt die Anfragegröße für einen typischen MAGIC Production-Einsatz entweder 8,000 oder 16,000.

Das Verhältnis von Lese- und Schreibzugriffen hängt von der bereitgestellten Plattform ab. MEDITECH schätzt die durchschnittliche Mischung aus Lesen und Schreiben und drückt sie dann als Prozentsätze aus. MEDITECH schätzt außerdem den für jeden MEDITECH-Host erforderlichen durchschnittlichen, nachhaltigen IOPS-Wert auf einer bestimmten MEDITECH-Plattform. In der folgenden Tabelle sind die plattformspezifischen I/O-Eigenschaften von MEDITECH zusammengefasst.

MEDITECH-Kategorie	MEDITECH Platform	Durchschnittlicher Zufälliger Lesezugriff %	Durchschnittlicher Zufälliger Schreibvorgang %	Durchschnittliche kontinuierliche IOPS pro MEDITECH Host
1	EXPENSE, 6.x	20	80	750
2-6	EXPANSIV	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	ZAUBERN KANN	90	10	400

In einem MEDITECH-System muss die durchschnittliche IOPS-Stufe jedes Hosts den in der obigen Tabelle definierten IOPS-Werten entsprechen. Zur Ermittlung der richtigen Storage-Größenbemessung basierend auf jeder Plattform werden die in der obigen Tabelle angegebenen IOPS-Werte als Teil der in beschriebenen Dimensionierungsmethodik verwendet "Technische Spezifikationen für kleine, mittlere und große Architekturen" Abschnitt.

MEDITECH erfordert, dass die durchschnittliche zufällige Schreiblatenz unter 1 ms für jeden Host bleibt. Allerdings gelten temporäre Erhöhungen der Schreiblatenz auf 2 ms während Backup- und Neuzuweisung-Jobs als akzeptabel. MEDITECH erfordert auch die durchschnittliche Random-Read-Latenz, um unter 7 ms für Hosts der Kategorie 1 und unter 5 ms für Hosts der Kategorie 2 zu bleiben. Diese Latenzanforderungen gelten für jeden Host, unabhängig davon, welche MEDITECH-Plattform verwendet wird.

In der folgenden Tabelle sind die I/O-Merkmale aufgeführt, die Sie bei der Dimensionierung von NetApp Storage für MEDITECH-Workloads berücksichtigen müssen.

Parameter	MEDITECH-Kategorie	EXPANSIV	MEDITECH 6.x	C/S 5.x	ZAUBERN KANN
Anfragegröße	1-6	4 KB	4 KB	4 KB	8 KB oder 16.000
Zufällig/sequenziell		100 % zufällige Zugriffe	100 % zufällige Zugriffe	100 % zufällige Zugriffe	100 % zufällige Zugriffe
Kontinuierliche IOPS	1	750	750	K. A.	K. A.
	2-6	750	750	600	400
Lese-/Schreibverhältnis	1-6	20 % Lesen, 80 % Schreiben	20 % Lesen, 80 % Schreiben	40 % Lesen, 60 % Schreiben	90 % Lesen, 10 % Schreiben
Schreiblatenz		<1 ms	<1 ms	<1 ms	<1 ms
Temporäre Schreiblatenz mit Spitzenlasten	1-6	<2 ms	<2 ms	<2 ms	<2 ms
Leselatenz	1	<7 ms	<7 ms	K. A.	K. A.
	2-6	<5 ms	<5 ms	<5 ms	<5 ms

MEDITECH-Hosts in den Kategorien 3 bis 6 haben die gleichen I/O-Eigenschaften wie Kategorie 2. Für die MEDITECH-Kategorien 2 bis 6 unterscheidet sich die Anzahl der Hosts, die in jeder Kategorie eingesetzt werden.

Das NetApp Storage-System sollte gemäß den Performance-Anforderungen in den vorherigen Abschnitten beschrieben werden. Zusätzlich zu dem MEDITECH-Produktions-Workload muss das NetApp Storage-System in der Lage sein, die MEDITECH-Performance-Ziele während des Backup-Betriebs zu halten, wie im folgenden Abschnitt beschrieben.

Beschreibung Des Backup Workloads

MEDITECH zertifizierte Backup-Software sichert die von jedem MEDITECH-Host in einem MEDITECH-System verwendete LUN. Damit sich die Backups in einem applikationskonsistenten Zustand befinden, stellt die Backup-Software das MEDITECH-System still und stellt E/A-Anfragen auf die Festplatte aus. Während das System in einem stillgelegten Status ist, gibt die Backup-Software einen Befehl für das NetApp Storage-System aus, um eine NetApp Snapshot Kopie der Volumes zu erstellen, die die LUNs enthalten. Die Backup-Software stellt später das MEDITECH-System auf, wodurch Produktions-I/O-Anfragen weiter an die Datenbank laufen können. Die Software erstellt ein NetApp FlexClone Volume auf Grundlage der Snapshot Kopie. Dieses Volume wird von der Backup-Quelle verwendet, während I/O-Anfragen für die Produktion auf den übergeordneten Volumes fortgesetzt werden, die die LUNs hosten.

Der von der Backup Software generierte Workload stammt aus dem sequenziellen Lesen der LUNs in den FlexClone Volumes. Der Workload ist als 100 % sequenzieller Lese-Workload mit einer Anfragegröße von 64,000 definiert. Für den MEDITECH-Produktions-Workload besteht das Performance-Kriterium darin, die erforderlichen IOPS und die entsprechende Lese-/Schreib-Latenz beizubehalten. Bei dem Backup-Workload wird die Aufmerksamkeit jedoch auf den gesamten Datendurchsatz (Mbps) verlagert, der während des Backup-Vorgangs generiert wird. MEDITECH LUN-Backups müssen in einem achtstündigen Backup-Fenster erstellt werden. NetApp empfiehlt jedoch, die Datensicherung aller MEDITECH LUNs in höchstens sechs Stunden zu erstellen. Der Ziel, das Backup in weniger als sechs Stunden abzuschließen, können Ereignisse wie eine ungeplante Zunahme des MEDITECH-Workloads, Hintergrundvorgänge im NetApp ONTAP oder das Datenwachstum im Laufe der Zeit in den Griff bekommen. Bei jedem dieser Ereignisse kann es zu einer zusätzlichen Backup-Zeit kommen. Unabhängig von der Menge der gespeicherten Applikationsdaten erstellt die Backup-Software für jeden MEDITECH-Host ein vollständiges Backup der gesamten LUN auf Blockebene.

Berechnen Sie den sequentiellen Lesedurchsatz, der erforderlich ist, um die Sicherung in diesem Fenster als Funktion der anderen beteiligten Faktoren abzuschließen:

- Die gewünschte Backup-Dauer
- Die Anzahl der LUNs
- Die Größe jeder LUN, die gesichert werden soll

Zum Beispiel, in einer MEDITECH-Umgebung mit 50 Hosts, in der die LUN-Größe jedes Hosts 200GB ist, ist die LUN-Gesamtkapazität zum Sichern 10 TB.

Um 10 TB Daten in acht Stunden zu sichern, ist der folgende Durchsatz erforderlich:

- = (10 x 10^6)MB (8 x 3,600)s
- = 347,2 MB

Zur Berücksichtigung von ungeplanten Ereignissen wird jedoch ein konservatives Backup-Fenster von 5.5 Stunden ausgewählt, um Reserven jenseits der empfohlenen sechs Stunden zu bieten.

Um 10 TB Daten in acht Stunden zu sichern, ist der folgende Durchsatz erforderlich:

- = (10 x 10^6)MB (5.5 x 3,600)s
- = 500 MBit/Sek.

Bei einer Durchsatzrate von 500 MBit/Sek. kann das Backup innerhalb eines 5.5-Stunden-Zeitrahmens abgeschlossen werden, der innerhalb der Backup-Anforderung von 8 Stunden liegt.

Die folgende Tabelle bietet einen Überblick über die I/O-Merkmale des Backup-Workloads, der bei der Größe des Storage-Systems verwendet werden soll.

Parameter	Alle Plattformen
Anfragegröße	64 K
Zufällig/sequenziell	100 % sequenziell
Lese-/Schreibverhältnis	100 % Lesen
Durchschnittlicher Durchsatz	Abhängig von der Anzahl der MEDITECH-Hosts und der Größe der einzelnen LUNs: Datensicherung muss innerhalb von 8 Stunden abgeschlossen sein.
Erforderliche Backup-Dauer	8 Stunden

Cisco UCS Referenzarchitektur für MEDITECH

Die Architektur für MEDITECH ON FlexPod basiert auf Guidance von MEDITECH, Cisco und NetApp und auf Partnererfahrung in der Zusammenarbeit mit MEDITECH Kunden aller Größen. Die Architektur ist anpassungsfähig und wendet Best Practices für MEDITECH an, je nach Rechenzentrumsstrategie des Kunden: Ob klein oder groß, zentralisiert, verteilt oder mandantenfähig.

Bei der Bereitstellung von MEDITECH hat Cisco UCS-Referenzarchitekturen entwickelt, die sich direkt an die Best Practices von MEDITECH richten. Cisco UCS ist eine nahtlos integrierte Lösung für hohe Performance, hohe Verfügbarkeit, Zuverlässigkeit und Skalierbarkeit zur Unterstützung von Arztpraxen und Krankenhaussystemen mit mehreren tausend Betten.

Technische Spezifikationen für kleine, mittlere und große Architekturen

In diesem Abschnitt wird eine Beispielliste der Materialien für Storage-Architekturen unterschiedlicher Größe vorgestellt.

Stückliste für kleine, mittlere und große Architekturen

Das FlexPod Design ist eine flexible Infrastruktur, die viele verschiedene Komponenten und Softwareversionen umfasst. Nutzung "TR-4036: FlexPod Technische Spezifikationen" Als Leitfaden zur Montage einer gültigen FlexPod-Konfiguration. Die Konfigurationen in der folgenden Tabelle sind die Mindestanforderungen für FlexPod und sind nur ein Beispiel. Je nach Bedarf können die Konfigurationen für jede Produktfamilie in verschiedenen Umgebungen und Anwendungsfällen erweitert werden.

Für diese Größenbemessung entspricht klein einer MEDITECH-Umgebung der Kategorie 3, mittel bis Kategorie 5 und groß bis Kategorie 6.

	Klein	Mittel	Groß
Plattform	Ein NetApp AFF A220 HA-Paar für All-Flash-Storage-Systeme	Ein NetApp AFF A220 HA-Paar	Ein HA-Paar der NetApp AFF A300 All-Flash-Storage-Systeme
Platten-Shelfs	9 TB x 3,8 TB	13 TB x 3,8 TB	19 TB x 3,8 TB
Größe der MEDITECH-Datenbank	3 TB BIS 12 TB	17 TB	>30 TB
MEDITECH IOPS	<22,000 IOPS	>25,000 IOPS	>32,000 IOPS
IOPS insgesamt	22000	27000	35000
Raw	34,2 TB	44 TB	68,4 TB
Nutzbare Kapazität	18,53 tib	27,96 tib	33,8 2 tib
Effektive Kapazität (2:1 Storage-Effizienz)	55.6 tib	83,89 tib	101,47 tib

In einigen Kundenumgebungen können mehrere MEDITECH-Produktions-Workloads gleichzeitig ausgeführt werden oder es bestehen höhere IOPS-Anforderungen. In solchen Fällen sollte die Größe der Storage-Systeme zusammen mit dem NetApp Account Team den erforderlichen IOPS und die nötige Kapazität entsprechen. Sie sollten in der Lage sein, die richtige Plattform für die Workloads zu bestimmen. So betreiben Kunden beispielsweise erfolgreich mehrere MEDITECH-Umgebungen auf einem NetApp AFF A700 All-Flash-Storage-System HA-Paar.

Die folgende Tabelle zeigt die für MEDITECH-Konfigurationen erforderliche Standardsoftware.

Software	Produktfamilie	Version/Release	Details
Storage	ONTAP	Allgemeine Verfügbarkeit mit ONTAP 9.4 (GA)	
Netzwerk	Cisco UCS Fabric Interconnects	Cisco UCSM 4.x	Aktuelle empfohlene Version
	Cisco Nexus Ethernet Switches	7.0(3)I7(6)	Aktuelle empfohlene Version
	Cisco FC: Cisco MDS 9132T	8.3 (2)	Aktuelle empfohlene Version
Hypervisor	Hypervisor	VMware vSphere ESXi 6.7	
	Virtual Machines (VMs)	Windows 2016	
Vereinfachtes	Hypervisor-Managementsystem	VMware vCenter Server 6.7 U1 (VCSA)	
	NetApp Virtual Storage Console (VSC)	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4.0	
	Cisco UCS Manager	4.x	

Die folgende Tabelle zeigt eine kleine (Kategorie 3) Beispielkonfiguration – Infrastrukturkomponenten.

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108-Gehäuse	1	Unterstützt bis zu acht Blades mit halber oder vier Vollbreiten-Blades. Fügen Sie Gehäuse hinzu, wenn der Serverbedarf wächst.
	Cisco-Gehäuse-I/O-Module	2 x 2208	8 GB x 10-GB-Uplink-Ports
	Cisco UCS Blade Server	4 x B200 M5	Jeweils mit 2 x 14 Kernen, 2,6 GHz oder höhere Taktrate und 384 GB BIOS 3.2(3#)
	Cisco UCS Virtual Interface-Karten	4 x UCS 1440	VMware ESXi fNIC FC-Treiber: 1.6.0.47 VMware ESXi ELNIC Ethernet-Treiber: 1.0.27.0 (siehe Interoperabilitätsmatrix:
	2 Cisco UCS Fabric Interconnects (FI)	2x UCS 6454 FI	Fabric Interconnects der vierten Generation mit Unterstützung für 10/25 GB Ethernet und 32 GB FC
Netzwerk	Cisco Ethernet Switches	2 x Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB, 100 GB
Datennetzwerk Storage-Netzwerk	IP Network Nexus 9k für BLOB Storage		FI- und UCS-Gehäuse
	FC – CISCO MDS 9132T		Zwei Cisco 9132T-Switches
Storage	NetApp AFF A300 All-Flash-Storage-System	1 HA-Paar	2-Node-Cluster für alle MEDITECH-Workloads (File Server, Image Server, SQL Server, VMware usw.)
	DS224C Festplatten-Shelf	1 DS224C Festplatten-Shelf	
	Solid State Drive (SSD)	9 x 3,8 TB	

Die folgende Tabelle zeigt eine mittlere (Kategorie 5) Beispielkonfiguration – Infrastrukturkomponenten

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1	Unterstützt bis zu acht Blades mit halber oder vier Vollbreiten-Blades. Fügen Sie Gehäuse hinzu, wenn der Serverbedarf wächst.
	Cisco-Gehäuse-I/O-Module	2 x 2208	8 GB x 10-GB-Uplink-Ports
	Cisco UCS Blade Server	6 x B200 M5	Jeweils mit 2 x 16 Kernen, 2,5 GHz/oder höherer Taktfrequenz und 384 GB oder mehr Speicher-BIOS 3.2 (3#)
	Virtuelle Cisco UCS Schnittstellenkarte (VIC)	6 UCS 1440 VIC	VMware ESXi fNIC FC driver: 1.6.0.47 VMware ESXi ELNIC Ethernet driver: 1.0.27.0 (siehe Interoperabilitäts-Matrix:)
	2 Cisco UCS Fabric Interconnects (FI)	2x UCS 6454 FI	Fabric Interconnects der vierten Generation mit Unterstützung für 10 GB/25 GB/100 GB Ethernet und 32 GB FC
Netzwerk	Cisco Ethernet Switches	2 x Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB, 100 GB
Datennetzwerk Storage-Netzwerk	IP Network Nexus 9k für BLOB Storage		
	FC – CISCO MDS 9132T		Zwei Cisco 9132T-Switches
Storage	NetApp AFF A220 All-Flash-Storage-System	2 HA-Paar	2-Node-Cluster für alle MEDITECH-Workloads (File Server, Image Server, SQL Server, VMware usw.)
	DS224C Festplatten-Shelf	1 x DS224C Festplatten-Shelf	
	SSD	13 x 3,8 TB	

Die folgende Tabelle zeigt eine große (Kategorie 6) Beispielkonfiguration – Infrastrukturkomponenten.

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1	
	Cisco-Gehäuse-I/O-Module	2 x 2208	8 x 10-GB-Uplink-Ports
	Cisco UCS Blade Server	8 x B200 M5	Jeweils mit 2 x 24 Cores, 2,7 GHz und 768 GB BIOS 3.2 (3#)
	Virtuelle Cisco UCS Schnittstellenkarte (VIC)	8 UCS 1440 VIC	VMware ESXi fNIC FC driver: 1.6.0.47 VMware ESXi ELNIC Ethernet Treiber: 1.0.27.0 (Interoperabilitätsmatrix überprüfen:
	2 Cisco UCS Fabric Interconnects (FI)	2x UCS 6454 FI	Fabric Interconnects der vierten Generation mit Unterstützung für 10 GB/25 GB/100 GB Ethernet und 32 GB FC
Netzwerk	Cisco Ethernet Switches	2 x Nexus 9336c-FX2	2 x Cisco Nexus 9332PQ1, 10 GB, 25 GB, 40 GB, 100 GB
Datennetzwerk Storage-Netzwerk	IP Network N9k für BLOB Storage		
	FC – CISCO MDS 9132T		Zwei Cisco 9132T-Switches
Storage	AFF A300	1 HA-Paar	2-Node-Cluster für alle MEDITECH-Workloads (File Server, Image Server, SQL Server, VMware usw.)
	DS224C Festplatten-Shelf	1 x DS224C Festplatten-Shelfs	
	SSD	19 x 3,8 TB	

Diese Konfigurationen bieten einen Ausgangspunkt für Hinweise zum Sizing. In einigen Kundenumgebungen können mehrere MEDITECH-Produktions- und nicht-MEDITECH-Workloads gleichzeitig ausgeführt werden, oder es kann zu höheren IOP-Anforderungen kommen. Legen Sie gemeinsam mit dem NetApp Account Team die Größe der Storage-Systeme basierend auf den erforderlichen IOPS, Workloads und Kapazität fest, um die richtige Plattform für die Workloads zu ermitteln.

Weitere Informationen

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

- FlexPod Datacenter mit FC Cisco Validated Design

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- NetApp Deployment Guidelines für MEDITECH-Umgebungen.

  "https://fieldportal.netapp.com/content/248456" (NetApp Login erforderlich)

- NetApp Sizing Guidelines für MEDITECH-Umgebungen.

  "www.netapp.com/us/media/tr-4190.pdf"

- Implementierung von FlexPod Datacenter für Epic EHR

  "www.netapp.com/us/media/tr-4693.pdf"

- FlexPod-Designzone

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

- FlexPod DC mit FC Storage (MDS Switches) mit NetApp AFF, vSphere 6.5U1 und Cisco UCS Manager

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco Gesundheitswesen

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

Danksagungen

Die folgenden Personen haben zur Erstellung und Erstellung dieses Leitfadens beigetragen.

- Brandon Agee, Technical Marketing Engineer, NetApp
- John Duignan, Solutions Architect, Gesundheitswesen, NetApp
- Ketan Mota, Product Manager, NetApp
- Jon Ebmeier, Technical Solutions Architect, Cisco Systems, Inc
- Mike Brennan, Product Manager, Cisco Systems, Inc

Bereitstellungsleitfaden für das FlexPod-Rechenzentrum für MEDITECH

TR-4753: FlexPod-Datacenter for MEDITECH Deployment Guide

Brandon Agee und John Duignan, NetApp Mike Brennan und Jon Ebmeier, Cisco

In Zusammenarbeit mit: 

Gesamtvorteile der Lösung

Durch den Aufbau einer MEDITECH-Umgebung auf dem Architekturfundament von FlexPod kann Ihr Gesundheitsunternehmen eine Verbesserung der Mitarbeiterproduktivität und eine Verringerung der Investitions- und Betriebskosten erwarten. Das FlexPod Datacenter für MEDITECH bietet verschiedene für das Gesundheitswesen spezifische Vorteile:

- **Vereinfachter Betrieb und geringere Kosten.** Kosten und Komplexität älterer Plattformen werden eliminiert, indem sie durch effizientere und skalierbarere gemeinsame Ressourcen ersetzt werden, die das Klinikpersonal überall unterstützen können. Diese Lösung bietet eine höhere Ressourcenauslastung und damit einen höheren ROI.
- * Schnellere Bereitstellung der Infrastruktur.* ob bereits ein Rechenzentrum oder ein Remote-Standort, mit dem integrierten und getesteten Design von FlexPod Datacenter können Sie Ihre neue Infrastruktur mit weniger Aufwand in kürzerer Zeit einsatzbereit haben.
- **Zertifizierter Storage.** NetApp ONTAP Datenmanagement-Software mit MEDITECH bietet Ihnen die überlegene Zuverlässigkeit eines getesteten und zertifizierten Storage-Anbieters. MEDITECH zertifiziert keine anderen Infrastrukturkomponenten.
- **Scale-out-Architektur** SAN und NAS von Terabyte (TB) auf Petabyte im zweistelligen Bereich (PB) skalieren, ohne laufende Applikationen neu zu konfigurieren.
- **Unterbrechungsfreier Betrieb.** Durchführung von Storage-Wartungen, Hardware-Lebenszyklusoperationen und FlexPod Upgrades ohne Unterbrechung des Geschäftsbetriebs
- **Sichere Mandantenfähigkeit.** Unterstützung der gestiegenen Anforderungen an eine virtualisierte Shared IT-Infrastruktur für Server und Storage, die eine sichere Mandantenfähigkeit von kundenspezifischen Informationen ermöglicht, insbesondere wenn Ihr System mehrere Instanzen von Datenbanken und Software hostet.
- **Ressourcenoptimierung in Pools** Reduzierung der Anzahl physischer Server und Storage Controller, Load-Balancing der Workload-Anforderungen, Steigerung der Auslastung bei gleichzeitiger Performance-Verbesserung
- * Quality of Service (QoS).* FlexPod bietet QoS auf dem gesamten Stack. Branchenführende QoS-Netzwerk-, Computing- und Storage-Richtlinien ermöglichen differenzierte Service-Level in einer gemeinsam genutzten Umgebung. Diese Richtlinien ermöglichen optimale Performance für Workloads und helfen, unkontrollierte Applikationen zu isolieren und zu kontrollieren.
- **Storage-Effizienz.** Senken Sie die Storage-Kosten mit dem "NetApp „7:1 Storage-Effizienz“-Garantie".
- **Agilität.** mit den branchenführenden Tools für Workflow-Automatisierung, Orchestrierung und Management von FlexPod Systemen kann Ihr IT-Team viel schneller auf geschäftliche Anforderungen reagieren. Diese Geschäftsanforderungen können von MEDITECH-Backups und Bereitstellungen von mehr Test- und Schulungsumgebungen bis zu Analysedatenbanken-Replikationen für Population Health Management-Initiativen reichen.
- * Höhere Produktivität.* Schnelle Bereitstellung und Skalierung dieser Lösung für ein optimales Anwendererlebnis im Klinikpersonal.
- **NetApp Data Fabric.** mit der NetApp Data-Fabric-Architektur werden Daten über Standorte, physische Grenzen und Applikationen hinweg zusammengeführt. NetApp Data Fabric wurde für Unternehmen in einer datenorientierten Welt entwickelt. Daten werden an diversen Orten erstellt und verwendet. Häufig sind eine Nutzung und die gemeinsame Nutzung an anderen Orten, Applikationen und Infrastrukturen

erforderlich. Daher benötigen Sie eine Möglichkeit, Ihre Daten konsistent und integriert zu managen. Die Data-Fabric-Strategie bietet ein Datenmanagement, mit dem DIE IT-ABTEILUNGEN die Kontrolle behalten. Gleichzeitig wird die ständig zunehmende Komplexität IM IT-BEREICH verringert.

FlexPod

Neuer Infrastrukturansatz für MEDITECH EHRs

Gesundheitsdienstleister Unternehmen wie Ihres stehen unter Druck, um die Vorteile umfangreicher Investitionen in branchenführende elektronische Gesundheitsdaten (EHRs) von MEDITECH optimal zu nutzen. Wenn Unternehmen ihre Rechenzentren für MEDITECH-Lösungen entwerfen, werden für geschäftskritische Anwendungen häufig die folgenden Ziele für ihre Datacenter-Architektur identifiziert:

- Hohe Verfügbarkeit der MEDITECH-Anwendungen
- Hohe Performance
- Einfache Implementierung von MEDITECH im Rechenzentrum
- Agilität und Skalierbarkeit, um mit neuen MEDITECH-Veröffentlichungen oder -Anwendungen Wachstum zu ermöglichen
- Auch die Wirtschaftlichkeit kann sich sehen
- Abstimmung mit MEDITECH Guidance und Zielplattformen
- Managebarkeit, Stabilität und einfache Support-Bedienung
- Robuste Datensicherung, Backup, Recovery und Business Continuance

Da MEDITECH-Anwender ihre Unternehmen weiterentwickeln, um zu Rechenschaftspflicht für Versorgungsunternehmen zu werden und sich an gestrafft zusammengeschilfte Kostenerstattungs-Modelle anzupassen, stellt die Herausforderung die erforderliche MEDITECH-Infrastruktur in einem effizienteren und agileren IT-Bereitstellungsmodell bereit.

Der Wert vorab validierter konvergenter Infrastrukturen

Aufgrund der übergreifenden Anforderung, eine vorhersehbare Performance des Systems mit geringer Latenz und eine hohe Verfügbarkeit zu gewährleisten, ist MEDITECH den Hardwareanforderungen seiner Kunden entsprechend präskriptiv.

FlexPod ist eine vorab validierte und umfassend getestete konvergente Infrastruktur aus der strategischen Partnerschaft von Cisco und NetApp. Sie wurde speziell für vorhersehbare System-Performance mit niedriger Latenz und Hochverfügbarkeit konzipiert. Dieser Ansatz führt zu MEDITECH-Compliance und schließlich zu einer optimalen Reaktionszeit für die Nutzer des MEDITECH-Systems.

Die FlexPod Lösung von Cisco und NetApp erfüllt die MEDITECH-Systemanforderungen mit einem leistungsstarken, modularen, vorab validierten, konvergenten, virtualisierten Effiziente, skalierbare und kostengünstige Plattform: Es bietet Folgendes:

- **Modulare Architektur.** FlexPod erfüllt die vielfältigen Anforderungen der modularen MEDITECH-Architektur mit speziell konfigurierten FlexPod-Plattformen für jeden spezifischen Workload. Alle Komponenten sind über einen Cluster-Server und eine Storage-Management-Fabric und ein zusammenhängendes Management-Toolset verbunden.
- **Branchenführende Technologie auf jeder Ebene des konvergenten Stacks.** Cisco, NetApp, VMware und Microsoft Windows zählen alle von Branchenanalysten in den jeweiligen Kategorien mit Servern, Netzwerk, Storage und Betriebssystemen auf Platz 1 oder Nummer 2.
- **Investitionsschutz mit standardisierter, flexibler IT.** die FlexPod-Referenzarchitektur erwartet neue

Produktversionen und Updates mit rigorosen, kontinuierlichen Interoperabilitätstests, die zukünftige Technologien berücksichtigen, sobald sie verfügbar werden.

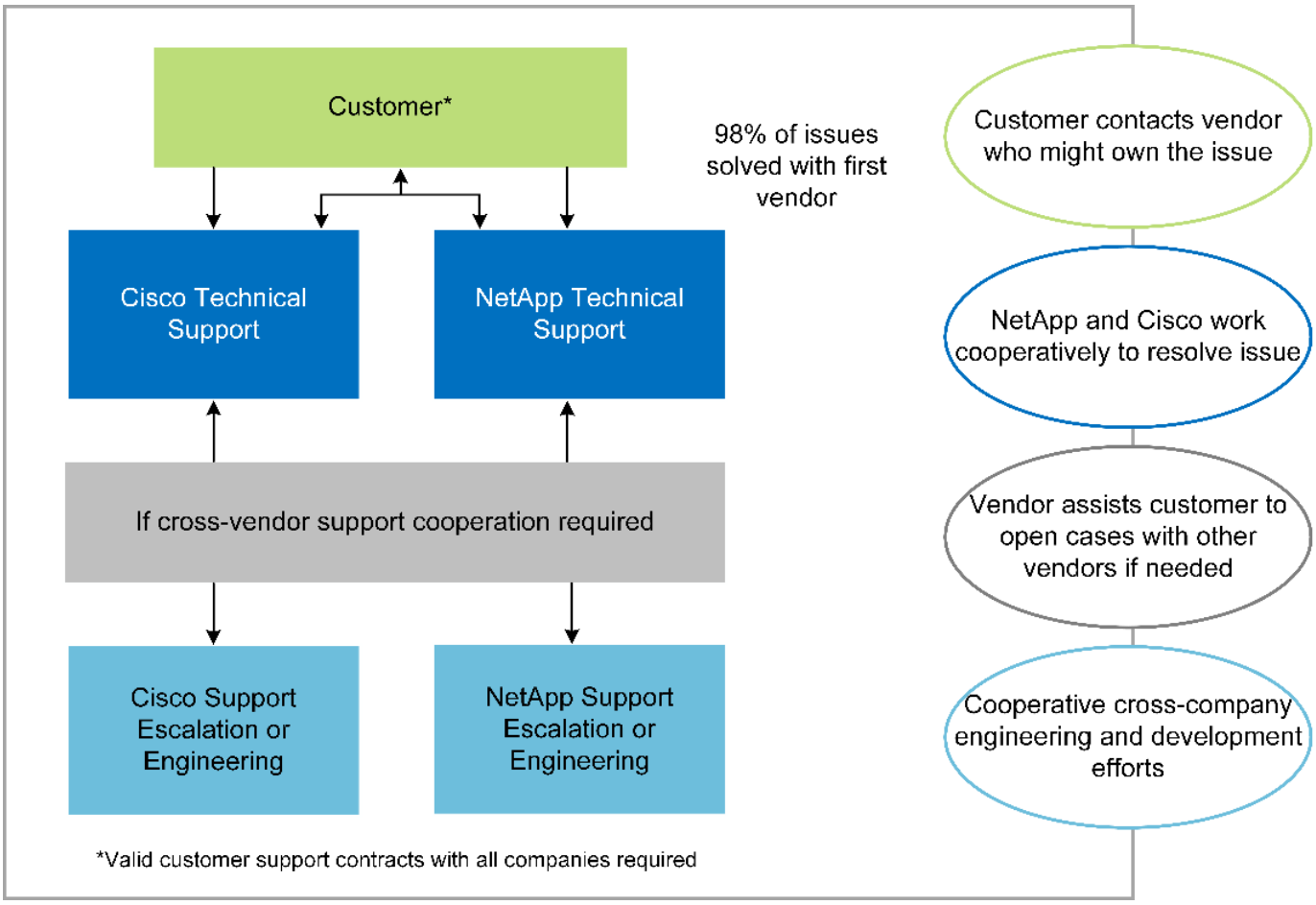
- **Bewährte Bereitstellung in einer Vielzahl von Umgebungen.** getestet und gemeinsam mit gängigen Hypervisoren, Betriebssystemen, Anwendungen und Infrastruktursoftware validiert, wurde FlexPod in mehreren MEDITECH-Kundenorganisationen installiert.

Bewährte FlexPod Architektur und kooperativer Support

FlexPod ist eine bewährte Datacenter-Lösung mit einer flexiblen Shared IT-Infrastruktur, die einfach skalierbar ist und sich so für wachsende Workload-Anforderungen skalieren lässt, ohne die Performance zu beeinträchtigen. Durch die Nutzung der FlexPod Architektur bietet diese Lösung alle Vorteile von FlexPod, u. a.:

- **Leistung zur Erfüllung der MEDITECH-Workload-Anforderungen.** je nach Anforderung Ihrer MEDITECH-Hardware-Konfiguration können verschiedene ONTAP-Plattformen implementiert werden, um die erforderlichen I/O- und Latenzanforderungen zu erfüllen.
- **Skalierbarkeit zur einfachen Bewältigung des wachsenden klinischen Datenvolumens.** Virtuelle Maschinen (VMs), Server und Storage-Kapazitäten lassen sich dynamisch nach Bedarf und ohne herkömmliche Einschränkungen skalieren.
- **Höhere Effizienz.** verringern Sie die Administrationszeit und die TCO mit einer konvergenten virtualisierten Infrastruktur, die leichter zu managen ist und die Daten effizienter speichert und gleichzeitig die Leistung der MEDITECH-Software steigert.
- **Geringeres Risiko** Minimieren Sie Geschäftsunterbrechungen mit einer vorab validierten Plattform, die auf einer definierten Architektur basiert, die Unsicherheiten bei Implementierungen beseitigt und sich an eine fortlaufende Optimierung der Workloads anpassen lässt.
- **Kooperativer Support für FlexPod** NetApp und Cisco haben ein solides, skalierbares und flexibles Support-Modell entwickelt, das die individuellen Support-Anforderungen der konvergenten FlexPod Infrastruktur erfüllt. Bei diesem Modell profitieren Kunden von der gebündelten Erfahrung, den gemeinsamen Ressourcen und dem Fachwissen des technischen Supports von NetApp und Cisco, um unabhängig von ihrem Speicherort des Problems Ihren FlexPod Support zu ermitteln und zu beheben. Das kooperative Supportmodell für FlexPod sorgt für einen effizienten Betrieb des FlexPod Systems und die Nutzung aktueller Technologien. Außerdem unterstützt Sie das Team mit einem erfahrenen Team bei der Behebung von Integrationsproblemen.

  Das kooperative Support-Modell für FlexPod eignet sich besonders für Einrichtungen im Gesundheitswesen, die geschäftskritische Applikationen wie MEDITECH auf der konvergenten FlexPod Infrastruktur ausführen. Die folgende Abbildung zeigt das kooperative Support-Modell für FlexPod.



Neben diesen Vorteilen bietet jede Komponente des FlexPod-Datacenter-Stacks mit MEDITECH-Lösung spezifische Vorteile für MEDITECH EHR-Workflows.

Cisco Unified Computing System

Das Cisco Unified Computing System (Cisco UCS) besteht aus einer zentralen Management-Domäne, die mit einer einheitlichen I/O-Infrastruktur verbunden ist. Damit die Infrastruktur kritische Patientendaten mit maximaler Verfügbarkeit liefern kann, wurde das Cisco UCS für MEDITECH-Umgebungen auf die von MEDITECH empfohlenen Infrastrukturempfehlungen und Best Practices abgestimmt.

Die Grundlage von MEDITECH auf der Cisco UCS-Architektur ist die Cisco UCS-Technologie mit integriertem Systemmanagement, Intel Xeon Prozessoren und Servervirtualisierung. Diese integrierten Technologien lösen die Herausforderungen von Datacentern und helfen Ihnen, Ihre Ziele für das Design von Rechenzentren für MEDITECH zu erreichen. Cisco UCS vereint das LAN-, SAN- und Systemmanagement in einem einzigen vereinfachten Link für Rack Server, Blade Server und VMs. Cisco UCS ist eine End-to-End-I/O-Architektur, in der Cisco Unified Fabric und Cisco Fabric Extender Technologie (FEX Technologie) integriert sind, um alle Komponenten des Cisco UCS über eine einzelne Network Fabric und eine einzelne Netzwerkebene zu verbinden.

Das System kann als einzelne oder mehrere logische Einheiten implementiert werden, die mehrere Blade-Chassis, Rack-Server, Racks und Datacenter integrieren und skalieren. Das System implementiert eine radikal vereinfachte Architektur, sodass keine redundanten Geräte mehr vorhanden sind, die herkömmliche Blade Server-Gehäuse und Rack-Server befüllen. In herkömmlichen Systemen führen redundante Geräte wie Ethernet- und FC-Adapter und Chassis-Management-Module zu einer komplexeren Umgebung. Cisco UCS besteht aus einem redundanten Paar Cisco UCS Fabric Interconnects (FIS), die einen einzigen Managementpunkt und einen einzigen Kontrollpunkt für den gesamten I/O-Datenverkehr bereitstellen.

Cisco UCS nutzt Serviceprofile, um sicherzustellen, dass die virtuellen Server in der Cisco UCS Infrastruktur ordnungsgemäß konfiguriert sind. Service-Profile bestehen aus Netzwerk-, Storage- und Computing-Richtlinien, die jeweils von Experten erstellt werden. Serviceprofile umfassen wichtige Serverinformationen über die Serveridentität wie LAN- und SAN-Adressierung, I/O-Konfigurationen, Firmware-Versionen, Boot Order, Network Virtual LAN (VLAN), physischen Port und QoS-Richtlinien. Service-Profile lassen sich dynamisch erstellen und sind in wenigen Minuten mit beliebigen physischen Servern im System verbunden – statt in Stunden oder Tagen. Die Zuordnung von Serviceprofilen zu physischen Servern erfolgt in einem einfachen, einzigen Vorgang und ermöglicht die Migration von Identitäten zwischen Servern in der Umgebung, ohne dass eine physische Konfiguration geändert werden muss. Sie ermöglicht die schnelle Bare Metal-Bereitstellung von Ersatzteilen für Altserver.

Durch die Verwendung von Service-Profilen kann sichergestellt werden, dass Server im gesamten Unternehmen konsistent konfiguriert werden. Wenn mehrere Cisco UCS Management-Domänen verwendet werden, kann Cisco UCS Central mithilfe globaler Serviceprofile Konfigurations- und Richtlinieninformationen über Domänen hinweg synchronisieren. Falls in einer Domäne Wartungsarbeiten durchgeführt werden müssen, kann die virtuelle Infrastruktur in eine andere Domäne migriert werden. Durch diesen Ansatz wird sichergestellt, dass selbst wenn eine einzelne Domäne offline ist, die Applikationen weiterhin mit hoher Verfügbarkeit ausgeführt werden.

Um zu zeigen, dass die Serverkonfigurationsanforderungen erfüllt werden, wurde Cisco UCS über einen Zeitraum von mehreren Jahren umfassend mit MEDITECH getestet. Cisco UCS ist eine unterstützte Serverplattform, die auf der MEDITECH Product Resources System Support-Website aufgeführt ist.

Cisco Networking

Cisco Nexus Switches und Cisco MDS Multilayer Directors bieten Konnektivität der Enterprise-Klasse sowie SAN-Konsolidierung. Die Multi-Protokoll-Speichernetzwerke von Cisco reduzieren das Geschäftsrisiko durch Flexibilität und Optionen: FC, Fibre Connection (FICON), FC over Ethernet (FCoE), SCSI over IP (iSCSI) und FC over IP (FCIP).

Cisco Nexus Switches bieten eines der umfangreichsten Datacenter-Netzwerk-Funktionen auf einer einzigen Plattform. Sie bieten hohe Performance und Dichte für Datacenter und Campus-Kerne. Zudem bieten sie umfassende Funktionen für Datacenter-Aggregation, End-of-row und Datacenter Interconnect-Implementierungen in einer äußerst stabilen modularen Plattform.

Das Cisco UCS integriert Rechenressourcen in Cisco Nexus Switches und eine Unified I/O Fabric, die verschiedene Arten von Netzwerkverkehr identifiziert und unterstützt. Der Datenverkehr umfasst Storage-I/O, Desktop-Datenströme, Management und Zugriff auf klinische und geschäftliche Applikationen. Sie erhalten:

- **Skalierbarkeit der Infrastruktur** Virtualisierung, effiziente Stromversorgung und Kühlung, Cloud-Skalierbarkeit mit Automatisierung, hoher Dichte und hoher Performance unterstützen effizientes Datacenter-Wachstum.
- **Betriebliche Kontinuität.** das Design integriert Hardware, NX-OS-Softwarefunktionen und Management, um Umgebungen ohne Ausfallzeiten zu unterstützen.
- **Netzwerk- und Computer-QoS.** Cisco bietet eine richtlinienbasierte Serviceklasse (CoS) und QoS für die gesamte Netzwerk-, Storage- und Computing-Fabric-Infrastruktur und sorgt damit für eine optimale Performance geschäftskritischer Applikationen.
- **Transportflexibilität.** Neue Netzwerktechnologien mit einer kostengünstigen Lösung schrittweise einführen.

Gemeinsam bieten Cisco UCS mit Cisco Nexus Switches und Cisco MDS Multilayer Directors eine optimale Computing-, Netzwerk- und SAN-Konnektivitätslösung für MEDITECH.

NetApp ONTAP

Auf NetApp Storage mit ONTAP Software fallen die Storage-Gesamtkosten geringer aus, während die Lese- und Schreibreaktionszeiten mit niedriger Latenz und die für MEDITECH-Workloads erforderlichen IOPS-Werte erreicht werden. ONTAP unterstützt sowohl All-Flash- als auch Hybrid-Storage-Konfigurationen und stellt damit eine optimale Storage-Plattform bereit, die die Anforderungen von MEDITECH erfüllt. Die Systeme mit Flash-Beschleunigung von NetApp haben die Validierung und Zertifizierung von MEDITECH erhalten, wodurch Unternehmen als MEDITECH-Kunde die Performance und Reaktionsfähigkeit eines wichtigen Systems für latenzempfindliche MEDITECH-Prozesse nutzen. Durch die Erstellung mehrerer Fehlerdomänen in einem einzigen Cluster können NetApp Systeme auch die Produktion von der nicht für die Produktion verwendeten Lösung isolieren. NetApp Systeme reduzieren mit ONTAP-QoS auch Performance-Probleme durch ein garantierte Minimum an Performance für Workloads.

Die Scale-out-Architektur der ONTAP Software kann flexibel an verschiedene I/O-Workloads angepasst werden. Um den erforderlichen Durchsatz und die niedrige Latenz zu erzielen, die klinische Applikationen erfordern, und gleichzeitig eine modulare Scale-out-Architektur bieten zu können, kommen meist All-Flash-Konfigurationen in ONTAP-Architekturen zum Einsatz. NetApp AFF Nodes können in demselben horizontal skalierbaren Cluster mit hybriden (HDD und Flash) Storage Nodes kombiniert werden, die sich zur Speicherung großer Datensätze mit hohem Durchsatz eignen. Neben einer von MEDITECH genehmigten Backup-Lösung können Sie Ihre MEDITECH-Umgebung aus teurem SSD-Storage (Solid-State Drive) auf günstigeren HDD-Speicher auf anderen Knoten klonen, replizieren und sichern. Dieser Ansatz erfüllt oder übertrifft die MEDITECH-Richtlinien für das SAN-basierte Klonen und das Sichern von Produktionspools.

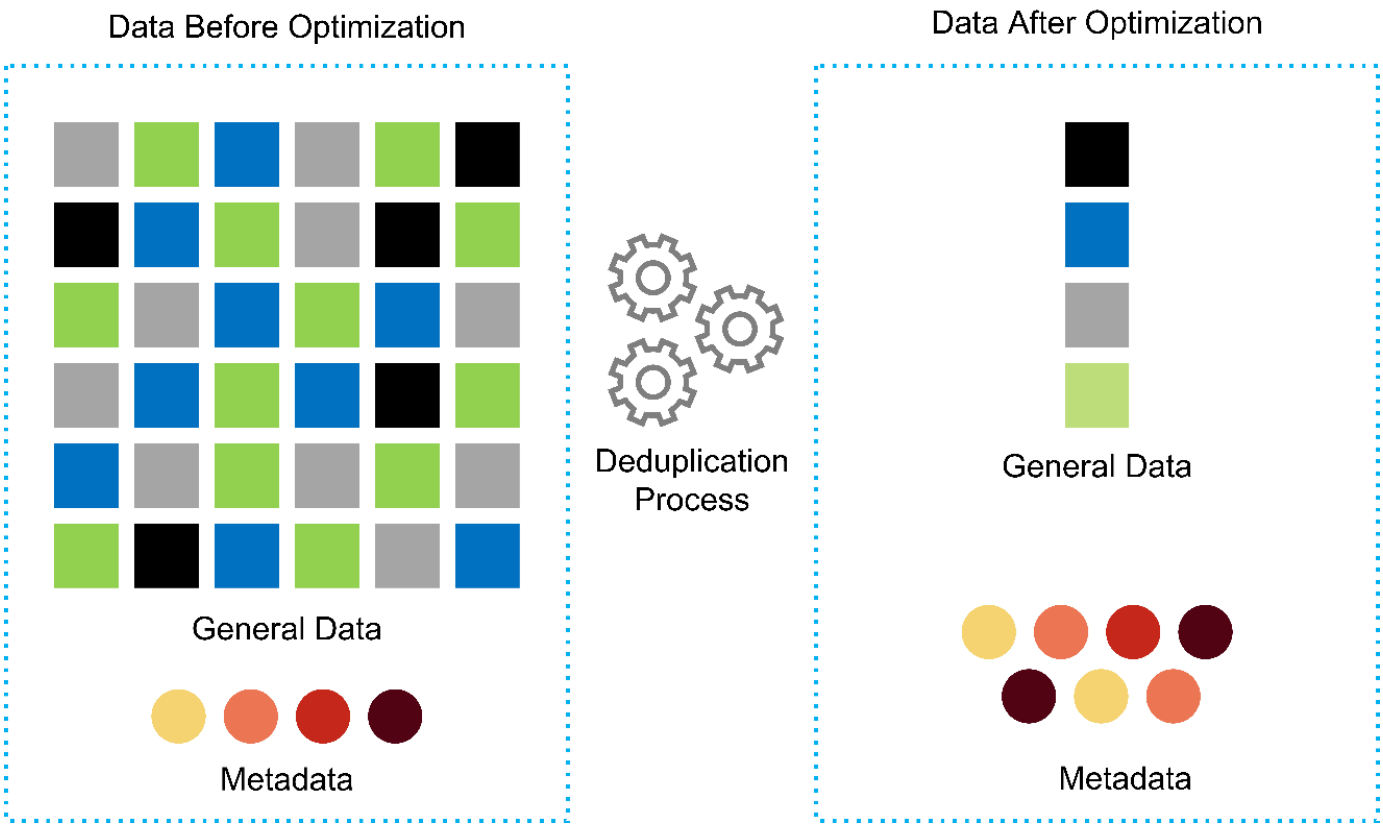
Viele der ONTAP-Funktionen sind besonders in MEDITECH-Umgebungen nützlich: Vereinfachtes Management, höhere Verfügbarkeit und Automatisierung sowie eine geringere Storage-Kapazität. Diese Funktionen bieten Ihnen:

- **Außergewöhnliche Performance.** die NetApp AFF Lösung verwendet die Unified Storage-Architektur, die ONTAP Software, die Managementoberfläche, umfassende Datenservices und erweiterte Funktionen, die die anderen NetApp FAS Produktfamilien bieten. Diese innovative Kombination aus All-Flash-Medien und ONTAP sorgt für eine konsistent niedrige Latenz und hohen IOPS von All-Flash-Storage mit der branchenführenden ONTAP Software.
- **Storage-Effizienz** Reduzieren Sie die Kapazitätsanforderungen an die Gesamtkapazität mit Deduplizierung, NetApp FlexClone Datenreplizierungstechnologie, Inline-Komprimierung, Inline-Data-Compaction, Thin Replication, Thin Provisioning, Und Deduplizierung von Aggregaten:

  Die NetApp Deduplizierung bietet Deduplizierung auf Block-Ebene in einem NetApp FlexVol Volume oder einer Datenkomponente. Im Wesentlichen werden bei der Deduplizierung doppelte Blöcke entfernt und nur eindeutige Blöcke im FlexVol Volume oder der Datenkomponente gespeichert.

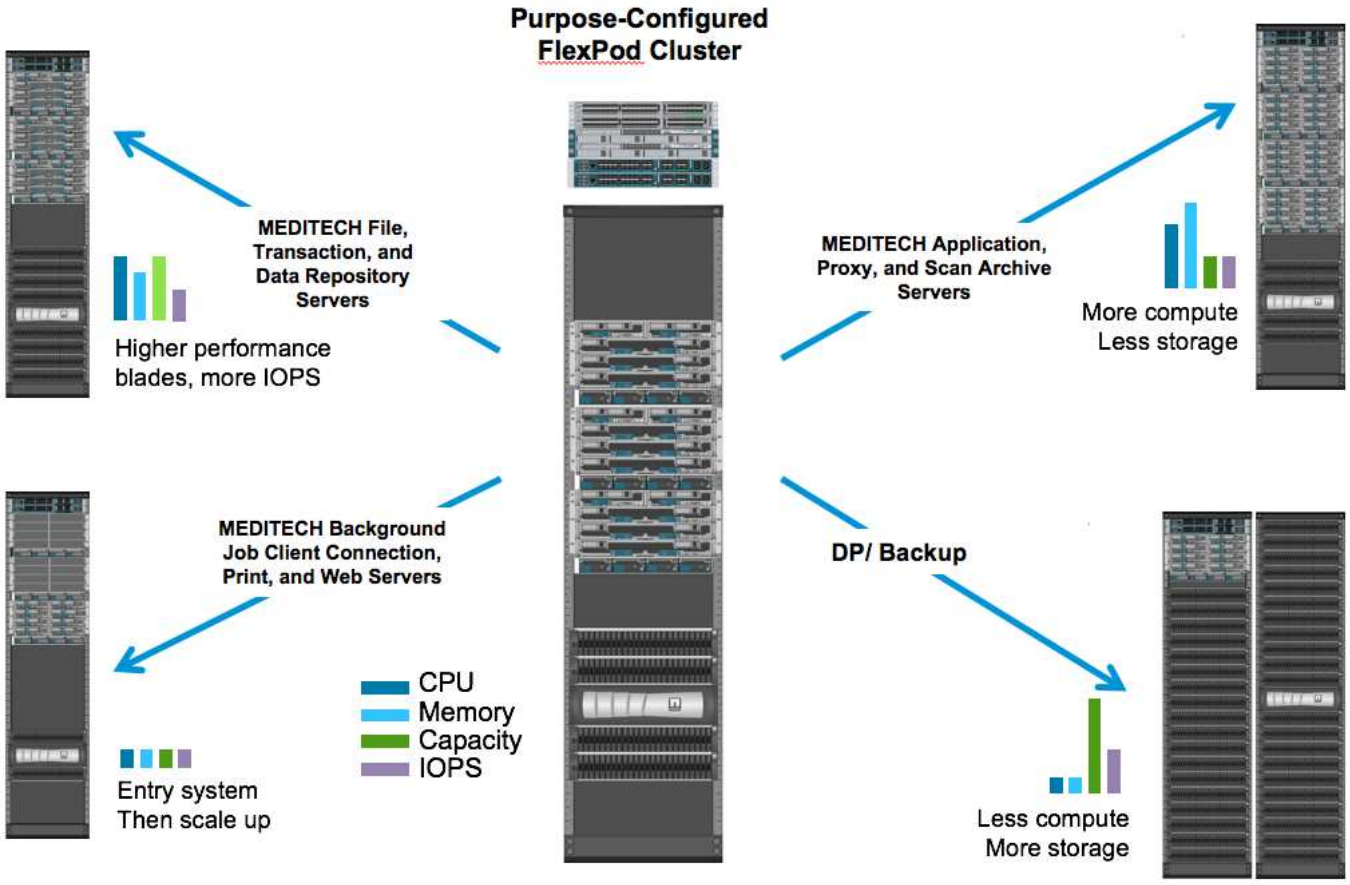
  Die Deduplizierung arbeitet mit einer hohen Granularität und wird auf dem aktiven File-System des FlexVol Volume oder der Datenkomponente betrieben. Die Deduplizierung ist applikationsunabhängig, weshalb Daten, die aus allen Applikationen stammen, die das NetApp System nutzen, dedupliziert werden können. Die Volume-Deduplizierung kann als Inline-Prozess ausgeführt werden (ab ONTAP 8.3.2). Sie können sie auch als Hintergrundprozess ausführen, der konfiguriert werden kann, automatisch auszuführen, zeitlich eingeplant zu werden oder manuell über die CLI, den NetApp ONTAP System Manager oder den NetApp Active IQ Unified Manager ausgeführt zu werden.

  Die folgende Abbildung zeigt, wie die NetApp Deduplizierung auf höchster Ebene funktioniert.



- **Platzsparendes Klonen** die FlexClone Funktion ermöglicht Ihnen die nahezu sofortige Erstellung von Klonen zur Aktualisierung der Backup- und Testumgebung. Diese Klone verbrauchen nur bei Änderungen mehr Storage.
- **NetApp Snapshot und SnapMirror Technologien.** ONTAP kann platzeffiziente Snapshot-Kopien der Logical Unit Numbers (LUNs) erstellen, die der MEDITECH-Host nutzt. Bei Implementierungen mit zwei Standorten kann SnapMirror Software für mehr Datenreplizierung und Ausfallsicherheit implementiert werden.
- * Integrierte Datensicherung.* vollständige Funktionen für Datensicherung und Disaster Recovery helfen Ihnen, Ihre kritischen Datenbestände zu schützen und Disaster Recovery zu ermöglichen.
- **Unterbrechungsfreier Betrieb.** Upgrades und Wartungen können durchgeführt werden, ohne Daten offline zu schalten.
- **QoS und Adaptive QoS (AQoS).** mit Storage QoS können Sie potenzielle problematische Workloads begrenzen. Wichtiger noch: QoS kann ein Performance-Minimum für kritische Workloads wie MEDITECH Production garantieren. Aufgrund von Engpässen kann NetApp QoS Probleme im Zusammenhang mit der Performance verringern. AQoS arbeitet mit vordefinierten Richtliniengruppen zusammen, die Sie direkt auf ein Volume anwenden können. Diese Richtliniengruppen können automatisch eine Durchsatzdecke oder eine Boden-zu-Volume-Größe skalieren und so das Verhältnis von IOPS zu Terabyte und Gigabyte beibehalten, wenn sich die Größe des Volumes ändert.
- **NetApp Data Fabric.** NetApp Data Fabric vereinfacht und integriert Datenmanagement in Cloud- und On-Premises-Umgebungen, um die digitale Transformation zu beschleunigen. Sie profitieren von konsistenten und integrierten Datenmanagementservices, Applikationen für Datentransparenz und Einblicke aus Daten, Datenzugriff und -Kontrolle sowie Datensicherung und -Sicherheit. NetApp ist in Amazon Web Services (AWS), Azure, Google Cloud Platform und IBM Cloud Clouds integriert, sodass Sie eine breite Auswahl haben.

Die folgende Abbildung zeigt die FlexPod-Architektur für MEDITECH-Workloads.



MEDITECH Übersicht

Medical Information Technology, Inc., allgemein bekannt als MEDITECH, ist ein Software-Unternehmen mit Sitz in Massachusetts, das Informationssysteme für Einrichtungen im Gesundheitswesen bereitstellt. MEDITECH stellt ein EHR-System bereit, das entwickelt wurde, um die neuesten Patientendaten zu speichern und zu organisieren und die Daten an das klinische Personal zu übertragen. Patientendaten umfassen u. a. demografische Daten, Krankengeschichte, Medikamente, Laborergebnisse; röntgenbilder und persönliche Daten wie Alter, Größe und Gewicht.

Es geht nicht mehr um den Umfang dieses Dokuments, um die vielfältigen Funktionen abzudecken, die die MEDITECH-Software unterstützt. Anhang A bietet weitere Informationen zu diesen vielfältigen MEDITECH-Funktionen. Für MEDITECH-Anwendungen sind mehrere VMs erforderlich, um diese Funktionen zu unterstützen. Um diese Anwendungen zu implementieren, lesen Sie die Empfehlungen von MEDITECH.

Für jede Implementierung benötigen alle MEDITECH-Softwaresysteme aus Sicht des Speichersystems eine verteilte, patientenorientierte Datenbank. MEDITECH hat eine eigene proprietäre Datenbank, die das Windows-Betriebssystem nutzt.

Bridgehead und CommVault sind die beiden Backup-Software-Applikationen, die von NetApp und MEDITECH zertifiziert sind. Dieses Dokument behandelt nicht die Implementierung dieser Backup-Applikationen.

Der Schwerpunkt dieses Dokuments liegt in der Aktivierung des FlexPod-Stacks (Server und Speicher), um die Performance-getriebenen Anforderungen der MEDITECH-Datenbank und der Backup-Anforderungen in der EHR-Umgebung zu erfüllen.

Speziell für bestimmte MEDITECH-Workloads entwickelt

MEDITECH verkauft keine Server-, Netzwerk- oder Speicherhardware, Hypervisoren oder Betriebssysteme weiter; Es gelten jedoch spezifische Anforderungen für jede Komponente des Infrastruktur-Stacks. Daher haben Cisco und NetApp zusammengearbeitet, um das FlexPod Datacenter erfolgreich zu testen, zu implementieren und zu unterstützen, um die Anforderungen von MEDITECH in der Produktionsumgebung von Kunden wie Ihrem zu erfüllen.

MEDITECH-Kategorien

MEDITECH ordnet die Bereitstellungsgröße einer Kategorienummer zu, die zwischen 1 und 6 reicht. Die Kategorie 1 stellt die kleinsten MEDITECH-Bereitstellungen dar, und die Kategorie 6 stellt die größten MEDITECH-Bereitstellungen dar.

Informationen zu den I/O-Merkmalen und Leistungsanforderungen eines MEDITECH Hosts in den einzelnen Kategorien finden Sie auf NetApp "TR-4190: NetApp Sizing Guidelines for MEDITECH Environments".

MEDITECH-Plattform

Die MEDITECH Expanse-Plattform ist die neueste Version der EHR-Software des Unternehmens. Frühere MEDITECH-Plattformen sind Client/Server 5.x und MAGIC. Dieser Abschnitt beschreibt die MEDITECH-Plattform (anwendbar auf Expense, 6.x, C/S 5.x und MAGIC), die den MEDITECH-Host und dessen Speicheranforderungen betrifft.

Für alle vorangegangenen MEDITECH-Plattformen laufen auf mehreren Servern die MEDITECH-Software, die verschiedene Aufgaben ausführt. Die vorherige Abbildung zeigt ein typisches MEDITECH-System, einschließlich MEDITECH-Hosts, die als Anwendungsserver und andere MEDITECH-Server dienen. Beispiele anderer MEDITECH-Server sind die Data Repository-Anwendung, die Anwendung Scannen und Archivierung sowie Background Job Clients. Die vollständige Liste anderer MEDITECH-Server finden Sie in den Dokumenten „Hardware Configuration Proposal“ (für neue Bereitstellungen) und „Hardware Evaluation Task“ (für bestehende Bereitstellungen). Diese Dokumente erhalten Sie von MEDITECH über den MEDITECH-Systemintegrator oder von Ihrem MEDITECH Technical Account Manager (TAM).

MEDITECH-Gastgeber

Ein MEDITECH-Host ist ein Datenbankserver. Dieser Host wird auch als MEDITECH-Dateiserver (für die Expense, 6.x oder C/S 5.x-Plattform) oder als ZAUBERMASCHINE (für die MAGIC-Plattform) bezeichnet. Dieses Dokument verwendet den Begriff MEDITECH Host, um auf einen MEDITECH-Dateiserver oder EINEN MAGIC Machine zu verweisen.

MEDITECH-Hosts können physische Server oder VMs sein, die auf dem Betriebssystem Microsoft Windows Server ausgeführt werden. Am häufigsten werden MEDITECH-Hosts in diesem Bereich als Windows-VMs bereitgestellt, die auf einem VMware ESXi-Server laufen. Nach diesem Schreiben ist VMware der einzige Hypervisor, den MEDITECH unterstützt. Ein MEDITECH-Host speichert seine Programme, Wörterbücher und Datendateien auf einem Microsoft Windows-Laufwerk (z. B. Laufwerk E) auf dem Windows-System.

In einer virtuellen Umgebung befindet sich ein Windows E -Laufwerk auf einem LUN, das über RDM (Raw Device Mapping) im physischen Kompatibilitätsmodus mit der VM verbunden ist. Die Verwendung von VMDK-Dateien (Virtual Machine Disk) als Windows E-Laufwerk in diesem Szenario wird von MEDITECH nicht unterstützt.

MEDITECH-Host-Workload-I/O-Eigenschaft

Das I/O-Merkmal jedes MEDITECH-Hosts und des gesamten Systems hängt von der MEDITECH-Plattform ab, die Sie bereitstellen. Alle MEDITECH-Plattformen (Expse, 6.x, C/S 5.x und MAGIC) erzeugen Workloads, die

zu 100% zufällig sind.

Die MEDITECH Expse-Plattform erzeugt den anspruchsvollsten Workload, da sie den höchsten Prozentsatz der Schreibvorgänge und die IOPS pro Host insgesamt hat, gefolgt von 6.x, C/S 5.x und DEN MAGIC-Plattformen.

Weitere Informationen zu den MEDITECH-Arbeitslastbeschreibungen finden Sie unter "TR-4190: NetApp Sizing Guidelines for MEDITECH Environments".

Datennetzwerk Storage-Netzwerk

MEDITECH verlangt, dass das FC-Protokoll für den Datenverkehr zwischen dem NetApp FAS- oder AFF-System und den MEDITECH-Hosts aller Kategorien verwendet wird.

Speicherpräsentation für MEDITECH Gastgeber

Jeder MEDITECH-Host verwendet zwei Windows-Laufwerke:

- **Laufwerk C.** Dieses Laufwerk speichert das Windows Server-Betriebssystem und die MEDITECH Host-Anwendungsdateien.
- **Drive E.** der MEDITECH-Host speichert seine Programme, Wörterbücher und Datendateien auf Laufwerk E des Windows-Server-Betriebssystems. Laufwerk E ist eine LUN, die über das NetApp FAS oder AFF System mithilfe des FC-Protokolls zugeordnet wird. MEDITECH verlangt, dass das FC-Protokoll verwendet wird, damit die IOPS-Anforderungen des MEDITECH-Hosts und die Lese- und Schreiblatenz erfüllt werden.

Namenskonvention von Volume und LUN

MEDITECH erfordert, dass eine spezielle Namenskonvention für alle LUNs verwendet wird.

Überprüfen Sie vor einer Speicherbereitstellung den Vorschlag für die MEDITECH-Hardwarekonfiguration, um die Namenskonvention für die LUNs zu bestätigen. Die Datensicherung von MEDITECH basiert auf der Namenskonvention des Volumes und der LUN, um die spezifischen LUNs zu identifizieren, die für das Backup erforderlich sind.

Umfassende Management Tools und Automatisierungsfunktionen

Cisco UCS mit Cisco UCS Manager

Cisco konzentriert sich auf drei Schlüsselelemente für eine herausragende Datacenter-Infrastruktur: Vereinfachung, Sicherheit und Skalierbarkeit. Die Cisco UCS Manager Software bietet in Kombination mit der Modularität der Plattform eine vereinfachte, sichere und skalierbare Desktop-Virtualisierungsplattform:

- **Vereinfacht.** Cisco UCS stellt einen radikal neuen Ansatz für Standard-Computing dar und bildet den Kern der Datacenter-Infrastruktur für alle Workloads. Cisco UCS bietet viele Funktionen und Vorteile, darunter eine Verringerung der Anzahl der erforderlichen Server sowie eine Reduzierung der Anzahl der Kabel pro Server. Eine weitere wichtige Funktion besteht in der Fähigkeit zur schnellen Implementierung oder Neubereitstellung von Servern über Cisco UCS Service-Profile. Da weniger Server und Kabel für das Management erforderlich sind und die optimierte Bereitstellung von Server- und Applikations-Workloads optimiert werden muss, werden die Betriebsabläufe vereinfacht. Dutzende von Blade- und Rack-Servern können mit Service-Profilen von Cisco UCS Manager innerhalb von Minuten bereitgestellt werden. Cisco UCS Serviceprofile machen Runbooks zur Server-Integration überflüssig und vermeiden die Konfigurationstendenzen. Dadurch wird die Zeit bis zur Produktivität für Endbenutzer beschleunigt, die Unternehmensflexibilität verbessert und IT-Ressourcen können anderen Aufgaben zugewiesen werden.

Der Cisco UCS Manager automatisiert viele routinemäßige und fehleranfällige Datacenter-Vorgänge, beispielsweise bei der Konfiguration und Bereitstellung der Server-, Netzwerk- und Infrastruktur für den Storage-Zugriff. Darüber hinaus ermöglichen Cisco UCS Blade Server der B-Serie und Rack Server der C-Serie mit großem Speicherbedarf eine hohe Benutzerdichte für Anwendungen, wodurch die Anforderungen an die Server-Infrastruktur verringert werden.

Vereinfachung führt zu einer schnelleren und erfolgreicheren MEDITECH-Infrastrukturbereitstellung.

- **Sicher.** Obwohl VMs von Natur aus sicherer sind als ihre physischen Vorgänger, bringen sie neue Sicherheitsherausforderungen mit sich. Geschäftskritische Web- und Applikations-Server, die eine gemeinsame Infrastruktur wie virtuelle Desktops nutzen, haben jetzt ein höheres Risiko für Sicherheitsbedrohungen. Der Inter- VM Traffic verfügt nun über ein wichtiges Sicherheitsüberbedenken, das Ihre IT-Manager beachten müssen, insbesondere in dynamischen Umgebungen, in denen sich die VMs mithilfe von VMware vMotion über die Server-Infrastruktur bewegen.

  Durch Virtualisierung wird daher das Richtlinien- und Sicherheitsbewusstsein auf VM-Ebene deutlich erhöht. Dies gilt insbesondere angesichts der dynamischen und flexiblen Art der VM-Mobilität über eine erweiterte Computing-Infrastruktur hinweg. Die einfache Zunahme der Anzahl neuer virtueller Desktops erhöht die Bedeutung einer virtualisierungskompatiblen Netzwerk- und Sicherheitsinfrastruktur. Die Cisco Datacenter-Infrastruktur (Cisco UCS, Cisco MDS und Lösungen der Cisco Nexus Familie) für die Desktop-Virtualisierung bietet solide Datacenter-, Netzwerk- und Desktop-Sicherheit mit umfassender Sicherheit vom Desktop bis zum Hypervisor. Zusätzliche Sicherheit wird durch Segmentierung von virtuellen Desktops, VM-fähigen Richtlinien und Administration sowie Netzwerksicherheit in der gesamten LAN- und WAN-Infrastruktur erzielt.

- **Skalierbar.** das Wachstum von Virtualisierungslösungen ist alles andere als unvermeidlich. Daher muss eine Lösung in der Lage sein, mit diesem Wachstum skalierbar zu sein und vorhersehbar zu skalieren. Die Cisco Virtualisierungslösungen unterstützen eine hohe VM-Dichte (VMs pro Server), während mehr Server bei nahezu linearer Performance skaliert werden können. Die Cisco Datacenter-Infrastruktur bietet eine flexible Plattform für Wachstum und erhöht die geschäftliche Flexibilität. Die Service-Profile von Cisco UCS Manager ermöglichen die bedarfsgesteuerte Host-Bereitstellung und erleichtern die Implementierung Hunderter Hosts ebenso wie Dutzende.

  Cisco UCS Server bieten nahezu lineare Performance und Skalierbarkeit. Cisco UCS nutzt die patentierte Cisco Extended Memory Technologie, um großen Speicherbedarf mit weniger Sockeln zu bieten (mit Skalierbarkeit auf bis zu 1 TB Speicher mit Servern für 2 und 4 Plätze). Durch den Einsatz von Unified Fabric Technologie als Baustein lässt sich die aggregierte Bandbreite von Cisco UCS Server auf bis zu 80 Gbit/s pro Server skalieren, und das nordgebundene Cisco UCS Fabric Interconnect kann mit einer Übertragungsrate von 2 Tbit/s arbeiten. Diese Funktion verhindert I/O- und Speicherengpässe der Desktop-Virtualisierung. Das Cisco UCS unterstützt mit seiner hochperformanten Unified Fabric-basierten Netzwerkarchitektur mit geringer Latenz hohe Mengen an Virtual Desktop-Datenverkehr, einschließlich hochauflösende Video- und Kommunikationsdaten. Darüber hinaus hilft ONTAP im Rahmen der FlexPod Virtualisierungslösungen die Datenverfügbarkeit und optimale Performance bei Boot- und Login-Anstürmen zu wahren.

  Cisco UCS, Cisco MDS und Cisco Nexus Datacenter-Infrastrukturdesigns bieten eine hervorragende Wachstumsplattform. Server-, Netzwerk- und Storage-Ressourcen lassen sich transparent skalieren, um Desktop-Virtualisierung, Datacenter-Applikationen und Cloud Computing zu unterstützen.

VMware vCenter Server

VMware vCenter Server bietet eine zentralisierte Plattform für das Management von MEDITECH-Umgebungen, mit der Ihr Gesundheitsunternehmen eine virtuelle Infrastruktur sicher automatisieren und bereitstellen kann:

- * Einfache Bereitstellung.* Schnelle und einfache Bereitstellung von vCenter Server mit einer virtuellen Appliance.
- **Zentrale Steuerung und Transparenz.** Verwalten Sie die gesamte VMware vSphere Infrastruktur von einem Ort aus.
- **Proaktive Optimierung.** Ressourcen zuweisen und optimieren für maximale Effizienz.
- **Management.** Verwenden Sie leistungsstarke Plug-ins und Tools, um das Management zu vereinfachen und die Kontrolle zu erweitern.

Virtual Storage Console für VMware vSphere

Virtual Storage Console (VSC), vSphere API for Storage Awareness (VASA) Provider und VMware Storage Replication Adapter (SRA) für VMware vSphere von NetApp bilden eine einzelne virtuelle Appliance. Die Produktsuite umfasst SRA und VASA Provider als Plug-ins für vCenter Server, das ein lückenloses Lifecycle Management für VMs in VMware Umgebungen bietet, die NetApp Storage-Systeme nutzen.

Die virtuelle Appliance für VSC, VASA Provider und SRA lässt sich nahtlos in den VMware vSphere Web Client integrieren und ermöglicht die Nutzung von SSO-Services. In einer Umgebung mit mehreren VMware vCenter Server-Instanzen muss jede zu verwaltende vCenter Server Instanz eine eigene, eingetragene Instanz von VSC haben. Über die VSC Dashboard-Seite können Sie den Gesamtstatus Ihrer Datastores und VMs schnell überprüfen.

Durch die Implementierung der virtuellen Appliance für VSC, VASA Provider und SRA können Sie die folgenden Aufgaben ausführen:

- **Verwenden Sie VSC für die Bereitstellung und das Management von Speicher und die Konfiguration des ESXi Hosts.** mit VSC können Sie Anmeldeinformationen hinzufügen, Anmeldeinformationen entfernen, Anmeldedaten zuweisen und Berechtigungen für Storage Controller in Ihrer VMware Umgebung einrichten. Darüber hinaus können auch ESXi Server gemanagt werden, die mit NetApp Storage-Systemen verbunden sind. Mit ein paar Klicks können Sie für alle Hosts empfohlene Best-Practice-Werte für Host Timeouts, NAS und Multipathing festlegen. Sie können auch Speicherdetails anzeigen und Diagnoseinformationen erfassen.
- **Verwenden Sie VASA Provider zum Erstellen von Storage-Funktionsprofilen und zum Einstellen von Alarmen.** VASA Provider für ONTAP ist bei der Aktivierung der VASA Provider-Erweiterung bei VSC registriert. Sie können Storage-Funktionsprofile und virtuelle Datastores erstellen und verwenden. Sie können auch Alarme festlegen, um Sie zu benachrichtigen, wenn die Schwellenwerte für Volumes und Aggregate fast voll sind. Sie können die Performance von VMDKs und den auf virtuellen Datastores erstellten VMs überwachen.
- **Verwenden Sie SRA für die Disaster Recovery.** mit SRA können geschützte und Recovery-Standorte in der Umgebung für Disaster Recovery bei Ausfällen konfiguriert werden.

NetApp OnCommand Insight und ONTAP

NetApp OnCommand Insight integriert das Infrastrukturmanagement in die Servicekette MEDITECH. Dieser Ansatz ermöglicht Ihrem Unternehmen im Gesundheitswesen eine bessere Kontrolle, Automatisierung und Analyse Ihrer Storage-, Netzwerk- und Computing-Infrastruktur. DIE SOFTWARE optimiert Ihre aktuelle Infrastruktur optimal und erleichtert die sinnvolle Planung neuer Investitionen. Außerdem werden die Risiken verringert, die mit komplexen Technologiemigrationen verbunden sind. Da es agentenfrei läuft, ist die Installation unkompliziert und unterbrechungsfrei. Installierte Storage- und SAN-Geräte werden kontinuierlich überwacht. Detaillierte Informationen sorgen für volle Transparenz Ihrer gesamten Storage-Umgebung. Sie erkennen falsch bzw. unzureichend genutzte oder verwaiste Ressourcen umgehend und können diese so wieder nutzbar machen. OnCommand Insight bietet Ihnen folgende Vorteile:

- **Optimierung vorhandener Ressourcen.** Identifizieren Sie falsch genutzte, unzureichend genutzte oder verwaiste Ressourcen, indem Sie bewährte Best Practices nutzen, um Probleme zu vermeiden und Service-Level einzuhalten.
- **Bessere Entscheidungen treffen** mit Echtzeitdaten lassen sich Kapazitätsprobleme schneller lösen, um zukünftige Anschaffungen präzise zu planen, zu Budgetüberschreitungen zu vermeiden und Investitionsausgaben hinauszuschieben.
- **Beschleunigen SIE IT-Initiativen** Verstehen Sie Ihre virtuellen Umgebungen, um Risiken zu managen, Ausfallzeiten zu minimieren und die Cloud-Implementierung zu beschleunigen.

Konzipieren

Die Architektur von FlexPod für MEDITECH basiert auf Guidance von MEDITECH, Cisco und NetApp und auf Erfahrungen unserer Partner in der Zusammenarbeit mit MEDITECH Kunden aller Größen. Die Architektur ist anpassungsfähig und wendet Best Practices für MEDITECH an, je nachdem, welche Datacenter-Strategie Sie haben, wie groß Ihr Unternehmen ist und ob Ihr System zentralisiert, verteilt oder mandantenfähig ist.

Die richtige Storage-Architektur kann durch die Gesamtgröße mit den IOPS-insgesamt bestimmt werden. Performance allein ist nicht der einzige Faktor. Basierend auf zusätzlichen Kundenanforderungen können Sie sich entscheiden, eine größere Anzahl Nodes zu verwenden. Der Vorteil von NetApp Storage besteht darin, dass Sie den Cluster bei sich ändernden Anforderungen einfach und unterbrechungsfrei vertikal skalieren können. Zudem lassen sich Nodes unterbrechungsfrei aus dem Cluster entfernen, um Geräte anderen Zwecken zuzuweisen oder während Geräteaktualisierungen einzuführen.

Dies sind einige der Vorteile der NetApp ONTAP Storage-Architektur:

- **Einfaches, unterbrechungsfreies Scale-up und Scale-out.** Dank des unterbrechungsfreien Betriebs von ONTAP können Sie Festplatten und Nodes aktualisieren, hinzufügen oder entfernen. Beginnen Sie mit vier Nodes und verschieben Sie auf sechs Nodes oder aktualisieren Sie unterbrechungsfrei auf größere Controller.
- **Storage-Effizienz** Reduzierung Ihrer Kapazitätsanforderungen mit Deduplizierung, NetApp FlexClone, Inline-Komprimierung, Inline-Data-Compaction, Thin Replication Thin Provisioning und Deduplizierung von Aggregaten Die FlexClone Funktion ermöglicht nahezu unmittelbare Klonerstellung zur Unterstützung von Aktualisierungen der Backup- und Testumgebung. Diese Klone verbrauchen nur bei Änderungen mehr Storage.
- **Disaster Recovery Schattendatenbankserver.** der Disaster Recovery Schattendatenbankserver ist Teil Ihrer Business Continuity-Strategie (wird zur Unterstützung von Read-Only Storage-Funktionen verwendet und möglicherweise als Storage-Lese-/Schreibinstanz konfiguriert). Daher haben die Platzierung und Größenbemessung des dritten Storage-Systems in der Regel dasselbe wie im Storage-System Ihrer Produktionsdatenbank.
- **Datenbankkonsistenz (einige Überlegungen erforderlich).** Wenn Sie NetApp SnapMirror Backup-Kopien in Bezug auf Business Continuity verwenden, siehe "TR-3446: SnapMirror Async Overview and Best Practices Guide".

Storage-Layout

Dedizierte Aggregate für MEDITECH-Hosts

Der erste Schritt zur Erfüllung der hohen Performance- und Hochverfügbarkeitsanforderungen von MEDITECH besteht darin, das Speicherlayout für die MEDITECH-Umgebung richtig zu gestalten, um die MEDITECH-Host-Produktionskosten auf einen dedizierten, hochperformanten Speicher zu isolieren.

Auf jedem Speichercontroller sollte ein dediziertes Aggregat bereitgestellt werden, um das Programm, das Wörterbuch und die Datendateien der MEDITECH-Hosts zu speichern. Um das Risiko zu beseitigen, dass andere Workloads dieselben Festplatten verwenden und die Performance beeinträchtigen, wird kein anderer Storage über diese Aggregate bereitgestellt.

> Speicherung, die Sie für die anderen MEDITECH-Server bereitstellen, sollte nicht auf das dedizierte Aggregat für die LUNs platziert werden, die von den MEDITECH-Hosts verwendet werden. Sie sollten den Speicher für andere MEDITECH-Server auf einem separaten Aggregat platzieren. Speicheranforderungen für andere MEDITECH-Server sind in den Dokumenten „Hardware Configuration Proposal“ (für neue Bereitstellungen) und „Hardware Evaluation Task“ (für bestehende Bereitstellungen) verfügbar. Diese Dokumente erhalten Sie von MEDITECH über den MEDITECH-Systemintegrator oder von Ihrem MEDITECH Technical Account Manager (TAM). NetApp Solution Engineers haben eventuell einen Rat an das NetApp MEDITECH Independent Software Vendor (ISV) Team, um eine ordnungsgemäße und vollständige Konfiguration des NetApp Storage-Größenbemessung zu ermöglichen.

Verteilen Sie den MEDITECH-Host-Workload gleichmäßig auf alle Storage-Controller

NetApp FAS und AFF Systeme werden als ein oder mehrere Hochverfügbarkeitspaare implementiert. NetApp empfiehlt, die MEDITECH Erweiterung und 6.x Workloads gleichmäßig auf alle Storage Controller zu verteilen, um die Computing-, Netzwerk- und Caching-Ressourcen auf jedem Storage Controller anzuwenden.

Verwenden Sie die folgenden Richtlinien, um die MEDITECH-Workloads gleichmäßig auf jeden Storage-Controller zu verteilen:

- Wenn Sie die IOPS für jeden MEDITECH-Host kennen, können Sie die MEDITECH-Erweiterung und 6.x-Workloads gleichmäßig auf alle Storage-Controller verteilen, indem Sie bestätigen, dass jeder Controller eine ähnliche Anzahl von IOPS von den MEDITECH-Hosts unterstützt.
- Wenn Sie die IOPS für jeden MEDITECH-Host nicht kennen, können Sie die MEDITECH-Expense und 6.x-Workloads immer noch gleichmäßig auf alle Storage-Controller verteilen. Füllen Sie diese Aufgabe aus, indem Sie bestätigen, dass die Kapazität der Aggregate für die MEDITECH-Hosts gleichmäßig auf alle Speicher-Controller verteilt ist. Auf diese Weise ist die Anzahl der Disketten über alle Datenaggregate hinweg identisch, die den MEDITECH-Hosts gewidmet sind.
- Verwenden Sie ähnliche Festplattentypen und identische RAID-Gruppen, um die Storage-Aggregate beider Controller zu erstellen, sodass die Workloads gleichmäßig verteilt werden. Wenden Sie sich an einen NetApp Certified Integrator, bevor Sie das Storage-Aggregat erstellen.

> Laut MEDITECH generieren zwei Hosts im MEDITECH-System höhere IOPS als die restlichen Hosts. Die LUNs für diese beiden Hosts sollten auf separaten Storage Controllern platziert werden. Sie sollten diese beiden Gastgeber mit Unterstützung des MEDITECH-Teams identifizieren, bevor Sie Ihr System bereitstellen.

Storage-Platzierung

Datenbank-Storage für MEDITECH-Hosts

Der Datenbank-Storage für einen MEDITECH-Host wird als Block-Gerät (das ist eine LUN) aus dem NetApp FAS oder AFF System dargestellt. Die LUN wird normalerweise als E-Laufwerk auf das Windows Betriebssystem eingebunden.

Anderer Storage

Das MEDITECH-Host-Betriebssystem und die Datenbankapplikation erzeugen normalerweise eine erhebliche Menge von IOPS auf dem Speicher. Die Speicherbereitstellung für die MEDITECH-Host-VMs und deren VMDK-Dateien gilt, falls erforderlich, als unabhängig von dem Speicher, der zur Erfüllung der MEDITECH-Leistungsschwellenwerte erforderlich ist.

Speicher, die für die anderen MEDITECH-Server bereitgestellt werden, sollten nicht auf das dedizierte Aggregat für die LUNs platziert werden, die die MEDITECH-Hosts verwenden. Platzieren Sie den Speicher für andere MEDITECH-Server auf einem separaten Aggregat.

Konfiguration von Storage Controllern

Hochverfügbarkeit

Um die Auswirkungen eines Controller-Ausfalls zu verringern und unterbrechungsfreie Upgrades des Storage-Systems zu ermöglichen, sollten Sie Ihr Storage-System im Hochverfügbarkeits-Modus mit Controllern in einem Hochverfügbarkeitspaar konfigurieren.

Bei der hochverfügbaren Controller-Paar-Konfiguration sollten Festplatten-Shelfs über mehrere Pfade mit Controllern verbunden werden. Diese Verbindung verbessert die Storage Resiliency, indem sie vor einem Single Path-Ausfall schützt. Darüber hinaus wird bei einem Controller-Failover die Performance-Konsistenz verbessert.

Storage Performance bei Storage Controller Failover

Bei Storage-Systemen, die mit Controllern in einem Hochverfügbarkeitspaar konfiguriert sind, übernimmt der Partner-Controller in dem unwahrscheinlichen Fall eines Controller-Ausfalls die Storage-Ressourcen und Workloads des ausgefallenen Controllers. Wenden Sie sich unbedingt an den Kunden, um die Performance-Anforderungen zu ermitteln, die bei einem Controller-Ausfall erfüllt werden müssen und die Systemgröße entsprechend zu bestimmen.

Hardware-gestützte Übernahme

NetApp empfiehlt die Hardware-gestützte Übernahme auf beiden Storage Controllern.

Durch die Hardware-gestützte Übernahme minimieren Sie die Storage Controller Failover-Zeit. Es ermöglicht es einem Controller Remote LAN Modul oder Service Processor Modul, seinen Partner über einen Controller-Ausfall schneller als ein Herzschlag Timeout-Trigger informieren kann, die Zeit, die es dauert, um Failover. Die Hardware-gestützte Übernahme ist standardmäßig für Storage-Controller in einer Hochverfügbarkeitskonfiguration aktiviert.

Weitere Informationen über die Hardware-gestützte Übernahme finden Sie im "ONTAP 9 Dokumentationszentrum".

Festplattentyp

Um die Anforderung von MEDITECH-Workloads durch niedrige Leseverzögerungsanforderungen zu unterstützen, empfiehlt NetApp, für Aggregate in AFF-Systemen, die speziell für die MEDITECH-Hosts geeignet sind, eine hochperformante SSD zu verwenden.

NetApp AFF

NetApp bietet hochperformante AFF-Arrays zur Bewältigung von MEDITECH-Workloads, die einen hohen Durchsatz erfordern und über zufällige Datenzugriffsmuster und Anforderungen an niedrige Latenz verfügen.

Für MEDITECH-Workloads bieten AFF-Arrays Leistungsvorteile gegenüber auf HDDs basierenden Systemen. Die Kombination aus Flash-Technologie und Enterprise-Datenmanagement bietet Vorteile in drei wichtigen Bereichen: Performance, Verfügbarkeit und Storage-Effizienz.

NetApp Support Tools und Services

NetApp bietet ein umfassendes Set an Support Tools und Services. Das NetApp AutoSupport Tool sollte auf NetApp All Flash FAS/FAS Systemen aktiviert und konfiguriert werden, um den Startaufruf zu melden, falls ein Hardwarefehler oder eine Fehlkonfiguration des Systems auftritt. Benachrichtigung des NetApp Support-Teams bei Home-Benachrichtigungen zur zeitnahen Behebung von Fehlern. NetApp Active IQ ist eine webbasierte Applikation, die auf AutoSupport Informationen Ihrer NetApp Systeme basiert und vorausschauend Informationen liefert, um Verfügbarkeit, Effizienz und Performance zu verbessern.

Implementierung und Konfiguration

Überblick

In diesem Dokument werden die in diesem Dokument angegebenen Richtlinien zum NetApp Storage für die Implementierung von FlexPod behandelt:

- Umgebungen, die ONTAP nutzen
- Umgebungen, die Cisco UCS Blade- und Rack-montierte Server verwenden

Dieses Dokument deckt nicht ab:

- Detaillierte Implementierung der FlexPod Datacenter-Umgebung

  Weitere Informationen finden Sie unter "FlexPod Datacenter mit FC Cisco Validated Design" (CVD).

- Ein Überblick über die MEDITECH-Softwareumgebungen, Referenzarchitekturen und die Best Practices für die Integration.

  Weitere Informationen finden Sie unter "TR-4300i: NetApp FAS and All-Flash-Storage-Systeme for MEDITECH Environments Best Practices Guide" (NetApp Login erforderlich).

- Quantitative Performance-Anforderungen und Hinweise zur Dimensionierung

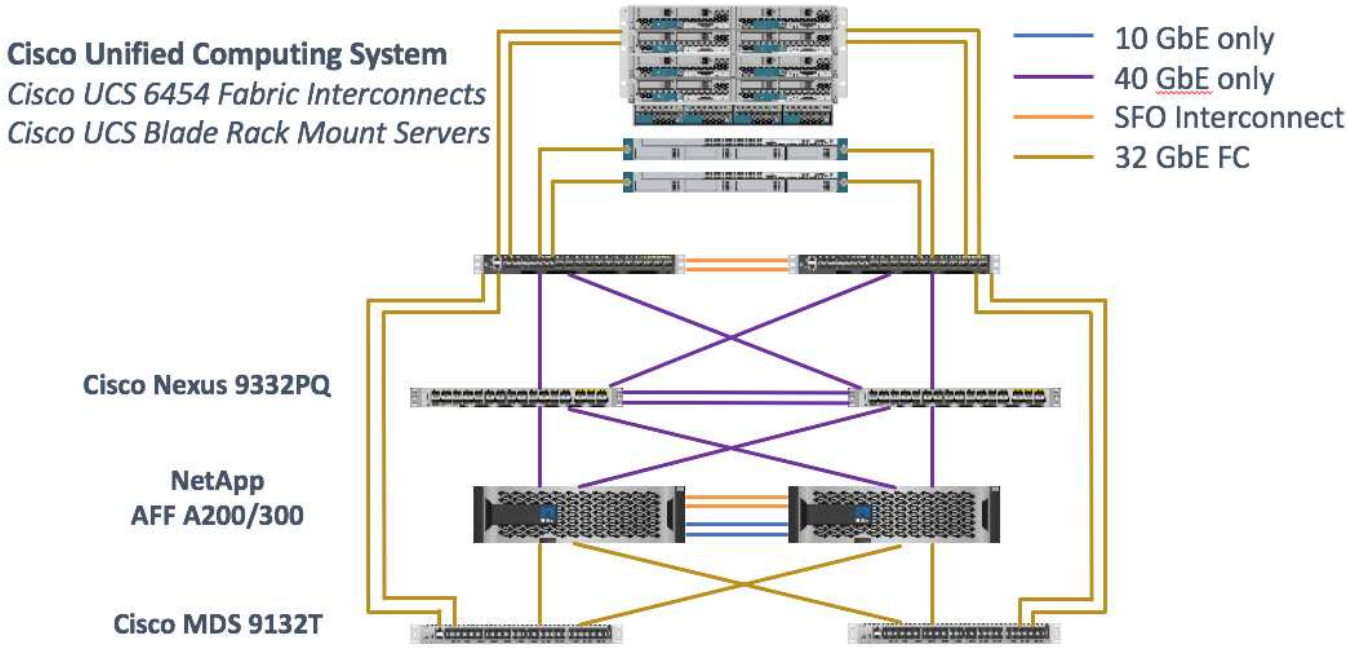
  Weitere Informationen finden Sie unter "TR-4190: NetApp Sizing Guidelines for MEDITECH Environments".

- Einsatz von NetApp SnapMirror Technologien für die Einhaltung von Backup- und Disaster-Recovery-Anforderungen
- Allgemeine Hinweise zur Implementierung von NetApp Storage.

In diesem Abschnitt wird eine Beispielkonfiguration mit Best Practices für die Infrastrukturbereitstellung erläutert sowie die verschiedenen Hardware- und Softwarekomponenten für die Infrastruktur und die Versionen, die Sie verwenden können, aufgeführt.

Verkabelungsdiagramm

Die folgende Abbildung zeigt das 32-GB-FC/40-GbE-Topologiediagramm für eine MEDITECH-Bereitstellung.



Verwenden Sie immer das "Interoperabilitäts-Matrix-Tool (IMT)" So überprüfen Sie, ob alle Versionen von Software und Firmware unterstützt werden. Die Tabelle in Abschnitt "MEDITECH Module und Komponenten" Führt die Hardware- und Softwarekomponenten der Infrastruktur auf, die bei den Tests verwendet wurden.

"Als Nächstes: Infrastrukturgrundlage"

Basiskonfiguration

Netzwerk-Konnektivität

Vor der Konfiguration der Infrastruktur müssen die folgenden Netzwerkverbindungen vorhanden sein:

- Die Link-Aggregation, die Port-Kanäle und virtuelle Port-Kanäle (vPCs) nutzt, wird durchgehend verwendet, wodurch das Design für eine höhere Bandbreite und hohe Verfügbarkeit ermöglicht wird:
  - VPC wird zwischen Cisco FI und Cisco Nexus Switches verwendet.
  - Jeder Server verfügt über virtuelle Netzwerk-Schnittstellenkarten (vNICs) mit redundanter Konnektivität zur Unified Fabric. Aus Gründen der Redundanz wird zwischen FIS ein NIC-Failover verwendet.
  - Jeder Server verfügt über virtuelle Host Bus Adapter (vHBAs) mit redundanter Konnektivität zum Unified Fabric.
- Das Cisco UCS-FI-SYSTEM ist wie empfohlen im End-Host-Modus konfiguriert und ermöglicht das dynamische Pinning von vNICs an Uplink-Switches.

Storage-Konnektivität

Vor der Konfiguration der Infrastruktur müssen die folgenden Speicherverbindungen vorhanden sein:

- Storage Port Interface Groups (ifgroups, vPC)
- 10-GB-Link zum Switch N9K-A
- 10-GB-Link zum Switch N9K-B
- In-Band-Management (aktiv-Passiv-Bond):

    - 1-GB-Link zum Management-Switch N9K-A
    - 1-GB-Link zum Management-Switch N9K-B
- 32-GB-FC-End-to-End-Konnektivität über Cisco MDS-Switches; Konfiguration von Einzel-Initiator-Zoning
- FC SAN-Boot für eine vollständige Statusfreies Computing; Server werden über LUNs im Boot-Volume gestartet, das auf dem AFF Storage-Cluster gehostet wird
- Alle MEDITECH-Workloads werden auf FC-LUNs gehostet, die sich über die Speicher-Controller-Knoten verteilen

Host-Software

Die folgende Software muss installiert sein:

- ESXi wurde auf den Cisco UCS Blades installiert
- Installation und Konfiguration von VMware vCenter (für alle in vCenter registrierten Hosts)
- VSC wird in VMware vCenter installiert und registriert
- NetApp Cluster konfiguriert

"Weiter: Cisco UCS Blade-Server- und Switch-Konfiguration."

Cisco UCS Blade-Server- und Switch-Konfiguration

Die Software FlexPod for MEDITECH ist auf jeder Stufe mit Fehlertoleranz ausgelegt. Es gibt keinen Single Point of Failure im System. Für eine optimale Performance empfiehlt Cisco den Einsatz von Hot-Spare Blade-Servern.

Dieses Dokument bietet allgemeine Hinweise zur Grundkonfiguration einer FlexPod-Umgebung für MEDITECH-Software. In diesem Abschnitt stellen wir grundlegende Schritte mit einigen Beispielen für die Vorbereitung des Cisco UCS Computing-Plattformelements der FlexPod-Konfiguration dar. Voraussetzung hierfür ist, dass die FlexPod Konfiguration gemäß den Anweisungen in den Rack-Einheiten mit Strom versorgt und verkabelt ist "FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-Series and Cisco UCS Manager 3.2"CVD.

Konfiguration des Cisco Nexus Switches

Für die Lösung wird ein fehlertolerantes Paar Ethernet Switches der Cisco Nexus 9300-Serie eingesetzt. Sie sollten diese Schalter wie im beschrieben verkabeln "Verkabelungsdiagramm" Abschnitt. Durch die Cisco Nexus-Konfiguration wird sichergestellt, dass Ethernet-Traffic-Ströme für die MEDITECH-Anwendung optimiert werden.

1. Führen Sie nach Abschluss der Ersteinrichtung und Lizenzierung die folgenden Befehle aus, um die globalen Konfigurationsparameter auf beiden Switches festzulegen:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Erstellen Sie auf jedem Switch mithilfe des globalen Konfigurationsmodus die VLANs für die Lösung:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Erstellen Sie die NTP-Verteilerschnittstelle (Network Time Protocol), Port-Kanäle, Port-Channel-Parameter und Port-Beschreibungen für die Fehlerbehebung per "FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-Series and Cisco UCS Manager 3.2"CVD.

Konfiguration für Cisco MDS 9132T

Die FC-Switches der Cisco MDS 9100 Serie bieten redundante 32-GB-FC-Konnektivität zwischen den NetApp AFF A200 oder AFF A300 Controllern und dem Cisco UCS Computing Fabric. Sie sollten die Kabel wie im beschrieben anschließen "Verkabelungsdiagramm" Abschnitt.

1. Führen Sie auf den Konsolen auf jedem MDS-Switch die folgenden Befehle aus, um die für die Lösung erforderlichen Funktionen zu aktivieren:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Konfigurieren einzelner Ports, Port-Kanäle und Beschreibungen gemäß dem FlexPod-Abschnitt zur Cisco MDS-Switch-Konfiguration in "FlexPod Datacenter mit FC Cisco Validated Design".
3. Um die erforderlichen virtuellen SANs (VSANs) für die Lösung zu erstellen, führen Sie im globalen Konfigurationsmodus die folgenden Schritte aus:

a. Führen Sie für den Fabric-A MDS Switch die folgenden Befehle aus:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

Die Port-Channel-Nummern in den letzten beiden Zeilen des Befehls wurden erstellt, wenn die einzelnen Ports, Port-Kanäle und Beschreibungen mithilfe des Referenzdokuments bereitgestellt wurden.

b. Führen Sie für den Fabric-B MDS Switch die folgenden Befehle aus:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

Die Port-Channel-Nummern in den letzten beiden Zeilen des Befehls wurden erstellt, wenn die einzelnen Ports, Port-Kanäle und Beschreibungen mithilfe des Referenzdokuments bereitgestellt wurden.

4. Erstellen Sie für jeden FC-Switch Geräte-Aliasnamen, die die Identifizierung jedes Geräts für laufende Vorgänge intuitiv machen, indem Sie die Details im Referenzdokument verwenden.
5. Erstellen Sie schließlich die FC-Zonen mithilfe der in Schritt 4 für jeden MDS-Switch erstellten Geräte-Aliasnamen wie folgt:
   a. Führen Sie für den Fabric-A MDS Switch die folgenden Befehle aus:

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. Führen Sie für den Fabric-B MDS Switch die folgenden Befehle aus:

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Anleitung zur Cisco UCS-Konfiguration

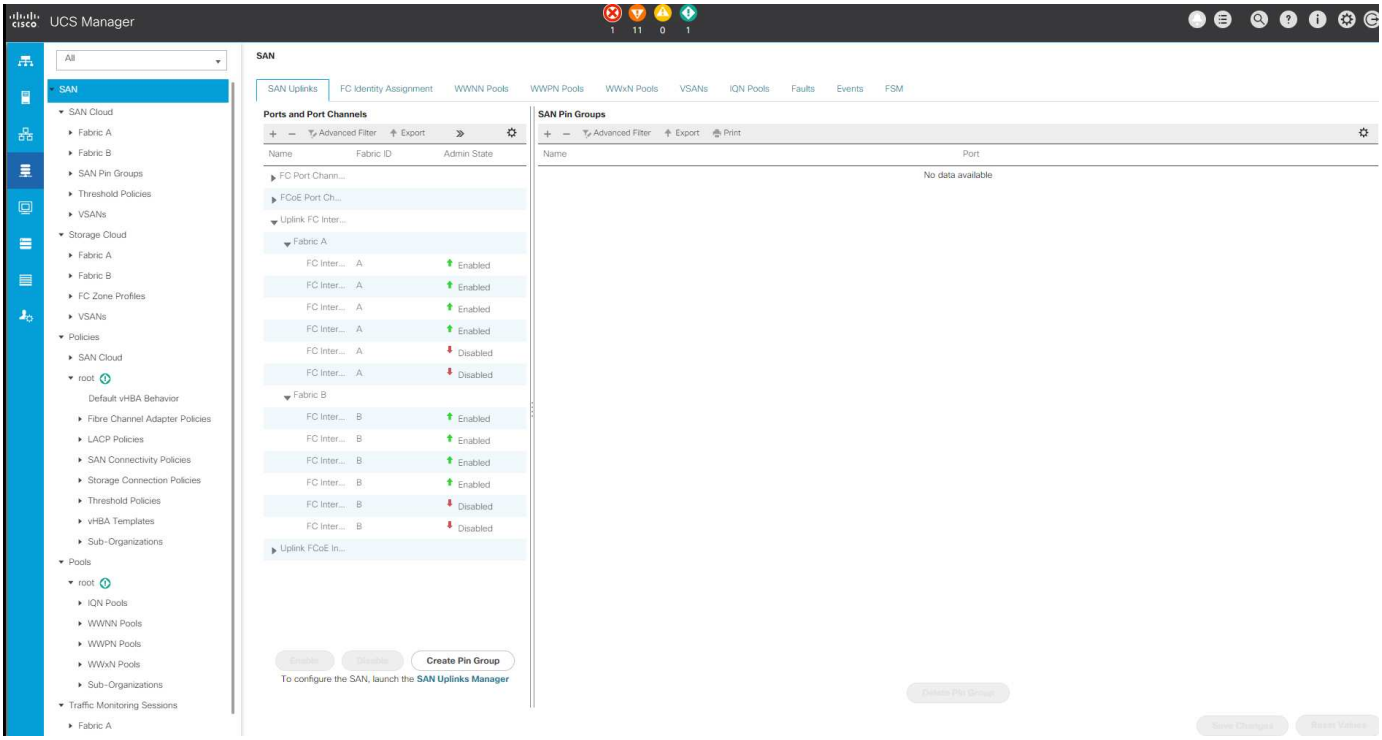
Mit Cisco UCS können Sie als MEDITECH-Kunde Ihre Fachexperten für Netzwerk-, Speicher- und Computing-Ressourcen optimal nutzen, um Richtlinien und Vorlagen zu erstellen, die auf Ihre spezifischen Anforderungen

abgestimmt sind. Nach ihrer Erstellung können diese Richtlinien und Vorlagen in Serviceprofilen zusammengefasst werden, die für konsistente, wiederholbare, zuverlässige und schnelle Implementierungen von Cisco Blade- und Rack-Servern sorgen.

Cisco UCS bietet drei Methoden zum Managen eines Cisco UCS-Systems, einer sogenannten Domäne:

- Cisco UCS Manager HTML5-GUI
- Cisco UCS CLI
- Cisco UCS Central für Umgebungen mit mehreren Domänen

Die folgende Abbildung zeigt einen Beispiel-Screenshot des SAN Node im Cisco UCS Manager.



In größeren Implementierungen können unabhängige Cisco UCS-Domänen auf der Ebene der großen MEDITECH-funktionalen Komponenten für eine höhere Fehlertoleranz ausgelegt werden.

Bei hochfehlertoleranten Designs mit zwei oder mehr Rechenzentren spielt Cisco UCS Central eine zentrale Rolle bei der Festlegung globaler Richtlinien und globaler Serviceprofile, die für eine konsistente Konsistenz zwischen den Hosts im gesamten Unternehmen sorgen.

Um die Cisco UCS Computing-Plattform einzurichten, gehen Sie die folgenden Verfahren vor. Führen Sie diese Verfahren durch, nachdem die Cisco UCS B200 M5 Blade Server im Cisco UCS 5108 AC Blade-Chassis installiert wurden. Zudem müssen Sie mit den Verkabelungsanforderungen konkurrieren, wie in beschrieben "Verkabelungsdiagramm" Abschnitt.

1. Aktualisieren Sie die Cisco UCS Manager Firmware auf Version 3.2(2f) oder höher.
2. Konfigurieren Sie die Berichterstellung, die Cisco „Call Home“-Funktionen und die NTP-Einstellungen für die Domäne.
3. Konfigurieren Sie die Server- und Uplink-Ports auf jedem Fabric Interconnect.
4. Bearbeiten Sie die Richtlinie zur Chassis-Erkennung.
5. Erstellen Sie die Adresspools für Out-of-Band-Management, Universal Unique Identifier (UUIDs), MAC-

Adresse, Server, den weltweiten Node-Namen (WWNN) und den weltweiten Port-Namen (WWPN).

6. Erstellen Sie die Ethernet- und FC-Uplink-Port-Kanäle und VSANs.
7. Erstellen von Richtlinien für SAN-Konnektivität, Netzwerkkontrolle, Server-Pool-Qualifizierung, Energiekontrolle, Server-BIOS, Und Standardwartung.
8. VNIC- und vHBA-Vorlagen erstellen.
9. VMedia- und FC-Boot-Richtlinien erstellen
10. Erstellen von Serviceprofilvorlagen und Serviceprofilen für jedes MEDITECH-Plattformelement.
11. Ordnen Sie die Service-Profile den entsprechenden Blade-Servern zu.

Die detaillierten Schritte zur Konfiguration der einzelnen Schlüsselelemente der Cisco UCS-Serviceprofile für FlexPod finden Sie im "FlexPod Datacenter with Fibre Channel Storage using VMware vSphere 6.5 Update 1, NetApp AFF A-Series and Cisco UCS Manager 3.2"CVD-Dokument.

"Als Nächstes: Best Practices für ESXi Konfiguration."

Best Practices für die ESXi Konfiguration

Konfigurieren Sie für die ESXi Host-seitige Konfiguration die VMware-Hosts so, wie es bei jedem Enterprise-Datenbank-Workload ausgeführt wird:

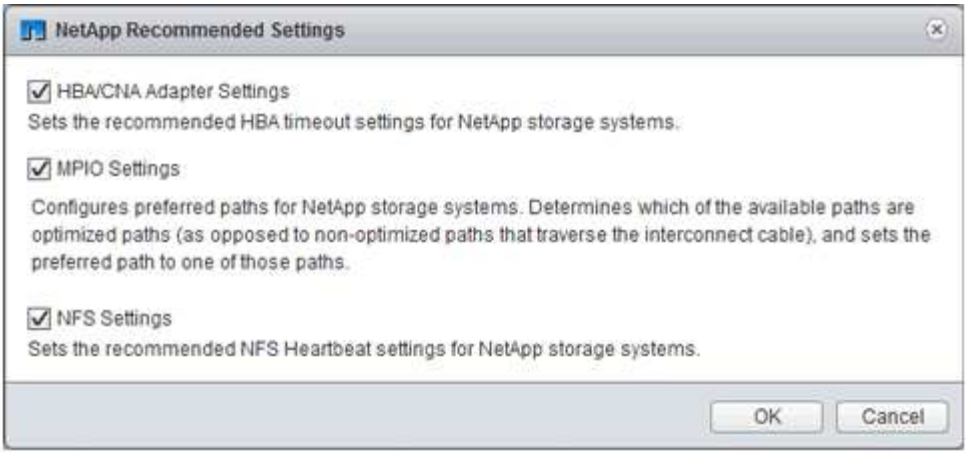
- VSC für VMware vSphere überprüft und legt die Einstellungen für das Multipathing des ESXi Hosts und die HBA-Zeitüberschreitungseinstellungen fest, die für NetApp Storage-Systeme am besten geeignet sind. Die VSC-Werte basieren auf strengen internen Tests von NetApp.
- Für eine optimale Storage-Performance sollten Sie in Betracht ziehen, Storage-Hardware zu nutzen, die VMware vStorage APIs – Array Integration (VAAI) unterstützt. Das NetApp Plug-in für VAAI ist eine Software-Bibliothek, in der die VMware Virtual Disk Libraries integriert sind, die auf dem ESXi Host installiert sind. Das Paket VMware VAAI ermöglicht die Auslagerung bestimmter Aufgaben von den physischen Hosts an das Storage Array.

  Aufgaben wie Thin Provisioning und Hardwarebeschleunigung können auf Array-Ebene ausgeführt werden, um die Workloads auf den ESXi Hosts zu verringern. Die Funktion zum Offload und zur Speicherplatzreservierung verbessern die Performance des VSC-Betriebs. Sie können das Plug-in-Installationspaket herunterladen und Anweisungen zum Installieren des Plug-ins von der NetApp Support Website erhalten.

  VSC legt ESXi Host-Timeouts, Multipath-Einstellungen und HBA-Zeitüberschreitungseinstellungen und andere Werte fest, um für optimale Performance und erfolgreiches Failover der NetApp Storage Controller zu sorgen. Führen Sie hierzu folgende Schritte aus:

  a. Wählen Sie auf der Startseite von VMware vSphere Web Client die Option vCenter > Hosts aus.
  b. Klicken Sie mit der rechten Maustaste auf einen Host, und wählen Sie dann Aktionen > NetApp VSC > Empfohlene Werte festlegen aus.
  c. Wählen Sie im Dialogfeld „Empfohlene Einstellungen von NetApp“ die Werte aus, die für Ihr System am besten geeignet sind.

     Standardmäßig werden die empfohlenen Standardwerte festgelegt.



a. Klicken Sie auf OK.

"Weiter: NetApp Konfiguration."

NetApp Konfiguration

Der NetApp Storage, der für MEDITECH-Softwareumgebungen implementiert wird, verwendet Storage-Controller in einer hochverfügbaren Paarkonfiguration. Speicher muss von beiden Controllern über das FC-Protokoll an MEDITECH-Datenbankserver übertragen werden. Die Konfiguration stellt den Storage beider Controller bereit, um die Applikationslast im normalen Betrieb gleichmäßig zu verteilen.

ONTAP-Konfiguration

In diesem Abschnitt werden ein Beispiel für die Implementierung und die Bereitstellung beschrieben, die die entsprechenden ONTAP Befehle verwenden. Der Schwerpunkt liegt dabei auf der Nutzung von Storage für die Implementierung des von NetApp empfohlenen Storage Layouts, in dem ein hochverfügbares Controller-Paar verwendet wird. Einer der größten Vorteile von ONTAP ist die Möglichkeit zur horizontalen Skalierung ohne Beeinträchtigungen der vorhandenen Hochverfügbarkeitspaare.

ONTAP-Lizenzen

Nach der Einrichtung der Storage Controller wenden Sie Lizenzen an, um die von NetApp empfohlenen ONTAP Funktionen zu aktivieren. Die Lizenzen für MEDITECH Workloads sind FC, CIFS, und NetApp Snapshot, SnapRestore, FlexClone, Und SnapMirror Technologien.

Zum Konfigurieren von Lizenzen öffnen Sie NetApp ONTAP System Manager, gehen Sie zu Configuration-Licenses und fügen dann die entsprechenden Lizenzen hinzu.

Alternativ können Sie mit dem folgenden Befehl Lizenzen über die CLI hinzufügen:

```
license add -license-code <code>
```

AutoSupport-Konfiguration

Das NetApp AutoSupport Tool sendet zusammenfassende Support-Informationen über HTTPS an NetApp. Führen Sie zum Konfigurieren von AutoSupport die folgenden ONTAP-Befehle aus:

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

Konfiguration für die Hardware-gestützte Übernahme

Aktivieren Sie auf jedem Node die Hardware-gestützte Übernahme, um die für die Initiierung einer Übernahme benötigte Zeit im unwahrscheinlichen Fall eines Controller-Ausfalls zu minimieren. Gehen Sie wie folgt vor, um die Hardware-gestützte Übernahme zu konfigurieren:

1. Führen Sie den folgenden ONTAP-Befehl an xxx aus.

   Setzen Sie die Partneraddress-Option auf die IP-Adresse des Management-Ports für `prod1-01`.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. Führen Sie den folgenden ONTAP-Befehl an xxx aus:

   Setzen Sie die Partneraddress-Option auf die IP-Adresse des Management-Ports für `cluster1-02`.

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. Führen Sie den folgenden ONTAP-Befehl aus, um die Hardware-gestützte Übernahme auf beiden zu aktivieren `prod1-01` Und das `prod1-02` HA-Controller-Paar.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"Als Nächstes: Aggregat-Konfiguration."

Konfiguration von Aggregaten

NetApp RAID DP

NetApp empfiehlt NetApp RAID DP Technologie als RAID-Typ für alle Aggregate in einem NetApp FAS oder AFF System, einschließlich regulärer NetApp Flash Pool Aggregate. Die MEDITECH-Dokumentation kann die Verwendung von RAID 10 angeben, MEDITECH hat jedoch die Verwendung von RAID DP genehmigt.

Größe und Anzahl der RAID-Gruppen

Die standardmäßige RAID-Gruppengröße ist 16. Diese Größe ist möglicherweise nicht optimal für die Aggregate für die MEDITECH Hosts auf Ihrer spezifischen Website. Informationen zur Anzahl der Festplatten, die NetApp empfiehlt, in einer RAID-Gruppe zu verwenden, finden Sie unter "NetApp TR-3838: Konfigurationsleitfaden für Storage-Subsysteme".

Die RAID-Gruppengröße ist für die Storage-Erweiterung wichtig, da NetApp empfiehlt, Festplatten zu einem Aggregat mit einer oder mehreren Festplattengruppen hinzuzufügen, die der RAID-Gruppengröße entsprechen. Die Anzahl der RAID-Gruppen hängt von der Anzahl der Datenfestplatten und der Größe der RAID-Gruppen ab. Verwenden Sie das Sizing Tool NetApp System Performance Modeler (SPM), um die Anzahl der benötigten Datendisks zu bestimmen. Nachdem Sie die Anzahl der Datenfestplatten bestimmt haben, passen Sie die RAID-Gruppengröße an, um die Anzahl der Parity-Festplatten im empfohlenen Bereich für RAID-Gruppengröße pro Festplattentyp zu minimieren.

Einzelheiten zur Verwendung des SPM-Dimensionierungstools für MEDITECH-Umgebungen finden Sie unter "NetApp TR-4190: NetApp Sizing Guidelines for MEDITECH Environments".

Überlegungen zur Storage-Erweiterung

Wenn Sie Aggregate mit mehr Festplatten erweitern, fügen Sie die Festplatten in Gruppen hinzu, die der aggregierten RAID-Gruppengröße entsprechen. Der nachfolgende Ansatz sorgt für konsistente Performance im gesamten Aggregat.

Beispiel: Wenn Sie einem Aggregat Storage hinzufügen möchten, das mit einer RAID-Gruppengröße von 20 erstellt wurde, empfiehlt NetApp die Anzahl der Festplatten, eine oder mehrere Gruppen mit 20 Festplatten hinzuzufügen. Also sollten Sie 20, 40, 60 usw. Festplatten hinzufügen.

Nach der Erweiterung von Aggregaten können Sie die Performance verbessern, indem Sie Neuzuweisung-Aufgaben auf den betroffenen Volumes oder Aggregaten ausführen, um vorhandene Daten-Stripes auf die neuen Festplatten zu verteilen. Diese Aktion ist hilfreich, insbesondere wenn das bestehende Aggregat fast voll war.

> Die Neuzuweisung von Zeitplänen sollte während der nicht produktiven Zeit geplant werden, da es sich um eine äußerst CPU- und festplattenbasierte Aufgabe handelt.

Weitere Informationen zur Verwendung der Neuzuordnung nach einer Aggregaterweiterung finden Sie unter "NetApp TR-3929: Reallocate Best Practices Guide".

Snapshot Kopien auf Aggregatebene

Setzen Sie die NetApp Snapshot Kopie-Reserve auf Aggregatebene auf null und deaktivieren Sie den standardmäßigen Snapshot Zeitplan für das Aggregat. Löschen Sie gegebenenfalls vorhandene Snapshot Kopien auf Aggregatebene.

"Weiter: Konfiguration Von Storage Virtual Machines."

Konfiguration von Storage Virtual Machines

Dieser Abschnitt bezieht sich auf die Implementierung auf ONTAP 8.3 und höher.

> Storage Virtual Machine (SVM) wird auch als Vserver in der ONTAP API und in der ONTAP CLI bezeichnet.

SVM für MEDITECH-Host-LUNs

Sie sollten eine dedizierte SVM pro ONTAP-Storage-Cluster erstellen, um die Aggregate zu besitzen und zu verwalten, die die LUNs für MEDITECH-Hosts enthalten.

Festlegung der Sprachcodierung für SVM

NetApp empfiehlt, die Sprachkodierung für alle SVMs festzulegen. Wenn zum Zeitpunkt des Erstellens der SVM keine Sprachkodiereinstellung angegeben ist, wird die Standardeinstellung für die Sprachkodierung verwendet. Die Standardeinstellung für die Sprachkodierung ist C.UTF-8 für ONTAP. Nachdem die Sprachcodierung festgelegt wurde, können Sie die Sprache einer SVM mit Infinite Volume später nicht mehr ändern.

Die Volumes, die der SVM zugeordnet sind, übernehmen die Einstellung für die SVM-Sprachkodierung, es sei denn, Sie geben bei der Erstellung der Volumes eine andere Einstellung an. Damit bestimmte Vorgänge funktionieren, sollten Sie die Einstellung für die Sprachkodierung in allen Volumes für Ihre Site konsistent verwenden. Beispielsweise muss bei SnapMirror die Quell- und Ziel-SVM über dieselbe Einstellung für die Sprachkodierung verfügen.

"Weiter: Volume-Konfiguration."

Konfiguration von Volumes

Volume-Provisionierung

MEDITECH-Volumes, die für MEDITECH-Hosts dediziert sind, können entweder dick sein oder über Thin Provisioning verfügen.

Standardmäßige Snapshot Kopien auf Volume-Ebene

Snapshot Kopien werden im Rahmen des Backup-Workflows erstellt. Jede Snapshot-Kopie kann verwendet werden, um zu unterschiedlichen Zeiten auf die in den MEDITECH LUNs gespeicherten Daten zuzugreifen. Die MEDITECH- genehmigte Backuplösung erstellt auf Grundlage dieser Snapshot-Kopien Thin-Provisioning-FlexClone-Volumes, um zeitpunktgenaue Kopien der MEDITECH-LUNs zu erstellen. Die MEDITECH-Umgebung ist in eine geprüfte Backup-Softwarelösung integriert. Daher empfiehlt NetApp, den Zeitplan für die Snapshot-Kopie in jedem der NetApp-FlexVol-Volumes zu deaktivieren, aus denen die MEDITECH-Produktionsdatenbank-LUNs bestehen.

Wichtig: FlexClone Volumes teilen sich den Platz des übergeordneten Datenträgers. Daher ist es wichtig, dass das Volume genügend Platz für die MEDITECH Daten-LUNs und die FlexClone Volumes hat, die die Backup-Server erstellen. FlexClone Volumes belegen in der Art und Weise, wie Daten-Volumes es tun, keinen zusätzlichen Speicherplatz. Wenn es jedoch in kurzer Zeit große Löschungen auf den MEDITECH LUNs gibt, könnten die Klon-Volumes wachsen.

Anzahl der Volumes pro Aggregat

Bei einem NetApp FAS-System, das Flash Pool oder NetApp Flash Cache Caching nutzt, empfiehlt NetApp die Bereitstellung von drei oder mehr Volumes pro Aggregat, die speziell zum Speichern des MEDITECH-Programms, des Wörterbuchs und von Datendateien verwendet werden.

Für AFF Systeme empfiehlt NetApp, vier oder mehr Volumes pro Aggregat zum Speichern des MEDITECH-Programms, des Wörterbuchs und der Datendateien einzurichten.

Umplanungszeitplan auf Volume-Ebene

Das Datenlayout des Speichers wird im Laufe der Zeit weniger optimal, insbesondere wenn es von schreibintensiven Workloads wie den Plattformen MEDITECH Expanse, 6.x und C/S 5.x genutzt wird. Im Laufe der Zeit kann diese Situation die Latenz beim sequenziellen Lesen erhöhen, was zum Abschluss des Backups führt. Schlechtes Daten-Layout oder Fragmentierung kann auch die Schreiblatenz beeinträchtigen. Die Neuzuordnung auf Volume-Ebene optimiert das Layout von Daten auf der Festplatte, um Schreiblatenzen und sequenziellen Lesezugriff zu verbessern. Das verbesserte Storage-Layout ermöglicht das Abschließen des Backups innerhalb des zugewiesenen Zeitfensters von 8 Stunden.

Best Practices in sich
NetApp empfiehlt zumindest die Implementierung eines wöchentlichen Volume-Neuzuweisungsplans, um Neuzuweisungen während der zugewiesenen Wartungsausfälle oder außerhalb der Stoßzeiten an einem Produktionsstandort durchzuführen. NetApp empfiehlt dringend, die Neuzuweisung-Aufgabe auf einem Volume gleichzeitig pro Controller auszuführen.

Weitere Informationen zum Bestimmen eines geeigneten Zeitplans für die Neuzuordnung von Volumes für Ihren Produktionsdatenbank-Storage finden Sie in Abschnitt 3.12 in "NetApp TR-3929: Reallocate Best Practices Guide". Dieser Abschnitt hilft Ihnen auch dabei, einen wöchentlichen Zeitplan für die Neuzuordnung einer überlasteten Site zu erstellen.

"Weiter: LUN-Konfiguration."

LUN-Konfiguration

Die Anzahl der MEDITECH-Hosts in Ihrer Umgebung bestimmt die Anzahl der LUNs, die innerhalb des NetApp FAS oder AFF-Systems erstellt wurden. Das Angebot für die Hardwarekonfiguration gibt die Größe jeder LUN an.

LUN Provisioning

MEDITECH LUNs, die für MEDITECH-Hosts dediziert sind, können entweder dick sein oder über Thin Provisioning verfügen.

Der LUN-Betriebssystem-Typ

Um die erstellten LUNs ordnungsgemäß auszurichten, müssen Sie den Betriebssystemtyp für die LUNs korrekt festlegen. Falsch ausgerichtete LUNs verursachen keinen unnötigen Schreibaufwand und es ist kostspielig, eine falsch ausgerichtete LUN zu korrigieren.

Der MEDITECH-Hostserver läuft normalerweise in der virtualisierten Windows-Server-Umgebung unter Verwendung des VMware vSphere-Hypervisors. Der Host-Server kann auch in der Windows Server-Umgebung auf einem Bare-Metal-Server ausgeführt werden. Informationen zum ermitteln des richtigen eingestellten Betriebssystemtyps finden Sie im Abschnitt „LUN erstellen“ von "Befehle für Clustered Data ONTAP 8.3: Manuelle Seitenreferenz".

Die LUN-Größe

Informationen zur Ermittlung der LUN-Größe für jeden MEDITECH-Host finden Sie im Dokument Hardware Configuration Proposal (New Deployment) oder in dem Dokument Hardware Evaluation Task (Existing

Deployment) von MEDITECH.

LUN-Präsentation

MEDITECH verlangt, dass die Speicherung von Programm-, Wörterbuch- und Datendateien auf MEDITECH-Hosts mithilfe des FC-Protokolls als LUNs dargestellt wird. In der virtuellen VMware Umgebung werden die LUNs den VMware ESXi-Servern präsentiert, die die MEDITECH-Hosts hosten. Dann ist jede LUN, die dem VMware ESXi Server präsentiert wird, jeder MEDITECH-Host-VM zugeordnet, indem sie RDM im physischen Kompatibilitätsmodus verwendet.

Sie sollten die LUNs den MEDITCH-Hosts präsentieren, indem Sie die richtigen LUN-Namenskonventionen verwenden. Beispielsweise müssen Sie zur einfachen Administration die LUN vorlegen `MTFS01E` An den MEDITECH-Gastgeber `mt-host-01`.

Wenn Sie den MEDITECH-Installer konsultieren, um eine konsistente Namenskonvention für die LUNs zu entwickeln, die die MEDITECH-Hosts nutzen, finden Sie in dem Vorschlag zur Hardwarekonfiguration von MEDITECH.

Ein Beispiel für einen MEDITECH-LUN-Namen ist `MTFS05E`, In denen:

- `MTFS` Bezeichnet den MEDITECH-Dateiserver (für den MEDITECH-Host).
- `05` Gibt die Host-Nummer an 5.
- `E` Bezeichnet das Windows E-Laufwerk.

"Weiter: Konfiguration Der Initiatorgruppe."

Konfiguration der Initiatorgruppe

Wenn Sie FC als Datennetzwerkprotokoll verwenden, erstellen Sie zwei Initiatorgruppen auf jedem Storage Controller. Die erste Initiatorgruppe enthält die WWPNs der FC-Host-Schnittstellenkarten auf den VMware ESXi Servern, die die MEDITECH-Host-VMs (iGroup für MEDITECH) hosten.

Sie müssen den Betriebssystemtyp der MEDITECH igroup entsprechend dem Umgebungseinstellungen festlegen. Beispiel:

- Verwenden Sie den Betriebssystemtyp der Initiatorgruppe `Windows` Für Applikationen, die auf Bare-Metal-Server-Hardware in einer Windows Server-Umgebung installiert sind.
- Verwenden Sie den Betriebssystemtyp der Initiatorgruppe `VMware` Für Applikationen, die mit dem VMware vSphere Hypervisor virtualisiert werden

> Der Betriebssystemtyp für eine Initiatorgruppe unterscheidet sich möglicherweise vom Betriebssystem für eine LUN. Beispielsweise sollten Sie für virtualisierte MEDITECH-Hosts den Betriebssystemtyp der Initiatorgruppe auf festlegen `VMware`. Für die LUNs, die von den virtualisierten MEDITECH-Hosts verwendet werden, sollten Sie den Betriebssystemtyp auf einstellen `Windows 2008 or later`. Verwenden Sie diese Einstellung, da das MEDITECH-Host-Betriebssystem die Windows Server 2008 R2 64-Bit Enterprise Edition ist.

Um den korrekten Wert für den Betriebssystemtyp zu ermitteln, finden Sie in den Abschnitten „LUN iGroup Create“ und „LUN Create“ im "Befehle für Clustered Data ONTAP 8.2: Manuelle Seitenreferenz".

"Danach LUN-Zuordnungen."

LUN-Zuordnungen

LUN-Zuordnungen für die MEDITECH-Hosts werden erstellt, wenn die LUNs erstellt sind.

MEDITECH Module und Komponenten

Die MEDITECH-Anwendung deckt mehrere Module und Komponenten ab. In der folgenden Tabelle sind die Funktionen aufgeführt, die von diesen Modulen abgedeckt werden. Weitere Informationen zum Einrichten und Bereitstellen dieser Module finden Sie in der MEDITECH-Dokumentation.

Funktion	Typ
Konnektivität	• Web-Server • Live-Anwendungsserver (WI – Web-Integration) • Anwendungsserver testen (WI) • SAML-Authentifizierungsserver (WI) • SAML-Proxy-Server (WI) • Datenbankserver
Infrastruktur	• File Server • Job-Client Im Hintergrund • Verbindungsserver • Transaktionsserver
Scannen und Archivierung	• Image Server
Daten-Repository	• SQL Server geschult sind
Geschäftliche und klinische Analysen	• Live Intelligence Server (BCA) • Test Intelligence Server (BCA) • Datenbankserver (BCA)

Funktion	Typ
Häuslichen Pflege	• Lösung für Remote-Standorte • Konnektivität • Infrastruktur • Drucken • Feldgeräte • Scannen • Anforderungen an den gehosteten Standort • Firewall-Konfiguration
Unterstützung	• Job-Client im Hintergrund (CALs – Client Access License)
Benutzergeräte	• Tablets • Feste Geräte
Drucken	• Live-Netzwerk-Druckserver (erforderlich; möglicherweise bereits vorhanden) • Netzwerk-Druckserver testen (erforderlich; möglicherweise bereits vorhanden)
Anforderungen Dritter	• First Databank (FDB) MedKnowledge Framework v4.3

Danksagungen

Die folgenden Personen haben zur Erstellung dieses Leitfadens beigetragen.

- Brandon Agee, Technical Marketing Engineer, NetApp
- Atul Bhalodia, Technical Marketing Engineer, NetApp
- Ketan Mota, Senior Product Manager, NetApp
- John Duignan, Solutions Architect – Gesundheitswesen, NetApp
- Jon Ebmeier, Cisco
- Mike Brennan, Cisco

Wo Sie weitere Informationen finden

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

FlexPod-Designzone

- "FlexPod-Designzone"

- "FlexPod Datacenter mit FC Storage (MDS Switches) mit NetApp AFF, vSphere 6.5U1 und Cisco UCS Manager"

Technische Berichte von NetApp

- "TR-3929: Reallocate Best Practices Guide"
- "TR-3987: Snap Creator Framework Plug-in für InterSystems Caché"
- "TR-4300i: NetApp FAS and All-Flash-Storage-Systeme for MEDITECH Environments Best Practices Guide"
- "TR-4017: FC SAN Best Practices"
- "TR-3446: SnapMirror Async Overview and Best Practices Guide"

ONTAP-Dokumentation

- "NetApp Produktdokumentation"
- "Dokumentation zu Virtual Storage Console (VSC) für vSphere"
- "ONTAP 9 Dokumentationszentrum":
  - "FC Express Guide für ESXi"
- "Dokumentation zu ONTAP 9.3":
  - "Software Setup Guide"
  - "Festplatten und Aggregate Power Guide"
  - "SAN-Administration-Leitfaden"
  - "SAN-Konfigurationsleitfaden"
  - "FC Configuration for Windows Express Guide"
  - "FC SAN Optimized AFF Setup Guide"
  - "High-Availability Configuration Guide Beschrieben"
  - "Logischer Storage-Management-Leitfaden"
  - "Performance Management Power Guide"
  - "SMB/CIFS Configuration Power Guide"
  - "SMB/CIFS-Referenz"
  - "Data Protection Power Guide"
  - "Leitfaden zur Datensicherheit mittels Tape-Backup und -Recovery"
  - "NetApp Encryption Power Guide"
  - "Netzwerk-Management-Leitfaden"
  - "Befehle: Handbuch Seitenreferenz für ONTAP 9.3"

Leitfäden zu Cisco Nexus, MDS, Cisco UCS und Cisco UCS Manager

- "Cisco UCS Server – Übersicht"
- "Übersicht über Cisco UCS Blade Server"
- "Cisco UCS B200 M5 Datenblatt"

- "Cisco UCS Manager – Übersicht"
- "Cisco UCS Manager 3.2 (3a) – Infrastrukturpaket" (Erfordert Cisco.com Autorisierung)
- "Switches Der Cisco Nexus 9300 Plattform"
- "Cisco MDS 9132T FC Switch"

FlexPod für die medizinische Bildverarbeitung

TR-4865: FlexPod für die medizinische Bildgebung

Jaya Kishore Esanakula und Atul Bhalodia, NetApp

Medizinische Bildverarbeitung macht 70 % aller Daten aus, die von Unternehmen im Gesundheitswesen generiert werden. Da die digitalen Modalitäten weiter vorankommen und neue Modalitäten entstehen, wird die Datenmenge weiter zunehmen. Beispielsweise erhöht der Übergang von analoger zu digitaler Pathologie die Bildgröße drastisch, und zwar mit einer Geschwindigkeit, die alle aktuell vorhandenen Strategien zur Datenverwaltung in Frage stellt.

COVID-19 hat die digitale Transformation klar umgestaltet, so eine jüngste "Bericht", COVID-19 hat den digitalen Handel um 5 Jahre beschleunigt. Die technologische Innovation, die durch Problemlöser angetrieben wird, verändert grundlegend die Art und Weise, wie wir unseren Alltag umsetzen. Dieser technologische Wandel wird viele wichtige Aspekte unseres Lebens, einschließlich des Gesundheitswesens, überholt.

Das Gesundheitswesen wird sich in den kommenden Jahren noch weiter verändern. COVID beschleunigt Innovationen im Gesundheitswesen, die die Branche mindestens mehrere Jahre voranbringen. Im Mittelpunkt dieser Veränderung steht die Notwendigkeit, die Gesundheitsversorgung flexibler im Umgang mit Pandemien zu gestalten, indem sie erschwinglicher, verfügbarer und zugänglicher ist, ohne die Zuverlässigkeit zu beeinträchtigen.

Die Grundlage dieses Wandels im Gesundheitswesen ist eine gut konzipierte Plattform. Eines der wichtigsten Messgrößen für die Plattform ist die einfache Implementierung von Plattformänderungen. Die Geschwindigkeit ist die neue Größenordnung und die Datensicherung kann nicht gefährdet werden. Einige der weltweit wichtigsten Daten werden von den klinischen Systemen erstellt und genutzt, die das Klinikteam unterstützen. NetApp hat kritische Daten in der Patientenversorgung vor Ort, vor Ort, in der Cloud oder in einem hybriden Umfeld zur Verfügung gestellt. Hybride Multi-Cloud-Umgebungen sind der derzeitige Stand der TECHNIK in BEZUG AUF IT-Architekturen.

Das Gesundheitswesen dreht sich, wie wir wissen, um Anbieter (Ärzte, Krankenschwestern, Radiologen, Techniker für medizinische Geräte usw.) und Patienten. Während wir Patienten und Anbieter enger zusammenbringen und der geografische Standort lediglich zu einem Datenpunkt wird, ist es für die zugrunde liegende Plattform noch wichtiger, verfügbar zu sein, wenn Anbieter und Patienten ihn benötigen. Die Plattform muss langfristig effizient und kostengünstig sein. Bei ihren Bemühungen, die Kosten für die Patientenversorgung noch weiter zu senken, "Rechenschaftspflichtige Versorgungsorganisationen" (ACOS) würde durch eine effiziente Plattform ermöglicht.

Bei Gesundheitsinformationssystemen, die von Gesundheitseinrichtungen genutzt werden, gibt es in der Frage des Build- oder Kaufs häufig eine einzige Antwort: Den Kauf. Das könnte aus vielen subjektiven Gründen sein. Über viele Jahre getroffene Kaufentscheidungen können heterogene Informationssysteme verursachen. Jedes System verfügt über bestimmte Anforderungen für die Plattform, auf der sie implementiert werden. Das größte Problem ist die große Vielfalt an Storage-Protokollen und Leistungsstufen, die Informationssysteme benötigen. Deshalb stellt die Plattformstandardisierung und eine optimale betriebliche Effizienz eine große

Herausforderung dar. Gesundheitseinrichtungen können sich nicht auf geschäftskritische Fragen konzentrieren, weil ihre Aufmerksamkeit durch triviale betriebliche Bedürfnisse wie die großen Plattformen, die ein vielfältiges Spektrum an Fähigkeiten und damit KMU-Bindung erfordern, noch viel zu hoch verteilt wird.

Die Herausforderungen lassen sich in folgende Kategorien einteilen:

- Heterogene Storage-Anforderungen
- Abteilungssilos
- Komplexität von IT-Abläufen
- Cloud-Konnektivität
- Cyber-Sicherheit
- Künstliche Intelligenz und Deep Learning

FlexPod bietet eine einzige Plattform, die FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS usw. von einer einzigen Plattform aus unterstützt. Mitarbeiter, Prozesse und Technologie sind Teil der DNA, die FlexPod entwickelt und darauf baut. FlexPod Adaptive QoS hilft bei der Auflösung der Abteilungssilos, indem mehrere geschäftskritische klinische Systeme auf derselben zugrunde liegenden FlexPod Plattform unterstützt werden. FlexPod ist FedRAMP-zertifiziert und nach FIPS 140-2 zertifiziert. Darüber hinaus sehen sich Einrichtungen im Gesundheitswesen unter anderem mit künstlicher Intelligenz und Deep Learning konfrontiert. FlexPod und NetApp meistern diese Herausforderungen und sorgen dafür, dass die Daten lokal oder in einer hybriden Multi-Cloud-Umgebung in einer standardisierten Plattform verfügbar sind. Weitere Informationen und eine Reihe von Kundenreferenzen finden Sie unter "FlexPod Gesundheitswesen".

Typische Informationen zur medizinischen Bildgebung und PACS-Systeme verfügen über die folgenden Funktionen:

- Empfang und Anmeldung
- Planung
- Bildgebung
- Transkription
- Vereinfachtes
- Datenaustausch
- Bildarchiv
- Bildanzeige für die Bildaufnahme und das Lesen von Bildern für Techniker und Bildanzeige für Kliniker

Was die Bildgebung betrifft, versucht der Gesundheitsbereich, die folgenden klinischen Herausforderungen zu lösen:

- Breitere Akzeptanz von "Natürliche Sprachverarbeitung" (NLP)-Assistenten von Technikern und Ärzten für Bildlesung. Die Röntgenabteilung kann von der Spracherkennung profitieren, um Berichte zu transkribieren. NLP kann zur Identifizierung und Anonymisierung der Patientenakte verwendet werden, insbesondere DICOM-Tags, die im DICOM-Bild eingebettet sind. NLP-Funktionen erfordern leistungsstarke Plattformen mit Reaktionszeiten mit niedriger Latenz für die Bildverarbeitung. FlexPod QoS bietet nicht nur Bereitstellung und Performance, sondern bietet auch ausgereifte Kapazitätsprognosen für zukünftiges Wachstum.
- Breitere Einführung standardisierter klinischer Behandlungspfade und Protokolle durch ACOs und kommunale Gesundheitsorganisationen. Bisher wurden klinische Behandlungspfade als statische Leitlinien verwendet und nicht als integrierter Workflow, der klinische Entscheidungen leitet. Dank der Fortschritte bei der NLP- und Bildverarbeitung können DICOM-Tags in Bilder als Fakten in klinische Behandlungspfade

integriert werden, um klinische Entscheidungen zu fördern. Daher erfordern diese Prozesse eine hohe Performance, niedrige Latenz und einen hohen Durchsatz von der zugrunde liegenden Infrastrukturplattform und den Storage-Systemen.

- ML-Modelle, die konvolutionelle neuronale Netze nutzen, ermöglichen die Automatisierung von Bildverarbeitungsfunktionen in Echtzeit und erfordern daher eine GPU-fähige Infrastruktur. FlexPod bietet sowohl die in dasselbe System integrierten CPU- als auch GPU-Compute-Komponenten und CPUs und GPUs können unabhängig voneinander skaliert werden.
- Wenn DICOM-Tags als Fakten in den Empfehlungen zu klinischen Best Practices verwendet werden, muss das System mehr Lesezugriffe auf DICOM-Artefakte mit niedriger Latenz und hohem Durchsatz durchführen.
- Bei der Auswertung von Bildern erfordert die Echtzeit-Zusammenarbeit zwischen Radiologen im gesamten Unternehmen eine hoch leistungsfähige Grafikverarbeitung auf den Endbenutzergeräten. NetApp bietet branchenführende VDI-Lösungen, die speziell für High-End-Grafikanwendungsfälle konzipiert und bewährt sind. Weitere Informationen finden Sie hier "Hier".
- Bild- und Medienmanagement in ACO Gesundheitsorganisationen können unabhängig vom Aufzeichnungssystem des Bildes eine einzige Plattform nutzen, indem sie Protokolle wie Digital Imaging und Communications in Medicine ("DICOM") Und Webzugriff auf DICOM-persistente Objekte ("WADO")
- Austausch von Gesundheitsinformationen ("HE") Enthält Bilder, die in Nachrichten eingebettet sind.
- Mobile Modalitäten wie Handheld-Geräte für drahtlose Scans (z. B. Handheld-Ultraschallscanner, die an ein Telefon angeschlossen sind) erfordern eine robuste Netzwerkinfrastruktur mit Sicherheit, Zuverlässigkeit und Latenz auf DoD-Ebene am Edge, im Core und in der Cloud. "Eine Data-Fabric-Strategie von NetApp" Unternehmen können diese Fähigkeit im gewünschten Umfang bereitstellen.
- Neuere Modalitäten haben einen exponentiellen Speicherbedarf. Zum Beispiel benötigen CT und MRI für jede Modalität ein paar hundert MBs, aber digitale pathologische Bilder (einschließlich ganzer Dias-Bildgebung) können ein paar GBs groß sein. FlexPod ist entworfen mit "Performance, Zuverlässigkeit und Skalierbarkeit sind grundlegende Merkmale".

Eine gut konzipierte Plattform für medizinische Bildgebungsverfahren steht im Mittelpunkt der Innovation. Die FlexPod Architektur bietet flexible Computing- und Storage-Funktionen mit branchenführender Storage-Effizienz.

Gesamtvorteile der Lösung

Durch die Ausführung einer Applikations-Imaging-Umgebung auf der Basis der FlexPod-Architektur kann Ihr Unternehmen im Gesundheitswesen mit einer höheren Mitarbeiterproduktivität und geringeren Investitions- und Betriebskosten rechnen. FlexPod bietet eine umfassend getestete und vorab validierte konvergente Lösung, die entwickelt und für eine vorhersehbare Performance des Systems mit niedriger Latenz und Hochverfügbarkeit konzipiert wurde. Dieser Ansatz führt zu einem hohen Komfort und letztendlich zu optimalen Reaktionszeiten für die Anwender des medizinischen Bildgebungssystems.

Verschiedene Komponenten des Bildgebungssystems benötigen möglicherweise den Speicherplatz auf den Dateisystemen SMB/CIFS, NFS, Ext4 oder NTFS. Diese Anforderung bedeutet, dass die Infrastruktur Datenzugriff über NFS-, SMB/CIFS- und SAN-Protokolle bieten muss. Ein einziges NetApp Storage-System kann die NFS-, SMB/CIFS- und SAN-Protokolle unterstützen, sodass keine ältere Verwendung protokollspezifischer Storage-Systeme erforderlich ist.

Die FlexPod Infrastruktur ist eine modulare, konvergierte, virtualisierte, skalierbare (horizontal und vertikal skalierbare) und kostengünstige Plattform. Mit der FlexPod Plattform können Sie Computing-, Netzwerk- und Storage-Ressourcen unabhängig horizontal skalieren und so die Applikationsimplementierung beschleunigen. Und die modulare Architektur ermöglicht auch bei horizontale und Upgrades von Systemen einen unterbrechungsfreien Betrieb.

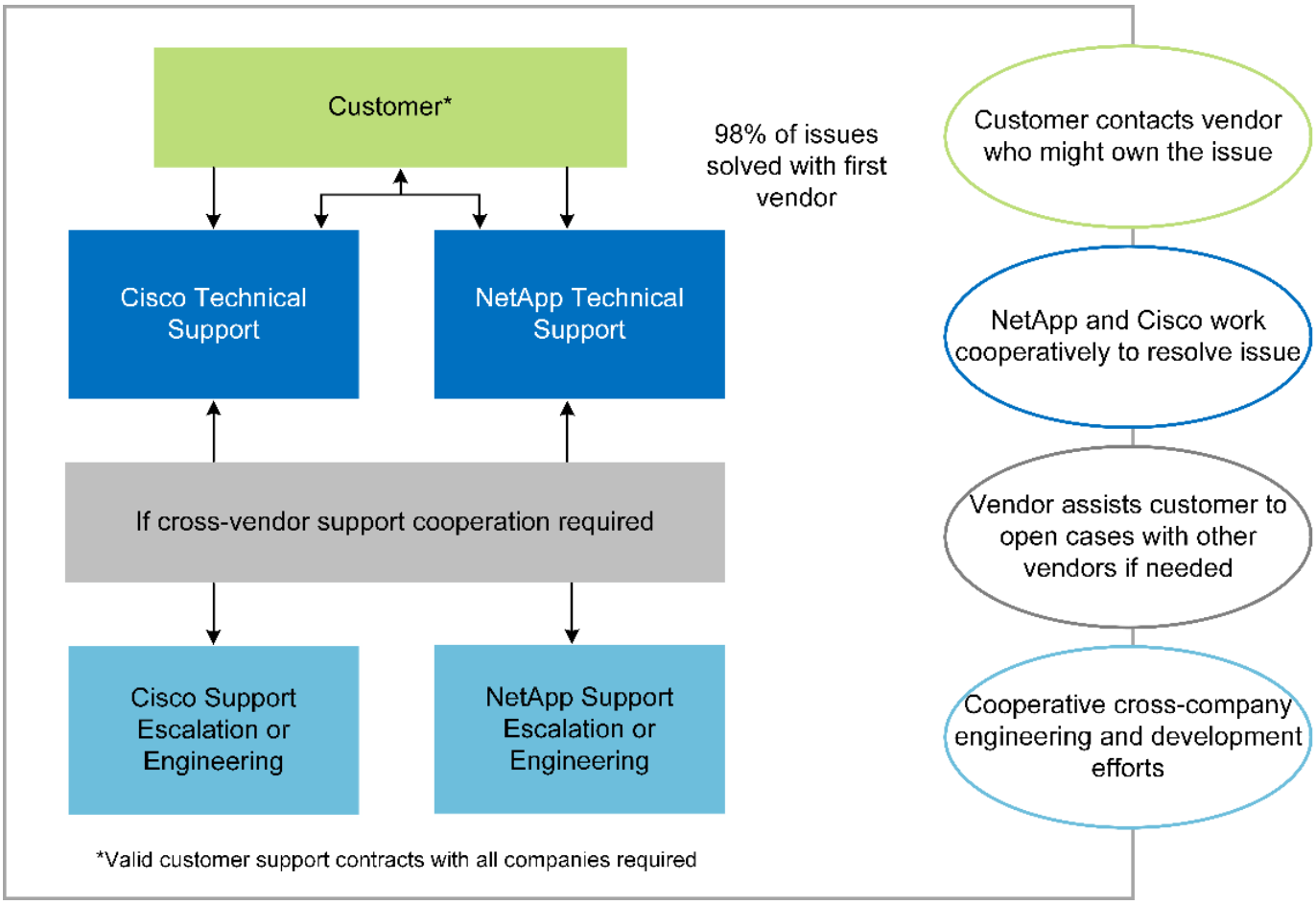
FlexPod bietet verschiedene für die medizinische Bildverarbeitung spezifische Vorteile:

- **System-Performance mit niedriger Latenz.** die Zeit der Radiologen ist eine Ressource mit hohem Wert, und die effiziente Nutzung der Zeit eines Radiologen ist von entscheidender Bedeutung. Wenn Sie warten, bis Bilder oder Videos geladen werden, kann dies zu einem Burnout des Arztes beitragen und die Effizienz des Arztes und die Patientensicherheit beeinträchtigen.
- **Modulare Architektur.** FlexPod Komponenten sind über einen Clustered Server, eine Storage Management Fabric und ein zusammenhängendes Management Toolset verbunden. Da die Bildungsinfrastruktur von Jahr zu Jahr wächst und die Zahl der Studien zunimmt, muss die zugrunde liegende Infrastruktur entsprechend skaliert werden. FlexPod ist in der Lage, Computing, Storage und Netzwerk unabhängig voneinander zu skalieren.
- **Schneller Einsatz der Infrastruktur.** ob in einem bestehenden Rechenzentrum oder an einem entfernten Standort – mit dem integrierten und geprüften Design von FlexPod Datacenter mit Medical Imaging ist die neue Infrastruktur mit weniger Aufwand in Betrieb.
- **Schnellere Applikationsimplementierung.** eine vorab validierte Architektur reduziert Integrationszeit und Risiken für jeden Workload. NetApp Technologie automatisiert die Infrastrukturimplementierung. Ganz gleich, ob Sie die Lösung für den ersten Rollout medizinischer Bildgebung, für eine Hardwareaktualisierung oder -Erweiterung einsetzen, Sie können mehr Ressourcen auf den geschäftlichen Nutzen des Projekts verlagern.
- **Vereinfachter Betrieb und niedrigere Kosten.** Sie können Ausgaben und Komplexität älterer proprietärer Plattformen vermeiden, indem Sie diese durch effizientere und skalierbarere gemeinsam genutzte Ressourcen ersetzen, die den dynamischen Anforderungen Ihrer Workloads gerecht werden. Diese Lösung bietet eine höhere Auslastung der Infrastrukturressourcen und somit einen höheren Return on Investment (ROI).
- **Scale-out-Architektur.** SAN und NAS können von Terabyte auf Petabyte im zweistelligen Bereich skaliert werden, ohne laufende Applikationen neu zu konfigurieren.
- **Unterbrechungsfreier Betrieb.** Storage-Wartungen, Hardware-Lebenszyklusoperationen und Software-Upgrades können ohne Unterbrechung des Geschäftsbetriebs durchgeführt werden.
- **Sichere Mandantenfähigkeit.** dieser Vorteil unterstützt die steigenden Anforderungen virtualisierter Shared Infrastrukturen für Server und Storage und ermöglicht eine sichere Mandantenfähigkeit für spezifische Daten, insbesondere wenn Sie mehrere Instanzen von Datenbanken und Software hosten.
- **Pool zur Ressourcenoptimierung.** dieser Vorteil kann Ihnen helfen, die Anzahl physischer Server und Storage Controller zu reduzieren, die Workload-Anforderungen auszugleichen, die Auslastung zu erhöhen und gleichzeitig die Performance zu verbessern.
- * Quality of Service (QoS).* FlexPod bietet QoS auf dem gesamten Stack. Diese branchenführenden QoS-Storage-Richtlinien ermöglichen differenzierte Service-Level in einer Shared IT-Umgebung. Diese Richtlinien helfen, die Performance für Workloads zu optimieren und unkontrollierte Applikationen zu isolieren und zu kontrollieren.
- **Unterstützung für Storage-Tier-SLAs durch den Einsatz von QoS.** Sie müssen nicht unterschiedliche Storage-Systeme für die verschiedenen Storage-Tiers einsetzen, die eine medizinische Bildgebungsumgebung normalerweise benötigt. Hierfür kann ein einzelner Storage-Cluster mit mehreren NetApp FlexVol Volumes mit spezifischen QoS-Richtlinien für verschiedene Tiers eingesetzt werden. Mit diesem Ansatz wird die Storage-Infrastruktur gemeinsam genutzt, indem die sich ändernden Anforderungen einer bestimmten Storage-Ebene dynamisch erfüllt werden. NetApp AFF kann unterschiedliche SLAs für Storage Tiers unterstützen, indem QoS auf der Ebene des FlexVol Volume verwendet wird. Dadurch ist kein Bedarf an verschiedenen Storage-Systemen für verschiedene Storage Tiers für die Applikation erforderlich.
- **Speichereffizienz.** Medizinische Bilder werden von der Bildanwendung in der Regel vorkomprimiert auf jpeg2k verlustfreie Kompression, die etwa 2.5:1 ist. Dies gilt jedoch für die Bildgebung von Anwendungen

und herstellerspezifisch. In größeren Applikations-Imaging-Umgebungen (größer als 1 PB) sind Storage-Einsparungen von 5 bis 10 % möglich und dank NetApp Storage-Effizienzfunktionen können die Storage-Kosten gesenkt werden. Arbeiten Sie mit Ihren Applikationsanbietern im Bereich bildgebende Verfahren und Ihrem NetApp Experten zusammen, um die potenzielle Storage-Effizienz für Ihr Bildgebungssystem auszuschöpfen.

- **Agilität.** mit den branchenführenden Tools für Workflow-Automatisierung, Orchestrierung und Management von FlexPod Systemen kann Ihr IT-Team viel schneller auf geschäftliche Anforderungen reagieren. Diese geschäftlichen Anforderungen reichen von Backup und Bereitstellung zusätzlicher Test- und Schulungsumgebungen für medizinische Bildgebung bis hin zu Replikationen von Analyseldatenbanken für Einwohnerzustands-Management-Initiativen.
- * Höhere Produktivität.* Sie können diese Lösung schnell implementieren und skalieren, um ein optimales Klinikerlebnis für Endbenutzer zu gewährleisten.
- **Data Fabric.** Ihre Data Fabric von NetApp verknüpft Daten über Standorte, physische Grenzen und Applikationen hinweg. Ihre Data Fabric von NetApp wurde für Unternehmen in einer datenorientierten Welt entwickelt. Daten werden an zahlreichen Orten erstellt und verwendet. Oft werden sie auch an mehreren Orten sowie in mehreren Applikationen und Infrastrukturen gleichzeitig genutzt. Sie benötigen also eine einheitliche und integrierte Strategie für das Management. Mit dieser Lösung kann Ihr IT-Team die Kontrolle über die Daten behalten und die ständig zunehmende Komplexität IM IT-BEREICH verringern.
- **FabricPool.** NetApp ONTAP FabricPool senkt die Storage-Kosten ohne Einbußen bei Performance, Effizienz, Sicherheit oder Schutz. FabricPool ist transparent für Enterprise-Applikationen und nutzt die Cloud-Effizienz weiter, indem die Storage-TCO gesenkt werden, ohne dass die Applikationsinfrastruktur umgestaltet werden muss. FlexPod bietet die Storage Tiering-Funktionen von FabricPool für eine effizientere Nutzung von ONTAP Flash Storage. Ausführliche Informationen finden Sie unter "FlexPod mit FabricPool".
- * FlexPod Sicherheit.* Sicherheit ist das Fundament von FlexPod. In den letzten Jahren ist Ransomware zu einer bedeutenden und wachsenden Bedrohung geworden. Ransomware ist eine Malware, die auf Crypto Virologie basiert, die Kryptografie verwendet, um schädliche Software zu erstellen. Diese Malware kann sowohl symmetrische und asymmetrische Schlüssel Verschlüsselung verwenden, um die Daten eines Opfers zu sperren und ein Lösegeld zu verlangen, um den Schlüssel zur Entschlüsselung der Daten. Informationen darüber, wie FlexPod hilft, Bedrohungen wie Ransomware abzuwehren, finden Sie unter "Die Lösung gegen Ransomware". FlexPod-Infrastrukturkomponenten "(FIPS) 140-2" entsprechen außerdem den Vorschriften des Federal Information Processing Standard.
- **Kooperativer Support für FlexPod** NetApp und Cisco haben ein solides, skalierbares und flexibles Support-Modell für den FlexPod entwickelt, das die individuellen Support-Anforderungen der konvergenten FlexPod Infrastruktur erfüllt. Bei diesem Modell profitieren Kunden von der gebündelten Erfahrung, den gemeinsamen Ressourcen und dem Fachwissen des technischen Supports von NetApp und Cisco, um unabhängig von ihrem Speicherort des Problems Ihren FlexPod Support zu ermitteln und zu beheben. Das kooperative Support-Modell für FlexPod unterstützt Sie bei der Überprüfung, ob Ihr FlexPod System effizient arbeitet und die Vorteile aktueller Technologie nutzt. Gleichzeitig bietet es ein erfahrenes Team zur Unterstützung bei der Behebung von Integrationsproblemen.

  Das kooperative Support-Modell für FlexPod ist besonders dann nützlich, wenn Ihr Unternehmen im Gesundheitswesen geschäftskritische Applikationen ausführt. Die folgende Abbildung zeigt einen Überblick über das kooperative Support-Modell für FlexPod.



Umfang

Dieses Dokument bietet einen technischen Überblick über ein Cisco Unified Computing System (Cisco UCS) und eine auf NetApp ONTAP basierende FlexPod Infrastruktur zum Hosten dieser Lösung für die medizinische Bildgebung.

Zielgruppe

Dieses Dokument richtet sich an technische Leiter im Gesundheitswesen sowie an Lösungstechniker von Cisco und NetApp Partnern und Professional Services-Mitarbeiter. NetApp geht davon aus, dass der Leser gute Kenntnisse der Konzepte zur Berechnung der Storage- und Computing-Größenbemessung sowie der technischen Vertrautheit mit dem medizinischen Bildgebungssystem, Cisco UCS und NetApp Storage-Systemen hat.

Applikationen für medizinische Bildgebung

Eine typische medizinische Bildgebungsapplikation bietet eine Suite an Applikationen, die zusammen eine Imaging-Lösung der Enterprise-Klasse für kleine, mittlere und große Unternehmen im Gesundheitswesen bilden.

Im Mittelpunkt der Produktsuite stehen die folgenden klinischen Funktionen:

- Enterprise Imaging Repository
- Unterstützt herkömmliche Bildquellen wie Radiologie und Kardiologie. Unterstützt werden auch andere Behandlungsbereiche wie Augenheilkunde, Dermatologie, Koloskopie und andere medizinische Bildgebungsobjekte wie Fotos und Videos.

- "Bildarchivierung und Kommunikationssystem" (PACS), ein computergestütztes Mittel, um die Rolle eines konventionellen radiologischen Films zu ersetzen
- Anbieterneutrales Archiv (VNA) für Enterprise-Bildgebung:
  - Skalierbare Konsolidierung von DICOM- und nicht-DICOM-Dokumenten
  - Zentrales medizinisches Bildgebungssystem
  - Unterstützung für die Dokumentsynchronisierung und Datenintegrität zwischen mehreren (PACSs) im Unternehmen
  - Das Lifecycle Management von Dokumenten durch ein regelbasiertes Expertensystem, das Dokumentmetadaten nutzt, z. B.:
  - Modalität-Typ
  - Alter des Studiums
  - Alter des Patienten (aktuell und zum Zeitpunkt der Bildaufnahme)
  - Zentrale Integrationsstelle innerhalb und außerhalb des Unternehmens (HIE):
  - Kontextabhängige Dokumentverknüpfung
  - Health Level Seven International (HL7), DICOM und WADO
  - Storage-unabhängige Archivierungsfunktion
- Integration mit anderen Gesundheitsinformationssystemen, die HL7 und kontextbezogene Verknüpfungen verwenden:
  - Ermöglicht EHRs, aus Patientendiagrammen, Bildgebungsworkflows usw. direkte Links zu Patientenbildern zu implementieren.
  - Hilft beim Einbetten der Bildhistorie der Längsversorgung eines Patienten in EHRs.
- Workflows für Radiologie-Technologen
- Enterprise-Viewer mit keinerlei Standfläche für die Anzeige von Bildern von jedem beliebigen Ort auf jedem fähigen Gerät aus
- Analysetools zur Nutzung von retrospektiven und Echtzeitdaten:
  - Compliance-Berichte
  - Operative Berichte
  - Berichte zur Qualitätskontrolle und Qualitätssicherung

Größe der Gesundheitseinrichtung und Plattformdimensionierung

Medizinische Einrichtungen werden großenteils durch standardbasierte Methoden klassifiziert, die Programme wie ACO unterstützen. Eine solche Klassifizierung nutzt das Konzept eines klinisch integrierten Netzwerks (CIN). Eine Gruppe von Krankenhäusern kann als CIN bezeichnet werden, wenn sie zusammenarbeiten und an bewährten Standard-klinischen Protokollen und -Pfaden halten, um den Wert der Pflege zu verbessern und die Patientenkosten zu reduzieren. Krankenhäuser innerhalb eines CIN haben Kontrollen und Praktiken an Bord Ärzte, die die Kernwerte des CIN folgen. Bisher beschränkte sich ein integriertes Bereitstellungsnetzwerk (IDN) auf Krankenhäuser und Arztgruppen. Ein CIN überschreitet traditionelle IDN-Grenzen, und ein CIN kann weiterhin Teil eines ACO sein. Nach den Grundsätzen eines CIN können Organisationen im Gesundheitswesen in kleine, mittlere und große Unternehmen eingestuft werden.

Kleine Unternehmen im Gesundheitswesen

Eine Gesundheitseinrichtung ist klein, wenn sie nur ein einziges Krankenhaus mit ambulanten Kliniken und eine stationäre Abteilung umfasst, aber sie ist nicht Teil eines CIN. Ärzte arbeiten als Pflegekräfte und

koordinieren die Patientenversorgung während eines Pflegekontinuums. Diese kleinen Unternehmen umfassen in der Regel von Ärzten betriebene Einrichtungen. Als integrierte Versorgung für den Patienten können sie eine Notfallversorgung und Traumata anbieten oder nicht. In der Regel führt ein kleines Unternehmen im Gesundheitswesen jährlich etwa 250,000 klinische Bildgebungsstudien durch. Bildgebungszentren sind als kleine Unternehmen im Gesundheitswesen und bieten Imaging-Services. Einige Unternehmen bieten auch Diktierservices im Bereich der Radiologie.

Mittelständische Unternehmen im Gesundheitswesen

Eine medizinische Einrichtung, die als mittelgroße Unternehmen eingestuft wird, wenn sie mehrere Krankenhaussysteme mit bestimmten Organisationen umfasst, wie z. B. die folgenden:

- Pflegekliniken für Erwachsene und stationäre Krankenhäuser für Erwachsene
- Arbeits- und Lieferabteilungen
- Kinderkliniken und Kinderkrankenhäuser
- Ein Krebsbehandlungszentrum
- Notfallabteilungen für Erwachsene
- Kindernotabteilungen
- Eine Familienmedizin und Primärversorgung Büro
- Ein Trauma-Zentrum für Erwachsene
- Ein Kindertrauma-Zentrum

In einer mittelgroßen Gesundheitseinrichtung befolgen Ärzte die Prinzipien eines CIN und arbeiten als eine Einheit. Krankenhäuser haben separate Funktionen für Krankenhaus, Arzt und Apotheke Abrechnung. Krankenhäuser können mit akademischen Forschungsinstituten in Verbindung gebracht werden und interventionelle klinische Forschung und Studien durchführen. Ein mittleres Unternehmen im Gesundheitswesen führt jährlich bis zu 500,000 klinische Bildgebungsstudien durch.

Große Organisationen im Gesundheitswesen

Eine Gesundheitseinrichtung gilt als groß, wenn sie die Merkmale einer mittelgroßen Gesundheitsorganisation einschließt und der Gemeinschaft an mehreren geografischen Standorten die mittelgroßen klinischen Fähigkeiten bietet.

Ein großes Gesundheitsunternehmen führt in der Regel folgende Funktionen aus:

- Hat eine zentrale Stelle für die Verwaltung der Gesamtfunktionen
- Beteiligt sich an Joint Ventures mit anderen Krankenhäusern
- Verhandelt die Tarife mit den zahlenden Organisationen jährlich
- Verhandelt die Tarife der Kostenträger nach Staat und Region
- Nimmt an aussagekräftigen ME-Programmen Teil
- Führt fortschrittliche klinische Forschung über Gesundheitsfürsorge der Bevölkerung durch, indem sie standardbasierte PHM-Tools (Population Health Management) verwendet
- Führt jährlich bis zu einer Million klinische Bildgebungsstudien durch

Einige große Unternehmen im Gesundheitswesen, die sich an einem CIN beteiligen, verfügen auch über KI-basierte Bildlesefunktionen. Diese Unternehmen führen in der Regel jährlich eine bis zwei Millionen klinische Studien durch.

Bevor Sie sich ansehen, wie diese verschiedenen Unternehmen in ein optimal dimensionierte FlexPod-System übersetzen, sollten Sie die verschiedenen FlexPod-Komponenten und die verschiedenen Funktionen eines FlexPod-Systems kennen.

FlexPod

Cisco Unified Computing System

Cisco UCS besteht aus einer zentralen Management-Domäne, die mit einer einheitlichen I/O-Infrastruktur verbunden ist. Cisco UCS für medizinische Bildgebungsumgebungen wurde auf die Empfehlungen und Best Practices für das medizinische Bildgebungssystem von NetApp abgestimmt, damit die Infrastruktur wichtige Patientendaten mit maximaler Verfügbarkeit bereitstellen kann.

Die Grundlage für die medizinische Bildgebung in Unternehmen ist die Cisco UCS-Technologie mit integriertem Systemmanagement, Intel Xeon Prozessoren und Servervirtualisierung. Diese integrierten Technologien lösen die Herausforderungen von Datacentern und ermöglichen es Ihnen, Ihre Ziele beim Design eines Datacenters mit einem typischen Bildgebungssystem zu erreichen. Cisco UCS vereint das LAN-, SAN- und Systemmanagement in einem einzigen vereinfachten Link für Rack Server, Blade Server und Virtual Machines (VMs). Cisco UCS besteht aus einem redundanten Paar Cisco UCS Fabric Interconnects, die einen zentralen Managementpunkt und eine zentrale Kontrollstelle für den gesamten I/O-Datenverkehr ermöglichen.

Cisco UCS verwendet Serviceprofile, um virtuelle Server in der Cisco UCS Infrastruktur richtig und konsistent zu konfigurieren. Serviceprofile umfassen wichtige Serverinformationen über die Serveridentität, z. B. LAN- und SAN-Adressierung, I/O-Konfigurationen, Firmware-Versionen, Boot Order, Network Virtual LAN (VLAN), physischen Port und QoS-Richtlinien. Service-Profile lassen sich dynamisch erstellen und sind mit beliebigen physischen Servern im System in Minutenschnelle anstatt in Stunden oder Tagen verbunden. Die Zuordnung von Serviceprofilen zu physischen Servern erfolgt in einer einzigen, einfachen Operation, die die Migration von Identitäten zwischen Servern in der Umgebung ermöglicht, ohne dass eine physische Konfiguration geändert werden muss. Ferner ermöglicht es die schnelle Bare-Metal-Bereitstellung von Ersatzteilen für ausgefallene Server.

Durch die Verwendung von Service-Profilen kann bestätigt werden, dass die Server im gesamten Unternehmen konsistent konfiguriert sind. Bei der Verwendung mehrerer Cisco UCS Management-Domänen kann Cisco UCS Central globale Serviceprofile verwenden, um Konfigurations- und Richtlinieninformationen über Domänen hinweg zu synchronisieren. Wenn Wartungsarbeiten in einer Domäne durchgeführt werden müssen, kann die virtuelle Infrastruktur in eine andere Domäne migriert werden. Selbst wenn eine einzelne Domain offline ist, laufen die Applikationen mit hoher Verfügbarkeit weiter.

Cisco UCS ist eine Lösung der nächsten Generation für Blade- und Rack-Server-Computing. Das System verfügt über ein verlustfreies 40 GbE Unified Network Fabric mit x86-Servern der Enterprise-Klasse. Es bietet eine integrierte, skalierbare, Multigehäuse-Plattform, in der alle Ressourcen in einer gemeinsamen Management-Domäne zusammengefasst werden. Cisco UCS beschleunigt die einfache, zuverlässige und sichere Bereitstellung neuer Services durch End-to-End-Bereitstellung und Migrationsunterstützung für virtualisierte und nicht virtualisierte Systeme. Cisco UCS bietet folgende Funktionen:

- Umfassendes Management
- Radikale Vereinfachung
- Hohe Performance

Cisco UCS besteht aus den folgenden Komponenten:

- **Compute.** das System basiert auf einer völlig neuen Klasse von Computersystemen, die Rack-Mount- und Blade-Server auf der Grundlage der Intel Xeon-Produktreihe für skalierbare Prozessoren beinhaltet.

- **Netzwerk.** das System ist in eine verlustfreie, 40 Gbit/s Unified Network Fabric mit geringer Latenz integriert. Diese Netzwerkgrundlage deckt LANs, SANs und hochperformante Computing-Netzwerke ab, bei denen es sich heute um separate Netzwerke handelt. Durch das Unified Fabric wird die Anzahl der Netzwerkadapter, Switches und Kabel reduziert. Darüber hinaus werden Stromverbrauch und Kühlungsbedarf gesenkt, was insgesamt zu niedrigeren Kosten führt.
- **Virtualisierung.** das System setzt das volle Potenzial der Virtualisierung frei, indem es die Skalierbarkeit, Performance und Betriebskontrolle virtueller Umgebungen verbessert. Die Sicherheit, Richtlinienumsetzung und Diagnosefunktionen von Cisco werden auf virtualisierte Umgebungen erweitert, um sich ändernde Geschäfts- und IT-Anforderungen besser zu unterstützen.
- **Speicherzugriff.** das System bietet konsolidierten Zugriff auf SAN Speicher und NAS über das Unified Fabric. Sie ist darüber hinaus ein ideales System für softwaredefinierten Storage. Durch die Kombination der Vorteile eines einzelnen Framework für das Management von Computing- und Storage-Servern über eine einzige Konsole kann QoS bei Bedarf implementiert werden, um die I/O-Drosselung im System zu injizieren. Außerdem können Ihre Server-Administratoren Storage-Ressourcen vorab Zugriffsrichtlinien für Storage-Ressourcen zuweisen, wodurch Storage-Konnektivität und -Management vereinfacht werden und die Produktivität erhöht wird. Neben externem Storage verfügen sowohl Rack- als auch Blade-Server über internen Storage, auf den über integrierte RAID-Controller zugegriffen werden kann. Durch die Einrichtung des Storage-Profils und der Festplattenkonfigurationsrichtlinie im Cisco UCS Manager werden die Storage-Anforderungen des Host-Betriebssystems und der Applikationsdaten durch benutzerdefinierte RAID-Gruppen erfüllt. Das Ergebnis ist Hochverfügbarkeit und bessere Performance.
- **Management.** das System integriert alle Systemkomponenten auf einzigartige Weise, sodass die gesamte Lösung als einzelne Einheit über den Cisco UCS Manager verwaltet werden kann. Zum Management aller Systemkonfiguration und -Vorgänge verfügt der Cisco UCS Manager über eine intuitive Benutzeroberfläche, eine CLI und ein leistungsstarkes Skriptbibliothek-Modul für Microsoft Windows PowerShell, das auf einer robusten API basiert.

Cisco Unified Computing System verbindet Netzwerke und Server auf Zugriffsebene. Dieses hochperformante Serversystem der nächsten Generation bietet Ihrem Datacenter ein hohes Maß an Workload-Flexibilität und Skalierbarkeit.

Cisco UCS Manager

Cisco UCS Manager bietet einheitliches, eingebettetes Management für alle Software- und Hardware-Komponenten im Cisco UCS. Durch den Einsatz von Technologie mit nur einem Anschluss managt, steuert und verwaltet UCS Manager mehrere Chassis für Tausende VMs. Über eine intuitive GUI, eine CLI oder eine XML API managen Administratoren das gesamte Cisco UCS als eine logische Einheit. Cisco UCS Manager befindet sich auf einem Paar Fabric Interconnects der Cisco UCS 6300 Serie, die eine Cluster-aktiv-Standby-Konfiguration für hohe Verfügbarkeit verwenden.

Cisco UCS Manager bietet eine einheitliche und integrierte Managementoberfläche, die Ihre Server, Ihr Netzwerk und Ihren Storage integriert. Der Cisco UCS Manager führt die automatische Erkennung durch, um den Bestand von zu erkennen, zu managen und Systemkomponenten bereitzustellen, die Sie hinzufügen oder ändern. Es bietet einen umfassenden Satz von XML-APIs für die Integration von Drittanbietern, und es deckt 9,000 Punkte der Integration. Außerdem unterstützt es die individuelle Entwicklung zur Automatisierung, zur Orchestrierung und um ein neues Maß an Systemtransparenz und Kontrolle zu erzielen.

Service-Profile profitieren sowohl von virtualisierten als auch von nicht virtualisierten Umgebungen. Sie steigern die Mobilität von nicht virtualisierten Servern, z. B. wenn Sie Workloads von Server zu Server verschieben oder einen Server für Services oder Upgrades offline schalten. Profile können auch in Verbindung mit Virtualisierungs-Clustern genutzt werden, um neue Ressourcen einfach online zu bringen und so die vorhandene VM-Mobilität zu ergänzen.

Weitere Informationen zum Cisco UCS Manager finden Sie im "Produktseite zu Cisco UCS Manager".

Unterscheidungsmerkmale von Cisco UCS

Cisco Unified Computing System revolutioniert die Verwaltung von Servern im Rechenzentrum. Die folgenden Alleinstellungsmerkmale von Cisco UCS und Cisco UCS Manager:

- **Embedded Management.** in Cisco UCS werden die Server über die eingebettete Firmware in den Fabric Interconnects verwaltet, sodass keine externen physischen oder virtuellen Geräte mehr gemanagt werden müssen.
- **Unified Fabric.** bei Cisco UCS, von Blade Server Chassis oder Rack Servern bis hin zu Fabric Interconnects wird für den LAN-, SAN- und Management-Datenverkehr ein einziges Ethernet-Kabel verwendet. Dieser konvergente I/O reduziert die Anzahl der Kabel, SFPs und Adapter, die Sie benötigen, wodurch wiederum die Investitions- und Betriebskosten der Gesamtlösung gesenkt werden.
- **Autodiscovery.** durch einfaches Einsetzen des Blade-Servers in das Gehäuse oder durch Anschluss von Rack-Servern an Fabric Interconnects erfolgt die Erkennung und Bestandsaufnahme der Computing-Ressourcen automatisch ohne Management-Eingriffe. Die Kombination aus Unified Fabric und automatischer Erkennung ermöglicht die einmalige Verkabelung der Architektur von Cisco UCS. Dort kann die Rechnerfunktion problemlos erweitert werden, während die bestehende externe Konnektivität mit LAN-, SAN- und Management-Netzwerken erhalten bleibt.
- **Policy-basierte Ressourcenklassifizierung.** Wenn eine Computing-Ressource vom Cisco UCS Manager erkannt wird, kann sie auf Basis der von Ihnen definierten Richtlinien automatisch in einen bestimmten Ressourcen-Pool klassifiziert werden. Diese Funktion ist nützlich für mandantenfähiges Cloud-Computing.
- **Kombiniertes Rack- und Blade-Server-Management.** Cisco UCS Manager kann Blade Server der B-Serie und Rack Server der C-Serie unter derselben Cisco UCS-Domäne verwalten. Diese Funktion und das statusfreie Computing machen Computing-Ressourcen zu einem echten Hardware-Formfaktor.
- **Modellbasierte Managementarchitektur.** die Cisco UCS Manager Architektur und Management Datenbank sind modellbasiert und datengetrieben. Die offene XML API für den Betrieb am Management-Modell ermöglicht eine einfache und skalierbare Integration von Cisco UCS Manager in andere Management-Systeme.
- **Richtlinien, Pools und Vorlagen.** der Managementansatz im Cisco UCS Manager basiert auf der Definition von Richtlinien, Pools und Vorlagen anstelle einer übersichtlichen Konfiguration. Sie ermöglicht einen einfachen, locker gekoppelten, datenfokussierten Ansatz beim Management von Computing-, Netzwerk- und Storage-Ressourcen.
- **Unloose referential Integrity.** in Cisco UCS Manager kann ein Service-Profil, ein Port-Profil oder Richtlinien auf andere Richtlinien oder andere logische Ressourcen mit loser referenzieller Integrität verweisen. Eine Richtlinie, auf die verwiesen wird, kann zum Zeitpunkt der Erstellung der verweisenden Richtlinie nicht existieren, aber eine Richtlinie kann gelöscht werden, auch wenn andere Richtlinien sich darauf beziehen. So können verschiedene Experten unabhängig voneinander arbeiten. Sie erhalten hohe Flexibilität, da verschiedene Experten verschiedener Domänen wie Netzwerk, Storage, Sicherheit, Server und Virtualisierung mit einem gemeinsamen Ansatz für eine komplexe Aufgabe zusammenarbeiten.
- **Policy Resolution.** in Cisco UCS Manager können Sie eine Baumstruktur der Organisationseinheit-Hierarchie erstellen, die die realen Mieter und organisatorischen Beziehungen nachahmt. Sie können verschiedene Richtlinien, Pools und Vorlagen auf verschiedenen Ebenen Ihrer Unternehmenshierarchie definieren. Eine Richtlinie, die sich auf eine andere Policy nach Namen bezieht, wird in der Organisationshierarchie mit der nächstbesten Policy-Übereinstimmung aufgelöst. Wenn in der Hierarchie der Root-Organisation keine Richtlinie mit einem bestimmten Namen gefunden wird, wird eine spezielle Richtlinie mit dem Namen „Default“ durchsucht. Diese Vorgehensweise zur Behebung von Richtlinien ermöglicht automatisierte Management-APIs und bietet den Eigentümern der verschiedenen Unternehmen große Flexibilität.
- **Service Profile und Stateless Computing.** ein Service-Profil ist eine logische Darstellung eines Servers mit seinen verschiedenen Identitäten und Richtlinien. Dieser logische Server kann jeder beliebigen physischen Ressource zugewiesen werden, sofern er die Ressourcenanforderungen erfüllt. Statusfreies

Computing ermöglicht die Beschaffung eines Servers innerhalb von Minuten, wobei früher Tage mit alten Server-Management-Systemen dauerte.

- **Integrierte Unterstützung der Mandantenfähigkeit.** die Kombination aus Richtlinien, Pools, Vorlagen, loser referenzieller Integrität, Richtlinienauflösung in der Unternehmenshierarchie und einem auf Serviceprofilen basierenden Ansatz für Computing-Ressourcen macht Cisco UCS Manager zur Nutzung mandantenfähiger Umgebungen, die in der Regel in Private und Public Clouds beobachtet werden.
- **Erweiterter Speicher** der Cisco UCS B200 M5 Blade Server der Enterprise-Klasse erweitert die Funktionen des Cisco Unified Computing System Portfolios in einem Blade-Formfaktor halber Breite. Der Cisco UCS B200 M5 nutzt die Leistung der neuesten skalierbaren Intel Xeon Prozessoren mit bis zu 3 TB RAM. Diese Funktion ermöglicht ein riesiges Verhältnis zwischen VM und physischen Servern, das viele Implementierungen benötigen. Oder bestimmte Architekturen können so umfangreiche Speichervorgänge wie Big Data unterstützen.
- **Virtualisierungsorientiertes Netzwerk.** die Cisco Virtual Machine Fabric Extender (VM-FEX)-Technologie macht die Netzwerkebene des Zugriffsnetzwerks der Host-Virtualisierung bewusst. Diese Erkenntnis verhindert eine Verschmutzung der Rechner- und Netzwerkdomänen durch Virtualisierung, wenn ein virtuelles Netzwerk durch Portprofile verwaltet wird, die vom Team Ihres Netzwerkadministrators definiert werden. VM-FEX entlastet zudem die Hypervisor-CPU, indem es das Switching in der Hardware durchführt. Dadurch kann die Hypervisor-CPU mehr Aufgaben rund um die Virtualisierung durchführen. Um das Cloud-Management zu vereinfachen, lässt sich die VM-FEX-Technologie nahtlos in VMware vCenter, Linux Kernel-Based Virtual Machine (KVM) und Microsoft Hyper-V SR-IOV integrieren.
- **Vereinfachte QoS.** auch wenn FC und Ethernet im Cisco UCS konvergiert werden, die integrierte Unterstützung für QoS und verlustfreies Ethernet machen es nahtlos. Durch die Darstellung aller Systemklassen auf einer grafischen Benutzeroberfläche wird die Netzwerk-QoS in Cisco UCS Manager vereinfacht.

Cisco Nexus IP und MDS Switches

Cisco Nexus Switches und Cisco MDS Multilayer Directors bieten Konnektivität der Enterprise-Klasse sowie SAN-Konsolidierung. Die Cisco Multi-Protokoll-Speichernetzwerke verringern Ihr Geschäftsrisiko durch Flexibilität und Optionen: FC, Fibre Connection (FICON), FC over Ethernet (FCoE), iSCSI und FC over IP (FCIP).

Cisco Nexus Switches bieten eines der umfangreichsten Datacenter-Netzwerk-Funktionen auf einer einzigen Plattform. Sie bieten hohe Performance und Dichte sowohl für das Datacenter als auch für den Campus-Kern. Zudem bieten sie umfassende Funktionen für Datacenter-Aggregation, End-of-row und Datacenter Interconnect-Implementierungen in einer äußerst stabilen modularen Plattform.

Cisco UCS integriert Rechenressourcen in Cisco Nexus Switches und eine Unified Fabric, die verschiedene Typen von Netzwerkverkehr identifiziert und unterstützt. Der Datenverkehr umfasst Storage-I/O, Desktop-Datenströme, Management und Zugriff auf klinische und geschäftliche Applikationen. Sie erhalten folgende Möglichkeiten:

- **Skalierbarkeit der Infrastruktur** Virtualisierung, effiziente Stromversorgung und Kühlung, Cloud-Skalierbarkeit mit Automatisierung, hoher Dichte und Performance unterstützen effizientes Datacenter-Wachstum.
- * Betriebskontinuität.* das Design umfasst Hardware, Cisco NX-OS Softwarefunktionen und Management zur Unterstützung von Umgebungen ohne Ausfallzeiten.
- **Transportflexibilität.** mit dieser kostengünstigen Lösung können Sie schrittweise neue Netzwerktechnologien einführen.

Gemeinsam bieten Cisco UCS mit Cisco Nexus Switches und MDS Multilayer Directors eine Computing-, Netzwerk- und SAN-Konnektivitätslösung für medizinisches Bildgebungssystem eines Unternehmens.

NetApp All-Flash-Storage

NetApp Storage mit ONTAP Software senkt die Storage-Gesamtkosten und bietet gleichzeitig Lese- und Schreibreaktionszeiten mit niedriger Latenz sowie hohe IOPS für die Workloads medizinischer Bildgebungssysteme. ONTAP unterstützt sowohl All-Flash- als auch Hybrid-Storage-Konfigurationen und schafft so ein optimales Storage-System, das die typischen Anforderungen medizinischer Bildgebungsverfahren erfüllt. NetApp Flash-Storage ermöglicht medizinischen Bildverarbeitungssystems die wichtigsten Komponenten mit hoher Performance und Reaktionsfähigkeit zur Unterstützung von latenzempfindlichen Systemen für die medizinische Bildgebung. Durch das Erstellen mehrerer Fehlerdomänen in einem einzigen Cluster kann die NetApp Technologie auch die Produktionsumgebungen aus den nicht für die Produktion verwendeten Umgebungen isolieren. Und indem NetApp garantiert, dass die System-Performance mit der minimalen QoS von ONTAP nicht unter ein bestimmtes Level für Workloads fällt, reduziert NetApp auch Performance-Probleme für Ihr System.

Die horizontal skalierbare Architektur der ONTAP Software kann flexibel an Ihre verschiedenen I/O-Workloads angepasst werden. Um den erforderlichen Durchsatz und die niedrige Latenz zu erzielen, die klinische Applikationen benötigen, und um eine modulare Scale-out-Architektur bereitzustellen, kommen meist All-Flash-Konfigurationen in ONTAP-Architekturen zum Einsatz. NetApp AFF Nodes können in demselben horizontal skalierbaren Cluster mit hybriden (HDD und Flash) Storage-Nodes kombiniert werden und eignen sich zur Speicherung großer Datensätze mit hohem Durchsatz. Sie können Ihre medizinische Bildgebungssystem-Umgebung von teurem SSD-Storage auf anderen Nodes klonen, replizieren und sichern und auf anderen Nodes preiswerteren HDD-Storage hinzufügen. Mit dem Cloud-fähigen NetApp Storage und einer Data Fabric von NetApp können Sie Backups in Objekt-Storage vor Ort oder in der Cloud erstellen.

Für die medizinische Bildverarbeitung wurde ONTAP von den führenden Bildgebungssystemen validiert. Das bedeutet, dass es getestet wurde, um schnelle und zuverlässige Leistung für die medizinische Bildgebung zu liefern. Zudem vereinfachen die folgenden Funktionen das Management, erhöhen die Verfügbarkeit und Automatisierung und verringern die benötigte Storage-Kapazität.

