FlexPod Express

FlexPod

NetApp
January 21, 2025

This PDF was generated from https://docs.netapp.com/de-de/flexpod/express/express-c-series-c190-design_executive_summary.html on January 21, 2025. Always check docs.netapp.com for the latest.

Inhalt

FlexPod Express 1
Design Guide: FlexPod Express mit Cisco UCS C-Series und NetApp AFF C190 Serie 1
FlexPod Express mit Cisco UCS C-Series und NetApp AFF C190 Series – Implementierungsleitfaden 8
Entwurfsleitfaden für FlexPod Express mit Cisco UCS C-Serie und AFF A220 Serie 106
Implementierungs-Leitfaden: FlexPod Express mit Cisco UCS C-Series und AFF A220 Serie 116
FlexPod Express mit VMware vSphere 6.7U1 und NetApp AFF A220 mit Direct-Attached IP-basiertem Storage 198
FlexPod Express für VMware vSphere 7.0 mit Cisco UCS Mini und NetApp AFF/FAS – NVA – Implementierung 310

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:[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

"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
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.

[Fehler: Fehlendes Grafikbild]

Die folgende Abbildung zeigt 10GBASE-T-Ports für den Anschluss über herkömmliche RJ-45 Ethernet-Kabel.

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

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

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

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.

[Fehler: Fehlendes Grafikbild]

"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:

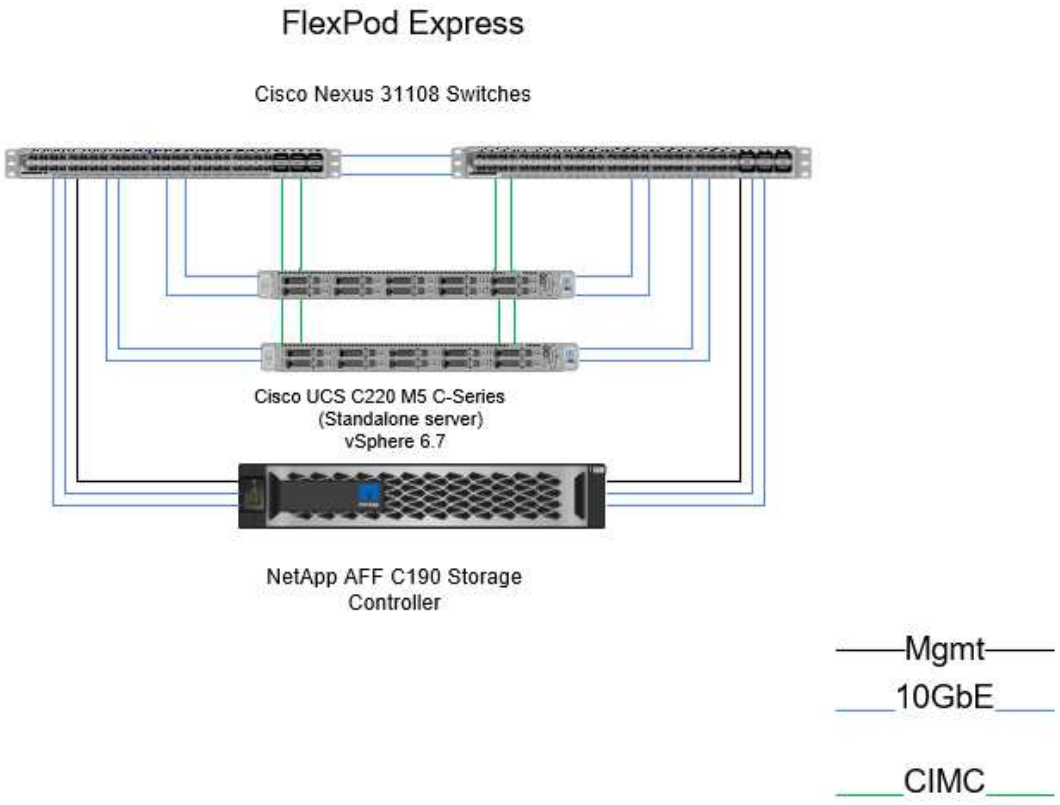
- Sorgfältig getestet
- Präskriptiv
- Minimale Implementierungsrisiken
- Beschleunigte Produkteinführungszeit

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

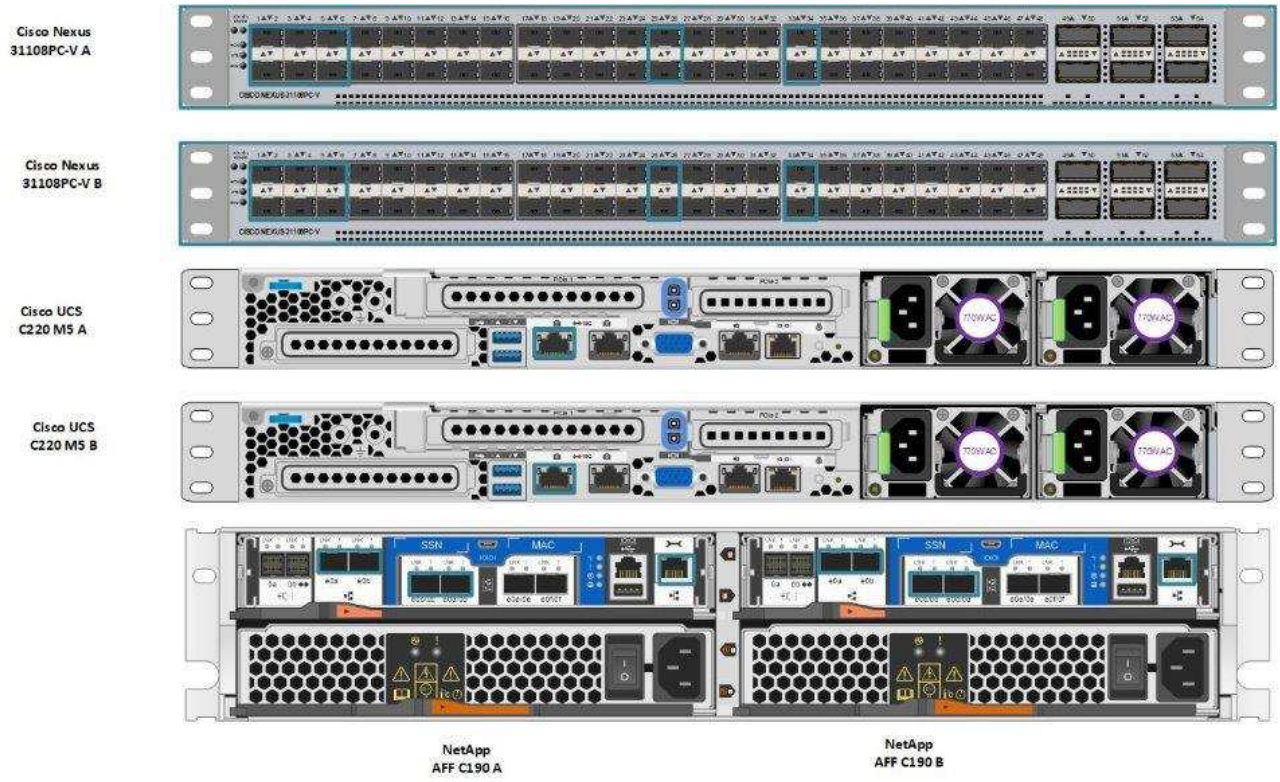
In dieser Tabelle ist die für alle VMware vSphere Implementierungen auf FlexPod Express erforderliche Software aufgeführt.

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.

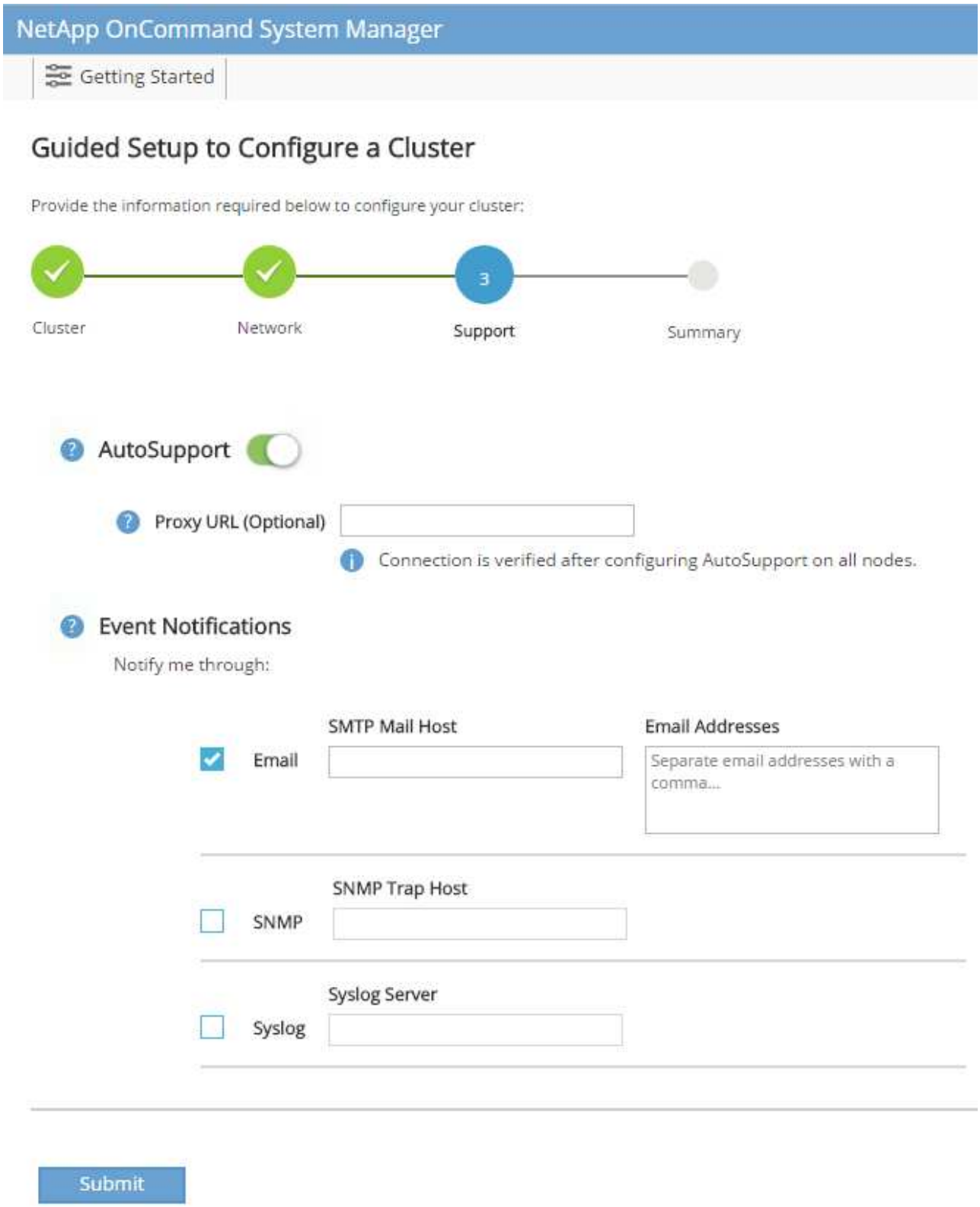
> Sie können auch einen alternativen NTP-Server eingeben. Die IP-Adresse `10.63.172.162` Von `<<var_ntp_server_ip>>` Ist die Nexus Management IP.

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>>`

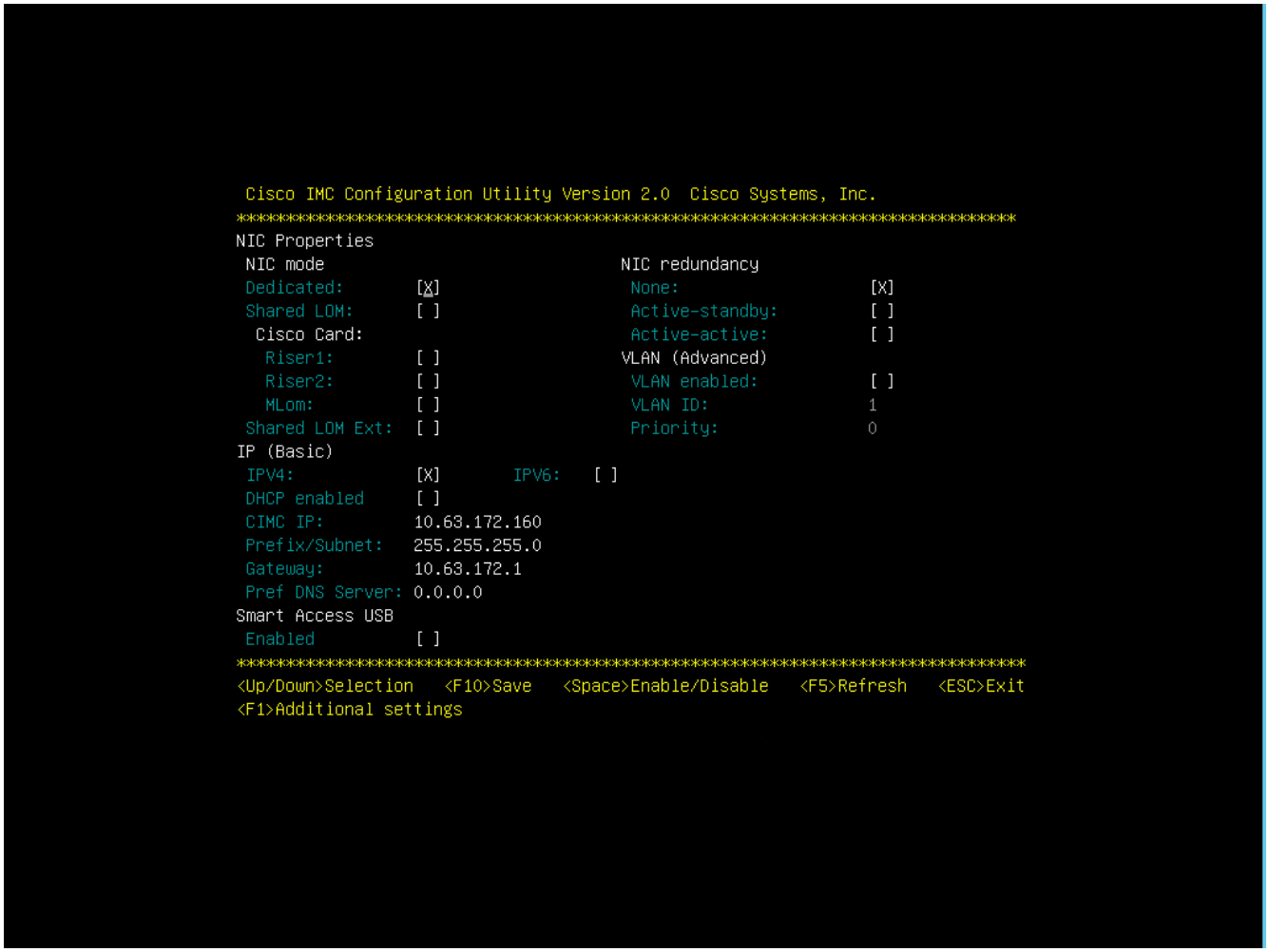
      Präfix/Subnetz: `<<cimc_netmask>>`

      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.

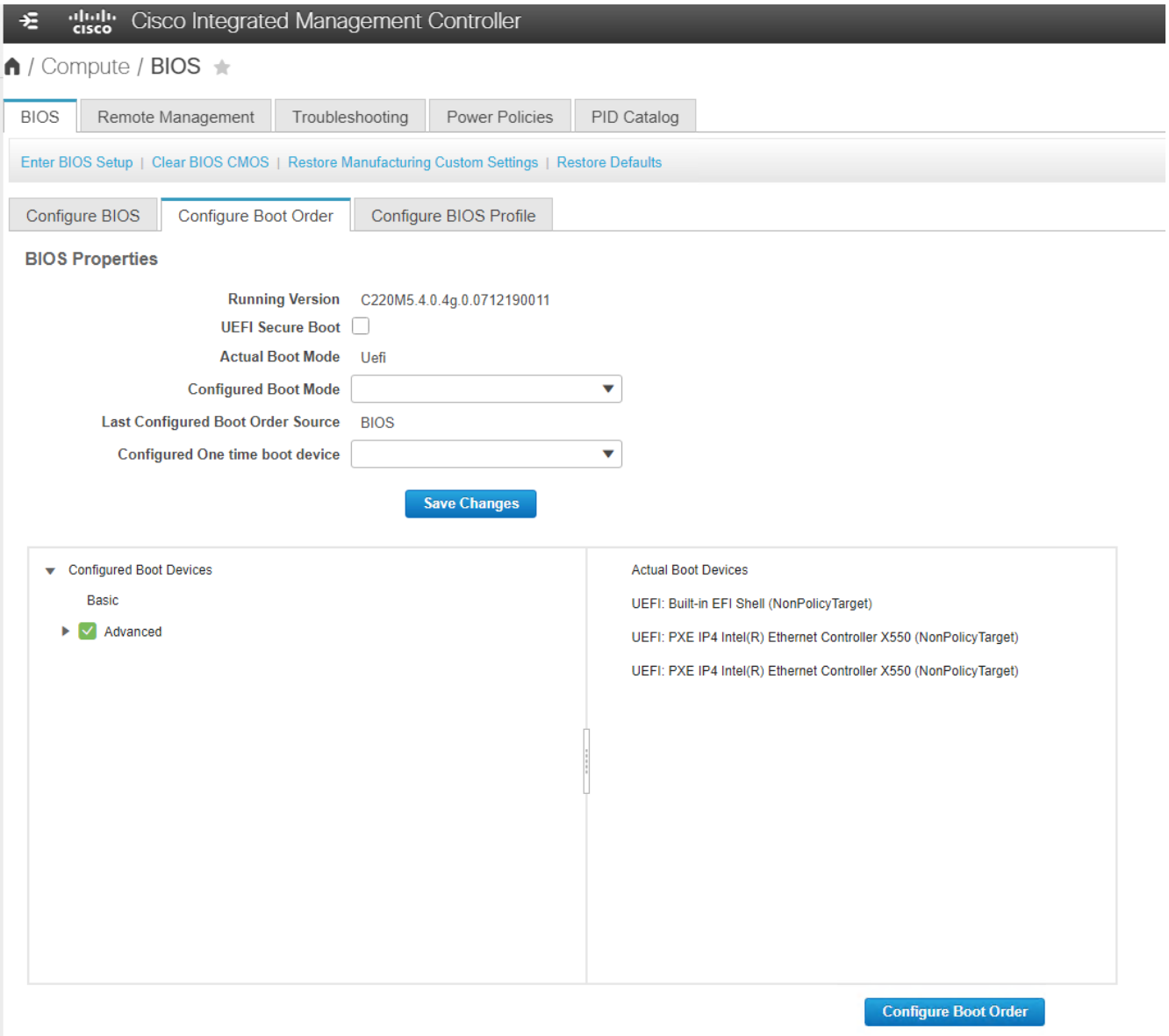
Eine kursiv formatierte Schriftart zeigt Variablen an, die für jeden ESXi-Host eindeutig sind.

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

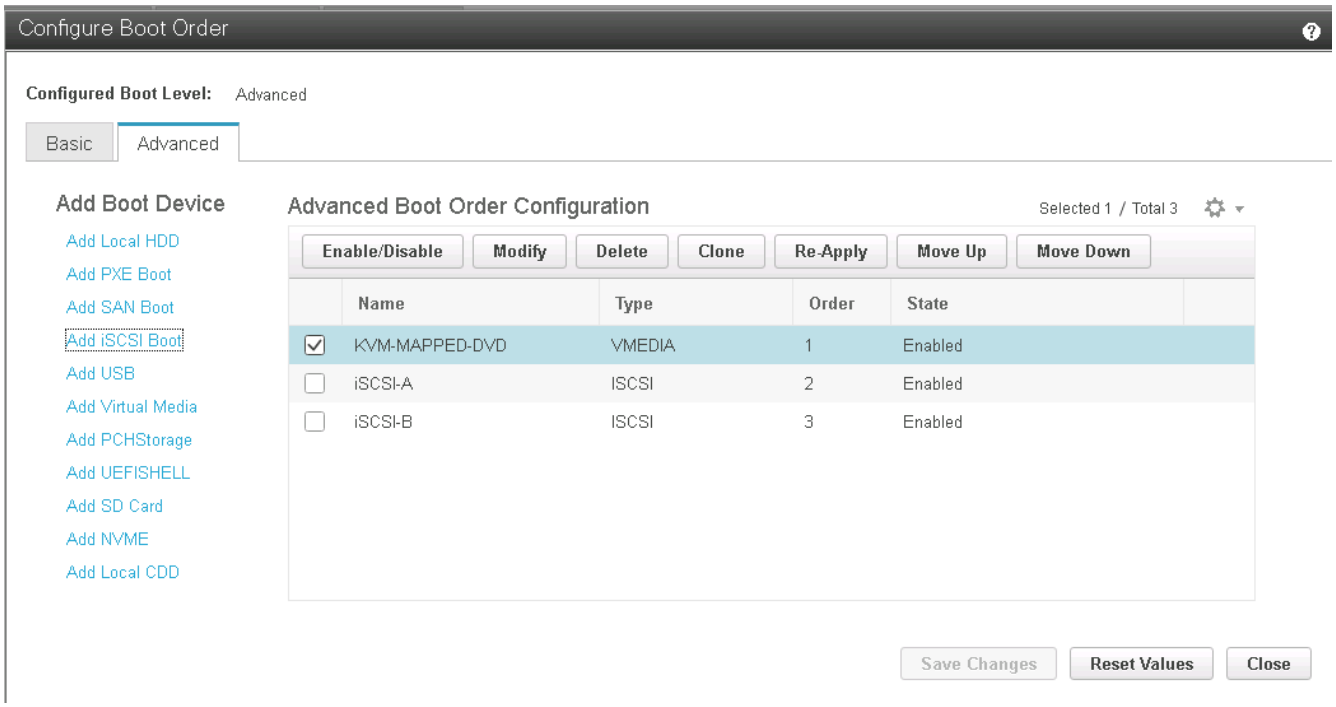
Status: Aktiviert

Bestellung: 3

Schlitz: MLOM

Anschluss: 3

4. Klicken Sie Auf Gerät Hinzufügen.
5. Klicken Sie auf Änderungen speichern und dann auf Schließen.

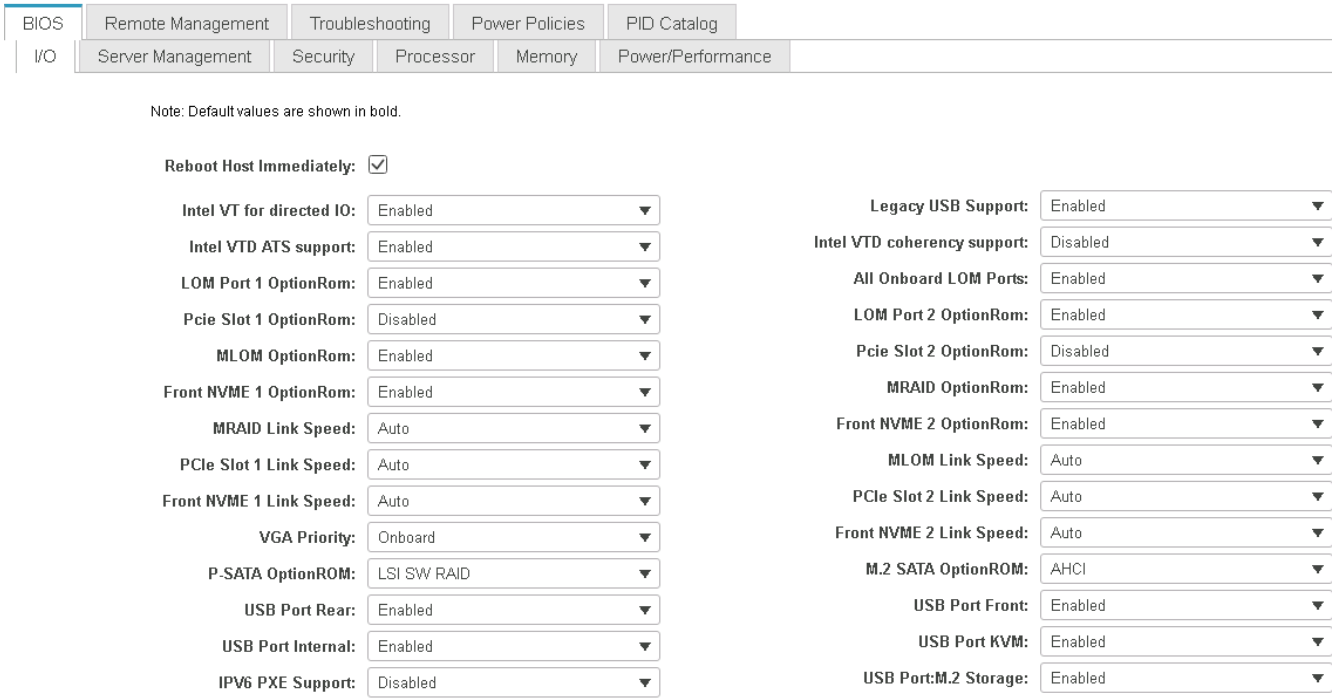


6. Starten Sie den Server neu, um mit Ihrer neuen Startreihenfolge zu starten.

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.

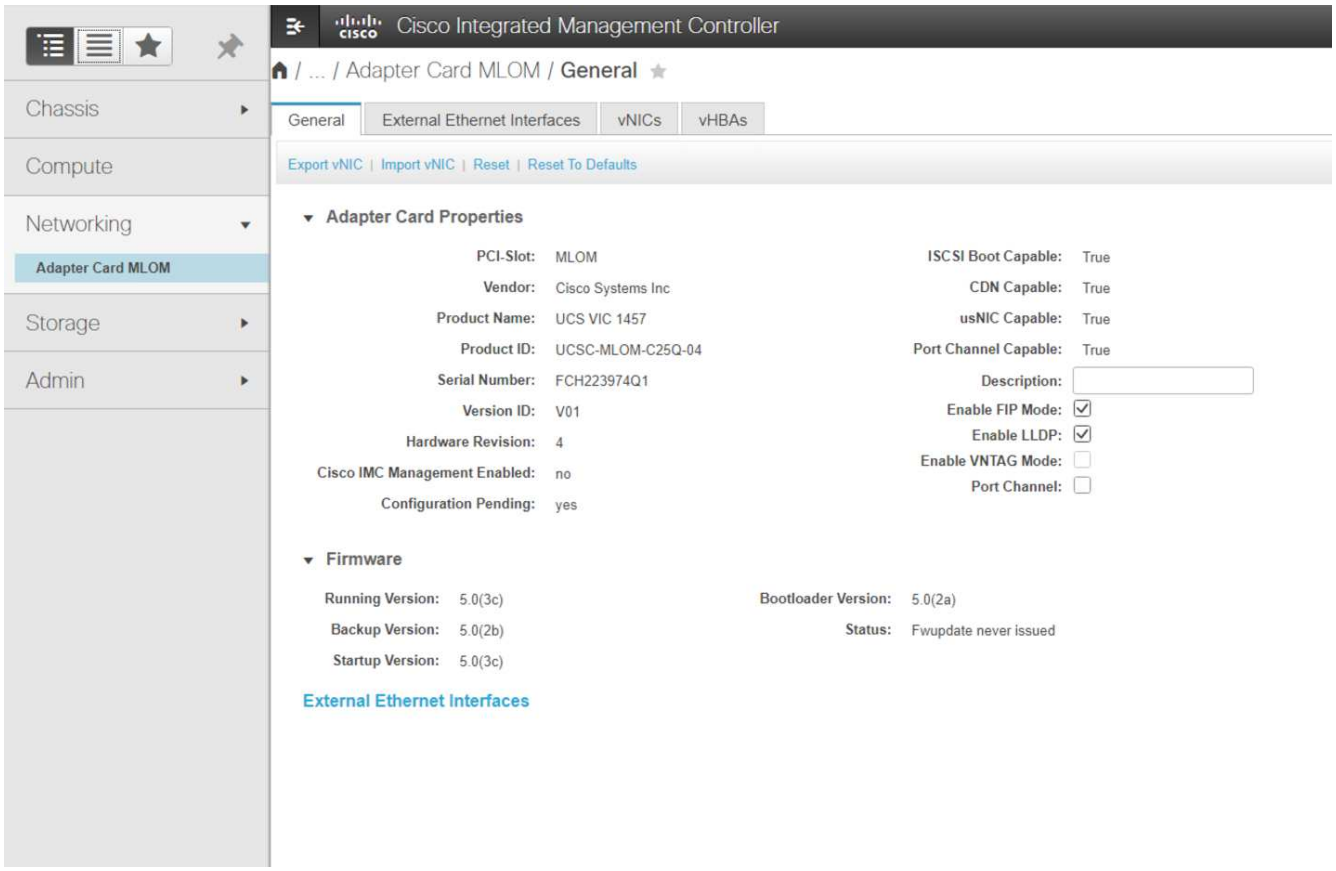


Konfigurieren Sie Cisco VIC1457 für iSCSI-Boot

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:

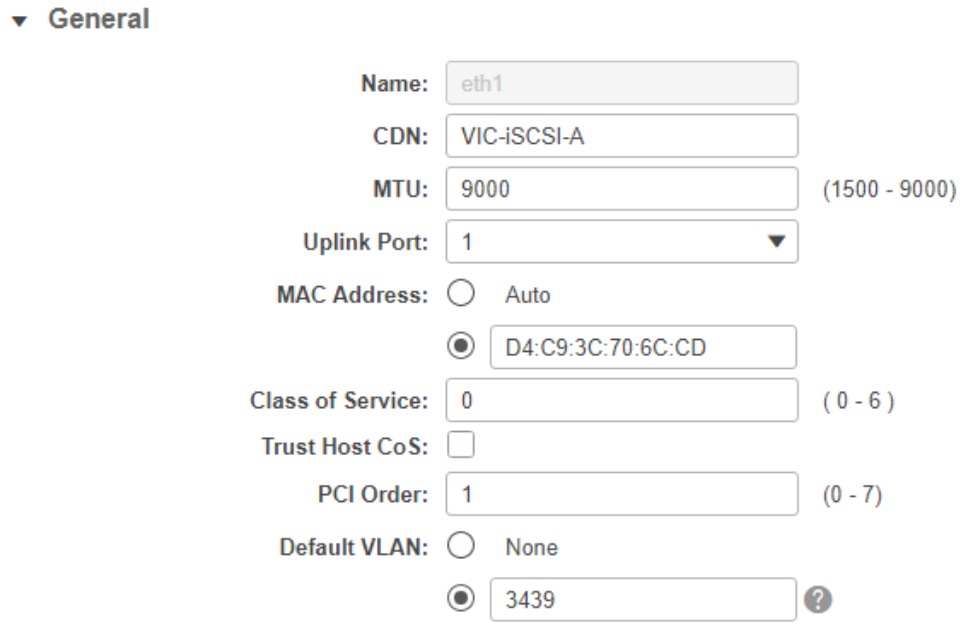
1. Klicken Sie auf der Registerkarte Netzwerk auf die Adapterkarte MLOM.
2. Deaktivieren Sie auf der Registerkarte Allgemein den Port-Kanal.
3. Speichern Sie die Änderungen, und starten Sie den CIMC neu.



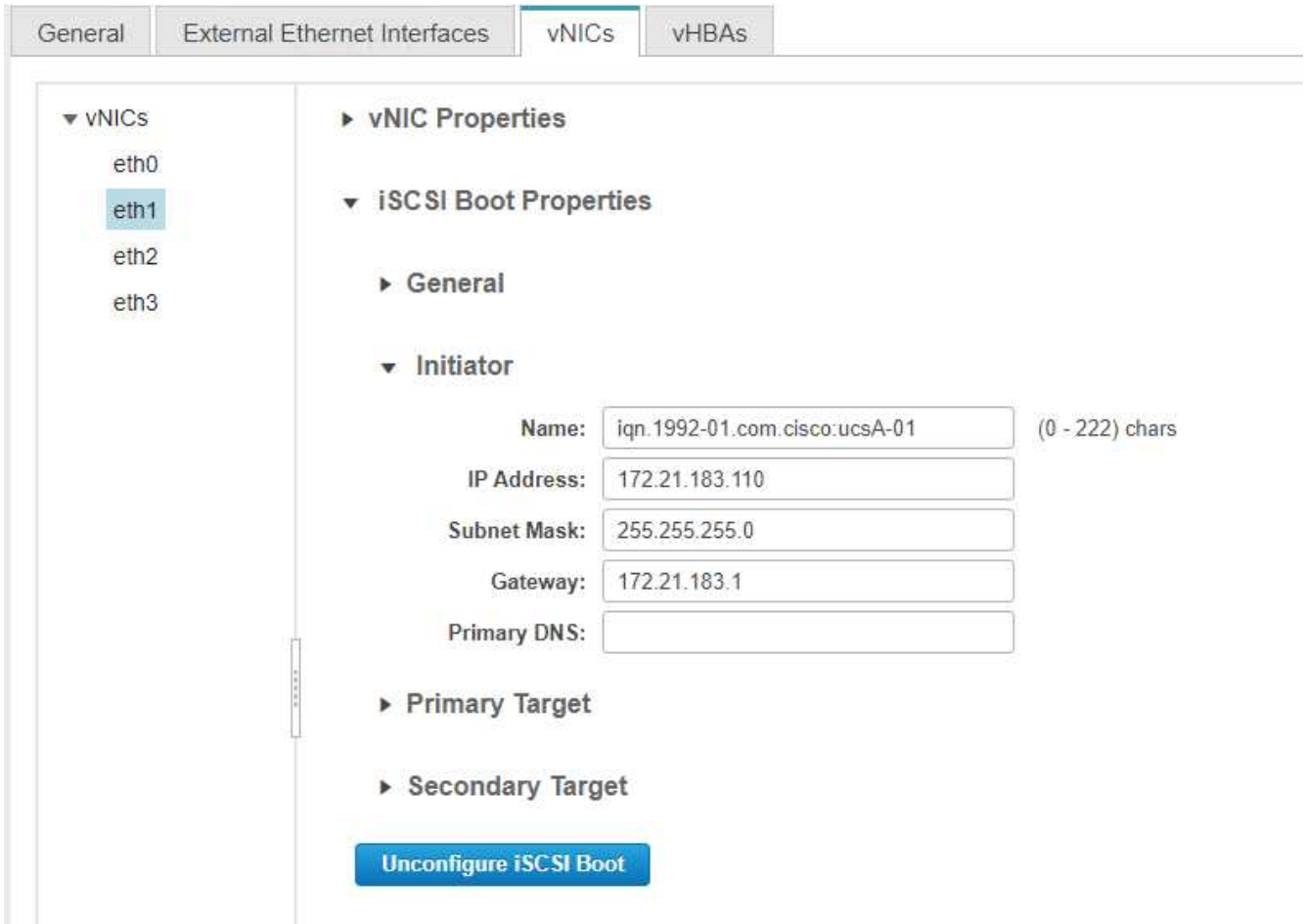
Erstellen von iSCSI-vNICs

Gehen Sie wie folgt vor, um iSCSI-vNICs zu erstellen:

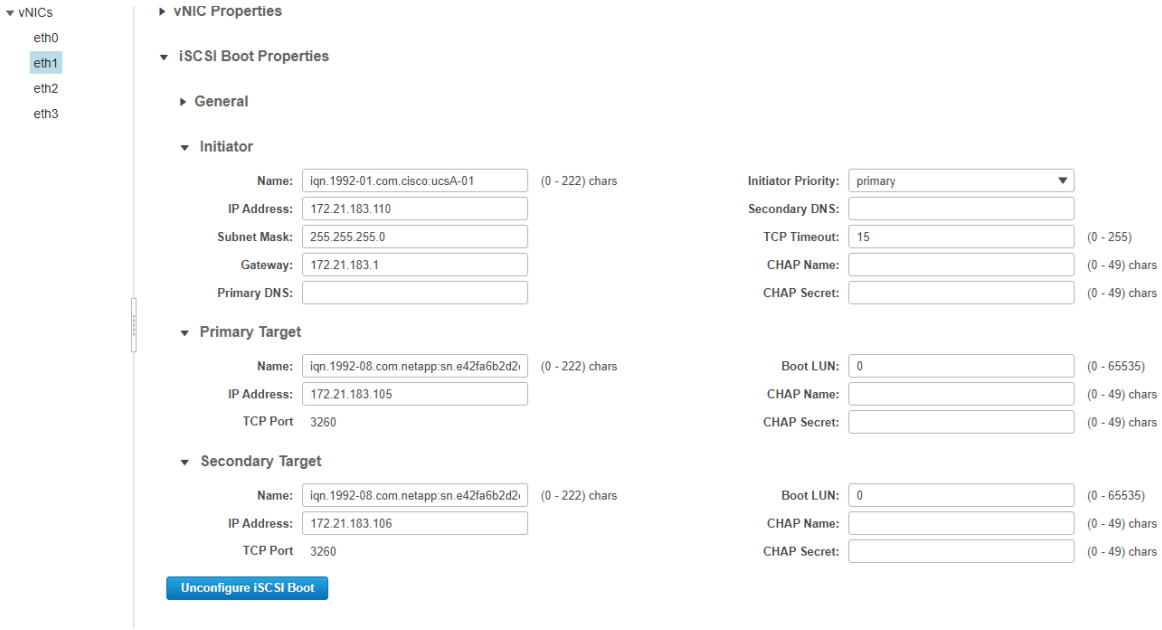
1. Klicken Sie auf der Registerkarte Netzwerk auf Adapterkarte MLOM.
2. Klicken Sie auf vNIC hinzufügen, um eine vNIC zu erstellen.
3. Geben Sie im Abschnitt vNIC hinzufügen die folgenden Einstellungen ein:
   - Name: Eth1
   - CDN-Name: ISCSI-vNIC-A
   - MTU: 9000
   - Standard-VLAN: `<<var_iscsi_vlan_a>>`
   - 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>>`



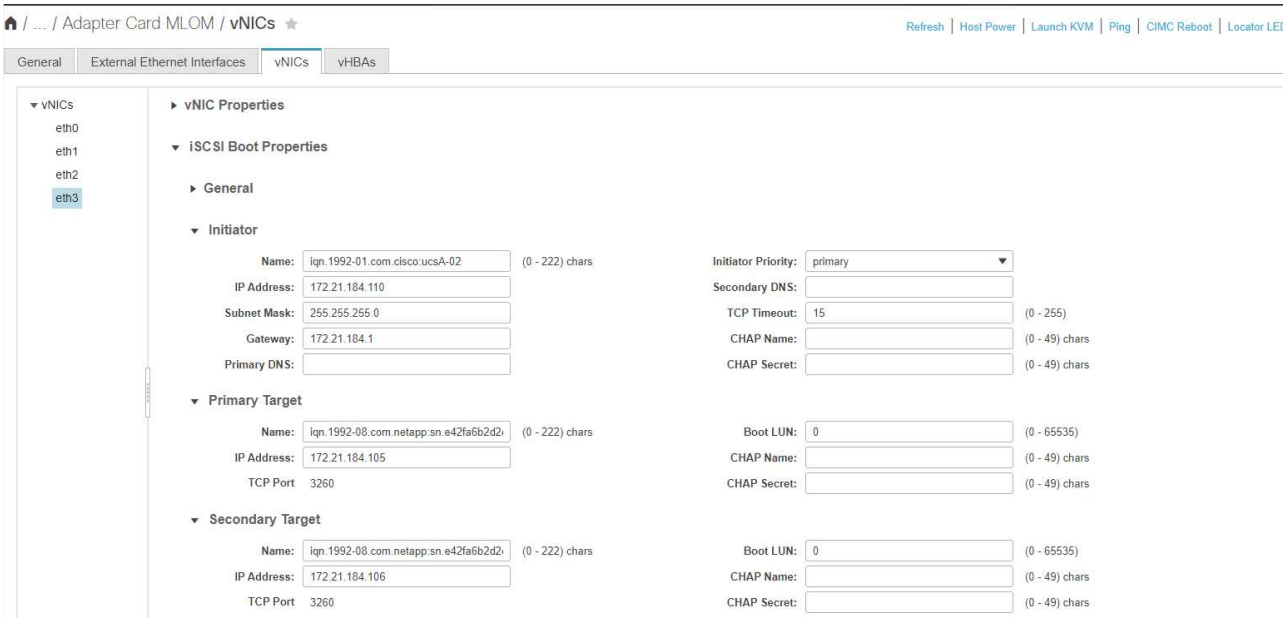
8. Geben Sie die Details des primären Ziels ein:
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von iscsi_lif01a
   - Boot-LUN: 0
9. Geben Sie die Details des sekundären Ziels ein:
   - Name: IQN-Nummer der Infrastruktur-SVM
   - IP-Adresse: IP-Adresse von iscsi_lif02a
   - Boot-LUN:0

> 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.

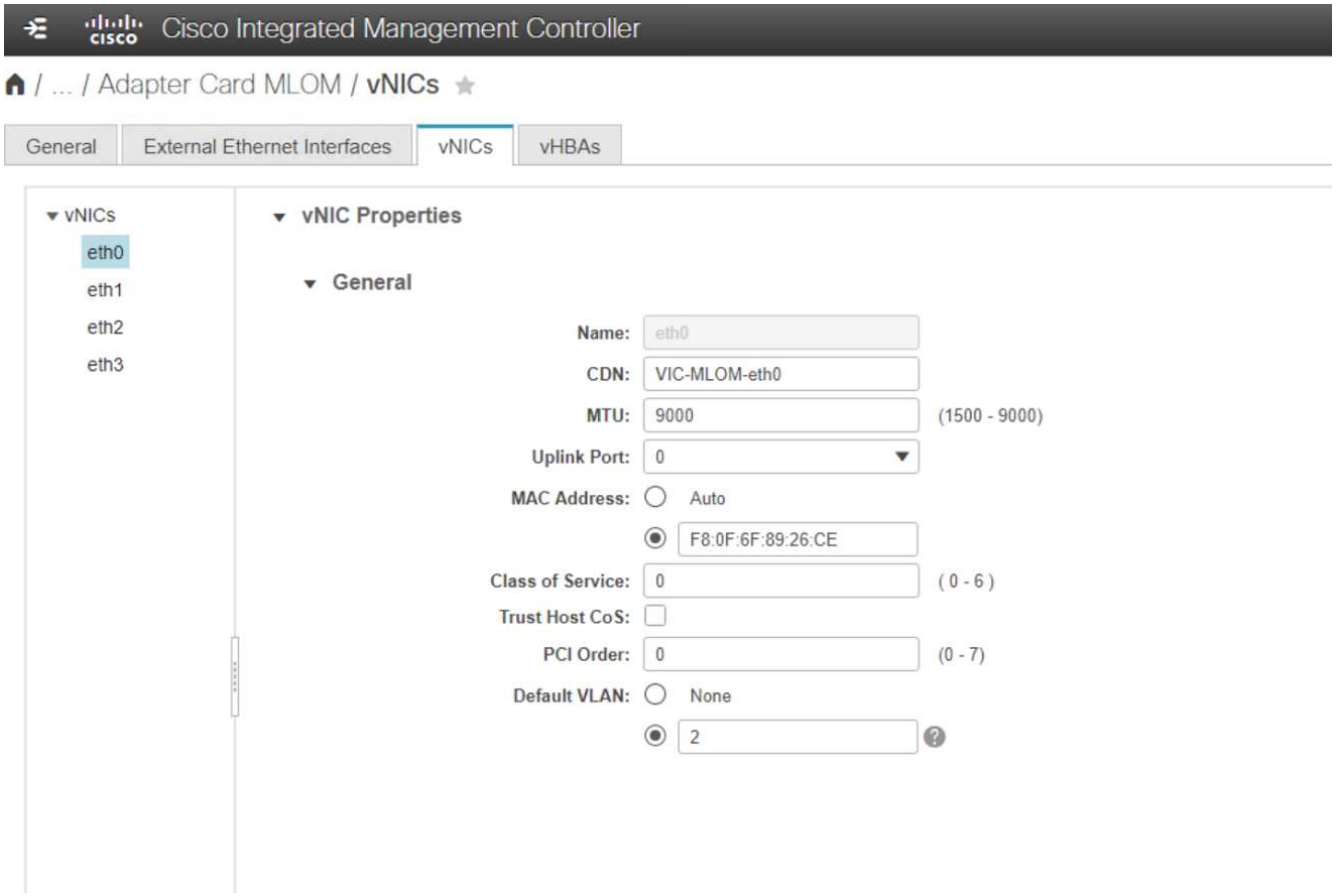
> Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.

16. Klicken Sie Auf Änderungen Speichern.
17. Wiederholen Sie diesen Vorgang, um iSCSI-Boot für Cisco UCS-Server B zu konfigurieren

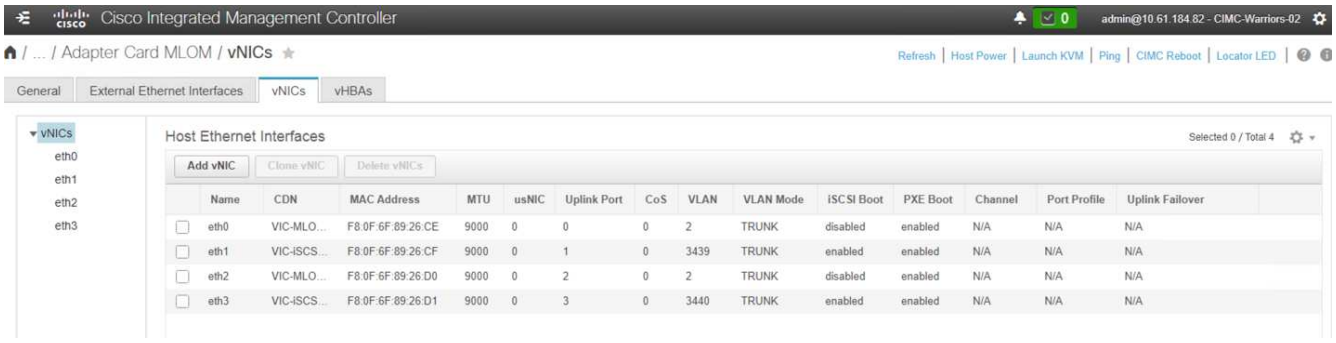
Konfigurieren Sie vNICs für ESXi

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.

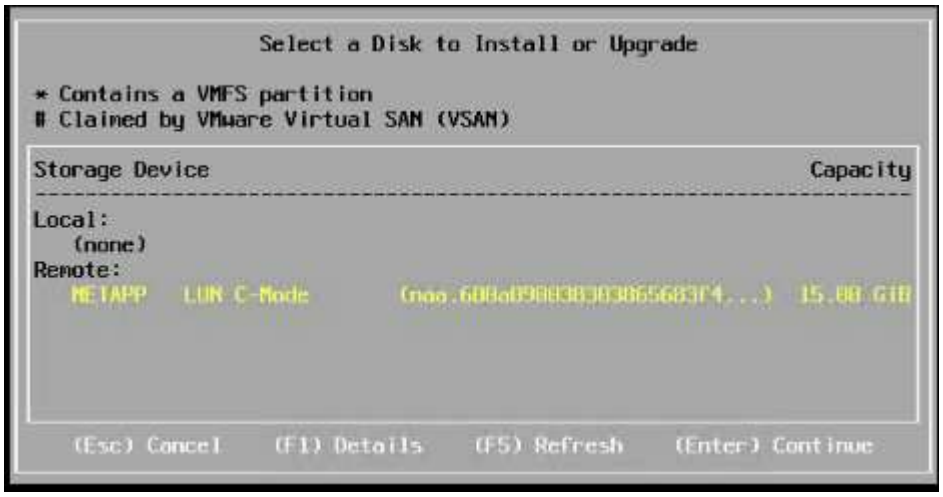
VMware ESXi installieren

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.



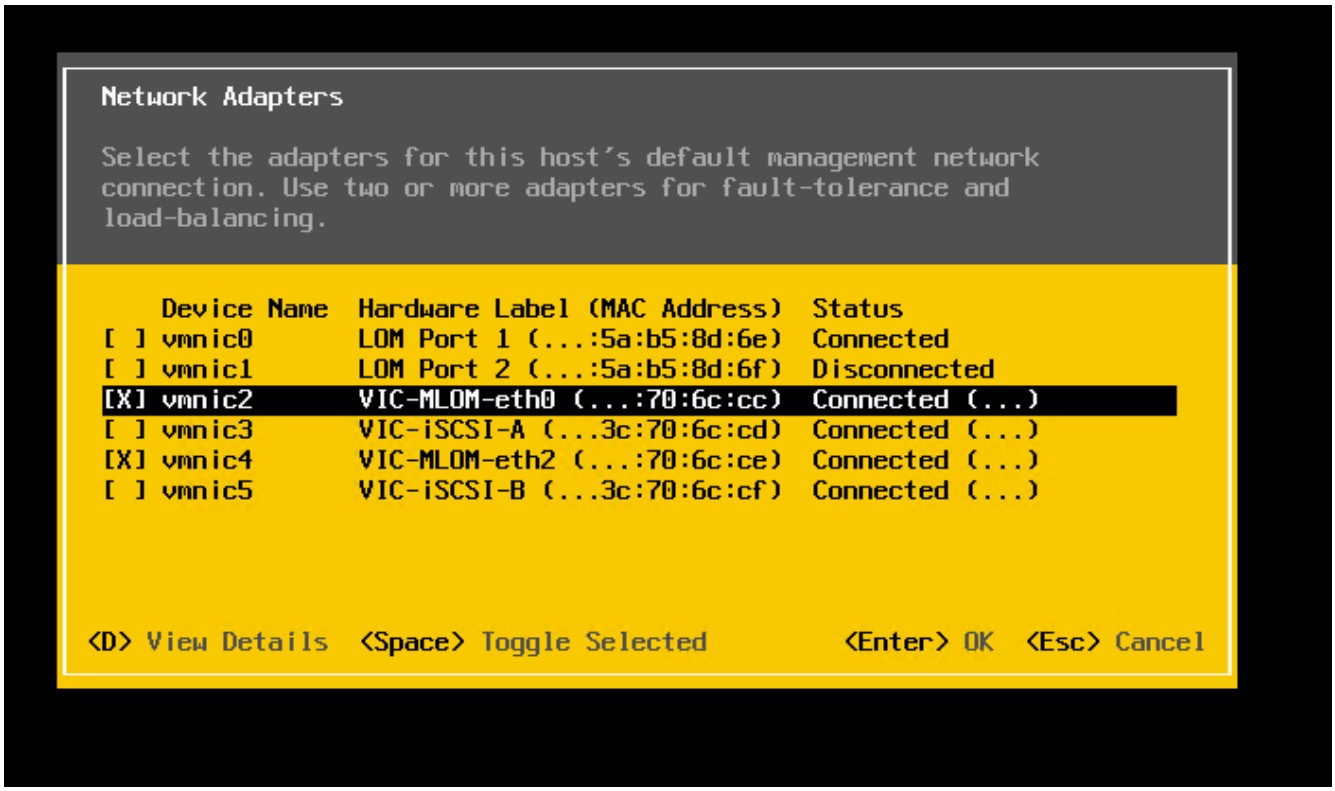
9. Wählen Sie das entsprechende Tastaturlayout aus, und drücken Sie die Eingabetaste.
10. Geben Sie das Root-Passwort ein und bestätigen Sie es, und drücken Sie die Eingabetaste.
11. Der Installer warnt Sie, dass vorhandene Partitionen auf dem Volume entfernt werden. Fahren Sie mit der Installation fort, 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.

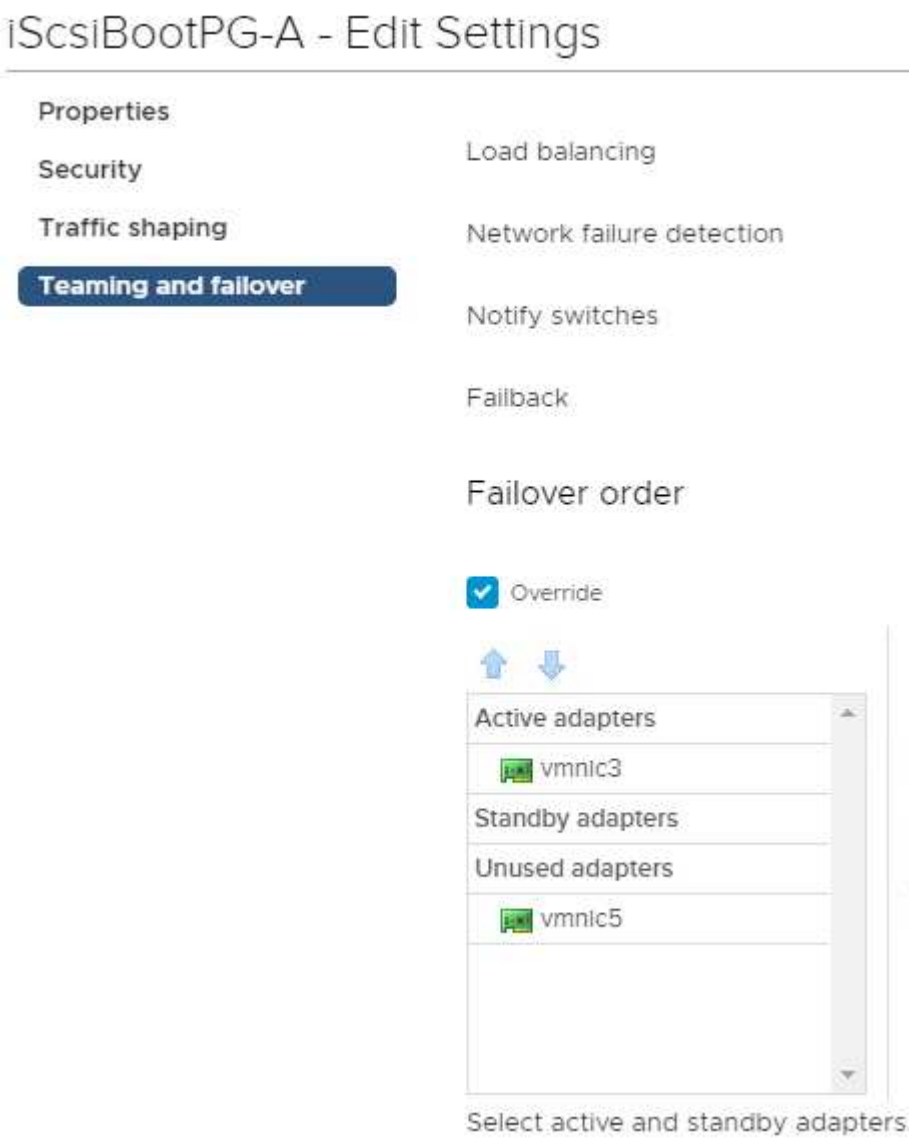
i. Klicken Sie auf Erstellen .