- **Überragende Performance.** die NetApp AFF Lösung verwendet dieselbe Unified Storage-Architektur, die ONTAP Software, die gleiche Managementoberfläche, umfassende Datenservices und erweiterte Funktionen wie die anderen NetApp FAS Produktfamilien. Diese innovative Kombination aus All-Flash-Medien und ONTAP bietet Ihnen die konsistent niedrige Latenz und hohe IOPS von All-Flash-Storage und branchenführende ONTAP Software.
- **Storage-Effizienz.** Sie können Ihre gesamten Kapazitätsanforderungen mit Ihrem NetApp SME reduzieren und verstehen, wie dies Ihr spezielles medizinisches Bildgebungssystem angewendet hat.
- **Platzsparendes Klonen** mit der FlexClone Funktion kann Ihr System nahezu sofort Klone erstellen, um eine Aktualisierung der Backup- und Testumgebung zu unterstützen. Diese Klone verbrauchen nur bei Änderungen zusätzlichen Storage.
- * Integrierte Datensicherung.* vollständige Funktionen für Datensicherung und Disaster Recovery helfen Ihnen, Ihre kritischen Datenbestände zu schützen und Disaster Recovery zu ermöglichen.
- **Unterbrechungsfreier Betrieb.** Upgrades und Wartungen können durchgeführt werden, ohne Daten offline zu schalten.
- **QoS.** Storage QoS hilft Ihnen, potenzielle problematische Workloads zu begrenzen. Vor allem, QoS schafft eine minimale Performance-Garantie, dass Ihre System-Performance nicht unter ein bestimmtes Niveau für kritische Workloads wie ein medizinisches Bildgebungssystem die Produktionsumgebung sinkt. Und durch die Begrenzung von Engpässen kann NetApp QoS auch Probleme mit der Performance verringern.
- **Data Fabric.** um den digitalen Wandel zu beschleunigen, vereinfacht und integriert die Data Fabric von NetApp das Datenmanagement über Cloud- und On-Premises-Umgebungen hinweg. Sie profitieren von konsistenten und integrierten Datenmanagementservices, Applikationen für erstklassige Datentransparenz und Einblicke aus Daten, Datenzugriff und -Kontrolle sowie Datensicherung und -Sicherheit. NetApp ist in große Public Clouds wie AWS, Azure, Google Cloud und IBM Cloud integriert. Wir bieten Ihnen eine große

Auswahl.

Host-Virtualisierung – VMware vSphere

FlexPod-Architekturen wurden mit VMware vSphere 6.x validiert. Diese Plattform ist eine der branchenführenden Virtualisierungsplattformen. Zur Implementierung und Ausführung der VMs wird VMware ESXi 6.x verwendet. VCenter Server Appliance 6.x wird zum Management der ESXi Hosts und VMs verwendet. Mehrere ESXi Hosts, die auf den Cisco UCS B200 M5 Blades ausgeführt werden, bilden ein VMware ESXi Cluster. Der VMware ESXi Cluster fasst Computing-, Arbeitsspeicher- und Netzwerkressourcen von allen Cluster-Nodes zusammen und bietet eine ausfallsichere Plattform für die VMs, die auf dem Cluster ausgeführt werden. Die VMware ESXi-Cluster-Funktionen, vSphere High Availability und Distributed Resource Scheduler (DRS) tragen alle zur Toleranz des vSphere-Clusters bei, Ausfälle zu widerstehen, und sie helfen die Ressourcen auf die VMware ESXi-Hosts zu verteilen.

Das NetApp Storage Plug-in und das Cisco UCS Plug-in lassen sich in VMware vCenter integrieren und ermöglichen damit betriebliche Workflows für Ihre erforderlichen Storage- und Computing-Ressourcen.

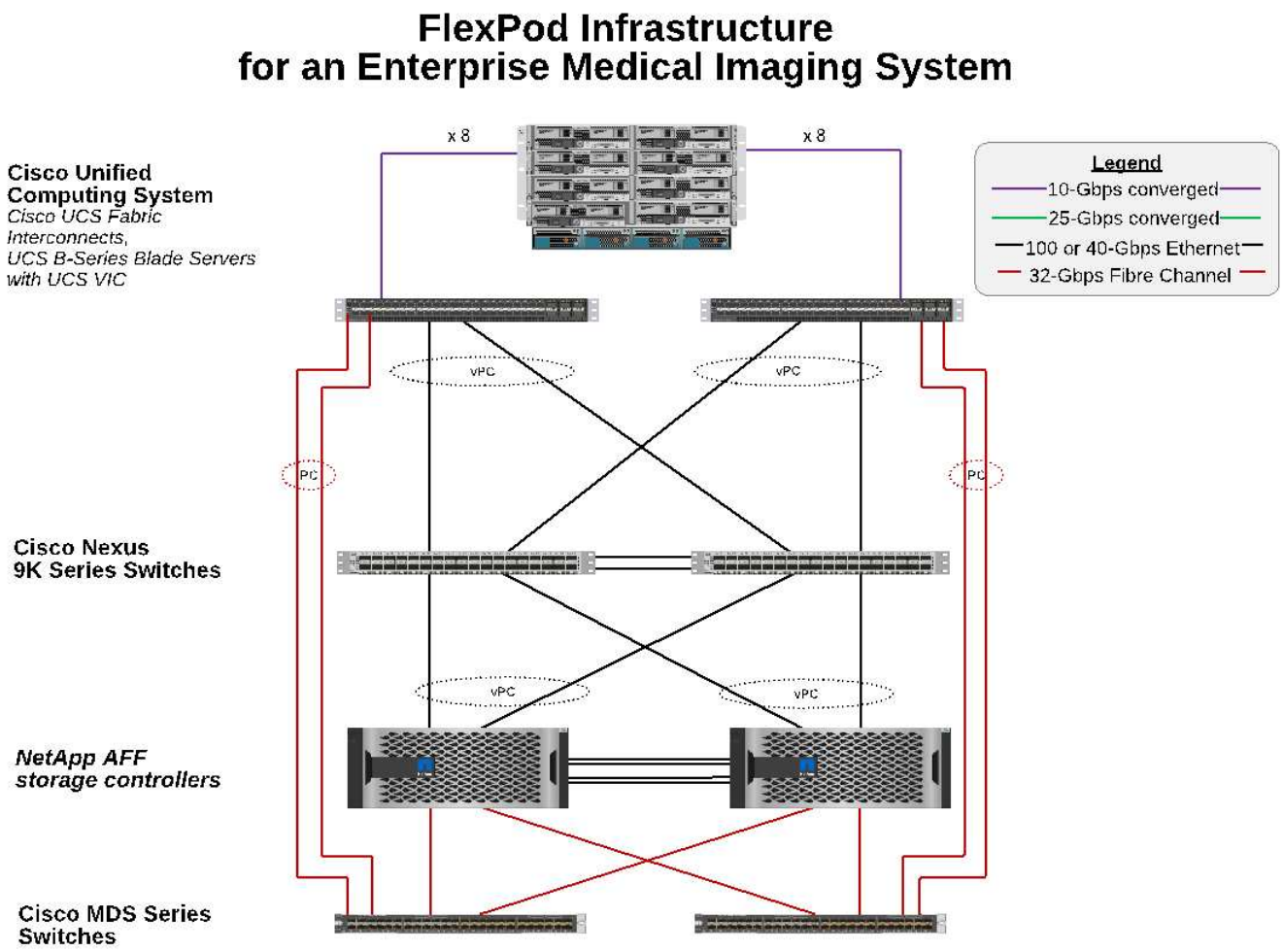
Das VMware ESXi Cluster und vCenter Server bieten Ihnen eine zentrale Plattform zur Bereitstellung von Umgebungen für die medizinische Bildgebung in VMs. Ihr Unternehmen im Gesundheitswesen kann alle Vorteile einer branchenführenden virtuellen Infrastruktur mit folgenden Vorteilen nutzen:

- * Einfache Bereitstellung.* Schnelle und einfache Bereitstellung von vCenter Server mit einer virtuellen Appliance.
- **Zentrale Steuerung und Transparenz.** Verwalten Sie die gesamte vSphere-Infrastruktur von einem Ort aus.
- **Proaktive Optimierung.** Ressourcen zuweisen, optimieren und migrieren für maximale Effizienz.
- **Management.** Verwenden Sie leistungsstarke Plug-ins und Tools, um das Management zu vereinfachen und die Kontrolle zu erweitern.

Der Netapp Architektur Sind

Die FlexPod-Architektur bietet Hochverfügbarkeit, wenn eine Komponente oder ein Link im gesamten Computing-, Netzwerk- und Storage Stack ausfällt. Mehrere Netzwerkpfade für Client-Zugriff und Storage-Zugriff ermöglichen Lastausgleich und eine optimale Ressourcenauslastung.

Die folgende Abbildung zeigt die 16-GB-FC-/40-GB-Ethernet-Topologie (40 GbE) für den Einsatz der Lösung für medizinische Bildgebsysteme.



Storage-Architektur

Mithilfe der in diesem Abschnitt aufgeführten Richtlinien zur Storage-Architektur können Sie Ihre Storage-Infrastruktur für ein medizinisches Bildgebungssystem eines Unternehmens konfigurieren.

Storage-Tiers

Eine typische medizinische Bildgebungsumgebung in Unternehmen setzt sich aus mehreren unterschiedlichen Storage-Tiers zusammen. Jeder Tier verfügt über spezifische Anforderungen an Performance und Storage-Protokoll. NetApp Storage unterstützt verschiedene RAID-Technologien, weitere Informationen sind verfügbar "Hier". Im Folgenden erfahren Sie, wie NetApp AFF Storage-Systeme die Anforderungen verschiedener Storage Tiers für das Bildgebungssystem erfüllen:

- **Performance Storage (Tier 1).** dieser Tier bietet eine hohe Leistung und hohe Redundanz für Datenbanken, Betriebssystemlaufwerke, VMware Virtual Machine File System (VMFS) Datenspeicher und so weiter. Block-I/O wird wie in ONTAP konfiguriert über Fibre in ein Shared-Storage-Array von SSD verschoben. Die minimale Latenz beträgt 1 ms bis 3 ms, wobei gelegentlich 5 ms Spitzenwert liegt. Diese Speicherebene wird in der Regel für den kurzfristigen Speicher-Cache verwendet, in der Regel 6 bis 12 Monate Bildspeicher für den schnellen Zugriff auf Online-DICOM-Bilder. Dieser Tier bietet hohe Performance und hohe Redundanz für Image-Caches, Datenbank-Backup usw. NetApp All-Flash-Arrays bieten eine Latenz von <1 ms bei einer kontinuierlichen Bandbreite, die weit unter den für eine typische medizinische Bildgebungsumgebung der Enterprise-Klasse erwarteten Servicezeiten liegt. NetApp ONTAP unterstützt sowohl RAID-TEC (Triple-Parity RAID zur Aufrechterhaltung des Ausfalls von drei Festplatten)

als auch RAID DP (Double-Parity RAID zur Erhaltung von zwei Festplattenausfällen).

- **Archivspeicher (Tier 2).** dieser Tier wird für typischen kostenoptimierten Dateizugriff, RAID 5- oder RAID 6-Speicher für größere Volumes und langfristige Archivierung mit geringeren Kosten/Leistung verwendet. NetApp ONTAP unterstützt sowohl RAID-TEC (Triple-Parity RAID zur Aufrechterhaltung des Ausfalls von drei Festplatten) als auch RAID DP (Double-Parity RAID zur Erhaltung von zwei Festplattenausfällen). Die NetApp FAS in FlexPod ermöglicht die I/O-Bildgebung von Applikationen über NFS/SMB auf ein SAS-Festplatten-Array. NetApp FAS Systeme bieten eine Latenz von ~10 ms bei kontinuierlicher Bandbreite. Dies ist weit unter den für Storage Tier 2 in einer Umgebung mit medizinischen Bildgebungssystemen eines Unternehmens erwarteten Servicezeiten.

Die Cloud-basierte Archivierung in einer Hybrid-Cloud-Umgebung kann für die Archivierung bei einem Public-Cloud-Storage-Provider mit S3 oder ähnlichen Protokollen verwendet werden. Die NetApp SnapMirror Technologie ermöglicht die Replizierung Imaging-Daten von All-Flash- oder FAS-Arrays auf langsamere festplattenbasierte Storage-Arrays oder auf Cloud Volumes ONTAP für AWS, Azure oder Google Cloud.

NetApp SnapMirror bietet branchenführende Datenreplizierungsfunktionen, um medizinische Bildgebungssysteme durch eine einheitliche Datenreplizierung zu schützen. Vereinfachtes Datensicherungsmanagement in einer Data-Fabric-Umgebung mit plattformübergreifender Replizierung – von Flash über Festplatten bis hin zur Cloud:

- Nahtloser und effizienter Datentransport zwischen NetApp Storage-Systemen zur Unterstützung von Backup und Disaster Recovery mit demselben Ziel-Volume und I/O-Datenstrom
- Failover auf ein beliebiges sekundäres Volume Wiederherstellung von zeitpunktgenauen Snapshots auf sekundärem Storage
- Schutz Ihrer wichtigsten Workloads durch eine synchrone Replikation ohne jeglichen Datenverlust (RPO=0)
- Weniger Netzwerk-Traffic: Geringerer Storage-Bedarf durch effiziente Abläufe
- Reduzierter Netzwerk-Traffic durch Beschränkung des Transports auf geänderte Datenblöcke
- Kein Verlust der Vorteile der Storage-Effizienz auf dem primären Storage während des Transports – einschließlich Deduplizierung, Komprimierung und Data-Compaction
- Zusätzliche Inline-Effizienz mit Netzwerkkomprimierung

Weitere Informationen finden Sie "Hier".

Die folgende Tabelle führt die einzelnen Tiers auf, die für ein typisches Bildgebungssystem benötigt werden, um eine bestimmte Latenz und Durchsatzleistung zu liefern.

Storage-Tier	Anforderungen	NetApp Empfehlung
1	Eine Latenz von 1 bis 5 ms beträgt ein Durchsatz von 35 bis 500 MB/s	AFF mit <1 ms Latenz AFF A300 HA-Paar mit zwei Festplatten-Shelfs kann einen Durchsatz von bis zu ~1,6 GB/s verarbeiten
2	Archivierung vor Ort	FAS mit einer Latenz von bis zu 30 ms
	Archivierung in Cloud	SnapMirror Replizierung auf Cloud Volumes ONTAP oder Backup-Archivierung mit NetApp StorageGRID Software

Konnektivität zum Storage-Netzwerk

FC Fabric

- Die FC Fabric eignet sich für I/O-Vorgänge des Host-Betriebssystems vom Computing bis zum Storage.
- Zwei FC-Fabrics (Fabric A und Fabric B) sind mit Cisco UCS Fabric A und UCS Fabric B verbunden.
- Auf jedem Controller-Node befindet sich eine Storage Virtual Machine (SVM) mit zwei logischen FC-Schnittstellen (LIFs). Auf jedem Node ist eine logische Schnittstelle mit Fabric A verbunden, und die andere ist mit Fabric B verbunden
- Ende-zu-End-Konnektivität mit 16 Gbit/s erfolgt über Cisco MDS Switches. Es sind ein einzelner Initiator, mehrere Ziel-Ports und Zoning konfiguriert.
- FC SAN Boot wird verwendet, um ein vollständiges Statusfreies Computing zu erstellen. Server werden aus LUNs im Boot-Volume gestartet, das auf dem AFF Storage-Cluster gehostet wird.

IP-Netzwerk für Storage-Zugriff über iSCSI, NFS und SMB/CIFS

- An jedem Controller-Node befinden sich zwei iSCSI LIFs in der SVM. Auf jedem Node ist eine logische Schnittstelle mit Fabric A verbunden, und die zweite ist mit Fabric B verbunden
- An jedem Controller-Node befinden sich zwei NAS-Daten-LIFs in der SVM. Auf jedem Node ist eine logische Schnittstelle mit Fabric A verbunden, und die zweite ist mit Fabric B verbunden
- Storage Port Interface Groups (virtueller Port Channel [vPC]) für 10 GB/s Link zum Switch N9k-A und für 10 GB/s Link zum Switch N9k-B.
- Workload in Ext4 oder NTFS-Dateisystemen von VM zum Storage:
  - ISCSI-Protokoll über IP:
- VMs gehostet im NFS-Datenspeicher:
  - VM-I/O-Vorgänge erfolgen über mehrere Ethernet-Pfade durch Nexus Switches.

In-Band-Management (aktiv/Passiv-Bond)

- 1-Gbit/s-Link zum Management-Switch N9k-A und 1 Gbit/s-Link zum Management-Switch N9k-B.

Backup und Recovery

FlexPod Datacenter basiert auf einem Storage-Array, das von der Datenmanagement-Software NetApp ONTAP gemanagt wird. Die ONTAP Software hat sich über 20 Jahre lang weiterentwickelt und bietet viele Datenmanagement-Funktionen für VMs, Oracle Datenbanken, SMB/CIFS-Dateifreigaben und NFS. Zudem stellt sie Sicherungstechnologien wie die NetApp Snapshot Technologie, die SnapMirror Technologie und die Datenreplizierungstechnologie NetApp FlexClone bereit. Die NetApp SnapCenter Software verfügt über einen Server und einen GUI-Client zur Verwendung von ONTAP Snapshot, SnapRestore und FlexClone Funktionen für VM, SMB/CIFS File Shares, NFS und Oracle Datenbanken Backup und Recovery.

Die NetApp SnapCenter Software beschäftigt "Patentiert" Snapshot Technologie, um sofort ein Backup einer kompletten VM oder Oracle-Datenbank auf einem NetApp-Speicher-Volume zu erstellen. Im Vergleich mit Oracle Recovery Manager (RMAN) benötigen Snapshot Kopien keine vollständige Baseline Backup-Kopie, da sie nicht als physische Kopien von Blöcken gespeichert werden. Snapshot-Kopien werden als Zeiger auf die Storage-Blöcke gespeichert, während sie sich beim Erstellen der Snapshot Kopien im ONTAP WAFL File-System befanden. Aufgrund dieser engen physischen Beziehung verbleiben die Snapshot Kopien im selben Storage Array wie die Originaldaten. Zudem können Snapshot Kopien auf Dateiebene erstellt werden, um Ihnen eine granularere Kontrolle für das Backup zu bieten.

Die Snapshot Technologie basiert auf einer Redirect-on-Write-Technik. Er enthält anfangs nur Metadaten-Zeiger und verbraucht erst dann viel Speicherplatz, wenn sich die ersten Daten in einen Storage-Block ändern. Wenn ein vorhandener Block von einer Snapshot Kopie gesperrt wird, wird ein neuer Block vom Dateisystem ONTAP WAFL als aktive Kopie geschrieben. Dieser Ansatz vermeidet die doppelten Schreibvorgänge, die bei der Change-on-Write-Technik auftreten.

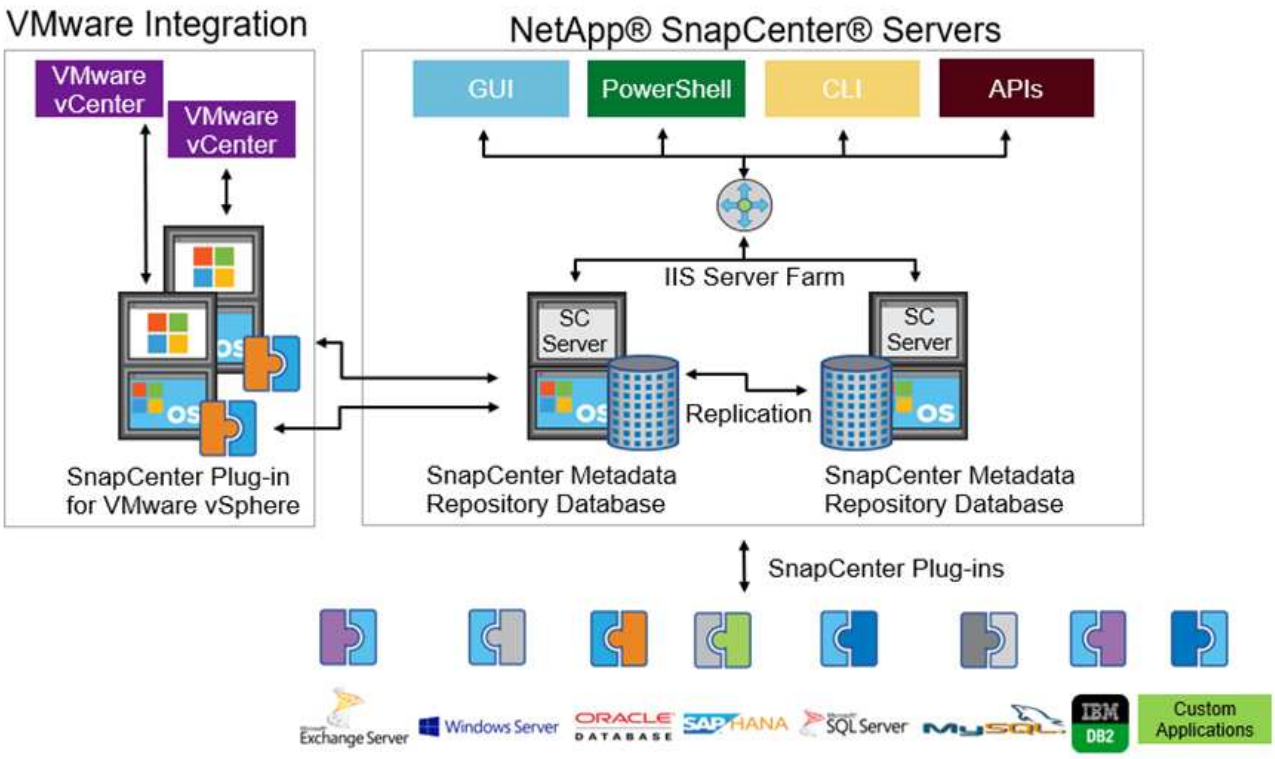
Bei Datenbank-Backups von Oracle erzielen Snapshot Kopien unglaubliche Zeiteinsparungen. Ein Backup, das beispielsweise mit RMAN allein 26 Stunden dauerte, kann mithilfe der SnapCenter Software weniger als zwei Minuten dauern.

Und da bei der Datenwiederherstellung keine Datenblöcke kopiert, sondern stattdessen die Zeiger auf die applikationskonsistenten Snapshot Block-Images überträgt, wenn die Snapshot Kopie erstellt wurde, kann eine Snapshot Backup-Kopie fast sofort wiederhergestellt werden. Klonen von SnapCenter erstellt eine separate Kopie von Metadaten-Pointern auf eine vorhandene Snapshot Kopie und bindet die neue Kopie an einen Ziel-Host. Dieser Prozess läuft auch schnell und speichereffizient ab.

In der folgenden Tabelle sind die Hauptunterschiede zwischen Oracle RMAN und NetApp SnapCenter Software zusammengefasst.

	Backup	Wiederherstellen	Klon	Vollständige Backups Erforderlich	Speicherplatznutzung	Externer Text
RMAN	Langsam	Langsam	Langsam	Ja.	Hoch	Ja.
SnapCenter	Schnell	Schnell	Schnell	Nein	Niedrig	Ja.

Die folgende Abbildung zeigt die SnapCenter Architektur.



Weltweit werden NetApp MetroCluster Konfigurationen von Tausenden Unternehmen für Hochverfügbarkeit

(HA), Vermeidung von Datenverlusten und unterbrechungsfreien Betrieb innerhalb und außerhalb des Datacenters eingesetzt. MetroCluster ist eine kostenlose Funktion der ONTAP Software, die Daten und Konfigurationen zwischen zwei ONTAP Clustern an separaten Standorten oder Ausfall-Domains synchron spiegelt. MetroCluster bietet kontinuierlich verfügbaren Storage für Applikationen, indem es automatisch zwei Ziele bewältigt: Recovery Point Objective (RPO) von null durch synchrones Spiegeln von Daten, die auf das Cluster geschrieben werden. Recovery Time Objective (RTO) von nahezu null durch Spiegelung der Konfiguration und automatisierten Zugriff auf Daten am zweiten Standort MetroCluster sorgt für Einfachheit durch automatische Spiegelung von Daten und Konfigurationen zwischen den beiden unabhängigen Clustern an den beiden Standorten. Wenn Storage innerhalb eines Clusters bereitgestellt wird, wird dieser automatisch auf das zweite Cluster am zweiten Standort gespiegelt. Die NetApp SyncMirror-Technologie sorgt für eine komplette Kopie aller Daten mit einem RPO von null. , So können Workloads von einem Standort aus jederzeit auf den anderen Standort umschalten und weiterhin Daten ohne Datenverlust bereitstellen. Weitere Informationen finden Sie hier "Hier".

Netzwerkbetrieb

Ein Cisco Nexus Switch-Paar stellt redundante Pfade für den IP-Datenverkehr vom Computing zum Storage und für externe Clients der Image-Viewer des medizinischen Bildgebungssystems bereit:

- Die Link-Aggregation, die Port-Kanäle und vPCs nutzt, wird durchgehend verwendet, was das Design für eine höhere Bandbreite und hohe Verfügbarkeit ermöglicht:
  - VPC wird zwischen dem NetApp Storage-Array und den Cisco Nexus Switches verwendet.
  - VPC wird zwischen dem Cisco UCS Fabric Interconnect und den Cisco Nexus Switches verwendet.
  - Jeder Server verfügt über virtuelle Netzwerk-Schnittstellenkarten (vNICs) mit redundanter Konnektivität zum Unified Fabric. Für Redundanz wird NIC Failover zwischen Fabric Interconnects verwendet.
  - Jeder Server verfügt über virtuelle Host Bus Adapter (vHBAs) mit redundanter Konnektivität zum Unified Fabric.
- Die Cisco UCS Fabric Interconnects sind gemäß der Empfehlung im End-Host-Modus konfiguriert, sodass vNICs dynamisch an Uplink-Switches gepinnen werden.
- Ein FC-Storage-Netzwerk wird von einem Paar Cisco MDS Switches bereitgestellt.

Computing – Cisco Unified Computing System

Zwei Cisco UCS Fabrics über verschiedene Fabric Interconnects bieten zwei Ausfall-Domains. Jede Fabric ist sowohl mit IP-Netzwerk-Switches als auch mit unterschiedlichen FC-Netzwerk-Switches verbunden.

Zum Ausführen von VMware ESXi werden für jedes Cisco UCS Blade identische Service-Profile gemäß den Best Practices von FlexPod erstellt. Jedes Service-Profil sollte die folgenden Komponenten aufweisen:

- Zwei vNICs (eine pro Fabric) für NFS, SMB/CIFS und Client- oder Management-Datenverkehr
- Zusätzliche erforderliche VLANs für die vNICs für NFS, SMB/CIFS und Client- oder Managementdatenverkehr
- Zwei vNICs (einer auf jeder Fabric) für den iSCSI-Datenverkehr
- Zwei Storage FC HBAs (einer pro Fabric) für FC-Datenverkehr zum Storage
- SAN Booting

Einheitliche

Auf dem VMware ESXi-Host-Cluster werden Workload-VMs ausgeführt. Der Cluster umfasst ESXi Instanzen, die auf Cisco UCS Blade-Servern ausgeführt werden.

Jeder ESXi-Host umfasst die folgenden Netzwerkkomponenten:

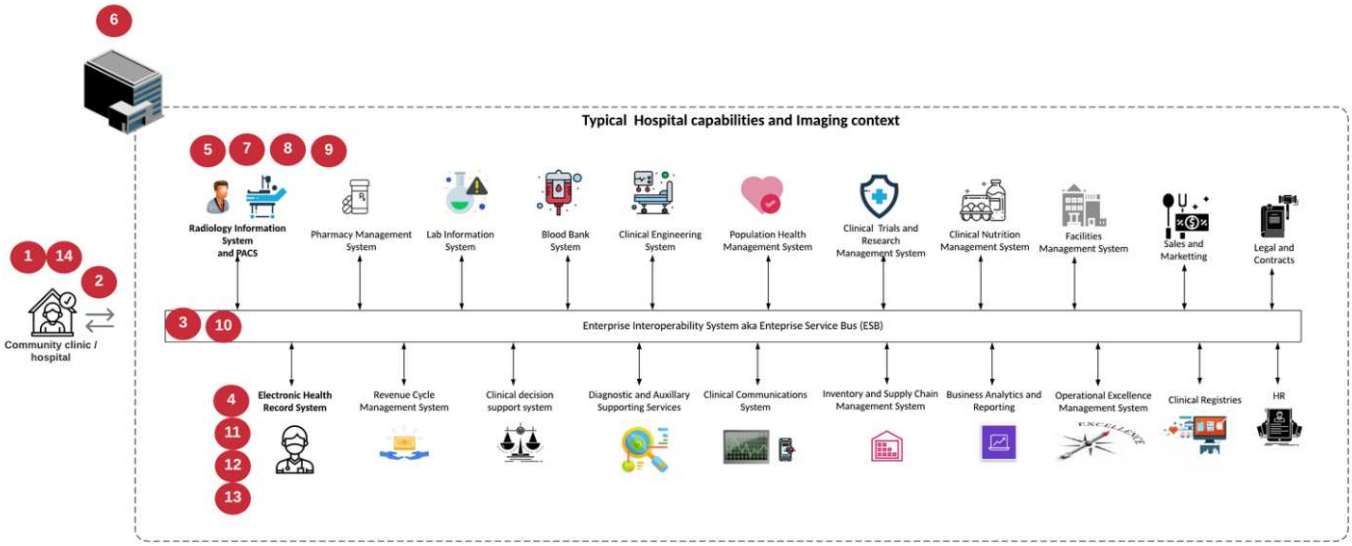
- SAN Booting über FC oder iSCSI
- Boot-LUNs auf NetApp Storage (in einem dedizierten FlexVol für Boot OS)
- Zwei vmnics (Cisco UCS vNIC) für NFS, SMB/CIFS oder Managementverkehr
- Zwei Storage HBAs (Cisco UCS FC vHBA) für FC-Datenverkehr zum Storage
- Standard-Switch oder verteilter virtueller Switch (je nach Bedarf)
- NFS-Datenspeicher für Workload VMs
- Management, Client-Traffic-Netzwerk und Storage-Netzwerk-Port-Gruppen für VMs
- Netzwerkadapter für Management, Client-Traffic und Storage-Zugriff (NFS, iSCSI oder SMB/CIFS) für jede VM
- VMware DRS ist aktiviert
- Natives Multipathing für FC- oder iSCSI-Pfade zum Storage aktiviert
- Deaktiviert die VMware Snapshots für VM
- NetApp SnapCenter für VMware für VM-Backups implementiert

Architektur des Bildgebungssystems für den medizinischen Bereich

In medizinischen Einrichtungen sind Bildgebungssysteme wichtige Applikationen und gut in die klinischen Workflows integriert – angefangen bei der Registrierung von Patienten bis hin zur Abrechnung über Aktivitäten im Umsatzzyklus.

Das folgende Diagramm zeigt die verschiedenen Systeme in einem typischen großen Krankenhaus; dieses Diagramm soll einen architektonischen Kontext zu einem medizinischen Bildgebungssystem liefern, bevor wir in die architektonischen Komponenten eines typischen medizinischen Bildgebungssystems hineinzoomen. Die Workflows unterscheiden sich sehr stark und sind für Krankenhäuser und Anwendungsfälle spezifisch.

Die Abbildung unten zeigt das medizinische Bildgebungssystem im Kontext eines Patienten, einer Gemeinschaftsklinik und eines großen Krankenhauses.



1. Der Patient besucht die Gemeinschaftsklinik mit Symptomen. Während der Konsultation legt der Gemeindearzt einen Bildgebungsauftrag auf, der in Form einer HL7-Auftragsnachricht an das größere

Krankenhaus geschickt wird.

2. Das EHR-System des Hausarztes sendet die HL7 Order/ORD-Nachricht an das große Krankenhaus.
3. Das Enterprise-Interoperabilitätssystem (auch bekannt als Enterprise Service Bus [ESB]) verarbeitet die Auftragsmeldung und sendet die Auftragsnachricht an das EHR-System.
4. Das EHR verarbeitet die Auftragsnachricht. Wenn kein Patientendatensatz vorhanden ist, wird ein neuer Patientendatensatz erstellt.
5. Der EHR-Auftrag sendet an das medizinische Bildgebungssystem.
6. Der Patient ruft das große Krankenhaus für einen Bildgebungstermin an.
7. Der Bildgebungs-Empfang und der Registrierungstisch planen den Patienten für einen Bildgebungstermin mit Hilfe von Radiologie-Informationen oder ähnlichen Systemen.
8. Der Patient kommt zum Termin für die Bildgebung, und die Bilder oder Videos werden erstellt und an das PACS gesendet.
9. Der Radiologe liest die Bilder und kommentiert die Bilder im PACS mit einem High-End-/GPU-Grafikprogramm. Bestimmte Bildgebungssysteme verfügen über AI-gestützte Funktionen zur Effizienzsteigerung, die in die Workflows für die Bildgebung integriert sind.
10. Die Ergebnisse der Bildbestellung werden in Form eines Auftragsergebnisses HL7 ORU über das ESB an die EHR gesendet.
11. Das EHR verarbeitet die Auftragsergebnisse in den Patientendatensatz, platziert das Miniaturbild mit einem kontextgerechten Link zum tatsächlichen DICOM-Bild. Ärzte können die Diagnose-Anzeige starten, wenn ein Bild mit höherer Auflösung aus dem EHR-System benötigt wird.
12. Der Arzt überprüft das Bild und gibt Arztnotizen in die Patientenakte ein. Der Arzt könnte das klinische Entscheidungsunterstützungssystem nutzen, um den Review-Prozess zu verbessern und bei der richtigen Diagnose für den Patienten zu helfen.
13. Das EHR-System sendet dann die Auftragsergebnisse in Form einer Auftragsergebnismeldung an das Gemeinschaftskrankenhaus. Wenn das Gemeinschaftskrankenhaus das vollständige Bild erhalten konnte, wird das Bild entweder über WADO oder DICOM gesendet.
14. Der Hausarzt schließt die Diagnose ab und stellt dem Patienten weitere Schritte zur Verfügung.

Ein typisches Bildgebungssystem verwendet eine N- Tiered Architecture. Die Kernkomponente eines medizinischen Bildgebungssystems ist ein Anwendungsserver, auf dem verschiedene Anwendungskomponenten gehostet werden. Typische Anwendungsserver basieren entweder auf Java Runtime oder auf C# .Net CLR. Die meisten medizinischen Bildgebungslösungen für Unternehmen verwenden einen Oracle Database Server, MS SQL Server oder Sybase als primäre Datenbank. Darüber hinaus verwenden einige medizinische Bildgebungssysteme der Enterprise-Klasse Datenbanken auch zur Content-Beschleunigung und zum Caching über eine geografische Region. Einige medizinische Bildgebungssysteme in Unternehmen verwenden auch NoSQL Datenbanken wie MongoDB, Redis usw. in Verbindung mit Servern zur Unternehmensintegration für DICOM-Schnittstellen und oder APIs.

Ein typisches medizinisches Bildgebungssystem bietet Zugriff auf Bilder für zwei unterschiedliche Benutzer: Diagnostischer Benutzer/Radiologe oder Arzt, der die Bildgebung bestellt hat.

Radiologen nutzen normalerweise High-End-, Grafikprogramme, die auf High-End-Computing- und Grafikworkstationen ausgeführt werden, die entweder physisch oder als Teil einer virtuellen Desktop-Infrastruktur ausgeführt werden. Wenn Sie den Weg hin zu einer Virtual Desktop Infrastructure antreten möchten, finden Sie weitere Informationen "Hier".

Als der Hurrikan Katrina zwei der größten Lehrkrankenhäuser Louisianas zerstörte, kamen führende Persönlichkeiten zusammen und bauten ein stabiles elektronisches Krankenakten-System mit mehr als 3000 virtuellen Desktops in Rekordzeit auf. Weitere Informationen zur Referenzarchitektur für Anwendungsfälle und

zu FlexPod Referenzpaketen finden Sie "Hier".

Klinikpersonal kann auf zwei primäre Arten auf Bilder zugreifen:

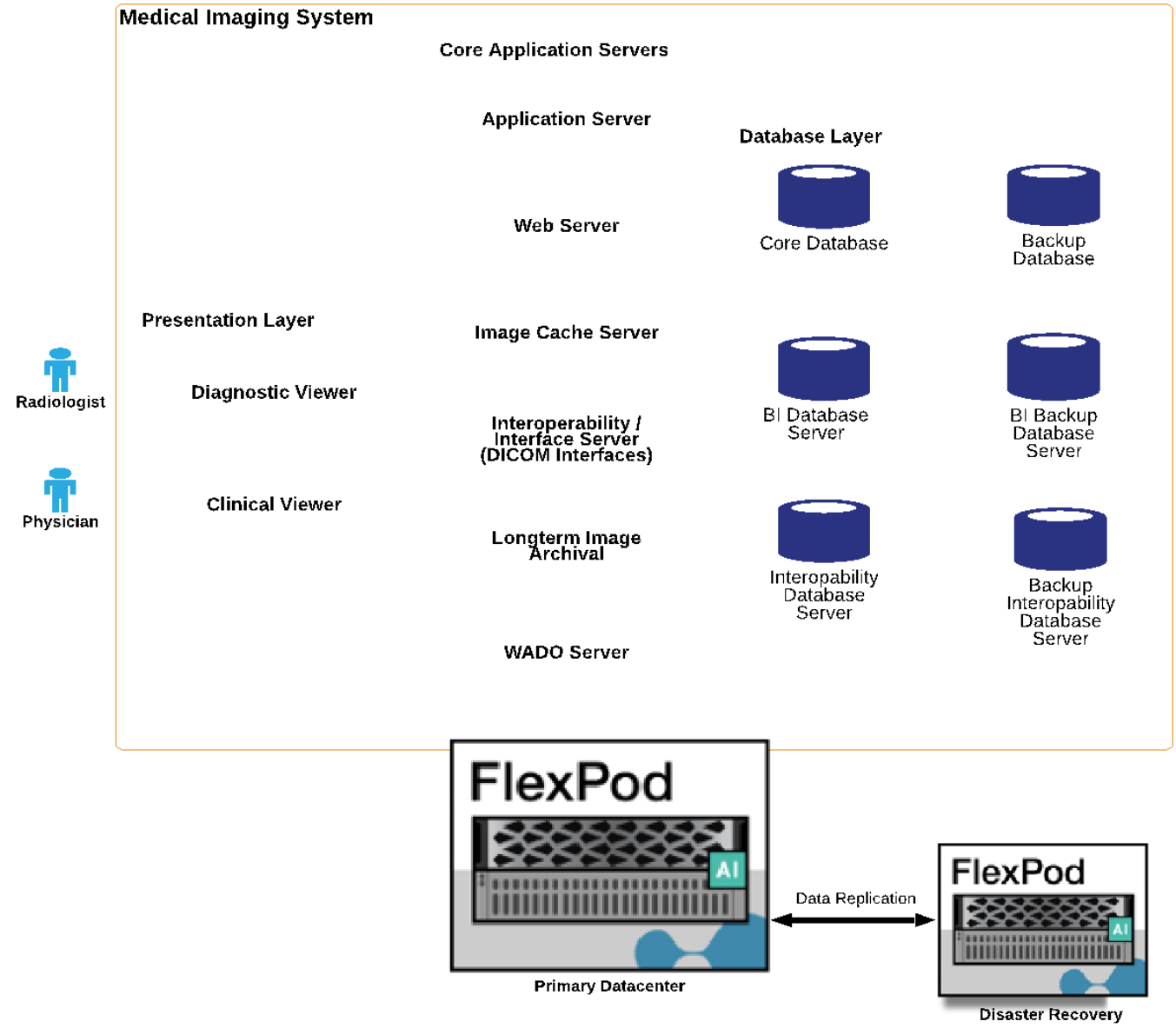
- **Webbasierter Zugriff.**, der in der Regel von EHR-Systemen verwendet wird, um PACS-Bilder als kontextbezogene Links in die elektronische Patientenakte (Electronic Medical Record, EMR) des Patienten zu integrieren, und Links, die in Bildgebungs-Workflows, Verfahren-Workflows, Fortschrittsnotizen-Workflows usw. platziert werden können. Über webbasierte Links können Patienten auch über Patientenportale auf Bilder zugreifen. Der webbasierte Zugriff verwendet ein Technologiemuster, das kontextbezogene Links genannt wird. Kontextbezogene Verknüpfungen können entweder statische Links/URIs mit den DICOM-Medien direkt oder dynamisch generierte Links/URIs unter Verwendung benutzerdefinierter Makros sein.
- **Thick Client.** einige medizinische Systeme des Unternehmens ermöglichen es Ihnen auch, einen Thick-Client-basierten Ansatz zu verwenden, um die Bilder anzuzeigen. Sie können einen Thick Client über das EMR des Patienten oder als eigenständige Anwendung starten.

Das medizinische Bildgebungssystem kann einen Bildzugriff auf eine Ärztegemeinschaft oder an CIN-beteiligte Ärzte ermöglichen. Typische medizinische Bildgebungssysteme umfassen Komponenten, die die Interoperabilität von Bildern mit anderen IT-Systemen im Gesundheitswesen innerhalb und außerhalb Ihres Unternehmens ermöglichen. Community-Ärzte können entweder über eine webbasierte Anwendung auf Bilder zugreifen oder eine Image Exchange-Plattform für die Interoperabilität von Bildern nutzen. Bildaustauschplattformen verwenden normalerweise entweder WADO oder DICOM als zugrunde liegendes Bildaustauschprotokoll.

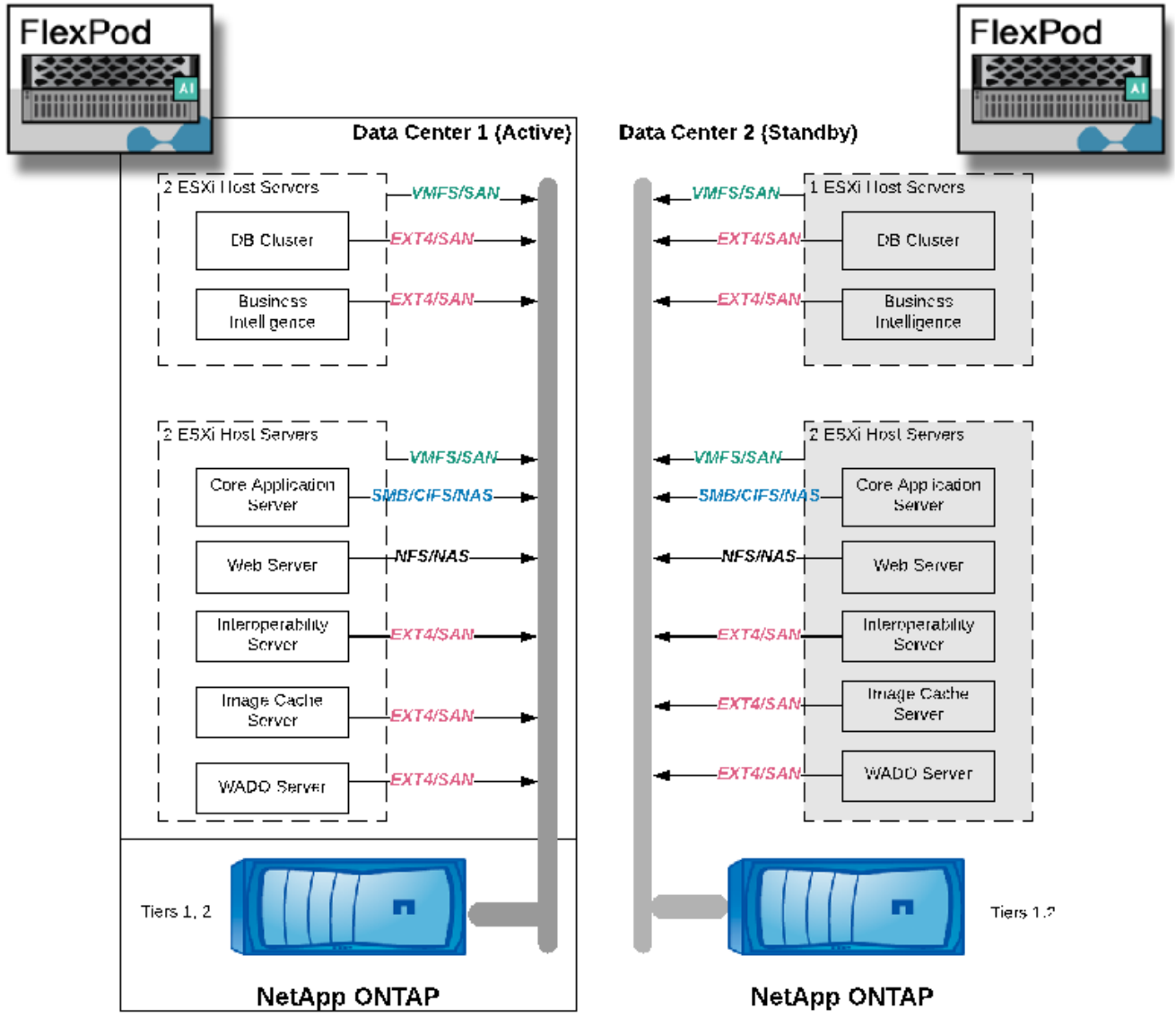
Medizinische Bildgebungssysteme können auch akademische medizinische Zentren unterstützen, die PACS- oder Bildgebungssysteme für den Einsatz in einem Klassenzimmer benötigen. Zur Unterstützung akademischer Aktivitäten kann ein typisches System für medizinische Bildgebung die Funktionen eines PACS-Systems in einem kleineren System oder einer nur für Lehre bestimmten Bildgebungsumgebung nutzen. Typische anbieterunabhängige Archivierungssysteme und einige medizinische Bildgebungssysteme der Enterprise-Klasse bieten Funktionen zum Morphing von DICOM-Bildern, um die für Lehrzwecke verwendeten Bilder zu anonymisieren. Durch Tag Morphing können medizinische Einrichtungen DICOM-Bilder anbieterunabhängig zwischen medizinischen Bildgebungssystemen verschiedener Anbieter austauschen. Durch Tag Morphing können medizinische Bildgebungssysteme eine unternehmensweite, anbieterneutrale Archivierungsfunktion für medizinische Bilder implementieren.

Medizinische Bildgebungssysteme werden "GPU-basierte Computing-Funktionen" allmählich zur Verbesserung menschlicher Workflows genutzt, indem sie die Bilder vorverarbeiten und so die Effizienz erhöhen. Typische medizinische Bildgebungssysteme der Enterprise-Klasse nutzen die branchenführenden NetApp Storage-Effizienzfunktionen. Medizinische Bildgebungssysteme der Enterprise-Klasse verwenden RMAN für Backup-, Recovery- und Wiederherstellungsvorgänge. Um die Performance zu verbessern und die für das Backup benötigte Zeit zu verkürzen, ist die Snapshot Technologie für Backup-Vorgänge verfügbar. Zudem ist die SnapMirror Technologie für die Replizierung verfügbar.

Die Abbildung unten zeigt die logischen Applikationskomponenten in einer vielschichtigen Architekturansicht.



Die Abbildung unten zeigt die physischen Applikationskomponenten.



Die logischen Applikationskomponenten erfordern, dass die Infrastruktur eine Vielzahl von Protokollen und Filesystemen unterstützt. Die NetApp ONTAP Software unterstützt branchenführende Protokolle und Filesysteme.

In der folgenden Tabelle sind die Applikationskomponenten, das Storage-Protokoll und die Anforderungen an das Filesystem aufgeführt.

Anwendungskomponente	SAN/NAS	Typ des Filesystems	Storage-Tier	Replizierungstyp
VMware Host-Prod DB	Vor Ort	San	VMFS	Tier 1
Applikation	VMware Host-Prod DB	REP	San	VMFS
Tier 1	Applikation	VMware Host-Prod-Applikation	Vor Ort	San

Anwendungskomponente	SAN/NAS	Typ des Filesystems	Storage-Tier	Replizierungstyp
VMFS	Tier 1	Applikation	VMware Host-Prod-Applikation	REP
San	VMFS	Tier 1	Applikation	Hauptdatenbankserver
San	Ext4	Tier 1	Applikation	Backup-Datenbankserver
San	Ext4	Tier 1	Keine	Image-Cache-Server
NAS	SMB/CIFS	Tier 1	Keine	Archiv-Server
NAS	SMB/CIFS	Ebene 2	Applikation	Web-Server
NAS	SMB/CIFS	Tier 1	Keine	WADO Server
San	NFS	Tier 1	Applikation	Business Intelligence Server
San	NTFS	Tier 1	Applikation	Business Intelligence Backup
San	NTFS	Tier 1	Applikation	Interoperabilitäts-Server
San	Ext4	Tier 1	Applikation	Interoperabilitäts-Datenbankserver

Hardware- und Softwarekomponenten der Lösungsinfrastruktur

In den folgenden Tabellen sind die Hardware- bzw. Softwarekomponenten der FlexPod-Infrastruktur für das medizinische Bildgebungssystem aufgeführt.

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1 oder 2	Basierend auf der Anzahl der Blades, die zur Unterstützung der Anzahl der jährlichen Studien benötigt werden
	Cisco UCS Blade Server	B200 M5	Anzahl der Blades basierend auf der Anzahl der Studien jährlich mit 2 x 20 oder mehr Kernen, 2,7 GHz und 128 bis 384 GB RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Siehe
	2 Cisco UCS Fabric Interconnects	6454 oder höher	–

Schicht	Produktfamilie	Menge und Modell	Details
Netzwerk	Cisco Nexus Switches	2 Cisco Nexus 3000-Serie oder 9000-Serie	–
Datennetzwerk Storage-Netzwerk	IP-Netzwerk für Storage-Zugriff über SMB-/CIFS-, NFS- oder iSCSI-Protokolle	Gleiche Netzwerk-Switches wie oben	–
	Storage-Zugriff über FC	2 x Cisco MDS 9132T	–
Storage	NetApp AFF A400 All-Flash-Storage-System	1 oder mehr HA-Paar	Cluster mit zwei oder mehr Nodes
	Festplatten-Shelf	1 oder mehr DS224C oder NS224 Festplatten-Shelfs	Vollständig mit 24 Laufwerken bestückt
	SSD	>24, 1,2 TB oder mehr Kapazität	–

Software	Produktfamilie	Version/Release	Details
Medizinisches Bildgebungssystem der Enterprise-Klasse			
	MS SQL oder Oracle Database Server	Wie vom Anbieter medizinischer Bildgebungssysteme empfohlen	
	Keine SQL-DBs wie MongoDB Server	Wie vom Anbieter medizinischer Bildgebungssysteme empfohlen	
	Applikationsserver	Wie vom Anbieter medizinischer Bildgebungssysteme empfohlen	
	Integrationsserver (MS BizTalk, MultiSoft, Rhapsody, TIBCO)	Wie vom Anbieter medizinischer Bildgebungssysteme empfohlen	
	VMs	Linux (64 Bit)	
	VMs	Windows Server (64 Bit)	
Storage	ONTAP	ONTAP 9.7 oder höher	
Netzwerk	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 oder höher	
	Cisco Ethernet Switches	9.2(3)I7(2) oder höher	
	Cisco FC: Cisco MDS 9132T	8.4(2) oder höher	
Hypervisor	Hypervisor	VMware vSphere ESXi 6.7 U2 oder höher	

Software	Produktfamilie	Version/Release	Details
Vereinfachtes	Hypervisor-Managementsystem	VMware vCenter Server 6.7 U1 (vCSA) oder höher	
	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	
	SnapCenter	SnapCenter 4.3 oder höher	

Dimensionierung der Lösung

Storage-Dimensionierung

In diesem Abschnitt werden die Anzahl der Studien und die entsprechenden Infrastrukturanforderungen beschrieben.

Die in der folgenden Tabelle aufgeführten Speicheranforderungen gehen davon aus, dass die bestehenden Daten einen Wert von 1 Jahr haben und ein prognostiziertes Wachstum für ein Studienjahr im Primärsystem (Tier 1, 2) prognostiziert wird. Zusätzlicher Storage-Bedarf für das prognostizierte Wachstum von 3 Jahren über die ersten zwei Jahre hinaus wird separat aufgeführt.

	Klein	Mittel	Groß
Jährliche Studien	<250.000 Studien	250.000 bis 500.000 Studien	500.000–1 Million Studien
Tier-1-Storage			
IOPS (durchschnittlich)	1.5.000 BIS 5.000	5.000 BIS 15.000 U/MIN	15.000–40.000
IOPS (Spitzenauslastung)	5.000	20K	65.000
Durchsatz	50 bis 100 Mbit/s	50 bis 150 Mbit/s	100 bis 300 Mbit/s
Capacity Datacenter 1 (1 Jahr alte Daten und 1 Jahr neue Studie)	70 TB	140 TB	250 TB
Capacity Datacenter 1 (zusätzlicher Bedarf für 4 Jahre für neue Studie)	25 TB	45 TB	80 TB
Capacity Datacenter 2 (1 Jahr alte Daten und 1 Jahr neue Studie)	45 TB	110 TB	165 TB
Capacity Datacenter 2 (zusätzlicher Bedarf für 4 Jahre für neue Studie)	25 TB	45 TB	80 TB
Tier-2-Storage			
IOPS (durchschnittlich)	1K	2 K	3K
Kapazität Datacenter 1	320 TB	800 TB	2000 TB

Dimensionierung von Computing

In der folgenden Tabelle sind die Computing-Anforderungen für kleine, mittlere und große medizinische Bildgebungssysteme aufgeführt.

	Klein	Mittel	Groß
Jährliche Studien	<250.000 Studien	250.000 bis 500.000 Studien	500.000–1 Million Studien
Datacenter 1			
Anzahl der VMs	21	27	35
Gesamtzahl der virtuellen CPUs (vCPU	56	124	220
Gesamtspeicherbedarf	22GB	450 GB	900 GB
Spezifikationen für physischen Server (Blades) (vorausgesetzt 1 vCPU - = 1 Core)	4 x Server mit jeweils 20 Kernen und 192 GB RAM	8 x Server mit 20 Cores und jeweils 128 GB RAM	14 x Server mit 20 Cores und jeweils 128 GB RAM
Datacenter 2			
Anzahl der VMs	15	17	22
Gesamtzahl der vCPUs	42	72	140
Gesamtspeicherbedarf	179 GB	243 GB	513 GB
Spezifikationen für physischen Server (Blades) (vorausgesetzt 1 vCPU = 1 Kern)	3 x Server mit 20 Kernen und 168 GB RAM	6 x Server mit 20 Cores und jeweils 128 GB RAM	8 x Server mit 24 Cores und jeweils 128 GB RAM

Dimensionierung der Netzwerk- und Cisco UCS-Infrastruktur

In der folgenden Tabelle sind die Netzwerkanforderungen und die Anforderungen an die Cisco UCS Infrastruktur für kleine, mittlere und große medizinische Bildgebungssysteme aufgeführt.

	Klein	Mittel	Groß
Datacenter 1			
Anzahl der Storage-Node-Ports	2 konvergierte Netzwerkadapter (CNAs); 2 FCS	2 CNAs; 2 FCS	2 CNAs; 2 FCS
IP-Netzwerk-Switch-Ports (Cisco Nexus 9000)	Switch mit 48 Ports	Switch mit 48 Ports	Switch mit 48 Ports
FC-Switch (Cisco MDS)	Switch mit 32 Ports	Switch mit 32 Ports	Switch mit 48 Ports
Anzahl der Cisco UCS Gehäuse	1 x 5108	1 x 5108	2 x 5108
Cisco UCS Fabric Interconnect	2 x 6332	2 x 6332	2 x 6332

	Klein	Mittel	Groß
Datacenter 2			
Anzahl der Cisco UCS Gehäuse	1 x 5108	1 x 5108	1 x 5108
Cisco UCS Fabric Interconnect	2 x 6332	2 x 6332	2 x 6332
Anzahl der Storage-Node-Ports	2 CNAs; 2 FCS	2 CNAs; 2 FCS	2 CNAs; 2 FCS
IP-Netzwerk-Switch-Ports (Cisco Nexus 9000)	Switch mit 48 Ports	Switch mit 48 Ports	Switch mit 48 Ports
FC-Switch (Cisco MDS)	Switch mit 32 Ports	Switch mit 32 Ports	Switch mit 48 Ports

Best Practices in sich vereint

Best Practices für Storage

Hochverfügbarkeit

Das NetApp Storage Cluster Design bietet Hochverfügbarkeit auf jeder Ebene:

- Cluster-Nodes
- Back-End Storage-Konnektivität
- RAID-TEC zum Scheitern von drei Festplatten
- RAID DP zur Unterstützung des Ausfalls von zwei Festplatten
- Physische Konnektivität mit zwei physischen Netzwerken von jedem Node
- Mehrere Datenpfade zu Storage-LUNs und Volumes

Sichere Mandantenfähigkeit

NetApp Storage Virtual Machines (SVMs) bieten ein Virtual Storage Array-Konstrukt, das Ihre Sicherheitsdomäne, Ihre Richtlinien und Ihr virtuelles Networking voneinander trennt. NetApp empfiehlt die Erstellung separater SVMs für jede Mandantenorganisation, die Daten im Storage Cluster hostet.

Best Practices für NetApp Storage

Folgende NetApp Best Practices für Storage sind zu berücksichtigen:

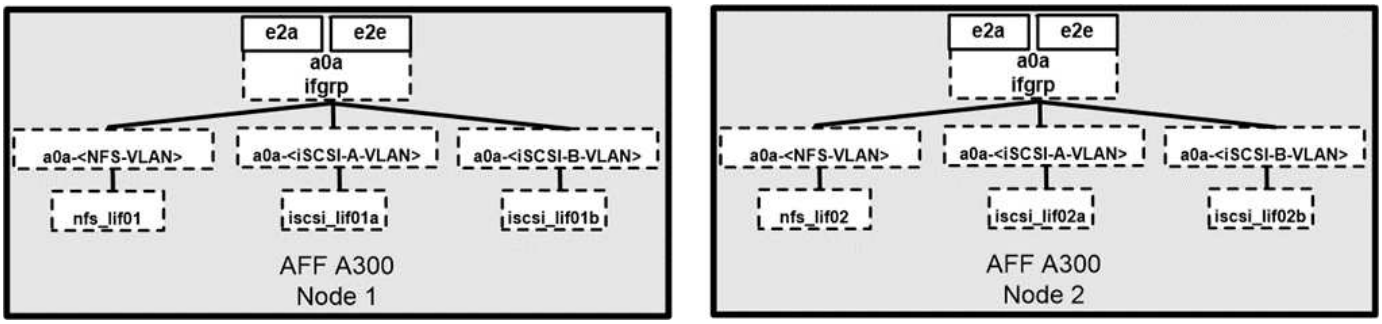
- Aktivieren Sie immer die NetApp AutoSupport-Technologie, die Support-Übersichtsinformationen an NetApp über HTTPS sendet.
- Vergewissern Sie sich, dass für jede SVM auf jedem Node im NetApp ONTAP Cluster eine LIF erstellt wird, um maximale Verfügbarkeit und Mobilität zu gewährleisten. Mithilfe des Asymmetric Logical Unit Access (ALUA) werden Pfade geparst und aktive optimierte (direkte) Pfade im Gegensatz zu aktiven nicht optimierten Pfaden identifiziert. ALUA wird für FC oder FCoE und iSCSI verwendet.
- Ein Volume, das nur LUNs enthält, muss nicht intern gemountet werden. Zudem ist kein Verbindungspfad erforderlich.
- Wenn Sie das CHAP (Challenge-Handshake Authentication Protocol) in ESXi für die Zielauthentifizierung verwenden, müssen Sie es auch in ONTAP konfigurieren. Verwenden Sie die CLI (`vserver iscsi`

`security create`) Oder NetApp ONTAP System Manager (bearbeiten Sie die Initiatorsicherheit unter „Storage“ > „SVMs“ > „SVM-Einstellungen“ > „Protocols“ > „iSCSI“).

SAN Booting

NetApp empfiehlt die Implementierung von SAN-Starts für Cisco UCS Server in der FlexPod Datacenter Lösung. Das Betriebssystem kann mit diesem Schritt sicher durch das NetApp AFF Storage-System gesichert werden, wodurch eine bessere Performance erzielt wird. Das in dieser Lösung beschriebene Design verwendet iSCSI SAN Boot.

Beim Booten über iSCSI SAN werden jedem Cisco UCS Server zwei iSCSI vNICs zugewiesen (einer für jede SAN-Fabric), die dem Storage redundante Konnektivität bieten. Die Speicher-Ports in diesem Beispiel, e2a und e2e, die mit den Cisco Nexus-Switches verbunden sind, werden zu einem logischen Port zusammengefasst, einer Interface Group (ifrp) (in diesem Beispiel a0a). Die iSCSI-VLANs werden auf der Initiatorgruppe erstellt, und die iSCSI-LIFs werden auf iSCSI-Portgruppen erstellt (in diesem Beispiel a0a-<iSCSI-A-VLAN>). Die iSCSI-Boot-LUN wird über die iSCSI-LIF den Servern mittels iGroups zur Verfügung gestellt. Dieser Ansatz ermöglicht es nur dem autorisierten Server, auf die Boot-LUN zuzugreifen. Informationen zu dem Port und dem LIF-Layout finden Sie in der Abbildung unten.



Anders als NAS-Netzwerkschnittstellen werden die SAN-Netzwerkschnittstellen nicht für den Failover beim Ausfall konfiguriert. Wenn stattdessen eine Netzwerkschnittstelle nicht mehr verfügbar ist, wählt der Host einen neuen optimierten Pfad zu einer verfügbaren Netzwerkschnittstelle aus. ALUA, ein von NetApp unterstützter Standard, bietet Informationen zu SCSI-Zielen, sodass ein Host den besten Pfad zum Storage ermitteln kann.

Storage-Effizienz und Thin Provisioning

NetApp gehört bereits zu den Branchenführern im Bereich der Innovationen im Bereich Storage-Effizienz, beispielsweise mit der ersten Deduplizierung für primäre Workloads und mit Inline-Data-Compaction, durch die eine stärkere Komprimierung erzielt und kleine Dateien sowie I/O-Daten effizient gespeichert werden. ONTAP unterstützt sowohl die Inline-Hintergrund-Deduplizierung als auch die Inline- und Hintergrund-Komprimierung.

Um die Vorteile der Deduplizierung in einer Blockumgebung ganz auszuschöpfen, müssen die LUNs einem Thin Provisioning unterzogen werden. Die jeweilige LUN wird dem VM-Administrator weiter so angezeigt, als ob sie die bereitgestellte Kapazität in Anspruch nimmt, allerdings werden die durch Deduplizierung erzielten Einsparungen dem Volume zugeführt und stehen dann für andere Zwecke zur Verfügung. NetApp empfiehlt, diese LUNs in FlexVol Volumes zu implementieren, die ebenfalls mit einem Thin Provisioning bereitgestellt sind und mit einer Kapazität die doppelte Größe der LUN aufweisen. Wenn Sie die LUN auf diese Weise bereitstellen, fungiert das FlexVol Volume als reines Kontingent. Der von der LUN konsumiert Storage wird im FlexVol Volume und dem zugehörigen Container-Aggregat.

Um maximale Einsparungen durch Deduplizierung zu erzielen, sollten Sie eventuell eine Hintergrund-Deduplizierung planen. Diese Prozesse nutzen jedoch Systemressourcen, wenn sie laufen. Sie sollten sie idealerweise in weniger aktiven Zeiten (z. B. an Wochenenden) planen oder häufiger ausführen, damit weniger geänderte Daten verarbeitet werden müssen. Die automatische Hintergrund-Deduplizierung für AFF Systeme hat geringere Auswirkungen auf Vordergrundaktivitäten. Die Hintergrund-Komprimierung (für

festplattenbasierte Systeme) verbraucht ebenfalls Ressourcen, sodass Sie sie nur für sekundäre Workloads mit begrenzten Performance-Anforderungen in Betracht ziehen sollten.

Um Servicequalität bieten zu können

Systeme mit ONTAP Software können mithilfe der ONTAP Storage-QoS-Funktion den Durchsatz in Megabit pro Sekunde (MB/s) begrenzen und die IOPS für unterschiedliche Storage-Objekte wie Dateien, LUNs, Volumes oder ganze SVMs beschränken. Durch anpassungsfähige QoS wird eine IOPS-Untergrenze (Minimum für QoS) und eine Obergrenze (Maximum an QoS) festgelegt, die basierend auf der Datastore-Kapazität und dem belegten Speicherplatz dynamisch angeglichen werden.

Durchsatzbegrenzungen sind für die Steuerung unbekannter Workloads oder von Test-Workloads vor einer Implementierung nützlich, um zu bestätigen, dass sie sich nicht auf andere Workloads auswirken. Sie können diese Einschränkungen auch einsetzen, um einen als problematisch identifizierten Workload einzuschränken. Minimale Service-Level auf Basis der IOPS werden ebenfalls unterstützt, um SAN-Objekten in ONTAP eine konsistente Performance bereitzustellen.

Bei einem NFS-Datastore kann eine QoS-Richtlinie auf das gesamte FlexVol Volume oder auf darin einzelne VMDK-Dateien (Virtual Machine Disk) angewendet werden. Mit VMFS Datastores (Cluster Shared Volumes [CSV] in Hyper-V), die ONTAP LUNs verwenden, können Sie die QoS-Richtlinien auf das FlexVol Volume anwenden, das die LUNs enthält, oder auf die einzelnen LUNs. Da ONTAP jedoch das VMFS nicht erkennt, können Sie die QoS-Richtlinien nicht auf einzelne VMDK-Dateien anwenden. Wenn Sie VMware Virtual Volumes (VVols) mit VSC 7.1 oder höher verwenden, können Sie mithilfe des Storage-Funktionsprofils maximale QoS für einzelne VMs festlegen.

Wenn Sie eine QoS-Richtlinie einschließlich VMFS oder CSV einer LUN zuweisen möchten, erhalten Sie die ONTAP SVM (angezeigt als) `Vserver`), LUN-Pfad und Seriennummer aus dem Menü Storage Systems auf der VSC Startseite. Wählen Sie das Storage-System (SVM) und anschließend „Related Objects“ > „SAN“ aus. Verwenden Sie diesen Ansatz, wenn Sie die QoS mit einem der ONTAP Tools angeben.

Sie können die maximale QoS-Durchsatzbegrenzung für ein Objekt in Megabit pro Sekunde und in IOPS festlegen. Wenn Sie beides verwenden, wird das erste erreichte Limit von ONTAP durchgesetzt. Ein Workload kann mehrere Objekte umfassen. Auf einen oder mehrere Workloads kann eine QoS-Richtlinie angewendet werden. Wenn Sie eine Richtlinie auf mehrere Workloads anwenden, teilen diese das in der Richtlinie zulässige Gesamtlimit. Geschachtelte Objekte werden nicht unterstützt (so kann beispielsweise nicht jede einzelne Datei in einem Volume eine eigene Richtlinie aufweisen). QoS-Mindestwerte können nur als IOPS angegeben werden.

Storage-Layout

Dieser Abschnitt enthält Best Practices für das Layout von LUNs, Volumes und Storage-Aggregaten.

Storage-LUNs

Zur optimalen Performance, Management und Backup empfiehlt NetApp die folgenden LUN-Design Best Practices:

- Erstellen Sie eine separate LUN zum Speichern von Datenbank- und Protokolldateien.
- Erstellen Sie eine separate LUN für jede Instanz, um Oracle Datenbank-Protokoll-Backups zu speichern. Die LUNs können Teil desselben Volumes sein.
- Stellen Sie LUNs mit Thin Provisioning bereit (deaktivieren Sie die Option „Speicherplatzreservierung“) für Datenbankdateien und Log-Dateien.
- Alle Bilddaten werden in FC LUNs gehostet. Erstellen Sie diese LUNs in FlexVol Volumes, die über die Aggregate verteilt sind, die Eigentum verschiedener Storage Controller Nodes sind.

Folgen Sie den Richtlinien im nächsten Abschnitt, um die LUNs in einem Storage Volume zu platzieren.

Storage Volumes

Für optimale Performance und optimalen Management empfiehlt NetApp die folgenden Best Practices für das Volume-Design:

- Isolierung von Datenbanken mit I/O-intensiven Abfragen auf separaten Storage Volumes
- Die Datendateien können auf eine einzelne LUN oder ein Volume platziert werden, aber für einen höheren Durchsatz werden mehrere Volumes/LUNs empfohlen.
- I/O-Parallelität kann durch die Verwendung eines beliebigen unterstützten Dateisystems erreicht werden, wenn mehrere LUNs verwendet werden.
- Platzieren Sie Datenbankdateien und Transaktionsprotokolle auf separaten Volumes, um die Recovery-Granularität zu erhöhen.
- Volume-Attribute wie automatische Größe, Snapshot Reserve, QoS usw. sollten in Betracht gezogen werden.

Aggregate

Aggregate sind der primäre Storage Container für NetApp Storage-Konfigurationen. Sie enthalten eine oder mehrere RAID-Gruppen, die aus Daten-Festplatten und Parity-Festplatten bestehen.

NetApp hat verschiedene Charakterisierungstests für I/O-Workloads mithilfe von gemeinsam genutzten und dedizierten Aggregaten mit separaten Datendateien und Transaktions-Log-Dateien durchgeführt. Die Tests zeigen, dass ein großes Aggregat mit mehreren RAID-Gruppen und -Laufwerken (HDDs oder SSDs) die Storage Performance optimiert und verbessert und Administratoren aus zwei Gründen einfacher zu managen ist:

- Ein großes Aggregat ermöglicht die I/O-Fähigkeit aller Laufwerke für alle Dateien.
- Ein großes Aggregat ermöglicht die effizienteste Nutzung von Festplattenspeicher.

Für eine effektive Disaster Recovery empfiehlt NetApp, das asynchrone Replikat auf einem Aggregat zu platzieren, das Teil eines separaten Storage-Clusters am Disaster Recovery-Standort ist, und mithilfe der SnapMirror Technologie Inhalte zu replizieren.

Für eine optimale Storage-Performance empfiehlt NetApp, mindestens 10 % freien Speicherplatz in einem Aggregat verfügbar zu haben.

Leitfaden für das Storage-Aggregat-Layout für AFF A300 Systeme (mit zwei Festplatten-Shelfs mit 24 Laufwerken) beinhaltet:

- Halten Sie zwei Spare-Laufwerke.
- Verwenden Sie die erweiterte Laufwerkpartitionierung, um drei Partitionen auf jedem Laufwerk zu erstellen: Root und Daten.
- Verwenden Sie für jedes Aggregat insgesamt 20 Daten-Partitionen und zwei Parity-Partitionen.

Best Practices für Backups

NetApp SnapCenter wird für VM- und Datenbank-Backups eingesetzt. NetApp empfiehlt die folgenden Best Practices für Backups:

- Wenn SnapCenter zur Erstellung von Snapshot Kopien für Backups bereitgestellt wird, schalten Sie den Snapshot Zeitplan für die FlexVol aus, die VMs und Applikationsdaten hosten.
- Erstellen Sie eine dedizierte FlexVol für Host-Boot-LUNs.
- Verwenden Sie für VMs, die denselben Zweck erfüllen, eine ähnliche oder eine einzelne Backup-Richtlinie.
- Sie können eine ähnliche oder einzelne Backup-Richtlinie je Workload-Typ verwenden. Verwenden Sie beispielsweise eine ähnliche Richtlinie für alle Datenbank-Workloads. Verwendung unterschiedlicher Richtlinien für Datenbanken, Webserver, virtuelle Desktops für Endbenutzer usw.
- Aktivieren Sie die Überprüfung des Backups in SnapCenter.
- Konfigurieren Sie die Archivierung der Backup-Snapshot-Kopien in der NetApp SnapVault Backup-Lösung.
- Konfigurieren Sie die Aufbewahrung der Backups auf Grundlage des Archivierungsplans auf dem Primärspeicher.

Best Practices für die Infrastruktur

Best Practices für die Netzwerkumgebung

NetApp empfiehlt die folgenden Best Practices für Netzwerke:

- Stellen Sie sicher, dass Ihr System redundante physische NICs für die Produktion und den Storage-Datenverkehr enthält.
- Getrennte VLANs für iSCSI-, NFS- und SMB/CIFS-Datenverkehr zwischen Computing und Storage
- Stellen Sie sicher, dass Ihr System ein dediziertes VLAN für den Client-Zugriff auf das medizinische Bildgebungssystem enthält.

Weitere Best Practices für Netzwerke finden Sie in den FlexPod Leitfäden für Infrastrukturdesign und Implementierung.

Best Practices für Computing

NetApp empfiehlt die folgende Best Practice für Computing:

- Stellen Sie sicher, dass jede angegebene vCPU von einem physischen Core unterstützt wird.

Best Practices für Virtualisierung

NetApp empfiehlt die folgenden Best Practices für die Virtualisierung:

- Verwenden Sie VMware vSphere 6 oder höher.
- Legen Sie das BIOS und die Betriebssystemebene des ESXi-Hostservers auf Benutzerdefiniert und hohe Performance fest.
- Erstellen Sie Backups in Zeiten geringerer Auslastung.

Best Practices für das medizinische Bildgebungssystem

Beachten Sie die folgenden Best Practices und einige Anforderungen eines typischen medizinischen Bildgebungssystems:

- Setzen Sie keinen virtuellen Speicher durch.
- Stellen Sie sicher, dass die Gesamtzahl der vCPUs der Anzahl der physischen CPUs entspricht.

- Bei einer großen Umgebung sind dedizierte VLANs erforderlich.
- Konfigurieren Sie Datenbank-VMs mit dedizierten HA Clustern.
- Stellen Sie sicher, dass die VM-BS-VMDKs in schnellem Tier-1-Storage gehostet werden.
- Ermitteln Sie gemeinsam mit dem Anbieter medizinischer Bildgebungssysteme den besten Ansatz zur Vorbereitung von VM-Vorlagen für eine schnelle Implementierung und Wartung.
- Für Management-, Storage- und Produktionsnetzwerke ist für die Datenbank LAN-Trennung erforderlich und das bei isoliertem VLANs für VMware vMotion.
- Verwenden Sie die auf dem NetApp Storage-Array basierende Replizierungstechnologie "SnapMirror" anstelle der vSphere-basierten Replizierung.
- Einsatz von Backup-Technologien, die VMware APIs nutzen; Backup-Fenster sollten sich außerhalb der normalen Geschäftszeiten befinden.

Schlussfolgerung

Durch die Ausführung einer medizinischen Bildgebungsumgebung mit FlexPod kann Ihre Gesundheitseinrichtung eine Verbesserung der Mitarbeiterproduktivität und niedrigere Kapital- und Betriebsausgaben erwarten. FlexPod bietet eine vorab validierte, umfassend getestete konvergente Infrastruktur aus der strategischen Partnerschaft von Cisco und NetApp. Sie wurde speziell für vorhersehbare System-Performance mit niedriger Latenz und Hochverfügbarkeit konzipiert. Dieser Ansatz führt zu einer optimalen Benutzererfahrung und einer optimalen Reaktionszeit für die Benutzer des medizinischen Bildgebungssystems.

Verschiedene Komponenten eines Bildgebungssystems für den medizinischen Bereich erfordern einen Datenspeicher in den Dateisystemen SMB/CIFS, NFS, Ext4 und NTFS. Daher muss Ihre Infrastruktur den Datenzugriff über NFS-, SMB/CIFS- und SAN-Protokolle gewährleisten. NetApp Storage-Systeme unterstützen diese Protokolle über ein einziges Storage Array.

Hochverfügbarkeit, Storage-Effizienz, zeitbezogene, Snapshot Kopien-basierte Backups, schnelle Restore-Vorgänge, Datenreplizierung für Disaster Recovery und die FlexPod Storage-Infrastrukturfunktionen stellen ein branchenführendes Storage- und Management-System bereit.

Weitere Informationen

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

- Design-Leitfaden: FlexPod Datacenter for AI/ML with Cisco UCS 480 ML for Deep Learning

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- FlexPod Datacenter-Infrastruktur mit VMware vSphere 6.7 U1, Cisco UCS der vierten Generation und NetApp AFF A-Series

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

- FlexPod Datacenter Oracle Database Backup with SnapCenter – Lösungsüberblick

"https://www.netapp.com/us/media/sb-3999.pdf"

- FlexPod Datacenter mit Oracle RAC Datenbanken auf Cisco UCS und NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- FlexPod Datacenter mit Oracle RAC auf Oracle Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod für Microsoft SQL Server

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- FlexPod von Cisco und NetApp

  "https://flexpod.com/"

- "NetApp Lösungen für MongoDB" Lösungsüberblick (NetApp Login erforderlich)

  "https://fieldportal.netapp.com/content/734702"

- TR-4700: SnapCenter Plug-in für Oracle Database

  "https://www.netapp.com/us/media/tr-4700.pdf"

- NetApp Produktdokumentation

  "https://www.netapp.com/us/documentation/index.aspx"

- Lösungen von FlexPod für Virtual Desktop Infrastructure (VDI)

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

Virtual Desktop Infrastructure

FlexPod-Datacenter mit Citrix Virtual Apps & Desktops 1912 LTSR und VMware vSphere 7 für bis zu 6000 Arbeitsplätze

Jeff Nichols, Cisco Suresh Thoppay, NetApp Dre Jackson, NetApp

Dieses Dokument enthält die Architektur und das Design einer Virtual Desktop Infrastructure für bis zu 6000 Endbenutzer-Computing. Die Lösung ist auf Cisco UCS B200 M5 Blade-Servern der fünften Generation virtualisiert und startet VMware vSphere 7.01 Update 1 über FC SAN vom AFF A400 Storage-Array. Die virtuellen Desktops werden mit Citrix Provisioning Server 1912 LTSR und Citrix RDS/Citrix Virtual Apps & Desktops 1912 LTSR mit einer Kombination aus RDS-gehosteten Shared-Desktops (6000), zusammengefassten und/oder nicht-persistenten gehosteten virtuellen Windows 10-Desktops (5000) bereitgestellt. Und persistente gehostete virtuelle Windows 10-Desktops, die mit Citrix Machine Creation Services (5000) bereitgestellt werden, um die Benutzerzahl zu unterstützen. Gegebenenfalls enthält das Dokument Best Practice-Empfehlungen und Hinweise zur Dimensionierung für die Implementierung dieser Lösung bei Kunden.

"FlexPod-Datacenter mit virtuellen Citrix Apps Desktops 1912 LTSR und VMware vSphere 7 für bis zu 6000 Arbeitsplätze"

FlexPod-Datacenter mit VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 und NetApp ONTAP 9.6 für bis zu 6700 Arbeitsplätze

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Dieses Dokument enthält eine Referenzarchitektur und einen Designleitfaden für eine Desktop-Workload mit 5000 Plätzen und 6000 Plätzen bei einer Endbenutzer-Computing-Umgebung auf FlexPod Datacenter mit Cisco UCS und der NetApp AFF A300 sowie der Datenmanagement-Software NetApp ONTAP. Die Lösung umfasst serverbasierte VMware Horizon RDS Windows Server 2019-Sitzungen, VMware Horizon persistente Full-Clone-Microsoft Windows 10 Virtual Desktops und VMware Horizon nichtpersistente, sofortige Clone-Microsoft Windows 10 Virtual Desktops auf VMware vSphere 6.7U2

"FlexPod-Datacenter mit VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 und NetApp ONTAP 9.6 für bis zu 6700 Arbeitsplätze"

3D-Grafikvisualisierung mit Citrix und NVIDIA - Whitepaper

In diesem Dokument wird die Performance von Citrix XenDesktop auf Citrix XenServer mit NVIDIA Tesla P4, P6 und P40 Karten auf Cisco UCS C240 M5 und B200 M5 Servern mit SPECviewperf 13 beschrieben.

"3D-Grafikvisualisierung mit Citrix und NVIDIA - Whitepaper"

FlexPod Datacenter mit Citrix XenDesktop/XenApp 7.15 und VMware vSphere 6.5 Update 1 für 6000 Seats

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

Dieses Dokument stellt eine Referenzarchitektur für ein Virtual Desktop- und Applikationsdesign bereit. Dazu wird Citrix XenApp/XenDesktop 7.15 auf Basis von Cisco UCS mit NetApp All Flash FAS (AFF) A300 Storage und der Hypervisor-Plattform VMware vSphere ESXi 6.5 verwendet.

Die Virtualisierung von Desktops und Applikationen unterliegt einem ständigen Wandel. Die neuen M5 hochperformanten Cisco UCS Blade Server und Cisco UCS Unified Fabric in Kombination als Teil der FlexPod Proven Infrastructure mit NetApp AFF Storage der neuesten Generation ergeben eine kompaktere, leistungsstärkere, zuverlässigere und effizientere Plattform.

"FlexPod Datacenter mit Citrix XenDesktop/XenApp 7.15 und VMware vSphere 6.5 Update 1 für 6000 Seats"

FlexPod-Datacenter mit VMware Horizon View 7.3 und VMware vSphere 6.5 Update 1 mit Cisco UCS Manager 3.2 für 5000 Arbeitsplätze

Ramesh Guduru, Cisco David Arnette, NetApp

Dieses Dokument enthält eine Referenzarchitektur, einen Design-Leitfaden und die Implementierung für eine End-User-Computing-Umgebung mit 5000 Plätzen für heterogene Workloads in FlexPod Datacenter mit Cisco UCS und NetApp All Flash FAS (AFF) A300 Storage. Die Lösung umfasst serverbasierte, auf VMware Horizon Server gehostete Remote Desktop-Sitzungen, VMware Horizon persistente Microsoft Windows 10 virtuelle Desktops und VMware Horizon nicht-persistente virtuelle Desktops mit Microsoft Windows 10 Instant Clone auf VMware vSphere 6.5.

"FlexPod-Datacenter mit VMware Horizon View 7.3 und VMware vSphere 6.5 Update 1 mit Cisco UCS Manager 3.2 für 5000 Arbeitsplätze"

FlexPod-Datacenter mit VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 und NetApp ONTAP 9.6 für bis zu 6700 Arbeitsplätze

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Dieses Dokument enthält eine Referenzarchitektur und einen Design-Leitfaden für eine Desktop-Workload-Umgebung mit 5000 Plätzen und 6000 Plätzen bei einer Endbenutzer-Computing-Umgebung auf FlexPod Datacenter mit Cisco UCS und NetApp AFF A300 sowie der Datenmanagement-Software NetApp ONTAP. Die Lösung umfasst

serverbasierte VMware Horizon RDS Windows Server 2019-Sitzungen, VMware Horizon persistent, Microsoft Windows 10 Virtual Desktops mit vollem Klon und VMware Horizon nicht-persistent, Virtual Desktops mit sofortigem Klonen von Microsoft Windows 10 auf VMware vSphere 6.7 U2.

"FlexPod-Datacenter mit VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 und NetApp ONTAP 9.6 für bis zu 6700 Arbeitsplätze"

Moderne Apps

FlexPod Datacenter for Combined AI and ML with Cisco UCS 480 ML for Deep Learning – Design

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Dieses Dokument enthält Design-Details zur Integration der Cisco UCS C480 ML M5 Plattform in die FlexPod Datacenter-Lösung. So wird ein einheitlicher Ansatz für die Bereitstellung von KI- und ML-Funktionen in der konvergenten Infrastruktur bereitgestellt. Da Kunden Server, die KI- und ML-Funktionen mit vertrauten Tools kombinieren, die sie zur Administration herkömmlicher FlexPod-Systeme verwenden, managen, werden sowohl der Administrations-Overhead als auch die Kosten für die Implementierung einer Deep-Learning-Plattform erheblich gesenkt. Das in diesem CVD präsentierte Design umfasst auch andere Cisco UCS Plattformen, wie einen C220 M5 Server mit zwei NVIDIA T4 GPUs und einen C240 M5 Server mit zwei NVIDIA V100 32-GB-PCIe-Karten als zusätzliche Optionen für gleichzeitige KI- und ML-Workloads.

"FlexPod Datacenter for Combined AI and ML with Cisco UCS 480 ML for Deep Learning – Design"

Implementierung des Plug-ins NetApp Trident CSI auf der Cisco Container-Plattform mit FlexPod

Dieses Dokument enthält schrittweise Anleitungen zur Implementierung des NetApp Trident CSI-Plug-ins (Container Storage Interface) auf einem Kubernetes-Mandanten-Cluster der Cisco Container-Plattform in einer FlexPod-Lösung.

"Implementierung des Plug-ins NetApp Trident CSI auf der Cisco Container-Plattform mit FlexPod"

FlexPod Datacenter für OpenShift Container-Plattform 4 – Implementierung

Haseb Niazi, Cisco Alan Cowles, NetApp

Red hat OpenShift ist eine Kubernetes-Container-Plattform für den Unternehmenseinsatz zur Verwaltung von Hybrid-Cloud- und Multi-Cloud-Implementierungen. Die Container-Plattform Red hat OpenShift umfasst alles, was für die Entwicklung und Implementierung von Hybrid Clouds, Enterprise-Containern sowie Kubernetes erforderlich ist. Es umfasst ein Linux-Betriebssystem der Enterprise-Klasse, Container-Laufzeit, Netzwerk, Monitoring, Container-Registrierung, Authentifizierungs- und Autorisierungslösungen.

Durch die Kombination von Red hat OpenShift mit der FlexPod Datacenter-Lösung können die Bereitstellung und das Management der Container-Infrastruktur vereinfacht werden. Kunden profitieren von höherer Effizienz, besserer Datensicherung, geringerem Risiko und der Flexibilität, diese hochverfügbare Infrastruktur der Enterprise-Klasse entsprechend den neuen geschäftlichen Anforderungen zu skalieren. Der vorab validierte konvergente Lösungsansatz ermöglicht Unternehmen die Geschwindigkeit, Flexibilität und Skalierbarkeit, die

für alle Initiativen zur Applikationsmodernisierung und zur digitalen Transformation erforderlich sind.

"FlexPod Datacenter für OpenShift Container-Plattform 4 – Implementierung"

FlexPod Datacenter mit Enterprise Edition für Containermanagement

Muhammad Afzal, Cisco John George, Cisco Amit Borulkar, NetApp Uday Shetty, Docker

Docker ist die weltweit führende Software-Container-Plattform für Entwickler und IT-Abläufe zur Erstellung, Auslieferung und Ausführung verteilter Applikationen überall. Mit einer Microservices-Architektur, die die nächste Generation DER IT bestimmt, finden Unternehmen mit großen Investitionen in monolithische Applikationen Möglichkeiten, Docker als Strategie zur Modernisierung ihrer Applikationsarchitekturen zu nutzen und das Unternehmen wettbewerbsfähig und kostengünstig zu halten. Containerisierung bietet die Agilität, Kontrolle und Portabilität, die Entwickler und IT-Abteilungen für die Erstellung und Implementierung von Applikationen in beliebigen Infrastrukturen benötigen. Die Docker Plattform ermöglicht die einfache Zusammensetzung verteilter Applikationen in einem schlanken Applikations-Container, der dynamisch und unterbrechungsfrei geändert werden kann. Dadurch lassen sich Applikationen über Entwicklungs-, Test- und Produktionsumgebungen hinweg verschieben, die auf physischen oder virtuellen Maschinen lokal ausgeführt werden, in Datacentern und über Netzwerke verschiedener Cloud-Service-Provider hinweg.

"FlexPod Datacenter mit Enterprise Edition für Containermanagement"

FlexPod Datacenter für OpenShift Container-Plattform 4 – Design

Haseb Niazi, Cisco Alan Cowles, NetApp

Cisco und NetApp haben gemeinsam eine Reihe von FlexPod Lösungen zur Unterstützung strategischer Datacenter-Plattformen entwickelt. Die FlexPod Lösung bietet eine integrierte Architektur, die Best Practices für Computing, Storage und Netzwerkdesign umfasst. Durch die Validierung der integrierten Architektur für die Kompatibilität verschiedener Komponenten werden IT-Risiken minimiert. Die Lösung löst auch IT-Problempunkte durch dokumentierte Designanleitungen, Implementierungsanleitungen und Support, die in verschiedenen Phasen (Planung, Entwurf und Implementierung) einer Bereitstellung verwendet werden können.

"FlexPod Datacenter für OpenShift Container-Plattform 4 – Design"

White Paper zur 3D-Grafikvisualisierung mit VMware und NVIDIA auf Cisco UCS

In diesem Dokument wird die Performance des VMware ESXi Hypervisors und von

VMware Horizon mit NVIDIA Tesla P4, P6 und P40 auf Cisco UCS C240 M5 Rack Servern und B200 M5 Blade Servern beschrieben.

"White Paper zur 3D-Grafikvisualisierung mit VMware und NVIDIA auf Cisco UCS"

3D-Grafikvisualisierung mit Citrix und NVIDIA - Whitepaper

In diesem Dokument wird die Performance von Citrix XenDesktop auf Citrix XenServer mit NVIDIA Tesla P4, P6 und P40 Karten auf Cisco UCS C240 M5 und B200 M5 Servern mit SPECviewperf 13 beschrieben.

"3D-Grafikvisualisierung mit Citrix und NVIDIA - Whitepaper"

FlexPod Express

Design Guide: FlexPod Express mit Cisco UCS C-Series und NetApp AFF C190 Serie

NVA-1139-DESIGN: FlexPod Express mit Cisco UCS C-Serie und NetApp AFF C190 Serie

Savita Kumari, NetApp

In Zusammenarbeit mit: 

Aktuell stellen immer mehr Unternehmen ihre Rechenzentren auf eine Shared IT Infrastructure und Cloud Computing um. Außerdem wünschen sich Unternehmen eine einfache und effektive Lösung für Remote-Standorte und Zweigstellen, die auf die ihnen in ihrem Datacenter vertraute Technologie basiert.

FlexPod Express ist eine vorab entwickelte Best Practice Datacenter-Architektur, die auf dem Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switch-Produktfamilie und NetApp AFF Systemen basiert. Die Komponenten von FlexPod Express sind wie ihre Kollegen aus dem FlexPod Datacenter, die Managementsynergien über die komplette IT-Infrastrukturumgebung hinweg in geringerem Umfang ermöglichen. FlexPod Datacenter und FlexPod Express sind optimale Plattformen für die Virtualisierung sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads.

"Weiter: Programmübersicht."

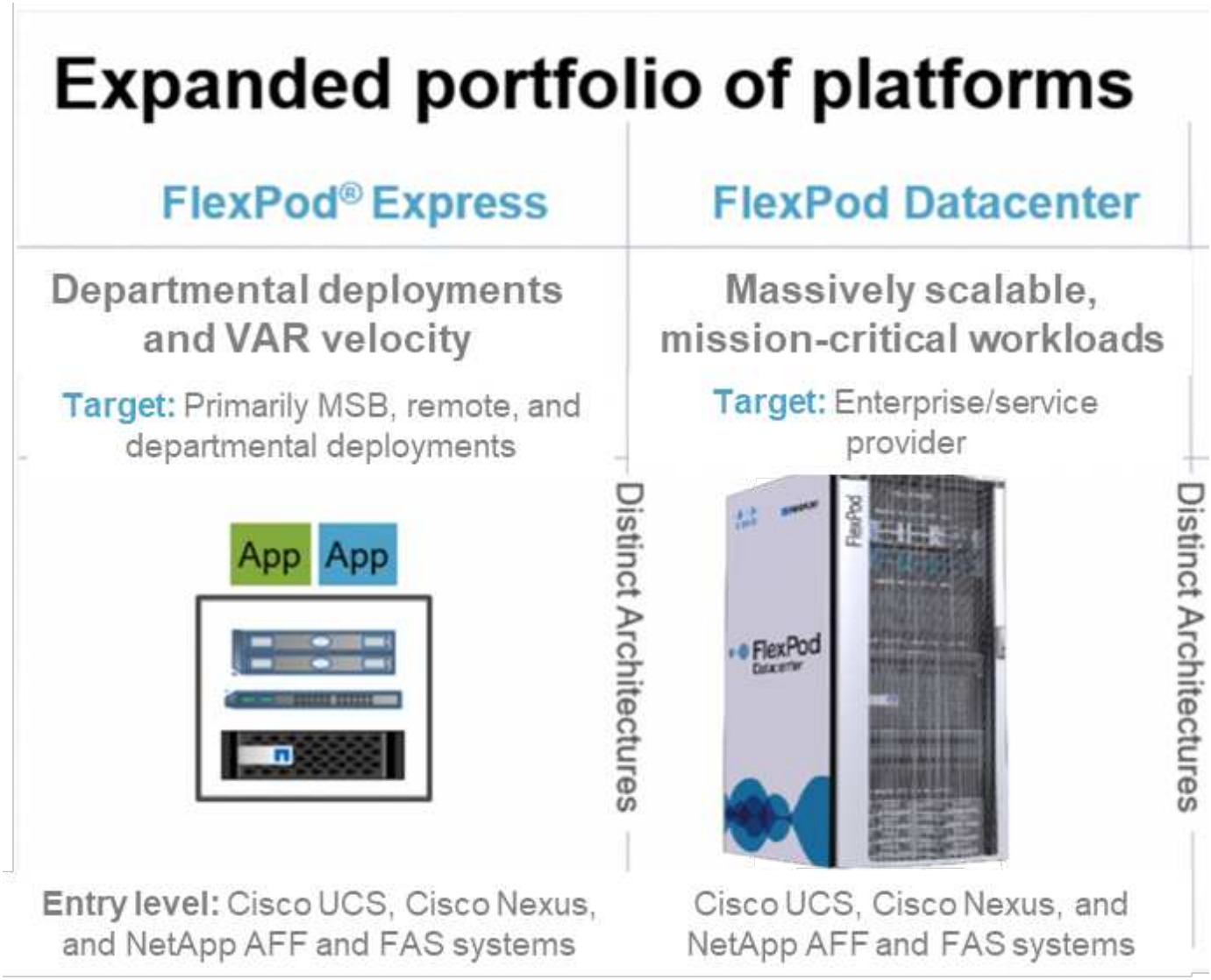
Programmzusammenfassung

FlexPod Converged Infrastructure-Portfolio

FlexPod Referenzarchitekturen werden als Cisco Validated Designs (CVDs) oder als NetApp Verified Architectures (NVAs) bereitgestellt. Abweichungen, die auf den Anforderungen des Kunden von einem bestimmten CVD oder NVA basieren, sind zulässig, wenn diese Abweichungen nicht zur Bereitstellung von nicht unterstützten Konfigurationen führen.

Das FlexPod Portfolio umfasst, wie in der folgenden Abbildung dargestellt, folgende Lösungen: FlexPod Express und FlexPod Datacenter.

- **FlexPod Express** ist eine Einstiegslösung mit Technologien von Cisco und NetApp.
- **FlexPod Datacenter** bietet eine optimale Mehrzweckgrundlage für verschiedene Workloads und Anwendungen.



NetApp Verified Architecture-Programm

Das Programm „NetApp Verified Architecture“ bietet verifizierte Architekturen für NetApp Lösungen an. Eine NVA-Lösung zeichnet sich durch folgende Merkmale aus:

- Sorgfältig getestet
- Präskriptiv
- Minimale Risiken bei der Implementierung
- Schnellere Markteinführung dieser Leitfaden beschreibt das Design von FlexPod Express mit VMware vSphere.

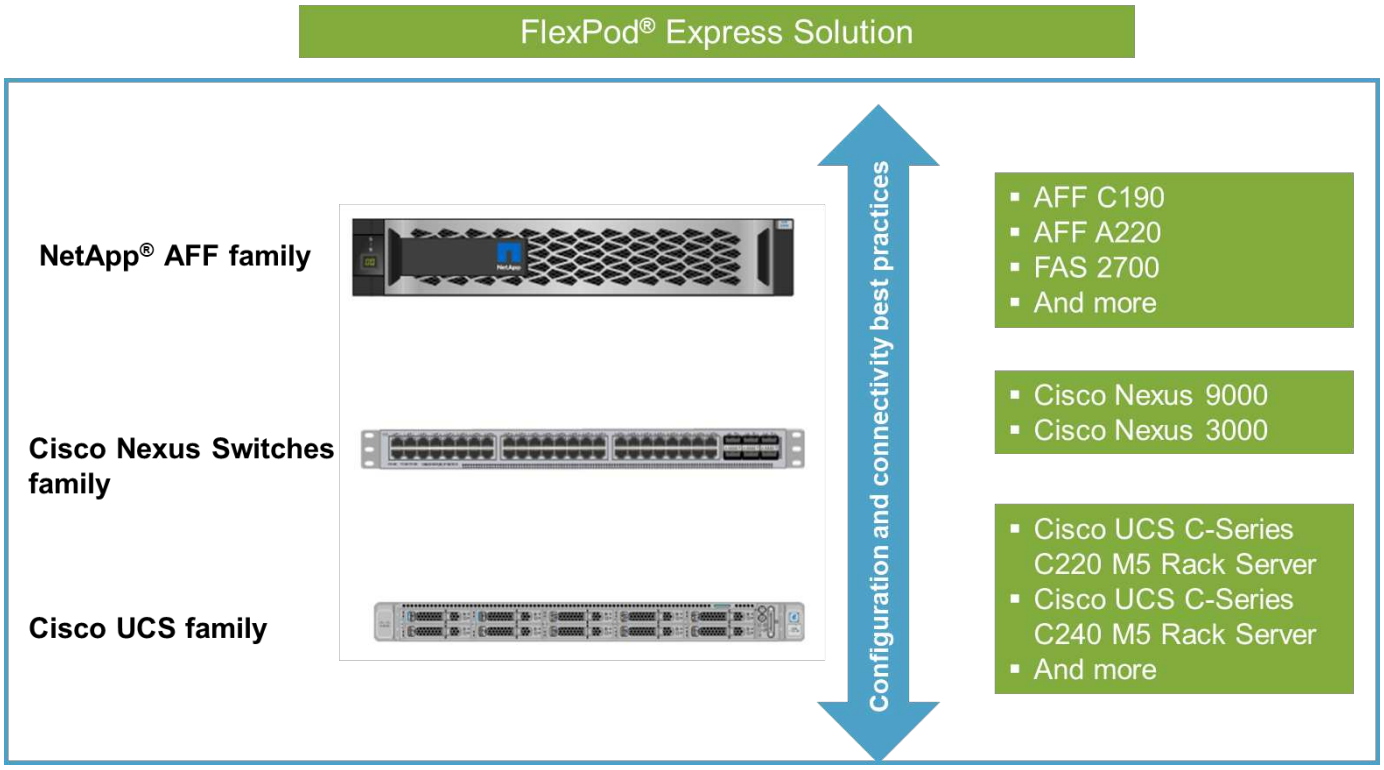
Darüber hinaus nutzt dieses Design das komplett neue AFF C190 System, auf dem NetApp ONTAP 9.6 Software, Cisco Nexus 31108 Switches und Cisco UCS C220 M5 Server als Hypervisor-Nodes ausgeführt werden.

Lösungsüberblick

FlexPod Express wurde für gemischte Virtualisierungs-Workloads entwickelt. Sie richtet sich an Remote-Standorte und Zweigniederlassungen sowie an kleine und mittelständische Unternehmen. Es ist auch optimal für größere Unternehmen, die eine dedizierte Lösung für einen bestimmten Zweck implementieren möchten.

Diese neue Lösung für FlexPod Express fügt neue Technologien wie NetApp ONTAP 9.6, NetApp AFF C190 System und VMware vSphere 6.7U2 hinzu.

In der folgenden Abbildung sind die Hardwarekomponenten aufgeführt, die in der FlexPod Express Lösung enthalten sind.

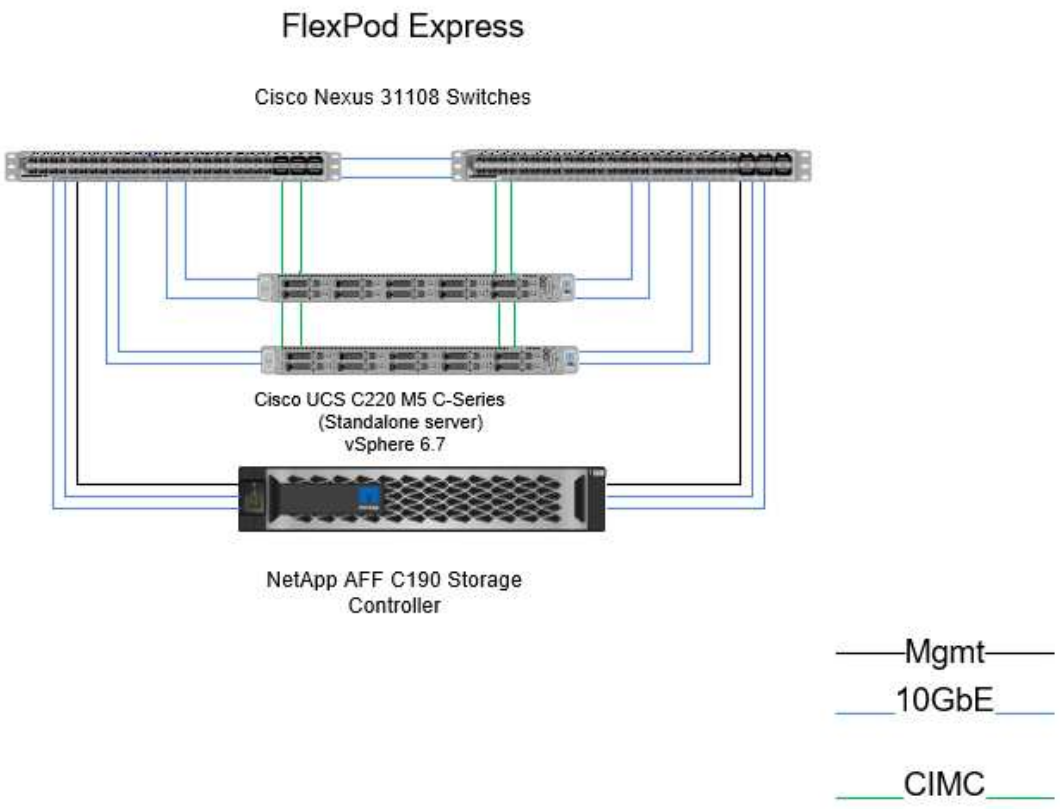


Zielgruppe

Dieses Dokument richtet sich an Personen, die die Vorteile einer Infrastruktur nutzen möchten, die eine effiziente IT liefert und IT-Innovationen unterstützt. Dieses Dokument richtet sich an Vertriebsmitarbeiter, Berater im Außendienst, Professional Services-Mitarbeiter, IT-Manager, Techniker des Partners und Kunden.

Lösungstechnologie

Diese Lösung nutzt die neuesten Technologien von NetApp, Cisco und VMware. Sie enthält das neue NetApp AFF C190 System, auf dem ONTAP 9.6 Software, zwei Cisco Nexus 31108 Switches und Cisco UCS C220 M5 Rack Server mit VMware vSphere 6.7U2 ausgeführt werden. Diese validierte Lösung, die in der folgenden Abbildung dargestellt ist, nutzt 10-Gigabit-Ethernet (10GbE)-Technologie. Beratung wird auch zur Skalierung durch Hinzufügen von zwei Hypervisor-Knoten zu einem Zeitpunkt, so dass die FlexPod Express-Architektur kann sich an die sich entwickelnden geschäftlichen Anforderungen eines Unternehmens anpassen.



"Next: Technologieanforderungen."

Technologieanforderungen erfüllt

Für FlexPod Express sind eine Kombination aus Hardware- und Softwarekomponenten erforderlich, die vom ausgewählten Hypervisor und von der Netzwerkgeschwindigkeit abhängig sind. Darüber hinaus enthält FlexPod Express die Hardwarekomponenten, die erforderlich sind, um dem System in Einheiten von zwei Hypervisor-Nodes hinzuzufügen.

Hardwareanforderungen

Unabhängig vom ausgewählten Hypervisor nutzen alle FlexPod Express Konfigurationen dieselbe Hardware. Selbst wenn sich die geschäftlichen Anforderungen ändern, können Sie auf derselben FlexPod Express Hardware einen anderen Hypervisor verwenden.

In der folgenden Tabelle sind die Hardwarekomponenten aufgeführt, die für diese FlexPod Express Konfiguration und für die Implementierung dieser Lösung erforderlich sind. Je nach den Anforderungen des Kunden können die in einer beliebigen Implementierung dieser Lösung verwendeten Hardwarekomponenten abweichen.

Trennt	Menge
AFF C190 2-Node-Cluster	1
Cisco UCS C220 M5 Server	2

Trennt	Menge
Cisco Nexus 31108 Switch	2
Cisco UCS Virtual Interface Card (VIC) 1457 für Cisco UCS C220 M5 Rack Server	2

Softwareanforderungen

In der folgenden Tabelle werden die Softwarekomponenten aufgeführt, die für die Implementierung der Architekturen der FlexPod Express Lösung erforderlich sind.

Software	Version	Details
Cisco Integrated Management Controller (CIMC)	4.0.4	Für C220 M5 Rack Server
Cisco NX-OS	7.0(3)I7(6)	Für Cisco Nexus 31108 Switches
NetApp ONTAP	9.6	Für NetApp AFF C190 Controller

In der folgenden Tabelle ist die erforderliche Software für alle VMware vSphere Implementierungen auf FlexPod Express aufgeführt.

Software	Version
VMware vCenter Server Appliance	6.7U2
VMware vSphere ESXi	6.7U2
NetApp VAAI Plug-in für ESXi	1.1.2
NetApp Virtual Storage Console	9.6

"Als Nächstes: Design-Entscheidungen."

Designs

Die in diesem Abschnitt aufgeführten Technologien wurden während der Designphase ausgewählt. Jede Technologie erfüllt einen bestimmten Zweck in der FlexPod Express Infrastrukturlösung.

NetApp AFF C190 Serie mit ONTAP 9.6

Bei dieser Lösung kommen zwei der neuesten NetApp Produkte zum Einsatz: Das NetApp AFF C190 System und die Software ONTAP 9.6.

AFF C190 System

Die Zielgruppe sind Kunden, die ihre IT-Infrastruktur mit All-Flash-Technologie zu einem erschwinglichen Preis modernisieren möchten. Das AFF C190 System wird mit der neuen Lizenzierung von ONTAP 9.6 und Flash Bundle ausgeliefert. Dies bedeutet, dass die folgenden Funktionen integriert sind:

- CIFS, NFS, iSCSI und FCP
- NetApp SnapMirror Datenreplizierungssoftware, NetApp SnapVault Backup Software, NetApp

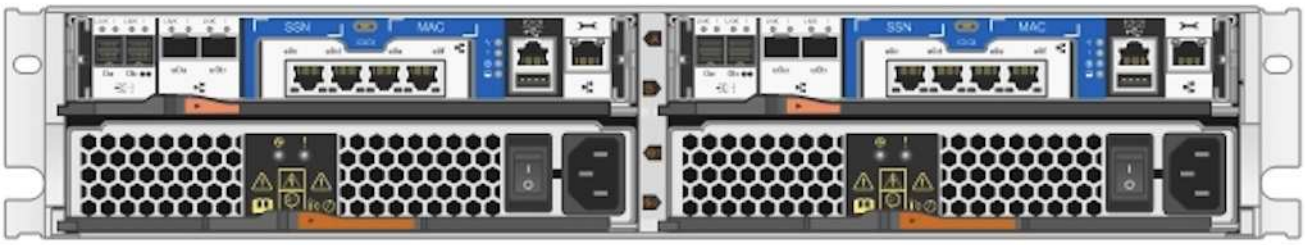
SnapRestore Software zur Datenwiederherstellung, NetApp SnapManager Storage Management Software-Suite und NetApp SnapCenter Software

- FlexVol Technologie
- Deduplizierung, Komprimierung und Data-Compaction
- Thin Provisioning
- Storage-QoS
- NetApp RAID DP Technologie
- Die NetApp Snapshot Technologie
- FabricPool

In den folgenden Abbildungen werden die beiden Optionen für die Host-Konnektivität dargestellt.

Die folgende Abbildung zeigt UTA 2-Ports, in die ein SFP+-Modul eingesetzt werden kann.

Die folgende Abbildung zeigt 10GBASE-T-Ports für den Anschluss über herkömmliche RJ-45 Ethernet-Kabel.



Für den 10GBASE-T-Port benötigen Sie einen 10GBASE-T-basierten Uplink Switch.

Das AFF C190 System wird ausschließlich mit 960 GB SSDs angeboten. Es gibt vier Phasen der Erweiterungen, aus denen Sie wählen können:

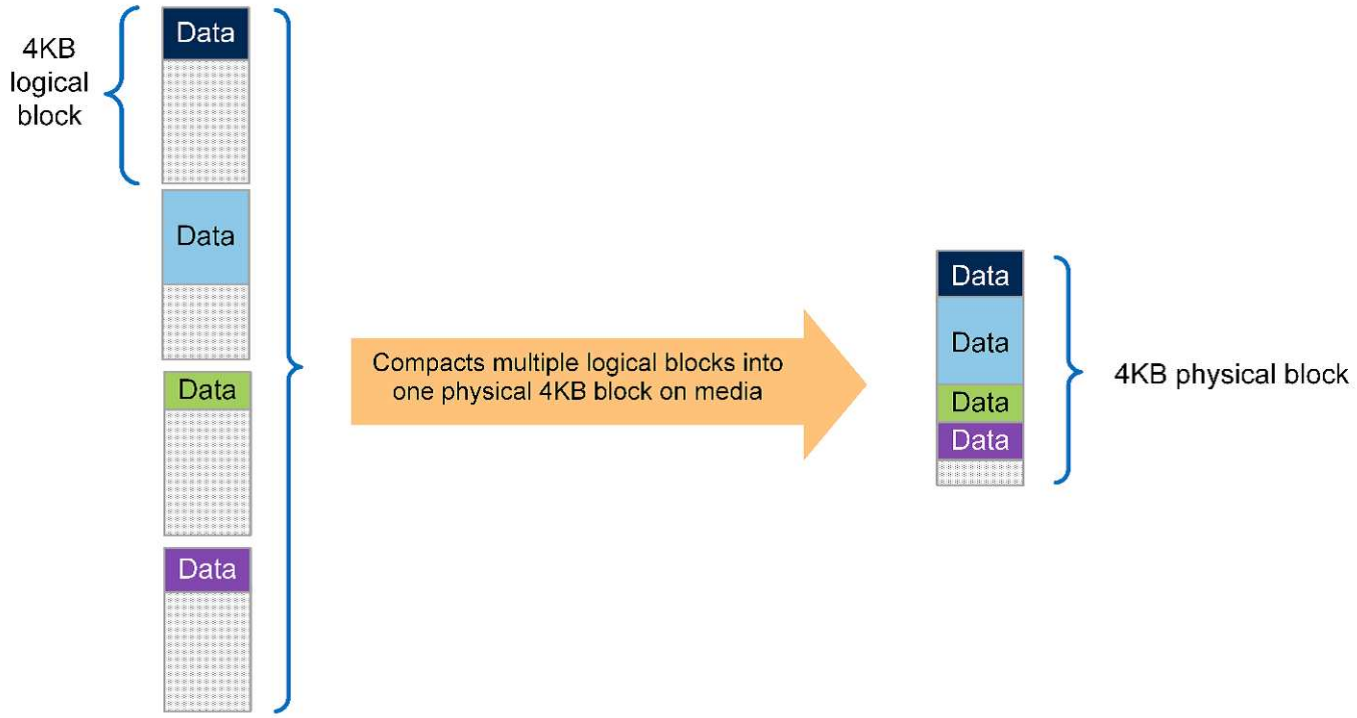
- 8 x 960 GB
- 12 x 960 GB
- 18 x 960 GB
- 24 x 960 GB

Weitere Informationen zum AFF C190 Hardware-System finden Sie im "NetApp AFF C190 All-Flash-Array-Seite".

ONTAP 9.6 Software

NetApp AFF C190 Systeme verwenden die neue Datenmanagement-Software ONTAP 9.6. ONTAP 9.6 ist die branchenweit führende Datenmanagement-Software der Enterprise-Klasse. Sie vereint ein neues Maß an Anwenderfreundlichkeit und Flexibilität mit leistungsfähigen Datenmanagement-Funktionen, Storage-Effizienzfunktionen und erstklassiger Cloud-Integration.

ONTAP 9.6 bietet verschiedene Funktionen, die sich gut für FlexPod Express eignen. In erster Linie ist das Engagement von NetApp für Storage-Effizienz, die eines der wichtigsten Funktionen für kleine Implementierungen sein kann. Die Markenzeichen von NetApp Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung, Data-Compaction und Thin Provisioning sind in ONTAP 9.6 erhältlich. Das NetApp WAFL System schreibt immer 4-KB-Blöcke. Daher werden in der Data-Compaction mehrere Blöcke in einem 4-KB-Block kombiniert, wenn die Datenblöcke ihren zugewiesenen Speicherplatz nicht nutzen. Dieser Prozess wird in der folgenden Abbildung dargestellt.



ONTAP 9.6 unterstützt nun optionale 512-Byte-Blockgrößen für NVMe-Volumes. Diese Funktion ist problemlos in das VMware Virtual Machine File System (VMFS) integriert, das nativ einen 512-Byte-Block verwendet. Sie können bei der 4K-Standardgröße bleiben oder optional die 512-Byte-Blockgröße festlegen.

Weitere Funktionserweiterungen in ONTAP 9.6:

- **NetApp Aggregate Encryption (NAE).** NAE weist Schlüssel auf Aggregatebene zu und verschlüsselt damit alle Volumes im Aggregat. Diese Funktion ermöglicht die Verschlüsselung und Deduplizierung von Volumes auf Aggregatebene.
- **NetApp ONTAP FlexGroup Volume Erweiterung**. In ONTAP 9.6 können Sie ein FlexGroup-Volume ganz einfach umbenennen. Es ist nicht erforderlich, ein neues Volume zu erstellen, um die Daten zu migrieren. Mit ONTAP System Manager oder CLI kann die Volume-Größe verringert werden.
- **FabricPool-Erweiterung.** ONTAP 9.6 bietet zusätzliche Unterstützung für Objektspeicher als Cloud-Tiers. Auch die Liste enthält Unterstützung für Google Cloud und Alibaba Cloud Object Storage Service (OSS). FabricPool unterstützt mehrere Objektspeicher wie AWS S3, Azure Blob, IBM Cloud Objekt-Storage und objektbasierte NetApp StorageGRID Storage-Software.

- **SnapMirror Verbesserung.** in ONTAP 9.6 wird eine neue Volume-Replikationsbeziehung standardmäßig verschlüsselt, bevor das Quell-Array verlassen wird und am SnapMirror Ziel entschlüsselt wird.

Cisco Nexus 3000 Serie

Der Cisco Nexus 31108PC-V ist ein Top-of-Rack (Tor) Switch mit 10 Gbit/s SFP+-48 Ports und 6 QSFP28-Ports. Jeder SFP+ Port kann mit 100 MB/s, 10 GB/s betrieben werden. Jeder QSFP28-Port kann im nativen 100-Gbit/s- oder 40-Gbit/s-Modus oder 4-mal 10-Gbit/s-Modus ausgeführt werden und bietet flexible Migrationsoptionen. Dieser Switch ist ein echter PHY-loser Switch, der für niedrige Latenz und niedrigen Stromverbrauch optimiert ist.

Die Cisco Nexus 31108PC-V Spezifikation umfasst die folgenden Komponenten:

- Schaltkapazität von 2,16 Tbit/s und Weiterleitungsrate von bis zu 1,2 Tbit/s für 31108 PC-V
- 48 SFP-Ports unterstützen 1- und 10-Gigabit-Ethernet (10 GbE); 6-mal QSFP28-Ports unterstützen 4 x 10 GbE oder 40 GbE jeweils oder 100 GbE

Die folgende Abbildung zeigt den Cisco Nexus 31108PC-V Switch.

Weitere Informationen zu Cisco Nexus 31108PC-V-Switches finden Sie unter "Datenblatt zu den Cisco Nexus 3172PQ-, 3172TQ-, 3172TQ-32T-, 3172PQ-XL- und 3172TQ-XL-Switches".

Cisco UCS C-Serie

Der Rack Server der Cisco UCS C-Serie wurde für FlexPod Express ausgewählt, da er dank der vielen Konfigurationsoptionen an spezifische Anforderungen einer FlexPod Express Implementierung angepasst werden kann.

Die Rack-Server der Cisco UCS C-Serie bieten Unified Computing in einem branchenüblichen Formfaktor zur Senkung der TCO und Steigerung der Flexibilität.

Die Rack-Server der Cisco UCS C-Serie bieten folgende Vorteile:

- Formfaktor-unabhängiger Einstieg in Cisco UCS
- Vereinfachte und schnelle Implementierung von Applikationen
- Erweiterung der Innovationen im Unified Computing und der Vorteile für Rack-Server
- Bessere Auswahl für Kunden mit einzigartigen Vorteilen in einem vertrauten Rack-Paket

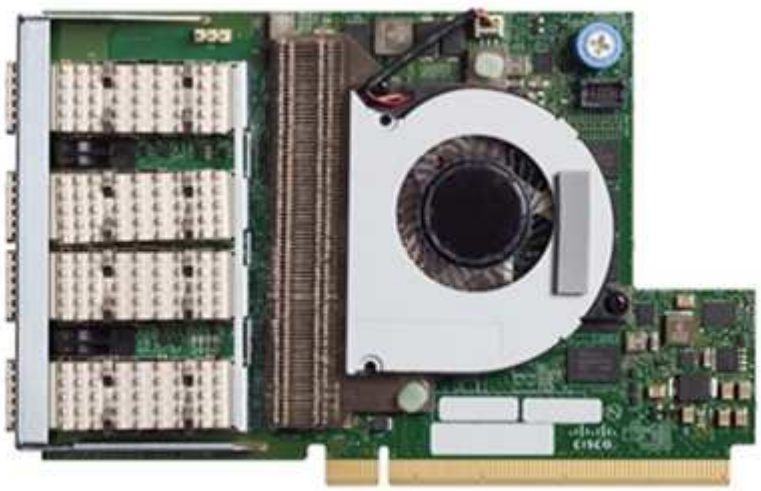
Der in der obigen Abbildung dargestellte Cisco UCS C220 M5 Rack Server gehört zu den vielseitigsten

universellen Unternehmensinfrastruktur und Applikations-Servern der Branche. Dieser 2-Socket-Rack-Server mit hoher Dichte bietet herausragende Performance und Effizienz für eine Vielzahl an Workloads, einschließlich Virtualisierung, Zusammenarbeit und Bare Metal-Applikationen. Rack-Server der Cisco UCS C-Serie können als Standalone-Server oder als Teil des Cisco UCS bereitgestellt werden, um die standardbasierten Unified Computing-Innovationen von Cisco zu nutzen, die dazu beitragen, die Gesamtbetriebskosten der Kunden zu senken und ihre geschäftliche Flexibilität zu steigern.

Weitere Informationen zu C220 M5 Servern finden Sie unter "Cisco UCS C220 M5 Rack Server – Datenblatt".

Cisco UCS VIC 1457-Konnektivität für C220 M5 Rack Server

Der in der folgenden Abbildung dargestellte Cisco UCS VIC 1457 Adapter ist eine SFP-Karte (Quad Port Small Form Factor Pluggable) auf dem Motherboard (mLOM), die für die M5-Generation von Cisco UCS C-Series Servern entwickelt wurde. Die Karte unterstützt 10/25 Gbit/s Ethernet oder FCoE. Die Karte kann dem Host standardkonforme PCIe-Schnittstellen zur Verfügung stellen, die dynamisch als NICs oder HBAs konfiguriert werden können.



Vollständige Informationen zum Cisco UCS VIC 1457-Adapter finden Sie unter "Datenblatt zur Cisco UCS Virtual Interface Card 1400-Serie".

VMware vSphere 6.7U2

VMware vSphere 6.7U2 ist eine der Hypervisor-Optionen zur Verwendung mit FlexPod Express. Mit VMware vSphere können Unternehmen ihren Strom- und Kühlungsbedarf senken und gleichzeitig die erworbene Computing-Kapazität vollständig nutzen. Darüber hinaus ermöglicht VMware vSphere den Schutz vor Hardware-Ausfällen (VMware High Availability, oder VMware HA) und den Lastausgleich für Computing-Ressourcen über einen Cluster von vSphere Hosts (VMware Distributed Resource Scheduler im Wartungsmodus oder VMware DRS-MM).

Da es nur den Kernel neu startet, können Kunden mit VMware vSphere 6.7U2 schnell booten und vSphere ESXi laden, ohne die Hardware neu zu starten. Der vSphere 6.7U2 vSphere-Client (HTML5-basierter Client) verfügt über einige neue Verbesserungen wie Developer Center mit Code Capture und API Explore. Mit Code Capture können Sie Ihre Aktionen im vSphere-Client aufzeichnen, um eine einfache, nutzbare Codeausgabe zu ermöglichen. VSphere 6.7U2 enthält darüber hinaus neue Funktionen wie DRS im Wartungsmodus (DRS-MM).

VMware vSphere 6.7U2 bietet folgende Funktionen:

- VMware erklärt das Implementierungsmodell für den VMware Platform Services Controller (PSC).

Ab der nächsten größeren vSphere Version steht externe PSC nicht zur Verfügung.

- Neues Protokoll zur Unterstützung von Backup und Wiederherstellung einer vCenter Server Appliance. Einführung von NFS und SMB als unterstützte Protokolloptionen, insgesamt bis zu 7 (HTTP, HTTPS, FTP, FTPS, SCP, NFS und SMB) bei der Konfiguration eines vCenter Servers für dateibasierte Backup- und Restore-Vorgänge.
- Neue Funktionen bei der Verwendung der Inhaltsbibliothek. Wenn vCenter Server für den erweiterten verknüpften Modus konfiguriert ist, können jetzt native VM-Vorlagen zwischen Inhaltsbibliotheken synchronisiert werden.
- Aktualisieren Sie auf "Client Plug-ins Seite".
- VMware vSphere Update Manager enthält auch Verbesserungen am vSphere Client. Sie können die Einhaltung von Anhängen-Checks durchführen und Aktionen beheben – alles über einen Bildschirm.

Weitere Informationen zu VMware vSphere 6.7 U2 finden Sie im "Blog-Seite von VMware vSphere".

Weitere Informationen zu den Updates für VMware vCenter Server 6.7 U2 finden Sie im "Versionshinweise".

Obwohl diese Lösung mit vSphere 6.7U2 validiert wurde, unterstützt sie alle vSphere Versionen, die sich für die anderen Komponenten durch das qualifiziert haben "NetApp Interoperabilitäts-Matrix-Tool (IMT)". NetApp empfiehlt die Implementierung der nächsten Version von vSphere, um deren Fixes und erweiterte Funktionen zu erhalten.

Boot-Architektur

Zu den unterstützten Optionen der FlexPod Express Boot-Architektur gehören:

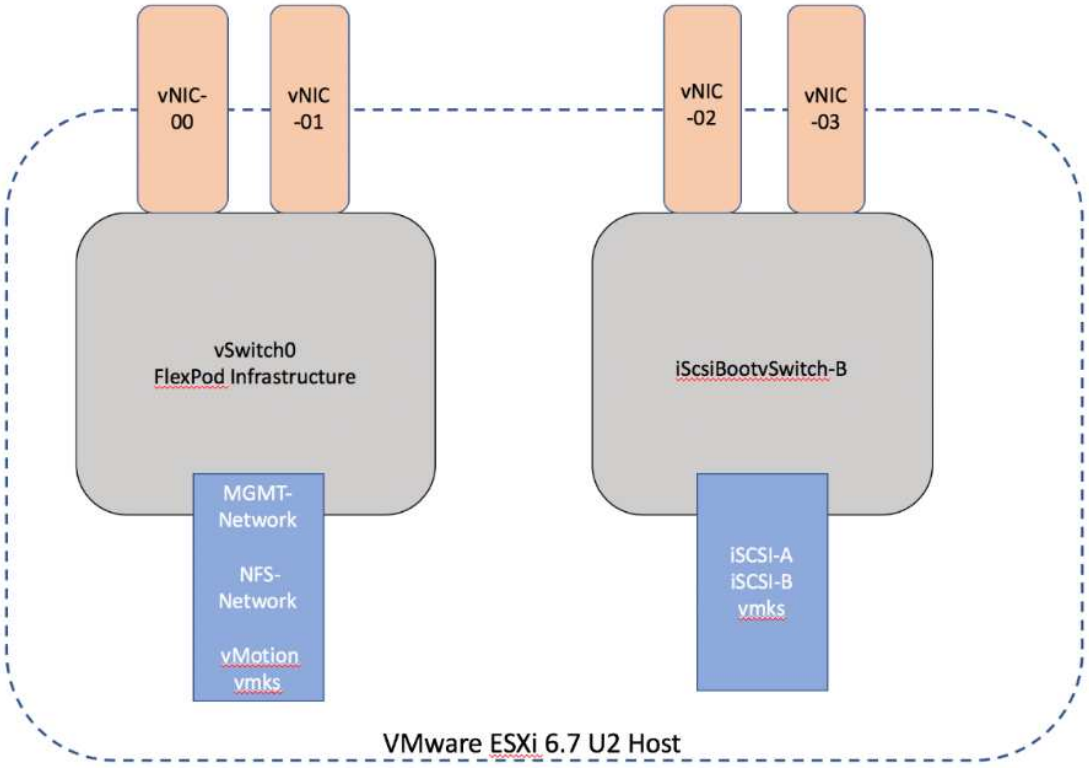
- ISCSI SAN LUN
- Cisco FlexFlash SD-Karte
- Lokale Festplatte

FlexPod Datacenter wird über iSCSI LUNs gestartet. Daher wird die Lösungsverwaltung durch iSCSI Boot für FlexPod Express verbessert.

Layout der ESXi Host Virtual Network Interface Card

Cisco UCS VIC 1457 verfügt über vier physische Ports. Diese Lösungsvalidierung umfasst die vier physischen Ports in Verwendung des ESXi Hosts. Wenn Sie eine kleinere oder größere Anzahl von NICs haben, haben Sie möglicherweise unterschiedliche VMNIC-Zahlen.

Bei einer iSCSI-Boot-Implementierung benötigt iSCSI separate virtuelle Netzwerkkarten (vNICs) für das iSCSI-Booten. Diese vNICs nutzen das iSCSI-VLAN der entsprechenden Fabric als natives VLAN und sind an die iSCSI-Boot-vSwitches angeschlossen, wie in der folgenden Abbildung dargestellt.



"Weiter: Fazit."

Schlussfolgerung

Das validierte Design von FlexPod Express ist eine einfache und effektive Lösung, die branchenführende Komponenten verwendet. Durch die Skalierung und die Bereitstellung von Optionen für die Hypervisor-Plattform kann FlexPod Express auf spezifische Geschäftsanforderungen zugeschnitten werden. FlexPod Express wurde für kleine bis mittelständische Unternehmen, Remote-Standorte und externe Niederlassungen sowie andere Unternehmen entwickelt, die dedizierte Lösungen benötigen.

"Weiter: Wo finden Sie zusätzliche Informationen."

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten und auf den folgenden Websites:

- AFF und FAS System Documentation Center

  "https://docs.netapp.com/platstor/index.jsp"

- AFF Dokumentationsmaterialien

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FlexPod Express with VMware vSphere 6.7 and NetApp AFF C190 Deployment Guide (in Bearbeitung)

- NetApp Dokumentation

  "https://docs.netapp.com"

FlexPod Express mit Cisco UCS C-Series und NetApp AFF C190 Series – Implementierungsleitfaden

NVA-1142-DEPLOY: FlexPod Express mit Cisco UCS C-Serie und NetApp AFF C190 Serie - NVA Deployment

Savita Kumari, NetApp

Aktuell stellen immer mehr Unternehmen ihre Rechenzentren auf Shared IT-Infrastrukturen und Cloud Computing um. Außerdem wünschen sich Unternehmen eine einfache und effektive Lösung für Remote-Standorte und Zweigstellen, die Technologien einsetzen, die ihnen in ihrem Datacenter vertraut sind.

FlexPod Express ist eine vorkonfigurierte Datacenter-Architektur mit Best Practices, die auf Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switch-Produktfamilie und NetApp Storage-Technologien basiert. Die Komponenten eines FlexPod Express Systems sind wie ihre Kollegen im FlexPod Datacenter, die Managementsynergien über die gesamte IT-Infrastrukturumgebung hinweg in geringerem Umfang ermöglichen. FlexPod Datacenter und FlexPod Express sind optimale Plattformen für die Virtualisierung sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads.

FlexPod Datacenter und FlexPod Express bieten eine Basiskonfiguration, die sich flexibel für eine Vielzahl von Anwendungsfällen und Anforderungen dimensionieren und optimieren lässt. Bestehende FlexPod Datacenter-Kunden können ihr FlexPod Express System mit den gewohnten Tools managen. Neue FlexPod Express Kunden können bei wachsenden Umgebungen mühelos auf das Management von FlexPod Datacenter umsteigen.

FlexPod Express ist die optimale Infrastrukturbasis für Remote-Standorte und externe Niederlassungen sowie für kleine bis mittelständische Unternehmen. Es ist außerdem eine optimale Lösung für Kunden, die eine Infrastruktur für einen dedizierten Workload bereitstellen möchten.

FlexPod Express bietet eine einfach zu managende Infrastruktur, die sich für fast alle Workloads eignet.

Lösungsüberblick

Diese FlexPod Express Lösung ist Teil des FlexPod Converged Infrastructure Programms.

FlexPod Converged Infrastructure Programm

FlexPod Referenzarchitekturen werden als Cisco Validated Designs (CVDs) oder NetApp Verified Architectures (NVAs) bereitgestellt. Abweichungen, die auf Kundenanforderungen von einem bestimmten CVD oder NVA basieren, sind zulässig, wenn diese Variationen keine nicht unterstützte Konfiguration erstellen.

Das FlexPod Programm umfasst zwei Lösungen: FlexPod Express und FlexPod Datacenter.

- **FlexPod Express.** bietet Kunden eine Einstiegslösung mit Technologien von Cisco und NetApp.

- **FlexPod Datacenter.** bietet eine optimale Mehrzweckgrundlage für verschiedene Workloads und Anwendungen.

NetApp Verified Architecture-Programm

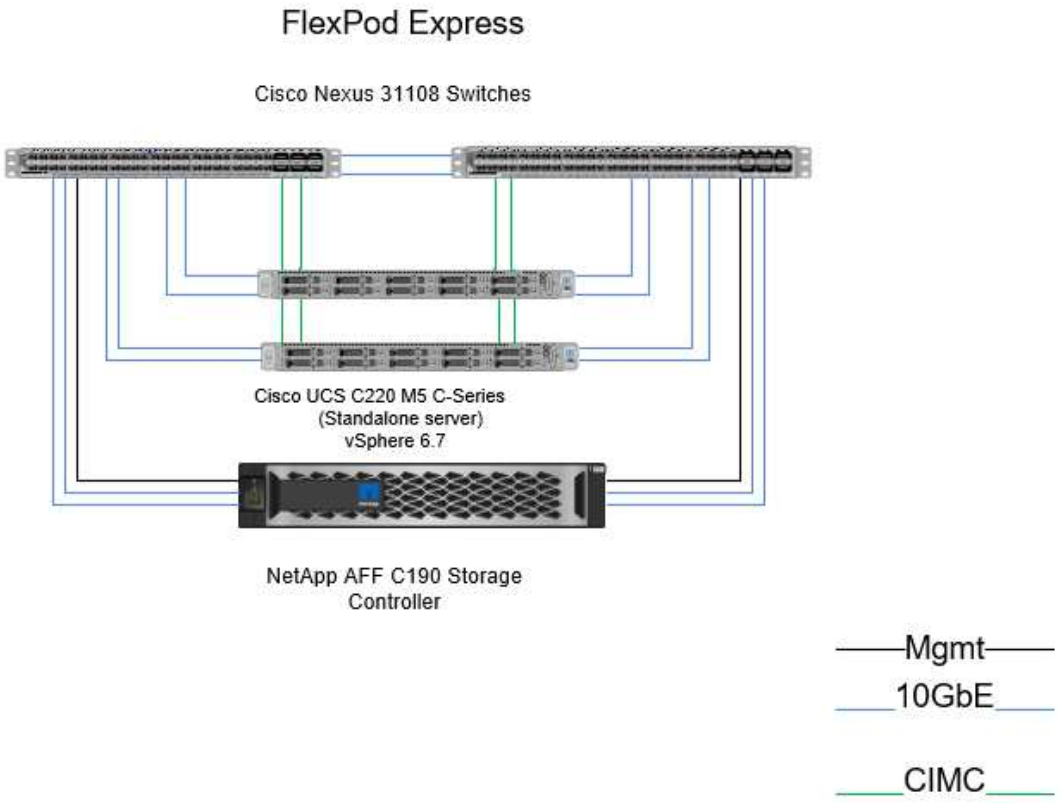
Das Programm „NetApp Verified Architecture“ bietet verifizierte Architekturen für NetApp Lösungen an. Eine NetApp Verified Architecture bietet eine NetApp Lösungsarchitektur folgende Eigenschaften:

- Sorgfältig getestet
- Präskriptiv
- Minimale Implementierungsrisiken
- Beschleunigte Produkteinführungszeit

Dieser Leitfaden beschreibt das Design von FlexPod Express mit VMware vSphere. Darüber hinaus verwendet dieses Design das komplett neue AFF C190 System (mit NetApp ONTAP 9.6), das Cisco Nexus 31108 und Cisco UCS C-Series C220 M5 Server als Hypervisor-Nodes.

Lösungstechnologie

Diese Lösung nutzt die neuesten Technologien von NetApp, Cisco und VMware. Diese Lösung umfasst das neue NetApp AFF C190 mit ONTAP 9.6, zwei Cisco Nexus 31108 Switches und Cisco UCS C220 M5 Rack Server mit VMware vSphere 6.7U2. Diese validierte Lösung nutzt 10-GbE-Technologie. Es wird auch eine Anleitung zur Skalierung der Computing-Kapazität bereitgestellt, indem jeweils zwei Hypervisor-Nodes hinzugefügt werden, damit sich die FlexPod Express-Architektur an die sich wandelnden Geschäftsanforderungen eines Unternehmens anpassen kann.



Um die vier physischen 10GbE-Ports auf dem VIC 1457 effizient zu nutzen, erstellen Sie zwei zusätzliche Links von jedem Server zu den oberen Rack Switches.

Zusammenfassung des Anwendungsfalls

Die FlexPod Express Lösung kann für verschiedene Anwendungsfälle eingesetzt werden. Dazu zählen:

- Remote-Standorte oder externe Niederlassungen
- Kleine und mittelständische Unternehmen
- Umgebungen, für die eine dedizierte und kostengünstige Lösung erforderlich ist

FlexPod Express eignet sich am besten für virtualisierte und gemischte Workloads. Obwohl diese Lösung mit vSphere 6.7U2 validiert wurde, unterstützt sie alle vSphere Versionen, die sich mit den anderen Komponenten durch das NetApp Interoperabilitäts-Matrix-Tool qualifiziert haben. NetApp empfiehlt den Einsatz von vSphere 6.7U2 aufgrund seiner Fixes und erweiterten Funktionen wie z. B.:

- Neue Protokollunterstützung für das Backup und die Wiederherstellung einer vCenter Server-Appliance, einschließlich HTTP, HTTPS, FTP, FTPS, SCP, NFS UND SMB.
- Neue Funktionen bei der Nutzung der Inhaltsbibliothek. Wenn vCenter Server für den erweiterten verknüpften Modus konfiguriert ist, können jetzt native VM-Vorlagen zwischen Inhaltsbibliotheken synchronisiert werden.
- Eine aktualisierte Client-Plug-in-Seite.
- Erweiterungen im vSphere Update Manager (VUM) und dem vSphere-Client hinzugefügt. Sie können nun die Aktionen „Anhängen“, „Überprüfung der Compliance“ und „Korrektur“ auf einem Bildschirm ausführen.

Weitere Informationen zu diesem Thema finden Sie im "Seite zu vSphere 6.7U2" Und das "VCenter Server 6.7U2 – Versionshinweise".

Technologieanforderungen erfüllt

Ein FlexPod Express System erfordert eine Kombination aus Hardware- und Softwarekomponenten. FlexPod Express beschreibt außerdem die Hardwarekomponenten, die erforderlich sind, um dem System in Einheiten von zwei Hypervisor-Nodes hinzuzufügen.

Hardwareanforderungen

Unabhängig vom ausgewählten Hypervisor nutzen alle FlexPod Express Konfigurationen dieselbe Hardware. Selbst wenn sich die geschäftlichen Anforderungen ändern, können Sie auf derselben FlexPod Express Hardware einen anderen Hypervisor verwenden.

In der folgenden Tabelle werden die erforderlichen Hardwarekomponenten für die Konfiguration und Implementierung von FlexPod Express aufgeführt. Je nach den Anforderungen des Kunden können die in einer beliebigen Implementierung dieser Lösung verwendeten Hardwarekomponenten abweichen.

Trennt	Menge
AFF C190: 2-Node-Cluster	1
Cisco C220 M5 Server	2
Cisco Nexus 31108PC-V-Switch	2
Cisco UCS Virtual Interface Card (VIC) 1457 für Cisco UCS C220 M5 Rack Server	2

In dieser Tabelle ist die zusätzlich zur Basiskonfiguration für die Implementierung von 10 GbE erforderliche Hardware aufgeführt.

Trennt	Menge
Cisco UCS C220 M5 Server	2
Cisco VIC 1457	2

Softwareanforderungen

In der folgenden Tabelle werden die Softwarekomponenten aufgeführt, die für die Implementierung der Architekturen der FlexPod Express Lösungen erforderlich sind.

Software	Version	Details
Cisco Integrated Management Controller (CIMC)	4.0.4	Für Cisco UCS C220 M5 Rack Server
Cisco Nenic-Treiber	1.0.0.29	Für VIC 1457 Schnittstellenkarten
Cisco NX-OS	7.0(3)I7(6)	Für Cisco Nexus 31108PC-V Switches
NetApp ONTAP	9.6	Für AFF C190 Controller

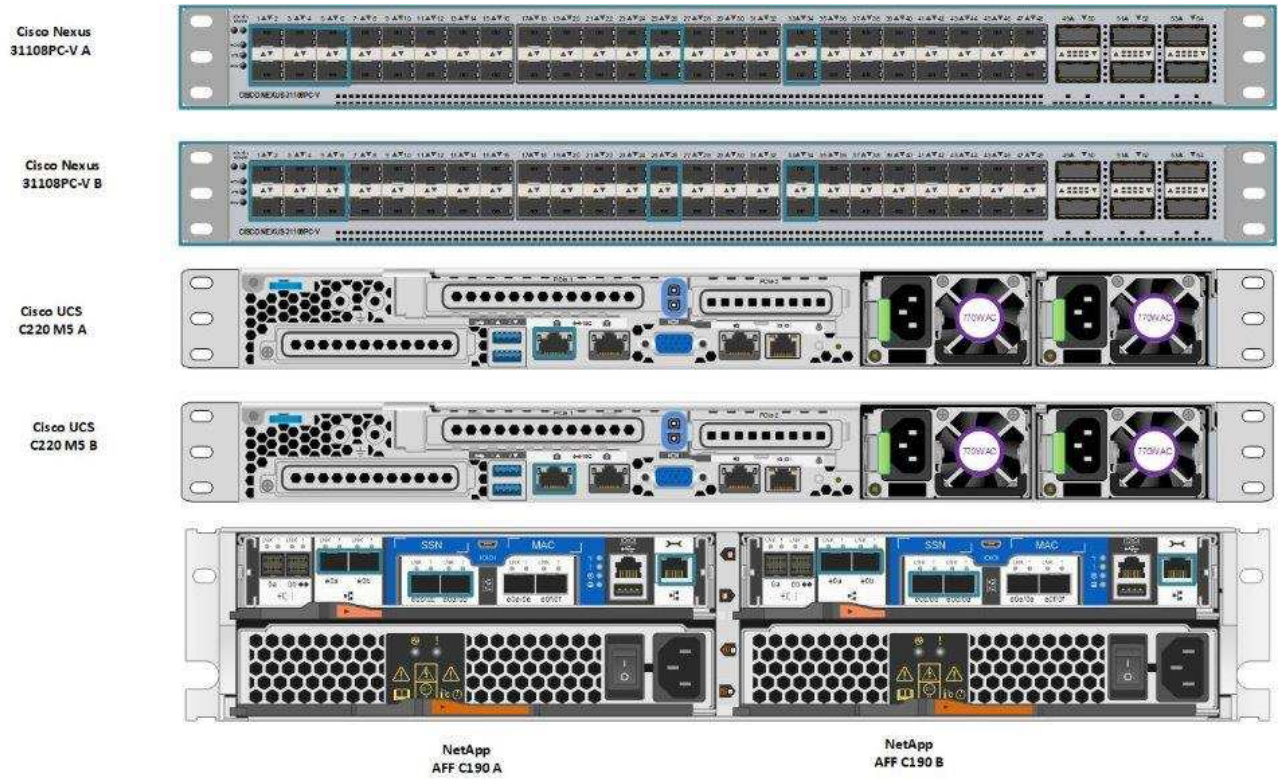
In dieser Tabelle ist die für alle VMware vSphere Implementierungen auf FlexPod Express erforderliche Software aufgeführt.

Software	Version
VMware vCenter Server Appliance	6.7U2
VMware vSphere ESXi Hypervisor	6.7U2
NetApp VAAI Plug-in für ESXi	1.1.2
NetApp VSC	9.6

Informationen zur FlexPod Express Verkabelung

Diese Referenzvalidierung ist verkabelt, wie in den folgenden Abbildungen und Tabellen gezeigt.

Diese Abbildung zeigt die Verkabelung zur Referenzvalidierung.



In der folgenden Tabelle sind die Verkabelungsinformationen für den Cisco Nexus Switch 31108PC-V-A aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus Switch 31108PC-V A	Eth1/1	NetApp AFF C190 Storage-Controller A	e0c
	Eth1/2	NetApp AFF C190 Storage-Controller B	e0c
	Eth1/3	Cisco UCS C220 C-Series Standalone Server A	MLOM0
	Eth1/4	Cisco UCS C220 C-Series Standalone Server B	MLOM0
	Eth1/5	Cisco UCS C220 C-Series Standalone Server A	MLOM1
	Eth1/6	Cisco UCS C220 C-Series Standalone Server B	MLOM1
	Eth1/25	Cisco Nexus Switch 31108PC-V B	Eth1/25
	Eth1/26	Cisco Nexus Switch 31108PC-V B	Eth1/26
	Eth1/33	NetApp AFF C190 Storage-Controller A	E0M
	Eth1/34	Cisco UCS C220 C-Series Standalone Server A	CIMC (FEX135/1/25)

In dieser Tabelle sind die Verkabelungsinformationen für den Cisco Nexus Switch 31108PC-V- B. aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus Switch 31108PC-V B	Eth1/1	NetApp AFF C190 Storage-Controller A	e0d
	Eth1/2	NetApp AFF C190 Storage-Controller B	e0d
	Eth1/3	Cisco UCS C220 C-Series Standalone Server A	MLOM2
	Eth1/4	Cisco UCS C220 C-Series Standalone Server B	MLOM2
	Eth1/5	Cisco UCS C220 C-Series Standalone Server A	MLOM3
	Eth1/6	Cisco UCS C220 C-Series Standalone Server B	MLOM3
	Eth1/25	Cisco Nexus Switch 31108 A	Eth1/25
	Eth1/26	Cisco Nexus Switch 31108 A	Eth1/26
	Eth1/33	NetApp AFF C190 Storage-Controller B	E0M
	Eth1/34	Cisco UCS C220 C-Series Standalone Server B	CIMC (FEX135/1/26)

In dieser Tabelle sind die Verkabelungsinformationen für NetApp AFF C190 Storage Controller aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF C190 Storage-Controller A	e0a	NetApp AFF C190 Storage-Controller B	e0a
	e0b	NetApp AFF C190 Storage-Controller B	e0b
	e0c	Cisco Nexus Switch 31108PC-V A	Eth1/1
	e0d	Cisco Nexus Switch 31108PC-V B	Eth1/1
	E0M	Cisco Nexus Switch 31108PC-V A	Eth1/33

In dieser Tabelle sind die Verkabelungsinformationen für NetApp AFF C190 Storage Controller B aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF C190 Storage-Controller B	e0a	NetApp AFF C190 Storage-Controller A	e0a
	e0b	NetApp AFF C190 Storage-Controller A	e0b
	e0c	Cisco Nexus Switch 31108PC-V A	Eth1/2
	e0d	Cisco Nexus Switch 31108PC-V B	Eth1/2
	E0M	Cisco Nexus Switch 31108PC-V B	Eth1/33

Implementierungsverfahren

Überblick

Dieses Dokument enthält Details zur Konfiguration eines vollständig redundanten, hochverfügbaren FlexPod Express-Systems. Um diese Redundanz Rechnung zu tragen, werden die in jedem Schritt konfigurierten Komponenten entweder als Komponente A oder Komponente B bezeichnet Controller A und Controller B identifizieren beispielsweise die beiden NetApp Storage Controller, die in diesem Dokument bereitgestellt werden. Switch A und Switch B identifizieren ein Paar Cisco Nexus-Switches.

Zusätzlich beschreibt dieses Dokument Schritte zur Bereitstellung mehrerer Cisco UCS-Hosts, die sequenziell als Server A, Server B usw. identifiziert werden können.

Um anzugeben, dass Sie in einem Schritt Informationen zu Ihrer Umgebung angeben sollten, `<<text>>` Wird als Teil der Befehlsstruktur angezeigt. Das folgende Beispiel enthält die `vlan create` Befehl:

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

Mit diesem Dokument können Sie die FlexPod Express Umgebung vollständig konfigurieren. Bei diesem Prozess müssen Sie in verschiedenen Schritten kundenspezifische Namenskonventionen, IP-Adressen und VLAN-Schemata (Virtual Local Area Network) einfügen. Die folgende Tabelle beschreibt die für die Implementierung erforderlichen VLANs, wie in diesem Leitfaden beschrieben. Diese Tabelle kann anhand der spezifischen Standortvariablen abgeschlossen und zur Implementierung der Konfigurationsschritte des Dokuments verwendet werden.

Wenn Sie separate in-Band- und Out-of-Band-Management-VLANs verwenden, müssen Sie eine Layer-3-Route zwischen ihnen erstellen. Für diese Validierung wurde ein gemeinsames Management-VLAN genutzt.

VLAN-Name	VLAN-Zweck	VLAN-ID	
Management-VLAN	VLAN für Management-Schnittstellen	3437	VSwitch0
NFS-VLAN	VLAN für NFS-Verkehr	3438	VSwitch0
VMware vMotion VLAN	VLAN, das für die Verschiebung von Virtual Machines (VMs) von einem physischen Host auf einen anderen festgelegt ist	3441	VSwitch0
VM-Traffic-VLAN	VLAN für den Datenverkehr von VM-Applikationen	3442	VSwitch0
ISCSI-A-VLAN	VLAN für iSCSI-Verkehr auf Fabric A	3439	IScsiBootvSwitch
ISCSI-B-VLAN	VLAN für iSCSI-Datenverkehr auf Fabric B	3440	IScsiBootvSwitch
Natives VLAN	VLAN, dem nicht getaggte Frames zugewiesen sind	2	

Die VLAN-Nummern sind in der gesamten Konfiguration von FlexPod Express erforderlich. Die VLANs werden als bezeichnet `<<var_xxxx_vlan>>`, Wo `xxxx` Dient dem VLAN (z. B. iSCSI-A).

In dieser Validierung wurden zwei vSwitches erstellt.

In der folgenden Tabelle sind die vSwitches der Lösung aufgeführt.

VSwitch-Name	Aktive Adapter	Ports	MTU	Lastverteilung
VSwitch0	Vmnic2, vmnic4	Standard (120)	9000	Route basierend auf IP-Hash
IScsiBootvSwitch	Vmnic3, vmnic5	Standard (120)	9000	Route basierend auf der ursprünglichen virtuellen Port-ID.

Die IP-Hash-Methode zum Lastausgleich erfordert die richtige Konfiguration für den zugrunde liegenden physischen Switch mithilfe von SRC-DST-IP EtherChannel mit einem statischen (Modus ein) Port-Kanal. Sollte die Konnektivität wegen einer möglichen Switch-Fehlkonfiguration zeitweise unterbrochen werden, muss während der Fehlerbehebung der Port-Channel-Einstellungen eines der beiden zugehörigen Uplink-Ports am Cisco Switch vorübergehend heruntergefahren werden, um die Kommunikation zum ESXi Management vmKernel Port wiederherzustellen.

In der folgenden Tabelle werden die erstellten VMware VMs aufgeführt.

VM-Beschreibung	Host-Name
VMware vCenter Server	FlexPod-VCSA

VM-Beschreibung	Host-Name
Virtual Storage Console	FlexPod-VSC

Implementierung von Cisco Nexus 31108PC-V

In diesem Abschnitt wird die in einer FlexPod Express Umgebung verwendete Cisco Nexus 331108PC-V Switch-Konfiguration beschrieben.

Ersteinrichtung des Cisco Nexus 31108PC-V Switches

In den folgenden Verfahren wird die Konfiguration von Cisco Nexus Switches für die Verwendung in einer grundlegenden FlexPod Express Umgebung beschrieben.

> Bei diesem Verfahren wird davon ausgegangen, dass Sie einen Cisco Nexus 31108PC-V mit NX-OS Software Version 7.0(3)I7(6) verwenden.

1. Nach dem ersten Booten und der Verbindung zum Konsolen-Port des Switches wird automatisch das Cisco NX-OS Setup gestartet. Diese Erstkonfiguration betrifft grundlegende Einstellungen wie den Switch-Namen, die mgmt0-Schnittstellenkonfiguration und die Einrichtung der Secure Shell (SSH).
2. Das FlexPod Express Managementnetzwerk lässt sich auf unterschiedliche Weise konfigurieren. Die mgmt0-Schnittstellen auf den 31108PC-V-Switches können an ein bestehendes Managementnetzwerk angeschlossen werden, oder die mgmt0-Schnittstellen der 31108PC-V-Switches können in einer Back-to-Back-Konfiguration angeschlossen werden. Dieser Link kann jedoch nicht für externen Managementzugriff wie SSH-Datenverkehr verwendet werden.

   > In diesem Implementierungsleitfaden werden die FlexPod Express Cisco Nexus 31108PC-V-Switches mit einem vorhandenen Managementnetzwerk verbunden.

3. Um die Cisco Nexus 31108PC-V-Switches zu konfigurieren, schalten Sie den Switch ein, und befolgen Sie die Anweisungen auf dem Bildschirm, wie hier bei der Ersteinrichtung beider Switches dargestellt, und ersetzen Sie die entsprechenden Werte für die Switch-spezifischen Informationen.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. Dann sehen Sie eine Zusammenfassung Ihrer Konfiguration, und Sie werden gefragt, ob Sie sie bearbeiten möchten. Wenn die Konfiguration korrekt ist, geben Sie ein `n`.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. Sie werden dann gefragt, ob Sie diese Konfiguration verwenden und speichern möchten. Wenn ja, geben Sie ein `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Wiederholen Sie dieses Verfahren für Cisco Nexus Switch B.

Aktivieren Sie die erweiterten Funktionen

Bestimmte erweiterte Funktionen müssen in Cisco NX-OS aktiviert sein, um zusätzliche Konfigurationsoptionen bereitzustellen. Um die entsprechenden Funktionen auf dem Cisco Nexus Switch A und Switch B zu aktivieren, geben Sie den Konfigurationsmodus mit dem Befehl (config t) ein und führen Sie die folgenden Befehle aus:

```
feature interface-vlan
feature lacp
feature vpc
```

Der Standard-Port-Channel-Load-Balancing-Hash verwendet die Quell- und Ziel-IP-Adressen, um den Load-Balancing-Algorithmus über die Schnittstellen im Port-Kanal zu bestimmen. Sie können eine bessere Verteilung über die Mitglieder des Port-Kanals erzielen, indem Sie mehr Inputs für den Hash-Algorithmus bereitstellen, der über die Quell- und Ziel-IP-Adressen hinausgeht. Aus dem gleichen Grund empfiehlt NetApp dringend, den Hash-Algorithmus der Quell- und Ziel-TCP-Ports hinzuzufügen.

Geben Sie im Konfigurationsmodus (config t) die folgenden Befehle ein, um die Konfiguration für den globalen Port Channel-Lastausgleich auf dem Cisco Nexus Switch A und Switch B festzulegen:

```
port-channel load-balance src-dst ip-l4port
```

Konfigurieren Sie die globale Spanning-Struktur

Die Cisco Nexus Plattform verwendet eine neue Sicherungsfunktion namens „Bridge Assurance“. Bridge Assurance schützt vor unidirektionalen Verbindungsfehlern oder anderen Softwarefehlern mit einem Gerät, das den Datenverkehr weiterführt, wenn der Spanning-Tree-Algorithmus nicht mehr ausgeführt wird. Die Ports können je nach Plattform in einen von mehreren Status platziert werden, einschließlich Netzwerk oder Edge.

NetApp empfiehlt, die Bridge-Assurance einzustellen, damit alle Ports standardmäßig für Netzwerkports gelten. Diese Einstellung zwingt den Netzwerkadministrator, die Konfiguration jedes Ports zu überprüfen. Außerdem werden die häufigsten Konfigurationsfehler angezeigt, z. B. nicht identifizierte Edge-Ports oder ein Nachbar, bei dem die Bridge-Assurance-Funktion nicht aktiviert ist. Außerdem ist es sicherer, den Spanning Tree Block viele Ports statt zu wenig zu haben, was den Standard-Port-Zustand ermöglicht, um die allgemeine Stabilität des Netzwerks zu verbessern.

Achten Sie beim Hinzufügen von Servern, Speicher- und Uplink-Switches auf den Spanning-Tree-Status, insbesondere wenn diese keine Bridge-Sicherheit unterstützen. In solchen Fällen müssen Sie möglicherweise den Porttyp ändern, um die Ports aktiv zu machen.

Die BPDU-Schutzfunktion (Bridge Protocol Data Unit) ist standardmäßig auf Edge-Ports als andere Schutzschicht aktiviert. Um Schleifen im Netzwerk zu vermeiden, wird der Port durch diese Funktion heruntergefahren, wenn BPDUs von einem anderen Switch auf dieser Schnittstelle angezeigt werden.

Führen Sie im Konfigurationsmodus (config t) die folgenden Befehle aus, um die standardmäßigen Spanning-Tree-Optionen, einschließlich des Standard-Porttyps und BPDU-Guard, am Cisco Nexus-Switch A und Switch B zu konfigurieren:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

Definieren Sie die VLANs

Bevor individuelle Ports mit unterschiedlichen VLANs konfiguriert sind, müssen auf dem Switch Layer- 2-VLANs definiert werden. Es ist auch eine gute Praxis, die VLANs zu benennen, um zukünftig eine einfache Fehlerbehebung zu ermöglichen.

Führen Sie im Konfigurationsmodus (config t) die folgenden Befehle aus, um die Layer- 2-VLANs auf dem Cisco Nexus Switch A und Switch B zu definieren und zu beschreiben:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Konfiguration von Zugriffs- und Management-Port-Beschreibungen

Wie bei der Zuordnung von Namen zu den Layer-2-VLANs können die Einstellungsbeschreibungen für alle Schnittstellen sowohl bei der Bereitstellung als auch bei der Fehlerbehebung helfen.

Geben Sie im Konfigurationsmodus (config t) bei jedem der Switches die folgenden Port-Beschreibungen für die FlexPod Express Large-Konfiguration ein:

Cisco Nexus Switch A

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus Switch B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Konfiguration der Server- und Storage-Managementschnittstellen

Die Management-Schnittstellen sowohl für den Server als auch für den Storage verwenden in der Regel nur ein einziges VLAN. Konfigurieren Sie daher die Ports der Managementoberfläche als Access Ports. Definieren Sie das Management-VLAN für jeden Switch und ändern Sie den Porttyp Spanning-Tree in Edge.

Geben Sie im Konfigurationsmodus (config t) die folgenden Befehle ein, um die Porteinstellungen für die Management-Schnittstellen sowohl der Server als auch des Storage zu konfigurieren:

Cisco Nexus Switch A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus Switch B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Führen Sie die globale Konfiguration des virtuellen Port-Channels durch

Über einen Virtual Port Channel (vPC) können Links, die physisch mit zwei verschiedenen Cisco Nexus-Switches verbunden sind, mit einem dritten Gerät als einzelner Port-Channel angezeigt werden. Das dritte Gerät kann ein Switch, Server oder ein anderes Netzwerkgerät sein. Ein vPC bietet Multipathing auf Layer-2-Ebene. Dadurch kann Redundanz erzeugt werden, indem die Bandbreite erhöht wird. Dies ermöglicht mehrere parallele Pfade zwischen Nodes und Lastverteilung, bei denen alternative Pfade vorhanden sind.

Ein vPC bietet die folgenden Vorteile:

- Aktivieren eines einzelnen Geräts zur Verwendung eines Port-Kanals über zwei vorgelagerte Geräte
- Verhindern blockierter Ports für Spanning-Tree-Protokolle
- Eine Topologie ohne Schleife
- Nutzung aller verfügbaren Uplink-Bandbreite
- Schnelle Konvergenz bei Ausfall der Verbindung oder eines Geräts
- Ausfallsicherheit auf Verbindungsebene
- Unterstützung für Hochverfügbarkeit

Die vPC-Funktion erfordert eine Ersteinrichtung zwischen den beiden Cisco Nexus-Switches, damit diese ordnungsgemäß funktionieren. Wenn Sie die Back-to-Back-mgt0-Konfiguration verwenden, verwenden Sie die

auf den Schnittstellen definierten Adressen und stellen Sie sicher, dass sie über die kommunizieren können `ping <<switch_A/B_mgmt0_ip_addr>>vrf` Management-Befehl.

Führen Sie im Konfigurationsmodus (config t) die folgenden Befehle aus, um die globale vPC-Konfiguration für beide Switches zu konfigurieren:

Cisco Nexus Switch A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus Switch B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Konfigurieren Sie die Speicheranschlusskanäle

Die NetApp Storage-Controller ermöglichen eine aktiv/aktiv-Verbindung zum Netzwerk mithilfe des Link Aggregation Control Protocol (LACP). Die Verwendung von LACP wird bevorzugt, da es sowohl Verhandlungen als auch Protokollierung zwischen den Switches hinzufügt. Da das Netzwerk für vPC eingerichtet ist, können Sie mit diesem Ansatz aktiv/aktiv-Verbindungen vom Storage zu separaten physischen Switches nutzen. Jeder Controller verfügt über zwei Links zu jedem der Switches. Alle vier Links sind jedoch Teil derselben vPC und Interface Group (ifrp).

Führen Sie im Konfigurationsmodus (config t) die folgenden Befehle auf jedem der Switches aus, um die einzelnen Schnittstellen und die daraus resultierende Port Channel-Konfiguration für die mit dem NetApp AFF Controller verbundenen Ports zu konfigurieren.

1. Führen Sie die folgenden Befehle an Switch A und Switch B aus, um die Port-Kanäle für Speicher-Controller A zu konfigurieren:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Führen Sie die folgenden Befehle an Switch A und Switch B aus, um die Port-Kanäle für Storage Controller B zu konfigurieren:

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

Konfigurieren Sie die Serververbindungen

Die Cisco UCS Server verfügen über eine virtuelle Schnittstellenkarte mit vier Ports, die zum Datenverkehr und Booten des ESXi Betriebssystems über iSCSI verwendet wird. Diese Schnittstellen werden für den Failover untereinander konfiguriert, wodurch über eine einzelne Verbindung hinaus eine zusätzliche Redundanz gewährleistet wird. Wenn diese Links über mehrere Switches verteilt werden, kann der Server sogar einen vollständigen Switch-Ausfall überstehen.

Führen Sie im Konfigurationsmodus (config t) die folgenden Befehle aus, um die Porteinstellungen für die mit jedem Server verbundenen Schnittstellen zu konfigurieren.

Cisco Nexus Switch A: Cisco UCS Server-A- und Cisco UCS Server-B-Konfiguration

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Cisco Nexus Switch B: Konfiguration von Cisco UCS Server A und Cisco UCS Server B

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Konfigurieren Sie die Server-Port-Kanäle

Führen Sie die folgenden Befehle auf Switch A und Switch B aus, um die Port-Kanäle für Server A zu konfigurieren:

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

Führen Sie die folgenden Befehle auf Switch A und Switch B aus, um die Port-Kanäle für Server B zu konfigurieren:

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

In dieser Lösungsvalidierung wurde eine MTU von 9000 verwendet. Sie können jedoch einen anderen Wert für die MTU konfigurieren, der Ihren Anwendungsanforderungen entspricht. Es ist wichtig, für die gesamte FlexPod Lösung denselben MTU-Wert festzulegen. Falsche MTU-Konfigurationen zwischen den Komponenten führen zu Paketfallen, und diese Pakete müssen erneut übertragen werden, was sich auf die Gesamtleistung der Lösung auswirkt.

Um die Lösung durch Hinzufügen weiterer Cisco UCS Server zu skalieren, führen Sie die vorherigen Befehle mit den Switch-Ports aus, die die neu hinzugefügten Server an Switches A und B angeschlossen wurden

Uplink in eine vorhandene Netzwerkinfrastruktur

Je nach verfügbarer Netzwerkinfrastruktur können zur Uplink der FlexPod Umgebung mehrere Methoden und Funktionen verwendet werden. Bei einer vorhandenen Cisco Nexus Umgebung empfiehlt NetApp den Einsatz

von vPCs, um die in der FlexPod Umgebung enthaltenen Cisco Nexus 31108 Switches in die Infrastruktur zu integrieren. Bei den Uplinks können 10-GbE-Uplinks für eine 10-GbE-Infrastrukturlösung oder 1 GbE für eine Infrastrukturlösung (sofern erforderlich) verwendet werden. Die zuvor beschriebenen Verfahren können zur Erstellung eines Uplink vPC in der vorhandenen Umgebung verwendet werden. Führen Sie den Kopierstart aus, um die Konfiguration nach Abschluss der Konfiguration auf jedem Switch zu speichern.

"Weiter: NetApp Verfahren zur Storage-Implementierung (Teil 1)."

Verfahren zur NetApp Storage-Implementierung (Teil 1)

In diesem Abschnitt wird das NetApp AFF Storage-Implementierungsverfahren beschrieben.

Installation von NetApp Storage Controller AFF C190 Serie

NetApp Hardware Universe

Die NetApp Hardware Universe (HWU) Applikation bietet unterstützte Hardware- und Softwarekomponenten für jede spezifische ONTAP-Version. Das Tool liefert Konfigurationsinformationen für alle NetApp Storage Appliances, die derzeit von der ONTAP Software unterstützt werden. Zudem bietet er eine Tabelle mit den Kompatibilitäten der Komponenten.

Vergewissern Sie sich, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, von der zu installierenden Version von ONTAP unterstützt werden:

Auf das zugreifen "HWU" Anwendung zum Anzeigen der Systemkonfigurationsleitfäden. Klicken Sie auf die Registerkarte Controller, um sich die Kompatibilität zwischen verschiedenen Versionen der ONTAP Software und den NetApp Storage Appliances mit den gewünschten Spezifikationen anzusehen.

Wenn Sie Komponenten nach Storage Appliance vergleichen möchten, klicken Sie alternativ auf Storage-Systeme vergleichen.

Voraussetzungen für Controller der Serie AFF FC190
Informationen zum Planen des physischen Standorts der Storage-Systeme finden Sie im NetApp Hardware Universe. Siehe folgende Abschnitte: • Elektrische Anforderungen • Unterstützte Netzkabel • Onboard-Ports und -Kabel

Storage Controller

Befolgen Sie die Anweisungen zur physischen Installation der Controller im AFF "C190" Dokumentation.

NetApp ONTAP 9.6

Konfigurationsarbeitsblatt

Bevor Sie das Setup-Skript ausführen, füllen Sie das Konfigurationsarbeitsblatt aus der Produktanleitung aus. Das Konfigurationsarbeitsblatt ist im ONTAP 9.6 Software-Setup-Leitfaden verfügbar.

Das System ist in einer Konfiguration mit zwei Nodes ohne Switches eingerichtet.

Die nachfolgende Tabelle enthält Informationen zur Installation und Konfiguration von ONTAP 9.6.

Cluster-Details	Wert für Cluster-Details
Cluster Node A IP-Adresse	<<var_nodeA_Mgmt_ip>>
Cluster-Node A-Netmask	<<var_nodeA_mgmt_maska>>
Cluster Node Ein Gateway	\<<var_nodeA_mgmt_Gateway>
Cluster-Node A-Name	<<var_nodeA>>
Cluster-Node B-IP-Adresse	<<var_nodeB_Mgmt_ip>>
Cluster-Node B-Netmask	<<var_nodeB_mgmt_maska>>
Cluster-Node B-Gateway	\<<var_nodeB_mgmt_Gateway>
Name für Cluster-Node B	<<var_nodeB>>
ONTAP 9.6-URL	\<<var_url_Boot_Software>
Name für Cluster	<<var_clustername>>
Cluster-Management-IP-Adresse	<<var_clustermgmt_ip>>
Cluster B-Gateway	<<var_clustermgmt_Gateway>>
Cluster B Netmask	<<var_clustermgmt_maska>>
Domain-Name	<<var_Domain_Name>>
DNS-Server-IP (Sie können mehrere eingeben)	<var_dns_Server_ip
NTP-Server-IP (Sie können mehrere eingeben)	\<<var_ntp_Server_ip>

Konfigurieren Sie Node A

Führen Sie die folgenden Schritte aus, um Node A zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg-C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   Lassen Sie das System booten.

   ```
   autoboot
   ```

2. Drücken Sie Strg-C, um das Startmenü aufzurufen.

Wenn ONTAP 9.6 nicht die Version der gerade gestarteten Software ist, fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Wenn ONTAP 9.6 die Version wird gebootet, wählen Sie Option 8 und y aus, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

3. Um neue Software zu installieren, wählen Sie Option 7.
4. Geben Sie y ein, um ein Upgrade durchzuführen.
5. Wählen Sie E0M für den Netzwerkport aus, den Sie für den Download verwenden möchten.
6. Geben Sie y ein, um jetzt neu zu starten.
7. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

8. Geben Sie die URL ein, auf der die Software gefunden werden kann.

Dieser Webserver muss pingfähig sein.

```
<<var_url_boot_software>>
```

9. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an.
10. Geben Sie y ein, um die neu installierte Software als Standard festzulegen, die für nachfolgende Neustarts verwendet werden soll.
11. Geben Sie y ein, um den Node neu zu booten.

Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

12. Drücken Sie Strg-C, um das Startmenü aufzurufen.
13. Wählen Sie Option 4 für saubere Konfiguration und Initialisieren Sie alle Festplatten.
14. Geben Sie y bis Zero Disks ein, setzen Sie die Konfiguration zurück und installieren Sie ein neues Dateisystem.
15. Geben Sie y ein, um alle Daten auf den Festplatten zu löschen.

Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert. Sie können mit der Node B-Konfiguration fortfahren, während die Festplatten für Node A auf Null gesetzt werden.

Beginnen Sie während der Initialisierung von Node A mit der Konfiguration von Node B.

Konfigurieren Sie Node B

Führen Sie die folgenden Schritte aus, um Node B zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg-C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Drücken Sie Strg-C, um das Startmenü aufzurufen.

```
autoboot
```

3. Drücken Sie bei der entsprechenden Aufforderung Strg-C.

> Wenn ONTAP 9.6 nicht die Version der gerade gestarteten Software ist, fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Wenn ONTAP 9.6 die Version wird gebootet, wählen Sie Option 8 und y aus, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

4. Um neue Software zu installieren, wählen Sie Option 7.A.
5. Geben Sie y ein, um ein Upgrade durchzuführen.
6. Wählen Sie E0M für den Netzwerkport aus, den Sie für den Download verwenden möchten.
7. Geben Sie y ein, um jetzt neu zu starten.
8. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Geben Sie die URL ein, auf der die Software gefunden werden kann.

> Dieser Webserver muss pingfähig sein.

```
<<var_url_boot_software>>
```

10. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an.
11. Geben Sie y ein, um die neu installierte Software als Standard festzulegen, die für nachfolgende Neustarts verwendet werden soll.
12. Geben Sie y ein, um den Node neu zu booten.

Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

13. Drücken Sie Strg-C, um das Startmenü aufzurufen.
14. Wählen Sie Option 4 für saubere Konfiguration und Initialisieren Sie alle Festplatten.
15. Geben Sie y bis Zero Disks ein, setzen Sie die Konfiguration zurück und installieren Sie ein neues Dateisystem.
16. Geben Sie y ein, um alle Daten auf den Festplatten zu löschen.

Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert.

Fortsetzung der Node A-Konfiguration und Cluster-Konfiguration

Führen Sie von einem Konsolen-Port-Programm, das an den Storage Controller A (Node A)-Konsolenport angeschlossen ist, das Node-Setup-Skript aus. Dieses Skript wird angezeigt, wenn ONTAP 9.6 das erste Mal auf dem Node gebootet wird.

In ONTAP 9.6 wurde das Verfahren zur Einrichtung von Nodes und Clustern geringfügig geändert. Der Cluster-Setup-Assistent wird nun zum Konfigurieren des ersten Knotens in einem Cluster verwendet, und der ONTAP System Manager (ehemals OnCommand System Manager) wird zum Konfigurieren des Clusters verwendet.

1. Befolgen Sie die Anweisungen zum Einrichten von Node A

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navigieren Sie zur IP-Adresse der Managementoberfläche des Knotens.

> Das Cluster-Setup kann auch über die CLI durchgeführt werden. In diesem Dokument wird die Cluster-Einrichtung mit der von System Manager geführten Einrichtung beschrieben.

3. Klicken Sie auf Guided Setup, um das Cluster zu konfigurieren.
4. Eingabe `<<var_clustername>>` Für den Cluster-Namen und `<<var_nodeA>>` Und `<<var_nodeB>>` Für jeden der Nodes, die Sie konfigurieren. Geben Sie das Passwort ein, das Sie für das Speichersystem verwenden möchten. Wählen Sie für den Cluster-Typ Cluster ohne Switch aus. Geben Sie die Cluster-Basislizenz ein.
5. Außerdem können Funktionslizenzen für Cluster, NFS und iSCSI eingegeben werden.
6. Eine Statusmeldung, die angibt, dass das Cluster erstellt wird. Diese Statusmeldung durchlaufen mehrere Statusarten. Dieser Vorgang dauert mehrere Minuten.
7. Konfigurieren des Netzwerks.

a. Deaktivieren Sie die Option IP-Adressbereich.

b. Eingabe `<<var_clustermgmt_ip>>` Im Feld Cluster-Management-IP-Adresse `<<var_clustermgmt_mask>>` Im Feld „Netzmaske“ und `<<var_clustermgmt_gateway>>` Im Feld Gateway. Verwenden Sie den … Wählen Sie im Feld Port die Option E0M für Node A aus

c. Die Node-Management-IP für Node A ist bereits gefüllt. Eingabe `<<var_nodeA_mgmt_ip>>` Für Node B.

d. Eingabe `<<var_domain_name>>` Im Feld DNS-Domain-Name. Eingabe `<<var_dns_server_ip>>` Im Feld IP-Adresse des DNS-Servers.

> Sie können mehrere IP-Adressen des DNS-Servers eingeben.

e. Eingabe `10.63.172.162` Im Feld primärer NTP-Server.

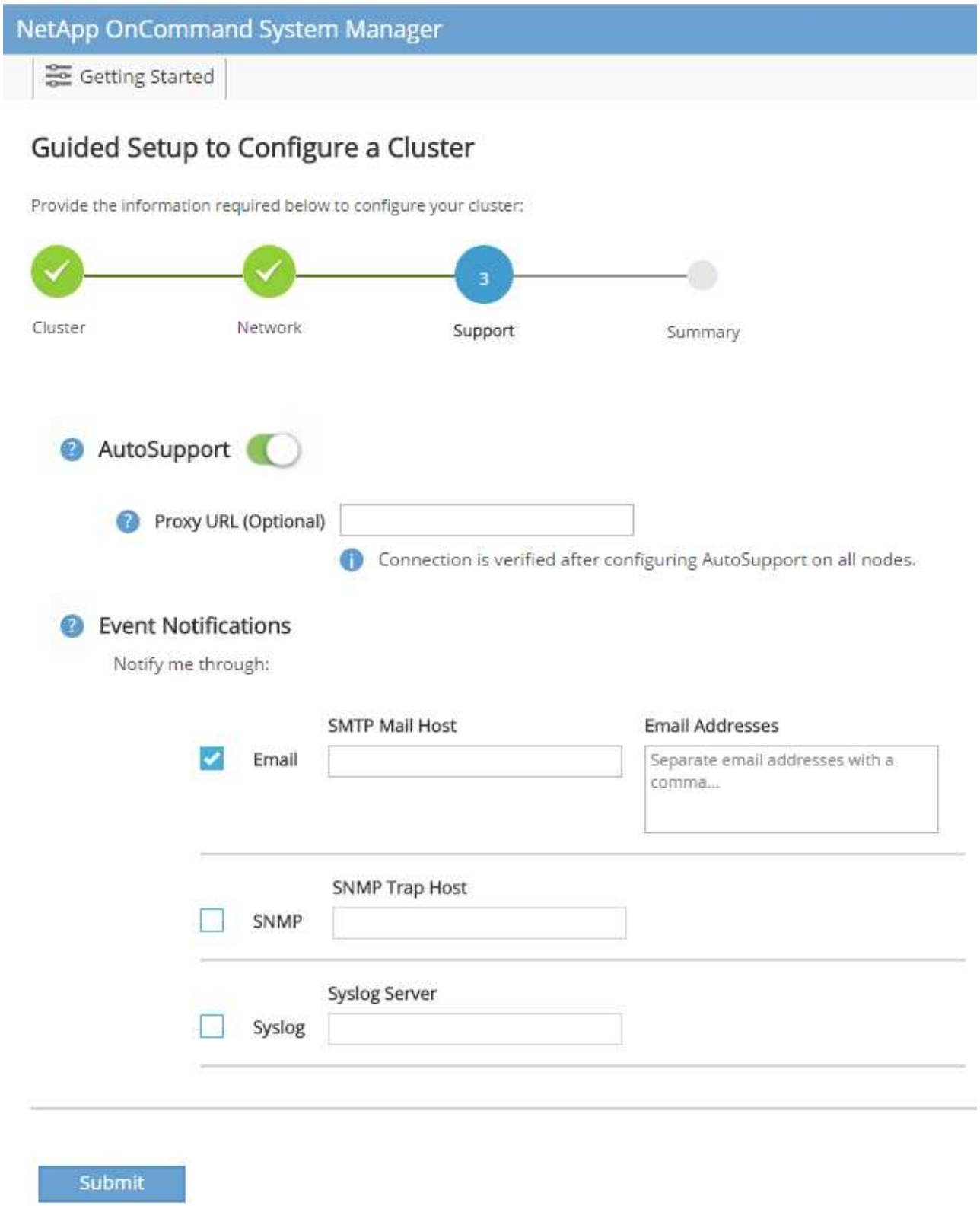
> Sie können auch einen alternativen NTP-Server eingeben. Die IP-Adresse `10.63.172.162` Von `<<var_ntp_server_ip>>` Ist die Nexus Management IP.

8. Konfigurieren Sie die Support-Informationen.

a. Wenn in Ihrer Umgebung ein Proxy für den Zugriff auf AutoSupport erforderlich ist, geben Sie die URL unter Proxy-URL ein.

b. Geben Sie den SMTP-Mail-Host und die E-Mail-Adresse für Ereignisbenachrichtigungen ein.

> Sie müssen mindestens die Methode für die Ereignisbenachrichtigung einrichten, bevor Sie fortfahren können. Sie können eine beliebige der Methoden auswählen.



Wenn das System angibt, dass die Cluster-Konfiguration abgeschlossen ist, klicken Sie auf Manage Your Cluster, um den Storage zu konfigurieren.

Fortsetzung der Storage-Cluster-Konfiguration

Nach der Konfiguration der Storage-Nodes und des Basis-Clusters können Sie die Konfiguration des Storage-Clusters fortsetzen.

Alle freien Festplatten auf Null stellen

Führen Sie den folgenden Befehl aus, um alle freien Festplatten im Cluster zu löschen:

```
disk zerospares
```

Legen Sie die Persönlichkeit der Onboard-UTA2-Ports fest

1. Überprüfen Sie den aktuellen Modus und den aktuellen Typ für die Ports, indem Sie den ausführen `ucadmin show` Befehl.

```
AFF C190::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. Überprüfen Sie, ob der aktuelle Modus der verwendeten Ports cna ist und der aktuelle Typ auf Ziel gesetzt ist. Wenn nicht, ändern Sie die Portpersönlichkeit mit dem folgenden Befehl:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Die Ports müssen offline sein, um den vorherigen Befehl auszuführen. Führen Sie den folgenden Befehl aus, um einen Port offline zu schalten:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Wenn Sie die Port-Persönlichkeit geändert haben, müssen Sie jeden Node neu booten, damit die Änderung wirksam wird.

Benennen Sie die logischen Management-Schnittstellen um

Führen Sie die folgenden Schritte aus, um die logischen Management-Schnittstellen (LIFs) umzubenennen:

1. Zeigt die aktuellen Management-LIF-Namen an.

```
network interface show –vserver <<clustername>>
```

2. Benennen Sie die Cluster-Management-LIF um.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Benennen Sie die Management-LIF für Node B um.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

Legen Sie für das Cluster-Management den automatischen Wechsel zurück

Legen Sie den Parameter „Auto-revert“ auf der Cluster-Managementoberfläche fest.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Richten Sie die Service Processor-Netzwerkschnittstelle ein

Um dem Service-Prozessor auf jedem Node eine statische IPv4-Adresse zuzuweisen, führen Sie die folgenden Befehle aus:

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Die Service-Prozessor-IP-Adressen sollten sich im gleichen Subnetz wie die Node-Management-IP-Adressen befinden.

Aktivieren Sie Storage-Failover in ONTAP

Führen Sie die folgenden Befehle in einem Failover-Paar aus, um zu überprüfen, ob das Storage-Failover aktiviert ist:

1. Überprüfen Sie den Status des Storage-Failovers.

```
storage failover show
```

> Beides `<<var_nodeA>>` Und `<<var_nodeB>>` Muss in der Lage sein, ein Takeover durchzuführen. Fahren Sie mit Schritt 3 fort, wenn die Knoten ein Takeover durchführen können.

2. Aktivieren Sie Failover bei einem der beiden Nodes.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> Durch die Aktivierung von Failover auf einem Node wird dies für beide Nodes möglich.

3. Überprüfen Sie den HA-Status des Clusters mit zwei Nodes.

> Dieser Schritt gilt nicht für Cluster mit mehr als zwei Nodes.