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.

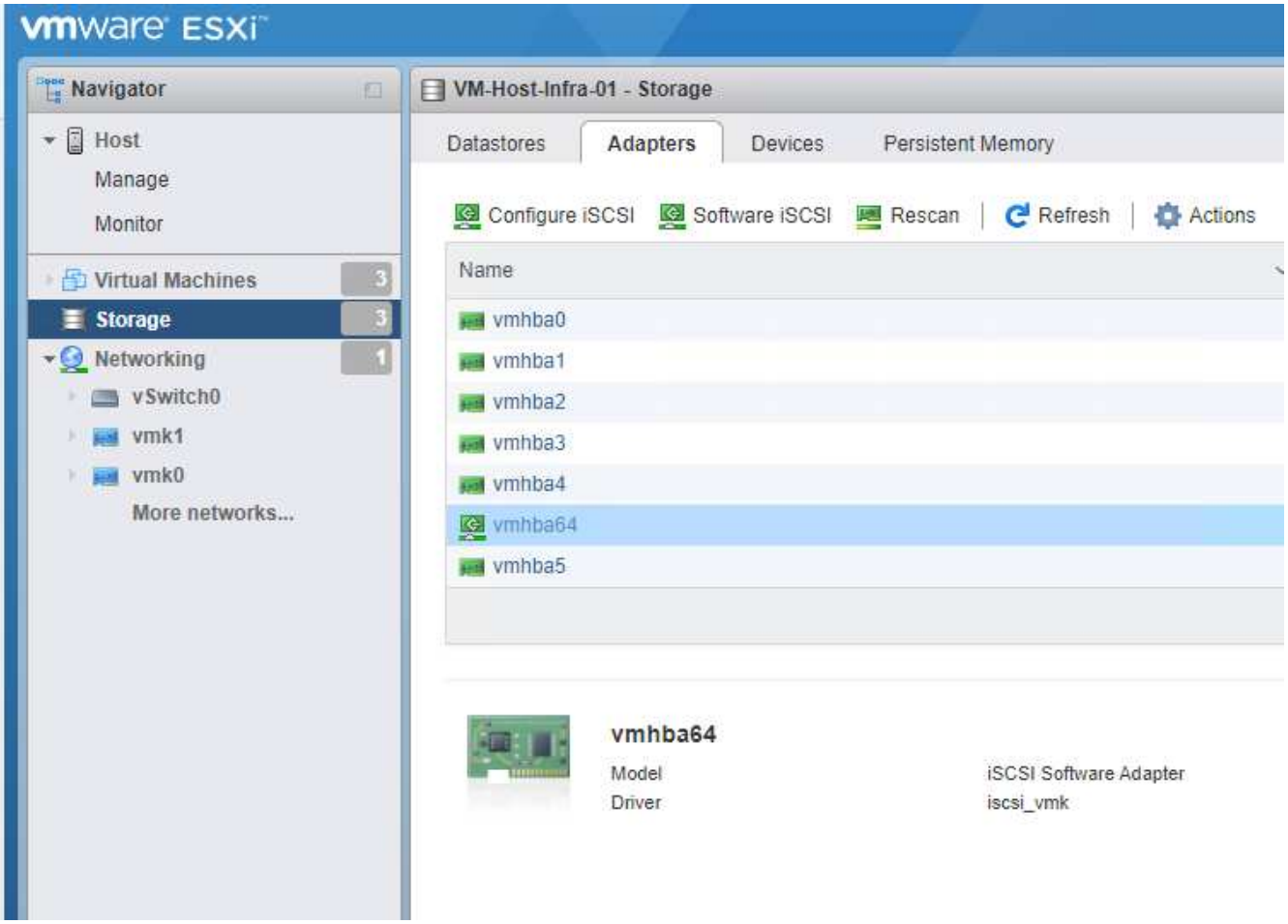
b. Klicken Sie auf Einstellungen bearbeiten auf iSCSIBootPG-B > Teaming und Failover > Failover-Reihenfolge > Vmnic5. Vmnic5 sollte aktiv sein und vmnic3 sollte nicht verwendet werden.



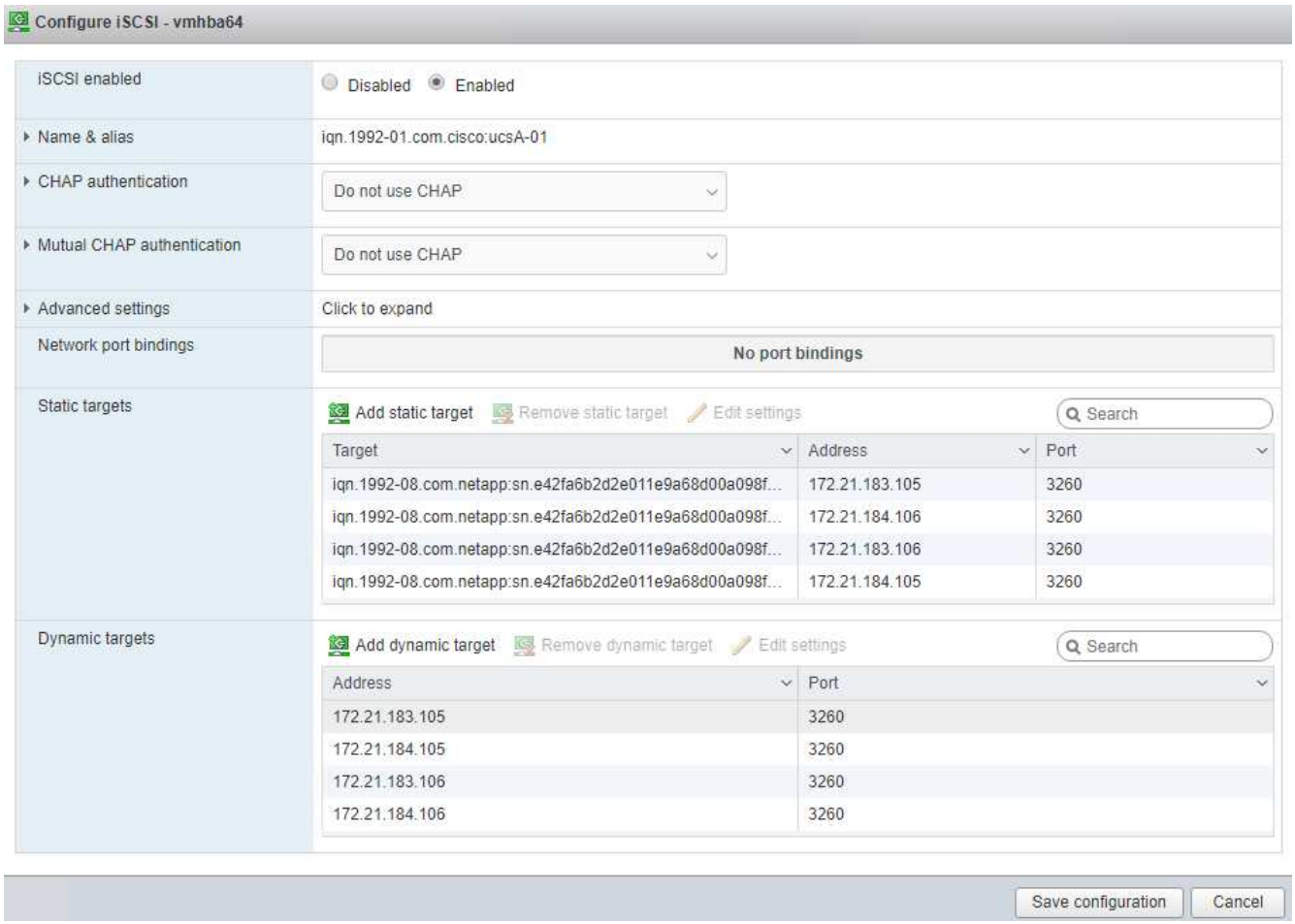
Konfigurieren Sie iSCSI-Multipathing

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.



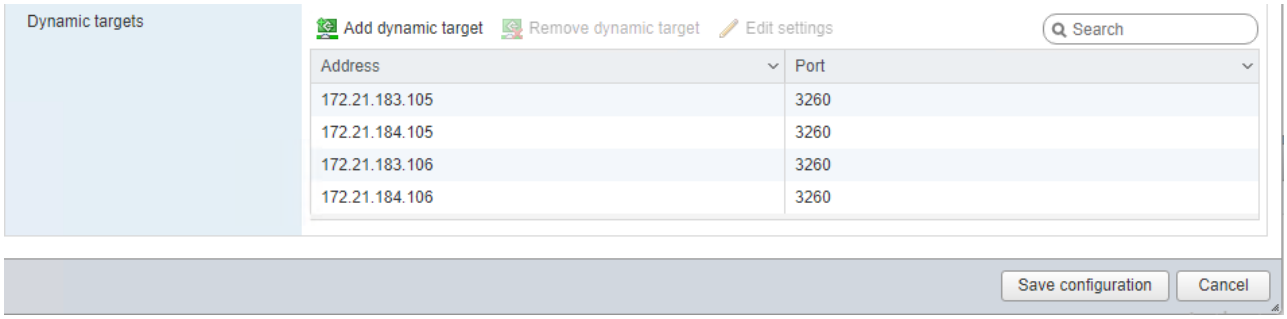
3. Klicken Sie unter dynamische Ziele auf dynamische Ziele hinzufügen.



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.

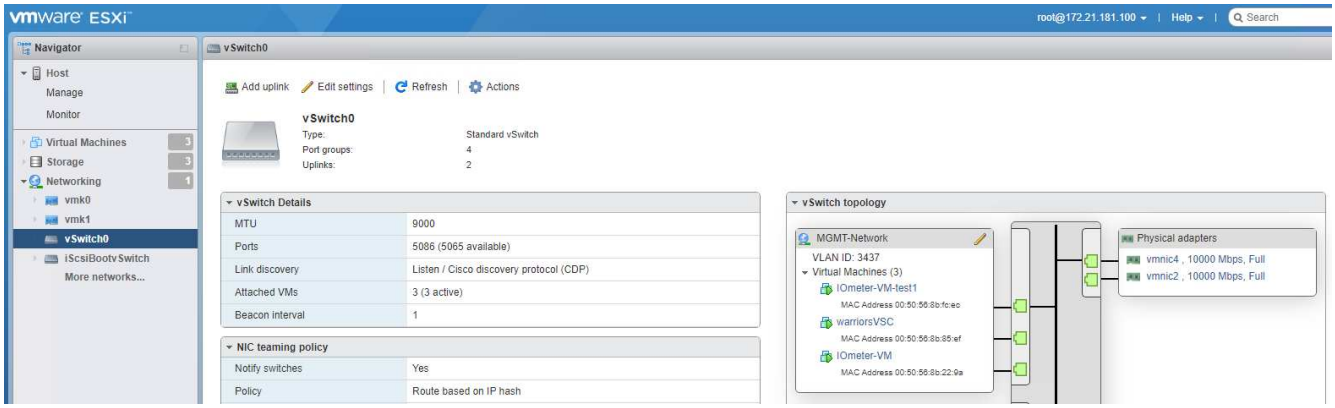


Sie können die iSCSI LIF IP-Adressen finden, indem Sie den Befehl show der Netzwerkschnittstelle auf dem NetApp Cluster ausführen oder sich in System Manager auf der Registerkarte Netzwerkschnittstellen ansehen.

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.

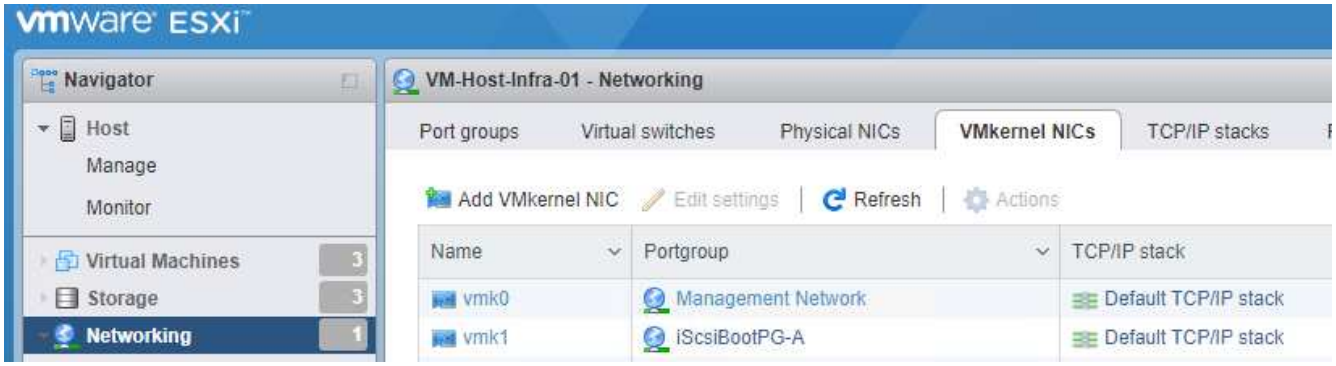
> Für die IP-Hash-Methode zum Lastausgleich muss der zugrunde liegende physische Switch mithilfe von SRC-DST-IP EtherChannel mit einem statischen (Mode- ein) Port-Kanal ordnungsgemäß konfiguriert werden. Aufgrund einer möglichen Switch-Fehlkonfiguration ist die Konnektivität möglicherweise zeitweise 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.

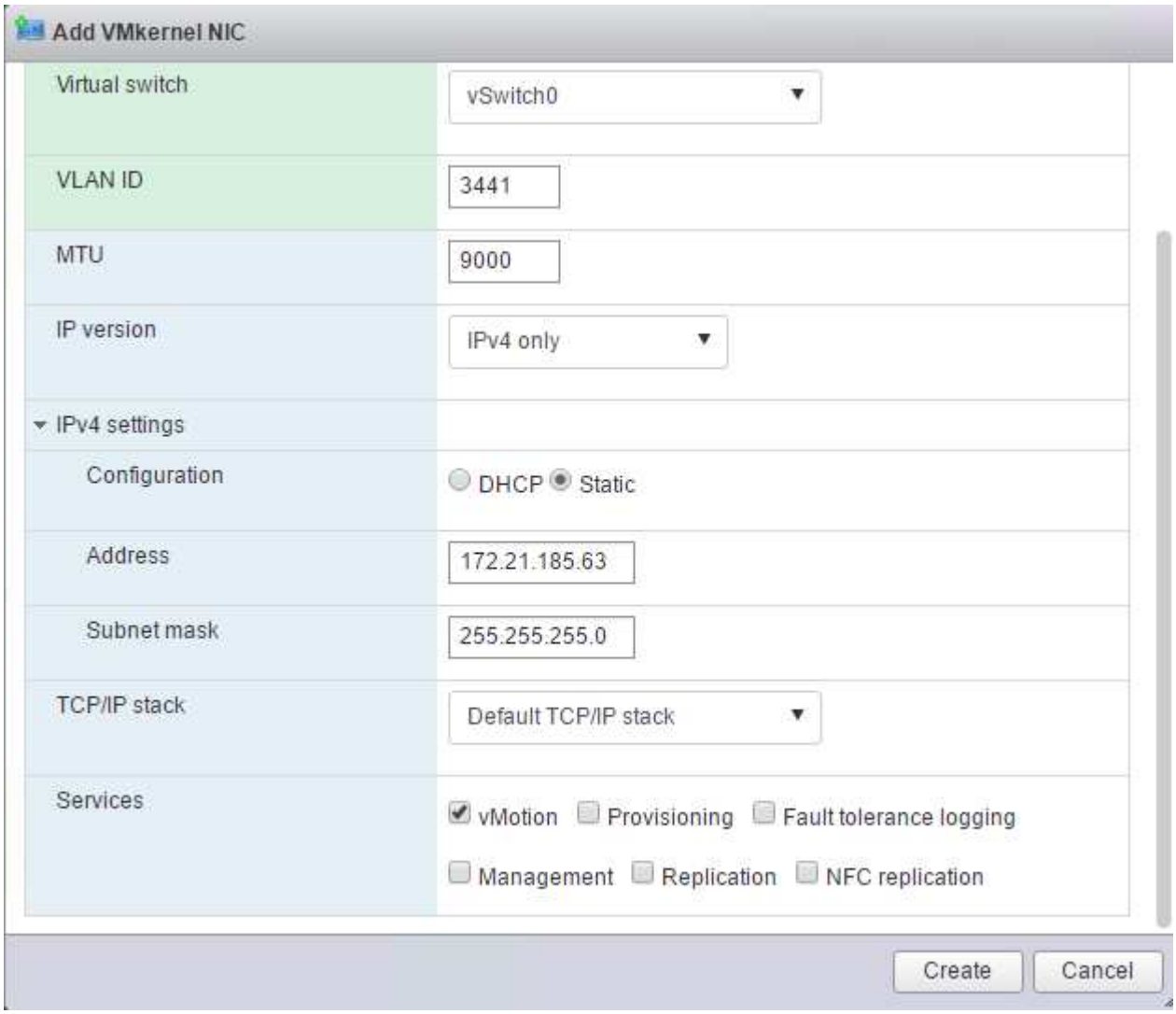
e. IPv4-Einstellungen erweitern.

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.

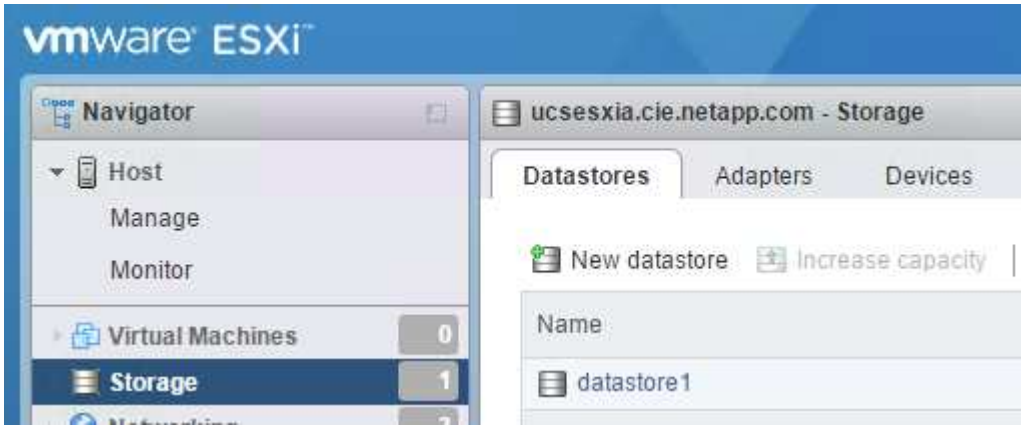


Es gibt viele Möglichkeiten, ESXi Networking zu konfigurieren, einschließlich der Verwendung des VMware vSphere Distributed Switches, wenn Ihre Lizenzierung es zulässt. In FlexPod Express werden alternative Netzwerkkonfigurationen unterstützt, wenn sie zur Erfüllung der geschäftlichen Anforderungen erforderlich sind.

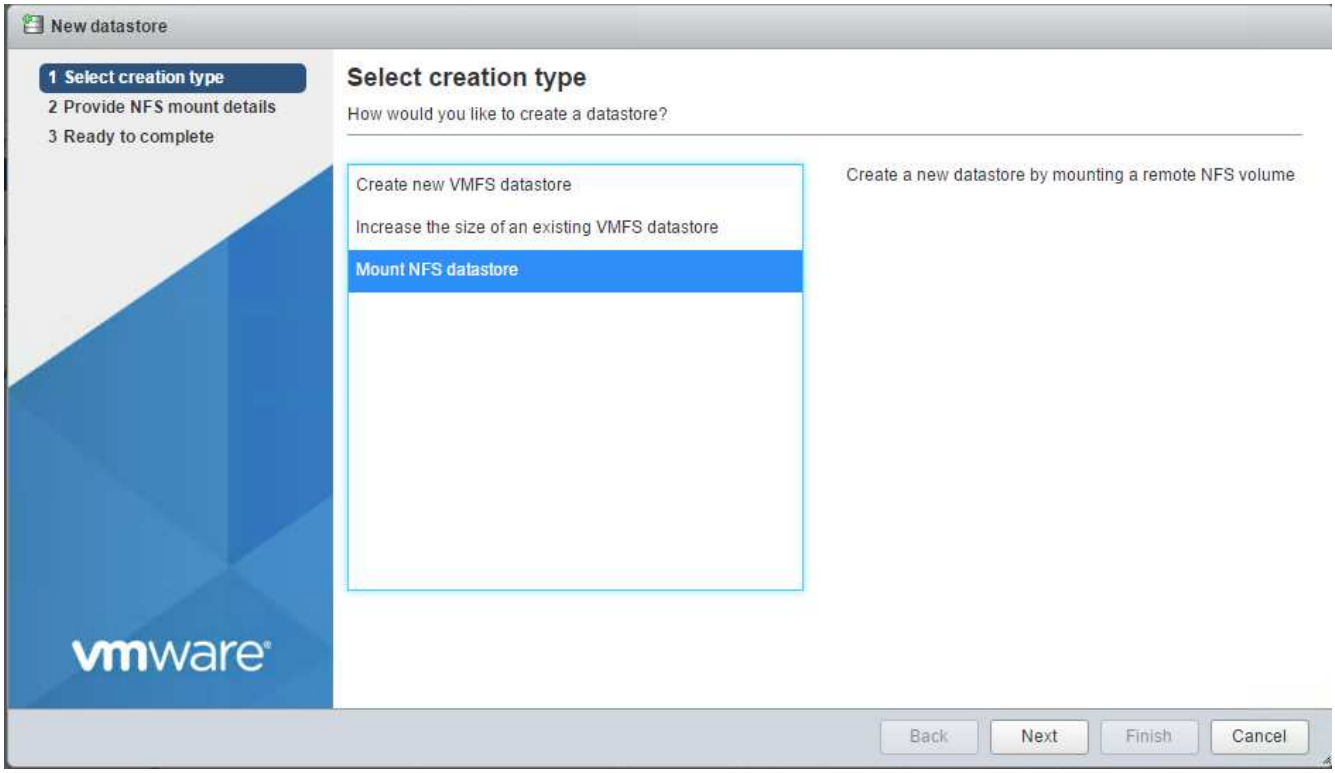
Montieren Sie die ersten Datenspeicher

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`

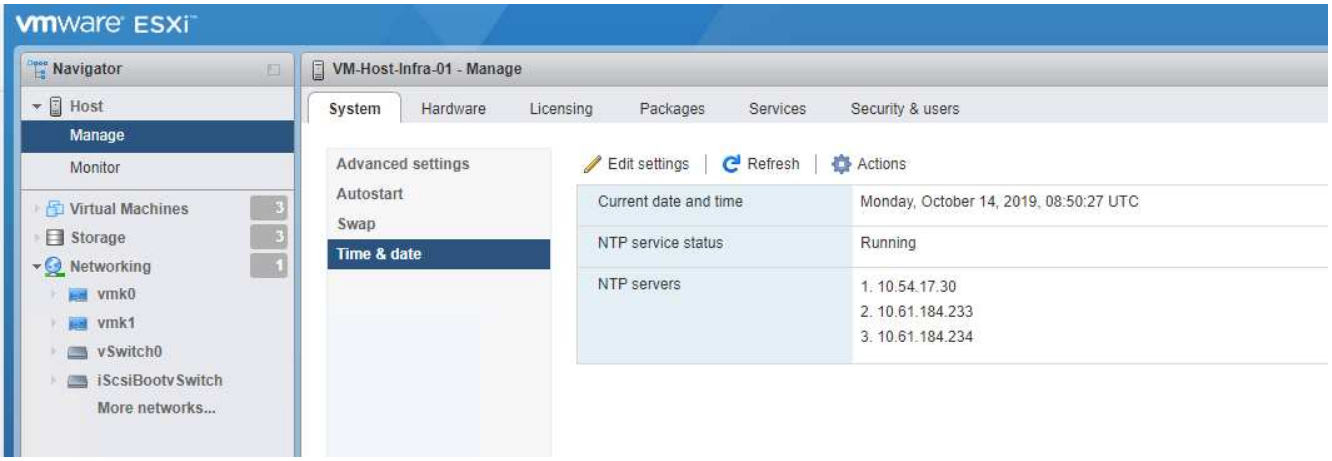
- NFS-Server: `<<var_nodea_nfs_lif>>`
- Weitersagen: `/infra_datastore`
- Stellen Sie sicher, dass NFS 3 ausgewählt ist.

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:

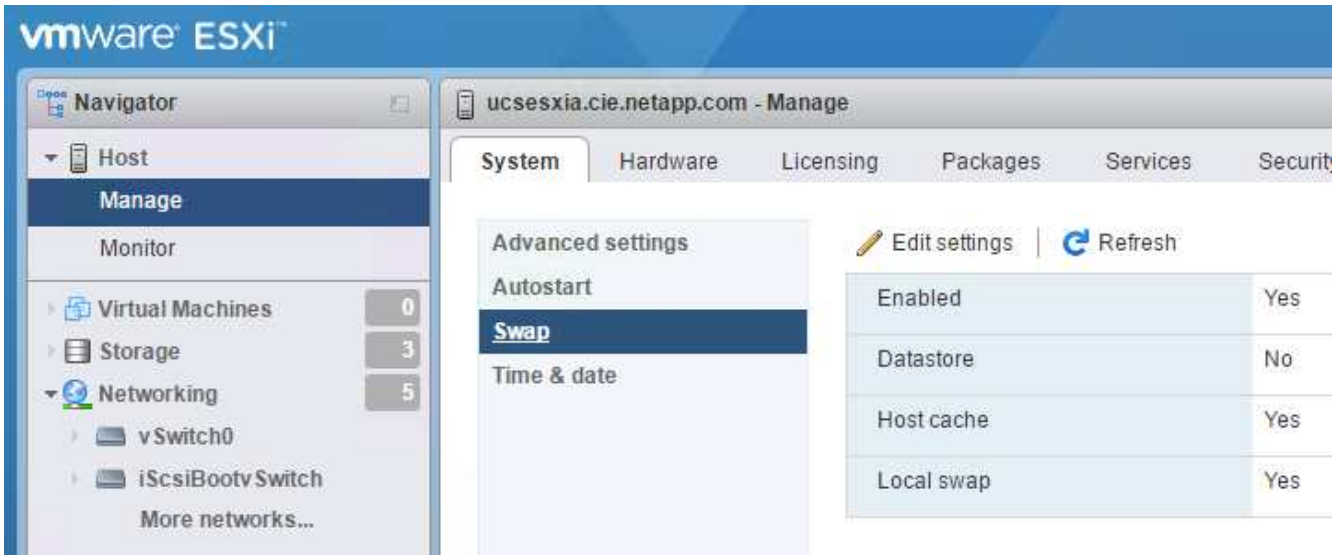
1. Klicken Sie im linken Navigationsbereich auf Verwalten. Wählen Sie im rechten Fensterbereich System aus, und klicken Sie anschließend auf Zeit und Datum.
2. Wählen Sie Network Time Protocol (Network Time Protocol verwenden) (NTP Client aktivieren) aus.
3. Wählen Sie Start und Stopp mit Host als Startrichtlinie 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.

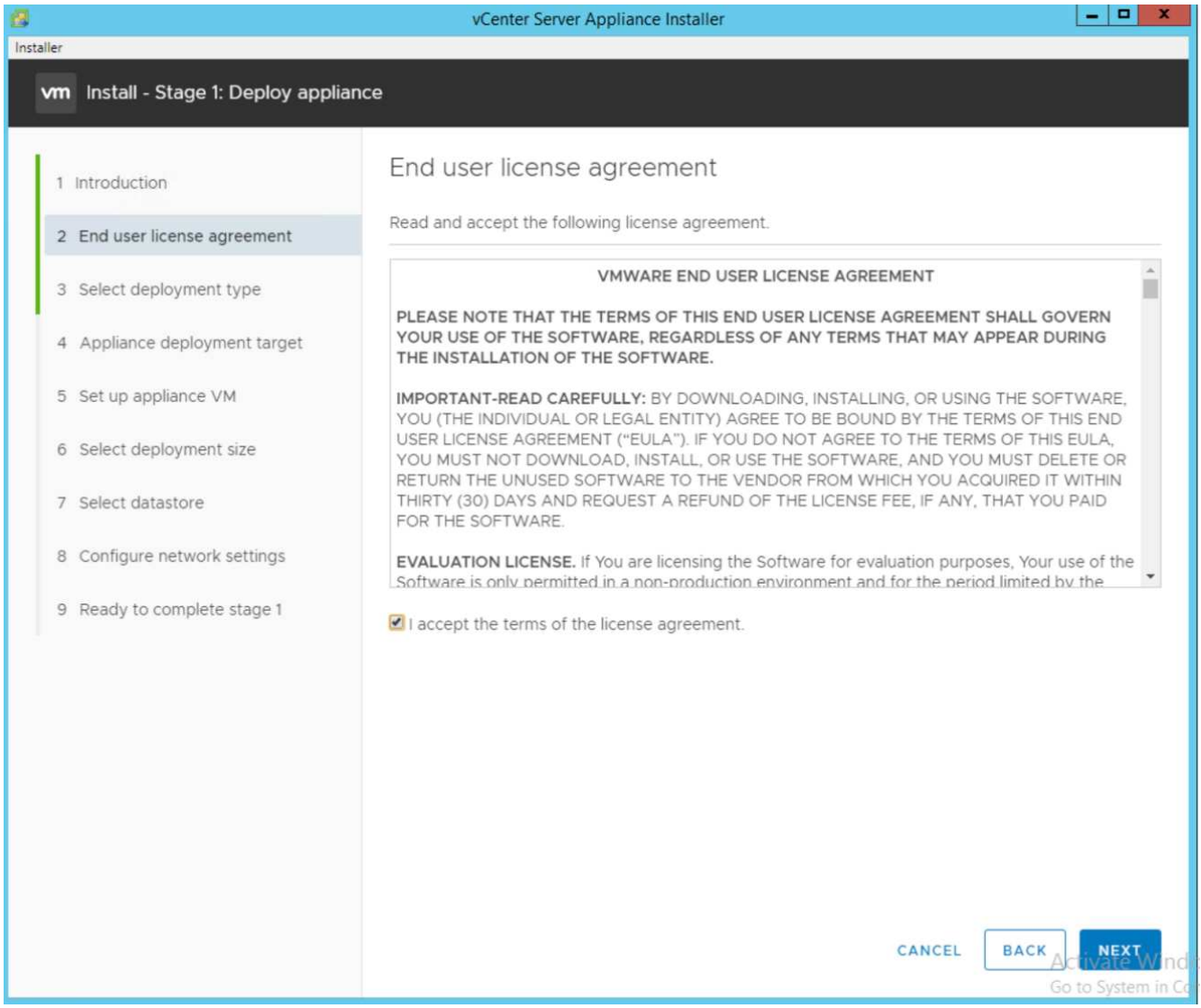
FlexPod Express verwendet die VMware vCenter Server Appliance (VCSA).

Laden Sie die VMware vCenter Server Appliance herunter

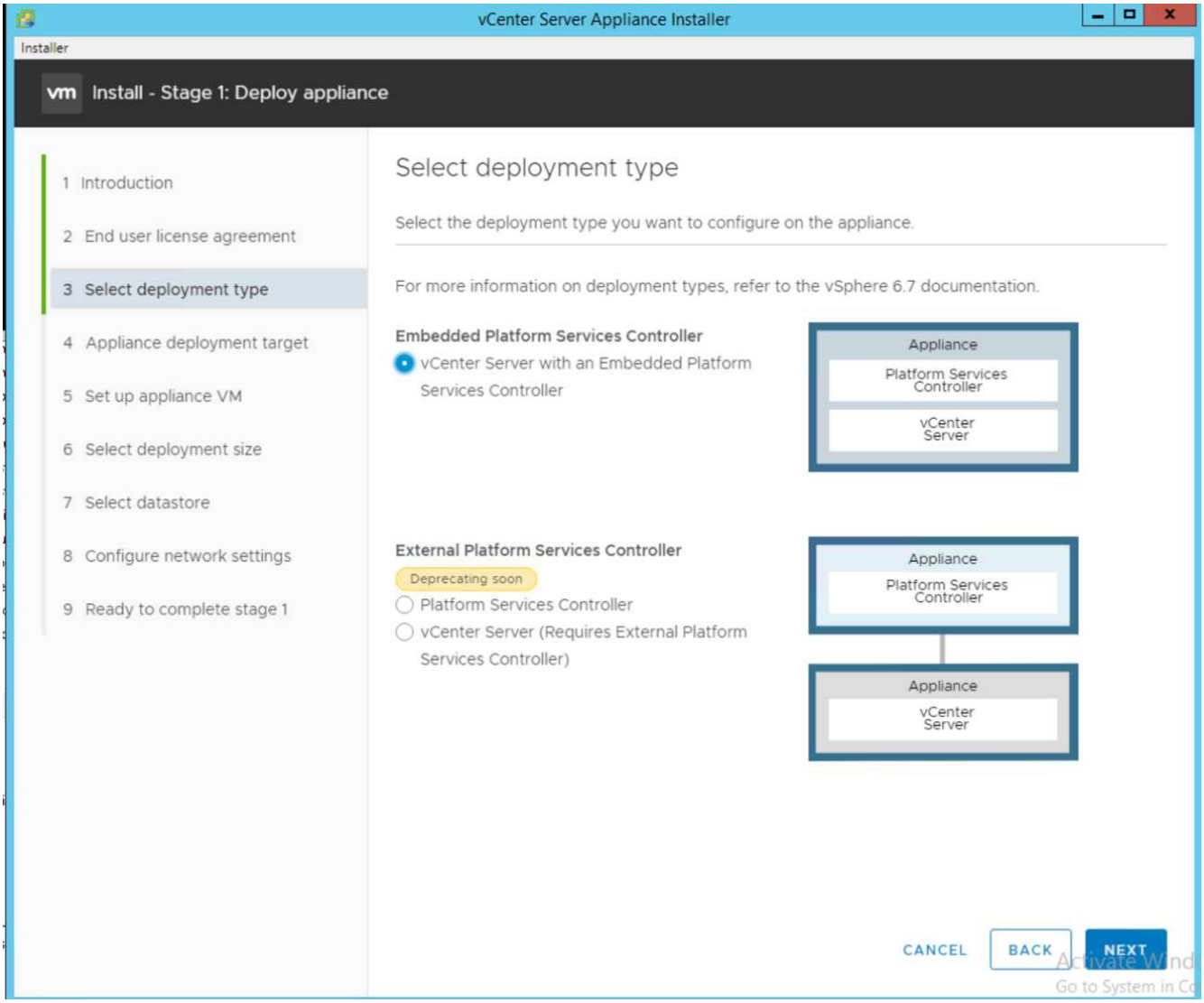
So laden Sie die VMware vCenter Server Appliance (VCSA) herunter:

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.

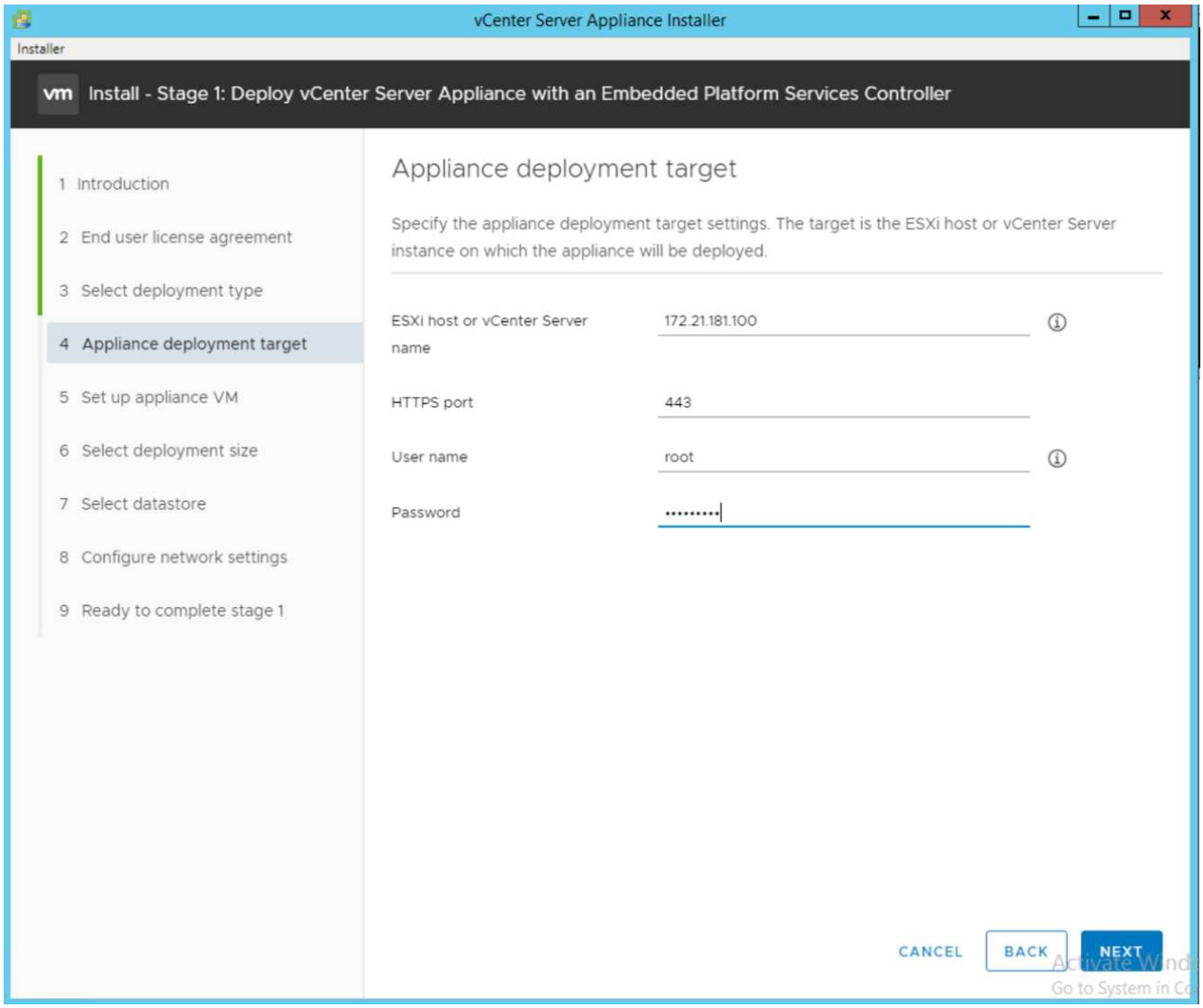


8. Wählen Sie als Bereitstellungstyp den Embedded Platform Services Controller aus.

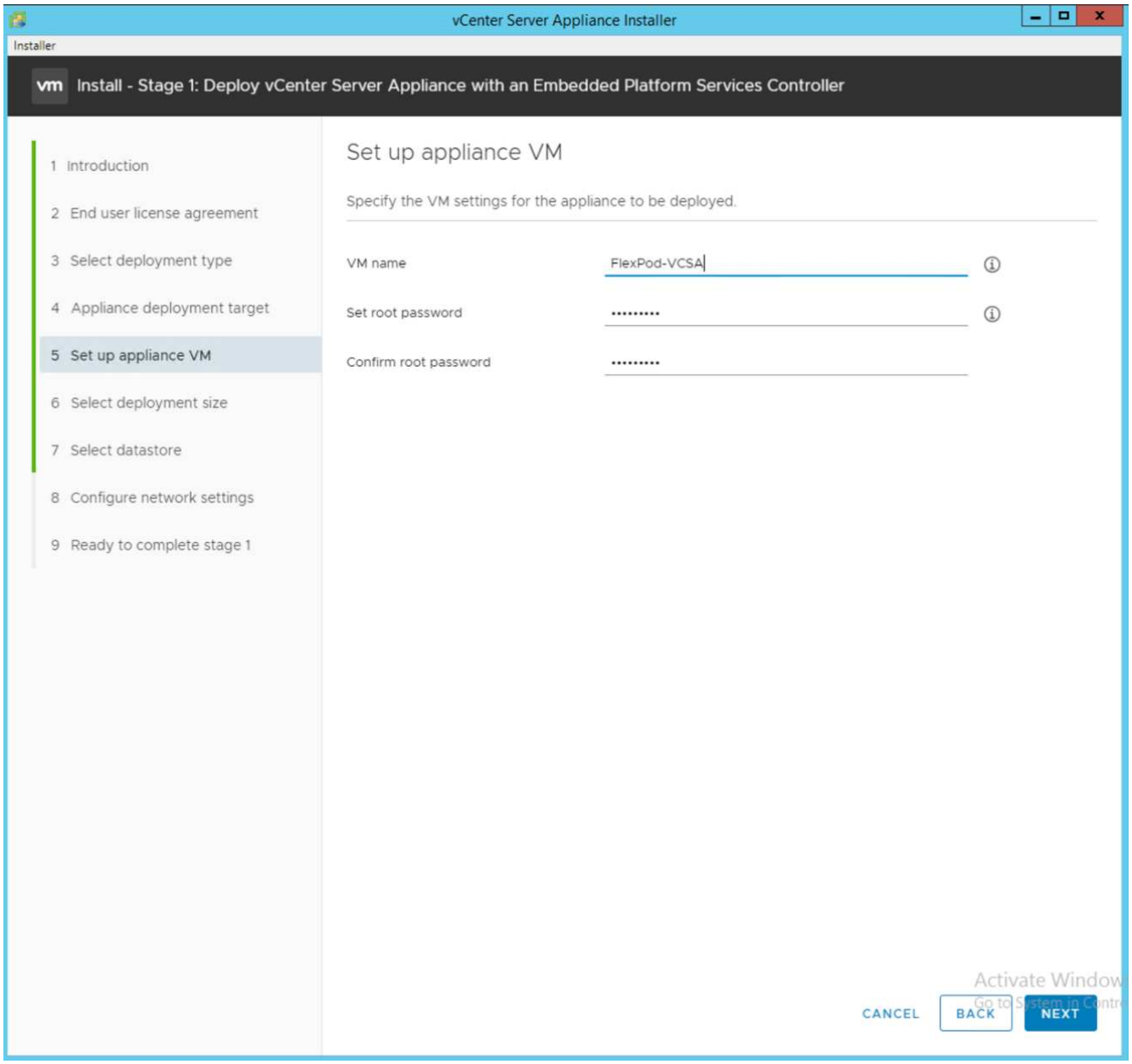


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

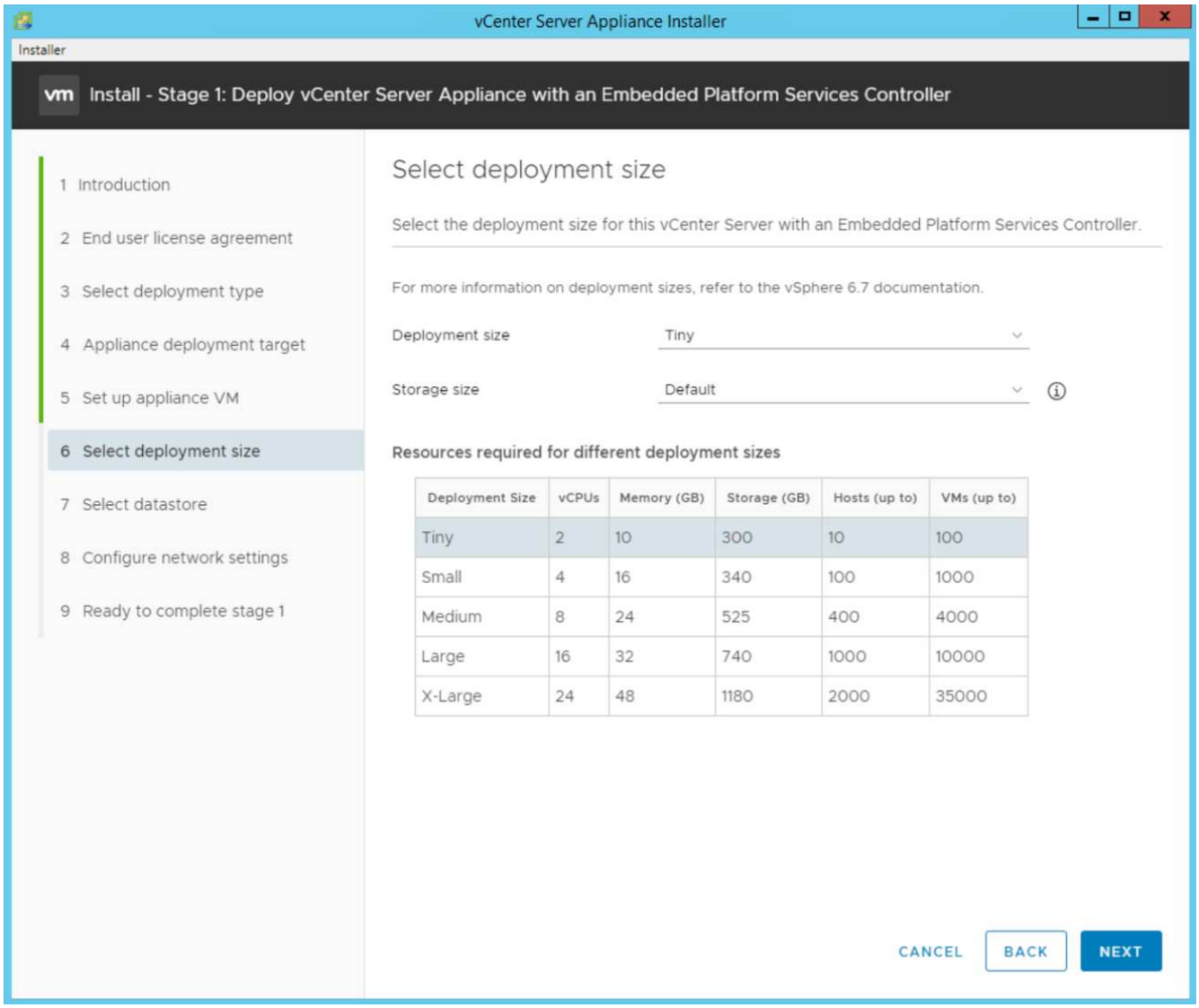
9. Geben Sie im Appliance Deployment Target die IP-Adresse eines bereitgestelltem ESXi-Hosts, den Root-Benutzernamen und das Root-Passwort ein.



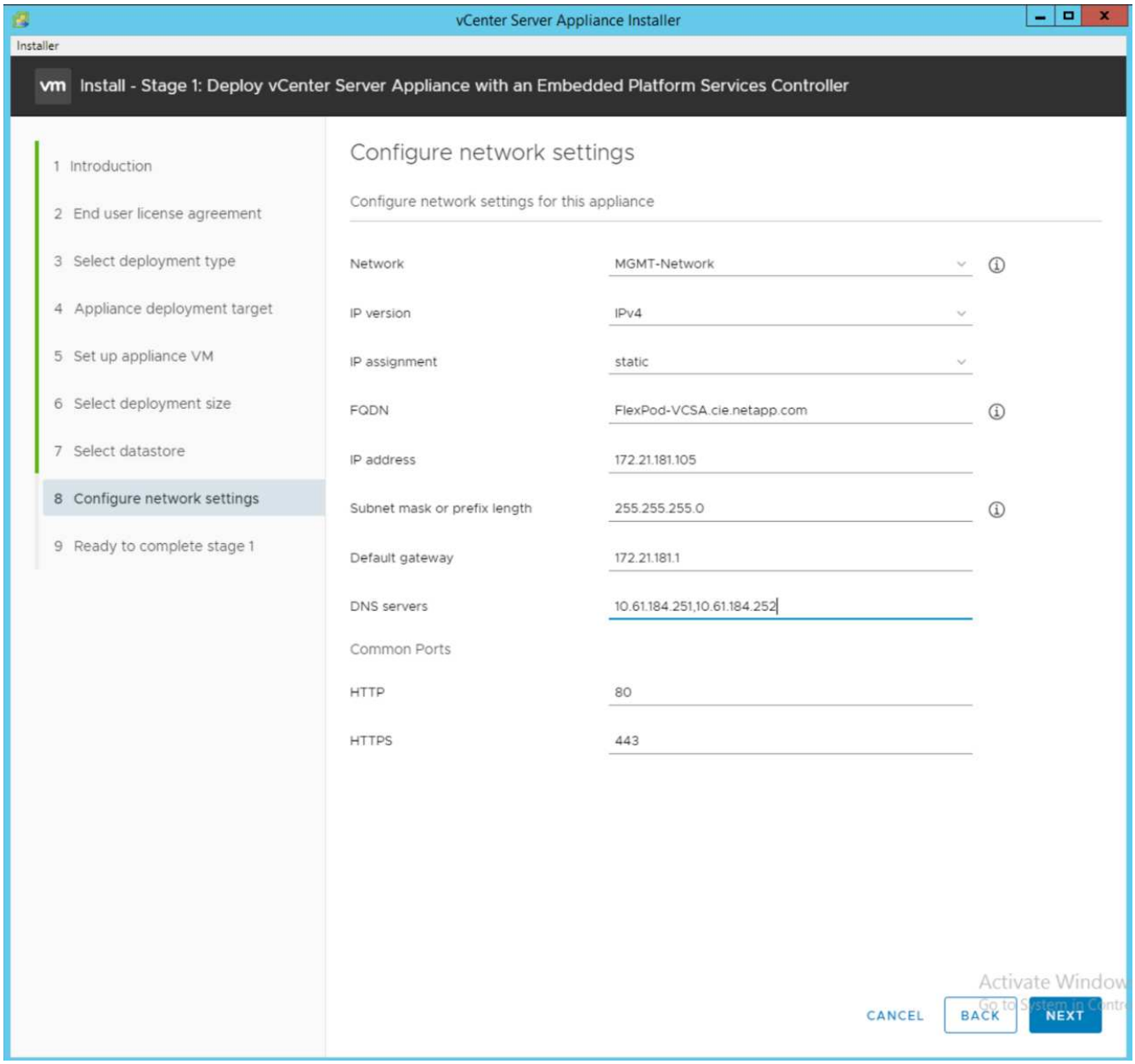
10. Legen Sie die Appliance-VM fest, indem Sie VCSA als VM-Name und das Root-Passwort eingeben, das Sie für VCSA verwenden möchten.



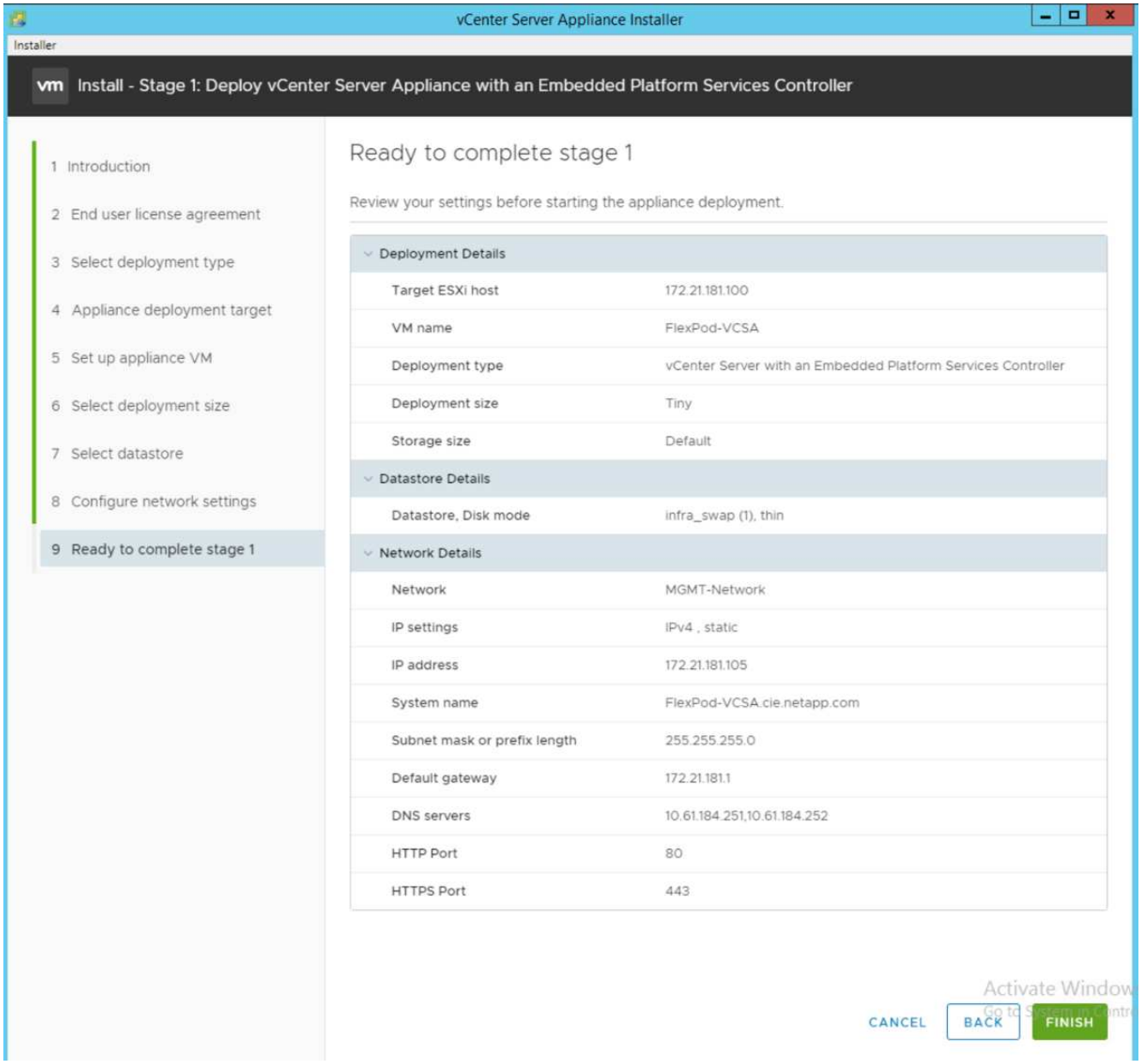
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



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.