```
cluster ha show
```

4. Fahren Sie mit Schritt 6 fort, wenn Hochverfügbarkeit konfiguriert ist. Wenn die Hochverfügbarkeit konfiguriert ist, wird bei Ausgabe des Befehls die folgende Meldung angezeigt:

```
High Availability Configured: true
```

5. Aktivieren Sie nur den HA-Modus für das Cluster mit zwei Nodes.

> Führen Sie diesen Befehl nicht für Cluster mit mehr als zwei Nodes aus, da es zu Problemen mit Failover kommt.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Überprüfung der korrekten Konfiguration von Hardware-Unterstützung und ggf. Änderung der Partner-IP-Adresse

```
storage failover hwassist show
```

Die Nachricht `Keep Alive Status: Error:` Zeigt an, dass einer der Controller keine hwassist-Warnungen von seinem Partner erhalten hat, was darauf hinweist, dass die Hardware-Unterstützung nicht konfiguriert ist. Führen Sie die folgenden Befehle aus, um die Hardware-Unterstützung zu konfigurieren.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Erstellen Sie eine Jumbo Frame MTU Broadcast-Domäne in ONTAP

Um eine Data Broadcast-Domäne mit einer MTU von 9000 zu erstellen, führen Sie die folgenden Befehle aus:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Entfernen Sie die Daten-Ports aus der Standard-Broadcast-Domäne

Die 10-GbE-Daten-Ports werden für iSCSI/NFS-Datenverkehr verwendet, diese Ports sollten aus der Standarddomäne entfernt werden. Die Ports e0e und e0f werden nicht verwendet und sollten auch aus der Standarddomäne entfernt werden.

Führen Sie den folgenden Befehl aus, um die Ports aus der Broadcast-Domäne zu entfernen:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deaktivieren Sie die Flusssteuerung bei UTA2-Ports

Eine NetApp Best Practice ist es, die Flusskontrolle bei allen UTA2-Ports, die mit externen Geräten verbunden sind, zu deaktivieren. Um die Flusssteuerung zu deaktivieren, führen Sie den folgenden Befehl aus:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Konfigurieren Sie LACP in ONTAP

Diese Art von Interface Group erfordert zwei oder mehr Ethernet-Schnittstellen und einen Switch, der LACP unterstützt. Stellen Sie sicher, dass die Konfiguration auf der Grundlage der Schritte in diesem Handbuch in Abschnitt 5.1 basiert.

Führen Sie an der Cluster-Eingabeaufforderung die folgenden Schritte aus:

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Konfigurieren Sie die Jumbo Frames in ONTAP

Um einen ONTAP-Netzwerkport zur Verwendung von Jumbo Frames zu konfigurieren (normalerweise mit einer MTU von 9,000 Byte), führen Sie die folgenden Befehle aus der Cluster-Shell aus:

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Erstellen von VLANs in ONTAP

Gehen Sie wie folgt vor, um VLANs in ONTAP zu erstellen:

1. Erstellen von NFS-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

   ```
   network port vlan create –node <<var_nodeA>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   network port vlan create –node <<var_nodeB>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
   <<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
   <<var_nfs_vlan_id>>
   ```

2. Erstellen von iSCSI-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. ERSTELLUNG VON MGMT-VLAN-Ports

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Datenaggregate in ONTAP erstellen

Während der ONTAP-Einrichtung wird ein Aggregat mit dem Root-Volume erstellt. Zum Erstellen weiterer Aggregate ermitteln Sie den Namen des Aggregats, den Node, auf dem er erstellt werden soll, und die Anzahl der enthaltenen Festplatten.

Führen Sie zum Erstellen von Aggregaten die folgenden Befehle aus:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Bewahren Sie mindestens eine Festplatte (wählen Sie die größte Festplatte) in der Konfiguration als Ersatzlaufwerk auf. Als Best Practice empfiehlt es sich, mindestens ein Ersatzteil für jeden Festplattentyp und jede Größe zu besitzen.

Beginnen Sie mit fünf Festplatten. Wenn zusätzlicher Storage erforderlich ist, können Sie einem Aggregat Festplatten hinzufügen.

Das Aggregat kann erst erstellt werden, wenn die Daten auf der Festplatte auf Null gesetzt werden. Führen Sie die aus `aggr show` Befehl zum Anzeigen des Erstellungsstatus des Aggregats. Fahren Sie nicht fort, bis aggr1_nodeA online ist.

Konfigurieren Sie die Zeitzone in ONTAP

Führen Sie den folgenden Befehl aus, um die Zeitsynchronisierung zu konfigurieren und die Zeitzone auf dem Cluster festzulegen:

```
timezone <<var_timezone>>
```

Im Osten der USA gilt beispielsweise die Zeitzone Amerika/New_York. Nachdem Sie mit der Eingabe des Zeitzonennamens begonnen haben, drücken Sie die Tabulatortaste, um die verfügbaren Optionen anzuzeigen.

Konfigurieren Sie SNMP in ONTAP

Führen Sie die folgenden Schritte aus, um die SNMP zu konfigurieren:

1. Konfigurieren Sie SNMP-Basisinformationen, z. B. Standort und Kontakt. Wenn Sie abgefragt werden, werden diese Informationen als angezeigt `sysLocation` Und `sysContact` Variablen in SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Konfigurieren Sie SNMP-Traps zum Senden an Remote-Hosts.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Konfigurieren Sie SNMPv1 in ONTAP

Um SNMPv1 zu konfigurieren, stellen Sie das freigegebene geheime Klartextkennwort ein, das als Community bezeichnet wird.

```
snmp community add ro <<var_snmp_community>>
```

Verwenden Sie die `snmp community delete all` Befehl mit Vorsicht. Wenn Community Strings für andere Überwachungsprodukte verwendet werden, entfernt dieser Befehl sie.

Konfigurieren Sie SNMPv3 in ONTAP

SNMPv3 erfordert, dass Sie einen Benutzer für die Authentifizierung definieren und konfigurieren. Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren:

1. Führen Sie die aus `security snmpusers` Befehl zum Anzeigen der Engine-ID.
2. Erstellen Sie einen Benutzer mit dem Namen `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Geben Sie die Engine-ID der autoritativen Einheit ein und wählen sie md5 als Authentifizierungsprotokoll aus.
4. Geben Sie bei der Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Authentifizierungsprotokoll ein.
5. Wählen Sie als Datenschutzprotokoll das aus.
6. Geben Sie bei Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Datenschutzprotokoll ein.

Konfigurieren Sie AutoSupport HTTPS in ONTAP

Das NetApp AutoSupport Tool sendet Zusammenfassung von Support-Informationen über HTTPS an NetApp. Führen Sie den folgenden Befehl aus, um AutoSupport zu konfigurieren:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Erstellen Sie eine Speicher-Virtual Machine

Um eine Storage Virtual Machine (SVM) für Infrastrukturen zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie die aus `vserver create` Befehl.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Das Datenaggregat wird zur Liste des Infrastruktur-SVM-Aggregats der NetApp VSC hinzugefügt.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Entfernen Sie die ungenutzten Storage-Protokolle der SVM, wobei NFS und iSCSI überlassen bleiben.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Aktivierung und Ausführung des NFS-Protokolls in der SVM Infrastructure

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Schalten Sie das ein `SVM vstorage` Parameter für das NetApp NFS VAAI Plug-in. Überprüfen Sie dann, ob NFS konfiguriert wurde.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Diese Befehle werden von ausgeführt `vserver` Befehlszeile, da SVMs zuvor Vserver genannt wurden.

Konfigurieren Sie NFSv3 in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
ESXi hostet Eine NFS-IP-Adresse	\<<var_esxi_hostA_nfs_ip>
ESXi Host B NFS-IP-Adresse	\<<var_esxi_hostB_nfs_ip>

Führen Sie die folgenden Befehle aus, um NFS auf der SVM zu konfigurieren:

1. Erstellen Sie eine Regel für jeden ESXi-Host in der Standard-Exportrichtlinie.
2. Weisen Sie für jeden erstellten ESXi Host eine Regel zu. Jeder Host hat seinen eigenen Regelindex. Ihr erster ESXi Host hat Regelindex 1, Ihr zweiter ESXi Host hat Regelindex 2 usw.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Weisen Sie die Exportrichtlinie dem Infrastruktur-SVM-Root-Volume zu.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

Die NetApp VSC verarbeitet automatisch die Exportrichtlinien, wenn Sie sie nach der Einrichtung von vSphere installieren möchten. Wenn Sie diese nicht installieren, müssen Sie Regeln für die Exportrichtlinie erstellen, wenn zusätzliche Server der Cisco UCS C-Serie hinzugefügt werden.

Erstellen Sie den iSCSI-Dienst in ONTAP

Führen Sie den folgenden Befehl aus, um den iSCSI-Service auf der SVM zu erstellen. Mit diesem Befehl wird auch der iSCSI-Service gestartet und der iSCSI-IQN für die SVM festgelegt. Überprüfen Sie, ob iSCSI konfiguriert wurde.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Spiegelung zur Lastverteilung von SVM-Root-Volumes in ONTAP erstellen

So erstellen Sie eine Spiegelung zur Lastverteilung des SVM-Root-Volumes in ONTAP:

1. Erstellen Sie ein Volume zur Lastverteilung der SVM Root-Volumes der Infrastruktur auf jedem Node.

   ```
   volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
   aggr1_nodeA –size 1GB –type DP
   volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
   aggr1_nodeB –size 1GB –type DP
   ```

2. Erstellen Sie einen Job-Zeitplan, um die Spiegelbeziehungen des Root-Volumes alle 15 Minuten zu aktualisieren.

   ```
   job schedule interval create -name 15min -minutes 15
   ```

3. Erstellen Sie die Spiegelungsbeziehungen.

   ```
   snapmirror create -source-path Infra-SVM:rootvol -destination-path
   Infra-SVM:rootvol_m01 -type LS -schedule 15min
   snapmirror create -source-path Infra-SVM:rootvol -destination-path
   Infra-SVM:rootvol_m02 -type LS -schedule 15min
   ```

4. Initialisieren Sie die Spiegelbeziehung und überprüfen Sie, ob sie erstellt wurde.

   ```
   snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
   snapmirror show
   ```

Konfigurieren Sie HTTPS-Zugriff in ONTAP

Gehen Sie wie folgt vor, um den sicheren Zugriff auf den Storage Controller zu konfigurieren:

1. Erhöhen Sie die Berechtigungsebene, um auf die Zertifikatbefehle zuzugreifen.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. In der Regel ist bereits ein selbstsigniertes Zertifikat vorhanden. Überprüfen Sie das Zertifikat, indem Sie den folgenden Befehl ausführen:

```
security certificate show
```

3. Bei jeder angezeigten SVM sollte der allgemeine Zertifikatname mit dem DNS-FQDN der SVM übereinstimmen. Die vier Standardzertifikate sollten gelöscht und durch selbstsignierte Zertifikate oder Zertifikate einer Zertifizierungsstelle ersetzt werden.

> ⓘ Das Löschen abgelaufener Zertifikate vor dem Erstellen von Zertifikaten ist eine bewährte Vorgehensweise. Führen Sie die aus `security certificate delete` Befehl zum Löschen abgelaufener Zertifikate. Verwenden Sie im folgenden Befehl DIE REGISTERKARTEN-Vervollständigung, um jedes Standardzertifikat auszuwählen und zu löschen.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Um selbstsignierte Zertifikate zu generieren und zu installieren, führen Sie die folgenden Befehle als einmalige Befehle aus. Ein Serverzertifikat für die Infrastruktur-SVM und die Cluster-SVM generieren. Verwenden Sie wieder die REGISTERKARTEN-Vervollständigung, um Sie beim Ausfüllen dieser Befehle zu unterstützen.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Um die Werte für die im folgenden Schritt erforderlichen Parameter zu erhalten, führen Sie den Befehl Security Certificate show aus.
6. Aktivieren Sie jedes Zertifikat, das gerade mit erstellt wurde `-server-enabled true` Und `-client-enabled false` Parameter. Verwenden Sie erneut DIE REGISTERKARTEN-Vervollständigung.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Konfigurieren und aktivieren Sie den SSL- und HTTPS-Zugriff und deaktivieren Sie den HTTP-Zugriff.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

Es ist normal, dass einige dieser Befehle eine Fehlermeldung ausgeben, die angibt, dass der Eintrag nicht vorhanden ist.

8. Kehren Sie zur Berechtigungsebene des Administrators zurück und erstellen Sie das Setup, damit die SVM vom Web verfügbar ist.

```
set –privilege admin
vserver services web modify –name spi –vserver * -enabled true
```

Erstellen Sie in ONTAP ein NetApp FlexVol Volume

Um ein NetApp FlexVol® Volume zu erstellen, geben Sie den Namen, die Größe und das Aggregat ein, auf dem es vorhanden ist. Erstellung von zwei VMware Datastore Volumes und einem Server Boot Volume

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Erstellen Sie LUNs in ONTAP

Führen Sie die folgenden Befehle aus, um zwei Boot-LUNs zu erstellen:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Beim Hinzufügen eines zusätzlichen Cisco UCS C-Series Servers müssen Sie eine zusätzliche Boot-LUN erstellen.

Erstellen von iSCSI LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Speicherknoten A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Speicherknoten A iSCSI-LIF01A-Netzwerkmaske	<<var_nodeA_iscsi_lif01a_Mask>>
Speicherknoten A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Speicherknoten Eine iSCSI-LIF01B-Netzwerkmaske	<<var_nodeA_iscsi_lif01b_Mask>>
Storage-Node B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Speicherknoten B iSCSI-LIF01A-Netzwerkmaske	<<var_nodeB_iscsi_lif01a_Mask>>
Storage Node B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
Speicherknoten B iSCSI-LIF01B-Netzwerkmaske	<<var_nodeB_iscsi_lif01b_Mask>>

Erstellen Sie vier iSCSI LIFs, zwei pro Node.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

Erstellen von NFS LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Storage-Node A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Storage Node A NFS LIF 01-Netzwerkmaske	<<var_nodeA_nfs_lif_01_maska>>
Storage-Node B NFS LIF 02-IP	<<var_nodeB_nfs_lif_02_ip>>
Storage Node B NFS LIF 02 Netzwerkmaske	<<var_nodeB_nfs_lif_02_maska>>

Erstellen Sie ein NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Hinzufügen eines Infrastruktur-SVM-Administrators

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Hinzufügen eines SVM-Administrators erforderlich sind.

Details	Detailwert
Vsmgmt-IP	<<var_svm_mgmt_ip>>
Vsmgmt-Netzwerkmaske	<<var_svm_mgmt_maska>>
Vsmgmt Standard-Gateway	<<var_svm_mgmt_Gateway>>

So fügen Sie dem Managementnetzwerk den SVM-Administrator und die logische SVM-Administrationsoberfläche der Infrastruktur hinzu:

1. Führen Sie den folgenden Befehl aus:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> Die SVM-Management-IP sollte sich hier im selben Subnetz wie die Storage-Cluster-Management-IP befinden.

2. Erstellen Sie eine Standardroute, damit die SVM-Managementoberfläche die Außenwelt erreichen kann.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Legen Sie ein Passwort für den SVM vsadmin-Benutzer fest und entsperren Sie den Benutzer.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Weiter: Implementierung von Rack-Servern der Cisco UCS C-Serie"

Bereitstellung von Rack-Server der Cisco UCS C-Serie

Dieser Abschnitt enthält ein detailliertes Verfahren zur Konfiguration eines Standalone-Rack-Servers der Cisco UCS C-Serie zur Verwendung in der FlexPod Express-Konfiguration.

Führen Sie das anfängliche Standalone-Server-Setup für den Cisco UCS C-Series für CIMC durch

Führen Sie diese Schritte für die Ersteinrichtung der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie durch.

In der folgenden Tabelle sind die Informationen aufgeführt, die für die Konfiguration von CIMC für jeden Standalone-Server der Cisco UCS C-Serie erforderlich sind.

Details	Detailwert
CIMC-IP-Adresse	<<cimc_ip>>
CIMC-Subnetzmaske	\<<cimc_Netzmaske
CIMC-Standard-Gateway	<<cimc_Gateway>>

Die CIMC-Version, die in dieser Validierung verwendet wird, ist CIMC 4.0.(4).

Alle Server

1. Schließen Sie den Cisco Keyboard-, Video- und Mausdongle (KVM) (im Lieferumfang des Servers enthalten) an den KVM-Port an der Vorderseite des Servers an. Schließen Sie einen VGA-Monitor und eine USB-Tastatur an die entsprechenden KVM-Dongle-Ports an.

   Schalten Sie den Server ein, und drücken Sie F8, wenn Sie dazu aufgefordert werden, die CIMC-Konfiguration einzugeben.

2. Legen Sie im CIMC-Konfigurationsprogramm die folgenden Optionen fest:
   a. NIC-Modus (Network Interface Card):

      Dediziert `[X]`

   b. IP (Basis):

      IPV4: `[X]`

      DHCP aktiviert: `[ ]`

      CIMC-IP: `<<cimc_ip>>`

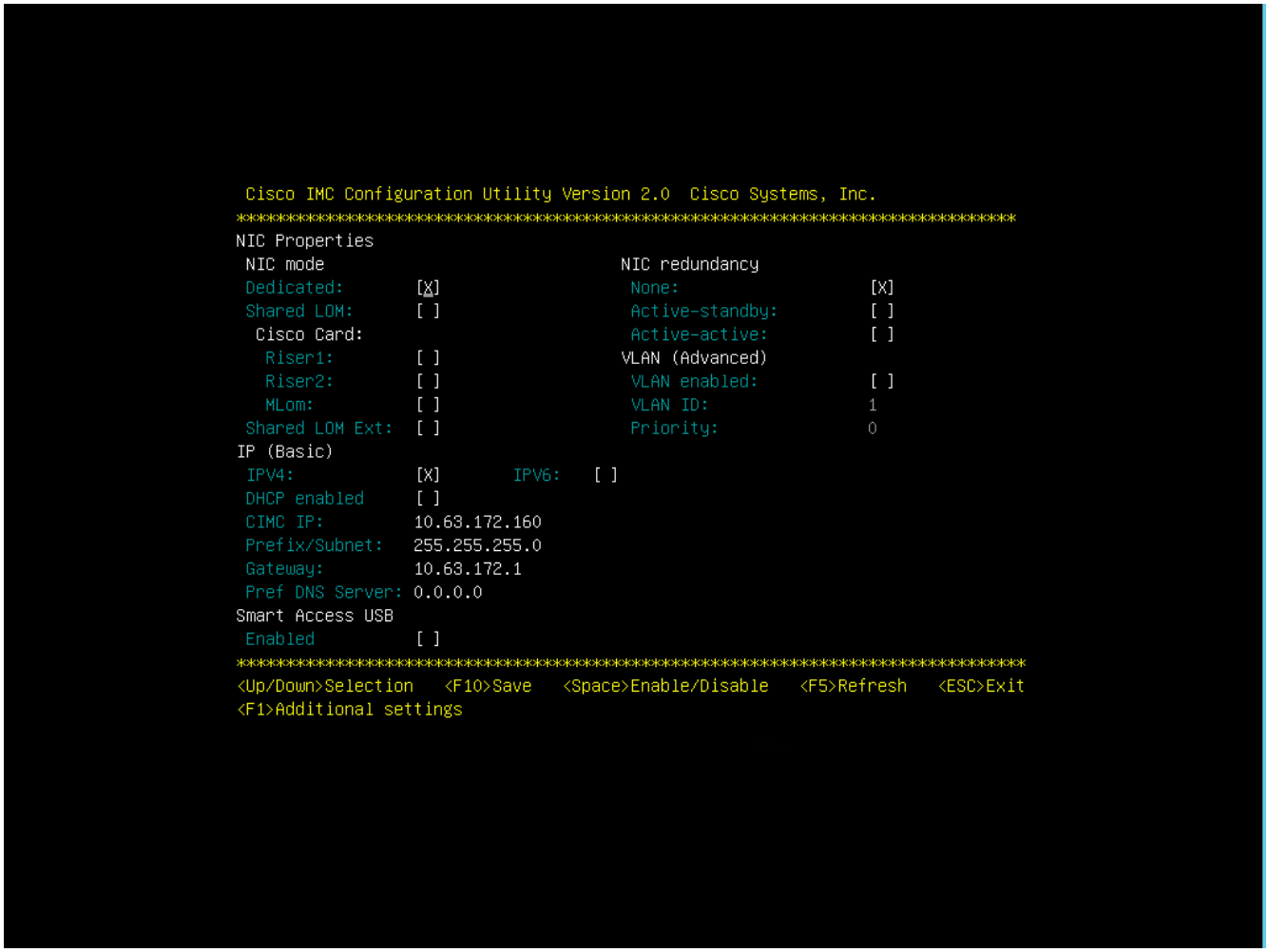
      Präfix/Subnetz: `<<cimc_netmask>>`

      Gateway: `<<cimc_gateway>>`

   c. VLAN (erweitert): Lassen Sie das Kontrollkästchen deaktiviert, um VLAN-Tagging zu deaktivieren.

      NIC-Redundanz

      Keine: `[X]`



3. Drücken Sie F1, um weitere Einstellungen anzuzeigen:
   a. Allgemeine Eigenschaften:

      Host-Name: `<<esxi_host_name>>`

      Dynamisches DNS: `[ ]`

      Werkseinstellungen: Löschen.

   b. Standardbenutzer (Basic):

      Standardpasswort: `<<admin_password>>`

      Kennwort erneut eingeben: `<<admin_password>>`

      Port-Eigenschaften: Standardwerte verwenden.

   Portprofile: Lassen Sie das Löschen.
4. Drücken Sie F10, um die Konfiguration der CIMC-Schnittstelle zu speichern.
5. Drücken Sie nach dem Speichern der Konfiguration Esc, um den Vorgang zu beenden.

Konfigurieren Sie den iSCSI-Start von Cisco UCS C-Series Servern

In dieser FlexPod-Express-Konfiguration wird der VIC1457 für das iSCSI-Booten verwendet.

In der folgenden Tabelle werden die Informationen aufgeführt, die für die Konfiguration des iSCSI-Startens erforderlich sind.

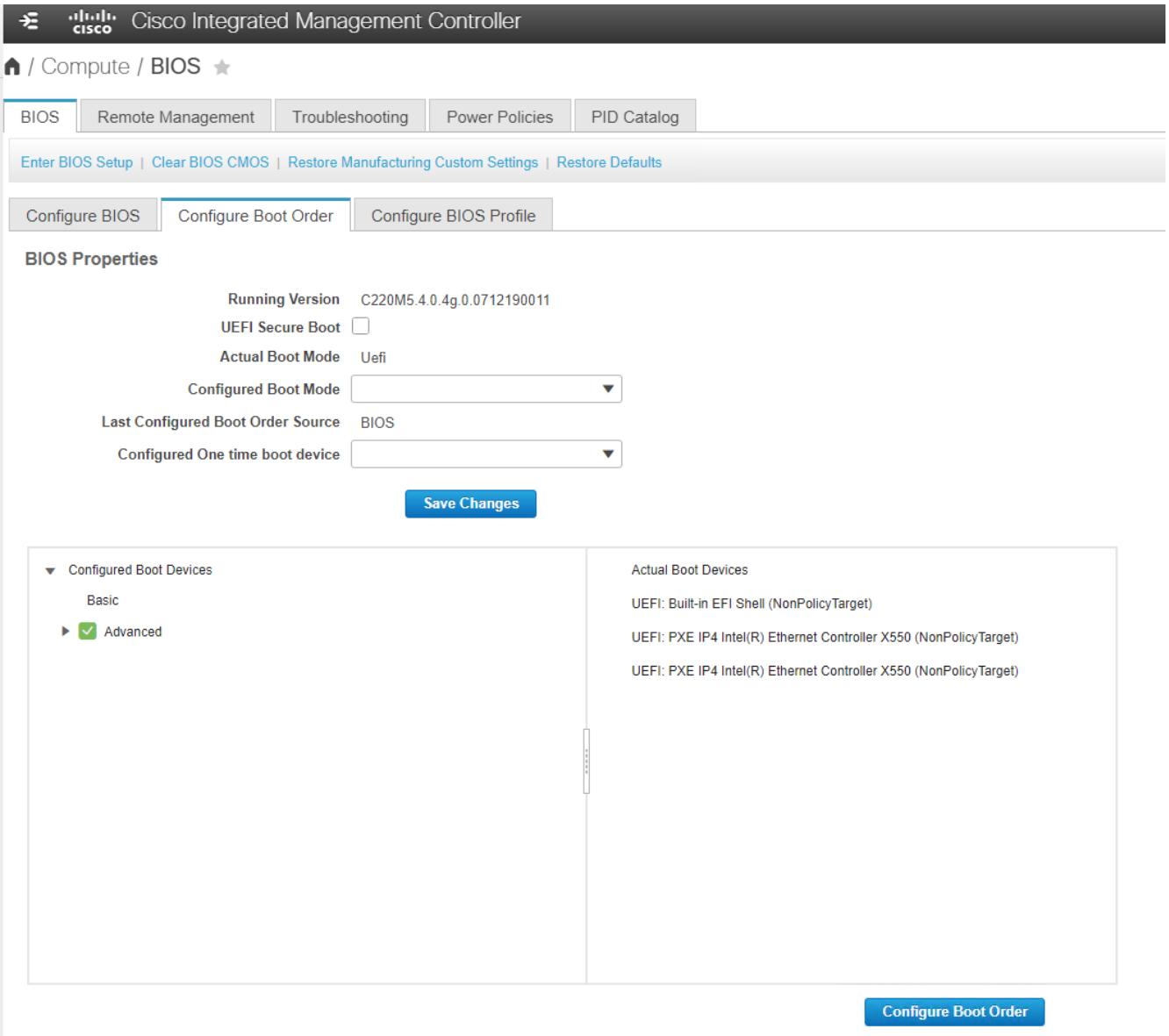
Eine kursiv formatierte Schriftart zeigt Variablen an, die für jeden ESXi-Host eindeutig sind.

Details	Detailwert
ESXi Host-Initiator Ein Name	<<var_ucs_Initiator_Name_A>>
ESXi Host, iSCSI A IP	<<var_esxi_Host_iscsiA_ip>>
ESXi-Host, iSCSI-A-Netzwerkmaske	<<var_esxi_Host_iscsiA_Maska>>
ESXi Host iSCSI Ein Standard-Gateway	\<<var_esxi_Host_iscsiA_Gateway>
ESXi Host-Initiator B-Name	\<<var_ucs_Initiator_Name_B>
ESXi-Host, iSCSI-B-IP	<<var_esxi_Host_iscsiB_ip>>
ESXi-Host-iSCSI-B-Netzwerkmaske	<<var_esxi_Host_iscsiB_Maska>>
ESXi Host iSCSI-B-Gateway	\<<var_esxi_Host_iscsiB_Gateway>
IP-Adresse iscsi_lif01a	<<var_iscsi_lif01a>>
IP-Adresse iscsi_lif02a	<<var_iscsi_lif02a>>
IP-Adresse iscsi_lif01b	<<var_iscsi_lif01b>>
IP-Adresse iscsi_lif02b	\<<var_iscsi_lif02b>
Infra_SVM IQN	<<var_SVM_IQN>>

Konfiguration der Startreihenfolge

Gehen Sie wie folgt vor, um die Konfiguration der Startreihenfolge festzulegen:

1. Klicken Sie im Browser-Fenster der CIMC-Schnittstelle auf die Registerkarte Compute, und wählen Sie BIOS aus.
2. Klicken Sie auf Startreihenfolge konfigurieren, und klicken Sie dann auf OK.



3. Konfigurieren Sie die folgenden Geräte, indem Sie auf das Gerät unter Startgerät hinzufügen klicken und zur Registerkarte Erweitert wechseln:

   a. Virtuellen Datenträger Hinzufügen:

      NAME: KVM-CD-DVD

      UNTERTYP: KVM GEMAPPTEN DVD

      Status: Aktiviert

      Bestellung: 1

   b. ISCSI-Boot hinzufügen:

      Name: ISCSI-A

      Status: Aktiviert

      Bestellung: 2

Schlitz: MLOM

Anschluss: 1

c. Klicken Sie auf iSCSI-Boot hinzufügen:

Name: ISCSI-B

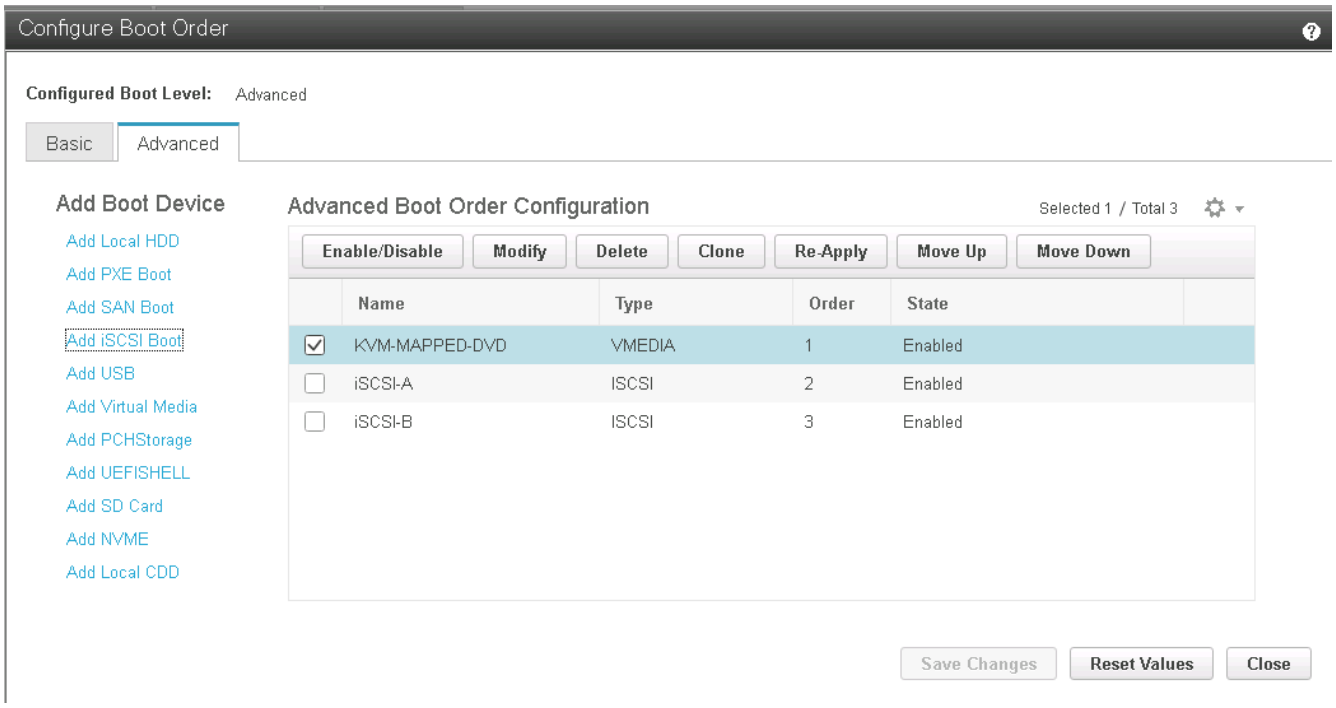
Status: Aktiviert

Bestellung: 3

Schlitz: MLOM

Anschluss: 3

4. Klicken Sie Auf Gerät Hinzufügen.
5. Klicken Sie auf Änderungen speichern und dann auf Schließen.

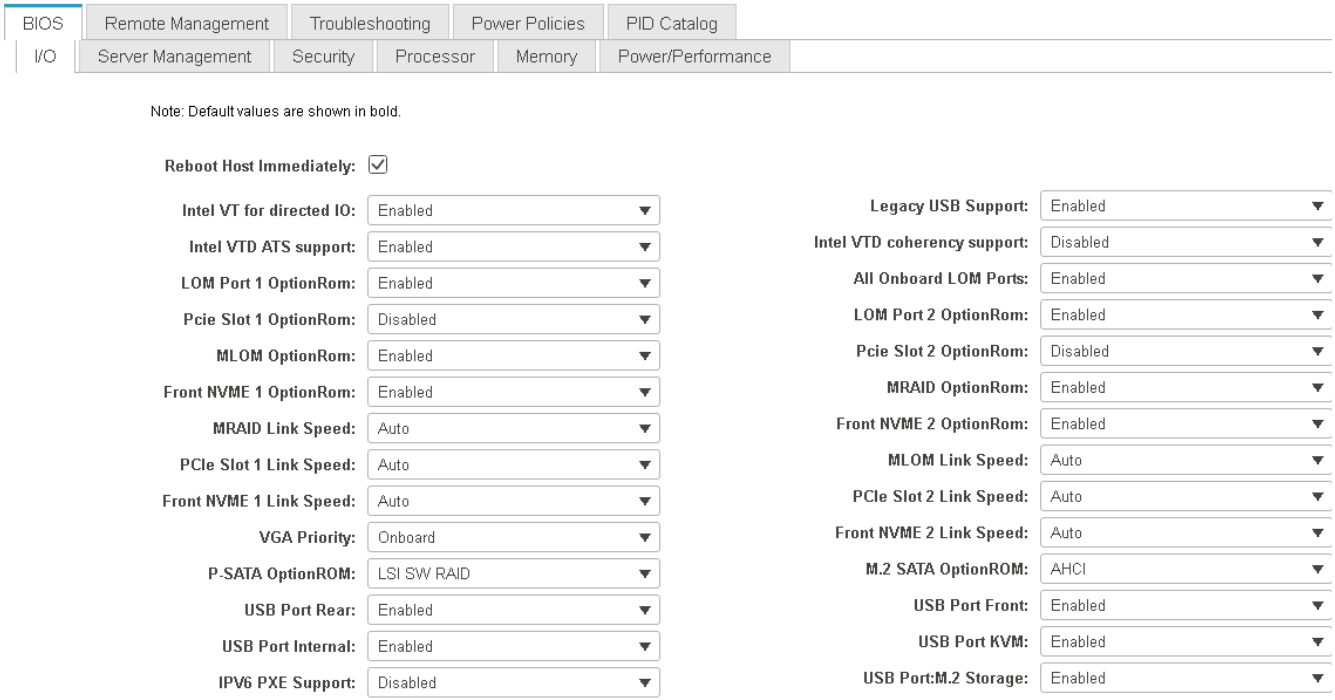


6. Starten Sie den Server neu, um mit Ihrer neuen Startreihenfolge zu starten.

Deaktivieren des RAID-Controllers (falls vorhanden)

Führen Sie die folgenden Schritte aus, wenn Ihr C-Series-Server einen RAID-Controller enthält. Beim Booten der SAN-Konfiguration ist kein RAID-Controller erforderlich. Optional können Sie den RAID-Controller auch physisch vom Server entfernen.

1. Klicken Sie unter der Registerkarte „Computing“ im linken Navigationsbereich in CIMC auf BIOS.
2. Wählen Sie BIOS konfigurieren.
3. Blättern Sie nach unten zu PCIe Slot:HBA Option ROM.
4. Wenn der Wert nicht bereits deaktiviert ist, setzen Sie ihn auf deaktiviert.

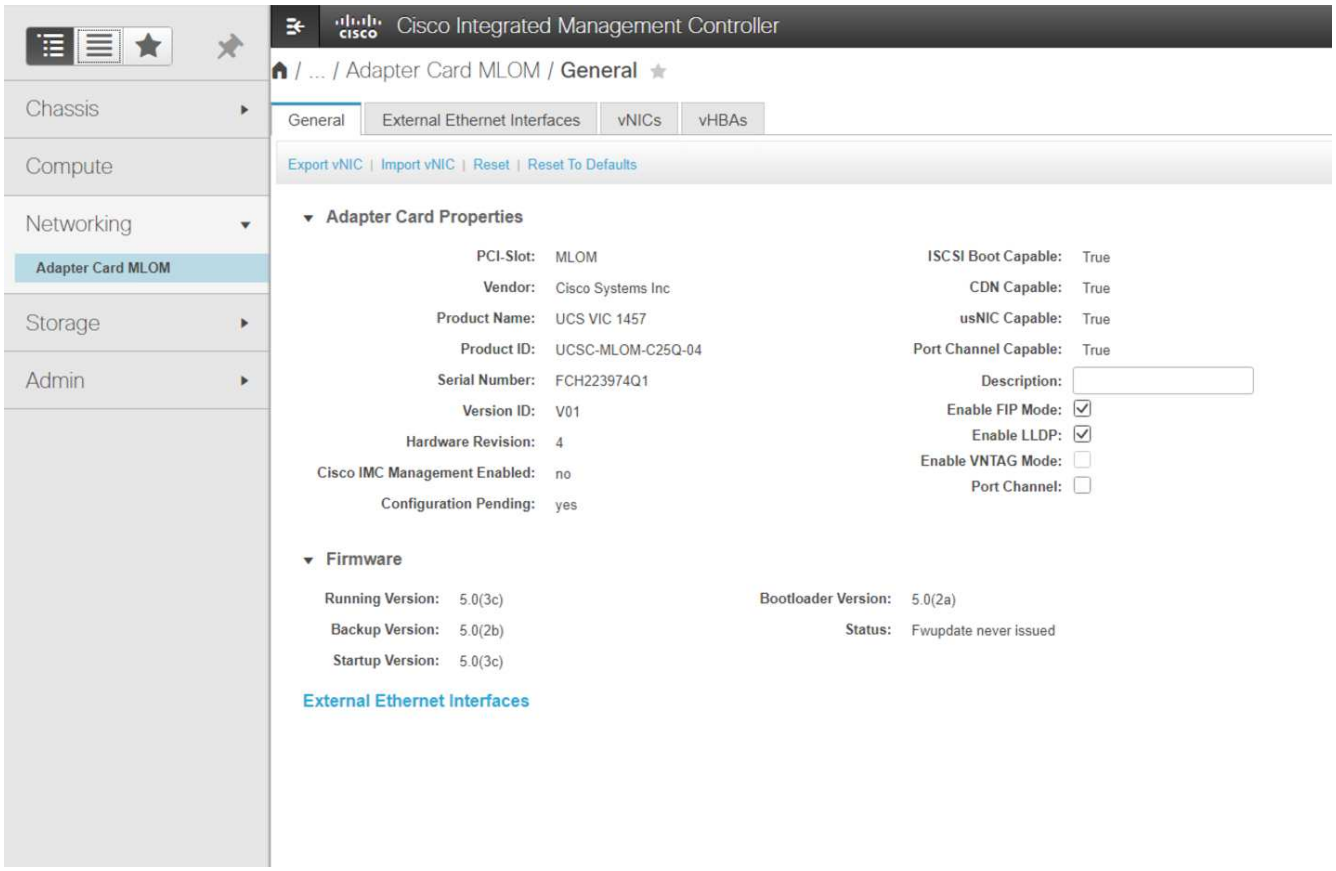


Konfigurieren Sie Cisco VIC1457 für iSCSI-Boot

Die folgenden Konfigurationsschritte gelten für den Cisco VIC 1457 für iSCSI Boot.

Das Standard-Port-Channeling zwischen den Ports 0, 1, 2 und 3 muss deaktiviert werden, bevor die vier einzelnen Ports konfiguriert werden können. Wenn das Port-Channeling nicht ausgeschaltet wird, werden nur zwei Ports für den VIC 1457 angezeigt. Führen Sie die folgenden Schritte durch, um den Port-Kanal auf dem CIMC zu aktivieren:

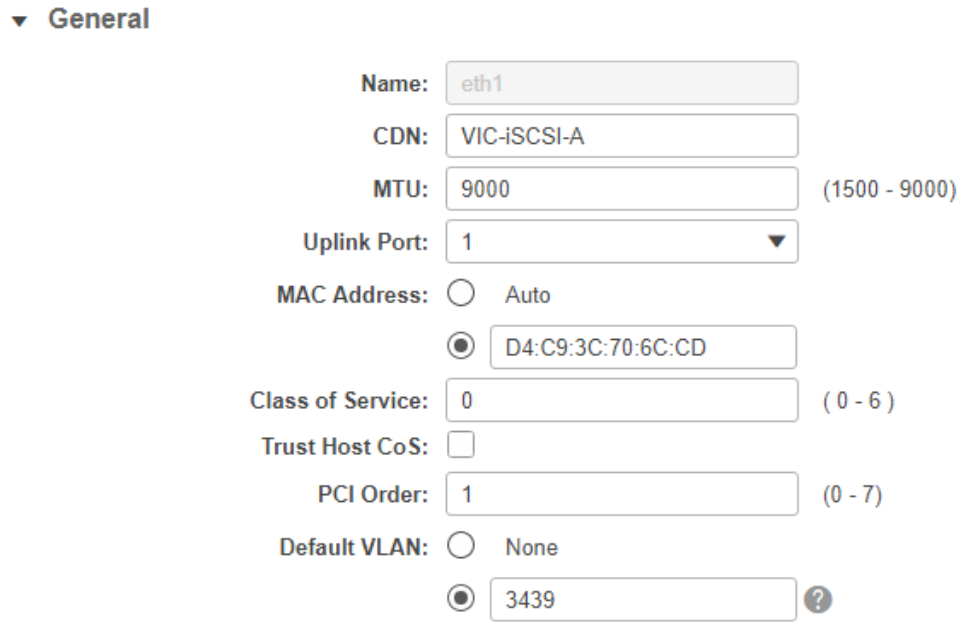
1. Klicken Sie auf der Registerkarte Netzwerk auf die Adapterkarte MLOM.
2. Deaktivieren Sie auf der Registerkarte Allgemein den Port-Kanal.
3. Speichern Sie die Änderungen, und starten Sie den CIMC neu.



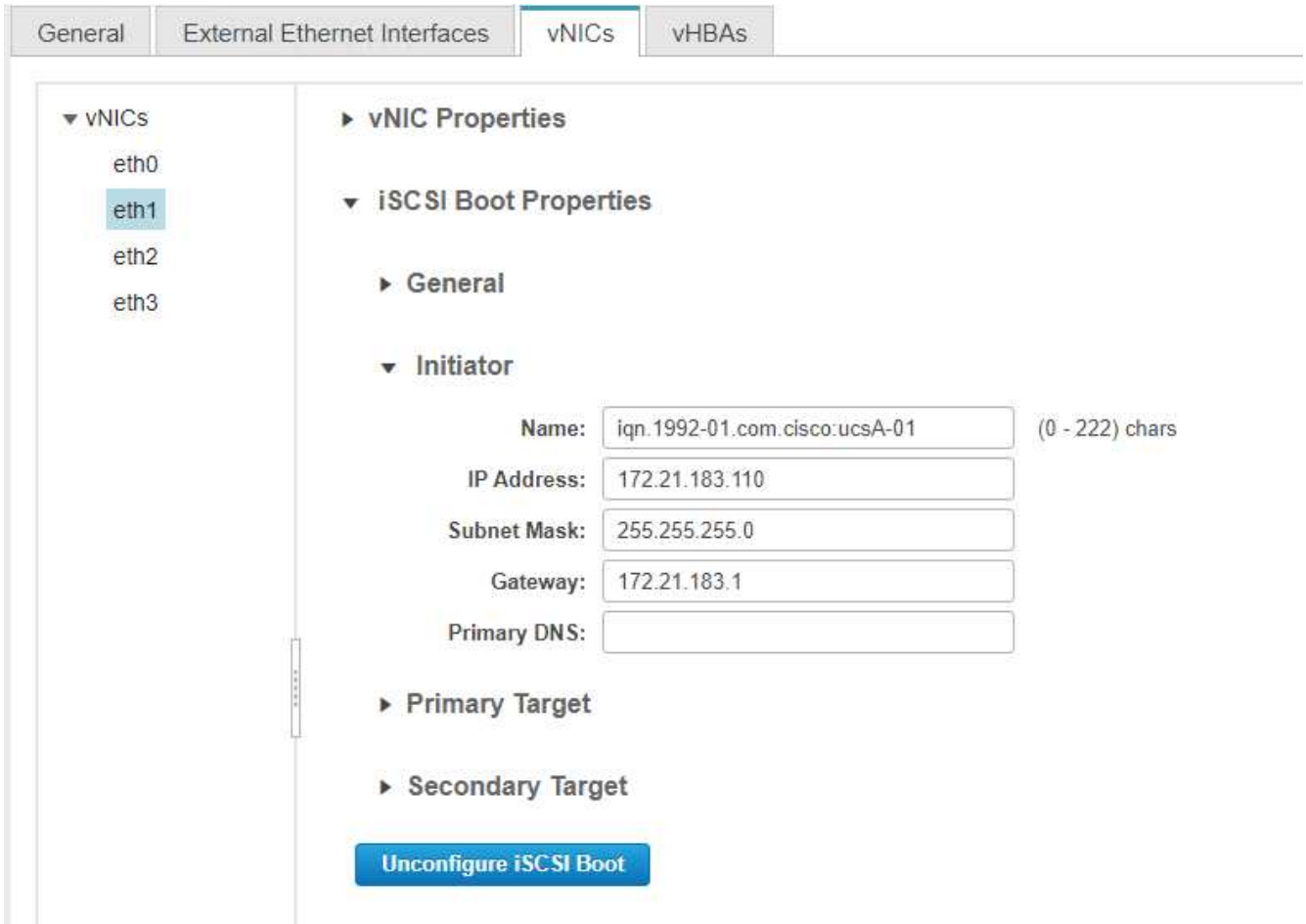
Erstellen von iSCSI-vNICs

Gehen Sie wie folgt vor, um iSCSI-vNICs zu erstellen:

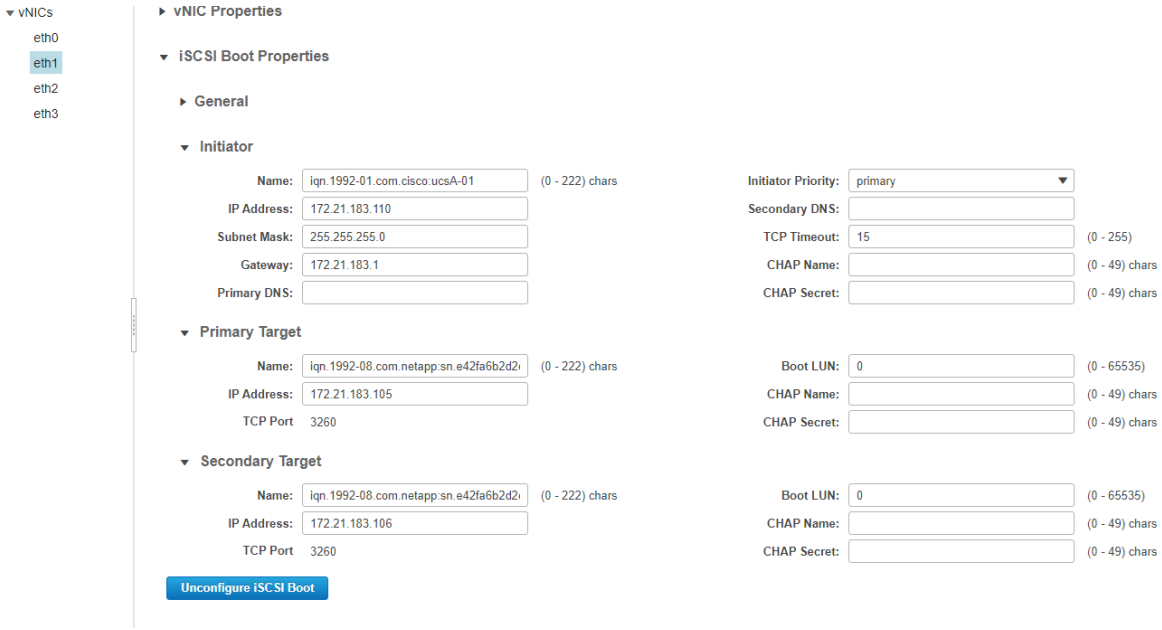
1. Klicken Sie auf der Registerkarte Netzwerk auf Adapterkarte MLOM.
2. Klicken Sie auf vNIC hinzufügen, um eine vNIC zu erstellen.
3. Geben Sie im Abschnitt vNIC hinzufügen die folgenden Einstellungen ein:
   - Name: Eth1
   - CDN-Name: ISCSI-vNIC-A
   - MTU: 9000
   - Standard-VLAN: `<<var_iscsi_vlan_a>>`
   - VLAN-Modus: TRUNK
   - PXE-Start aktivieren: Prüfen
4. Klicken Sie auf vNIC hinzufügen und dann auf OK.
5. Wiederholen Sie den Vorgang, um einen zweiten vNIC hinzuzufügen:
   - Benennen Sie die vNIC eth3.
   - CDN-Name: ISCSI-vNIC-B
   - Eingabe `<<var_iscsi_vlan_b>>` Als VLAN.
   - Stellen Sie den Uplink-Port auf 3 ein.



6. Wählen Sie links die vNIC eth1 aus.



7. Geben Sie unter iSCSI Boot Properties die Initiator-Details ein:
   - Name: `<<var_ucsa_initiator_name_a>>`
   - IP-Adresse: `<<var_esxi_hostA_iscsiA_ip>>`
   - Subnetzmaske: `<<var_esxi_hostA_iscsiA_mask>>`
   - Gateway: `<<var_esxi_hostA_iscsiA_gateway>>`



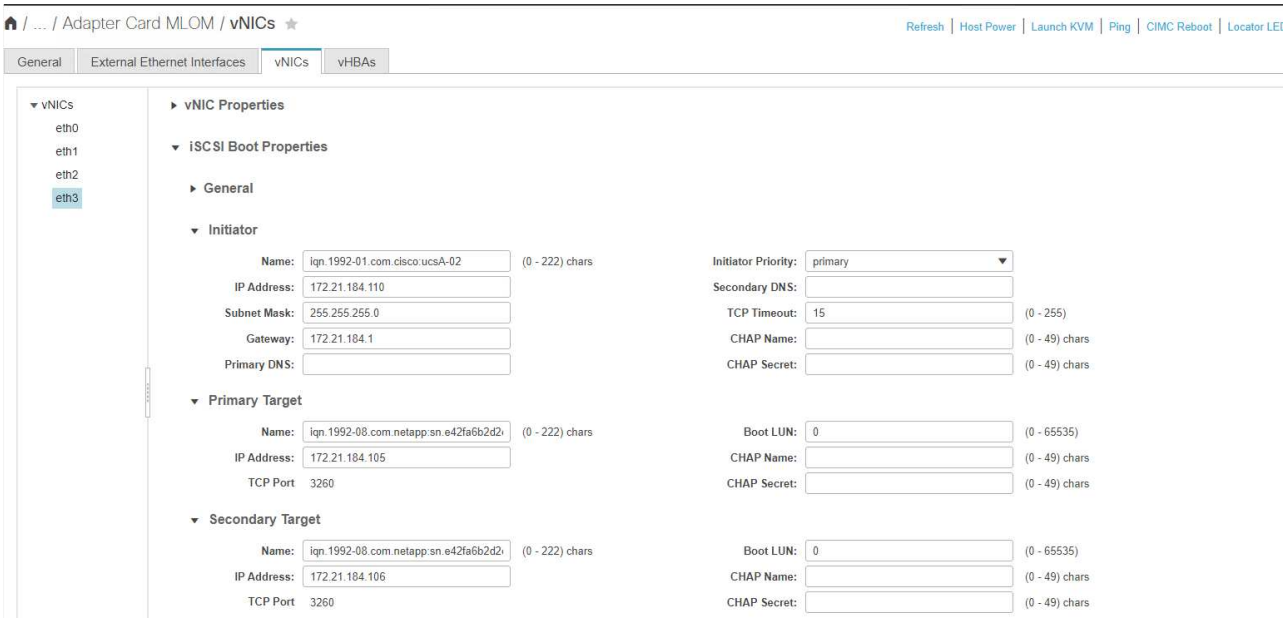
8. Geben Sie die Details des primären Ziels ein:
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von iscsi_lif01a
   - Boot-LUN: 0
9. Geben Sie die Details des sekundären Ziels ein:
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von iscsi_lif02a
   - Boot-LUN:0

> Sie können die Speicher-IQN-Nummer abrufen, indem Sie den ausführen `vserver iscsi show` Befehl.

> Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt. Darüber hinaus müssen die IQN-Namen für Initiatoren für jeden Server und für die iSCSI-vNIC eindeutig sein.

10. Klicken Sie Auf Änderungen Speichern.
11. Wählen Sie die vNIC eth3 aus, und klicken Sie auf die iSCSI-Boot-Schaltfläche oben im Abschnitt Host-Ethernet-Schnittstellen.
12. Wiederholen Sie den Vorgang, um eth3 zu konfigurieren.

13. Geben Sie die Initiator-Details ein:
    - Name: `<<var_ucsa_initiator_name_b>>`
    - IP-Adresse: `<<var_esxi_hostb_iscsib_ip>>`
    - Subnetzmaske: `<<var_esxi_hostb_iscsib_mask>>`
    - Gateway: `<<var_esxi_hostb_iscsib_gateway>>`



14. Geben Sie die Details des primären Ziels ein:
    - Name: IQN-Nummer der Infrastruktur-SVM
    - IP-Adresse: IP-Adresse von iscsi_lif01b
    - Boot-LUN: 0
15. Geben Sie die Details des sekundären Ziels ein:
    - Name: IQN-Nummer der Infrastruktur-SVM
    - IP-Adresse: IP-Adresse von iscsi_lif02b
    - Boot-LUN: 0

> Sie können die Speicher-IQN-Nummer mit dem abrufen `vserver iscsi show` Befehl.

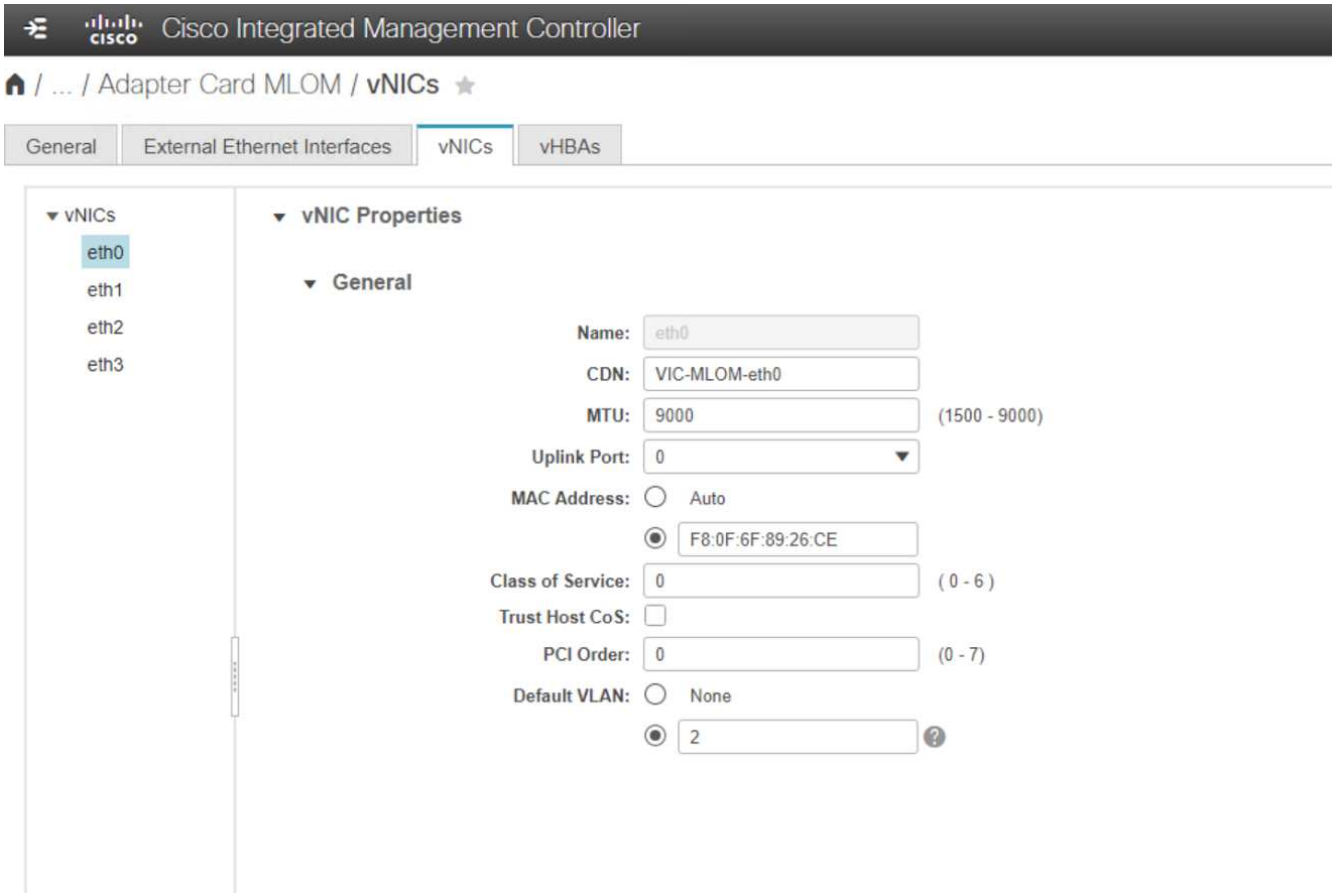
> Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.

16. Klicken Sie Auf Änderungen Speichern.
17. Wiederholen Sie diesen Vorgang, um iSCSI-Boot für Cisco UCS-Server B zu konfigurieren

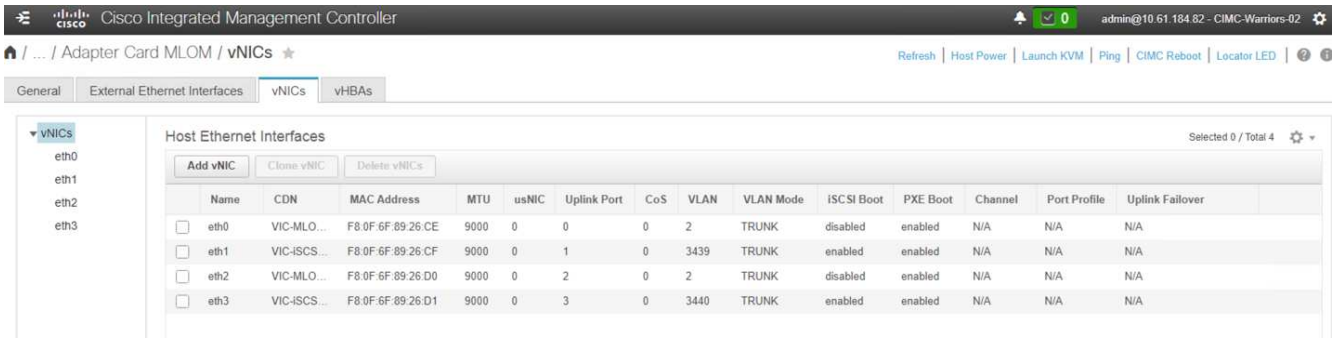
Konfigurieren Sie vNICs für ESXi

Gehen Sie wie folgt vor, um vNICs für ESXi zu konfigurieren:

1. Klicken Sie im CIMC-Schnittstellenbrowser-Fenster auf Inventar und anschließend im rechten Fensterbereich auf Cisco VIC-Adapter.
2. Wählen Sie unter Netzwerk > Adapterkarte MLOM die Registerkarte vNICs aus, und wählen Sie anschließend die darunter liegende vNICs aus.
3. Wählen Sie eth0 aus, und klicken Sie auf Eigenschaften.
4. Setzen Sie die MTU auf 9000. Klicken Sie Auf Änderungen Speichern.
5. Setzen Sie das VLAN auf natives VLAN 2.



6. Wiederholen Sie die Schritte 3 und 4 für eth1. Überprüfen Sie, ob der Uplink-Port für eth1 auf 1 gesetzt ist.



Dieses Verfahren muss für jeden ersten Cisco UCS Server-Knoten und jeden zusätzlichen Cisco UCS Server-Node, der der Umgebung hinzugefügt wurde, wiederholt werden.

"Weiter: NetApp Verfahren zur AFF Storage-Implementierung (Teil 2)."

NetApp AFF Storage-Implementierung (Teil 2)

ONTAP-SAN-Boot-Storage einrichten

Erstellen von iSCSI-Initiatorgruppen

Für diesen Schritt benötigen Sie die iSCSI-Initiator-IQNs aus der Serverkonfiguration.

Führen Sie zum Erstellen von Initiatorgruppen die folgenden Befehle über die SSH-Verbindung des Cluster-Management-Node aus. Um die drei in diesem Schritt erstellten Initiatorgruppen anzuzeigen, führen Sie den aus `igroup show` Befehl.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Dieser Schritt muss abgeschlossen sein, wenn zusätzliche Cisco UCS C-Series Server hinzugefügt werden.

Zuordnen von Boot-LUNs zu Initiatorgruppen

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

Dieser Schritt muss abgeschlossen sein, wenn zusätzliche Cisco UCS C-Series Server hinzugefügt werden.

"Weiter: VMware vSphere 6.7U2 Bereitstellungsverfahren."

Implementierungsverfahren für VMware vSphere 6.7U2

Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware ESXi 6.7U2 in einer FlexPod Express-Konfiguration. Die folgenden Implementierungsverfahren werden so angepasst, dass sie die in vorherigen Abschnitten beschriebenen Umgebungsvariablen enthalten.

Für die Installation von VMware ESXi in einer solchen Umgebung sind mehrere Methoden vorhanden. Dieses Verfahren verwendet die virtuelle KVM-Konsole und die virtuellen Medienfunktionen der CIMC-Schnittstelle für Server der Cisco UCS C-Serie, um Remote-Installationsmedien jedem einzelnen Server zuzuordnen.

Diese Prozedur muss für Cisco UCS Server A und Cisco UCS Server B abgeschlossen sein

Für alle zusätzlichen Nodes, die dem Cluster hinzugefügt werden, muss dieser Vorgang abgeschlossen sein.

Melden Sie sich bei der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie an

Die folgenden Schritte beschreiben die Methode zur Anmeldung an der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie. Sie müssen sich bei der CIMC-Schnittstelle anmelden, um die virtuelle KVM auszuführen, die es dem Administrator ermöglicht, die Installation des Betriebssystems über Remote-Medien zu starten.

Alle Hosts

1. Navigieren Sie zu einem Webbrowser, und geben Sie die IP-Adresse für die CIMC-Schnittstelle für die Cisco UCS C-Serie ein. In diesem Schritt wird die CIMC GUI-Anwendung gestartet.
2. Melden Sie sich bei der CIMC-UI mit dem Admin-Benutzernamen und den Anmeldedaten an.
3. Wählen Sie im Hauptmenü die Registerkarte Server aus.
4. Klicken Sie auf KVM-Konsole starten.

5. Wählen Sie in der virtuellen KVM-Konsole die Registerkarte Virtueller Datenträger aus.
6. Wählen Sie Karte CD/DVD.

Sie müssen eventuell zuerst auf virtuelle Geräte aktivieren klicken. Wählen Sie die Option Diese Sitzung akzeptieren, wenn Sie dazu aufgefordert werden.

7. Öffnen Sie die ISO-Image-Datei des VMware ESXi 6.7U2-Installationsprogramms, und klicken Sie auf Öffnen. Klicken Sie Auf Kartengerät.
8. Wählen Sie das Menü Power (aus) und dann Power Cycle System (Kaltstart). Klicken Sie Auf Ja.

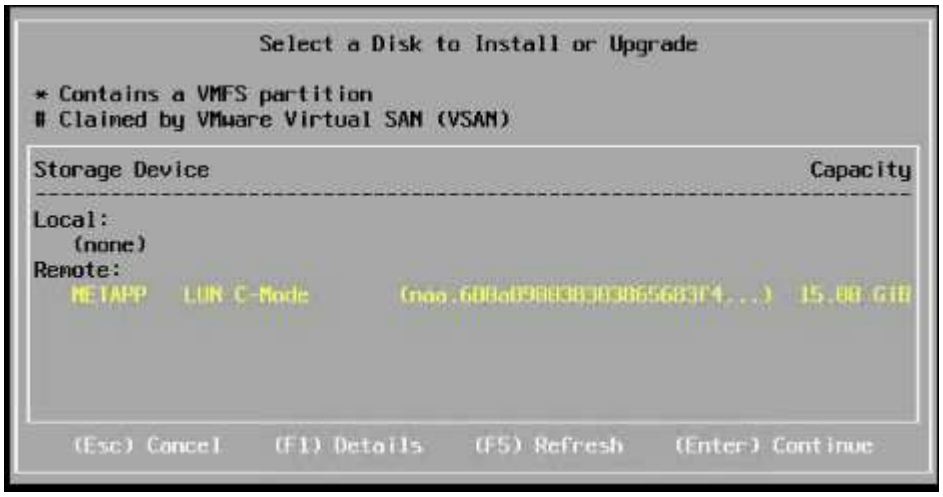
VMware ESXi installieren

In den folgenden Schritten wird die Installation von VMware ESXi auf jedem Host beschrieben.

Laden Sie DAS benutzerdefinierte ESXI 6.7U2 Cisco Image herunter

1. Navigieren Sie zum "Download-Seite für VMware vSphere" Für benutzerdefinierte ISOs.
2. Klicken Sie auf „Go to Downloads“ neben dem benutzerdefinierten Cisco Image für die ESXi 6.7U2-Installations-CD.
3. Laden Sie das benutzerdefinierte Cisco Image für die ESXi 6.7U2 Installations-CD (ISO) herunter.
4. Beim Systemstart erkennt die Maschine die VMware ESXi Installationsmedien.
5. Wählen Sie das VMware ESXi-Installationsprogramm aus dem angezeigten Menü aus. Das Installationsprogramm lädt, was mehrere Minuten dauern kann.

6. Drücken Sie nach dem Laden des Installers die Eingabetaste, um mit der Installation fortzufahren.
7. Nachdem Sie die Endbenutzer-Lizenzvereinbarung gelesen haben, akzeptieren Sie sie und fahren Sie mit der Installation fort, indem Sie auf F11 drücken.
8. Wählen Sie die NetApp LUN aus, die zuvor als Installationsfestplatte für ESXi eingerichtet wurde, und drücken Sie die Eingabetaste, um die Installation fortzusetzen.



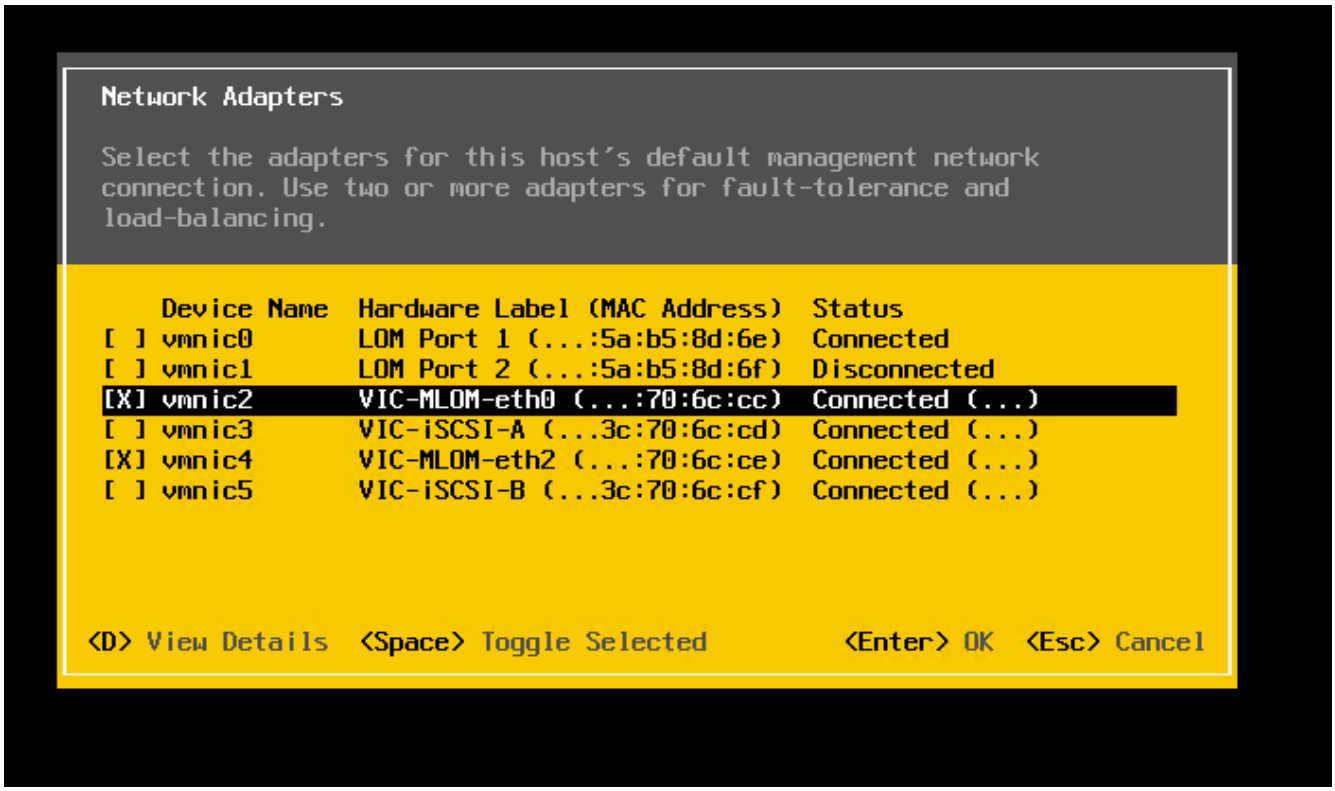
9. Wählen Sie das entsprechende Tastaturlayout aus, und drücken Sie die Eingabetaste.
10. Geben Sie das Root-Passwort ein und bestätigen Sie es, und drücken Sie die Eingabetaste.
11. Der Installer warnt Sie, dass vorhandene Partitionen auf dem Volume entfernt werden. Fahren Sie mit der Installation fort, indem Sie auf F11 drücken. Der Server startet nach der Installation von ESXi neu.

Einrichten des VMware ESXi Host-Managementnetzwerkes

Bei den folgenden Schritten wird beschrieben, wie das Management-Netzwerk für jeden VMware ESXi Host hinzugefügt wird.

Alle Hosts

1. Geben Sie nach dem Neustart des Servers die Option zum Anpassen des Systems ein, indem Sie F2 drücken.
2. Melden Sie sich mit root als Anmeldenamen und dem Root-Passwort an, das zuvor während des Installationsprozesses eingegeben wurde.
3. Wählen Sie die Option Managementnetzwerk konfigurieren.
4. Wählen Sie Netzwerkadapter aus, und drücken Sie die Eingabetaste.
5. Wählen Sie die gewünschten Ports für vSwitch0 aus. Drücken Sie Die Eingabetaste.
6. Wählen Sie die Ports aus, die eth0 und eth1 im CIMC entsprechen.



7. Wählen Sie VLAN (optional) aus, und drücken Sie die Eingabetaste.
8. Geben Sie die VLAN-ID ein `<<mgmt_vlan_id>>`. Drücken Sie Die Eingabetaste.
9. Wählen Sie im Menü Managementnetzwerk konfigurieren die Option IPv4-Konfiguration aus, um die IP-Adresse der Managementoberfläche zu konfigurieren. Drücken Sie Die Eingabetaste.
10. Markieren Sie mit den Pfeiltasten die Option statische IPv4-Adresse festlegen, und wählen Sie diese Option mithilfe der Leertaste aus.
11. Geben Sie die IP-Adresse zum Verwalten des VMware ESXi-Hosts ein `<<esxi_host_mgmt_ip>>`.
12. Geben Sie die Subnetzmaske für den VMware ESXi-Host ein `<<esxi_host_mgmt_netmask>>`.
13. Geben Sie das Standard-Gateway für den VMware ESXi-Host ein `<<esxi_host_mgmt_gateway>>`.
14. Drücken Sie die Eingabetaste, um die Änderungen an der IP-Konfiguration zu akzeptieren.
15. Rufen Sie das IPv6-Konfigurationsmenü auf.
16. Deaktivieren Sie IPv6 über die Leertaste, indem Sie die Option IPv6 aktivieren (Neustart erforderlich) deaktivieren. Drücken Sie Die Eingabetaste.
17. Rufen Sie das Menü auf, um die DNS-Einstellungen zu konfigurieren.
18. Da die IP-Adresse manuell zugewiesen wird, müssen auch die DNS-Informationen manuell eingegeben werden.
19. Geben Sie die IP-Adresse des primären DNS-Servers ein `<<nameserver_ip>>`.
20. (Optional) Geben Sie die IP-Adresse des sekundären DNS-Servers ein.
21. Geben Sie den FQDN für den VMware ESXi-Hostnamen ein: `<<esxi_host_fqdn>>`.
22. Drücken Sie die Eingabetaste, um die Änderungen an der DNS-Konfiguration zu akzeptieren.
23. Beenden Sie das Untermenü Verwaltungsnetzwerk konfigurieren, indem Sie Esc drücken.
24. Drücken Sie Y, um die Änderungen zu bestätigen und den Server neu zu starten.

25. Wählen Sie Fehlerbehebungsoptionen aus, und aktivieren Sie dann ESXi Shell und SSH.

> Diese Fehlerbehebungsoptionen können nach der Validierung gemäß der Sicherheitsrichtlinien des Kunden deaktiviert werden.

26. Drücken Sie zweimal Esc, um zum Hauptbildschirm der Konsole zurückzukehren.
27. Klicken Sie im Dropdown-Menü CIMC-Makros > statische Makros > Alt-F oben auf dem Bildschirm auf Alt-F1.
28. Melden Sie sich mit den richtigen Anmeldedaten für den ESXi Host an.
29. Geben Sie an der Eingabeaufforderung die folgende Liste von esxcli-Befehlen nacheinander ein, um die Netzwerkverbindung zu ermöglichen.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

Konfigurieren Sie den ESXi-Host

Verwenden Sie die Informationen in der folgenden Tabelle, um jeden ESXi Host zu konfigurieren.

Details	Detailwert
ESXi Hostname	\<<esxi_Host_fqdn>
ESXi Host-Management-IP	\<<esxi_Host_Mgmt_ip>
ESXi Host-Managementmaske	<<esxi_Host_mgmt_Netzmaske>>
ESXi Host-Management-Gateway	\<<esxi_Host_mgmt_Gateway>
ESXi Host, NFS-IP	\<<esxi_Host_NFS_ip>
ESXi Host-NFS-Maske	<<esxi_Host_NFS_Netmask>>
ESXi Host-NFS-Gateway	\<<esxi_Host_NFS_Gateway>
ESXi Host vMotion IP	<<esxi_Host_vMotion_ip>>
ESXi Host vMotion Maske	<<esxi_Host_vMotion_Netzmaske>>
ESXi Host vMotion Gateway	\<<esxi_Host_vMotion_Gateway>
ESXi Host, iSCSI A IP	\<<esxi_Host_iSCSI-A_ip>
ESXi Host iSCSI-A-Maske	\<<esxi_Host_iSCSI-A_Netzmaske>
ISCSI-A-Gateway für ESXi Host	\<<esxi_Host_iSCSI-A_Gateway>
ESXi-Host, iSCSI-B-IP	\<<esxi_Host_iSCSI-B_ip>
ISCSI-B-Maske für ESXi Host	\<<esxi_Host_iSCSI-B_Netmask>
ESXi Host iSCSI-B-Gateway	\<<esxi_Host_SCSI-B_Gateway>

Melden Sie sich beim ESXi-Host an

So melden Sie sich beim ESXi-Host an:

1. Öffnen Sie die Management-IP-Adresse des Hosts in einem Webbrowser.
2. Melden Sie sich beim ESXi-Host mit dem Root-Konto und dem Passwort an, das Sie während des Installationsvorgangs angegeben haben.
3. Lesen Sie die Aussage zum VMware Customer Experience Improvement Program. Klicken Sie nach Auswahl der richtigen Antwort auf OK.

Konfigurieren Sie den iSCSI-Bootvorgang

Gehen Sie wie folgt vor, um iSCSI-Starts zu konfigurieren:

1. Wählen Sie links die Option Netzwerk.
2. Wählen Sie rechts die Registerkarte Virtuelle Switches aus.

3. Klicken Sie auf iScsiBootvSwitch.
4. Wählen Sie Einstellungen bearbeiten aus.
5. Ändern Sie die MTU in 9000, und klicken Sie auf Speichern.
6. Benennen Sie den iSCSIBootPG-Port in iSCSIBootPG-A um

> Für das Booten über iSCSI werden in dieser Konfiguration Vmnic3 und vmnic5 verwendet. Wenn Sie zusätzliche NICs in Ihrem ESXi Host haben, haben Sie möglicherweise unterschiedliche vmnic-Zahlen. Um zu überprüfen, welche NICs für das Booten von iSCSI verwendet werden, stimmen Sie die MAC-Adressen auf den iSCSI vNICs in CIMC den vmnics in ESXi ab.

7. Wählen Sie im mittleren Fensterbereich die Registerkarte VMkernel NICs aus.
8. Wählen Sie VMkernel NIC hinzufügen aus.
   a. Geben Sie einen neuen Portgruppennamen von iScsiBootPG-B an
   b. Wählen Sie iScsiBootvSwitch für den virtuellen Switch aus.
   c. Eingabe `<<iscsib_vlan_id>>` Für die VLAN-ID.

d. Ändern Sie die MTU in 9000.

e. IPv4-Einstellungen erweitern.

f. Wählen Sie Statische Konfiguration.

g. Eingabe `<<var_hosta_iscsib_ip>>` Für Adresse.

h. Eingabe `<<var_hosta_iscsib_mask>>` Für Subnetzmaske.

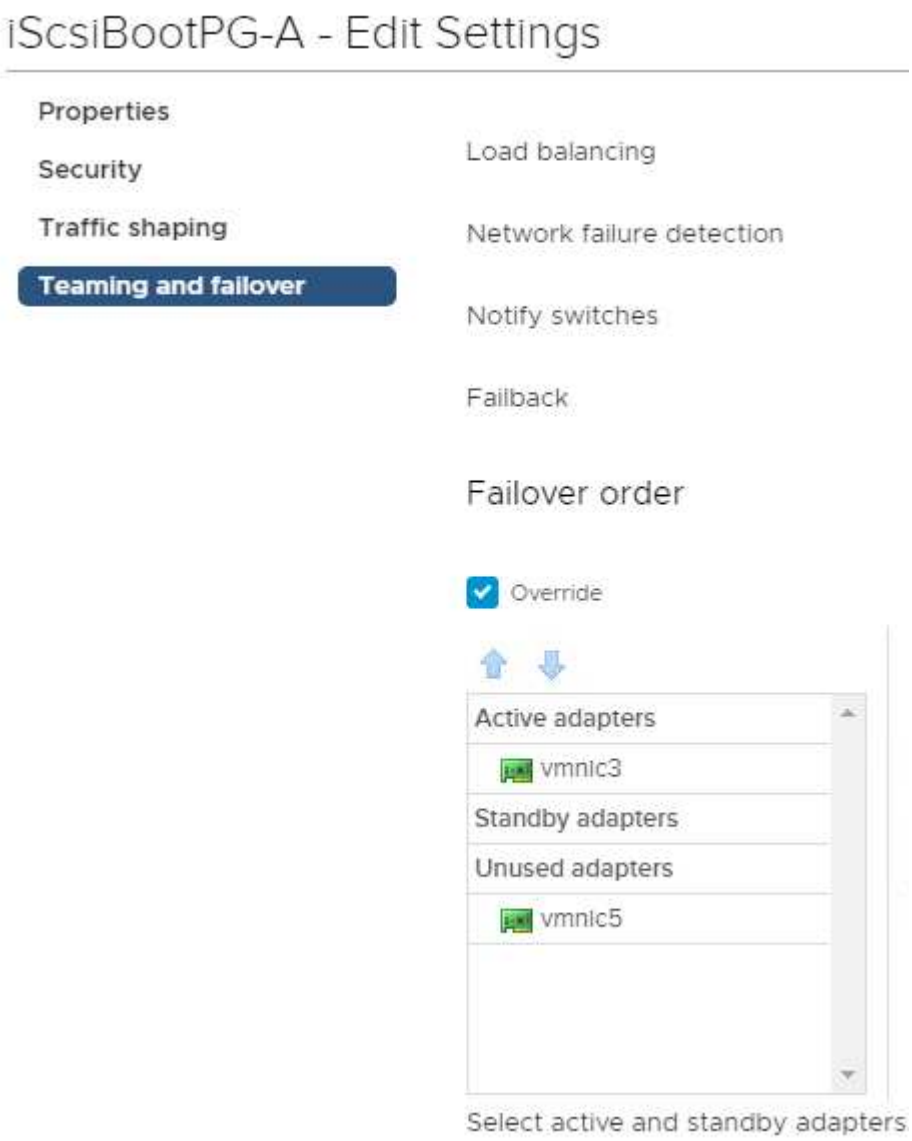
i. Klicken Sie auf Erstellen .

Stellen Sie die MTU auf iScsiBootPG-A auf 9000 ein

9. Führen Sie die folgenden Schritte aus, um das Failover festzulegen:

a. Klicken Sie auf Einstellungen bearbeiten auf iSCSIBootPG-A > Tiering und Failover > Failover Order > Vmnic3. Vmnic3 sollte aktiv sein und vmnic5 nicht verwendet werden.

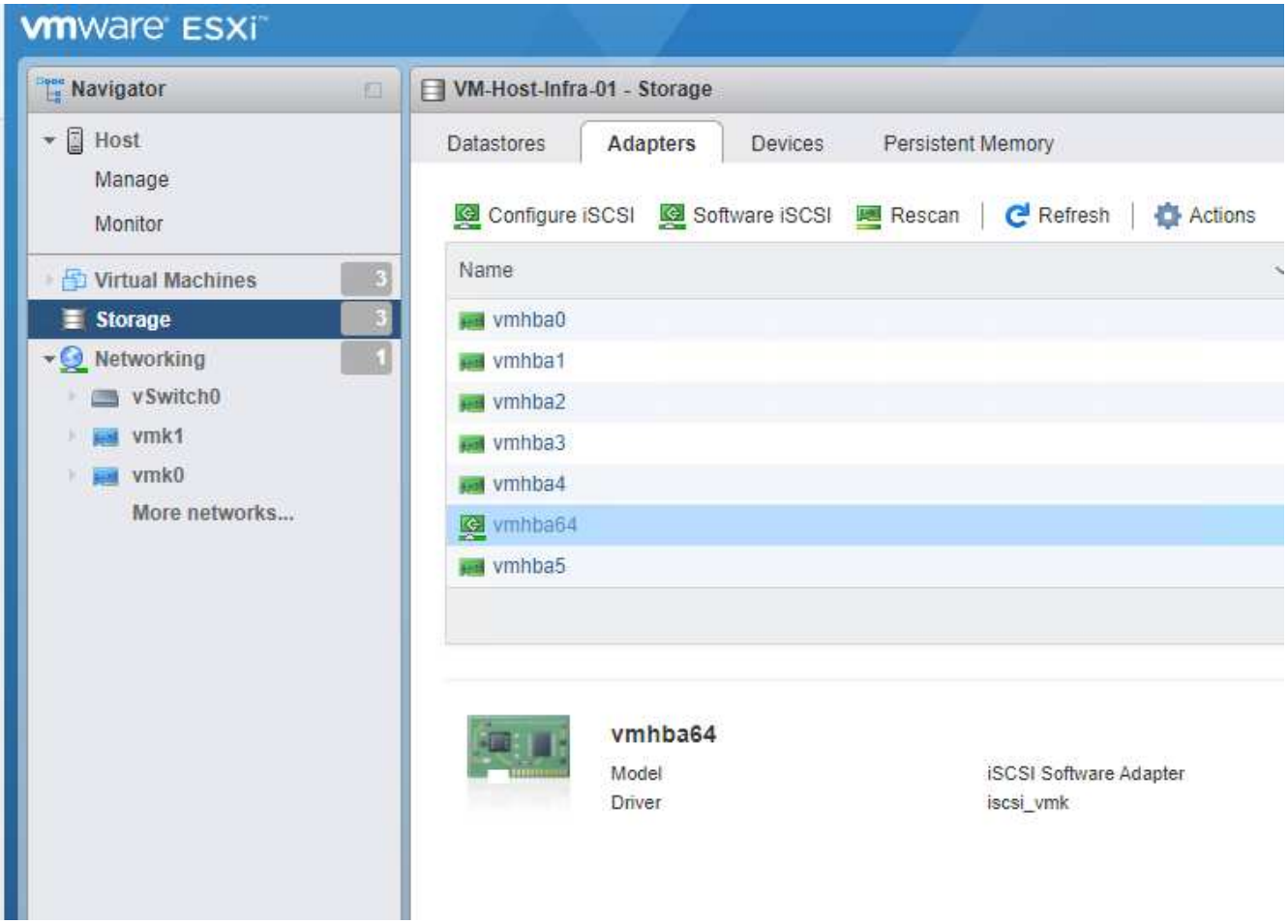
b. Klicken Sie auf Einstellungen bearbeiten auf iSCSIBootPG-B > Teaming und Failover > Failover-Reihenfolge > Vmnic5. Vmnic5 sollte aktiv sein und vmnic3 sollte nicht verwendet werden.



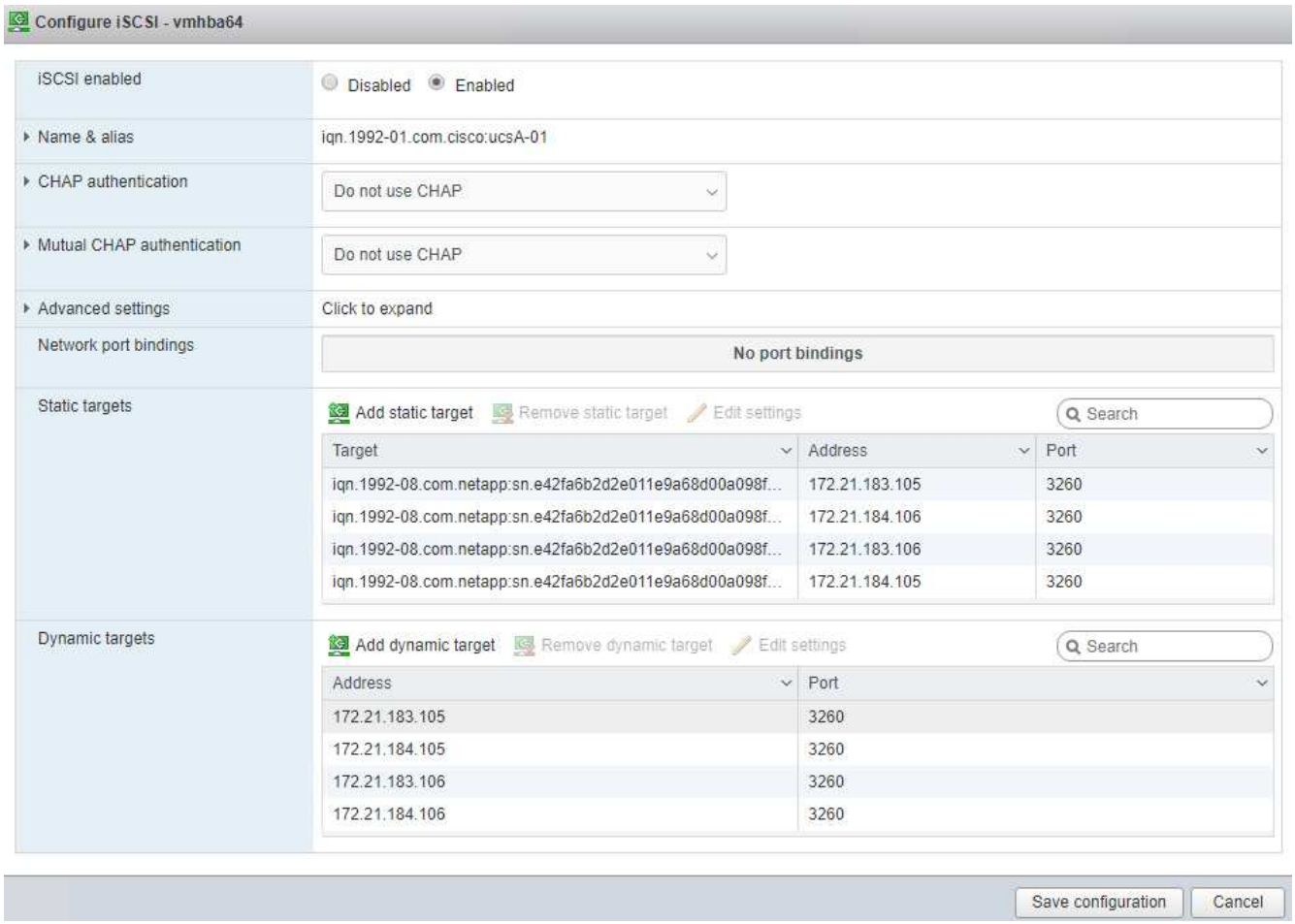
Konfigurieren Sie iSCSI-Multipathing

Gehen Sie wie folgt vor, um iSCSI-Multipathing auf den ESXi-Hosts einzurichten:

1. Wählen Sie im linken Navigationsbereich Storage aus. Klicken Sie Auf Adapter.
2. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf iSCSI konfigurieren.



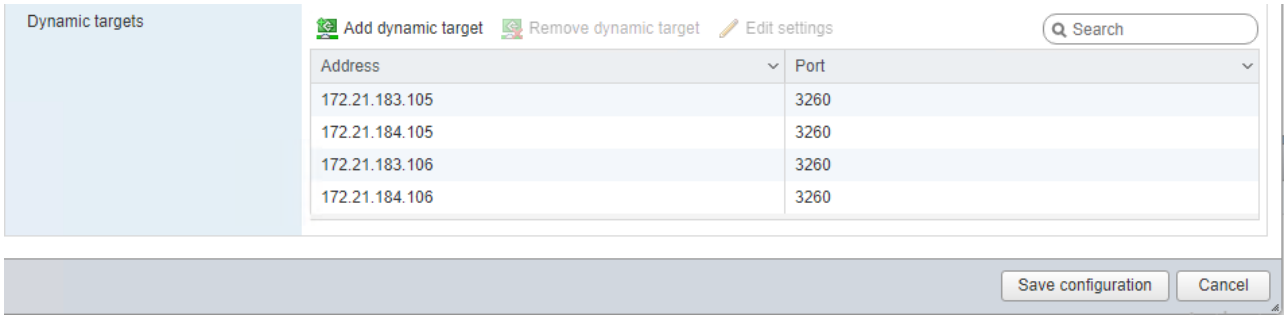
3. Klicken Sie unter dynamische Ziele auf dynamische Ziele hinzufügen.



4. Geben Sie die IP-Adresse ein `iscsi_lif01a`.

   a. Wiederholen Sie diesen Vorgang mit den IP-Adressen `iscsi_lif01b`, `iscsi_lif02a`, und `iscsi_lif02b`.

   b. Klicken Sie Auf Konfiguration Speichern.

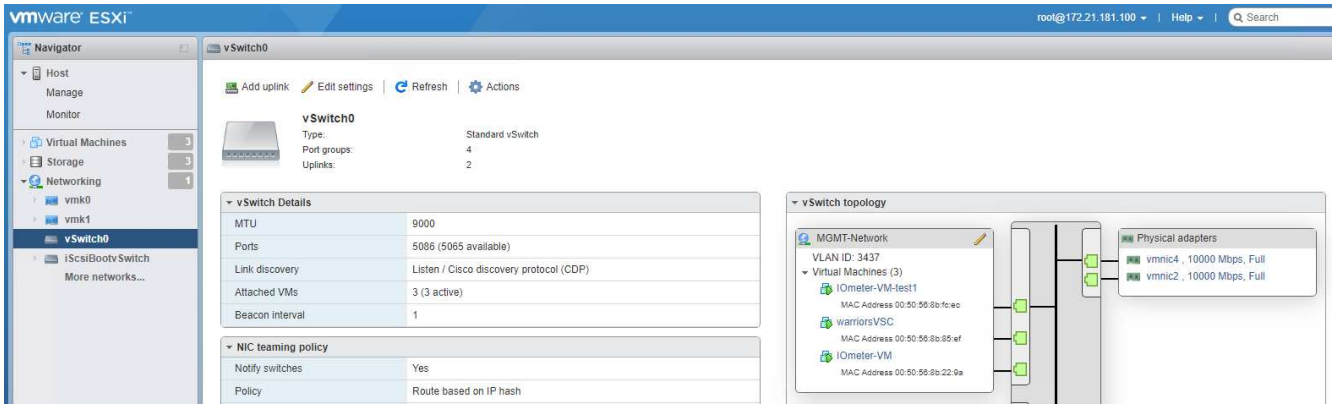


Sie können die iSCSI LIF IP-Adressen finden, indem Sie den Befehl show der Netzwerkschnittstelle auf dem NetApp Cluster ausführen oder sich in System Manager auf der Registerkarte Netzwerkschnittstellen ansehen.

Konfigurieren Sie den ESXi-Host

Führen Sie die folgenden Schritte aus, um ESXi-Starts zu konfigurieren:

1. Wählen Sie im linken Navigationsbereich die Option Netzwerk.
2. Wählen Sie vSwitch0 aus.



3. Wählen Sie Einstellungen Bearbeiten.
4. Ändern Sie die MTU in 9000.
5. Erweitern Sie NIC Teaming und stellen Sie sicher, dass sowohl vmnic2 als auch vmnic4 auf aktiv eingestellt sind und NIC Teaming und Failover auf Weiterleiten auf Grundlage von IP-Hash eingestellt sind.

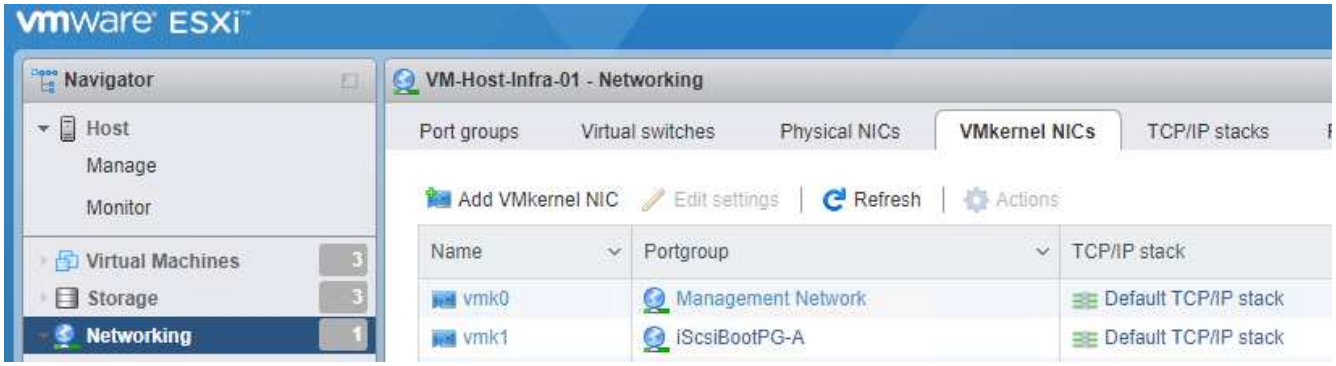
> Für die IP-Hash-Methode zum Lastausgleich muss der zugrunde liegende physische Switch mithilfe von SRC-DST-IP EtherChannel mit einem statischen (Mode- ein) Port-Kanal ordnungsgemäß konfiguriert werden. Aufgrund einer möglichen Switch-Fehlkonfiguration ist die Konnektivität möglicherweise zeitweise nicht mehr verfügbar. Wenn ja, fahren Sie dann vorübergehend einen der beiden verbundenen Uplink-Ports auf dem Cisco Switch herunter, um während der Fehlerbehebung für die Port-Channel-Einstellungen die Kommunikation mit dem ESXi Management vmKernel Port wiederherzustellen.

Konfigurieren Sie die Portgruppen und VMkernel NICs

Führen Sie die folgenden Schritte aus, um die Portgruppen und VMkernel-NICs zu konfigurieren:

1. Wählen Sie im linken Navigationsbereich die Option Netzwerk.
2. Klicken Sie mit der rechten Maustaste auf die Registerkarte Portgruppen.

3. Klicken Sie mit der rechten Maustaste auf VM Network, und wählen Sie Bearbeiten aus. Ändern Sie die VLAN-ID in `<<var_vm_traffic_vlan>>`.
4. Klicken Sie Auf Portgruppe Hinzufügen.
   a. Geben Sie den Namen der Portgruppe MGMT-Network an.
   b. Eingabe `<<mgmt_vlan>>` Für die VLAN-ID.
   c. Stellen Sie sicher, dass vSwitch0 ausgewählt ist.
   d. Klicken Sie auf Speichern.
5. Klicken Sie auf die Registerkarte VMkernel NICs.



6. Wählen Sie VMkernel NIC hinzufügen aus.
   a. Wählen Sie Neue Portgruppe.
   b. Benennen Sie die Portgruppe NFS-Network.
   c. Eingabe `<<nfs_vlan_id>>` Für die VLAN-ID.
   d. Ändern Sie die MTU in 9000.
   e. IPv4-Einstellungen erweitern.
   f. Wählen Sie Statische Konfiguration.
   g. Eingabe `<<var_hosta_nfs_ip>>` Für Adresse.

h. Eingabe `<<var_hosta_nfs_mask>>` Für Subnetzmaske.

i. Klicken Sie auf Erstellen .

7. Wiederholen Sie diesen Prozess für die Erstellung des vMotion VMkernel Port.
8. Wählen Sie VMkernel NIC hinzufügen aus.

a. Wählen Sie Neue Portgruppe.

b. Benennen Sie vMotion für die Portgruppe.

c. Eingabe `<<vmotion_vlan_id>>` Für die VLAN-ID.

d. Ändern Sie die MTU in 9000.

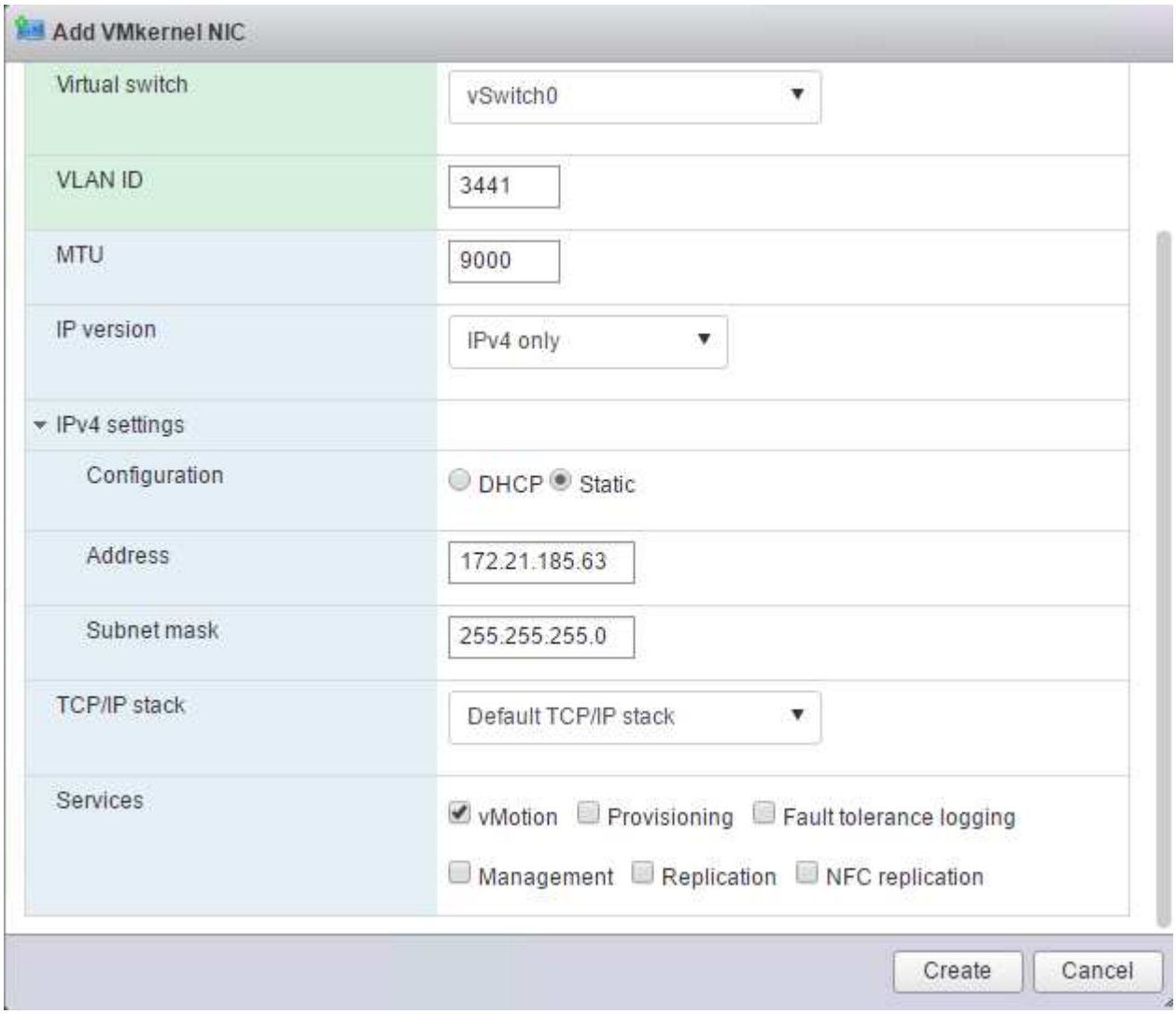
e. IPv4-Einstellungen erweitern.

f. Wählen Sie Statische Konfiguration.

g. Eingabe `<<var_hosta_vmotion_ip>>` Für Adresse.

h. Eingabe `<<var_hosta_vmotion_mask>>` Für Subnetzmaske.

i. Stellen Sie sicher, dass das Kontrollkästchen vMotion nach den IPv4-Einstellungen ausgewählt ist.

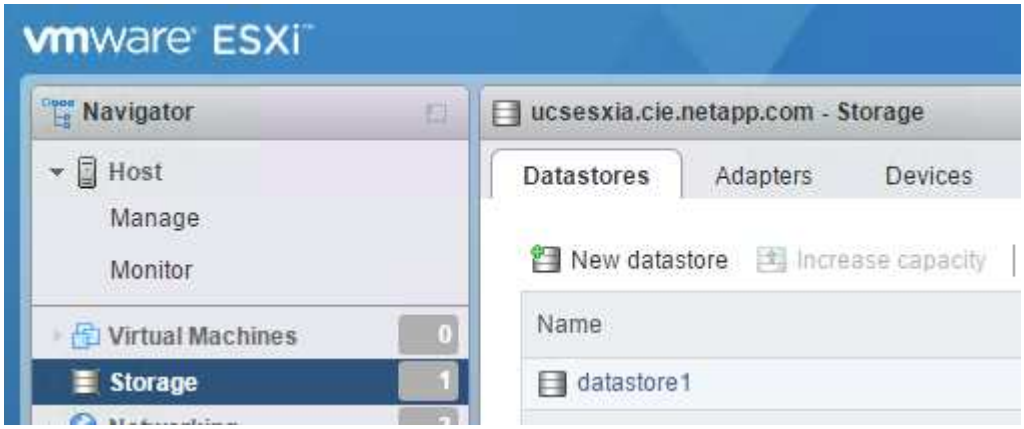


Es gibt viele Möglichkeiten, ESXi Networking zu konfigurieren, einschließlich der Verwendung des VMware vSphere Distributed Switches, wenn Ihre Lizenzierung es zulässt. In FlexPod Express werden alternative Netzwerkkonfigurationen unterstützt, wenn sie zur Erfüllung der geschäftlichen Anforderungen erforderlich sind.

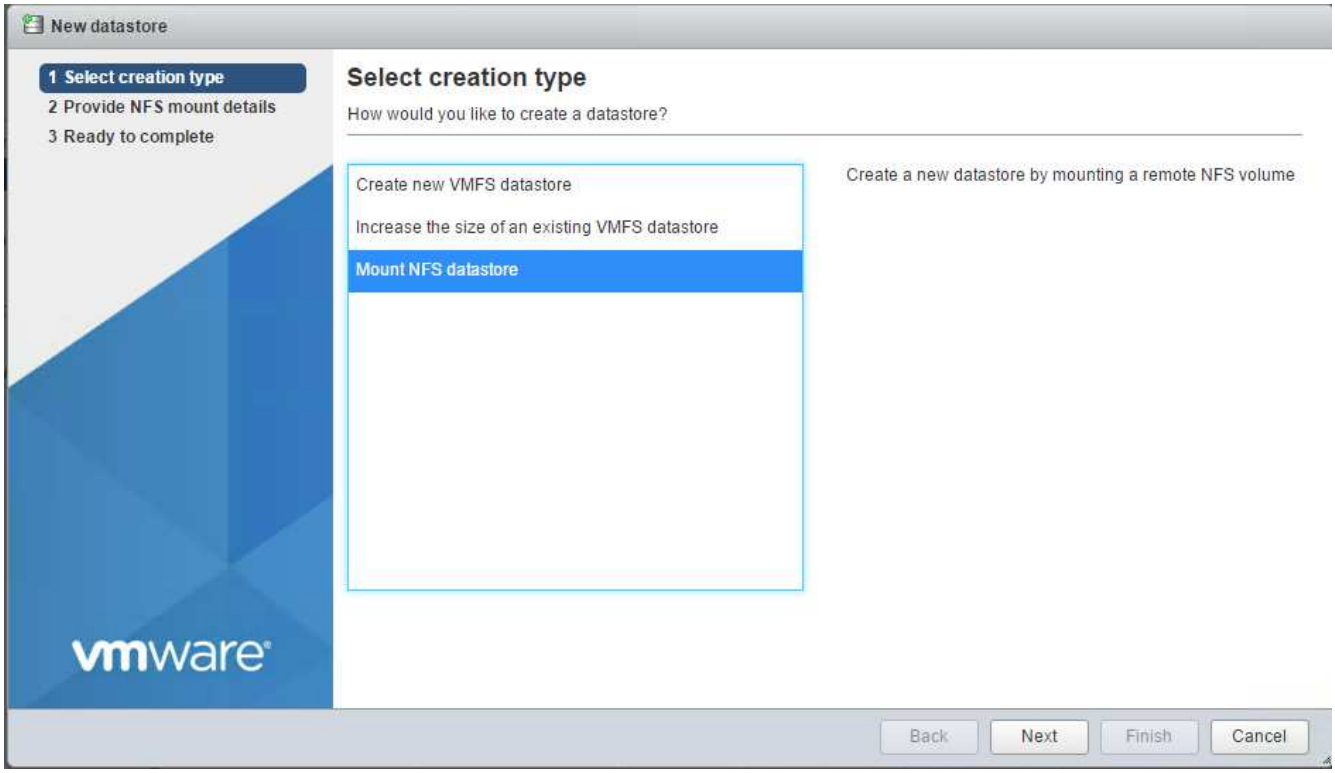
Montieren Sie die ersten Datenspeicher

Die ersten Datenspeicher, die gemountet werden sollen, sind die `infra_datastore` Datastore für VMs und das `infra_swap` Datenspeicher für VM-Auslagerungsdateien:

1. Klicken Sie im linken Navigationsbereich auf „Storage“ und dann auf New Datastore.



2. Wählen Sie Mount NFS Datastore aus.



3. Geben Sie die folgenden Informationen auf der Seite „NFS Mount Details angeben“ ein:
   - Name: `infra_datastore`

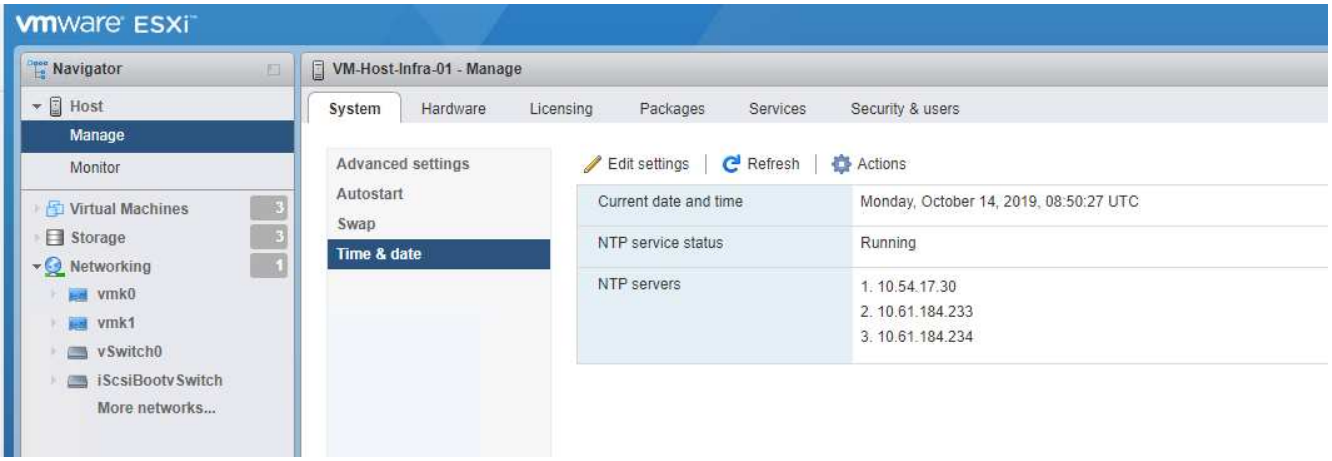
- NFS-Server: `<<var_nodea_nfs_lif>>`
- Weitersagen: `/infra_datastore`
- Stellen Sie sicher, dass NFS 3 ausgewählt ist.

4. Klicken Sie Auf Fertig Stellen. Die Aufgabe wird im Fenster Letzte Aufgaben ausgeführt.
5. Wiederholen Sie diesen Vorgang, um den zu mounten `infra_swap` Datenspeicher:
   - Name: `infra_swap`
   - NFS-Server: `<<var_nodea_nfs_lif>>`
   - Weitersagen: `/infra_swap`
   - Stellen Sie sicher, dass NFS 3 ausgewählt ist.

Konfigurieren Sie NTP

Gehen Sie wie folgt vor, um NTP für einen ESXi-Host zu konfigurieren:

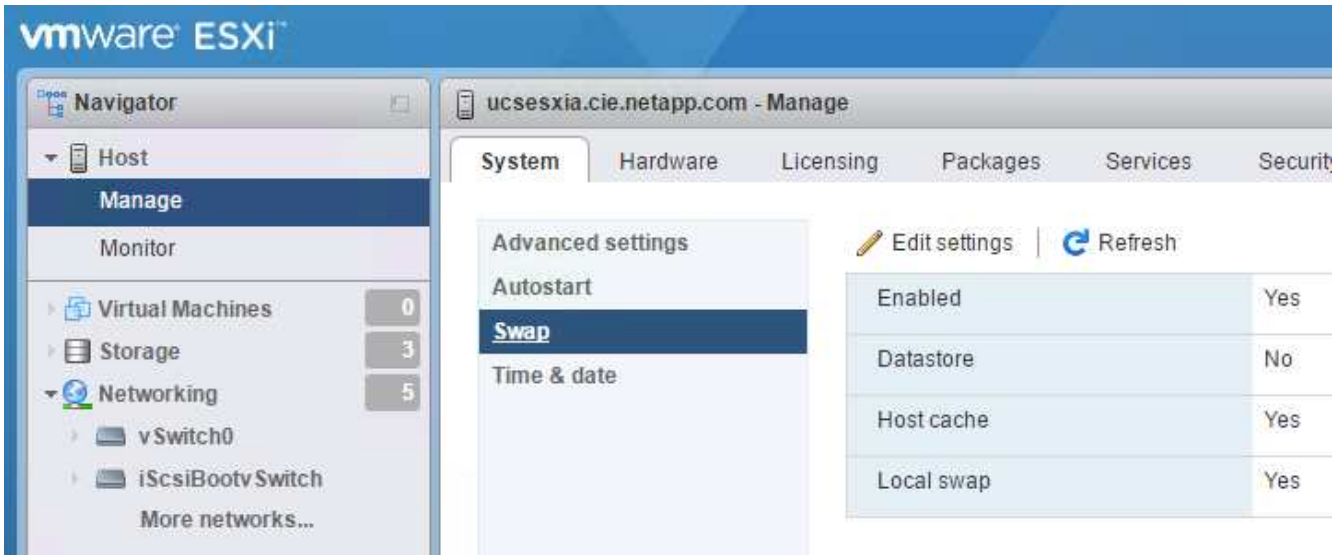
1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich System aus, und klicken Sie anschließend auf Zeit und Datum.
2. Wählen Sie Network Time Protocol (Network Time Protocol verwenden) (NTP Client aktivieren) aus.
3. Wählen Sie Start und Stopp mit Host als Startrichtlinie für den NTP-Dienst aus.
4. Eingabe `<<var_ntp>>` Als NTP-Server. Sie können mehrere NTP-Server festlegen.
5. Klicken Sie auf Speichern .



Verschieben Sie den Speicherort der VM-Auslagerungsdatei

Diese Schritte bieten Details zum Verschieben der VM-Auslagerungsdatei.

1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich das System aus, und klicken Sie dann auf Tausch.



2. Klicken Sie Auf Einstellungen Bearbeiten. Wählen Sie `infra_swap` In den Datastore-Optionen.

3. Klicken Sie auf Speichern .

"Weiter: VMware vCenter Server 6.7U2 Installationsverfahren."

Installationsverfahren für VMware vCenter Server 6.7U2

Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware vCenter Server 6.7 in einer FlexPod Express-Konfiguration.

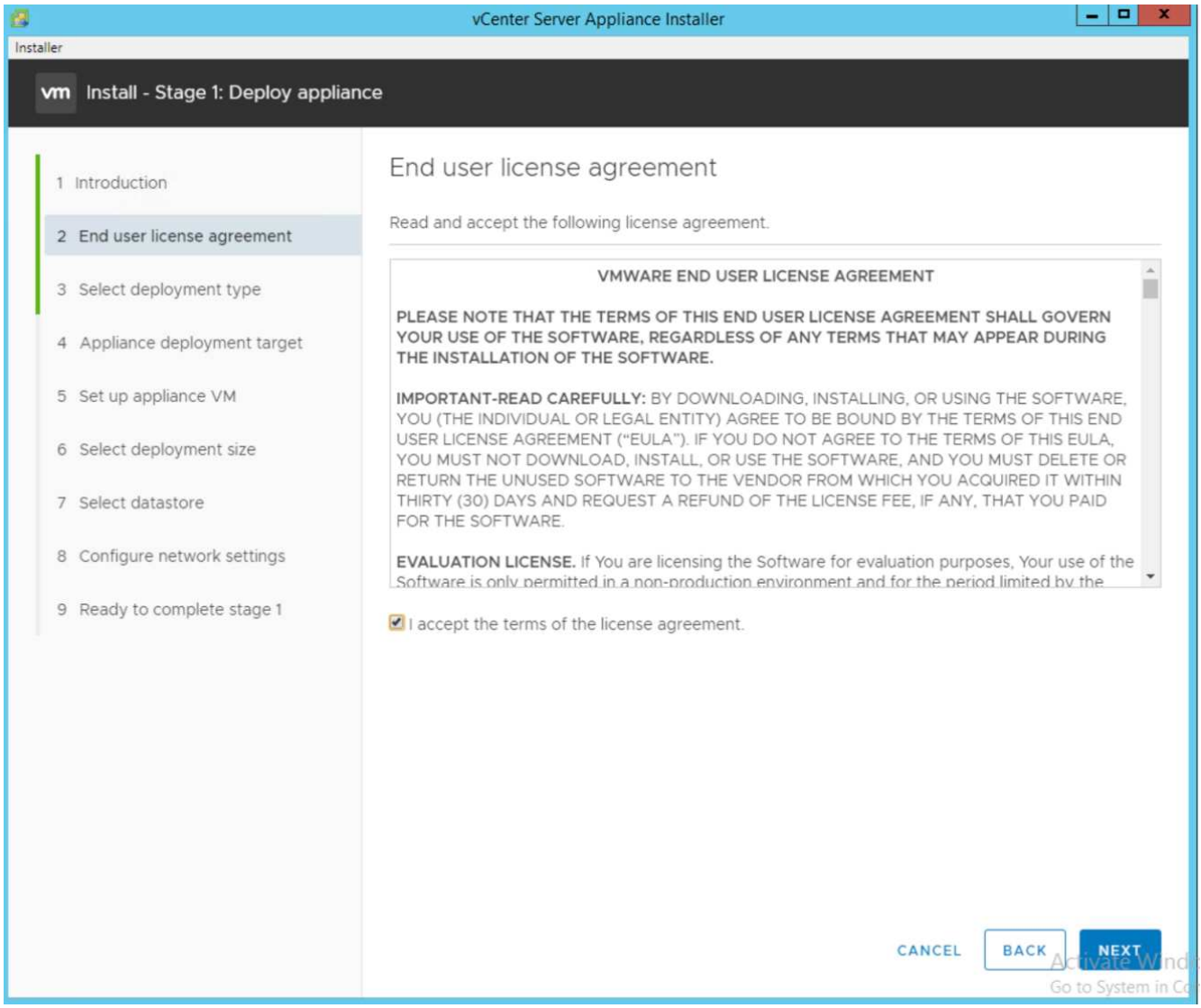
FlexPod Express verwendet die VMware vCenter Server Appliance (VCSA).

Laden Sie die VMware vCenter Server Appliance herunter

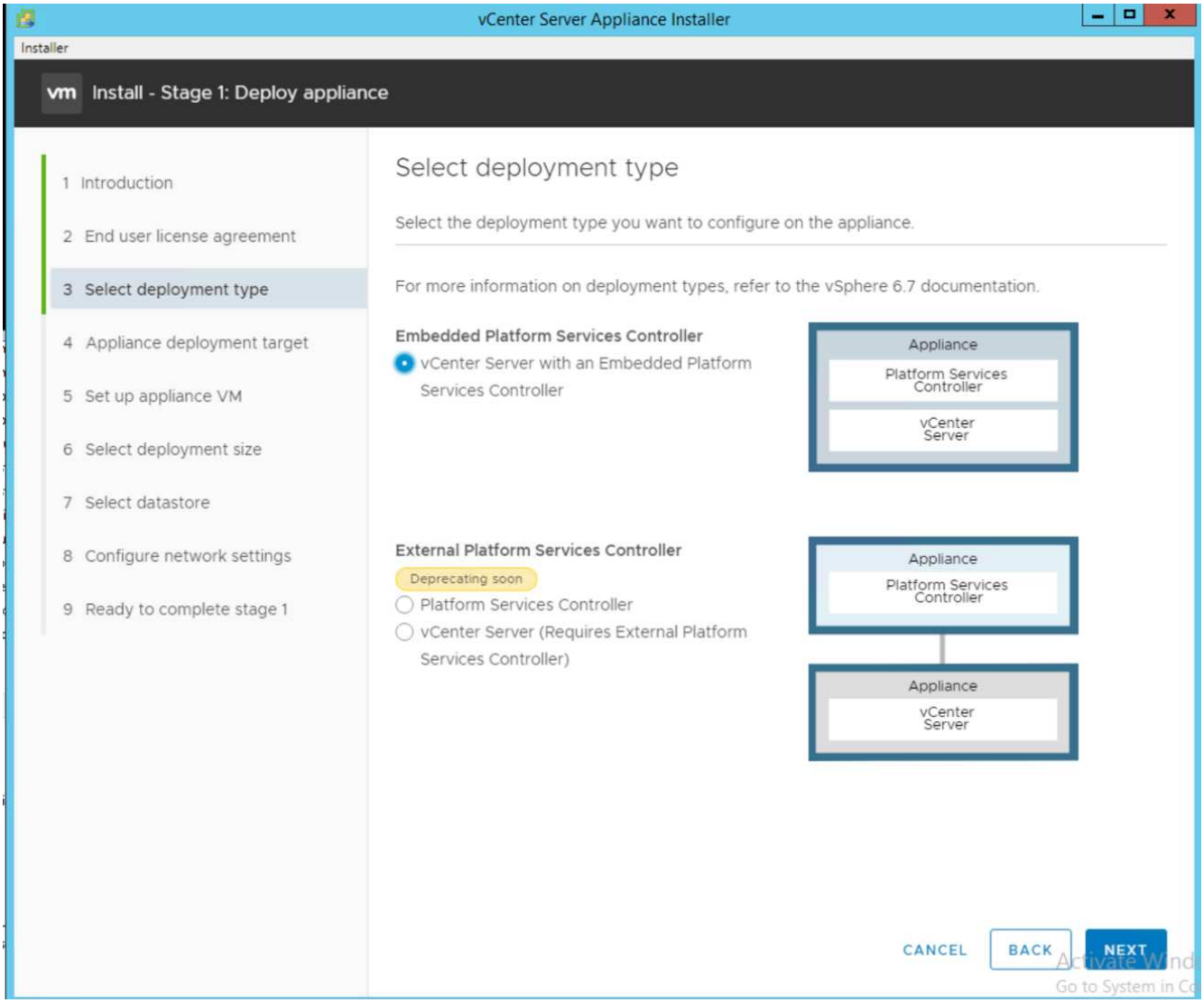
So laden Sie die VMware vCenter Server Appliance (VCSA) herunter:

1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.
2. Laden Sie die VCSA von der VMware-Website herunter.

3. Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.
4. Mounten Sie das ISO-Image.
5. Navigieren Sie zum verzeichnis vcsa- ui-Installer > win32. Doppelklicken `installer.exe`.
6. Klicken Sie Auf Installieren.
7. Klicken Sie auf der Seite Einführung auf Weiter.

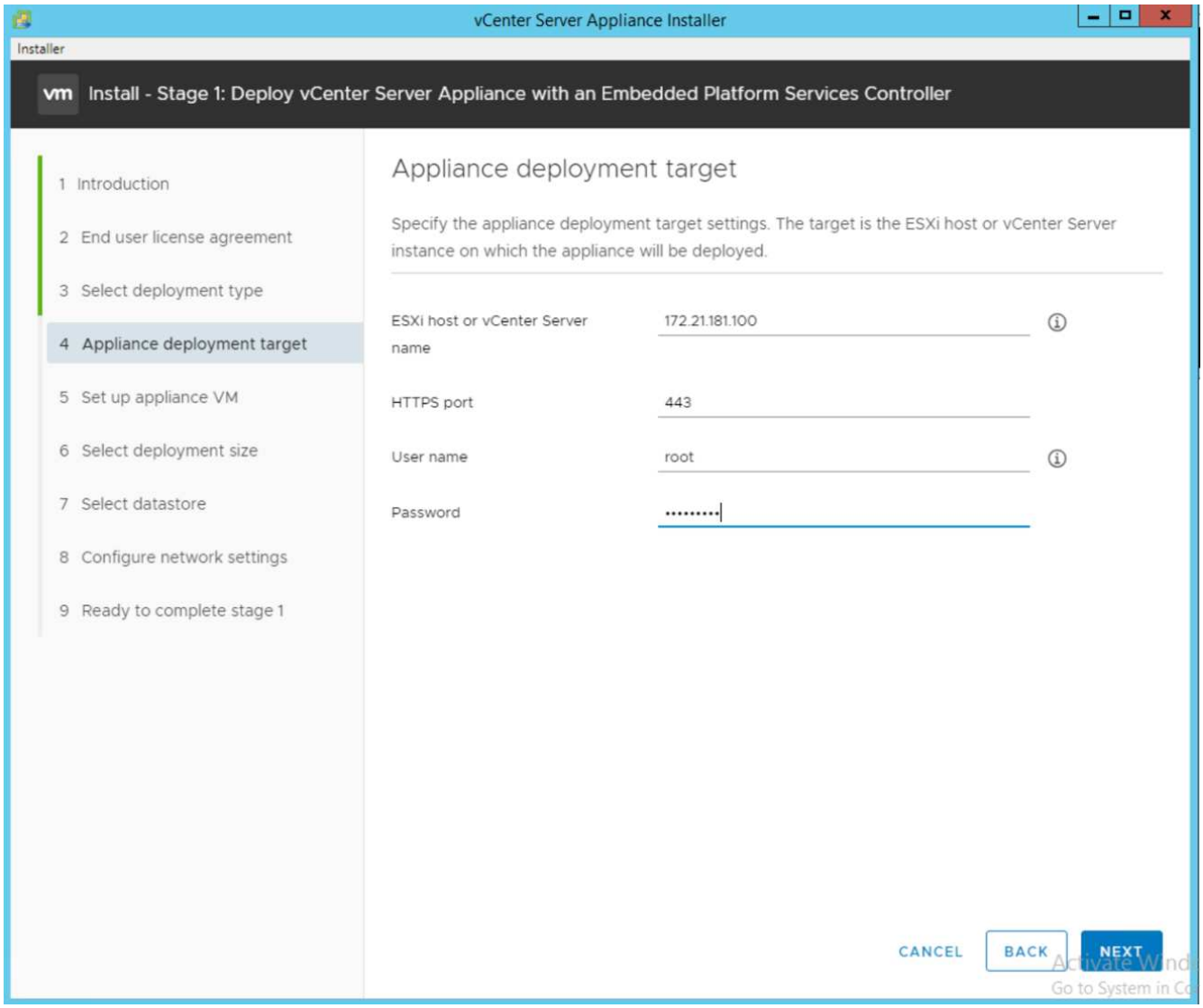


8. Wählen Sie als Bereitstellungstyp den Embedded Platform Services Controller aus.

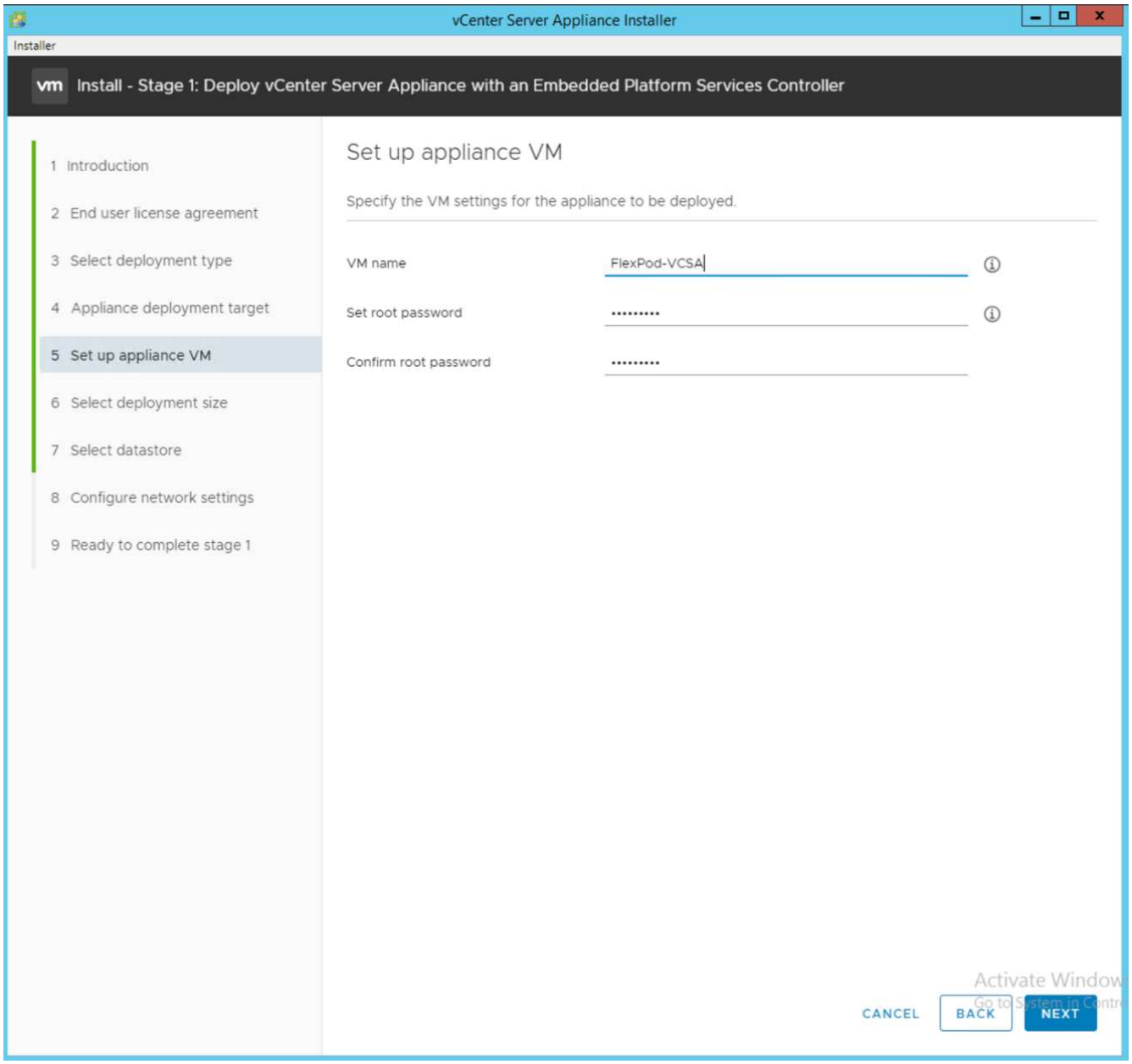


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

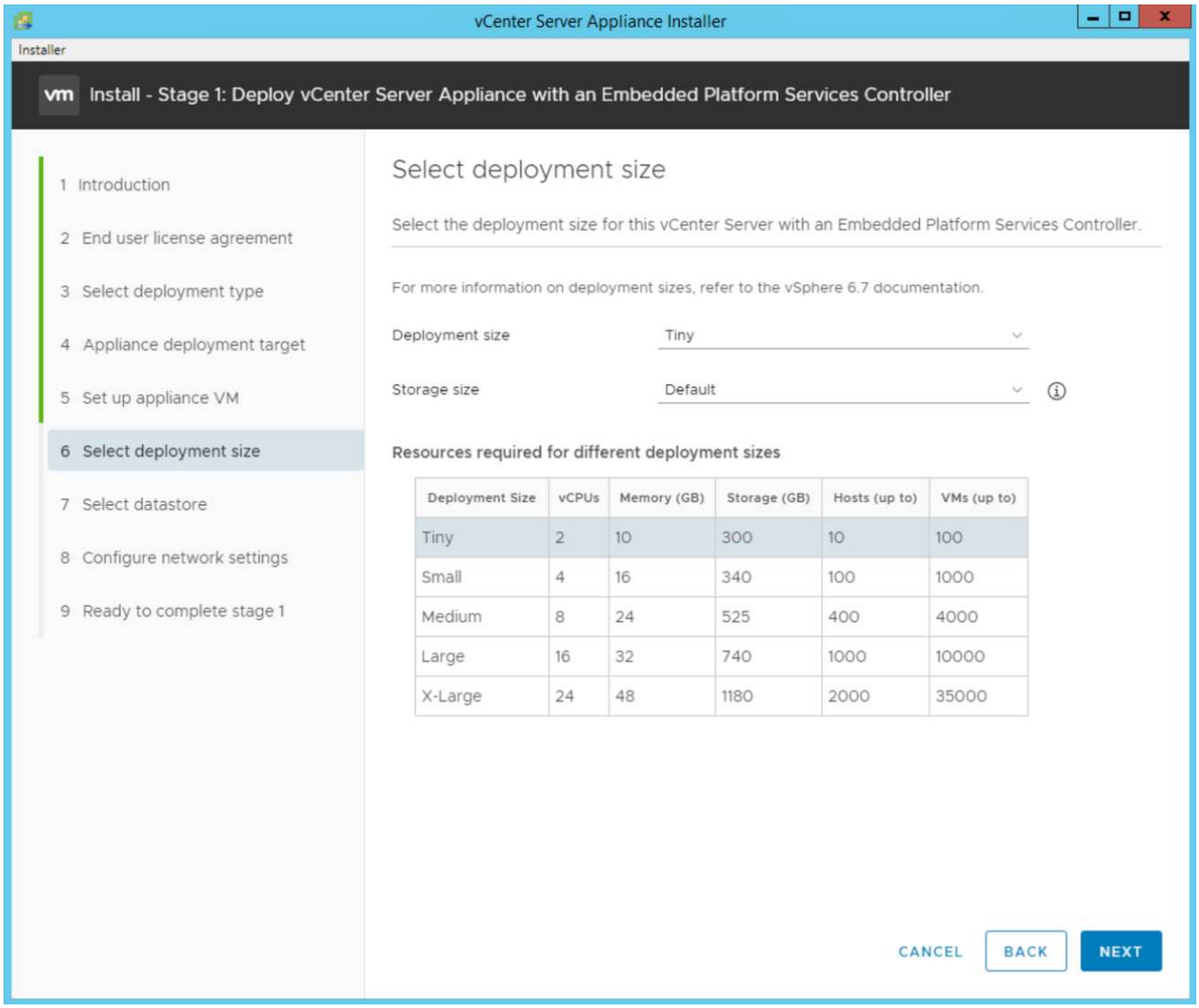
9. Geben Sie im Appliance Deployment Target die IP-Adresse eines bereitgestelltem ESXi-Hosts, den Root-Benutzernamen und das Root-Passwort ein.



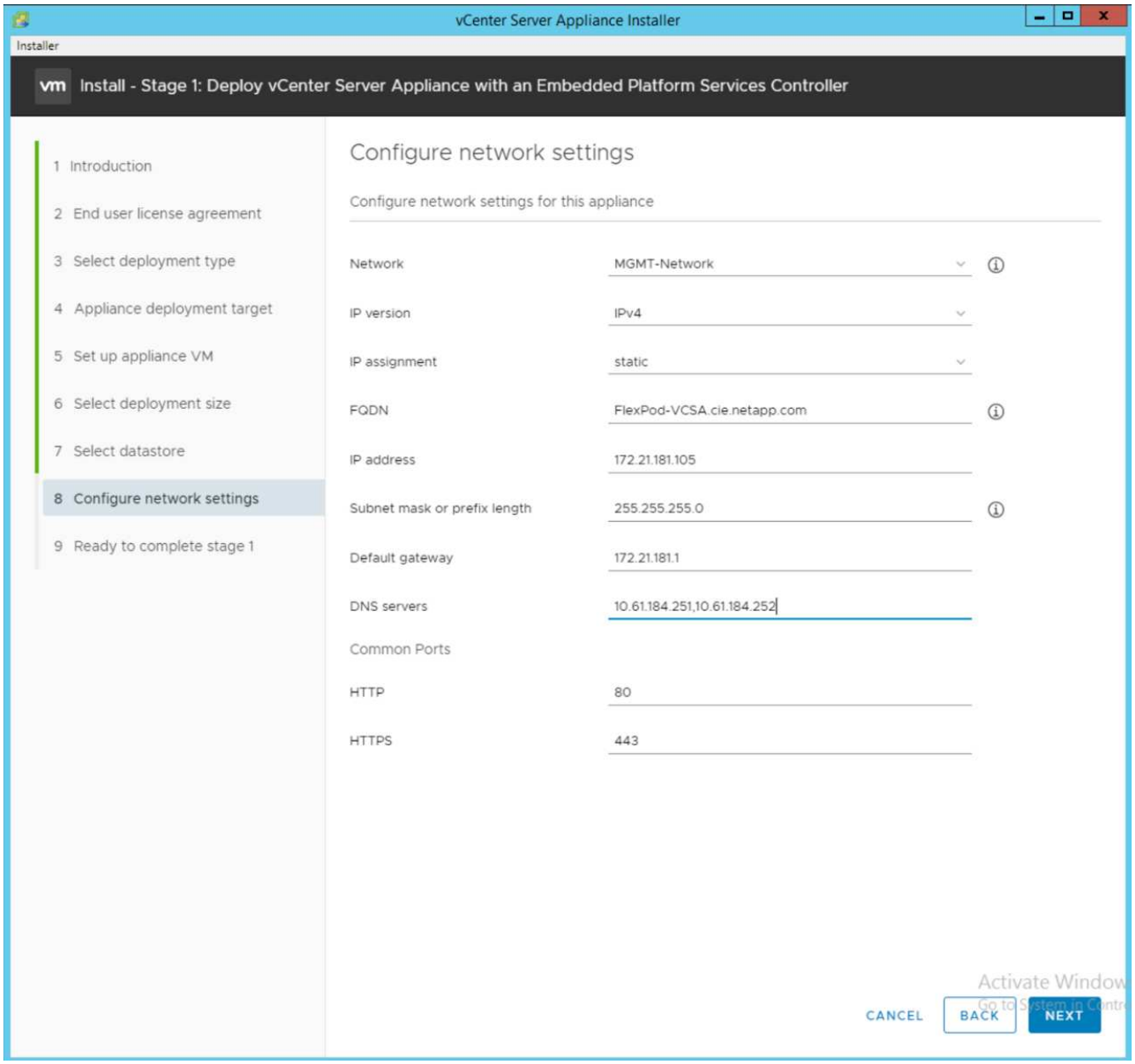
10. Legen Sie die Appliance-VM fest, indem Sie VCSA als VM-Name und das Root-Passwort eingeben, das Sie für VCSA verwenden möchten.



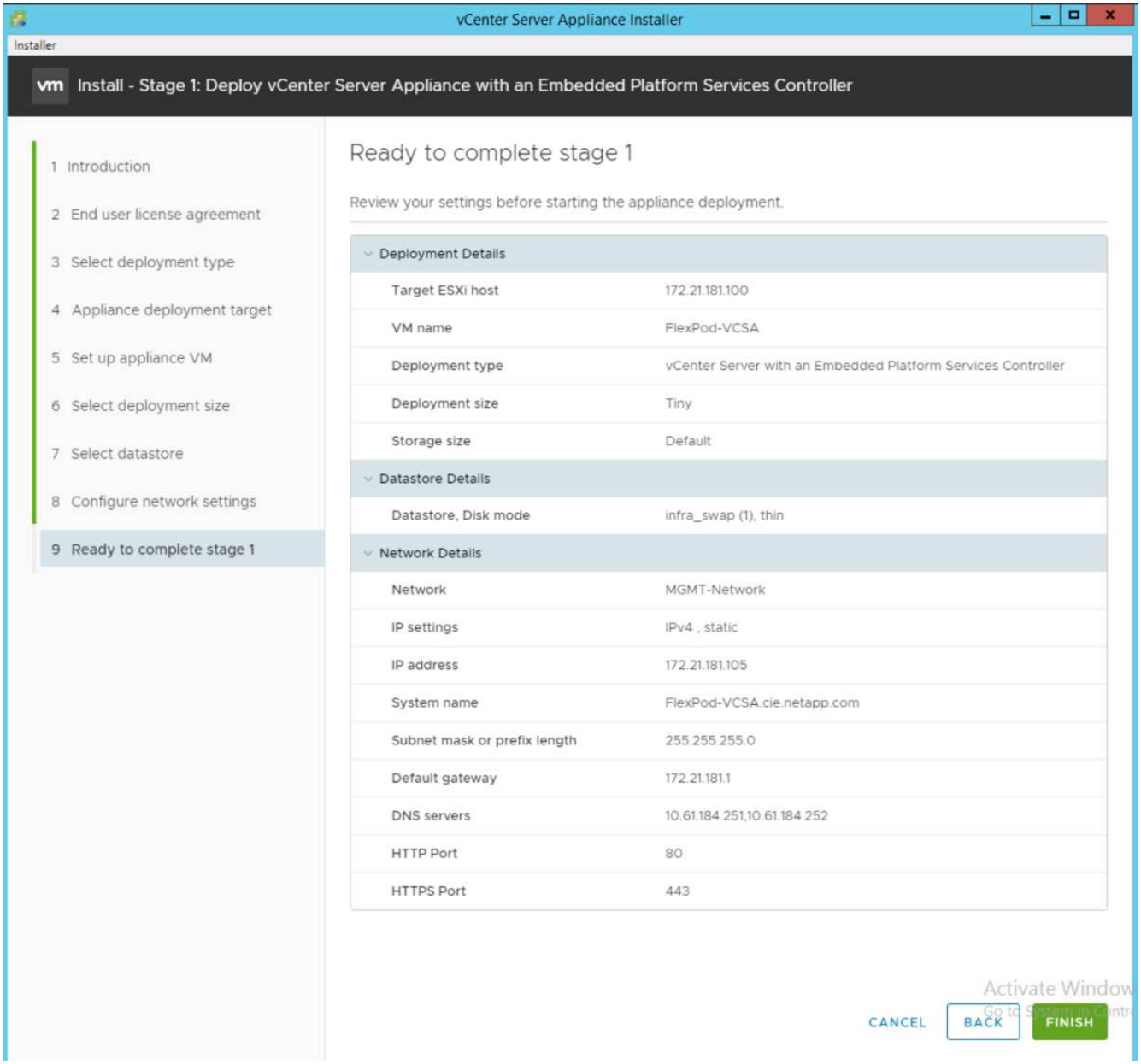
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



12. Wählen Sie die aus `infra_datastore` Datenspeicher: Klicken Sie Auf Weiter.
13. Geben Sie die folgenden Informationen auf der Seite Netzwerkeinstellungen konfigurieren ein, und klicken Sie auf Weiter.
    a. Wählen Sie MGMT-Network für Netzwerk.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse ein.
    d. Geben Sie die zu verwendenden Subnetzmaske ein.
    e. Geben Sie das Standard-Gateway ein.
    f. Geben Sie den DNS-Server ein.
14. Überprüfen Sie auf der Seite bereit zum Abschließen von Phase 1, ob die von Ihnen eingegebenen Einstellungen korrekt sind. Klicken Sie Auf Fertig Stellen.

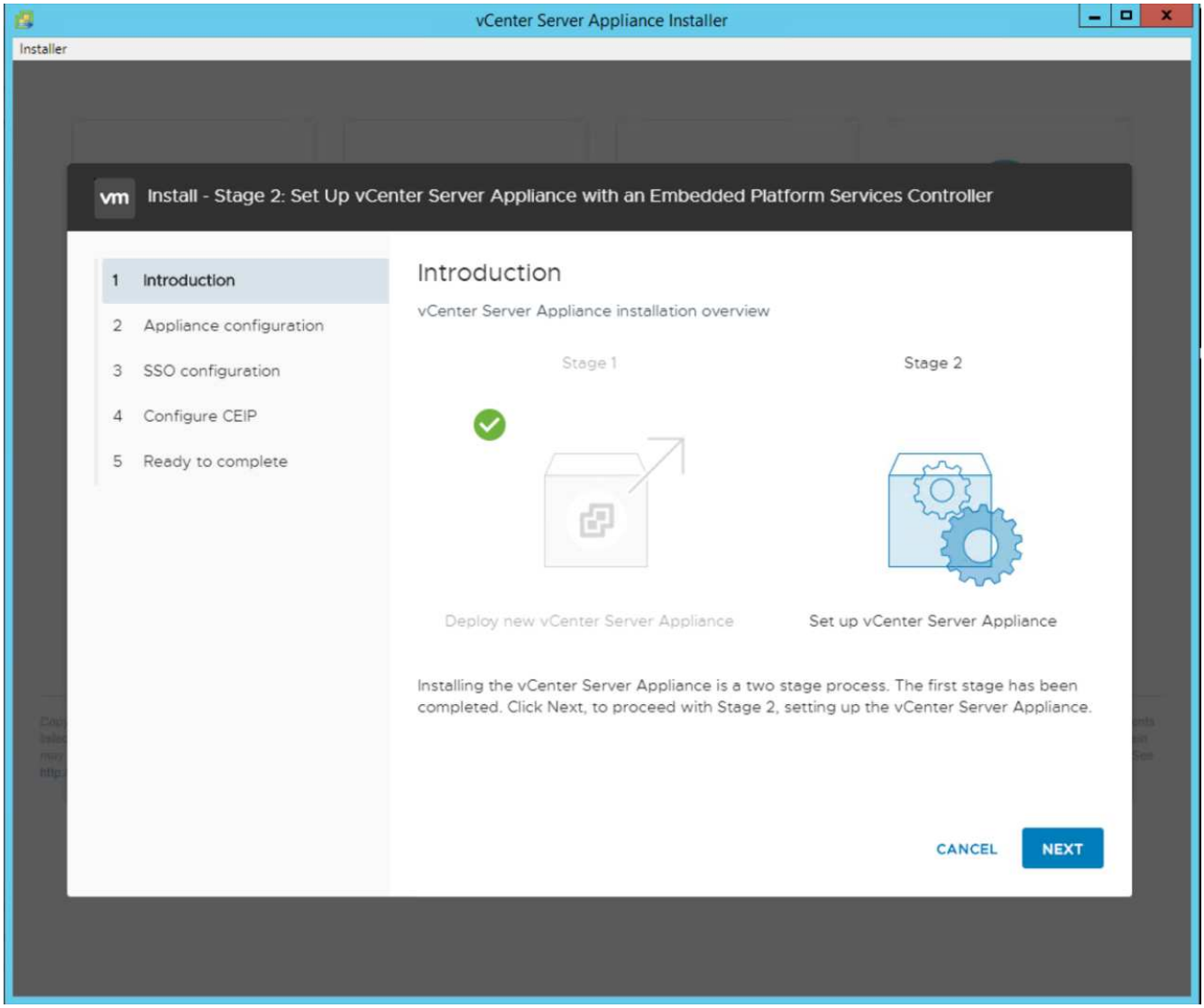


15. Überprüfen Sie Ihre Einstellungen in Phase 1, bevor Sie mit der Bereitstellung der Appliance beginnen.

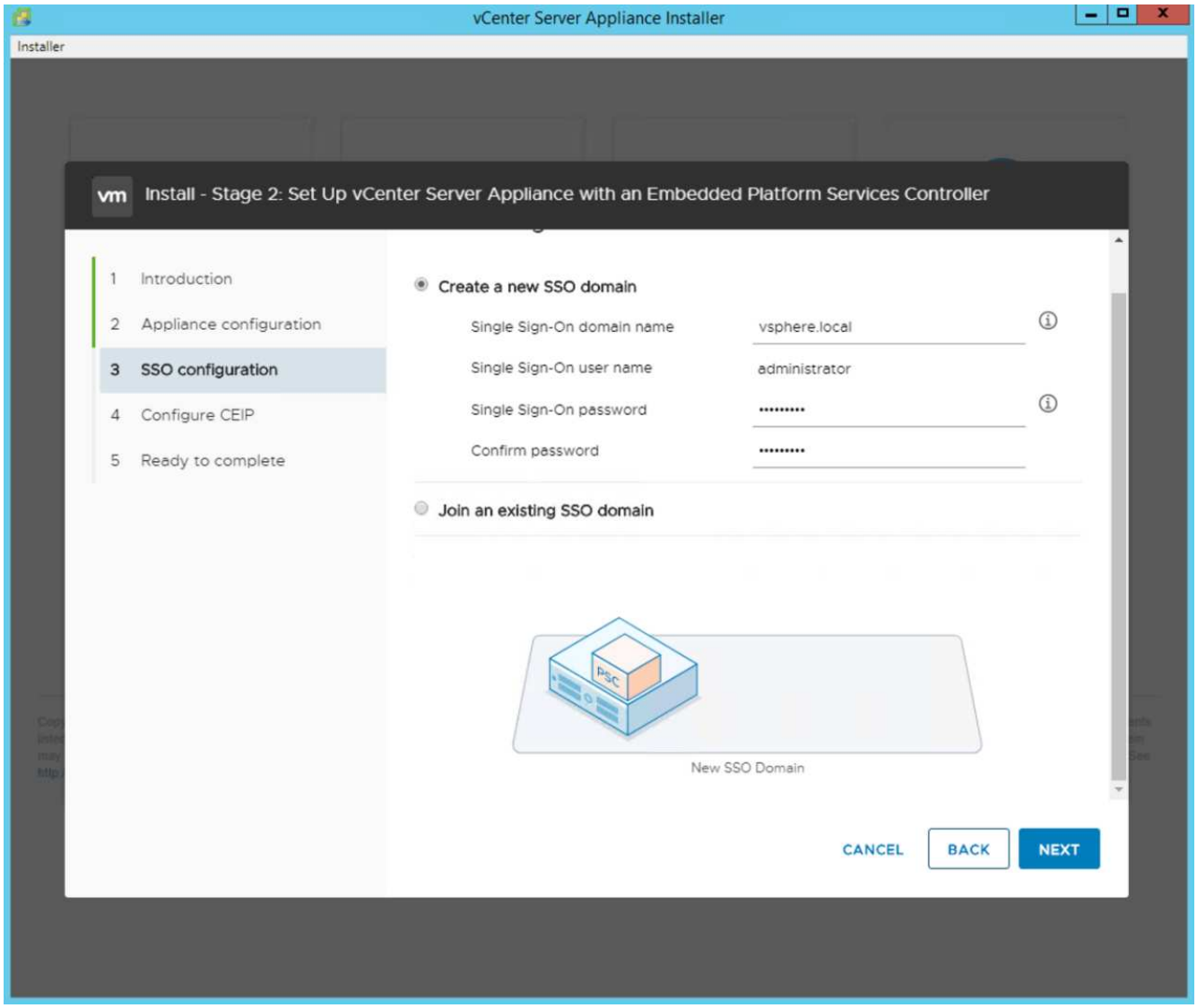


Die VCSA wird jetzt installiert. Dieser Vorgang dauert mehrere Minuten.

16. Wenn Phase 1 abgeschlossen ist, wird eine Meldung angezeigt, die angibt, dass sie abgeschlossen ist. Klicken Sie auf Weiter, um die Konfiguration von Phase 2 zu beginnen.
17. Klicken Sie auf der Seite Einführung in Phase 2 auf Weiter.

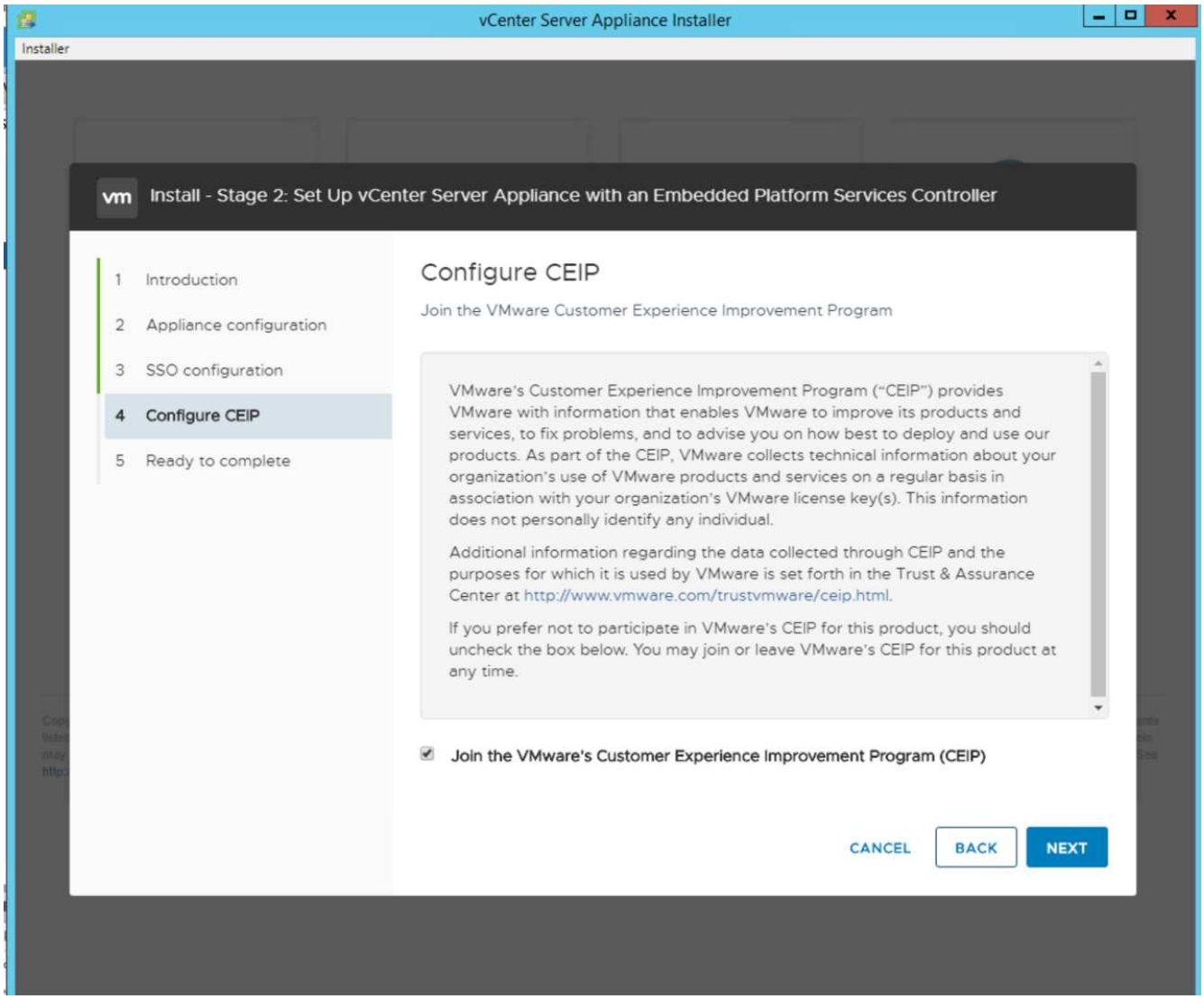


18. Eingabe `<<var_ntp_id>>` Für die NTP-Serveradresse. Sie können mehrere NTP-IP-Adressen eingeben.
19. Wenn Sie Hochverfügbarkeit (HA) in vCenter Server verwenden möchten, stellen Sie sicher, dass der SSH-Zugriff aktiviert ist.
20. Konfigurieren Sie den SSO-Domänennamen, das Passwort und den Standortnamen. Klicken Sie Auf Weiter.

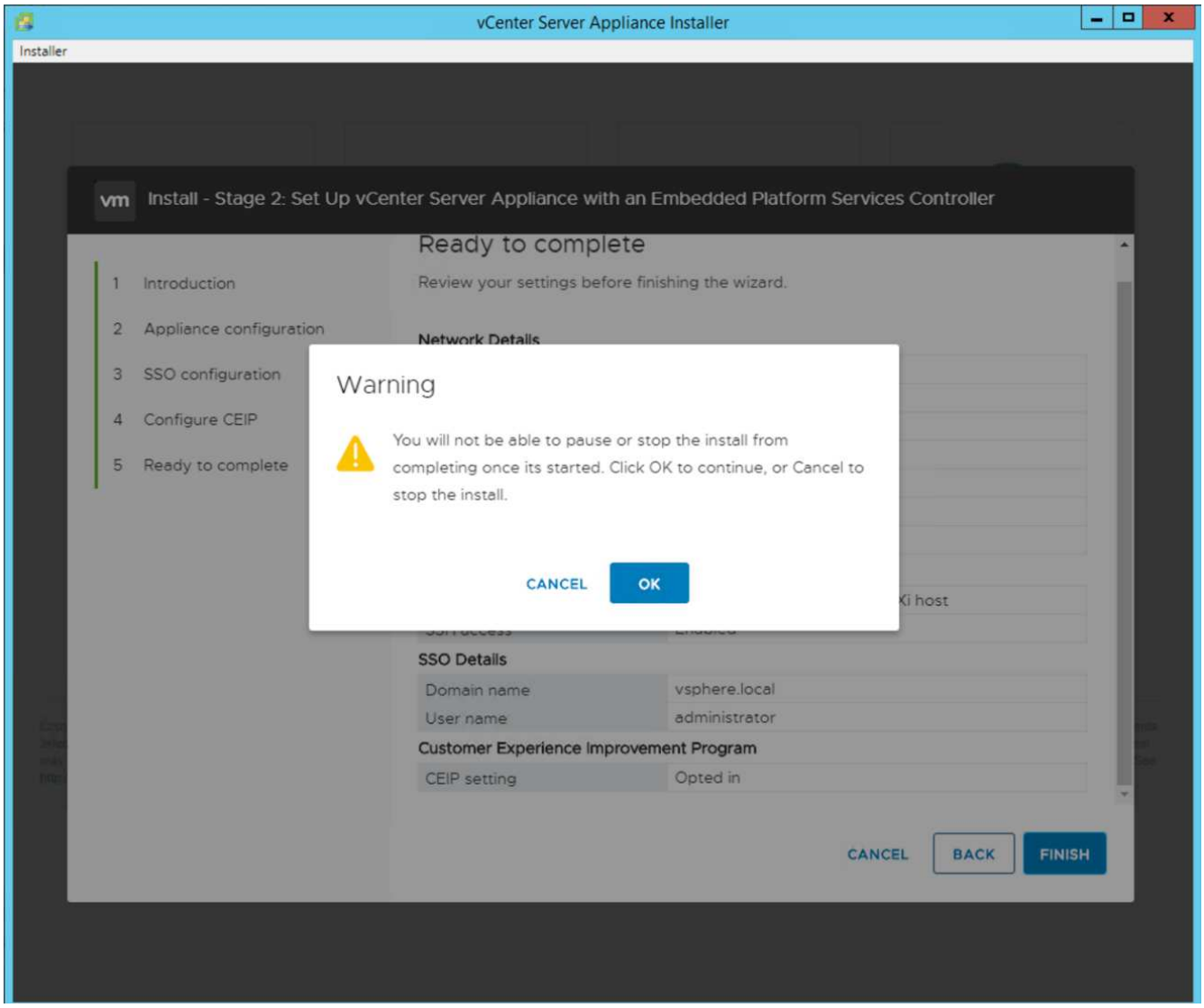


Notieren Sie diese Werte für Ihre Referenz, insbesondere wenn Sie vom abweichen `vsphere.local` Domain-Name:

21. Treten Sie auf Wunsch dem VMware Customer Experience-Programm bei. Klicken Sie Auf Weiter.



22. Zeigen Sie die Zusammenfassung Ihrer Einstellungen an. Klicken Sie auf Fertig stellen oder verwenden Sie die Schaltfläche Zurück, um die Einstellungen zu bearbeiten.
23. Es wird eine Meldung angezeigt, die besagt, dass Sie die Installation nach dem Start nicht unterbrechen oder beenden können. Klicken Sie auf OK, um fortzufahren.



Die Einrichtung der Appliance wird fortgesetzt. Dies dauert einige Minuten.

Es wird eine Meldung angezeigt, die angibt, dass das Setup erfolgreich war.

24. Die Links, die der Installer zum Zugriff auf vCenter Server bereitstellt, sind anklickbar.

"Als Nächstes: VMware vCenter Server 6.7U2 und vSphere Clustering-Konfiguration."

Clustering-Konfiguration für VMware vCenter Server 6.7U2 und vSphere

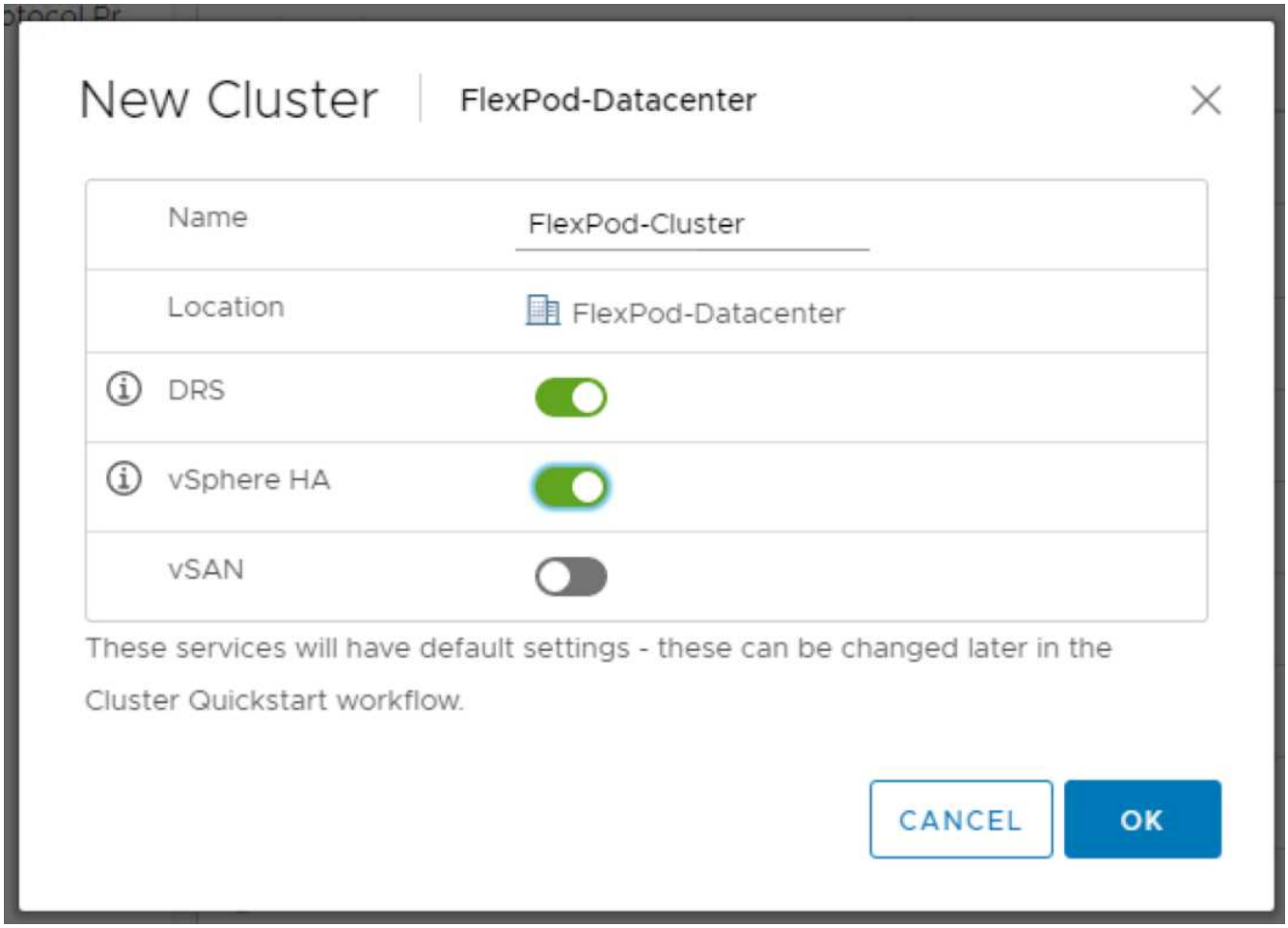
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

1. Navigieren Sie zu `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Klicken Sie auf vSphere Client starten.
3. Melden Sie sich mit dem Benutzernamen Administrator@vsphere.local und dem SSO-Passwort an, das Sie während des VCSA-Setups eingegeben haben.
4. Klicken Sie mit der rechten Maustaste auf den vCenter-Namen, und wählen Sie New Datacenter aus.
5. Geben Sie einen Namen für das Datacenter ein, und klicken Sie auf OK.

Erstellen eines vSphere Clusters

Gehen Sie zum Erstellen eines vSphere-Clusters wie folgt vor:

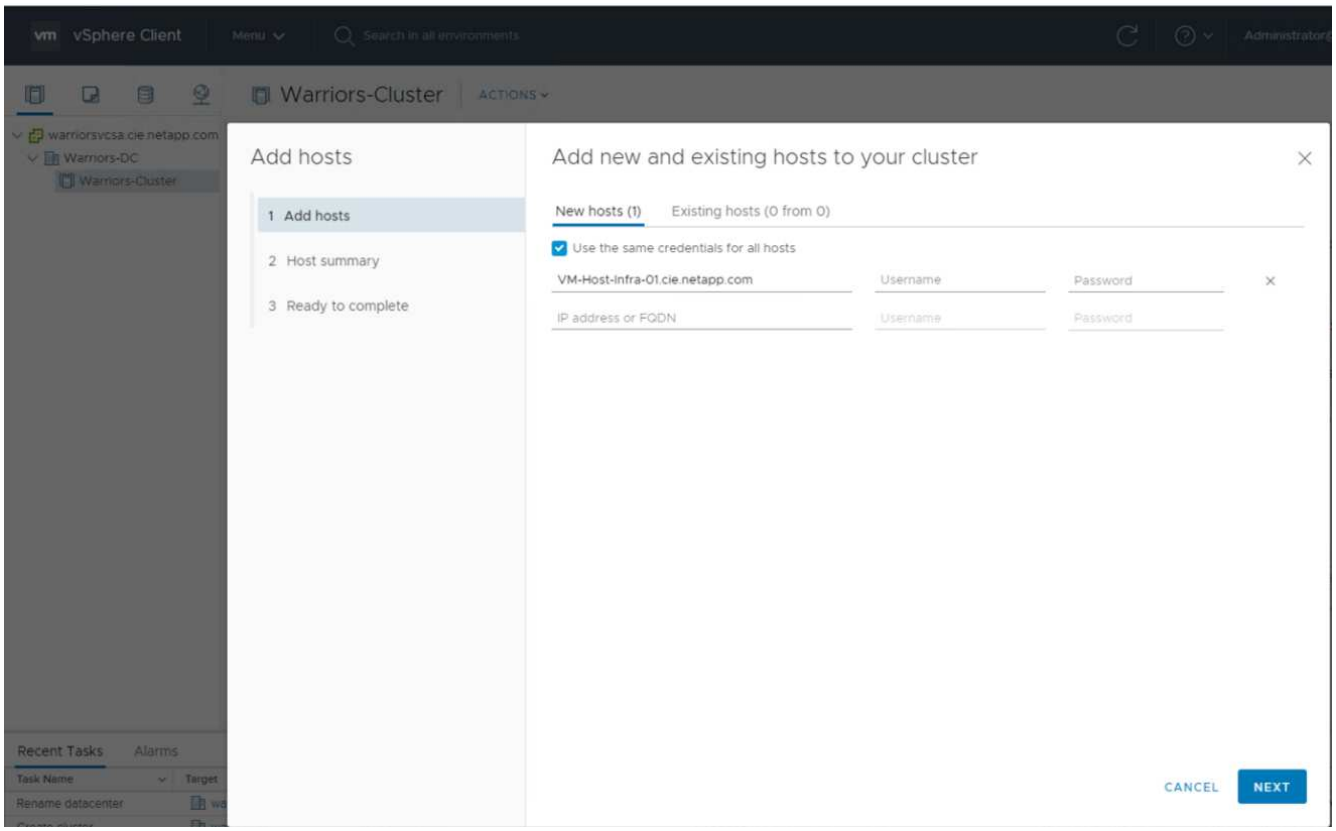
1. Klicken Sie mit der rechten Maustaste auf das neu erstellte Datacenter, und wählen Sie Neuer Cluster aus.
2. Geben Sie einen Namen für das Cluster ein.
3. Aktivieren Sie DR und vSphere HA, indem Sie die Kontrollkästchen auswählen.
4. Klicken Sie auf OK.



Fügen Sie die ESXi-Hosts dem Cluster hinzu

Führen Sie die folgenden Schritte aus, um dem Cluster die ESXi-Hosts hinzuzufügen:

1. Klicken Sie mit der rechten Maustaste auf das Cluster, und wählen Sie Host hinzufügen aus.



2. Gehen Sie wie folgt vor, um dem Cluster einen ESXi-Host hinzuzufügen:
   a. Geben Sie die IP oder den FQDN des Hosts ein. Klicken Sie Auf Weiter.
   b. Geben Sie den Benutzernamen und das Kennwort für den Root-Benutzer ein. Klicken Sie Auf Weiter.
   c. Klicken Sie auf Ja, um das Host-Zertifikat durch ein vom VMware-Zertifikatsserver signiertes Zertifikat zu ersetzen.
   d. Klicken Sie auf der Seite Host Summary auf Next.
   e. Klicken Sie auf das grüne Symbol +, um dem vSphere-Host eine Lizenz hinzuzufügen.
3. Dieser Schritt kann auf Wunsch später abgeschlossen werden.
   a. Klicken Sie auf Weiter, um den Sperrmodus deaktiviert zu lassen.
   b. Klicken Sie auf der Seite VM-Speicherort auf Weiter.
   c. Überprüfen Sie die Seite „bereit für Fertigstellung“. Verwenden Sie die Zurück-Taste, um Änderungen vorzunehmen, oder wählen Sie Fertig stellen.
4. Wiederholen Sie die Schritte 1 und 2 für Cisco UCS Host B.

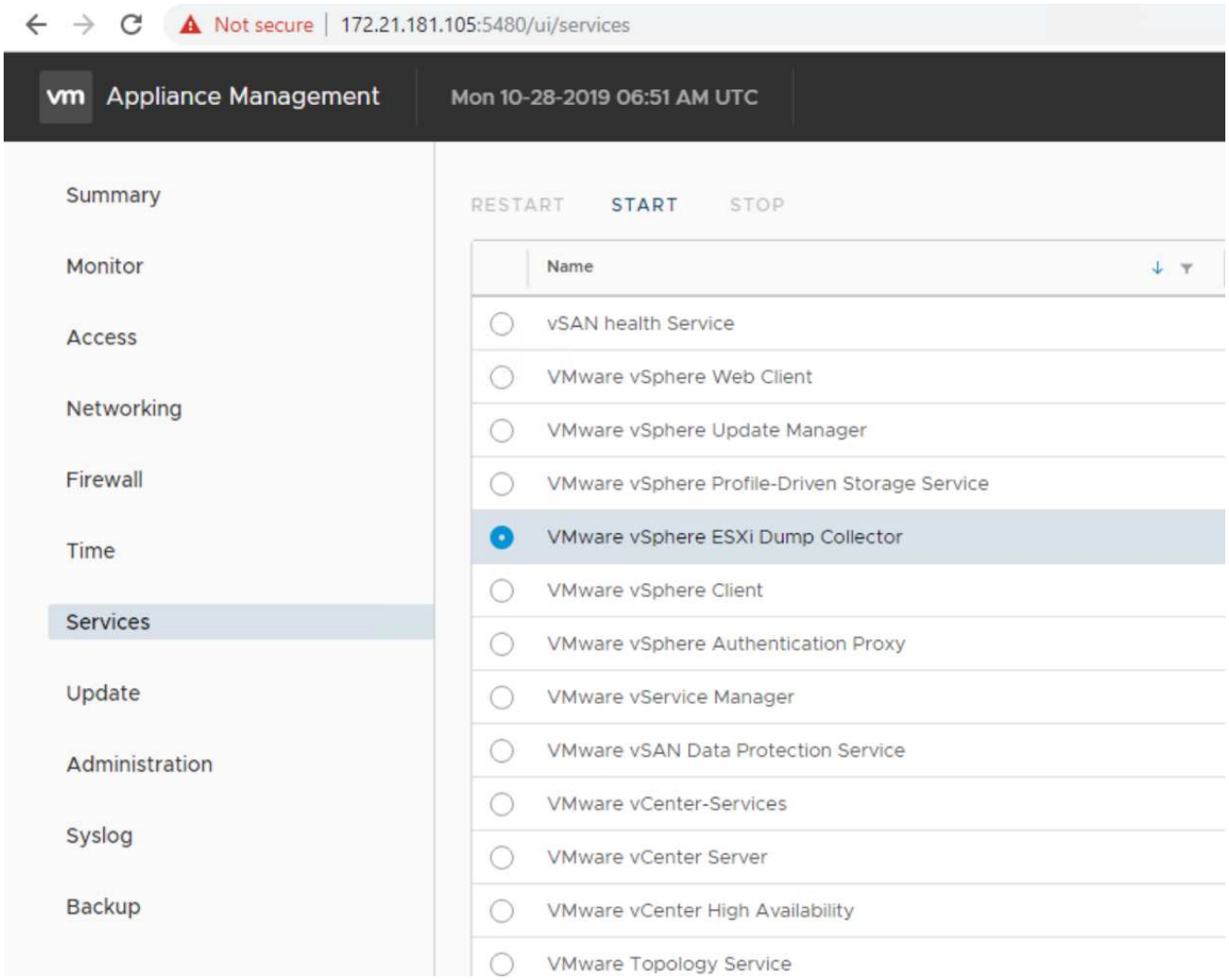
> Dieser Prozess muss für alle zusätzlichen Hosts abgeschlossen werden, die zur Konfiguration von FlexPod Express hinzugefügt werden.

Konfigurieren Sie coredump auf den ESXi-Hosts

Führen Sie die folgenden Schritte aus, um coredump auf den ESXi-Hosts zu konfigurieren:

1. Melden Sie sich bei HTTPS an:// "VCenter" IP:5480/, geben Sie Root für den Benutzernamen ein, und geben Sie das Root-Passwort ein.

2. Klicken Sie auf Services und wählen Sie VMware vSphere ESXI Dump Collector.
3. Starten Sie den VMware vSphere ESXI Dump Collector Service.



4. Stellen Sie mithilfe von SSH eine Verbindung zum Management-IP-ESXi-Host her, geben Sie Root für den Benutzernamen ein und geben Sie das Root-Passwort ein.
5. Führen Sie folgende Befehle aus:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. Die Nachricht `Verified the configured netdump server is running` Wird angezeigt, nachdem Sie den letzten Befehl eingegeben haben.

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

Dieser Prozess muss für alle zusätzlichen, FlexPod Express hinzugefügten Hosts abgeschlossen sein.

`ip_address_of_core_dump_collector` In dieser Validierung befindet sich die vCenter IP.

"Weiter: Implementierungsverfahren für NetApp Virtual Storage Console 9.6."

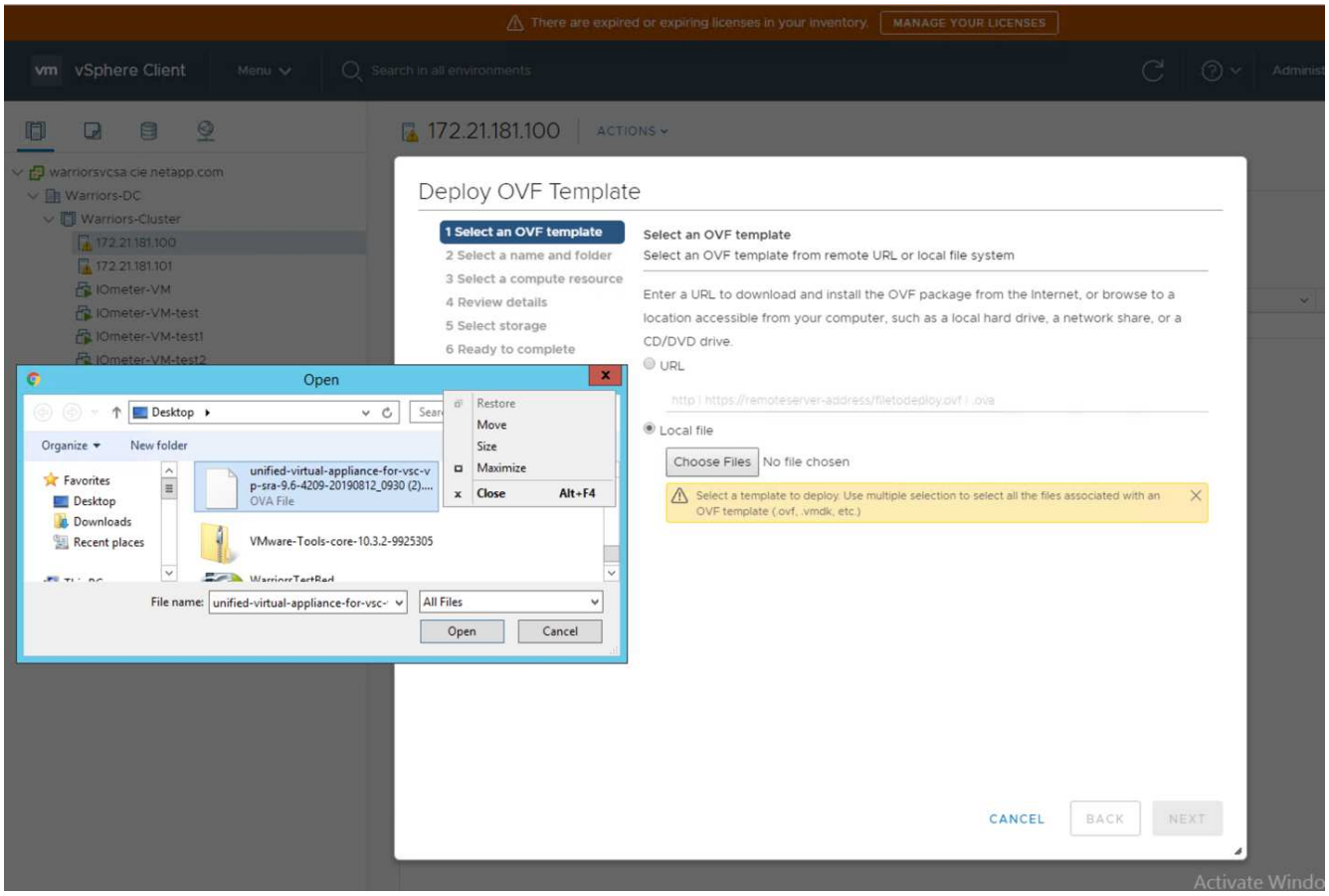
Implementierungsverfahren für NetApp Virtual Storage Console 9.6

Dieser Abschnitt beschreibt die Implementierungsverfahren für die NetApp Virtual Storage Console (VSC).

Installieren Sie Virtual Storage Console 9.6

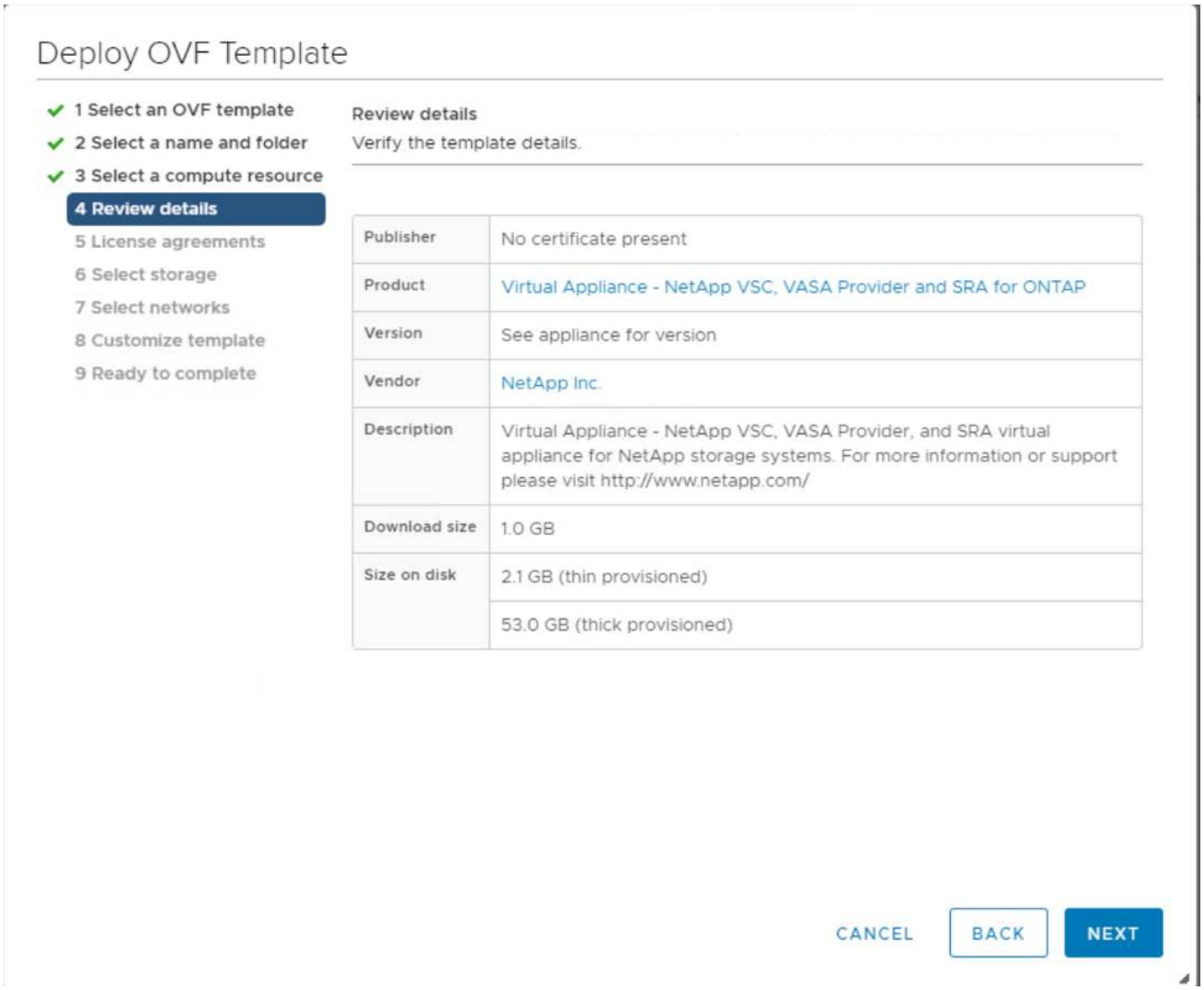
Gehen Sie wie folgt vor, um die VSC 9.6-Software mithilfe einer OVF-Implementierung (Open Virtualization Format) zu installieren:

1. Wechseln Sie zu vSphere Web Client > Host Cluster > Deploy OVF Template.
2. Öffnen Sie die VSC OVF-Datei, die von der NetApp Support-Website heruntergeladen wurde.

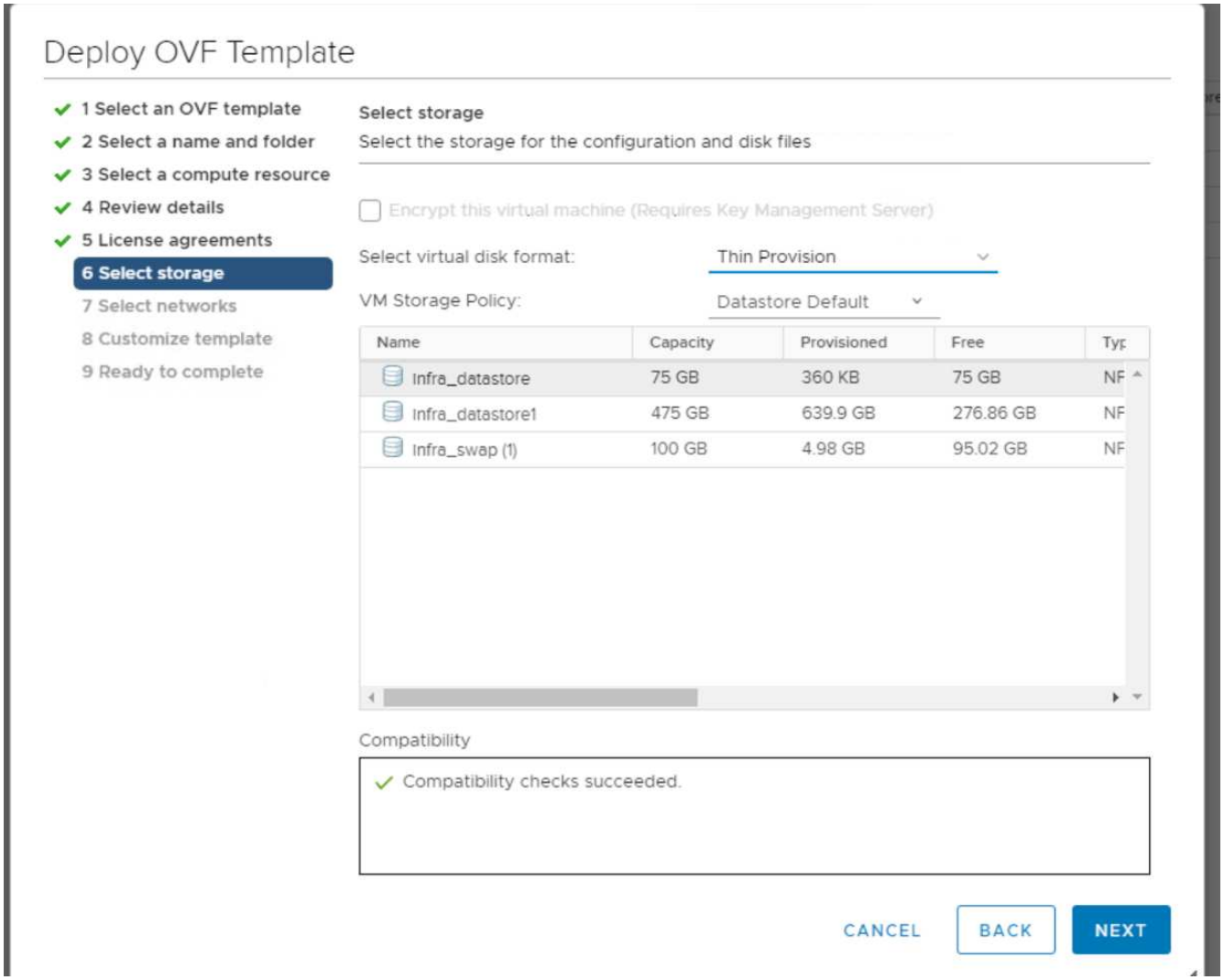


3. Geben Sie den VM-Namen ein, und wählen Sie ein Datacenter oder einen Ordner aus, in dem die Bereitstellung erfolgen soll. Klicken Sie Auf Weiter.

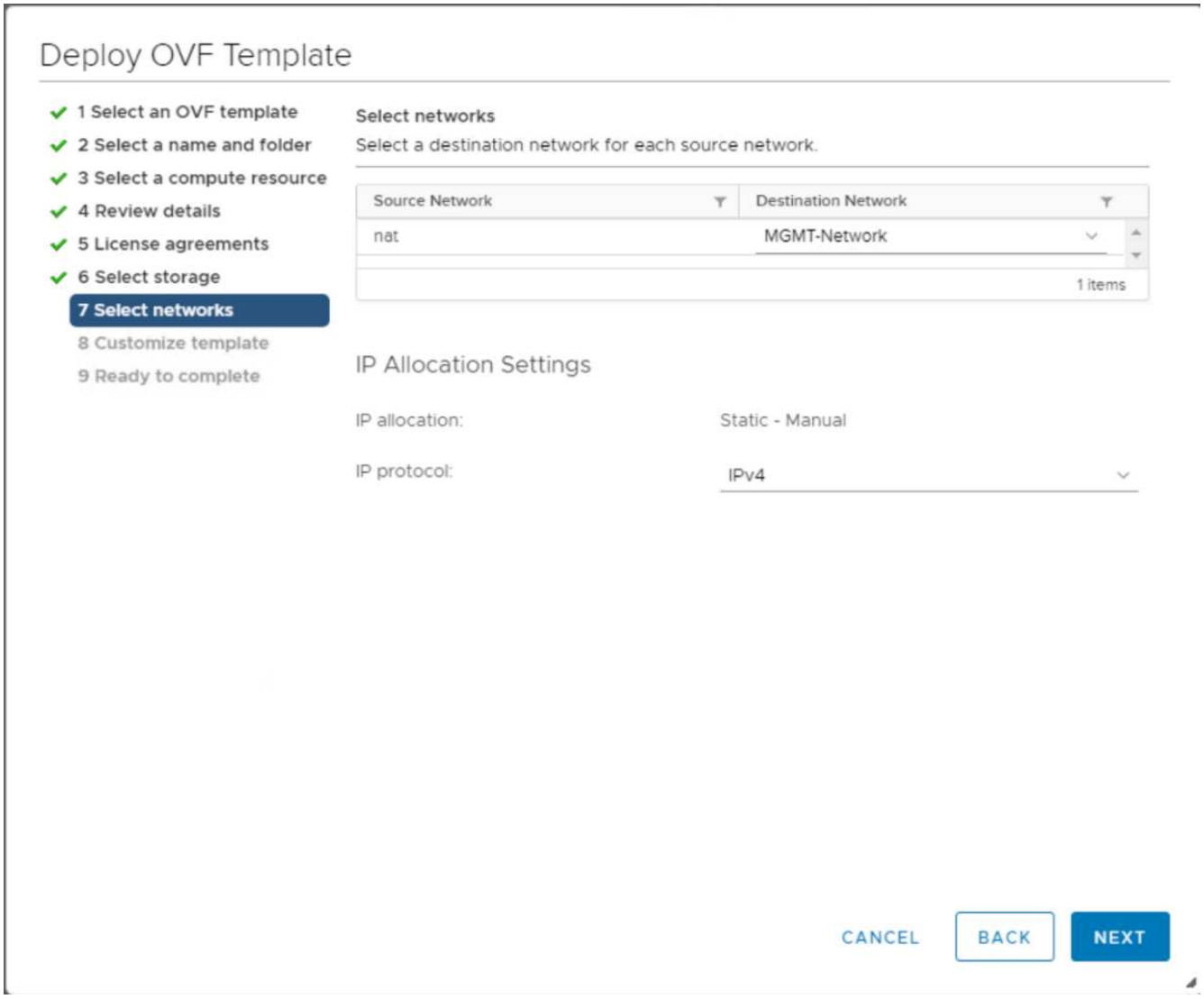
4. Wählen Sie das FlexPod Cluster ESXi Cluster aus und klicken Sie auf Weiter.
5. Überprüfen Sie die Details und klicken Sie auf Weiter.



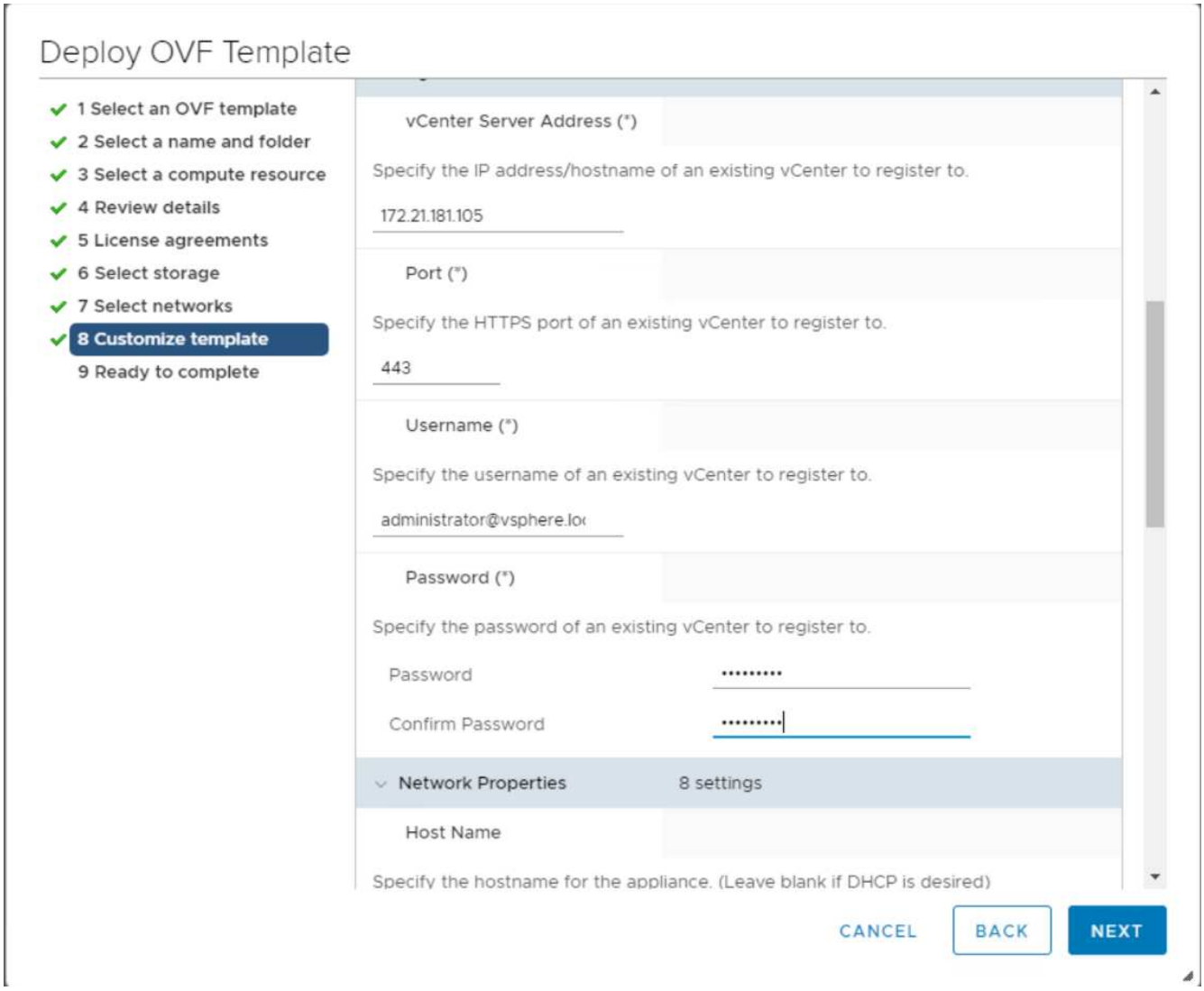
6. Klicken Sie auf Akzeptieren, um die Lizenz zu akzeptieren, und klicken Sie auf Weiter.
7. Wählen Sie das Format der virtuellen Thin Provisioning-Festplatte und einen der NFS-Datenspeicher aus. Klicken Sie Auf Weiter.



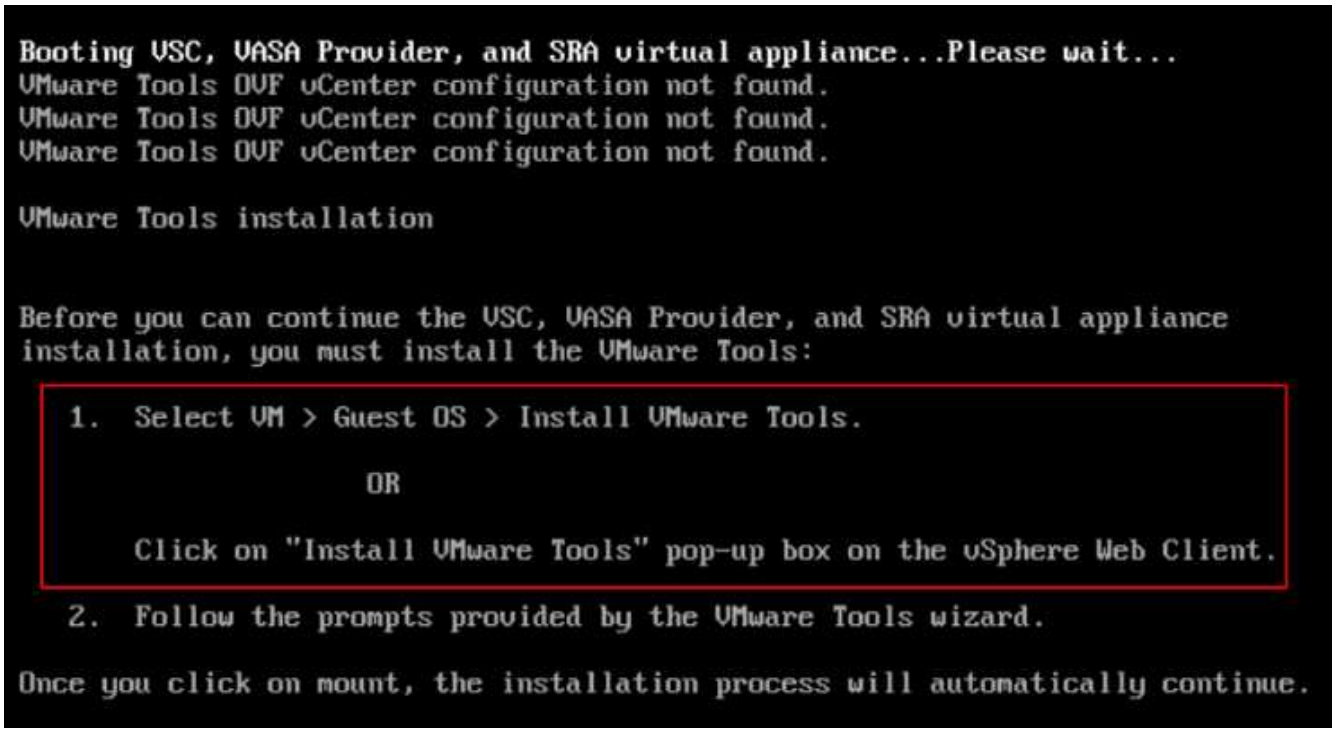
8. Wählen Sie unter Netzwerke auswählen ein Zielnetzwerk aus, und klicken Sie auf Weiter.



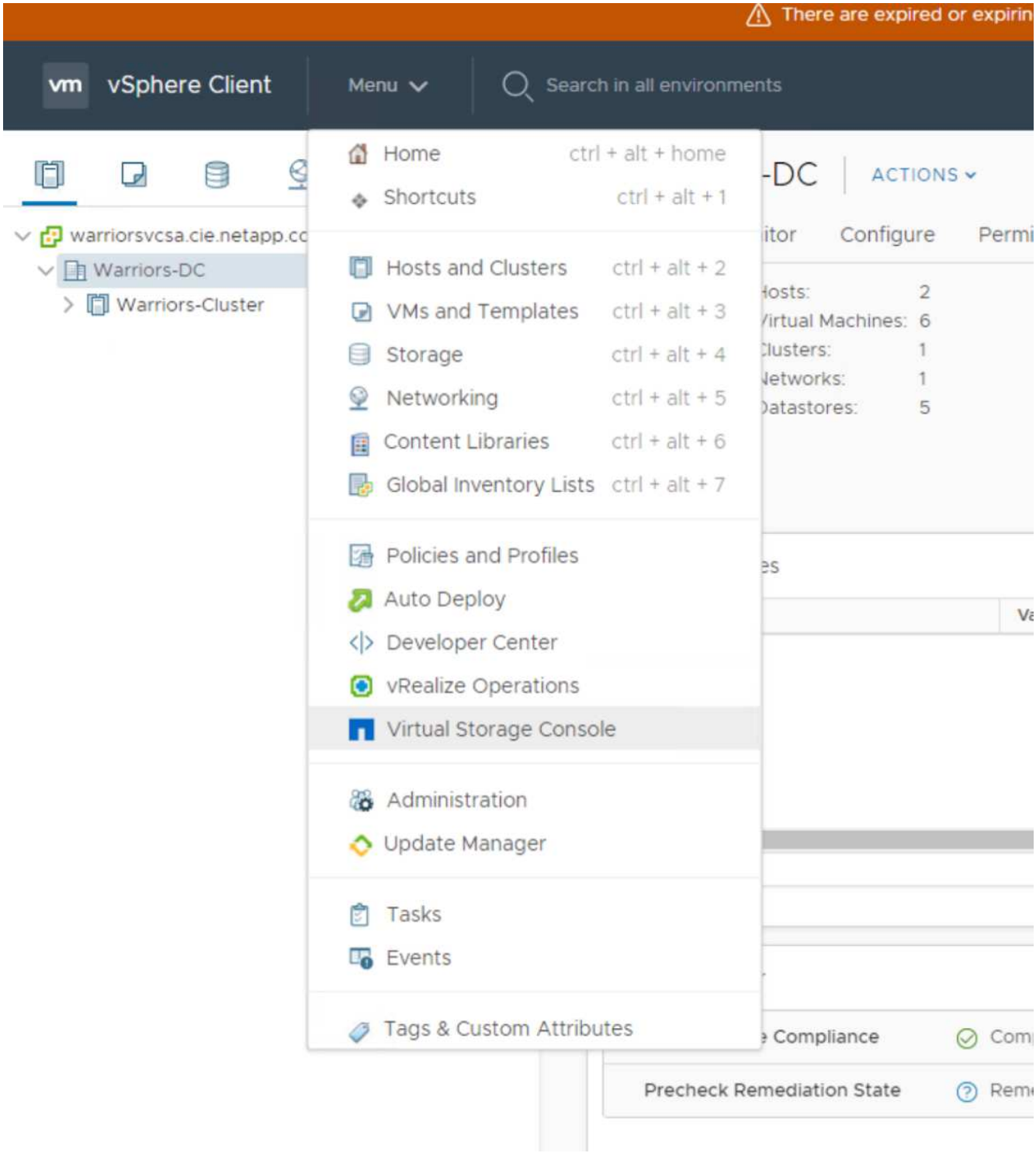
9. Geben Sie in der Vorlage „Anpassen“ das VSC Administratorpasswort, den vCenter-Namen oder die IP-Adresse und andere Konfigurationsdetails ein, und klicken Sie auf „Weiter“.



10. Überprüfen Sie die eingegebenen Konfigurationsdetails und klicken Sie auf „Fertig stellen“, um die Implementierung der NetApp-VSC VM abzuschließen.
11. Schalten Sie die NetApp-VSC VM ein und öffnen Sie die VM-Konsole.
12. Während des Bootens von NetApp-VSC VMs sehen Sie eine Eingabeaufforderung zur Installation von VMware Tools. Wählen Sie in vCenter NetApp-VSC VM > Gastbetriebssystem > VMware Tools installieren aus.



13. Während der Anpassung der OVF-Vorlage wurden Informationen zur Netzwerkkonfiguration und Registrierung für vCenter bereitgestellt. Nach der Ausführung der NetApp-VSC VM sind VSC, vSphere API for Storage Awareness (VASA) und VMware Storage Replication Adapter (SRA) bei vCenter registriert.
14. Melden Sie sich vom vCenter Client ab, und melden Sie sich erneut an. Bestätigen Sie im Home Menü, dass die NetApp VSC installiert ist.



Laden Sie das NetApp NFS VAAI Plug-in herunter und installieren Sie es

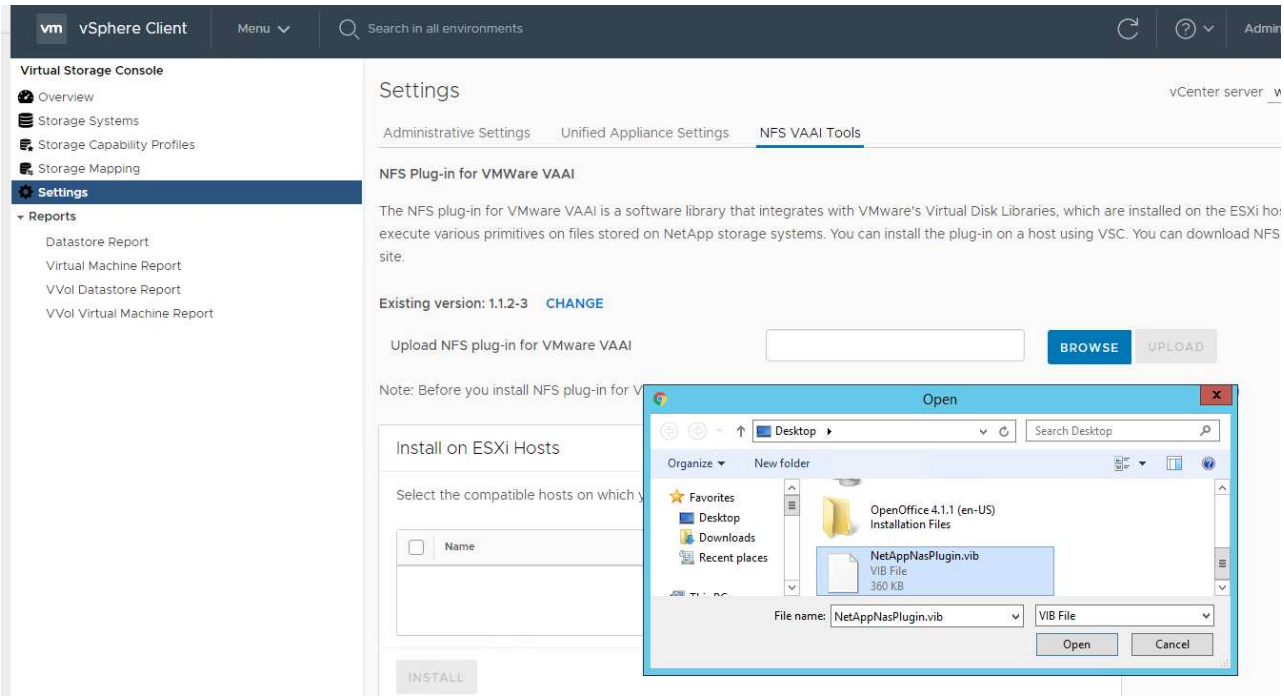
So laden Sie das NetApp NFS VAAI Plug-in herunter und installieren es:

1. Laden Sie das NetApp NFS Plug-in 1.1.2 für VMware herunter `. vib` Datei von der NFS Plugin Download-Seite und speichern Sie sie auf Ihrem lokalen Computer oder Admin-Host.
2. Laden Sie das NetApp NFS Plug-in für VMware VAAI herunter:
   a. Wechseln Sie zum "Software Download Seite".

b. Scrollen Sie nach unten und klicken Sie auf NetApp NFS Plug-in for VMware VAAI.

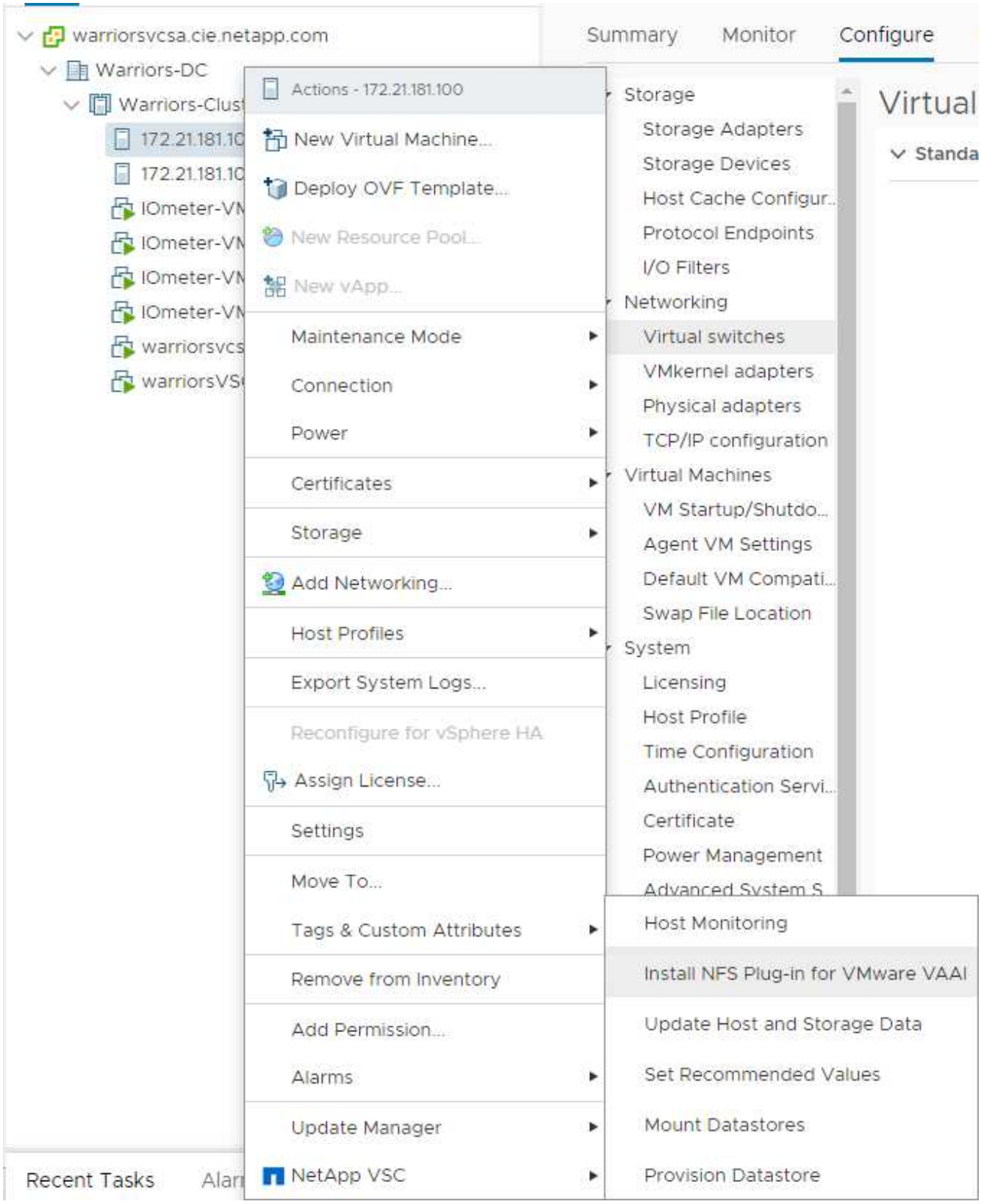
c. Wählen Sie im Startbildschirm des vSphere Web Client die Option Virtual Storage Console aus.

d. Laden Sie unter Virtual Storage Console > Einstellungen > NFS VAAI Tools das NFS-Plug-in hoch, indem Sie die Option Datei auswählen und dort navigieren, wo das heruntergeladene Plug-in gespeichert ist.



3. Klicken Sie auf Hochladen, um das Plug-in nach vCenter zu übertragen.

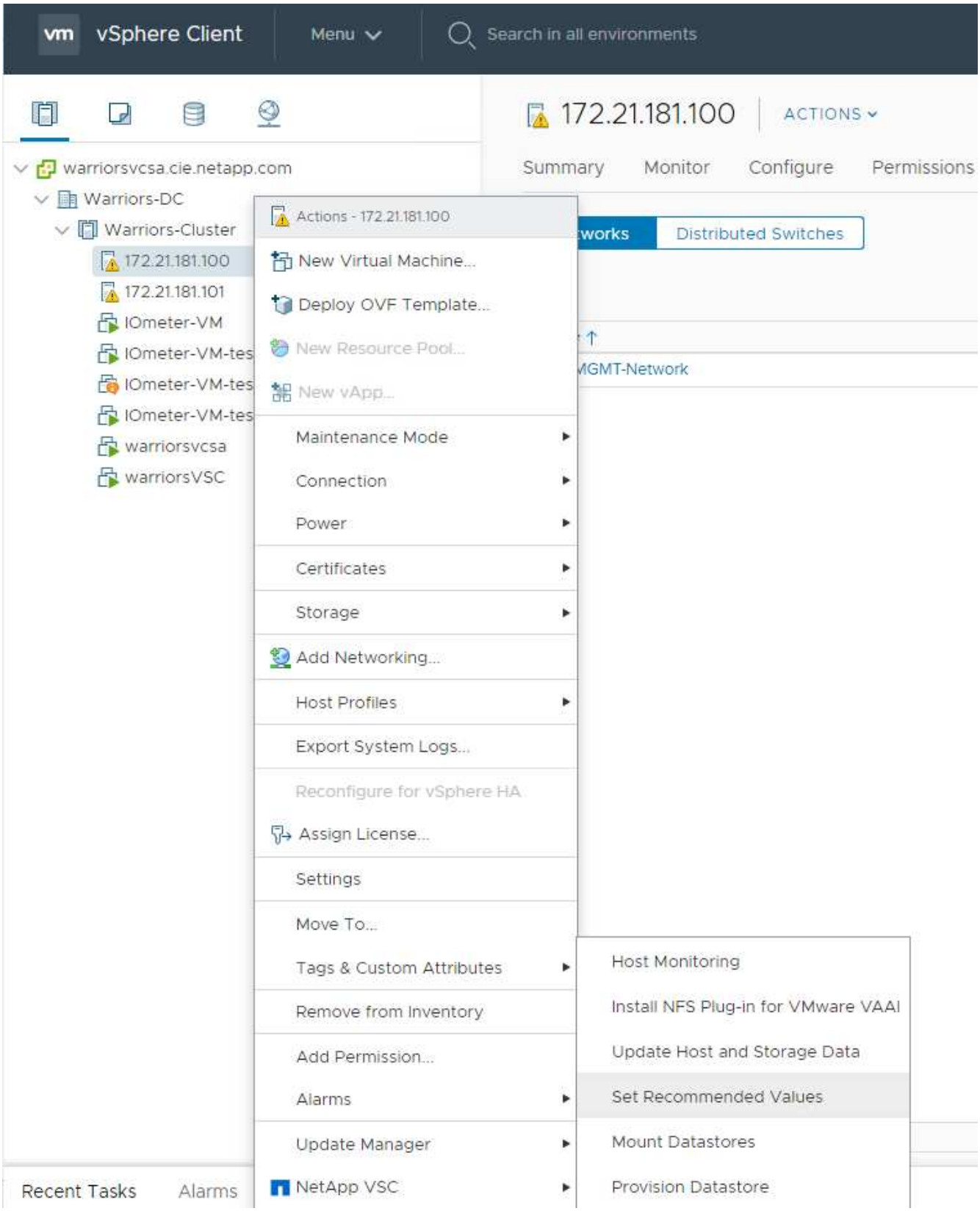
4. Wählen Sie den Host aus, und wählen Sie dann NetApp VSC > NFS-Plug-in für VMware VAAI installieren aus.



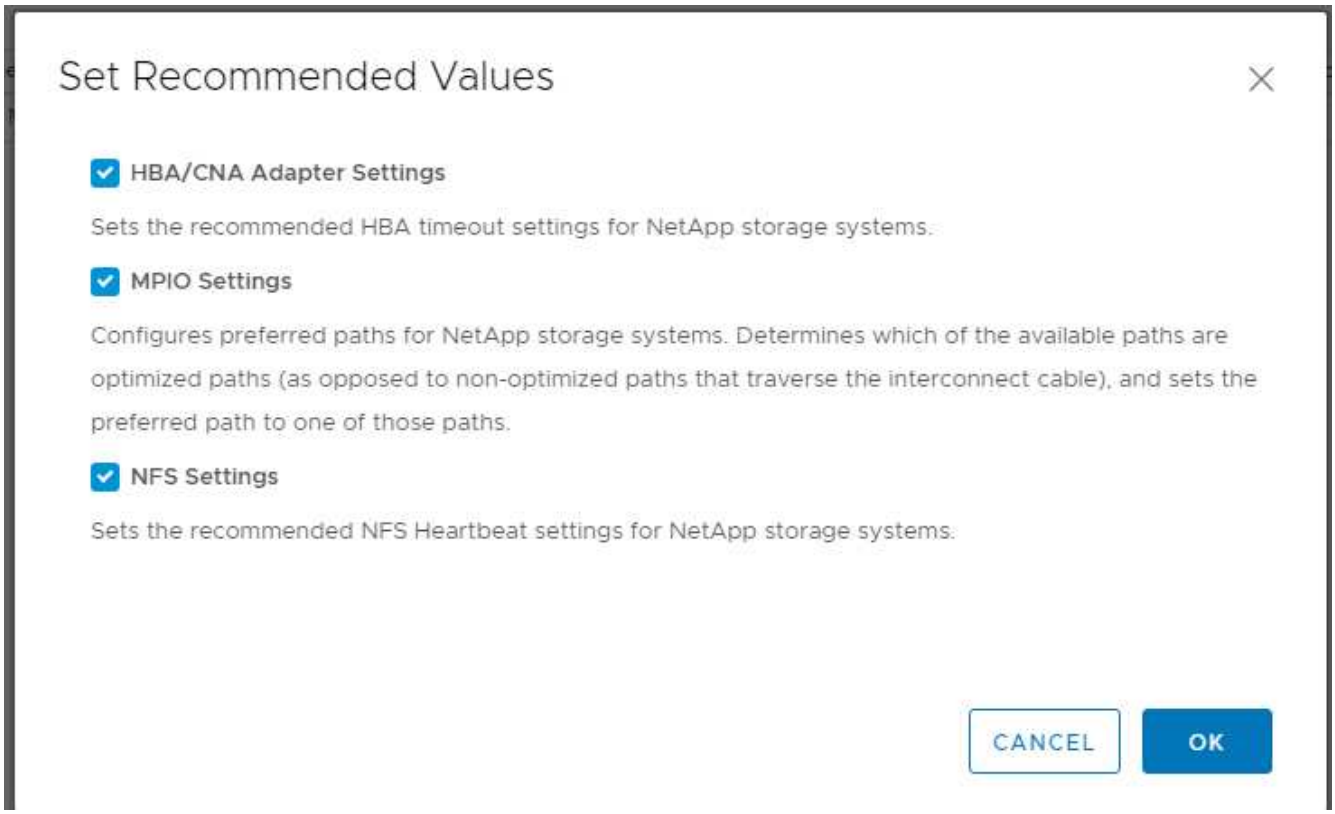
Optimale Speichereinstellungen für die ESXi Hosts verwenden

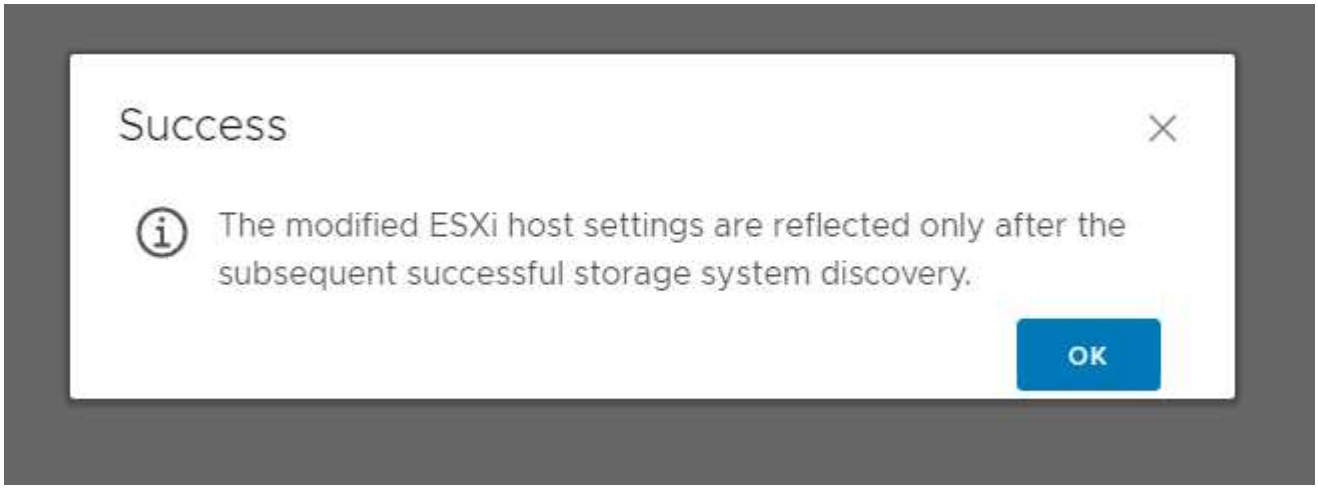
VSC ermöglicht die automatisierte Konfiguration der Storage-Einstellungen für alle ESXi Hosts, die mit NetApp Storage Controllern verbunden sind. Gehen Sie wie folgt vor, um diese Einstellungen zu verwenden:

1. Wählen Sie im Hauptmenü die Option vCenter > Hosts und Clusters aus. Klicken Sie für jeden ESXi Host mit der rechten Maustaste, und wählen Sie NetApp VSC > Empfohlene Werte festlegen aus.



2. Überprüfen Sie die Einstellungen, die Sie auf die ausgewählten vSphere-Hosts anwenden möchten. Klicken Sie auf OK, um die Einstellungen anzuwenden.





3. Starten Sie DEN ESXI-Host neu, nachdem diese Einstellungen angewendet wurden.

Schlussfolgerung

FlexPod Express ist eine einfache und effiziente Lösung und bietet ein validiertes Design mit branchenführenden Komponenten. Durch die Skalierung bis hin zum Hinzufügen von Komponenten kann FlexPod Express gezielt auf spezifische Unternehmensanforderungen zugeschnitten werden. FlexPod Express wurde für kleine bis mittelständische Unternehmen, ROBOs und andere Unternehmen entwickelt, die dedizierte Lösungen benötigen.

Danksagungen

Die Autoren möchten John George für seine Unterstützung und seinen Beitrag zu diesem Design anerkennen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten bzw. auf den folgenden Websites:

NetApp Produktdokumentation

http://docs. "netapp".Com

FlexPod Express with Guide

NVA-1139-DESIGN: FlexPod Express mit Cisco UCS C-Serie und NetApp AFF C190 Serie

"https://www.netapp.com/us/media/nva-1139-design.pdf"

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	November 2019	Erste Version.

Entwurfsleitfaden für FlexPod Express mit Cisco UCS C-Serie und AFF A220 Serie

NVA-1125-DESIGN: FlexPod Express mit Cisco UCS C-Serie und AFF A220 Serie

Savita Kumari, NetApp in Partnerschaft mit:

Aktuell stellen immer mehr Unternehmen ihre Rechenzentren auf eine Shared IT Infrastructure und Cloud Computing um. Außerdem wünschen sich Unternehmen eine einfache und effektive Lösung für Remote-Standorte und Zweigstellen, die ihnen die Technologie nutzt, die sie mit ihrem Datacenter vertraut sind.

FlexPod Express ist eine vorkonfigurierte Datacenter-Architektur mit Best Practices, die auf Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switch-Produktfamilie und NetApp AFF basiert. Die Komponenten von FlexPod Express sind wie ihre Kollegen aus dem FlexPod Datacenter, die Managementsynergien über die komplette IT-Infrastrukturumgebung hinweg in geringerem Umfang ermöglichen. FlexPod Datacenter und FlexPod Express sind optimale Plattformen für die Virtualisierung sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads.

"Weiter: Programmübersicht."

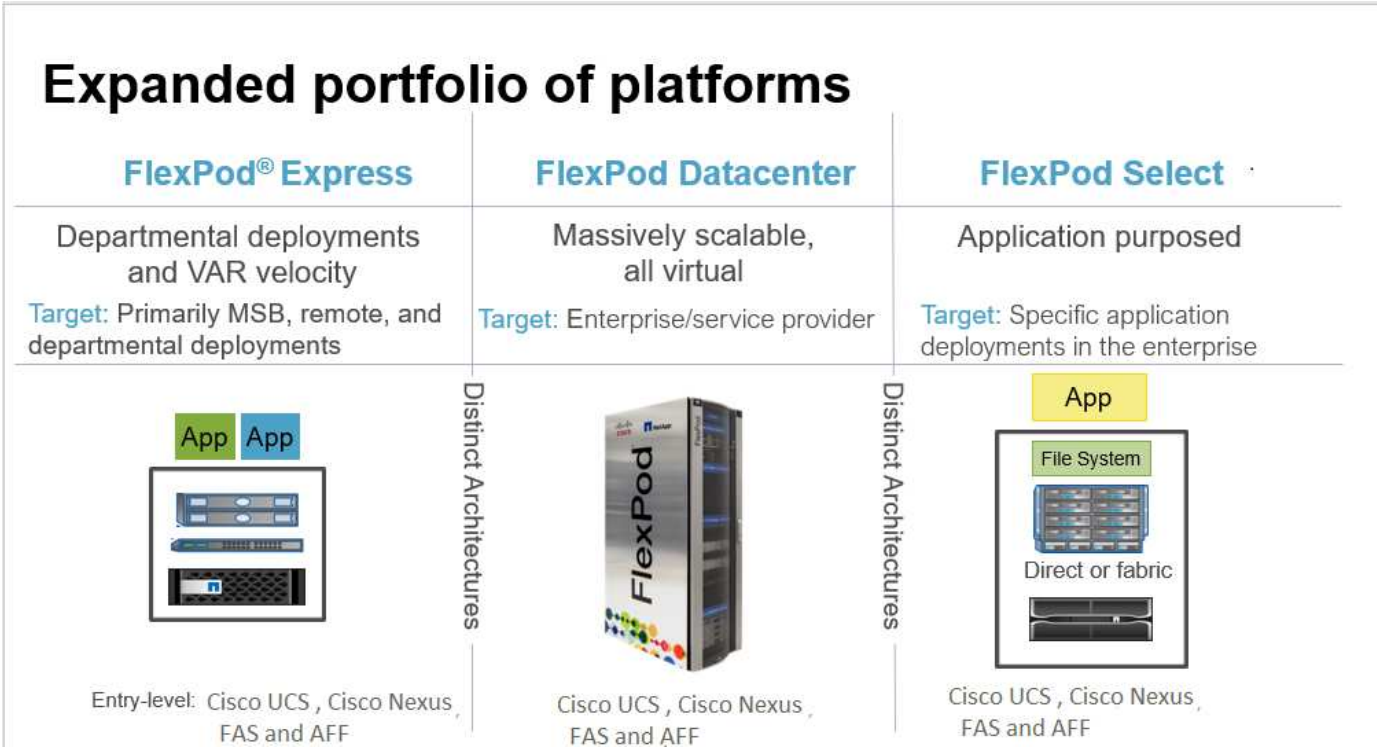
Programmzusammenfassung

FlexPod Portfolio für konvergente Infrastrukturen

FlexPod Referenzarchitekturen werden als Cisco Validated Designs (CVDs) oder als NetApp Verified Architectures (NVAs) bereitgestellt. Abweichungen, die auf den Anforderungen des Kunden von einem bestimmten CVD oder NVA basieren, sind zulässig, wenn Variationen nicht zur Implementierung von nicht unterstützten Konfigurationen führen.

Wie in der folgenden Abbildung dargestellt, umfasst das FlexPod Portfolio drei Lösungen: FlexPod Express, FlexPod Datacenter und FlexPod Select:

- **FlexPod Express.** bietet eine Einstiegslösung, die aus Technologien von Cisco und NetApp besteht.
- **FlexPod Datacenter.** bietet eine optimale Mehrzweckgrundlage für verschiedene Workloads und Anwendungen.
- **FlexPod Select.** integriert die besten Aspekte des FlexPod-Rechenzentrums und stimmt die Infrastruktur auf eine bestimmte Anwendung ab.



NetApp Verified Architecture-Programm

Das NVA-Programm bietet Kunden eine verifizierte Architektur für NetApp Lösungen an. Eine NVA bedeutet, dass die NetApp Lösung folgende Eigenschaften hat:

- Sorgfältig getestet
- Präskriptiv
- Minimale Risiken bei der Implementierung
- Schnellere Produkteinführungszeiten

Dieser Leitfaden beschreibt das Design von FlexPod Express mit VMware vSphere. Darüber hinaus nutzt

dieses Design das brandneue AFF A220 System, auf dem NetApp ONTAP 9.4 Software, Cisco Nexus 3172P Switches und Cisco UCS C220 M5 Server als Hypervisor-Nodes ausgeführt werden.

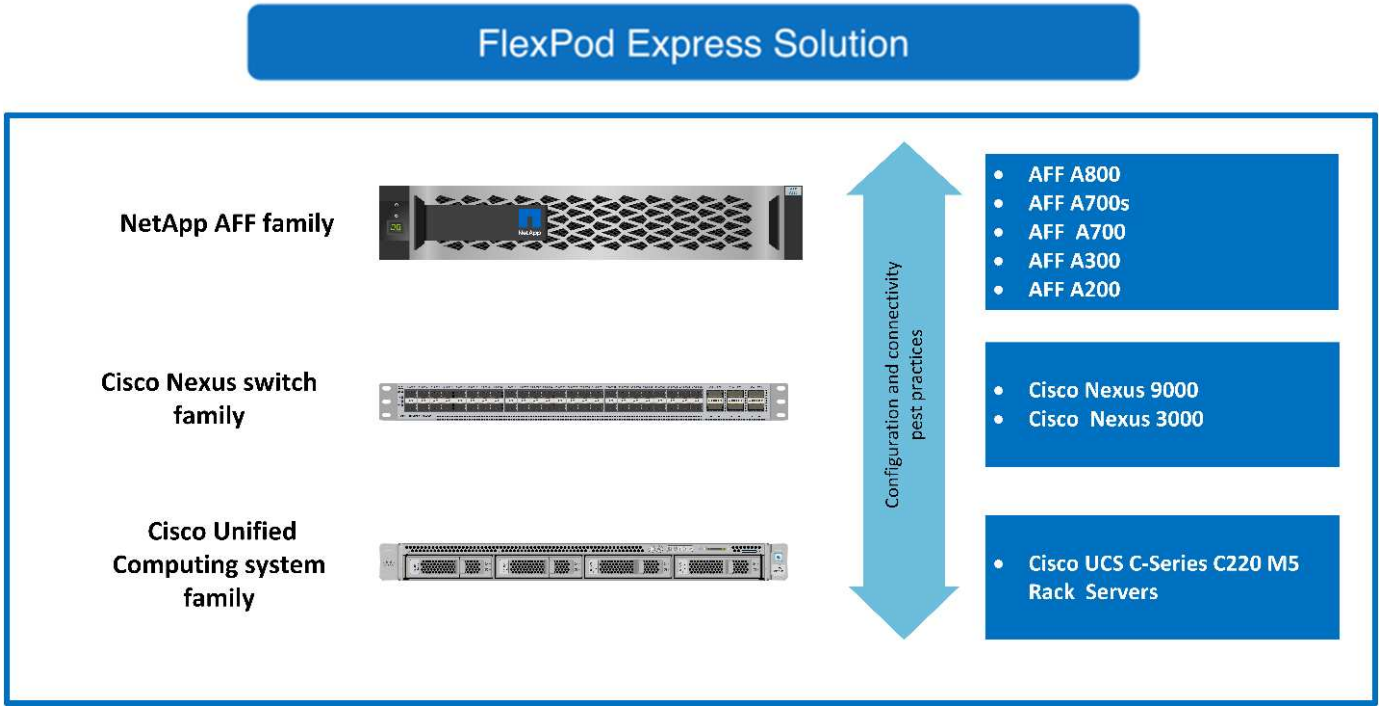
Dieses Dokument ist zwar für AFF A220 validiert, unterstützt aber auch die FAS2700.

"Weiter: Lösungsübersicht."

Lösungsüberblick

FlexPod Express wurde für gemischte Virtualisierungs-Workloads entwickelt. Sie richtet sich an Remote-Standorte und Zweigniederlassungen sowie an kleine und mittelständische Unternehmen. Für größere Unternehmen, die eine dedizierte Lösung für einen bestimmten Zweck implementieren möchten, ist dies optimal. Diese neue Lösung für FlexPod Express fügt neue Technologien wie NetApp ONTAP 9.4, NetApp AFF A220 und VMware vSphere 6.7 hinzu.

In der folgenden Abbildung sind die Hardwarekomponenten aufgeführt, die in der FlexPod Express Lösung enthalten sind.



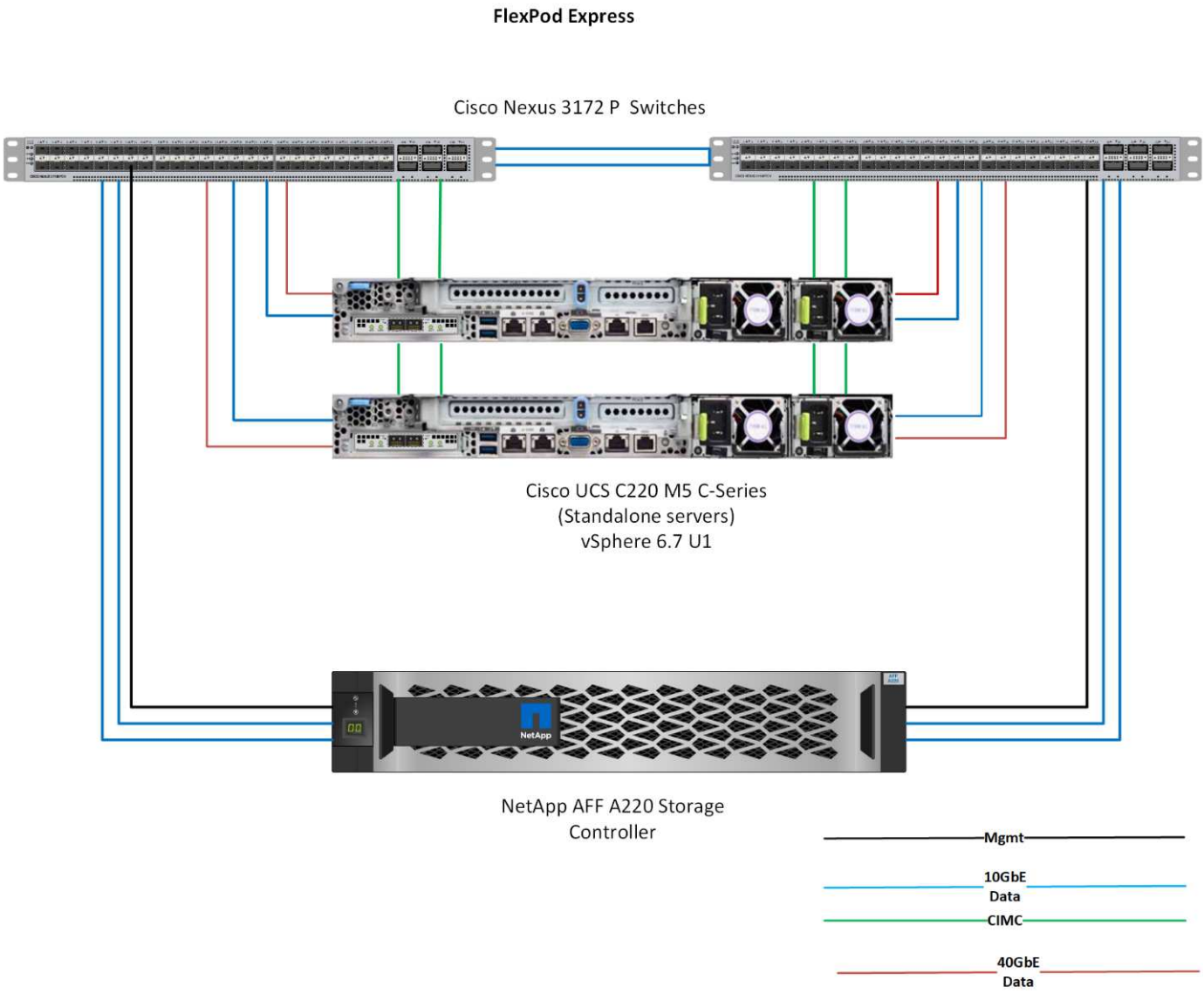
Zielgruppe

Dieses Dokument richtet sich an all jene, die die Vorteile einer Infrastruktur nutzen möchten, die eine effiziente IT liefert und IT-Innovationen unterstützt. Dieses Dokument richtet sich an Vertriebsmitarbeiter, Berater im Außendienst, Professional Services-Mitarbeiter, IT-Manager, Techniker des Partners und Kunden.

Lösungstechnologie

Diese Lösung nutzt die neuesten Technologien von NetApp, Cisco und VMware. Diese Lösung umfasst das neue NetApp AFF A220 System, auf dem ONTAP 9.4 Software, zwei Cisco Nexus 3172P Switches und Cisco UCS C220 M5 Rack Server mit VMware vSphere 6.7 ausgeführt werden. Die validierte Lösung nutzt 10-Gigabit Ethernet (10GbE)-Technologie. Die folgende Abbildung zeigt eine Übersicht. Beratung wird auch zur

Skalierung durch Hinzufügen von zwei Hypervisor-Knoten zu einem Zeitpunkt, so dass die FlexPod Express-Architektur kann sich an die sich entwickelnden geschäftlichen Anforderungen eines Unternehmens anpassen.



40 GbE ist nicht validiert, wird aber von einer unterstützten Infrastruktur unterstützt.

"Next: Technologieanforderungen."

Technologieanforderungen erfüllt

Für FlexPod Express sind eine Kombination aus Hardware- und Softwarekomponenten erforderlich, die vom ausgewählten Hypervisor und von der Netzwerkgeschwindigkeit abhängig sind. Darüber hinaus enthält FlexPod Express die Hardwarekomponenten, die erforderlich sind, um dem System in Einheiten von zwei Hypervisor-Nodes hinzuzufügen.

Hardwareanforderungen

Unabhängig vom ausgewählten Hypervisor nutzen alle FlexPod Express Konfigurationen dieselbe Hardware. Daher kann auch bei sich ändernden Geschäftsanforderungen jeder Hypervisor auf derselben FlexPod

Express Hardware ausgeführt werden.

In der folgenden Tabelle werden die Hardwarekomponenten aufgeführt, die für alle FlexPod Express Konfigurationen und 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
AFF A220 2-Node-Cluster	1
Cisco UCS C220 M5 Server	2
Cisco Nexus 3172P-Switch	2
Cisco UCS Virtual Interface Card (VIC) 1387 für Cisco UCS C220 M5 Rack Server	2
Cisco CVR-QSFP-SFP10G Adapter	4

Softwareanforderungen

In den folgenden Tabellen werden die Softwarekomponenten aufgeführt, die für die Implementierung der Architekturen der FlexPod Express Lösung erforderlich sind.

In der folgenden Tabelle sind die Softwareanforderungen für die grundlegende FlexPod Express Implementierung aufgeführt.

Software	Version	Details
Cisco Integrated Management Controller (CIMC)	3.1.3	Für C220 M5 Rack Server
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Für Cisco Nexus 3172P-Switches
NetApp ONTAP	9.4	Für AFF A220 Controller

In der folgenden Tabelle ist die erforderliche Software für alle VMware vSphere Implementierungen auf FlexPod Express aufgeführt.

Software	Version
VMware vCenter Server Appliance	6.7
VMware vSphere ESXi	6.7
NetApp VAAI Plug-in für ESXi	1.1.2

"Als Nächstes: Design-Entscheidungen."

Designs

Während der Architektur dieses Designs wurden folgende Technologien ausgewählt. Jede Technologie erfüllt einen bestimmten Zweck in der FlexPod Express Infrastrukturlösung.

NetApp AFF A220 Serie mit ONTAP 9.4

Bei dieser Lösung werden zwei der neuesten NetApp Produkte genutzt: Die Software NetApp AFF A220 und ONTAP 9.4.

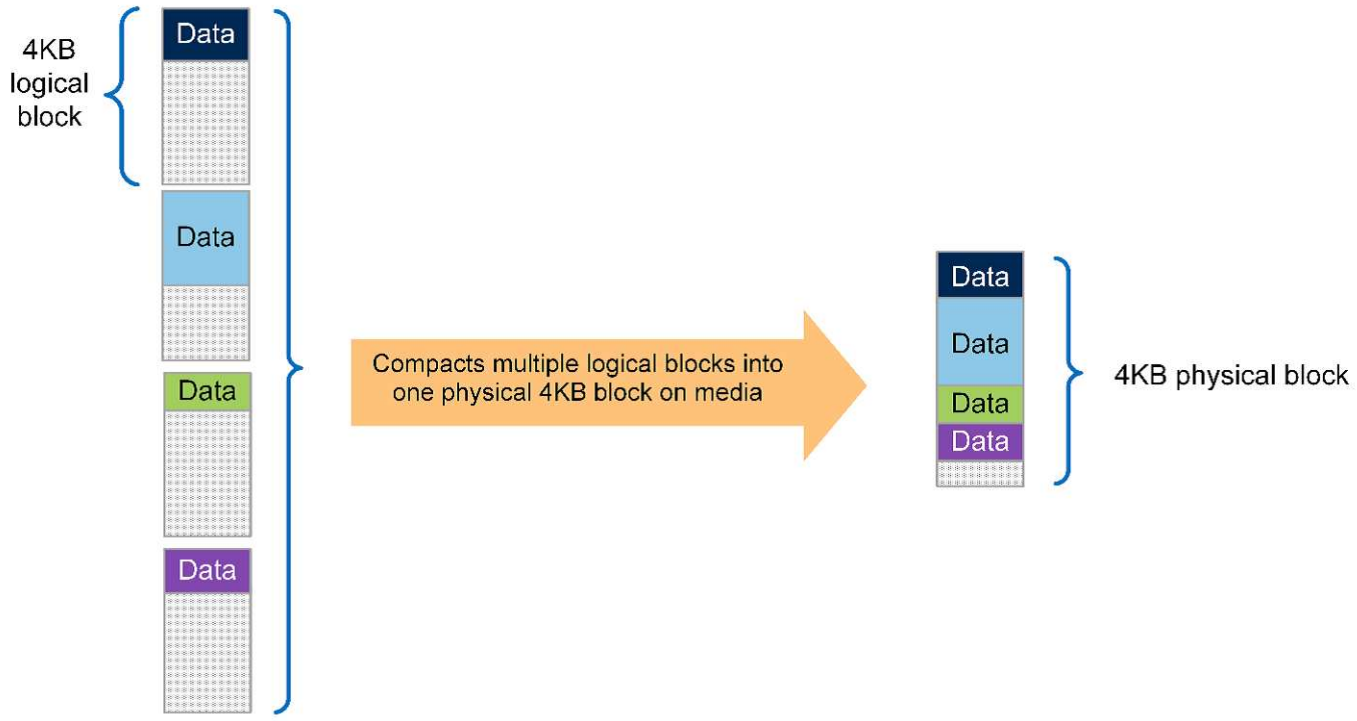
AFF A220 System

Weitere Informationen zum AFF A220 Hardwaresystem finden Sie unter "AFF A-Series Homepage".

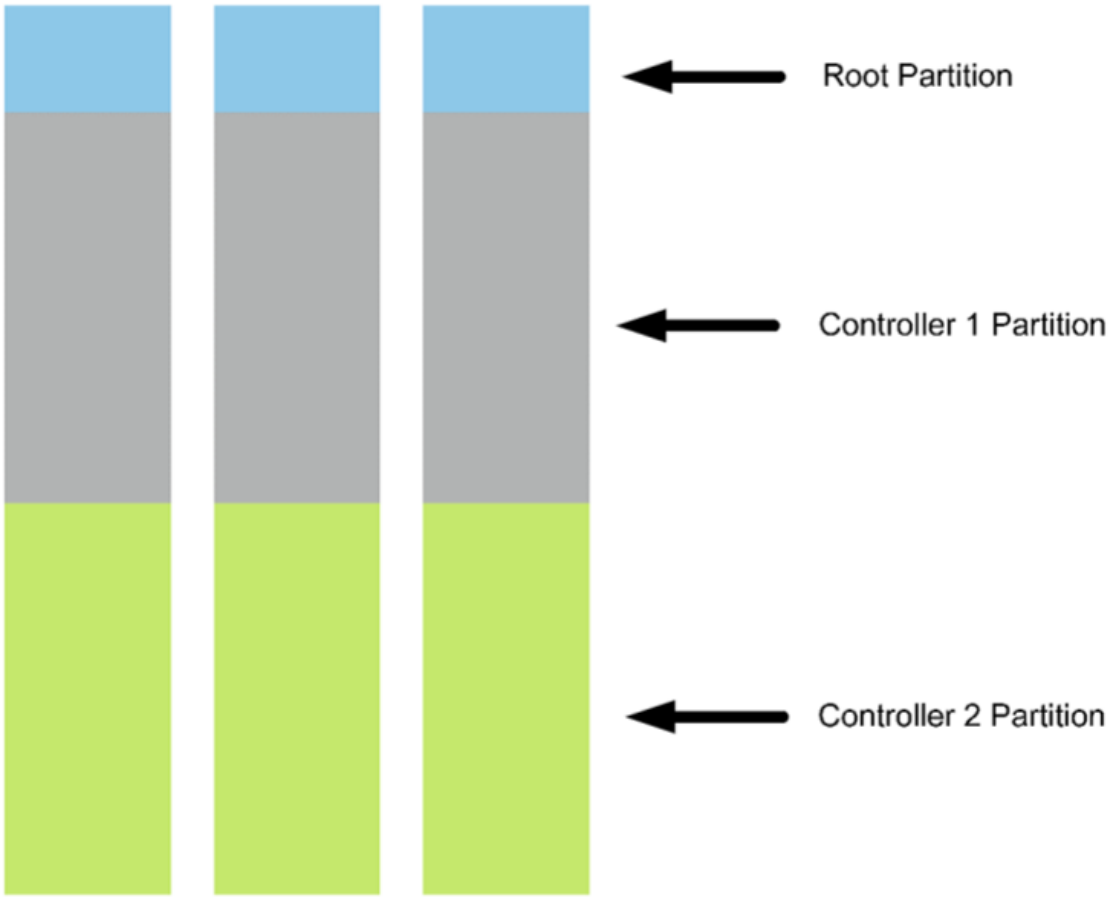
ONTAP 9.4 Software

NetApp AFF A220 Systeme verwenden die neue Software ONTAP 9.4. ONTAP 9.4 ist die branchenweit führende Datenmanagement-Software der Enterprise-Klasse. Sie vereint ein neues Maß an Anwenderfreundlichkeit und Flexibilität mit leistungsfähigen Datenmanagement-Funktionen, Storage-Effizienzfunktionen und erstklassiger Cloud-Integration.

ONTAP 9.4 bietet verschiedene Funktionen, die sich gut für FlexPod Express eignen. In erster Linie ist das Engagement von NetApp für Storage-Effizienz, die eines der wichtigsten Funktionen für kleine Implementierungen sein kann. Die brandneuen NetApp Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und Thin Provisioning sind in ONTAP 9.4 mit Data-Compaction verfügbar. Da das NetApp WAFL System immer 4-KB-Blöcke schreibt, werden in der Data-Compaction mehrere Blöcke in einem 4-KB-Block kombiniert, wenn die Datenblöcke nicht den zugewiesenen Speicherplatz von 4 KB nutzen. Dieser Prozess wird in der folgenden Abbildung dargestellt.



Zudem kann die Root-Daten-Partitionierung auf dem AFF A220 System verwendet werden. Diese Partitionierung ermöglicht das Root-Aggregat und zwei Datenaggregate, die auf die Festplatten im System verteilt werden können. Daher können beide Controller in einem AFF A220 Cluster mit zwei Nodes die Performance aller Festplatten im Aggregat nutzen. Siehe folgende Abbildung.



Diese nur einige der Kernfunktionen, die die FlexPod Express Lösung ergänzen. Weitere Informationen zu den zusätzlichen Funktionen von ONTAP 9.4 finden Sie im "ONTAP 9 Datenmanagement-Software – Datenblatt". Siehe auch die NetApp "ONTAP 9 Dokumentationszentrum" , die aktualisiert wurde, um ONTAP 9.4 zu enthalten.

Cisco Nexus 3000 Serie

Der Cisco Nexus 3172P ist ein robuster, kostengünstiger Switch mit 1/10/40/100-Gbit/s-Switches. Der Cisco Nexus 3172PQ Switch, einer Komponente der Unified Fabric Familie, ist ein kompakter 1-Rack-Switch (1 HE) für Datacenter-Implementierungen der Top-of-Rack-Einheiten. (Siehe folgende Abbildung.) Sie bietet bis zu 72 1/10-GbE-Ports in 1 HE oder 48 1/10 GbE und sechs 40-GbE-Ports in 1 HE. Und für maximale Flexibilität der physischen Schicht unterstützt sie auch 1/10/40 Gbit/s.

Da alle Modelle der Cisco Nexus Serie auf demselben zugrunde liegenden Betriebssystem ausgeführt werden, werden NX-OS, mehrere Cisco Nexus Modelle in den FlexPod Express und FlexPod Datacenter Lösungen unterstützt.

Leistungsspezifikationen umfassen:

- Durchsatz des Linienverkehrs (beide Ebenen 2 und 3) auf allen Ports
- Konfigurierbare Maximum Transmission Units (MTUs) mit bis zu 9216 Bytes (Jumbo Frames)

Weitere Informationen zu Cisco Nexus 3172-Switches finden Sie im "Datenblatt zu den Cisco Nexus 3172PQ-, 3172TQ-, 3172TQ-32T-, 3172PQ-XL- und 3172TQ-XL-Switches".

Cisco UCS C-Serie

Der Rack Server der Cisco UCS C-Serie wurde für FlexPod Express ausgewählt, da er dank der vielen Konfigurationsoptionen an spezifische Anforderungen einer FlexPod Express Implementierung angepasst werden kann.

Die Rack-Server der Cisco UCS C-Serie bieten Unified Computing in einem branchenüblichen Formfaktor zur Senkung der TCO und Steigerung der Flexibilität.

Die Rack-Server der Cisco UCS C-Serie bieten folgende Vorteile:

- Formfaktor-unabhängiger Einstieg in Cisco UCS
- Vereinfachte und schnelle Implementierung von Applikationen
- Erweiterung der Innovationen im Unified Computing und der Vorteile für Rack-Server
- Bessere Auswahl für Kunden mit einzigartigen Vorteilen in einem vertrauten Rack-Paket

Der Cisco UCS C220 M5 Rack Server (in der vorherigen Abbildung) gehört zu den vielseitigsten Universal-Enterprise-Infrastrukturen und -Applikations-Servern der Branche. Dieser 2-Socket-Rack-Server mit hoher Dichte bietet herausragende Performance und Effizienz für eine Vielzahl an Workloads, einschließlich Virtualisierung, Zusammenarbeit und Bare Metal-Applikationen. Cisco UCS Rack Server der C-Serie können als Standalone-Server oder als Teil des Cisco UCS bereitgestellt werden, um die standardbasierten Unified Computing-Innovationen von Cisco zu nutzen, die zur Senkung der Gesamtbetriebskosten von Kunden und zur Steigerung ihrer geschäftlichen Flexibilität beitragen.

Weitere Informationen zu C220 M5 Servern finden Sie im "Cisco UCS C220 M5 Rack Server – Datenblatt".

Konnektivitätsoptionen für C220 M5 Rack Server

Die Konnektivitätsoptionen für die C220 M5 Rack Server lauten wie folgt:

- **Cisco UCS VIC 1387**

  Der Cisco UCS VIC 1387 (in der folgenden Abbildung) bietet erweitertes Dual-Port QSFP+ 40 GbE und FC over Ethernet (FCoE) in einem Formfaktor mit modularem LAN-on-Motherboard (mLOM). Der mLOM-Steckplatz kann verwendet werden, um einen Cisco VIC zu installieren, ohne einen PCIe-Steckplatz

(Peripheral Component Interconnect Express) zu verwenden, wodurch eine größere I/O-Erweiterbarkeit möglich ist.

Weitere Informationen zum Cisco UCS VIC 1387-Adapter finden Sie im "Cisco UCS Virtual Interface Card 1387" Datenblatt.

- **CVR-QSFP-SFP10G ADAPTER**

  Das Cisco QSA Modul wandelt einen QSFP-Port in einen SFP- oder SFP+-Port um. Mit diesem Adapter können Kunden flexibel jedes SFP+- oder SFP-Modul oder Kabel verwenden, um eine Verbindung zu einem Port mit niedrigerer Geschwindigkeit am anderen Ende des Netzwerks herzustellen. Diese Flexibilität ermöglicht eine kostengünstige Transition zu 40 GbE durch maximale Nutzung von hochdichten 40-GbE QSFP-Plattformen. Dieser Adapter unterstützt alle SFP+-Optiken und KabelReichweiten und unterstützt mehrere 1GbE-SFP-Module. Da dieses Projekt mithilfe von 10GbE Konnektivität validiert wurde und der verwendete VIC 1387 40GbE ist, wird der CVR-QSFP-SFP10G Adapter (in der folgenden Abbildung) für die Konvertierung verwendet.

VMware vSphere 6.7

VMware vSphere 6.7 ist eine Hypervisor-Option zur Verwendung mit FlexPod Express. Mit VMware vSphere können Unternehmen ihren Strom- und Kühlungsbedarf senken und gleichzeitig die erworbene Computing-Kapazität vollständig nutzen. VMware vSphere ermöglicht außerdem den Schutz vor Hardware-Ausfällen

(VMware High Availability, oder VMware HA) und den Lastausgleich von Ressourcen über einen Cluster von vSphere Hosts (VMware Distributed Resource Scheduler oder VMware DRS).

Da es nur den Kernel neu startet, ermöglicht VMware vSphere 6.7 Kunden den „schnellen Start“, wo es vSphere ESXi lädt, ohne die Hardware neu zu starten. Diese Funktion ist nur für Plattformen und Treiber auf der Quick Boot Whitelist verfügbar. VSphere 6.7 erweitert die Funktionen des vSphere Client. Dieser kann etwa 90 % der Funktionen des vSphere Web Client nutzen.

In vSphere 6.7 hat VMware diese Funktion erweitert, damit Kunden Enhanced vMotion Compatibility (EVC) nicht pro Virtual Machine (VM), sondern nicht pro Host-Basis festlegen können. In vSphere 6.7 hat VMware auch die APIs offengelegt, die zur Erstellung sofortiger Klone verwendet werden können.

Einige Funktionen von vSphere 6.7 U1:

- Voll ausgestattete HTML5 Web-basierte vSphere Client
- VMotion für NVIDIA GRID vGPU-VMs Unterstützung für Intel FPGA.
- VCenter Server Converge Tool für den Wechsel von externen PCs zu internen PCS
- Verbesserungen für vSAN (HCI Updates):
- Erweiterte Content-Bibliothek.

Weitere Informationen zu vSphere 6.7 U1 finden Sie unter "Was ist neu in vCenter Server 6.7 Update 1". Obwohl diese Lösung mit vSphere 6.7 validiert wurde, unterstützt sie jede vSphere Version, die für die anderen Komponenten durch das NetApp Interoperabilitäts-Matrix-Tool qualifiziert ist. NetApp empfiehlt die Implementierung von vSphere 6.7U1 für seine Fixes und erweiterten Funktionen.

Boot-Architektur

Es werden die folgenden Optionen für die Boot-Architektur von FlexPod Express unterstützt:

- ISCSI SAN LUN
- Cisco FlexFlash SD-Karte
- Lokale Festplatte

Da FlexPod Datacenter über iSCSI LUNs gestartet wird, wird die Lösungsverwaltung durch iSCSI Boot für FlexPod Express verbessert.

"Als Nächstes: Lösungsüberprüfung."

Verifizierung der Lösung

Cisco und NetApp haben FlexPod Express als eine der führenden Infrastrukturplattformen für ihre Kunden konzipiert und entwickelt. Da die Lösung mit branchenführenden Komponenten entwickelt wurde, können Kunden darauf vertrauen, dass FlexPod Express als Infrastrukturgrundlage dient. Die FlexPod Express Architektur wurde den grundlegenden Prinzipien des FlexPod Portfolios gerecht und von Cisco und NetApp Datacenter-Architekten und Ingenieuren umfassend getestet. Von Redundanz und Verfügbarkeit bis hin zu jedem einzelnen Feature – die gesamte FlexPod Express Architektur wurde validiert, um das Vertrauen unserer Kunden zu stärken und das Vertrauen in den Entwicklungsprozess zu stärken.

VMware vSphere 6.7 wurde auf den Komponenten der FlexPod Express Infrastruktur verifiziert. Bei dieser Validierung wurden 10-GbE-Uplink-Konnektivitätsoptionen für den Hypervisor berücksichtigt.

"Weiter: Fazit."

Schlussfolgerung

FlexPod Express bietet eine einfache und effektive Lösung mit einem validierten Design mit branchenführenden Komponenten. Durch die Skalierung und die Bereitstellung der Optionen für die Hypervisor-Plattform kann FlexPod Express auf spezifische Geschäftsanforderungen zugeschnitten werden. FlexPod Express wurde für kleine bis mittelständische Unternehmen, Remote-Standorte, Zweigstellen und andere Unternehmen konzipiert, die dedizierte Lösungen benötigen.

"Weiter: Wo finden Sie zusätzliche Informationen."

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in den folgenden Dokumenten und auf den folgenden Websites:

- NetApp Dokumentation

  "https://docs.netapp.com"

- FlexPod Express mit VMware vSphere 6.7 und NetApp AFF A220 Implementierungsleitfaden

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

Implementierungs-Leitfaden: FlexPod Express mit Cisco UCS C-Series und AFF A220 Serie

NVA-1123-DEPLOY: FlexPod Express mit VMware vSphere 6.7 und NetApp AFF A220 Implementierungsleitfaden

Savita Kumari, NetApp

In Zusammenarbeit mit: 

Aktuell stellen immer mehr Unternehmen ihre Rechenzentren auf eine Shared IT Infrastructure und Cloud Computing um. Außerdem wünschen sich Unternehmen eine einfache und effektive Lösung für Remote-Standorte und Zweigstellen, die ihnen die Technologie nutzt, die sie in ihrem Datacenter kennen.

FlexPod Express ist eine vorkonfigurierte Datacenter-Architektur mit Best Practices, die auf Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switch-Produktfamilie und NetApp Storage-Technologien

basiert. Die Komponenten eines FlexPod Express Systems sind wie ihre Kollegen im FlexPod Datacenter, die Managementsynergien über die gesamte IT-Infrastrukturumgebung hinweg in geringerem Umfang ermöglichen. FlexPod Datacenter und FlexPod Express sind optimale Plattformen für die Virtualisierung sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads.

FlexPod Datacenter und FlexPod Express bieten eine Basiskonfiguration, die sich flexibel für eine Vielzahl von Anwendungsfällen und Anforderungen dimensionieren und optimieren lässt. Bestehende FlexPod Datacenter-Kunden können ihr FlexPod Express System mit den gewohnten Tools managen. Neue FlexPod Express Kunden können sich mühelos an das Management von FlexPod Datacenter anpassen, wenn ihre Umgebung wächst.

FlexPod Express ist die optimale Infrastrukturbasis für Remote-Standorte und externe Niederlassungen sowie für kleine bis mittelständische Unternehmen. Es ist außerdem eine optimale Lösung für Kunden, die eine Infrastruktur für einen dedizierten Workload bereitstellen möchten.

FlexPod Express bietet eine einfach zu managende Infrastruktur, die sich für fast alle Workloads eignet.

Lösungsüberblick

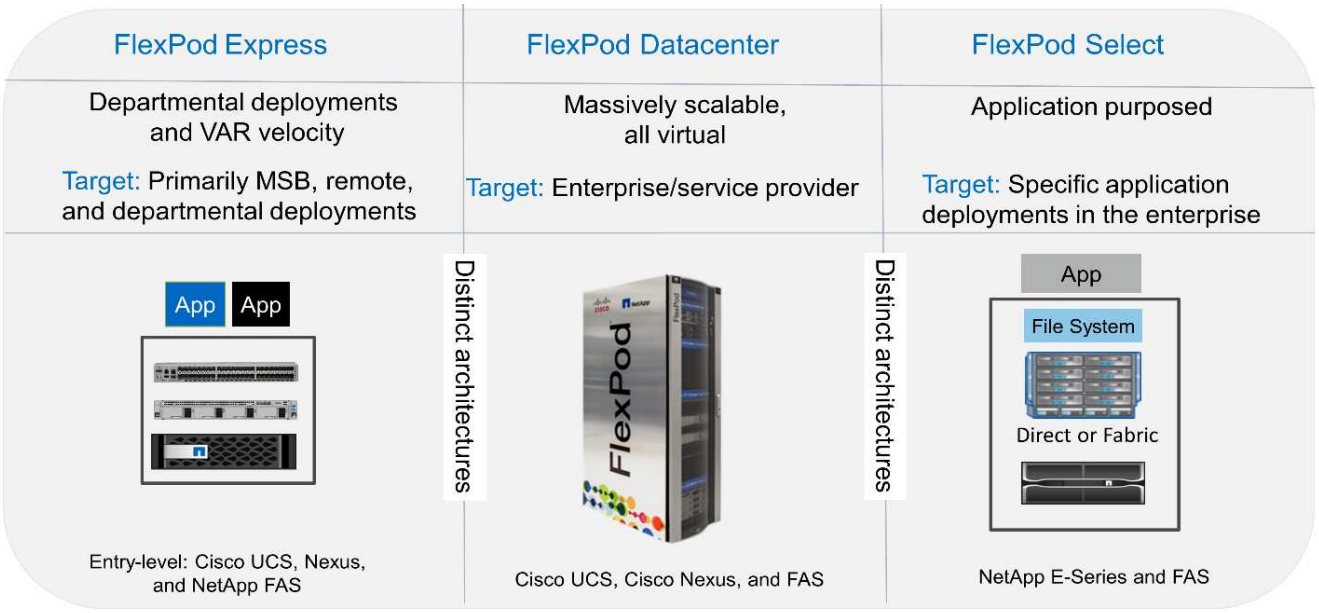
Diese FlexPod Express Lösung ist Teil des FlexPod Converged Infrastructure Programms.

FlexPod Converged Infrastructure Programm

FlexPod Referenzarchitekturen werden als Cisco Validated Designs (CVDs) oder NetApp Verified Architectures (NVAs) bereitgestellt. Abweichungen, die auf Kundenanforderungen von einem bestimmten CVD oder NVA basieren, sind zulässig, wenn diese Variationen keine nicht unterstützte Konfiguration erstellen.

Wie in der Abbildung unten dargestellt, umfasst das FlexPod Programm drei Lösungen: FlexPod Express, FlexPod Datacenter und FlexPod Select:

- **FlexPod Express.** bietet Kunden eine Einstiegslösung mit Technologien von Cisco und NetApp.
- **FlexPod Datacenter.** bietet eine optimale Mehrzweckgrundlage für verschiedene Workloads und Anwendungen.
- **FlexPod Select.** integriert die besten Aspekte des FlexPod-Rechenzentrums und stimmt die Infrastruktur auf eine bestimmte Anwendung ab.



NetApp Verified Architecture das Programm

Das Programm „NetApp Verified Architecture“ bietet verifizierte Architekturen für NetApp Lösungen an. Eine NetApp Verified Architecture bietet eine NetApp Lösungsarchitektur folgende Eigenschaften:

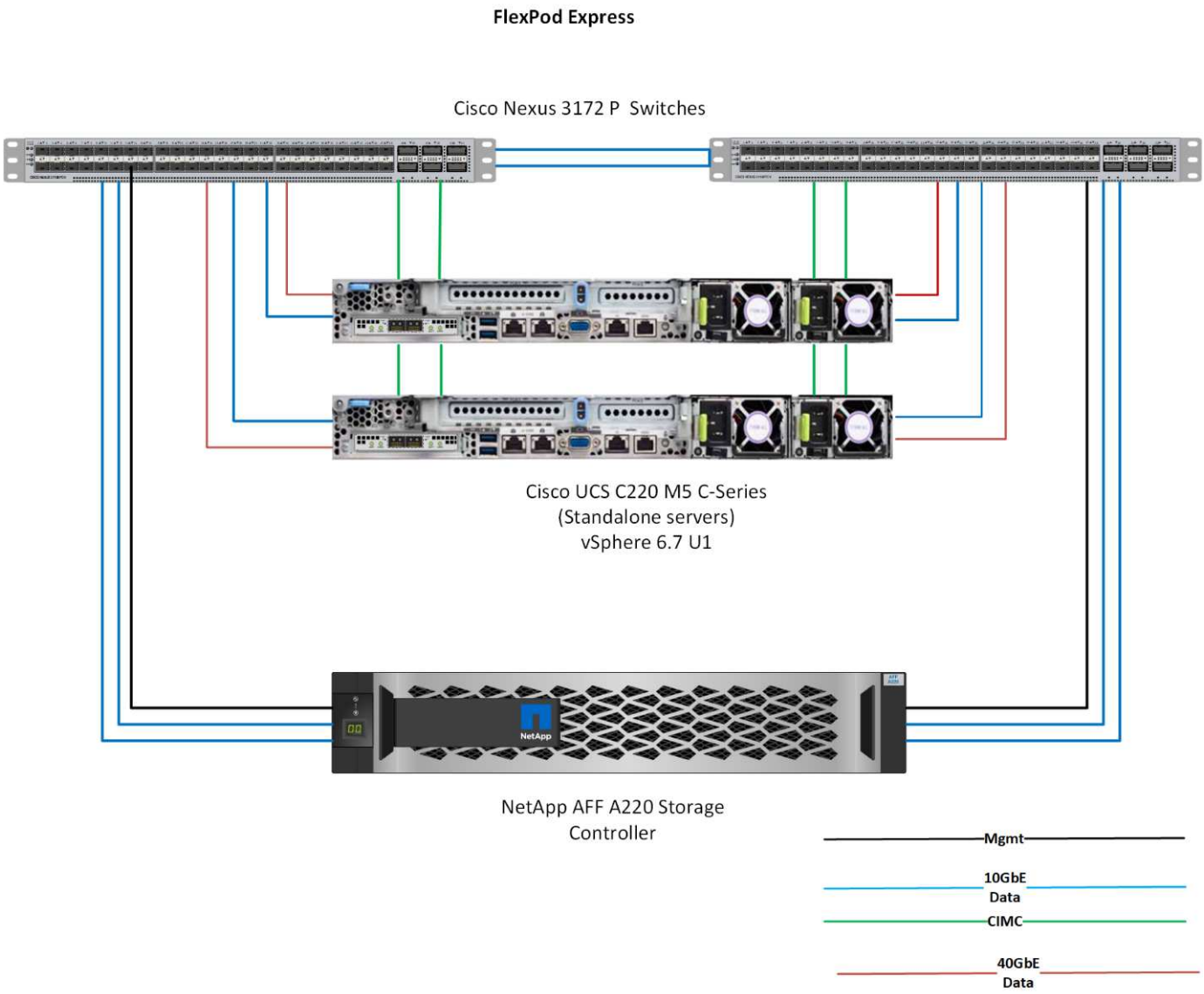
- Sorgfältig getestet
- Präskriptiv
- Minimale Risiken bei der Implementierung
- Schnellere Produkteinführungszeiten

Dieser Leitfaden beschreibt das Design von FlexPod Express mit VMware vSphere. Darüber hinaus verwendet dieses Design das komplett neue AFF A220 System, auf dem NetApp ONTAP 9.4, Cisco Nexus 3172P und Cisco UCS C-Series C220 M5 Server als Hypervisor-Nodes ausgeführt werden.

Lösungstechnologie

Diese Lösung nutzt die neuesten Technologien von NetApp, Cisco und VMware. Diese Lösung umfasst das neue NetApp AFF A220 mit ONTAP 9.4, zwei Cisco Nexus 3172P Switches und Cisco UCS C220 M5 Rack Servern, auf denen VMware vSphere 6.7 ausgeführt wird. Diese validierte Lösung nutzt 10-GbE-Technologie. Es wird auch eine Anleitung zur Skalierung der Computing-Kapazität bereitgestellt, indem jeweils zwei Hypervisor-Nodes hinzugefügt werden, damit sich die FlexPod Express-Architektur an die sich wandelnden Geschäftsanforderungen eines Unternehmens anpassen kann.

Die folgende Abbildung zeigt die FlexPod Express Architektur mit einer VMware vSphere 10-GbE-Architektur.



Diese Validierung verwendet 10-GbE-Konnektivität und einen Cisco UCS VIC 1387, der 40 GbE beträgt. Für eine 10GbE-Konnektivität kommt der CVR-QSFP-SFP10G Adapter zum Einsatz.

Zusammenfassung des Anwendungsfalls

Die FlexPod Express Lösung kann für verschiedene Anwendungsfälle eingesetzt werden. Dazu zählen:

- Remote-Standorte oder Niederlassungen
- Kleine und mittelständische Unternehmen
- Umgebungen, für die eine dedizierte und kostengünstige Lösung erforderlich ist

FlexPod Express eignet sich am besten für virtualisierte und gemischte Workloads.

Obwohl diese Lösung mit vSphere 6.7 validiert wurde, unterstützt sie jede vSphere Version, die für die anderen Komponenten durch das NetApp Interoperabilitäts-Matrix-Tool qualifiziert ist. NetApp empfiehlt die Implementierung von vSphere 6.7U1 für seine Fixes und erweiterten Funktionen.

Einige Funktionen von vSphere 6.7 U1:

- Voll ausgestattetem HTML5 webbasierter vSphere Client
- VMotion für NVIDIA GRID vGPU-VMs Unterstützung für Intel FPGA
- VCenter Server Converge Tool für den Wechsel von externen PCs zu internen PCS
- Erweiterungen für vSAN (HCI Updates)
- Erweiterte Content-Bibliothek

Weitere Informationen zu vSphere 6.7 U1 finden Sie unter "Was ist neu in vCenter Server 6.7 Update 1".

Technologieanforderungen erfüllt

Ein FlexPod Express System erfordert eine Kombination aus Hardware- und Softwarekomponenten. FlexPod Express beschreibt außerdem die Hardwarekomponenten, die erforderlich sind, um dem System in Einheiten von zwei Hypervisor-Nodes hinzuzufügen.

Hardwareanforderungen

Unabhängig vom ausgewählten Hypervisor nutzen alle FlexPod Express Konfigurationen dieselbe Hardware. Daher kann auch bei sich ändernden Geschäftsanforderungen jeder Hypervisor auf derselben FlexPod Express Hardware ausgeführt werden.

In der folgenden Tabelle werden die Hardwarekomponenten aufgeführt, die für alle FlexPod Express Konfigurationen erforderlich sind.

Trennt	Menge
AFF A220 HA-PAAR	1
Cisco C220 M5 Server	2
Cisco Nexus 3172P-Switch	2
Cisco UCS Virtual Interface Card (VIC) 1387 für den C220 M5 Server	2
CVR-QSFP-SFP10G ADAPTER	4

In der folgenden Tabelle ist die zusätzlich zur Basiskonfiguration für die 10-GbE-Implementierung erforderliche Hardware aufgeführt.

Trennt	Menge
Cisco UCS C220 M5 Server	2
Cisco VIC 1387	2
CVR-QSFP-SFP10G ADAPTER	4

Softwareanforderungen

In der folgenden Tabelle werden die erforderlichen Softwarekomponenten für die Implementierung der Architekturen der FlexPod Express Lösungen aufgeführt.

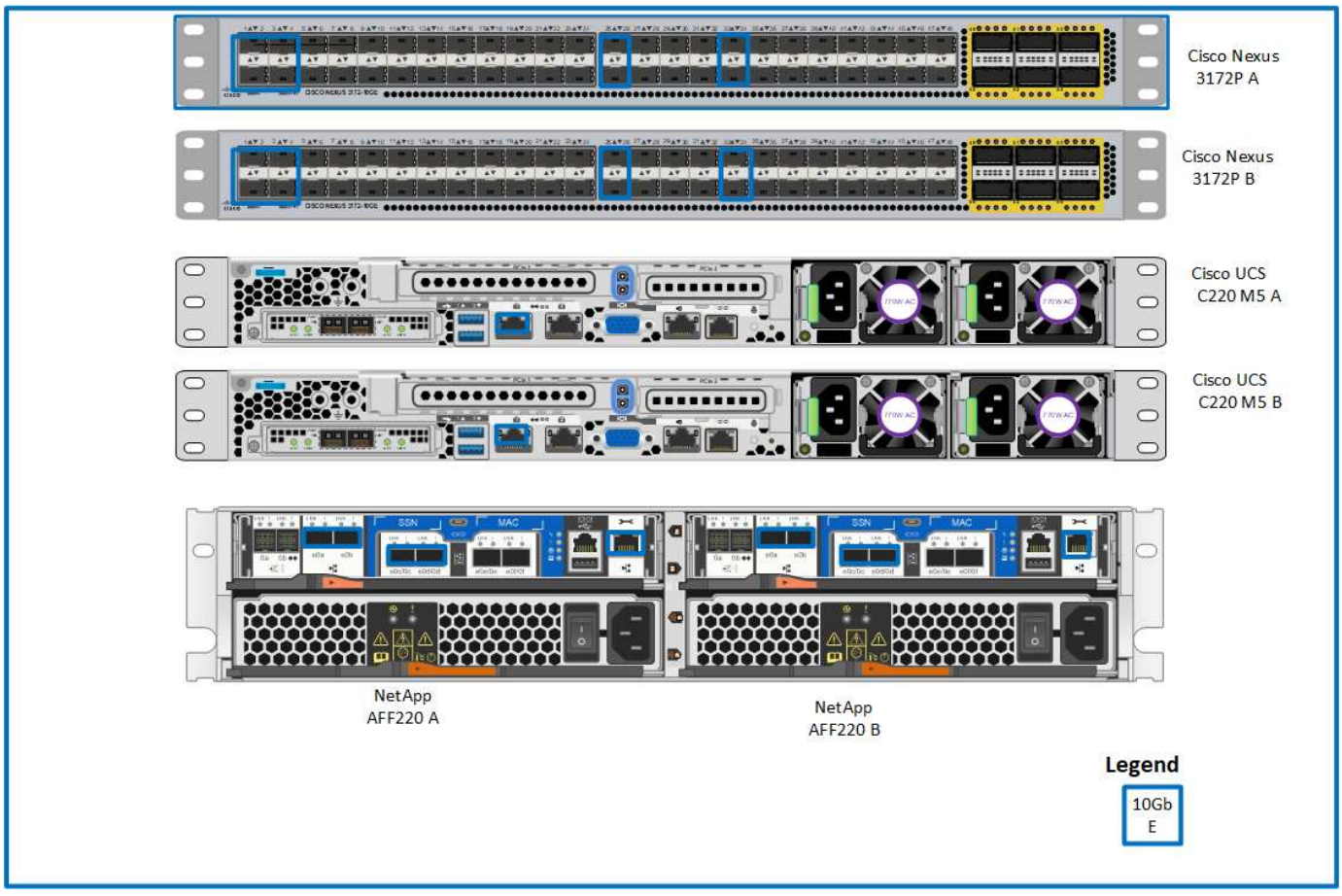
Software	Version	Details
Cisco Integrated Management Controller (CIMC)	3.1 (3g)	Für Cisco UCS C220 M5 Rack Server
Cisco Nenic-Treiber	1.0.25.0	Für VIC 1387 Schnittstellenkarten
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Für Cisco Nexus 3172P-Switches
NetApp ONTAP	9.4	Für AFF A220 Controller

In der folgenden Tabelle ist die für alle VMware vSphere Implementierungen auf FlexPod Express erforderliche Software aufgeführt.

Software	Version
VMware vCenter Server Appliance	6.7
VMware vSphere ESXi Hypervisor	6.7
NetApp VAAI Plug-in für ESXi	1.1.2

Informationen zur FlexPod Express Verkabelung

Die folgende Abbildung zeigt die Verkabelung zur Referenzvalidierung.



Die folgende Tabelle zeigt die Verkabelungsinformationen für den Cisco Nexus Switch 3172P A

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus-Switch 3172P A	Eth1/1	NetApp AFF A220 Storage-Controller A	e0c
	Eth1/2	NetApp AFF A220 Storage-Controller B	e0c
	Eth1/3	Cisco UCS C220 C-Series Standalone Server A	MLOM1 mit CVR-QSFP-SFP10G Adapter
	Eth1/4	Cisco UCS C220 C-Series Standalone Server B	MLOM1 mit CVR-QSFP-SFP10G Adapter
	Eth1/25	Cisco Nexus Switch 3172P B	Eth1/25
	Eth1/26	Cisco Nexus Switch 3172P B	Eth1/26
	Eth1/33	NetApp AFF A220 Storage-Controller A	E0M
	Eth1/34	Cisco UCS C220 C-Series Standalone Server A	CIMC

Die folgende Tabelle zeigt die Verkabelungsinformationen für den Cisco Nexus Switch 3172P B

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus Switch 3172P B	Eth1/1	NetApp AFF A220 Storage-Controller A	e0d
	Eth1/2	NetApp AFF A220 Storage-Controller B	e0d
	Eth1/3	Cisco UCS C220 C-Series Standalone Server A	MLOM2 mit CVR-QSFP-SFP10G Adapter
	Eth1/4	Cisco UCS C220 C-Series Standalone Server B	MLOM2 mit CVR-QSFP-SFP10G Adapter
	Eth1/25	Cisco Nexus-Switch 3172P A	Eth1/25
	Eth1/26	Cisco Nexus-Switch 3172P A	Eth1/26
	Eth1/33	NetApp AFF A220 Storage-Controller B	E0M
	Eth1/34	Cisco UCS C220 C-Series Standalone Server B	CIMC

In der folgenden Tabelle sind die Verkabelungsinformationen für NetApp AFF A220 Storage Controller aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF A220 Storage-Controller A	e0a	NetApp AFF A220 Storage-Controller B	e0a
	e0b	NetApp AFF A220 Storage-Controller B	e0b
	e0c	Cisco Nexus-Switch 3172P A	Eth1/1
	e0d	Cisco Nexus Switch 3172P B	Eth1/1
	E0M	Cisco Nexus-Switch 3172P A	Eth1/33

Die folgende Tabelle zeigt die Verkabelungsinformationen für NetApp AFF A220 Storage Controller B.

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF A220 Storage-Controller B	e0a	NetApp AFF A220 Storage-Controller A	e0a
	e0b	NetApp AFF A220 Storage-Controller A	e0b
	e0c	Cisco Nexus-Switch 3172P A	Eth1/2
	e0d	Cisco Nexus Switch 3172P B	Eth1/2
	E0M	Cisco Nexus Switch 3172P B	Eth1/33

Implementierungsverfahren

Dieses Dokument enthält Details zur Konfiguration eines vollständig redundanten, hochverfügbaren FlexPod Express-Systems. Um diese Redundanz Rechnung zu tragen, werden die in jedem Schritt konfigurierten Komponenten entweder als Komponente A oder Komponente B bezeichnet Controller A und Controller B identifizieren beispielsweise die beiden NetApp Storage Controller, die in diesem Dokument bereitgestellt werden. Switch A und Switch B identifizieren ein Paar Cisco Nexus-Switches.

Zusätzlich beschreibt dieses Dokument Schritte zur Bereitstellung mehrerer Cisco UCS-Hosts, die sequenziell als Server A, Server B usw. identifiziert werden können.

Um anzugeben, dass Sie in einem Schritt Informationen zu Ihrer Umgebung angeben sollten, `<<text>>` Wird als Teil der Befehlsstruktur angezeigt. Das folgende Beispiel enthält die `vlan create` Befehl:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Mit diesem Dokument können Sie die FlexPod Express Umgebung vollständig konfigurieren. Bei diesem Prozess müssen Sie in verschiedenen Schritten kundenspezifische Namenskonventionen, IP-Adressen und VLAN-Schemata (Virtual Local Area Network) einfügen. Die folgende Tabelle beschreibt die für die Implementierung erforderlichen VLANs, wie in diesem Leitfaden beschrieben. Diese Tabelle kann anhand der spezifischen Standortvariablen abgeschlossen und zur Implementierung der Konfigurationsschritte des Dokuments verwendet werden.

Wenn Sie separate in-Band- und Out-of-Band-Management-VLANs verwenden, müssen Sie eine Layer-3-Route zwischen ihnen erstellen. Für diese Validierung wurde ein gemeinsames Management-VLAN genutzt.

EIN Name	VLAN-Zweck	ID zur Validierung dieses Dokuments verwendet
Management-VLAN	VLAN für Management-Schnittstellen	3437
Natives VLAN	VLAN, dem nicht getaggte Frames zugewiesen sind	2
NFS-VLAN	VLAN für NFS-Verkehr	3438
VMware vMotion VLAN	VLAN, das für die Verschiebung von virtuellen Maschinen von einem physischen Host zum anderen bestimmt ist	3441
Datenverkehr-VLAN für Virtual Machines	VLAN für den Datenverkehr von Virtual-Machine-Applikationen	3442
ISCSI-A-VLAN	VLAN für iSCSI-Verkehr auf Fabric A	3439
ISCSI-B-VLAN	VLAN für iSCSI-Datenverkehr auf Fabric B	3440

Die VLAN-Nummern sind in der gesamten Konfiguration von FlexPod Express erforderlich. Die VLANs werden als bezeichnet `<<var_xxxx_vlan>>`, Wo `xxxx` Dient dem VLAN (z. B. iSCSI-A).

In der folgenden Tabelle sind die erstellten virtuellen VMware-Maschinen aufgeführt.

Beschreibung der virtuellen Maschine	Host-Name
VMware vCenter Server	

Cisco Nexus 3172P-Implementierungsverfahren

Im folgenden Abschnitt wird die in einer FlexPod Express-Umgebung verwendete Cisco Nexus 3172P-Switch-Konfiguration beschrieben.

Ersteinrichtung des Cisco Nexus 3172P-Switch

In den folgenden Verfahren wird die Konfiguration von Cisco Nexus Switches für die Verwendung in einer grundlegenden FlexPod Express Umgebung beschrieben.

Bei diesem Verfahren wird davon ausgegangen, dass Sie einen Cisco Nexus 3172P mit NX-OS-Softwareversion 7.0(3)I7(5) verwenden.

1. Nach dem ersten Booten und der Verbindung zum Konsolen-Port des Switches wird automatisch das Cisco NX-OS Setup gestartet. Diese Erstkonfiguration betrifft grundlegende Einstellungen wie den Switch-Namen, die mgmt0-Schnittstellenkonfiguration und die Einrichtung der Secure Shell (SSH).
2. Das FlexPod Express Managementnetzwerk lässt sich auf unterschiedliche Weise konfigurieren. Die mgmt0-Schnittstellen der 3172P-Switches können an ein bestehendes Managementnetzwerk angeschlossen werden, oder die mgmt0-Schnittstellen der 3172P-Switches können in einer Back-to-Back-Konfiguration angeschlossen werden. Dieser Link kann jedoch nicht für externen Managementzugriff wie SSH-Datenverkehr verwendet werden.

   In diesem Implementierungsleitfaden werden die FlexPod Express Cisco Nexus 3172P-Switches mit einem vorhandenen Managementnetzwerk verbunden.
3. Um die Cisco Nexus 3172P-Schalter zu konfigurieren, schalten Sie den Switch ein und befolgen Sie die Anweisungen auf dem Bildschirm, wie hier bei der Ersteinrichtung beider Switches dargestellt, und ersetzen Sie die entsprechenden Werte für die Switch-spezifischen Informationen.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. Dann sehen Sie eine Zusammenfassung Ihrer Konfiguration, und Sie werden gefragt, ob Sie sie bearbeiten möchten. Wenn die Konfiguration korrekt ist, geben Sie ein `n`.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. Sie werden dann gefragt, ob Sie diese Konfiguration verwenden und speichern möchten. Wenn ja, geben Sie ein `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Wiederholen Sie dieses Verfahren für Cisco Nexus Switch B.

Aktivieren Sie erweiterte Funktionen

Bestimmte erweiterte Funktionen müssen in Cisco NX-OS aktiviert sein, um zusätzliche Konfigurationsoptionen bereitzustellen.

> Der `interface-vlan` Die Funktion ist nur erforderlich, wenn Sie die Back-to-Back-Funktion verwenden `mgmt0` Option, die in diesem Dokument beschrieben wird. Mit dieser Funktion können Sie dem Schnittstellen-VLAN (Switch Virtual Interface) eine IP-Adresse zuweisen, die dem Switch (z. B. über SSH) eine bandinterne Verwaltungskommunikation ermöglicht.

1. Um die entsprechenden Funktionen bei Cisco Nexus Switch A und Switch B zu aktivieren, wechseln Sie mit dem Befehl in den Konfigurationsmodus `(config t)` Und führen Sie folgende Befehle aus:

```
feature interface-vlan
feature lacp
feature vpc
```

   Der Standard-Port-Channel-Load-Balancing-Hash verwendet die Quell- und Ziel-IP-Adressen, um den Load-Balancing-Algorithmus über die Schnittstellen im Port-Kanal zu bestimmen. Sie können eine bessere Verteilung über die Mitglieder des Port-Kanals erzielen, indem Sie mehr Inputs für den Hash-Algorithmus bereitstellen, der über die Quell- und Ziel-IP-Adressen hinausgeht. Aus dem gleichen Grund empfiehlt NetApp dringend, den Hash-Algorithmus der Quell- und Ziel-TCP-Ports hinzuzufügen.

2. Im Konfigurationsmodus (`config t`Geben Sie die folgenden Befehle ein, um die Konfiguration für den globalen Port Channel-Lastenausgleich auf Cisco Nexus Switch A und Switch B festzulegen:

```
port-channel load-balance src-dst ip-l4port
```

Führen Sie eine globale Spanning-Tree-Konfiguration durch

Die Cisco Nexus Plattform verwendet eine neue Sicherungsfunktion namens „Bridge Assurance“. Bridge Assurance schützt vor unidirektionalen Verbindungsfehlern oder anderen Softwarefehlern mit einem Gerät, das den Datenverkehr weiterführt, wenn der Spanning-Tree-Algorithmus nicht mehr ausgeführt wird. Die Ports können je nach Plattform in einen von mehreren Status platziert werden, einschließlich Netzwerk oder Edge.

NetApp empfiehlt, die Bridge-Assurance einzustellen, damit alle Ports standardmäßig für Netzwerkports gelten. Diese Einstellung zwingt den Netzwerkadministrator, die Konfiguration jedes Ports zu überprüfen. Außerdem werden die häufigsten Konfigurationsfehler angezeigt, z. B. nicht identifizierte Edge-Ports oder ein Nachbar, bei dem die Bridge-Assurance-Funktion nicht aktiviert ist. Außerdem ist es sicherer, den Spanning Tree Block viele Ports statt zu wenig zu haben, was den Standard-Port-Zustand ermöglicht, um die allgemeine Stabilität des Netzwerks zu verbessern.

Achten Sie beim Hinzufügen von Servern, Speicher- und Uplink-Switches auf den Spanning-Tree-Status, insbesondere wenn sie keine Bridge-Sicherheit unterstützen. In solchen Fällen müssen Sie möglicherweise den Porttyp ändern, um die Ports aktiv zu machen.

Die BPDU-Schutzfunktion (Bridge Protocol Data Unit) ist standardmäßig auf Edge-Ports als andere Schutzschicht aktiviert. Um Schleifen im Netzwerk zu vermeiden, wird der Port durch diese Funktion

heruntergefahren, wenn BPDUs von einem anderen Switch auf dieser Schnittstelle angezeigt werden.

Im Konfigurationsmodus (`config t`), führen Sie die folgenden Befehle aus, um die standardmäßigen Spanning-Tree-Optionen, einschließlich des Standard-Porttyps und BPDU Guard, auf Cisco Nexus Switch A und Switch B zu konfigurieren:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Definieren Sie VLANs

Bevor individuelle Ports mit unterschiedlichen VLANs konfiguriert sind, müssen auf dem Switch die Layer-2-VLANs definiert werden. Es ist auch eine gute Praxis, die VLANs zu benennen, um zukünftig eine einfache Fehlerbehebung zu ermöglichen.

Im Konfigurationsmodus (`config t`), führen Sie die folgenden Befehle aus, um die Layer-2-VLANs auf Cisco Nexus Switch A und Switch B zu definieren und zu beschreiben:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Konfiguration von Zugriffs- und Management-Port-Beschreibungen

Wie bei der Zuordnung von Namen zu den Layer-2-VLANs kann das Festlegen von Beschreibungen für alle Schnittstellen sowohl bei der Bereitstellung als auch bei der Fehlerbehebung hilfreich sein.

Im Konfigurationsmodus (`config t`) Geben Sie bei jedem der Switches die folgenden Portbeschreibungen für die FlexPod Express Large-Konfiguration ein:

Cisco Nexus Switch A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Cisco Nexus Switch B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Konfiguration der Server- und Storage-Managementschnittstellen

Die Management-Schnittstellen sowohl für den Server als auch für den Storage verwenden in der Regel nur ein einziges VLAN. Konfigurieren Sie daher die Ports der Managementoberfläche als Access Ports. Definieren Sie das Management-VLAN für jeden Switch und ändern Sie den Porttyp Spanning-Tree in Edge.

Im Konfigurationsmodus (`config t`Geben Sie die folgenden Befehle ein, um die Porteinstellungen für die Verwaltungsschnittstellen der Server und des Speichers zu konfigurieren:

Cisco Nexus Switch A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus Switch B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Globale Konfiguration des virtuellen Port-Channels durchführen

Über einen Virtual Port Channel (vPC) können Links, die physisch mit zwei verschiedenen Cisco Nexus-Switches verbunden sind, mit einem dritten Gerät als einzelner Port-Channel angezeigt werden. Das dritte Gerät kann ein Switch, Server oder ein anderes Netzwerkgerät sein. Ein vPC bietet Multipathing auf Layer-2-Ebene. Dadurch kann Redundanz erzeugt werden, indem die Bandbreite erhöht wird. Dies ermöglicht mehrere parallele Pfade zwischen Nodes und Lastverteilung zwischen alternativen Pfaden.

Ein vPC bietet die folgenden Vorteile:

- Aktivieren eines einzelnen Geräts zur Verwendung eines Port-Kanals über zwei vorgelagerte Geräte
- Blockierte Ports für Spanning-Tree-Protokolle werden eliminiert
- Eine Topologie ohne Schleife
- Nutzung aller verfügbaren Uplink-Bandbreite
- Schnelle Konvergenz bei Ausfall der Verbindung oder eines Geräts
- Ausfallsicherheit auf Verbindungsebene
- Unterstützung für Hochverfügbarkeit

Die vPC-Funktion erfordert eine Ersteinrichtung zwischen den beiden Cisco Nexus-Switches, damit diese ordnungsgemäß funktionieren. Wenn Sie die Back-to-Back-mmmt0-Konfiguration verwenden, verwenden Sie die auf den Schnittstellen definierten Adressen und stellen Sie sicher, dass sie über den Ping kommunizieren können `[switch_A/B_mgmt0_ip_addr]vrf` Management-Befehl.

Im Konfigurationsmodus (`config t`Führen Sie die folgenden Befehle aus, um die globale vPC-Konfiguration für beide Switches zu konfigurieren:

Cisco Nexus Switch A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Cisco Nexus Switch B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Konfigurieren Sie Speicher-Port-Kanäle

Die NetApp Storage-Controller ermöglichen eine aktiv/aktiv-Verbindung zum Netzwerk mithilfe des Link Aggregation Control Protocol (LACP). Die Verwendung von LACP wird bevorzugt, da es sowohl Verhandlungen als auch Protokollierung zwischen den Switches hinzufügt. Da das Netzwerk für vPC eingerichtet ist, können Sie mit diesem Ansatz aktiv/aktiv-Verbindungen vom Storage zu separaten physischen Switches nutzen. Jeder Controller verfügt über zwei Links zu jedem der Switches. Alle vier Links sind jedoch Teil derselben vPC und Interface Group (IFGRP).

Im Konfigurationsmodus (`config t`), führen Sie auf jedem der Switches die folgenden Befehle aus, um die einzelnen Schnittstellen und die daraus resultierende Port Channel-Konfiguration für die mit dem NetApp AFF Controller verbundenen Ports zu konfigurieren.

1. Führen Sie die folgenden Befehle an Switch A und Switch B aus, um die Port-Kanäle für Speicher-Controller A zu konfigurieren:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Führen Sie die folgenden Befehle an Switch A und Switch B aus, um die Port-Kanäle für Speicher-Controller B zu konfigurieren

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

In dieser Lösungsvalidierung wurde eine MTU von 9000 verwendet. Basierend auf Anwendungsanforderungen können Sie jedoch einen entsprechenden Wert für die MTU konfigurieren. Es ist wichtig, für die gesamte FlexPod Lösung denselben MTU-Wert festzulegen. Falsche MTU-Konfigurationen zwischen Komponenten führen zu Paketverluste und diesen Paketen.

Serververbindungen konfigurieren

Die Cisco UCS Server haben eine virtuelle Interface Card mit zwei Ports, VIC1387, die für den Datenverkehr und das Booten des ESXi Betriebssystems über iSCSI verwendet wird. Diese Schnittstellen werden für den Failover untereinander konfiguriert, wodurch über eine einzelne Verbindung hinaus eine zusätzliche

Redundanz gewährleistet wird. Wenn diese Links über mehrere Switches verteilt werden, kann der Server sogar einen vollständigen Switch-Ausfall überstehen.

Im Konfigurationsmodus (`config t`), führen Sie die folgenden Befehle aus, um die Porteinstellungen für die Schnittstellen zu konfigurieren, die mit jedem Server verbunden sind.

Cisco Nexus Switch A: Cisco UCS Server-A- und Cisco UCS Server-B-Konfiguration

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Cisco Nexus Switch B: Konfiguration von Cisco UCS Server A und Cisco UCS Server B

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

In dieser Lösungsvalidierung wurde eine MTU von 9000 verwendet. Basierend auf Anwendungsanforderungen können Sie jedoch einen entsprechenden Wert für die MTU konfigurieren. Es ist wichtig, für die gesamte FlexPod Lösung denselben MTU-Wert festzulegen. Falsche MTU-Konfigurationen zwischen Komponenten führen zum Paketfallen, und diese Pakete müssen erneut übertragen werden. Dies wirkt sich auf die Gesamt-Performance der Lösung aus.

Um die Lösung durch Hinzufügen weiterer Cisco UCS Server zu skalieren, führen Sie die vorherigen Befehle mit den Switch-Ports aus, die die neu hinzugefügten Server an Switches A und B angeschlossen wurden

Uplink zur bestehenden Netzwerkinfrastruktur

Je nach verfügbarer Netzwerkinfrastruktur können zur Uplink der FlexPod Umgebung mehrere Methoden und Funktionen verwendet werden. Bei einer vorhandenen Cisco Nexus Umgebung empfiehlt NetApp den Einsatz

von vPCs, um die in der FlexPod Umgebung enthaltenen Cisco Nexus 3172P Switches in die Infrastruktur zu integrieren. Bei den Uplinks kann es sich um 10-GbE-Uplinks für eine 10-GbE-Infrastrukturlösung oder 1 GbE für eine 1-GbE-Infrastrukturlösung (sofern erforderlich) handelt. Die zuvor beschriebenen Verfahren können zur Erstellung eines Uplink vPC in der vorhandenen Umgebung verwendet werden. Stellen Sie sicher, dass Sie den Kopierlauf ausführen, um die Konfiguration nach Abschluss der Konfiguration auf jedem Switch zu speichern.

"Weiter: NetApp Verfahren für die Storage-Implementierung (Teil 1)"

Verfahren zur NetApp Storage-Implementierung (Teil 1)

In diesem Abschnitt wird das NetApp AFF Storage-Implementierungsverfahren beschrieben.

Installation eines NetApp Storage Controllers der AFF2xx Serie

NetApp Hardware Universe

Die NetApp Hardware Universe (HWU) Applikation bietet unterstützte Hardware- und Softwarekomponenten für jede spezifische ONTAP-Version. Das Tool liefert Konfigurationsinformationen für alle NetApp Storage Appliances, die derzeit von der ONTAP Software unterstützt werden. Zudem bietet er eine Tabelle mit den Kompatibilitäten der Komponenten.

Vergewissern Sie sich, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, von der zu installierenden Version von ONTAP unterstützt werden:

1. Auf das zugreifen "HWU" Anwendung zum Anzeigen der Systemkonfigurationsleitfäden. Klicken Sie auf die Registerkarte Controller, um sich die Kompatibilität zwischen verschiedenen Versionen der ONTAP Software und den NetApp Storage Appliances mit den gewünschten Spezifikationen anzusehen.
2. Wenn Sie Komponenten nach Storage Appliance vergleichen möchten, klicken Sie alternativ auf Storage-Systeme vergleichen.

Voraussetzungen für Controller AFF2XX Serie
Informationen zum Planen des physischen Standorts der Storage-Systeme finden Sie im NetApp Hardware Universe. Beachten Sie die folgenden Abschnitte: Elektrische Anforderungen, unterstützte Netzkabel sowie integrierte Anschlüsse und Kabel.

Storage Controller

Befolgen Sie die Anweisungen zur physischen Installation der Controller im "AFF A220: Dokumentation".

NetApp ONTAP 9.4

Konfigurationsarbeitsblatt

Bevor Sie das Setup-Skript ausführen, füllen Sie das Konfigurationsarbeitsblatt aus der Produktanleitung aus. Das Konfigurationsarbeitsblatt ist im verfügbar "ONTAP 9.4 – Leitfaden für die Software-Einrichtung".

ⓘ Das System ist in einer Konfiguration mit zwei Nodes ohne Switches eingerichtet.

Die nachfolgende Tabelle enthält Informationen zur Installation und Konfiguration von ONTAP 9.4.

Cluster-Details	Wert für Cluster-Details
Cluster Node A IP-Adresse	<<var_nodeA_Mgmt_ip>>
Cluster-Node A-Netmask	<<var_nodeA_mgmt_maska>>
Cluster Node Ein Gateway	\<<var_nodeA_mgmt_Gateway>
Cluster-Node A-Name	<<var_nodeA>>
Cluster-Node B-IP-Adresse	<<var_nodeB_Mgmt_ip>>
Cluster-Node B-Netmask	<<var_nodeB_mgmt_maska>>
Cluster-Node B-Gateway	\<<var_nodeB_mgmt_Gateway>
Name für Cluster-Node B	<<var_nodeB>>
ONTAP 9.4-URL	\<<var_url_Boot_Software>
Name für Cluster	<<var_clustername>>
Cluster-Management-IP-Adresse	<<var_clustermgmt_ip>>
Cluster B-Gateway	<<var_clustermgmt_Gateway>>
Cluster B Netmask	<<var_clustermgmt_maska>>
Domain-Name	<<var_Domain_Name>>
DNS-Server-IP (Sie können mehrere eingeben)	<<var_dns_Server_ip>>
NTP-Server-IP (Sie können mehrere eingeben)	\<<var_ntp_Server_ip>

Konfigurieren Sie Node A

Führen Sie die folgenden Schritte aus, um Node A zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg-C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Lassen Sie das System booten.

   ```
   autoboot
   ```

3. Drücken Sie Strg-C, um das Startmenü aufzurufen.

   Wenn ONTAP 9.4 nicht die Version der gerade gestarteten Software ist, fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Wenn ONTAP 9.4 die Version wird gebootet, wählen Sie Option 8 und y aus, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

4. Um neue Software zu installieren, wählen Sie Option `7`.

5. Eingabe `y` Um ein Upgrade durchzuführen.

6. Wählen Sie `e0M` Für den Netzwerkanschluss, den Sie für den Download verwenden möchten.
7. Eingabe `y` Jetzt neu starten.
8. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Geben Sie die URL ein, auf der die Software gefunden werden kann.

   Dieser Webserver muss pingfähig sein.

```
<<var_url_boot_software>>
```

10. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an.
11. Eingabe `y` So legen Sie die neu installierte Software als Standard fest, die bei einem späteren Neustart verwendet wird.
12. Eingabe `y` Um den Node neu zu booten.

    Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

13. Drücken Sie Strg-C, um das Startmenü aufzurufen.
14. Wählen Sie die Option `4` Für saubere Konfiguration und Initialisieren aller Festplatten.
15. Eingabe `y` Setzen Sie die Konfiguration auf Null Festplatten zurück, und installieren Sie ein neues Dateisystem.
16. Eingabe `y` Um alle Daten auf den Festplatten zu löschen.

    Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert. Sie können mit der Node B-Konfiguration fortfahren, während die Festplatten für Node A auf Null gesetzt werden.

17. Beginnen Sie während der Initialisierung von Node A mit der Konfiguration von Node B.

Konfigurieren Sie Node B

Führen Sie die folgenden Schritte aus, um Node B zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg-C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Drücken Sie Strg-C, um das Startmenü aufzurufen.

```
autoboot
```

3. Drücken Sie bei der entsprechenden Aufforderung Strg-C.

   Wenn ONTAP 9.4 nicht die Version der gerade gestarteten Software ist, fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Wenn ONTAP 9.4 die Version wird gebootet, wählen Sie Option 8 und y aus, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

4. Um neue Software zu installieren, wählen Sie Option 7.
5. Eingabe `y` Um ein Upgrade durchzuführen.
6. Wählen Sie `e0M` Für den Netzwerkanschluss, den Sie für den Download verwenden möchten.
7. Eingabe `y` Jetzt neu starten.
8. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Geben Sie die URL ein, auf der die Software gefunden werden kann.

   Dieser Webserver muss pingfähig sein.

```
<<var_url_boot_software>>
```

10. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an.
11. Eingabe `y` So legen Sie die neu installierte Software als Standard fest, die bei einem späteren Neustart verwendet wird.
12. Eingabe `y` Um den Node neu zu booten.

    Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

13. Drücken Sie Strg-C, um das Startmenü aufzurufen.
14. Wählen Sie Option 4 für saubere Konfiguration und Initialisieren Sie alle Festplatten.
15. Eingabe `y` Setzen Sie die Konfiguration auf Null Festplatten zurück, und installieren Sie ein neues Dateisystem.
16. Eingabe `y` Um alle Daten auf den Festplatten zu löschen.

    Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert.

Fortsetzung der Konfiguration von Node A und Cluster

Führen Sie von einem Konsolen-Port-Programm, das an den Storage Controller A (Node A)-Konsolenport angeschlossen ist, das Node-Setup-Skript aus. Dieses Skript wird angezeigt, wenn ONTAP 9.4 das erste Mal auf dem Node gebootet wird.

> In ONTAP 9.4 wurde das Verfahren zur Einrichtung von Nodes und Clustern geringfügig geändert. Der Cluster-Setup-Assistent wird jetzt zum Konfigurieren des ersten Node in einem Cluster verwendet, während System Manager zum Konfigurieren des Clusters verwendet wird.

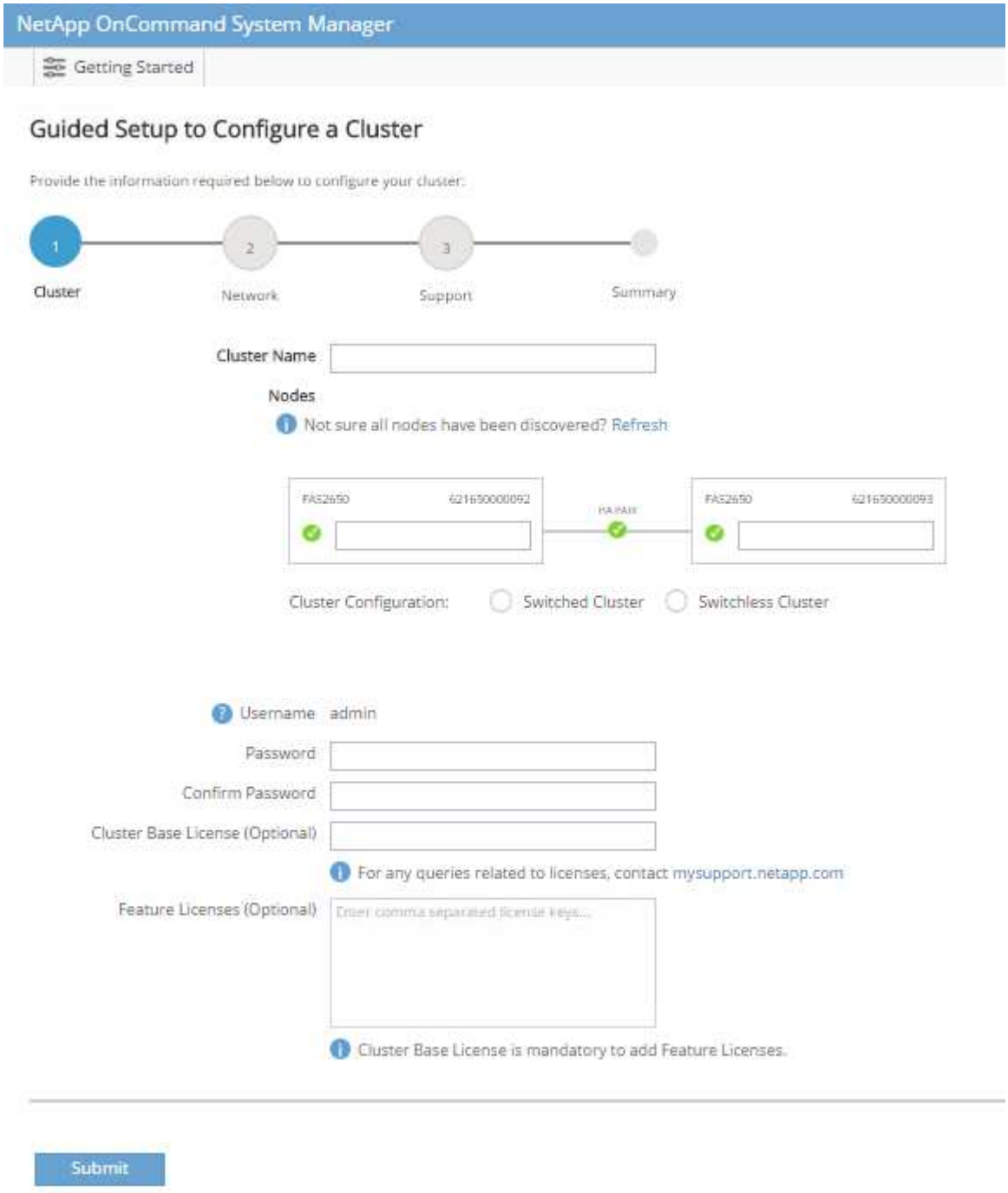
1. Befolgen Sie die Anweisungen zum Einrichten von Node A

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navigieren Sie zur IP-Adresse der Managementoberfläche des Knotens.

   Das Cluster-Setup kann auch über die CLI durchgeführt werden. In diesem Dokument wird die Cluster-Einrichtung mit der von NetApp System Manager geführten Einrichtung beschrieben.

3. Klicken Sie auf Guided Setup, um das Cluster zu konfigurieren.
4. Eingabe `<<var_clustername>>` Für den Cluster-Namen und `<<var_nodeA>>` Und `<<var_nodeB>>` Für jeden der Nodes, die Sie konfigurieren. Geben Sie das Passwort ein, das Sie für das Speichersystem verwenden möchten. Wählen Sie für den Cluster-Typ Cluster ohne Switch aus. Geben Sie die Cluster-Basislizenz ein.



5. Außerdem können Funktionslizenzen für Cluster, NFS und iSCSI eingegeben werden.
6. Eine Statusmeldung, die angibt, dass das Cluster erstellt wird. Diese Statusmeldung durchlaufen mehrere Statusarten. Dieser Vorgang dauert mehrere Minuten.
7. Konfigurieren des Netzwerks.
   a. Deaktivieren Sie die Option IP-Adressbereich.

b. Eingabe <<var_clustermgmt_ip>> Im Feld Cluster-Management-IP-Adresse <<var_clustermgmt_mask>> Im Feld „Netzmaske“ und <<var_clustermgmt_gateway>> Im Feld Gateway. Verwenden Sie den … Wählen Sie im Feld Port die Option E0M für Node A aus

c. Die Node-Management-IP für Node A ist bereits gefüllt. Eingabe <<var_nodeA_mgmt_ip>> Für Node B.

d. Eingabe <<var_domain_name>> Im Feld DNS-Domain-Name. Eingabe <<var_dns_server_ip>> Im Feld IP-Adresse des DNS-Servers.

   Sie können mehrere IP-Adressen des DNS-Servers eingeben.

e. Eingabe <<var_ntp_server_ip>> Im Feld primärer NTP-Server.

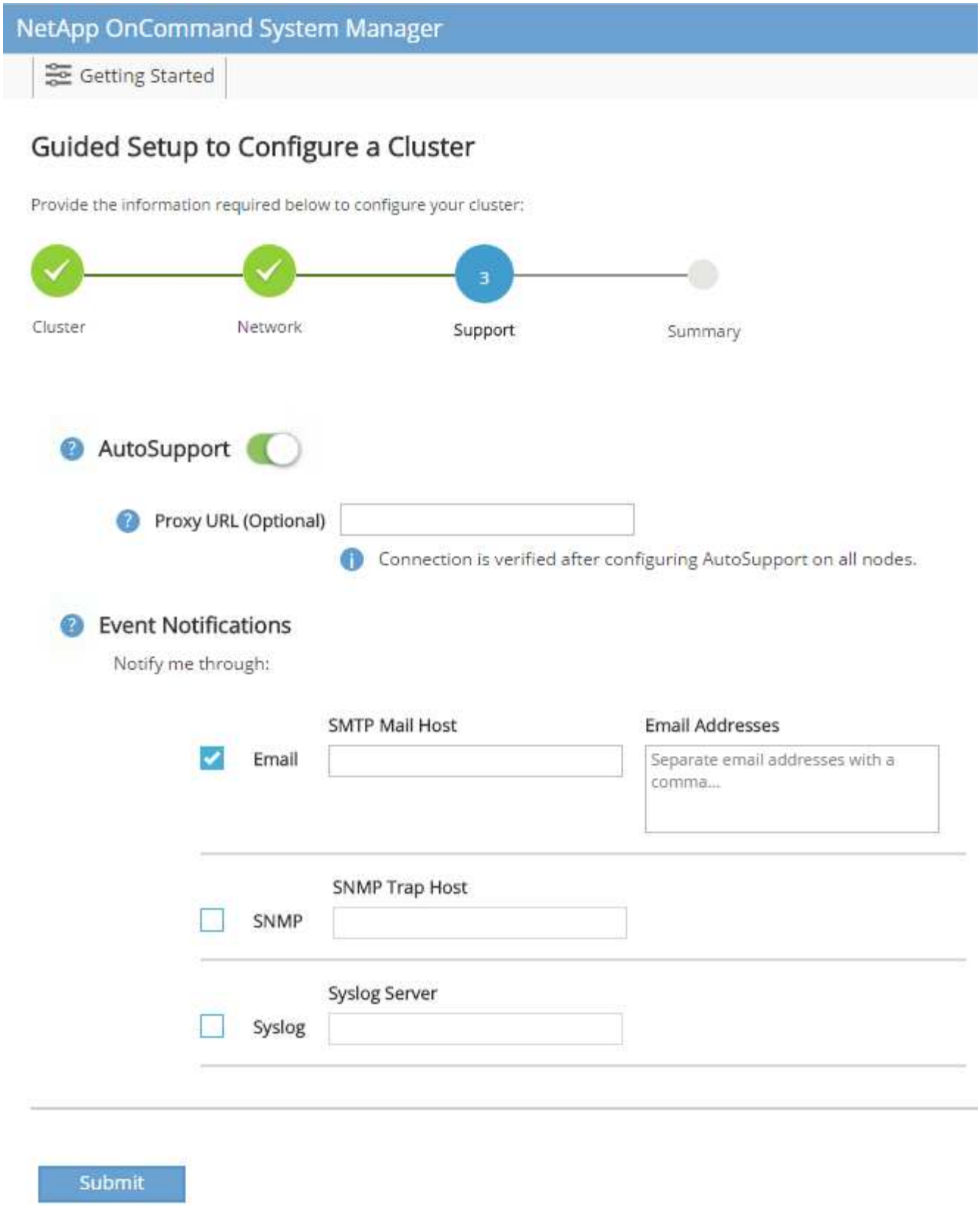
   Sie können auch einen alternativen NTP-Server eingeben.

8. Konfigurieren Sie die Support-Informationen.

   a. Wenn in Ihrer Umgebung ein Proxy für den Zugriff auf AutoSupport erforderlich ist, geben Sie die URL unter Proxy-URL ein.

   b. Geben Sie den SMTP-Mail-Host und die E-Mail-Adresse für Ereignisbenachrichtigungen ein.

      Sie müssen mindestens die Methode für die Ereignisbenachrichtigung einrichten, bevor Sie fortfahren können. Sie können eine beliebige der Methoden auswählen.



9. Klicken Sie, wenn angegeben wird, dass die Cluster-Konfiguration abgeschlossen ist, auf Manage Your Cluster, um den Storage zu konfigurieren.

Fortführung der Storage-Cluster-Konfiguration

Nach der Konfiguration der Storage-Nodes und des Basis-Clusters können Sie die Konfiguration des Storage-Clusters fortsetzen.

Alle freien Festplatten auf Null stellen

Führen Sie den folgenden Befehl aus, um alle freien Festplatten im Cluster zu löschen:

```
disk zerospares
```

Onboard-UTA2-Ports als Persönlichkeit festlegen

1. Überprüfen Sie den aktuellen Modus und den aktuellen Typ der Ports, indem Sie den ausführen `ucadmin show` Befehl.

```
AFF A220::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. Überprüfen Sie, ob der aktuelle Modus der verwendeten Ports lautet `cna` Und dass der aktuelle Typ auf festgelegt ist `target`. Wenn nicht, ändern Sie die Portpersönlichkeit mit dem folgenden Befehl:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Die Ports müssen offline sein, um den vorherigen Befehl auszuführen. Führen Sie den folgenden Befehl aus, um einen Port offline zu schalten:

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

Wenn Sie die Port-Persönlichkeit geändert haben, müssen Sie jeden Node neu booten, damit die Änderung wirksam wird.

Logische Management-Schnittstellen (LIFs) umbenennen

Um die Management-LIFs umzubenennen, führen Sie die folgenden Schritte aus:

1. Zeigt die aktuellen Management-LIF-Namen an.

```
network interface show –vserver <<clustername>>
```

2. Benennen Sie die Cluster-Management-LIF um.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Benennen Sie die Management-LIF für Node B um.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

Legen Sie für das Cluster-Management den automatischen Wechsel zurück

Stellen Sie die ein `auto-revert` Parameter auf der Cluster-Managementoberfläche.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Richten Sie die Service Processor-Netzwerkschnittstelle ein

Um dem Service-Prozessor auf jedem Node eine statische IPv4-Adresse zuzuweisen, führen Sie die folgenden Befehle aus:

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Die Service-Prozessor-IP-Adressen sollten sich im gleichen Subnetz wie die Node-Management-IP-Adressen befinden.

Aktivieren Sie Storage-Failover in ONTAP

Führen Sie die folgenden Befehle in einem Failover-Paar aus, um zu überprüfen, ob das Storage-Failover aktiviert ist:

1. Überprüfen Sie den Status des Storage-Failovers.

   ```
   storage failover show
   ```

   Beides `<<var_nodeA>>` Und `<<var_nodeB>>` Muss in der Lage sein, ein Takeover durchzuführen. Fahren Sie mit Schritt 3 fort, wenn die Knoten ein Takeover durchführen können.

2. Aktivieren Sie Failover bei einem der beiden Nodes.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

   Durch die Aktivierung von Failover auf einem Node wird dies für beide Nodes möglich.

3. Überprüfen Sie den HA-Status des Clusters mit zwei Nodes.

   Dieser Schritt gilt nicht für Cluster mit mehr als zwei Nodes.

   ```
   cluster ha show
   ```

4. Fahren Sie mit Schritt 6 fort, wenn Hochverfügbarkeit konfiguriert ist. Wenn die Hochverfügbarkeit konfiguriert ist, wird bei Ausgabe des Befehls die folgende Meldung angezeigt:

   ```
   High Availability Configured: true
   ```

5. Aktivieren Sie nur den HA-Modus für das Cluster mit zwei Nodes.

   ⓘ Führen Sie diesen Befehl nicht für Cluster mit mehr als zwei Nodes aus, da es zu Problemen mit Failover kommt.

   ```
   cluster ha modify -configured true
   Do you want to continue? {y|n}: y
   ```

6. Überprüfung der korrekten Konfiguration von Hardware-Unterstützung und ggf. Änderung der Partner-IP-Adresse

   ```
   storage failover hwassist show
   ```

   Die Nachricht `Keep Alive Status : Error: did not receive hwassist keep alive`

`alerts from partner` Zeigt an, dass die Hardware-Unterstützung nicht konfiguriert ist. Führen Sie die folgenden Befehle aus, um die Hardware-Unterstützung zu konfigurieren.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Jumbo Frame MTU Broadcast-Domäne in ONTAP erstellen

Um eine Data Broadcast-Domäne mit einer MTU von 9000 zu erstellen, führen Sie die folgenden Befehle aus:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Entfernen Sie Daten-Ports aus der Standard-Broadcast-Domäne

Die 10-GbE-Daten-Ports werden für iSCSI/NFS-Datenverkehr verwendet, diese Ports sollten aus der Standarddomäne entfernt werden. Die Ports e0e und e0f werden nicht verwendet und sollten auch aus der Standarddomäne entfernt werden.

Führen Sie den folgenden Befehl aus, um die Ports aus der Broadcast-Domäne zu entfernen:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deaktivieren Sie die Flusssteuerung bei UTA2-Ports

Eine NetApp Best Practice ist es, die Flusskontrolle bei allen UTA2-Ports, die mit externen Geräten verbunden sind, zu deaktivieren. Um die Flusssteuerung zu deaktivieren, führen Sie den folgenden Befehl aus:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Konfigurieren Sie IFGRP LACP in ONTAP

Diese Art von Interface Group erfordert zwei oder mehr Ethernet-Schnittstellen und einen Switch, der LACP unterstützt. Stellen Sie sicher, dass der Switch ordnungsgemäß konfiguriert ist.

Führen Sie an der Cluster-Eingabeaufforderung die folgenden Schritte aus.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Konfigurieren Sie Jumbo Frames in NetApp ONTAP

Um einen ONTAP-Netzwerkport zur Verwendung von Jumbo Frames zu konfigurieren (die in der Regel über eine MTU von 9,000 Byte verfügen), führen Sie die folgenden Befehle aus der Cluster-Shell aus:

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Erstellen von VLANs in ONTAP

Gehen Sie wie folgt vor, um VLANs in ONTAP zu erstellen:

1. Erstellen von NFS-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. Erstellen von iSCSI-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. ERSTELLUNG VON MGMT-VLAN-Ports

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Erstellen von Aggregaten in ONTAP

Während der ONTAP-Einrichtung wird ein Aggregat mit dem Root-Volume erstellt. Zum Erstellen weiterer Aggregate ermitteln Sie den Namen des Aggregats, den Node, auf dem er erstellt werden soll, und die Anzahl der enthaltenen Festplatten.

Führen Sie zum Erstellen von Aggregaten die folgenden Befehle aus:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Bewahren Sie mindestens eine Festplatte (wählen Sie die größte Festplatte) in der Konfiguration als Ersatzlaufwerk auf. Als Best Practice empfiehlt es sich, mindestens ein Ersatzteil für jeden Festplattentyp und jede Größe zu besitzen.

Beginnen Sie mit fünf Festplatten. Wenn zusätzlicher Storage erforderlich ist, können Sie einem Aggregat Festplatten hinzufügen.

Das Aggregat kann erst erstellt werden, wenn die Daten auf der Festplatte auf Null gesetzt werden. Führen Sie die aus `aggr show` Befehl zum Anzeigen des Erstellungsstatus des Aggregats. Fahren Sie erst fort `aggr1`_`nodeA` Ist online.

Konfigurieren Sie die Zeitzone in ONTAP

Führen Sie den folgenden Befehl aus, um die Zeitsynchronisierung zu konfigurieren und die Zeitzone auf dem Cluster festzulegen:

```
timezone <<var_timezone>>
```

Beispielsweise ist die Zeitzone im Osten der USA `America/New York`. Nachdem Sie mit der Eingabe des Zeitzonennamens begonnen haben, drücken Sie die Tabulatortaste, um die verfügbaren Optionen anzuzeigen.

Konfigurieren Sie SNMP in ONTAP

Führen Sie die folgenden Schritte aus, um die SNMP zu konfigurieren:

1. Konfigurieren Sie SNMP-Basisinformationen, z. B. Standort und Kontakt. Wenn Sie abgefragt werden, werden diese Informationen als angezeigt `sysLocation` Und `sysContact` Variablen in SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Konfigurieren Sie SNMP-Traps zum Senden an Remote-Hosts.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Konfigurieren Sie SNMPv1 in ONTAP

Um SNMPv1 zu konfigurieren, stellen Sie das freigegebene geheime Klartextkennwort ein, das als Community bezeichnet wird.

```
snmp community add ro <<var_snmp_community>>
```

Verwenden Sie die `snmp community delete all` Befehl mit Vorsicht. Wenn Community Strings für andere Überwachungsprodukte verwendet werden, entfernt dieser Befehl sie.

Konfigurieren Sie SNMPv3 in ONTAP

SNMPv3 erfordert, dass Sie einen Benutzer für die Authentifizierung definieren und konfigurieren. Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren:

1. Führen Sie die aus `security snmpusers` Befehl zum Anzeigen der Engine-ID.
2. Erstellen Sie einen Benutzer mit dem Namen `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Geben Sie die Engine-ID der autorisierenden Einheit ein, und wählen Sie aus `md5` Als Authentifizierungsprotokoll.
4. Geben Sie bei der Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Authentifizierungsprotokoll ein.
5. Wählen Sie `des` Als Datenschutzprotokoll.
6. Geben Sie bei Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Datenschutzprotokoll ein.

Konfigurieren Sie AutoSupport HTTPS in ONTAP

Das NetApp AutoSupport Tool sendet Zusammenfassung von Support-Informationen über HTTPS an NetApp. Führen Sie den folgenden Befehl aus, um AutoSupport zu konfigurieren:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Erstellen Sie eine Speicher-Virtual Machine

Um eine Storage Virtual Machine (SVM) für Infrastrukturen zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie die aus `vserver create` Befehl.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Das Datenaggregat wird zur Liste des Infrastruktur-SVM-Aggregats der NetApp VSC hinzugefügt.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Entfernen Sie die ungenutzten Storage-Protokolle der SVM, wobei NFS und iSCSI überlassen bleiben.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Aktivierung und Ausführung des NFS-Protokolls in der SVM Infrastructure

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. Schalten Sie das ein `SVM vstorage` Parameter für das NetApp NFS VAAI Plug-in. Überprüfen Sie dann, ob NFS konfiguriert wurde.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

Diese Befehle werden von ausgeführt `vserver` In der Befehlszeile, da Storage Virtual Machines zuvor Server genannt wurden.

Konfigurieren Sie NFSv3 in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
ESXi hostet Eine NFS-IP-Adresse	\<<var_esxi_hostA_nfs_ip>
ESXi Host B NFS-IP-Adresse	\<<var_esxi_hostB_nfs_ip>

Führen Sie die folgenden Befehle aus, um NFS auf der SVM zu konfigurieren:

1. Erstellen Sie eine Regel für jeden ESXi-Host in der Standard-Exportrichtlinie.
2. Weisen Sie für jeden erstellten ESXi Host eine Regel zu. Jeder Host hat seinen eigenen Regelindex. Ihr erster ESXi Host hat Regelindex 1, Ihr zweiter ESXi Host hat Regelindex 2 usw.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Weisen Sie die Exportrichtlinie dem Infrastruktur-SVM-Root-Volume zu.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

Die NetApp VSC verarbeitet automatisch die Exportrichtlinien, wenn Sie sie nach der Einrichtung von vSphere installieren möchten. Wenn Sie diese nicht installieren, müssen Sie Regeln für die Exportrichtlinie erstellen, wenn zusätzliche Server der Cisco UCS C-Serie hinzugefügt werden.

Erstellen Sie den iSCSI-Dienst in ONTAP

Gehen Sie wie folgt vor, um den iSCSI-Service zu erstellen:

1. Erstellen Sie den iSCSI-Service für die SVM. Mit diesem Befehl wird auch der iSCSI-Service gestartet und der iSCSI-IQN für die SVM festgelegt. Überprüfen Sie, ob iSCSI konfiguriert wurde.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Spiegelung zur Lastverteilung von SVM-Root-Volumes in ONTAP erstellen

1. Erstellen Sie ein Volume zur Load-Sharing-Spiegelung des SVM Root-Volumes der Infrastruktur auf jedem Node.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. Erstellen Sie einen Job-Zeitplan, um die Spiegelbeziehungen des Root-Volumes alle 15 Minuten zu aktualisieren.

```
job schedule interval create -name 15min -minutes 15
```

3. Erstellen Sie die Spiegelungsbeziehungen.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Initialisieren Sie die Spiegelbeziehung und überprüfen Sie, ob sie erstellt wurde.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Konfigurieren Sie HTTPS-Zugriff in ONTAP

Gehen Sie wie folgt vor, um den sicheren Zugriff auf den Storage Controller zu konfigurieren:

1. Erhöhen Sie die Berechtigungsebene, um auf die Zertifikatbefehle zuzugreifen.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. In der Regel ist bereits ein selbstsigniertes Zertifikat vorhanden. Überprüfen Sie das Zertifikat, indem Sie den folgenden Befehl ausführen:

```
security certificate show
```

3. Bei jeder angezeigten SVM sollte der allgemeine Zertifikatname mit dem DNS-FQDN der SVM übereinstimmen. Die vier Standardzertifikate sollten gelöscht und durch selbstsignierte Zertifikate oder Zertifikate einer Zertifizierungsstelle ersetzt werden.

   Das Löschen abgelaufener Zertifikate vor dem Erstellen von Zertifikaten ist eine bewährte Vorgehensweise. Führen Sie die aus `security certificate delete` Befehl zum Löschen abgelaufener Zertifikate. Verwenden Sie im folgenden Befehl DIE REGISTERKARTEN-Vervollständigung, um jedes Standardzertifikat auszuwählen und zu löschen.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Um selbstsignierte Zertifikate zu generieren und zu installieren, führen Sie die folgenden Befehle als einmalige Befehle aus. Ein Serverzertifikat für die Infrastruktur-SVM und die Cluster-SVM generieren. Verwenden Sie wieder die REGISTERKARTEN-Vervollständigung, um Sie beim Ausfüllen dieser Befehle zu unterstützen.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Um die Werte für die im folgenden Schritt erforderlichen Parameter zu erhalten, führen Sie den aus `security certificate show` Befehl.

6. Aktivieren Sie jedes Zertifikat, das gerade mit erstellt wurde `-server-enabled true` Und `-client-enabled false` Parameter. Verwenden Sie erneut DIE REGISTERKARTEN-Vervollständigung.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Konfigurieren und aktivieren Sie den SSL- und HTTPS-Zugriff und deaktivieren Sie den HTTP-Zugriff.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
–vserver <<var_clustername>>
```

Es ist normal, dass einige dieser Befehle eine Fehlermeldung ausgeben, die angibt, dass der Eintrag nicht vorhanden ist.

8. Kehren Sie zur Berechtigungsstufe für den Administrator zurück, und erstellen Sie das Setup, damit SVM über das Internet verfügbar ist.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Erstellen Sie in ONTAP ein NetApp FlexVol Volume

Um ein NetApp FlexVol Volume zu erstellen, geben Sie den Namen, die Größe und das Aggregat ein, auf dem es vorhanden ist. Erstellung von zwei VMware Datastore Volumes und einem Server Boot Volume

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Aktivieren Sie die Deduplizierung in ONTAP

Um die Deduplizierung auf entsprechenden Volumes zu aktivieren, führen Sie folgende Befehle aus:

```
volume efficiency on –vserver Infra-SVM -volume infra_datastore_1
volume efficiency on –vserver Infra-SVM -volume esxi_boot
```

Erstellen Sie LUNs in ONTAP

Führen Sie die folgenden Befehle aus, um zwei Boot-LUNs zu erstellen:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Beim Hinzufügen eines zusätzlichen Cisco UCS C-Series Servers muss eine zusätzliche Boot-LUN erstellt werden.

Erstellen von iSCSI LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Speicherknoten A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Speicherknoten A iSCSI-LIF01A-Netzwerkmaske	<<var_nodeA_iscsi_lif01a_Mask>>
Speicherknoten A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Speicherknoten Eine iSCSI-LIF01B-Netzwerkmaske	<<var_nodeA_iscsi_lif01b_Mask>>
Storage-Node B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Speicherknoten B iSCSI-LIF01A-Netzwerkmaske	<<var_nodeB_iscsi_lif01a_Mask>>
Storage Node B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
Speicherknoten B iSCSI-LIF01B-Netzwerkmaske	<<var_nodeB_iscsi_lif01b_Mask>>

1. Erstellen Sie vier iSCSI LIFs, zwei pro Node.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Erstellen von NFS LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Storage-Node A NFS LIF 01 IP	<<var_nodeA_nfs_lif_01_ip>>
Storage Node A NFS LIF 01-Netzwerkmaske	<<var_nodeA_nfs_lif_01_maska>>
Storage-Node B NFS LIF 02-IP	<<var_nodeB_nfs_lif_02_ip>>
Storage Node B NFS LIF 02 Netzwerkmaske	<<var_nodeB_nfs_lif_02_maska>>

1. Erstellen Sie ein NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Hinzufügen eines SVM-Administrators für die Infrastruktur

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Vsmgmt-IP	<<var_svm_mgmt_ip>>
Vsmgmt-Netzwerkmaske	<<var_svm_mgmt_maska>>
Vsmgmt Standard-Gateway	<<var_svm_mgmt_Gateway>>

So fügen Sie dem Managementnetzwerk den SVM-Administrator und die logische SVM-Administrationsoberfläche der Infrastruktur hinzu:

1. Führen Sie den folgenden Befehl aus:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> Die SVM-Management-IP sollte sich hier im selben Subnetz wie die Storage-Cluster-Management-IP befinden.

2. Erstellen Sie eine Standardroute, damit die SVM-Managementoberfläche die Außenwelt erreichen kann.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Legen Sie ein Passwort für den SVM vsadmin-Benutzer fest und entsperren Sie den Benutzer.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Weiter: Cisco UCS C-Series Rack Server Deployment Procedure"

Cisco UCS C-Serie Rack-Server-Implementierung Verfahren

Der folgende Abschnitt enthält ein detailliertes Verfahren zur Konfiguration eines Standalone-Rack-Servers der Cisco UCS C-Serie zur Verwendung in der FlexPod Express-Konfiguration.

Führen Sie die Ersteinrichtung für den Standalone-Server der Cisco UCS C-Serie für den Cisco Integrated Management Server durch

Führen Sie diese Schritte für die Ersteinrichtung der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie durch.

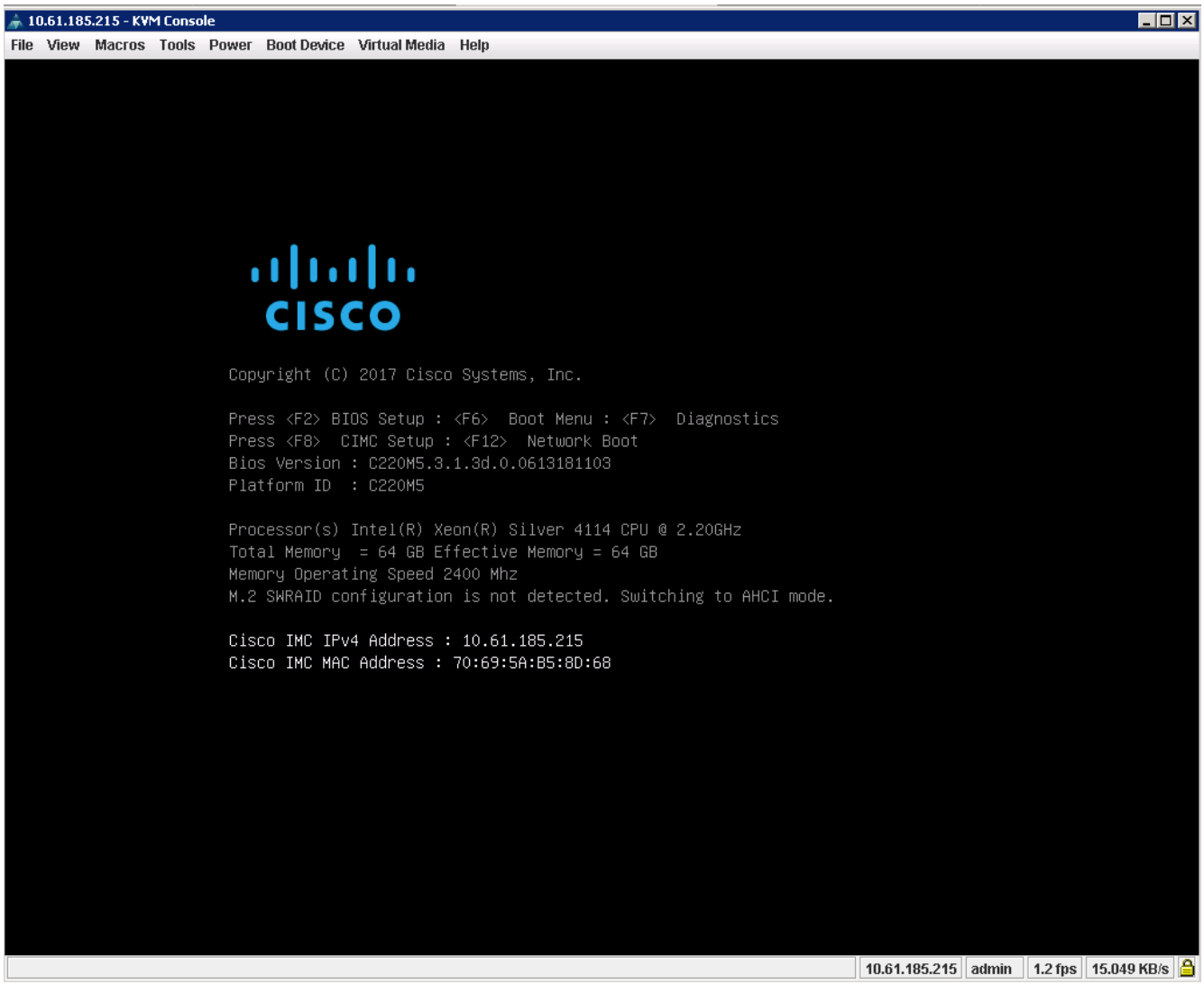
In der folgenden Tabelle sind die Informationen aufgeführt, die für die Konfiguration von CIMC für jeden Standalone-Server der Cisco UCS C-Serie erforderlich sind.

Details	Detailwert
CIMC-IP-Adresse	<<cimc_ip>>
CIMC-Subnetzmaske	<<cimc_Netzmaske>>
CIMC-Standard-Gateway	<<cimc_Gateway>>

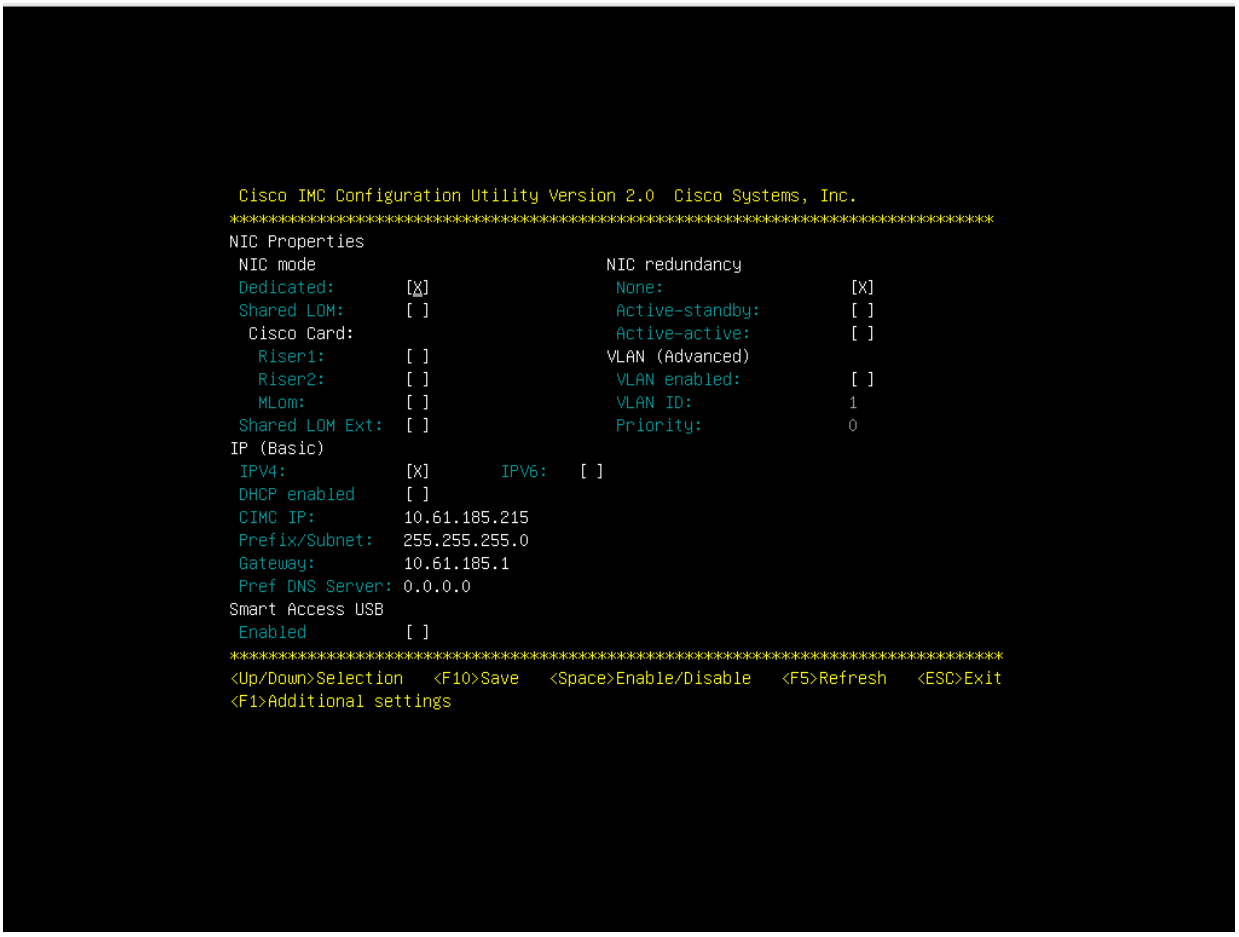
Die CIMC-Version, die in dieser Validierung verwendet wird, ist CIMC 3.1.3(g).

Alle Server

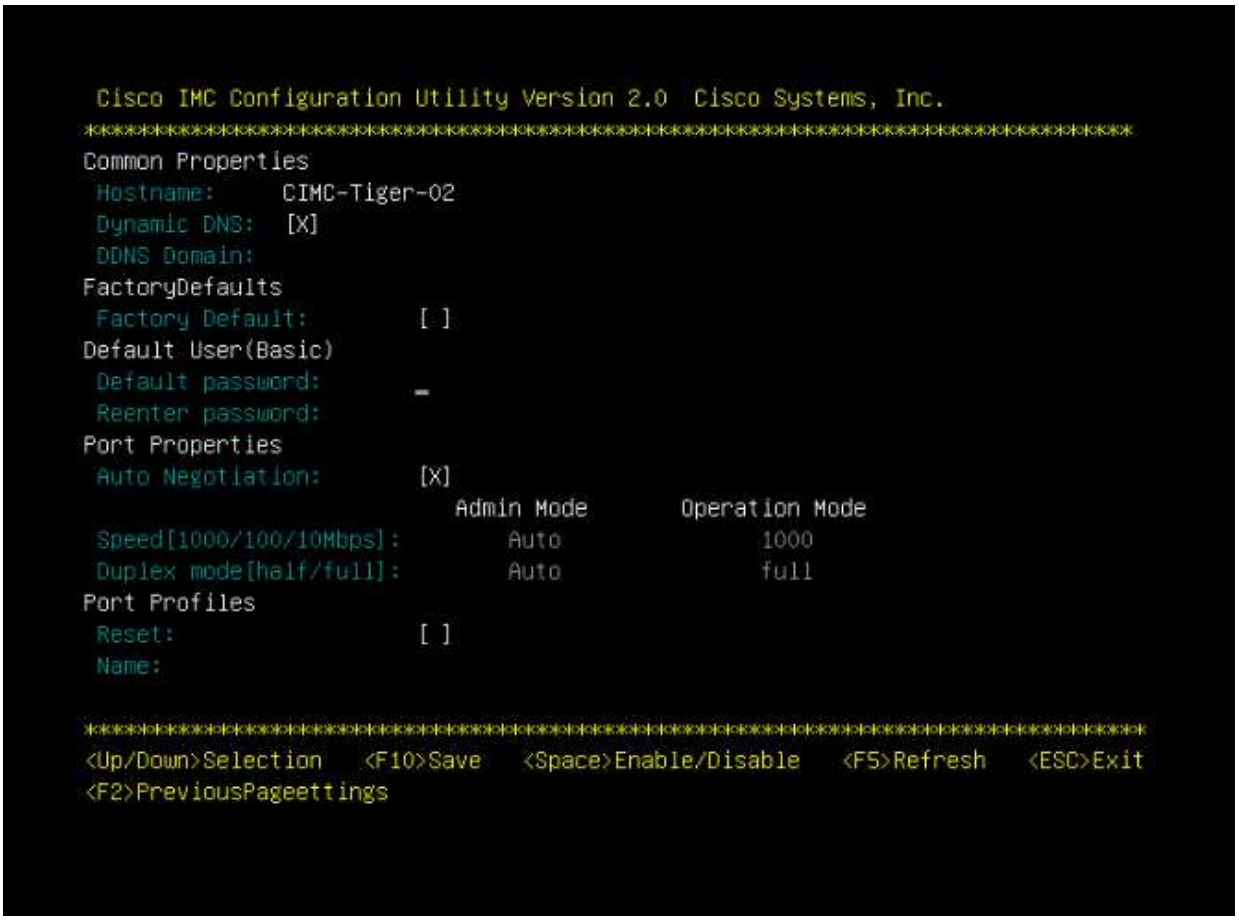
1. Schließen Sie den Cisco Keyboard-, Video- und Mausdongle (KVM) (im Lieferumfang des Servers enthalten) an den KVM-Port an der Vorderseite des Servers an. Schließen Sie einen VGA-Monitor und eine USB-Tastatur an die entsprechenden KVM-Dongle-Ports an.
2. Schalten Sie den Server ein, und drücken Sie F8, wenn Sie dazu aufgefordert werden, die CIMC-Konfiguration einzugeben.



3. Legen Sie im CIMC-Konfigurationsprogramm die folgenden Optionen fest:
   - NIC-Modus (Network Interface Card):
     - Dediziert [X]
   - IP (Basis):
     - IPV4: [X]
     - DHCP aktiviert: [ ]
     - CIMC-IP: <<cimc_ip>>
     - Präfix/Subnetz: <<cimc_Netmask>>
     - Gateway: <<cimc_Gateway>>
   - VLAN (erweitert): Lassen Sie das Kontrollkästchen deaktiviert, um VLAN-Tagging zu deaktivieren.
     - NIC-Redundanz
     - Keine: [X]



4. Drücken Sie F1, um weitere Einstellungen anzuzeigen.
   - Allgemeine Eigenschaften:
     - Host-Name: <<esxi_Host_Name>>
     - Dynamisches DNS: [ ]
     - Werkseinstellungen: Löschen.
   - Standardbenutzer (Basic):
     - Standardpasswort: <<admin_password>>
     - Geben Sie das Passwort erneut ein: <<admin_password>>
     - Port-Eigenschaften: Standardwerte verwenden.
     - Portprofile: Lassen Sie das Löschen.



5. Drücken Sie F10, um die Konfiguration der CIMC-Schnittstelle zu speichern.
6. Drücken Sie nach dem Speichern der Konfiguration Esc, um den Vorgang zu beenden.

Konfigurieren Sie den iSCSI-Start von Cisco UCS C-Series Servern

In dieser FlexPod Express-Konfiguration wird der VIC1387 für das iSCSI-Booten verwendet.

In der folgenden Tabelle werden die Informationen aufgeführt, die für die Konfiguration des iSCSI-Startens erforderlich sind.

Kursiv formatierte Schriftart zeigt Variablen an, die für jeden ESXi-Host eindeutig sind.

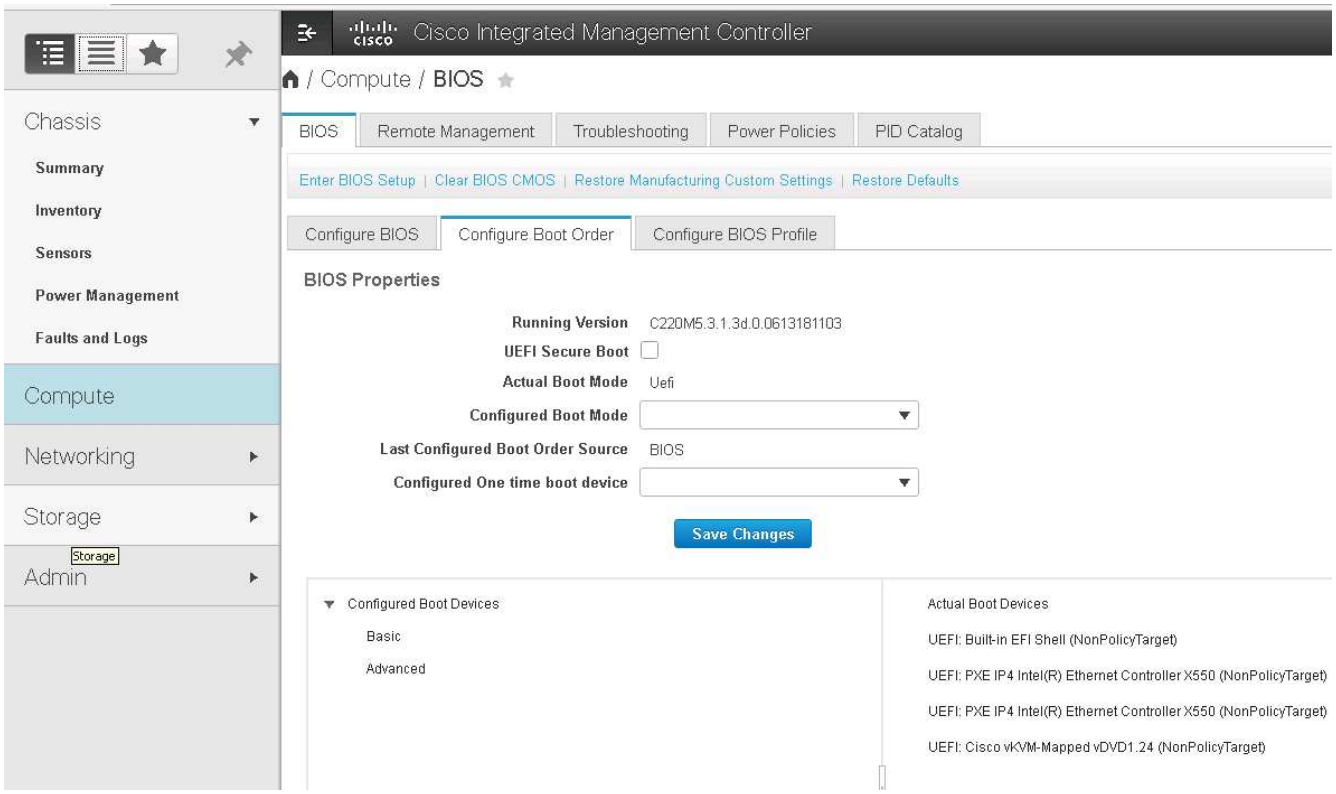
Details	Detailwert
ESXi Host-Initiator Ein Name	<<var_ucs_Initiator_Name_A>>
ESXi Host, iSCSI A IP	<<var_esxi_Host_iscsiA_ip>>
ESXi-Host, iSCSI-A-Netzwerkmaske	<<var_esxi_Host_iscsiA_Maska>>
ESXi Host iSCSI Ein Standard-Gateway	\<<var_esxi_Host_iscsiA_Gateway>
ESXi Host-Initiator B-Name	\<<var_ucs_Initiator_Name_B>
ESXi-Host, iSCSI-B-IP	<<var_esxi_Host_iscsiB_ip>>
ESXi-Host-iSCSI-B-Netzwerkmaske	<<var_esxi_Host_iscsiB_Maska>>
ESXi Host iSCSI-B-Gateway	\<<var_esxi_Host_iscsiB_Gateway>

Details	Detailwert
IP-Adresse iscsi_lif01a	
IP-Adresse iscsi_lif02a	
IP-Adresse iscsi_lif01b	
IP-Adresse iscsi_lif02b	
Infra_SVM IQN	

Konfiguration der Startreihenfolge

Gehen Sie wie folgt vor, um die Konfiguration der Startreihenfolge festzulegen:

1. Klicken Sie im Browser-Fenster der CIMC-Schnittstelle auf die Registerkarte Server, und wählen Sie BIOS aus.
2. Klicken Sie auf Startreihenfolge konfigurieren, und klicken Sie dann auf OK.



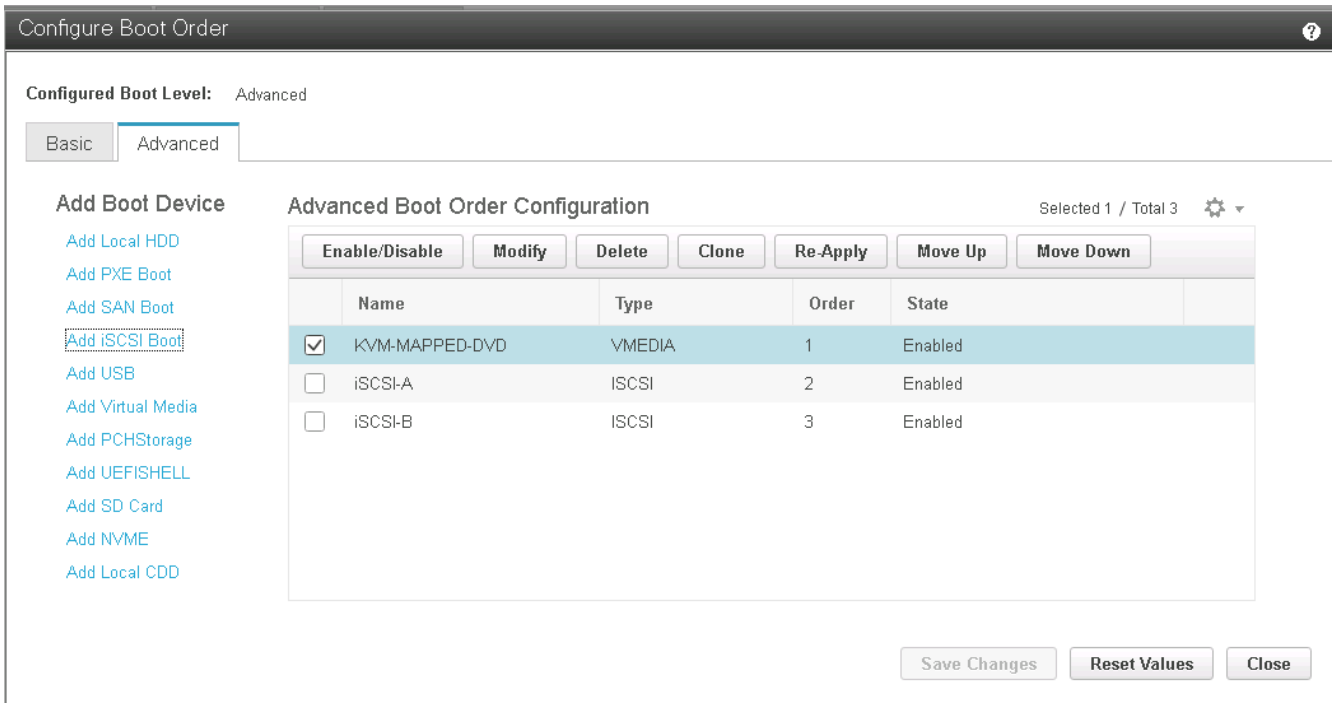
3. Konfigurieren Sie die folgenden Geräte, indem Sie unter Startgerät hinzufügen auf das Gerät klicken und zur Registerkarte Erweitert wechseln.
   - Fügen Sie Einen Virtuellen Datenträger Hinzu
     - NAME: KVM-CD-DVD
     - UNTERTYP: KVM GEMAPPTEN DVD
     - Status: Aktiviert
     - Bestellung: 1
   - Fügen Sie iSCSI Boot hinzu.

- Name: ISCSI-A
- Status: Aktiviert
- Bestellung: 2
- Schlitz: MLOM
- Port: 0

◦ Klicken Sie auf iSCSI Boot hinzufügen.

- Name: ISCSI-B
- Status: Aktiviert
- Bestellung: 3
- Schlitz: MLOM
- Anschluss: 1

4. Klicken Sie Auf Gerät Hinzufügen.
5. Klicken Sie auf Änderungen speichern und dann auf Schließen.

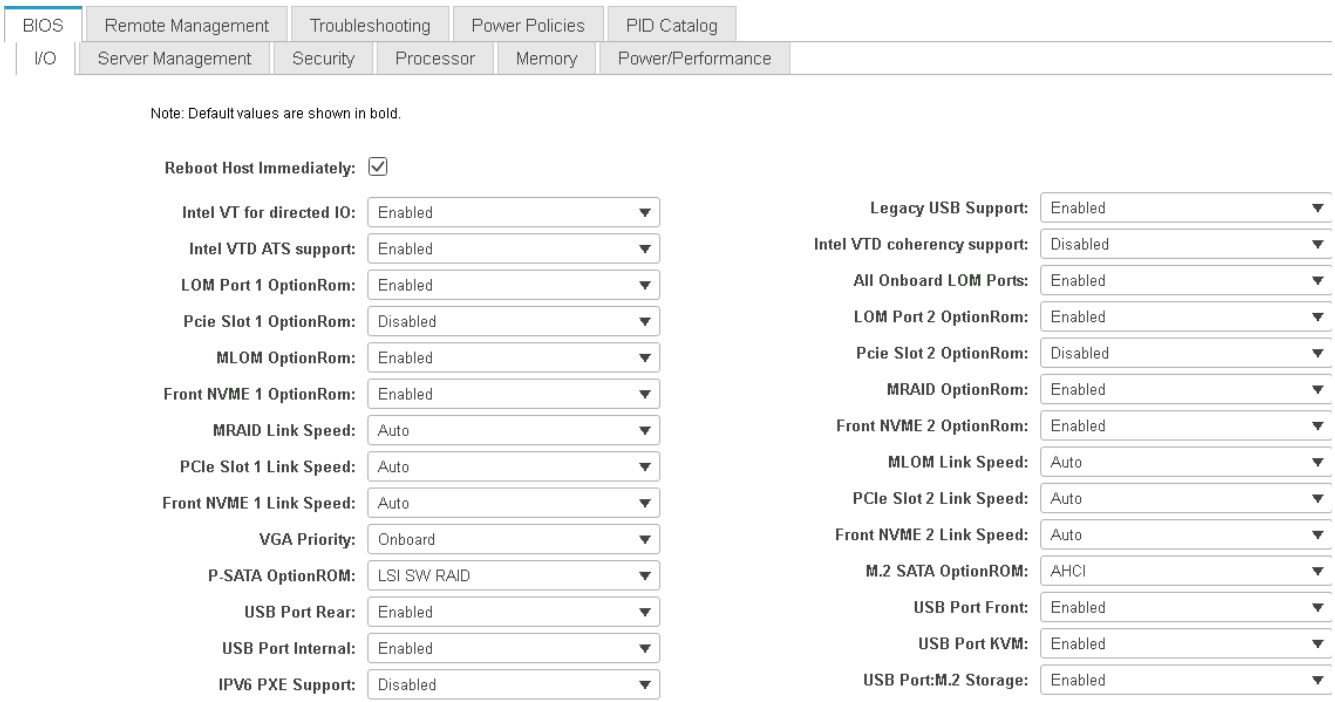


6. Starten Sie den Server neu, um mit Ihrer neuen Startreihenfolge zu starten.

Deaktivieren des RAID-Controllers (falls vorhanden)

Führen Sie die folgenden Schritte aus, wenn Ihr C-Series-Server einen RAID-Controller enthält. Beim Booten der SAN-Konfiguration ist kein RAID-Controller erforderlich. Optional können Sie den RAID-Controller auch physisch vom Server entfernen.

1. Klicken Sie im linken Navigationsbereich in CIMC auf BIOS.
2. Wählen Sie BIOS konfigurieren.
3. Blättern Sie nach unten zu PCIe Slot:HBA Option ROM.
4. Wenn der Wert nicht bereits deaktiviert ist, setzen Sie ihn auf deaktiviert.



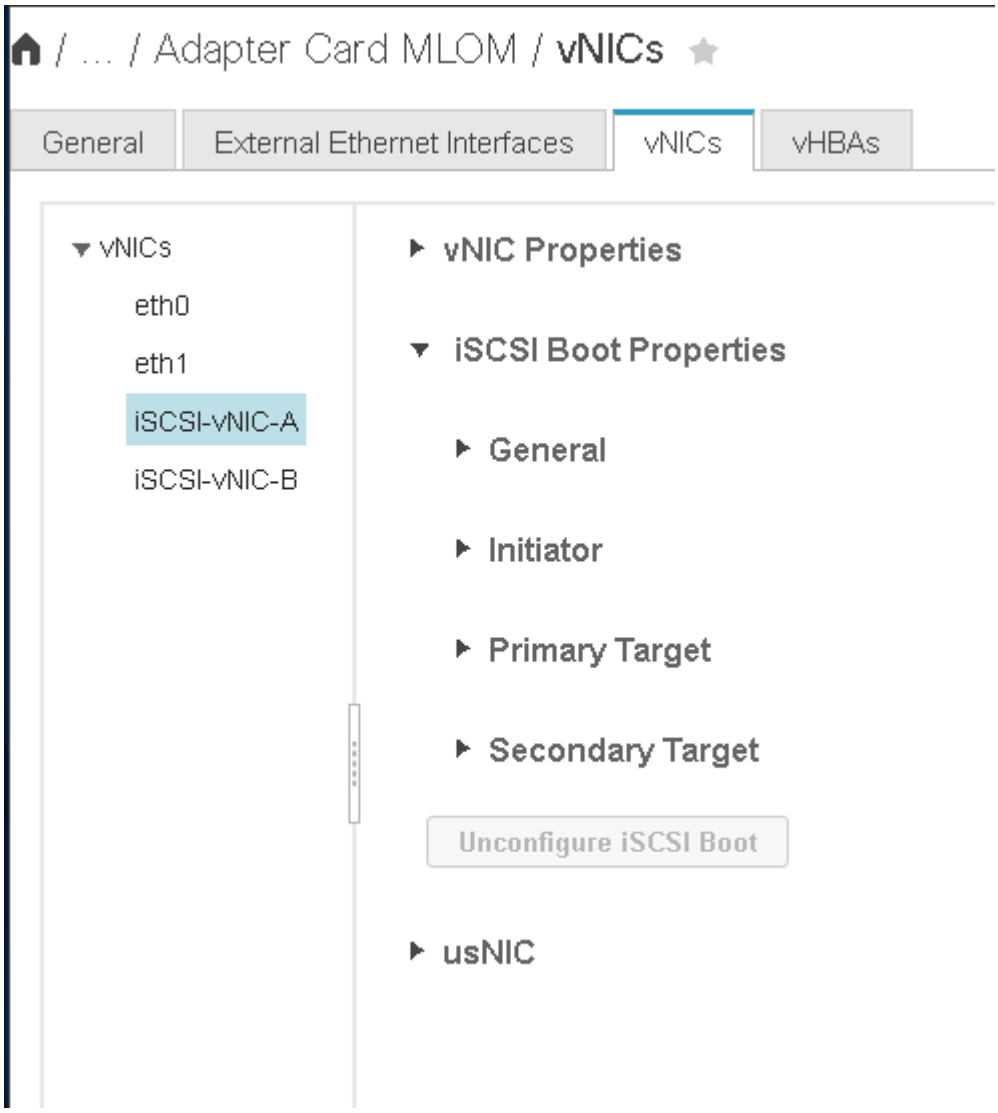
Konfigurieren Sie Cisco VIC1387 für iSCSI Boot

Die folgenden Konfigurationsschritte gelten für den Cisco VIC 1387 für iSCSI Boot.

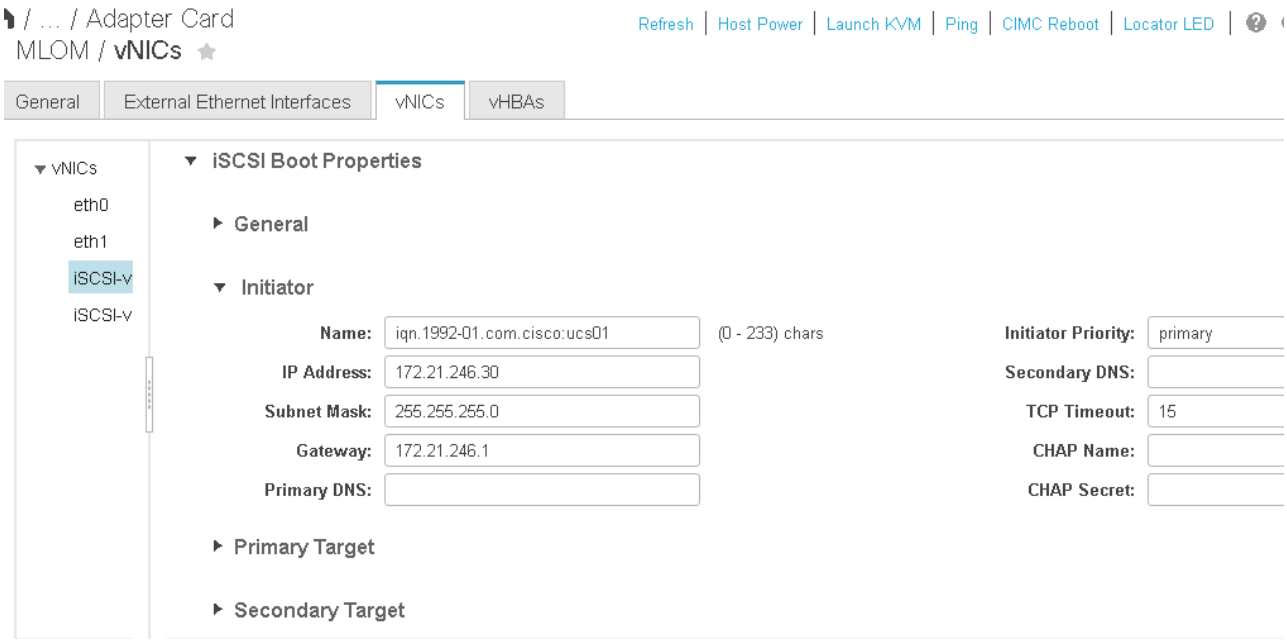
Erstellen von iSCSI-vNICs

1. Klicken Sie auf Hinzufügen, um einen vNIC zu erstellen.
2. Geben Sie im Abschnitt vNIC hinzufügen die folgenden Einstellungen ein:
   - Name: ISCSI-vNIC-A
   - MTU: 9000
   - Standard-VLAN: `<<var_iscsi_vlan_a>>`
   - VLAN-Modus: TRUNK
   - PXE-Start aktivieren: Prüfen

3. Klicken Sie auf vNIC hinzufügen und dann auf OK.
4. Wiederholen Sie den Vorgang, um einen zweiten vNIC hinzuzufügen.
   a. Benennen Sie die vNIC `iSCSI-vNIC-B`.
   b. Eingabe `<<var_iscsi_vlan_b>>` Als VLAN.
   c. Setzen Sie den Uplink-Port auf `1`.
5. Wählen Sie die vNIC aus `iSCSI-vNIC-A` Auf der linken Seite.



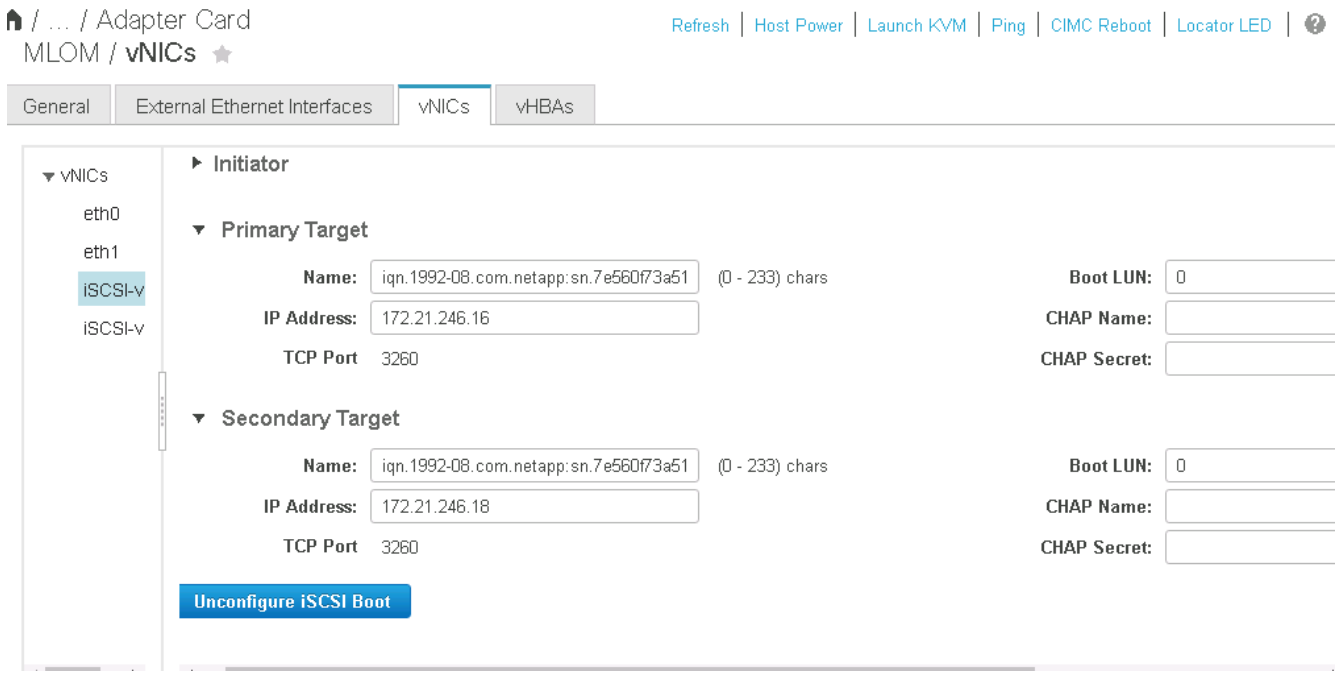
6. Geben Sie unter iSCSI Boot Properties die Initiator-Details ein:
   - Name: <<var_ucsa_Initiator_Name_a>>
   - IP-Adresse: <<var_esxi_hostA_iscsiA_ip>>
   - Subnetzmaske: <<var_esxi_hostA_iscsiA_maska>>
   - Gateway: <<var_esxi_hostA_iscsiA_Gateway>>



7. Geben Sie die Details des primären Ziels ein.
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von `iscsi_lif01a`
   - Boot-LUN: 0
8. Geben Sie die Details des sekundären Ziels ein.
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von `iscsi_lif02a`
   - Boot-LUN: 0

   Sie können die Speicher-IQN-Nummer abrufen, indem Sie den ausführen `vserver iscsi show` Befehl.

   Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.



9. Klicken Sie auf iSCSI konfigurieren.
10. Wählen Sie die vNIC aus `iSCSI-vNIC- B` Und klicken Sie auf die Schaltfläche iSCSI-Start oben im Abschnitt Host-Ethernet-Schnittstellen.
11. Wiederholen Sie den zu konfigurierenden Vorgang `iSCSI-vNIC-B`.
12. Geben Sie die Initiator-Details ein.
    - Name: `<<var_ucsa_initiator_name_b>>`
    - IP-Adresse: `<<var_esxi_hostb_iscsib_ip>>`
    - Subnetzmaske: `<<var_esxi_hostb_iscsib_mask>>`
    - Gateway: `<<var_esxi_hostb_iscsib_gateway>>`
13. Geben Sie die Details des primären Ziels ein.
    - Name: IQN-Nummer der Infrastruktur-SVM
    - IP-Adresse: IP-Adresse von `iscsi_lif01b`
    - Boot-LUN: 0
14. Geben Sie die Details des sekundären Ziels ein.
    - Name: IQN-Nummer der Infrastruktur-SVM
    - IP-Adresse: IP-Adresse von `iscsi_lif02b`
    - Boot-LUN: 0

    Sie können die Speicher-IQN-Nummer mit dem abrufen `vserver iscsi show` Befehl.

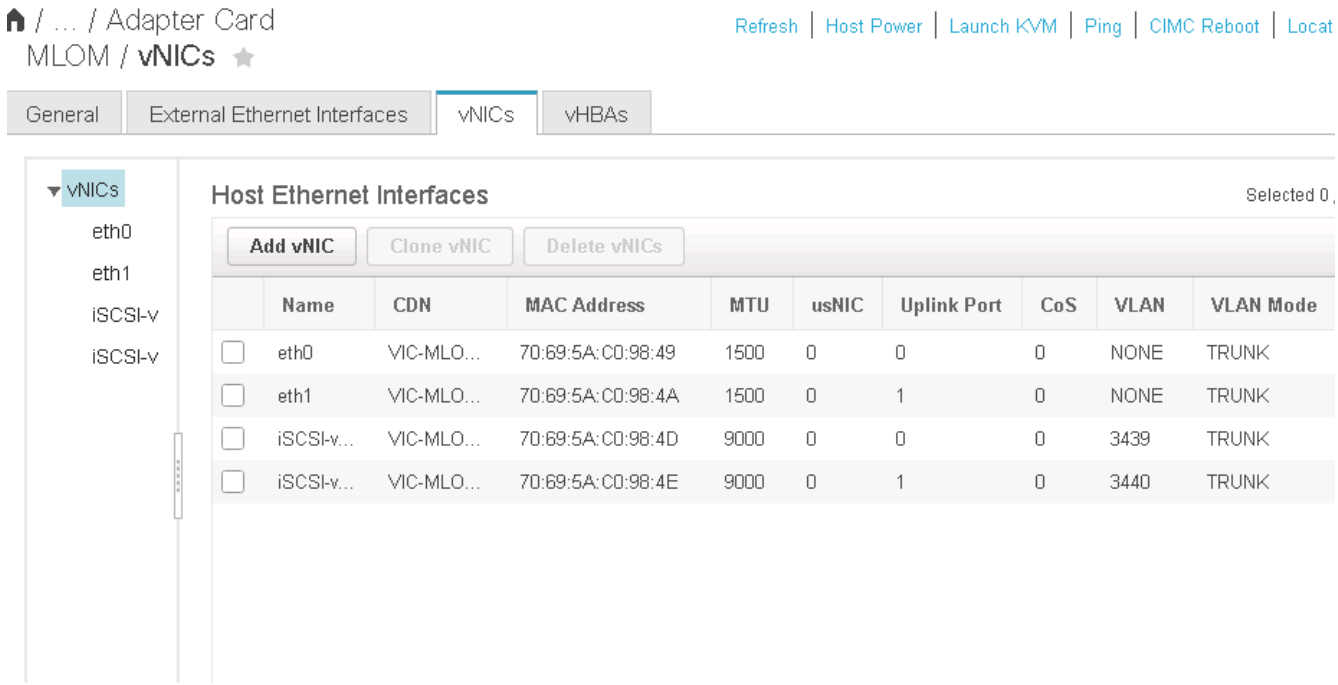
    Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.

15. Klicken Sie auf ISCSI konfigurieren.

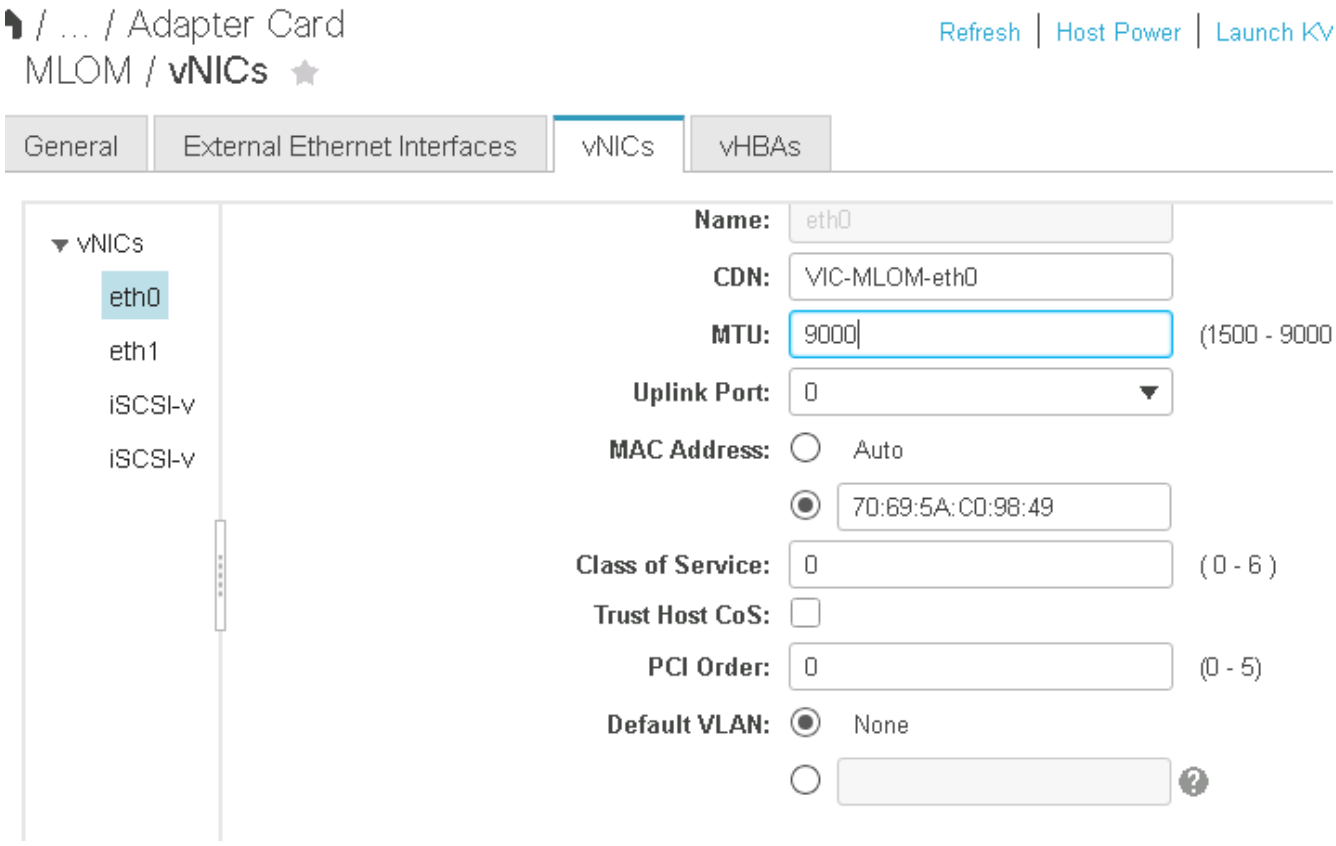
16. Wiederholen Sie diesen Vorgang, um iSCSI-Boot für Cisco UCS-Server B zu konfigurieren

Konfigurieren Sie vNICs für ESXi

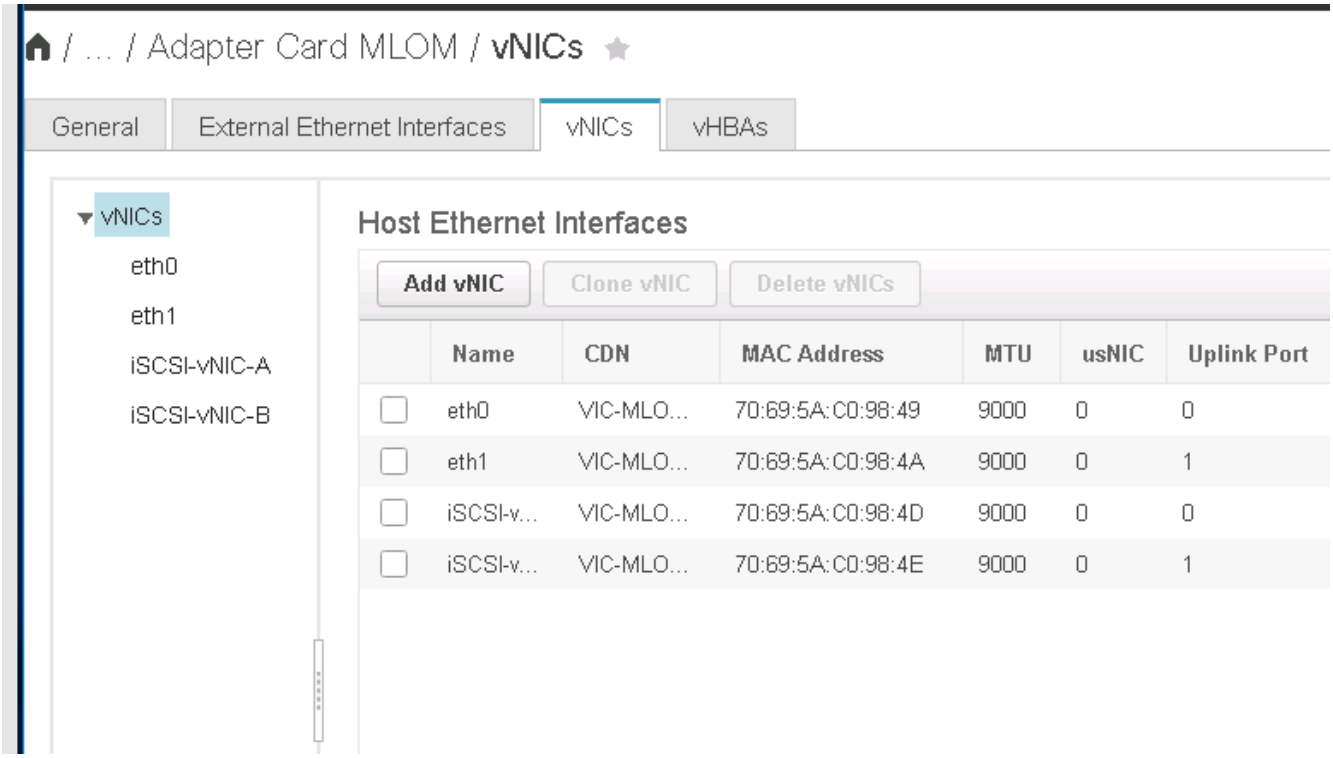
1. Klicken Sie im CIMC-Schnittstellenbrowser-Fenster auf Inventar und anschließend im rechten Fensterbereich auf Cisco VIC-Adapter.
2. Wählen Sie unter Adapterkarten Cisco UCS VIC 1387 aus und wählen Sie dann die darunter liegende vNICs aus.



3. Wählen Sie eth0 aus, und klicken Sie auf Eigenschaften.
4. Setzen Sie die MTU auf 9000. Klicken Sie Auf Änderungen Speichern.



5. Wiederholen Sie die Schritte 3 und 4 für eth1. Überprüfen Sie, ob der Uplink-Port auf festgelegt ist `1` Für eth1.



Dieses Verfahren muss für jeden ersten Cisco UCS Server-Knoten und jeden zusätzlichen Cisco UCS Server-Knoten, der der Umgebung hinzugefügt wurde, wiederholt werden.

"Weiter: NetApp Verfahren für die AFF-Storage-Implementierung (Teil 2)"

NetApp Verfahren zur Implementierung von AFF-Storage (Teil 2)

Einrichtung von ONTAP SAN Boot Storage

Erstellen von iSCSI-Initiatorgruppen

Um Initiatorgruppen zu erstellen, führen Sie den folgenden Schritt aus:

Für diesen Schritt benötigen Sie die iSCSI-Initiator-IQNs aus der Serverkonfiguration.

1. Führen Sie über die SSH-Verbindung des Cluster-Management-Node die folgenden Befehle aus. Um die drei in diesem Schritt erstellten Initiatorgruppen anzuzeigen, führen Sie den Befehl igroup show aus.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Dieser Schritt muss abgeschlossen sein, wenn zusätzliche Cisco UCS C-Series Server hinzugefügt werden.

Zuordnen von Boot-LUNs zu Initiatorgruppen

Führen Sie die folgenden Befehle aus der SSH-Verbindung für das Cluster-Management aus, um Boot-LUNs Initiatorgruppen zuzuordnen:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A –igroup
VM-Host-Infra- A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- B –igroup
VM-Host-Infra- B –lun-id 0
```

Dieser Schritt muss abgeschlossen sein, wenn zusätzliche Cisco UCS C-Series Server hinzugefügt werden.