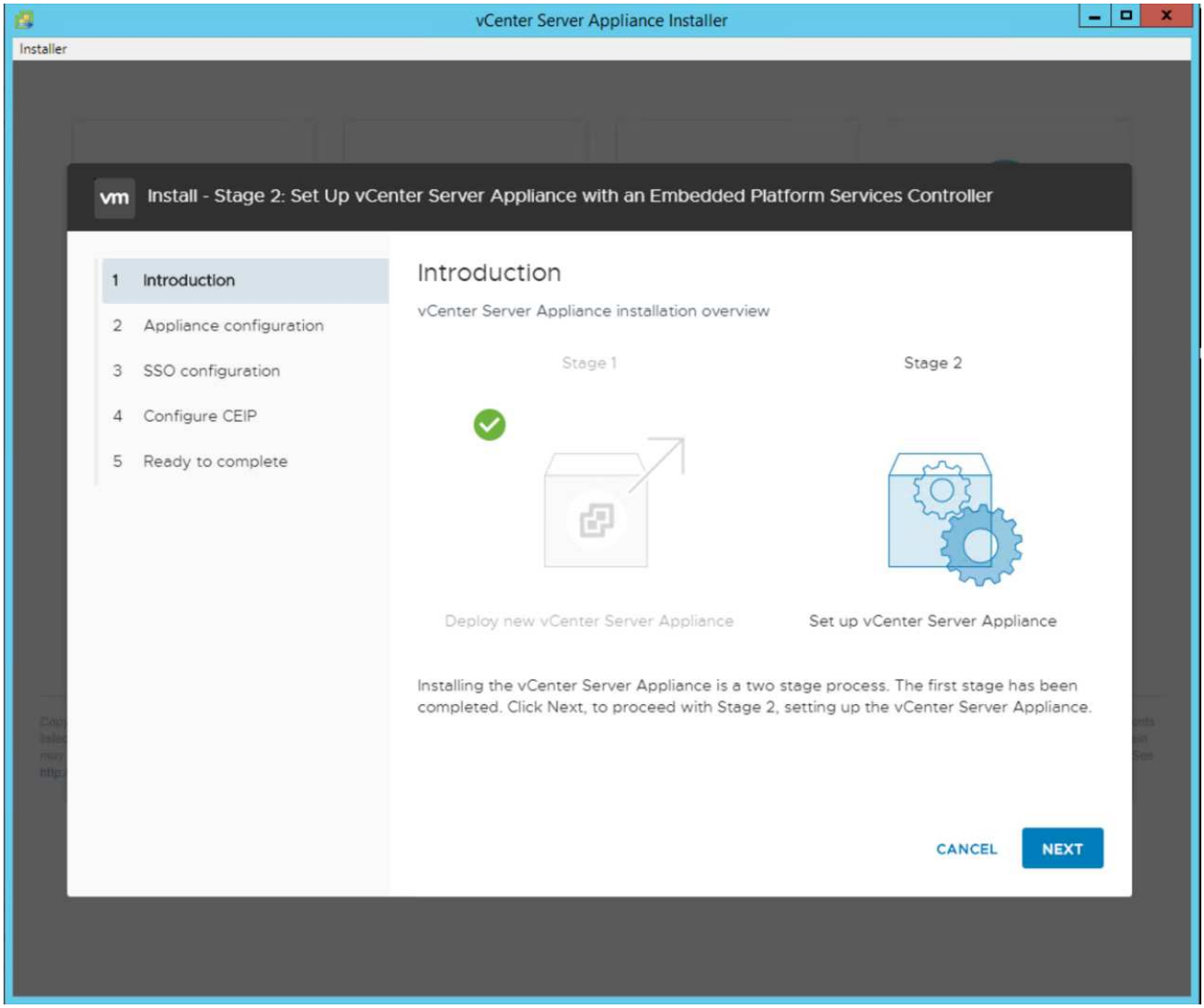


15. Überprüfen Sie Ihre Einstellungen in Phase 1, bevor Sie mit der Bereitstellung der Appliance beginnen.

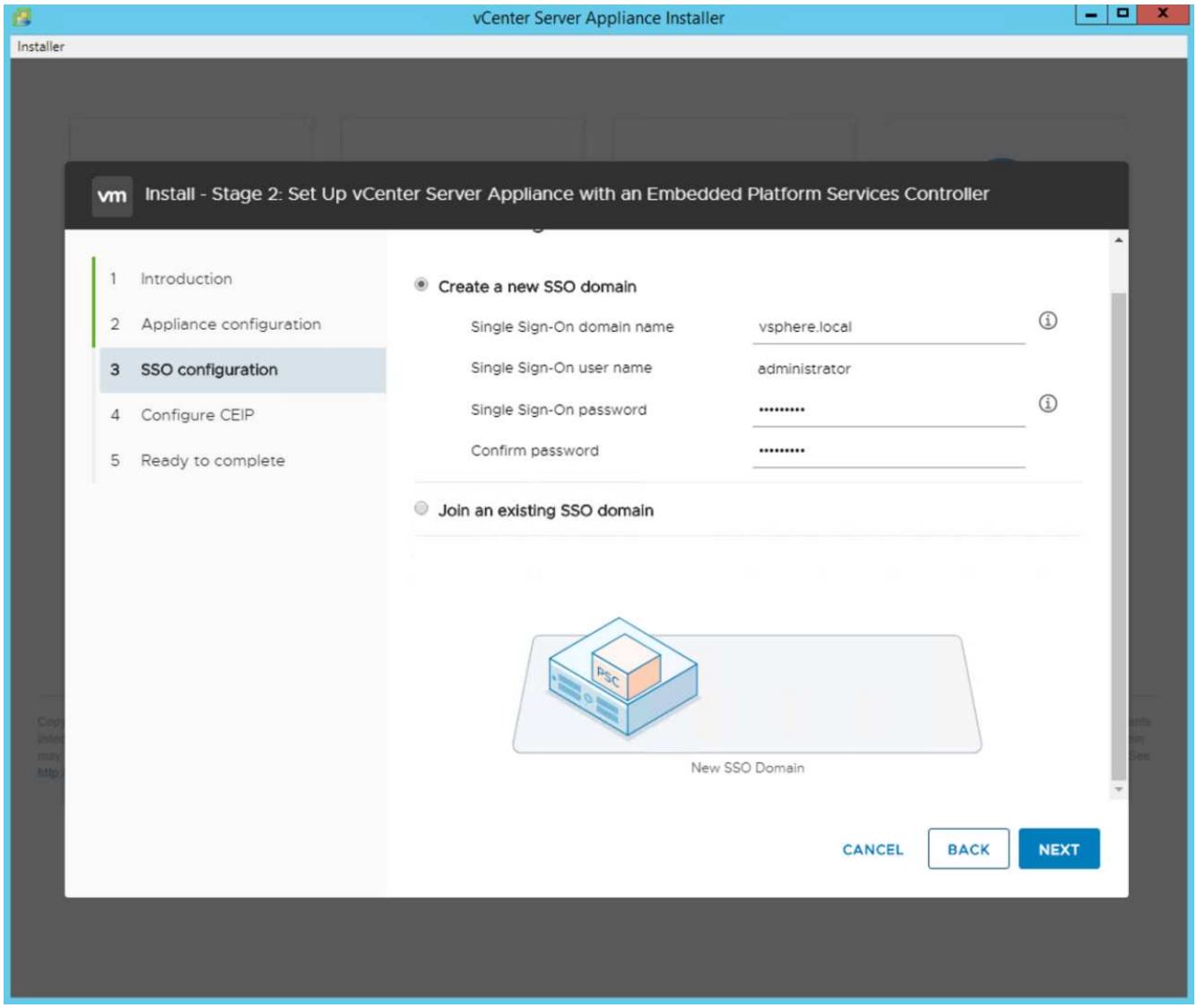


Die VCSA wird jetzt installiert. Dieser Vorgang dauert mehrere Minuten.

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.

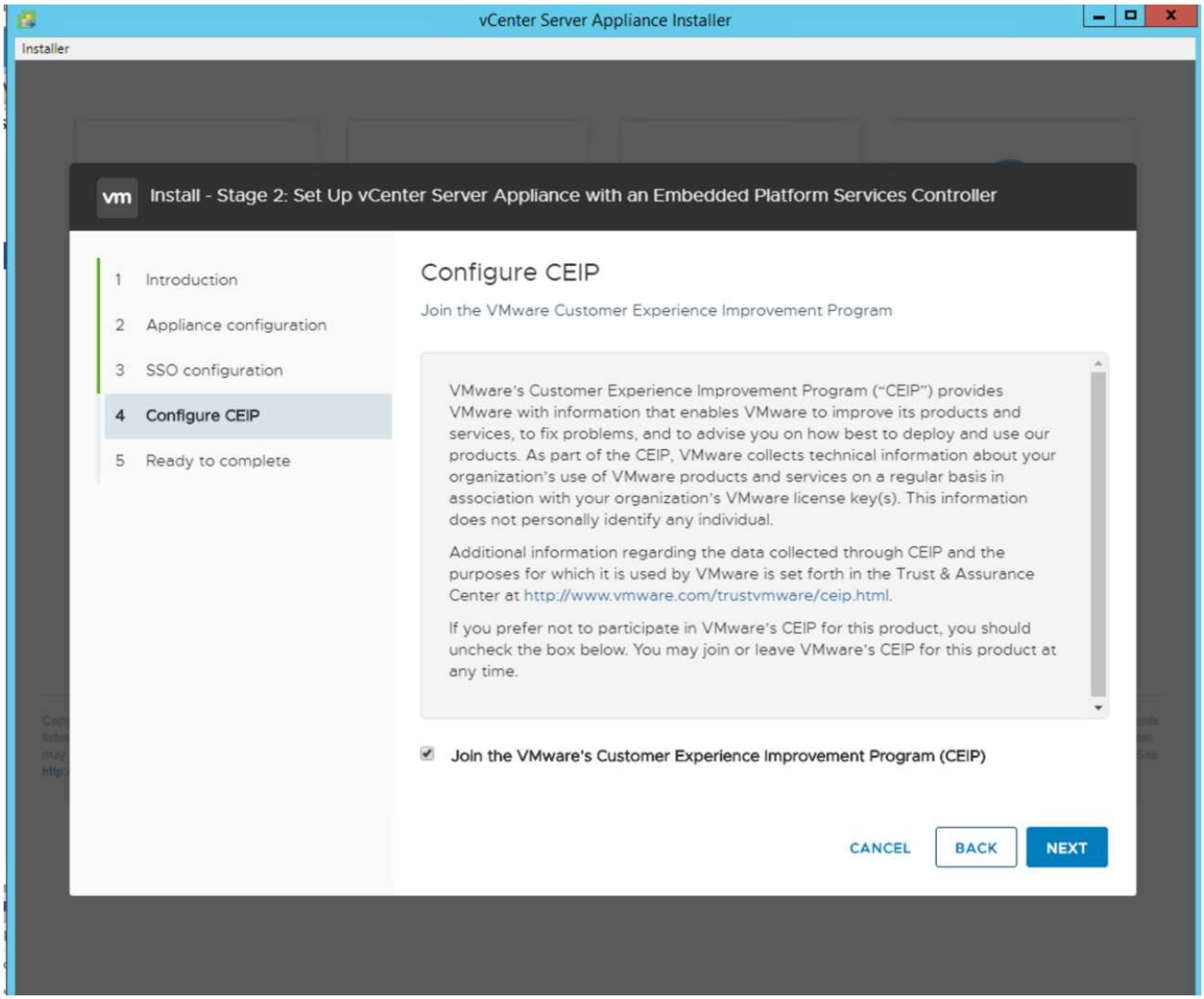


18. Eingabe `<<var_ntp_id>>` Für die NTP-Serveradresse. Sie können mehrere NTP-IP-Adressen eingeben.
19. Wenn Sie Hochverfügbarkeit (HA) in vCenter Server verwenden möchten, stellen Sie sicher, dass der SSH-Zugriff aktiviert ist.
20. Konfigurieren Sie den SSO-Domänennamen, das Passwort und den Standortnamen. Klicken Sie Auf Weiter.

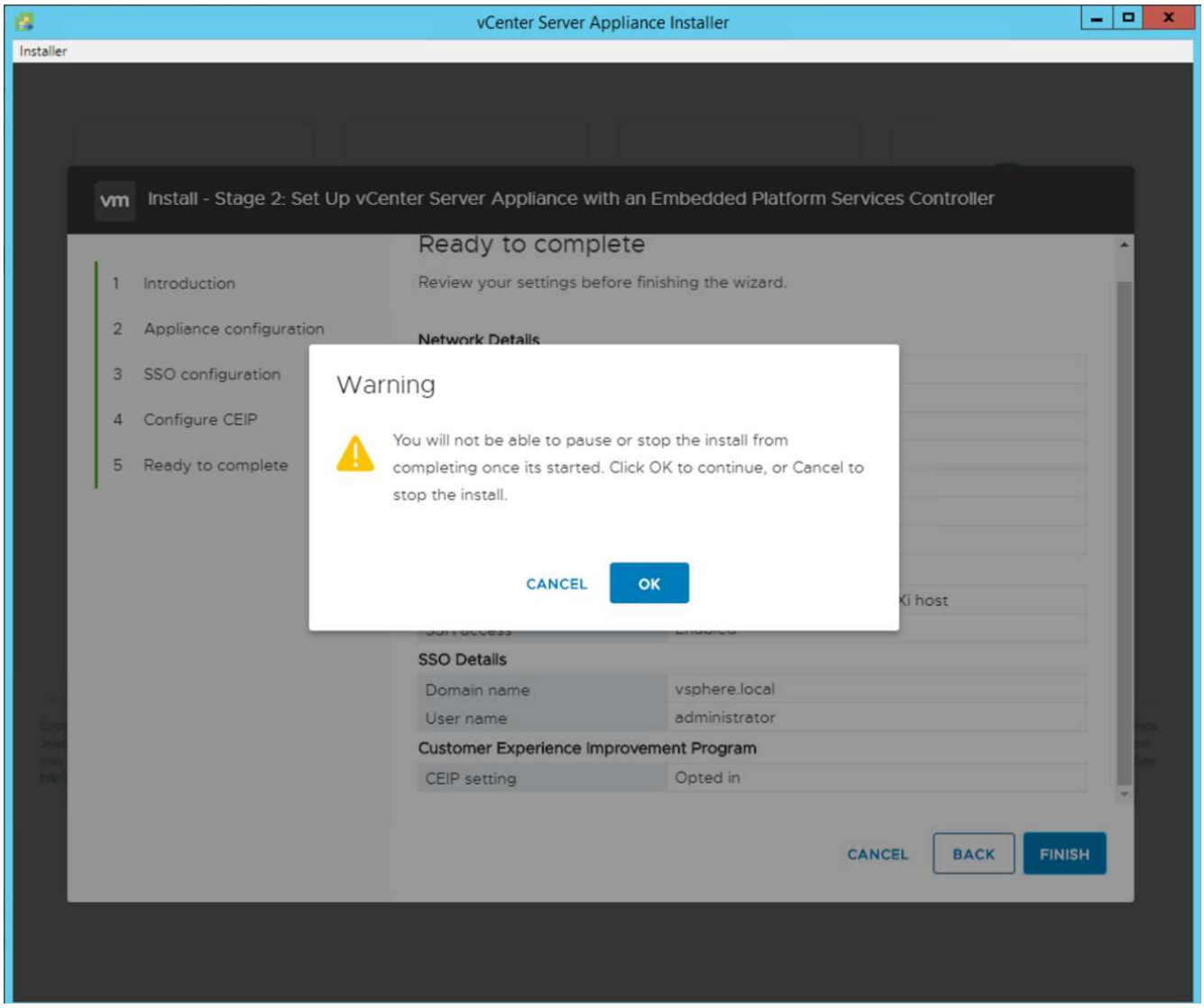


Notieren Sie diese Werte für Ihre Referenz, insbesondere wenn Sie vom abweichen `vsphere.local` Domain-Name:

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

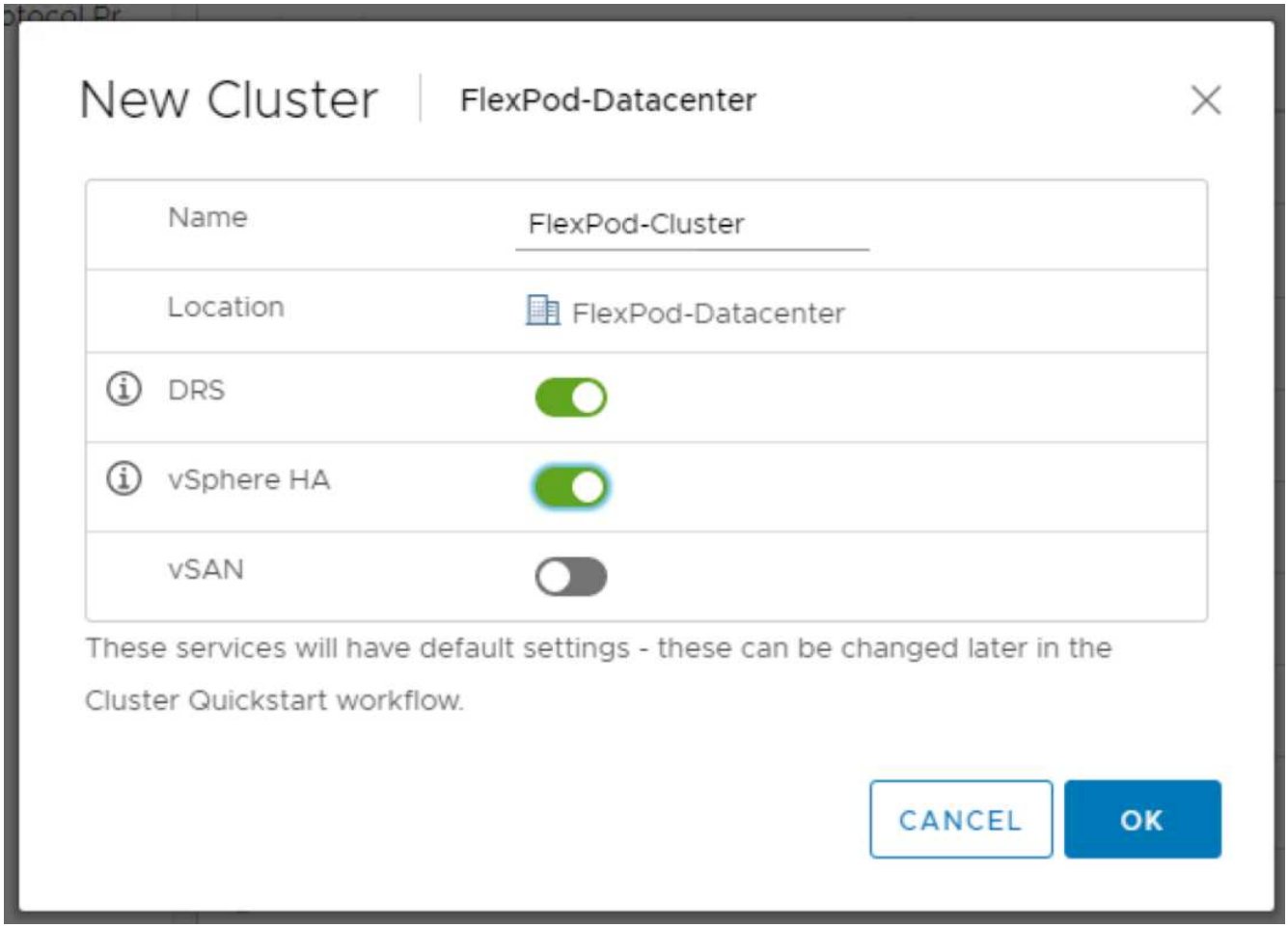
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

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:

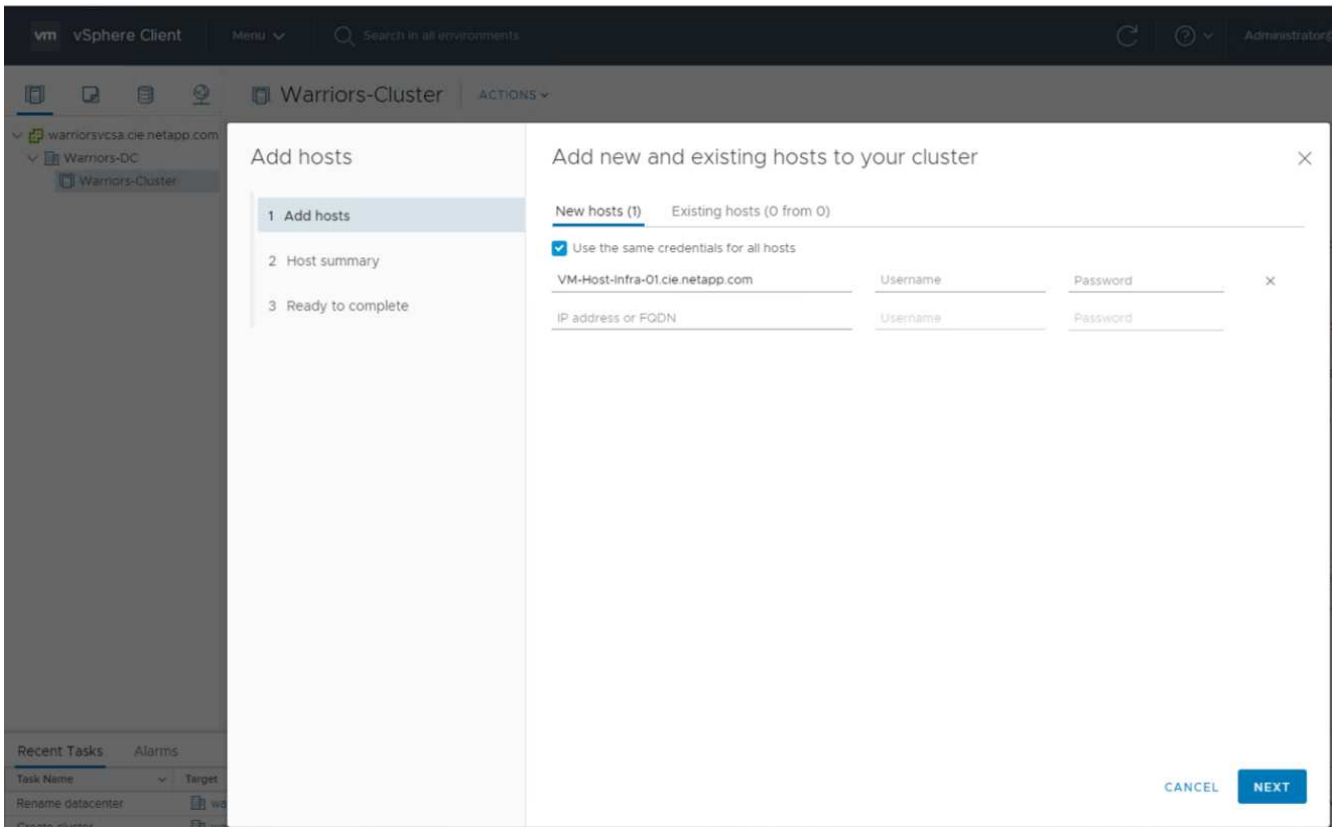
1. Klicken Sie mit der rechten Maustaste auf das neu erstellte Datacenter, und wählen Sie Neuer Cluster aus.
2. Geben Sie einen Namen für das Cluster ein.
3. Aktivieren Sie DR und vSphere HA, indem Sie die Kontrollkästchen auswählen.
4. Klicken Sie auf OK.



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.

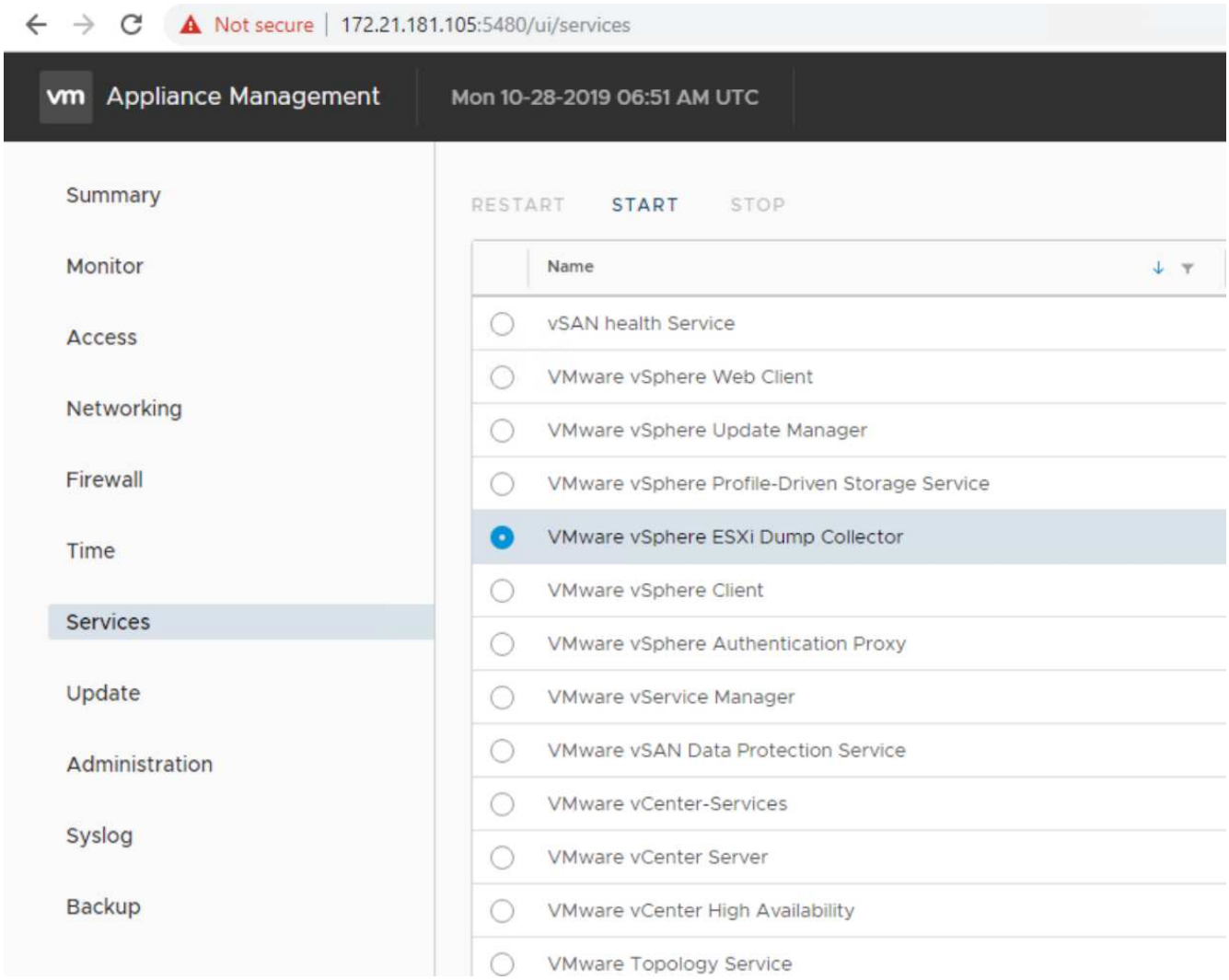
> Dieser Prozess muss für alle zusätzlichen Hosts abgeschlossen werden, die zur Konfiguration von FlexPod Express hinzugefügt werden.

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."