"Weiter: VMware vSphere 6.7 Deployment Procedure."

Implementierungsverfahren für VMware vSphere 6.7

Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware ESXi 6.7 in einer FlexPod Express-Konfiguration. Die folgenden Implementierungsverfahren werden so angepasst, dass sie die in vorherigen Abschnitten beschriebenen Umgebungsvariablen enthalten.

Für die Installation von VMware ESXi in einer solchen Umgebung sind mehrere Methoden vorhanden. Dieses Verfahren verwendet die virtuelle KVM-Konsole und die virtuellen Medienfunktionen der CIMC-Schnittstelle für Server der Cisco UCS C-Serie, um Remote-Installationsmedien jedem einzelnen Server zuzuordnen.

Diese Prozedur muss für Cisco UCS Server A und Cisco UCS Server B abgeschlossen sein

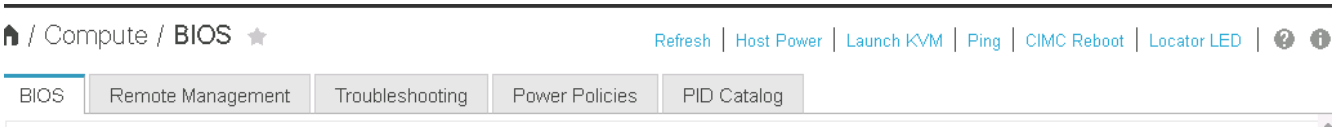
Für alle zusätzlichen Nodes, die dem Cluster hinzugefügt werden, muss dieser Vorgang abgeschlossen sein.

Melden Sie sich bei der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie an

Die folgenden Schritte beschreiben die Methode zur Anmeldung an der CIMC-Schnittstelle für Standalone-Server der Cisco UCS C-Serie. Sie müssen sich bei der CIMC-Schnittstelle anmelden, um die virtuelle KVM auszuführen, die es dem Administrator ermöglicht, die Installation des Betriebssystems über Remote-Medien zu starten.

Alle Hosts

1. Navigieren Sie zu einem Webbrowser, und geben Sie die IP-Adresse für die CIMC-Schnittstelle für die Cisco UCS C-Serie ein. In diesem Schritt wird die CIMC GUI-Anwendung gestartet.
2. Melden Sie sich bei der CIMC-UI mit dem Admin-Benutzernamen und den Anmeldedaten an.
3. Wählen Sie im Hauptmenü die Registerkarte Server aus.
4. Klicken Sie auf KVM-Konsole starten.



5. Wählen Sie in der virtuellen KVM-Konsole die Registerkarte Virtueller Datenträger aus.
6. Wählen Sie Karte CD/DVD.

Sie müssen eventuell zuerst auf virtuelle Geräte aktivieren klicken. Wählen Sie die Option Diese Sitzung akzeptieren, wenn Sie dazu aufgefordert werden.

7. Rufen Sie die ISO-Image-Datei des VMware ESXi 6.7-Installationsprogramms auf, und klicken Sie auf Öffnen. Klicken Sie Auf Kartengerät.
8. Wählen Sie das Menü Power (aus) und dann Power Cycle System (Kaltstart). Klicken Sie Auf Ja.

VMware ESXi installieren

In den folgenden Schritten wird die Installation von VMware ESXi auf jedem Host beschrieben.

Laden Sie das benutzerdefinierte ESXI 6.7 Cisco Image herunter

1. Navigieren Sie zum "Download-Seite für VMware vSphere" Für benutzerdefinierte ISOs.
2. Klicken Sie neben der Cisco Custom Image for ESXi 6.7 GA Install-CD auf Go to Downloads.
3. Laden Sie die Cisco Custom Image for ESXi 6.7 GA Install CD (ISO) herunter.

Alle Hosts

1. Beim Systemstart erkennt die Maschine die VMware ESXi Installationsmedien.
2. Wählen Sie das VMware ESXi-Installationsprogramm aus dem angezeigten Menü aus.

   Das Installationsprogramm wird geladen. Dies dauert einige Minuten.

3. Drücken Sie nach dem Laden des Installers die Eingabetaste, um mit der Installation fortzufahren.
4. Nachdem Sie die Endbenutzer-Lizenzvereinbarung gelesen haben, akzeptieren Sie sie und fahren Sie mit der Installation fort, indem Sie auf F11 drücken.
5. Wählen Sie die NetApp LUN aus, die zuvor als Installationsfestplatte für ESXi eingerichtet wurde, und drücken Sie die Eingabetaste, um die Installation fortzusetzen.

6. Wählen Sie das entsprechende Tastaturlayout aus, und drücken Sie die Eingabetaste.
7. Geben Sie das Root-Passwort ein und bestätigen Sie es, und drücken Sie die Eingabetaste.
8. Der Installer warnt Sie, dass vorhandene Partitionen auf dem Volume entfernt werden. Fahren Sie mit der Installation fort, indem Sie auf F11 drücken. Der Server startet nach der Installation von ESXi neu.

Einrichten des VMware ESXi Host-Managementnetzwerkes

Bei den folgenden Schritten wird beschrieben, wie das Management-Netzwerk für jeden VMware ESXi Host hinzugefügt wird.

Alle Hosts

1. Geben Sie nach dem Neustart des Servers die Option zum Anpassen des Systems ein, indem Sie F2 drücken.
2. Melden Sie sich mit root als Anmeldenamen und dem Root-Passwort an, das zuvor während des Installationsprozesses eingegeben wurde.
3. Wählen Sie die Option Managementnetzwerk konfigurieren.
4. Wählen Sie Netzwerkadapter aus, und drücken Sie die Eingabetaste.
5. Wählen Sie die gewünschten Ports für vSwitch0 aus. Drücken Sie Die Eingabetaste.

   Wählen Sie die Ports aus, die eth0 und eth1 im CIMC entsprechen.

6. Wählen Sie VLAN (optional) aus, und drücken Sie die Eingabetaste.
7. Geben Sie die VLAN-ID ein `<<mgmt_vlan_id>>`. Drücken Sie Die Eingabetaste.
8. Wählen Sie im Menü Managementnetzwerk konfigurieren die Option IPv4-Konfiguration aus, um die IP-Adresse der Managementoberfläche zu konfigurieren. Drücken Sie Die Eingabetaste.
9. Markieren Sie mit den Pfeiltasten die Option statische IPv4-Adresse festlegen, und wählen Sie diese Option mithilfe der Leertaste aus.
10. Geben Sie die IP-Adresse zum Verwalten des VMware ESXi-Hosts ein `<<esxi_host_mgmt_ip>>`.
11. Geben Sie die Subnetzmaske für den VMware ESXi-Host ein `<<esxi_host_mgmt_netmask>>`.
12. Geben Sie das Standard-Gateway für den VMware ESXi-Host ein `<<esxi_host_mgmt_gateway>>`.
13. Drücken Sie die Eingabetaste, um die Änderungen an der IP-Konfiguration zu akzeptieren.
14. Rufen Sie das IPv6-Konfigurationsmenü auf.
15. Deaktivieren Sie IPv6 über die Leertaste, indem Sie die Option IPv6 aktivieren (Neustart erforderlich) deaktivieren. Drücken Sie Die Eingabetaste.
16. Rufen Sie das Menü auf, um die DNS-Einstellungen zu konfigurieren.
17. Da die IP-Adresse manuell zugewiesen wird, müssen auch die DNS-Informationen manuell eingegeben werden.
18. Geben Sie die IP-Adresse des primären DNS-Servers ein[nameserver_ip].
19. (Optional) Geben Sie die IP-Adresse des sekundären DNS-Servers ein.
20. Geben Sie den FQDN für den VMware ESXi-Hostnamen ein:[esxi_host_fqdn].
21. Drücken Sie die Eingabetaste, um die Änderungen an der DNS-Konfiguration zu akzeptieren.
22. Beenden Sie das Untermenü Verwaltungsnetzwerk konfigurieren, indem Sie Esc drücken.
23. Drücken Sie Y, um die Änderungen zu bestätigen und den Server neu zu starten.
24. Melden Sie sich von der VMware Konsole aus, indem Sie Esc drücken.

Konfigurieren Sie den ESXi-Host

Sie benötigen die Informationen in der folgenden Tabelle, um jeden ESXi Host zu konfigurieren.

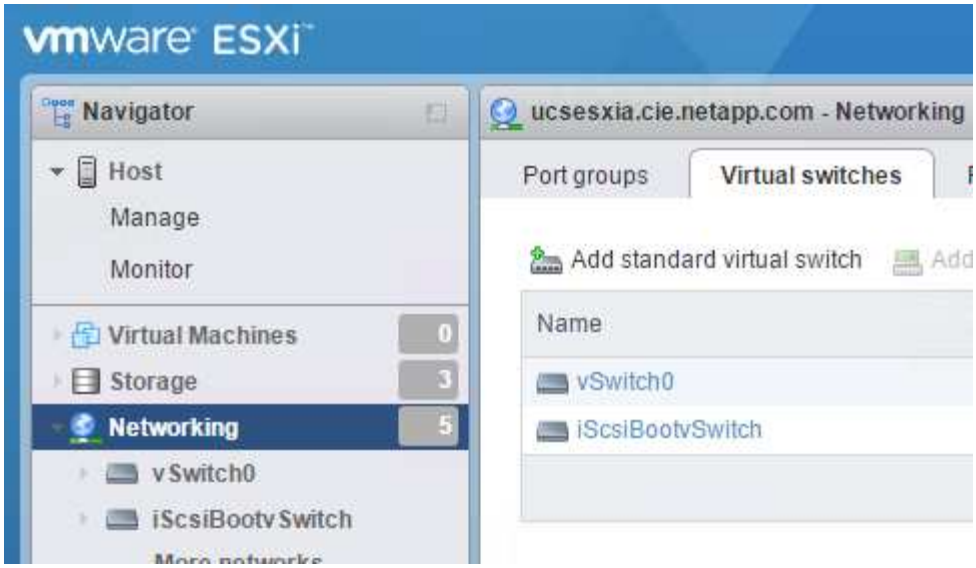
Details	Wert
ESXi Hostname	
ESXi Host-Management-IP	
ESXi Host-Managementmaske	
ESXi Host-Management-Gateway	
ESXi Host, NFS-IP	
ESXi Host-NFS-Maske	
ESXi Host-NFS-Gateway	
ESXi Host vMotion IP	
ESXi Host vMotion Maske	
ESXi Host vMotion Gateway	
ESXi Host, iSCSI A IP	
ESXi Host iSCSI-A-Maske	
ISCSI-A-Gateway für ESXi Host	
ESXi-Host, iSCSI-B-IP	
ISCSI-B-Maske für ESXi Host	
ESXi Host iSCSI-B-Gateway	

Melden Sie sich beim ESXi-Host an

1. Öffnen Sie die Management-IP-Adresse des Hosts in einem Webbrowser.
2. Melden Sie sich beim ESXi-Host mit dem Root-Konto und dem Passwort an, das Sie während des Installationsvorgangs angegeben haben.
3. Lesen Sie die Aussage zum VMware Customer Experience Improvement Program. Klicken Sie nach Auswahl der richtigen Antwort auf OK.

Konfigurieren Sie den iSCSI-Bootvorgang

1. Wählen Sie links die Option Netzwerk.
2. Wählen Sie rechts die Registerkarte Virtuelle Switches aus.

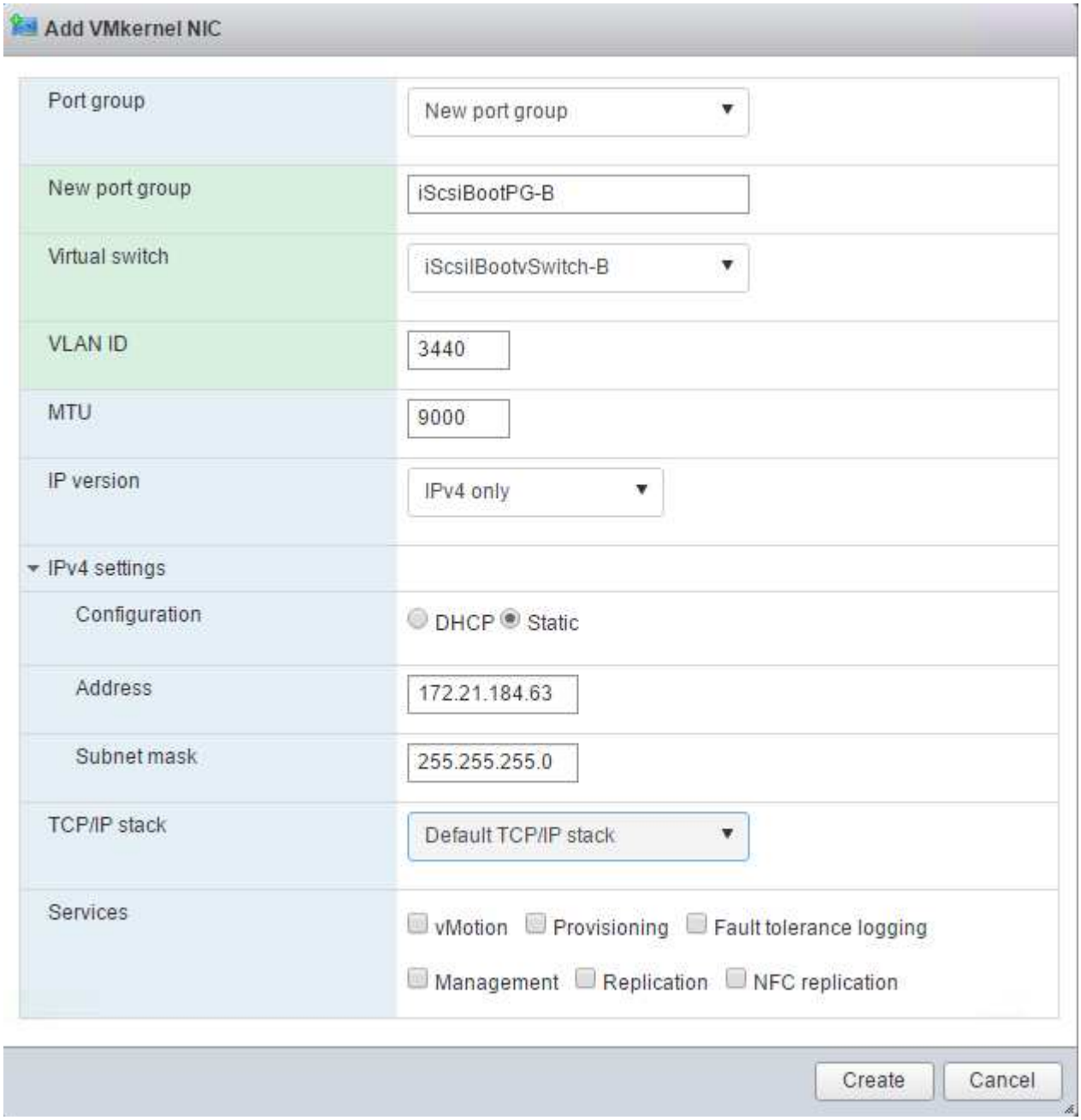


3. Klicken Sie auf iScsiBootvSwitch.
4. Wählen Sie Einstellungen bearbeiten aus.
5. Ändern Sie die MTU in 9000, und klicken Sie auf Speichern.
6. Klicken Sie im linken Navigationsbereich auf Netzwerk, um zur Registerkarte Virtuelle Switches zurückzukehren.
7. Klicken Sie Auf Standard-Virtuellen Switch Hinzufügen.
8. Geben Sie den Namen an `iScsiBootvSwitch-B` Für den vSwitch-Namen.
   - Setzen Sie die MTU auf 9000.
   - Wählen Sie vmnic3 aus den Optionen Uplink 1.
   - Klicken Sie Auf Hinzufügen.

> Vmnic2 und vmnic3 werden für das Booten von iSCSI in dieser Konfiguration verwendet. Wenn Sie zusätzliche NICs in Ihrem ESXi Host haben, haben Sie möglicherweise unterschiedliche vmnic-Zahlen. Um zu überprüfen, welche NICs für das Booten von iSCSI verwendet werden, stimmen Sie die MAC-Adressen auf den iSCSI vNICs in CIMC den vmnics in ESXi ab.

9. Wählen Sie im mittleren Fensterbereich die Registerkarte VMkernel NICs aus.
10. Wählen Sie VMkernel NIC hinzufügen aus.
    - Geben Sie einen neuen Portgruppennamen von an `iScsiBootPG-B`.
    - Wählen Sie iScsiBootvSwitch-B für den virtuellen Switch aus.
    - Eingabe `<<iscsib_vlan_id>>` Für die VLAN-ID.
    - Ändern Sie die MTU in 9000.
    - IPv4-Einstellungen erweitern.
    - Wählen Sie Statische Konfiguration.
    - Eingabe `<<var_hosta_iscsib_ip>>` Für Adresse.
    - Eingabe `<<var_hosta_iscsib_mask>>` Für Subnetzmaske.

◦ Klicken Sie auf Erstellen .

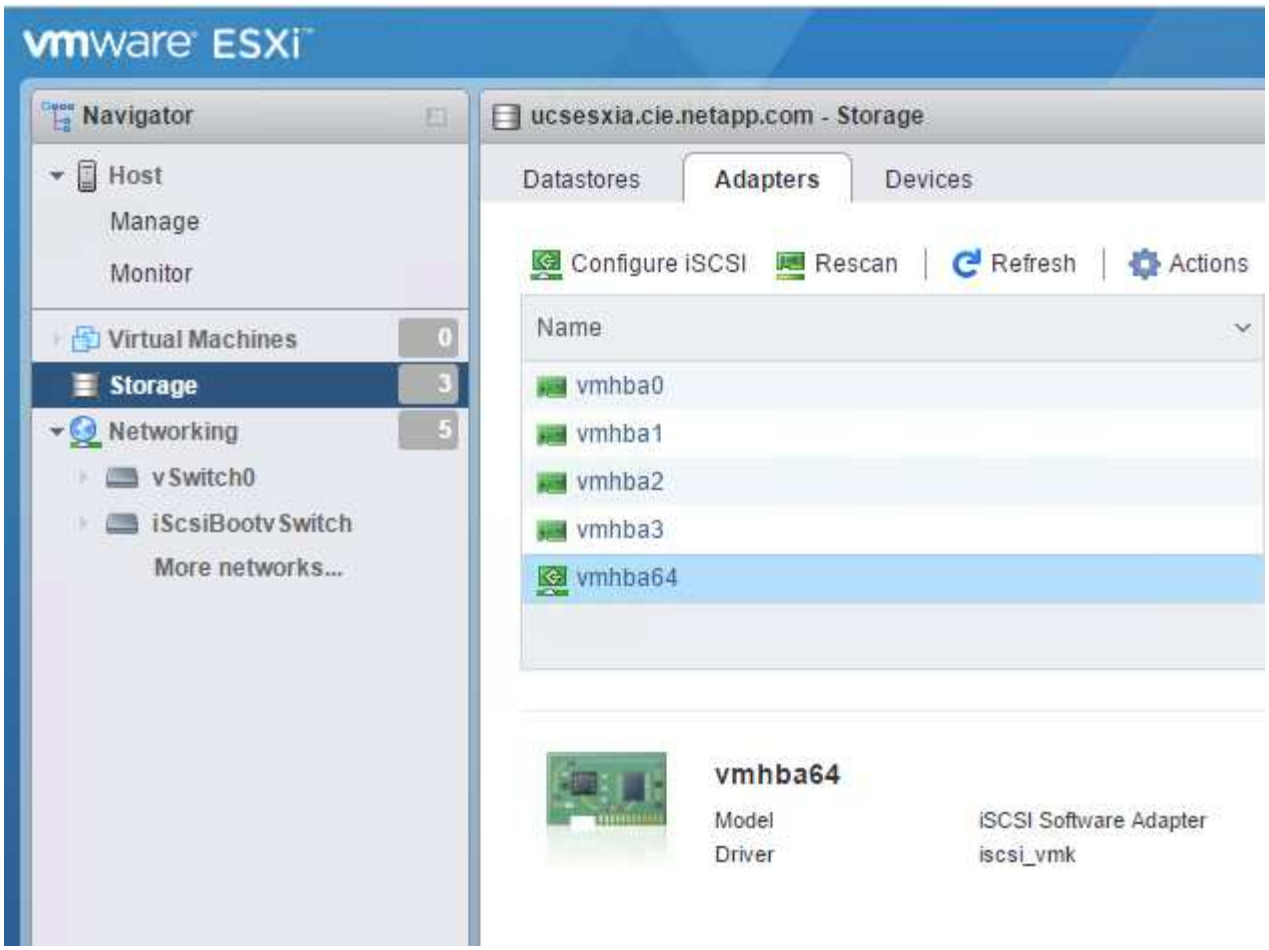


Setzen Sie die MTU auf 9000 auf `iScsiBootPG- A.`

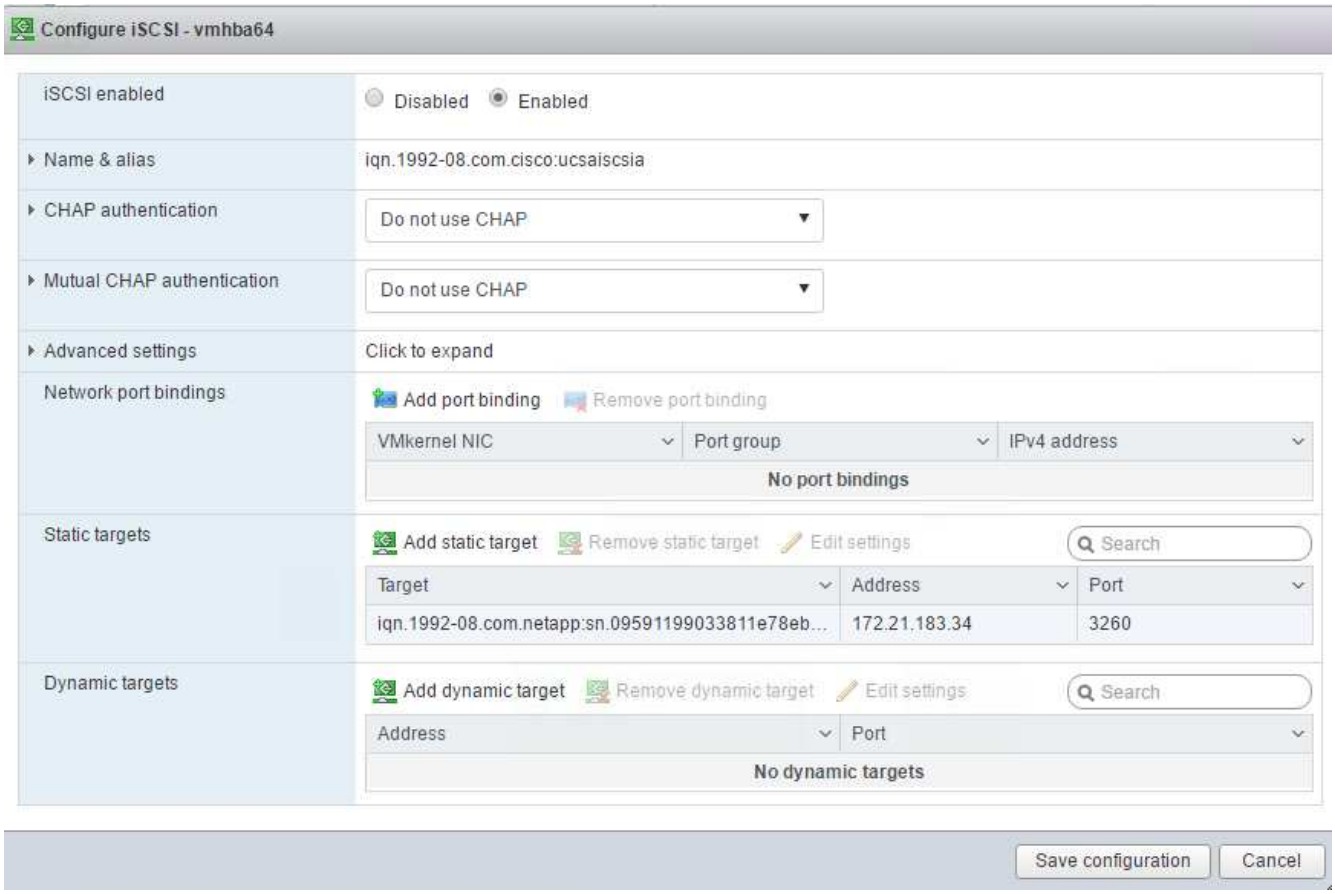
Konfigurieren Sie iSCSI-Multipathing

Gehen Sie wie folgt vor, um iSCSI-Multipathing auf den ESXi-Hosts einzurichten:

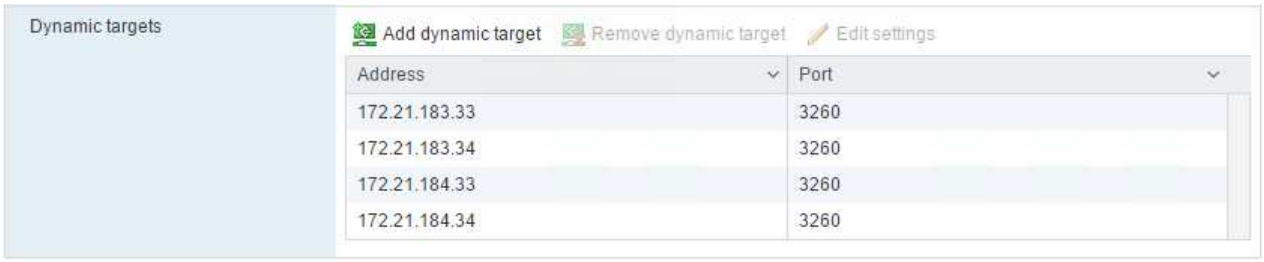
1. Wählen Sie im linken Navigationsbereich Storage aus. Klicken Sie Auf Adapter.
2. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf iSCSI konfigurieren.



3. Klicken Sie unter dynamische Ziele auf dynamische Ziele hinzufügen.



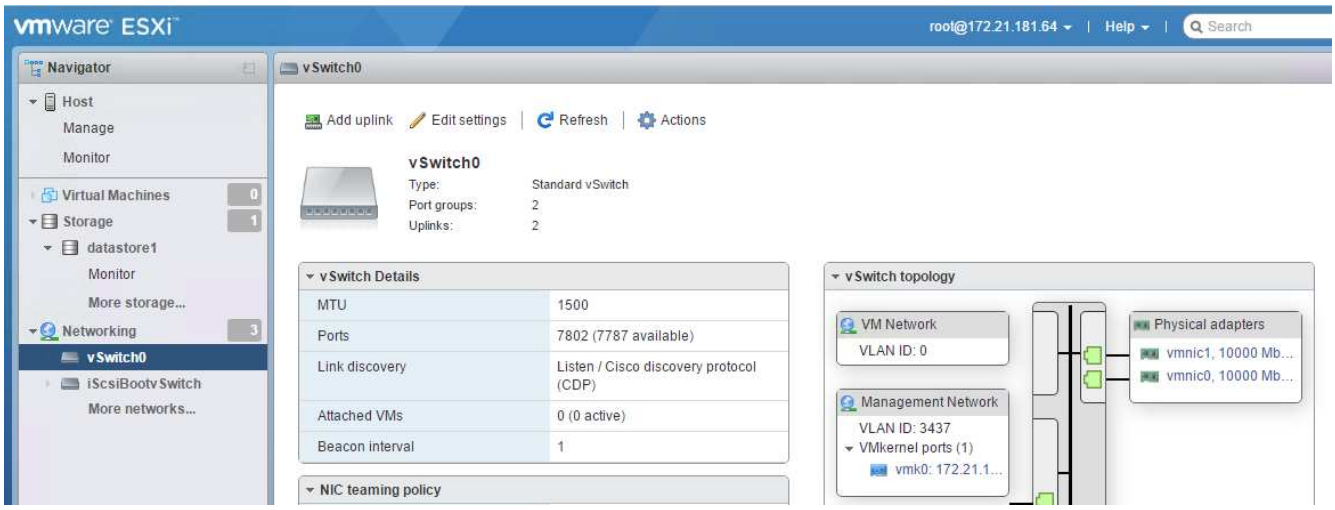
4. Geben Sie die IP-Adresse ein `iscsi_lif01a`.
   - Wiederholen Sie diesen Vorgang mit den IP-Adressen `iscsi_lif01b`, `iscsi_lif02a`, und `iscsi_lif02b`.
   - Klicken Sie Auf Konfiguration Speichern.



Sie können die iSCSI LIF IP-Adressen finden, indem Sie den Befehl `Network Interface show `im NetApp Cluster ausführen oder die Registerkarte Netzwerkschnittstellen im OnCommand System Manager ansehen.

Konfigurieren Sie den ESXi-Host

1. Wählen Sie im linken Navigationsbereich die Option Netzwerk.
2. Wählen Sie vSwitch0 aus.



3. Wählen Sie Einstellungen Bearbeiten.
4. Ändern Sie die MTU in 9000.
5. Erweitern Sie NIC Teaming und stellen Sie sicher, dass sowohl vmnic0 als auch vmnic1 auf aktiv gesetzt sind.

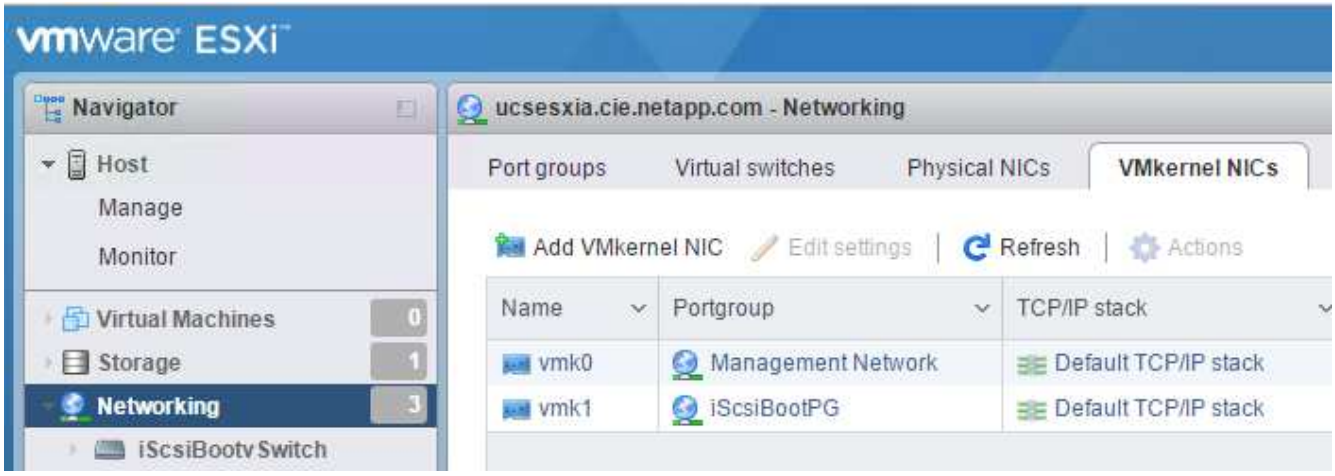
Konfigurieren Sie die Portgruppen und VMkernel NICs

1. Wählen Sie im linken Navigationsbereich die Option Netzwerk.
2. Klicken Sie mit der rechten Maustaste auf die Registerkarte Portgruppen.

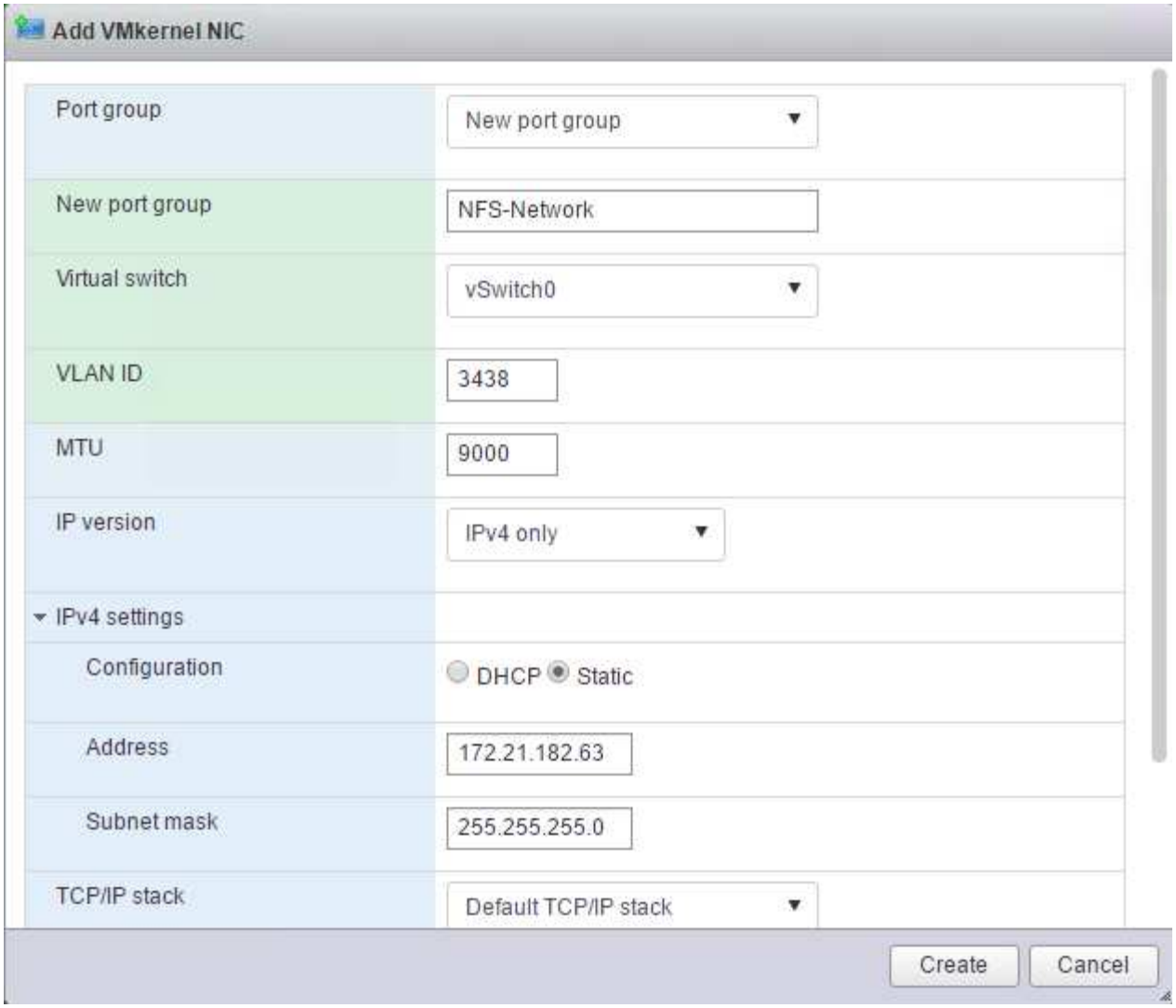
3. Klicken Sie mit der rechten Maustaste auf VM Network, und wählen Sie Bearbeiten aus. Ändern Sie die VLAN-ID in `<<var_vm_traffic_vlan>>`.
4. Klicken Sie Auf Portgruppe Hinzufügen.
   - Benennen Sie die Portgruppe `MGMT-Network`.
   - Eingabe `<<mgmt_vlan>>` Für die VLAN-ID.
   - Stellen Sie sicher, dass vSwitch0 ausgewählt ist.

- Klicken Sie Auf Hinzufügen.

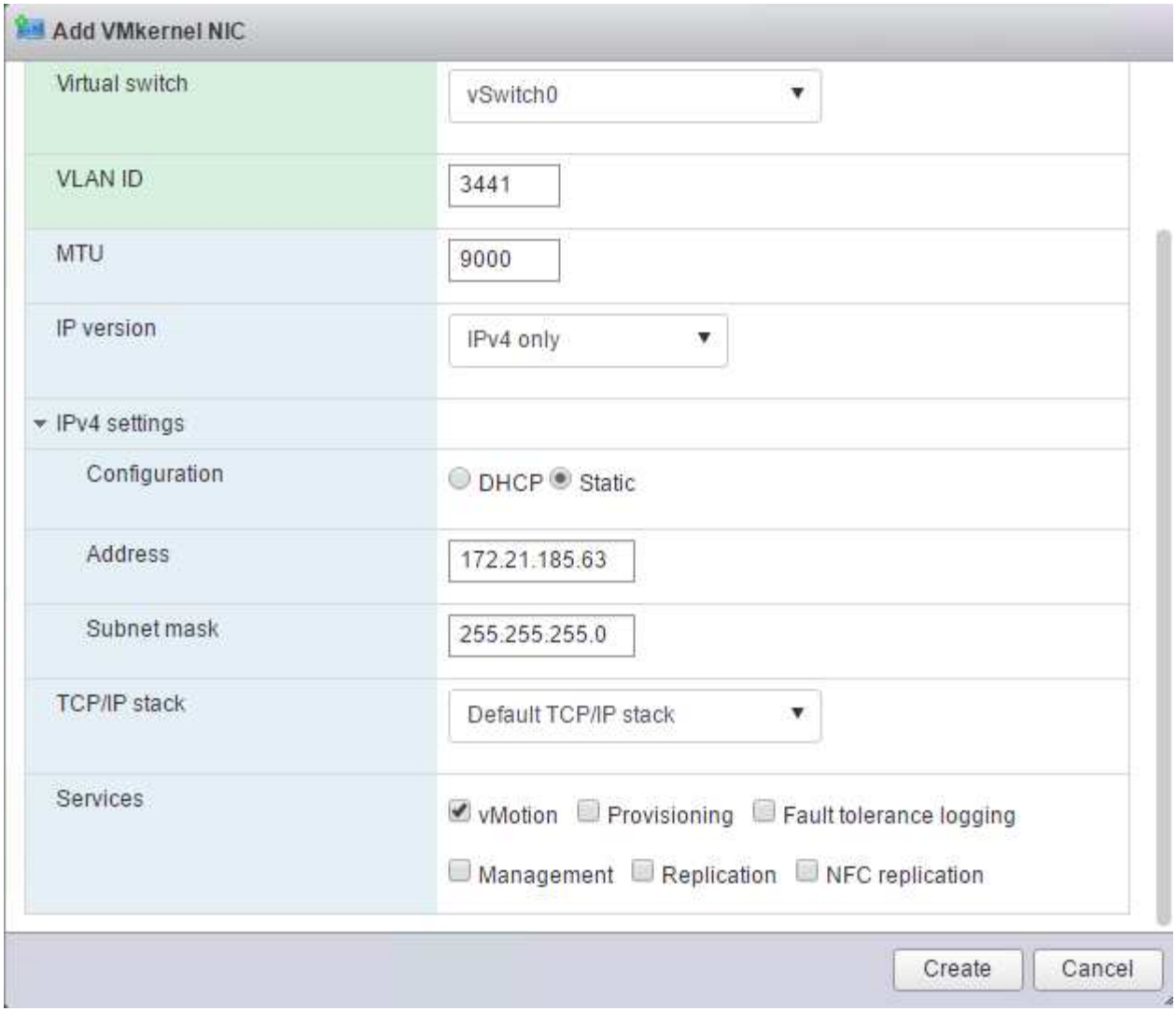
5. Klicken Sie auf die Registerkarte VMkernel NICs.



6. Wählen Sie VMkernel NIC hinzufügen aus.
   - Wählen Sie Neue Portgruppe.
   - Benennen Sie die Portgruppe `NFS-Network`.
   - Eingabe `<<nfs_vlan_id>>` Für die VLAN-ID.
   - Ändern Sie die MTU in 9000.
   - IPv4-Einstellungen erweitern.
   - Wählen Sie Statische Konfiguration.
   - Eingabe `<<var_hosta_nfs_ip>>` Für Adresse.
   - Eingabe `<<var_hosta_nfs_mask>>` Für Subnetzmaske.
   - Klicken Sie auf Erstellen .



7. Wiederholen Sie diesen Prozess für die Erstellung des vMotion VMkernel Port.
8. Wählen Sie VMkernel NIC hinzufügen aus.
    a. Wählen Sie Neue Portgruppe.
    b. Benennen Sie vMotion für die Portgruppe.
    c. Eingabe `<<vmotion_vlan_id>>` Für die VLAN-ID.
    d. Ändern Sie die MTU in 9000.
    e. IPv4-Einstellungen erweitern.
    f. Wählen Sie Statische Konfiguration.
    g. Eingabe `<<var_hosta_vmotion_ip>>` Für Adresse.
    h. Eingabe `<<var_hosta_vmotion_mask>>` Für Subnetzmaske.
    i. Stellen Sie sicher, dass das Kontrollkästchen vMotion nach den IPv4-Einstellungen ausgewählt ist.

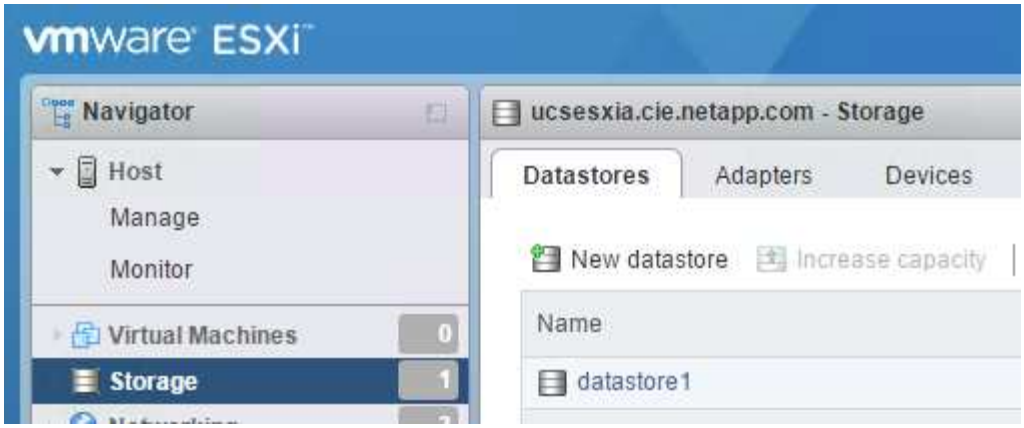


Es gibt viele Möglichkeiten, ESXi Networking zu konfigurieren, einschließlich der Verwendung des VMware vSphere Distributed Switches, wenn Ihre Lizenzierung es zulässt. In FlexPod Express werden alternative Netzwerkkonfigurationen unterstützt, wenn sie zur Erfüllung der geschäftlichen Anforderungen erforderlich sind.

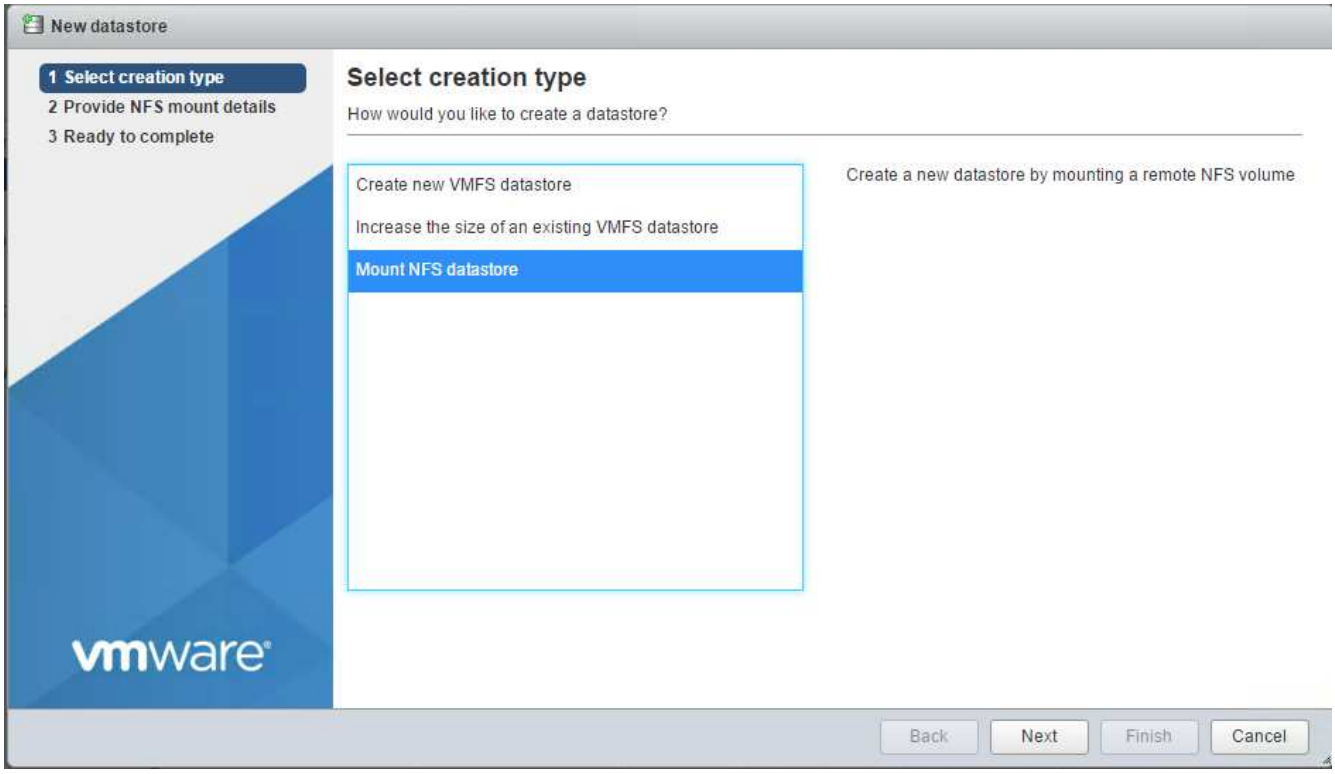
Erste Datastores mounten

Die ersten zu gemounteten Datenspeicher sind der Infra_Datastore_1 für Virtual Machines und der Infra_swap-Datenspeicher für Swap-Dateien virtueller Maschinen.

1. Klicken Sie im linken Navigationsbereich auf „Storage“ und dann auf New Datastore.



2. Wählen Sie Mount NFS Datastore aus.



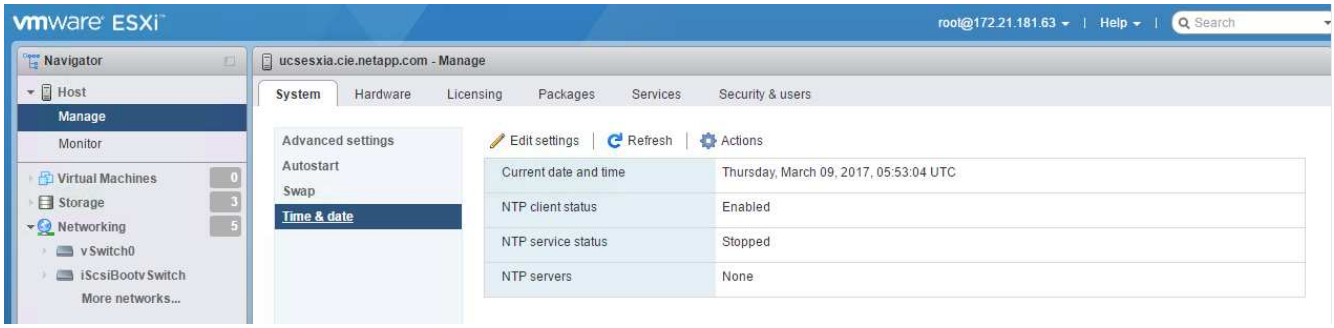
3. Geben Sie als Nächstes die folgenden Informationen auf der Seite „NFS Mount Details angeben“ ein:
   - Name: `infra_datastore_1`
   - NFS-Server: `<<var_nodea_nfs_lif>>`
   - Freigabe: /Infra_Datastore_1
   - Stellen Sie sicher, dass NFS 3 ausgewählt ist.
4. Klicken Sie Auf Fertig Stellen. Die Aufgabe wird im Fenster Letzte Aufgaben ausgeführt.
5. Wiederholen Sie diesen Vorgang für die Bereitstellung des Infra_swap-Datenspeichers:
   - Name: `infra_swap`
   - NFS-Server: `<<var_nodea_nfs_lif>>`
   - Weitersagen: `/infra_swap`

- Stellen Sie sicher, dass NFS 3 ausgewählt ist.

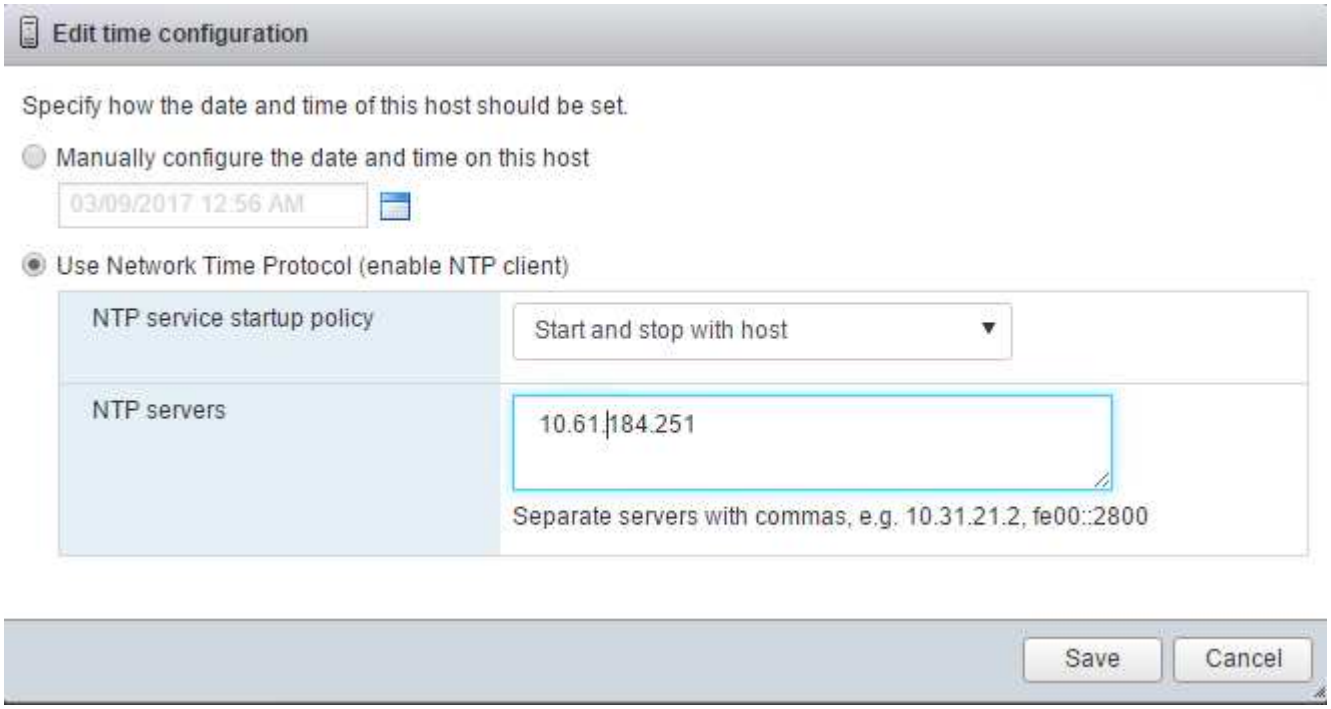
Konfigurieren Sie NTP

Gehen Sie wie folgt vor, um NTP für einen ESXi-Host zu konfigurieren:

1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich System aus, und klicken Sie anschließend auf Zeit und Datum.



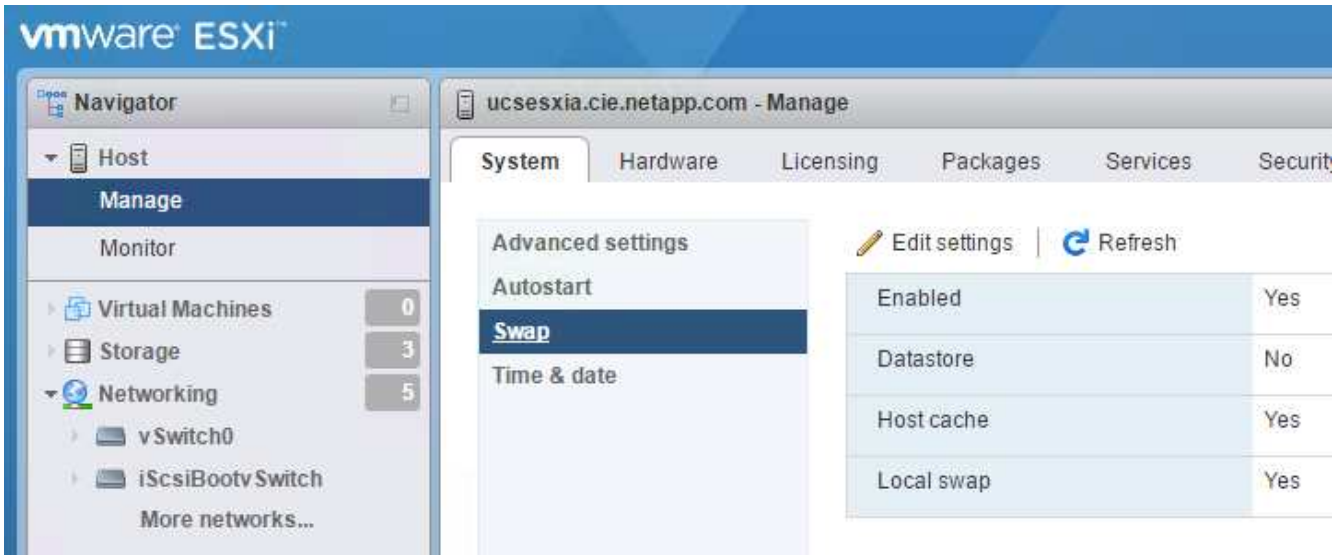
2. Wählen Sie Network Time Protocol (Network Time Protocol verwenden) (NTP Client aktivieren) aus.
3. Wählen Sie Start und Stopp mit Host als Startrichtlinie für den NTP-Dienst aus.
4. Eingabe `<<var_ntp>>` Als NTP-Server. Sie können mehrere NTP-Server festlegen.
5. Klicken Sie auf Speichern .



Verschieben Sie den Speicherort der Swap-Datei der virtuellen Maschine

Diese Schritte enthalten Details zum Verschieben des Speicherorts der Swap-Datei der virtuellen Maschine.

1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich das System aus, und klicken Sie dann auf Tausch.



2. Klicken Sie Auf Einstellungen Bearbeiten. Wählen Sie Infra_swap aus den Datenspeicheroptionen aus.

3. Klicken Sie auf Speichern .

Installieren Sie das NetApp NFS Plug-in 1.0.20 für VMware VAAI

Gehen Sie wie folgt vor, um das NetApp NFS Plug-in 1.0.20 für VMware VAAI zu installieren.

1. Geben Sie die folgenden Befehle ein, um zu überprüfen, ob VAAI aktiviert ist:

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Wenn VAAI aktiviert ist, erzeugen diese Befehle die folgende Ausgabe:

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Wenn VAAI nicht aktiviert ist, geben Sie die folgenden Befehle ein, um VAAI zu aktivieren:

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Diese Befehle erzeugen die folgende Ausgabe:

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Laden Sie das NetApp NFS Plug-in für VMware VAAI herunter:
   a. Wechseln Sie zum "Software Download Seite".
   b. Scrollen Sie nach unten und klicken Sie auf NetApp NFS Plug-in for VMware VAAI.
   c. Wählen Sie die ESXi-Plattform aus.
   d. Laden Sie entweder das Offline-Bundle (.zip) oder das Online-Bundle (.vib) des neuesten Plug-ins herunter.
4. Installieren Sie das Plug-in auf dem ESXi Host mithilfe der ESX CLI.
5. STARTEN Sie DEN ESXI-Host neu.

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"Dann installieren Sie VMware vCenter Server 6.7"

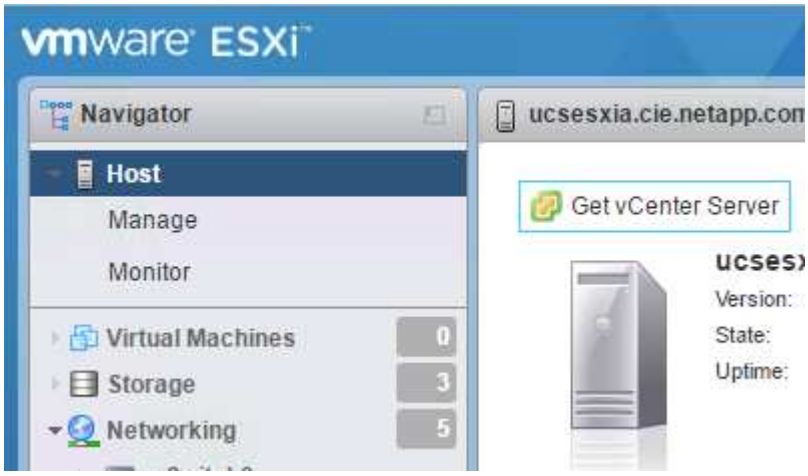
Installieren Sie VMware vCenter Server 6.7

Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware vCenter Server 6.7 in einer FlexPod Express-Konfiguration.

FlexPod Express verwendet die VMware vCenter Server Appliance (VCSA).

Laden Sie die VMware vCenter Server Appliance herunter

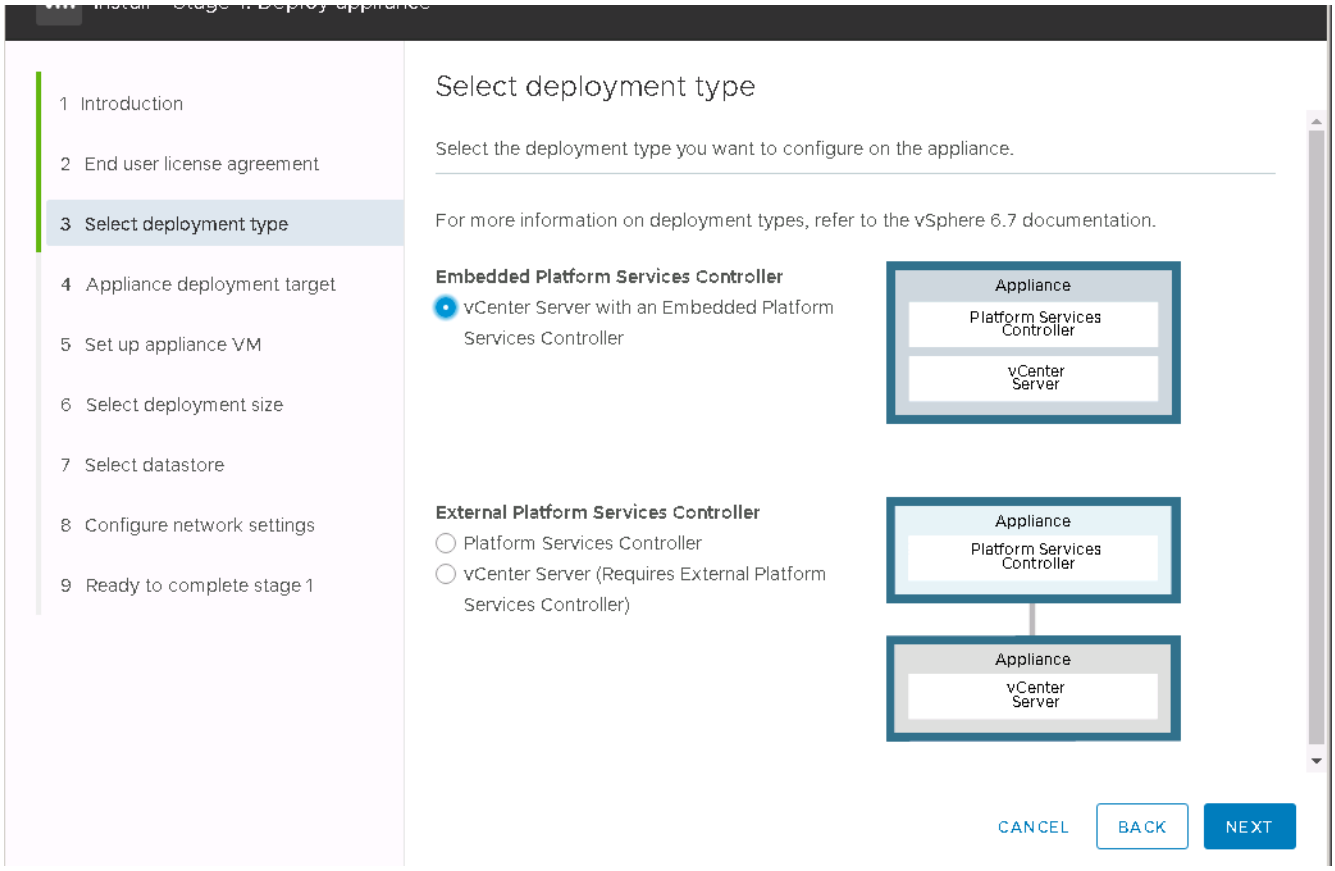
1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.



2. Laden Sie die VCSA von der VMware-Website herunter.

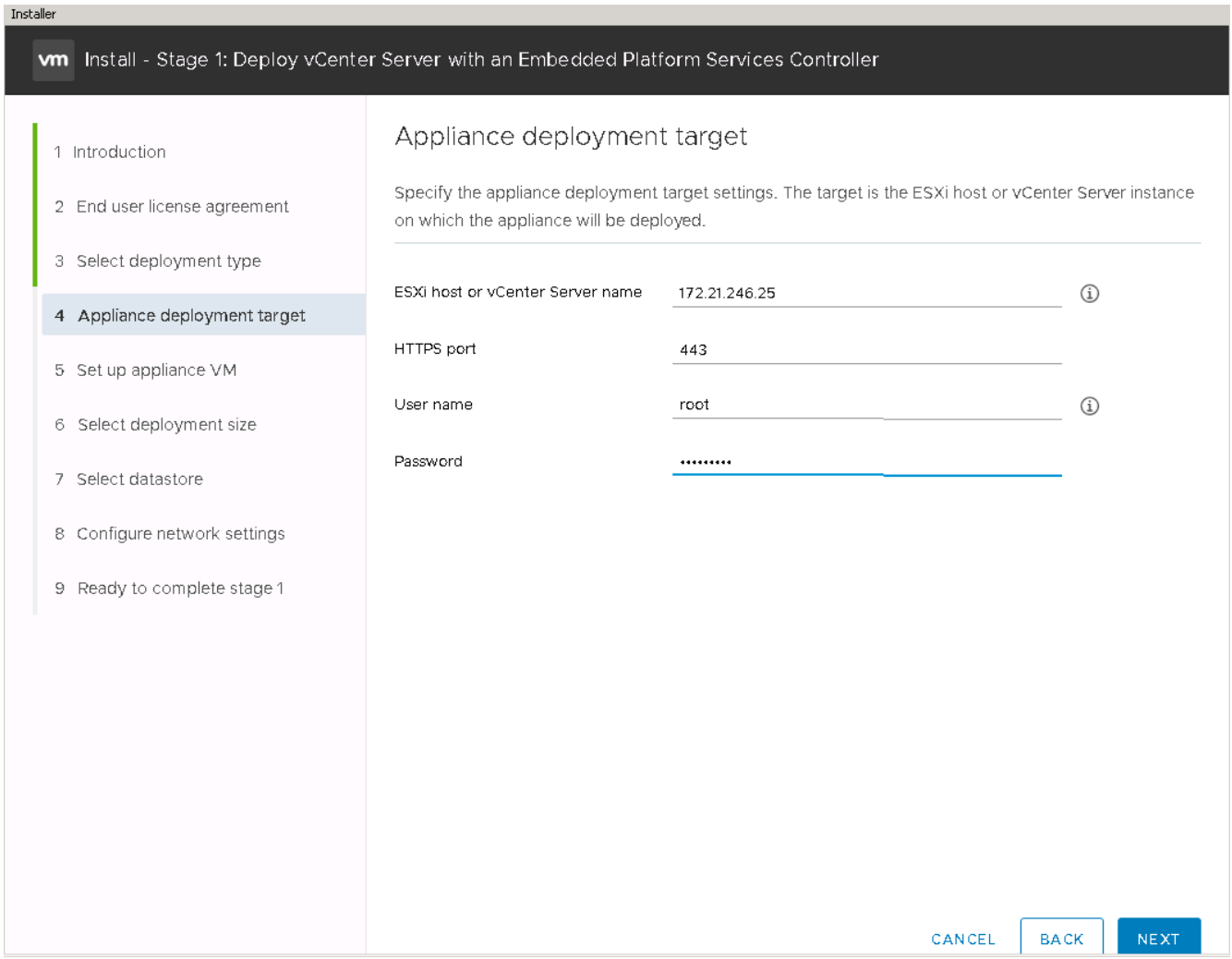
> Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.

3. Mounten Sie das ISO-Image.
4. Navigieren Sie zum verzeichnis vcsa-ui-Installer > win32. Doppelklicken Sie auf Installer.exe.
5. Klicken Sie Auf Installieren.
6. Klicken Sie auf der Seite Einführung auf Weiter.
7. Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung.
8. Wählen Sie als Bereitstellungstyp den Embedded Platform Services Controller aus.

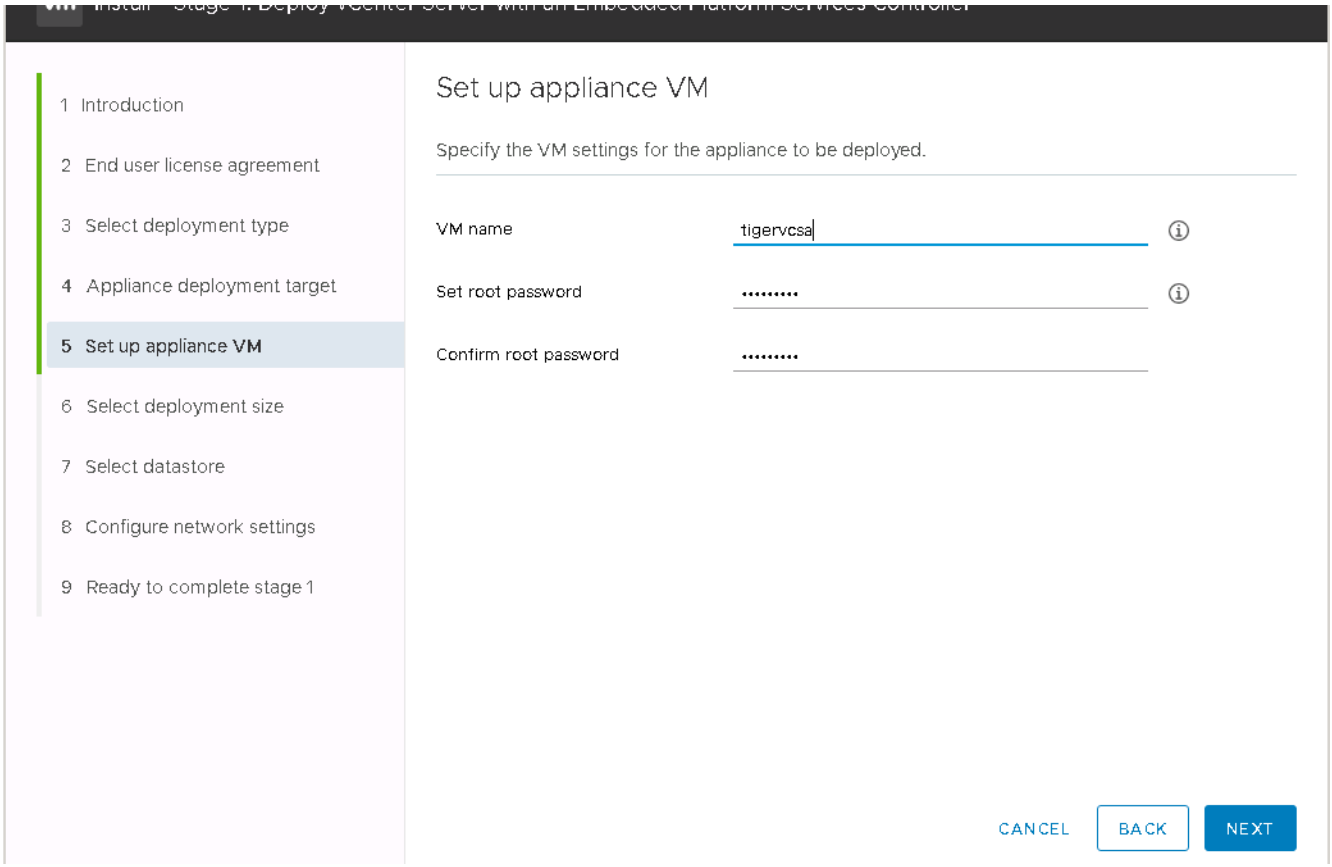


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

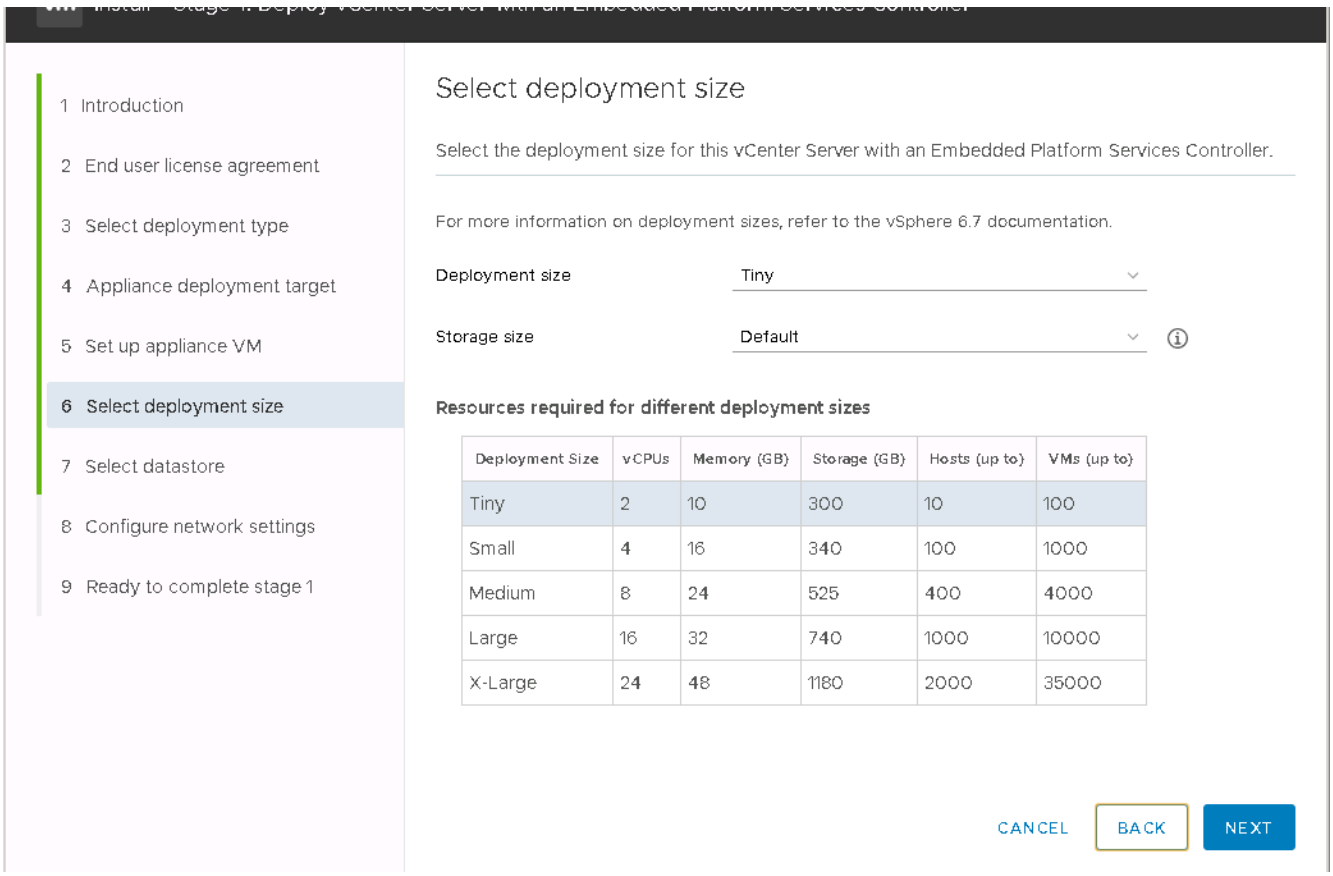
9. Geben Sie im Bereitstellungsziel der Appliance die IP-Adresse eines bereitgestellten ESXi-Hosts sowie den Root-Benutzernamen und das Root-Passwort ein.



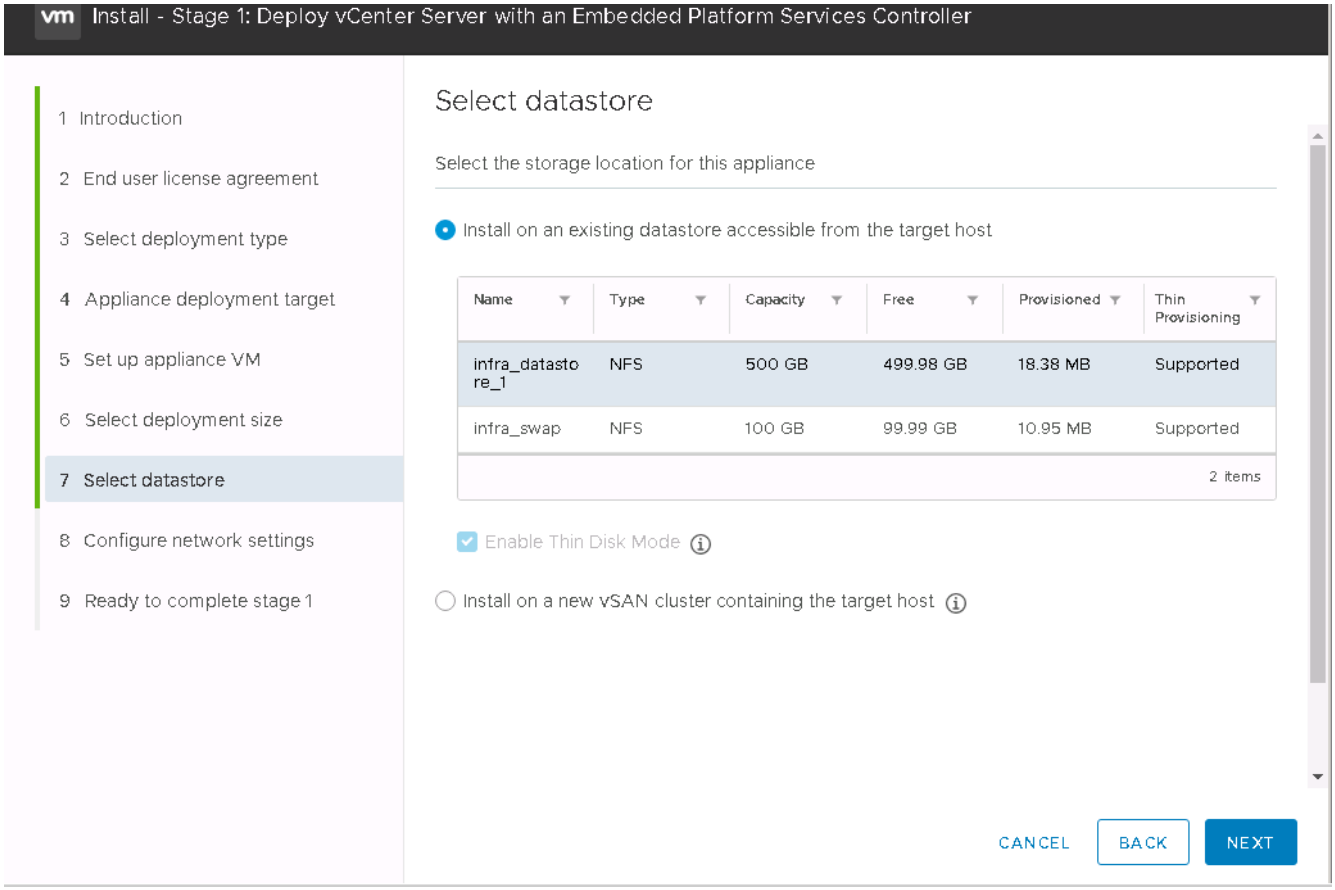
10. Legen Sie die Appliance-VM fest, indem Sie eingeben `VCSA` Als VM-Name und das Root-Passwort, das Sie für den VCSA verwenden möchten.



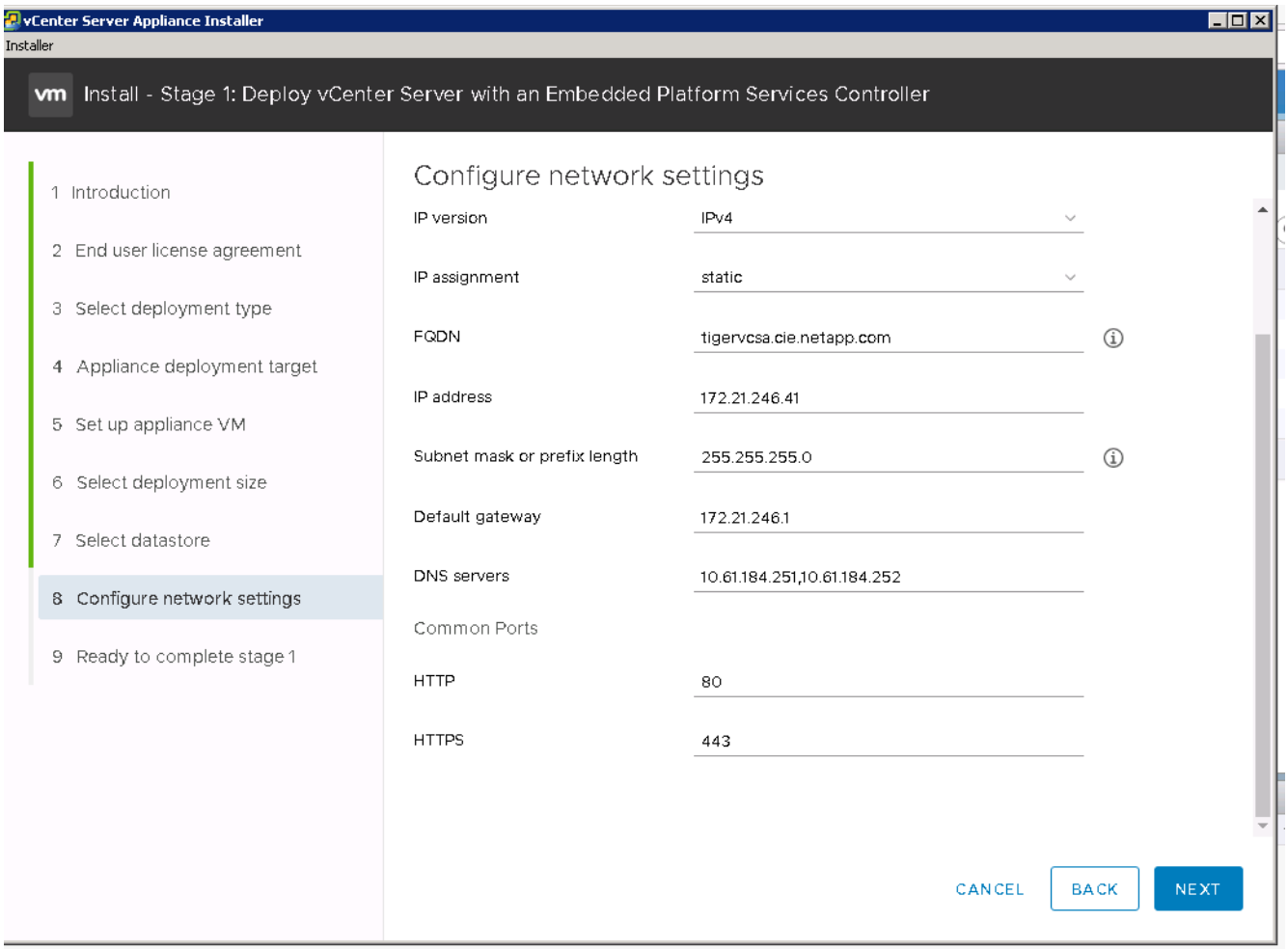
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



12. Wählen Sie den Infra_Datastore_1 aus. Klicken Sie Auf Weiter.

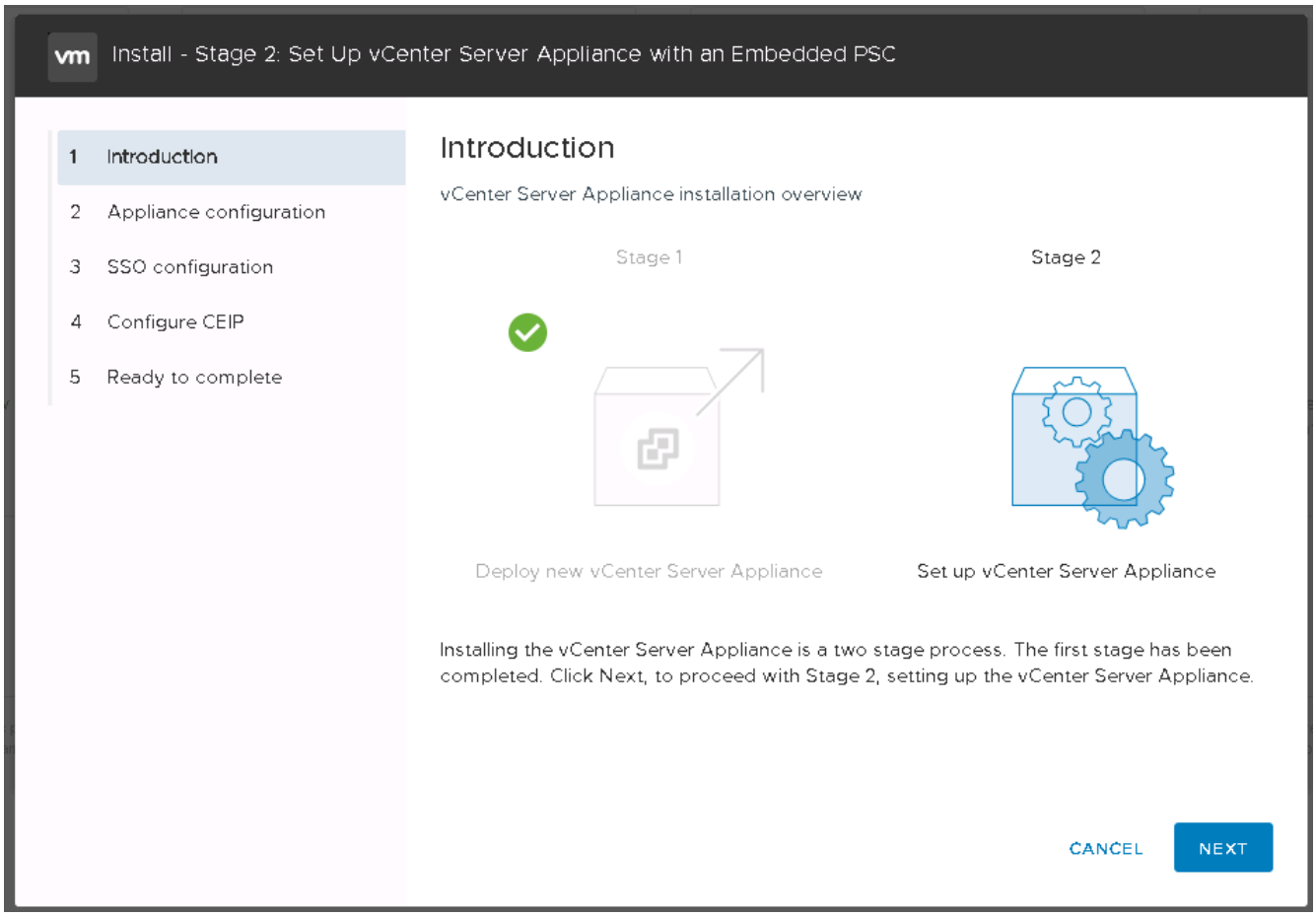


13. Geben Sie die folgenden Informationen auf der Seite Netzwerkeinstellungen konfigurieren ein, und klicken Sie auf Weiter.
    a. Wählen Sie MGMT-Network für Netzwerk.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse ein.
    d. Geben Sie die zu verwendenden Subnetzmaske ein.
    e. Geben Sie das Standard-Gateway ein.
    f. Geben Sie den DNS-Server ein.
14. Überprüfen Sie auf der Seite bereit zum Abschließen von Phase 1, ob die von Ihnen eingegebenen Einstellungen korrekt sind. Klicken Sie Auf Fertig Stellen.



Die VCSA wird jetzt installiert. Dieser Vorgang dauert mehrere Minuten.

15. Wenn Phase 1 abgeschlossen ist, wird eine Meldung angezeigt, die angibt, dass sie abgeschlossen ist. Klicken Sie auf Weiter, um die Konfiguration von Phase 2 zu beginnen.
16. Klicken Sie auf der Seite Einführung in Phase 2 auf Weiter.



17. Eingabe `<<var_ntp_id>>` Für die NTP-Serveradresse. Sie können mehrere NTP-IP-Adressen eingeben.

    Wenn Sie Hochverfügbarkeit (HA) in vCenter Server verwenden möchten, stellen Sie sicher, dass der SSH-Zugriff aktiviert ist.

18. Konfigurieren Sie den SSO-Domänennamen, das Passwort und den Standortnamen. Klicken Sie Auf Weiter.

    Notieren Sie diese Werte für Ihre Referenz, insbesondere wenn Sie vom vsphere.local Domain Name abweichen.

19. Treten Sie auf Wunsch dem VMware Customer Experience-Programm bei. Klicken Sie Auf Weiter.
20. Zeigen Sie die Zusammenfassung Ihrer Einstellungen an. Klicken Sie auf Fertig stellen oder verwenden Sie die Schaltfläche Zurück, um die Einstellungen zu bearbeiten.
21. Es wird eine Meldung angezeigt, die besagt, dass Sie die Installation nach dem Start nicht unterbrechen oder beenden können. Klicken Sie auf OK, um fortzufahren.

    Die Einrichtung der Appliance wird fortgesetzt. Dies dauert einige Minuten.

    Es wird eine Meldung angezeigt, die angibt, dass das Setup erfolgreich war.

    Die Links, die der Installer zum Zugriff auf vCenter Server bereitstellt, sind anklickbar.

"Als Nächstes konfigurieren Sie VMware vCenter Server 6.7 und vSphere Clustering."

Konfiguration von VMware vCenter Server 6.7 und vSphere Clustering

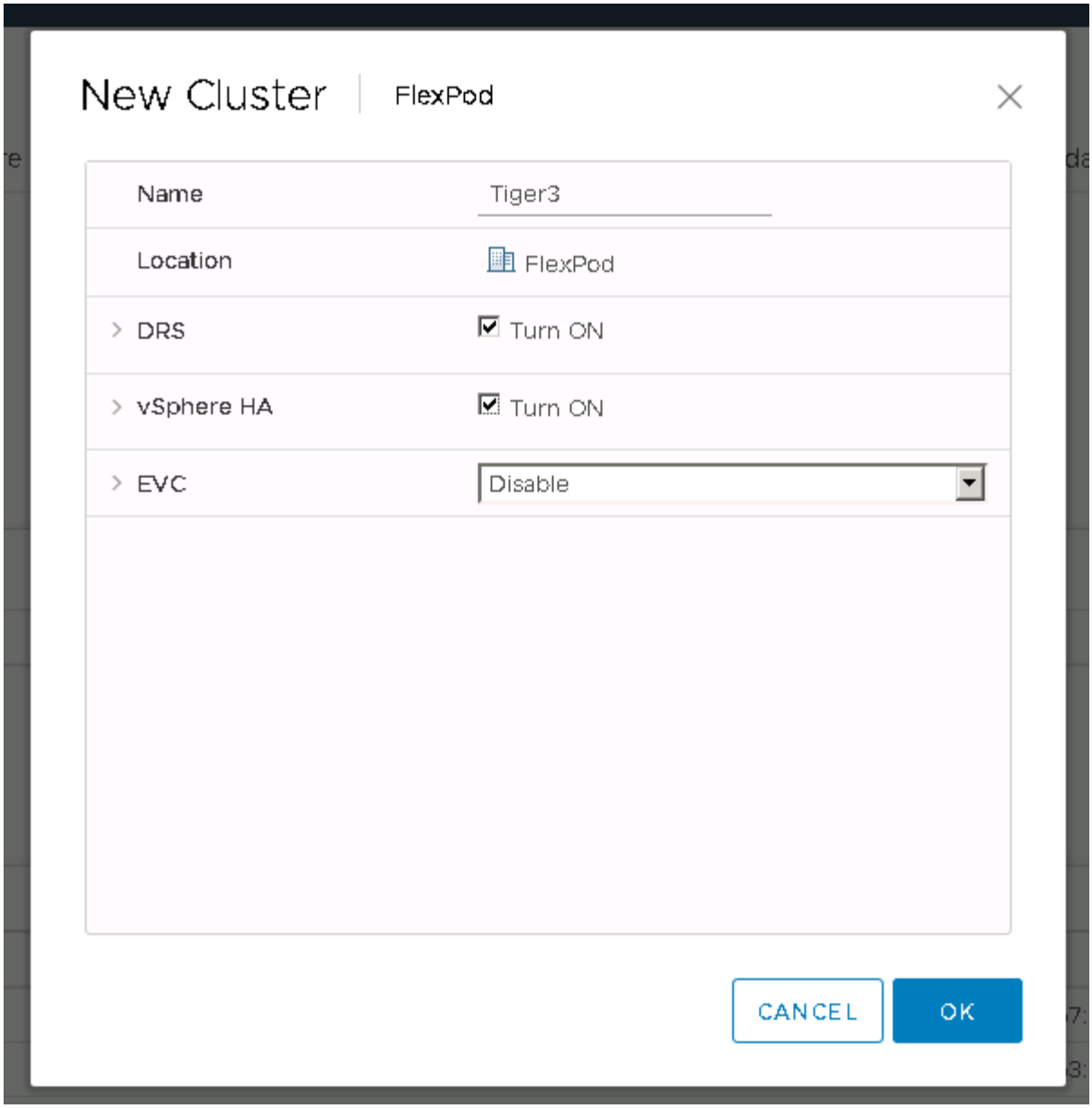
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

1. Navigieren Sie zu https://<<FQDN oder IP von vCenter>>/vsphere-Client/.
2. Klicken Sie auf vSphere Client starten.
3. Melden Sie sich mit dem Benutzernamen administrator@vsphere.local und dem SSO-Passwort an, das Sie während des VCSA-Einrichtungsvorgangs eingegeben haben.
4. Klicken Sie mit der rechten Maustaste auf den vCenter-Namen, und wählen Sie New Datacenter aus.
5. Geben Sie einen Namen für das Datacenter ein, und klicken Sie auf OK.

VSphere Cluster erstellen

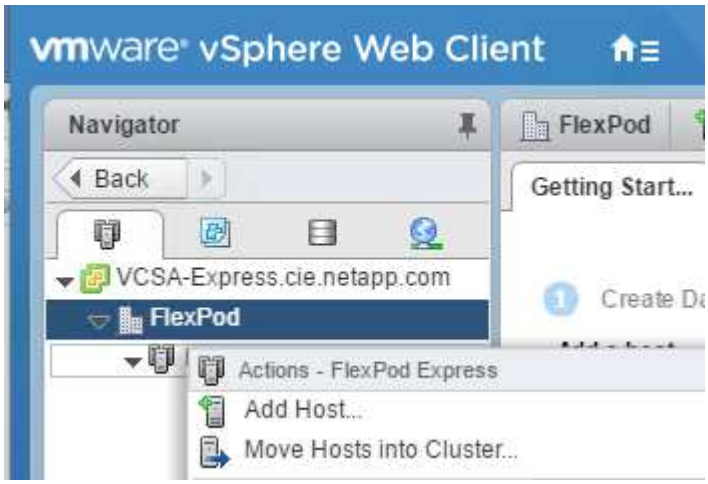
Führen Sie die folgenden Schritte aus, um einen vSphere-Cluster zu erstellen:

1. Klicken Sie mit der rechten Maustaste auf das neu erstellte Datacenter, und wählen Sie Neuer Cluster aus.
2. Geben Sie einen Namen für das Cluster ein.
3. Aktivieren Sie DR und vSphere HA, indem Sie die Kontrollkästchen auswählen.
4. Klicken Sie auf OK.



Fügen Sie ESXi-Hosts zum Cluster hinzu

1. Klicken Sie mit der rechten Maustaste auf das Cluster, und wählen Sie Host hinzufügen aus.



2. Gehen Sie wie folgt vor, um dem Cluster einen ESXi-Host hinzuzufügen:
   a. Geben Sie die IP oder den FQDN des Hosts ein. Klicken Sie Auf Weiter.
   b. Geben Sie den Benutzernamen und das Kennwort für den Root-Benutzer ein. Klicken Sie Auf Weiter.
   c. Klicken Sie auf Ja, um das Host-Zertifikat durch ein vom VMware-Zertifikatsserver signiertes Zertifikat zu ersetzen.
   d. Klicken Sie auf der Seite Host Summary auf Next.
   e. Klicken Sie auf das grüne Symbol +, um dem vSphere-Host eine Lizenz hinzuzufügen.

      Dieser Schritt kann auf Wunsch später abgeschlossen werden.

   f. Klicken Sie auf Weiter, um den Sperrmodus deaktiviert zu lassen.
   g. Klicken Sie auf der Seite VM-Speicherort auf Weiter.
   h. Überprüfen Sie die Seite „bereit für Fertigstellung“. Verwenden Sie die Zurück-Taste, um Änderungen vorzunehmen, oder wählen Sie Fertig stellen.
3. Wiederholen Sie die Schritte 1 und 2 für Cisco UCS Host B. Dieser Prozess muss für alle zusätzlichen Hosts abgeschlossen werden, die zur Konfiguration von FlexPod Express hinzugefügt werden.

Konfigurieren Sie coredump auf ESXi Hosts

1. Stellen Sie mithilfe von SSH eine Verbindung zum Management-IP-ESXi-Host her, geben Sie Root für den Benutzernamen ein und geben Sie das Root-Passwort ein.
2. Führen Sie folgende Befehle aus:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. Die Nachricht `Verified the configured netdump server is running` Wird angezeigt, nachdem Sie den letzten Befehl eingegeben haben.

Dieser Prozess muss für alle zusätzlichen, FlexPod Express hinzugefügten Hosts abgeschlossen sein.

Schlussfolgerung

FlexPod Express ist eine einfache und effiziente Lösung und bietet ein validiertes Design mit branchenführenden Komponenten. Durch die Skalierung bis hin zum Hinzufügen weiterer Komponenten kann FlexPod Express gezielt auf spezifische Geschäftsanforderungen angepasst werden. FlexPod Express wurde für kleine und mittelständische Unternehmen, Großunternehmen und andere Unternehmen konzipiert, die dedizierte Lösungen benötigen.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Daten finden Sie in

den folgenden Dokumenten bzw. auf den folgenden Websites:

- NetApp Produktdokumentation

  "http://docs.netapp.com"

- Entwurfsleitfaden FlexPod Express mit VMware vSphere 6.7 und NetApp AFF A220

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

FlexPod Express mit VMware vSphere 6.7U1 und NetApp AFF A220 mit Direct-Attached IP-basiertem Storage

NVA-1131-DEPLOY: FlexPod Express mit VMware vSphere 6.7U1 und NetApp AFF A220 mit Direct-Attached IP-basiertem Storage

See Lakshmi Lanka, NetApp

Aktuell stellen immer mehr Unternehmen ihre Rechenzentren auf eine Shared IT Infrastructure und Cloud Computing um. Außerdem wünschen sich Unternehmen eine einfache und effektive Lösung für Remote-Standorte und Zweigstellen, die ihnen die Technologie nutzt, die sie in ihrem Datacenter kennen.

FlexPod Express ist eine vorkonfigurierte Best Practice-Architektur auf Grundlage des Cisco Unified Computing System (Cisco UCS), der Cisco Nexus Switches-Familie und NetApp Storage-Technologien. Die Komponenten eines FlexPod Express Systems sind wie ihre Kollegen im FlexPod Datacenter, die Managementsynergien über die gesamte IT-Infrastrukturumgebung hinweg in geringerem Umfang ermöglichen. FlexPod Datacenter und FlexPod Express sind optimale Plattformen für die Virtualisierung sowie für Bare-Metal-Betriebssysteme und Enterprise Workloads.

FlexPod Datacenter und FlexPod Express bieten eine Basiskonfiguration, die sich flexibel an eine Vielzahl von Anwendungsfällen und Anforderungen anpassen lässt. Bestehende FlexPod Datacenter-Kunden können ihr FlexPod Express System mit den gewohnten Tools managen. Neue FlexPod Express Kunden können sich mühelos an das Management von FlexPod Datacenter anpassen, wenn ihre Umgebung wächst.

FlexPod Express ist die optimale Infrastrukturbasis für Remote-Standorte und Zweigstellen (ROBOs) und für kleine bis mittelständische Unternehmen. Es ist außerdem eine optimale Lösung für Kunden, die eine Infrastruktur für einen dedizierten Workload bereitstellen möchten.

FlexPod Express bietet eine einfach zu managende Infrastruktur, die sich für fast alle Workloads eignet.

Lösungsüberblick

Diese FlexPod Express Lösung ist Bestandteil des konvergenten Infrastrukturprogramms von FlexPod.

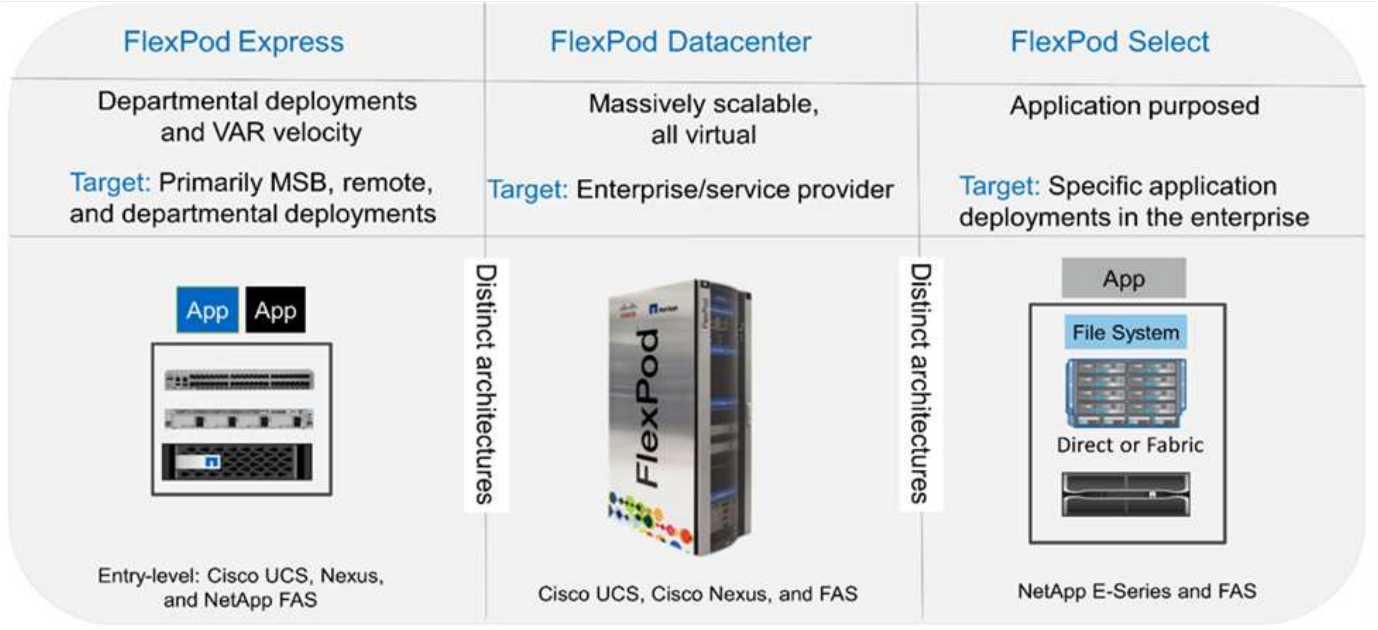
FlexPod Converged Infrastructure Programm

FlexPod Referenzarchitekturen werden als Cisco Validated Designs (CVDs) oder NetApp Verified Architectures (NVAs) bereitgestellt. Abweichungen, die auf Kundenanforderungen von einem bestimmten CVD oder NVA basieren, sind zulässig, wenn diese Variationen keine nicht unterstützte Konfiguration erstellen.

Wie in der Abbildung unten dargestellt, umfasst das FlexPod Programm drei Lösungen: FlexPod Express, FlexPod Datacenter und FlexPod Select:

- **FlexPod Express** bietet Kunden eine Einstiegslösung mit Technologien von Cisco und NetApp.
- **FlexPod Datacenter** bietet eine optimale Mehrzweckgrundlage für verschiedene Workloads und Anwendungen.
- **FlexPod Select** umfasst die besten Aspekte des FlexPod-Datacenter und stimmt die Infrastruktur auf eine bestimmte Applikation ab.

In der folgenden Abbildung sind die technischen Komponenten der Lösung dargestellt.



NetApp Verified Architecture das Programm

Das NVA-Programm bietet Kunden eine verifizierte Architektur für NetApp Lösungen an. Eine NVA bietet eine NetApp Lösungsarchitektur mit folgenden Eigenschaften:

- Sorgfältig getestet
- Präskriptiv
- Minimale Risiken bei der Implementierung
- Schnellere Produkteinführungszeiten

Dieser Leitfaden beschreibt das Design von FlexPod Express mit Direct-Attached NetApp Storage. In den folgenden Abschnitten werden die zum Design dieser Lösung verwendeten Komponenten aufgeführt.

Hardwarekomponenten

- NetApp AFF A220
- Cisco UCS Mini
- CISCO UCS B200 M5
- Cisco UCS VIC 1440/1480

- Switches Der Cisco Nexus 3000-Serie

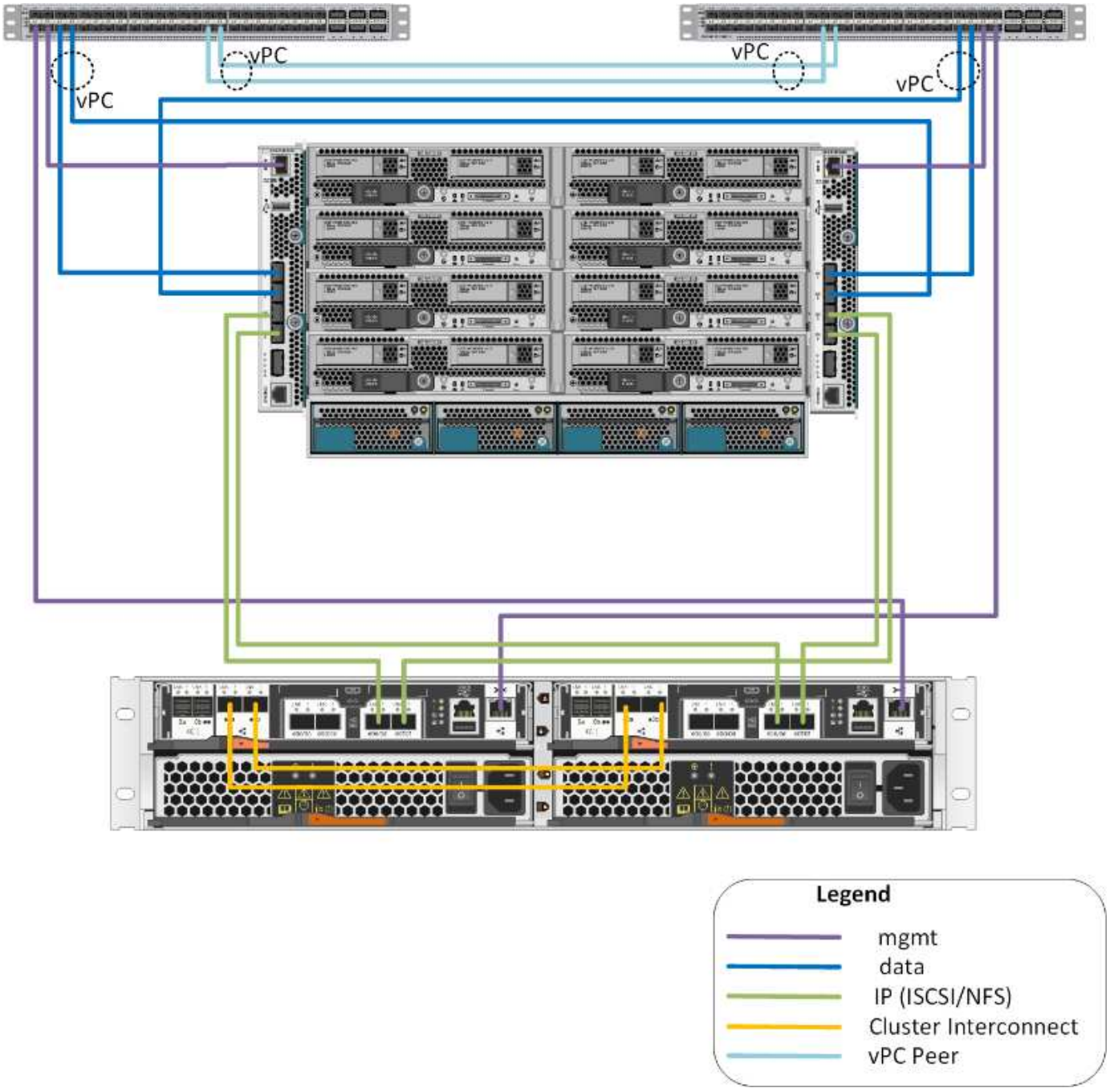
Softwarekomponenten

- NetApp ONTAP 9 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Cisco NXOS Firmware 7.0(3)I6(1)

Lösungstechnologie

Diese Lösung nutzt die neuesten Technologien von NetApp, Cisco und VMware. Sie umfasst das neue NetApp AFF A220 mit ONTAP 9.5, zwei Cisco Nexus 31108PCV Switches und Cisco UCS B200 M5 Servern mit VMware vSphere 6.7U1. Diese validierte Lösung setzt Direct Connect IP Storage über 10-GbE-Technologie ein.

Die folgende Abbildung zeigt FlexPod Express mit der VMware vSphere 6.7U1 IP-basierten Direct Connect-Architektur.



Zusammenfassung des Anwendungsfalls

Die FlexPod Express Lösung kann für verschiedene Anwendungsfälle eingesetzt werden. Dazu zählen:

- Roboter
- Kleine und mittelständische Unternehmen
- Umgebungen, für die eine dedizierte und kostengünstige Lösung erforderlich ist

FlexPod Express eignet sich am besten für virtualisierte und gemischte Workloads.

Technologieanforderungen erfüllt

Ein FlexPod Express System erfordert eine Kombination aus Hardware- und

Softwarekomponenten. FlexPod Express beschreibt außerdem die Hardwarekomponenten, die erforderlich sind, um dem System in Einheiten von zwei Hypervisor-Nodes hinzuzufügen.

Hardwareanforderungen

Unabhängig vom ausgewählten Hypervisor nutzen alle FlexPod Express Konfigurationen dieselbe Hardware. Daher kann auch bei sich ändernden Geschäftsanforderungen jeder Hypervisor auf derselben FlexPod Express Hardware ausgeführt werden.

In der folgenden Tabelle werden die Hardwarekomponenten aufgeführt, die für alle FlexPod Express Konfigurationen erforderlich sind.

Trennt	Menge
AFF A220 HA-PAAR	1
Cisco UCS B200 M5 Server	2
Cisco Nexus 31108PCV-Switch	2
Cisco UCS Virtual Interface Card (VIC) 1440 für den Cisco UCS B200 M5 Server	2
Cisco UCS Mini mit zwei integrierten UCS-FI-M-6324 Fabric Interconnects	1

Softwareanforderungen

In der folgenden Tabelle werden die Softwarekomponenten aufgeführt, die für die Implementierung der Architekturen der FlexPod Express Lösungen erforderlich sind.

Software	Version	Details
Cisco UCS Manager	4.0(1b)	Für Cisco UCS Fabric Interconnect FI-6324UP
Cisco Blade Software	4.0(1b)	Für Cisco UCS B200 M5 Server
Cisco Nenic-Treiber	1.0.25.0	Für Cisco VIC 1440 Schnittstellenkarten
Cisco NX-OS	7.0(3)I6(1)	Für Cisco Nexus 31108PCV Switches
NetApp ONTAP	9.5	Für AFF A220 Controller

In der folgenden Tabelle ist die erforderliche Software für alle VMware vSphere Implementierungen auf FlexPod Express aufgeführt.

Software	Version
VMware vCenter Server Appliance	6.7U1
VMware vSphere ESXi Hypervisor	6.7U1

Informationen zur FlexPod Express Verkabelung

Die Verkabelung zur Referenzvalidierung ist in den folgenden Tabellen dokumentiert.

In der folgenden Tabelle sind die Verkabelungsinformationen für den Cisco Nexus Switch 31108PCV A. aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus Switch 31108PCV A	Eth1/1	NetApp AFF A220 Storage-Controller A	E0M
	Eth1/2	Cisco UCS Mini FI-A	Mgmt0
	Eth1/3	Cisco UCS Mini FI-A	Eth1/1
	Eth 1/4	Cisco UCS-Mini FI-B	Eth1/1
	Eth 1/13	CISCO NX 31108PCV B	Eth 1/13
	Eth 1/14	CISCO NX 31108PCV B	Eth 1/14

In der folgenden Tabelle sind die Verkabelungsinformationen für den Cisco Nexus Switch 31108PCV B aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco Nexus Switch 31108PCV B	Eth1/1	NetApp AFF A220 Storage-Controller B	E0M
	Eth1/2	Cisco UCS-Mini FI-B	Mgmt0
	Eth1/3	Cisco UCS Mini FI-A	Eth1/2
	Eth 1/4	Cisco UCS-Mini FI-B	Eth1/2
	Eth 1/13	CISCO NX 31108PCV A	Eth 1/13
	Eth 1/14	CISCO NX 31108PCV A	Eth 1/14

In der folgenden Tabelle sind die Verkabelungsinformationen für NetApp AFF A220 Storage Controller aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF A220 Storage-Controller A	e0a	NetApp AFF A220 Storage-Controller B	e0a
	e0b	NetApp AFF A220 Storage-Controller B	e0b
	e0e	Cisco UCS Mini FI-A	Eth1/3
	e0f	Cisco UCS-Mini FI-B	Eth1/3
	E0M	CISCO NX 31108PCV A	Eth1/1

In der folgenden Tabelle sind die Verkabelungsinformationen für NetApp AFF A220 Storage Controller B aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
NetApp AFF A220 Storage-Controller B	e0a	NetApp AFF A220 Storage-Controller B	e0a
	e0b	NetApp AFF A220 Storage-Controller B	e0b
	e0e	Cisco UCS Mini FI-A	Eth1/4
	e0f	Cisco UCS-Mini FI-B	Eth1/4
	E0M	CISCO NX 31108PCV B	Eth1/1

In der folgenden Tabelle sind die Verkabelungsinformationen für Cisco UCS Fabric Interconnect A aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco UCS Fabric Interconnect A	Eth1/1	CISCO NX 31108PCV A	Eth1/3
	Eth1/2	CISCO NX 31108PCV B	Eth1/3
	Eth1/3	NetApp AFF A220 Storage-Controller A	e0e
	Eth1/4	NetApp AFF A220 Storage-Controller B	e0e
	Mgmt0	CISCO NX 31108PCV A	Eth1/2

In der folgenden Tabelle sind die Verkabelungsinformationen für Cisco UCS Fabric Interconnect B aufgeführt

Lokales Gerät	Lokaler Port	Remote-Gerät	Remote-Port
Cisco UCS Fabric Interconnect B	Eth1/1	CISCO NX 31108PCV A	Eth1/4
	Eth1/2	CISCO NX 31108PCV B	Eth1/4
	Eth1/3	NetApp AFF A220 Storage-Controller A	e0f
	Eth1/4	NetApp AFF A220 Storage-Controller B	e0f
	Mgmt0	CISCO NX 31108PCV B	Eth1/2

Implementierungsverfahren

Dieses Dokument enthält Details zur Konfiguration eines vollständig redundanten, hochverfügbaren FlexPod Express-Systems. Um diese Redundanz Rechnung zu tragen, werden die in jedem Schritt konfigurierten Komponenten entweder als Komponente A oder Komponente B bezeichnet Controller A und Controller B identifizieren beispielsweise die beiden NetApp Storage Controller, die in diesem Dokument bereitgestellt werden. Switch A und Switch B identifizieren ein Paar Cisco Nexus-Switches. Fabric Interconnect A und Fabric Interconnect B sind die zwei integrierten Nexus Fabric Interconnects.

Zusätzlich beschreibt dieses Dokument Schritte zur Bereitstellung mehrerer Cisco UCS-Hosts, die sequenziell als Server A, Server B usw. identifiziert werden können.

Um anzugeben, dass Sie in einem Schritt Informationen zu Ihrer Umgebung angeben sollten, `<<text>>` Wird als Teil der Befehlsstruktur angezeigt. Das folgende Beispiel enthält die `vlan create` Befehl:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Mit diesem Dokument können Sie die FlexPod Express Umgebung vollständig konfigurieren. Bei diesem Prozess müssen Sie in verschiedenen Schritten kundenspezifische Namenskonventionen, IP-Adressen und VLAN-Schemata (Virtual Local Area Network) einfügen. Die folgende Tabelle beschreibt die für die Implementierung erforderlichen VLANs, wie in diesem Leitfaden beschrieben. Diese Tabelle kann anhand der spezifischen Standortvariablen abgeschlossen und zur Implementierung der Konfigurationsschritte des Dokuments verwendet werden.

Wenn Sie separate bandinterne und Out-of-Band-Management-VLANs verwenden, müssen Sie eine Layer-3-Route zwischen ihnen erstellen. Für diese Validierung wurde ein gemeinsames Management-VLAN genutzt.

VLAN-Name	VLAN-Zweck	ID, die bei der Validierung dieses Dokuments verwendet wird
Management-VLAN	VLAN für Management-Schnittstellen	18
Natives VLAN	VLAN, dem nicht getaggte Frames zugewiesen sind	2
NFS-VLAN	VLAN für NFS-Verkehr	104
VMware vMotion VLAN	VLAN, das für die Verschiebung von Virtual Machines (VMs) von einem physischen Host auf einen anderen festgelegt ist	103
VM-Traffic-VLAN	VLAN für den Datenverkehr von VM-Applikationen	102
ISCSI-A-VLAN	VLAN für iSCSI-Verkehr auf Fabric A	124
ISCSI-B-VLAN	VLAN für iSCSI-Datenverkehr auf Fabric B	125

Die VLAN-Nummern sind in der gesamten Konfiguration von FlexPod Express erforderlich. Die VLANs werden als bezeichnet `<<var_xxxx_vlan>>`, Wo `xxxx` Dient dem VLAN (z. B. iSCSI-A).

In der folgenden Tabelle werden die erstellten VMware VMs aufgeführt.

VM-Beschreibung	Host-Name
VMware vCenter Server	Seahawks-vcsa.cie.netapp.com

Cisco Nexus 31108PCV-Implementierungsverfahren

In diesem Abschnitt wird die in einer FlexPod Express Umgebung verwendete Cisco Nexus 31308PCV-Switch-Konfiguration beschrieben.

Ersteinrichtung des Cisco Nexus 31108PCV Switches

Dieses Verfahren beschreibt die Konfiguration der Cisco Nexus Switches für die Verwendung in einer grundlegenden FlexPod Express Umgebung.

> Bei diesem Verfahren wird davon ausgegangen, dass Sie einen Cisco Nexus 31108PCV verwenden, der NX-OS-Software-Version 7.0(3)I6(1) ausführt.

1. Nach dem ersten Booten und der Verbindung zum Konsolen-Port des Switches wird automatisch das Cisco NX-OS Setup gestartet. Diese Erstkonfiguration betrifft grundlegende Einstellungen wie den Switch-Namen, die mgmt0-Schnittstellenkonfiguration und die Einrichtung der Secure Shell (SSH).
2. Das FlexPod Express Managementnetzwerk lässt sich auf unterschiedliche Weise konfigurieren. Die mgmt0-Schnittstellen auf den 31108PCV-Switches können mit einem vorhandenen Managementnetzwerk verbunden werden, oder die mgmt0-Schnittstellen der 31108PCV-Switches können in einer Back-to-Back-Konfiguration angeschlossen werden. Dieser Link kann jedoch nicht für externen Managementzugriff wie SSH-Datenverkehr verwendet werden.

   In diesem Implementierungsleitfaden werden die Cisco Nexus 31108PCV-Switches von FlexPod Express mit einem vorhandenen Managementnetzwerk verbunden.
3. Um die Cisco Nexus 31108PCV-Switches zu konfigurieren, schalten Sie den Switch ein, und befolgen Sie die Anweisungen auf dem Bildschirm, wie hier bei der Ersteinrichtung der beiden Switches dargestellt, und ersetzen Sie die entsprechenden Werte für die Switch-spezifischen Informationen.

   ```
   This setup utility will guide you through the basic configuration of the
   system. Setup configures only enough connectivity for management of the
   system.
   ```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. Eine Zusammenfassung Ihrer Konfiguration wird angezeigt, und Sie werden gefragt, ob Sie die Konfiguration bearbeiten möchten. Wenn die Konfiguration korrekt ist, geben Sie ein `n`.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. Sie werden dann gefragt, ob Sie diese Konfiguration verwenden und speichern möchten. Wenn ja, geben Sie ein `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Wiederholen Sie die Schritte 1 bis 5 für Cisco Nexus Switch B.

Aktivieren Sie erweiterte Funktionen

Bestimmte erweiterte Funktionen müssen in Cisco NX-OS aktiviert sein, um zusätzliche Konfigurationsoptionen bereitzustellen.

1. Um die entsprechenden Funktionen bei Cisco Nexus Switch A und Switch B zu aktivieren, wechseln Sie mit dem Befehl in den Konfigurationsmodus `(config t)` Und führen Sie folgende Befehle aus:

```
feature interface-vlan
feature lacp
feature vpc
```

> Der Standard-Port-Channel-Load-Balancing-Hash verwendet die Quell- und Ziel-IP-Adressen, um den Load-Balancing-Algorithmus über die Schnittstellen im Port-Kanal zu bestimmen. Sie können eine bessere Verteilung über die Mitglieder des Port-Kanals erzielen, indem Sie mehr Inputs für den Hash-Algorithmus bereitstellen, der über die Quell- und Ziel-IP-Adressen hinausgeht. Aus dem gleichen Grund empfiehlt NetApp dringend, den Hash-Algorithmus der Quell- und Ziel-TCP-Ports hinzuzufügen.

2. Im Konfigurationsmodus `(config t)`, Führen Sie die folgenden Befehle aus, um die globale Port Channel Load-Balancing-Konfiguration auf Cisco Nexus Switch A und Switch B festzulegen:

```
port-channel load-balance src-dst ip-l4port
```

Führen Sie eine globale Spanning-Tree-Konfiguration durch

Die Cisco Nexus Plattform verwendet eine neue Sicherungsfunktion namens „Bridge Assurance“. Bridge Assurance schützt vor unidirektionalen Verbindungsfehlern oder anderen Softwarefehlern mit einem Gerät, das den Datenverkehr weiterführt, wenn der Spanning-Tree-Algorithmus nicht mehr ausgeführt wird. Die Ports können je nach Plattform in einen von mehreren Status platziert werden, einschließlich Netzwerk oder Edge.

NetApp empfiehlt, die Bridge-Assurance einzustellen, damit alle Ports standardmäßig für Netzwerkports gelten. Diese Einstellung zwingt den Netzwerkadministrator, die Konfiguration jedes Ports zu überprüfen. Außerdem werden die häufigsten Konfigurationsfehler angezeigt, z. B. nicht identifizierte Edge-Ports oder ein Nachbar, bei dem die Bridge-Assurance-Funktion nicht aktiviert ist. Außerdem ist es sicherer, den Spanning Tree Block viele Ports statt zu wenig zu haben, was den Standard-Port-Zustand ermöglicht, um die allgemeine Stabilität des Netzwerks zu verbessern.

Achten Sie beim Hinzufügen von Servern, Speicher- und Uplink-Switches auf den Spanning-Tree-Status, insbesondere wenn diese keine Bridge-Sicherheit unterstützen. In solchen Fällen müssen Sie möglicherweise den Porttyp ändern, um die Ports aktiv zu machen.

Die BPDU-Schutzfunktion (Bridge Protocol Data Unit) ist standardmäßig auf Edge-Ports als andere Schutzschicht aktiviert. Um Schleifen im Netzwerk zu vermeiden, wird der Port durch diese Funktion heruntergefahren, wenn BPDUs von einem anderen Switch auf dieser Schnittstelle angezeigt werden.

Im Konfigurationsmodus (`config t`), führen Sie die folgenden Befehle aus, um die standardmäßigen Spanning-Tree-Optionen, einschließlich des Standard-Porttyps und BPDU Guard, auf Cisco Nexus Switch A und Switch B zu konfigurieren:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Definieren Sie VLANs

Bevor individuelle Ports mit unterschiedlichen VLANs konfiguriert sind, müssen auf dem Switch Layer-2-VLANs definiert werden. Es ist auch eine gute Praxis, die VLANs zu benennen, um zukünftig eine einfache Fehlerbehebung zu ermöglichen.

Im Konfigurationsmodus (`config t`), führen Sie die folgenden Befehle aus, um die Layer-2-VLANs auf Cisco Nexus Switch A und Switch B zu definieren und zu beschreiben:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Konfiguration von Zugriffs- und Management-Port-Beschreibungen

Wie bei der Zuordnung von Namen zu den Layer-2-VLANs können die Einstellungsbeschreibungen für alle Schnittstellen sowohl bei der Bereitstellung als auch bei der Fehlerbehebung helfen.

Im Konfigurationsmodus (`config t`) Geben Sie bei jedem der Switches die folgenden Portbeschreibungen für die FlexPod Express Large-Konfiguration ein:

Cisco Nexus Switch A

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Cisco Nexus Switch B

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Konfiguration der Server- und Storage-Managementschnittstellen

Die Management-Schnittstellen sowohl für den Server als auch für den Storage verwenden in der Regel nur ein einziges VLAN. Konfigurieren Sie daher die Ports der Managementoberfläche als Access Ports. Definieren Sie das Management-VLAN für jeden Switch und ändern Sie den Porttyp Spanning-Tree in Edge.

Im Konfigurationsmodus (`config t`Führen Sie die folgenden Befehle aus, um die Porteinstellungen für die Verwaltungsschnittstellen der Server und des Speichers zu konfigurieren:

Cisco Nexus Switch A

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Cisco Nexus Switch B

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Fügen Sie die NTP-Distributionsschnittstelle hinzu

Cisco Nexus Switch A

Führen Sie im globalen Konfigurationsmodus die folgenden Befehle aus.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Cisco Nexus Switch B

Führen Sie im globalen Konfigurationsmodus die folgenden Befehle aus.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

Globale Konfiguration des virtuellen Port-Channels durchführen

Über einen Virtual Port Channel (vPC) können Links, die physisch mit zwei verschiedenen Cisco Nexus-Switches verbunden sind, mit einem dritten Gerät als einzelner Port-Channel angezeigt werden. Das dritte Gerät kann ein Switch, Server oder ein anderes Netzwerkgerät sein. Ein vPC bietet Multipathing auf Layer-2-Ebene. Dadurch kann Redundanz erzeugt werden, indem die Bandbreite erhöht wird. Dies ermöglicht mehrere parallele Pfade zwischen Nodes und Lastverteilung zwischen alternativen Pfaden.

Ein vPC bietet die folgenden Vorteile:

- Aktivieren eines einzelnen Geräts zur Verwendung eines Port-Kanals über zwei vorgelagerte Geräte
- Blockierte Ports für Spanning-Tree-Protokolle werden eliminiert
- Eine Topologie ohne Schleife
- Nutzung aller verfügbaren Uplink-Bandbreite
- Schnelle Konvergenz bei Ausfall der Verbindung oder eines Geräts
- Ausfallsicherheit auf Verbindungsebene
- Unterstützung für Hochverfügbarkeit

Die vPC-Funktion erfordert eine Ersteinrichtung zwischen den beiden Cisco Nexus-Switches, damit diese ordnungsgemäß funktionieren. Wenn Sie die Back-to-Back-mmmt0-Konfiguration verwenden, verwenden Sie die auf den Schnittstellen definierten Adressen und stellen Sie sicher, dass sie über den Ping kommunizieren können `<<switch_A/B_mgmt0_ip_addr>>vrf` Management-Befehl.

Im Konfigurationsmodus (`config t`Führen Sie die folgenden Befehle aus, um die globale vPC-Konfiguration für beide Switches zu konfigurieren:

Cisco Nexus Switch A

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Cisco Nexus Switch B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

In dieser Lösungsvalidierung wurde eine MTU (Maximum Transmission Unit) von 9000 verwendet. Basierend auf Anwendungsanforderungen können Sie jedoch einen entsprechenden Wert für die MTU konfigurieren. Es ist wichtig, für die gesamte FlexPod Lösung denselben MTU-Wert festzulegen. Falsche MTU-Konfigurationen zwischen Komponenten führen zum Paketabfallenlassen.

Uplink zur bestehenden Netzwerkinfrastruktur

Je nach verfügbarer Netzwerkinfrastruktur können zur Uplink der FlexPod Umgebung mehrere Methoden und Funktionen verwendet werden. Wenn eine vorhandene Cisco Nexus Umgebung vorhanden ist, empfiehlt NetApp die Verwendung von vPCs, um die in der FlexPod Umgebung enthaltenen Cisco Nexus 31108PVC-Switches in die Infrastruktur zu integrieren. Bei den Uplinks können 10-GbE-Uplinks für eine 10-GbE-Infrastrukturlösung oder 1 GbE für eine Infrastrukturlösung (sofern erforderlich) verwendet werden. Die zuvor beschriebenen Verfahren können zur Erstellung eines Uplink vPC in der vorhandenen Umgebung verwendet werden. Stellen Sie sicher, dass Sie den Kopierlauf ausführen, um die Konfiguration nach Abschluss der Konfiguration auf jedem Switch zu speichern.

Verfahren zur NetApp Storage-Implementierung (Teil 1)

In diesem Abschnitt wird das NetApp AFF Storage-Implementierungsverfahren beschrieben.

Installation von NetApp Storage Controller AFF2xx Series

NetApp Hardware Universe

Der "NetApp Hardware Universe" Die HWU Applikation bietet unterstützte Hardware- und Softwarekomponenten für jede spezifische ONTAP Version. Das Tool liefert Konfigurationsinformationen für alle NetApp Storage Appliances, die derzeit von der ONTAP Software unterstützt werden. Zudem bietet er eine Tabelle mit den Kompatibilitäten der Komponenten.

Vergewissern Sie sich, dass die Hardware- und Softwarekomponenten, die Sie verwenden möchten, von der zu installierenden Version von ONTAP unterstützt werden:

1. Auf das zugreifen "HWU" Anwendung zum Anzeigen der Systemkonfigurationsleitfäden. Wählen Sie die Registerkarte „Vergleichen“ Storage-Systeme aus. Hier sehen Sie die Kompatibilität zwischen verschiedenen Versionen der ONTAP Software und den NetApp Storage Appliances mit den gewünschten Spezifikationen.
2. Wenn Sie Komponenten nach Storage Appliance vergleichen möchten, klicken Sie alternativ auf Storage-Systeme vergleichen.

Voraussetzungen für Controller AFF2XX Serie
Zur Planung des physischen Standorts der Storage-Systeme finden Sie in den folgenden Abschnitten: Unterstützte elektrische Netzstromkabel Onboard-Ports und Kabel

Storage Controller

Befolgen Sie die Anweisungen zur physischen Installation der Controller im "AFF A220: Dokumentation".

Konfigurationsarbeitsblatt

Bevor Sie das Setup-Skript ausführen, füllen Sie das Konfigurationsarbeitsblatt aus der Produktanleitung aus. Das Konfigurationsarbeitsblatt ist im verfügbar "ONTAP 9.5 – Leitfaden für die Software-Einrichtung" (Verfügbar im "ONTAP 9 Dokumentationszentrum"). Die folgende Tabelle enthält Informationen zur Installation und Konfiguration von ONTAP 9.5.

Das System ist in einer Konfiguration mit zwei Nodes ohne Switches eingerichtet.

Cluster-Details	Wert Für Cluster-Details
Cluster Node A IP-Adresse	<<var_nodeA_Mgmt_ip>>
Cluster-Node A-Netmask	<<var_nodeA_mgmt_maska>>
Cluster Node Ein Gateway	\<<var_nodeA_mgmt_Gateway>
Cluster-Node A-Name	<<var_nodeA>>
Cluster-Node B-IP-Adresse	<<var_nodeB_Mgmt_ip>>
Cluster-Node B-Netmask	<<var_nodeB_mgmt_maska>>
Cluster-Node B-Gateway	\<<var_nodeB_mgmt_Gateway>
Name für Cluster-Node B	<<var_nodeB>>
ONTAP 9.5-URL	\<<var_url_Boot_Software>
Name für Cluster	<<var_clustername>>
Cluster-Management-IP-Adresse	<<var_clustermgmt_ip>>
Cluster B-Gateway	<<var_clustermgmt_Gateway>>
Cluster B Netmask	<<var_clustermgmt_maska>>
Domain-Name	<<var_Domain_Name>>
DNS-Server-IP (Sie können mehrere eingeben)	<<var_dns_Server_ip>>
NTP-SERVER A-IP	<< Switch-a-ntp-ip >>
NTP-SERVER B-IP	<< Switch-b-ntp-ip >>

Konfigurieren Sie Node A

Führen Sie die folgenden Schritte aus, um Node A zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg- C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Lassen Sie das System booten.

```
autoboot
```

3. Drücken Sie Strg- C, um das Startmenü aufzurufen.

   Bei ONTAP 9. 5 ist nicht die Version der Software, die gerade gestartet wird. Fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Bei ONTAP 9. 5 wird die Version gebootet. Wählen Sie Option 8 und y, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

4. Um neue Software zu installieren, wählen Sie Option `7`.
5. Eingabe `y` Um ein Upgrade durchzuführen.
6. Wählen Sie `e0M` Für den Netzwerkanschluss, den Sie für den Download verwenden möchten.
7. Eingabe `y` Jetzt neu starten.
8. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Geben Sie die URL ein, auf der die Software gefunden werden kann.

   Dieser Webserver muss pingfähig sein.

10. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an.
11. Eingabe `y` So legen Sie die neu installierte Software als Standard fest, die bei einem späteren Neustart verwendet wird.
12. Eingabe `y` Um den Node neu zu booten.

    Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

13. Drücken Sie Strg- C, um das Startmenü aufzurufen.
14. Wählen Sie die Option `4` Für saubere Konfiguration und Initialisieren aller Festplatten.
15. Eingabe `y` Setzen Sie die Konfiguration auf Null Festplatten zurück, und installieren Sie ein neues Dateisystem.
16. Eingabe `y` Um alle Daten auf den Festplatten zu löschen.

    Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert. Sie können mit der Node B-Konfiguration fortfahren, während die Festplatten für Node A auf Null gesetzt werden.

17. Beginnen Sie während der Initialisierung von Node A mit der Konfiguration von Node B.

Konfigurieren Sie Node B

Führen Sie die folgenden Schritte aus, um Node B zu konfigurieren:

1. Stellt eine Verbindung mit dem Konsolen-Port des Storage-Systems her. Es sollte eine Loader-A-Eingabeaufforderung angezeigt werden. Wenn sich das Storage-System jedoch in einer Reboot-Schleife befindet, drücken Sie Strg-C, um die Autoboot-Schleife zu beenden, wenn Sie diese Meldung sehen:

   ```
   Starting AUTOBOOT press Ctrl-C to abort...
   ```

2. Drücken Sie Strg-C, um das Startmenü aufzurufen.

   ```
   autoboot
   ```

3. Drücken Sie bei der entsprechenden Aufforderung Strg-C.

   Bei ONTAP 9. 5 ist nicht die Version der Software, die gerade gestartet wird. Fahren Sie mit den folgenden Schritten fort, um neue Software zu installieren. Wenn ONTAP 9.4 die Version wird gebootet, wählen Sie Option 8 und y aus, um den Node neu zu booten. Fahren Sie dann mit Schritt 14 fort.

4. Um neue Software zu installieren, wählen Sie Option 7.
5. Eingabe `y` Um ein Upgrade durchzuführen.
6. Wählen Sie `e0M` Für den Netzwerkanschluss, den Sie für den Download verwenden möchten.
7. Eingabe `y` Jetzt neu starten.
8. Geben Sie an den jeweiligen Stellen die IP-Adresse, die Netmask und das Standard-Gateway für E0M ein.

   ```
   <<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
   ```

9. Geben Sie die URL ein, auf der die Software gefunden werden kann.

   Dieser Webserver muss pingfähig sein.

   ```
   <<var_url_boot_software>>
   ```

10. Drücken Sie die Eingabetaste, um den Benutzernamen anzuzeigen, und geben Sie keinen Benutzernamen an
11. Eingabe `y` So legen Sie die neu installierte Software als Standard fest, die bei einem späteren Neustart verwendet wird.
12. Eingabe `y` Um den Node neu zu booten.

    Beim Installieren der neuen Software führt das System möglicherweise Firmware-Upgrades für das BIOS und die Adapterkarten durch. Dies führt zu einem Neustart und möglichen Stopps an der Loader-A-Eingabeaufforderung. Wenn diese Aktionen auftreten, kann das System von diesem Verfahren abweichen.

13. Drücken Sie Strg-C, um das Startmenü aufzurufen.
14. Wählen Sie Option 4 für saubere Konfiguration und Initialisieren Sie alle Festplatten.
15. Eingabe `y` Setzen Sie die Konfiguration auf Null Festplatten zurück, und installieren Sie ein neues Dateisystem.
16. Eingabe `y` Um alle Daten auf den Festplatten zu löschen.

    Die Initialisierung und Erstellung des Root-Aggregats kann je nach Anzahl und Typ der verbundenen Festplatten 90 Minuten oder mehr dauern. Nach Abschluss der Initialisierung wird das Storage-System neu gestartet. Beachten Sie, dass die Initialisierung von SSDs erheblich schneller dauert.

Fortsetzung von Node A-Konfiguration und Cluster-Konfiguration

Führen Sie von einem Konsolen-Port-Programm, das an den Storage Controller A (Node A)-Konsolenport angeschlossen ist, das Node-Setup-Skript aus. Dieses Skript wird angezeigt, wenn ONTAP 9.5 das erste Mal auf dem Node gebootet wird.

In ONTAP 9.5 wurde das Verfahren zur Einrichtung von Nodes und Clustern geringfügig geändert. Der Cluster-Setup-Assistent wird jetzt zum Konfigurieren des ersten Node in einem Cluster verwendet, während System Manager zum Konfigurieren des Clusters verwendet wird.

1. Befolgen Sie die Anweisungen zum Einrichten von Node A

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navigieren Sie zur IP-Adresse der Managementoberfläche des Knotens.

> Das Cluster-Setup kann auch über die CLI durchgeführt werden. In diesem Dokument wird die Cluster-Einrichtung mit der von NetApp System Manager geführten Einrichtung beschrieben.

3. Klicken Sie auf Guided Setup, um das Cluster zu konfigurieren.
4. Eingabe `<<var_clustername>>` Für den Cluster-Namen und `<<var_nodeA>>` Und `<<var_nodeB>>` Für jeden der Nodes, die Sie konfigurieren. Geben Sie das Passwort ein, das Sie für das Speichersystem verwenden möchten. Wählen Sie für den Cluster-Typ Cluster ohne Switch aus. Geben Sie die Cluster-Basislizenz ein.
5. Außerdem können Funktionslizenzen für Cluster, NFS und iSCSI eingegeben werden.
6. Eine Statusmeldung, die angibt, dass das Cluster erstellt wird. Diese Statusmeldung durchlaufen mehrere Statusarten. Dieser Vorgang dauert mehrere Minuten.
7. Konfigurieren des Netzwerks.
   a. Deaktivieren Sie die Option IP-Adressbereich.

b. Eingabe <<var_clustermgmt_ip>> Im Feld Cluster-Management-IP-Adresse <<var_clustermgmt_mask>> Im Feld „Netzmaske“ und <<var_clustermgmt_gateway>> Im Feld Gateway. Verwenden Sie die Auswahl … im Feld Port, um E0M von Knoten A. auszuwählen

c. Die Node-Management-IP für Node A ist bereits gefüllt. Eingabe <<var_nodeA_mgmt_ip>> Für Node B.

d. Eingabe <<var_domain_name>> Im Feld DNS-Domain-Name. Eingabe <<var_dns_server_ip>> Im Feld IP-Adresse des DNS-Servers.

   Sie können mehrere IP-Adressen des DNS-Servers eingeben.

e. Eingabe <<switch-a-ntp-ip>> Im Feld primärer NTP-Server.

   Sie können auch einen alternativen NTP-Server als eingeben <<switch- b-ntp-ip>>.

8. Konfigurieren Sie die Support-Informationen.
   a. Wenn in Ihrer Umgebung ein Proxy für den Zugriff auf AutoSupport erforderlich ist, geben Sie die URL unter Proxy-URL ein.
   b. Geben Sie den SMTP-Mail-Host und die E-Mail-Adresse für Ereignisbenachrichtigungen ein.

      Sie müssen mindestens die Methode für die Ereignisbenachrichtigung einrichten, bevor Sie fortfahren können. Sie können eine beliebige der Methoden auswählen.

9. Klicken Sie, wenn angegeben wird, dass die Cluster-Konfiguration abgeschlossen ist, auf Manage Your Cluster, um den Storage zu konfigurieren.

Fortführung der Storage-Cluster-Konfiguration

Nach der Konfiguration der Storage-Nodes und des Basis-Clusters können Sie die Konfiguration des Storage-Clusters fortsetzen.

Alle freien Festplatten auf Null stellen

Führen Sie den folgenden Befehl aus, um alle freien Festplatten im Cluster zu löschen:

```
disk zerospares
```

Onboard-UTA2-Ports als Persönlichkeit festlegen

1. Überprüfen Sie den aktuellen Modus und den aktuellen Typ der Ports, indem Sie den ausführen `ucadmin show` Befehl.

```
AFFA220-Clus::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. Überprüfen Sie, ob der aktuelle Modus der verwendeten Ports lautet `cna` Und dass der aktuelle Typ auf festgelegt ist `target`. Falls nicht, ändern Sie die Portpersönlichkeit, indem Sie den folgenden Befehl ausführen:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Die Ports müssen offline sein, um den vorherigen Befehl auszuführen. Führen Sie den folgenden Befehl aus, um einen Port offline zu schalten:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Wenn Sie die Port-Persönlichkeit geändert haben, müssen Sie jeden Node neu booten, damit die Änderung wirksam wird.

Aktivieren Sie Das Cisco Discovery-Protokoll

Führen Sie den folgenden Befehl aus, um das Cisco Discovery Protocol (CDP) auf den NetApp Storage Controllern zu aktivieren:

```
node run -node * options cdpd.enable on
```

Aktivieren Sie auf allen Ethernet-Ports das Link-Layer Discovery Protocol

Aktivieren Sie den Austausch von LLDP (Link-Layer Discovery Protocol)-Nachbarinformationen zwischen Speicher und Netzwerk-Switches, indem Sie den folgenden Befehl ausführen. Dieser Befehl aktiviert LLDP auf allen Ports aller Nodes im Cluster.

```
node run * options lldp.enable on
```

Benennen Sie logische Management-Schnittstellen um

Führen Sie die folgenden Schritte aus, um die logischen Management-Schnittstellen (LIFs) umzubenennen:

1. Zeigt die aktuellen Management-LIF-Namen an.

   ```
   network interface show –vserver <<clustername>>
   ```

2. Benennen Sie die Cluster-Management-LIF um.

   ```
   network interface rename –vserver <<clustername>> –lif
   cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
   ```

3. Benennen Sie die Management-LIF für Node B um.

   ```
   network interface rename -vserver <<clustername>> -lif
   cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
   ```

Legen Sie für das Cluster-Management den automatischen Wechsel zurück

Stellen Sie die ein `auto-revert` Parameter auf der Cluster-Managementoberfläche.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Richten Sie die Service Processor-Netzwerkschnittstelle ein

Um dem Service-Prozessor auf jedem Node eine statische IPv4-Adresse zuzuweisen, führen Sie die folgenden Befehle aus:

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Die Service-Prozessor-IP-Adressen sollten sich im gleichen Subnetz wie die Node-Management-IP-Adressen befinden.

Aktivieren Sie Storage-Failover in ONTAP

Führen Sie die folgenden Befehle in einem Failover-Paar aus, um zu überprüfen, ob das Storage-Failover aktiviert ist:

1. Überprüfen Sie den Status des Storage-Failovers.

   ```
   storage failover show
   ```

   Beides `<<var_nodeA>>` Und `<<var_nodeB>>` Muss in der Lage sein, ein Takeover durchzuführen. Fahren Sie mit Schritt 3 fort, wenn die Knoten ein Takeover durchführen können.

2. Aktivieren Sie Failover bei einem der beiden Nodes.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. Überprüfen Sie den HA-Status des Clusters mit zwei Nodes.

   Dieser Schritt gilt nicht für Cluster mit mehr als zwei Nodes.

   ```
   cluster ha show
   ```

4. Fahren Sie mit Schritt 6 fort, wenn Hochverfügbarkeit konfiguriert ist. Wenn die Hochverfügbarkeit konfiguriert ist, wird bei Ausgabe des Befehls die folgende Meldung angezeigt:

   ```
   High Availability Configured: true
   ```

5. Aktivieren Sie nur den HA-Modus für das Cluster mit zwei Nodes.

   Führen Sie diesen Befehl nicht für Cluster mit mehr als zwei Nodes aus, da es zu Problemen mit Failover kommt.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Überprüfung der korrekten Konfiguration von Hardware-Unterstützung und ggf. Änderung der Partner-IP-Adresse

```
storage failover hwassist show
```

Die Nachricht `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` Zeigt an, dass die Hardware-Unterstützung nicht konfiguriert ist. Führen Sie die folgenden Befehle aus, um die Hardware-Unterstützung zu konfigurieren.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Jumbo Frame MTU Broadcast-Domäne in ONTAP erstellen

Um eine Data Broadcast-Domäne mit einer MTU von 9000 zu erstellen, führen Sie die folgenden Befehle aus:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Entfernen Sie Daten-Ports aus der Standard-Broadcast-Domäne

Die 10-GbE-Daten-Ports werden für iSCSI/NFS-Datenverkehr verwendet, diese Ports sollten aus der Standarddomäne entfernt werden. Die Ports e0e und e0f werden nicht verwendet und sollten auch aus der Standarddomäne entfernt werden.

Führen Sie den folgenden Befehl aus, um die Ports aus der Broadcast-Domäne zu entfernen:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Deaktivieren Sie die Flusssteuerung bei UTA2-Ports

Eine NetApp Best Practice ist es, die Flusskontrolle bei allen UTA2-Ports, die mit externen Geräten verbunden sind, zu deaktivieren. Um die Flusssteuerung zu deaktivieren, führen Sie die folgenden Befehle aus:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

Die direkte Verbindung zum ONTAP UCS Mini unterstützt LACP nicht.

Konfigurieren Sie Jumbo Frames in NetApp ONTAP

Um einen ONTAP-Netzwerkport zur Verwendung von Jumbo Frames zu konfigurieren (die in der Regel über eine MTU von 9,000 Byte verfügen), führen Sie die folgenden Befehle aus der Cluster-Shell aus:

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

Erstellen von VLANs in ONTAP

Gehen Sie wie folgt vor, um VLANs in ONTAP zu erstellen:

1. Erstellen von NFS-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. Erstellen von iSCSI-VLAN-Ports und Hinzufügen dieser zu der Data Broadcast-Domäne

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. ERSTELLUNG VON MGMT-VLAN-Ports

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

Erstellen von Aggregaten in ONTAP

Während der ONTAP-Einrichtung wird ein Aggregat mit dem Root-Volume erstellt. Zum Erstellen weiterer Aggregate ermitteln Sie den Namen des Aggregats, den Node, auf dem er erstellt werden soll, und die Anzahl der enthaltenen Festplatten.

Führen Sie zum Erstellen von Aggregaten die folgenden Befehle aus:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Bewahren Sie mindestens eine Festplatte (wählen Sie die größte Festplatte) in der Konfiguration als Ersatzlaufwerk auf. Als Best Practice empfiehlt es sich, mindestens ein Ersatzteil für jeden Festplattentyp und jede Größe zu besitzen.

Beginnen Sie mit fünf Festplatten. Wenn zusätzlicher Storage erforderlich ist, können Sie einem Aggregat Festplatten hinzufügen.

Das Aggregat kann erst erstellt werden, wenn die Daten auf der Festplatte auf Null gesetzt werden. Führen Sie die aus `aggr show` Befehl zum Anzeigen des Erstellungsstatus des Aggregats. Fahren Sie erst fort `aggr1_nodeA` Ist online.

Konfigurieren Sie die Zeitzone in ONTAP

Führen Sie den folgenden Befehl aus, um die Zeitsynchronisierung zu konfigurieren und die Zeitzone auf dem Cluster festzulegen:

```
timezone <<var_timezone>>
```

Beispielsweise ist die Zeitzone im Osten der USA `America/New_York`. Nachdem Sie mit der Eingabe des Zeitzonennamens begonnen haben, drücken Sie die Tabulatortaste, um die verfügbaren Optionen anzuzeigen.

Konfigurieren Sie SNMP in ONTAP

Führen Sie die folgenden Schritte aus, um die SNMP zu konfigurieren:

1. Konfigurieren Sie SNMP-Basisinformationen, z. B. Standort und Kontakt. Wenn Sie abgefragt werden, werden diese Informationen als angezeigt `sysLocation` Und `sysContact` Variablen in SNMP.

```
snmp contact <<var_snmp_contact>>
snmp location "<<var_snmp_location>>"
snmp init 1
options snmp.enable on
```

2. Konfigurieren Sie SNMP-Traps zum Senden an Remote-Hosts.

```
snmp traphost add <<var_snmp_server_fqdn>>
```

Konfigurieren Sie SNMPv1 in ONTAP

Um SNMPv1 zu konfigurieren, stellen Sie das freigegebene geheime Klartextkennwort ein, das als Community bezeichnet wird.

```
snmp community add ro <<var_snmp_community>>
```

Verwenden Sie die `snmp community delete all` Befehl mit Vorsicht. Wenn Community Strings für andere Überwachungsprodukte verwendet werden, entfernt dieser Befehl sie.

Konfigurieren Sie SNMPv3 in ONTAP

SNMPv3 erfordert, dass Sie einen Benutzer für die Authentifizierung definieren und konfigurieren. Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren:

1. Führen Sie die aus `security snmpusers` Befehl zum Anzeigen der Engine-ID.
2. Erstellen Sie einen Benutzer mit dem Namen `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Geben Sie die Engine-ID der autorisierenden Einheit ein, und wählen Sie aus `md5` Als Authentifizierungsprotokoll.
4. Geben Sie bei der Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Authentifizierungsprotokoll ein.
5. Wählen Sie `des` Als Datenschutzprotokoll.
6. Geben Sie bei Aufforderung ein Kennwort mit einer Mindestlänge von acht Zeichen für das Datenschutzprotokoll ein.

Konfigurieren Sie AutoSupport HTTPS in ONTAP

Das NetApp AutoSupport Tool sendet Zusammenfassung von Support-Informationen über HTTPS an NetApp. Führen Sie den folgenden Befehl aus, um AutoSupport zu konfigurieren:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Erstellen Sie eine Speicher-Virtual Machine

Um eine Storage Virtual Machine (SVM) für Infrastrukturen zu erstellen, gehen Sie wie folgt vor:

1. Führen Sie die aus `vserver create` Befehl.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. Das Datenaggregat wird zur Liste des Infrastruktur-SVM-Aggregats der NetApp VSC hinzugefügt.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Entfernen Sie die ungenutzten Storage-Protokolle der SVM, wobei NFS und iSCSI überlassen bleiben.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Aktivierung und Ausführung des NFS-Protokolls in der SVM Infrastructure

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Schalten Sie das ein `SVM vstorage` Parameter für das NetApp NFS VAAI Plug-in. Überprüfen Sie dann, ob NFS konfiguriert wurde.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Diese Befehle werden von ausgeführt `vserver` Die Befehlszeile war, da SVMs zuvor Server genannt wurden

Konfigurieren Sie NFSv3 in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
ESXi hostet Eine NFS-IP-Adresse	\<<var_esxi_hostA_nfs_ip>
ESXi Host B NFS-IP-Adresse	\<<var_esxi_hostB_nfs_ip>

Führen Sie die folgenden Befehle aus, um NFS auf der SVM zu konfigurieren:

1. Erstellen Sie eine Regel für jeden ESXi-Host in der Standard-Exportrichtlinie.
2. Weisen Sie für jeden erstellten ESXi Host eine Regel zu. Jeder Host hat seinen eigenen Regelindex. Ihr erster ESXi Host hat Regelindex 1, Ihr zweiter ESXi Host hat Regelindex 2 usw.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
–protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Weisen Sie die Exportrichtlinie dem Infrastruktur-SVM-Root-Volume zu.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

Die NetApp VSC verarbeitet automatisch die Exportrichtlinien, wenn Sie sie nach der Einrichtung von vSphere installieren möchten. Wenn Sie diese nicht installieren, müssen Sie Regeln für die Exportrichtlinie erstellen, wenn zusätzliche Server der Cisco UCS B-Serie hinzugefügt werden.

Erstellen Sie den iSCSI-Dienst in ONTAP

Gehen Sie wie folgt vor, um den iSCSI-Service zu erstellen:

1. Erstellen Sie den iSCSI-Service für die SVM. Mit diesem Befehl wird auch der iSCSI-Service gestartet und der iSCSI Qualified Name (IQN) für die SVM festgelegt. Überprüfen Sie, ob iSCSI konfiguriert wurde.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Spiegelung zur Lastverteilung von SVM-Root-Volumes in ONTAP erstellen

So erstellen Sie eine Spiegelung zur Lastverteilung des SVM-Root-Volumes in ONTAP:

1. Erstellen Sie ein Volume zur Lastverteilung der SVM Root-Volumes der Infrastruktur auf jedem Node.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DPvolume create –vserver Infra_Vserver
–volume rootvol_m02 –aggregate aggr1_nodeB –size 1GB –type DP
```

2. Erstellen Sie einen Job-Zeitplan, um die Spiegelbeziehungen des Root-Volumes alle 15 Minuten zu aktualisieren.

```
job schedule interval create -name 15min -minutes 15
```

3. Erstellen Sie die Spiegelungsbeziehungen.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Initialisieren Sie die Spiegelbeziehung und überprüfen Sie, ob sie erstellt wurde.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

Konfigurieren Sie HTTPS-Zugriff in ONTAP

Gehen Sie wie folgt vor, um den sicheren Zugriff auf den Storage Controller zu konfigurieren:

1. Erhöhen Sie die Berechtigungsebene, um auf die Zertifikatbefehle zuzugreifen.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. In der Regel ist bereits ein selbstsigniertes Zertifikat vorhanden. Überprüfen Sie das Zertifikat, indem Sie den folgenden Befehl ausführen:

```
security certificate show
```

3. Bei jeder angezeigten SVM sollte der allgemeine Zertifikatname mit dem vollständig qualifizierten DNS-Domänennamen (FQDN) der SVM übereinstimmen. Die vier Standardzertifikate sollten gelöscht und durch selbstsignierte Zertifikate oder Zertifikate einer Zertifizierungsstelle ersetzt werden.

   Das Löschen abgelaufener Zertifikate vor dem Erstellen von Zertifikaten ist eine bewährte Vorgehensweise. Führen Sie die aus `security certificate delete` Befehl zum Löschen abgelaufener Zertifikate. Verwenden Sie im folgenden Befehl DIE REGISTERKARTEN-Vervollständigung, um jedes Standardzertifikat auszuwählen und zu löschen.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. Um selbstsignierte Zertifikate zu generieren und zu installieren, führen Sie die folgenden Befehle als einmalige Befehle aus. Ein Serverzertifikat für die Infrastruktur-SVM und die Cluster-SVM generieren. Verwenden Sie wieder die REGISTERKARTEN-Vervollständigung, um Sie beim Ausfüllen dieser Befehle zu unterstützen.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Um die Werte für die im folgenden Schritt erforderlichen Parameter zu erhalten, führen Sie den aus `security certificate show` Befehl.
6. Aktivieren Sie jedes Zertifikat, das gerade mit erstellt wurde `-server-enabled true` Und `-client-enabled false` Parameter. Verwenden Sie erneut DIE REGISTERKARTEN-Vervollständigung.

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Konfigurieren und aktivieren Sie den SSL- und HTTPS-Zugriff und deaktivieren Sie den HTTP-Zugriff.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

Es ist normal, dass einige dieser Befehle eine Fehlermeldung ausgeben, die angibt, dass der Eintrag nicht vorhanden ist.

8. Kehren Sie zur Berechtigungsstufe für den Administrator zurück, und erstellen Sie das Setup, damit SVM über das Internet verfügbar ist.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Erstellen Sie in ONTAP ein NetApp FlexVol Volume

Um ein NetApp FlexVol® Volume zu erstellen, geben Sie den Namen, die Größe und das Aggregat ein, auf dem es vorhanden ist. Erstellung von zwei VMware Datastore Volumes und einem Server Boot Volume

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Aktivieren Sie die Deduplizierung in ONTAP

Um die Deduplizierung auf entsprechenden Volumes einmal am Tag zu aktivieren, führen Sie folgende Befehle aus:

```
volume efficiency modify –vserver Infra-SVM –volume esxi_boot –schedule
sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_1
–schedule sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_2
–schedule sun-sat@0
```

Erstellen Sie LUNs in ONTAP

Um zwei LUNs (Boot Logical Unit Numbers) zu erstellen, führen Sie die folgenden Befehle aus:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Beim Hinzufügen eines zusätzlichen Cisco UCS C-Series Servers muss eine zusätzliche Boot-LUN erstellt werden.

Erstellen von iSCSI LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Speicherknoten A iSCSI LIF01A	<<var_nodeA_iscsi_lif01a_ip>>
Speicherknoten A iSCSI-LIF01A-Netzwerkmaske	<<var_nodeA_iscsi_lif01a_Mask>>
Speicherknoten A iSCSI LIF01B	<<var_nodeA_iscsi_lif01b_ip>>
Speicherknoten Eine iSCSI-LIF01B-Netzwerkmaske	<<var_nodeA_iscsi_lif01b_Mask>>
Storage-Node B iSCSI LIF01A	<<var_nodeB_iscsi_lif01a_ip>>
Speicherknoten B iSCSI-LIF01A-Netzwerkmaske	<<var_nodeB_iscsi_lif01a_Mask>>
Storage Node B iSCSI LIF01B	<<var_nodeB_iscsi_lif01b_ip>>
Speicherknoten B iSCSI-LIF01B-Netzwerkmaske	<<var_nodeB_iscsi_lif01b_Mask>>

1. Erstellen Sie vier iSCSI LIFs, zwei pro Node.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Erstellen von NFS LIFs in ONTAP

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Storage Node A NFS LIF 01 A IP	<<var_nodeA_nfs_lif_01_a_ip>>
Storage Node A NFS LIF 01 A Netzwerkmaske	<<var_nodeA_nfs_lif_01_a_maska>>
Storage-Node A NFS-LIF 01 b IP	<<var_nodeA_nfs_lif_01_b_ip>>
Storage Node A NFS LIF 01 b Netzwerkmaske	<<var_nodeA_nfs_lif_01_b_maska>>
Storage-Node B NFS-LIF 02 A-IP	<<var_nodeB_nfs_lif_02_A_ip>>
Storage-Node B NFS-LIF 02 A Netzwerkmaske	<<var_nodeB_nfs_lif_02_A_Mask>>
Storage-Node B NFS-LIF 02 b IP	<<var_nodeB_nfs_lif_02_b_ip>>
Storage Node B NFS LIF 02 b Netzwerkmaske	<<var_nodeB_nfs_lif_02_b_maska>>

1. Erstellen Sie ein NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

Hinzufügen eines SVM-Administrators für die Infrastruktur

In der folgenden Tabelle sind die Informationen aufgeführt, die zum Abschließen dieser Konfiguration erforderlich sind.

Details	Detailwert
Vsmgmt-IP	<<var_svm_mgmt_ip>>
Vsmgmt-Netzwerkmaske	<<var_svm_mgmt_maska>>
Vsmgmt Standard-Gateway	<<var_svm_mgmt_Gateway>>

So fügen Sie dem Managementnetzwerk den SVM-Administrator und die SVM-Administrations-LIF der Infrastruktur hinzu:

1. Führen Sie den folgenden Befehl aus:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
-data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

Die SVM-Management-IP sollte sich hier im selben Subnetz wie die Storage-Cluster-Management-IP befinden.

2. Erstellen Sie eine Standardroute, damit die SVM-Managementoberfläche die Außenwelt erreichen kann.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. Legen Sie ein Passwort für die SVM fest `vsadmin` Benutzer und entsperren Sie den Benutzer.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver
```

Konfiguration des Cisco UCS Servers

FlexPod Cisco UCS Base

Ersteinrichtung des Cisco UCS 6324 Fabric Interconnects für FlexPod Umgebungen durchführen

In diesem Abschnitt werden ausführliche Verfahren zur Konfiguration von Cisco UCS für die Verwendung in einer FlexPod ROBO-Umgebung mithilfe von Cisco UCS Manager beschrieben.

Cisco UCS Fabric Interconnect 6324 A

Cisco UCS verwendet Netzwerke und Server auf Zugriffsebene. Dieses hochperformante Serversystem der nächsten Generation bietet ein Datacenter mit einem hohen Grad an Workload-Flexibilität und Skalierbarkeit.

Cisco UCS Manager 4.0(1b) unterstützt das 6324 Fabric Interconnect, das Fabric Interconnect in das Cisco UCS Gehäuse integriert. Es bietet eine integrierte Lösung für eine kleinere Implementierungsumgebung. Cisco UCS Mini vereinfacht das Systemmanagement und spart Kosten für kostengünstige Implementierungen.

Die Hardware- und Software-Komponenten unterstützen das Unified Fabric von Cisco, das auf mehreren Arten von Datacenter-Datenverkehr über einen einzelnen konvergierten Netzwerkadapter ausgeführt wird.

Ersteinrichtung des Systems

Wenn Sie zum ersten Mal auf einen Fabric Interconnect in einer Cisco UCS Domäne zugreifen, werden Sie von einem Setup-Assistenten aufgefordert, die folgenden Informationen zu erhalten, die für die Konfiguration des Systems erforderlich sind:

- Installationsmethode (GUI oder CLI)
- Setup-Modus (Wiederherstellung aus vollständigem System-Backup oder Ersteinrichtung)
- Systemkonfigurationstyp (Standalone- oder Cluster-Konfiguration)
- Systemname
- Admin-Passwort

- Management-Port-IPv4-Adresse und Subnetzmaske oder IPv6-Adresse und -Präfix
- Standard-Gateway-IPv4- oder IPv6-Adresse
- DNS-Server IPv4- oder IPv6-Adresse
- Standard-Domain-Name

In der folgenden Tabelle sind die Informationen aufgeführt, die erforderlich sind, um die Erstkonfiguration von Cisco UCS auf Fabric Interconnect A abzuschließen

Details	**Detail/Wert**
Systemname	<<var_ucs_clustername>>
Administratorpasswort	<<var_password>>
Management-IP-Adresse: Fabric Interconnect A	<<var_ucsa_Mgmt_ip>>
Management-Netmask: Fabric Interconnect A	<<var_ucsa_mgmt_maska>>
Standard-Gateway: Fabric Interconnect A	<<var_ucsa_mgmt_Gateway>>
Cluster-IP-Adresse	<<var_ucs_Cluster_ip>>
IP-Adresse des DNS-Servers	<<var_Nameserver_ip>>
Domain-Name	<<var_Domain_Name>>

Gehen Sie folgendermaßen vor, um Cisco UCS für die Verwendung in einer FlexPod-Umgebung zu konfigurieren:

1. Stellen Sie eine Verbindung zum Konsolen-Port des ersten Cisco UCS 6324 Fabric Interconnect A her

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Überprüfen Sie die auf der Konsole angezeigten Einstellungen. Wenn sie richtig sind, antworten `yes` Zum Anwenden und Speichern der Konfiguration.
3. Warten Sie, bis die Anmelde-Eingabeaufforderung angezeigt wird, um zu überprüfen, ob die Konfiguration gespeichert wurde.

In der folgenden Tabelle sind die Informationen aufgeführt, die erforderlich sind, um die Erstkonfiguration von Cisco UCS auf Fabric Interconnect B abzuschließen

Details	**Detail/Wert**
Systemname	<<var_ucs_clustername>>
Administratorpasswort	<<var_password>>
Management-IP-Adresse-FI B	<<var_ucsd_Mgmt_ip>>
Management-Netmask-FI B	<<var_ucsd_Mgmt_Maske>>
Standard-Gateway-FI B	\<<var_ucsd_Mgmt_Gateway>
Cluster-IP-Adresse	<<var_ucs_Cluster_ip>>
DNS-Server-IP-Adresse	<<var_Nameserver_ip>>
Domain-Name	<<var_Domain_Name>>

1. Stellen Sie eine Verbindung zum Konsolen-Port auf dem zweiten Cisco UCS 6324 Fabric Interconnect B her

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Warten Sie, bis die Anmelde-Eingabeaufforderung angezeigt wird, um zu bestätigen, dass die Konfiguration gespeichert wurde.

Melden Sie sich bei Cisco UCS Manager an

So melden Sie sich in der Cisco Unified Computing System (UCS)-Umgebung an:

1. Öffnen Sie einen Webbrowser, und navigieren Sie zur Cisco UCS Fabric Interconnect Cluster-Adresse.

   Möglicherweise müssen Sie mindestens 5 Minuten warten, nachdem Sie den zweiten Fabric Interconnect für den Einsatz von Cisco UCS Manager konfiguriert haben.

2. Klicken Sie auf den Link UCS Manager starten, um Cisco UCS Manager zu starten.
3. Akzeptieren Sie die erforderlichen Sicherheitszertifikate.
4. Geben Sie bei der entsprechenden Aufforderung den Benutzernamen admin ein und geben Sie das Administratorpasswort ein.
5. Klicken Sie auf Anmelden, um sich bei Cisco UCS Manager anzumelden.

Cisco UCS Manager, Softwareversion 4.0(1b)

In diesem Dokument wird vorausgesetzt, dass die Software von Cisco UCS Manager, Version 4.0(1b), verwendet wird. Für ein Upgrade der Cisco UCS Manager Software und der Cisco UCS 6324 Fabric

Interconnect Software finden Sie unter "Cisco UCS Manager – Installations- und Upgrade-Leitfäden"

Konfigurieren Sie Cisco UCS Call Home

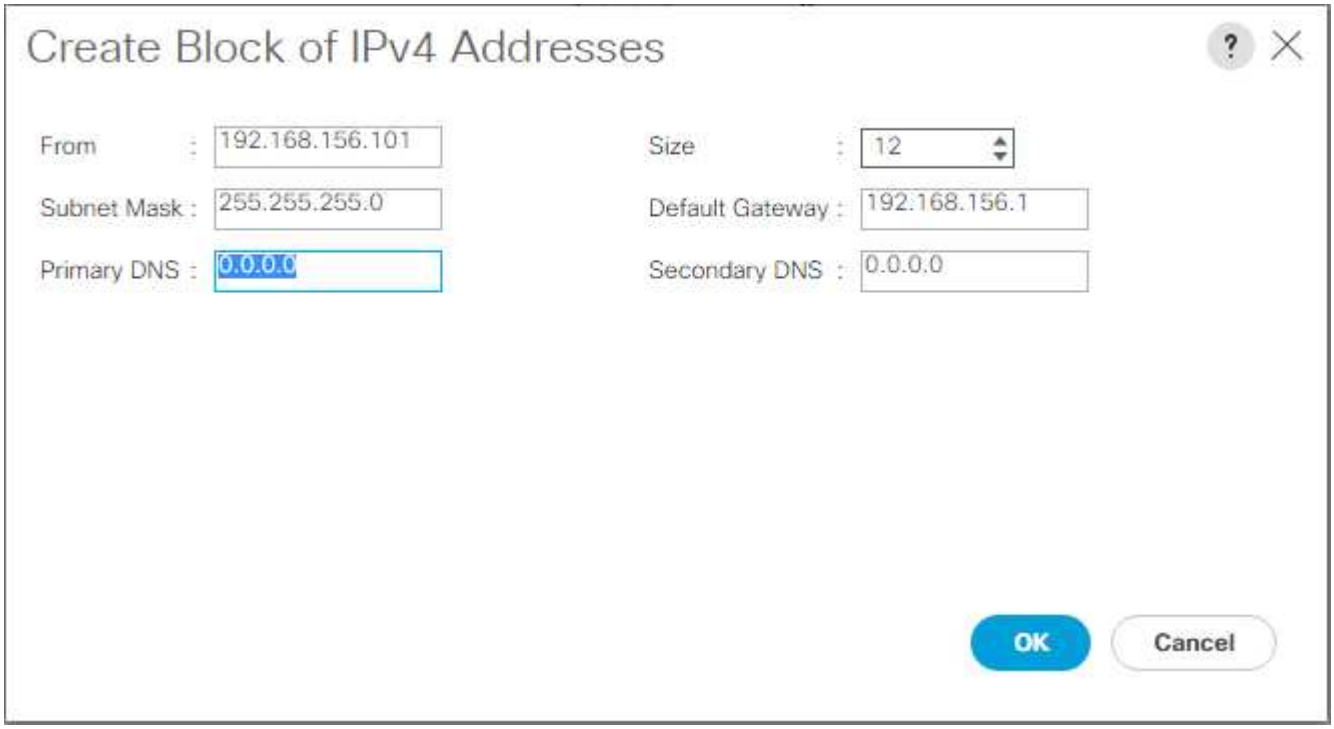
Cisco empfiehlt ausdrücklich die Konfiguration von „Call Home“ in Cisco UCS Manager. Die Konfiguration von „Call Home“ beschleunigt die Lösung von Support-Fällen. Gehen Sie wie folgt vor, um Call Home zu konfigurieren:

1. Klicken Sie in Cisco UCS Manager links auf Admin.
2. Wählen Sie Alle > Kommunikationsverwaltung > Call Home.
3. Ändern Sie den Status in ein.
4. Füllen Sie alle Felder gemäß Ihren Verwaltungseinstellungen aus, und klicken Sie auf Änderungen speichern und auf OK, um die Konfiguration der Call Home abzuschließen.

Fügen Sie einen Block von IP-Adressen für Tastatur, Video und Mauszugriff hinzu

Um einen Block von IP-Adressen für Tastatur-, Video-, Maus- (KVM)-Zugriff in der Cisco UCS-Umgebung zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Erweitern Sie Pools > Root > IP-Pools.
3. Klicken Sie mit der rechten Maustaste auf IP-Pool-ext-Management, und wählen Sie Block von IPv4-Adressen erstellen.
4. Geben Sie die Start-IP-Adresse des Blocks, die Anzahl der erforderlichen IP-Adressen sowie die Subnetzmaske und Gateway-Informationen ein.



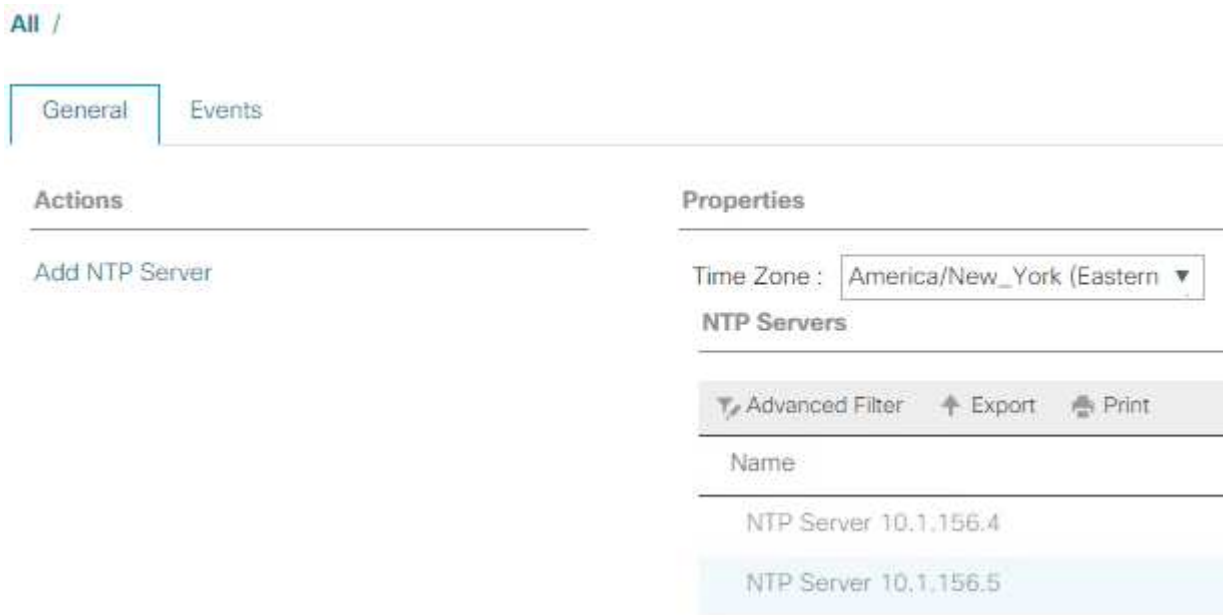
5. Klicken Sie auf OK, um den Block zu erstellen.
6. Klicken Sie in der Bestätigungsmeldung auf OK.

Synchronisieren Sie Cisco UCS mit NTP

So synchronisieren Sie die Cisco UCS-Umgebung mit den NTP-Servern auf den Nexus-Switches:

1. Klicken Sie in Cisco UCS Manager links auf Admin.
2. Erweitern Sie Alles > Zeitzonenmanagement.
3. Wählen Sie Zeitzone.
4. Wählen Sie im Fensterbereich Eigenschaften die entsprechende Zeitzone im Menü Zeitzone aus.
5. Klicken Sie auf Änderungen speichern und dann auf OK.
6. Klicken Sie auf NTP-Server hinzufügen.
7. Eingabe `<switch-a-ntp-ip> or <Nexus-A-mgmt-IP>` Klicken Sie anschließend auf OK. Klicken Sie auf OK.

8. Klicken Sie auf NTP-Server hinzufügen.
9. Eingabe `<switch-b-ntp-ip> or <Nexus-B-mgmt-IP>` Klicken Sie anschließend auf OK. Klicken Sie auf OK auf die Bestätigung.



Bearbeiten der Richtlinie für die Gehäuseermittlung

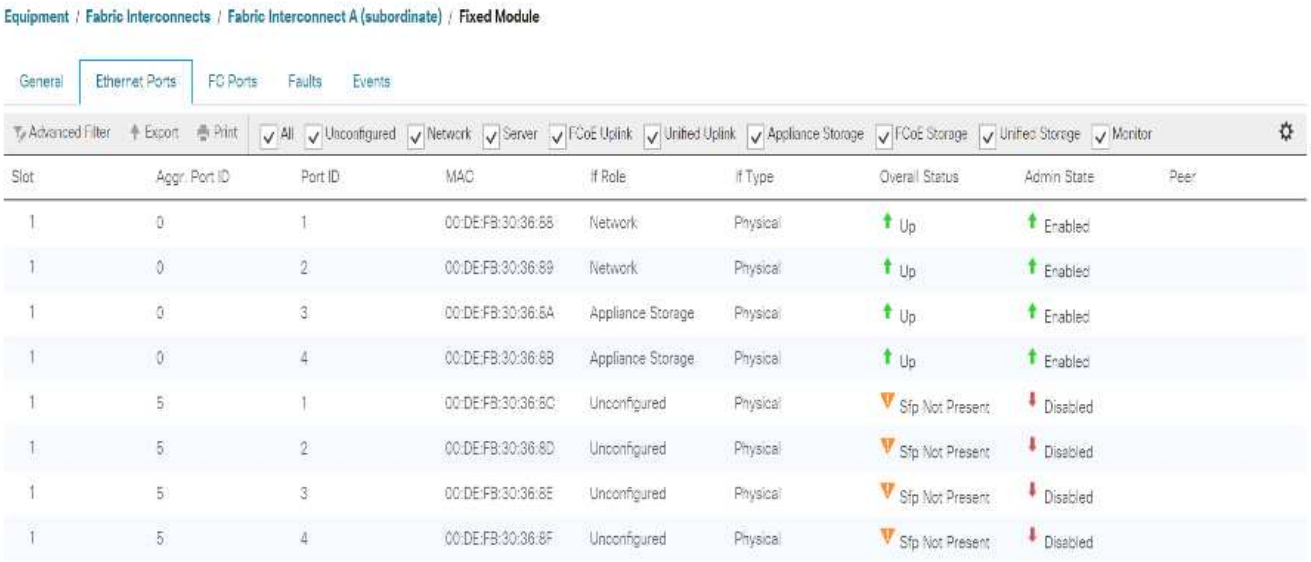
Durch die Festlegung der Erkennungsrichtlinie wird das Hinzufügen eines Cisco UCS B-Series Gehäuses und von zusätzlichen Fabric Extendern für weitere Cisco UCS C-Serie-Konnektivität vereinfacht. Gehen Sie wie folgt vor, um die Richtlinie zur Chassis-Erkennung zu ändern:

1. Klicken Sie im Cisco UCS Manager links auf Equipment, und wählen Sie in der zweiten Liste die Option Equipment aus.
2. Wählen Sie im rechten Fensterbereich die Registerkarte Richtlinien aus.
3. Legen Sie unter globalen Richtlinien die Chassis/FEX Discovery-Richtlinie so fest, dass sie der Mindestanzahl von Uplink-Ports entspricht, die zwischen dem Chassis oder Fabric Extendern (Fexes) und den Fabric Interconnects verkabelt sind.
4. Legen Sie die Einstellung „Gruppierung verknüpfen“ auf Port Channel fest. Wenn die zu errichtende Umgebung eine große Menge an Multicast-Datenverkehr enthält, setzen Sie die Einstellung Multicast Hardware-Hash auf aktiviert.
5. Klicken Sie Auf Änderungen Speichern.
6. Klicken Sie auf OK.

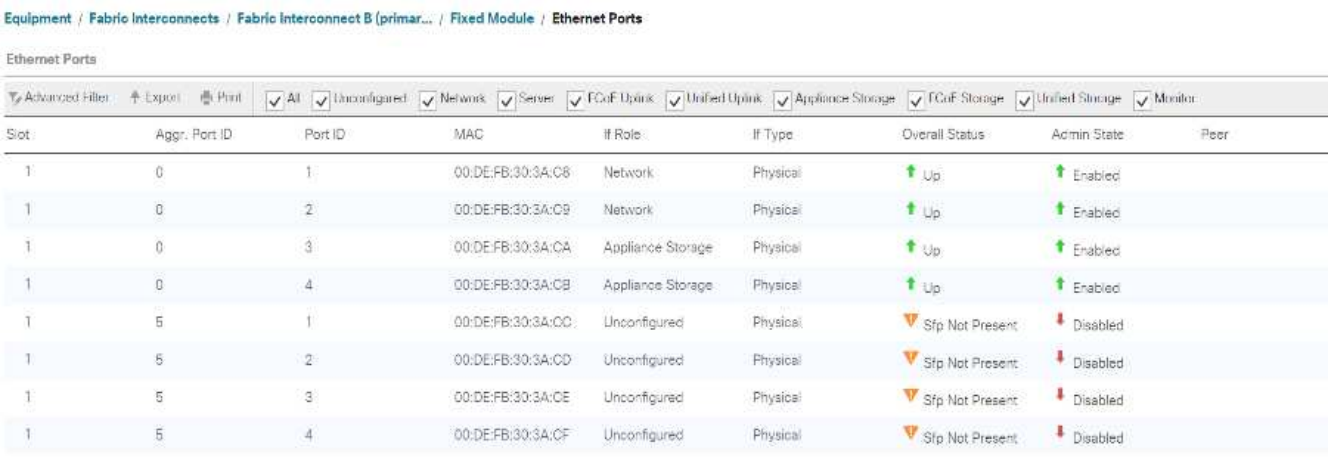
Unterstützung von Server-, Uplink- und Storage-Ports

Führen Sie die folgenden Schritte aus, um Server- und Uplink-Ports zu aktivieren:

1. Wählen Sie im Cisco UCS Manager im Navigationsbereich die Registerkarte Geräte aus.
2. Erweitern Sie Geräte > Fabric Interconnects > Fabric Interconnect A > Feste Module.
3. Erweitern Sie Ethernet-Ports.
4. Wählen Sie die Ports 1 und 2 aus, die mit den Cisco Nexus 31108-Switches verbunden sind, klicken Sie mit der rechten Maustaste, und wählen Sie als Uplink-Port konfigurieren aus.
5. Klicken Sie auf Ja, um die Uplink-Ports zu bestätigen, und klicken Sie auf OK.
6. Wählen Sie die Ports 3 und 4 aus, die mit den NetApp Storage Controllern verbunden sind, klicken Sie mit der rechten Maustaste, und wählen Sie als Appliance-Port konfigurieren aus.
7. Klicken Sie auf Ja, um die Geräteanschlüsse zu bestätigen.
8. Klicken Sie im Fenster als Appliance-Port konfigurieren auf OK.
9. Klicken Sie zur Bestätigung auf OK.
10. Wählen Sie im linken Fensterbereich unter Fabric Interconnect A die Option Fixed Module aus
11. Vergewissern Sie sich auf der Registerkarte Ethernet-Ports, dass die Ports in der Spalte „Wenn-Rolle“ richtig konfiguriert wurden. Wenn auf dem Skalierbarkeitsport Server der C-Serie konfiguriert wurden, klicken Sie darauf, um die Anschlussverbindung dort zu überprüfen.



12. Erweitern Sie die Ausrüstung > Fabric Interconnects > Fabric Interconnect B > Festes Modul.
13. Erweitern Sie Ethernet-Ports.
14. Wählen Sie Ethernet-Ports 1 und 2 aus, die mit den Cisco Nexus 31108-Switches verbunden sind, klicken Sie mit der rechten Maustaste, und wählen Sie als Uplink-Port konfigurieren.
15. Klicken Sie auf Ja, um die Uplink-Ports zu bestätigen, und klicken Sie auf OK.
16. Wählen Sie die Ports 3 und 4 aus, die mit den NetApp Storage Controllern verbunden sind, klicken Sie mit der rechten Maustaste, und wählen Sie als Appliance-Port konfigurieren aus.
17. Klicken Sie auf Ja, um die Geräteanschlüsse zu bestätigen.
18. Klicken Sie im Fenster als Appliance-Port konfigurieren auf OK.
19. Klicken Sie zur Bestätigung auf OK.
20. Wählen Sie im linken Fensterbereich unter Fabric Interconnect B die Option Fixed Module aus
21. Vergewissern Sie sich auf der Registerkarte Ethernet-Ports, dass die Ports in der Spalte „Wenn-Rolle“ richtig konfiguriert wurden. Wenn auf dem Skalierbarkeitsport Server der C-Serie konfiguriert wurden, klicken Sie darauf, um die Anschlussverbindung dort zu überprüfen.



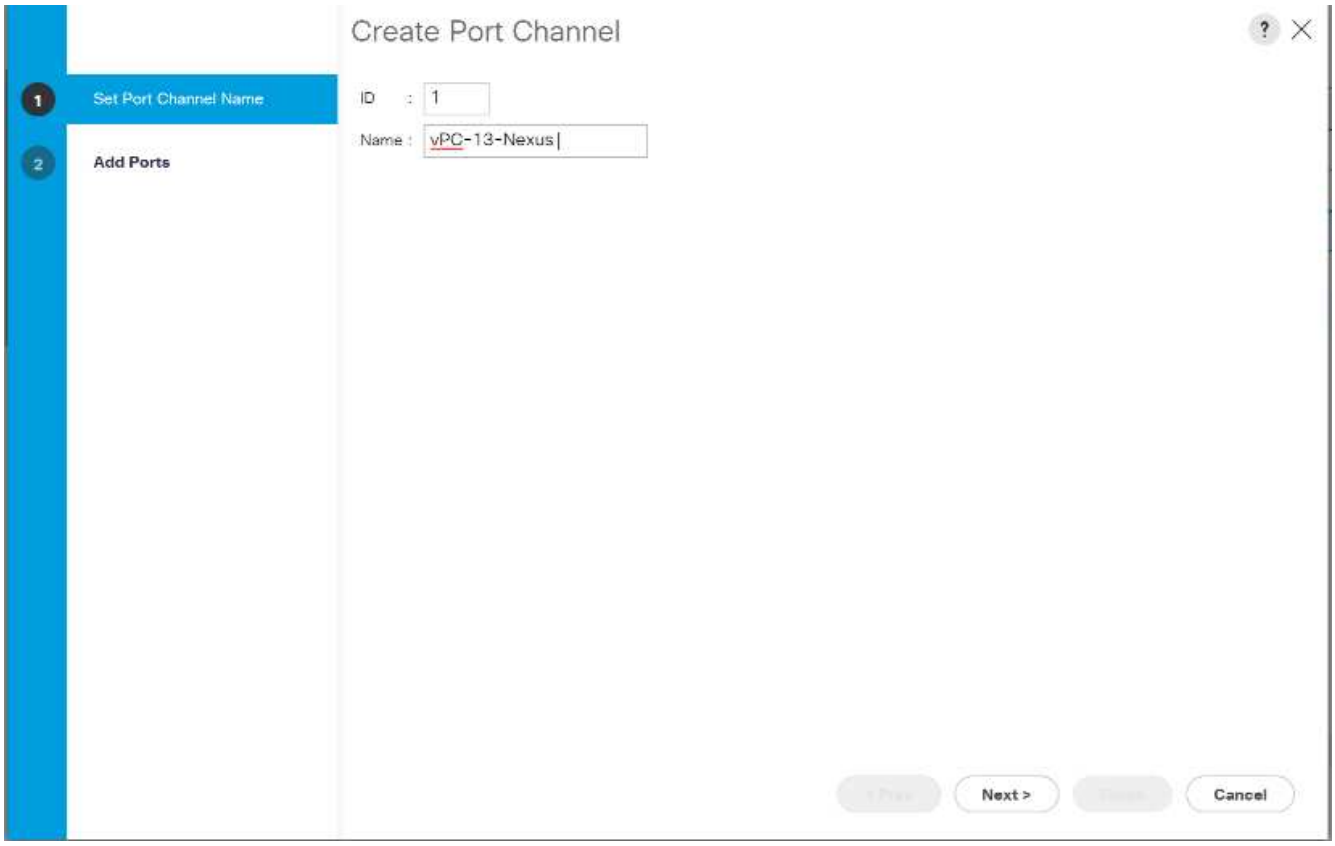
Erstellen von Uplink-Port-Kanälen zu Cisco Nexus 31108 Switches

Gehen Sie wie folgt vor, um die erforderlichen Port-Channels in der Cisco UCS-Umgebung zu konfigurieren:

1. Wählen Sie im Cisco UCS Manager im Navigationsbereich die Registerkarte LAN aus.

> In diesem Verfahren werden zwei Port-Kanäle erstellt: Einer von Fabric A zu Cisco Nexus 31108 Switches und einer von Fabric B zu beiden Cisco Nexus 31108 Switches. Wenn Sie Standardschalter verwenden, ändern Sie dieses Verfahren entsprechend. Wenn Sie 1-Gigabit-Ethernet-Switches (1 GbE) und GLC-T-SFPs auf den Fabric Interconnects verwenden, müssen die Schnittstellengeschwindigkeiten der Ethernet-Ports 1/1 und 1/2 in den Fabric Interconnects auf 1 Gbit/s festgelegt sein.

2. Erweitern Sie unter LAN > LAN Cloud die Struktur Fabric A.
3. Klicken Sie mit der rechten Maustaste auf Port Channels.
4. Wählen Sie Port Channel Erstellen.
5. Geben Sie 13 als eindeutige ID des Port-Kanals ein.
6. Geben Sie den Namen des Port-Kanals vPC-13-Nexus ein.
7. Klicken Sie Auf Weiter.



8. Wählen Sie die folgenden Ports aus, die dem Port-Kanal hinzugefügt werden sollen:
   a. Steckplatz-ID 1 und Port 1
   b. Steckplatz-ID 1 und Port 2
9. Klicken Sie auf >>, um die Ports dem Port-Kanal hinzuzufügen.
10. Klicken Sie auf Fertig stellen, um den Port-Kanal zu erstellen. Klicken Sie auf OK.

11. Wählen Sie unter Port Channels den neu erstellten Port-Kanal aus.

    Der Port-Kanal sollte einen Gesamtstatus von up aufweisen.

12. Erweitern Sie im Navigationsbereich unter LAN > LAN Cloud die Struktur B.
13. Klicken Sie mit der rechten Maustaste auf Port Channels.
14. Wählen Sie Port Channel Erstellen.
15. Geben Sie 14 als eindeutige ID des Port-Kanals ein.
16. Geben Sie den Namen des Port-Kanals vPC-14-Nexus ein. Klicken Sie Auf Weiter.
17. Wählen Sie die folgenden Ports aus, die dem Port-Kanal hinzugefügt werden sollen:
    a. Steckplatz-ID 1 und Port 1
    b. Steckplatz-ID 1 und Port 2
18. Klicken Sie auf >>, um die Ports dem Port-Kanal hinzuzufügen.
19. Klicken Sie auf Fertig stellen, um den Port-Kanal zu erstellen. Klicken Sie auf OK.
20. Wählen Sie unter Port Channels den neu erstellten Port-Channel aus.
21. Der Port-Kanal sollte einen Gesamtstatus von up aufweisen.

Erstellen einer Organisation (optional)

Unternehmen organisieren Ressourcen und beschränken den Zugriff auf verschiedene Gruppen innerhalb DER IT-Abteilung, wodurch Mandantenfähigkeit der Computing-Ressourcen ermöglicht wird.

> Obwohl dieses Dokument nicht die Verwendung von Organisationen übernimmt, enthält dieses Verfahren Anweisungen zum Erstellen eines solchen Dokuments.

Gehen Sie wie folgt vor, um ein Unternehmen in der Cisco UCS-Umgebung zu konfigurieren:

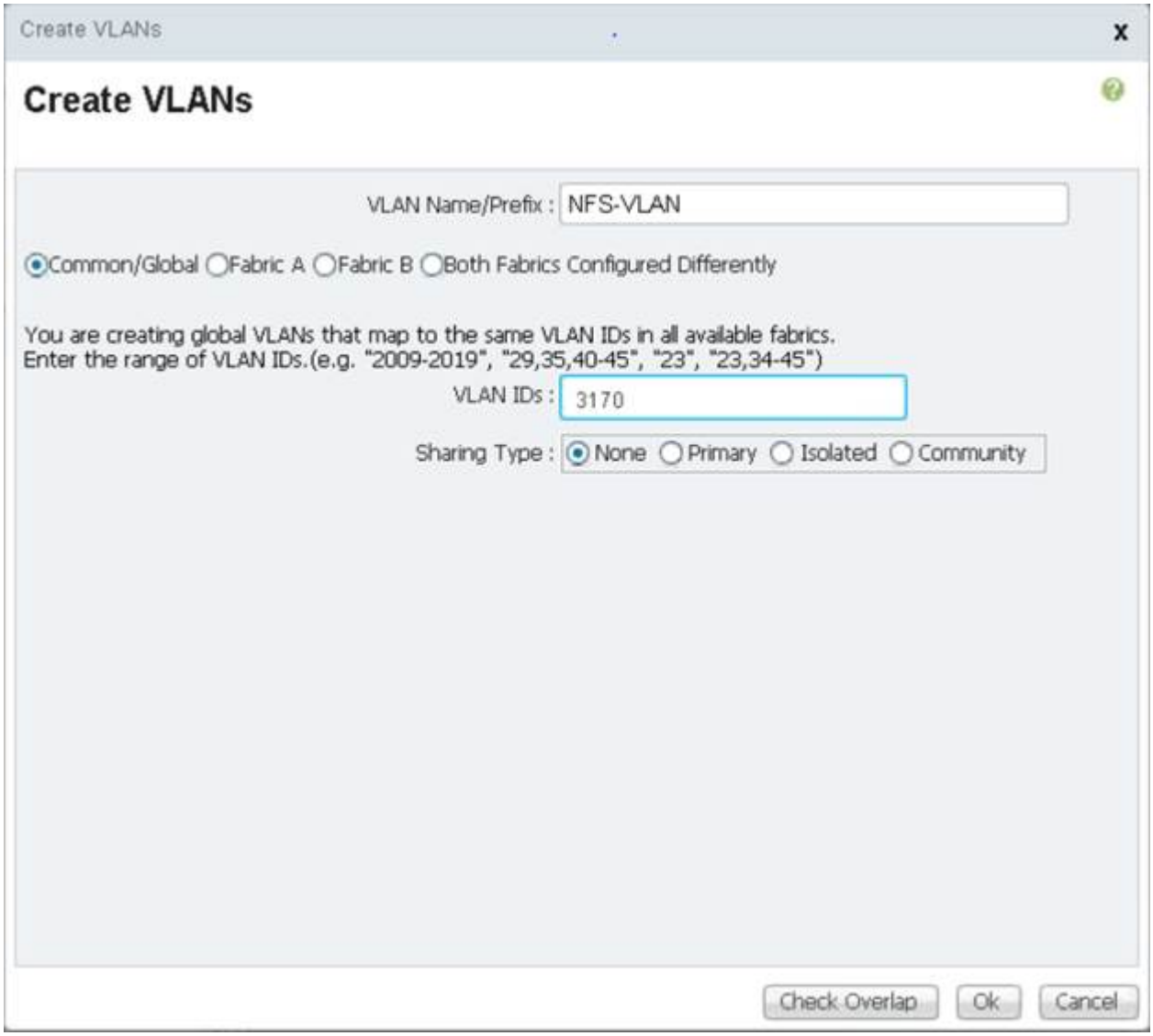
1. Wählen Sie im Cisco UCS Manager im Menü Neu in der Symbolleiste oben im Fenster die Option Organisation erstellen aus.
2. Geben Sie einen Namen für die Organisation ein.
3. Optional: Geben Sie eine Beschreibung für die Organisation ein. Klicken Sie auf OK.
4. Klicken Sie in der Bestätigungsmeldung auf OK.

Konfigurieren von Storage-Appliance-Ports und Storage-VLANs

Gehen Sie wie folgt vor, um die Ports der Speichergeräte und Speicher-VLANs zu konfigurieren:

1. Wählen Sie im Cisco UCS Manager die Registerkarte LAN aus.
2. Erweitern Sie die Cloud der Appliances.
3. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
4. Wählen Sie VLANs erstellen aus.
5. Geben Sie NFS-VLAN als Name für das NFS-VLAN für die Infrastruktur ein.
6. Lassen Sie „Allgemein/global“ ausgewählt.
7. Eingabe `<<var_nfs_vlan_id>>` Für die VLAN-ID.

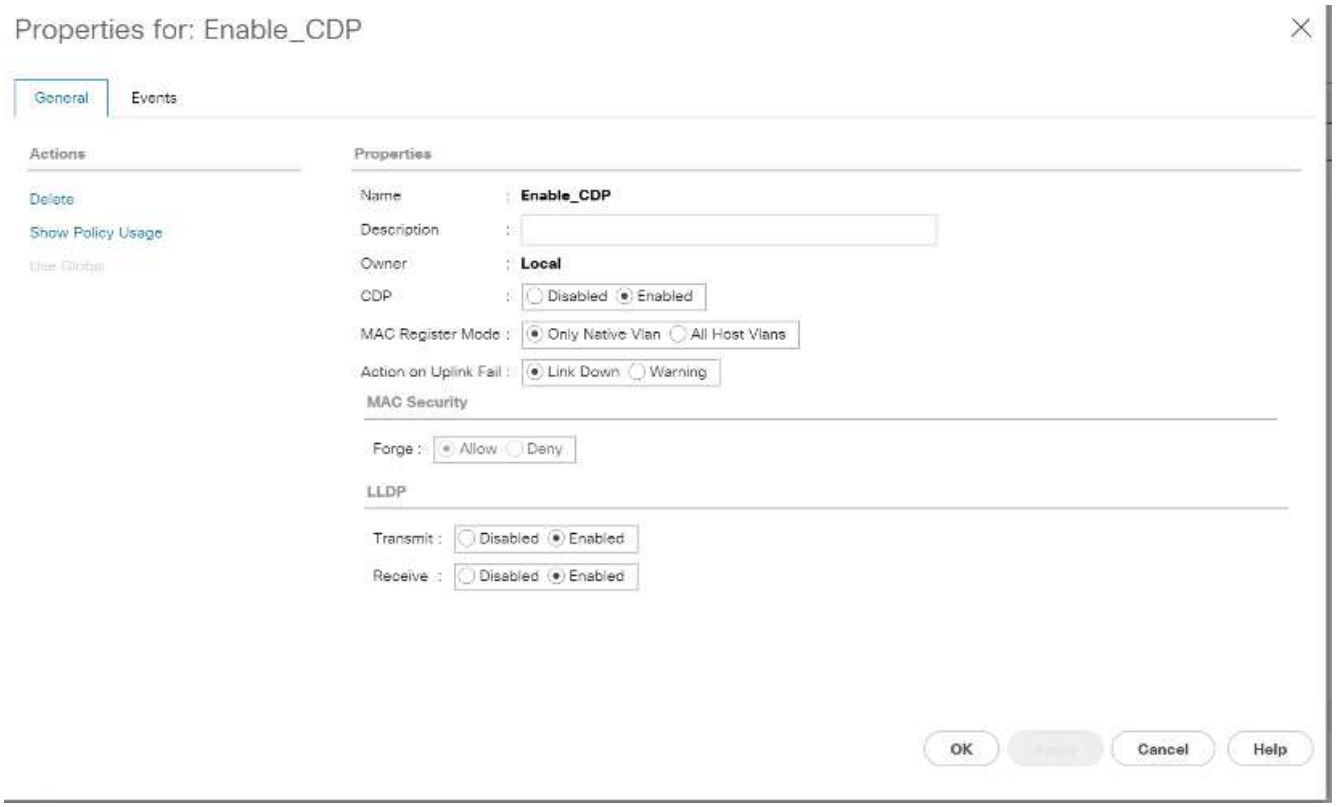
8. Den Freigabetyp auf Keine setzen lassen.



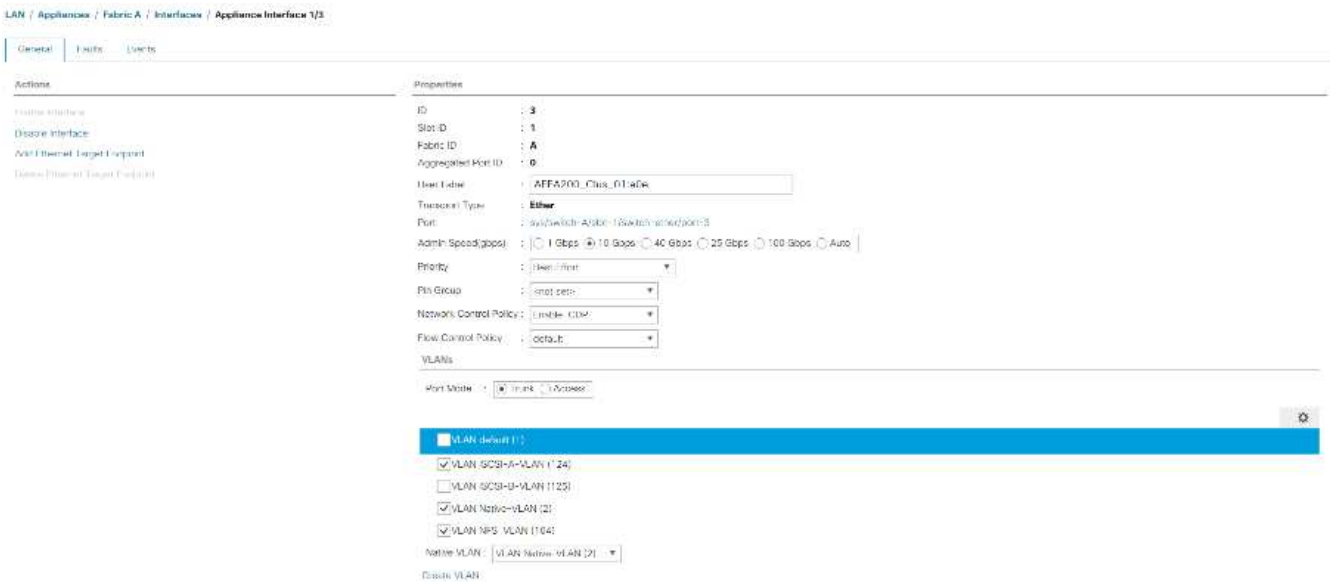
9. Klicken Sie auf OK, und klicken Sie erneut auf OK, um das VLAN zu erstellen.
10. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
11. Wählen Sie VLANs erstellen aus.
12. Geben Sie das iSCSI-A-VLAN als Namen für die iSCSI-Fabric-Infrastruktur Ein VLAN ein.
13. Lassen Sie „Allgemein/global“ ausgewählt.
14. Eingabe `<<var_iscsi-a_vlan_id>>` Für die VLAN-ID.
15. Klicken Sie auf OK, und klicken Sie erneut auf OK, um das VLAN zu erstellen.
16. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
17. Wählen Sie VLANs erstellen aus.
18. Geben Sie das iSCSI-B-VLAN als Namen für das iSCSI-Fabric-B-VLAN der Infrastruktur ein.
19. Lassen Sie „Allgemein/global“ ausgewählt.
20. Eingabe `<<var_iscsi-b_vlan_id>>` Für die VLAN-ID.
21. Klicken Sie auf OK, und klicken Sie erneut auf OK, um das VLAN zu erstellen.

22. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
23. Wählen Sie VLANs erstellen aus.
24. Geben Sie Native-VLAN als Namen für das Native VLAN ein.
25. Lassen Sie „Allgemein/global“ ausgewählt.
26. Eingabe `<<var_native_vlan_id>>` Für die VLAN-ID.
27. Klicken Sie auf OK, und klicken Sie erneut auf OK, um das VLAN zu erstellen.

28. Erweitern Sie im Navigationsbereich unter LAN > Richtlinien Appliances und klicken Sie mit der rechten Maustaste auf Network Control Policies.
29. Wählen Sie Netzwerksteuerungsrichtlinie Erstellen.
30. Richtlinie benennen `Enable_CDP_LLPD` Und wählen Sie neben CDP aktiviert aus.
31. Aktivieren Sie die Funktionen zum Senden und Empfangen von LLDP.

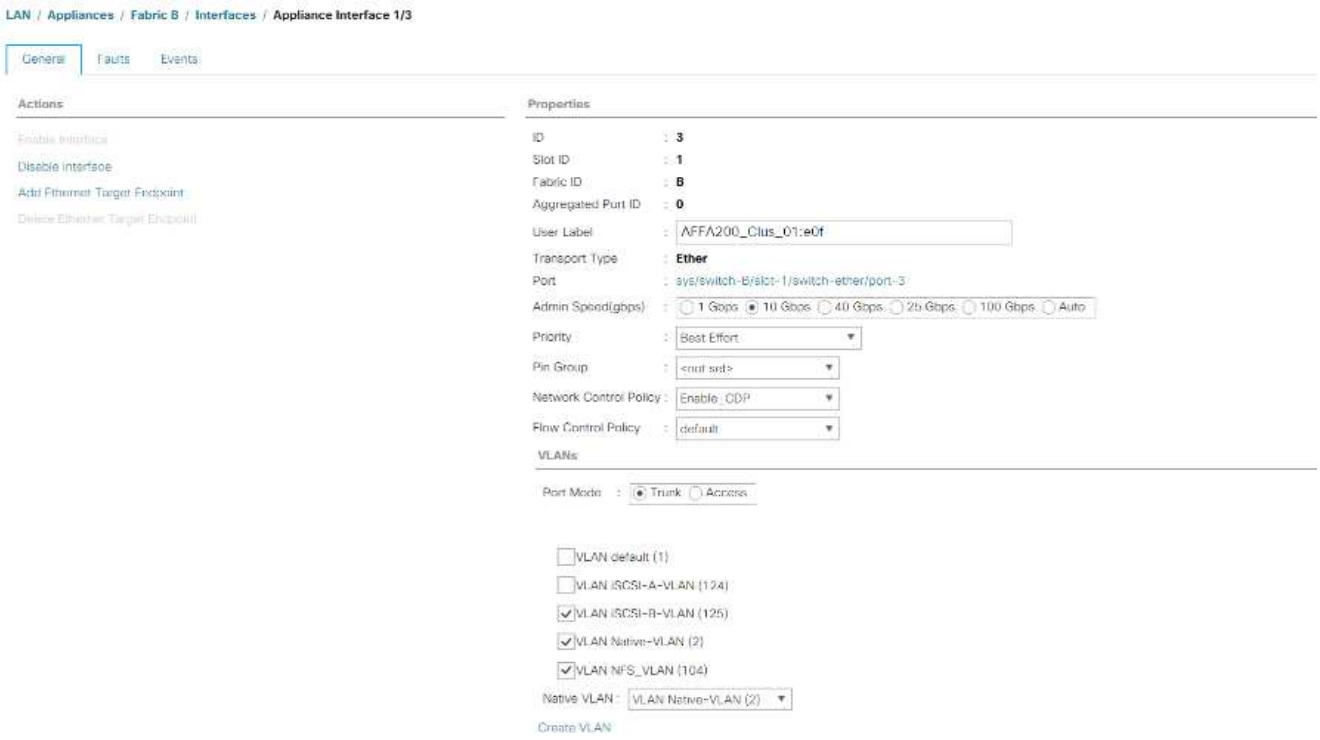


32. Klicken Sie auf OK und anschließend erneut auf OK, um die Richtlinie zu erstellen.
33. Erweitern Sie im Navigationsbereich unter LAN > Appliances Cloud die Struktur Fabric A.
34. Erweitern Sie Schnittstellen.
35. Wählen Sie Die Appliance-Schnittstelle 1/3.
36. Geben Sie im Feld „Benutzerbeschriftung“ Informationen ein, die den Port des Speichercontrollers angeben, z. B. `<storage_controller_01_name>:e0e`. Klicken Sie auf Änderungen speichern und OK.
37. Wählen Sie Enable_CDP Network Control Policy und Save Changes and OK.
38. Wählen Sie unter VLANs iSCSI-A-VLAN, NFS-VLAN und natives VLAN aus. Legen Sie das native VLAN als natives VLAN fest. Deaktivieren Sie die Standard-VLAN-Auswahl.
39. Klicken Sie auf Änderungen speichern und OK.



40. Wählen Sie unter Fabric A Appliance Interface 1/4 aus
41. Geben Sie im Feld „Benutzerbeschriftung“ Informationen ein, die den Port des Speichercontrollers angeben, z. B. `<storage_controller_02_name>:e0e`. Klicken Sie auf Änderungen speichern und OK.
42. Wählen Sie Enable_CDP Network Control Policy und Save Changes and OK.
43. Wählen Sie unter VLANs iSCSI-A-VLAN, NFS-VLAN und natives VLAN aus.
44. Legen Sie das native VLAN als natives VLAN fest.
45. Deaktivieren Sie die Standard-VLAN-Auswahl.
46. Klicken Sie auf Änderungen speichern und OK.
47. Erweitern Sie im Navigationsbereich unter LAN > Appliances Cloud den Strukturbaum B.
48. Erweitern Sie Schnittstellen.
49. Wählen Sie Die Appliance-Schnittstelle 1/3.
50. Geben Sie im Feld „Benutzerbeschriftung“ Informationen ein, die den Port des Speichercontrollers angeben, z. B. `<storage_controller_01_name>:e0f`. Klicken Sie auf Änderungen speichern und OK.
51. Wählen Sie Enable_CDP Network Control Policy und Save Changes and OK.
52. Wählen Sie unter VLANs das iSCSI-B-VLAN, NFS-VLAN und natives VLAN aus. Legen Sie das native

VLAN als natives VLAN fest. Heben Sie die Auswahl des Standard-VLAN auf.

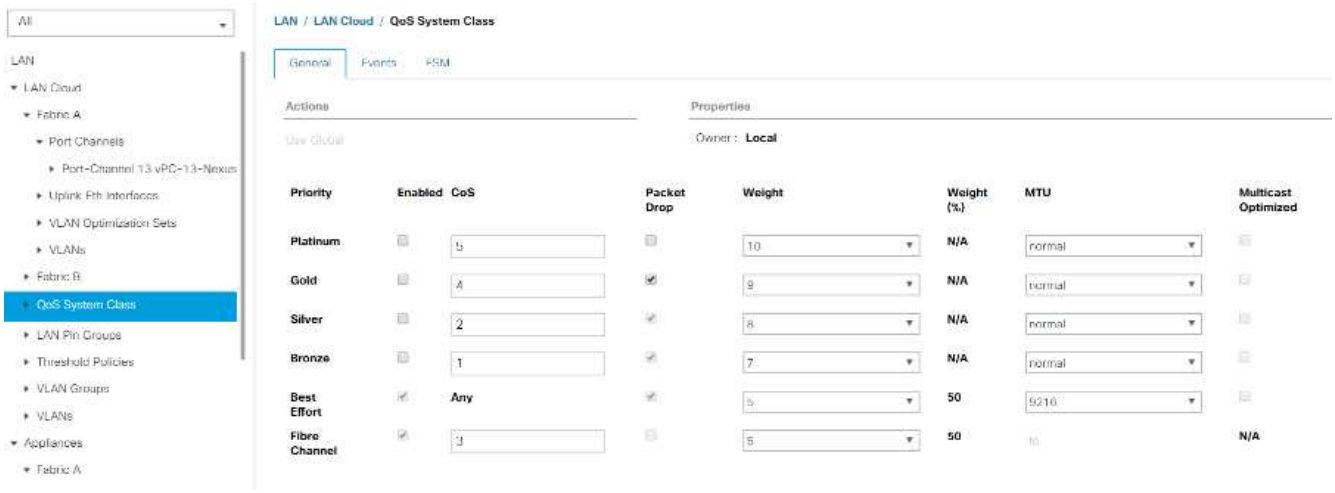


53. Klicken Sie auf Änderungen speichern und OK.
54. Wählen Sie unter Fabric B Appliance Interface 1/4 aus
55. Geben Sie im Feld „Benutzerbeschriftung“ Informationen ein, die den Port des Speichercontrollers angeben, z. B. `<storage_controller_02_name>:e0f`. Klicken Sie auf Änderungen speichern und OK.
56. Wählen Sie Enable_CDP Network Control Policy und Save Changes and OK.
57. Wählen Sie unter VLANs das iSCSI-B-VLAN, NFS-VLAN und natives VLAN aus. Legen Sie das native VLAN als natives VLAN fest. Heben Sie die Auswahl des Standard-VLAN auf.
58. Klicken Sie auf Änderungen speichern und OK.

Jumbo Frames in der Cisco UCS Fabric festlegen

Gehen Sie wie folgt vor, um Jumbo Frames zu konfigurieren und Servicequalität in der Cisco UCS Fabric zu ermöglichen:

1. Klicken Sie in Cisco UCS Manager im Navigationsbereich auf die Registerkarte LAN.
2. Wählen Sie LAN > LAN Cloud > QoS System Class.
3. Klicken Sie im rechten Fensterbereich auf die Registerkarte Allgemein.
4. Geben Sie in der Zeile „Beste Anstrengung“ in das Feld unter der MTU-Spalte 9216 ein.



5. Klicken Sie Auf Änderungen Speichern.
6. Klicken Sie auf OK.

Cisco UCS-Chassis anerkennen

Gehen Sie wie folgt vor, um alle Cisco UCS-Gehäuse zu bestätigen:

1. Wählen Sie im Cisco UCS Manager die Registerkarte „Equipment“ aus und erweitern Sie anschließend rechts die Registerkarte „Equipment“.
2. Erweitern Sie Geräte > Gehäuse.
3. Wählen Sie in den Aktionen für Gehäuse 1 die Option Gehäuse bestätigen aus.
4. Klicken Sie auf OK und anschließend auf OK, um das Gehäuse zu bestätigen.
5. Klicken Sie auf Schließen, um das Fenster Eigenschaften zu schließen.

Laden der Firmware-Images des Cisco UCS 4.0(1b)

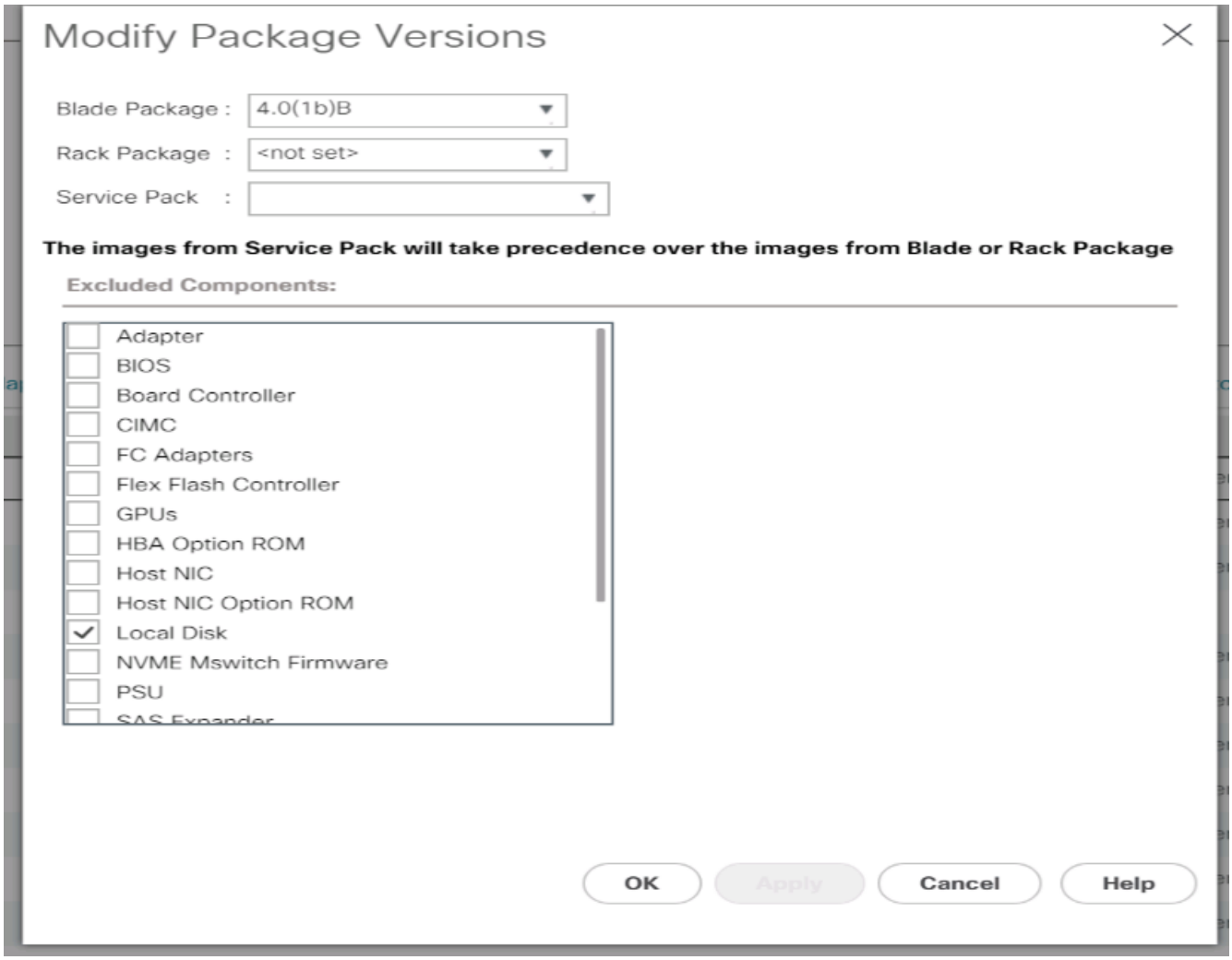
Informationen zum Upgrade der Cisco UCS Manager Software und der Cisco UCS Fabric Interconnect Software auf Version 4.0(1b) finden Sie unter "Cisco UCS Manager – Installations- und Upgrade-Leitfäden".

Erstellen des Host-Firmware-Pakets

Mithilfe der Firmware-Management-Richtlinien kann der Administrator die entsprechenden Pakete für eine bestimmte Serverkonfiguration auswählen. Diese Richtlinien umfassen oft Pakete für Adapter-, BIOS-, Board-Controller, FC-Adapter, HBA-Option-ROM (Host Bus Adapter) und Storage Controller-Eigenschaften.

Gehen Sie wie folgt vor, um eine Firmware-Management-Richtlinie für eine bestimmte Server-Konfiguration in der Cisco UCS-Umgebung zu erstellen:

1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Erweitern Sie Die Host-Firmware-Pakete.
4. Wählen Sie Standard.
5. Wählen Sie im Bereich Aktionen die Option Paketversionen ändern aus.
6. Wählen Sie die Version 4.0(1b) für beide Blade-Pakete aus.



7. Klicken Sie erneut auf OK und anschließend auf OK, um das Host-Firmware-Paket zu ändern.

Erstellen Sie MAC-Adressenpools

Um die erforderlichen MAC-Adressenpools für die Cisco UCS-Umgebung zu konfigurieren, führen Sie die folgenden Schritte aus:

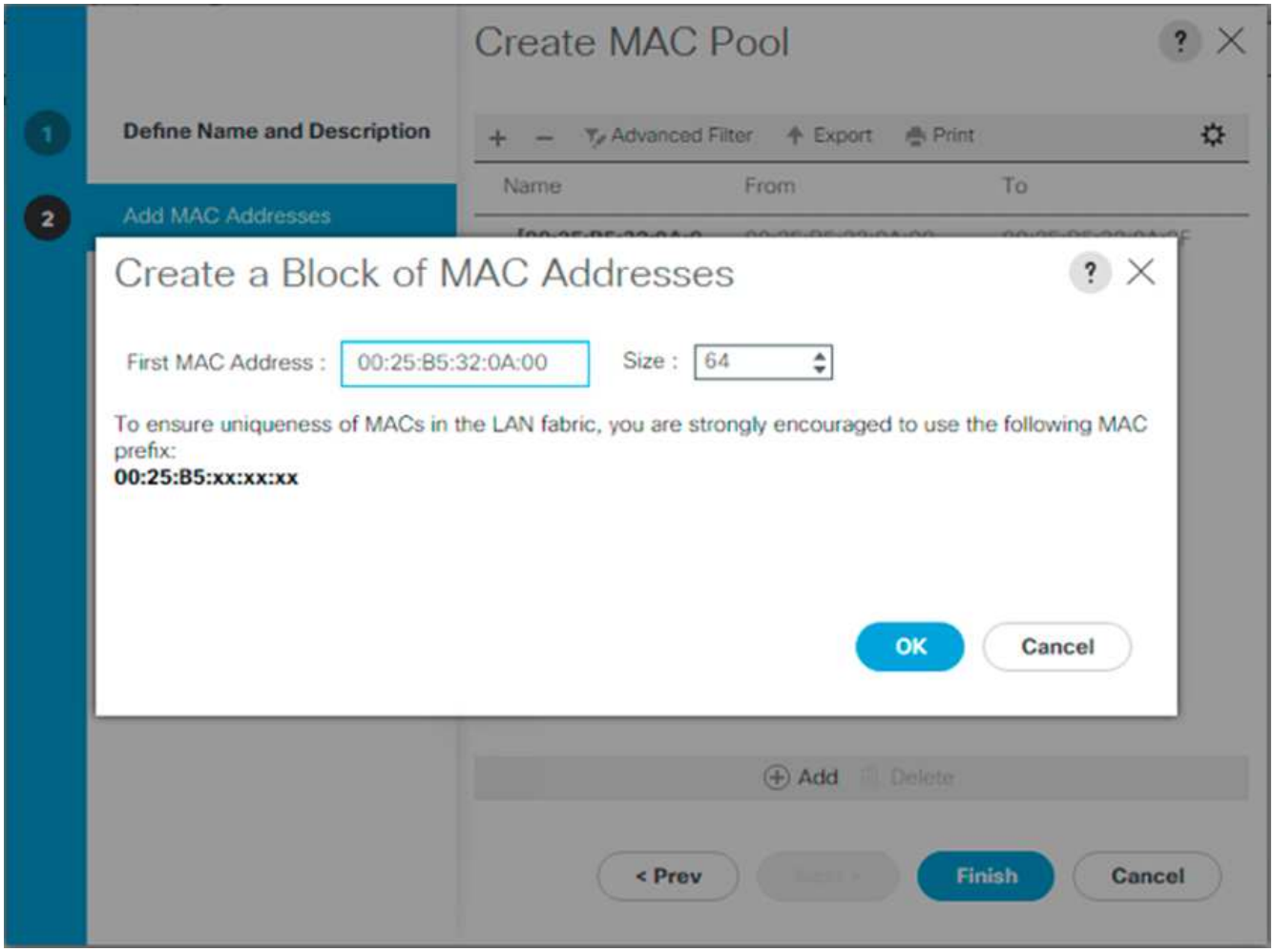
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Pools > Root aus.

   Bei diesem Verfahren werden zwei MAC-Adressenpools erstellt, einer für jede Switching-Fabric.

3. Klicken Sie mit der rechten Maustaste auf MAC-Pools unter der Stammorganisation.
4. Wählen Sie MAC-Pool erstellen, um den MAC-Adressenpool zu erstellen.
5. Geben Sie MAC-Pool-A als Namen des MAC-Pools ein.
6. Optional: Geben Sie eine Beschreibung für den MAC-Pool ein.
7. Wählen Sie sequenziell als Option für Zuweisungsreihenfolge aus. Klicken Sie Auf Weiter.
8. Klicken Sie Auf Hinzufügen.
9. Geben Sie eine Start-MAC-Adresse an.

Für die FlexPod-Lösung empfiehlt es sich, 0A in das nächste Oktett der Startadresse MAC-Adresse einzulegen, um alle MAC-Adressen als Fabric A-Adressen zu identifizieren. In unserem Beispiel haben wir das Beispiel der Einbindung der Cisco UCS-Domänennummer-Informationen, die uns 00:25:B5:32:0A:00 als unsere erste MAC-Adresse geben, weitergeführt.

10. Geben Sie eine Größe für den MAC-Adressenpool an, die ausreichend ist, um die verfügbaren Blade- oder Serverressourcen zu unterstützen. Klicken Sie auf OK.



11. Klicken Sie Auf Fertig Stellen.
12. Klicken Sie in der Bestätigungsmeldung auf OK.
13. Klicken Sie mit der rechten Maustaste auf MAC-Pools unter der Stammorganisation.
14. Wählen Sie MAC-Pool erstellen, um den MAC-Adressenpool zu erstellen.
15. Geben Sie MAC-Pool-B als Namen des MAC-Pools ein.
16. Optional: Geben Sie eine Beschreibung für den MAC-Pool ein.
17. Wählen Sie sequenziell als Option für Zuweisungsreihenfolge aus. Klicken Sie Auf Weiter.
18. Klicken Sie Auf Hinzufügen.
19. Geben Sie eine Start-MAC-Adresse an.

Für die FlexPod Lösung wird empfohlen, 0B neben dem letzten Oktett der StartMAC-Adresse einzulegen, um alle MAC-Adressen in diesem Pool als Fabric B-Adressen zu identifizieren. Auch hier haben wir in unserem Beispiel die Informationen zur Cisco UCS-Domain, die uns 00:25:B5:32:0B:00 als unsere erste MAC-Adresse geben, weitergeführt.

20. Geben Sie eine Größe für den MAC-Adressenpool an, die ausreichend ist, um die verfügbaren Blade- oder Serverressourcen zu unterstützen. Klicken Sie auf OK.
21. Klicken Sie Auf Fertig Stellen.
22. Klicken Sie in der Bestätigungsmeldung auf OK.

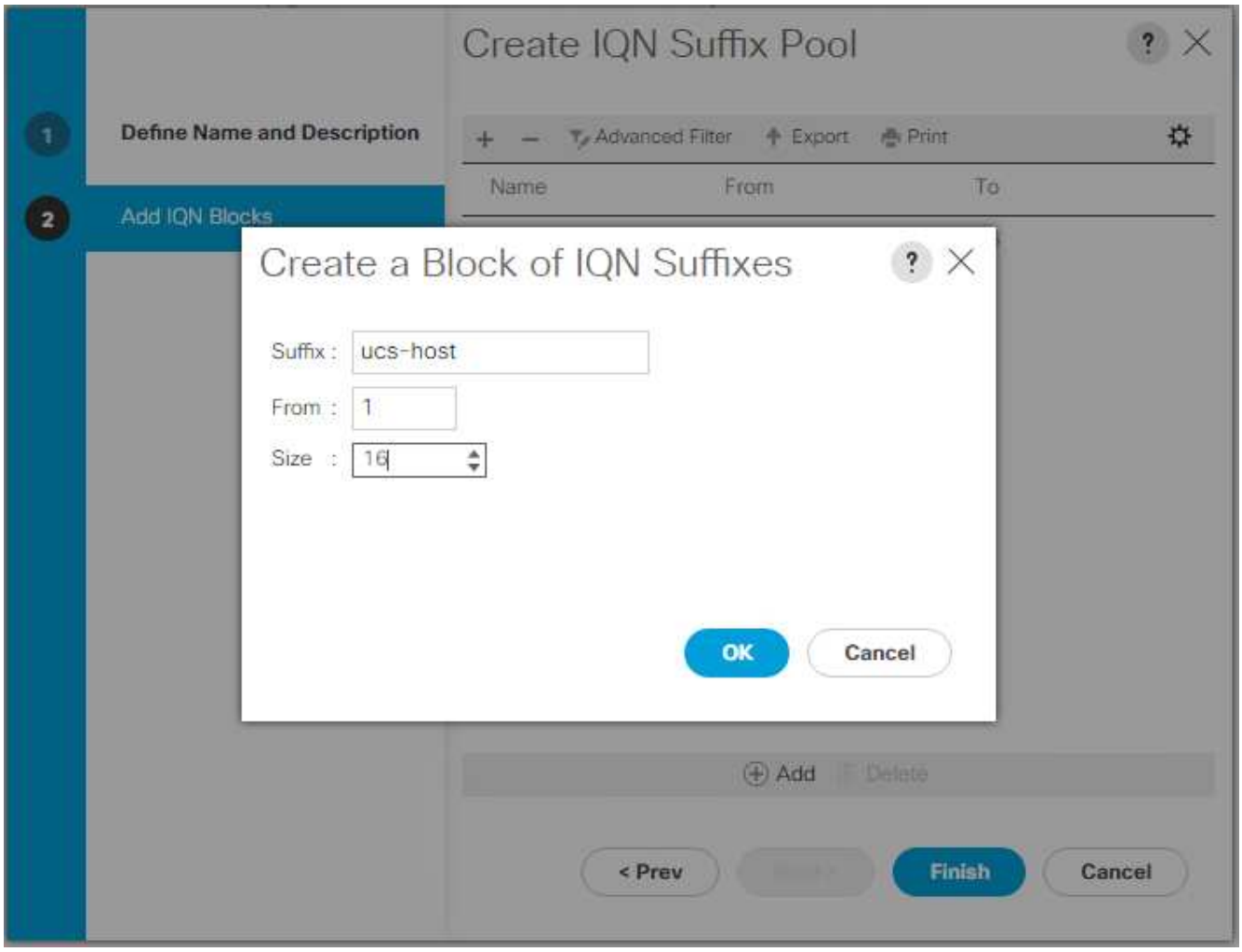
ISCSI-IQN-Pool erstellen

Führen Sie die folgenden Schritte aus, um die erforderlichen IQN-Pools für die Cisco UCS-Umgebung zu konfigurieren:

1. Klicken Sie im Cisco UCS Manager links auf SAN.
2. Wählen Sie Pools > Root aus.
3. Klicken Sie mit der rechten Maustaste auf IQN-Pools.
4. Wählen Sie Create IQN Suffix Pool aus, um den IQN-Pool zu erstellen.
5. Geben Sie IQN-Pool für den Namen des IQN-Pools ein.
6. Optional: Geben Sie eine Beschreibung für den IQN-Pool ein.
7. Eingabe `iqn.1992-08.com.cisco` Als Präfix.
8. Wählen Sie sequenziell für Zuweisungsreihenfolge aus. Klicken Sie Auf Weiter.
9. Klicken Sie Auf Hinzufügen.
10. Eingabe `ucs-host` Als das Suffix.

Wenn mehrere Cisco UCS Domänen verwendet werden, muss möglicherweise ein spezifischer IQN-Suffix verwendet werden.

11. Geben Sie 1 in das Feld von ein.
12. Geben Sie die Größe des IQN-Blocks an, der ausreicht, um die verfügbaren Serverressourcen zu unterstützen. Klicken Sie auf OK.



13. Klicken Sie Auf Fertig Stellen.

Erstellen Sie iSCSI-Initiator-IP-Adressenpools

Gehen Sie wie folgt vor, um den erforderlichen IP Pools iSCSI Boot für die Cisco UCS-Umgebung zu konfigurieren:

1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Pools > Root aus.
3. Klicken Sie mit der rechten Maustaste auf IP-Pools.
4. Wählen Sie IP-Pool erstellen.
5. Geben Sie iSCSI-IP-Pool-A als Name des IP-Pools ein.
6. Optional: Geben Sie eine Beschreibung für den IP-Pool ein.
7. Wählen Sie sequenziell für die Zuweisungsreihenfolge aus. Klicken Sie Auf Weiter.
8. Klicken Sie auf Hinzufügen, um einen Block mit IP-Adresse hinzuzufügen.
9. Geben Sie im Feld von den Anfang des Bereichs ein, der als iSCSI-IP-Adressen zugewiesen werden soll.
10. Legen Sie die Größe auf genügend Adressen fest, um die Server aufzunehmen. Klicken Sie auf OK.
11. Klicken Sie Auf Weiter.
12. Klicken Sie Auf Fertig Stellen.

13. Klicken Sie mit der rechten Maustaste auf IP-Pools.
14. Wählen Sie IP-Pool erstellen.
15. Geben Sie iSCSI-IP-Pool-B als Name des IP-Pools ein.
16. Optional: Geben Sie eine Beschreibung für den IP-Pool ein.
17. Wählen Sie sequenziell für die Zuweisungsreihenfolge aus. Klicken Sie Auf Weiter.
18. Klicken Sie auf Hinzufügen, um einen Block mit IP-Adresse hinzuzufügen.
19. Geben Sie im Feld von den Anfang des Bereichs ein, der als iSCSI-IP-Adressen zugewiesen werden soll.
20. Legen Sie die Größe auf genügend Adressen fest, um die Server aufzunehmen. Klicken Sie auf OK.
21. Klicken Sie Auf Weiter.
22. Klicken Sie Auf Fertig Stellen.

Erstellen Sie einen UUID-Suffix-Pool

Gehen Sie wie folgt vor, um den erforderlichen UUID-Suffix-Pool (Universally Unique Identifier) für die Cisco UCS-Umgebung zu konfigurieren:

1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Pools > Root aus.
3. Klicken Sie mit der rechten Maustaste auf UUID Suffix Pools.
4. Wählen Sie Create UUID Suffix Pool.
5. Geben Sie den UUID-Pool als Namen des UUID-Suffix-Pools ein.
6. Optional: Geben Sie eine Beschreibung für den UUID-Suffix-Pool ein.
7. Behalten Sie das Präfix an der abgeleiteten Option.
8. Wählen Sie sequenziell für die Zuweisungsreihenfolge aus.
9. Klicken Sie Auf Weiter.
10. Klicken Sie auf Hinzufügen, um einen Block von UUIDs hinzuzufügen.
11. Behalten Sie das Feld von bei bei der Standardeinstellung.
12. Geben Sie eine Größe für den UUID-Block an, die ausreicht, um die verfügbaren Blade- oder Server-Ressourcen zu unterstützen. Klicken Sie auf OK.
13. Klicken Sie Auf Fertig Stellen.
14. Klicken Sie auf OK.

Erstellen Sie den Server-Pool

So konfigurieren Sie den erforderlichen Server-Pool für die Cisco UCS-Umgebung:

> Es empfiehlt sich die Erstellung einzigartiger Server Pools, um die in der jeweiligen Umgebung erforderliche Granularität zu erreichen.

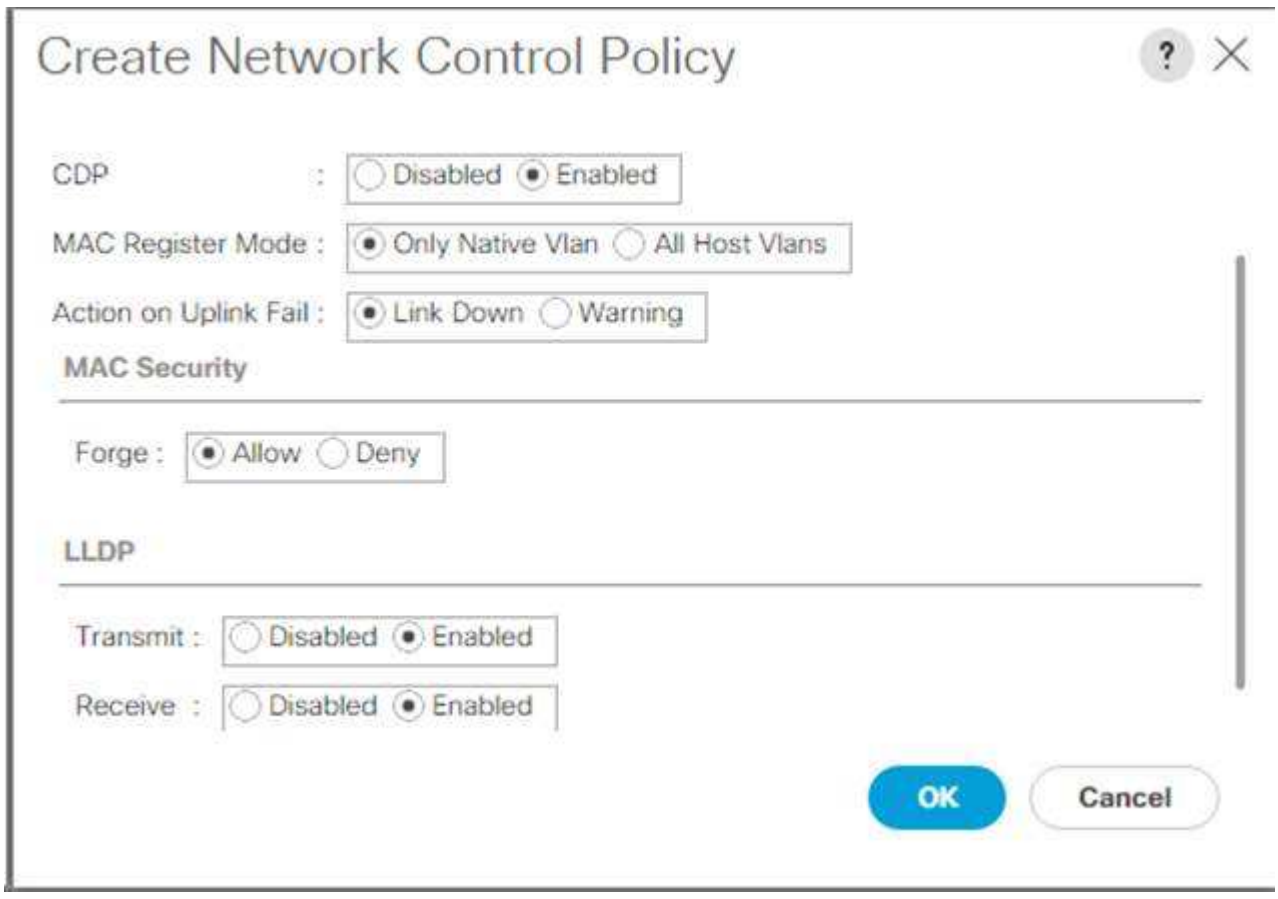
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Pools > Root aus.
3. Klicken Sie mit der rechten Maustaste auf Server Pools.

4. Wählen Sie Serverpool Erstellen.
5. Geben Sie `Infra-Pool `als Namen des Serverpools ein.
6. Optional: Geben Sie eine Beschreibung für den Server-Pool ein. Klicken Sie Auf Weiter.
7. Wählen Sie zwei (oder mehr) Server aus, die für das VMware Management-Cluster verwendet werden sollen, und klicken Sie auf >>, um sie dem `Infra-Pool `sServerpool hinzuzufügen.
8. Klicken Sie Auf Fertig Stellen.
9. Klicken Sie auf OK.

Erstellen Sie die Network Control Policy für das Cisco Discovery Protocol und das Link Layer Discovery Protocol

Gehen Sie wie folgt vor, um eine Netzwerkkontrollrichtlinie für das Cisco Discovery Protocol (CDP) und das Link Layer Discovery Protocol (LLDP) zu erstellen:

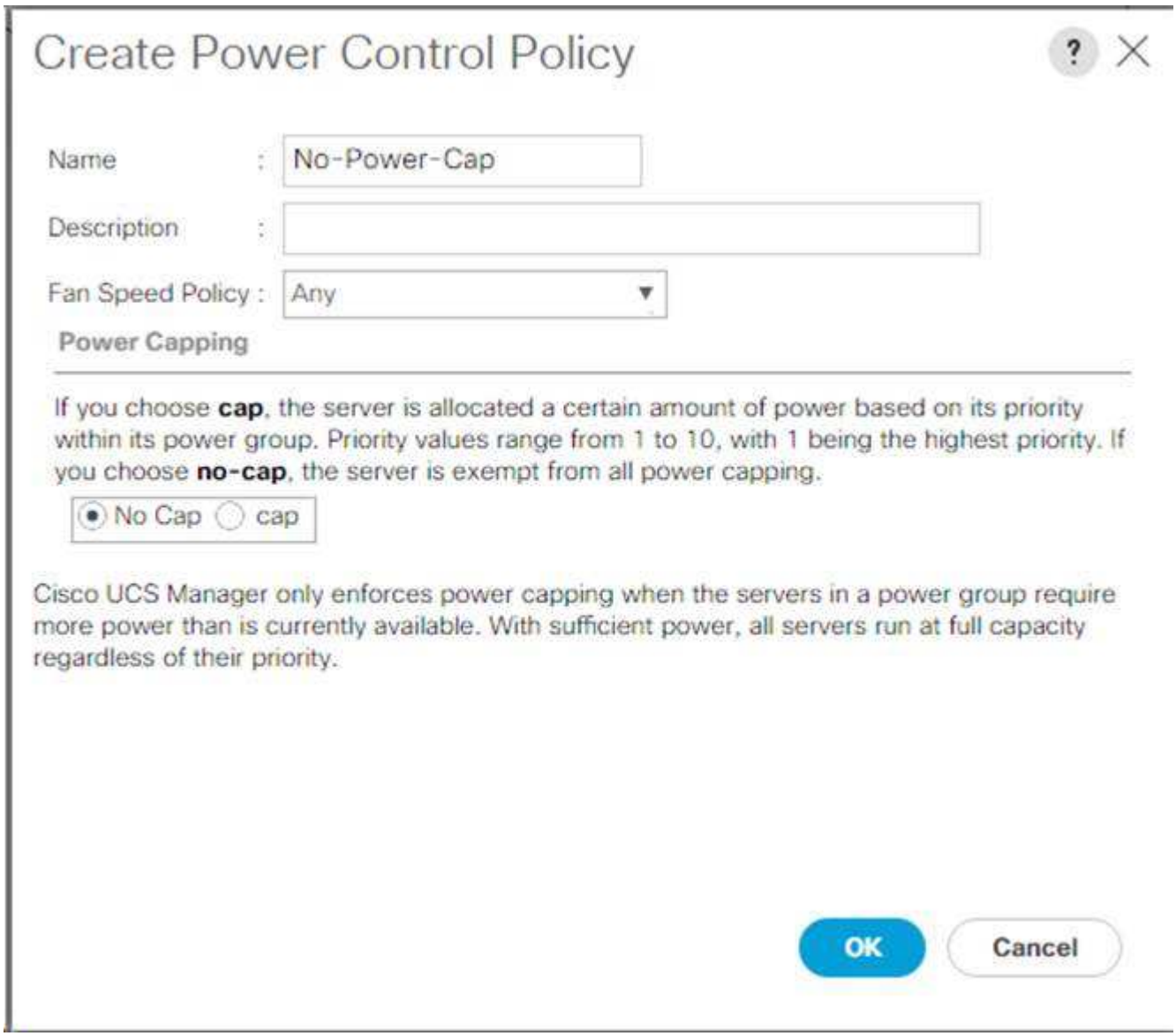
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf Network Control Policies.
4. Wählen Sie Netzwerksteuerungsrichtlinie Erstellen.
5. Geben Sie den Namen der Enable-CDP-LLDP-Richtlinie ein.
6. Wählen Sie bei CDP die Option Enabled aus.
7. Scrollen Sie bei LLDP nach unten und wählen Sie aktiviert für Senden und Empfangen aus.
8. Klicken Sie auf OK, um die Netzwerksteuerungsrichtlinie zu erstellen. Klicken Sie auf OK.



Energiekontrollrichtlinie erstellen

Um eine Energiekontrollrichtlinie für die Cisco UCS-Umgebung zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie in Cisco UCS Manager links auf die Registerkarte Server.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf Energiekontrollrichtlinien.
4. Wählen Sie Energiesteuerungsrichtlinie Erstellen.
5. Geben Sie als Name der Energieregerichtlinie den Namen No-Power-Cap ein.
6. Ändern Sie die Einstellung für die Stromkappung auf „Keine Kap.“.
7. Klicken Sie auf OK, um die Energiekontrollrichtlinie zu erstellen. Klicken Sie auf OK.

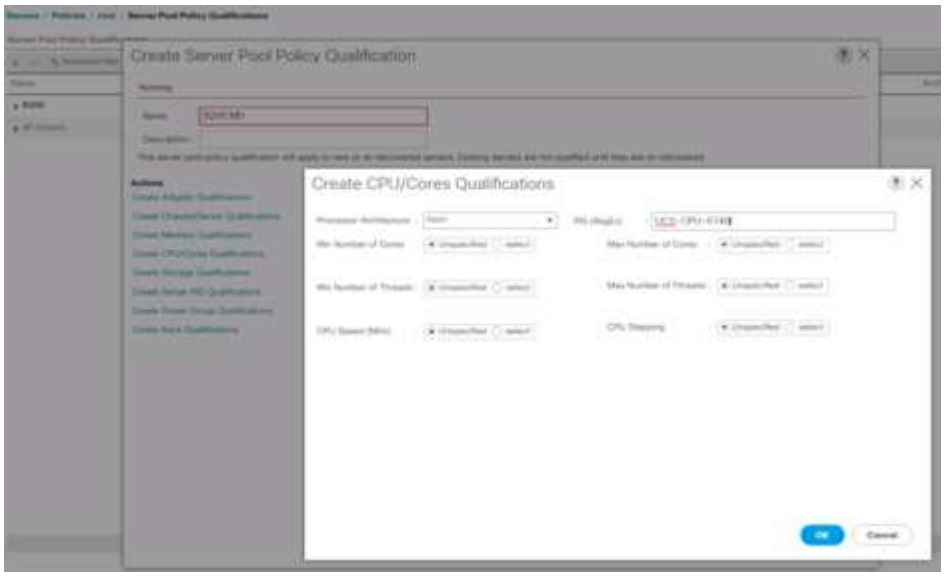


Serverpool-Qualifikationsrichtlinie erstellen (optional)

Gehen Sie wie folgt vor, um eine optionale Qualifikationsrichtlinie für den Server-Pool für die Cisco UCS-Umgebung zu erstellen:

Dieses Beispiel erstellt eine Richtlinie für Cisco UCS Server der B-Serie mit Intel E2660 v4 Xeon Broadwell Prozessoren.

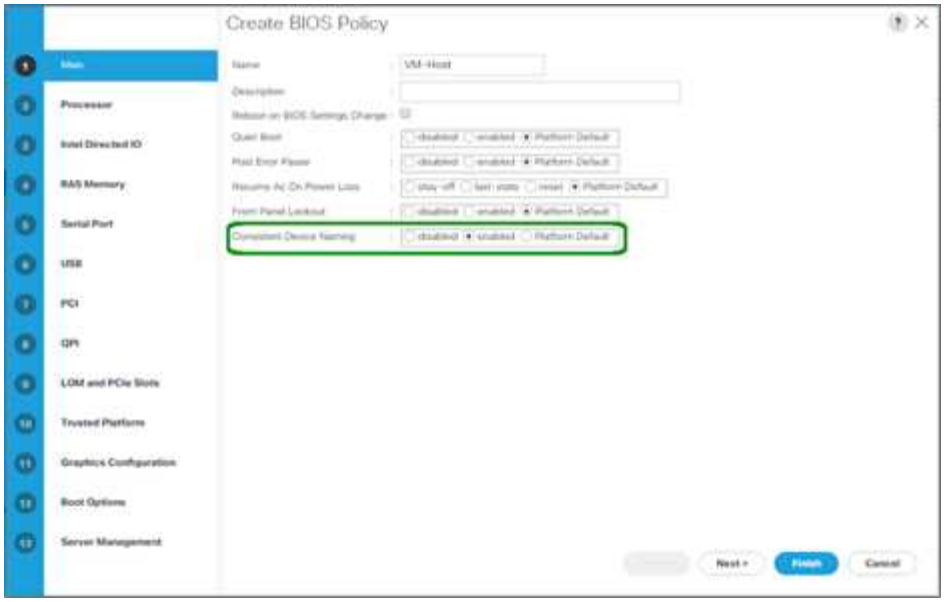
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Wählen Sie Die Qualifikationen Für Die Serverpool-Richtlinie Aus.
4. Wählen Sie Create Server Pool Policy Qualification oder Add aus.
5. Benennen Sie die Richtlinie Intel.
6. Wählen Sie CPU/Cores erstellen Qualifizierungen aus.
7. Wählen Sie Xeon für den Prozessor/die Architektur aus.
8. Eingabe `<UCS-CPU- PID>` Als Prozess-ID (PID).
9. Klicken Sie auf OK, um die CPU/Core-Qualifizierung zu erstellen.
10. Klicken Sie auf OK, um die Richtlinie zu erstellen, und klicken Sie anschließend auf OK, um die Bestätigung zu erhalten.



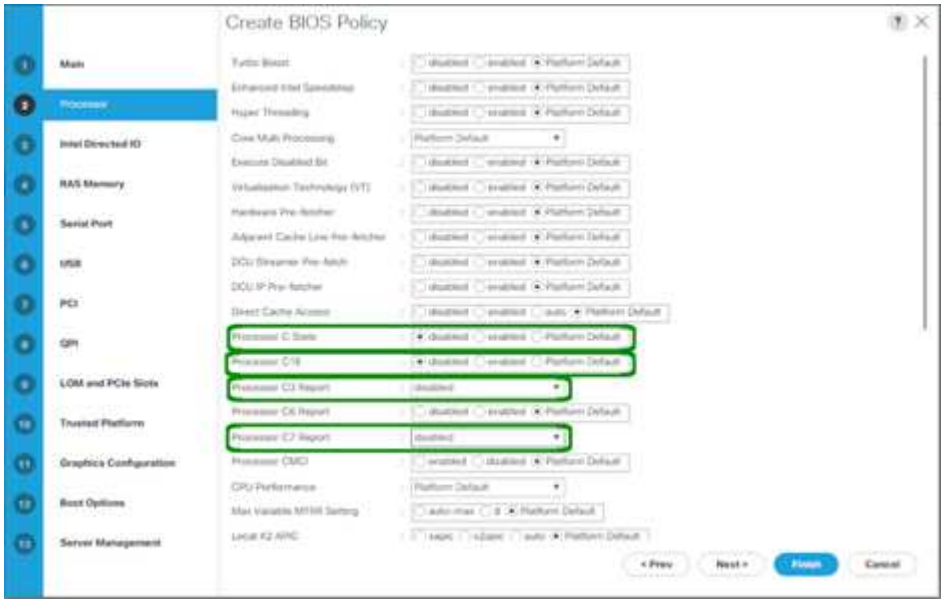
Erstellen der Server-BIOS-Richtlinie

Gehen Sie wie folgt vor, um eine Server-BIOS-Richtlinie für die Cisco UCS-Umgebung zu erstellen:

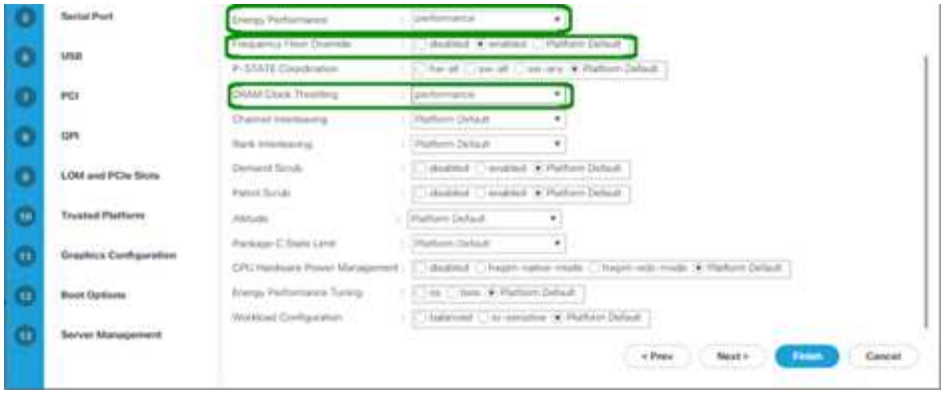
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf BIOS-Richtlinien.
4. Wählen Sie BIOS-Richtlinie erstellen.
5. Geben Sie den VM-Host als Namen der BIOS-Richtlinie ein.
6. Ändern Sie die Einstellung für den stillen Start auf deaktiviert.
7. Ändern Sie die konsistente Gerätenennung in aktiviert.



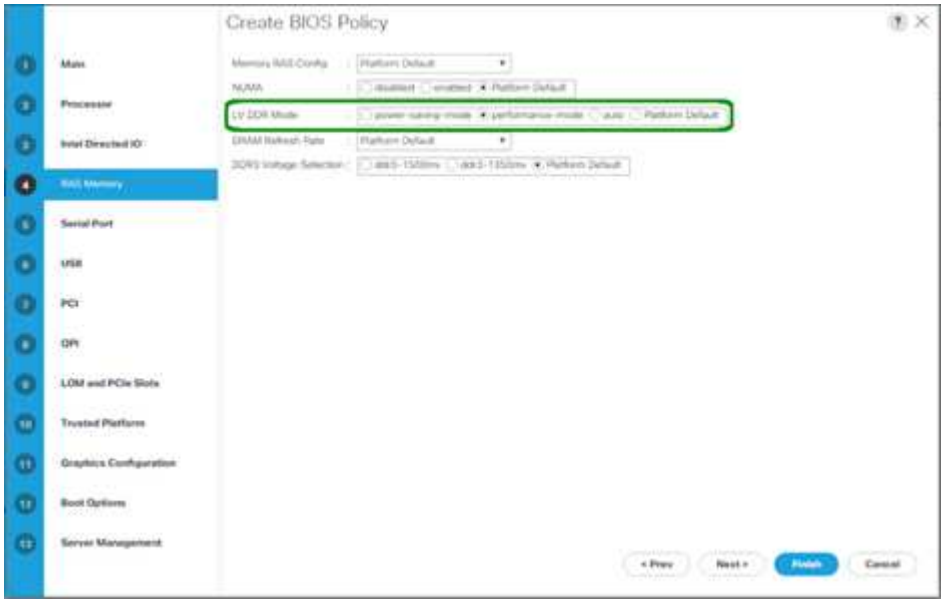
8. Wählen Sie die Registerkarte Prozessor aus, und legen Sie die folgenden Parameter fest:
   - Prozessor-C-Status: Deaktiviert
   - Prozessor C1E: Deaktiviert
   - Prozessor-C3-Bericht: Deaktiviert
   - Prozessor-C7-Bericht: Deaktiviert



9. Blättern Sie nach unten zu den übrigen Prozessoroptionen, und legen Sie die folgenden Parameter fest:
   - Energie Leistung: Leistung
   - Frequenzbereich: Aktiviert
   - DRAM-Clock-Drosselung: Performance



10. Klicken Sie auf RAS-Speicher, und legen Sie die folgenden Parameter fest:
    - LV DDR-Modus: Leistungsmodus

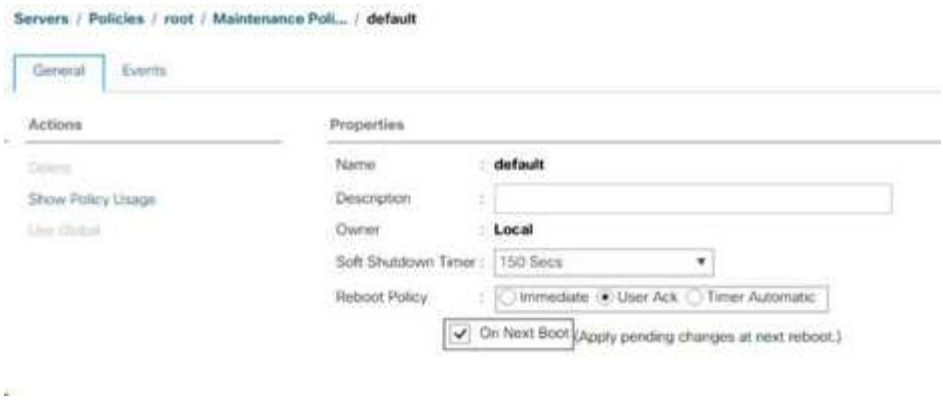


11. Klicken Sie auf Fertig stellen, um die BIOS-Richtlinie zu erstellen.
12. Klicken Sie auf OK.

Aktualisieren Sie die Standard-Wartungsrichtlinie

Gehen Sie wie folgt vor, um die Standardwartungsrichtlinie zu aktualisieren:

1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Wählen Sie Wartungsrichtlinien > Standard.
4. Ändern Sie die Richtlinie für den Neustart in Benutzerack.
5. Wählen Sie auf Next Boot, um die Wartungsfenster an Server-Administratoren zu delegieren.



6. Klicken Sie Auf Änderungen Speichern.
7. Klicken Sie auf OK, um die Änderung zu übernehmen.

VNIC-Vorlagen erstellen

Führen Sie zum Erstellen mehrerer vNIC-Vorlagen (Virtual Network Interface Card) für die Cisco UCS-Umgebung die in diesem Abschnitt beschriebenen Verfahren aus.

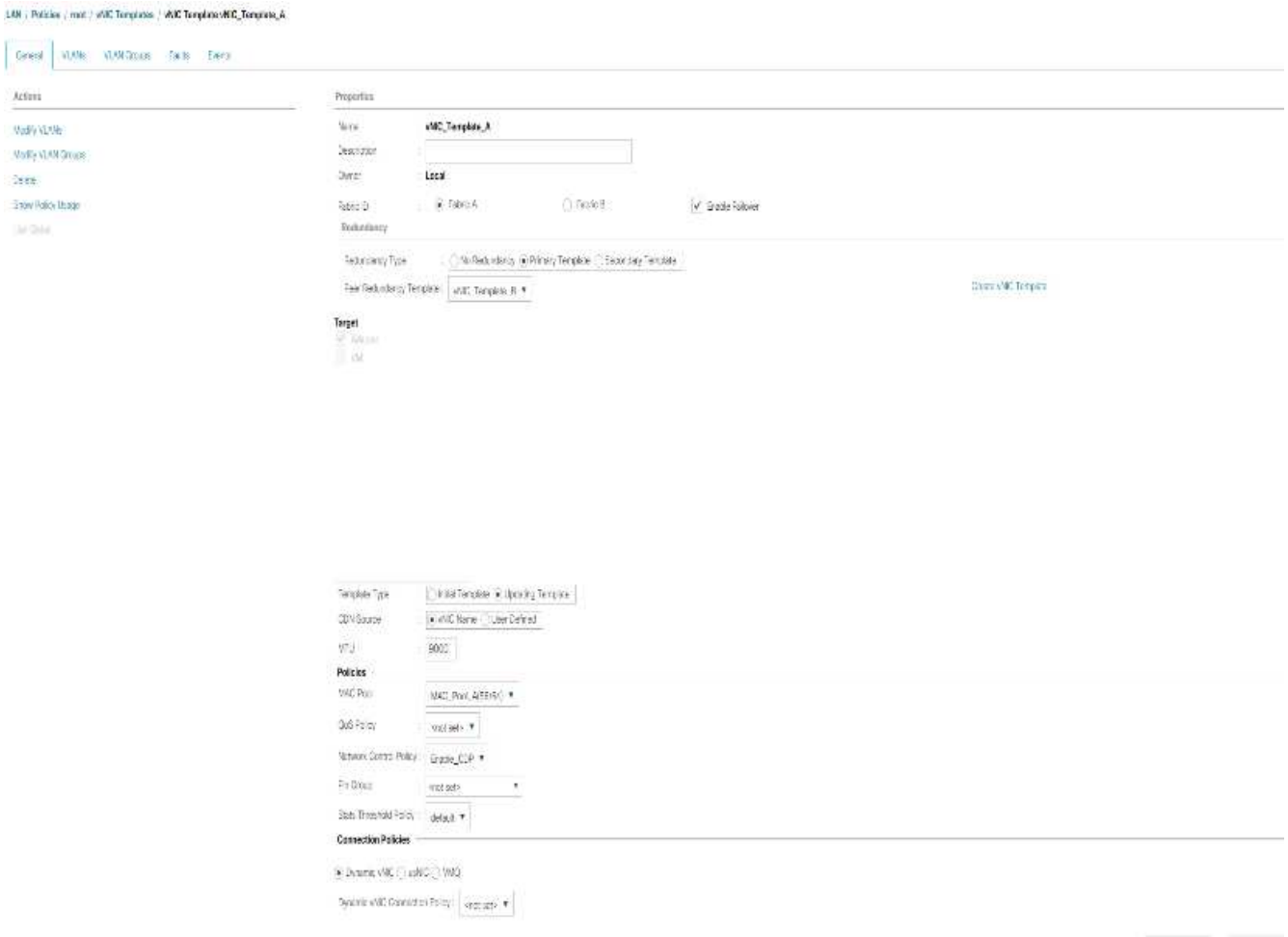
Es werden insgesamt vier vNIC-Vorlagen erstellt.

Erstellung von Infrastruktur-vNICs

Führen Sie zum Erstellen einer vNIC für die Infrastruktur die folgenden Schritte aus:

1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf vNIC-Vorlagen.
4. Wählen Sie vNIC-Vorlage erstellen.
5. Eingabe `Site-XX-vNIC_A` Als vNIC-Vorlagenname.
6. Wählen Sie Update-Template als Vorlagentyp aus.
7. Wählen Sie für die Fabric-ID die Option Fabric A. aus
8. Stellen Sie sicher, dass die Option Failover aktivieren nicht ausgewählt ist.
9. Primäre Vorlage für Redundanztyp auswählen.
10. Lassen Sie die Vorlage für Peer-Redundanz auf gesetzt `<not set>`.
11. Stellen Sie unter Target sicher, dass nur die Adapteroption ausgewählt ist.
12. Einstellen `Native-VLAN` Als natives VLAN.
13. Wählen Sie vNIC-Name für die CDN-Quelle aus.
14. Geben Sie für MTU 9000 ein.
15. Wählen Sie unter zugelassene VLANs die Option aus `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`Und Site-XX-vMotion. Verwenden Sie die Strg-Taste, um diese Mehrfachauswahl zu treffen.
16. Klicken Sie Auf Auswählen. Diese VLANs sollten nun unter ausgewählten VLANs angezeigt werden.
17. Wählen Sie in der Liste MAC-Pool die Option aus `MAC_Pool_A`.

18. Wählen Sie in der Liste Netzwerkkontrollrichtlinie Pool-A aus
19. Wählen Sie in der Liste Netzwerksteuerungsrichtlinie die Option Enable-CDP-LLDP.
20. Klicken Sie auf OK, um die vNIC-Vorlage zu erstellen.
21. Klicken Sie auf OK.

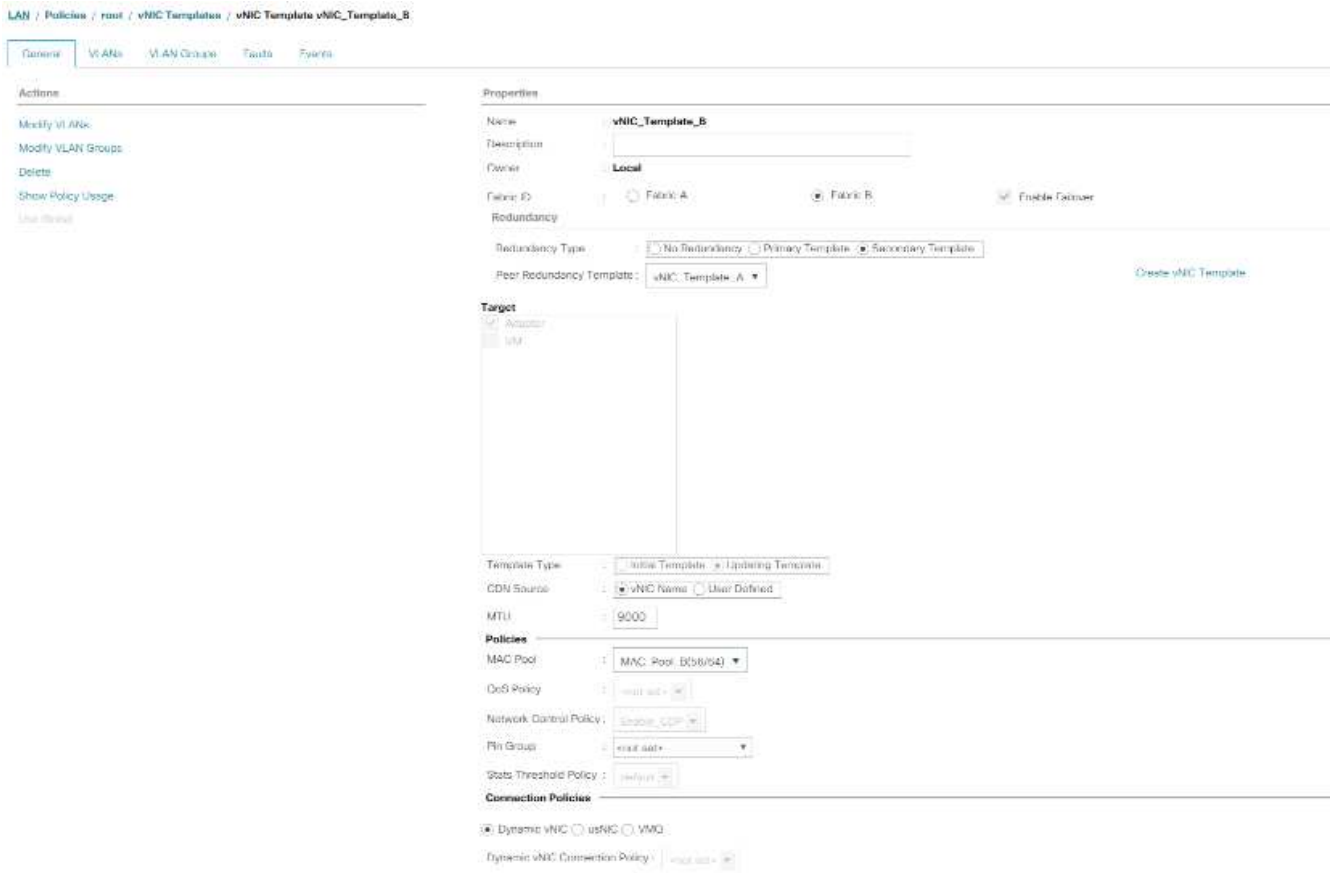


Gehen Sie wie folgt vor, um die sekundäre Redundanzvorlage Infra-B zu erstellen:

1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf vNIC-Vorlagen.
4. Wählen Sie vNIC-Vorlage erstellen.
5. Geben Sie `Site-XX-vNIC_B `als vNIC-Vorlagenname ein.
6. Wählen Sie Update-Template als Vorlagentyp aus.
7. Wählen Sie für Fabric-ID Fabric B aus
8. Wählen Sie die Option Failover aktivieren.

> Die Auswahl von Failover ist ein wichtiger Schritt zur Verbesserung der Link Failover-Zeit, indem sie auf Hardwareebene verarbeitet wird, und zum Schutz vor möglichen NIC-Ausfällen, die nicht vom virtuellen Switch erkannt werden.

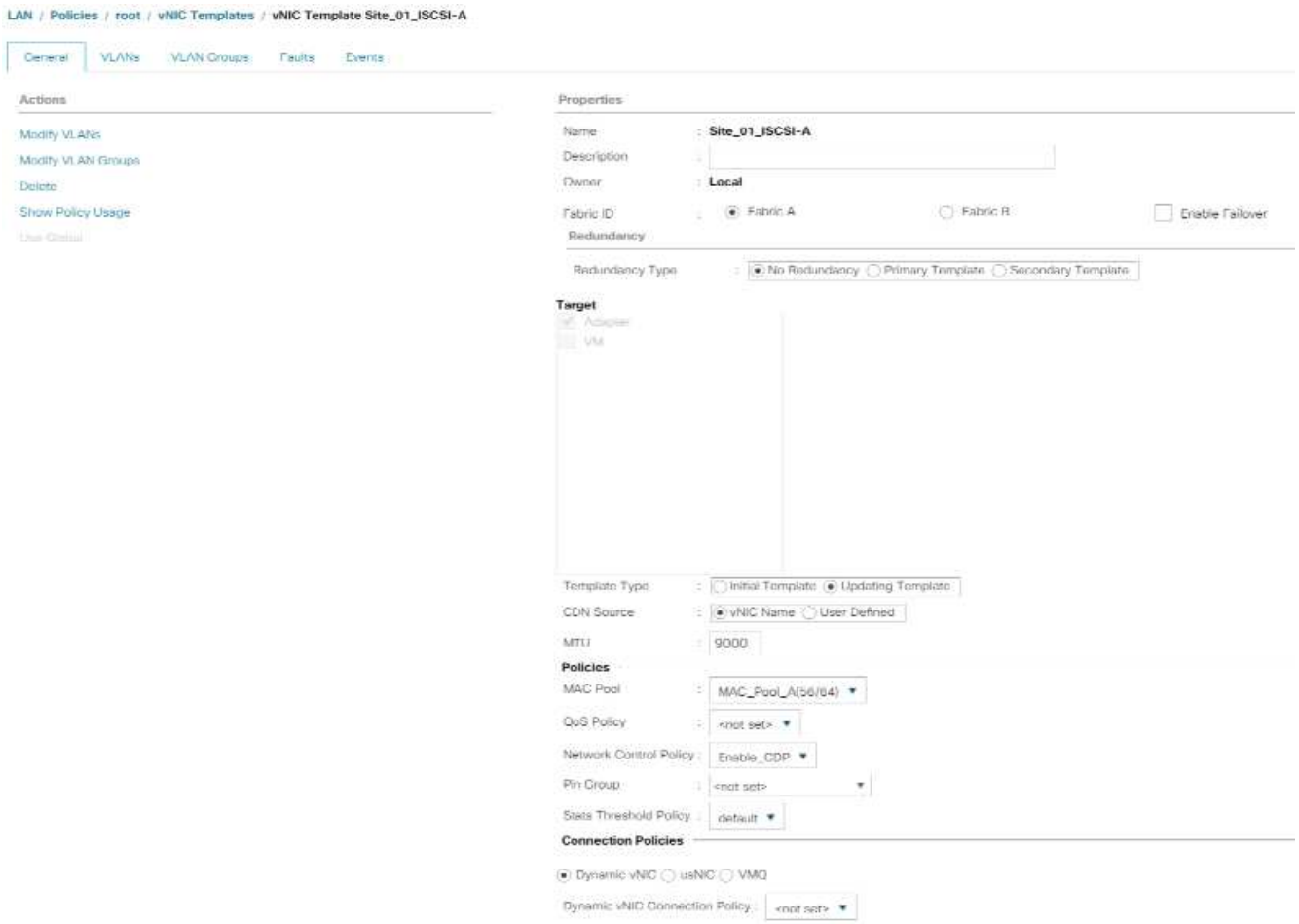
9. Primäre Vorlage für Redundanztyp auswählen.
10. Lassen Sie die Vorlage für Peer-Redundanz auf gesetzt `vNIC_Template_A`.
11. Stellen Sie unter Target sicher, dass nur die Adapteroption ausgewählt ist.
12. Einstellen `Native-VLAN` Als natives VLAN.
13. Wählen Sie vNIC-Name für die CDN-Quelle aus.
14. Geben Sie für MTU ein `9000`.
15. Wählen Sie unter zugelassene VLANs die Option aus `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic`Und Site-XX-vMotion. Verwenden Sie die Strg-Taste, um diese Mehrfachauswahl zu treffen.
16. Klicken Sie Auf Auswählen. Diese VLANs sollten nun unter ausgewählten VLANs angezeigt werden.
17. Wählen Sie in der Liste MAC-Pool die Option aus `MAC_Pool_B`.
18. Wählen Sie in der Liste Netzwerksteuerungsrichtlinie Pool-B aus
19. Wählen Sie in der Liste Netzwerksteuerungsrichtlinie die Option Enable-CDP-LLDP.
20. Klicken Sie auf OK, um die vNIC-Vorlage zu erstellen.
21. Klicken Sie auf OK.



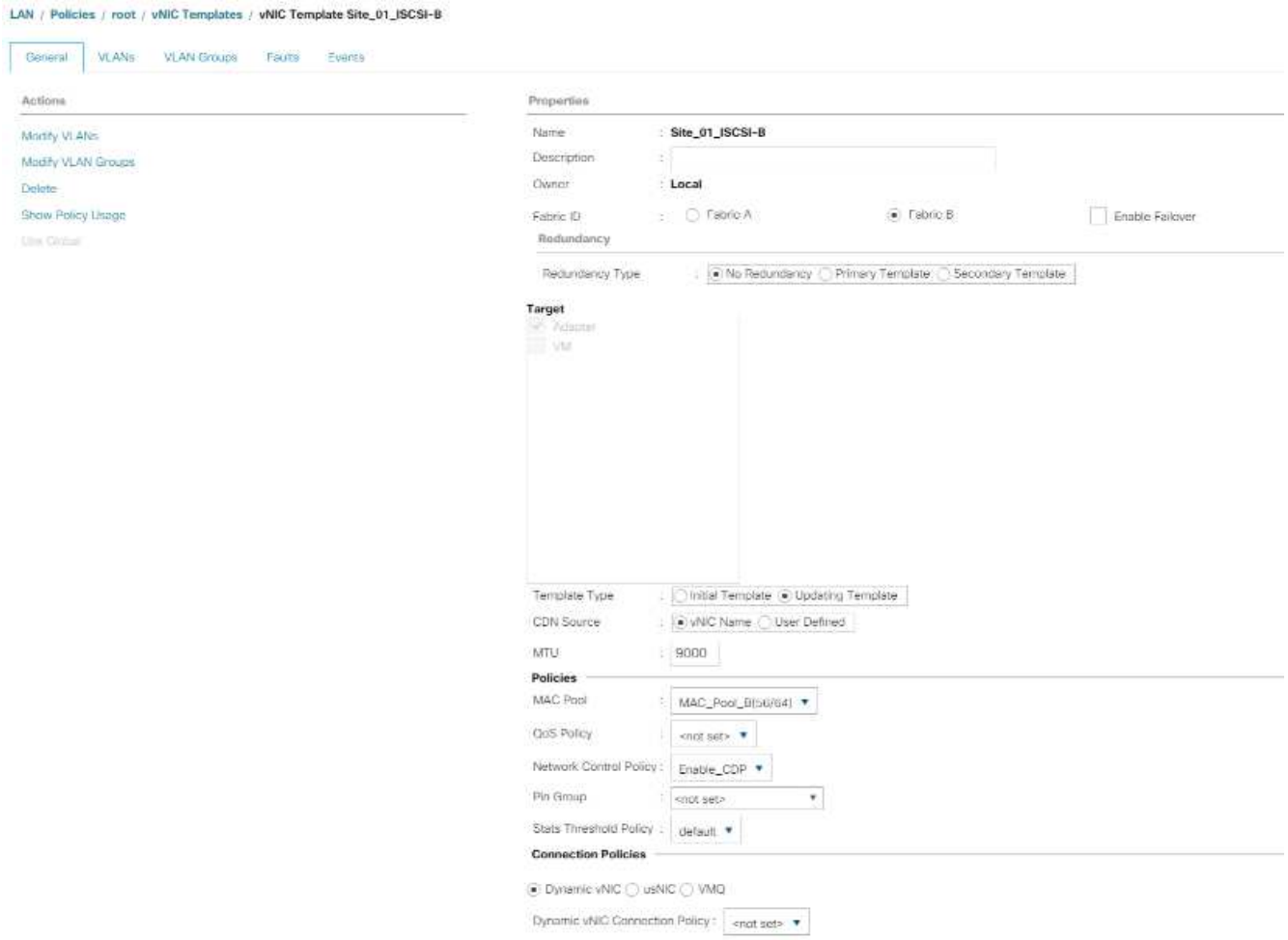
Erstellen von iSCSI-vNICs

Gehen Sie wie folgt vor, um iSCSI-vNICs zu erstellen:

1. Wählen Sie links LAN aus.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf vNIC-Vorlagen.
4. Wählen Sie vNIC-Vorlage erstellen.
5. Eingabe `Site- 01-iSCSI_A` Als vNIC-Vorlagenname.
6. Wählen Sie Stoff A. Wählen Sie die Option Failover aktivieren nicht aus.
7. Setzen Sie den Redundanztyp auf Keine Redundanz.
8. Stellen Sie unter Target sicher, dass nur die Adapteroption ausgewählt ist.
9. Wählen Sie Vorlage für Vorlagentyp aktualisieren aus.
10. Wählen Sie unter VLANs nur Site- 01-iSCSI_A_VLAN aus.
11. Wählen Sie Site- 01-iSCSI_A_VLAN als natives VLAN aus.
12. Lassen Sie den vNIC-Namen für die CDN-Quelle festgelegt.
13. Geben Sie unter MTU 9000 ein.
14. Wählen Sie aus der Liste MAC-Pool die Option MAC-Pool-A aus
15. Wählen Sie in der Liste Netzwerksteuerungsrichtlinie die Option Enable-CDP-LLDP.
16. Klicken Sie auf OK, um die Erstellung der vNIC-Vorlage abzuschließen.
17. Klicken Sie auf OK.



18. Wählen Sie links LAN aus.
19. Wählen Sie Richtlinien > Root.
20. Klicken Sie mit der rechten Maustaste auf vNIC-Vorlagen.
21. Wählen Sie vNIC-Vorlage erstellen.
22. Eingabe `Site- 01-iSCSI_B` Als vNIC-Vorlagenname.
23. Wählen Sie Stoff B aus Wählen Sie die Option Failover aktivieren nicht aus.
24. Setzen Sie den Redundanztyp auf Keine Redundanz.
25. Stellen Sie unter Target sicher, dass nur die Adapteroption ausgewählt ist.
26. Wählen Sie Vorlage für Vorlagentyp aktualisieren aus.
27. Wählen Sie unter VLANs nur aus `Site- 01-iSCSI_B_VLAN`.
28. Wählen Sie `Site- 01-iSCSI_B_VLAN` Als natives VLAN.
29. Lassen Sie den vNIC-Namen für die CDN-Quelle festgelegt.
30. Geben Sie unter MTU 9000 ein.
31. Wählen Sie aus der Liste MAC-Pool die Option aus `MAC-Pool-B`.
32. Wählen Sie aus der Liste Netzwerksteuerungsrichtlinie die Option aus `Enable-CDP-LLDP`.
33. Klicken Sie auf OK, um die Erstellung der vNIC-Vorlage abzuschließen.
34. Klicken Sie auf OK.



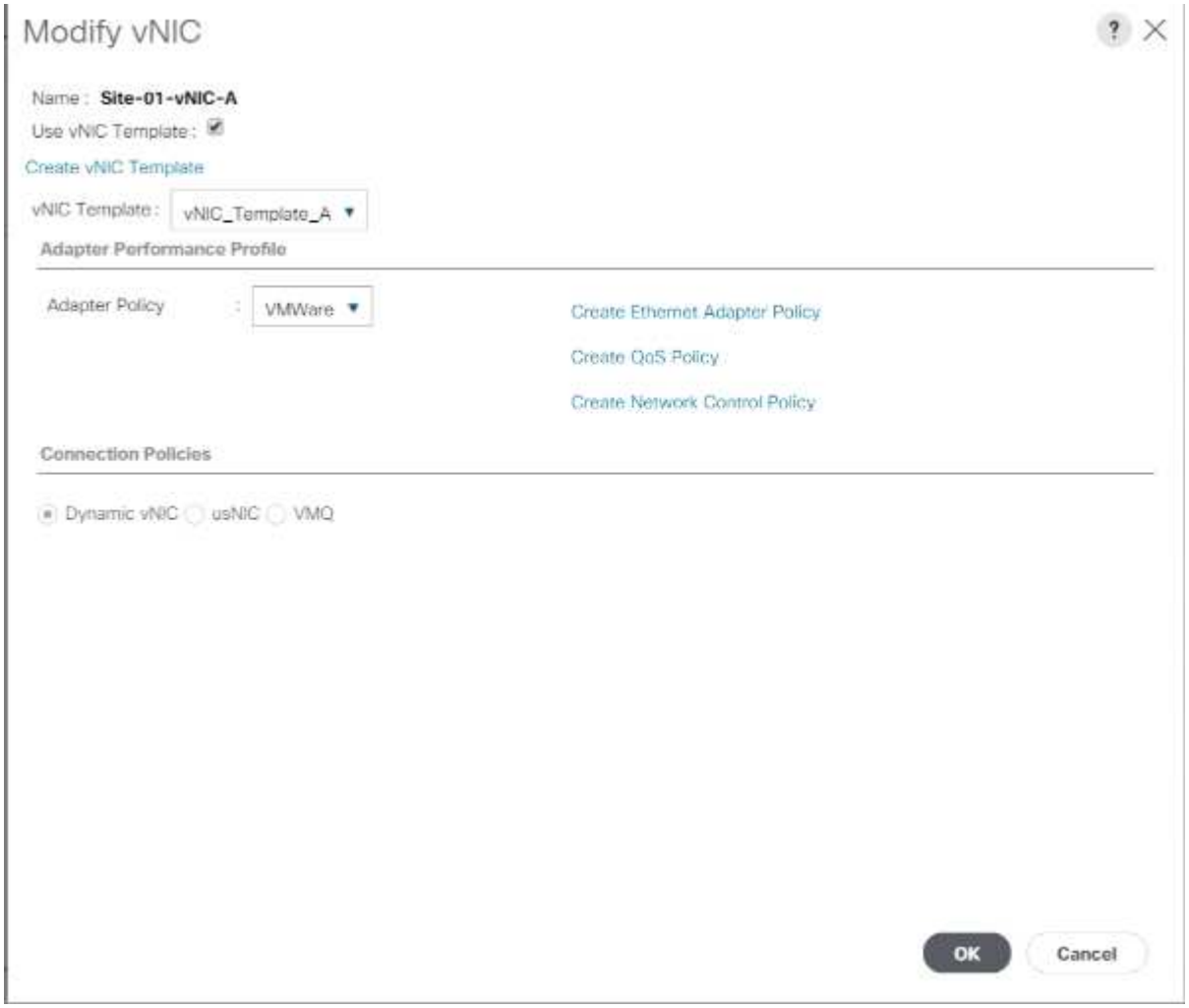
LAN-Konnektivitätsrichtlinie für iSCSI-Boot erstellen

Dieses Verfahren gilt für eine Cisco UCS-Umgebung, in der sich zwei iSCSI-LIFs auf Cluster-Node 1 befinden (`iscsi_lif01a` Und `iscsi_lif01b`) Und zwei iSCSI LIFs befinden sich auf Cluster Node 2 (`iscsi_lif02a` Und `iscsi_lif02b`). Es wird außerdem davon ausgegangen, dass die A-LIFs mit Fabric A (Cisco UCS 6324 A) verbunden sind und die B-LIFs mit Fabric B (Cisco UCS 6324 B) verbunden sind.

Gehen Sie wie folgt vor, um die erforderliche Infrastruktur-LAN-Konnektivitätsrichtlinie zu konfigurieren:

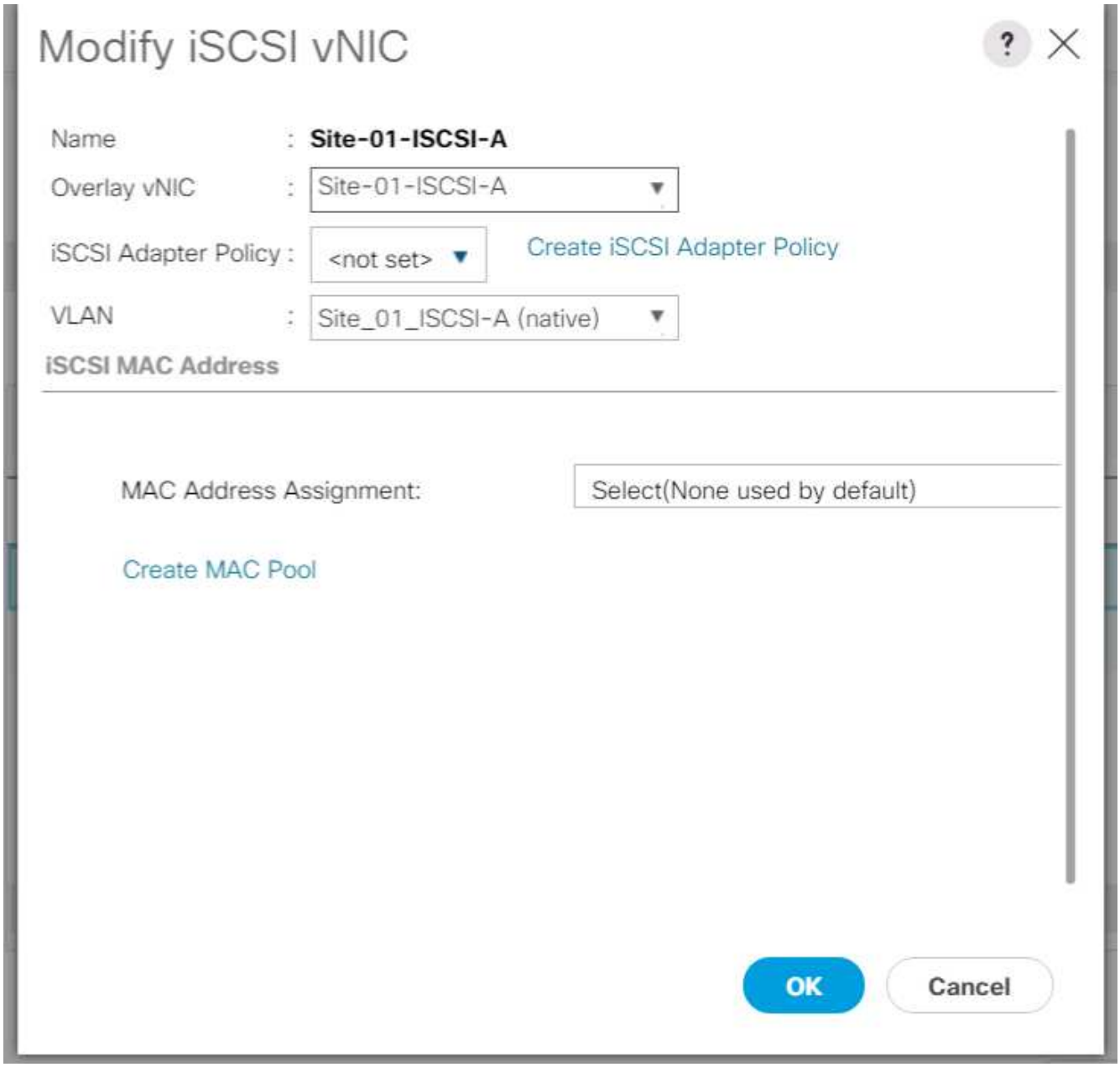
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie LAN > Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf LAN Connectivity Policies.
4. Wählen Sie LAN-Verbindungsrichtlinie erstellen.
5. Eingabe `Site-XX-Fabric-A` Als Name der Richtlinie.
6. Klicken Sie oben auf Hinzufügen, um einen vNIC hinzuzufügen.
7. Geben Sie im Dialogfeld vNIC erstellen ein `Site-01-vNIC-A` Als Name der vNIC.
8. Wählen Sie die Option vNIC-Vorlage verwenden aus.
9. Wählen Sie in der Liste vNIC-Vorlage die Option aus `vNIC_Template_A`.

10. Wählen Sie aus der Dropdown-Liste Adapterrichtlinie VMware aus.
11. Klicken Sie auf OK, um diese vNIC zur Richtlinie hinzuzufügen.

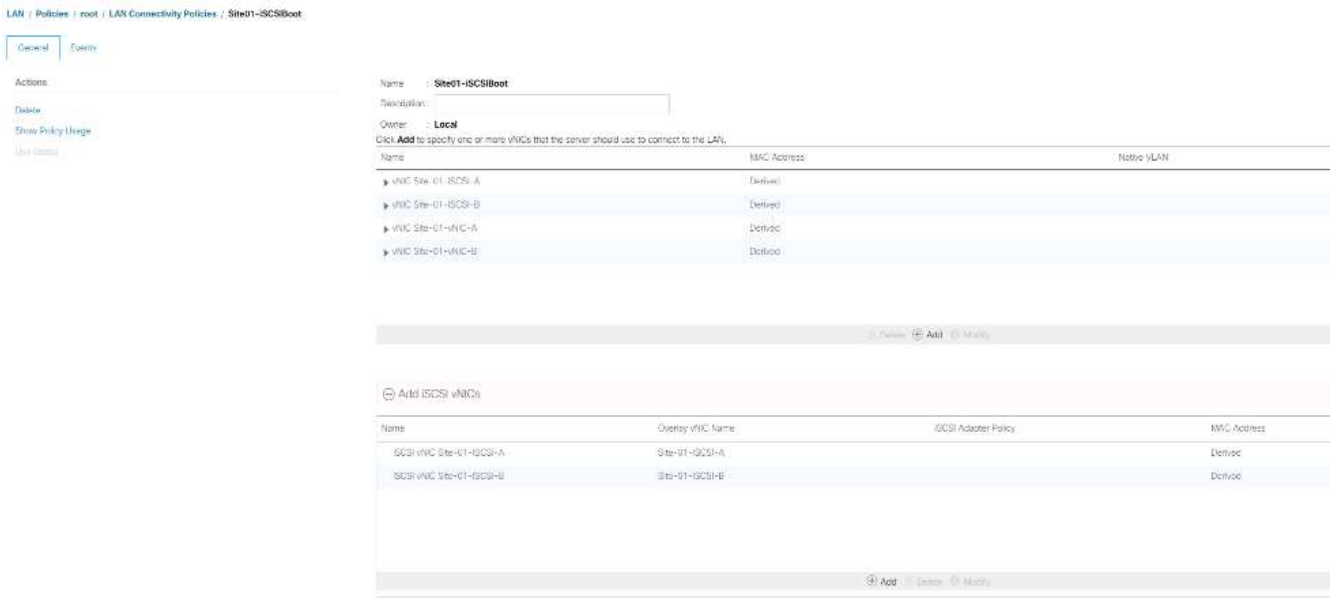


12. Klicken Sie oben auf Hinzufügen, um einen vNIC hinzuzufügen.
13. Geben Sie im Dialogfeld vNIC erstellen ein `Site-01-vNIC-B` Als Name der vNIC.
14. Wählen Sie die Option vNIC-Vorlage verwenden aus.
15. Wählen Sie in der Liste vNIC-Vorlage die Option aus `vNIC_Template_B`.
16. Wählen Sie aus der Dropdown-Liste Adapterrichtlinie VMware aus.
17. Klicken Sie auf OK, um diese vNIC zur Richtlinie hinzuzufügen.
18. Klicken Sie oben auf Hinzufügen, um einen vNIC hinzuzufügen.
19. Geben Sie im Dialogfeld vNIC erstellen ein `Site-01- iSCSI-A` Als Name der vNIC.
20. Wählen Sie die Option vNIC-Vorlage verwenden aus.
21. Wählen Sie in der Liste vNIC-Vorlage die Option aus `Site-01-iSCSI-A`.
22. Wählen Sie aus der Dropdown-Liste Adapterrichtlinie VMware aus.
23. Klicken Sie auf OK, um diese vNIC zur Richtlinie hinzuzufügen.
24. Klicken Sie oben auf Hinzufügen, um einen vNIC hinzuzufügen.

25. Geben Sie im Dialogfeld vNIC erstellen ein `Site-01-iSCSI-B` Als Name der vNIC.
26. Wählen Sie die Option vNIC-Vorlage verwenden aus.
27. Wählen Sie in der Liste vNIC-Vorlage die Option aus `Site-01-iSCSI-B`.
28. Wählen Sie aus der Dropdown-Liste Adapterrichtlinie VMware aus.
29. Klicken Sie auf OK, um diese vNIC zur Richtlinie hinzuzufügen.
30. Erweitern Sie die Option iSCSI vNICs hinzufügen.
31. Klicken Sie im Bereich iSCSI vNICs hinzufügen auf die Option Lower Add, um die iSCSI vNIC hinzuzufügen.
32. Geben Sie im Dialogfeld iSCSI vNIC erstellen ein `Site-01-iSCSI-A` Als Name der vNIC.
33. Wählen Sie die vNIC Overlay unter aus `Site-01-iSCSI-A`.
34. Lassen Sie die iSCSI-Adapter-Policy-Option nicht festgelegt.
35. Wählen Sie das VLAN unter aus `Site-01-iSCSI-Site-A` (Nativ)
36. Wählen Sie Keine (standardmäßig verwendet) als MAC-Adresszuweisung.
37. Klicken Sie auf OK, um die iSCSI-vNIC zur Richtlinie hinzuzufügen.



38. Klicken Sie im Bereich iSCSI vNICs hinzufügen auf die Option Lower Add, um die iSCSI vNIC hinzuzufügen.
39. Geben Sie im Dialogfeld iSCSI vNIC erstellen ein `Site-01-iSCSI-B` Als Name der vNIC.
40. Wählen Sie die Overlay vNIC als Standort-01-iSCSI-B aus
41. Lassen Sie die iSCSI-Adapter-Policy-Option nicht festgelegt.
42. Wählen Sie das VLAN unter aus `Site-01-iSCSI-Site-B` (Nativ)
43. Wählen Sie Keine (standardmäßig verwendet) als MAC-Adresszuweisung.
44. Klicken Sie auf OK, um die iSCSI-vNIC zur Richtlinie hinzuzufügen.
45. Klicken Sie Auf Änderungen Speichern.



Erstellen Sie die vMedia-Richtlinie für den Installationsstart von VMware ESXi 6.7U1

In den NetApp Data ONTAP-Einrichtungsschritten ist ein HTTP-Web-Server erforderlich, der für das Hosting von NetApp Data ONTAP sowie VMware-Software verwendet wird. Die hier erstellte vMedia Policy bildet VMware ESXi 6 ab. 7U1 ISO auf den Cisco UCS Server, um die ESXi-Installation zu starten. Gehen Sie wie folgt vor, um diese Richtlinie zu erstellen:

1. Wählen Sie im Cisco UCS Manager links Server aus.
2. Wählen Sie Richtlinien > Root.
3. Wählen Sie vMedia Policies.
4. Klicken Sie auf Hinzufügen, um eine neue vMedia Policy zu erstellen.
5. Richtlinie ESXi-6.7U1-HTTP benennen
6. Geben Sie im Feld Beschreibung die ISO-Einstellungen für ESXi 6.7U1 ein.
7. Wählen Sie Ja, um den Montagefehler erneut zu versuchen.
8. Klicken Sie Auf Hinzufügen.
9. Benennen Sie den Mount ESXi-6.7U1-HTTP.
10. Wählen Sie den CDD-Gerätetyp aus.
11. Wählen Sie das HTTP-Protokoll aus.
12. Geben Sie die IP-Adresse des Webservers ein.

> Die DNS-Server-IPs wurden früher nicht in die KVM-IP eingegeben, daher ist es notwendig, die IP des Webservers anstelle des Hostnamens einzugeben.

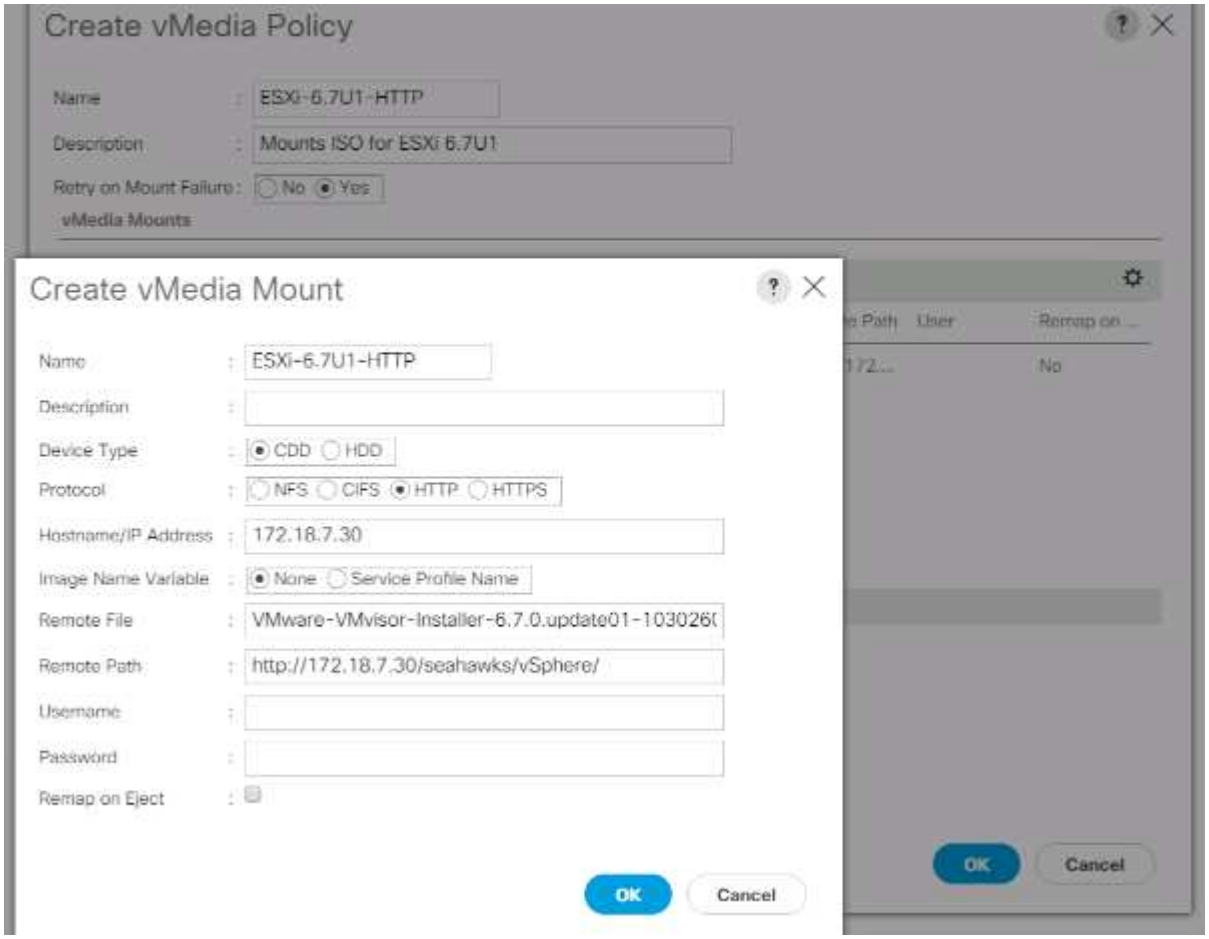
13. Eingabe `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Als Name der Remote-Datei.

    Dieser VMware ESXi 6.7U1 ISO kann von heruntergeladen werden "VMware-Downloads".

14. Geben Sie im Feld Remote Path den Pfad des Webservers zur ISO-Datei ein.

15. Klicken Sie auf OK, um den vMedia Mount zu erstellen.
16. Klicken Sie erneut auf OK und anschließend auf OK, um die Erstellung der vMedia Policy abzuschließen.

    Bei allen neuen Servern, die der Cisco UCS Umgebung hinzugefügt werden, kann die vMedia-Service-Profilvorlage zur Installation des ESXi Hosts verwendet werden. Beim ersten Booten startet der Host in den ESXi Installer, da die über SAN bereitgestellte Festplatte leer ist. Nach der Installation von ESXi wird auf die vMedia nicht verwiesen, solange auf die Boot-Diskette zugegriffen werden kann.



ISCSI-Startrichtlinie erstellen

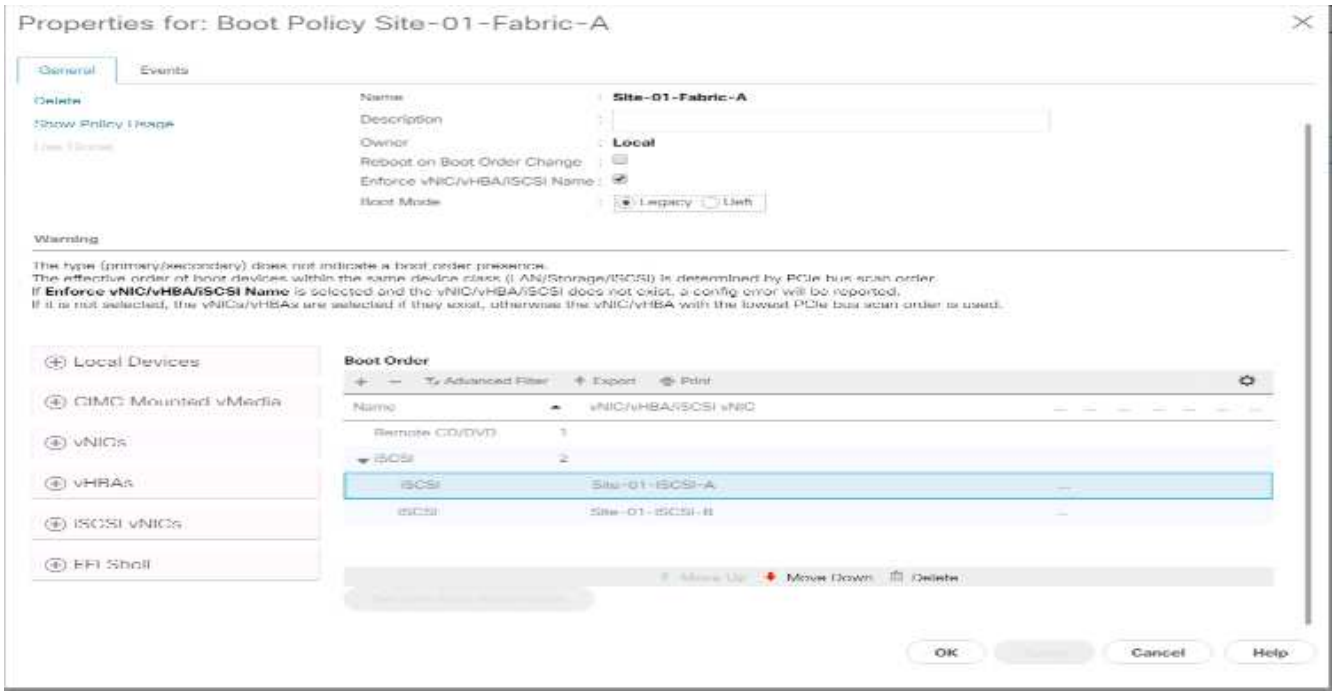
Das Verfahren in diesem Abschnitt gilt für eine Cisco UCS-Umgebung, in der sich zwei logische iSCSI-Schnittstellen (LIFs) auf Cluster-Node 1 befinden (`iscsi_lif01a` Und `iscsi_lif01b`) Und zwei iSCSI LIFs befinden sich auf Cluster Node 2 (`iscsi_lif02a` Und `iscsi_lif02b`). Es wird außerdem davon ausgegangen, dass die A LIFs mit Fabric A (Cisco UCS Fabric Interconnect A) verbunden sind und die B LIFs mit Fabric B (Cisco UCS Fabric Interconnect B) verbunden sind.

> Bei diesem Verfahren wird eine Boot-Richtlinie konfiguriert. Die Richtlinie konfiguriert das primäre Ziel so, dass es sein soll `iscsi_lif01a`.

Gehen Sie wie folgt vor, um eine Boot-Richtlinie für die Cisco UCS-Umgebung zu erstellen:

1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf Startrichtlinien.

4. Wählen Sie Boot Policy Erstellen.
5. Eingabe `Site-01-Fabric-A` Als Name der Boot-Richtlinie.
6. Optional: Geben Sie eine Beschreibung für die Boot Policy ein.
7. Lassen Sie die Option Neu starten bei der Änderung der Startreihenfolge deaktiviert.
8. Der Boot-Modus ist alt.
9. Erweitern Sie das Dropdown-Menü Lokale Geräte, und wählen Sie Remote-CD/DVD hinzufügen.
10. Erweitern Sie das Dropdown-Menü iSCSI vNICs, und wählen Sie iSCSI Boot hinzufügen.
11. Geben Sie im Dialogfeld iSCSI-Boot hinzufügen ein `Site-01-iSCSI-A`. Klicken Sie auf OK.
12. Wählen Sie iSCSI-Boot hinzufügen.
13. Geben Sie im Dialogfeld iSCSI-Boot hinzufügen ein `Site-01-iSCSI-B`. Klicken Sie auf OK.
14. Klicken Sie auf OK, um die Richtlinie zu erstellen.



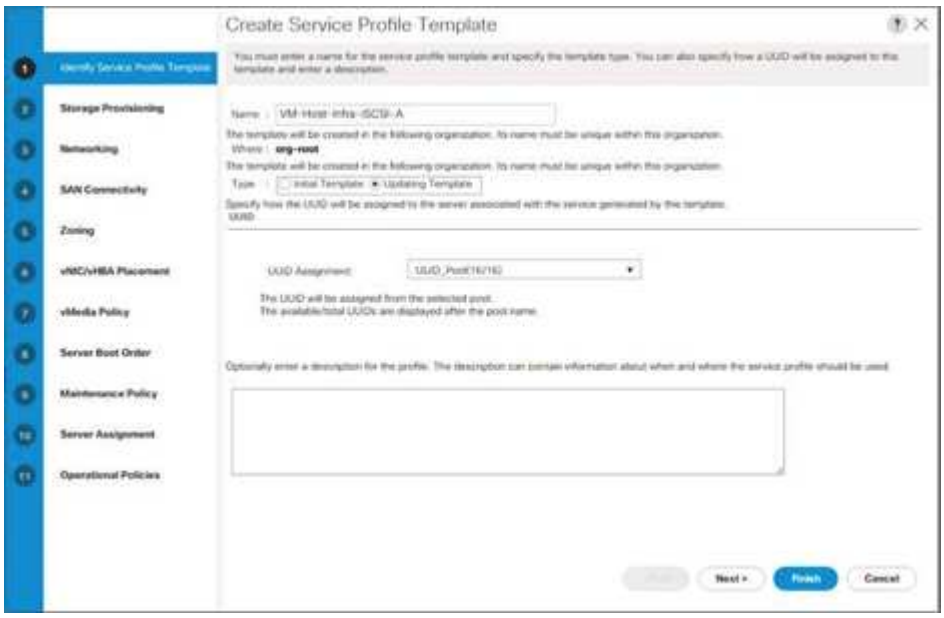
Erstellen einer Service-Profilvorlage

In diesem Verfahren wird eine Service-Profilvorlage für Infrastruktur-ESXi-Hosts für Fabric A-Boot erstellt.

Um die Service-Profilvorlage zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Service Profile Vorlagen > root.
3. Klicken Sie mit der rechten Maustaste auf „Root“.
4. Wählen Sie Dienstprofilvorlage erstellen, um den Assistenten Dienstprofilvorlage erstellen zu öffnen.
5. Eingabe `VM-Host-Infra-iSCSI-A` Trägt den Namen der Service-Profilvorlage bei. Diese Service-Profil-Vorlage ist für das Booten von Storage-Node 1 in Fabric A konfiguriert
6. Wählen Sie die Option Vorlage aktualisieren aus.

7. Wählen Sie unter UUID die Option aus `UUID_Pool` Als UUID-Pool. Klicken Sie Auf Weiter.



Konfiguration der Speicherbereitstellung

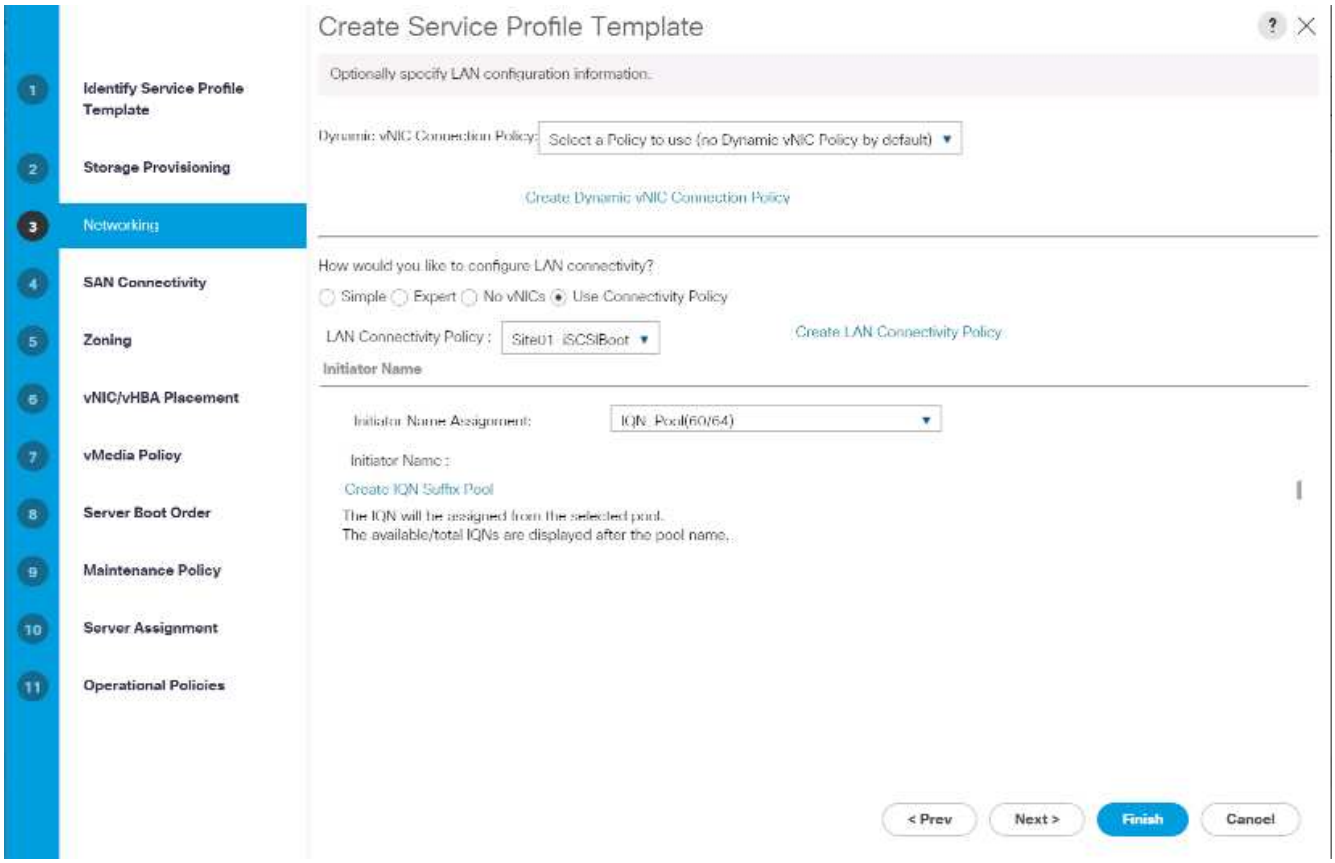
Gehen Sie wie folgt vor, um die Speicherbereitstellung zu konfigurieren:

1. Wenn Sie Server ohne physische Laufwerke haben, klicken Sie auf Konfigurationsrichtlinie für lokale Festplatten, und wählen Sie die lokale SAN Boot-Speicherrichtlinie aus. Wählen Sie andernfalls die Standard-Richtlinie für lokalen Speicher aus.
2. Klicken Sie Auf Weiter.

Netzwerkoptionen konfigurieren

Gehen Sie wie folgt vor, um die Netzwerkoptionen zu konfigurieren:

1. Behalten Sie die Standardeinstellung für die dynamische vNIC-Verbindungsrichtlinie bei.
2. Wählen Sie die Option Verbindungsrichtlinie verwenden, um die LAN-Konnektivität zu konfigurieren.
3. Wählen Sie iSCSI-Boot aus dem Dropdown-Menü LAN Connectivity Policy.
4. Wählen Sie `IQN_Pool` In Initiator-Namenszuweisung. Klicken Sie Auf Weiter.



Konfigurieren Sie die SAN-Konnektivität

Gehen Sie wie folgt vor, um die SAN-Konnektivität zu konfigurieren:

1. Wählen Sie für die vHBAs „Nein“ aus, um die Konfiguration von SAN-Verbindungen vorzunehmen. Option.
2. Klicken Sie Auf Weiter.

Konfigurieren Sie das Zoning

Klicken Sie zum Konfigurieren des Zoning einfach auf Weiter.

Konfiguration der vNIC/HBA-Platzierung

Gehen Sie wie folgt vor, um die Platzierung von vNIC/HBA zu konfigurieren:

1. Lassen Sie in der Dropdown-Liste Platzierung auswählen die Platzierungsrichtlinie als Platzierung des Systems durchführen lassen.
2. Klicken Sie Auf Weiter.

VMedia-Richtlinie konfigurieren

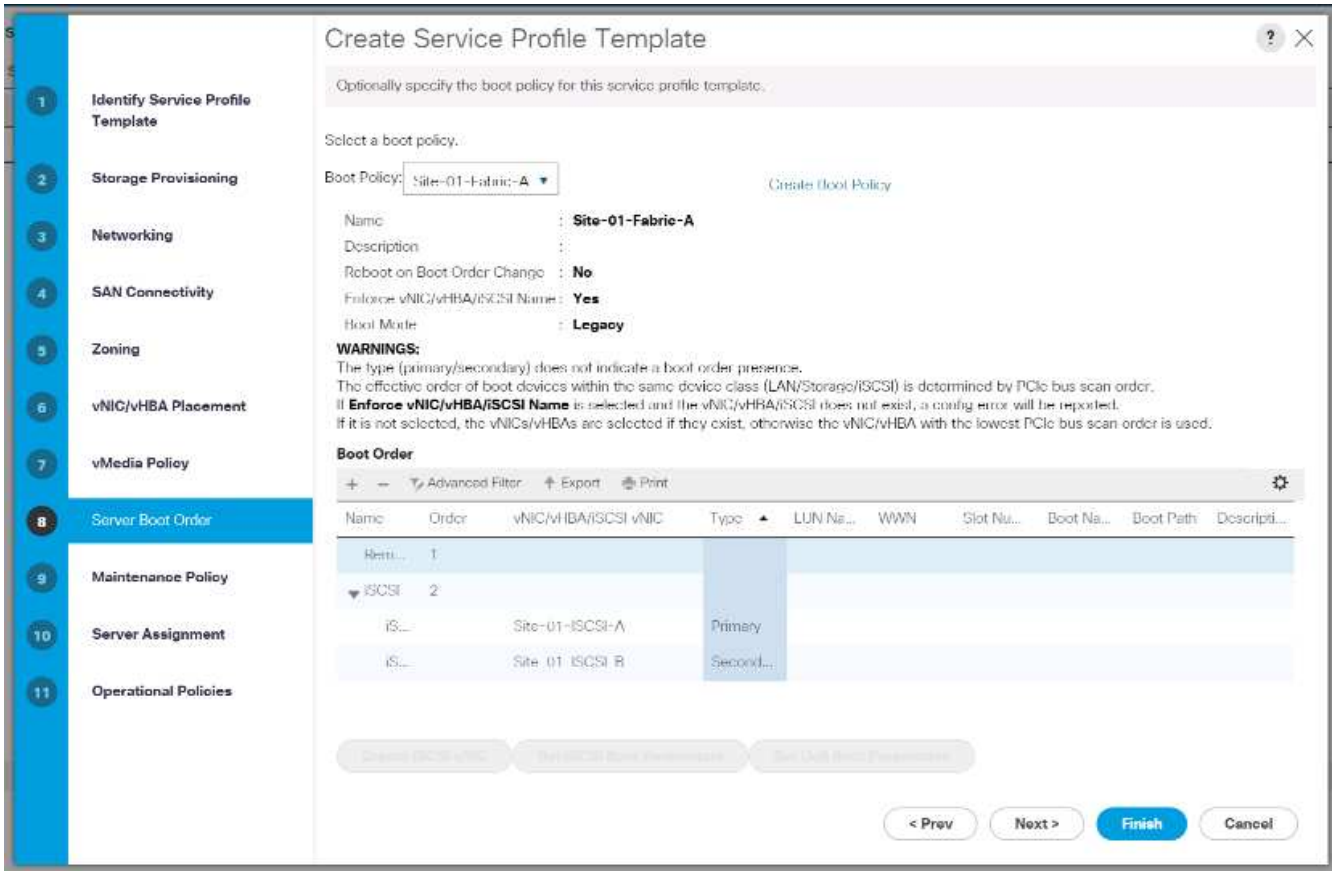
Gehen Sie wie folgt vor, um die vMedia-Richtlinie zu konfigurieren:

1. Wählen Sie keine vMedia Policy aus.
2. Klicken Sie Auf Weiter.

Server-Startreihenfolge konfigurieren

Gehen Sie wie folgt vor, um die Server-Startreihenfolge zu konfigurieren:

1. Wählen Sie `Boot-Fabric-A` Für Boot Policy.



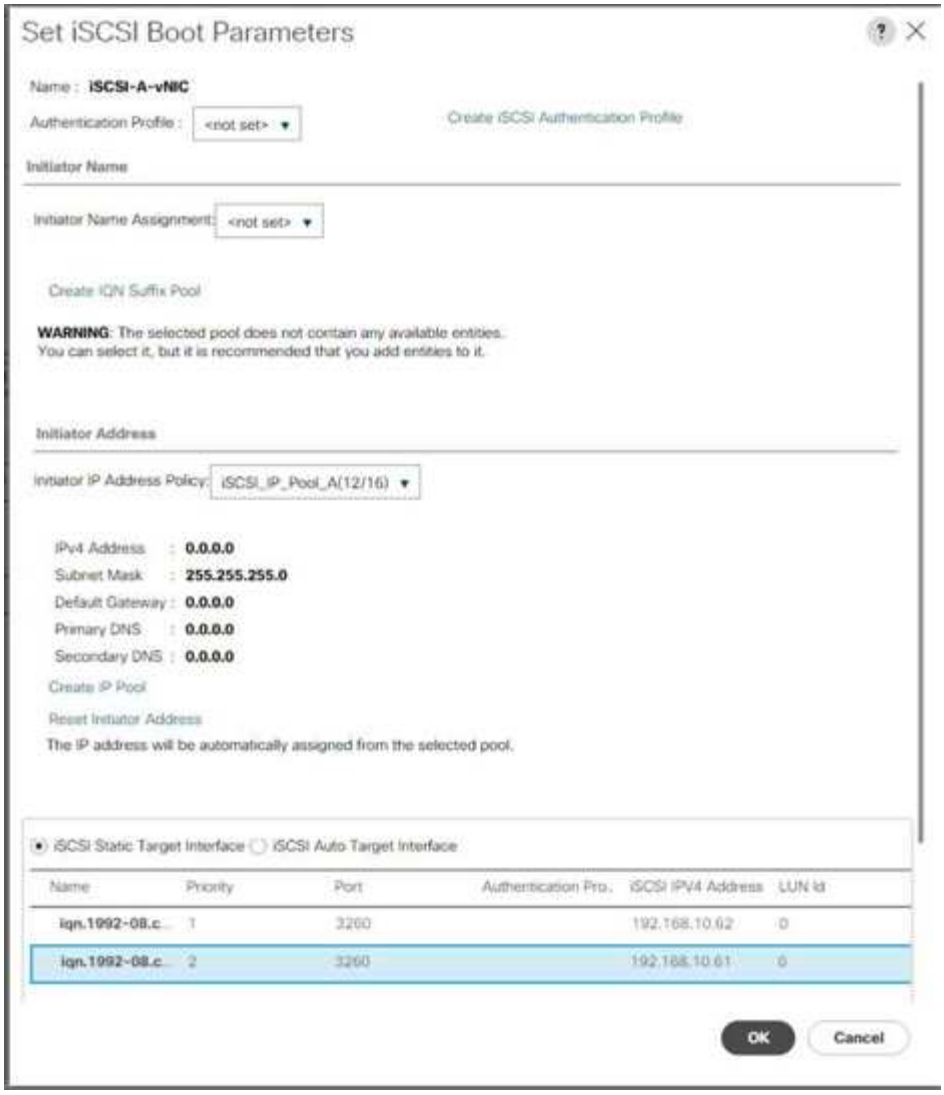
2. Wählen Sie in der Boor-Reihenfolge aus `Site-01- iSCSI-A`.
3. Klicken Sie auf iSCSI-Startparameter festlegen.
4. Lassen Sie im Dialogfeld iSCSI-Boot-Parameter festlegen die Option Authentication Profile nicht auf gesetzt, es sei denn, Sie haben unabhängig eine für Ihre Umgebung geeignete Option erstellt.
5. Lassen Sie das Dialogfeld „Initiator Name Assignment“ nicht so eingestellt, dass der in den vorherigen Schritten definierte Single Service Profile Initiator Name verwendet wird.
6. Einstellen `iSCSI_IP_Pool_A` Als Initiator-IP-Adressrichtlinie.
7. Wählen Sie die Option iSCSI Static Target Interface.
8. Klicken Sie Auf Hinzufügen.
9. Geben Sie den iSCSI-Zielnamen ein. Um den iSCSI-Zielnamen Infra-SVM zu erhalten, melden Sie sich bei der Storage-Cluster-Managementoberfläche an, und führen Sie den aus `iscsi show` Befehl.

```
bb04-aff300::> iscsi show
            Target                          Target                          Status
Vserver     Name                            Alias                           Admin
----------- ------------------------------- ------------------------------- ------
Infra-SVM   iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                            Infra-SVM                       up
```

10. Geben Sie die IP-Adresse von ein `iscsi_lif_02a` Für das Feld IPv4-Adresse.

11. Klicken Sie auf OK, um das statische iSCSI-Ziel hinzuzufügen.
12. Klicken Sie Auf Hinzufügen.
13. Geben Sie den iSCSI-Zielnamen ein.
14. Geben Sie die IP-Adresse von ein `iscsi_lif_01a` Für das Feld IPv4-Adresse.

15. Klicken Sie auf OK, um das statische iSCSI-Ziel hinzuzufügen.



Die Ziel-IPs wurden mit Storage Node 02 IP zuerst und Storage Node 01 IP Sekunde festgelegt. Dies setzt voraus, dass die Boot-LUN auf Node 01 ist. Der Host wird über den Pfad zu Node 01 gebootet, wenn die Reihenfolge in diesem Verfahren verwendet wird.

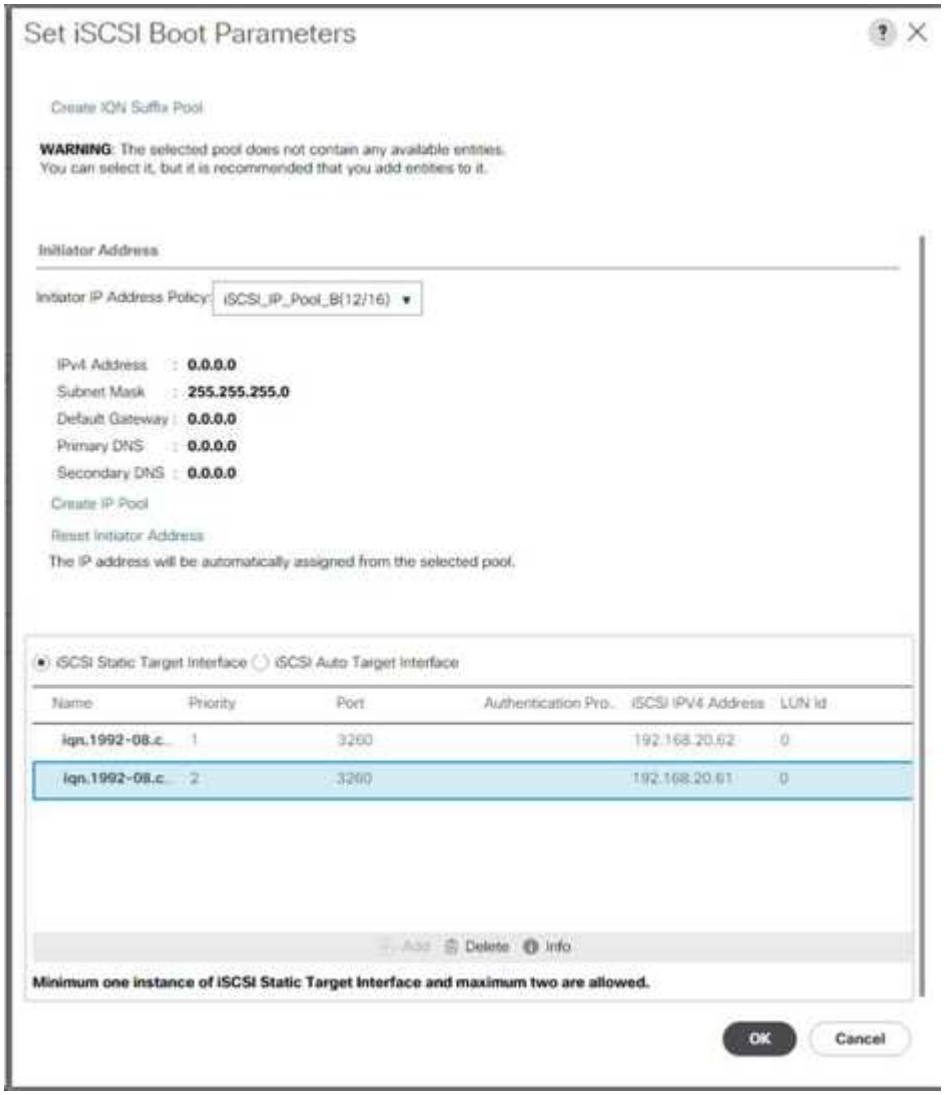
16. Wählen Sie in der Startreihenfolge iSCSI-B-vNIC aus.
17. Klicken Sie auf iSCSI-Startparameter festlegen.
18. Lassen Sie im Dialogfeld iSCSI-Boot-Parameter festlegen die Option Authentication Profile nicht als festgelegt, es sei denn, Sie haben unabhängig eine für Ihre Umgebung geeignete Option erstellt.
19. Lassen Sie das Dialogfeld „Initiator Name Assignment“ nicht so eingestellt, dass der in den vorherigen Schritten definierte Single Service Profile Initiator Name verwendet wird.
20. Einstellen `iSCSI_IP_Pool_B` Als Richtlinie für die Initiator-IP-Adresse.
21. Wählen Sie die Option iSCSI Static Target Interface.
22. Klicken Sie Auf Hinzufügen.
23. Geben Sie den iSCSI-Zielnamen ein. Um den iSCSI-Zielnamen Infra-SVM zu erhalten, melden Sie sich bei der Storage-Cluster-Managementoberfläche an, und führen Sie den aus `iscsi show` Befehl.

```
bb04-aff300::> iscsi show
          Target                          Target                         Status
Vserver   Name                            Alias                          Admin
--------- ------------------------------- ------------------------------ ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                      up
```

24. Geben Sie die IP-Adresse von ein `iscsi_lif_02b` Für das Feld IPv4-Adresse.

25. Klicken Sie auf OK, um das statische iSCSI-Ziel hinzuzufügen.
26. Klicken Sie Auf Hinzufügen.
27. Geben Sie den iSCSI-Zielnamen ein.
28. Geben Sie die IP-Adresse von ein `iscsi_lif_01b` Für das Feld IPv4-Adresse.

29. Klicken Sie auf OK, um das statische iSCSI-Ziel hinzuzufügen.

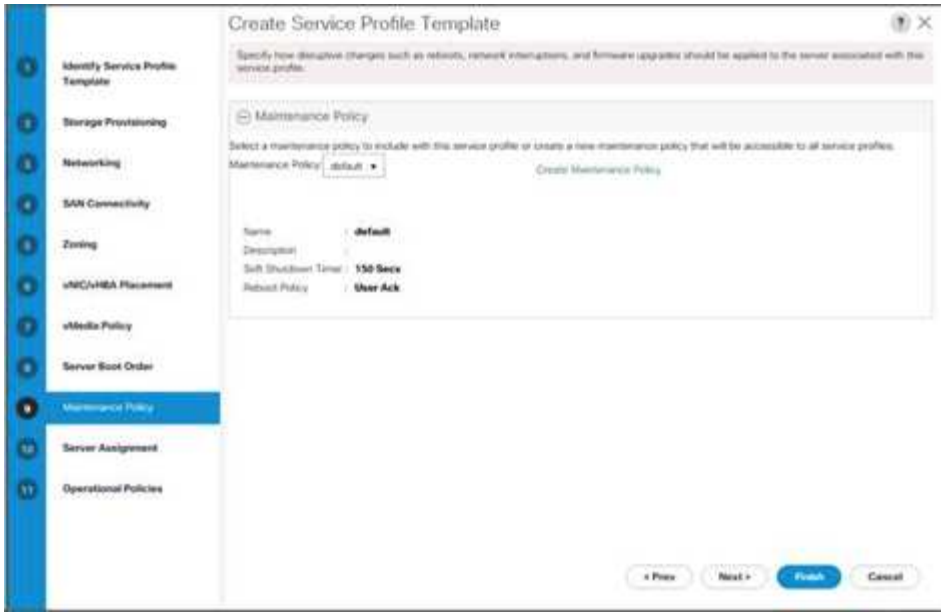


30. Klicken Sie Auf Weiter.

Wartungsrichtlinie konfigurieren

Gehen Sie wie folgt vor, um die Wartungsrichtlinie zu konfigurieren:

1. Ändern Sie die Wartungsrichtlinie in den Standardwert.

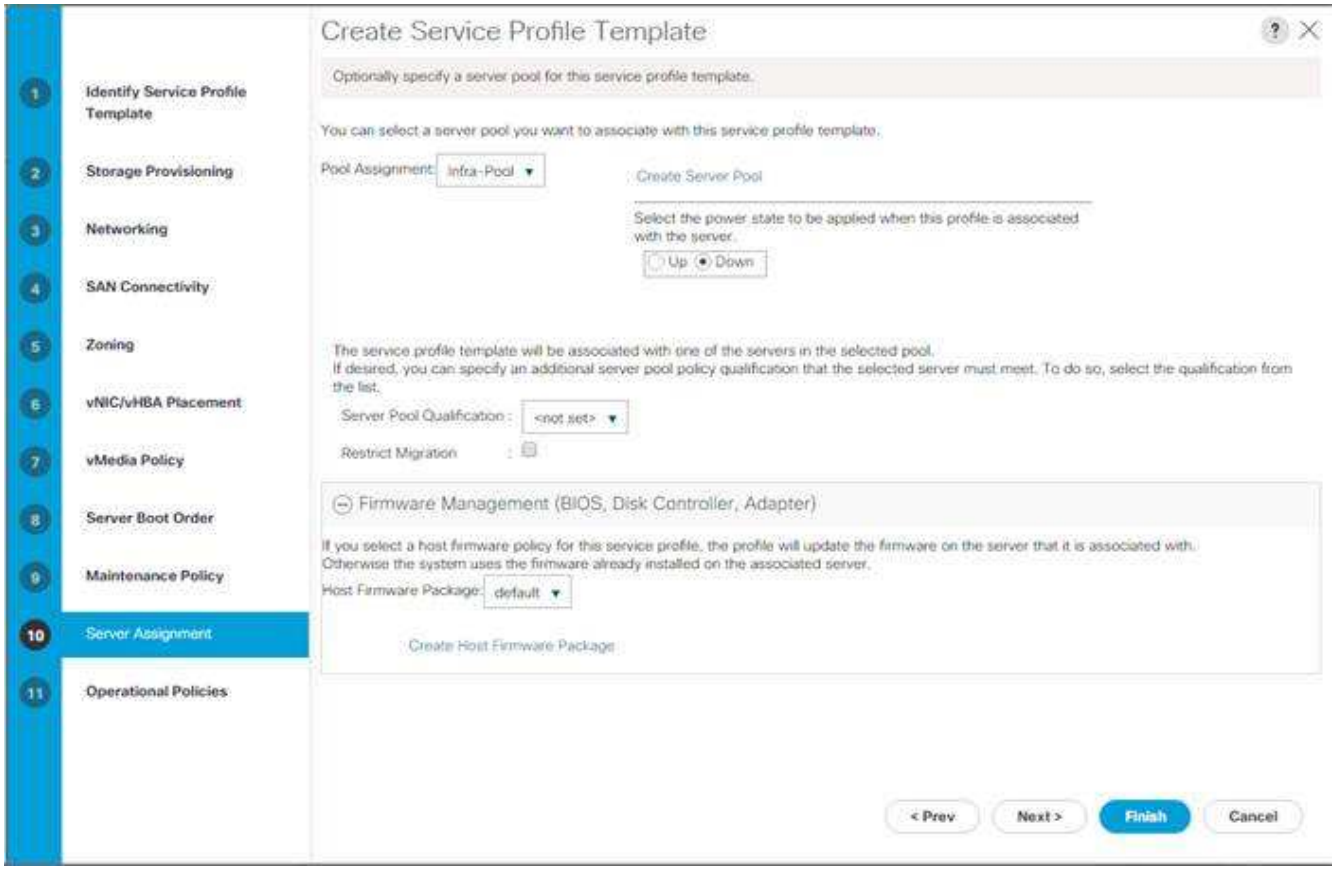


2. Klicken Sie Auf Weiter.

Konfigurieren Sie die Serverzuweisung

Gehen Sie wie folgt vor, um die Serverzuweisung zu konfigurieren:

1. Wählen Sie in der Liste Poolzuweisung die Option Infra-Pool aus.
2. Wählen Sie nach unten als Betriebszustand aus, der angewendet werden soll, wenn das Profil mit dem Server verknüpft ist.
3. Erweitern Sie die Firmware-Verwaltung unten auf der Seite und wählen Sie die Standardrichtlinie aus.

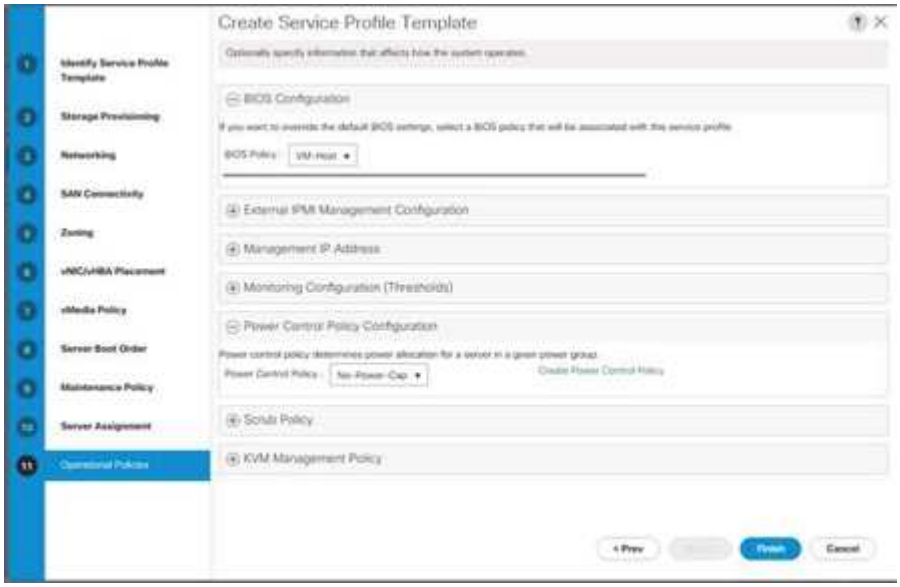


4. Klicken Sie Auf Weiter.

Konfiguration von Betriebsrichtlinien

Gehen Sie wie folgt vor, um die Betriebsrichtlinien zu konfigurieren:

1. Wählen Sie aus der Dropdown-Liste BIOS-Richtlinie VM-Host aus.
2. Erweitern Sie die Konfiguration der Energiesteuerungsrichtlinie, und wählen Sie in der Dropdown-Liste Stromsteuerungsrichtlinie die Option Keine Einschaltgrenze aus.



3. Klicken Sie auf Fertig stellen, um die Service-Profilvorlage zu erstellen.
4. Klicken Sie in der Bestätigungsmeldung auf OK.

VMedia-fähige Service-Profilvorlage erstellen

Gehen Sie wie folgt vor, um eine Service-Profilvorlage zu erstellen, bei der vMedia aktiviert ist:

1. Stellen Sie eine Verbindung zum UCS Manager her, und klicken Sie links auf Server.
2. Wählen Sie Service Profile Templates > root > Service Template VM-Host-Infra-iSCSI-A.
3. Klicken Sie mit der rechten Maustaste auf VM-Host-Infra-iSCSI-A, und wählen Sie Create a Clone aus.
4. Benennen Sie den Klon `VM-Host-Infra-iSCSI-A-vM`.
5. Wählen Sie die neu erstellte VM-Host-Infra-iSCSI-A-VM aus, und wählen Sie rechts die Registerkarte vMedia Policy aus.
6. Klicken Sie auf vMedia Policy ändern.
7. Wählen Sie ESXi-6 aus. 7U1-HTTP vMedia Policy und klicken Sie auf OK.
8. Klicken Sie zur Bestätigung auf OK.

Erstellen von Serviceprofilen

Um Service-Profile aus der Vorlage für Service-Profile zu erstellen, gehen Sie wie folgt vor:

1. Stellen Sie eine Verbindung zum Cisco UCS Manager her, und klicken Sie links auf Server.
2. Erweitern Sie Server > Service Profile Templates > Root > Service Template <Name>.
3. Klicken Sie in Aktionen auf Service-Profil aus Vorlage erstellen und konkurrieren Sie mit den folgenden Schritten:
   a. Eingabe `Site- 01-Infra-0` Als Namenspräfix.
   b. Eingabe `2` Als Anzahl der zu erstellenden Instanzen.
   c. Wählen Sie root als Organisation aus.
   d. Klicken Sie auf OK, um die Serviceprofile zu erstellen.

4. Klicken Sie in der Bestätigungsmeldung auf OK.

5. Überprüfen Sie die Serviceprofile `Site-01-Infra-01` Und `Site-01-Infra-02` Wurden erstellt.

> Die Serviceprofile werden automatisch den Servern in ihren zugewiesenen Serverpools zugeordnet.

Storage-Konfiguration Teil 2: Boot-LUNs und Initiatorgruppen

Einrichtung von ONTAP Boot Storage

Erstellen von Initiatorgruppen

Führen Sie die folgenden Schritte aus, um Initiatorgruppen zu erstellen:

1. Führen Sie die folgenden Befehle über die SSH-Verbindung des Cluster-Managementknoten aus:

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-01-iqn>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-02-iqn>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi
–ostype vmware –initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

> Verwenden Sie die in Tabelle 1 und Tabelle 2 aufgeführten Werte für die IQN-Informationen.

2. Um die drei gerade erstellten Initiatorgruppen anzuzeigen, führen Sie den aus `igroup show` Befehl.

Zuordnen von Boot-LUNs zu Initiatorgruppen

Führen Sie den folgenden Schritt aus, um Boot-LUNs Initiatorgruppen zuzuordnen:

1. Führen Sie über die SSH-Verbindung für das Storage-Cluster-Management die folgenden Befehle aus:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A
–igroup VM-Host-Infra-01 –lun-id 0lun map –vserver Infra-SVM –volume
esxi_boot –lun VM-Host-Infra- B –igroup VM-Host-Infra-02 –lun-id 0
```

Implementierungsverfahren für VMware vSphere 6.7U1

In diesem Abschnitt werden ausführliche Verfahren zum Installieren von VMware ESXi 6.7U1 in einer FlexPod Express Konfiguration beschrieben. Nach Abschluss der Verfahren werden zwei gestartete ESXi-Hosts bereitgestellt.

Für die Installation von ESXi in einer VMware-Umgebung sind mehrere Methoden vorhanden. Diese Verfahren konzentrieren sich darauf, wie die integrierte KVM-Konsole und die Funktionen für virtuelle Medien im Cisco UCS Manager verwendet werden, um Remote-Installationsmedien einzelnen Servern zuzuordnen und eine Verbindung zu ihren Boot-LUNs herzustellen.

Laden Sie das individuelle Cisco Image für ESXi 6.7U1 herunter

Wenn das benutzerdefinierte VMware ESXi Image nicht heruntergeladen wurde, führen Sie die folgenden Schritte aus, um den Download abzuschließen:

1. Klicken Sie auf den folgenden Link: VMware vSphere Hypervisor (ESXi) 6.7U1.
2. Sie benötigen eine Benutzer-ID und ein Passwort für "VMware.com" Um diese Software herunterzuladen.
3. Laden Sie die herunter `.iso` Datei:

Cisco UCS Manager

Das Cisco UCS IP KVM ermöglicht es dem Administrator, die Installation des Betriebssystems über Remote-Medien zu starten. Es ist erforderlich, sich in der Cisco UCS-Umgebung anzumelden, um IP KVM auszuführen.

So melden Sie sich in der Cisco UCS-Umgebung an:

1. Öffnen Sie einen Webbrowser, und geben Sie die IP-Adresse für die Cisco UCS-Cluster-Adresse ein. In diesem Schritt wird die Cisco UCS Manager-Applikation gestartet.
2. Klicken Sie auf den Link UCS Manager starten unter HTML, um die HTML 5 UCS Manager GUI zu starten.
3. Wenn Sie aufgefordert werden, Sicherheitszertifikate anzunehmen, akzeptieren Sie diese bei Bedarf.
4. Geben Sie bei der entsprechenden Aufforderung ein `admin` Geben Sie als Benutzername das Administratorpasswort ein.
5. Um sich bei Cisco UCS Manager anzumelden, klicken Sie auf Anmelden.
6. Klicken Sie im Hauptmenü auf Server auf der linken Seite.
7. Wählen Sie Server > Service-Profile > root > aus `VM-Host-Infra-01`.
8. Mit der rechten Maustaste klicken `VM-Host-Infra-01` Und wählen Sie KVM-Konsole aus.
9. Befolgen Sie die Anweisungen, um die Java-basierte KVM-Konsole zu starten.
10. Wählen Sie Server > Service-Profile > root > aus `VM-Host-Infra-02`.
11. Mit der rechten Maustaste klicken `VM-Host-Infra-02`. Und wählen Sie KVM-Konsole aus.
12. Befolgen Sie die Anweisungen, um die Java-basierte KVM-Konsole zu starten.

Einrichtung der VMware ESXi-Installation

ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

Um den Server für die Betriebssysteminstallation vorzubereiten, führen Sie die folgenden Schritte auf jedem ESXi-Host durch:

1. Klicken Sie im KVM-Fenster auf Virtueller Datenträger.
2. Klicken Sie Auf Virtuelle Geräte Aktivieren.
3. Wenn Sie aufgefordert werden, eine unverschlüsselte KVM-Sitzung anzunehmen, akzeptieren Sie diese bei Bedarf.
4. Klicken Sie auf Virtueller Datenträger und wählen Sie Karte CD/DVD.
5. Navigieren Sie zur ISO-Image-Datei des ESXi Installers, und klicken Sie auf Öffnen.
6. Klicken Sie Auf Kartengerät.

7. Klicken Sie auf die Registerkarte KVM, um den Serverstart zu überwachen.

ESXi installieren

ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

So installieren Sie VMware ESXi auf der iSCSI-bootfähigen LUN der Hosts, gehen Sie auf jedem Host wie folgt vor:

1. Starten Sie den Server, indem Sie Boot Server auswählen und auf OK klicken. Klicken Sie anschließend erneut auf OK.
2. Beim Neustart erkennt das System das Vorhandensein des ESXi-Installationsmediums. Wählen Sie das ESXi-Installationsprogramm aus dem Startmenü aus, das angezeigt wird.
3. Drücken Sie nach dem Laden des Installers die Eingabetaste, um mit der Installation fortzufahren.
4. Lesen und akzeptieren Sie die Endbenutzer-Lizenzvereinbarung (EULA). Drücken Sie F11, um zu akzeptieren und fortzufahren.
5. Wählen Sie die LUN aus, die zuvor als Installationsfestplatte für ESXi eingerichtet wurde, und drücken Sie die Eingabetaste, um mit der Installation fortzufahren.
6. Wählen Sie das entsprechende Tastaturlayout aus, und drücken Sie die Eingabetaste.
7. Geben Sie das Root-Passwort ein und bestätigen Sie es, und drücken Sie die Eingabetaste.
8. Das Installationsprogramm gibt eine Warnung aus, dass das ausgewählte Laufwerk neu partitioniert wird. Drücken Sie F11, um mit der Installation fortzufahren.
9. Wählen Sie nach Abschluss der Installation die Registerkarte Virtueller Datenträger aus, und löschen Sie die P-Markierung neben dem ESXi-Installationsmedium. Klicken Sie Auf Ja.

> Das ESXi-Installationsabbild muss nicht zugeordnet werden, um sicherzustellen, dass der Server in ESXi und nicht in das Installationsprogramm neu gestartet wird.

10. Drücken Sie nach Abschluss der Installation die Eingabetaste, um den Server neu zu starten.
11. Binden Sie im Cisco UCS Manager das aktuelle Service-Profil an die nicht-vMedia-Serviceprofilvorlage, um zu verhindern, dass die ESXi Installations-iso über HTTP gemountet wird.