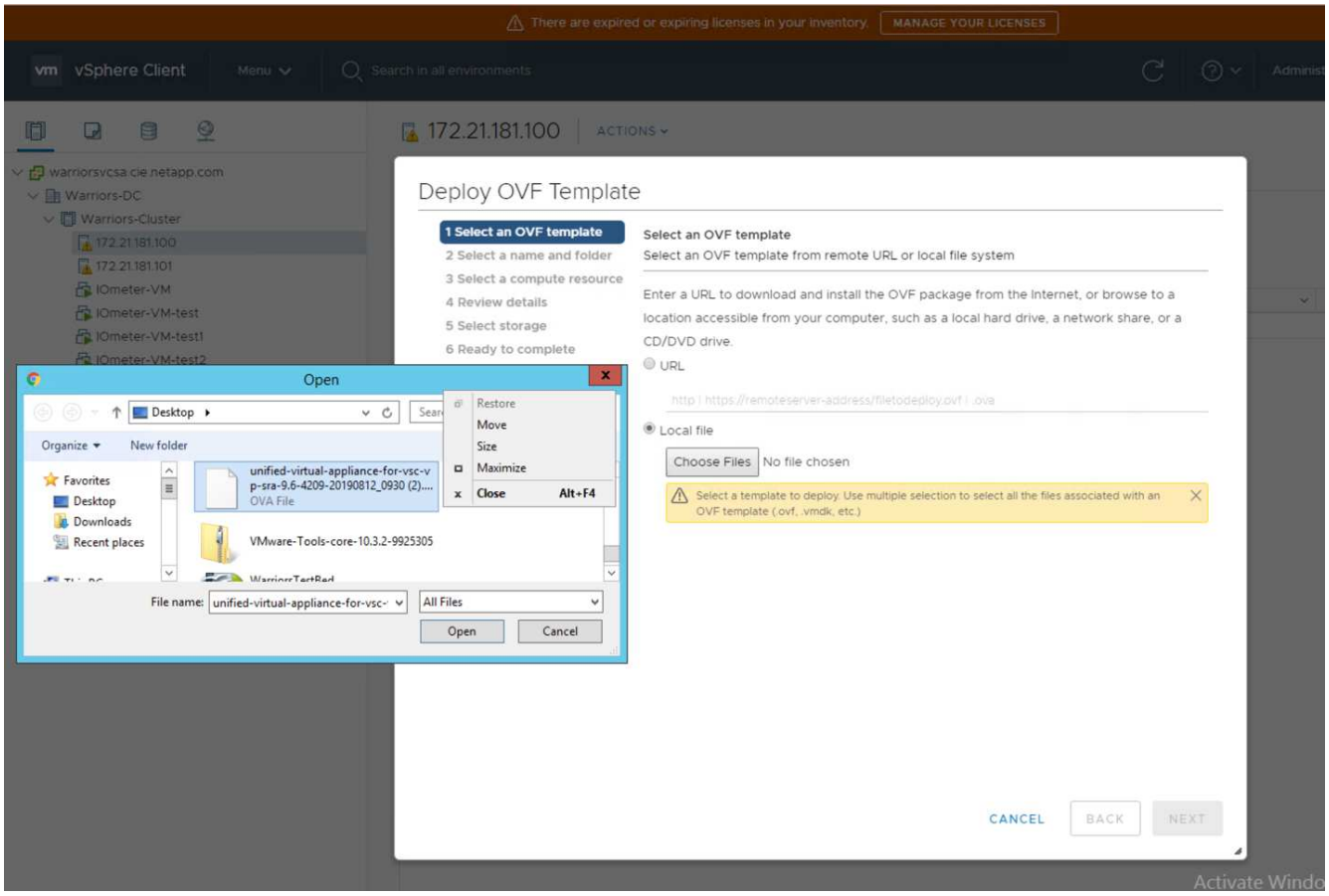
Implementierungsverfahren für NetApp Virtual Storage Console 9.6

Dieser Abschnitt beschreibt die Implementierungsverfahren für die NetApp Virtual Storage Console (VSC).

Installieren Sie Virtual Storage Console 9.6

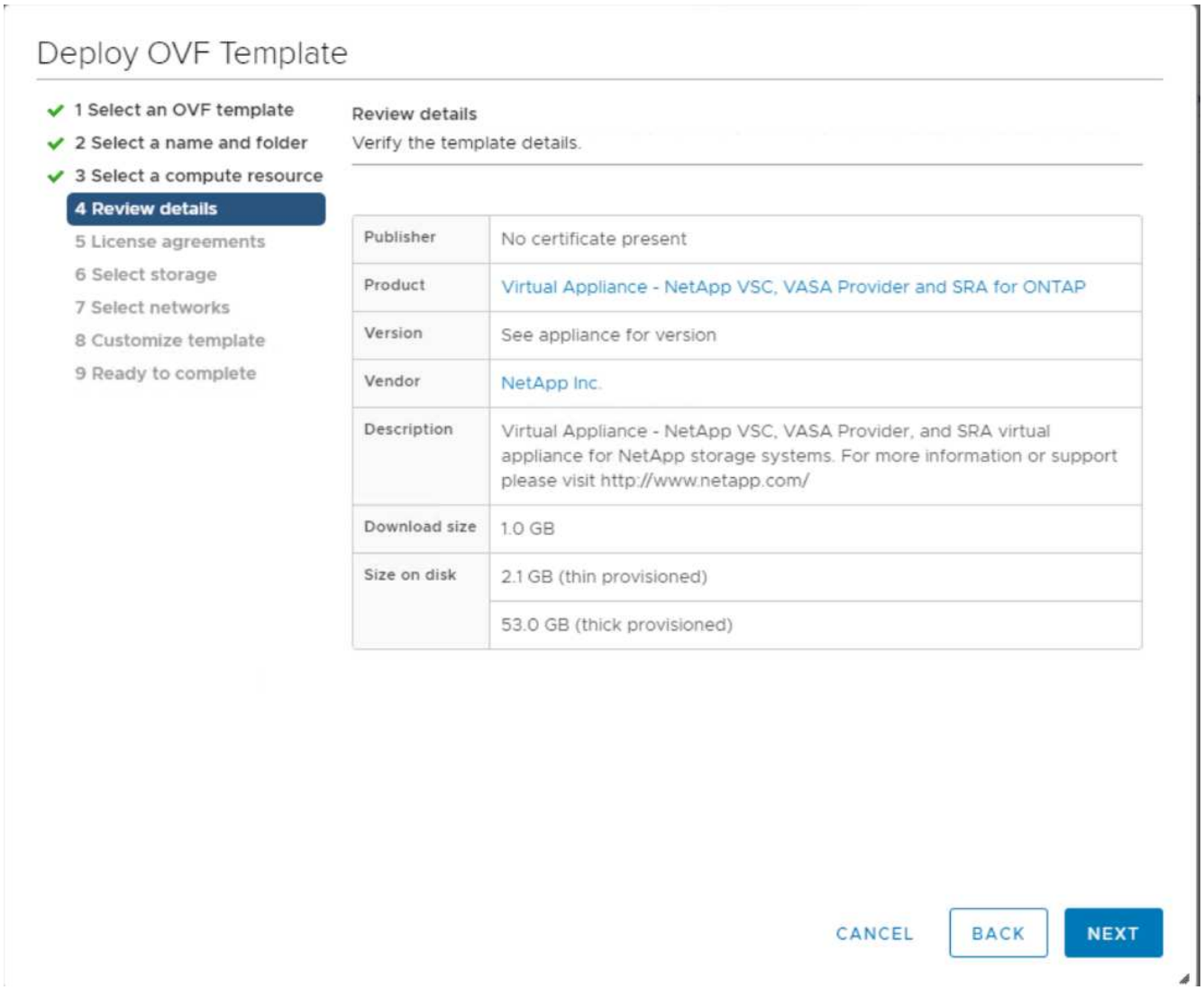
Gehen Sie wie folgt vor, um die VSC 9.6-Software mithilfe einer OVF-Implementierung (Open Virtualization Format) zu installieren:

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.

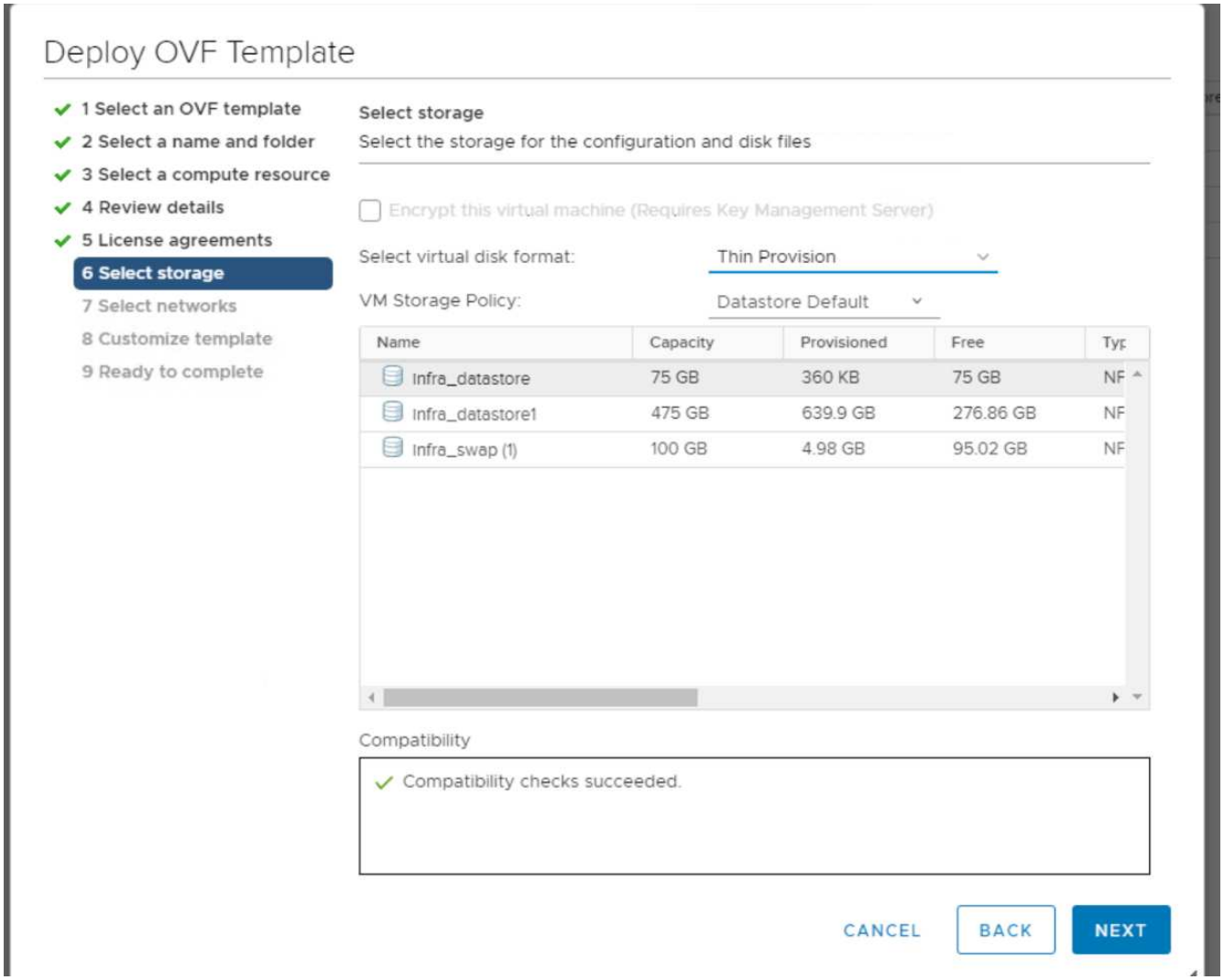


3. Geben Sie den VM-Namen ein, und wählen Sie ein Datacenter oder einen Ordner aus, in dem die Bereitstellung erfolgen soll. Klicken Sie Auf Weiter.

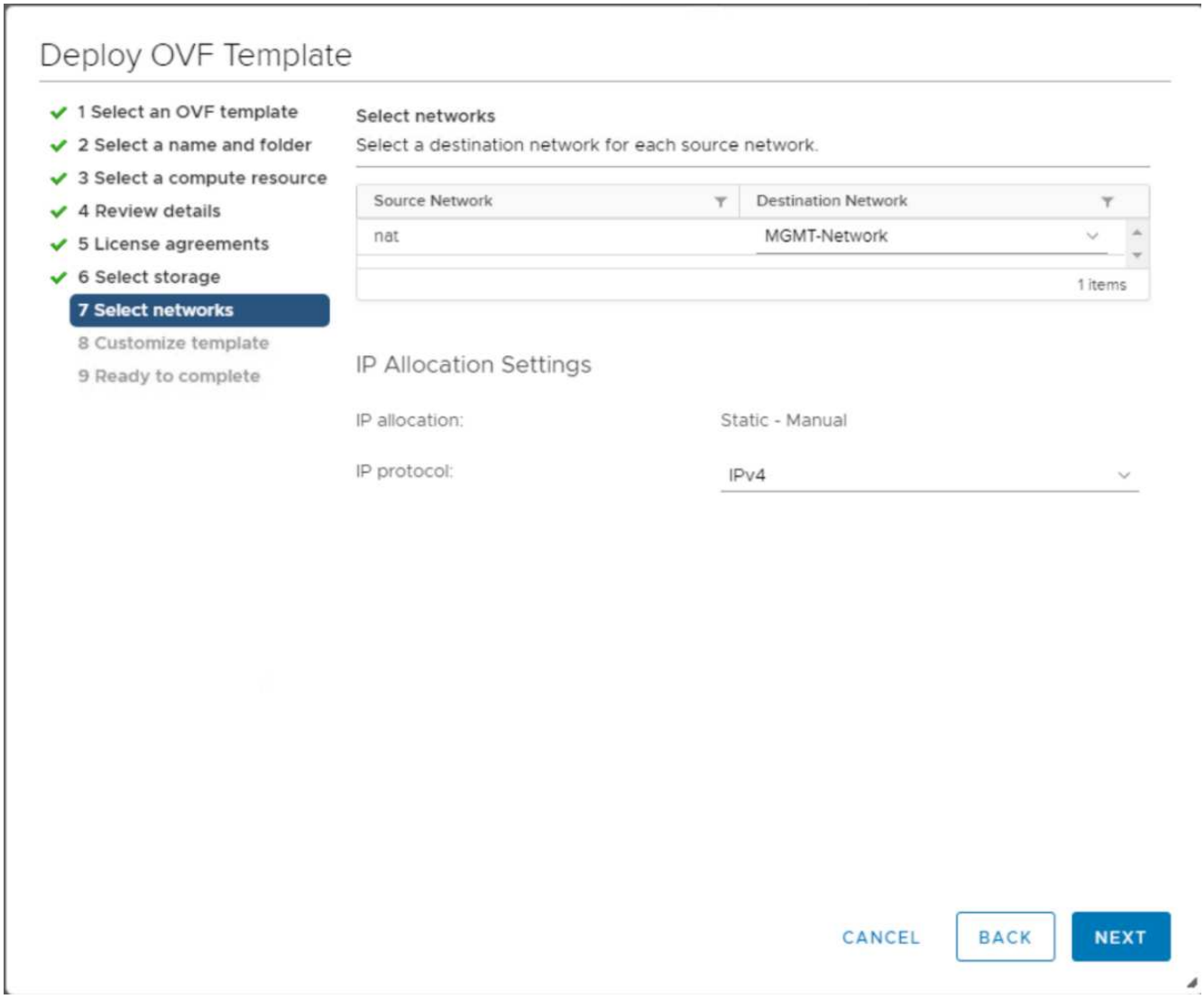
4. Wählen Sie das FlexPod Cluster ESXi Cluster aus und klicken Sie auf Weiter.
5. Überprüfen Sie die Details und klicken Sie auf Weiter.



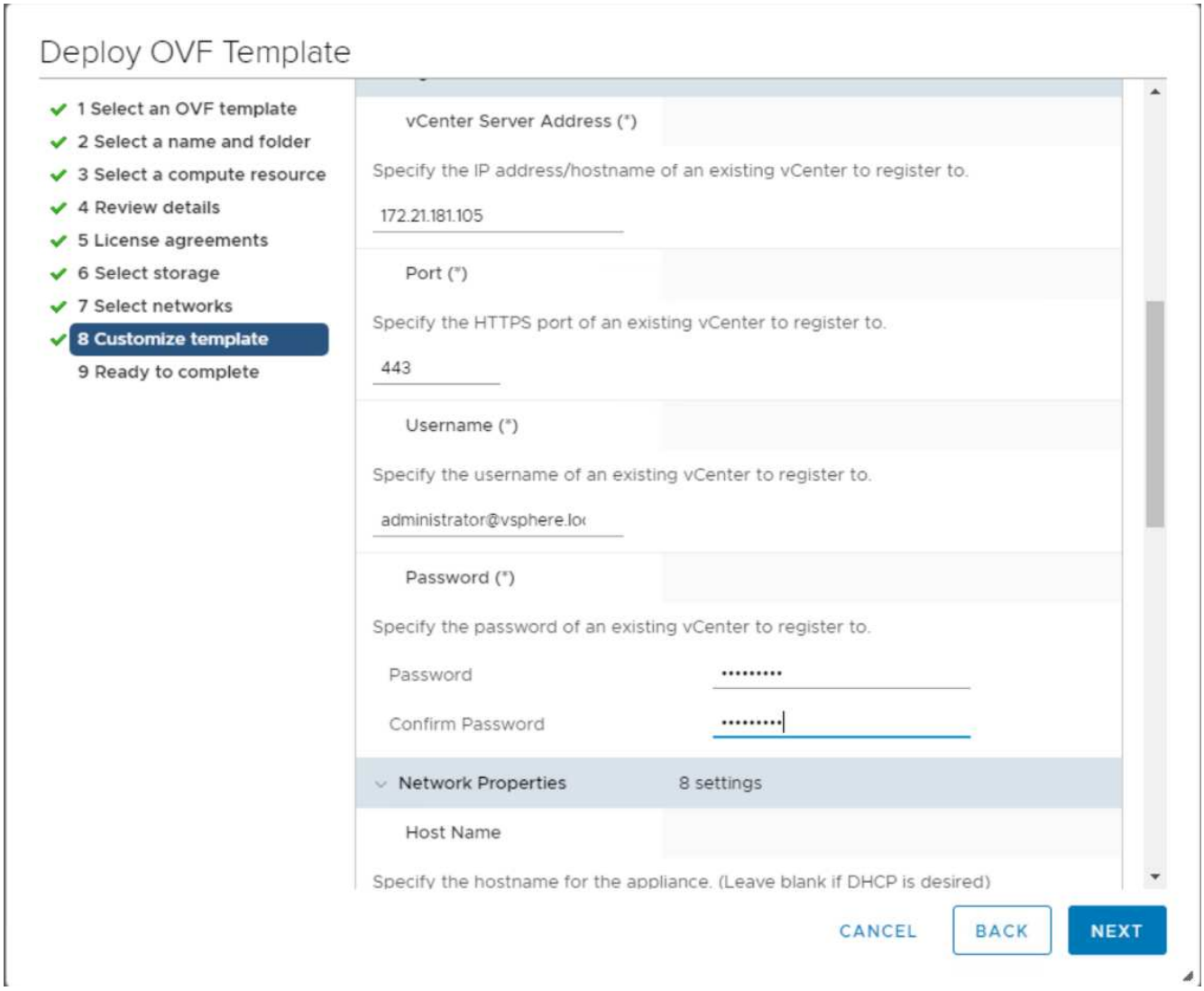
6. Klicken Sie auf Akzeptieren, um die Lizenz zu akzeptieren, und klicken Sie auf Weiter.
7. Wählen Sie das Format der virtuellen Thin Provisioning-Festplatte und einen der NFS-Datenspeicher aus. Klicken Sie Auf Weiter.



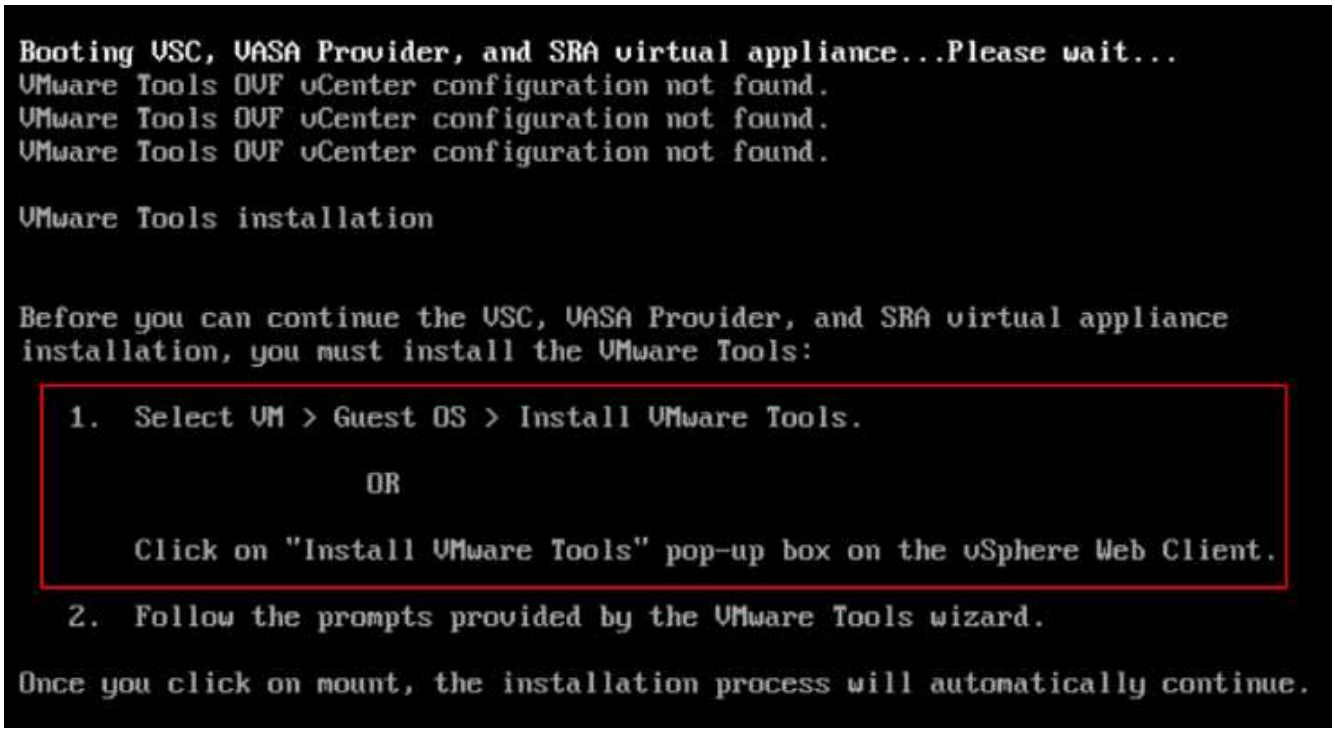
8. Wählen Sie unter Netzwerke auswählen ein Zielnetzwerk aus, und klicken Sie auf Weiter.



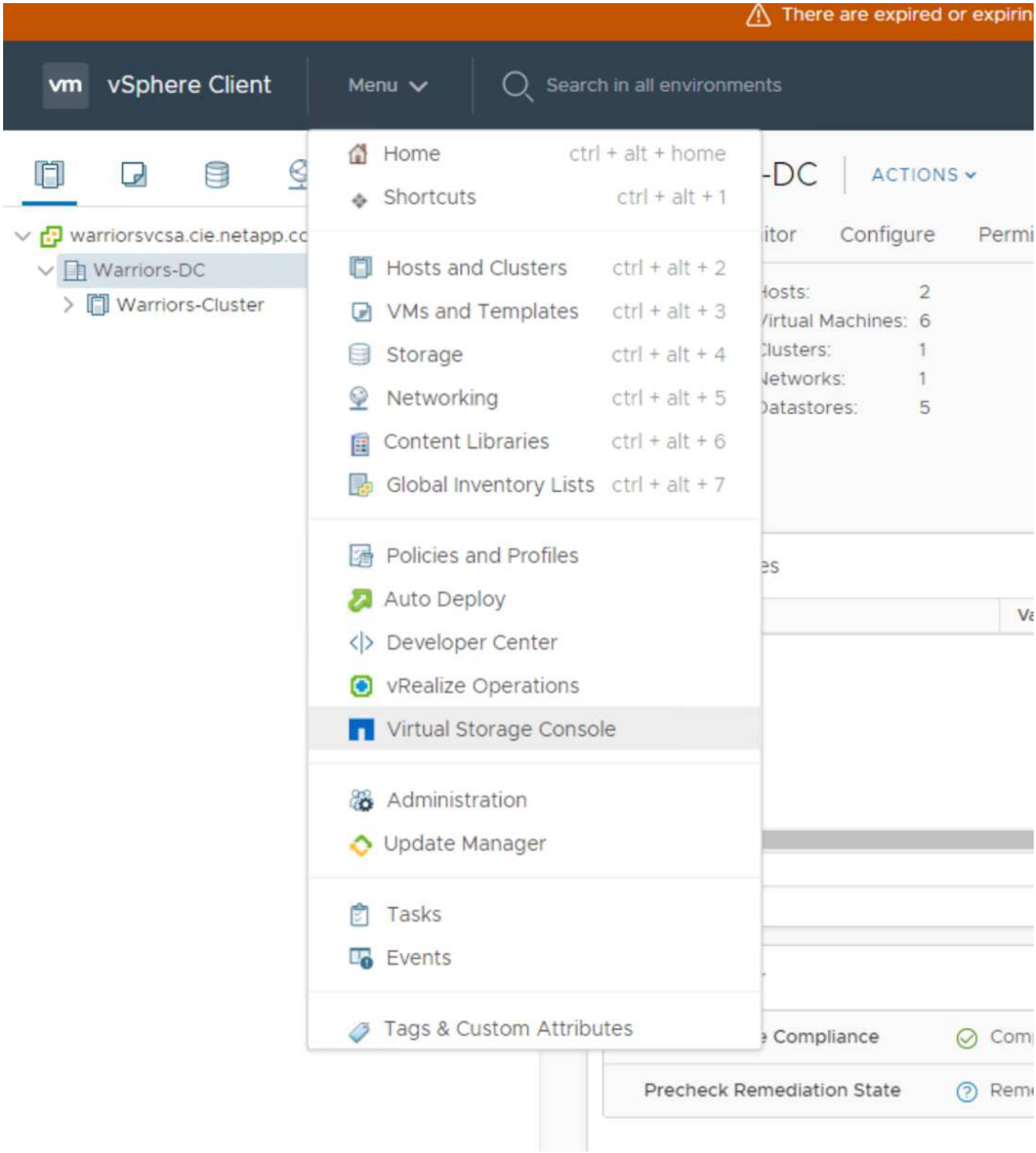
9. Geben Sie in der Vorlage „Anpassen“ das VSC Administratorpasswort, den vCenter-Namen oder die IP-Adresse und andere Konfigurationsdetails ein, und klicken Sie auf „Weiter“.



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

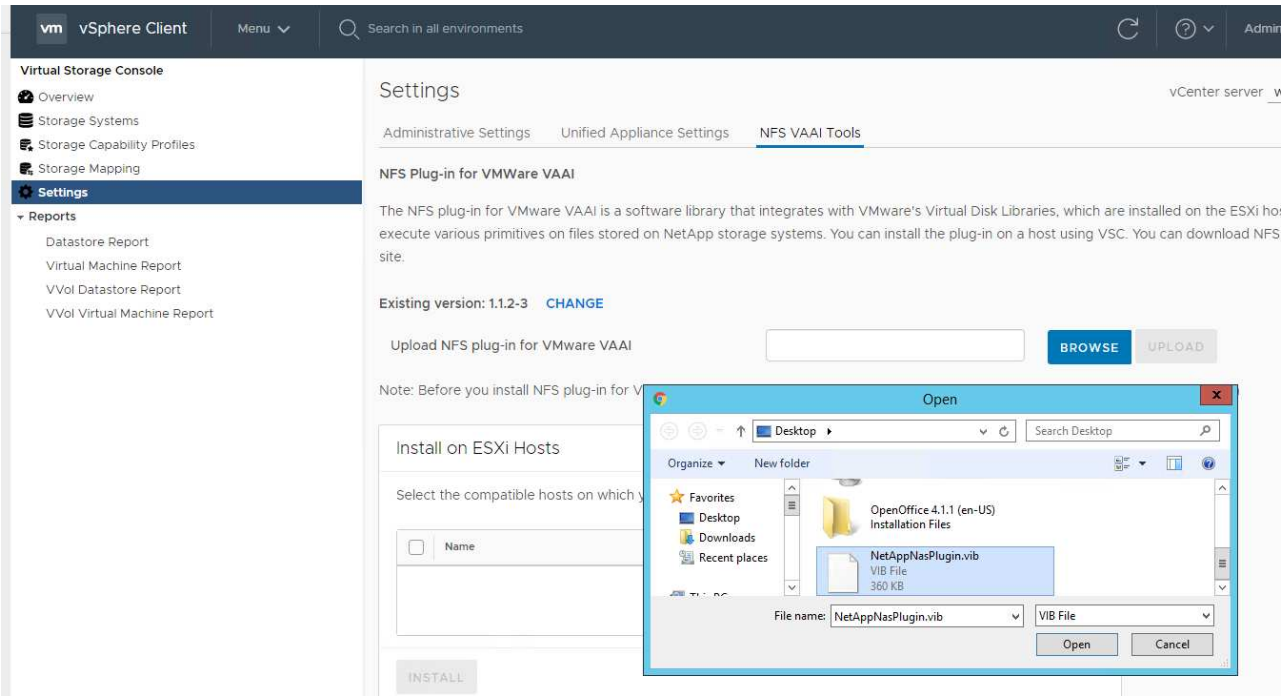
So laden Sie das NetApp NFS VAAI Plug-in herunter und installieren es:

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.

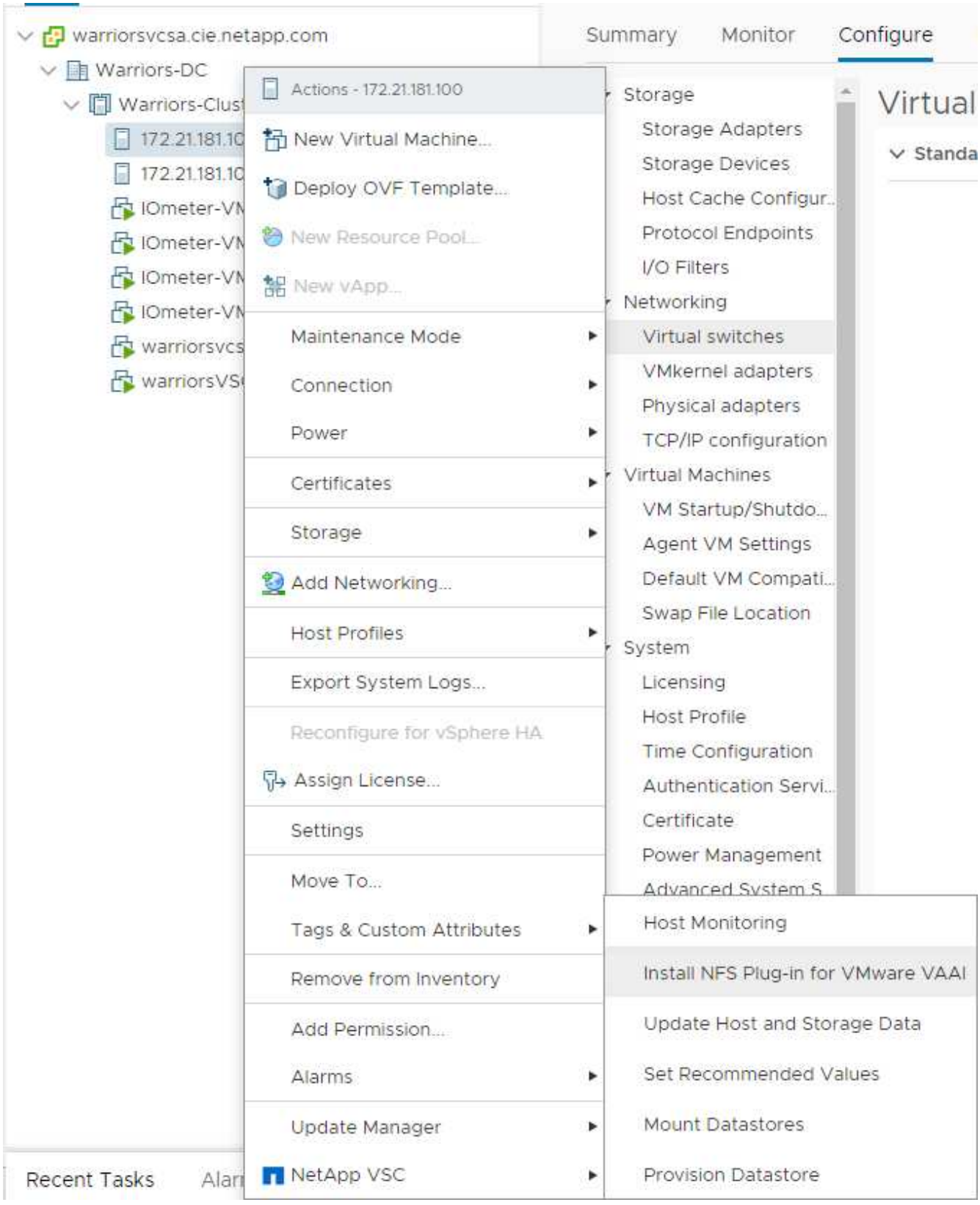
c. Wählen Sie im Startbildschirm des vSphere Web Client die Option Virtual Storage Console aus.

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.

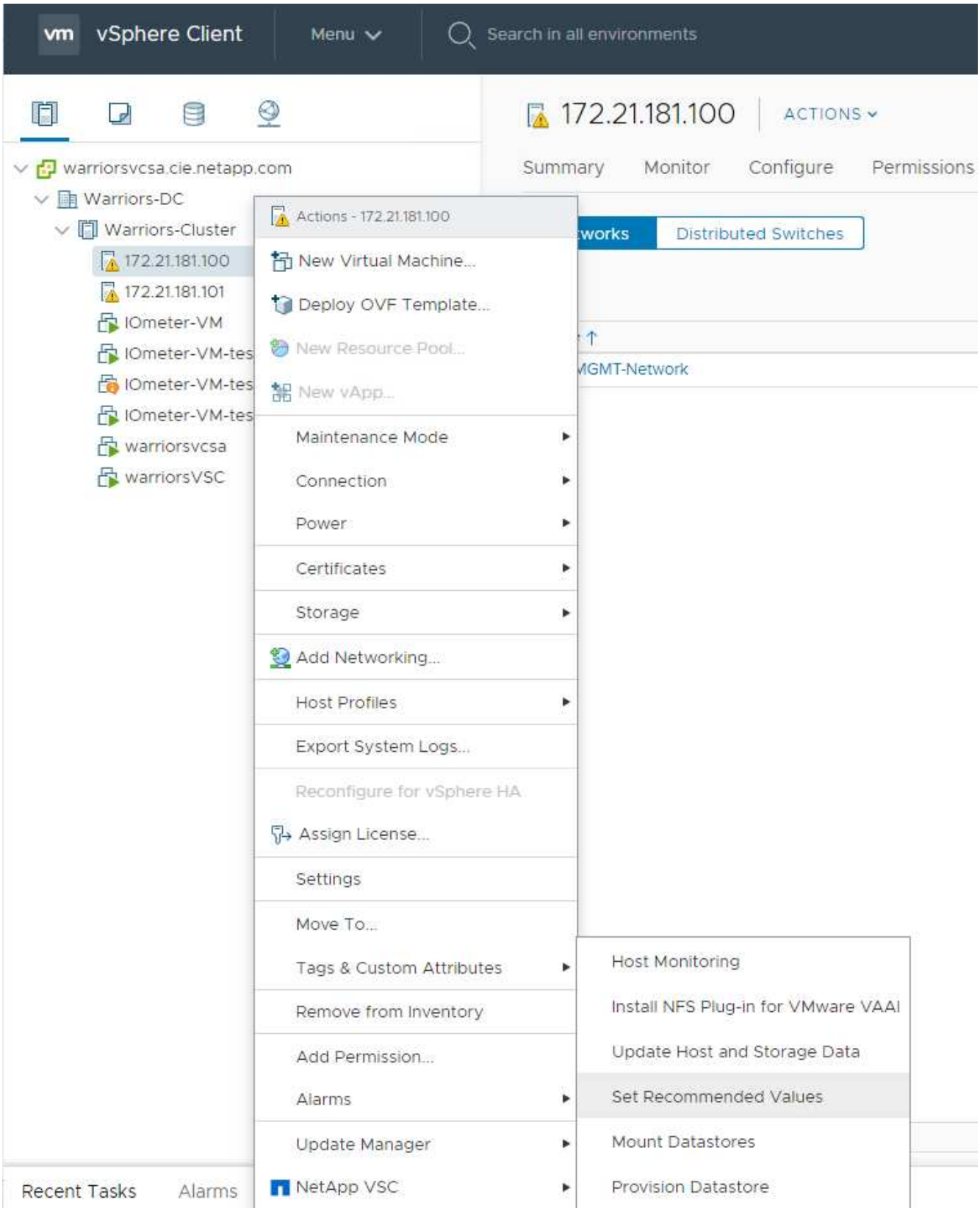
4. Wählen Sie den Host aus, und wählen Sie dann NetApp VSC > NFS-Plug-in für VMware VAAI installieren aus.



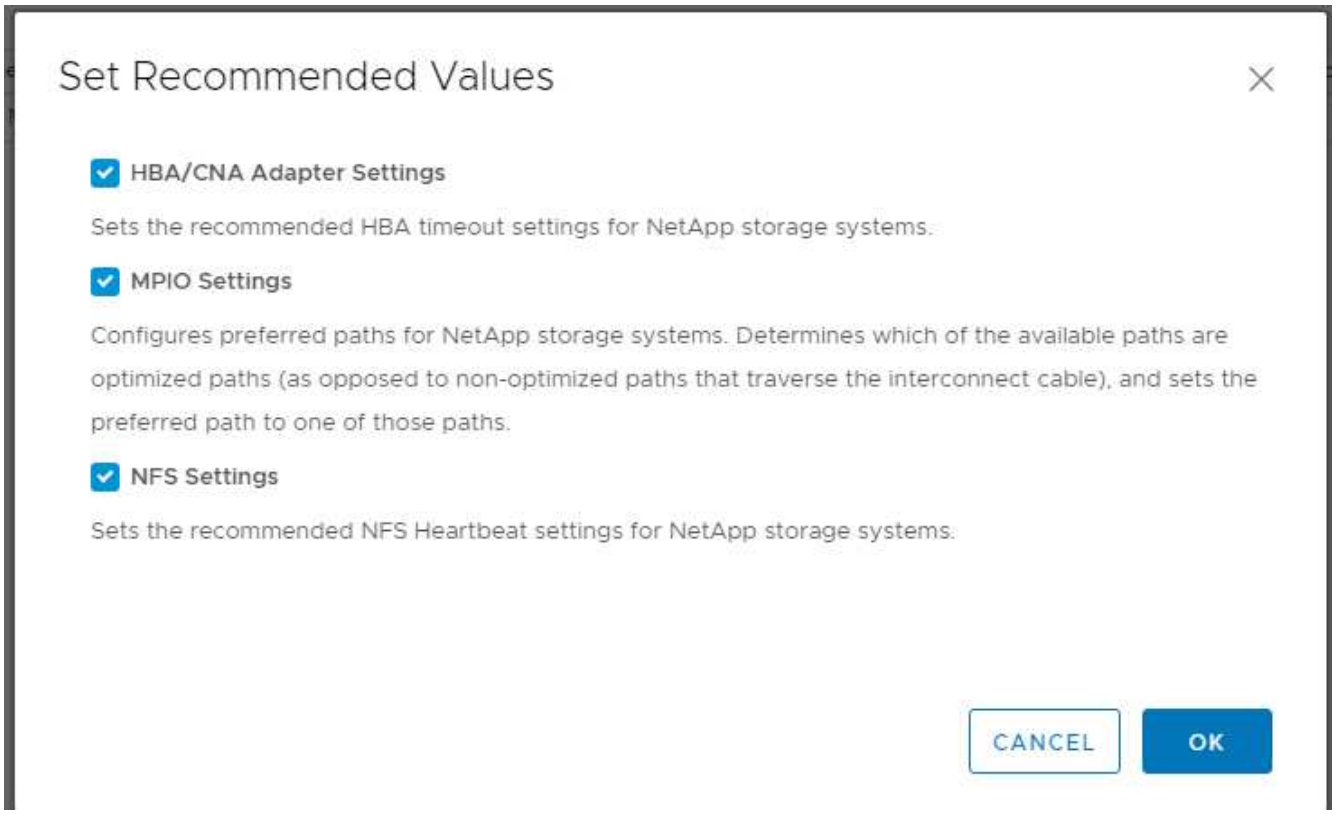
Optimale Speichereinstellungen für die ESXi Hosts verwenden

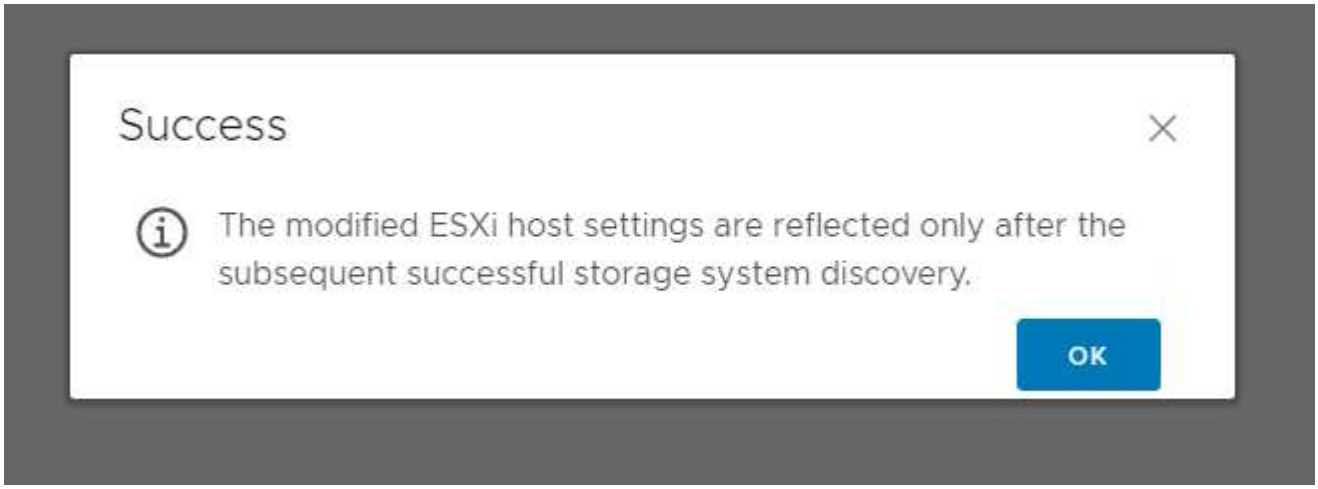
VSC ermöglicht die automatisierte Konfiguration der Storage-Einstellungen für alle ESXi Hosts, die mit NetApp Storage Controllern verbunden sind. Gehen Sie wie folgt vor, um diese Einstellungen zu verwenden:

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."

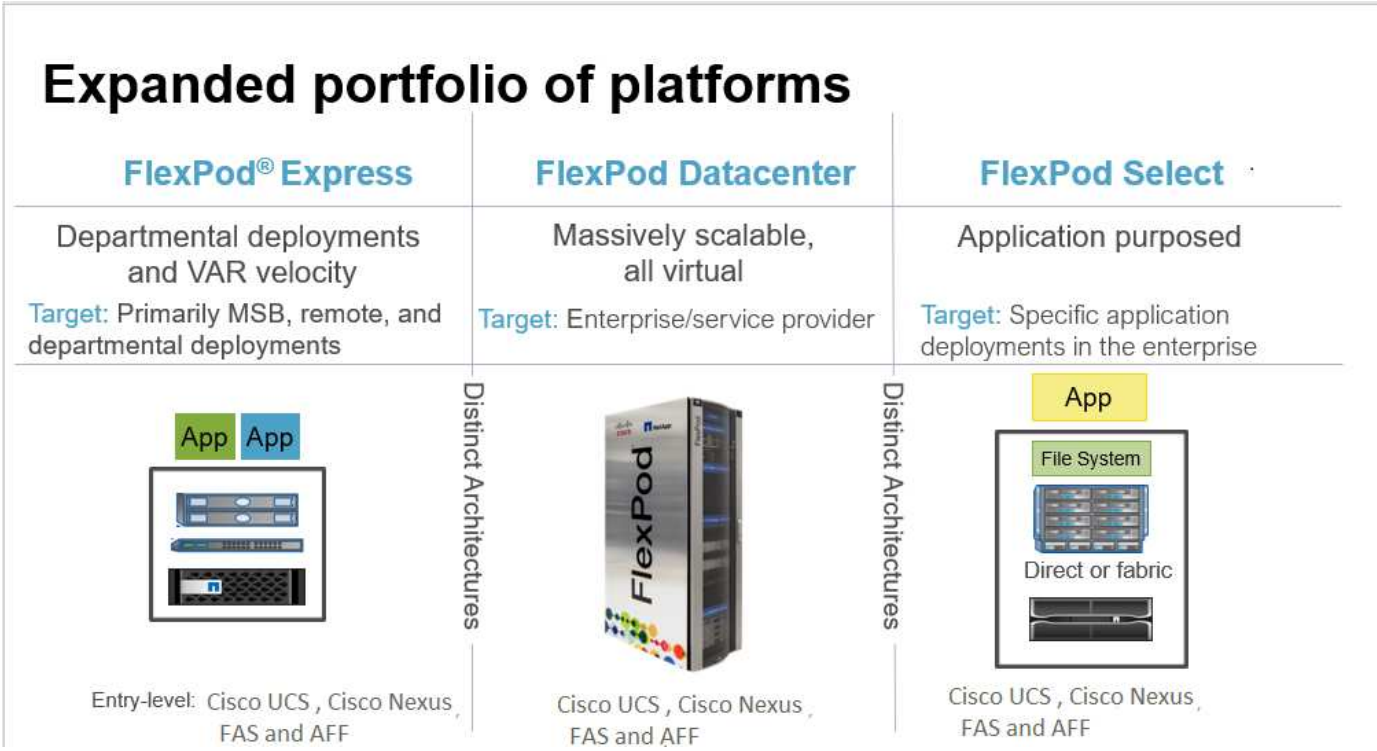
Programmzusammenfassung

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.

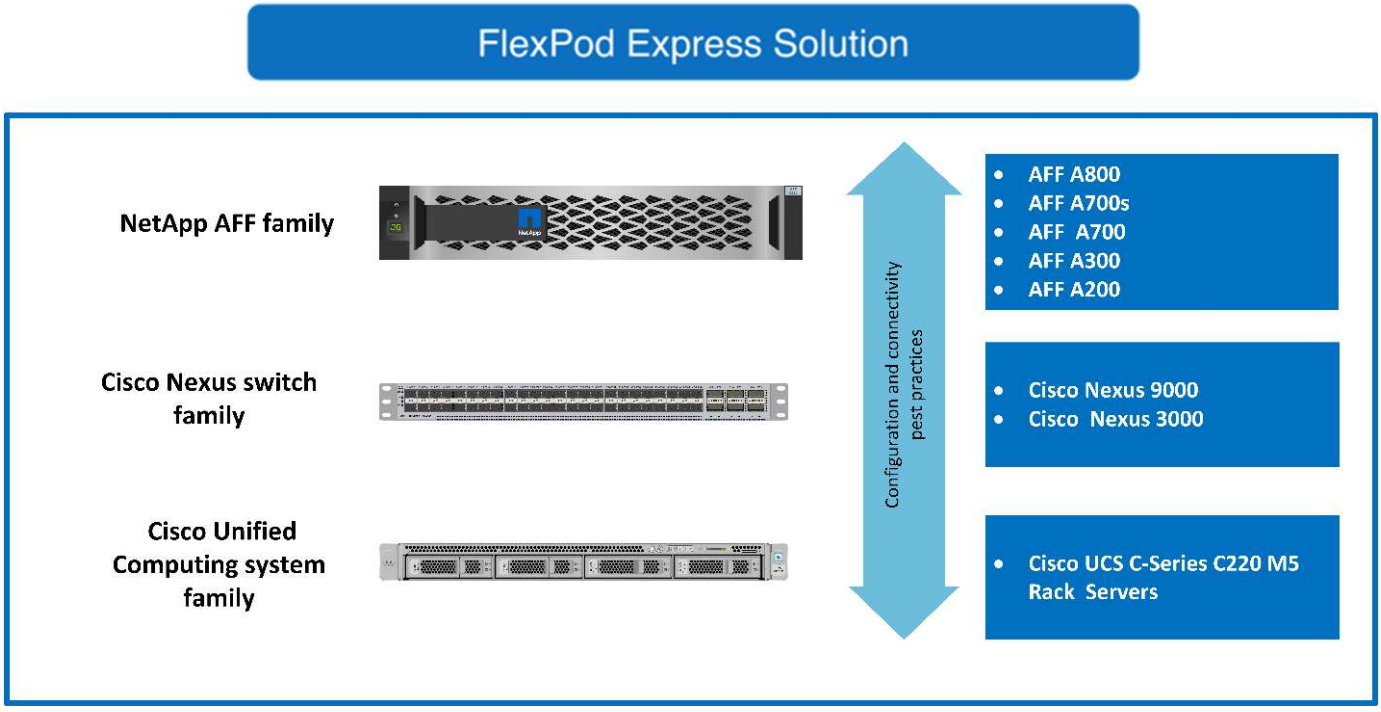
Dieses Dokument ist zwar für AFF A220 validiert, unterstützt aber auch die FAS2700.

"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.



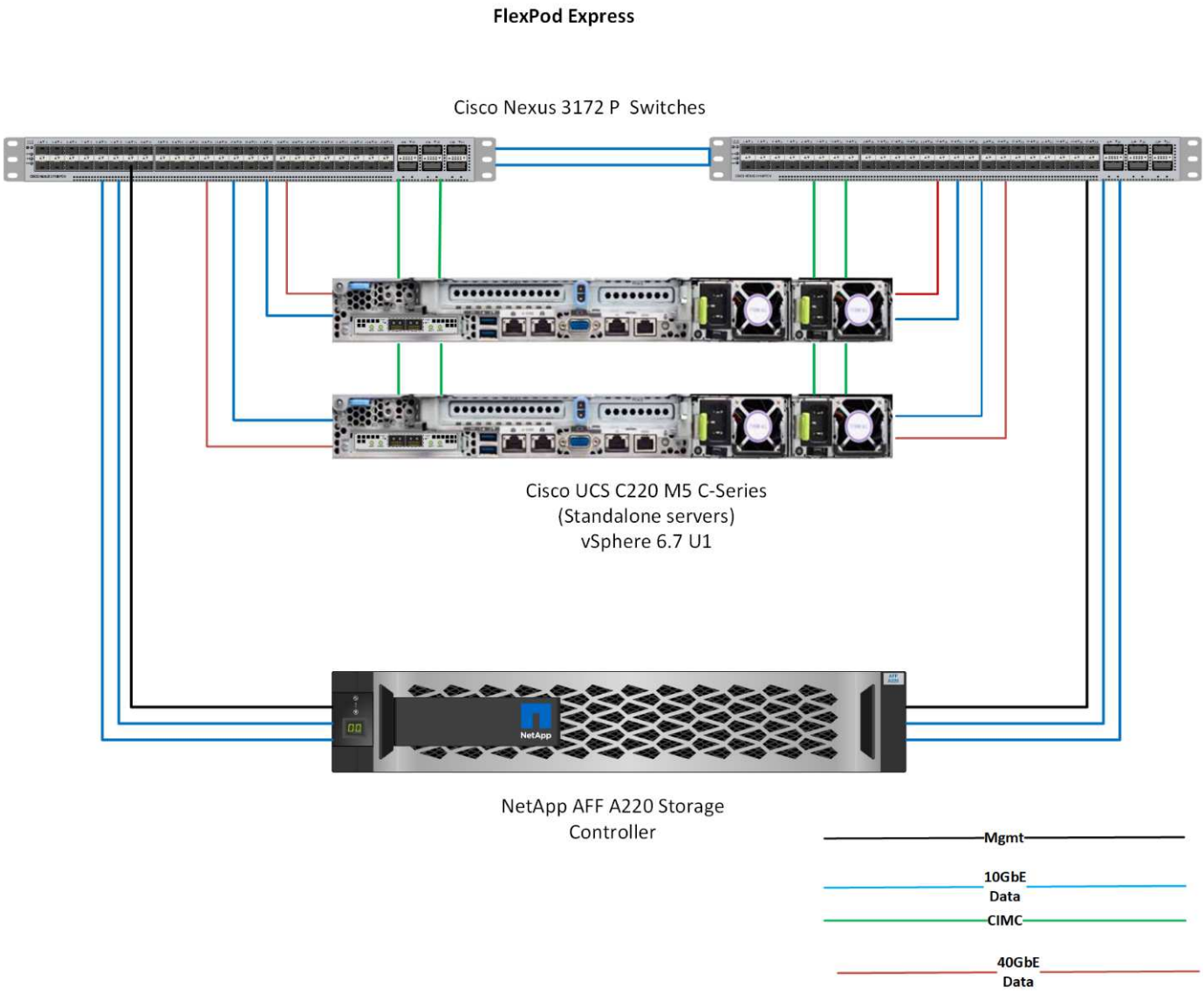
Zielgruppe

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.