Einrichten des Managementnetzwerkes für ESXi-Hosts

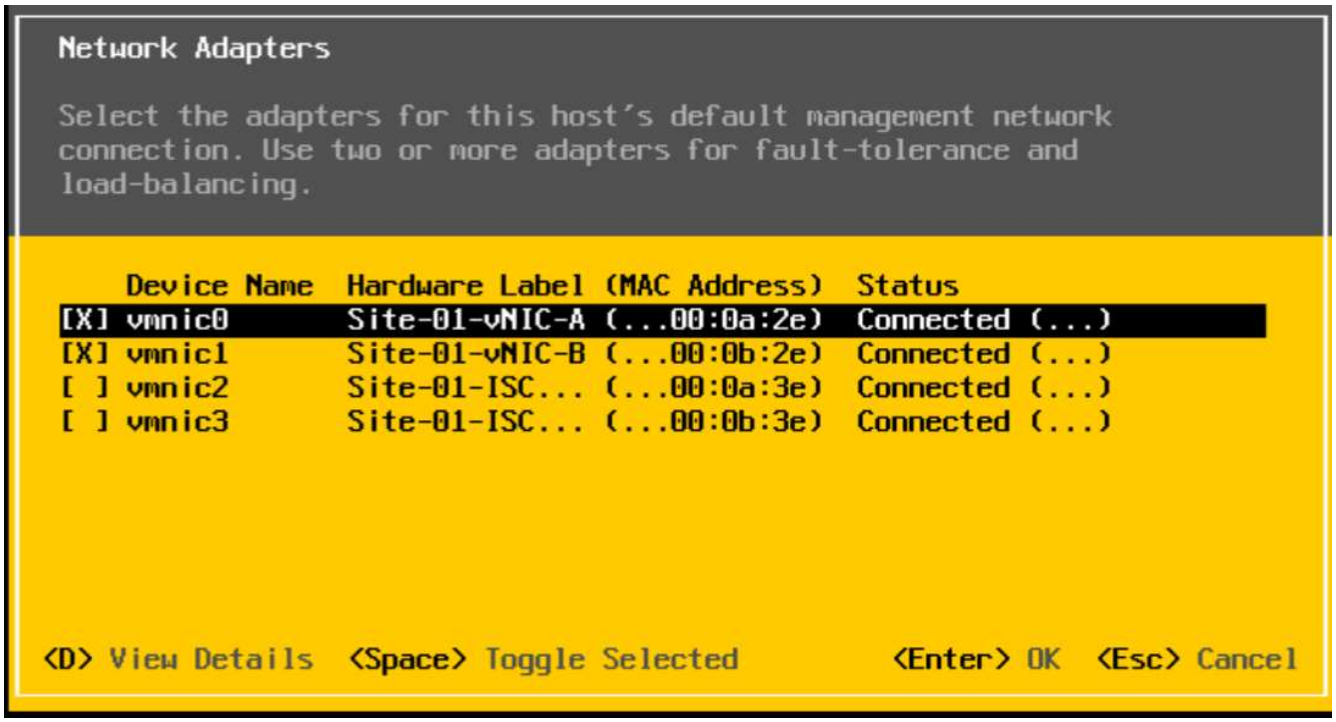
Für jeden VMware Host ist das Hinzufügen eines Managementnetzwerks erforderlich, um den Host zu verwalten. Um ein Management-Netzwerk für die VMware-Hosts hinzuzufügen, führen Sie die folgenden Schritte auf jedem ESXi-Host aus:

ESXi Host VM-Host-Infra-01 und VM-Host-Infra-02

Gehen Sie wie folgt vor, um jeden ESXi-Host mit Zugriff auf das Managementnetzwerk zu konfigurieren:

1. Drücken Sie nach dem Neustart des Servers F2, um das System anzupassen.
2. Melden Sie sich als an `root`Geben Sie das entsprechende Passwort ein, und drücken Sie die Eingabetaste, um sich anzumelden.
3. Wählen Sie Fehlerbehebungsoptionen aus, und drücken Sie die Eingabetaste.
4. Wählen Sie ESXi Shell aktivieren und drücken Sie die Eingabetaste.
5. Wählen Sie SSH aktivieren, und drücken Sie die Eingabetaste.

6. Drücken Sie Esc, um das Menü Fehlerbehebungsoptionen zu verlassen.
7. Wählen Sie die Option Managementnetzwerk konfigurieren, und drücken Sie die Eingabetaste.
8. Wählen Sie Netzwerkadapter aus, und drücken Sie die Eingabetaste.
9. Stellen Sie sicher, dass die Nummern im Feld Hardwarebezeichnung mit den Nummern im Feld Gerätename übereinstimmen.
10. Drücken Sie Die Eingabetaste.



11. Wählen Sie die Option VLAN (Optional) aus, und drücken Sie die Eingabetaste.
12. Geben Sie das ein `<ib-mgmt-vlan-id>` Und drücken Sie die Eingabetaste.
13. Wählen Sie IPv4-Konfiguration aus, und drücken Sie die Eingabetaste.
14. Wählen Sie die Option statische IPv4-Adresse und Netzwerkkonfiguration festlegen, indem Sie die Leertaste verwenden.
15. Geben Sie die IP-Adresse zur Verwaltung des ersten ESXi-Hosts ein.
16. Geben Sie die Subnetzmaske für den ersten ESXi-Host ein.
17. Geben Sie das Standard-Gateway für den ersten ESXi-Host ein.
18. Drücken Sie die Eingabetaste, um die Änderungen an der IP-Konfiguration zu akzeptieren.
19. Wählen Sie die Option DNS-Konfiguration aus, und drücken Sie die Eingabetaste.

> Da die IP-Adresse manuell zugewiesen wird, müssen auch die DNS-Informationen manuell eingegeben werden.

20. Geben Sie die IP-Adresse des primären DNS-Servers ein.
21. Optional: Geben Sie die IP-Adresse des sekundären DNS-Servers ein.
22. Geben Sie den FQDN für den ersten ESXi-Host ein.
23. Drücken Sie die Eingabetaste, um die Änderungen an der DNS-Konfiguration zu akzeptieren.

24. Drücken Sie Esc, um das Menü Verwaltungsnetzwerk konfigurieren zu beenden.
25. Wählen Sie Testmanagement-Netzwerk aus, um zu überprüfen, ob das Verwaltungsnetzwerk ordnungsgemäß eingerichtet ist, und drücken Sie die Eingabetaste.
26. Drücken Sie die Eingabetaste, um den Test auszuführen. Drücken Sie erneut die Eingabetaste, sobald der Test abgeschlossen ist. Überprüfen Sie die Umgebung, wenn ein Fehler auftritt.
27. Wählen Sie erneut das Managementnetzwerk konfigurieren aus, und drücken Sie die Eingabetaste.
28. Wählen Sie die IPv6-Konfigurationsoption aus, und drücken Sie die Eingabetaste.
29. Wählen Sie in der Leertaste IPv6 deaktivieren (Neustart erforderlich), und drücken Sie die Eingabetaste.
30. Drücken Sie Esc, um das Untermenü Verwaltungsnetzwerk konfigurieren zu beenden.
31. Drücken Sie Y, um die Änderungen zu bestätigen und den ESXi-Host neu zu starten.

VMware ESXi Host VMkernel Port vmk0 MAC-Adresse zurücksetzen (optional)

ESXi Host VM-Host-Infra-01 und VM-Host-Infra-02

Die MAC-Adresse des Management-VMkernel-Ports vmk0 ist standardmäßig dieselbe wie die MAC-Adresse des Ethernet-Ports, auf dem er platziert wird. Wenn die Boot-LUN des ESXi-Hosts einem anderen Server mit unterschiedlichen MAC-Adressen neu zugeordnet wird, tritt ein MAC-Adressenkonflikt auf, da vmk0 die zugewiesene MAC-Adresse behält, wenn die ESXi-Systemkonfiguration nicht zurückgesetzt wird. So setzen Sie die MAC-Adresse von vmk0 auf eine zufällige, von VMware zugewiesene MAC-Adresse zurück:

1. Drücken Sie im Hauptmenü der ESXi-Konsole Strg-Alt-F1, um auf die Befehlszeilenoberfläche der VMware-Konsole zuzugreifen. Im UCSM KVM wird in der Liste der statischen Makros Strg-Alt-F1 angezeigt.
2. Melden Sie sich als Root an.
3. Typ `esxcfg-vmknic –l` Um eine detaillierte Liste der Schnittstelle vmk0 zu erhalten. Vmk0 sollte ein Teil der Verwaltungsnetzwerk-Portgruppe sein. Beachten Sie die IP-Adresse und die Netzmaske von vmk0.
4. Geben Sie zum Entfernen von vmk0 den folgenden Befehl ein:

```
esxcfg-vmknic –d “Management Network”
```

5. Um vmk0 erneut mit einer zufälligen MAC-Adresse hinzuzufügen, geben Sie den folgenden Befehl ein:

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. Überprüfen Sie, ob vmk0 mit einer zufälligen MAC-Adresse erneut hinzugefügt wurde

```
esxcfg-vmknic –l
```

7. Typ `exit` So melden Sie sich von der Befehlszeilenschnittstelle ab.
8. Drücken Sie Strg-Alt-F2, um zur Menü-Schnittstelle der ESXi-Konsole zurückzukehren.

Melden Sie sich bei VMware ESXi Hosts mit dem VMware Host-Client an

ESXi Host-VM-Host-Infra-01

So melden Sie sich über den VMware Host-Client am VM-Host-Infra-01 ESXi-Host an:

1. Öffnen Sie einen Webbrowser auf der Management-Workstation, und navigieren Sie zum `VM-Host-Infra-01` Management-IP-Adresse:
2. Klicken Sie auf VMware Host Client öffnen.
3. Eingabe `root` Für den Benutzernamen.
4. Geben Sie das Root-Passwort ein.
5. Klicken Sie auf Anmelden, um die Verbindung herzustellen.
6. Wiederholen Sie diesen Vorgang, um sich bei anzumelden `VM-Host-Infra-02` In einem separaten Browser-Tab oder -Fenster.

Installation von VMware Treibern für die Cisco Virtual Interface Card (VIC)

Laden Sie das Offline Bundle für den folgenden VMware VIC-Treiber für die Management Workstation herunter und extrahieren Sie es.

- Nenic Driver Version 1.0.25.0

ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

So installieren Sie VMware VIC-Treiber auf dem ESXi Host VM-Host-Infra-01 und VM-Host-Infra-02:

1. Wählen Sie auf jedem Host-Client die Option Speicher aus.
2. Klicken Sie mit der rechten Maustaste auf Datenspeicher 1, und wählen Sie Durchsuchen.
3. Klicken Sie im Datastore-Browser auf Hochladen.
4. Navigieren Sie zum gespeicherten Speicherort für die heruntergeladenen VIC-Treiber, und wählen Sie VMW-ESX-6.7.0-nenic-1.0.25.0-offline_Bundle-11271332.zip.
5. Klicken Sie im Datastore-Browser auf Hochladen.
6. Klicken Sie auf Öffnen, um die Datei in Datenspeicher 1 hochzuladen.
7. Stellen Sie sicher, dass die Datei auf beide ESXi Hosts hochgeladen wurde.
8. Setzen Sie jeden Host in den Wartungsmodus, wenn er nicht bereits vorhanden ist.
9. Verbinden Sie sich über SSH mit jedem ESXi Host über eine Shell-Verbindung oder ein Putty-Terminal.
10. Melden Sie sich als root mit dem Root-Passwort an.
11. Führen Sie auf jedem Host folgende Befehle aus:

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. Melden Sie sich auf jedem Host beim Host-Client an, sobald der Neustart abgeschlossen ist, und beenden Sie den Wartungsmodus.

Einrichten der VMkernel-Ports und des virtuellen Switches

ESXi Host VM-Host-Infra-01 und VM-Host-Infra-02

Um die VMkernel-Ports und die virtuellen Switches auf den ESXi-Hosts einzurichten, gehen Sie wie folgt vor:

1. Wählen Sie auf dem Host-Client links die Option Netzwerk.
2. Wählen Sie im mittleren Fensterbereich die Registerkarte Virtuelle Switches aus.
3. Wählen Sie vSwitch0 aus.
4. Wählen Sie Einstellungen bearbeiten aus.
5. Ändern Sie die MTU in 9000.
6. Erweitern Sie NIC Teaming.
7. Wählen Sie im Abschnitt Failover-Reihenfolge vmnic1 aus, und klicken Sie auf aktiv markieren.
8. Stellen Sie sicher, dass vmnic1 jetzt den Status „aktiv“ aufweist.
9. Klicken Sie auf Speichern .
10. Wählen Sie links die Option Netzwerk.
11. Wählen Sie im mittleren Fensterbereich die Registerkarte Virtuelle Switches aus.
12. Wählen Sie iScsiBootvSwitch aus.
13. Wählen Sie Einstellungen bearbeiten aus.
14. Ändern Sie die MTU in 9000
15. Klicken Sie auf Speichern .
16. Wählen Sie die Registerkarte VMkernel NICs aus.
17. Wählen Sie vmk1 iScsiBootPG.
18. Wählen Sie Einstellungen bearbeiten aus.
19. Ändern Sie die MTU in 9000.
20. Erweitern Sie IPv4-Einstellungen und ändern Sie die IP-Adresse in eine Adresse außerhalb des UCS iSCSI-IP-Pool-A

> Um IP-Adressenkonflikte zu vermeiden, wenn die Cisco UCS iSCSI IP-Pool-Adressen neu zugewiesen werden sollen, wird empfohlen, für die iSCSI VMkernel-Ports unterschiedliche IP-Adressen im gleichen Subnetz zu verwenden.

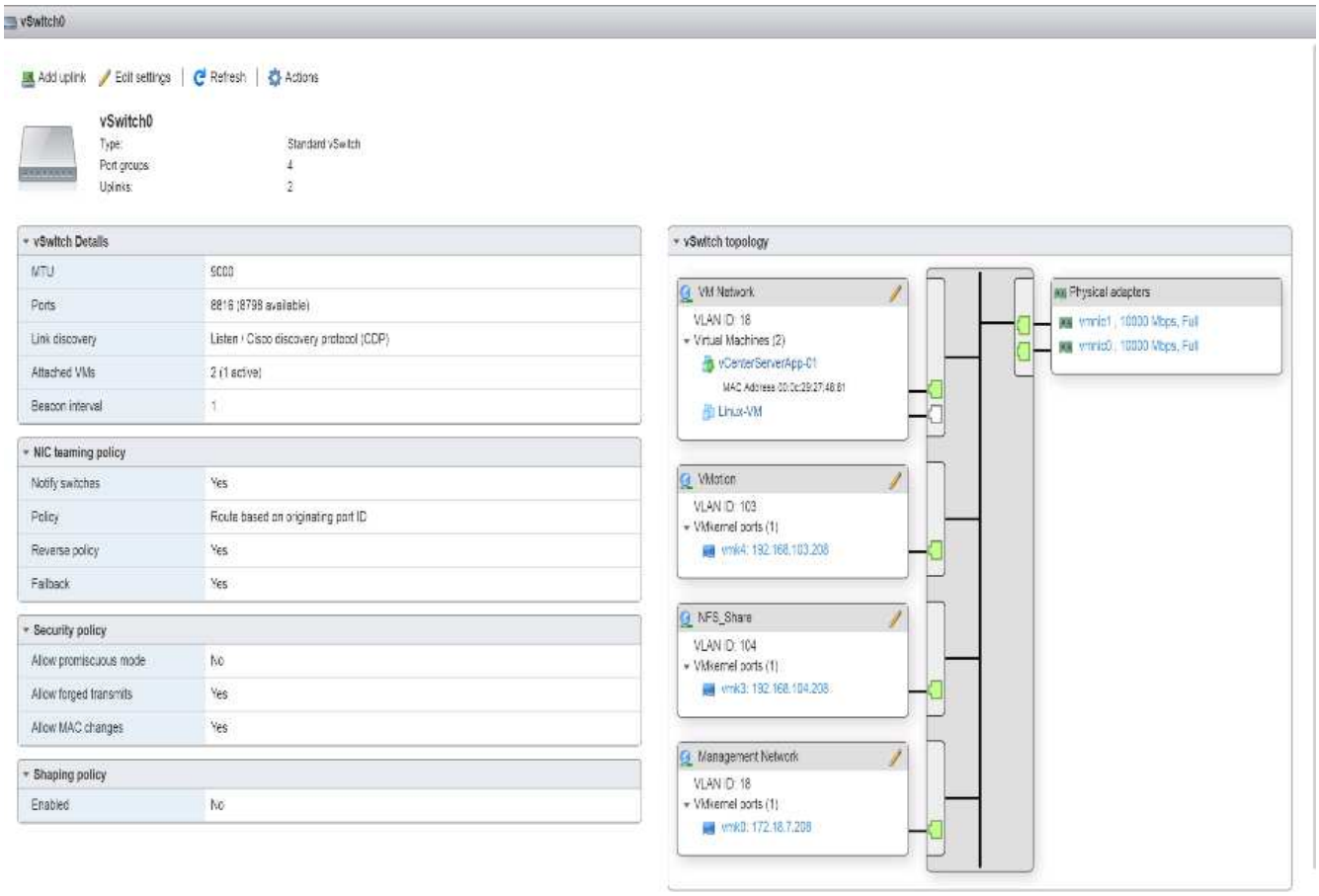
21. Klicken Sie auf Speichern .
22. Wählen Sie die Registerkarte Virtuelle Switches aus.
23. Wählen Sie den virtuellen Standard-Switch hinzufügen aus.
24. Geben Sie einen Namen von an `iScsciBootvSwitch-B` Für den vSwitch-Namen.
25. Setzen Sie die MTU auf 9000.
26. Wählen Sie vmnic3 aus dem Dropdown-Menü Uplink 1.
27. Klicken Sie Auf Hinzufügen.
28. Wählen Sie im mittleren Fensterbereich die Registerkarte VMkernel NICs aus.
29. Wählen Sie VMkernel NIC hinzufügen aus

30. Geben Sie einen neuen Portgruppennamen von iScsiBootPG-B an
31. Wählen Sie iScciBootvSwitch-B für virtuellen Switch aus.
32. Setzen Sie die MTU auf 9000. Geben Sie keine VLAN-ID ein.
33. Wählen Sie statisch für die IPv4-Einstellungen aus, und erweitern Sie die Option, um die Adresse und die Subnetzmaske in der Konfiguration bereitzustellen.

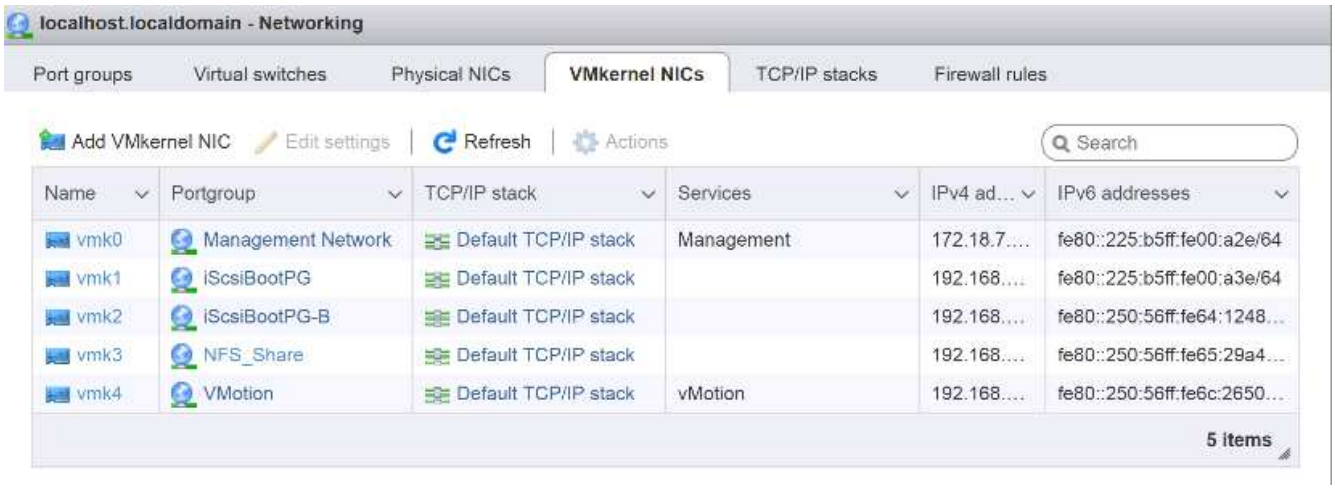
> Um IP-Adressenkonflikte zu vermeiden, sollten die Cisco UCS iSCSI IP-Pool-Adressen neu zugewiesen werden, wird empfohlen, für die iSCSI VMkernel-Ports unterschiedliche IP-Adressen im gleichen Subnetz zu verwenden.

34. Klicken Sie auf Erstellen .
35. Wählen Sie auf der linken Seite Netzwerk und dann die Registerkarte Portgruppen aus.
36. Klicken Sie im mittleren Fensterbereich mit der rechten Maustaste auf VM Network, und wählen Sie Entfernen.
37. Klicken Sie auf Entfernen, um das Entfernen der Portgruppe abzuschließen.
38. Wählen Sie im mittleren Fensterbereich Port-Gruppe hinzufügen aus.
39. Geben Sie einen Namen für das Management-Netzwerk der Portgruppe ein, und geben Sie ein `<ib-mgmt-vlan-id>` Stellen Sie im Feld VLAN ID sicher, dass der virtuelle Switch vSwitch0 ausgewählt ist.
40. Klicken Sie auf Hinzufügen, um die Änderungen für das IB-MGMT-Netzwerk abzuschließen.
41. Wählen Sie oben die Registerkarte für VMkernel NICs aus.
42. Klicken Sie auf VMkernel NIC hinzufügen.
43. Geben Sie für neue Portgruppe VMotion ein.
44. Wählen Sie für virtuellen Switch vSwitch0 ausgewählt aus.
45. Eingabe `<vmotion-vlan-id>` Für die VLAN-ID.
46. Ändern Sie die MTU in 9000.
47. Wählen Sie statische IPv4-Einstellungen und erweitern Sie IPv4-Einstellungen.
48. Geben Sie die IP-Adresse und die Netmask für ESXi Host vMotion ein.
49. Wählen Sie den vMotion Stack TCP/IP-Stack aus.
50. Wählen Sie vMotion unter Services aus.
51. Klicken Sie auf Erstellen .
52. Klicken Sie auf VMkernel NIC hinzufügen.
53. Geben Sie für neue Portgruppe NFS_Share ein.
54. Wählen Sie für virtuellen Switch vSwitch0 ausgewählt aus.
55. Eingabe `<infra-nfs-vlan-id>` Für die VLAN-ID
56. Ändern Sie die MTU in 9000.
57. Wählen Sie statische IPv4-Einstellungen und erweitern Sie IPv4-Einstellungen.
58. Geben Sie die NFS-IP-Adresse und die Netzmaske der ESXi-Hostinfrastruktur ein.
59. Wählen Sie keine der Services aus.
60. Klicken Sie auf Erstellen .

61. Wählen Sie die Registerkarte Virtuelle Switches aus, und wählen Sie dann vSwitch0 aus. Die Eigenschaften für vSwitch0 VMkernel NICs sollten dem folgenden Beispiel ähnlich sein:



62. Wählen Sie die Registerkarte VMkernel NICs aus, um die konfigurierten virtuellen Adapter zu bestätigen. Die aufgeführten Adapter sollten dem folgenden Beispiel ähnlich sein:

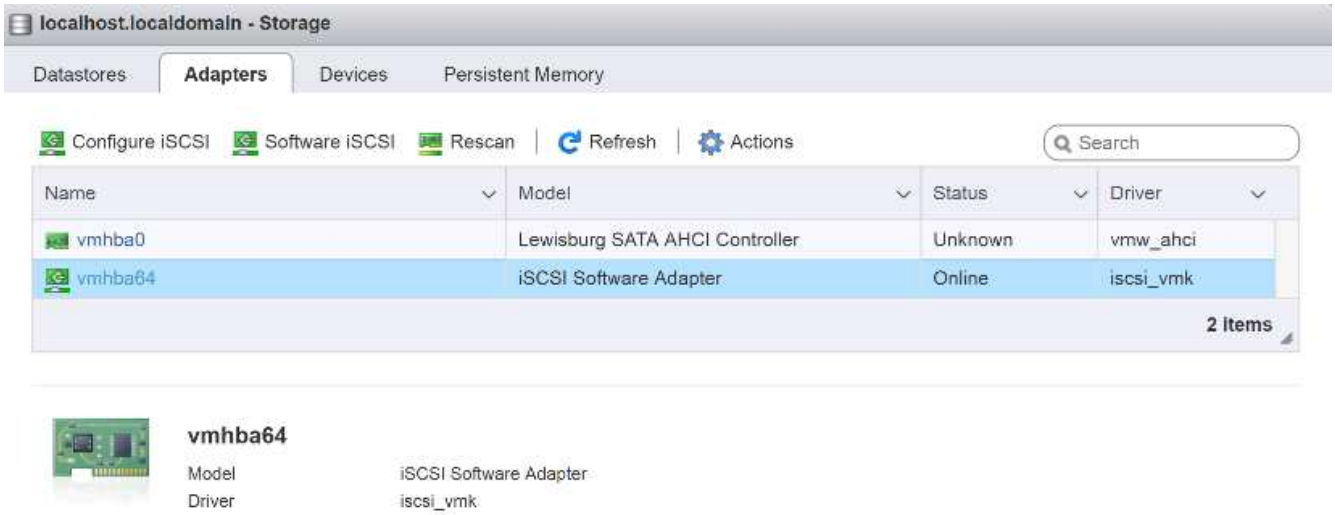


ISCSI-Multipathing einrichten

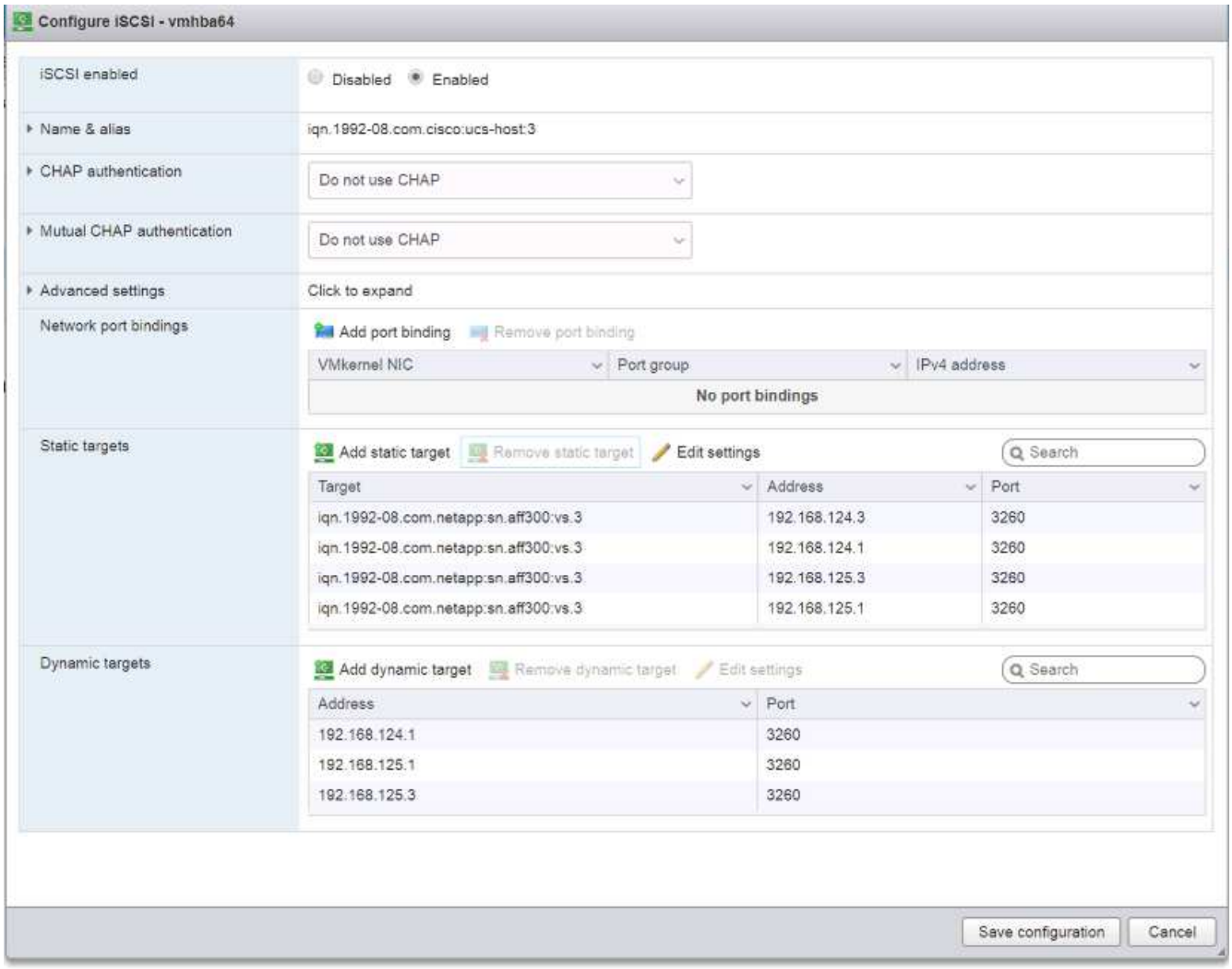
ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

So richten Sie iSCSI-Multipathing auf den ESXi-Host-VM-Host-Infra-01 und VM-Host-Infra-02 ein:

1. Wählen Sie auf jedem Host-Client links die Option Speicher aus.
2. Klicken Sie im mittleren Fensterbereich auf Adapter.
3. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf iSCSI konfigurieren.



4. Klicken Sie unter dynamische Ziele auf dynamische Ziele hinzufügen.
5. Geben Sie die IP-Adresse von ein `iSCSI_lif01a`.
6. Wiederholen Sie die Eingabe dieser IP-Adressen: `iscsi_lif01b`, `iscsi_lif02a`, und `iscsi_lif02b`.
7. Klicken Sie Auf Konfiguration Speichern.



Um alle zu erhalten `iscsi_lif` IP-Adressen: Melden Sie sich bei der NetApp Storage Cluster Managementoberfläche an, und führen Sie den aus `network interface show` Befehl.

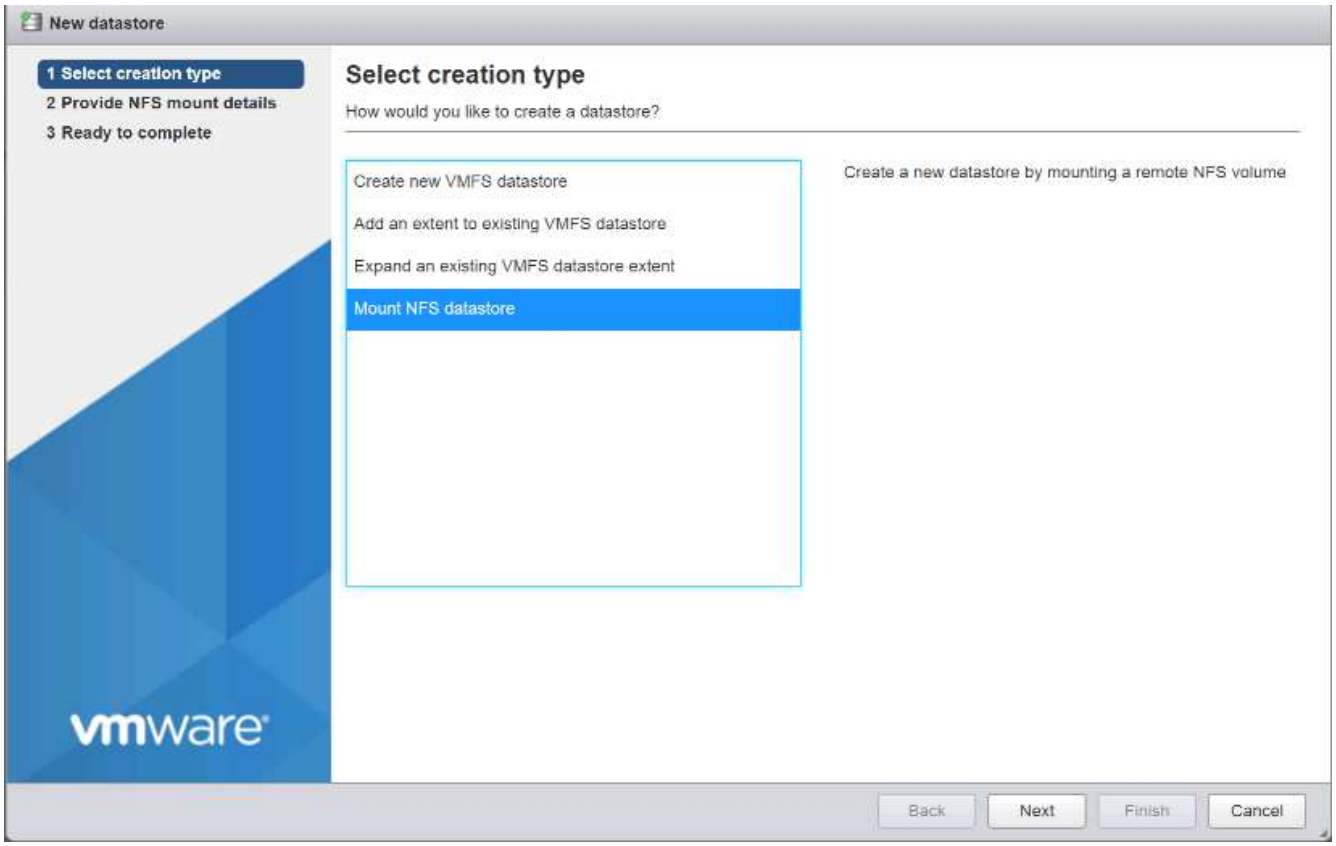
Der Host liest den Speicheradapter automatisch wieder ein, und die Ziele werden statischen Zielen hinzugefügt.

Bereitstellung erforderlicher Datastores

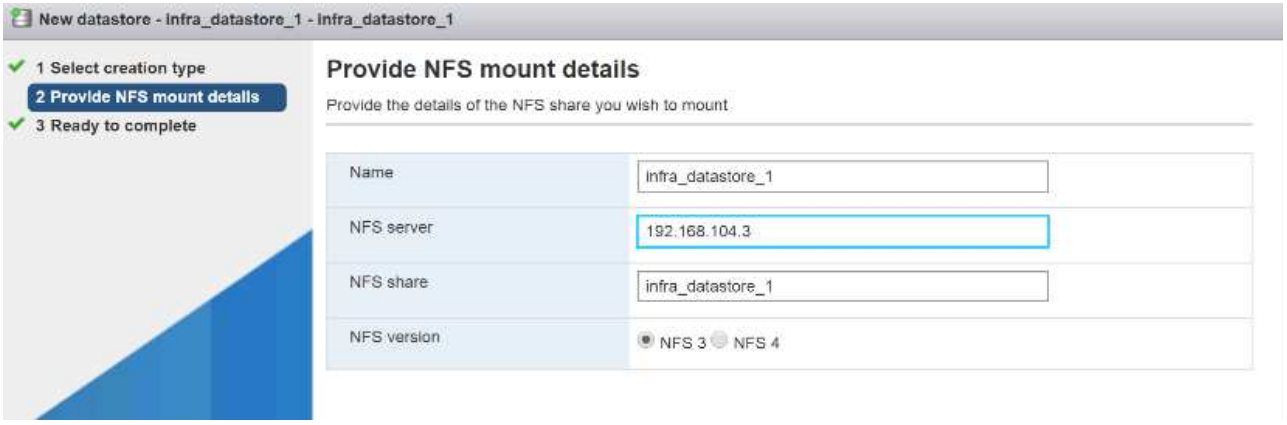
ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

Um die erforderlichen Datastores zu mounten, führen Sie die folgenden Schritte auf jedem ESXi Host aus:

1. Wählen Sie im Host-Client links die Option Speicher aus.
2. Wählen Sie im mittleren Fensterbereich Datenspeicher aus.
3. Wählen Sie im mittleren Fensterbereich New Datastore aus, um einen neuen Datenspeicher hinzuzufügen.
4. Wählen Sie im Dialogfeld Neuer Datastore die Option Mount NFS Datastore aus, und klicken Sie auf Next.

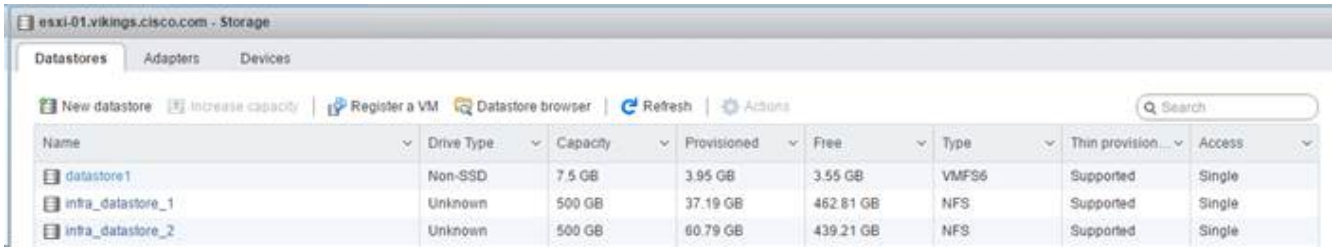


5. Führen Sie auf der Seite „NFS Mount Details angeben“ die folgenden Schritte aus:
   a. Eingabe `infra_datastore_1` Für den Namen des Datenspeichers.
   b. Geben Sie die IP-Adresse für das ein `nfs_lif01_a` LIF für den NFS-Server:
   c. Eingabe `/infra_datastore_1` Für den NFS-Share.
   d. NFS-Version auf NFS 3 einstellen.
   e. Klicken Sie Auf Weiter.



6. Klicken Sie Auf Fertig Stellen. Der Datastore sollte nun in der Datastore-Liste angezeigt werden.
7. Wählen Sie im mittleren Fensterbereich New Datastore aus, um einen neuen Datenspeicher hinzuzufügen.
8. Wählen Sie im Dialogfeld Neuer Datastore die Option Mount NFS Datastore aus, und klicken Sie auf Weiter.

9. Führen Sie auf der Seite „NFS Mount Details angeben“ die folgenden Schritte aus:
    a. Eingabe `infra_datastore_2` Für den Namen des Datenspeichers.
    b. Geben Sie die IP-Adresse für das ein `nfs_lif02_a` LIF für den NFS-Server:
    c. Eingabe `/infra_datastore_2` Für den NFS-Share.
    d. NFS-Version auf NFS 3 einstellen.
    e. Klicken Sie Auf Weiter.
10. Klicken Sie Auf Fertig Stellen. Der Datastore sollte nun in der Datastore-Liste angezeigt werden.



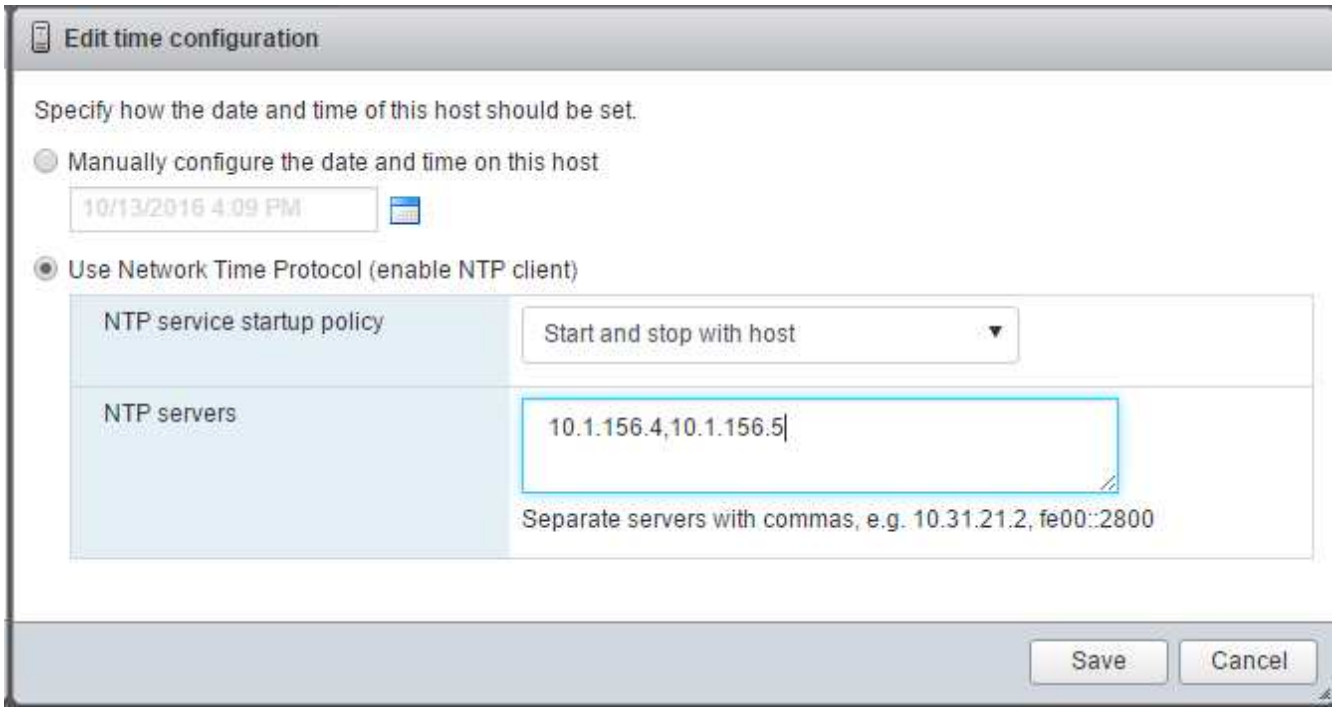
11. Mounten Sie beide Datenspeicher auf beiden ESXi Hosts.

Konfigurieren Sie NTP auf ESXi Hosts

ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

Gehen Sie auf jedem Host wie folgt vor, um NTP auf den ESXi-Hosts zu konfigurieren:

1. Wählen Sie im Host-Client links die Option Verwalten aus.
2. Wählen Sie im mittleren Fensterbereich die Registerkarte Uhrzeit und Datum aus.
3. Klicken Sie Auf Einstellungen Bearbeiten.
4. Stellen Sie sicher, dass das Network Time Protocol (NTP-Client aktivieren) ausgewählt ist.
5. Wählen Sie im Dropdown-Menü Start und Stopp mit Host aus.
6. Geben Sie die beiden Nexus-Switch-NTP-Adressen in das durch Komma getrennte NTP-Server-Feld ein.



7. Klicken Sie auf Speichern, um die Konfigurationsänderungen zu speichern.
8. Wählen Sie Actions > NTP Service > Start aus.
9. Überprüfen Sie, ob der NTP-Dienst jetzt ausgeführt wird und die Uhr jetzt auf ungefähr die richtige Zeit eingestellt ist

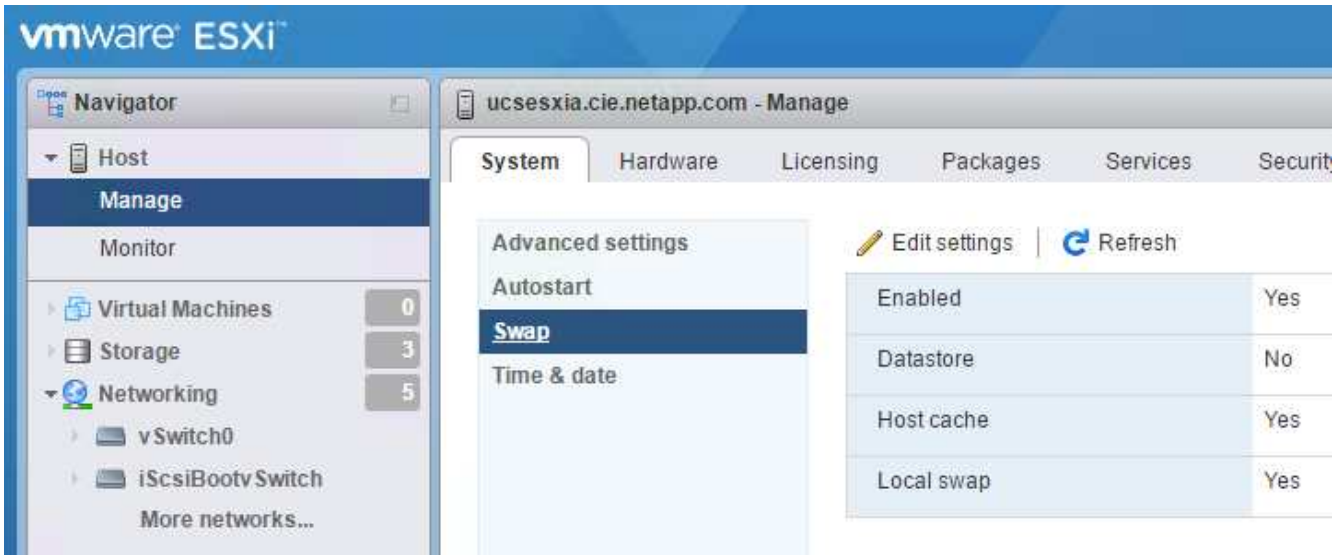
Die NTP-Serverzeit kann von der Hostzeit leicht abweichen.

Konfiguration des ESXi Host-Auslagerungaus

ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

Führen Sie die folgenden Schritte auf jedem Host aus, um den Host-Swap auf den ESXi Hosts zu konfigurieren:

1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich die Option System aus, und klicken Sie auf Tausch.



2. Klicken Sie Auf Einstellungen Bearbeiten. Wählen Sie `infra_swap` In den Datastore-Optionen.

3. Klicken Sie auf Speichern .

Installieren Sie das NetApp NFS Plug-in 1.1.2 für VMware VAAI

Um das NetApp NFS-Plug-in 1 zu installieren. 1.2 für VMware VAAI, führen Sie die folgenden Schritte aus.

1. Laden Sie das NetApp NFS Plug-in für VMware VAAI herunter:
   a. Wechseln Sie zum "NetApp Software Download-Seite".
   b. Scrollen Sie nach unten und klicken Sie auf NetApp NFS Plug-in for VMware VAAI.
   c. Wählen Sie die ESXi-Plattform aus.
   d. Laden Sie entweder das Offline-Bundle (.zip) oder das Online-Bundle (.vib) des neuesten Plug-ins herunter.
2. Das NetApp NFS Plug-in für VMware VAAI steht an der IMT-Qualifizierung mit ONTAP 9.5 aus. Einzelheiten zur Interoperabilität werden bald beim NetApp IMT veröffentlicht.
3. Installieren Sie das Plug-in auf dem ESXi Host mithilfe der ESX CLI.
4. STARTEN Sie DEN ESXI-Host neu.

Installieren Sie VMware vCenter Server 6.7

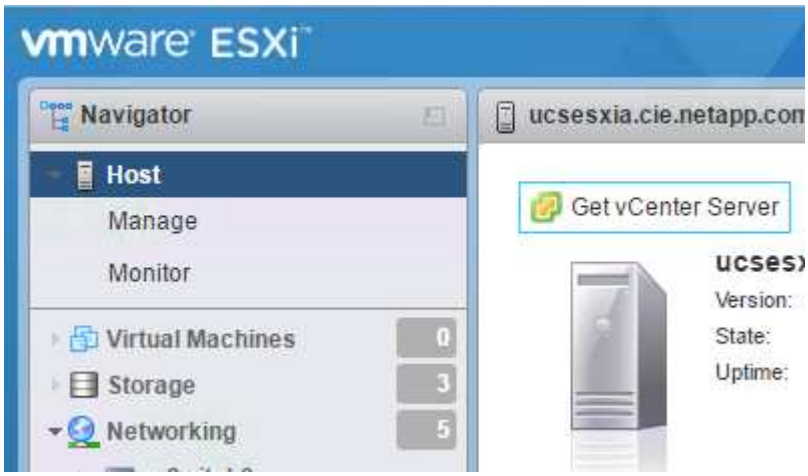
Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware vCenter Server 6.7 in einer FlexPod Express-Konfiguration.

FlexPod Express verwendet die VMware vCenter Server Appliance (VCSA).

Installieren Sie die VMware vCenter Server Appliance

Gehen Sie wie folgt vor, um VCSA zu installieren:

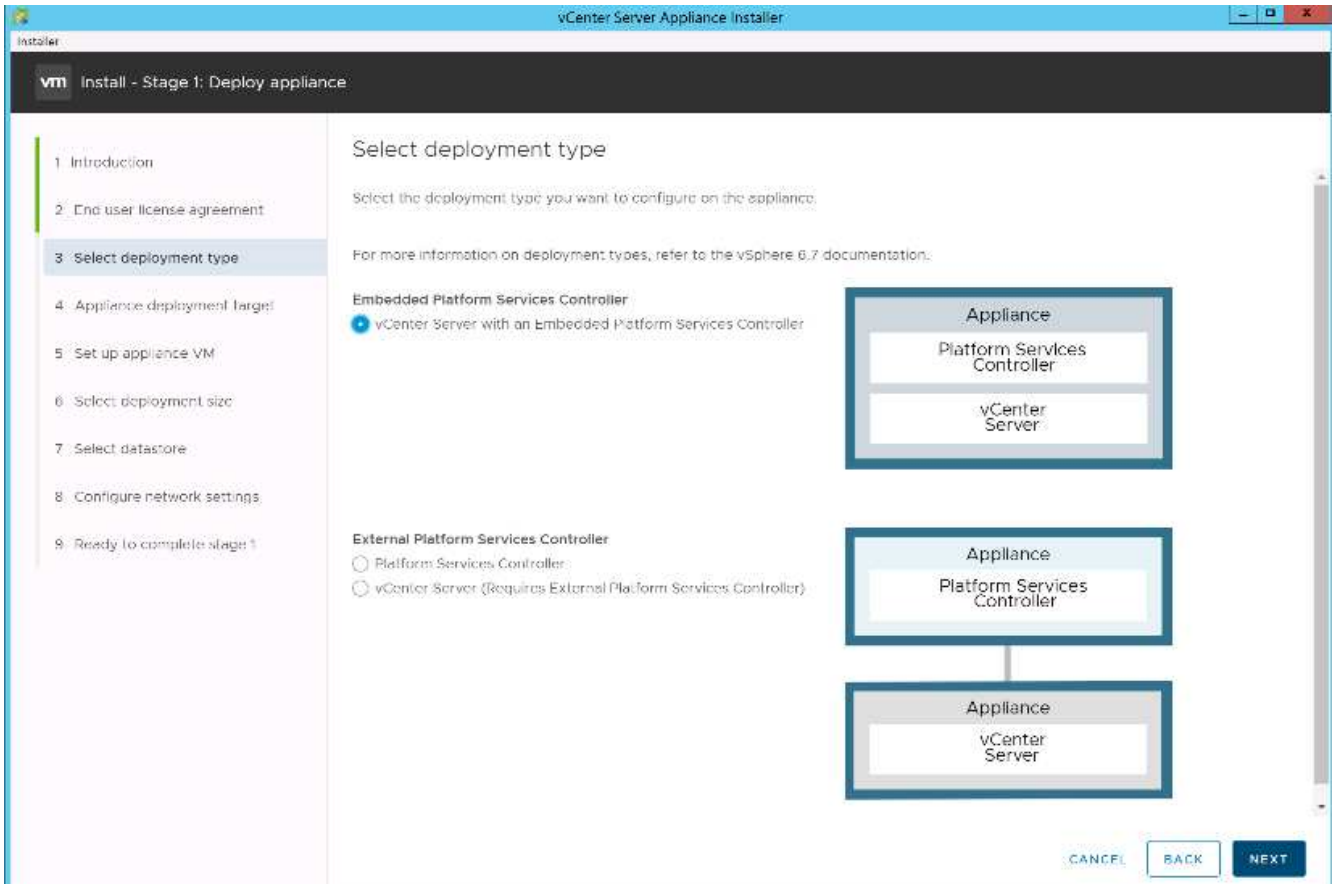
1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.



2. Laden Sie die VCSA von der VMware-Website herunter.

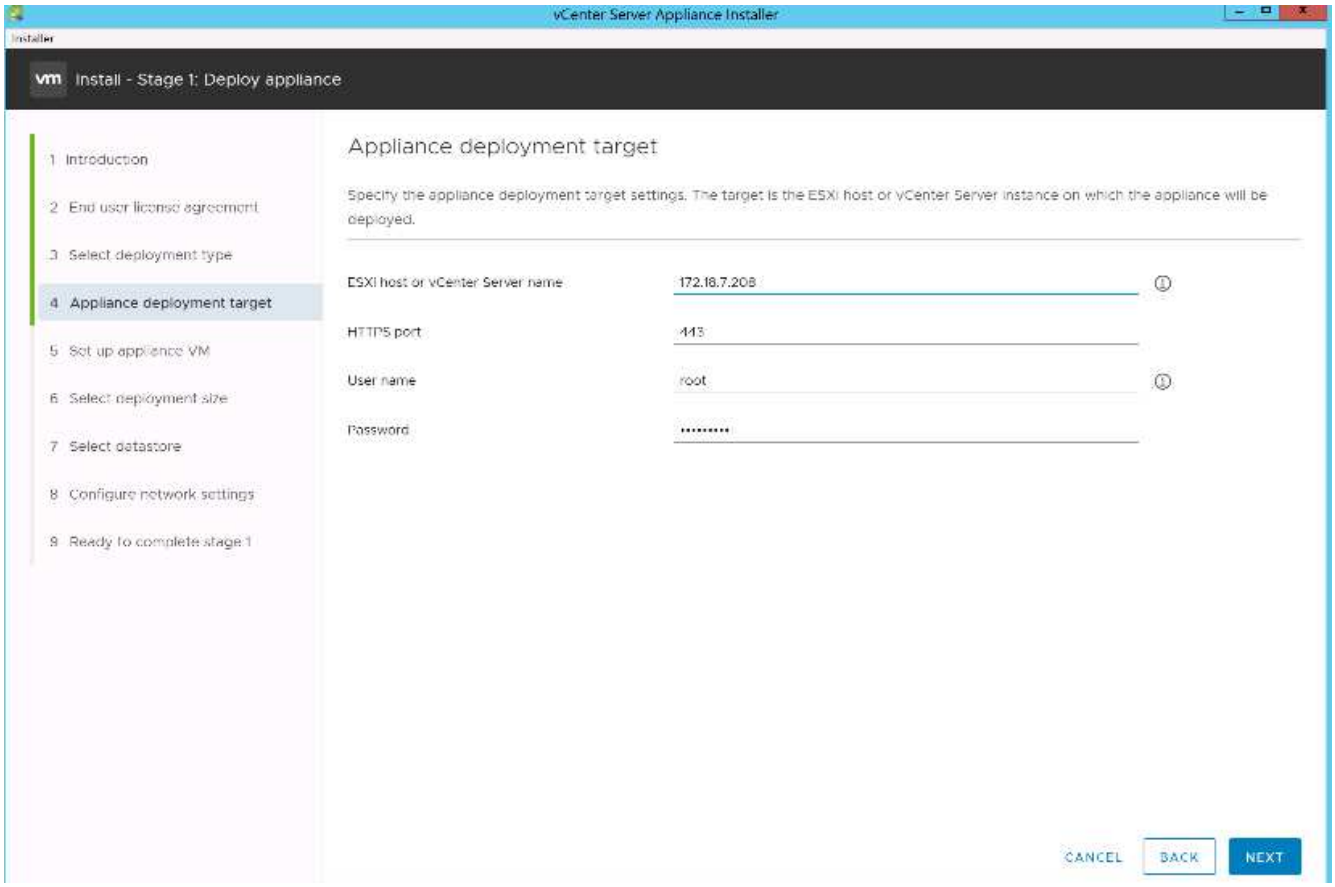
Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.

3. Mounten Sie das ISO-Image.
4. Navigieren Sie zum `vcsa-ui-installer` > `win32` Verzeichnis. Doppelklicken `installer.exe`.
5. Klicken Sie Auf Installieren.
6. Klicken Sie auf der Seite Einführung auf Weiter.
7. Akzeptieren Sie die EULA.
8. Wählen Sie als Bereitstellungstyp den Embedded Platform Services Controller aus.

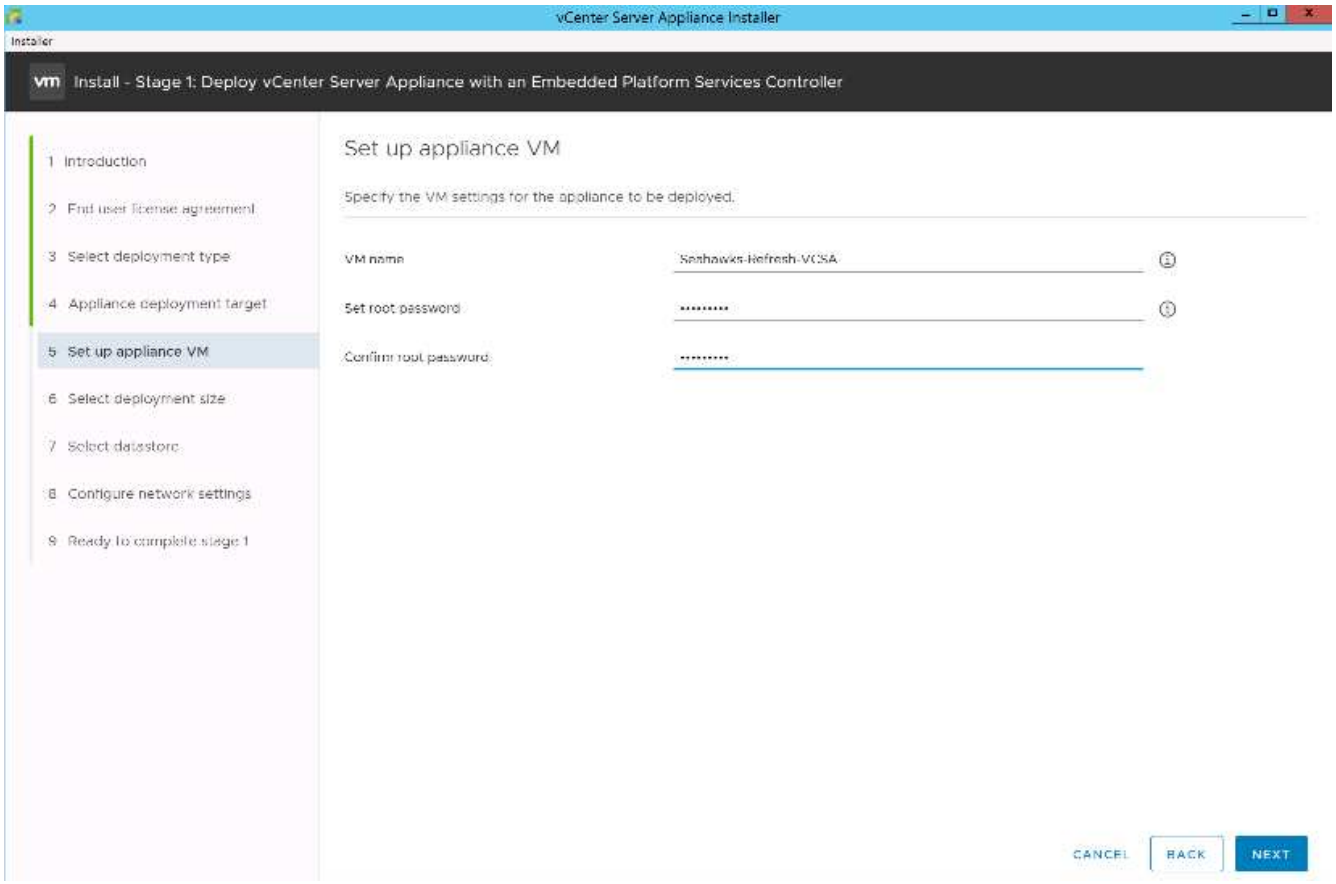


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

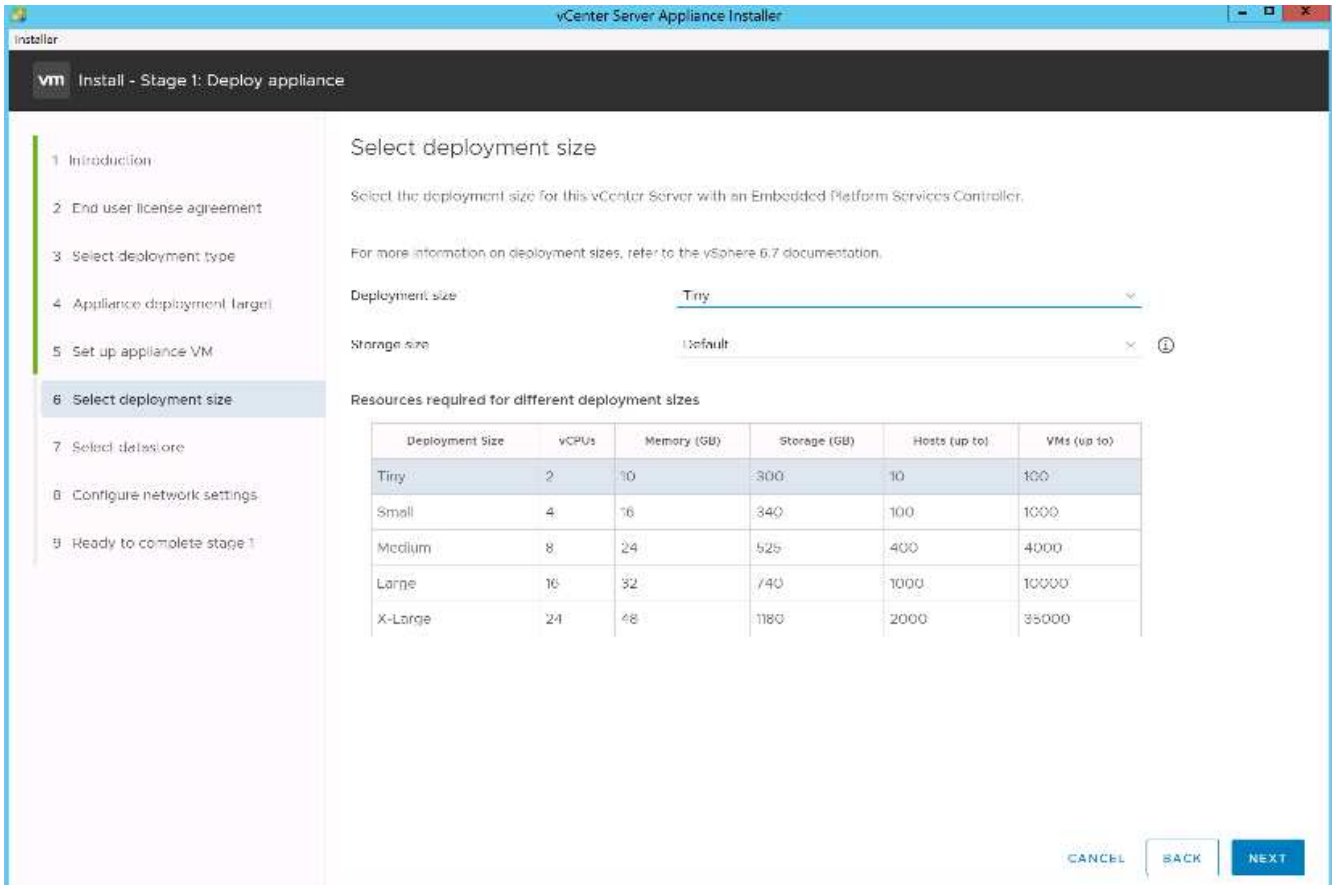
9. Geben Sie auf der Seite Appliance Deployment Target die IP-Adresse eines bereitgestellten ESXi-Hosts, den Root-Benutzernamen und das Root-Passwort ein. Klicken Sie Auf Weiter.



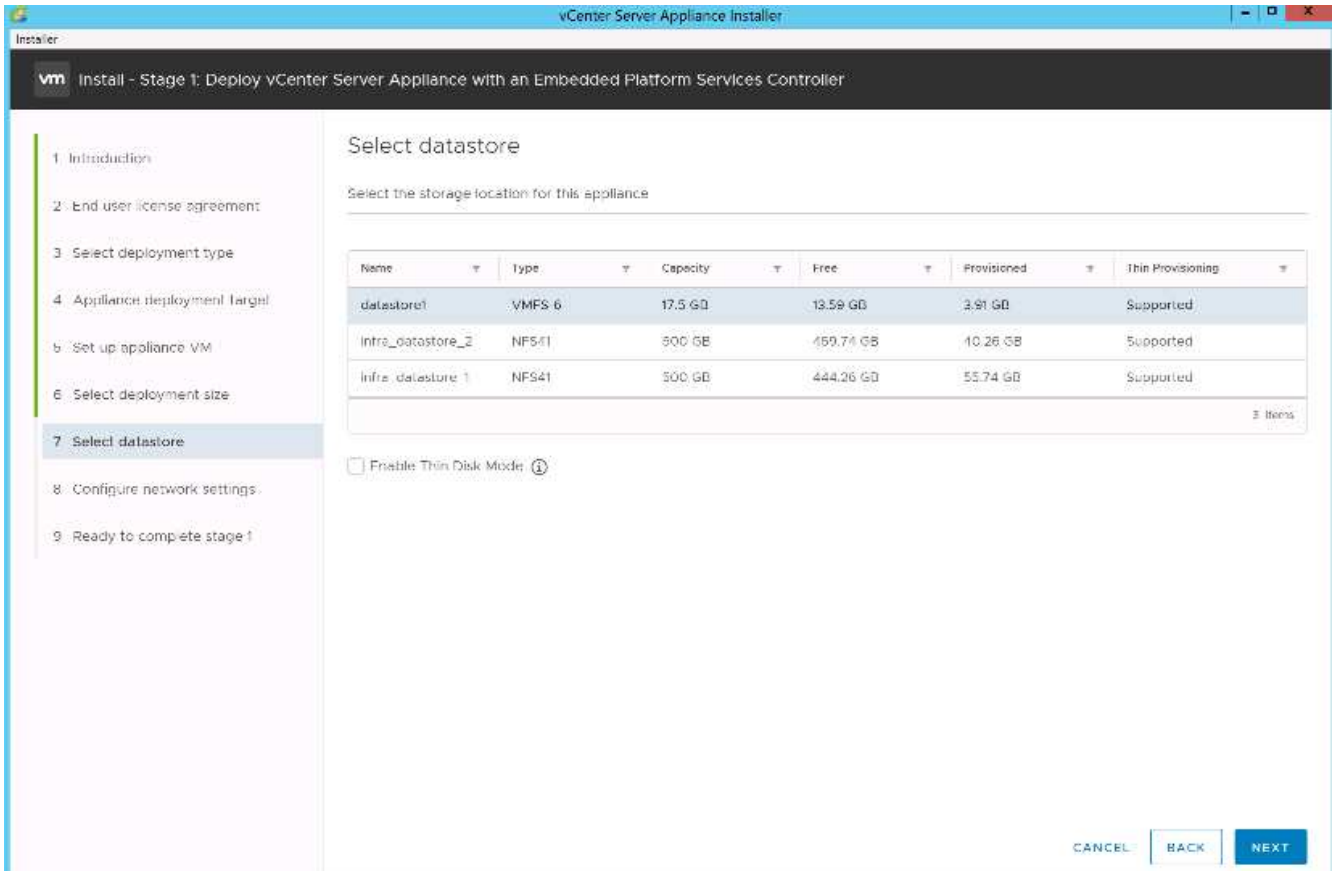
10. Legen Sie die Appliance-VM fest, indem Sie VCSA als VM-Name und das Root-Passwort eingeben, das Sie für VCSA verwenden möchten. Klicken Sie Auf Weiter.



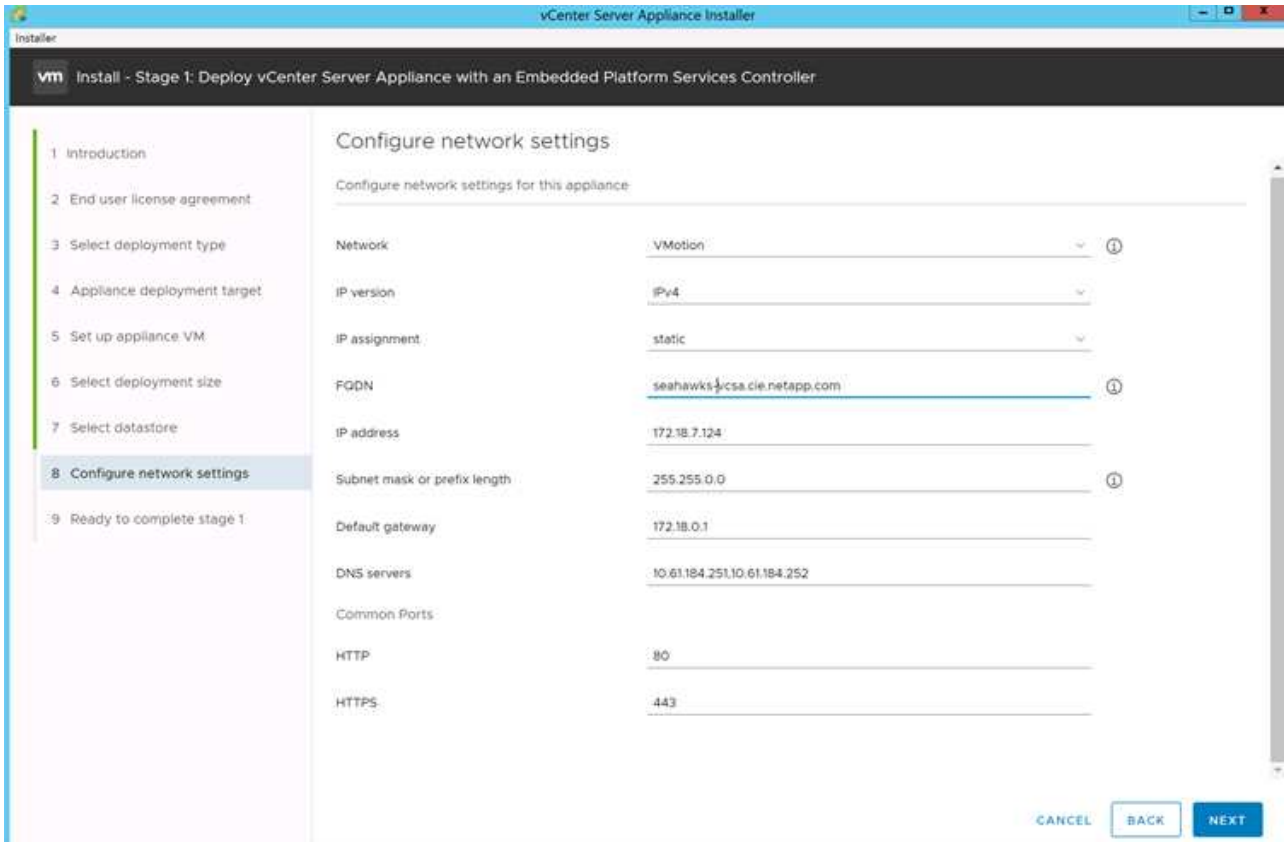
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



12. Wählen Sie die aus `infra_datastore_1` Datenspeicher: Klicken Sie Auf Weiter.



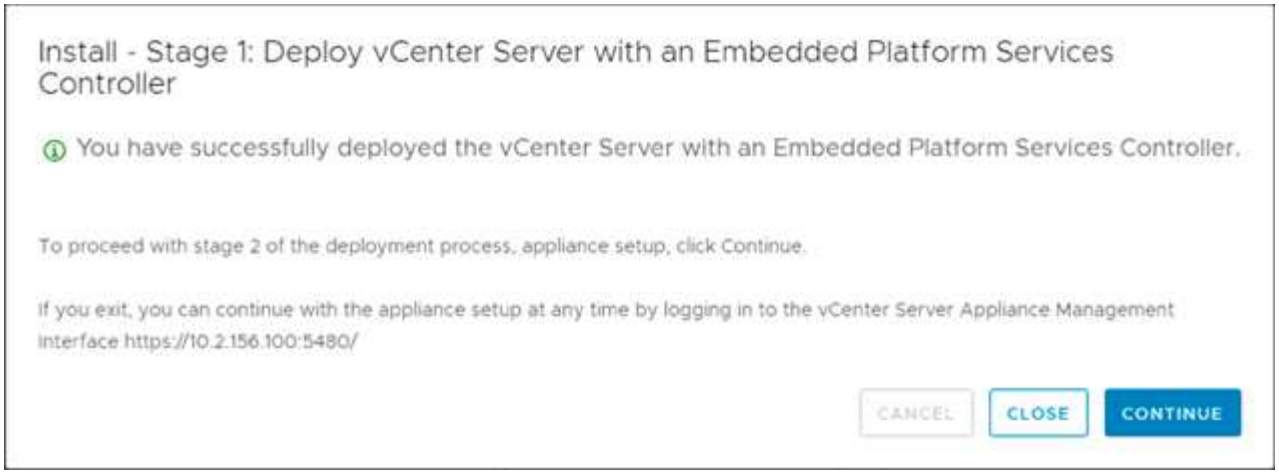
13. Geben Sie auf der Seite Netzwerkeinstellungen konfigurieren die folgenden Informationen ein, und klicken Sie auf Weiter.
    a. Wählen SIE MGMT-Network als Netzwerk aus.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse ein.
    d. Geben Sie die zu verwendenden Subnetzmaske ein.
    e. Geben Sie das Standard-Gateway ein.
    f. Geben Sie den DNS-Server ein.



14. Überprüfen Sie auf der Seite bereit zum Abschließen von Phase 1, ob die von Ihnen eingegebenen Einstellungen korrekt sind. Klicken Sie Auf Fertig Stellen.

    Die VCSA wird jetzt installiert. Dieser Vorgang dauert mehrere Minuten.

15. Wenn Phase 1 abgeschlossen ist, wird eine Meldung angezeigt, die angibt, dass sie abgeschlossen ist. Klicken Sie auf Weiter, um die Konfiguration von Phase 2 zu beginnen.



16. Klicken Sie auf der Seite Einführung in Phase 2 auf Weiter.
17. Eingabe `<<var_ntp_id>>` Für die NTP-Serveradresse. Sie können mehrere NTP-IP-Adressen eingeben.

    Wenn Sie Hochverfügbarkeit in vCenter Server verwenden möchten, stellen Sie sicher, dass der SSH-Zugriff aktiviert ist.
18. Konfigurieren Sie den SSO-Domänennamen, das Passwort und den Standortnamen. Klicken Sie Auf Weiter.

    Notieren Sie diese Werte für Ihre Referenz, insbesondere wenn Sie vom abweichen `vsphere.local` Domain-Name:
19. Treten Sie auf Wunsch dem VMware Customer Experience-Programm bei. Klicken Sie Auf Weiter.
20. Zeigen Sie die Zusammenfassung Ihrer Einstellungen an. Klicken Sie auf Fertig stellen oder verwenden Sie die Schaltfläche Zurück, um die Einstellungen zu bearbeiten.
21. Es wird eine Meldung angezeigt, die besagt, dass Sie die Installation nach dem Start nicht anhalten oder beenden können. Klicken Sie auf OK, um fortzufahren.

    Die Einrichtung der Appliance wird fortgesetzt. Dies dauert einige Minuten.

    Es wird eine Meldung angezeigt, die angibt, dass das Setup erfolgreich war.

    Die Links, die der Installer zum Zugriff auf vCenter Server bereitstellt, sind anklickbar.

Konfiguration von VMware vCenter Server 6.7 und vSphere Clustering

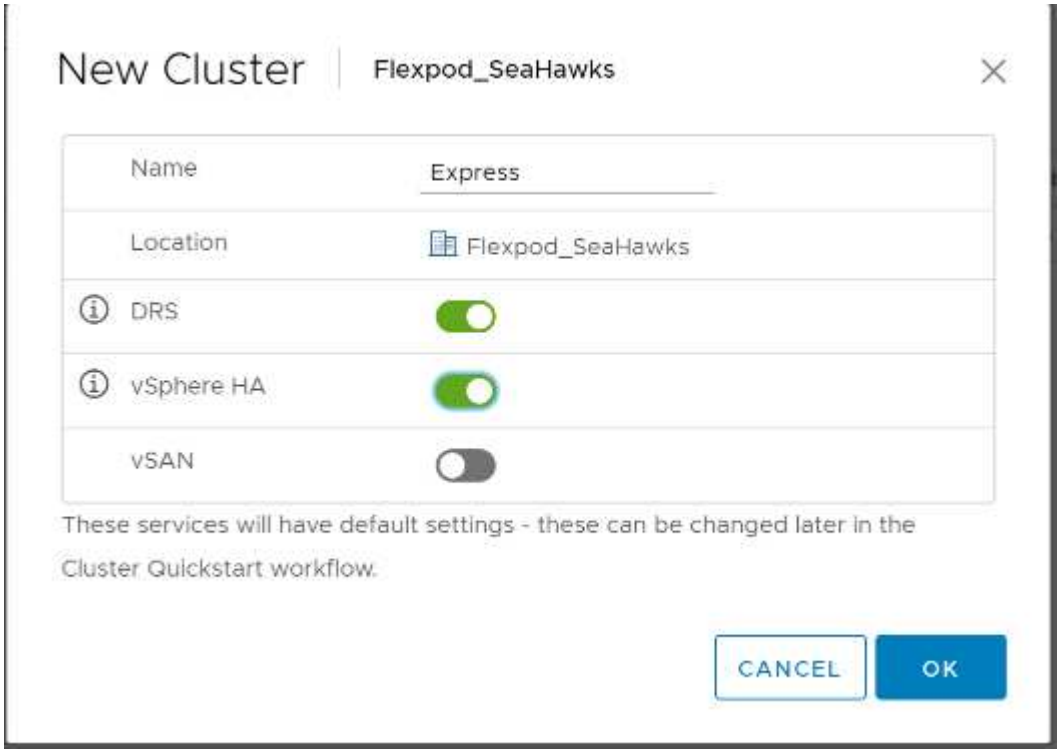
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

1. Navigieren Sie zu https://<<FQDN oder IP von vCenter>>/vsphere-Client/.
2. Klicken Sie auf vSphere Client starten.
3. Melden Sie sich mit dem Benutzernamen administrator@vsphere.local und dem SSO-Passwort an, das Sie während des VCSA-Setups eingegeben haben.
4. Klicken Sie mit der rechten Maustaste auf den vCenter-Namen, und wählen Sie New Datacenter aus.
5. Geben Sie einen Namen für das Datacenter ein, und klicken Sie auf OK.

Erstellen Sie vSphere Cluster.

Gehen Sie zum Erstellen eines vSphere-Clusters wie folgt vor:

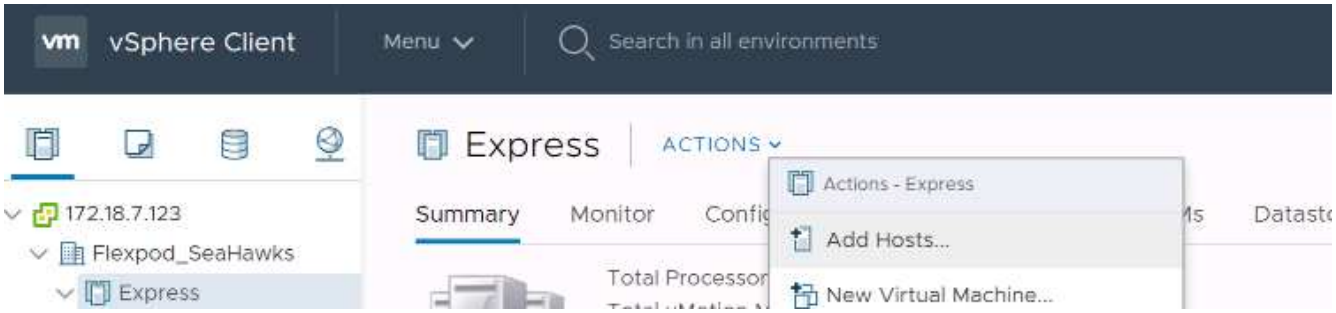
1. Klicken Sie mit der rechten Maustaste auf das neu erstellte Datacenter, und wählen Sie Neuer Cluster aus.
2. Geben Sie einen Namen für das Cluster ein.
3. Wählen Sie DRS und vSphere HA-Optionen aus und aktivieren Sie sie.
4. Klicken Sie auf OK.



ESXi Hosts zu Cluster hinzufügen

Führen Sie die folgenden Schritte aus, um dem Cluster ESXi-Hosts hinzuzufügen:

1. Wählen Sie im Menü Aktionen des Clusters die Option Host hinzufügen aus.



2. Gehen Sie wie folgt vor, um dem Cluster einen ESXi-Host hinzuzufügen:
   a. Geben Sie die IP oder den FQDN des Hosts ein. Klicken Sie Auf Weiter.
   b. Geben Sie den Benutzernamen und das Kennwort für den Root-Benutzer ein. Klicken Sie Auf Weiter.
   c. Klicken Sie auf Ja, um das Host-Zertifikat durch ein vom VMware-Zertifikatsserver signiertes Zertifikat zu ersetzen.

d. Klicken Sie auf der Seite Host Summary auf Next.

e. Klicken Sie auf das grüne Symbol +, um dem vSphere-Host eine Lizenz hinzuzufügen.

> Dieser Schritt kann auf Wunsch später abgeschlossen werden.

f. Klicken Sie auf Weiter, um den Sperrmodus deaktiviert zu lassen.

g. Klicken Sie auf der Seite VM-Speicherort auf Weiter.

h. Überprüfen Sie die Seite „bereit für Fertigstellung“. Verwenden Sie die Zurück-Taste, um Änderungen vorzunehmen, oder wählen Sie Fertig stellen.

3. Wiederholen Sie die Schritte 1 und 2 für Cisco UCS Host B.

Dieser Prozess muss für alle zusätzlichen Hosts abgeschlossen werden, die zur Konfiguration von FlexPod Express hinzugefügt werden.

Konfigurieren Sie coredump auf ESXi Hosts

ESXi Dump Collector-Setup für über iSCSI gestartete Hosts

ESXi-Hosts, die mit iSCSI mit dem VMware iSCSI-Software-Initiator gestartet wurden, müssen so konfiguriert werden, dass Core Dumps für den ESXi Dump Collector, der Teil von vCenter ist, ausgeführt werden. Der Dump Collector ist auf der vCenter-Appliance standardmäßig nicht aktiviert. Dieses Verfahren sollte am Ende der vCenter-Bereitstellung ausgeführt werden. So richten Sie den ESXi Dump Collector ein:

1. Melden Sie sich beim vSphere Web Client als administrator@vsphere.local an, und wählen Sie Home.
2. Klicken Sie im mittleren Fensterbereich auf Systemkonfiguration.
3. Wählen Sie im linken Fensterbereich Dienste aus.
4. Klicken Sie unter Dienste auf VMware vSphere ESXi Dump Collector.
5. Klicken Sie im mittleren Fensterbereich auf das grüne Startsymbol, um den Service zu starten.
6. Klicken Sie im Menü Aktionen auf Starttyp bearbeiten.
7. Wählen Sie Automatisch.
8. Klicken Sie auf OK.
9. Stellen Sie eine Verbindung zu jedem ESXi Host her, indem Sie SSH als Root verwenden.
10. Führen Sie folgende Befehle aus:

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

Die Nachricht `Verified the configured netdump server is running` Wird angezeigt, nachdem Sie den letzten Befehl ausgeführt haben.

> Dieser Prozess muss für alle zusätzlichen, FlexPod Express hinzugefügten Hosts abgeschlossen sein.

Schlussfolgerung

FlexPod Express ist eine einfache und effiziente Lösung und bietet ein validiertes Design mit branchenführenden Komponenten. Durch die Skalierung bis hin zum Hinzufügen weiterer Komponenten kann FlexPod Express gezielt auf spezifische Geschäftsanforderungen angepasst werden. FlexPod Express wurde für kleine und mittelständische Unternehmen, Großunternehmen und andere Unternehmen konzipiert, die dedizierte Lösungen benötigen.

Weitere Informationen

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

- NVA- 1130-DESIGN: FlexPod Express mit VMware vSphere 6.7U1 und NetApp AFF A220 mit Direct-Attached IP=basiertem Storage NVA-Design

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- AFF and FAS Systems Documentation Center

  "http://docs.netapp.com/platstor/index.jsp"

- ONTAP 9 Dokumentationszentrum

  "http://docs.netapp.com/ontap-9/index.jsp"

- NetApp Produktdokumentation

  "https://docs.netapp.com"

FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp AFF/FAS – NVA – Implementierung

Jyh-shing Chen, NetApp

Die FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp AFF/FAS Lösung nutzt Cisco UCS Mini mit B200 M5 Blade Servern, Cisco UCS 6324 in-Chassis Fabric Interconnects, Cisco Nexus 31108PC-V Switches oder andere konforme Switches, NetApp AFF A220, C190 oder das Controller-HA-Paar der FAS2700 Serie Mit der NetApp ONTAP 9.7 Datenmanagement-Software ausgeführt wird. Dieses Dokument zur Implementierung der NetApp Verified Architecture (NVA) enthält die detaillierten Schritte, die zur Konfiguration der Infrastrukturkomponenten und zur Implementierung von VMware vSphere 7.0 und den zugehörigen Tools erforderlich sind, um eine äußerst zuverlässige und hochverfügbare virtuelle FlexPod Express-Infrastruktur zu erstellen.

"FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp AFF/FAS – NVA – Implementierung"

FlexPod und Sicherheit

FlexPod, die Lösung gegen Ransomware

TR-4802: FlexPod, die Lösung gegen Ransomware

Arvind Ramakrishnan, NetApp

In Zusammenarbeit mit: 

Um Ransomware zu verstehen, ist es notwendig, zunächst ein paar wichtige Punkte zur Kryptografie zu verstehen. Kryptografische Methoden ermöglichen die Verschlüsselung von Daten mit einem gemeinsamen geheimen Schlüssel (symmetrische Schlüsselverschlüsselung) oder einem Schlüsselpaar (asymmetrische Verschlüsselungsschlüsselverschlüsselung). Einer dieser Schlüssel ist ein weit verbreiteter öffentlicher Schlüssel und der andere ist ein nicht offenbarter privater Schlüssel.

Ransomware ist eine Art von Malware, die auf Kryptovirologie basiert, die die Verwendung von Kryptografie ist, um schädliche Software zu erstellen. Diese Malware kann sowohl symmetrische und asymmetrische Schlüssel Verschlüsselung zu machen, um ein Opfer Daten zu sperren und ein Lösegeld zu verlangen, um den Schlüssel zur Entschlüsselung der Daten des Opfers.

Wie funktioniert Ransomware?

In den folgenden Schritten wird beschrieben, wie Ransomware die Daten des Opfers mit Kryptografie verschlüsselt, ohne dabei Möglichkeiten zur Entschlüsselung oder Wiederherstellung des Opfers haben zu müssen:

1. Der Angreifer generiert ein Schlüsselpaar wie bei der asymmetrischen Schlüsselverschlüsselung. Der erzeugte öffentliche Schlüssel wird innerhalb der Malware abgelegt und anschließend die Malware freigegeben.
2. Nachdem die Malware den Computer oder das System des Opfers eingegeben hat, erzeugt sie einen zufällig symmetrischen Schlüssel, indem sie einen Pseudorandom Number Generator (PRNG) oder einen anderen praktikablen Zufallszahlengenerator verwendet.
3. Die Malware verwendet diesen symmetrischen Schlüssel, um die Daten des Opfers zu verschlüsseln. Es verschlüsselt schließlich den symmetrischen Schlüssel, indem der Angreifer den öffentlichen Schlüssel verwendet, der in die Malware eingebettet wurde. Die Ausgabe dieses Schritts ist ein asymmetrischer Chiffretext des verschlüsselten symmetrischen Schlüssels und des symmetrischen Chiffretextes der Daten des Opfers.
4. Die Malware zerosiert (löscht) die Daten des Opfers und den symmetrischen Schlüssel, der verwendet wurde, um die Daten zu verschlüsseln, so dass kein Spielraum für die Wiederherstellung.
5. Das Opfer zeigt nun den asymmetrischen Chiffretext des symmetrischen Schlüssels und einen Lösegeld-Wert, der bezahlt werden muss, um den symmetrischen Schlüssel zu erhalten, der verwendet wurde, um die Daten zu verschlüsseln.

6. Das Opfer zahlt das Lösegeld und teilt den asymmetrischen Chiffretext mit dem Angreifer. Der Angreifer entschlüsselt den Chiffretext mit seinem privaten Schlüssel, was zu dem symmetrischen Schlüssel führt.
7. Der Angreifer teilt diesen symmetrischen Schlüssel mit dem Opfer, der verwendet werden kann, um alle Daten zu entschlüsseln und somit vom Angriff zu erholen.

Herausforderungen

Bei einem Ransomware-Angriff stehen Einzelpersonen und Unternehmen vor folgenden Herausforderungen:

- Die wichtigste Herausforderung besteht darin, dass sie die Produktivität des Unternehmens oder der Person sofort belastet. Es braucht Zeit, in den Status der Normalität zurückzukehren, da alle wichtigen Dateien wieder gewonnen werden müssen und die Systeme gesichert werden müssen.
- Sie könnten zu einer Verletzung der Daten führen, die vertrauliche und vertrauliche Informationen enthält, die Kunden oder Kunden gehören, und zu einer Krisensituation führen, die ein Unternehmen eindeutig vermeiden möchte.
- Es besteht eine sehr gute Möglichkeit, dass Daten in die falschen Hände geraten oder vollständig gelöscht werden. Dies führt zu einem Punkt ohne Rückkehr, der für Unternehmen und Einzelpersonen verheerend sein könnte.
- Nach der Bezahlung des Lösegeld gibt es keine Garantie, dass der Angreifer den Schlüssel zur Wiederherstellung der Daten zur Verfügung stellt.
- Es besteht keine Gewissheit, dass der Angreifer die Übertragung sensibler Daten absieht, obwohl er das Lösegeld bezahlt.
- In großen Unternehmen ist die Identifizierung von Schlupflöcher, die zu einem Ransomware-Angriff geführt haben, eine mühsame Aufgabe, und es ist mit großem Aufwand auch möglich, alle Systeme zu sichern.

Wer ist gefährdet?

Jeder kann von Ransomware angegriffen werden, auch von Einzelpersonen und großen Unternehmen. Unternehmen, die keine klar definierten Sicherheitsmaßnahmen und -Praktiken implementieren, sind noch anfälliger für solche Angriffe. Die Auswirkungen des Angriffs auf ein großes Unternehmen können mehrere Male größer sein als das, was ein einzelner ertragen könnte.

Ransomware macht ca. 28 % aller Malware-Angriffe aus. Mit anderen Worten: Mehr als jeder vierte Malware-Vorfall ist ein Ransomware-Angriff. Ransomware kann sich automatisch und wahllos über das Internet verbreiten, und, wenn es einen Sicherheitsverfall gibt, kann es in die Systeme des Opfers und weiter auf andere verbundene Systeme zu verbreiten. Angreifer neigen dazu, Personen oder Organisationen anzugreifen, die sehr viel File Sharing betreiben, sehr sensible und kritische Daten haben oder einen unzureichenden Schutz gegen Angriffe bieten.

Angreifer neigen dazu, sich auf die folgenden potenziellen Ziele zu konzentrieren:

- Universitäten und Studentengemeinden
- Regierungsbehörden und Behörden um
- Krankenhäuser
- Banken

Dies ist keine umfassende Liste von Zielen. Sie können sich nicht vor Angriffen schützen, wenn Sie außerhalb einer dieser Kategorien fallen.

Wie kommt Ransomware in ein System oder verteilt?

Ransomware kann auf verschiedene Weise in ein System eintreten oder auf andere Systeme übergreifen. In der heutigen Welt sind fast alle Systeme über das Internet, LANs, WANs usw. miteinander verbunden. Die Menge der Daten, die zwischen diesen Systemen generiert und ausgetauscht werden, steigt nur.

Ransomware kann sich am häufigsten mit vielen Methoden ausbreiten und auf die Daten zugreifen – wir nutzen sie täglich.

- E-Mail
- P2P-Netzwerke
- Dateien werden heruntergeladen
- Soziale Netzwerke
- Mobilgeräte
- Verbindung zu unsicheren öffentlichen Netzwerken herstellen
- Zugriff auf Web-URLs

Konsequenzen eines Datenverlusts

Die Folgen oder Auswirkungen von Datenverlusten können breiter ausfallen, als Unternehmen erwarten würden. Die Auswirkungen können variieren, je nach Dauer der Ausfallzeit oder Zeitraum, in dem ein Unternehmen keinen Zugriff auf seine Daten hat. Je länger der Angriff andauere, desto größer ist der Einfluss auf die Einnahmen, Marke und den Ruf der Organisation. Zudem kann sich ein Unternehmen mit rechtlichen Fragen und einem starken Produktivitätsrückgang konfrontiert sehen.

Während diese Probleme im Laufe der Zeit weiter bestehen, beginnen sie zu vergrößern und könnten am Ende eine Kultur einer Organisation ändern, je nachdem, wie sie auf den Angriff reagiert. In der heutigen Welt verbreiten sich Informationen schnell, und negative Nachrichten über eine Organisation können ihren Ruf dauerhaft schädigen. Ein Unternehmen könnte hohe Einbußen bei Datenverlusten verzeichnen, die letztendlich zur Schließung eines Unternehmens führen können.

Finanzielle Auswirkungen

Laut einer aktuellen "McAfee-Bericht"Die durch Cyberkriminalität verursachten globalen Kosten belaufen sich auf rund 600 Milliarden US-Dollar, was etwa 0.8 % des weltweiten BIP entspricht. Wenn dieser Betrag mit der weltweit wachsenden Internetwirtschaft von 4.2 Billionen Dollar verglichen wird, entspricht dies einer Wachstumssteuer von 14 %.

Ransomware ist einen bedeutenden Anteil dieser finanziellen Kosten. Die durch Ransomware-Angriffe verursachten Kosten im Jahr 2018 belaufen sich auf ca. 8 Milliarden US-Dollar—einem Betrag, der 2019 auf 11.5 Milliarden US-Dollar geschätzt wird.

Welche Lösung bietet sich an?

Eine Wiederherstellung nach einem Ransomware-Angriff mit minimaler Downtime ist nur durch die Implementierung eines proaktiven Disaster-Recovery-Plans möglich. Die Fähigkeit, sich von einem Angriff zu erholen, ist gut, aber einen Angriff insgesamt zu verhindern ist ideal.

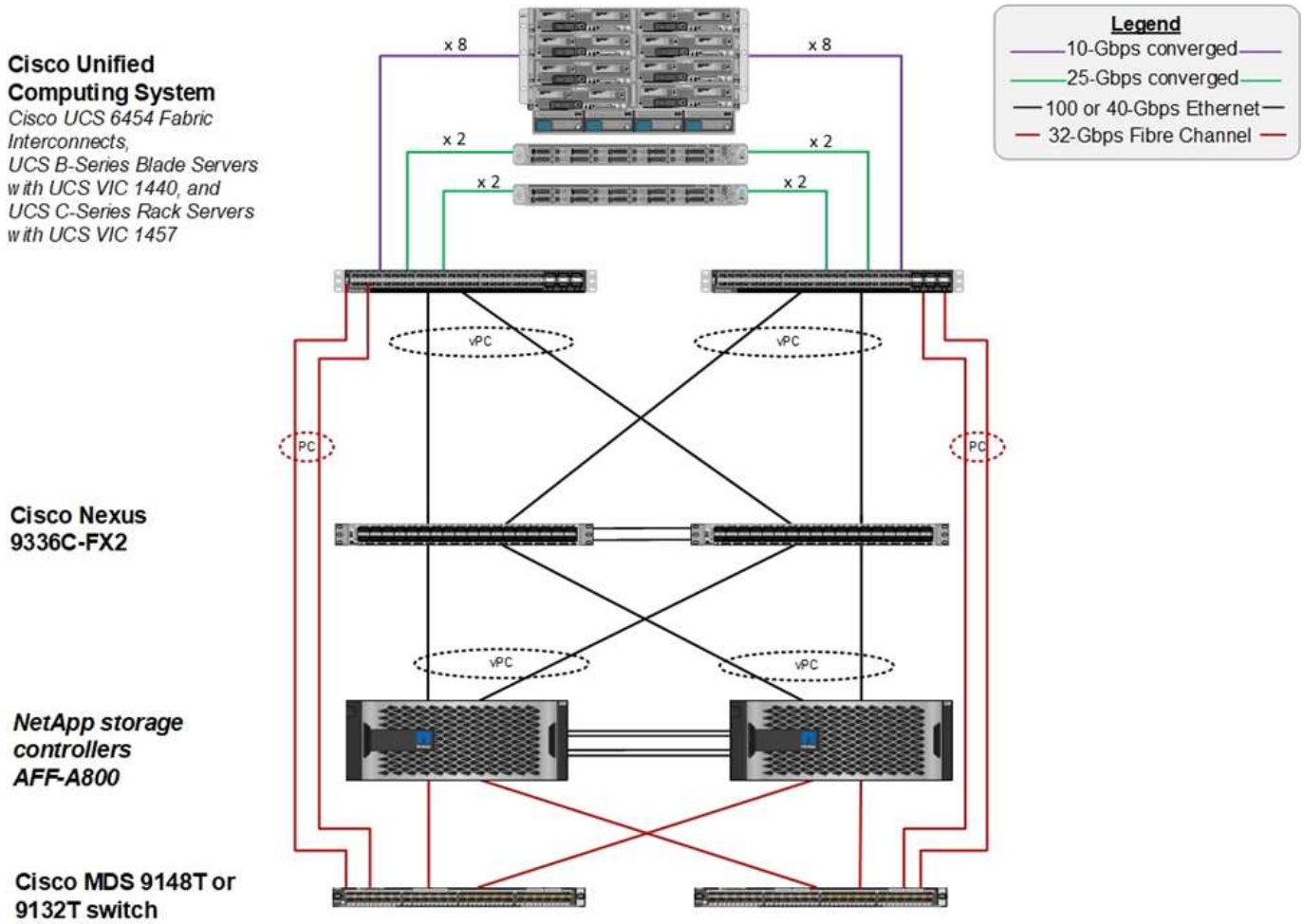
Obwohl es verschiedene Fronten gibt, die Sie überprüfen und beheben müssen, um einen Angriff zu verhindern, ist die Kernkomponente, mit der Sie einen Angriff verhindern oder beheben können, das Rechenzentrum.

Das Datacenter-Design und die Funktionen, die es zur Sicherung von Endpunkten in Netzwerk, Computing und Storage bietet, spielen eine entscheidende Rolle beim Aufbau einer sicheren Umgebung für den täglichen Betrieb. In diesem Dokument wird erläutert, wie die Funktionen einer Hybrid-Cloud-Infrastruktur von FlexPod bei einem Angriff eine schnelle Daten-Recovery ermöglichen und außerdem Angriffe komplett verhindern können.

Übersicht über FlexPod

FlexPod ist eine vorkonfigurierte, integrierte und validierte Architektur, die Server der Cisco Unified Computing System (Cisco UCS), Switches der Cisco Nexus Familie, Cisco MDS Fabric Switches und NetApp Storage Arrays in einer einzigen flexiblen Architektur kombiniert. Die Lösungen von FlexPod wurden für Hochverfügbarkeit ohne Single Points of Failure konzipiert und sorgen gleichzeitig für Kosteneffizienz und Designflexibilität, um eine Vielzahl von Workloads zu unterstützen. Ein FlexPod-Design kann verschiedene Hypervisoren und Bare Metal-Server unterstützen und sich ebenfalls entsprechend den Workload-Anforderungen des Kunden dimensionieren und optimieren lassen.

Die Abbildung unten zeigt die FlexPod Architektur und hebt die Hochverfügbarkeit auf allen Ebenen des Stacks deutlich hervor. Die Infrastrukturkomponenten von Storage, Netzwerk und Computing sind so konfiguriert, dass bei einem Ausfall einer Komponente sofort ein Failover zum verbleibenden Partner möglich ist.



Ein großer Vorteil für ein FlexPod System ist, dass es vorab integriert und für mehrere Workloads validiert

wurde. Für jede Lösungsvalidierung werden detaillierte Design- und Implementierungsleitfäden veröffentlicht. In diesen Dokumenten finden Sie Best Practices, die Sie für Workloads einsetzen müssen, damit sie nahtlos auf FlexPod ausgeführt werden können. Diese Lösungen basieren auf erstklassigen Computing-, Netzwerk- und Storage-Produkten sowie einer Vielzahl von Funktionen, die auf Sicherheit und Härtung der gesamten Infrastruktur liegen.

"IBM X-Force Threat Intelligence Index" staaten, „menschliche Fehler, die für zwei Drittel der kompromittierten Aufzeichnungen verantwortlich sind, einschließlich historischer 424 % Sprung in die falsch konfigurierte Cloud-Infrastruktur.“

Mit einem FlexPod-System vermeiden Sie Fehlkonfiguration Ihrer Infrastruktur, indem Sie Automatisierung durch Ansible-Playbooks verwenden, die ein lückenloses Setup der Infrastruktur gemäß den Best Practices in Cisco Validated Designs (CVDs) und NetApp Verified Architectures (NVAs) durchführen.

Schutzmaßnahmen gegen Ransomware

In diesem Abschnitt werden die wichtigsten Funktionen der NetApp ONTAP Datenmanagement-Software sowie die Tools für Cisco UCS und Cisco Nexus erläutert, mit denen Sie gegen Ransomware-Angriffe sichern und wiederherstellen können.

NetApp ONTAP

Die ONTAP Software bietet viele nützliche Funktionen für die Datensicherung, von denen die meisten für Kunden mit einem ONTAP System kostenlos sind. Sie können die folgenden Funktionen zu jeder Zeit nutzen, um Daten vor Angriffen zu schützen:

- **NetApp Snapshot Technologie.** Eine Snapshot-Kopie ist ein schreibgeschütztes Image eines Volumes, das den Status eines Filesystems zu einem bestimmten Zeitpunkt erfasst. Diese Kopien helfen, Daten ohne Auswirkungen auf die System-Performance zu sichern und belegen gleichzeitig nicht viel Storage. NetApp empfiehlt, einen Zeitplan für die Erstellung von Snapshot-Kopien zu erstellen. Sie sollten auch eine lange Aufbewahrungszeit halten, weil einige Malware kann ruhend gehen und dann wieder aktivieren Wochen oder Monate nach einer Infektion. Im Falle eines Angriffs kann das Volume mithilfe einer Snapshot-Kopie zurückgesetzt werden, die vor der Infektion erstellt wurde.
- **NetApp SnapRestore Technologie.** SnapRestore Daten-Recovery-Software ist extrem nützlich, um Daten zu beschädigen oder nur die Datei Inhalte zurücksetzen. SnapRestore setzt die Attribute eines Volume nicht zurück. Dies ist wesentlich schneller als ein Administrator, indem er Dateien aus der Snapshot Kopie in das aktive Filesystem kopiert. Die Geschwindigkeit, mit der Daten wiederhergestellt werden können, ist hilfreich, wenn viele Dateien so schnell wie möglich wiederhergestellt werden müssen. Wird ein Angriff verursacht, hilft dieser äußerst effiziente Recovery-Prozess der schnellen Wiederherstellung des Geschäftsbetriebs.
- **NetApp SnapCenter Technologie.** die SnapCenter Software nutzt Storage-basierte Backup- und Replizierungsfunktionen von NetApp, um applikationskonsistente Datensicherung zu ermöglichen. Diese Software lässt sich in Enterprise-Applikationen integrieren und bietet applikationsspezifische und datenbankspezifische Workflows, um die Anforderungen von Applikations-, Datenbank- und Administratoren virtueller Infrastrukturen zu erfüllen. SnapCenter bietet eine unkomplizierte Enterprise-Plattform zur sicheren Koordinierung und Verwaltung der Datensicherung für alle Applikationen, Datenbanken und Filesysteme. Die Fähigkeit zur applikationskonsistenten Datensicherung ist bei der Datenwiederherstellung wichtig, da Applikationen schneller in einem konsistenten Status wiederhergestellt werden können.
- **NetApp SnapLock Technologie.** SnapLock stellt ein speziellen Volume zur Verfügung, in dem Dateien gespeichert und in einen nicht löschbaren, nicht überschreibbaren Zustand versetzt werden können. Die Produktionsdaten des Benutzers, die sich in einem FlexVol Volume befinden, können durch NetApp

SnapMirror bzw. SnapVault Technologie gespiegelt oder in ein SnapLock Volume archiviert werden. Die Dateien im SnapLock Volume, das Volume selbst und das Hosting-Aggregat können bis zum Ende der Aufbewahrungsdauer nicht gelöscht werden.

- **NetApp FPolicy Technologie.** Verwenden Sie FPolicy Software, um Angriffe zu verhindern, indem Operationen auf Dateien mit bestimmten Erweiterungen dierlauben. Ein FPolicy-Ereignis kann für bestimmte Dateivorgänge ausgelöst werden. Das Ereignis ist mit einer Richtlinie verknüpft, die die Engine aufruft, die es verwenden muss. Sie können eine Richtlinie mit einer Reihe von Dateierweiterungen konfigurieren, die möglicherweise Ransomware enthalten könnten. Wenn eine Datei mit einer nicht zulässigen Erweiterung versucht, einen nicht autorisierten Vorgang auszuführen, verhindert FPolicy die Ausführung dieses Vorgangs.

Netzwerk: Cisco Nexus

Die Cisco NX OS-Software unterstützt die NetFlow-Funktion, die eine verbesserte Erkennung von Netzwerkanomalien und -Sicherheit ermöglicht. NetFlow erfasst die Metadaten jedes Gesprächs im Netzwerk, die an der Kommunikation beteiligten Parteien, das verwendete Protokoll und die Dauer der Transaktion. Nachdem die Informationen aggregiert und analysiert wurden, können sie einen Einblick in das normale Verhalten geben.

Die gesammelten Daten ermöglichen außerdem die Identifizierung fragwürdiger Aktivitätsmuster, wie etwa die Verbreitung von Malware im Netzwerk, die ansonsten unbemerkt bleiben kann.

NetFlow verwendet Flows, um Statistiken für die Netzwerküberwachung bereitzustellen. Ein Flow ist ein unidirektionaler Strom von Paketen, der auf einer Quellschnittstelle (oder VLAN) ankommt und die gleichen Werte für die Schlüssel hat. Ein Schlüssel ist ein identifizierter Wert für ein Feld innerhalb des Pakets. Sie erstellen einen Flow mithilfe eines Flow-Datensatzes, um die eindeutigen Tasten für Ihren Flow zu definieren. Sie können die Daten, die NetFlow für Ihre Ströme sammelt, mit Hilfe eines Flow-Exporterers in einen Remote NetFlow Collector, wie z. B. Cisco Stealthwatch, exportieren. Stealthwatch verwendet diese Informationen für die kontinuierliche Überwachung des Netzwerks und bietet Bedrohungserkennung in Echtzeit sowie eine Forensik zum Vorfallsreaktion, falls ein Ransomware-Ausbruch auftritt.

Computing: Cisco UCS

Cisco UCS ist der Computing-Endpunkt in einer FlexPod Architektur. Sie können mehrere Cisco Produkte verwenden, um diese Stack-Ebene auf Betriebssystemebene zu sichern.

Sie können die folgenden wichtigen Produkte auf der Computing- oder Anwendungsebene implementieren:

- **Cisco Advanced Malware Protection (AMP) for Endpoints.** Diese Lösung wird auf Microsoft Windows und Linux Betriebssystemen unterstützt und umfasst Funktionen für Prävention, Erkennung und Reaktion. Diese Sicherheitssoftware verhindert Verstöße, blockiert Malware am Einstiegspunkt und überwacht und analysiert kontinuierlich die Datei- und Prozessaktivitäten, um Bedrohungen schnell zu erkennen, einzudämmen und zu beseitigen, die den Schutz vor der Front-Line-Lösung ausweichen können.

  Die Komponente „bösartiger Aktivitätsschutz“ (MAP) von AMP überwacht kontinuierlich alle Endpoint-Aktivitäten und ermöglicht die Laufzeiterkennung und das Blockieren des anormalen Verhaltens eines laufenden Programms auf dem Endpunkt. Wenn beispielsweise das Endpunktverhalten auf Ransomware hinweist, werden die abgebrochene Prozesse beendet, um Endpunktverschlüsselung zu verhindern und den Angriff zu stoppen.

- **Cisco Advanced Malware Protection for Email Security.** E-Mails sind das erste Fahrzeug, um Malware zu verbreiten und Cyber-Angriffe durchzuführen. Im Durchschnitt werden an einem einzigen Tag rund 100 Milliarden E-Mails ausgetauscht, die Angreifern einen ausgezeichneten Penetrationsvektor in die Systeme des Benutzers bieten. Daher ist es absolut unerlässlich, sich gegen diese Angriffslinie zu verteidigen.

AMP analysiert E-Mails auf Bedrohungen wie Zero-Day-Exploits und entstickende Malware, die in bösartigen Anhängen verborgen sind. Darüber hinaus nutzt es branchenführende URL-Informationen, um schädliche Links zu bekämpfen. Anwender erhalten erweiterten Schutz vor Spear-Phishing, Ransomware und anderen anspruchsvollen Angriffen.

- **Intrusion Prevention System der nächsten Generation (NGIPS).** Cisco Firepower NGIPS kann als physische Appliance im Datacenter oder als virtuelle Appliance auf VMware (NGIPSv für VMware) eingesetzt werden. Dieses hocheffiziente Abwehrsystem für Angriffe sorgt für zuverlässige Leistung und niedrige Gesamtbetriebskosten. Der Schutz vor Bedrohungen kann durch optionale Abonnementlizenzen erweitert werden, um AMP, Transparenz und Kontrolle von Anwendungen sowie URL-Filterfunktionen bereitzustellen. Virtualisierte NGIPS überprüft den Datenverkehr zwischen Virtual Machines (VMs) und erleichtert die Bereitstellung und das Management von NGIPS-Lösungen an Standorten mit begrenzten Ressourcen. Dadurch wird der Schutz sowohl für physische als auch für virtuelle Ressourcen erhöht.

Sichern Sie Ihre Daten und stellen Sie sie auf FlexPod wieder her

Dieser Abschnitt beschreibt, wie die Daten eines Endbenutzers im Falle eines Angriffs wiederhergestellt werden können und wie Angriffe durch die Verwendung eines FlexPod-Systems verhindert werden können.

Testbed-Übersicht

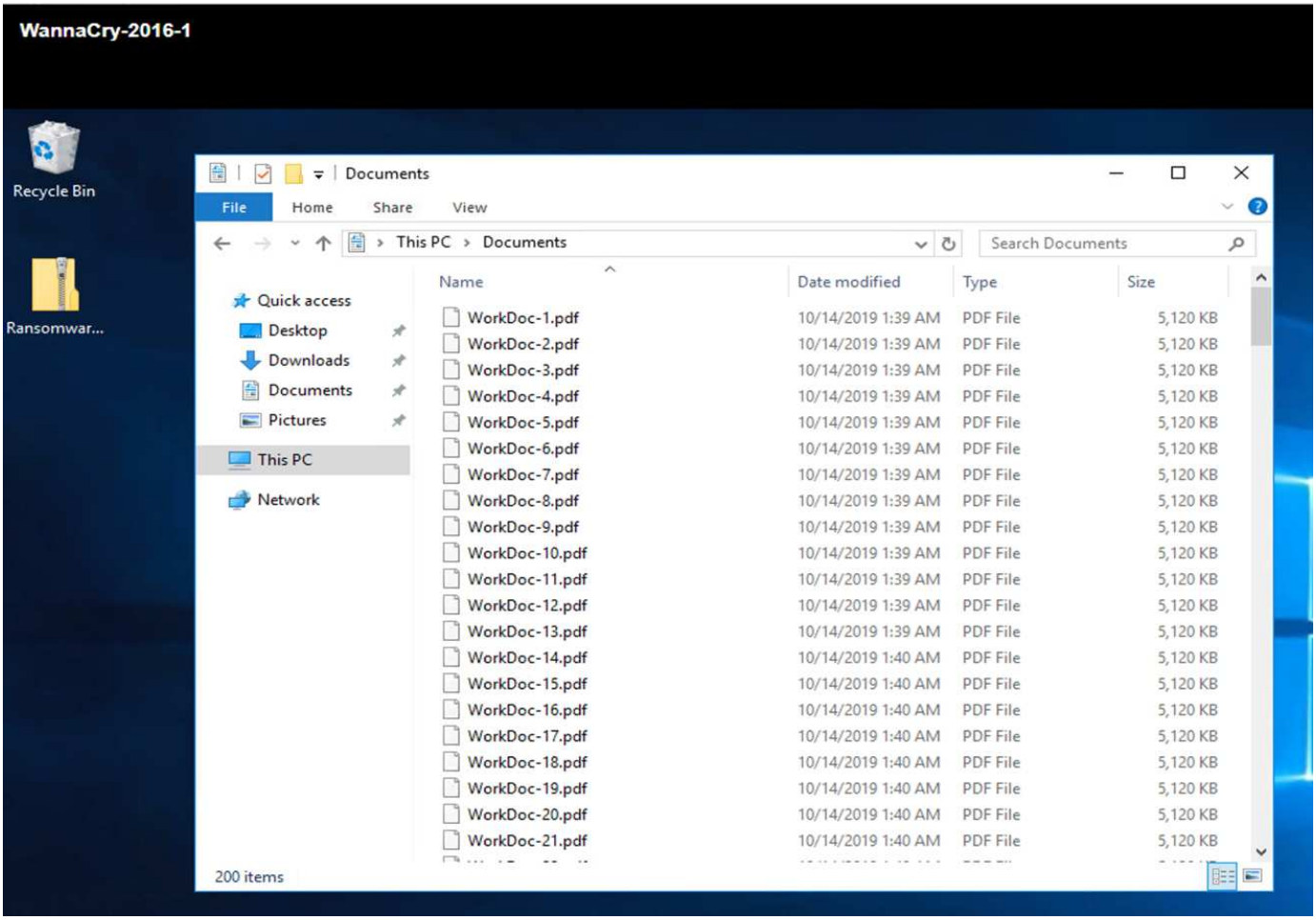
Zur Präsentation von FlexPod-Erkennung, -Korrektur und -Vorbeugung wurde ein Testbed auf Basis der Richtlinien erstellt, die in der neuesten CVD-Plattform angegeben sind, die zum Zeitpunkt der Erstellung dieses Dokuments verfügbar sind: "FlexPod Datacenter mit VMware vSphere 6.7 U1, Cisco UCS der vierten Generation und NetApp AFF A-Series CVD".

In der VMware vSphere Infrastruktur wurde eine Windows 2016 VM mit einer CIFS-Freigabe durch die NetApp ONTAP Software implementiert. Dann wurde NetApp FPolicy auf der CIFS-Freigabe konfiguriert, um die Ausführung von Dateien mit bestimmten Extension-Typen zu verhindern. Darüber hinaus wurde die NetApp SnapCenter Software implementiert, um die Snapshot Kopien der VMs in der Infrastruktur zu managen, um applikationskonsistente Snapshot Kopien zu ermöglichen.

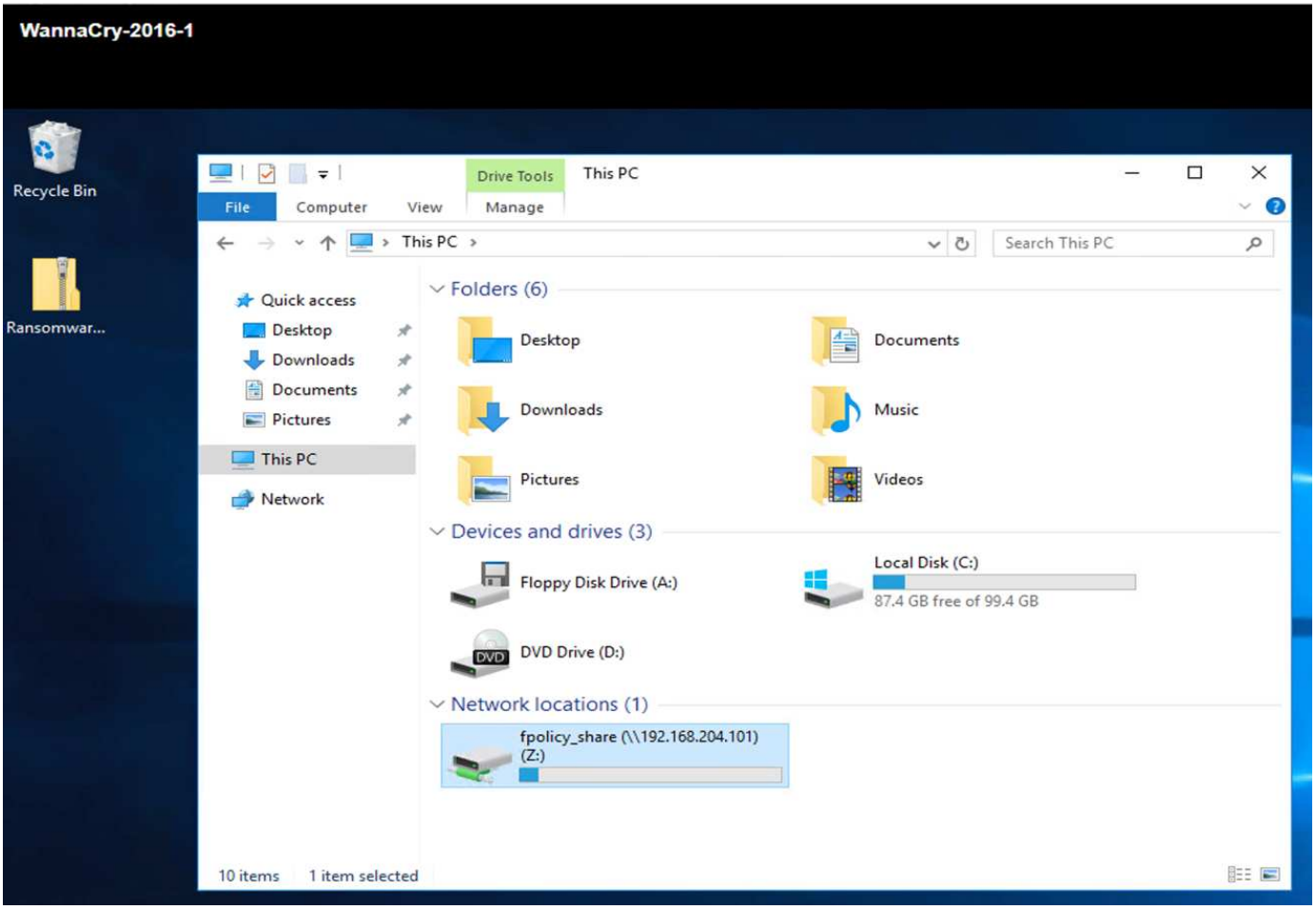
Status der VM und ihrer Dateien vor einem Angriff

In diesem Abschnitt werden der Status der Dateien vor einem Angriff auf die VM und die ihr zugewiesene CIFS-Freigabe angezeigt.

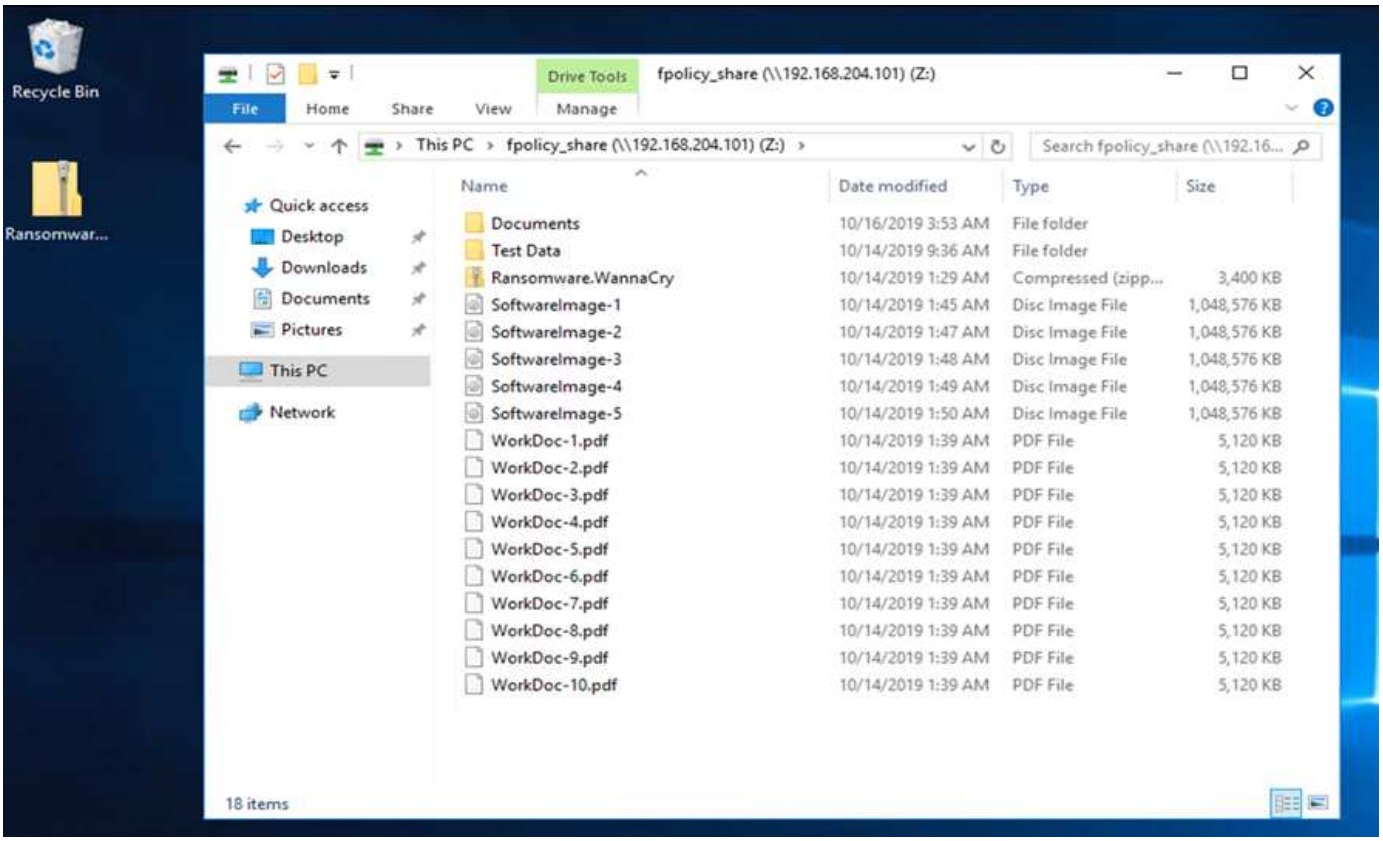
Der Ordner Dokumente der VM hatte eine Reihe von PDF-Dateien, die noch nicht durch die WannaCry Malware verschlüsselt wurden.



Der folgende Screenshot zeigt die CIFS-Freigabe, die der VM zugeordnet war.



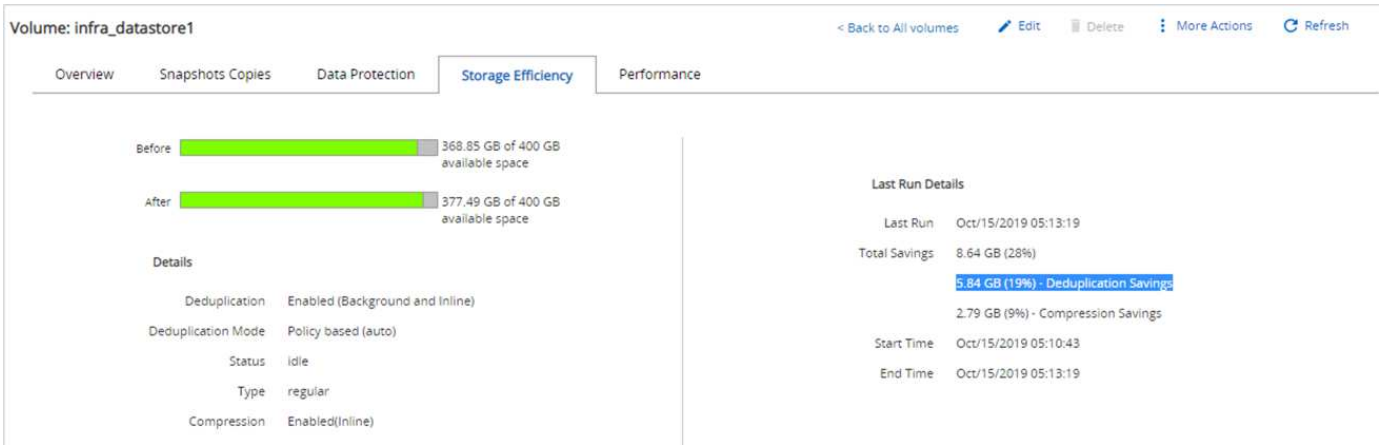
Der folgende Screenshot zeigt die Dateien auf der CIFS-Freigabe `fpolicy_share` Die noch nicht durch die WannaCry-Malware verschlüsselt wurden.



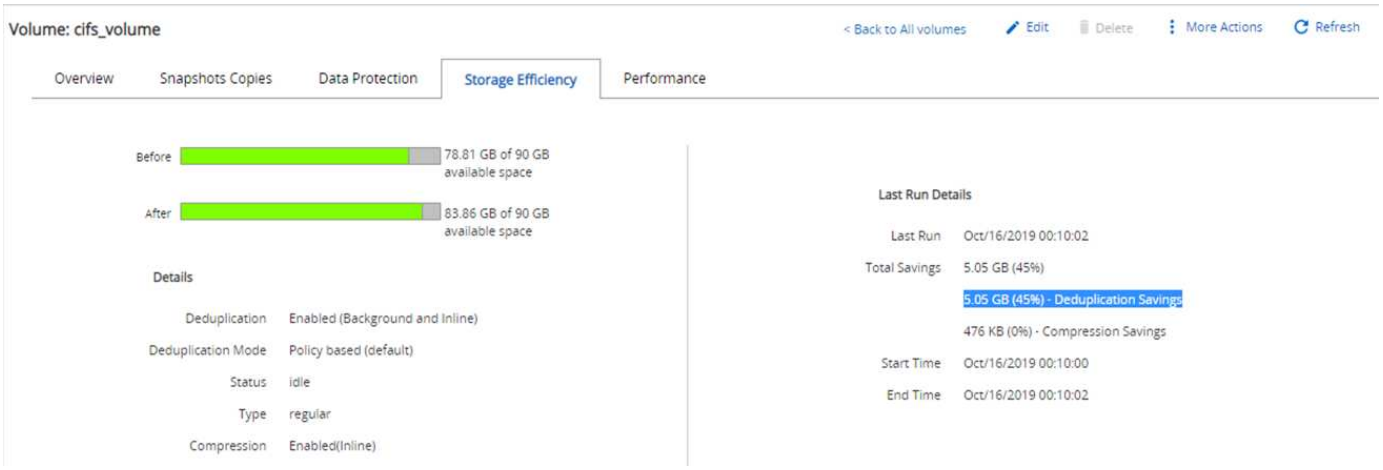
Deduplizierung und Snapshot-Informationen vor einem Angriff

Details zur Storage-Effizienz und die Größe der Snapshot-Kopie vor einem Angriff werden als Referenz während der Erkennungsphase angezeigt.

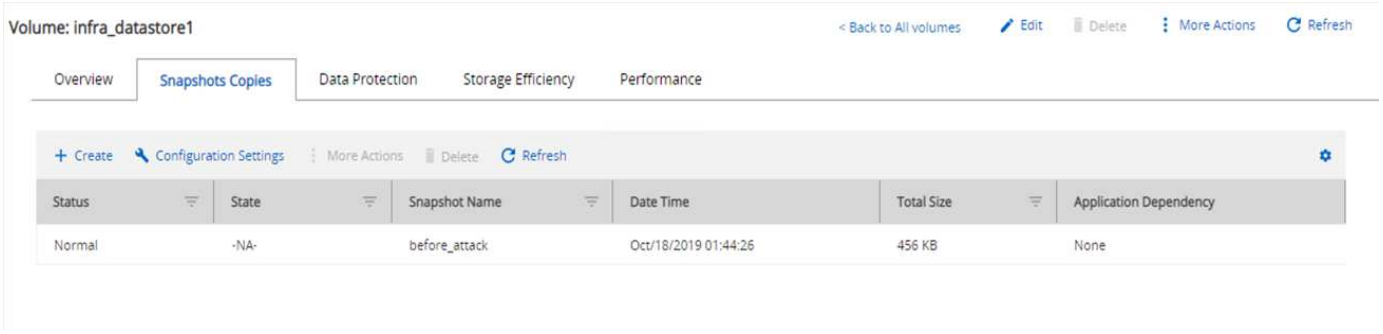
Storage-Einsparungen von 19 % wurden durch Deduplizierung auf dem Volume, das die VM hostet, erzielt.



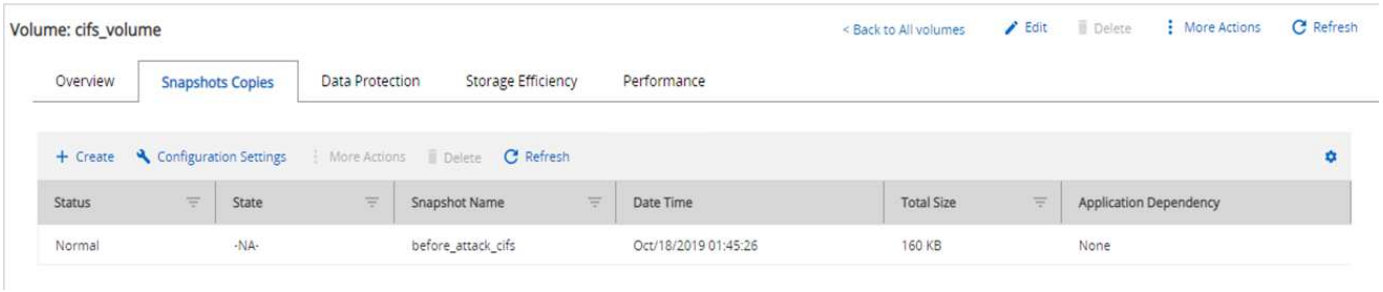
Durch Deduplizierung beim CIFS-Share wurden Storage-Einsparungen von 45 % erzielt `fpolicy_share`.



Für das Volume, das die VM hostet, wurde eine Snapshot-Kopie von 456 KB beobachtet.



Für den CIFS-Share wurde eine Snapshot Kopie von 160 KB beobachtet `fpolicy_share`.



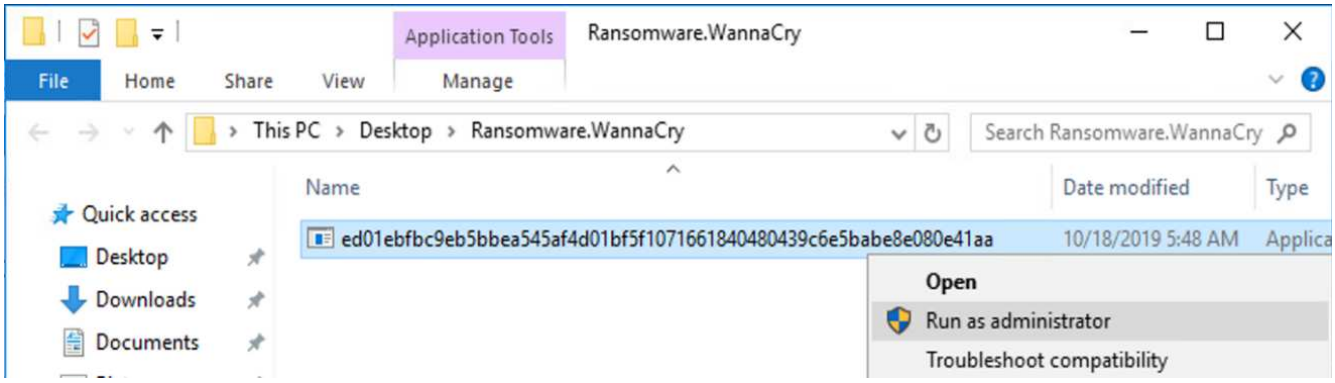
WannaCry-Infektion auf VM und CIFS-Share

In diesem Abschnitt zeigen wir, wie die WannaCry-Malware in die FlexPod-Umgebung eingeführt wurde und welche Änderungen am System beobachtet wurden.

Die folgenden Schritte zeigen, wie die WannaCry-Malware-Binärdatei in die VM eingeführt wurde:

1. Die gesicherte Malware wurde extrahiert.

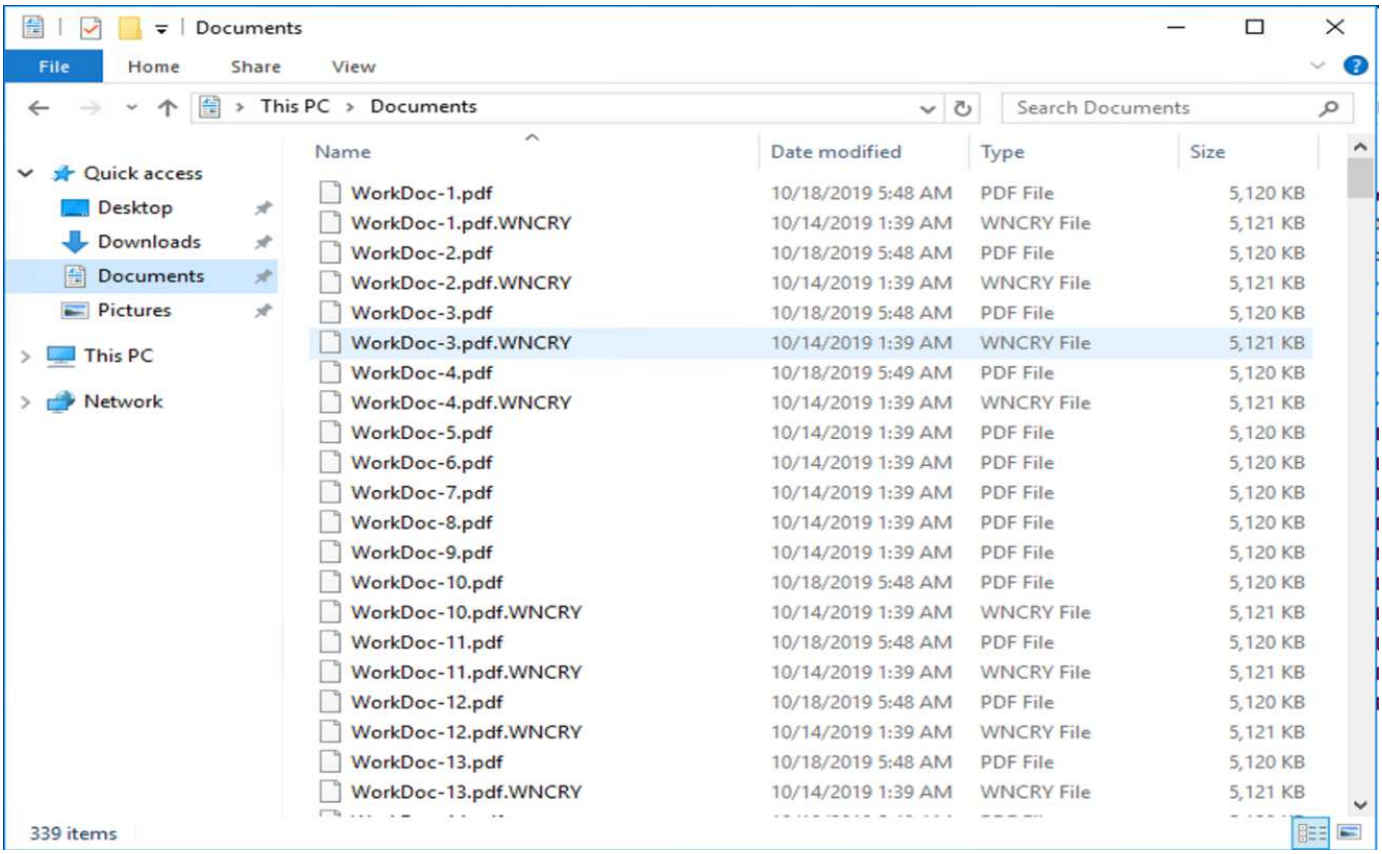
2. Die Binärdatei wurde ausgeführt.



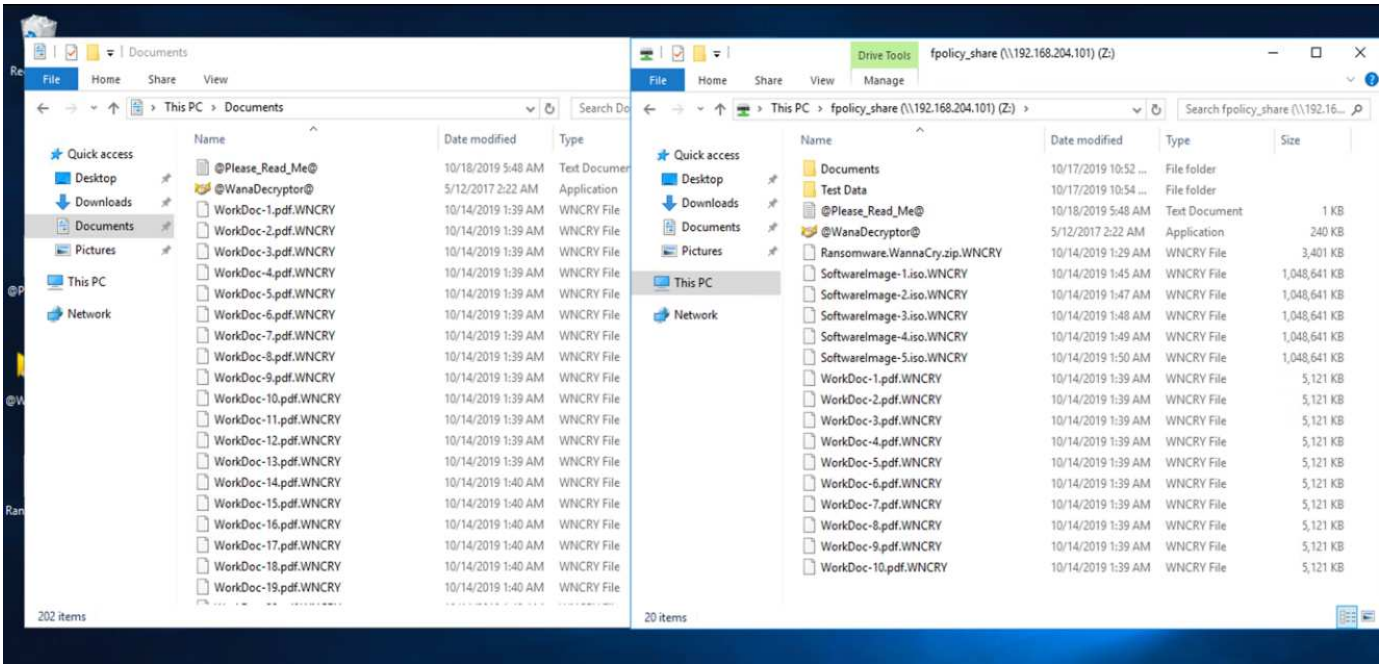
Fall 1: WannaCry verschlüsselt das Dateisystem innerhalb der VM und zugeordnete CIFS-Freigabe

Das lokale Dateisystem und die zugeordnete CIFS-Share wurden durch den WannaCry Malware verschlüsselt.

Malware beginnt, Dateien mit WNCRY-Erweiterungen zu verschlüsseln.



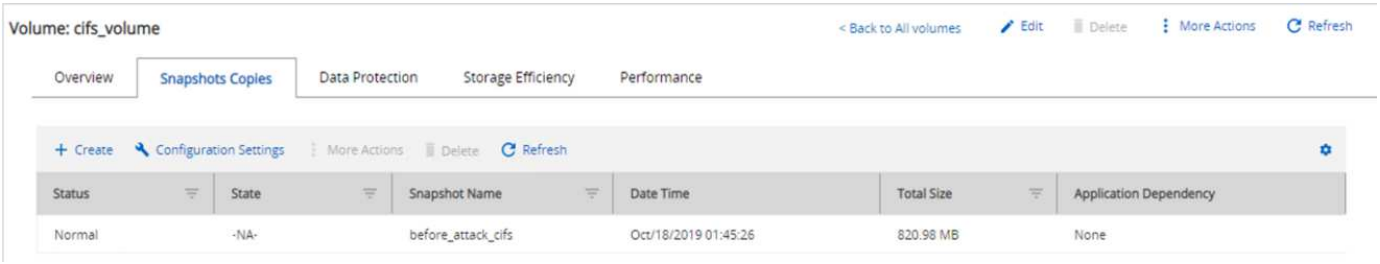
Die Malware verschlüsselt alle Dateien in der lokalen VM und der zugeordneten Freigabe.



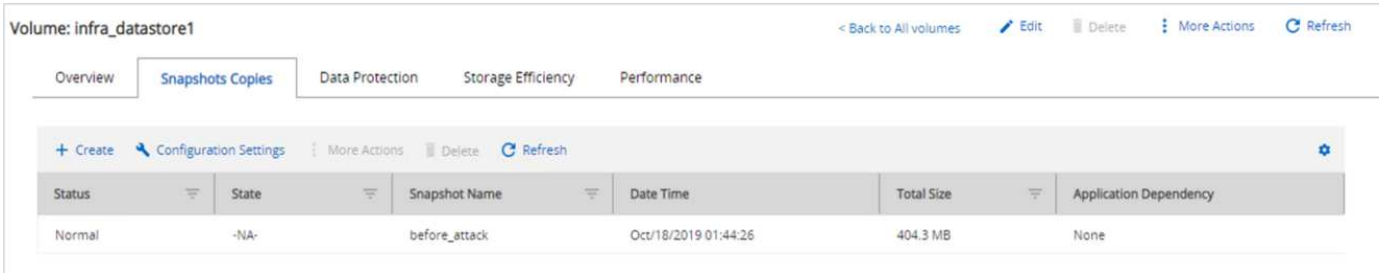
Erkennung

Als die Malware mit der Verschlüsselung der Dateien begann, führte sie zu einem exponentiellen Anstieg der Größe der Snapshot-Kopien und einer deutlichen Verringerung der Storage-Effizienz in Prozent.

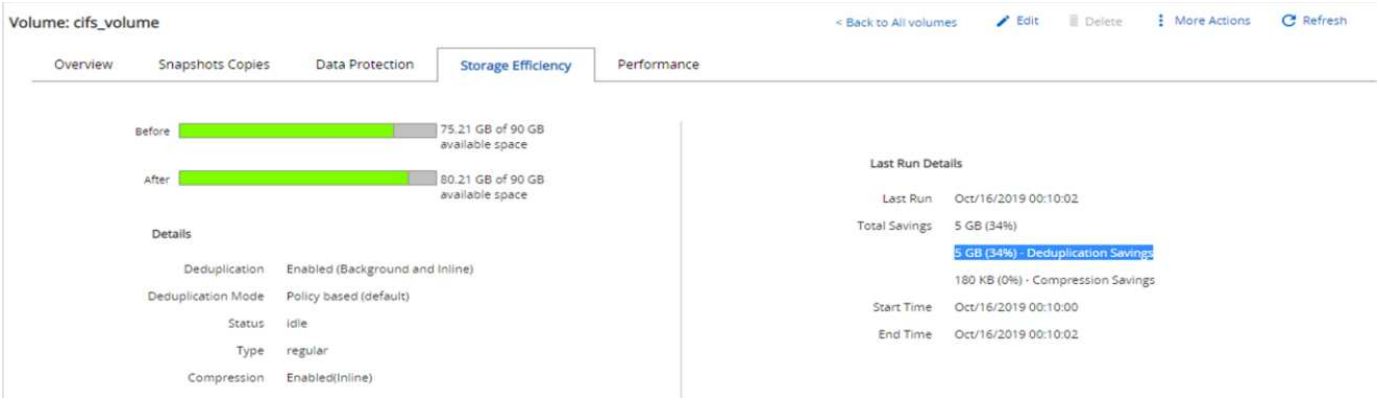
Wir erkannten eine drastische Zunahme der Snapshot-Größe auf 820.98MB für das Volume, das während des Angriffs die CIFS-Freigabe hostet.



Wir erkannten eine Erhöhung der Snapshot-Kopie auf 404,3MB für den Volumen, der die VM hostet.



Die Storage-Effizienz für das Volume, auf dem der CIFS-Share gehostet wird, sank auf 34 %.



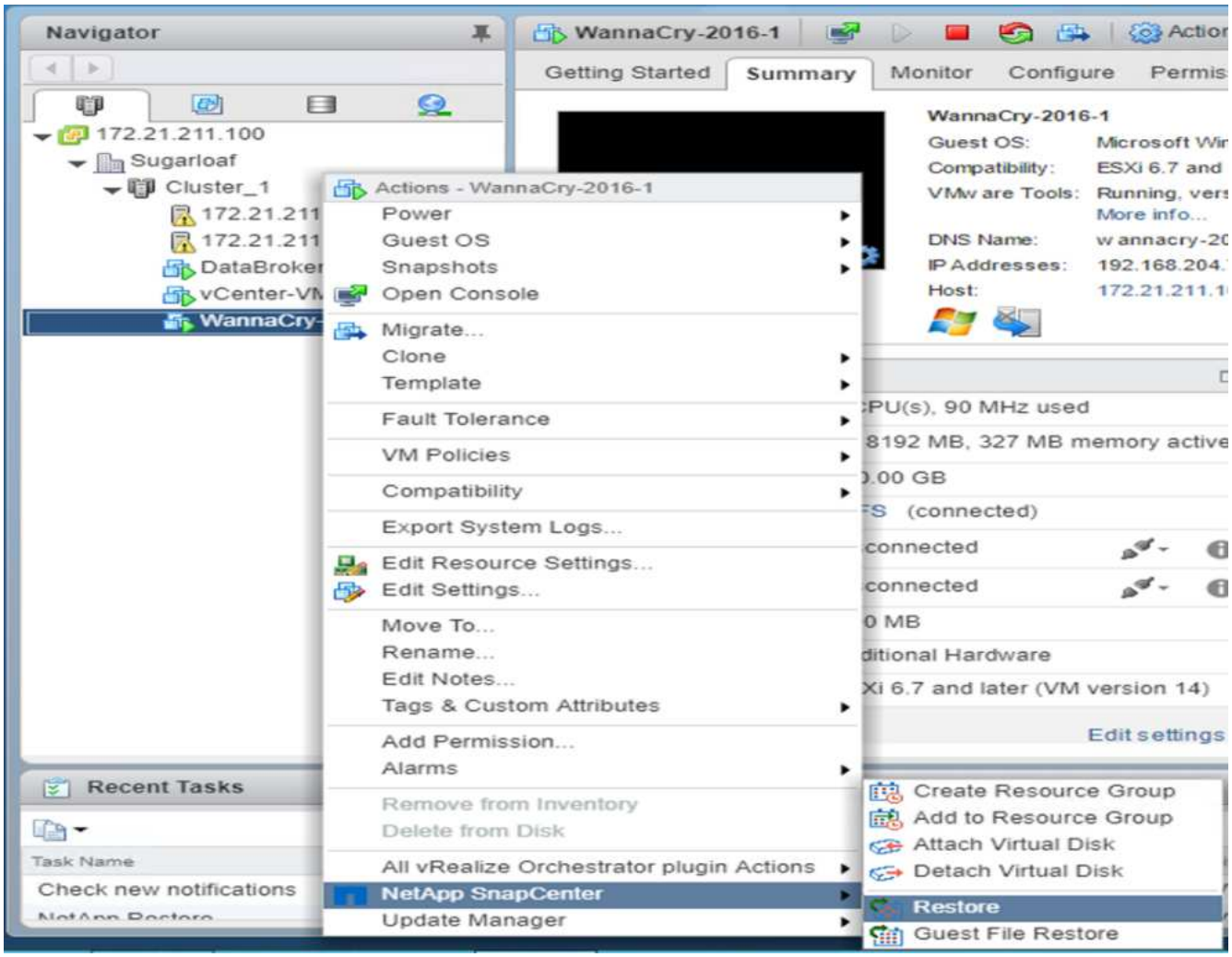
Korrekturmaßnahmen

Stellen Sie die VM wieder her und zugewiesenes CIFS Share, indem Sie vor dem Angriff eine saubere Snapshot Kopie erstellen.

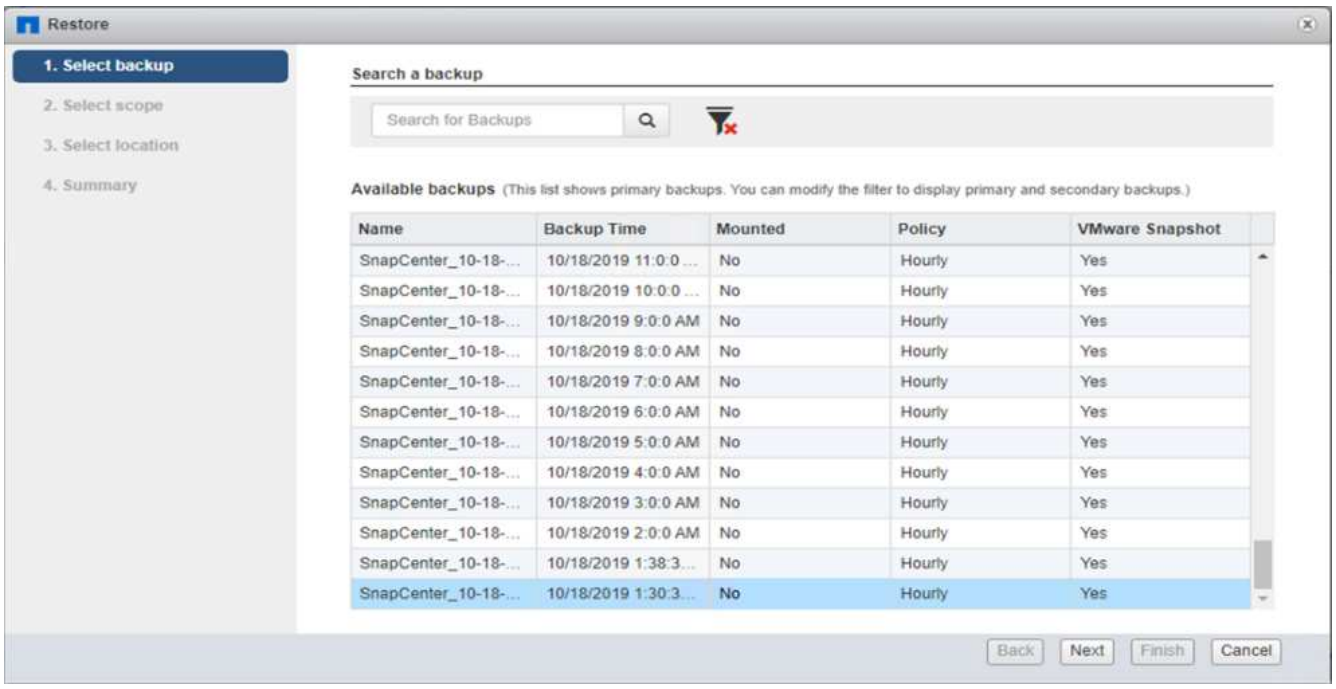
VM wiederherstellen

Um die VM wiederherzustellen, führen Sie die folgenden Schritte aus:

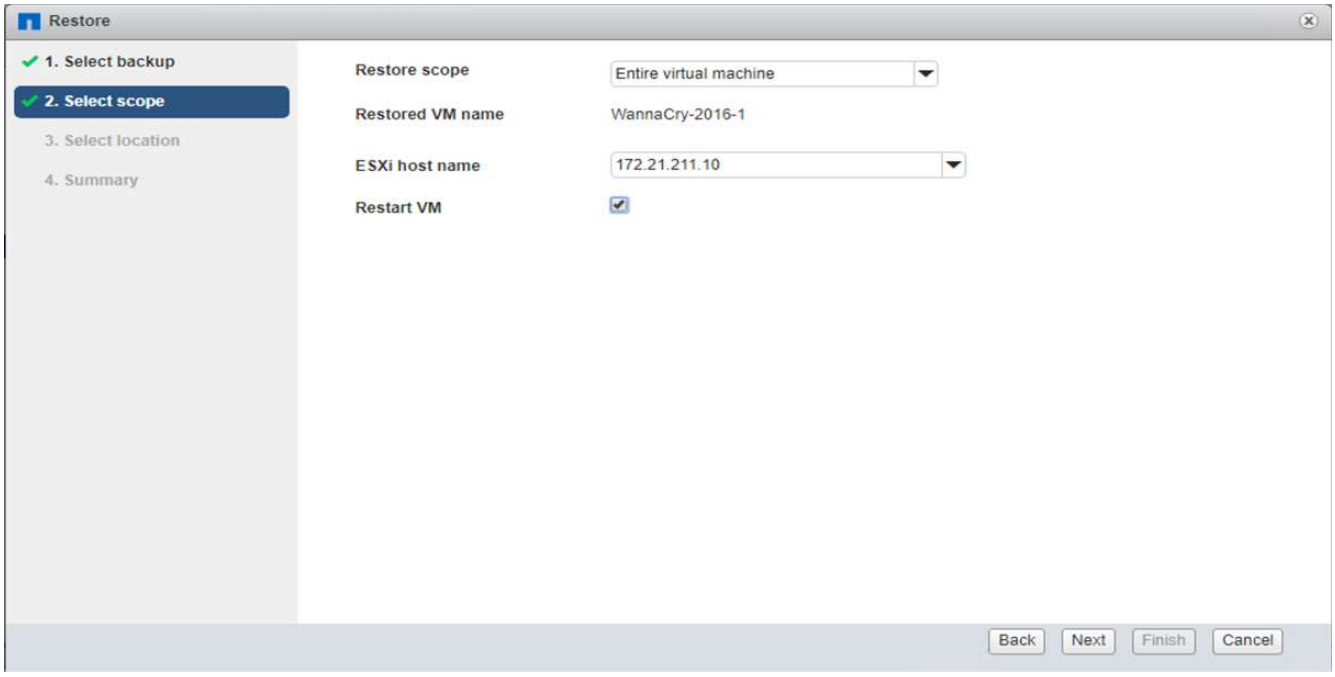
1. Verwenden Sie die mit SnapCenter erstellte Snapshot Kopie zum Wiederherstellen der VM.



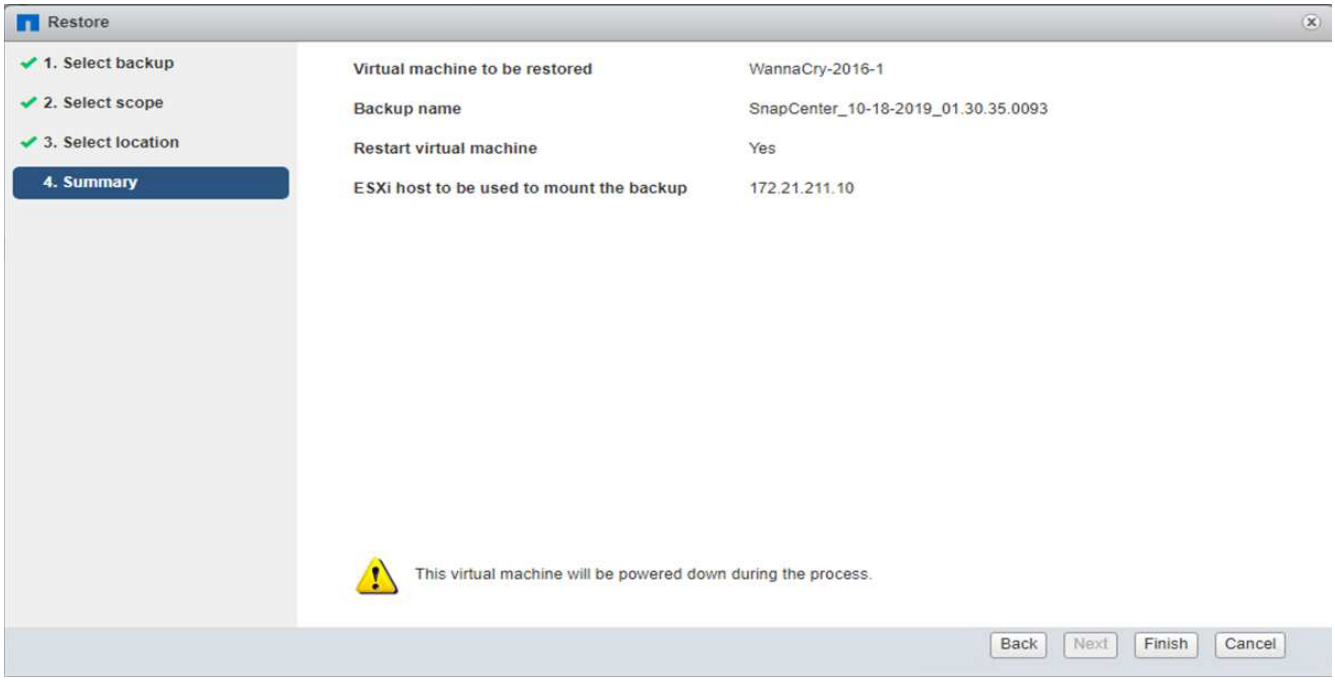
2. Wählen Sie die gewünschte VMware- konsistente Snapshot Kopie für die Wiederherstellung aus.



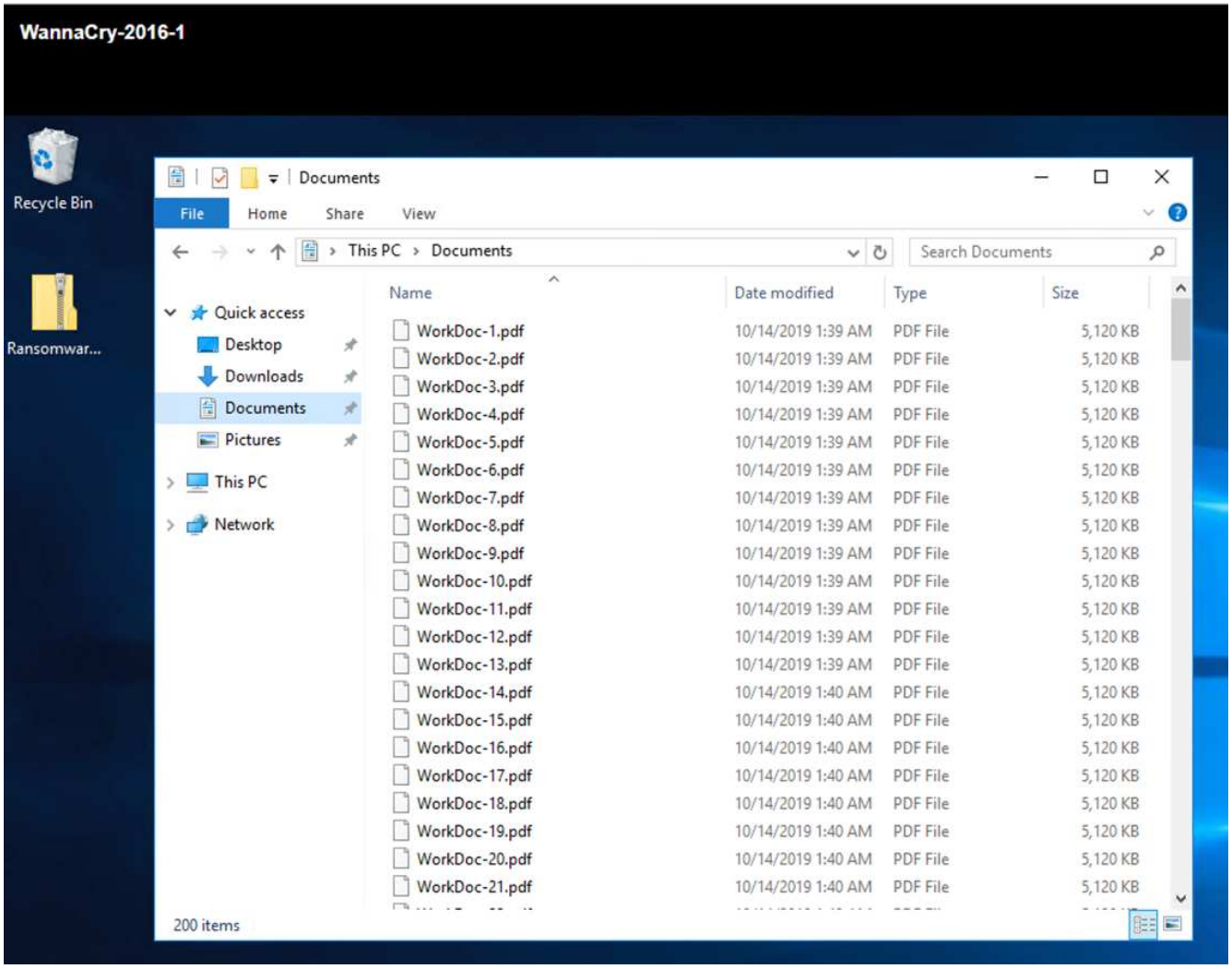
3. Die gesamte VM wird wiederhergestellt und neu gestartet.



4. Klicken Sie auf Fertig stellen, um den Wiederherstellungsvorgang zu starten.



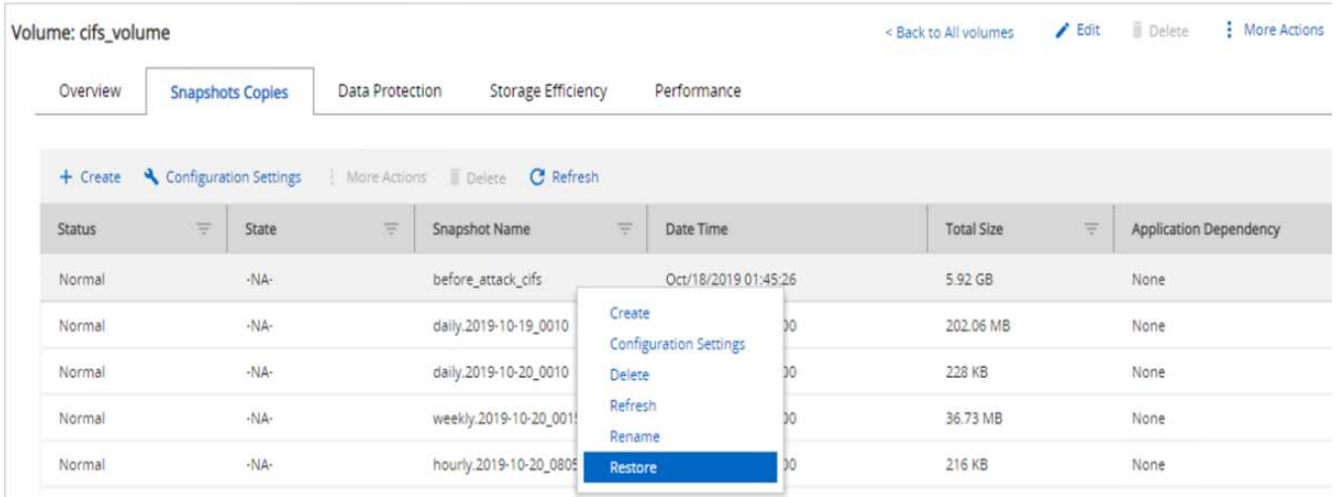
5. Die VM und ihre Dateien sind wiederhergestellt.



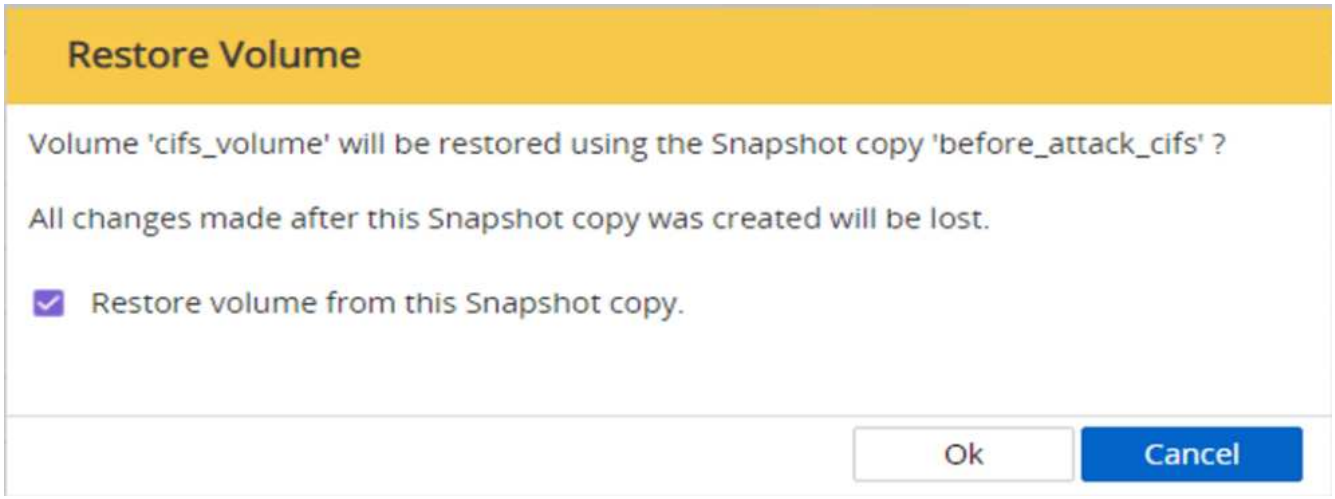
CIFS-Freigabe wiederherstellen

Gehen Sie wie folgt vor, um die CIFS-Freigabe wiederherzustellen:

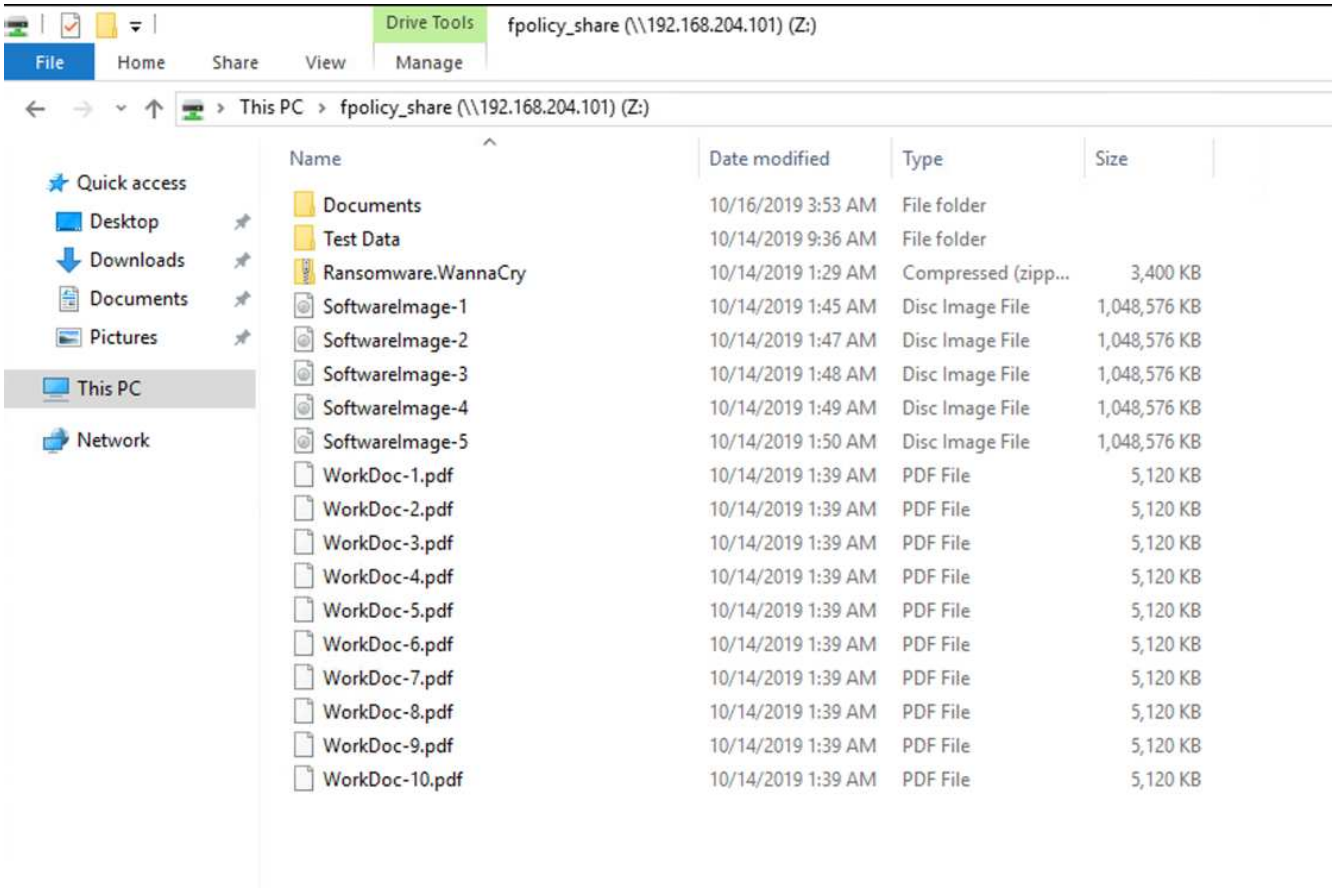
1. Verwenden Sie die Snapshot-Kopie des vor dem Angriff aufgenommene Volumes, um die Freigabe wiederherzustellen.



2. Klicken Sie auf OK, um den Wiederherstellungsvorgang zu starten.



3. Zeigen Sie die CIFS-Freigabe nach der Wiederherstellung an.



Fall 2: WannaCry verschlüsselt Dateisystem innerhalb der VM und versucht, die zugewiesene CIFS-Freigabe zu verschlüsseln, die durch FPolicy geschützt ist

Prävention

FPolicy konfigurieren

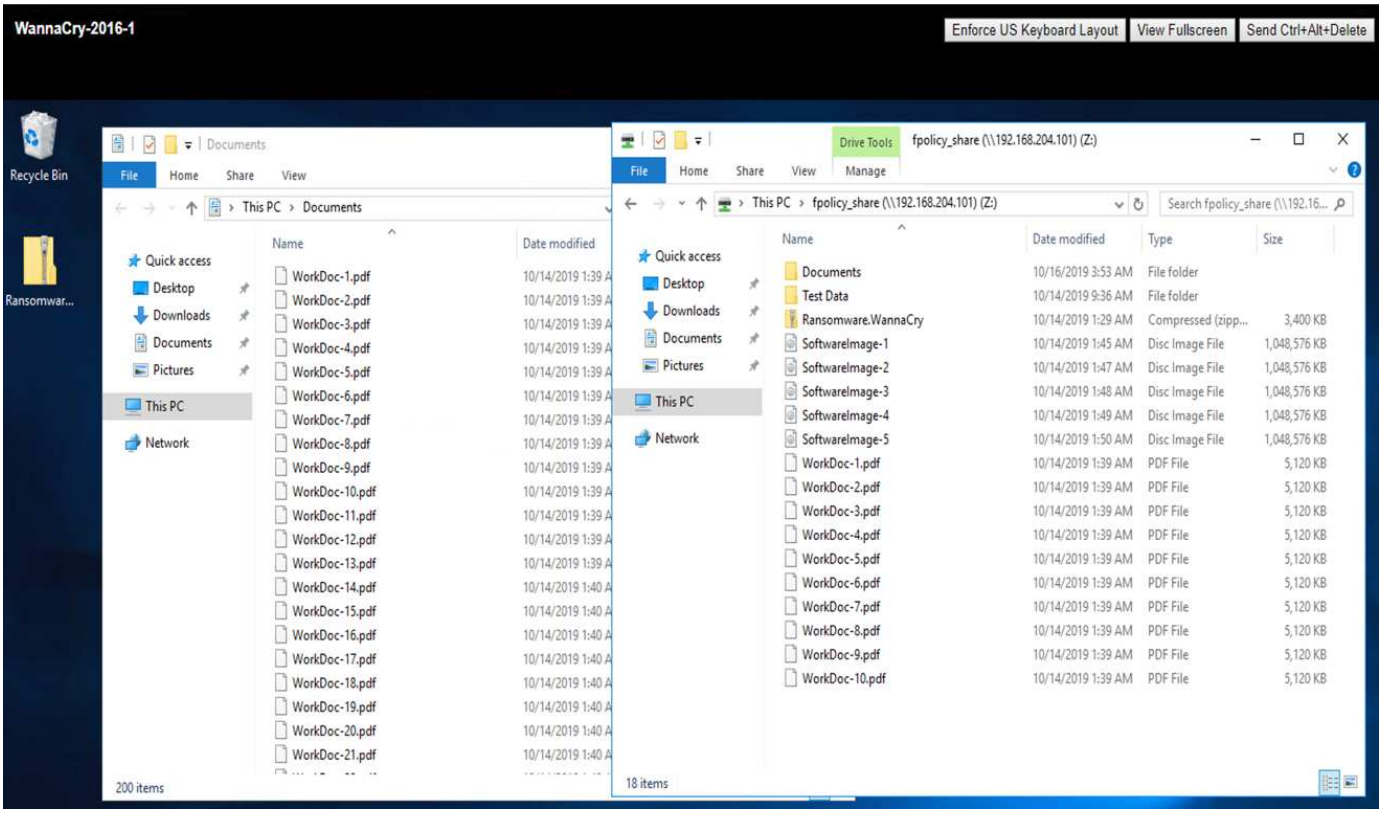
Führen Sie die folgenden Befehle auf dem ONTAP-Cluster aus, um FPolicy auf der CIFS-Freigabe zu

konfigurieren:

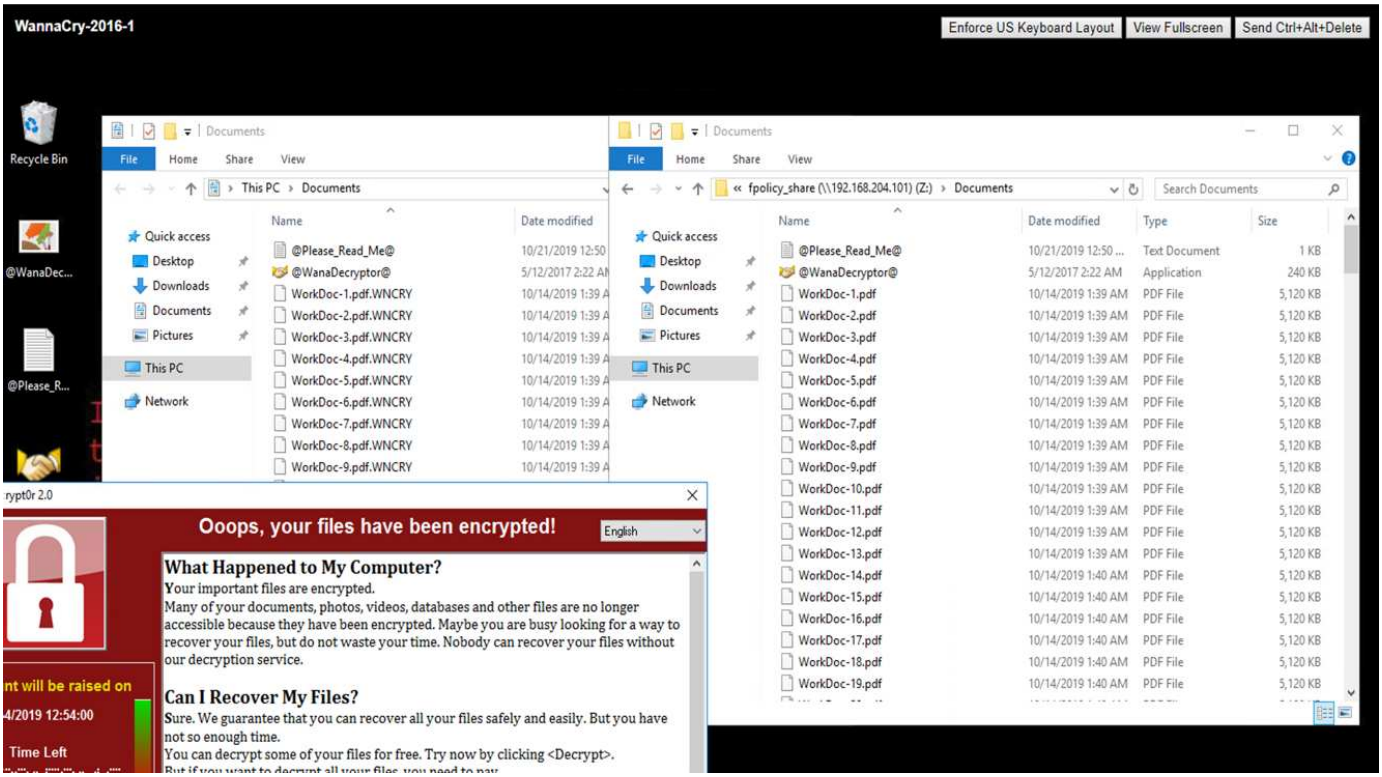
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Mit dieser Richtlinie sind Dateien mit den Erweiterungen WNCRY, Locky und ad4c nicht berechtigt, die Dateivorgänge zum Erstellen, Umbenennen, Schreiben oder Öffnen auszuführen.

Anzeigen des Status von Dateien vor dem Angriff – sie sind unverschlüsselt und in einem sauberen System.



Die Dateien auf der VM sind verschlüsselt. Die WannaCry Malware versucht, die Dateien in der CIFS-Share zu verschlüsseln, aber FPolicy verhindert, dass sie die Dateien zu beeinflussen.



Geschäftsbetrieb ohne Lösegeld fortsetzen

Die in diesem Dokument beschriebenen NetApp Funktionen helfen Ihnen, Daten innerhalb weniger Minuten nach einem Angriff wiederherzustellen und Angriffe an erster Stelle zu vermeiden, sodass der Geschäftsbetrieb ungehindert weitergeführt werden kann.

Sie können einen Zeitplan für Snapshot Kopien festlegen, um die gewünschte Recovery-Zeitvorgabe (Recovery Point Objective, RPO) zu erfüllen. Auf Snapshot Kopien basierende Wiederherstellungsvorgänge sind sehr schnell. Somit kann ein sehr geringes Recovery Time Objective (RTO) erreicht werden.

Vor allem müssen Sie kein Lösegeld als Folge eines Angriffs zahlen, und Sie können schnell wieder zu normalen Operationen.

Schlussfolgerung

Ransomware ist ein Produkt der organisierten Kriminalität und die Angreifer arbeiten nicht mit ethischen Werten. Sie können den Schlüssel zur Entschlüsselung auch nach Erhalt des Lösegeld nicht zur Verfügung stellen. Die Opfer verlieren nicht nur ihre Daten, sondern sie gehen auch deutlich über die mit dem Verlust von Produktionsdaten verbundenen Konsequenzen nach.

Laut A "Forbes-Artikel", Nur 19% der Ransomware-Opfer bekommen ihre Daten nach dem Lösegeld zurück. Daher empfehlen die Autoren, im Falle eines Angriffs kein Lösegeld zu zahlen, weil dies den Glauben des Angreifers an ihr Geschäftsmodell stärkt.

Backup- und Restore-Prozesse spielen bei der Ransomware-Recovery eine wichtige Rolle. Daher müssen sie als integraler Bestandteil der Geschäftsplanung einbezogen werden. Die Implementierung dieser Vorgänge sollte so geplant werden, dass die Recovery-Funktionen bei einem Angriff keine Kompromisse eingehen.

Entscheidend ist dabei, den richtigen Technologiepartner auf diesem Weg zu wählen. FlexPod stellt die meisten erforderlichen Funktionen nativ und ohne zusätzliche Kosten in einem All-Flash FAS System zur Verfügung.

Danksagungen

Der Autor dankt den folgenden Personen für ihre Unterstützung bei der Erstellung dieses Dokuments:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Weitere Informationen

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

- NetApp Snapshot Software

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- SnapCenter Backup-Management

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- SnapLock Datenkonformität

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- NetApp Produktdokumentation

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen

TR-4892: FIPS 140-2 Security-konforme FlexPod Lösung für das Gesundheitswesen

JayaKishore Esanakula, NetApp John McAbel, Cisco

Das Health Information Technology for Economic and Clinical Health Act (HITECH) erfordert die Federal Information Processing Standard (FIPS) 140-2-validierte

Verschlüsselung elektronischer geschützter Gesundheitsdaten (ePHI). Anwendungen und Software FÜR den Bereich Health Information Technology (HITS) müssen mit FIPS 140-2 konform sein, um die Zertifizierung zum Promoting Interoperability Program (ehemals sinnvoller Einsatz des Incentive-Programms) zu erhalten. Teilnahmeberechtigte Anbieter und Krankenhäuser müssen einen FIPS 140-2 (Level 1)-konformen TREFFER für die Aufnahme von Incentives für Medicare und Medicaid sowie die Vermeidung von Kostenerstattungen durch das Center for Medicare and Medicaid (CMS) verwenden. Nach FIPS 140-2 zertifizierte Verschlüsselungsalgorithmen gelten als technische Sicherheitsmaßnahmen, die gemäß der erforderlich sind "Sicherheitsregel" Des Health Information Portability and Accountability Act (HIPAA).

FIPS 140-2 ist eine USA Dieser Standard erfüllt die Sicherheitsanforderungen für kryptografische Module in Hardware, Software und Firmware, die sensible Daten schützen. Die Einhaltung der Standards ist für die Verwendung durch die USA vorgeschrieben Regierungsbehörden und IT wird häufig auch in regulierten Branchen wie Finanzdienstleistungen und Gesundheitswesen eingesetzt. Dieser technische Bericht hilft dem Leser, den FIPS 140-2-Sicherheitsstandard auf hohem Niveau zu verstehen. Außerdem hilft es dem Publikum, verschiedene Bedrohungen zu verstehen, denen Organisationen im Gesundheitswesen gegenüberstehen. Außerdem hilft der technische Bericht einem zu verstehen, wie ein FIPS 140-2-konformes FlexPod System zum Schutz von Gesundheitsressourcen bei der Implementierung auf einer konvergenten FlexPod Infrastruktur beitragen kann.

Umfang

Dieses Dokument bietet eine technische Übersicht zu einem Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS und einer auf NetApp ONTAP basierenden FlexPod Infrastruktur zum Hosten von IT-Applikationen oder Lösungen im Gesundheitswesen, die FIPS 140-2 Sicherheit erfordern.

Zielgruppe

Dieses Dokument richtet sich an technische Leiter im Gesundheitswesen sowie an Lösungstechniker von Cisco und NetApp Partnern und Professional Services-Mitarbeiter. NetApp geht davon aus, dass der Leser gute Kenntnisse der Konzepte zur Berechnung der Storage- und Computing-Größenbemessung sowie der technischen Vertrautheit mit Bedrohungen für das Gesundheitswesen, mit der Sicherheit im Gesundheitswesen, MIT IT-Systemen im Gesundheitswesen, mit Cisco UCS und NetApp Storage-Systemen hat.

"Die nächste: Cyber-Sicherheitsbedrohungen im Gesundheitswesen."

Cyber-Sicherheitsbedrohungen im Gesundheitswesen

"Zurück: Einführung."

Jedes Problem stellt eine neue Chance dar – ein Beispiel für eine solche Chance wird von der COVID-Pandemie präsentiert. Laut A "Bericht" Durch das Department of Health and Human Services (HHS) Cybersecurity Program hat die COVID-Antwort zu einer erhöhten Anzahl von Ransomware-Angriffen geführt. In der dritten Märzwoche 2020 wurden 6,000 neue Internet-Domains registriert. Mehr als 50 % der Domänen haben Malware gehostet. Ransomware-Angriffe verliefen 2020 fast 50 % aller Datenschutzverstöße im Gesundheitswesen mit Auswirkungen auf mehr als 630 Organisationen im Gesundheitswesen und rund 29 Millionen Datensätze im

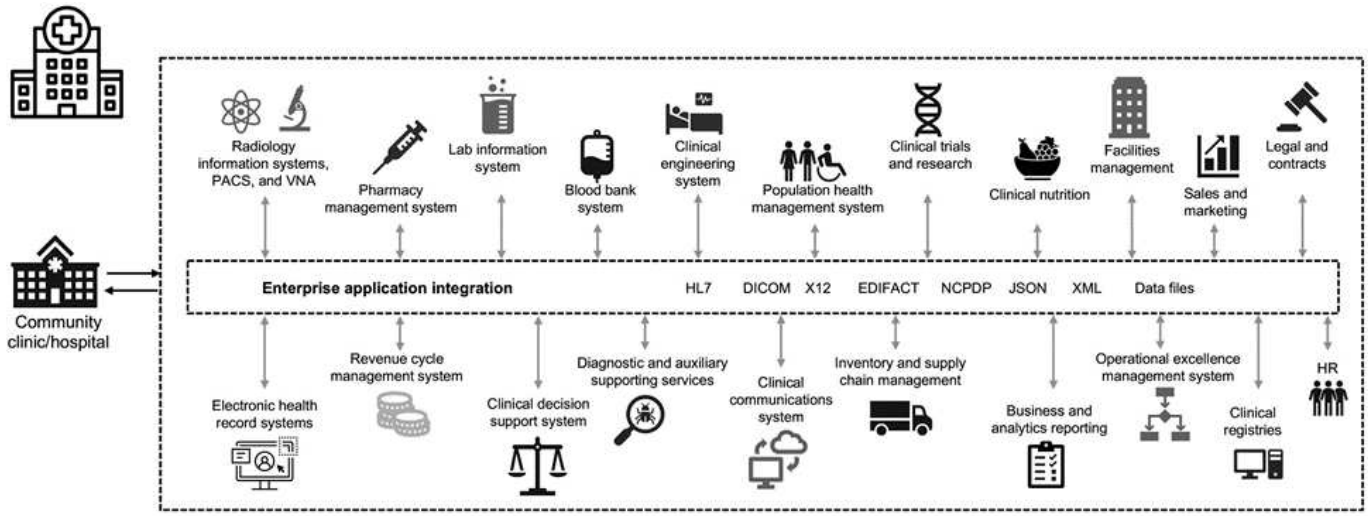
Gesundheitswesen. 19 Leaker/Sites verdoppelten die Erpressung. Mit 24.5 % Sicherheitsverletzungen hat sich die Branche im Jahr 2020 die höchste Anzahl von Datenverletzungen festgestellt.

Böswillige Mitarbeiter versuchten, die Sicherheit und den Datenschutz von geschützten Gesundheitsdaten (PHI) zu verletzen, indem sie die Informationen verkaufen oder sie bedrohen, sie zu zerstören oder auszusetzen. Es werden häufig gezielte und Massenübertragungsversuche unternommen, um sich unbefugten Zugriff auf ePHI zu verschaffen. Rund 75 % der exponierten Patientenakten im zweiten Halbjahr 2020 waren auf kompromittierte Geschäftspartner zurückzuführen.

Die folgende Liste der Gesundheitseinrichtungen wurde von den böswilligen Agenten ins Visier gesetzt:

- Krankenhaussysteme
- Life-Science-Labore
- Forschungslabors
- Rehabilitationseinrichtungen
- Kommune Krankenhäuser und Kliniken

Die Vielfalt der Applikationen, die ein Gesundheitswesen ausmachen, ist unbestreitbar und wird zunehmend komplexer. Büros für Informationssicherheit stehen vor der Herausforderung, eine Governance für eine Vielzahl VON IT-Systemen und -Assets zu gewährleisten. Die folgende Abbildung zeigt die klinischen Möglichkeiten eines typischen Krankenhaussystems.



Patientendaten bilden das Herzstück dieses Bildes. Der Verlust von Patientendaten und das Stigma, das mit sensiblen Erkrankungen verbunden ist, sind sehr real. Weitere sensible Themen sind das Risiko sozialer Ausgrenzung, Erpressung, Profiling, die Anfälligkeit für zielgerichtetes Marketing, Ausbeutung und die mögliche finanzielle Haftung gegenüber Kostenträgern über medizinische Informationen jenseits der Privilegien des Zahlers.

Bedrohungen für die Gesundheit sind multidimensional in der Natur und in der Wirkung. Regierungen weltweit haben verschiedene Bestimmungen zur Sicherung von ePHI erlassen. Die schädlichen Auswirkungen und die sich immer weiter entwickelnden Bedrohungen für das Gesundheitswesen erschweren es Organisationen im Gesundheitswesen, alle Bedrohungen zu schützen.

Im Folgenden finden Sie eine Liste der häufigsten Bedrohungen, die im Gesundheitswesen identifiziert werden:

- Ransomware-Angriffe
- Verlust oder Diebstahl von Geräten oder Daten mit vertraulichen Informationen
- Phishing-Angriffe
- Angriffe auf angeschlossene medizinische Geräte, die die Patientensicherheit beeinträchtigen können
- E-Mail-Phishing-Angriffe
- Verlust oder Diebstahl von Geräten oder Daten
- Protokollkompromiss für Remote Desktops
- Softwareschwachstelle

Einrichtungen im Gesundheitswesen arbeiten in juristischen und gesetzlichen Regelungen, die so kompliziert sind wie ihre digitalen Ökosysteme. Zu dieser Umgebung gehören u. a. die folgenden:

- Office des National Coordinators (for Healthcare Technology) ONC-zertifizierte Standards für Interoperabilität in der elektronischen Gesundheitsinformationstechnologie
- Medicare Access und das Kinderversicherungsprogramm ReacreAuthorization Act (MACRA)/sinnvolle Nutzung
- Mehrfachverpflichtungen nach der Food and Drug Administration (FDA)
- Die Gemeinsame Akkreditierungsverfahren der Kommission
- HIPAA-Anforderungen erfüllt
- Anforderungen von HITECH
- Mindeststandards für akzeptable Risiken für Kostenträger
- Datenschutzregeln und Sicherheitsregeln
- Anforderungen des Bundesgesetzes zur Modernisierung der Informationssicherheit, die in Bundesverträge und Forschungszuschüsse von Behörden wie den nationalen Gesundheitseinrichtungen aufgenommen werden
- Payment Card Industry Data Security Standard (PCI-DSS)
- Substanzmissbrauch und Mental Health Services Administration (SAMHSA) Anforderungen
- Der Gramm-Leach-Bliley Act für die Finanzverarbeitung
- Das Stark-Gesetz bezieht sich auf die Erbringung von Dienstleistungen an verbundene Organisationen
- Family Educational Rights and Privacy Act (FERPA) für Institutionen, die an der Hochschulbildung teilnehmen
- Genetic Information Nondiscrimination Act (GINA)
- Die neue Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union

Die Standards der Sicherheitsarchitektur entwickeln sich rasant weiter, um zu verhindern, dass böswillige Akteure ein System der Gesundheitsinformationen beeinträchtigen. Einer dieser Standards ist FIPS 140-2, definiert durch das National Institute of Standards and Technology (NIST). Die FIPS-Veröffentlichung 140-2 enthält Angaben zu den USA Behördliche Anforderungen für ein kryptografisches Modul. Die Sicherheitsanforderungen decken Bereiche ab, die sich auf eine sichere Konstruktion und Implementierung eines kryptografischen Moduls beziehen und können auf EINEN TREFFER angewendet werden. Klar definierte kryptografische Grenzen sorgen für ein einfacheres Sicherheitsmanagement und bleiben mit den kryptografischen Modulen auf dem aktuellen Stand. Diese Grenzen verhindern schwache Crypto-Module, die problemlos von böswilligen Akteuren genutzt werden können. Sie können auch menschliche Fehler beim Management von Standard-kryptografischen Modulen verhindern.

NIST hat zusammen mit dem Communications Security Establishment (CSE) das Cryptographic Module Validation Program (CMVP) eingerichtet, um kryptografische Module für FIPS 140-2 Validierungsstufen zu zertifizieren. Mithilfe eines FIPS 140-2-2-zertifizierten Moduls sind Bundesbehörden zum Schutz sensibler oder wertvoller Daten während der Übertragung und im Ruhezustand verpflichtet. Aufgrund des Erfolgs beim Schutz sensibler oder wertvoller Informationen haben sich viele Gesundheitssysteme für die Verschlüsselung von ePHI entschieden, indem FIPS 140-2-2-kryptografische Module verwendet werden, die über das gesetzlich geforderte Mindestsicherheitsniveau hinausgehen.

Die Nutzung und Implementierung der FlexPod FIPS 140-2 Funktionen dauert nur Stunden (nicht Tage). Die FIPS-Compliance-Konformität ist für die meisten Unternehmen im Gesundheitswesen verfügbar, unabhängig von der Größe. Mit klar definierten kryptografischen Grenzen und gut dokumentierten und einfachen Implementierungsschritten legt eine FIPS 140-2-2-konforme FlexPod-Architektur solide Sicherheitsgrundlage für die Infrastruktur fest und ermöglicht einfache Verbesserungen zur weiteren Erhöhung des Schutzes von Sicherheitsbedrohungen.

"Weiter: Überblick über FIPS 140-2."

Überblick über FIPS 140-2

"Früher: Cybersicherheitsbedrohungen im Gesundheitswesen."

"FIPS 140-2" Gibt die Sicherheitsanforderungen für ein kryptografisches Modul an, das in einem Sicherheitssystem verwendet wird, das vertrauliche Informationen in Computer- und Telekommunikationssystemen schützt. Ein kryptografisches Modul sollte aus Hardware, Software, Firmware oder einer Kombination verschiedener Komponenten besteht. FIPS gilt für die kryptografischen Algorithmen, die Schlüsselgenerierung und den Schlüsselmanager, die sich innerhalb einer kryptografischen Grenze befinden. Es ist wichtig zu wissen, dass sich FIPS 140-2 speziell auf das kryptografische Modul bezieht, nicht auf das Produkt, die Architektur, die Daten oder das Ecosystem. Das kryptografische Modul, das in den Schlüsselbegriffen später in diesem Dokument definiert wird, ist die spezifische Komponente (ob Hardware, Software und/oder Firmware), die zugelassene Sicherheitsfunktionen implementiert. Zudem gibt FIPS 140-2 vier Level an. Genehmigte kryptografische Algorithmen sind auf allen Ebenen gemeinsam. Zu den wichtigsten Elementen und Anforderungen der einzelnen Sicherheitsstufen gehören:

- **Sicherheitsstufe 1**
  - Legt grundlegende Sicherheitsanforderungen für ein kryptografisches Modul fest (mindestens ein genehmigter Algorithmus oder eine Sicherheitsfunktion ist erforderlich).
  - Für Stufe 1 über die grundlegenden Anforderungen für produktionsbereite Komponenten hinaus sind keine festgelegten physischen Sicherheitsmechanismen erforderlich.
- **Sicherheitsstufe 2**
  - Erweitert die physikalischen Sicherheitsmechanismen durch Hinzufügen der Notwendigkeit für Manipulationsbeweise durch die Verwendung von manipulationssicheren Lösungen wie Beschichtungen oder Dichtungen, Verriegelungen an abnehmbaren Abdeckungen oder Türen der kryptografischen Module.
  - Erfordert mindestens die rollenbasierte Zugriffssteuerung (Role-Based Access Control, RBAC), bei der das kryptografische Modul die Autorisierung eines Bedieners oder Administrators authentifiziert, eine bestimmte Rolle anzunehmen und entsprechende Funktionen auszuführen.

- **Sicherheitsstufe 3**
  - Baut auf den manipulationssicheren Anforderungen der Stufe 2 auf und versucht, einen weiteren Zugriff auf kritische Sicherheitsparameter (CSPs) innerhalb des kryptografischen Moduls zu verhindern.
  - Physische Sicherheitsmechanismen, die auf Ebene 3 erforderlich sind, sollen eine hohe Wahrscheinlichkeit haben, Versuche auf physischen Zugriff zu erkennen und darauf zu reagieren, oder jede Verwendung oder Änderung des kryptografischen Moduls. Beispiele dafür sind starke Gehäuse, Sabotagedetektion und Reaktionsschaltungen, die alle Klartext-CSPs aufzählen, wenn eine abnehmbare Abdeckung auf dem kryptografischen Modul geöffnet wird.
  - Erfordert identitätsbasierte Authentifizierungsmechanismen zur Verbesserung der Sicherheit der in Level 2 angegebenen RBAC-Mechanismen. Ein kryptografisches Modul authentifiziert die Identität eines Operators und stellt sicher, dass der Operator berechtigt ist, eine Rolle zu verwenden und die Funktionen der Rolle auszuführen.
- **Sicherheitsstufe 4**
  - Höchster Sicherheitsgrad in FIPS 140-2.
  - Die nützlichste Stufe für Vorgänge in physisch ungeschützten Umgebungen
  - Auf dieser Ebene sollen die physischen Sicherheitsmechanismen einen vollständigen Schutz um das kryptografische Modul gewährleisten, der dafür verantwortlich ist, unbefugte physische Zugriffsversuche zu erkennen und darauf zu reagieren.
  - Das Eindringen oder Eindringen des kryptografischen Moduls sollte eine hohe Erkennungswahrscheinlichkeit haben und zur sofortigen Zeroisierung aller unsicheren oder plaintext CSPs führen.

"Nächster: Kontrollebene oder Datenebene."

Kontrollebene oder Datenebene

"Zurück: Übersicht von FIPS 140-2."

Bei der Implementierung einer FIPS 140-2-2-Strategie ist es wichtig zu verstehen, welche Daten geschützt werden. Diese kann leicht in zwei Bereiche unterteilt werden: Kontrollebene und Datenebene. Eine Kontrollebene bezieht sich auf die Aspekte, die Einfluss auf die Kontrolle und den Betrieb der Komponenten im FlexPod System haben, z. B. Administratorzugriff auf die NetApp Storage Controller, Cisco Nexus Switches und Cisco UCS Server. Der Schutz auf dieser Ebene wird durch die Einschränkung der Protokolle und kryptografischen Cypher ermöglicht, mit denen Administratoren Geräte verbinden und Änderungen vornehmen können. In einer Datenebene werden die tatsächlichen Informationen, wie zum Beispiel PHI, innerhalb des FlexPod-Systems bezeichnet. Diese wird durch Verschlüsselung von Daten im Ruhezustand und bei FIPS geschützt, sodass die verwendeten kryptografischen Module die Standards erfüllen.

"Als Nächstes: FlexPod Cisco UCS Computing und FIPS 140"

FlexPod Cisco UCS Computing und FIPS 140-2

"Zurück: Kontrollebene vs. Datenebene."

Eine FlexPod Architektur kann mit einem Cisco UCS Server konzipiert werden, der FIPS

140-2 konform ist. Gemäß der U. S. NIST, Cisco UCS Server können im Compliance-Modus nach FIPS 140-2 Level 1 betrieben werden. Eine vollständige Liste FIPS-konformer Cisco Komponenten finden Sie unter "Cisco FIPS 140 Seite". Cisco UCS Manager ist nach FIPS 140-2 zertifiziert.

Cisco UCS und Fabric Interconnect

Der Cisco UCS Manager ist implementiert und läuft über die Cisco Fabric Interconnects (FIS).

Weitere Informationen zum Cisco UCS und zur Aktivierung von FIPS finden Sie im "Dokumentation zu Cisco UCS Manager".

Um den FIPS-Modus auf dem Cisco Fabric Interconnect auf jedem Fabric A und B zu aktivieren, führen Sie die folgenden Befehle aus:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Um eine FI in einem Cluster auf Cisco UCS Manager Release 3.2(3) durch EINE FI-FUNKTION auf einer älteren Version als Cisco UCS Manager Release 3.2(3) zu ersetzen, deaktivieren Sie den FIPS-Modus (deaktivieren `fips-mode`) Auf dem vorhandenen FI vor dem Hinzufügen der Ersatz-FI zum Cluster. Nach der Bildung des Clusters wird der FIPS-Modus als Teil des Starts des Cisco UCS Managers automatisch aktiviert.

Cisco bietet die folgenden wichtigen Produkte, die auf Computing- oder Applikationsebene implementiert werden können:

- **Cisco Advanced Malware Protection (AMP) für Endpunkte.** unterstützt auf Microsoft Windows- und Linux-Betriebssystemen bietet diese Lösung Funktionen für Prävention, Erkennung und Reaktion. Diese Sicherheitssoftware verhindert Verstöße, blockiert Malware am Einstiegspunkt und überwacht und analysiert kontinuierlich die Datei- und Prozessaktivitäten, um Bedrohungen schnell zu erkennen, einzudämmen und zu beseitigen, die den Schutz vor der Front-Line-Lösung ausweichen können. Die Komponente „bösartiger Aktivitätsschutz“ (MAP) von AMP überwacht kontinuierlich alle Endpoint-Aktivitäten und ermöglicht die Laufzeiterkennung und das Blockieren des anormalen Verhaltens eines laufenden Programms auf dem Endpunkt. Wenn beispielsweise das Endpunktverhalten auf Ransomware hinweist, werden die abgebrochene Prozesse beendet, um Endpunktverschlüsselung zu verhindern und den Angriff zu stoppen.
- **AMP für E-Mail-Sicherheit.** E-Mails sind das Hauptfahrzeug, um Malware zu verbreiten und Cyberangriffe auszuführen. Im Durchschnitt werden an einem einzigen Tag rund 100 Milliarden E-Mails ausgetauscht, die Angreifern einen ausgezeichneten Penetrationsvektor in die Systeme des Benutzers bieten. Daher ist es absolut unerlässlich, sich gegen diese Angriffslinie zu verteidigen. AMP analysiert E-Mails auf Bedrohungen wie Zero-Day-Exploits und entstickende Malware, die in bösartigen Anhängen verborgen sind. Darüber hinaus nutzt es branchenführende URL-Informationen, um schädliche Links zu bekämpfen. Anwender erhalten erweiterten Schutz vor Spear-Phishing, Ransomware und anderen anspruchsvollen Angriffen.
- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS kann als physische Appliance im Datacenter oder als virtuelle Appliance auf VMware (NGIPSv für VMware) eingesetzt werden. Dieses hocheffiziente Abwehrsystem für Angriffe sorgt für zuverlässige Leistung und niedrige Gesamtbetriebskosten. Der Schutz vor Bedrohungen kann durch optionale Abonnementlizenzen erweitert

werden, um AMP, Transparenz und Kontrolle von Anwendungen sowie URL-Filterfunktionen bereitzustellen. Das virtualisierte NGIPS überprüft den Datenverkehr zwischen Virtual Machines (VMs) und vereinfacht die Bereitstellung und das Management von NGIPS-Lösungen an Standorten mit begrenzten Ressourcen. Dadurch wird der Schutz sowohl für physische als auch für virtuelle Ressourcen erhöht.

"Als Nächstes: Cisco Networking mit FlexPod und FIPS 140-2"

FlexPod Cisco Networking und FIPS 140-2

"Früher: FlexPod Cisco UCS Computing und FIPS 140-2."

Cisco MDS

Plattform der Cisco MDS 9000 Serie mit Software 8.4.x ist "FIPS 140-2 konform". Cisco MDS implementiert kryptografische Module und folgende Services für SNMPv3 und SSH.

- Sitzungseinrichtung unterstützt jeden Service
- Alle zugrunde liegenden kryptografischen Algorithmen, die die wichtigsten Ableitfunktionen der Dienste unterstützen
- Hashing für jeden Service
- Symmetrische Verschlüsselung für jeden Service

Führen Sie vor Aktivierung des FIPS-Modus die folgenden Aufgaben auf dem MDS-Switch aus:

1. Geben Sie Ihren Passwörtern mindestens acht Zeichen lang.
2. Deaktivieren Sie Telnet. Benutzer sollten sich nur mit SSH einloggen.
3. Deaktivieren Sie die Remote-Authentifizierung über RADIUS/TACACS+. Nur lokale Benutzer des Switches können authentifiziert werden.
4. Deaktivieren Sie SNMP v1 und v2. Alle bestehenden Benutzerkonten auf dem Switch, die für SNMPv3 konfiguriert wurden, sollten nur mit SHA für die Authentifizierung und AES/3DES für den Datenschutz konfiguriert werden.
5. VRRP deaktivieren.
6. Löschen Sie alle IKE-Richtlinien, die MD5 für die Authentifizierung oder DES für die Verschlüsselung besitzen. Ändern Sie die Richtlinien, sodass sie SHA für die Authentifizierung und 3DES/AES für die Verschlüsselung verwenden.
7. Löschen Sie alle SSH Server RSA1-Tastenfelder.

Gehen Sie wie folgt vor, um den FIPS-Modus zu aktivieren und den FIPS-Status auf dem MDS-Switch anzuzeigen:

1. Zeigt den FIPS-Status an.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Richten Sie den 2048-Bit-SSH-Schlüssel ein.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Aktivieren Sie den FIPS-Modus.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Zeigt den FIPS-Status an.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Speichern Sie die Konfiguration in der laufenden Konfiguration.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Starten Sie den MDS-Switch neu

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Zeigt den FIPS-Status an.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Weitere Informationen finden Sie unter "Aktivieren des FIPS-Modus".

Cisco Nexus

Die Switches der Cisco Nexus 9000 Serie (Version 9.3) sind "FIPS 140-2 konform". Cisco Nexus implementiert kryptografische Module und die folgenden Services für SNMPv3 und SSH.

- Sitzungseinrichtung unterstützt jeden Service
- Alle zugrunde liegenden kryptografischen Algorithmen, die die wichtigsten Ableitfunktionen der Dienste unterstützen
- Hashing für jeden Service
- Symmetrische Verschlüsselung für jeden Service

Führen Sie vor Aktivierung des FIPS-Modus die folgenden Aufgaben auf dem Cisco Nexus-Switch aus:

1. Deaktivieren Sie Telnet. Benutzer sollten sich nur mit Secure Shell (SSH) anmelden.
2. Deaktivieren Sie SNMPv1 und v2. Alle bestehenden Benutzerkonten auf dem Gerät, die für SNMPv3 konfiguriert wurden, sollten nur mit SHA für die Authentifizierung und AES/3DES für den Datenschutz konfiguriert werden.
3. Löschen Sie alle SSH-Server RSA1-Schlüsselpaare.
4. Aktivieren Sie die HMAC-SHA1-Nachrichtenintegritätsprüfung (MIC) für die Verwendung während der Aushandlung des Cisco TrustSec Security Association Protocol (SAP). Geben Sie dazu den sap-Hash-Algorithmus ein `HMAC-SHA-1` Befehl aus dem `cts-manual` Oder `cts-dot1x` Modus.

Gehen Sie wie folgt vor, um den FIPS-Modus auf dem Nexus Switch zu aktivieren:

1. Einrichten des SSH-Schlüssels mit 2048 Bit.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Richten Sie den 2048-Bit-SSH-Schlüssel ein.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Aktivieren Sie den FIPS-Modus.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Starten Sie den Nexus Switch neu.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Zeigt den FIPS-Status an.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Darüber hinaus unterstützt die Cisco NX OS-Software die NetFlow-Funktion, die eine verbesserte Erkennung von Netzwerkanomalien und -Sicherheit ermöglicht. NetFlow erfasst die Metadaten jedes Gesprächs im Netzwerk, die an der Kommunikation beteiligten Parteien, das verwendete Protokoll und die Dauer der Transaktion. Nachdem die Informationen aggregiert und analysiert wurden, können sie einen Einblick in das normale Verhalten geben. Die gesammelten Daten ermöglichen außerdem die Identifizierung fragwürdiger Aktivitätsmuster, wie etwa die Verbreitung von Malware im Netzwerk, die ansonsten unbemerkt bleiben kann. NetFlow verwendet Flows, um Statistiken für die Netzwerküberwachung bereitzustellen. Ein Flow ist ein unidirektionaler Strom von Paketen, der auf einer Quellschnittstelle (oder VLAN) ankommt und die gleichen Werte für die Schlüssel hat. Ein Schlüssel ist ein identifizierter Wert für ein Feld innerhalb des Pakets. Sie erstellen einen Flow mithilfe eines Flow-Datensatzes, um die eindeutigen Tasten für Ihren Flow zu definieren. Sie können die Daten, die NetFlow für Ihre Ströme sammelt, mit Hilfe eines Flow-Exporterers in einen Remote NetFlow Collector, wie z. B. Cisco Stealthwatch, exportieren. Stealthwatch verwendet diese Informationen für die kontinuierliche Überwachung des Netzwerks und bietet Bedrohungserkennung in Echtzeit sowie eine Forensik zum Vorfallsreaktion, falls ein Ransomware-Ausbruch auftritt.

"Als Nächstes: FlexPod ONTAP Storage und FIPS 140"

FlexPod NetApp ONTAP Storage und FIPS 140-2

"Früher: FlexPod Networking mit Cisco und FIPS 140-2."

NetApp bietet verschiedene Hardware, Software und Services, die verschiedene Komponenten der im Rahmen des Standards validierten kryptografischen Module umfassen können. Daher verwendet NetApp verschiedene Ansätze zur Einhaltung von FIPS 140-2 für die Kontrollebene und Datenebene:

- NetApp umfasst kryptografische Module, die eine Level-1-Validierung für die Verschlüsselung von Daten während der Übertragung und Daten im Ruhezustand erzielt haben.
- NetApp übernimmt sowohl Hardware- als auch Softwaremodule, die vom Anbieter dieser Komponenten nach FIPS 140-2 validiert wurden. So nutzt die NetApp Storage Encryption Lösung beispielsweise validierte Laufwerke der FIPS Level 2.
- NetApp Produkte können ein validiertes Modul so verwenden, dass die Standards erfüllt werden, obwohl das Produkt oder die Funktion nicht innerhalb der Validierungsgrenze liegt. Beispielsweise ist NetApp Volume Encryption (NVE) FIPS 140-2-2-konform. Obwohl diese Prüfung nicht separat durchgeführt wird, nutzt sie das nach Level 1 zertifizierte NetApp kryptografische Modul. Weitere Informationen zu Compliance-Besonderheiten für Ihre ONTAP Version erhalten Sie bei Ihrem FlexPod SME.

NetApp Cryptographic Module sind nach FIPS 140-2 Level 1 zertifiziert

- Das NetApp Cryptographic Security Module (NCSM) ist nach FIPS 140-2 Level 1 zertifiziert.

Die Self-Encrypting Drives von NetApp sind nach FIPS 140-2 Level 2 zertifiziert

NetApp erwirbt Self-Encrypting Drives (SEDs), die vom ursprünglichen Equipment-Hersteller (OEM) nach FIPS 140-2 validiert wurden. Kunden, die diese Laufwerke suchen, müssen bei der Bestellung angeben. Laufwerke werden auf Ebene 2 validiert. Die folgenden NetApp Produkte können validierte SEDs nutzen:

- AFF A-Series und FAS Storage-Systeme
- E-Series und EF-Series Storage-Systeme

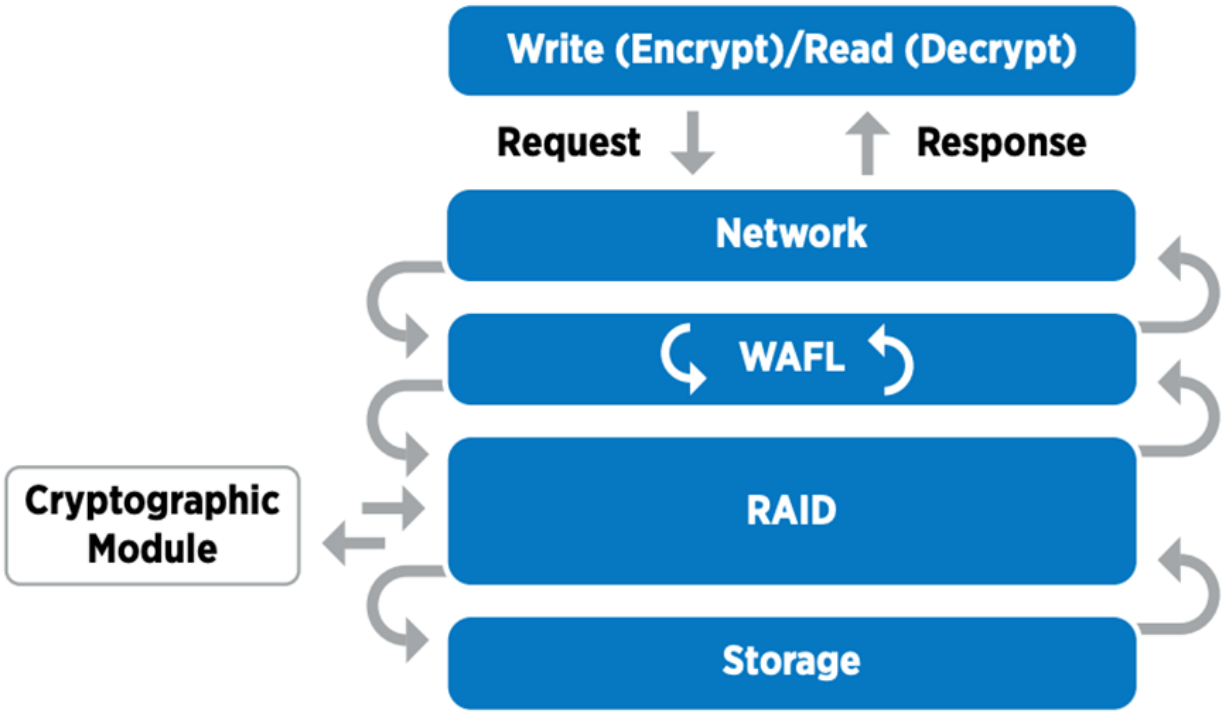
NetApp Aggregate Encryption und NetApp Volume Encryption

Die Technologien NVE und NetApp Aggregate Encryption (NAE) ermöglichen die Verschlüsselung von Daten auf Volume- und Aggregatebene. Dadurch ist die Lösung unabhängig von dem physischen Laufwerk.

NVE ist eine softwarebasierte Lösung zur Verschlüsselung von Daten im Ruhezustand, die ab ONTAP 9.1 verfügbar ist und seit ONTAP 9.2 FIPS 140-2-konform ist. Mit NVE kann ONTAP Daten mit einer Granularität pro Volume verschlüsseln. NAE, der mit ONTAP 9.6 verfügbar ist, ist ein nicht weiter ausumendes NVE-Systems. ONTAP kann Daten für jedes Volume verschlüsseln und die Volumes können Schlüssel über das Aggregat hinweg gemeinsam nutzen. Sowohl NVE als auch NAE nutzen 256-Bit-Verschlüsselung nach AES. Daten können auch ohne SEDs auf Festplatte gespeichert werden. Mit NVE und NAE können Sie Storage-Effizienzfunktionen auch bei aktivierter Verschlüsselung nutzen. Eine reine Verschlüsselung auf Applikationsebene besiegt alle Vorteile der Storage-Effizienz. Mit NVE und NAE bleiben Storage-Effizienzfunktionen erhalten, da die Daten vom Netzwerk über NetApp WAFL bis zur RAID-Schicht erfasst werden, über die bestimmt wird, ob die Daten verschlüsselt werden sollen. Für bessere Storage-Effizienz kann die Aggregatdeduplizierung mit NAE verwendet werden. NVE Volumes und NAE-Volumes können gleichzeitig im selben NAE-Aggregat bestehen. NAE-Aggregate unterstützen keine unverschlüsselten Volumes.

So funktioniert der Prozess: Wenn Daten verschlüsselt werden, wird er an das kryptografische Modul gesendet, das nach FIPS 140-2 Level 1 zertifiziert ist. Das kryptografische Modul verschlüsselt die Daten und

sendet sie zurück an die RAID-Schicht. Die verschlüsselten Daten werden dann an die Festplatte gesendet. Somit sind die Daten mit der Kombination von NVE und NAE bereits auf dem Weg zur Festplatte verschlüsselt. Lesezugriffe folgen dem umgekehrten Pfad. Mit anderen Worten: Die Daten lassen die Festplatte verschlüsselt, werden an RAID gesendet, durch das kryptografische Modul entschlüsselt und dann den Rest des Stacks, wie in der folgenden Abbildung dargestellt, hochgeschickt.



NVE kommt mit einem softwarebasierten kryptografischen Modul zum Einsatz, das nach FIPS 140-2 Level 1 zertifiziert ist.

Weitere Informationen zu NVE finden Sie im "NVE Datenblatt".

NVE schützt Daten in der Cloud. Cloud Volumes ONTAP und Azure NetApp Files bieten Daten im Ruhezustand nach FIPS 140-2-2-konform.

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig bei Nutzung der NVE-Lizenz und im integrierten oder externen Verschlüsselungsmanagement verschlüsselt. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können. Die im Aggregat erstellten Volumes werden standardmäßig verschlüsselt. Sie können den Standardwert überschreiben, wenn Sie das Volume verschlüsseln.

CLI-BEFEHLE VON ONTAP NAE

Bevor Sie die folgenden CLI-Befehle ausführen, stellen Sie sicher, dass für das Cluster die erforderliche NVE-Lizenz vorhanden ist.

Um ein Aggregat zu erstellen und zu verschlüsseln, führen Sie den folgenden Befehl aus (wenn es auf einer ONTAP 9.6 und höher Cluster CLI ausgeführt wird):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Um ein nicht-NAE-Aggregat in ein NAE-Aggregat zu konvertieren, führen Sie den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI laufen):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Um ein NAE-Aggregat in ein nicht-NAE- Aggregat zu konvertieren, führen Sie den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

CLI-BEFEHLE VON ONTAP NVE

Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können. Die im Aggregat erstellten Volumes werden standardmäßig verschlüsselt.

Führen Sie zum Erstellen eines Volumes auf einem Aggregat, das über NAE aktiviert ist, den folgenden Befehl aus (wenn Sie auf einem ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Um die Verschlüsselung eines vorhandenen Volume „inplace“ ohne Volume-Verschiebung zu aktivieren, führen Sie den folgenden Befehl aus (wenn Sie auf einer ONTAP 9.6 und höher Cluster CLI ausführen):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

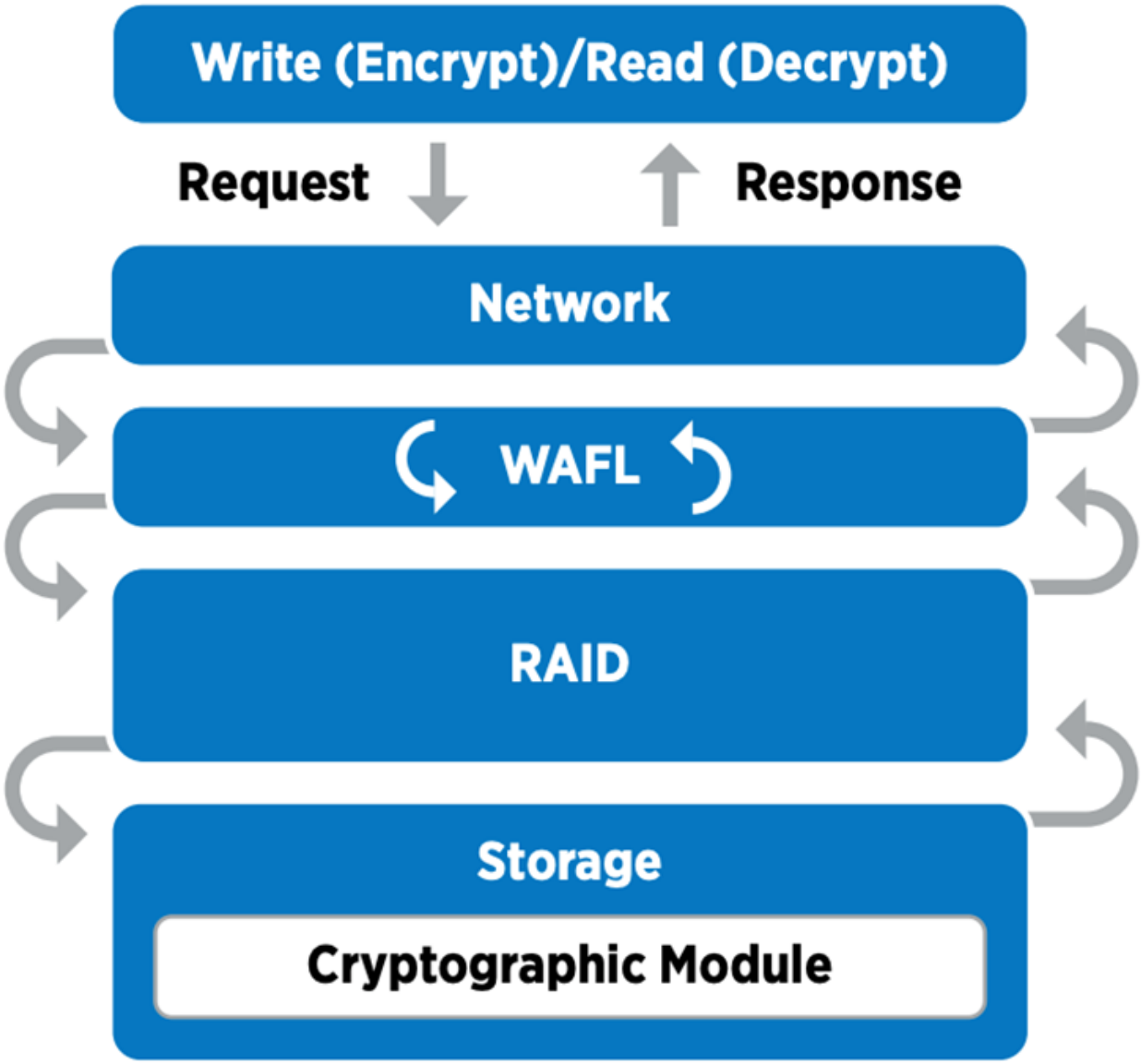
Führen Sie den folgenden CLI-Befehl aus, um zu überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE nutzt SEDs, um die Datenverschlüsselung durch einen hardwarebeschleunigten Mechanismus durchzuführen.

NSE kann mit Self-Encrypting Drives nach FIPS 140-2 Level 2 verwendet werden, um Compliance und die Rückgabe von Ersatzteilen zu ermöglichen. Dazu wird der Schutz von Daten im Ruhezustand durch transparente AES-256-Bit-Festplattenverschlüsselung ermöglicht. Die Laufwerke führen alle Datenverschlüsselungsvorgänge intern aus, wie in der folgenden Abbildung dargestellt, einschließlich Schlüsselgenerierung. Um unbefugten Zugriff auf die Daten zu verhindern, muss sich das Speichersystem mit dem Laufwerk authentifizieren und einen Authentifizierungsschlüssel verwenden, der bei der ersten Verwendung des Laufwerks eingerichtet wurde.



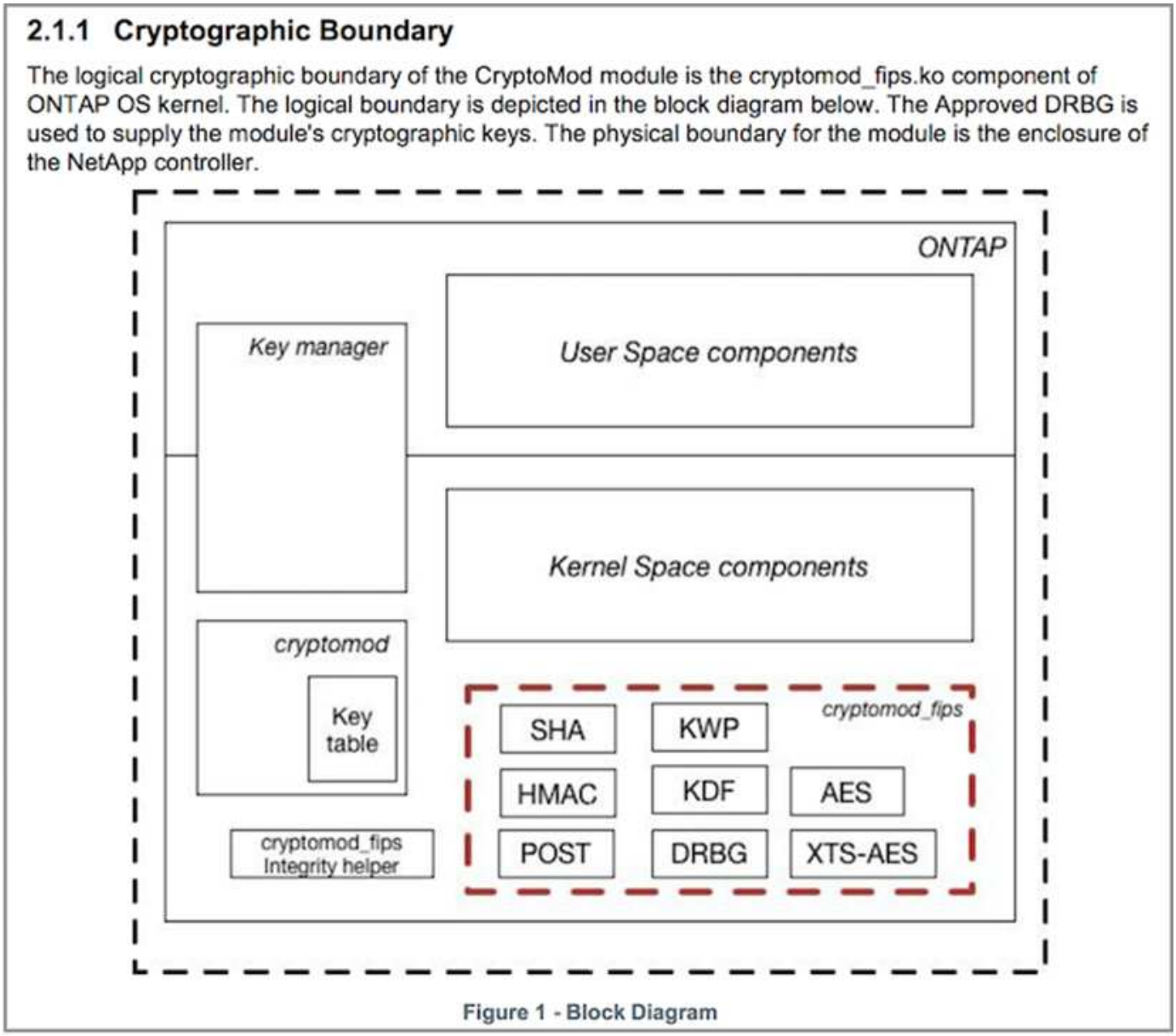
NSE verwendet Hardware-Verschlüsselung auf jedem Laufwerk, das nach FIPS 140-2 Level 2 zertifiziert ist.

Weitere Informationen zu NSE finden Sie unter "NSE Datenblatt".

Schlüsselmanagement

Der FIPS 140-2-Standard gilt für das kryptografische Modul gemäß der Definition der Grenze, wie in der

folgenden Abbildung dargestellt.



Der Schlüsselmanager verfolgt alle von ONTAP verwendeten Datenschlüssel. NSE SEDs verwenden den Schlüsselmanager, um die Authentifizierungsschlüssel für NSE SEDs festzulegen. Bei Verwendung des Schlüsselmanagers besteht die kombinierte NVE und NAE-Lösung aus einem softwarebasierten kryptografischen Modul und einem Schlüsselmanager. NVE verwendet für jedes Volume einen eindeutigen XTS-AES 256-Datenverschlüsselung, der vom Schlüsselmanager gespeichert wird. Der für ein Daten-Volume verwendete Schlüssel liegt nur bei dem Daten-Volume in diesem Cluster und wird bei der Erstellung des verschlüsselten Volume generiert. Auf ähnliche Weise verwendet ein NAE-Volume eindeutige XTS-AES 256-Datenschlüssel pro Aggregat, das ebenfalls vom Schlüsselmanager gespeichert wird. NAE-Schlüssel werden erzeugt, wenn das verschlüsselte Aggregat erstellt wird. ONTAP generiert keine Schlüssel vorab, verwendet sie nicht oder zeigt sie in Klartext an. Sie werden vom Schlüsselmanager gespeichert und geschützt.

Unterstützung von externen Schlüsselmanagern

Ab ONTAP 9.3 werden externe Schlüsselmanager sowohl in NVE als auch in NSE-Lösungen unterstützt. Der FIPS 140-2-Standard gilt für das kryptografische Modul, das bei der Implementierung des jeweiligen Anbieters verwendet wird. In den meisten Fällen nutzen FlexPod und ONTAP Kunden eine der folgenden Validierungen

(entsprechend der "NetApp Interoperabilitätsmatrix") Schlüsselmanager:

- Gemalto oder SafeNet AT
- Vormetric (Thales)
- IBM SKLM
- Utimaco (ehemals Mikrofokus, HPE)

NSE und NVMe SED-Authentifizierungsschlüssel werden mithilfe des branchenüblichen OASIS Key Management Interoperability Protocol (KMIP) an einem externen Schlüsselmanager gesichert. Nur das Storage-System, das Laufwerk und der Schlüsselmanager haben Zugriff auf den Schlüssel. Wenn das Laufwerk außerhalb der Sicherheitsdomain verschoben wird, kann es nicht entsperrt werden. So verhindert es Datenverluste. Außerdem speichert der externe Schlüsselmanager NVE Volume Encryption Keys und NAE Aggregate Encryption Keys. Wenn Controller und Datenträger keinen Zugriff mehr auf den externen Schlüsselmanager haben, sind die NVE- und NAE-Volumes nicht zugänglich und können nicht entschlüsselt werden.

Der folgende Beispielbefehl fügt zwei wichtige Managementserver zur Liste der Server hinzu, die vom externen Schlüsselmanager für Store Virtual Machine (SVM) verwendet werden. `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Wenn ein FlexPod Datacenter in einem Szenario mit Mandantenfähigkeit zum Einsatz kommt, ermöglicht ONTAP Benutzern die Trennung der Mandantenfähigkeit – und zwar aus Sicherheitsgründen auf SVM-Ebene.

Führen Sie den folgenden CLI-Befehl aus, um die Liste der externen Schlüsselmanager zu überprüfen:

```
fp-health::> security key-manager external show
```

Kombinierte Verschlüsselung für doppelte Verschlüsselung (mehrstufige Verteidigung)

Wenn Sie den Zugriff auf Daten getrennt halten und sicherstellen müssen, dass die Daten jederzeit geschützt sind, kann NSE SEDs mit Verschlüsselung auf Netzwerk- oder Fabric-Ebene kombiniert werden. NSE SEDs stehen wie ein Backstop, wenn ein Administrator die Verschlüsselung auf höherer Ebene nicht konfiguriert oder falsch konfiguriert. So können NSE SEDs mit NVE und NAE kombiniert werden, um zwei unterschiedliche Verschlüsselungsebenen zu schaffen.

NetApp ONTAP Cluster-weite Kontrollebene FIPS-Modus

Die NetApp ONTAP Datenmanagement-Software verfügt über eine FIPS-Mode-Konfiguration, die eine zusätzliche Sicherheit für den Kunden erzeugt. Dieser FIPS-Modus gilt nur für die Kontrollebene. Wenn der FIPS-Modus entsprechend den Schlüsselelementen von FIPS 140 aktiviert ist, sind Transport Layer Security v1 (TLSv1) und SSLv3 deaktiviert, und nur TLS v1.1 und TLS v1.2 bleiben aktiviert.

> Die Cluster-weite ONTAP Kontrollscheibe im FIPS-Modus ist konform mit FIPS 140-2 Level 1. Im Cluster-weiten FIPS-Modus kommt ein softwarebasiertes kryptografisches Modul zum Einsatz, das von NCSM bereitgestellt wird.

FIPS 140-2 Compliance-Modus für Cluster-weite Kontrollebene sichert alle Kontrollschnittstellen von ONTAP.

Standardmäßig ist der Modus nur für FIPS 140-2 deaktiviert; Sie können diesen Modus jedoch aktivieren, indem Sie den einstellen `is- fips-enabled` Parameter an `true` Für das `security config modify` Befehl.

Führen Sie den folgenden Befehl aus, um den FIPS-Modus auf dem ONTAP Cluster zu aktivieren:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Wenn der SSL-FIPS-Modus aktiviert ist, wird die SSL-Kommunikation von ONTAP zu den externen Client- oder Serverkomponenten außerhalb von ONTAP auf FIPS-Beschwerde kryptografisch für SSL verwendet.

Um den FIPS-Status für das gesamte Cluster anzuzeigen, führen Sie die folgenden Befehle aus:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Als Nächstes: Lösungsvorteile der konvergenten FlexPod Infrastruktur"

Lösungsvorteile der konvergenten FlexPod Infrastruktur

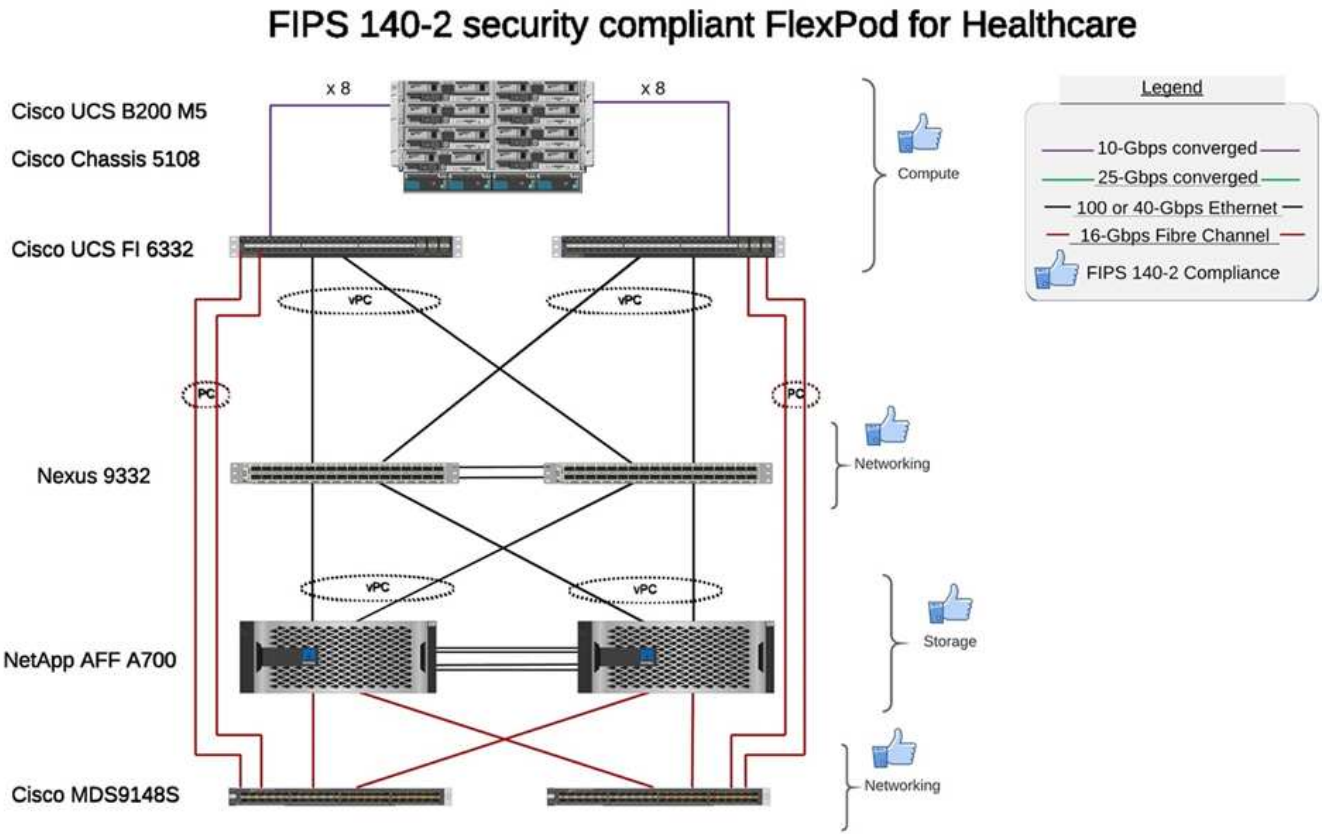
"Früher: FlexPod NetApp ONTAP Storage und FIPS 140-2."

Organisationen im Gesundheitswesen verfügen über mehrere geschäftskritische Systeme. Zwei der kritischsten Systeme sind das elektronische Gesundheitsakten (EHR) und das medizinische Bildgebungssystem. Um die FIPS-Einrichtung auf einem FlexPod System zu demonstrieren, haben wir ein Open-Source-EHR- und ein Open-Source-System für die Bildarchivierung und das Kommunikationssystem (PACS) für die Lab-Einrichtung und die Workload-Validierung im FlexPod System verwendet. Eine vollständige Liste aller EHR-Funktionen, logischen EHR-Applikationskomponenten und die Vorteile von EHR-Systemen bei Implementierung in einem FlexPod-System finden Sie unter "TR-4881: FlexPod für elektronische Krankenakten". Eine vollständige Liste der Funktionen eines Bildgebungssystems für die medizinische Bildgebung, logischer Applikationskomponenten und der Vorteile medizinischer Bildgebungssysteme bei der Implementierung mit FlexPod finden Sie unter "TR-4865: FlexPod für die medizinische Bildgebung".

Während der FIPS-Einrichtung und Workload-Validierung übten wir Workload-Merkmale aus, die einer typischen Gesundheitseinrichtung entsprechen. Wir haben beispielsweise ein Open Source EHR-System genutzt, um realistische Zugriffsszenarien für Patientendaten und Änderungen einzuschließen. Zudem wurden Workloads für die medizinische Bildgebung durchgeführt, einschließlich digitaler Bildgebung und Kommunikation in medizinischen Objekten (DICOM) `*. dcm` Dateiformat. DICOM-Objekte mit Metadaten wurden sowohl im Datei- als auch im Block-Storage gespeichert. Darüber hinaus haben wir Multipathing-Funktionen über einen virtualisierten RedHat Enterprise Linux (RHEL) Server implementiert. Wir speicherten DICOM-Objekte auf einem NFS, gemounteten LUNs über iSCSI und gemounteten LUNs über FC. Bei der FIPS-Einrichtung und -Validierung wurde festgestellt, dass die konvergente FlexPod Infrastruktur unsere Erwartungen übertroffen und sich nahtlos an eine Lösung anstellte.

Die folgende Abbildung zeigt das FlexPod System zur FIPS-Einrichtung und -Validierung. Wir haben die

genutzt "FlexPod Datacenter mit VMware vSphere 7.0 und NetApp ONTAP 9.7 Cisco Validated Design (CVD)" Während des Setups.



Hardware- und Softwarekomponenten der Lösungsinfrastruktur

In den folgenden beiden Abbildungen sind die Hardware- und Software-Komponenten aufgeführt, die jeweils bei der Aktivierung von FIPS-Tests auf einem FlexPod verwendet werden. Beispiele sind die Empfehlungen in diesen Tabellen. Sie sollten mit Ihrem NetApp SME zusammenarbeiten, um sicherzustellen, dass die Komponenten für Ihr Unternehmen geeignet sind. Vergewissern Sie sich außerdem, dass die Komponenten und Versionen von unterstützt werden "NetApp Interoperabilitäts-Matrix-Tool" (IMT) und "Cisco Hardware Compatibility List (HCL)".

Schicht	Produktfamilie	Menge und Modell	Details
Computing	Cisco UCS 5108 Chassis	1 oder 2	
	Cisco UCS Blade Server	3 B200 M5	Jeweils mit 2x 20 Cores, 2,7 GHz und 128 bis 384 GB RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Siehe
	2 Cisco UCS Fabric Interconnects	6332	-
Netzwerk	Cisco Nexus Switches	2 x Cisco Nexus 9332	-

Schicht	Produktfamilie	Menge und Modell	Details
Datennetzwerk Storage-Netzwerk	IP-Netzwerk für Storage-Zugriff über SMB-/CIFS-, NFS- oder iSCSI-Protokolle	Gleiche Netzwerk-Switches wie oben	-
	Storage-Zugriff über FC	2 x Cisco MDS 9148S	-
Storage	NetApp AFF A700 All-Flash-Storage-System	1 Cluster	Cluster mit zwei Nodes
	Festplatten-Shelf	Ein DS224C oder NS224 Festplatten-Shelf	Vollständig mit 24 Laufwerken bestückt
	SSD	>24, 1,2 TB oder mehr Kapazität	-

Software	Produktfamilie	Version/Release	Details
Verschiedene	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64-Bit)	-
	NetApp ONTAP	ONTAP 9.7 oder höher	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 oder höher	-
	Cisco Switches der Ethernet-Serie 3000 oder 9000	Für 9000-Serie, 7.0(3)I7(7) oder höher für 3000-Serie, 9.2(4) oder höher	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) oder höher	-
	Hypervisor	VMware vSphere ESXi 6.7 U2 oder höher	-
Storage	Hypervisor-Managementsystem	VMware vCenter Server 6.7 U3 (vCSA) oder höher	-
Netzwerk	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	-
	NetApp SnapCenter	SnapCenter 4.3 oder höher	-
	Cisco UCS Manager	4.1(1c) oder höher	
Hypervisor	ESXi		
Vereinfachtes	Hypervisor-ManagementsystemVMware vCenter Server 6.7 U3 (vCSA) oder höher		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 oder höher	

Software	Produktfamilie	Version/Release	Details
	NetApp SnapCenter	SnapCenter 4.3 oder höher	
	Cisco UCS Manager	4.1(1c) oder höher	

"Als Nächstes: Weitere FlexPod-Sicherheitsüberlegungen."

Weitere Sicherheitsaspekte bei FlexPod

"Previous – Lösungsvorteile der konvergenten FlexPod Infrastruktur"

Die FlexPod-Infrastruktur ist eine modulare, konvergierte, optional virtualisierte, skalierbare (horizontale und vertikale Skalierung) und kostengünstige Plattform. Mit der FlexPod Plattform können Sie Computing-, Netzwerk- und Storage-Ressourcen unabhängig horizontal skalieren und so die Applikationsimplementierung beschleunigen. Und die modulare Architektur ermöglicht auch bei horizontale und Upgrade-Vorgängen mit Systemen einen unterbrechungsfreien Betrieb.

Für verschiedene Komponenten eines HIT-Systems müssen die Daten in den Dateisystemen SMB/CIFS, NFS, Ext4 und NTFS gespeichert werden. Diese Anforderung bedeutet, dass die Infrastruktur Datenzugriff über NFS-, CIFS- und SAN-Protokolle bieten muss. Ein einziges NetApp Storage-System kann alle diese Protokolle unterstützen, sodass keine herkömmliche Vorgehensweise bei protokollspezifischen Storage-Systemen erforderlich ist. Zusätzlich kann ein einzelnes NetApp Storage-System mehrere HIT-Workloads wie EHRs, PACS oder VNA, Genomik, VDI usw. unterstützen Bei garantierten und konfigurierbaren Performance-Leveln.

DIE IMPLEMENTIERUNG in einem FlexPod System bringt VERSCHIEDENE Vorteile mit SICH, die speziell auf das Gesundheitswesen zugeschnitten sind. Die folgende Liste enthält eine ausführliche Beschreibung der folgenden Vorteile:

- **FlexPod Sicherheit**. Sicherheit ist die Grundlage eines FlexPod Systems. In den letzten Jahren ist Ransomware zu einer Bedrohung geworden. Ransomware ist eine Art von Malware, die auf Kryptovirologie basiert, die Verwendung von Kryptographie zum Aufbau von schädlicher Software. Diese Malware kann sowohl symmetrische und asymmetrische Schlüssel Verschlüsselung verwenden, um die Daten eines Opfers zu sperren und ein Lösegeld zu verlangen, um den Schlüssel zur Entschlüsselung der Daten. Informationen darüber, wie die FlexPod Lösung hilft, Bedrohungen wie Ransomware abzuwehren, finden Sie unter "TR-4802: Die Lösung gegen Ransomware". FlexPod Infrastrukturkomponenten sind auch "FIPS 140-2 konform".
- **Cisco Intersight.** Cisco Intersight ist eine innovative, Cloud-basierte Management-als-Service-Plattform, die eine zentrale Konsole für FlexPod Management und Orchestrierung in einem kompletten Stack bereitstellt. Die Intersight-Plattform verwendet FIPS 140-2-2-konforme kryptografische Module. Die Out-of-Band-Management-Architektur der Plattform macht sie für einige Standards oder Audits wie HIPAA außer Reichweite. Es werden nie individuelle identifizierbare Gesundheitsinformationen im Netzwerk an das Intersight-Portal gesendet.
- **NetApp FPolicy Technologie.** NetApp FPolicy (eine Entwicklung der Namensdateirichtlinie) ist ein Benachrichtigungs-Framework für den Dateizugriff über NFS- oder SMB/CIFS-Protokolle. Diese Technologie ist seit über zehn Jahren Bestandteil der ONTAP Datenmanagement-Software und hilft bei der Erkennung von Ransomware. Diese Zero Trust Engine bietet zusätzliche Sicherheitsmaßnahmen, die über Berechtigungen in Zugriffssteuerungslisten (Access Control Lists, ACLs) hinausgehen. FPolicy verfügt über zwei Betriebsmodi: Nativ und extern:
  - Der native Modus bietet sowohl Blacklisting als auch Whitelisting von Dateierweiterungen.

- Der externe Modus verfügt über die gleichen Funktionen wie der native Modus, kann aber auch mit einem FPolicy-Server integriert werden, der extern zum ONTAP-System läuft, sowie einem SIEM-System (Security Information and Event Management). Weitere Informationen zum Kampf gegen Ransomware finden Sie im "Fighting Ransomware: Teil drei – ONTAP FPolicy, ein weiteres leistungsstarkes Native Tool (aka Free)" blog:

- **Daten im Ruhezustand**. ONTAP 9 und höher verfügt über drei FIPS 140-2-konforme Verschlüsselungslösungen für Daten im Ruhezustand:
  - NSE ist eine Hardware-Lösung mit Self-Encrypting Drives.
  - NVE ist eine Softwarelösung, die die Verschlüsselung von beliebigen Daten-Volumes auf jedem Festplattentyp, auf der diese aktiviert ist, mit einem eindeutigen Schlüssel für jedes Volume ermöglicht.
  - NAE ist eine Software-Lösung, die die Verschlüsselung beliebiger Daten-Volumes auf jedem beliebigen Laufwerkstyp ermöglicht und bei jedem Aggregat mit eindeutigen Schlüsseln aktiviert wird.

> Ab ONTAP 9.7 sind NAE und NVE standardmäßig aktiviert, wenn das NetApp NVE Lizenzpaket mit dem Namen VE vorhanden ist.

- **Daten im Flug**. Ab ONTAP 9.8 unterstützt Internet Protocol Security (IPsec) die End-to-End-Verschlüsselung für den gesamten IP-Datenverkehr zwischen einem Client und einer ONTAP SVM. Die IPsec-Datenverschlüsselung für den gesamten IP-Datenverkehr umfasst NFS-, iSCSI- und SMB/CIFS-Protokolle. IPsec bietet die einzige Verschlüsselung im Flug für iSCSI-Datenverkehr.
- **End-to-End-Datenverschlüsselung in einer hybriden Multi-Cloud-Data-Fabric** Kunden, die Verschlüsselungstechnologien für ruhende Daten wie NSE oder NVE und Cluster Peering Encryption (CPE) für Datenreplizierungsverkehr verwenden, können nun mithilfe ONTAP von IPsec eine End-to-End-Verschlüsselung zwischen Client und Storage in ihrer hybriden Multi-Cloud Data Fabric verwenden 9.8. Ab ONTAP 9 können Sie den FIPS 140-2-Compliance-Modus für Cluster-weite Kontrollebene-Schnittstellen aktivieren. Standardmäßig ist der reine FIPS 140-2-Modus deaktiviert. Ab ONTAP 9.6 unterstützt CPE die TLS 1.2 AES-256 GCM-Verschlüsselung für ONTAP Datenreplizierungsfunktionen wie NetApp SnapMirror, NetApp SnapVault und NetApp FlexCache Technologien. Die Verschlüsselung wird über einen vorab freigegebenen Schlüssel (PSK) zwischen zwei Cluster-Peers eingerichtet.
- **Sichere Mandantenfähigkeit**. Dies ist auch in der Lage, die erhöhten Anforderungen virtualisierter Server- und Storage-Infrastrukturen zu erfüllen. Dies ermöglicht eine sichere Mandantenfähigkeit für applikationsspezifische Informationen, insbesondere zum Hosten mehrerer Instanzen von Datenbanken und Software.

"Weiter: Fazit."

Schlussfolgerung

"Früher: Weitere FlexPod-Sicherheitsüberlegungen."

Durch die Ausführung Ihrer Applikationen im Gesundheitswesen auf einer FlexPod Plattform ist Ihr Unternehmen im Gesundheitswesen durch eine Plattform mit FIPS 140-2-Zertifizierung besser geschützt. FlexPod bietet mehrschichtigen Schutz auf jeder einzelnen Komponente: computing, Netzwerk und Storage. Die Datensicherungsfunktionen von FlexPod schützen Daten im Ruhezustand und im Übertragungsprozess und sorgen dafür, dass Backups bei Bedarf sicher und bereit bleiben.

Vermeiden Sie menschliche Fehler durch den Einsatz der vorab validierten Designs von FlexPod, die

umfassend getestete konvergente Infrastrukturen aus der strategischen Partnerschaft von Cisco und NetApp enthalten. Ein FlexPod System wurde speziell für vorhersehbare Performance mit niedriger Latenz und Hochverfügbarkeit konzipiert und bietet auch dann niedrige Auswirkungen, wenn FIPS 140-2 Computing-, Netzwerk- und Storage-Ebenen aktiviert ist. Dieser Ansatz führt zu einer optimalen Benutzererfahrung und einer optimalen Reaktionszeit für Benutzer Ihres HIT-Systems.

"Weiter: Danksagungen, Versionsverlauf, und wo finden Sie zusätzliche Informationen."

Danksagungen, Versionsverlauf und weitere Informationen finden

"Zurück: Schlussfolgerung."

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

- Cisco MDS 9000-Produktreihe NX-OS Security Configuration Guide

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp and Federal Information Processing Standard (FIPS) Veröffentlichung 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- NetApp Leitfaden zur Härtung von ONTAP 9

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- NetApp Encryption Power Guide

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Datenblatt zu NVE und NAE

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NSE Datenblatt

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- ONTAP 9 Dokumentationszentrum

  http://docs.netapp.com

- NetApp and Federal Information Processing Standard (FIPS) Veröffentlichung 140-2

https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Cisco und FIPS 140-2 Compliance

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Cyber-Sicherheitsverfahren für mittelgroße und große Organisationen im Gesundheitswesen

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco und Cryptographic Module Validation Program (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption und NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption und NetApp Aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- NetApp Storage Encryption

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod für elektronische Krankenakten

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Bild: Whitepaper „Data Now: Improving Performance in Epic EHR Environments with Cloud-Connected Flash Technology“

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- FlexPod Datacenter für Epic EHR-Infrastruktur

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- FlexPod Datacenter for Epic EHR Deployment Guide

  https://www.netapp.com/media/10658-tr-4693.pdf

- FlexPod-Datacenter-Infrastruktur für MEDITECH-Software

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- Der FlexPod-Standard gilt auch für MEDITECH Software

https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod for MEDITECH Directional Sizing Guide

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod für medizinische Bildverarbeitung

  https://www.netapp.com/media/19793-tr-4865.pdf

- KI im Gesundheitswesen

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- FlexPod für das Gesundheitswesen vereinfachen den Wandel

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod von Cisco und NetApp

  https://flexpod.com/

Danksagungen

- Abhinav Singh, Technical Marketing Engineer, NetApp
- Brian O'Nahony, Solution Architect Healthcare (Epic), NetApp
- Brian Pruitt, Pursuit Business Development Manager, NetApp
- Arvind Ramakrishnan, Senior Solutions Architect, NetApp
- Michael Hommer, FlexPod Global Field CTO, NetApp

Versionsverlauf

Version	Datum	Versionsverlauf des Dokuments
Version 1.0	April 2021	Erste Version

Cisco Intersight mit NetApp ONTAP Storage

Cisco Intersight with NetApp Storage – Quick Start Guide

In Zusammenarbeit mit: 

Einführung

NetApp und Cisco bieten gemeinsam Cisco Intersight, eine Komplettansicht des FlexPod Ecosystems. Durch diese vereinfachte Integration entsteht eine einheitliche Management-Plattform für alle Komponenten in der FlexPod-Infrastruktur und der FlexPod-Lösung. Cisco Intersight ermöglicht Ihnen die Überwachung von NetApp Storage, Cisco Computing und VMware Inventar. Außerdem können Sie Workflows orchestrieren oder automatisieren, um Storage- und Virtualisierungsaufgaben gemeinsam durchzuführen.

Verwandte Informationen

Weitere Informationen finden Sie in den folgenden Dokumenten und auf den folgenden Websites:

"TR 4883: FlexPod Datacenter with ONTAP 9.8, ONTAP Storage Connector for Cisco Intersight und Cisco Intersight Managed Mode"

"Cisco Intersight-Hilfe-Center"

"Cisco Intersight – Erste Schritte – Übersicht"

"Intersight Appliance Install and Upgrade Guide"

Was ist neu

In diesem Abschnitt werden die neuen Funktionen aufgeführt, die für Cisco Intersight mit NetApp ONTAP Storage verfügbar sind.

Januar 2024

- NetApp Storage-Orchestrierung mit Referenz-Workflows, die jetzt über die in GitHub zum Download zur Verfügung stehen "FlexPod Intersight Workflow-Repository". Weitere Informationen zu den neuen Referenz-Workflows in GitHub finden Sie unter "Anwendungsfall 2: NetApp Storage-Orchestrierung anhand von Referenz-Workflows".

November 2023

- Die Seite NVMe-Namespaces im Abschnitt Inventar der Benutzeroberfläche wurde hinzugefügt.

August 2023

Ein Upgrade auf NetApp Active IQ Unified Manager 9.13GA ist erforderlich, um Kompatibilität und volle Funktionalität mit der aktuellen Version sicherzustellen.

- Verbesserung des Tasks Neue intelligente NetApp-LUN, um deutlich die Verfügbarkeit von Auswahloptionen für das Erstellen einer neuen Initiatorgruppe oder das Auswählen einer vorhandenen Initiatorgruppe anzuzeigen. Wenn Benutzer jetzt das Kontrollkästchen aktivieren, um eine neue Initiatorgruppe zu erstellen, ist der Parameter zur Auswahl einer vorhandenen Initiatorgruppe nicht mehr verfügbar. Wenn Benutzer das Kontrollkästchen deaktivieren, um eine neue Initiatorgruppe zu erstellen, wird der vorhandene Parameter für die Initiatorgruppe dann verfügbar.
- Erweitert die Aufgaben Neue NetApp-LUN-Zuordnung und NetApp-LUN-Zuordnung entfernen. Die neue Beziehung zwischen der LUN und der Initiatorgruppe wird jetzt aktualisiert. Die UI-Bestandsaufnahme wird bei der Ausführung der Aufgabe sofort sowohl für die LUN als auch für die Initiatorgruppe aktualisiert.
- Die Seite „Prüfungen“ wird jetzt ordnungsgemäß geladen, wenn sich die Benutzer zum ersten Mal anmelden, und es ist keine Aktualisierung mehr erforderlich.

Juli 2023

Ein Upgrade auf NetApp Active IQ Unified Manager 9.13GA ist erforderlich, um Kompatibilität und volle Funktionalität mit der aktuellen Version sicherzustellen.

- Aktualisierte Namen für NetApp-Storage-Aufgaben. Unter Use Case 3 Benutzerdefinierte Workflows mit Designer-freiem Formular finden Sie eine vollständige Liste der umbenannten Aufgaben.
- Die IP-Adresse der NFS-Schnittstelle wurde als Ausgabe des Tasks „Neues NetApp-NAS-Smart-Volume“ hinzugefügt.
- Der Registerkarte „Checks“ wurde eine Überprüfung hinzugefügt, ob es sich bei der ASUP Übertragung um eine HTTPS-Übertragung handelt.
- Der richtige Tier-Typ für alle Tiers wird nun ordnungsgemäß unter der Benutzeroberfläche „Tiers“ angezeigt.
- Alle kompatiblen Lizenzen werden jetzt ordnungsgemäß auf der Seite Lizenzen angezeigt.
- Der genaue Wert für CIFS-Freigaben ohne oder ohne Home-Verzeichnis wird jetzt auf der Seite Freigaben angezeigt.
- Sortierung und Filterung sind jetzt für die zugeordnete Spalte auf der SEITE LUNS aktiviert.
- Sortieren und Filtern aktiviert nun die Spalte Authentifizierung aktiviert auf der Seite NTP-Server.
- Neue Prüfungen und die folgenden entsprechenden Kategorien wurden der Registerkarte Prüfungen hinzugefügt.
  - Sicherheit
  - Anti-Ransomware
  - Gesteigerte
  - Andere
- In der Detailansicht „Bestand“ wird jetzt ein Bericht anstelle der physisch genutzten Kapazität verwendet.

Juni 2023

Ein Upgrade auf NetApp Active IQ Unified Manager 9.13RC1 ist erforderlich, um die Kompatibilität und vollständige Funktionalität der aktuellen Version sicherzustellen.

- Aktualisierte Namen für NetApp-Storage-Aufgaben. Siehe "Anwendungsfall 3: Benutzerdefinierte Workflows mit Designer-freiem Formular" Für die vollständige Liste der umbenannten Aufgaben.

April 2023

- Die Registerkarten Protection Policies (SnapMirror) und Snapshot Policies wurden im Abschnitt Inventar der Benutzeroberfläche auf der Seite Policies hinzugefügt.
- Die Seite NFS-Clients wurde im Abschnitt „Inventar“ der Benutzeroberfläche hinzugefügt.
- Geschützte Spalte auf der Seite Speicher-VMs im Abschnitt Inventar der Benutzeroberfläche hinzugefügt.
- Geändert, wie Informationen zur Datenreduzierung gemeldet und angezeigt werden.
- Die Registerkarten „Lokale Ebene“ und „Cloud-Ebene“ wurden auf der Seite „Tiers“ im Abschnitt „Inventar“ der Benutzeroberfläche hinzugefügt.
- Die Spalte Knoten wird nun nach der Spalte Name auf der Seite Ports im Abschnitt Inventar der Benutzeroberfläche angezeigt.

Januar 2023

Ein Upgrade auf NetApp Active IQ Unified Manager 9.12 GA ist erforderlich, um Kompatibilität und vollständigen Funktionalität der aktuellen Version zu gewährleisten. Eine Liste bekannter Probleme in Bezug auf diese Version finden Sie unter Bekannte Probleme.

- Intersight Interoperabilitätsprüfungen können jetzt bei Kompatibilitätsprüfungen zwischen den Firmware-Modi UCSM und IMM unterscheiden.
- Schutzbeziehungen werden für ONTAP 9.7 nicht in Intersight angezeigt. Dieses Problem wurde in ONTAP 9.8RC1 behoben.

August 2022

Ein Upgrade auf NetApp Active IQ Unified Manager 9.11 GA ist erforderlich, um Kompatibilität und vollständigen Funktionalität der aktuellen Version zu gewährleisten. Eine Liste bekannter Probleme in Bezug auf diese Version finden Sie unter Bekannte Probleme.

- Aktualisierte Berechnung der verfügbaren Cluster-Kapazität, die dem System Manager entspricht
- Aktualisierte Cluster General Seite, um die Zusammenfassung der Performance-Metriken auszublenden, bis Performance-Daten gefüllt sind
- Problem mit der allgemeinen Cluster-Seite, das gelegentlich die Seite aufhängt, wurde behoben
- CIFS-Freigaben, CIFS-Services, qtrees und SVM SnapMirror-Richtlinien wurden zum Back-End-Inventar hinzugefügt.
- Freigaben und qtrees wurden im UI-Navigationsmenü unter dem Abschnitt „Logischer Bestand“ hinzugefügt
- Freigaben wurden als Registerkarte von einer ausgewählten Storage-VM hinzugefügt
- CIFS-Serviceinformationen auf der Registerkarte Speicher-VM Allgemein hinzugefügt, wenn die Speicher-VM CIFS aktiviert ist
- Es wurde eine Cluster-Scheckseite hinzugefügt, auf der Benutzer die Konfiguration von NetApp Storage-Systemen unter Einhaltung von Best Practices überprüfen können

Juli 2022

- Verbesserte Grafikfunktionen für Cluster Data Reduction Ratio sind jetzt im Capacity Widget verfügbar

- Die Registerkarte FC-Schnittstellen wurde der Seite Netzwerkschnittstellen hinzugefügt
- Erstellen eines neuen Volumens mit der generischen "New Storage Volume" Aufgabe setzt nun Volumen-Raum-Garantie auf keine und Snapshot Reserve Prozent auf 0%
- Kommentarfeld unter der Task Snapshot-Richtlinie bearbeiten ist jetzt optional und muss nicht mehr zwingend angegeben werden
- Verbesserte Einheitlichkeit bei UI-Bestand und -Orchestrierung
- Die Kapazitätsinformationen von Intersight in der Clusterkapazität entsprechen jetzt der System Manager
- Kontrollkästchen unter Neue Aufgabe für virtuelle Speicher hinzugefügt, um alle Parameter beim Erstellen einer neuen Managementoberfläche anzuzeigen, um die Benutzerfreundlichkeit zu verbessern
- Protokolle unter Client Match verschoben, jetzt in Übereinstimmung mit System Manager
- Allgemeine Seite „Exportrichtlinie“ mit Zugriffsprotokoll(en)
- igroup Entfernung wird jetzt bedingt protokolliert
- „Failover Policy“ und „autorevert“ Parameter für NAS unter New Storage NAS Data Interface und New Storage iSCSI Data Interface hinzugefügt
- Rollback für New Storage NAS Smart Volume Task entfernt jetzt die Exportrichtlinie, wenn keine anderen Volumes verbunden sind
- Hat Verbesserungen für Smart Volume und Smart LUN-Aufgaben vorgenommen

April 2022

Um die Kompatibilität und vollständige Funktionalität zukünftiger Versionen sicherzustellen, wird ein Upgrade des NetApp Active IQ Unified Manager auf Version 9.10P1 empfohlen.

- Seite „Broadcast Domain to Ethernet Port Detail“ hinzugefügt
- Veränderte den Begriff „Aggregat“ zu „Tier“ für das Aggregat und SVM innerhalb der Benutzeroberfläche
- Änderung des Begriffs „Cluster Status“ in „Array Status“
- MTU-Filter funktioniert jetzt für <,>,=,⇐,>= Zeichen
- Seite „Netzwerkschnittstelle“ wurde der Cluster-Bestandsaufnahme hinzugefügt
- AutoSupport zu Cluster Inventory hinzugefügt
- Hinzugefügt `cdpd.enable` Node-Option
- Objekt für CDP-Nachbar hinzugefügt
- NetApp Workflow-Storage-Aufgaben wurden innerhalb von Cisco Intersight hinzugefügt. Siehe "Anwendungsfall 3: Benutzerdefinierte Workflows mit Designer-freiem Formular" Eine vollständige Liste aller NetApp Storage-Aufgaben.

Januar 2022

- Es wurden ereignisbasierte Intersight-Alarme für NetApp Active IQ Unified Manager 9.10 oder höher hinzugefügt.

Um die Kompatibilität und vollständige Funktionalität zukünftiger Versionen sicherzustellen, wird ein Upgrade des NetApp Active IQ Unified Manager auf Version 9.10 empfohlen.

- Legen Sie jedes Protokoll explizit für Storage Virtual Machine fest (wahr oder falsch)

- Zugewiesenes clusterHealthStatus Status ok-with-inused to OK
- Die Spalte „Systemzustand“ wurde auf der Seite „Cluster-Liste“ in die Spalte „Cluster Status“ umbenannt
- Zeigt das Speicher-Array „nicht erreichbar“ an, wenn das Cluster ausgefallen ist oder nicht erreichbar ist
- Die Spalte „Systemzustand“ wurde auf der Seite „Cluster General“ in die Spalte „Array Status“ umbenannt
- SVM hat jetzt eine Registerkarte „Volumes“, die alle Volumes für die SVM zeigt
- Das Volumen hat einen Abschnitt mit der Snapshot-Kapazität
- Lizenzen werden jetzt korrekt angezeigt

Oktober 2021

- Aktualisierte Liste der NetApp Storage-Aufgaben, die innerhalb von Cisco Intersight verfügbar sind Siehe "Anwendungsfall 3: Benutzerdefinierte Workflows mit Designer-freiem Formular" Eine vollständige Liste aller NetApp Storage-Aufgaben.
- „Systemzustand“ wurde auf der Seite „Cluster-Liste“ hinzugefügt.
- Erweiterte Details jetzt auf der Seite Allgemein für ein ausgewähltes Cluster verfügbar.
- Auf die NTP-Server-Tabelle kann jetzt über das Navigationsbereich zugegriffen werden.
- Neue Registerkarte „Sensoren“ mit der Seite „Allgemein“ für die Storage Virtual Machine hinzugefügt.
- VLAN und Link Aggregation Group Zusammenfassung jetzt verfügbar unter der Port General Seite.
- Spalte „Gesamtkapazität“, die in der Tabelle „Gesamtkapazität des Volumes“ hinzugefügt wurde
- Spalten zu Latenz, IOPS und Durchsatz, die unter Durchschnittliche Volume-Statistiken, Durchschnittliche LUN-Statistiken, Durchschnittliche Aggregatstatistiken, Durchschnittliche Storage VM-Statistiken und Durchschnittliche Node-Statistiken hinzugefügt werden

> ⓘ Die oben genannten Performance-Kennzahlen stehen nur für Storage Arrays zur Verfügung, die über NetApp Active IQ Unified Manager 9.9 oder höher überwacht werden.

Bekannte Probleme

- Wenn Sie eine AIQUM-Version 9.11 oder eine frühere Version verwenden, tritt eine Diskrepanz zwischen den angezeigten Werten auf der Seite „Speicherliste“ und dem Balken „Kapazität“ auf der Seite „Allgemein speichern“ auf. Um dieses Problem zu lösen, sollten Sie auf AIQUM 9.12 oder höher aktualisieren, um die Genauigkeit der angezeigten Kapazitätswerte zu gewährleisten.
- Wenn Sie AIQUM 9.11 oder eine frühere Version nutzen, können alle Überprüfungen, die auf der Registerkarte „Interoperabilität“ auf der Seite „integrierte Systeme“ durchgeführt werden, IMM und UCSM Cisco Komponenten nicht genau unterscheiden. Um dieses Problem zu beheben, sollten Sie auf AIQUM 9.12 aktualisieren, um sicherzustellen, dass alle Komponenten ordnungsgemäß identifiziert werden.
- Damit die Intersight-Speicherbestandsdaten während des Datenerfassungsprozesses nicht beeinflusst werden, müssen alle nicht unterstützten ONTAP-Cluster (z. B. Versionen unter ONTAP 9.7P1) aus dem Active IQ Unified Manager (AIQUM) entfernt werden.
- Für alle beanspruchten Ziele ist eine AIQUM-Version von 9.11 erforderlich, um eine erfolgreiche Durchführung von FlexPod Integrated System Interoperability Abfragen zu ermöglichen.
- Die Seite Speicherbestandsprüfungen wird nicht ausgefüllt, wenn der ONTAP-Cluster mit einem FQDN zu AIQUM hinzugefügt wird. Benutzer müssen AIQUM ONTAP-Cluster mithilfe einer IP-Adresse hinzufügen.

Anforderungen

Überprüfen Sie, ob Sie die Hardware-, Software- und Lizenzierungsanforderungen für die NetApp ONTAP-Storage-Integration mit Cisco Intersight erfüllen.

Hardware- und Softwareanforderungen

Dies sind die Mindestanforderungen an Hardware und Software, die für die Implementierung der Lösung erforderlich sind. Je nach den Anforderungen des Kunden können die in einer konkreten Implementierung dieser Lösung verwendeten Komponenten variieren.

Komponente	Anforderungsdetails
NetApp ONTAP	ONTAP 9.7P1 und höher
NetApp Active IQ Unified Manager	Die neueste Version von NetApp Active IQ Unified Manager ist erforderlich (derzeit 9.14RC1).
NetApp Storage Array	Alle ONTAP ASA-, AFF- und FAS-Storage-Arrays werden für ONTAP 9.7P1 und höher unterstützt
Virtualisierungshypervisor	VSphere 7.0 und höher

Siehe "Von Cisco Intersight unterstützte Systeme" Für die Mindestanforderungen von Cisco UCS Compute Komponenten und der UCSM Version

Cisco Intersight Lizenzierungsanforderungen

Cisco Intersight bietet Services wie Infrastrukturservice und Cloud Orchestrator Service zum Managen, Automatisieren und Optimieren von physischem Storage (NetApp-Storage). Mit diesen Services können Sie Cisco UCS-Server und Cisco HyperFlex-System verwalten. Beim Infrastructure Service und Cloud Orchestrator Service kommt ein abonnementbasiertes Lizenzmodell mit mehreren Tiers zum Einsatz. Sie können die erforderliche Cisco UCS Server Volume-Tier für die ausgewählte Abonnementlaufzeit auswählen.

Lizenzmodell

Das Lizenzmodell von Cisco Intersight Infrastructure Services wurde vereinfacht und bietet nun die folgenden zwei Ebenen:

- **Cisco Intersight Infrastructure Services Essentials** - die Lizenzstufe Essentials bietet Serververwaltung einschließlich globaler Statusüberwachungsfunktionen, Inventarisierung, proaktiven Support durch Cisco TAC-Integration, Multi-Faktor-Authentifizierung sowie SDK- und API-Zugriff.
- * Cisco Intersight Infrastructure Services Advantage* - die Advantage-Lizenz-Tier bietet fortschrittliches Servermanagement mit erweiterter Transparenz, Integration in die Systeme anderer Anbieter, Automatisierung von Hardware und Software von Cisco und Drittanbietern sowie Multi-Domain-Lösungen.

Weitere Informationen zu den Funktionen, die von verschiedenen Lizenzstufen abgedeckt werden, finden Sie unter "Infrastructure Services Lizenz".

Bevor Sie beginnen

Für die Überwachung und Orchestrierung von NetApp Storage von Cisco Intersight benötigen Sie NetApp Active IQ Unified Manager und Cisco Intersight Assist Virtual

Appliance in der vCenter Umgebung.

Installation oder Upgrade von NetApp Active IQ Unified Manager

Installation oder Upgrade auf Active IQ Unified Manager (aktuelle Version erforderlich, derzeit 9.14RC1), falls nicht. Weitere Anweisungen finden Sie im "NetApp Active IQ Unified Manager Dokumentation".

Installieren Sie Die Cisco Intersight Assist Virtual Appliance

Stellen Sie sicher, dass Sie die erfüllen "Cisco Intersight Virtual Appliance Licensing-, System- und Netzwerkanforderungen".

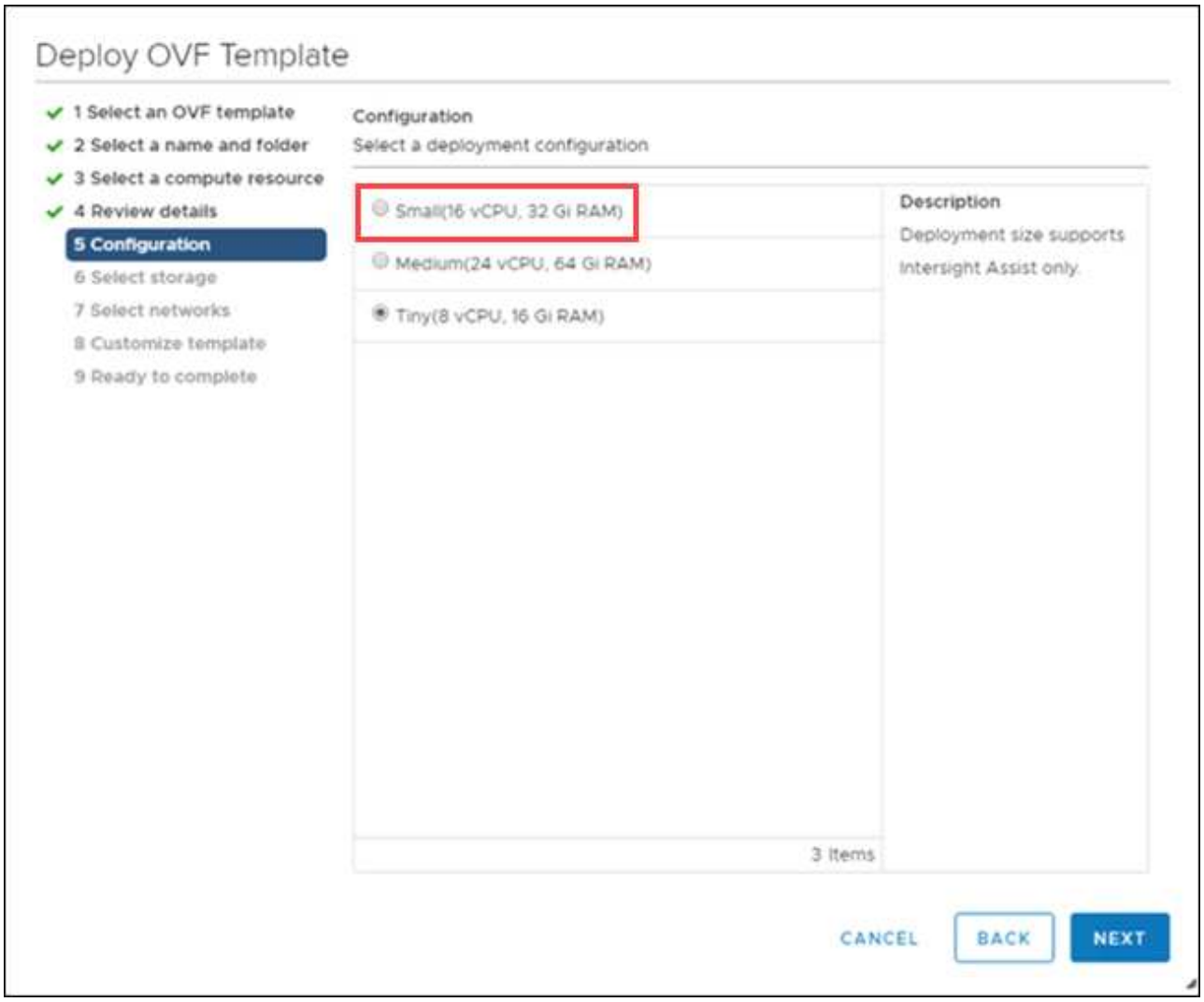
Schritte

1. Erstellen Sie ein Cisco Intersight-Konto. Besuchen Sie "https://intersight.com/" So erstellen Sie Ihr Intersight-Konto. Sie müssen über eine gültige Cisco ID verfügen, um ein Cisco Intersight-Konto zu erstellen.
2. Laden Sie die Intersight Virtual Appliance unter herunter "software.cisco.com". Weitere Informationen finden Sie im "Intersight Appliance Install and Upgrade Guide".
3. OVA bereitstellen. Zur Bereitstellung der OVA sind DNS und NTP erforderlich.

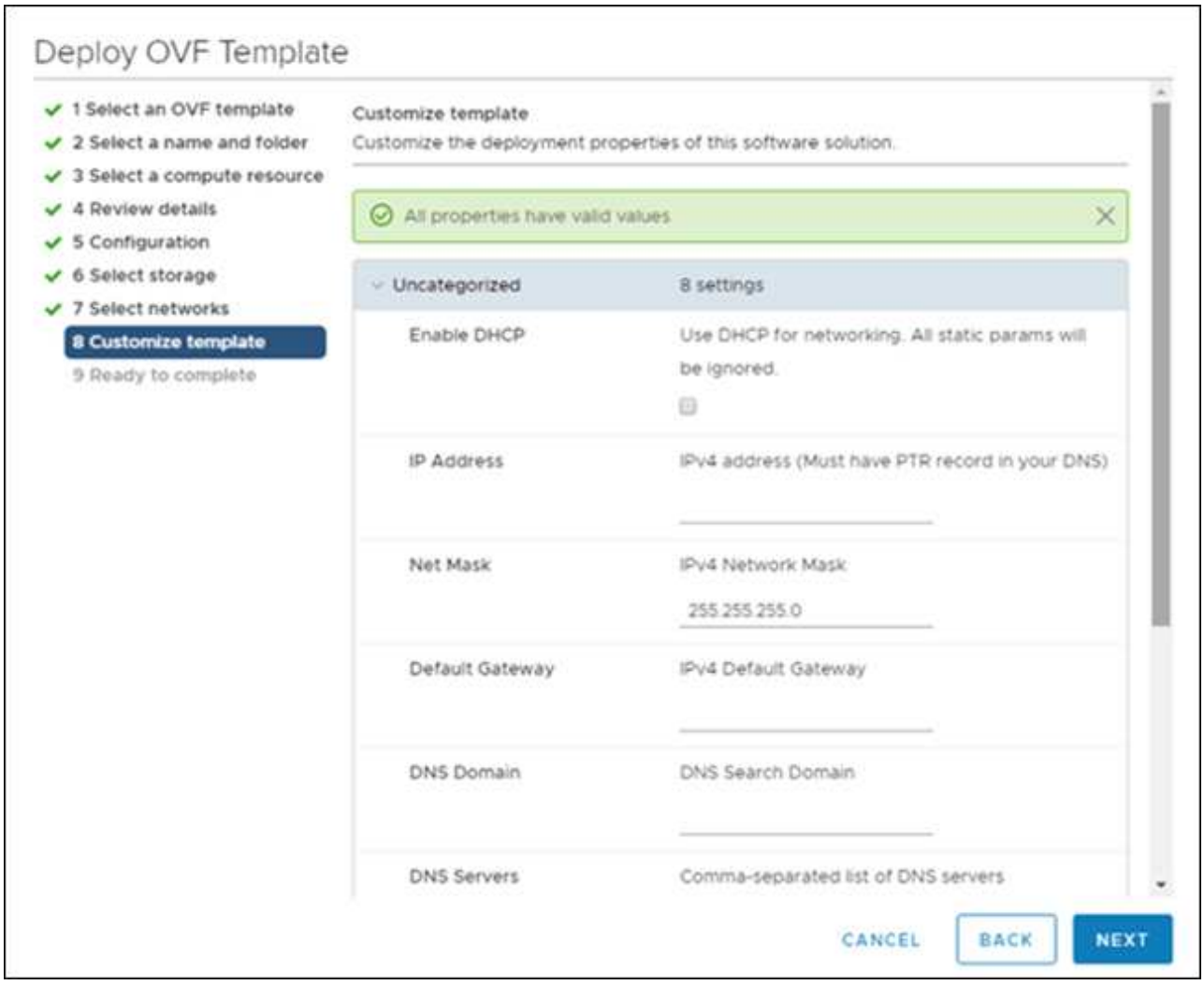
    a. Konfigurieren Sie DNS mit A/PTR- und CNAME-Alias-Datensätzen, bevor Sie die OVA bereitstellen. Siehe das folgende Beispiel.

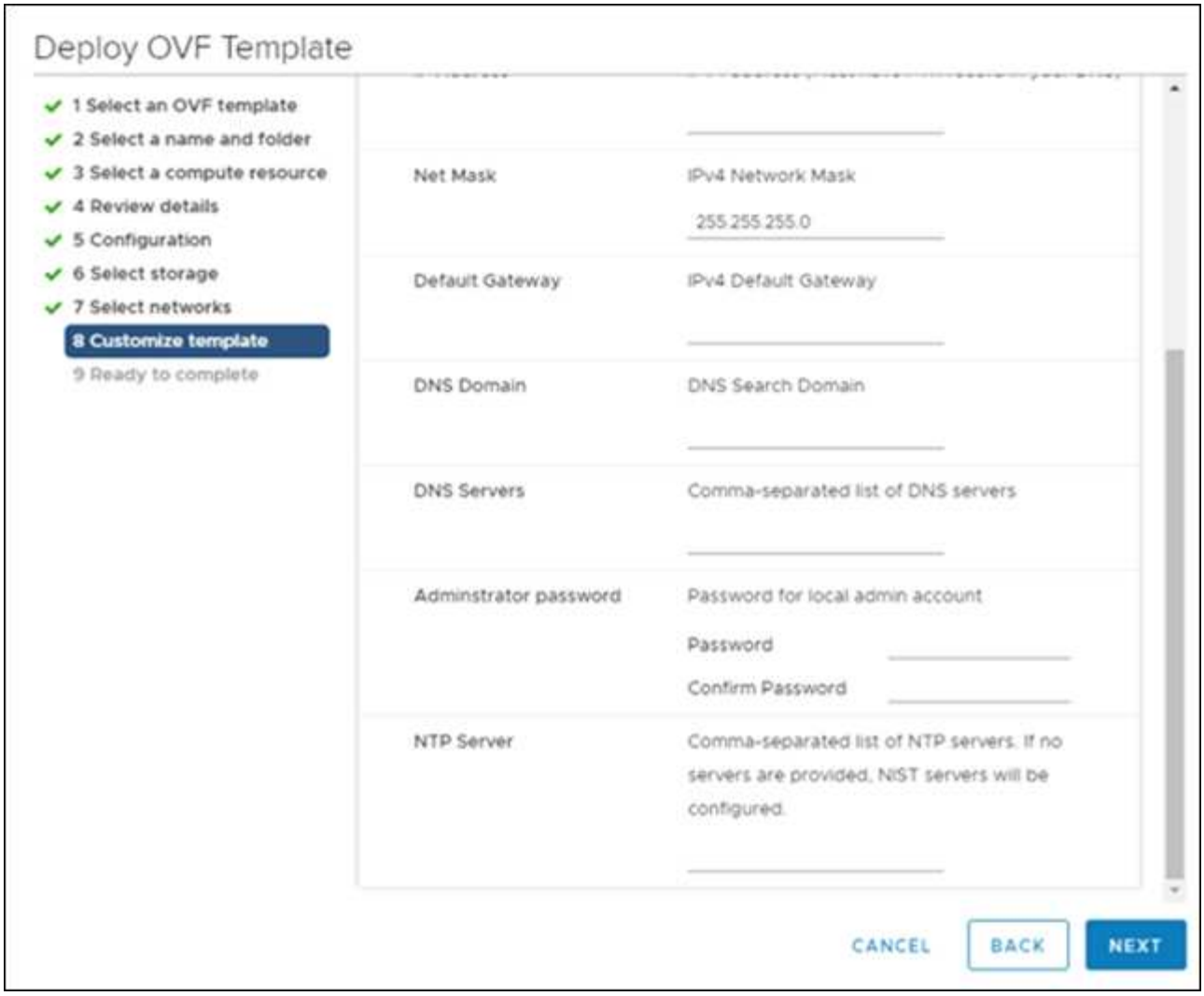
    b. Wählen Sie die geeignete Konfigurationsgröße (klein, klein oder mittel) basierend auf Ihren OVA-Bereitstellungsanforderungen für die Intersight Virtual Appliance aus.

    TIPP: für ein ONTAP Cluster mit zwei Nodes und einer großen Anzahl an Speicherobjekten empfiehlt NetApp, die kleine Option (16 vCPU, 32 Gi RAM) zu verwenden.



c. Passen Sie auf der Seite **Vorlage anpassen** die Bereitstellungseigenschaften der OVF-Vorlage an. Das Administratorpasswort wird für die lokalen Benutzer verwendet: Admin(`webUI/cli/ssh`).


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Configuration
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Uncategorized
8 settings
Enable DHCP
Use DHCP for networking. All static params will be ignored.
IP Address
IPv4 address (Must have PTR record in your DNS)
Net Mask
IPv4 Network Mask
255.255.255.0
Default Gateway
IPv4 Default Gateway
DNS Domain
DNS Search Domain
DNS Servers
Comma-separated list of DNS servers
CANCEL
BACK
NEXT



a. Klicken Sie Auf **Weiter**.

4. Nach der Bereitstellung der Intersight Assist-Appliance.

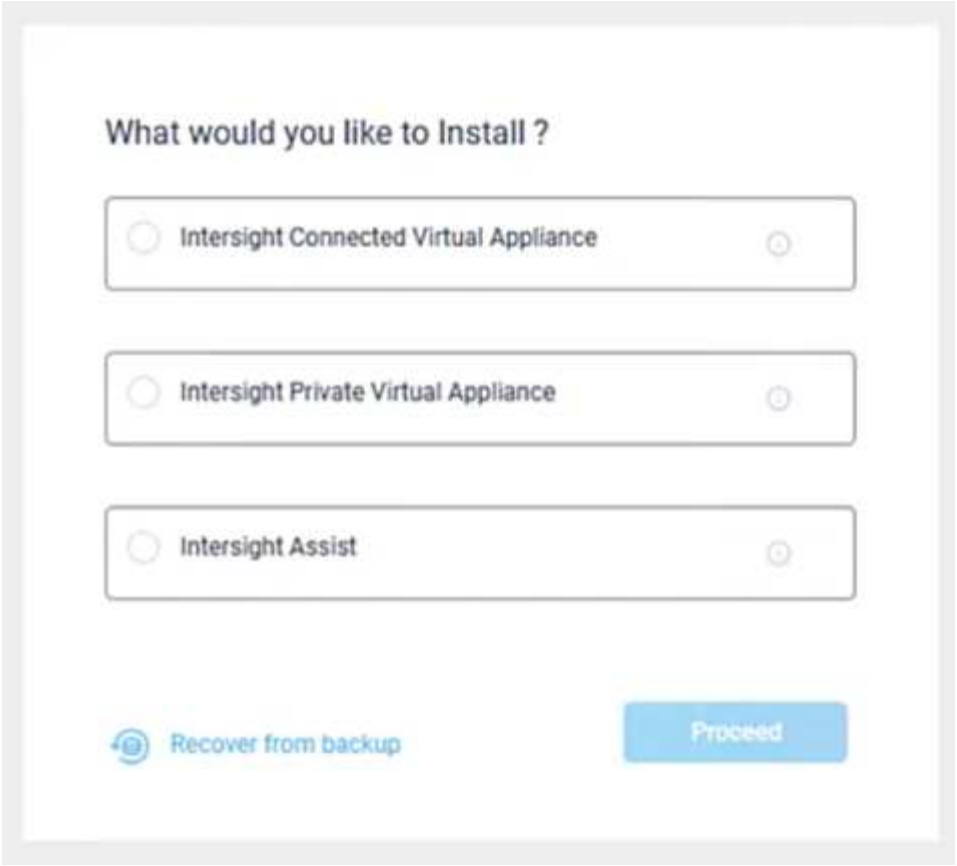
   a. Navigieren Sie zu https://FQDN-of-your-appliance So schließen Sie die Einrichtung Ihrer Appliance nach der Installation ab.

      Die Installation wird automatisch gestartet. Die Installation kann je nach Bandbreite bis zu Intersight.com bis zu einer Stunde in Anspruch nehmen. Es kann auch einige Sekunden dauern, bis der sichere Standort betriebsbereit ist, nachdem die VM eingeschaltet wurde.

   b. Wählen Sie während des Prozesses nach der Implementierung die folgende Option aus:

      - **Intersight Assist.** mit dieser Bereitstellung kann das SaaS-Modell eine Verbindung zu Cisco Intersight herstellen.

        Wenn Sie Intersight Assist auswählen, notieren Sie sich die Geräte-ID und den Antragscode, bevor Sie fortfahren.



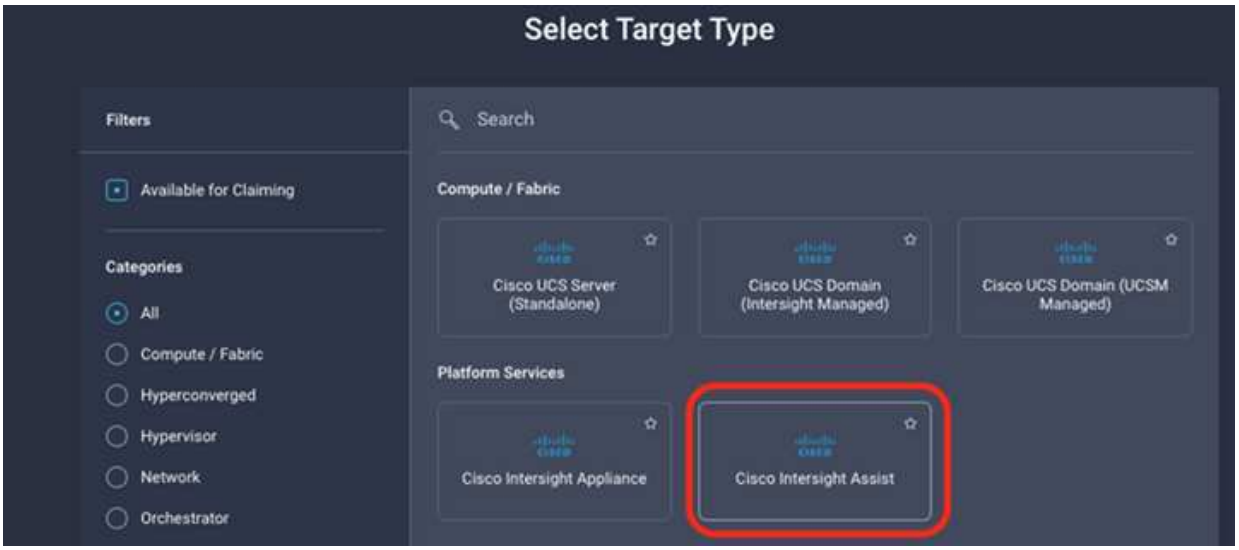
a. Klicken Sie Auf **Weiter**.

b. Wählen Sie **Intersight Assist** aus, und führen Sie die folgenden Schritte aus:

   i. Navigieren Sie unter zu Ihrem SaaS Intersight Konto "https://intersight.com".

   ii. Klicken Sie auf **Ziele**, **Cisco Intersight Assist** und dann auf **Start**.

   iii. Fordern Sie das Gerät **Cisco Intersight Assist** an, indem Sie die Geräte-ID und den Forderungscode von Ihrem neu eingesetzten virtuellen Intersight Assist-Gerät kopieren und einfügen.



   iv. Kehren Sie zum **Cisco Intersight Assist**-Gerät zurück und klicken Sie auf **Weiter.** möglicherweise müssen Sie den Browser aktualisieren.

Der Download- und Installationsprozess beginnt. Die Binärdateien werden von Intersight Cloud auf Ihre On-Prem-Appliance übertragen. Die Zeit für die Fertigstellung hängt von der Bandbreite der Intersight Cloud ab.

Konfigurieren Sie AIQ um Proxy-Server für den IMT-Dienst

Wenn Sie einen Proxy-Server mit AIQ um für Cisco Intersight mit NetApp ONTAP Storage verwenden, müssen Sie das Setup über die Befehlszeilenschnittstelle (CLI) konfigurieren, um den Interoperabilitäts-Matrix-Tool-Service (IMT) zu nutzen. Der IMT-Service ist auf der Seite * Integrated Systems* auf der Registerkarte **Interoperabilität** verfügbar. Sie müssen die Einstellungen für den AIQ um-Proxyserver über die Active IQ Unified Manager-Diag-Shell (Virtual Machine) konfigurieren.

Informationen zum Zugriff auf die Shell von AIQ um Diag finden Sie unter "So greifen Sie auf die Active IQ Unified Manager Virtual Machine (OVA) DIAG Shell zu"

Schritte

1. Melden Sie sich am AIQ um Terminal an und führen Sie den folgenden Befehl aus, um sich bei um anzumelden.

```
um cli login -u <um maintenance user name>
```

Beispiel

```
um cli login -u admin
```

2. Stellen Sie die ein `imt_proxy_host` Und `imt_proxy_port` Durch Ausführen der folgenden Befehle.

Der IMT-Proxy ist eine separate Konfiguration mit den AutoSupport (ASUP) Proxy-Konfigurationen.

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

Beispiel

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

Die Konfigurationen des IMT-Proxyservers unterstützen keine Authentifizierung.

3. Zeigen Sie die IMT-Proxydetails an, um die zu überprüfen `proxy_host` Und `proxy_port` Einstellungen

über den folgenden Befehl:

```
um option list |grep imt
```

Ziele der Forderung

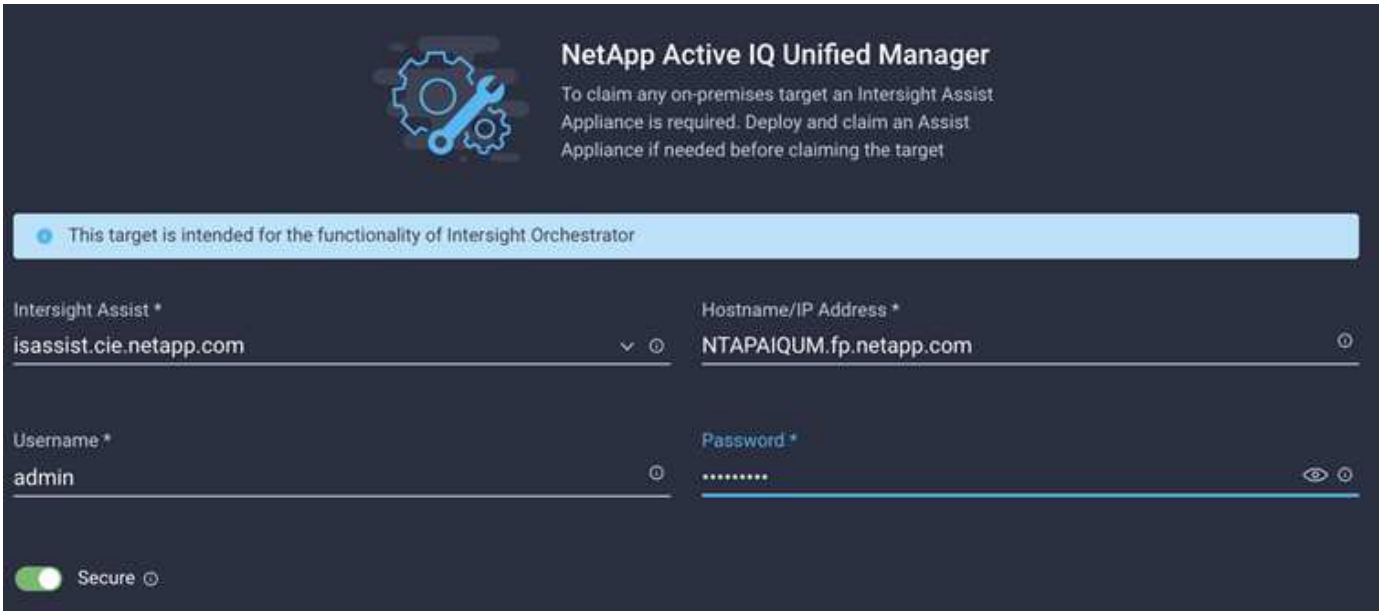
Nach der Installation von Cisco Intersight Assist können Sie Ihre NetApp Storage- und Virtualisierungsgeräte beanspruchen. Kehren Sie zur Seite **Intersight Targets** zurück und fügen Sie Ihre vCenter- und NetApp Active IQ Unified Manager-Ziele hinzu.

Stellen Sie sicher, dass das NetApp Active IQ Unified Manager (AIQ um) API-Gateway aktiviert ist.

Navigieren Sie im NetApp IQ Unified Manager zu **Einstellungen > Allgemein > Funktionseinstellungen**.

Das folgende Beispiel zeigt das Ziel NetApp AIQ um, das von Cisco Intersight in Anspruch genommen wird.

Wenn Sie ein NetApp AIQ um Ziel anfordern, werden alle von Active IQ Unified Manager gemanagten Cluster automatisch zu Intersight hinzugefügt.

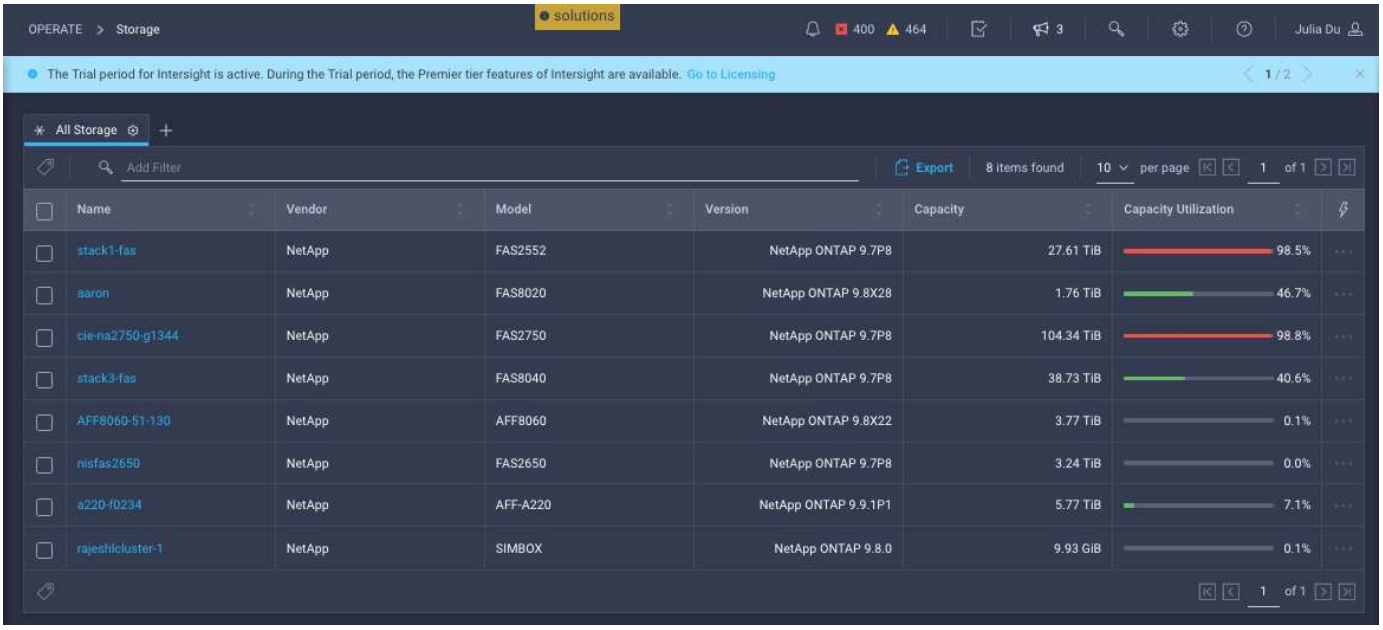


Überwachen Sie NetApp Storage von Cisco Intersight

Nachdem die Ziele beansprucht wurden, stehen die Registerkarten für NetApp Storage, Storage-Inventar und Virtualisierung zur Verfügung, wenn Sie eine Advantage-Tier-Lizenz besitzen. Bei einer Premier Tier-Lizenz stehen Registerkarten zur Orchestrierung zur Verfügung.

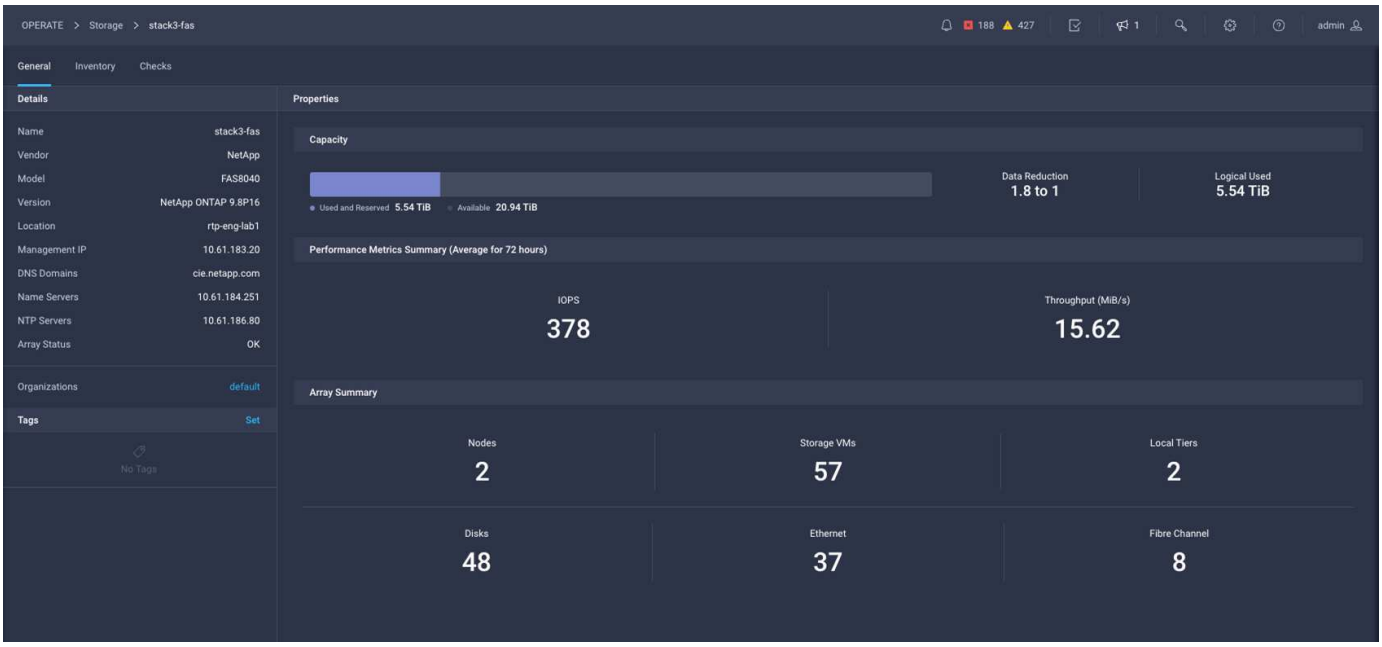
Überblick über den Storage-Bestand

Im folgenden Screenshot wird der Bildschirm **Bedienung > Speicher** angezeigt.



Der folgende Screenshot zeigt die Übersicht zum Storage Cluster.

Die folgenden Performancekennzahlen werden nur angezeigt, wenn das Speicher-Array über NetApp Active IQ Unified Manager 9.9 oder höher überwacht wird.

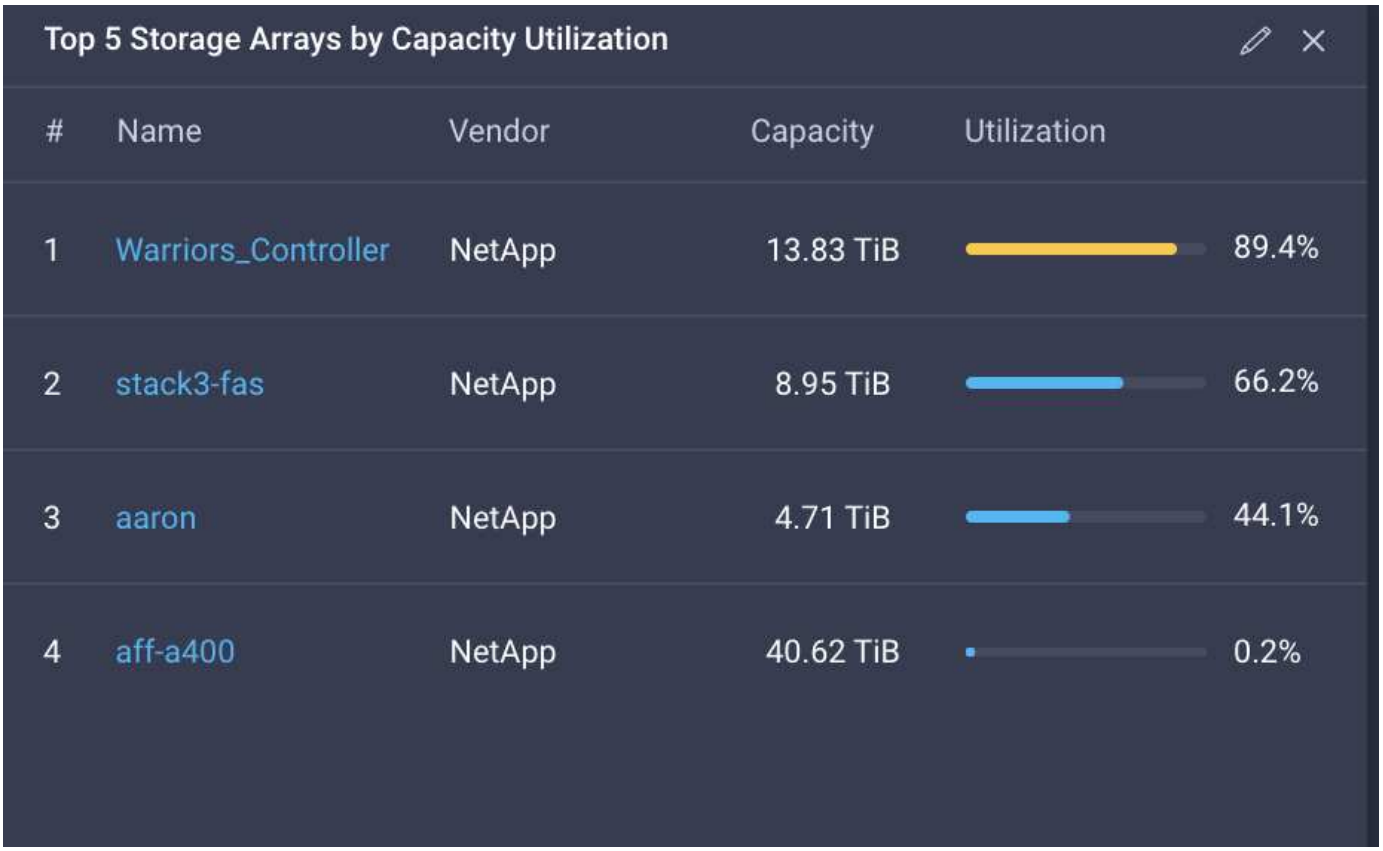


Storage-Widgets

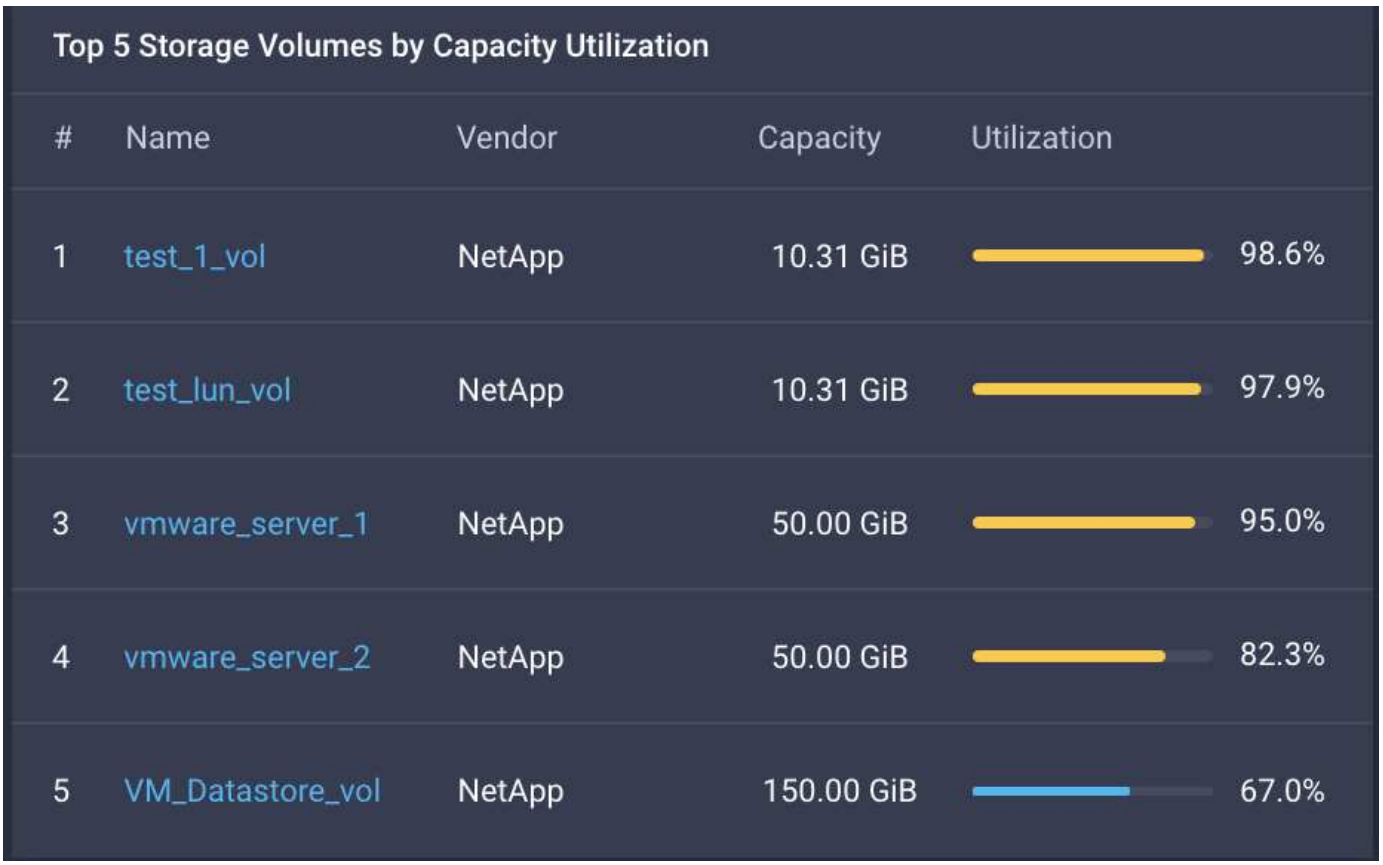
Um Storage-Widgets anzuzeigen, navigieren Sie zu **Überwachung > Dashboards > NetApp Storage Widgets anzeigen**.

- Der folgende Screenshot zeigt das Widget „Storage Version Summary“.

- Dieser Screenshot zeigt die Top 5 Storage Arrays nach Kapazitätsauslastung.



- Dieser Screenshot zeigt die Top 5 Storage Volumes nach Kapazitätsauslastung.



Anwendungsfälle

Dies sind einige Anwendungsbeispiele für die Überwachung und Orchestrierung von NetApp Storage von Cisco Intersight.

Anwendungsfall 1: Monitoring des NetApp Storage-Bestands und der Widgets

Wenn die NetApp Storage-Umgebung in Cisco Intersight verfügbar ist, können Sie NetApp Storage-Objekte aus dem Storage-Inventar im Detail überwachen und erhalten einen Überblick über die Storage Widgets.

1. Implementieren Sie Intersight Assist OVA (OnPrem Task in vCenter Umgebung).
2. Fügen Sie NetApp AIQ um Geräte in Intersight Assist hinzu.
3. Gehen Sie zu **Storage** und navigieren Sie durch den NetApp Storage-Bestand.
4. Fügen Sie **Widgets** für NetApp Storage zu Ihrem **Monitor Dashboard** hinzu.

Anwendungsfall 2: NetApp Storage-Orchestrierung mithilfe von Referenz-Workflows

Wenn NetApp Storage- und vCenter-Umgebungen in Cisco Intersight zur Verfügung stehen, können Sie End-to-End-Referenz-Workflows verwenden, die in GitHub über die verfügbar sind "FlexPod Intersight Workflow-Repository".

Die Referenz-Workflows umfassen Storage- und Virtualisierungsaufgaben. Die README-Datei für das Repository bietet die Voraussetzungen für die Ausführung von Workflows, Links zu hilfreichen Ressourcen (einschließlich Dokumentation zum Importieren eines Workflows) und Dokumentationslinks für jeden Referenz-Workflow.

Jeder Workflow hat einen Ordner im Repository, der zwei Dateien enthält:

- Die JSON-Datei zum Herunterladen und Importieren in Intersight,
- Eine Dokumentationsdatei, die eine Ansicht der Aufgaben im Workflow, Workflow-Eingaben und eine Beispielausführung des Workflows bietet.

Führen Sie folgende Schritte aus, um einen Referenz-Workflow zu importieren und zu verwenden:

1. Implementieren Sie Intersight Assist OVA (OnPrem Task in vCenter Umgebung).
2. Fügen Sie NetApp AIQ um Geräte in Intersight Assist hinzu.
3. Fügen Sie das vCenter-Ziel über Intersight Assist zu Intersight hinzu.
4. Laden Sie die JSON-Datei für einen Referenz-Workflow aus dem FlexPod-Intersight-Workflow-Repository herunter.
5. Importieren Sie den Workflow in Intersight, und führen Sie den Workflow aus.

Hier eine Liste der Workflows, die im GitHub FlexPod-Intersight-Workflow-Repository zur Verfügung stehen:

- Initiatoren zu NetApp-Initiatorgruppe hinzufügen
- Neue Exportrichtlinie für NetApp-Volumen
- Neuer NAS-Datenspeicher mit NetApp Smart Volume
- Neue NetApp FC-Datenschnittstelle

- Neue NetApp-Initiatorgruppe
- Neue NetApp iSCSI-Datenschnittstelle
- Neue NetApp NAS-Datenschnittstelle
- Die neue NetApp Storage Virtual Machine
- Neuer VMFS-Datenspeicher mit NetApp Smart LUN
- Initiatoren aus NetApp-Initiatorgruppe entfernen
- Entfernen Sie den NAS-Datenspeicher mithilfe des NetApp-Smart-Volumes
- Entfernen Sie die NetApp-Exportrichtlinie
- NetApp Initiatorgruppe entfernen
- Entfernen Sie den VMFS-Datenspeicher mithilfe der intelligenten NetApp-LUN
- Aktualisieren Sie den NAS-Datenspeicher mit dem NetApp Smart Volume
- Aktualisieren Sie den VMFS-Datenspeicher mit der intelligenten NetApp-LUN

Anwendungsfall 3: Benutzerdefinierte Workflows mit Designer-freiem Formular

Wenn die NetApp Storage- und vCenter-Umgebungen in Cisco Intersight verfügbar sind, können Sie benutzerdefinierte Workflows mit NetApp Storage- und Virtualisierungsaufgaben erstellen.

1. Bereitstellen der Intersight Assist OVA (OnPrem Task in vCenter Umgebung)
2. Fügen Sie NetApp AIQ um Geräte in Intersight Assist hinzu.
3. Fügen Sie vCenter-Ziel über Intersight Assist zu Intersight hinzu.
4. Navigieren Sie in Intersight zur Registerkarte **Orchestration**.
5. Wählen Sie **Workflow Erstellen**.
6. Fügen Sie Ihren Workflows Storage- und Virtualisierungsaufgaben hinzu.

   Im Folgenden sind die NetApp Storage-Aufgaben aufgeführt, die bei Cisco Intersight verfügbar sind:

   - ACL zu NetApp-CIFS-Freigabe hinzufügen
   - Client-Match zu NetApp-Exportrichtlinienregel hinzufügen
   - Exportrichtlinie zum NetApp-Volume hinzufügen
   - Initiatoren zu NetApp-Initiatorgruppe hinzufügen
   - Regel zur NetApp-Exportrichtlinie hinzufügen
   - Fügen Sie der NetApp-Snapshot-Richtlinie einen Zeitplan hinzu
   - Bestätigen Sie den NetApp-Lizenzstatus
   - Bestätigen Sie den FCP-Protokollstatus der NetApp Storage Virtual Machine
   - Bearbeiten Sie NetApp Aggregate für Storage Virtual Machine
   - Bearbeiten Sie die Richtlinie für asynchronen NetApp SnapMirror
   - Bearbeiten Sie die ACL-Berechtigung für die NetApp-CIFS-Freigabe
   - NetApp-Exportrichtlinienregel bearbeiten
   - Bearbeiten Sie die NetApp-Snapshot-Richtlinie
   - NetApp-Snapshot-Richtlinienzeitplan bearbeiten

- NetApp-Volume-Sicherheitstyp bearbeiten
- Bearbeiten Sie die Snapshot-Richtlinie des NetApp-Volumes
- Aktivieren Sie NetApp CIFS-Dienste
- Erweitern Sie die NetApp-LUN
- Neue Richtlinie für asynchronen NetApp SnapMirror
- Neuer NetApp CIFS-Server
- Neue NetApp CIFS-Freigabe
- Finden Sie die LUN-Zuordnung der NetApp-Initiatorgruppe
- Suchen Sie NetApp-LUN nach ID
- Suchen Sie NetApp-Volumes nach ID
- Neue NetApp-Exportrichtlinie
- Neue NetApp FC-Datenschnittstelle
- Neue NetApp-Initiatorgruppe
- Neue NetApp iSCSI-Datenschnittstelle
- Neue NetApp-Spiegelungen zur Lastverteilung für das SVM-Root-Volume
- Neue NetApp-LUN
- Neue NetApp-LUN-Zuordnung
- Neue NetApp NAS-Datenschnittstelle
- Neues NetApp NAS Smart Volume
- Neue intelligente NetApp-LUN
- Neue NetApp SnapMirror Beziehung für Volumes
- Neue NetApp Snapshot-Richtlinie
- Die neue NetApp Storage Virtual Machine
- Neues NetApp-Volume
- Neuer NetApp-Volume-Snapshot
- Registrieren Sie DNS für NetApp Storage Virtual Machine
- Entfernen Sie die ACL aus der NetApp-CIFS-Freigabe
- Entfernen Sie die Clientübereinstimmung aus der NetApp-Exportrichtlinienregel
- Exportrichtlinie aus NetApp-Volume entfernen
- Initiator aus NetApp-Initiatorgruppe entfernen
- Entfernen Sie den NetApp CIFS-Server
- Entfernen Sie die NetApp-CIFS-Freigabe
- Entfernen Sie die NetApp-Exportrichtlinie
- Entfernen Sie die NetApp FC-Datenschnittstelle
- NetApp Initiatorgruppe entfernen
- Entfernen Sie die NetApp IP-Schnittstelle
- Entfernen Sie NetApp-Spiegelungen zur Lastverteilung für das SVM-Root-Volume

- Entfernen Sie die NetApp-LUN
- Entfernen Sie die NetApp-LUN-Zuordnung
- Entfernen Sie das NetApp NAS Smart Volume
- Entfernen Sie die NetApp Smart LUN
- Entfernen Sie die NetApp SnapMirror Beziehung für Volume
- Entfernen Sie die NetApp SnapMirror Richtlinie
- Entfernen Sie die NetApp-Snapshot-Richtlinie
- Entfernen Sie die virtuelle Speichermaschine von NetApp
- Entfernen Sie das NetApp-Volume
- Entfernen Sie den NetApp-VolumeSnapshot
- Regel aus NetApp-Exportrichtlinie entfernen
- Entfernen Sie die Planung aus der NetApp-Snapshot-Richtlinie
- Benennen Sie NetApp-VolumeSnapshot um
- Aktualisieren Sie NetApp-Spiegelungen zur Lastverteilung für das SVM-Root-Volume
- Aktualisieren Sie die NetApp-Volume-Kapazität

Infrastruktur

End-to-End NVMe für FlexPod mit Cisco UCSM, VMware vSphere 7.0 und NetApp ONTAP 9

TR-4914: End-to-End NVMe for FlexPod with Cisco UCSM, VMware vSphere 7.0 and NetApp ONTAP 9

Chris Schmitt und Kamini Singh, NetApp

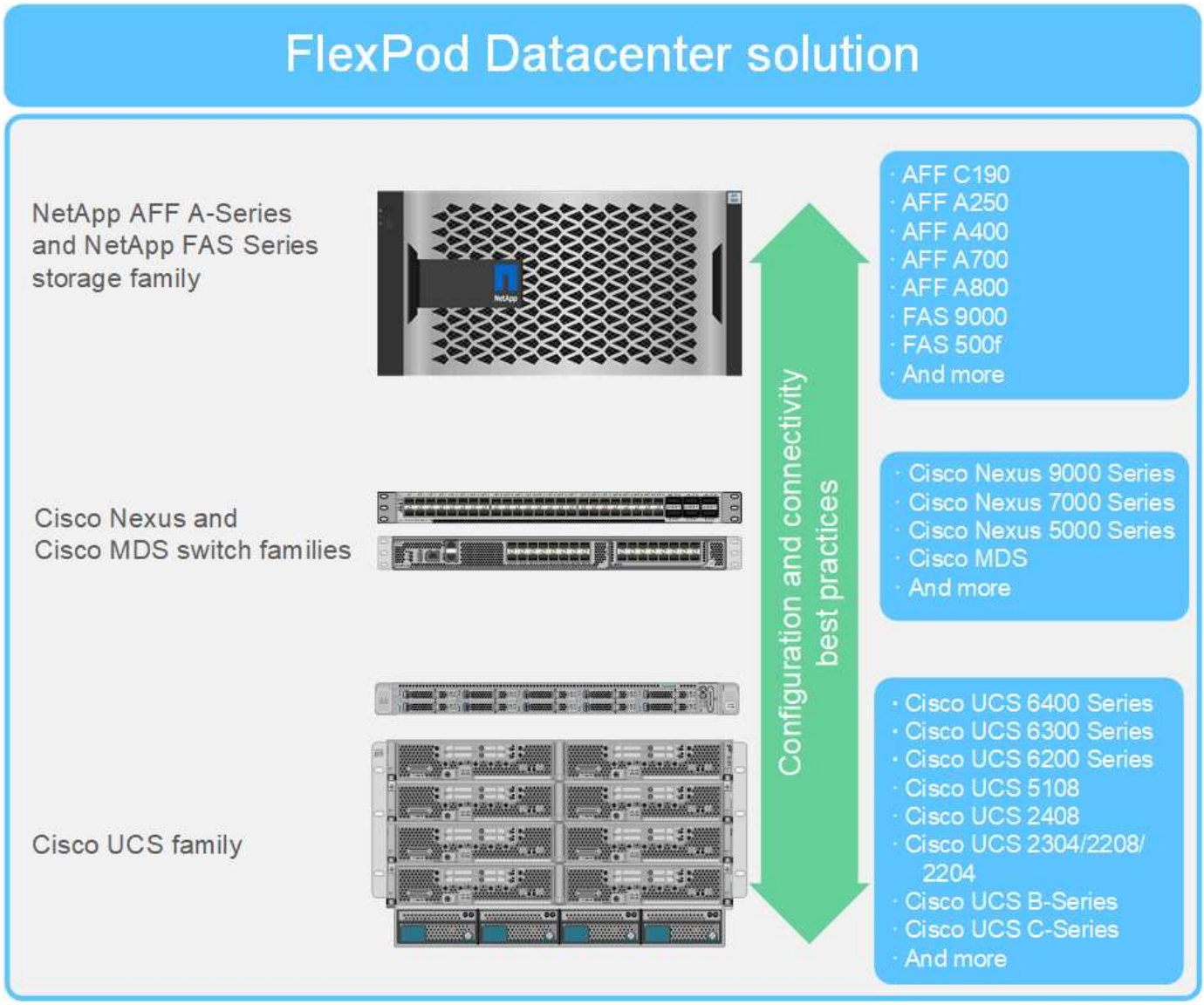
In Zusammenarbeit mit: 

Der NVMe-Storage-Standard, eine moderne Kerntechnologie, verändert den Zugriff und die Datenübertragung zu Enterprise-Storage durch sehr hohe Bandbreite und den Storage-Zugriff mit sehr niedriger Latenz für aktuelle und zukünftige Speichertechnologien. NVMe ersetzt den SCSI-Befehlssatz durch den NVMe-Befehlssatz.

NVMe wurde für die Verwendung mit nicht-flüchtigen Flash-Laufwerken, Multi-Core-CPUs und Gigabyte an Speicher konzipiert. Darüber hinaus profitiert es von den deutlichen Fortschritten in der Informatik seit den 1970er Jahren und ermöglicht optimierte Befehlssätze, die Daten effizienter analysieren und bearbeiten. Eine vollständige NVMe Architektur ermöglicht es Datacenter-Administratoren zudem, das Ausmaß zu überdenken, in dem sie ihre virtualisierten und Container-Umgebungen verschieben können, und das Ausmaß der Skalierbarkeit, die ihre transaktionsorientierten Datenbanken unterstützen können.

FlexPod ist eine Datacenter-Architektur mit Best Practices und umfasst Cisco Unified Computing System (Cisco UCS), Cisco Nexus Switches, Cisco MDS Switches und NetApp AFF Systeme. Diese Komponenten werden sowohl von Cisco als auch von NetApp entsprechend den Best Practices miteinander verbunden und konfiguriert, sodass eine hervorragende Plattform zur Ausführung einer Vielzahl von Enterprise Workloads zuverlässig bereitgestellt wird. FlexPod kann horizontal skaliert werden, um die Performance und Kapazität zu steigern (Computing-, Netzwerk- oder Storage-Ressourcen werden je nach Bedarf einzeln hinzugefügt). Alternativ können Sie auch horizontal skalieren, wenn mehrere konsistente Implementierungen erforderlich sind (beispielsweise die Einrichtung zusätzlicher FlexPod-Stacks).

Die Produktfamilien von FlexPod in der folgenden Abbildung.



FlexPod ist die ideale Plattform zur Einführung von FC-NVMe. Es kann durch Hinzufügen der Cisco UCS VIC 1400 Serie und Port Expander in bestehenden Cisco UCS B200 M5 oder M6 Servern oder Cisco UCS C-Series M5 oder M6 Rack Servern unterstützt werden. Zudem lassen sich einfache, unterbrechungsfreie Software-Upgrades für das Cisco UCS System, die Cisco MDS 32Gbps Switches, Und die NetApp AFF Storage-Arrays. Nach Installation der unterstützten Hardware und Software ist die Konfiguration von FC-NVMe vergleichbar mit der FCP-Konfiguration.

NetApp ONTAP 9.5 und höher bietet eine umfassende FC-NVMe-Lösung. Ein unterbrechungsfreies Software-Update der ONTAP für AFF A300, AFF A400, AFF A700, AFF A700s und AFF A800 Arrays ermöglicht diesen Geräten die Unterstützung eines End-to-End-NVMe-Storage-Stacks. Daher können Server mit HBAs (Host Bus Adapter) der sechsten Generation und NVMe-Treiber-Unterstützung über natives NVMe mit diesen Arrays kommunizieren.

Ziel

Diese Lösung bietet einen allgemeinen Überblick über die FC-NVMe Performance mit VMware vSphere 7 auf FlexPod. Die Lösung wurde verifiziert, dass sie den FC-NVMe-Datenverkehr erfolgreich bestanden hat, und Performance-Matrizen wurden für FC-NVMe mit verschiedenen Datenblockgrößen erfasst.

Vorteile der Lösung

End-to-End-NVMe für FlexPod bietet Kunden hervorragenden Mehrwert und bietet folgende Vorteile:

- NVMe setzt auf PCIe, ein Hardwareprotokoll mit hoher Geschwindigkeit und hoher Bandbreite, das wesentlich schneller ist als ältere Standards wie SCSI, SAS und SATA. Cisco UCS Server und NetApp Storage Array für die meisten anspruchsvollen Applikationen sind mit hoher Bandbreite und äußerst geringer Latenz verbunden.
- Eine FC-NVMe-Lösung ist verlustfrei in der Lage, die Skalierbarkeitsanforderungen von Applikationen der neuesten Generation zu erfüllen. Zu diesen neuen Technologien zählen künstliche Intelligenz (KI), maschinelles Lernen (ML), Deep Learning (DL), Echtzeitanalysen und andere geschäftskritische Applikationen.
- Geringere IT-Kosten durch effiziente Nutzung aller Ressourcen im gesamten Stack
- Verkürzt die Reaktionszeiten erheblich und steigert die Applikations-Performance – dies entspricht einem höheren IOPS-Wert und einem höheren Durchsatz bei niedrigerer Latenz. Die Lösung bietet ~60 % mehr Performance und verringert die Latenz um ~50 % bei bestehenden Workloads.
- FC-NVMe ist ein optimiertes Protokoll mit ausgezeichneten Warteschlangen, besonders in Situationen mit mehr I/O-Operationen pro Sekunde (IOPS, also mehr Transaktionen) und parallelen Aktivitäten.
- Ermöglicht unterbrechungsfreie Software Upgrades der FlexPod Komponenten wie Cisco UCS, Cisco MDS und der NetApp AFF Storage Arrays. Erfordert keine Änderung an Applikationen.

"Als Nächstes: Testansatz."

Testansatz

"Zurück: Einführung."

Dieser Abschnitt bietet einen allgemeinen Überblick über die Validierungstests für FC-NVMe auf FlexPod. Sie enthält sowohl die Testumgebung/Konfiguration als auch den angenommenen Testplan für die Durchführung der Workload-Tests im Hinblick auf FC-NVMe für FlexPod mit VMware vSphere 7.

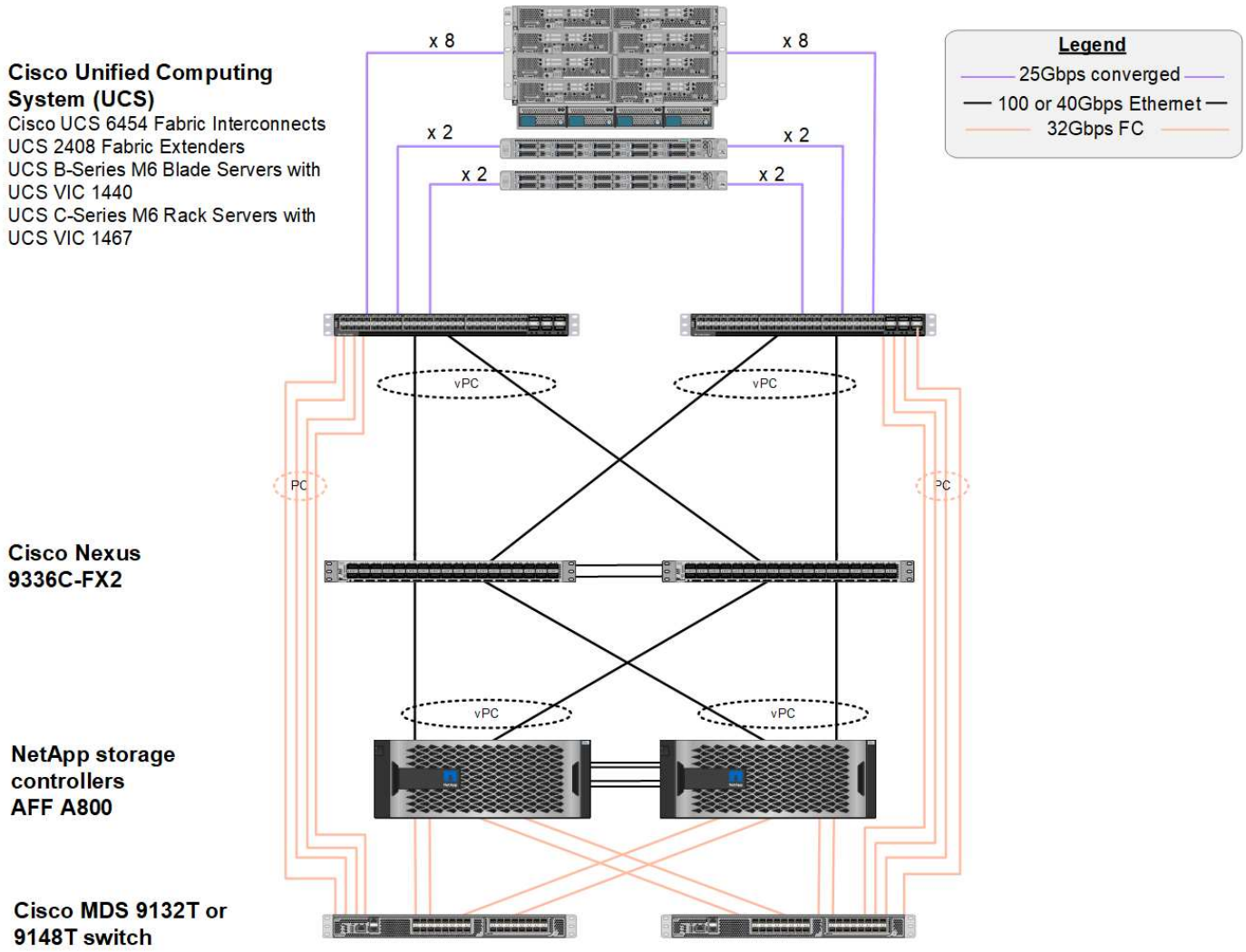
Testumgebung

Die Switches der Cisco Nexus 9000 Serie unterstützen zwei Betriebsmodi:

- Standalone-Modus für NX-OS unter Verwendung der Cisco NX-OS Software
- ACI Fabric-Modus mit der Cisco Application Centric Infrastructure (Cisco ACI) Plattform

Im Standalone-Modus funktioniert der Switch wie ein typischer Cisco Nexus Switch mit höherer Portdichte, niedriger Latenz sowie 40-GbE- und 100-GbE-Konnektivität.

FlexPod mit NX-OS wurde als vollständig redundant auf den Computing-, Netzwerk- und Storage-Ebenen konzipiert. Es gibt keinen Single Point of Failure aus der Perspektive eines Geräts oder Datenpfads. Die Abbildung unten zeigt die verschiedenen Elemente des neuesten FlexPod Designs, die in dieser Validierung von FC-NVMe verwendet werden.



Hinsichtlich FC SAN verwendet dieses Design die neuesten Cisco UCS 6454 Fabric Interconnects der vierten Generation sowie die Cisco UCS VIC 1400 Plattform mit Port-Erweiterung in den Servern. Die Cisco UCS B200 M6 Blade Server im Cisco UCS Chassis verwenden den Cisco UCS VIC 1440 mit Port-Expander, der mit dem IOM des Cisco UCS 2408 Fabric Extender verbunden ist. Jeder Fibre Channel over Ethernet (FCoE) Virtual Host Bus Adapter (vHBA) hat eine Geschwindigkeit von 40 Gbit/s. Die von Cisco UCS verwalteten Cisco UCS C220 M5 Rack Server nutzen den Cisco UCS VIC 1457 mit zwei Schnittstellen mit 25 Gbit/s zu jedem Fabric Interconnect. Jeder C220 M5 FCoE vHBA hat eine Geschwindigkeit von 50 Gbit/s.

Die Fabric Interconnects sind über 32 Gbit/s SAN-Port-Kanäle mit den Cisco MDS 9148T der neuesten Generation oder 9132T FC Switches verbunden. Die Konnektivität zwischen den Cisco MDS Switches und dem NetApp AFF A800 Storage-Cluster ist ebenfalls 32 Gbit/s FC. Diese Konfiguration unterstützt 32 Gbit/s FC für Fibre Channel Protocol (FCP) und FC-NVMe Storage zwischen dem Storage-Cluster und Cisco UCS. Für diese Validierung werden vier FC-Verbindungen zu jedem Storage Controller verwendet. Bei jedem Storage-Controller werden die vier FC-Ports für FCP- und FC-NVMe-Protokolle verwendet.

Die Konnektivität zwischen den Cisco Nexus Switches und dem NetApp AFF A800 Storage-Cluster der neuesten Generation ist ebenfalls 100 Gbit/s mit Port-Channels auf den Storage Controllern und vPCs auf den Switches. Die NetApp AFF A800 Storage-Controller sind mit NVMe-Festplatten auf dem PCIe-Bus (Peripheral Connect Interface Express) mit höherer Geschwindigkeit ausgestattet.

Die in dieser Validierung verwendete FlexPod Implementierung basiert auf "FlexPod Datacenter mit Cisco UCS 4.2(1) im UCS Managed Mode, VMware vSphere 7.0U2 und NetApp ONTAP 9.9".

Validierte Hardware und Software

In der folgenden Tabelle sind die während der Lösungsvalidierung verwendeten Hardware- und Softwareversionen aufgeführt. Beachten Sie, dass Cisco und NetApp Interoperabilitätsmatrixe verfügen, die referenziert werden sollten, um den Support für jede spezifische Implementierung von FlexPod zu bestimmen. Weitere Informationen finden Sie in den folgenden Ressourcen:

- "NetApp Interoperabilitäts-Matrix-Tool"
- "Cisco UCS Hardware and Software Interoperability Tool"

Schicht	Gerät	Bild	Kommentare
Computing	• Zwei Cisco UCS 6454 Fabric Interconnects • Ein Cisco UCS 5108 Blade-Chassis mit zwei Cisco UCS 2408 I/O-Modulen • Vier Cisco UCS B200 M6 Blades, jeweils mit einem Cisco UCS VIC 1440 Adapter und einer Port-Erweiterungskarte	Version 4.2 (1f)	Mit Cisco UCS Manager, Cisco UCS VIC 1440 und Port-Erweiterung
CPU	Zwei Intel Xeon Gold 6330 CPUs mit 2.0 GHz, mit 42 MB Layer 3 Cache und 28 Cores pro CPU	–	–
Speicher	1024 GB (16 x 64 GB DIMMs mit 3200 MHz)	–	–
Netzwerk	Zwei Cisco Nexus 9336C-FX2 Switches im Standalone-Modus mit NX-OS	Version 9.3(8)	–
Datennetzwerk Storage-Netzwerk	Zwei Cisco MDS 9132T 32-Gbit/s-FC-Switches mit 32 Ports	Version 8.4(2c)	Unterstützung für FC-NVMe SAN-Analysen
Storage	Zwei NetApp AFF A800 Storage-Controller mit 24 x 1,8-TB-NVMe-SSDs	NetApp ONTAP 9.9.1P1	–
Software	Cisco UCS Manager	Version 4.2 (1f)	–
	VMware vSphere	7,0U2	–
	VMware ESXi	7.0.2	–
	Nativer VMware ESXi Fibre Channel NIC-Treiber (NFNIC)	5.0.0.12	Unterstützung für FC-NVMe auf VMware

Schicht	Gerät	Bild	Kommentare
	Nativer VMware ESXi Ethernet NIC-Treiber (NNIC)	1.0.35.0	–
Testwerkzeug	FIO	3.19	–

Testplan

Wir haben einen Performance-Testplan entwickelt, um NVMe auf FlexPod unter Verwendung eines synthetischen Workloads zu validieren. Mit diesem Workload konnten wir 8 KB zufällige Lese- und Schreibvorgänge sowie Lese- und Schreibvorgänge mit 64 KB ausführen. Wir haben VMware ESXi Hosts benutzt, um unsere Testfälle gegen den AFF A800 Storage auszuführen.

Wir haben FIO, ein Open-Source-Tool für synthetische I/O, das zur Performance-Messung verwendet werden kann, um unseren synthetischen Workload zu generieren.

Um unsere Performance-Tests abzuschließen, haben wir sowohl für Storage als auch für Server mehrere Konfigurationsschritte durchgeführt. Im Folgenden finden Sie die detaillierten Schritte der Implementierung:

1. Was den Storage angeht, haben wir vier Storage Virtual Machines (SVMs, ehemals Vserver), acht Volumes pro SVM und einen Namespace pro Volume erstellt. Wir haben 1-TB-Volumes und 960-GB-Namespaces erstellt. Wir haben vier LIFs pro SVM und ein Subsystem pro SVM erstellt. Die SVM-LIFs wurden gleichmäßig über die acht verfügbaren FC-Ports des Clusters verteilt.
2. Auf Serverseite haben wir auf jedem unserer ESXi Hosts eine einzelne Virtual Machine (VM) erstellt, die insgesamt vier VMs entspricht. Wir haben FIO auf unseren Servern installiert, um die synthetischen Workloads auszuführen.
3. Nachdem der Storage und die VMs konfiguriert wurden, konnten wir eine Verbindung zu den Storage-Namespaces der ESXi Hosts herstellen. Dadurch konnten wir auf Basis unseres Namespace Datastores erstellen und dann auf Basis dieser Datastores Virtual Machine Disks (VMDKs) erstellen.

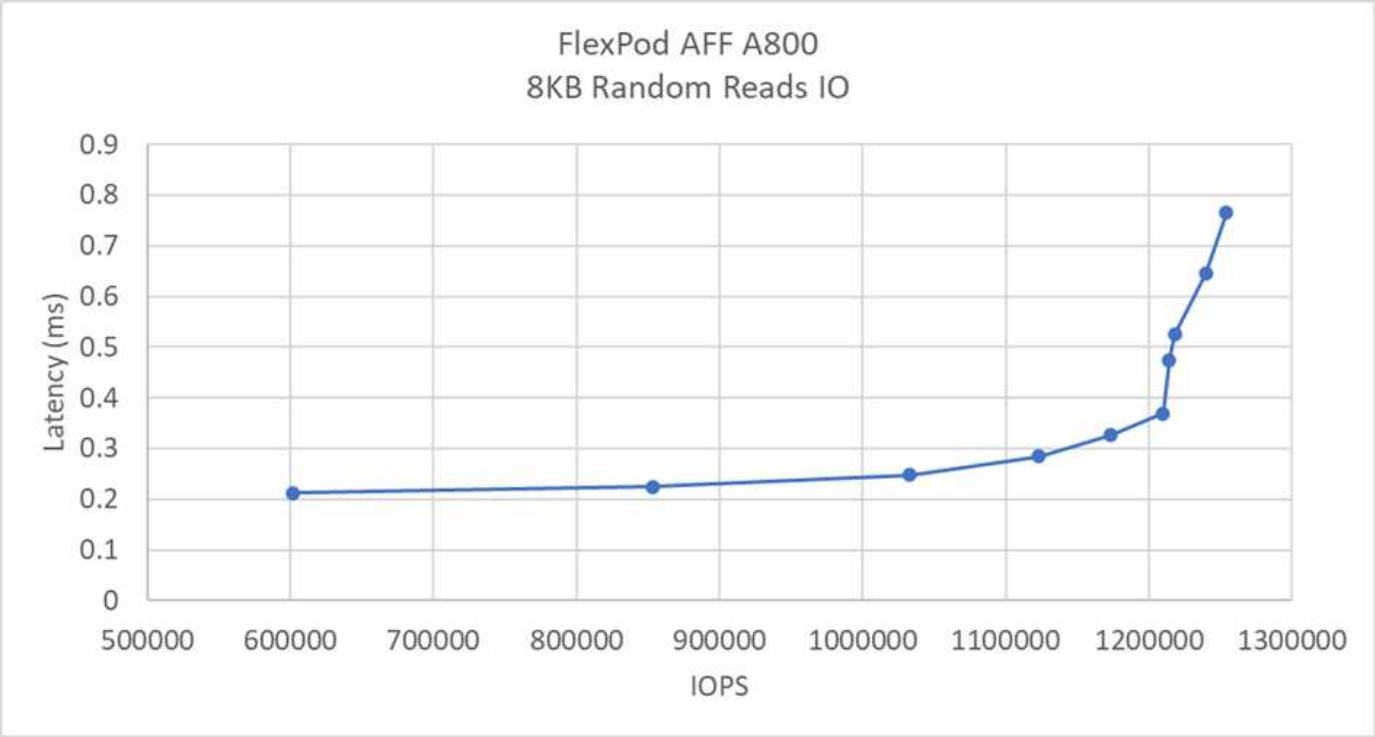
"Weiter: Testergebnisse."

Testergebnisse

"Früher: Testansatz."

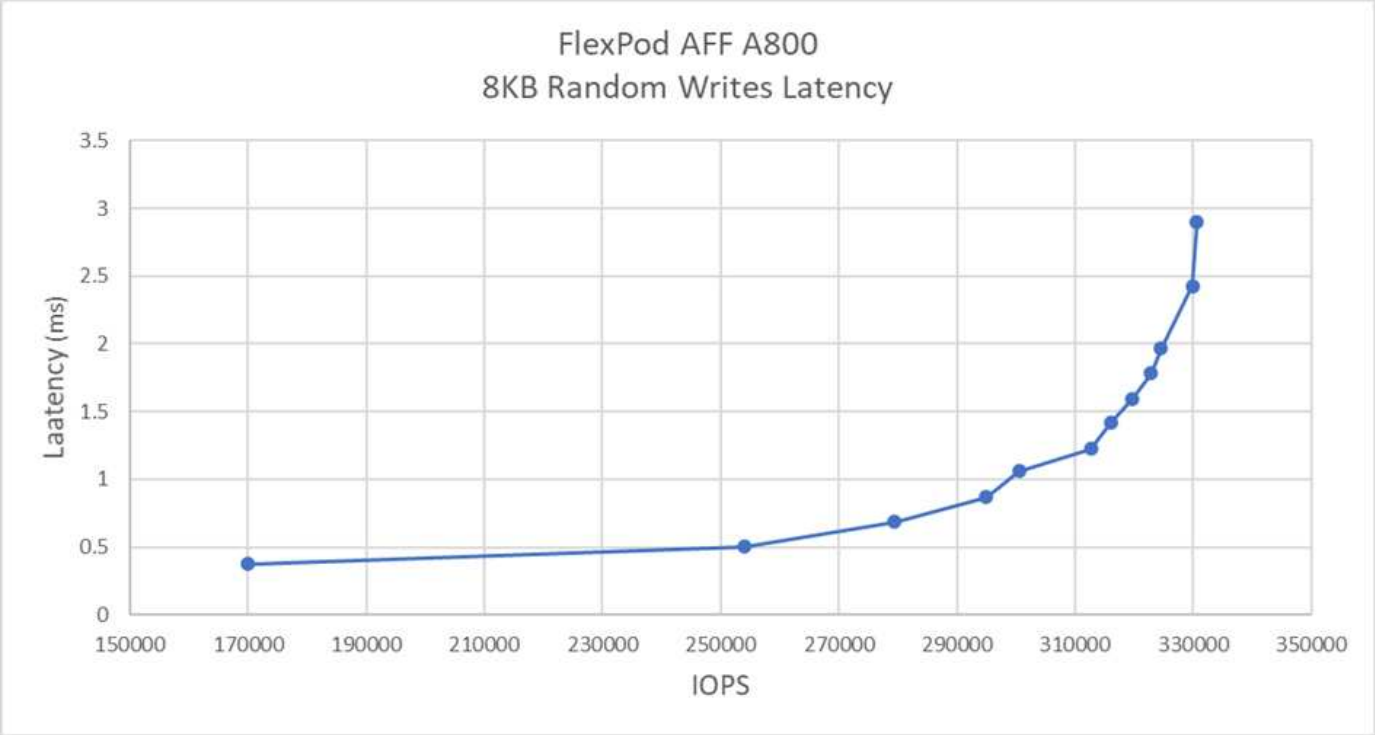
Die Tests bestanden aus der Ausführung der FIO-Workloads, um die FC-NVMe-Performance in Bezug auf IOPS und Latenz zu messen.

Das folgende Diagramm zeigt unsere Ergebnisse bei der Ausführung eines Workloads mit 100 % zufälligen Lesevorgängen mit 8-KB-Blockgrößen.



In unseren Tests stellten wir fest, dass das System bei einer Latenz von weniger als 0,35 ms durch eine serverseitige Latenz über 1,2 Millionen IOPS erreicht hat.

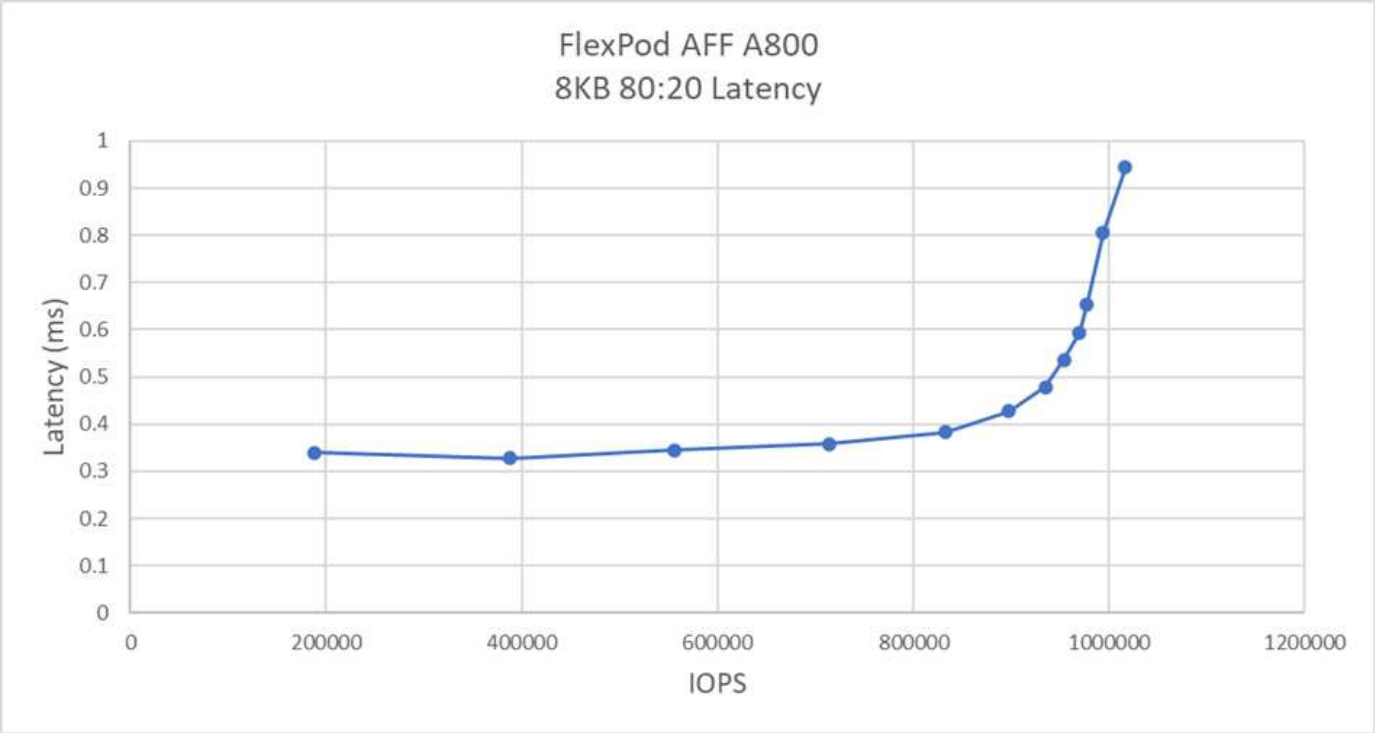
Das folgende Diagramm zeigt unsere Ergebnisse bei der Ausführung eines Workloads mit 100 % zufälligen Schreibvorgängen mit 8-KB-Blockgrößen.



In unseren Tests stellten wir fest, dass das System fast bis 300.000 IOPS erreicht hat und dabei eine serverseitige Latenz von nur weniger als 1 ms erzielt hat.

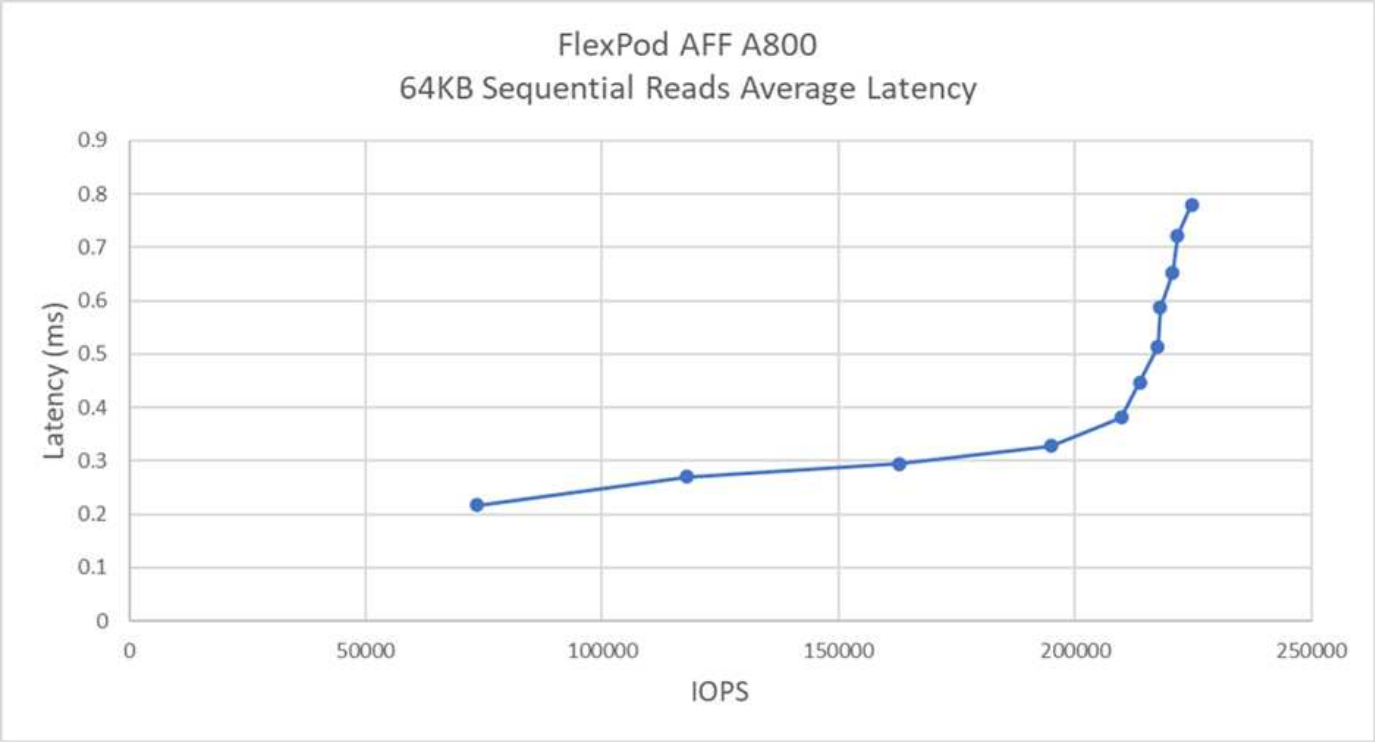
Bei 8 KB Blockgröße mit 80 % zufälligen Lesevorgängen und 20 % Schreibvorgängen beobachteten wir die

folgenden Ergebnisse:



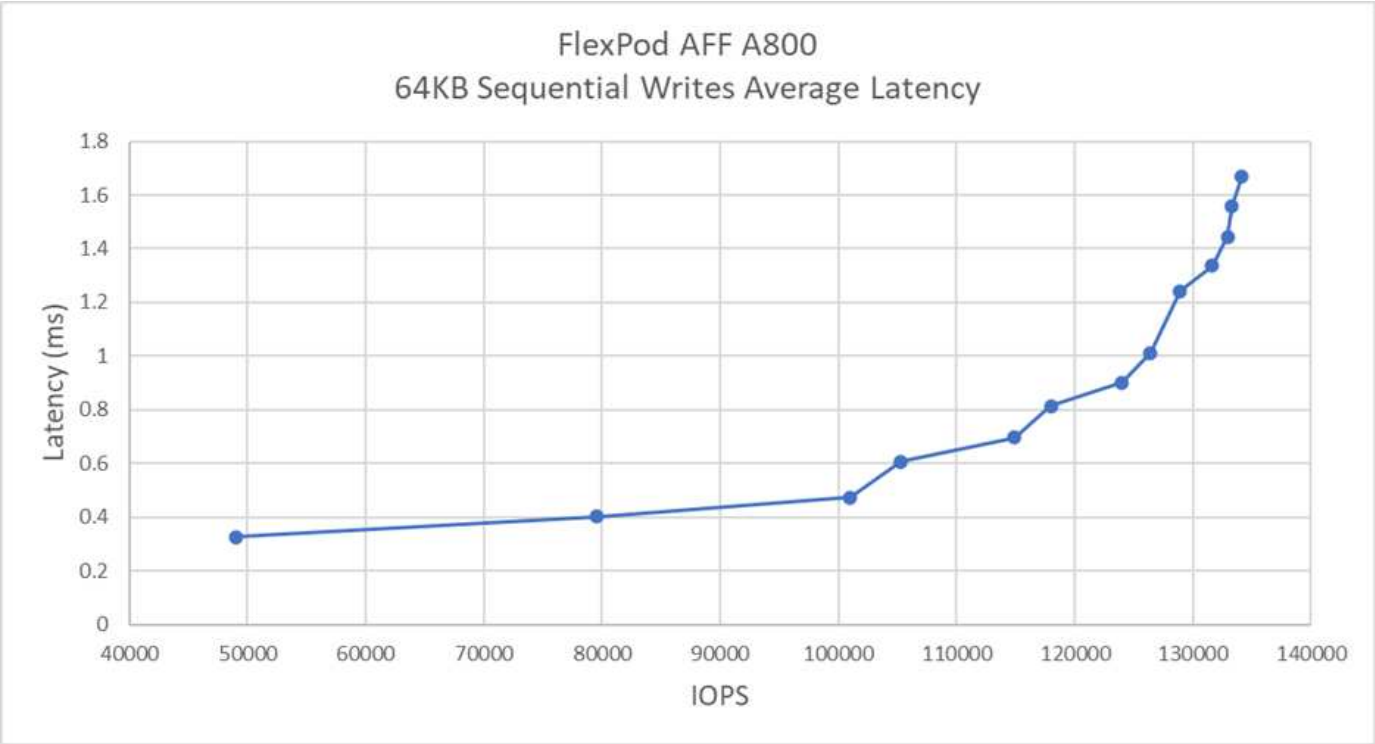
In unseren Tests stellten wir fest, dass das System über 1 Mio. IOPS erreichte und dabei eine Latenz von nur knapp unter 1 ms bei serverseitiger Latenz erreichte.

Bei 64 KB Blockgröße und 100 % sequenziellen Lesevorgängen haben wir die folgenden Ergebnisse beobachtet:



In unseren Tests stellten wir fest, dass das System ungefähr 250.000 IOPS erreichte und dabei eine Latenz von nur knapp unter 1 ms bei serverseitiger Latenz erreichte.

Bei 64 KB Blockgröße und 100 % sequenziellen Schreibvorgängen haben wir die folgenden Ergebnisse beobachtet:



In unseren Tests stellten wir fest, dass das System ungefähr 120.000 IOPS erreichte und dabei eine Latenz von unter 1 ms bei serverseitiger Latenz erreichte.

"Weiter: Fazit."

Schlussfolgerung

"Zurück: Testergebnisse."

Der für diese Lösung beobachtete Durchsatz betrug 14 GB/s und 220.000 IOPS für einen sequenziellen Lese-Workload mit einer Latenz von unter 1 ms. Bei zufälligen Lese-Workloads erreichten wir einen Durchsatz von 9,5 GB/s und 1,25 Mio. IOPS. FlexPod kann diese Performance mit FC-NVMe bereitstellen und kann so die Anforderungen aller geschäftskritischen Applikationen erfüllen.

FlexPod Datacenter mit VMware vSphere 7.0 U2 ist die optimale Grundlage für eine Shared-Infrastruktur für die Implementierung von FC-NVMe für verschiedene IT-Workloads. Auf diese Weise erhalten Applikationen, die ihn benötigen, hochperformanten Storage-Zugriff. Da FC-NVMe jedoch mit Hochverfügbarkeit, Multipathing und zusätzlichem Betriebssystem-Support weiter entwickelt wird, eignet sich FlexPod hervorragend als bevorzugte Plattform und bietet die Skalierbarkeit und Zuverlässigkeit, die zur Unterstützung dieser Funktionen erforderlich sind.

Mit FlexPod haben Cisco und NetApp eine Plattform geschaffen, die sich flexibel und skalierbar für zahlreiche Anwendungsfälle und Applikationen ist. Mit FC-NVMe bietet FlexPod eine weitere Funktion, mit der Unternehmen geschäftskritische Applikationen effizient und effektiv gleichzeitig in derselben Shared IT-Infrastruktur unterstützen können. Dank der Flexibilität und Skalierbarkeit von FlexPod können Kunden mit einer geeigneten Infrastruktur beginnen, die mit den neuen Geschäftsanforderungen mitwächst.

Weitere Informationen

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

- Cisco Unified Computing System (UCS)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Fabric Interconnects der Cisco UCS 6400-Serie – Datenblatt

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Blade Server-Chassis der Cisco UCS 5100-Serie

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Blade Server der Cisco UCS B-Serie

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Cisco UCS C-Serie Rack Server

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Cisco Unified Computing System Adapter

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Switches Der Cisco Nexus 9000-Serie

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Cisco MDS 9000 Multilayer Fabric Switches

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Cisco MDS 9132T 32-Gbit/s-Fibre Channel Switch mit 32 Ports

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A-Series

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere

"https://www.vmware.com/products/vsphere"

- VMware vCenter Server

  "http://www.vmware.com/products/vcenter-server/overview.html"

- Best Practices für ein modernes SAN

  "https://www.netapp.com/us/media/tr-4080.pdf"

- Einführung von End-to-End-NVMe für FlexPod

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

Interoperabilitätsmatrixe

- NetApp Interoperabilitäts-Matrix-Tool

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

- Cisco UCS Hardware Compatibility Matrix

  "https://ucshcltool.cloudapps.cisco.com/public/"

- VMware Compatibility Guide

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

Danksagungen

Die Autoren bedanken sich herzlich bei John George von Cisco und Scott Lane und Bobby Oommen von NetApp für die Unterstützung und Anleitung, die bei der Projektdurchführung enthalten sind.

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"https://www.netapp.com/company/legal/copyright/"

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"