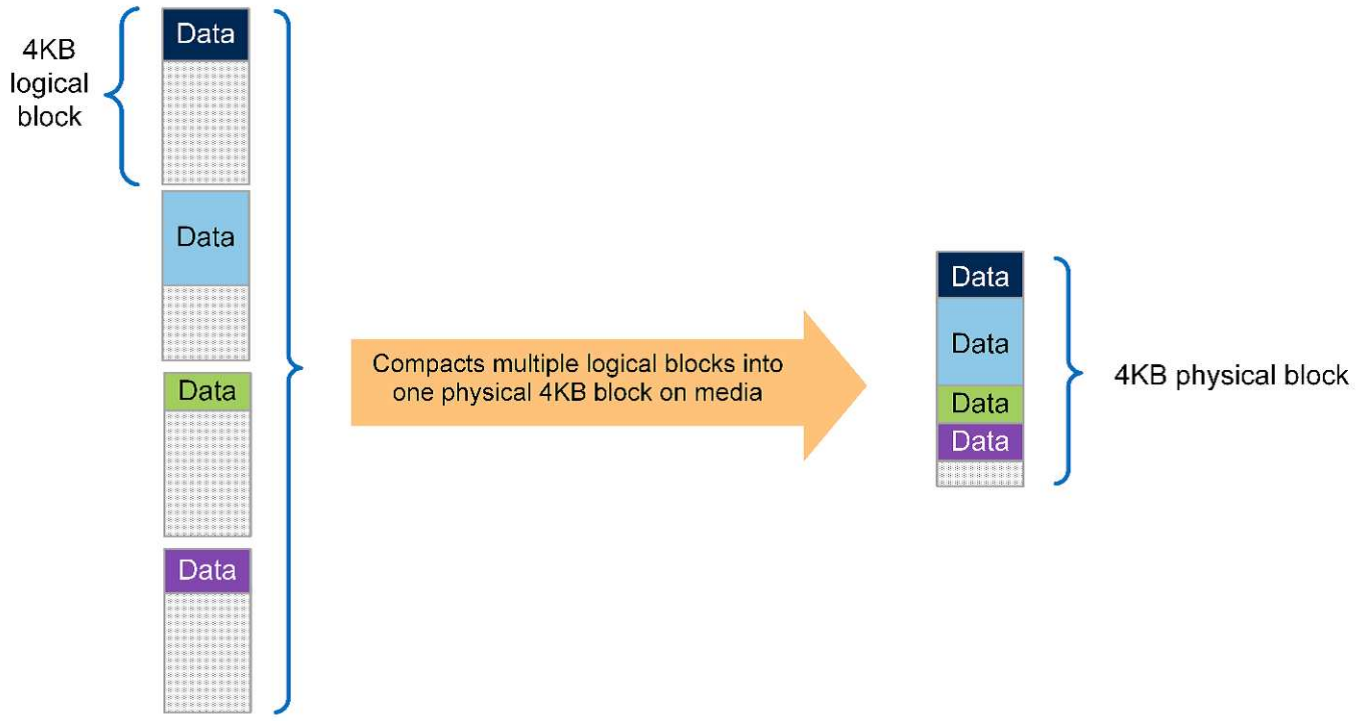
AFF A220 System

Weitere Informationen zum AFF A220 Hardwaresystem finden Sie unter "AFF A-Series Homepage".

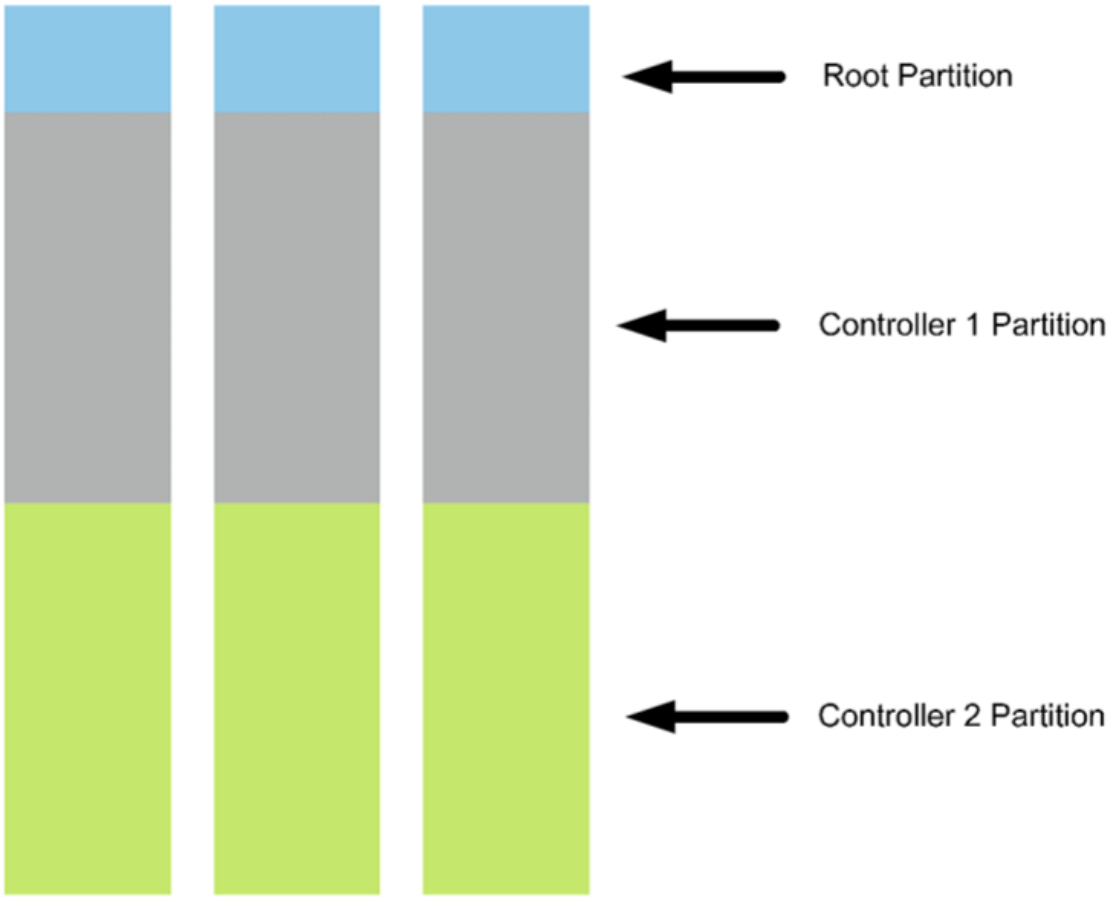
ONTAP 9.4 Software

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

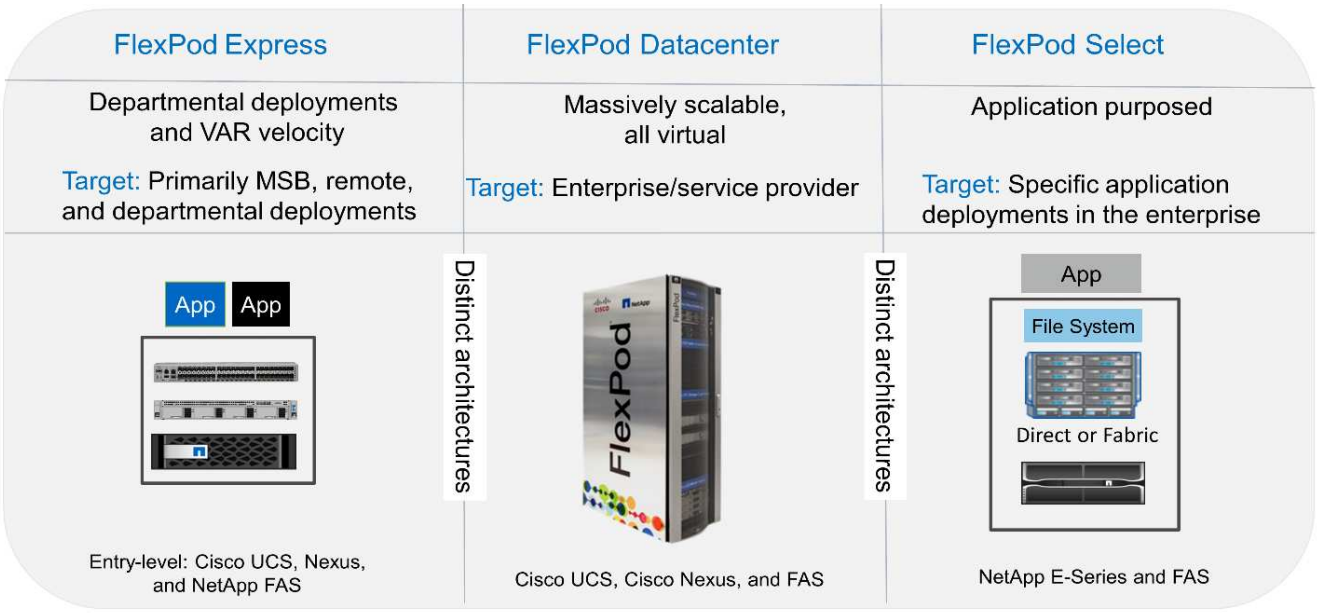
Diese FlexPod Express Lösung ist Teil des FlexPod Converged Infrastructure Programms.

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:

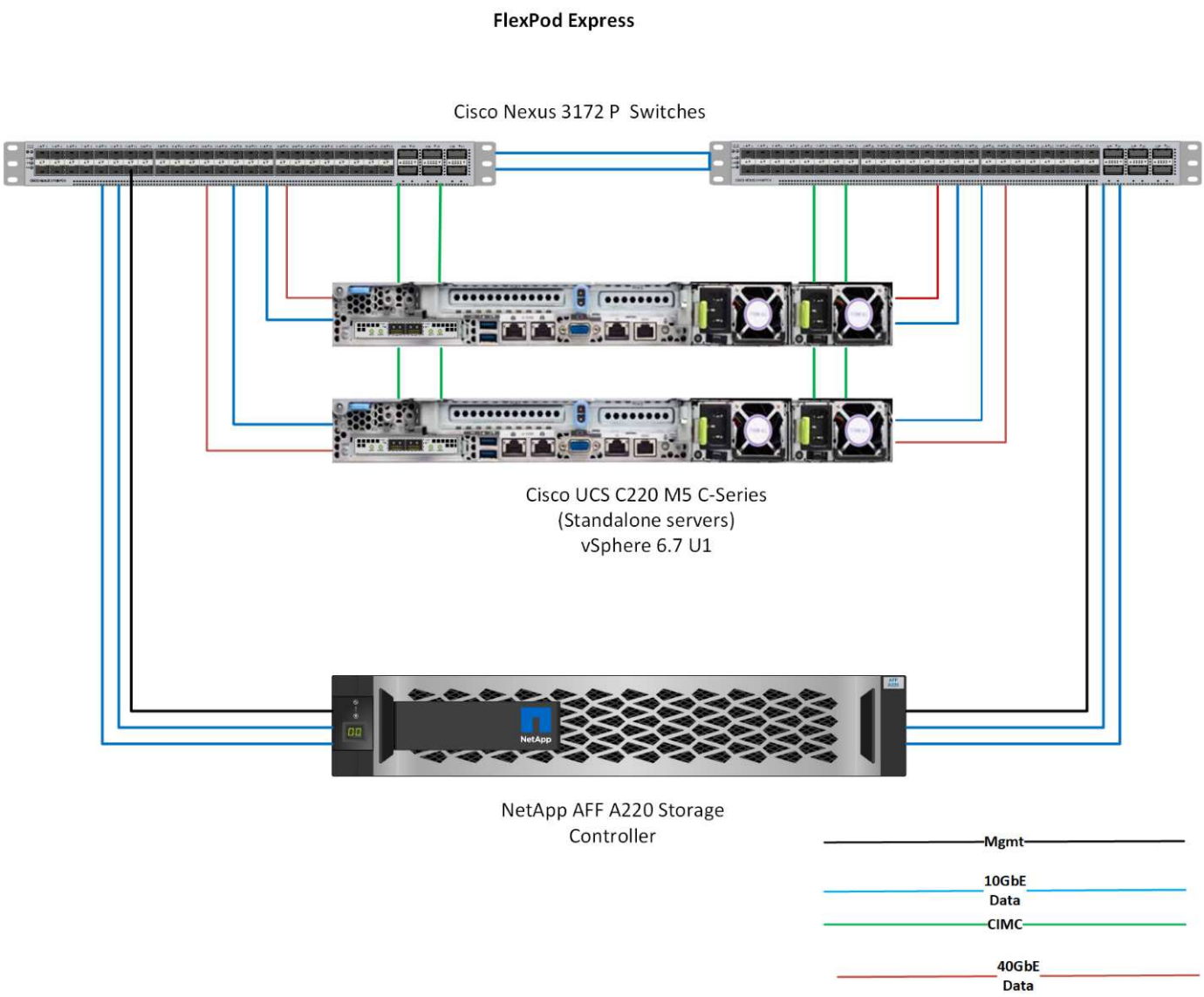
- Sorgfältig getestet
- Präskriptiv
- Minimale Risiken bei der Implementierung
- Schnellere Produkteinführungszeiten

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.

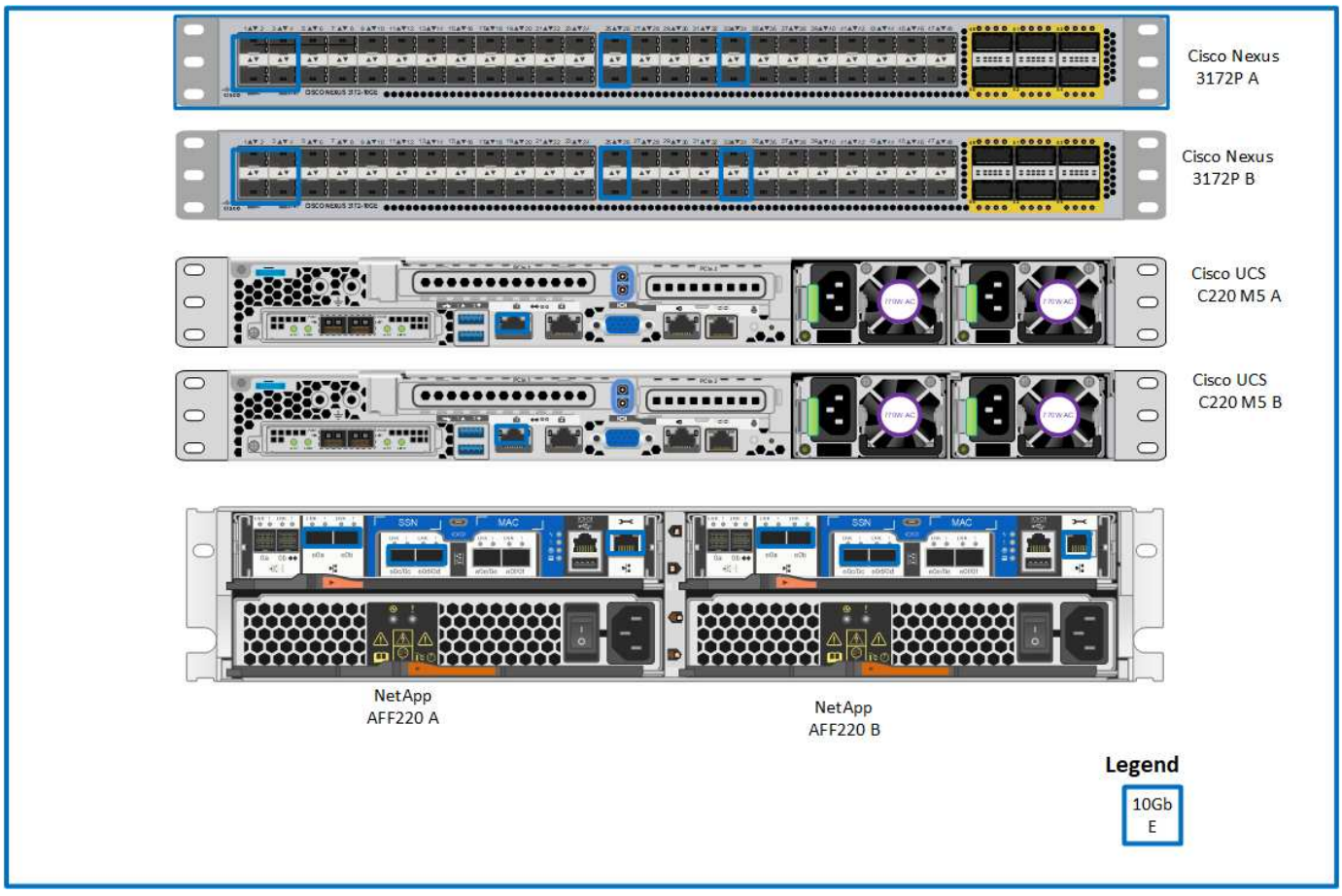
Software	Version	Details
Cisco Integrated Management Controller (CIMC)	3.1 (3g)	Für Cisco UCS C220 M5 Rack Server
Cisco Nenic-Treiber	1.0.25.0	Für VIC 1387 Schnittstellenkarten
Cisco NX-OS	nxos.7.0.3.I7.5.bin	Für Cisco Nexus 3172P-Switches
NetApp ONTAP	9.4	Für AFF A220 Controller

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.

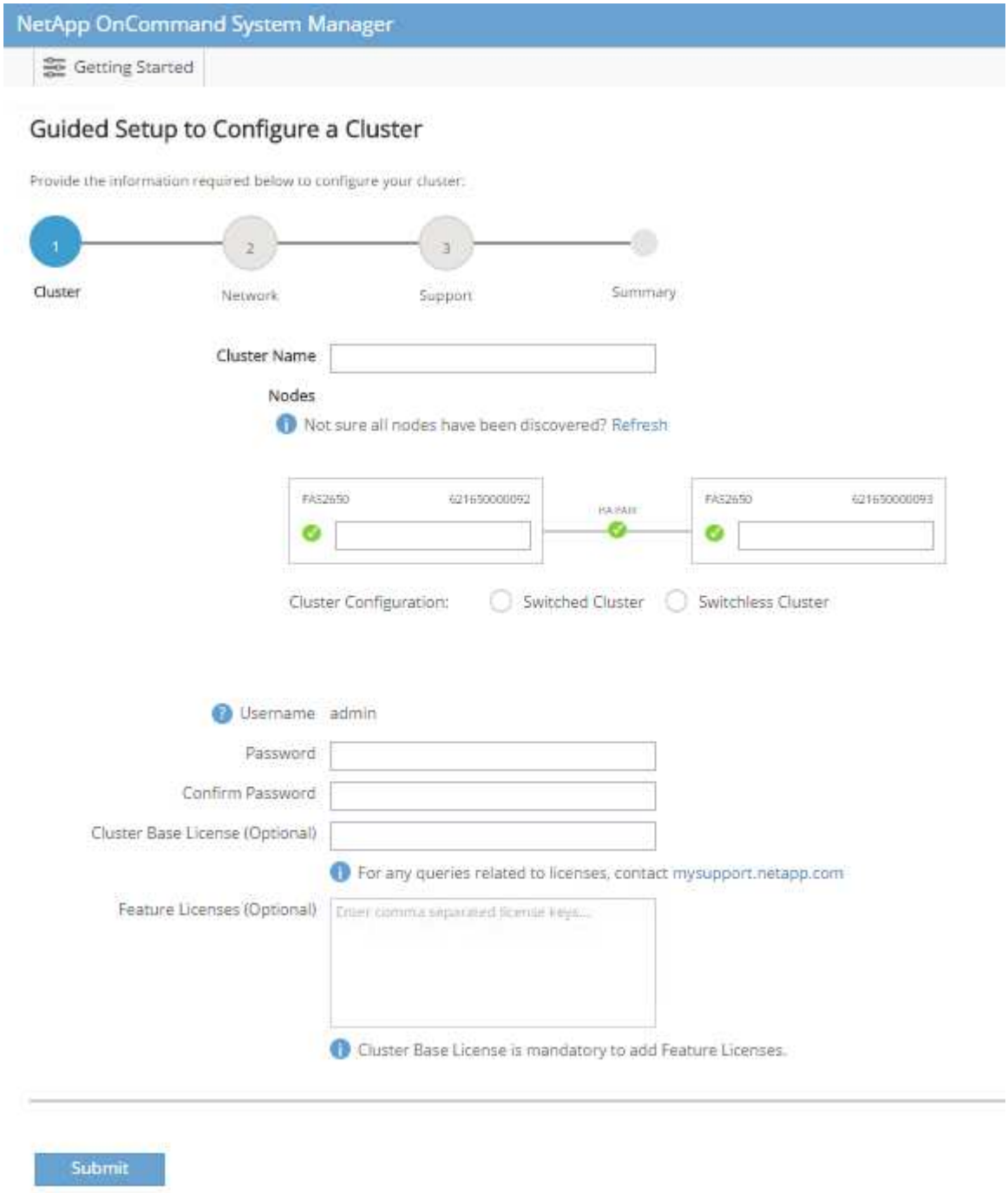
1. Befolgen Sie die Anweisungen zum Einrichten von Node A

```
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.

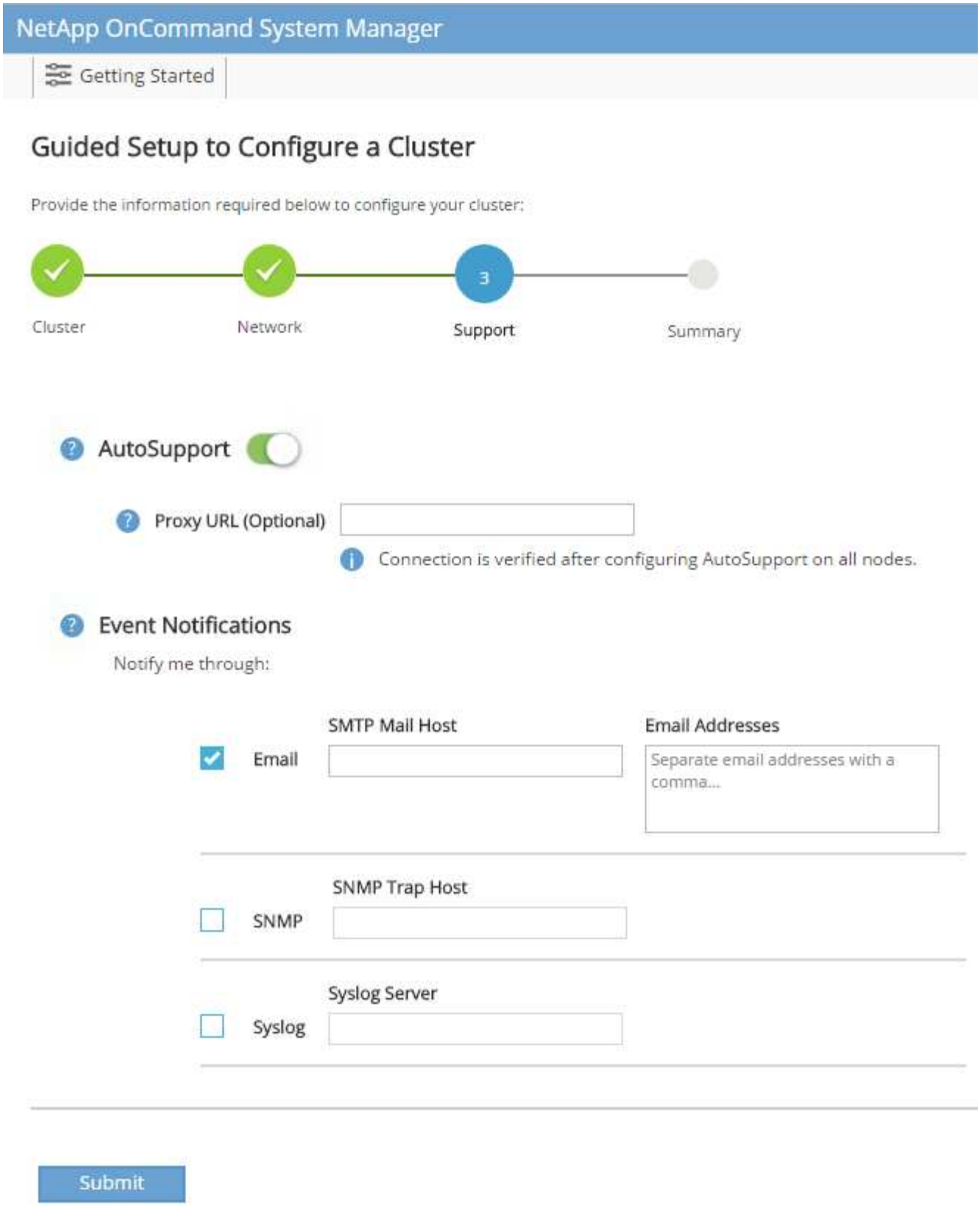
   Sie können auch einen alternativen NTP-Server eingeben.

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.

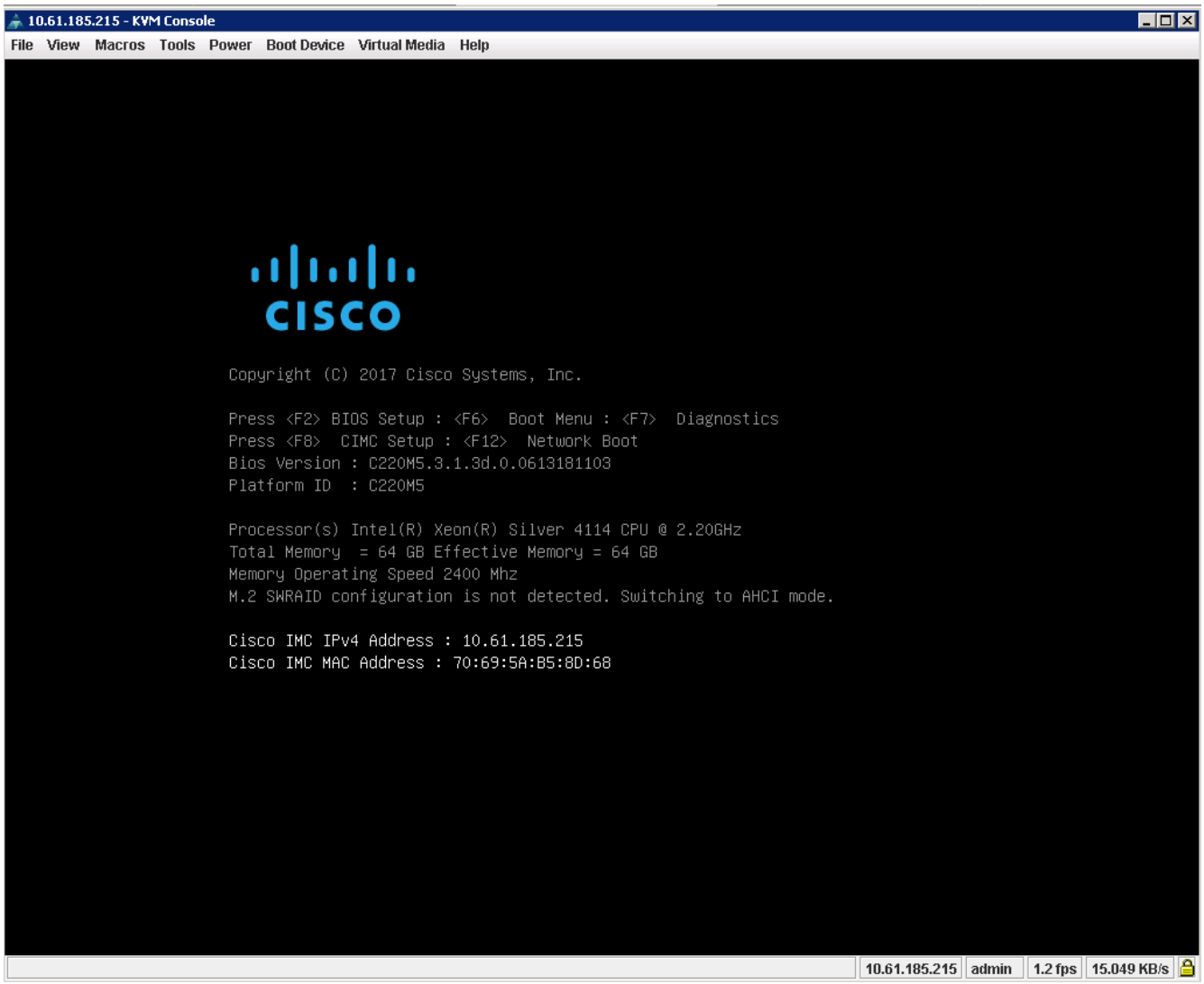
In der folgenden Tabelle sind die Informationen aufgeführt, die für die Konfiguration von CIMC für jeden Standalone-Server der Cisco UCS C-Serie erforderlich sind.

Details	Detailwert
CIMC-IP-Adresse	<<cimc_ip>>
CIMC-Subnetzmaske	<<cimc_Netzmaske>>
CIMC-Standard-Gateway	<<cimc_Gateway>>

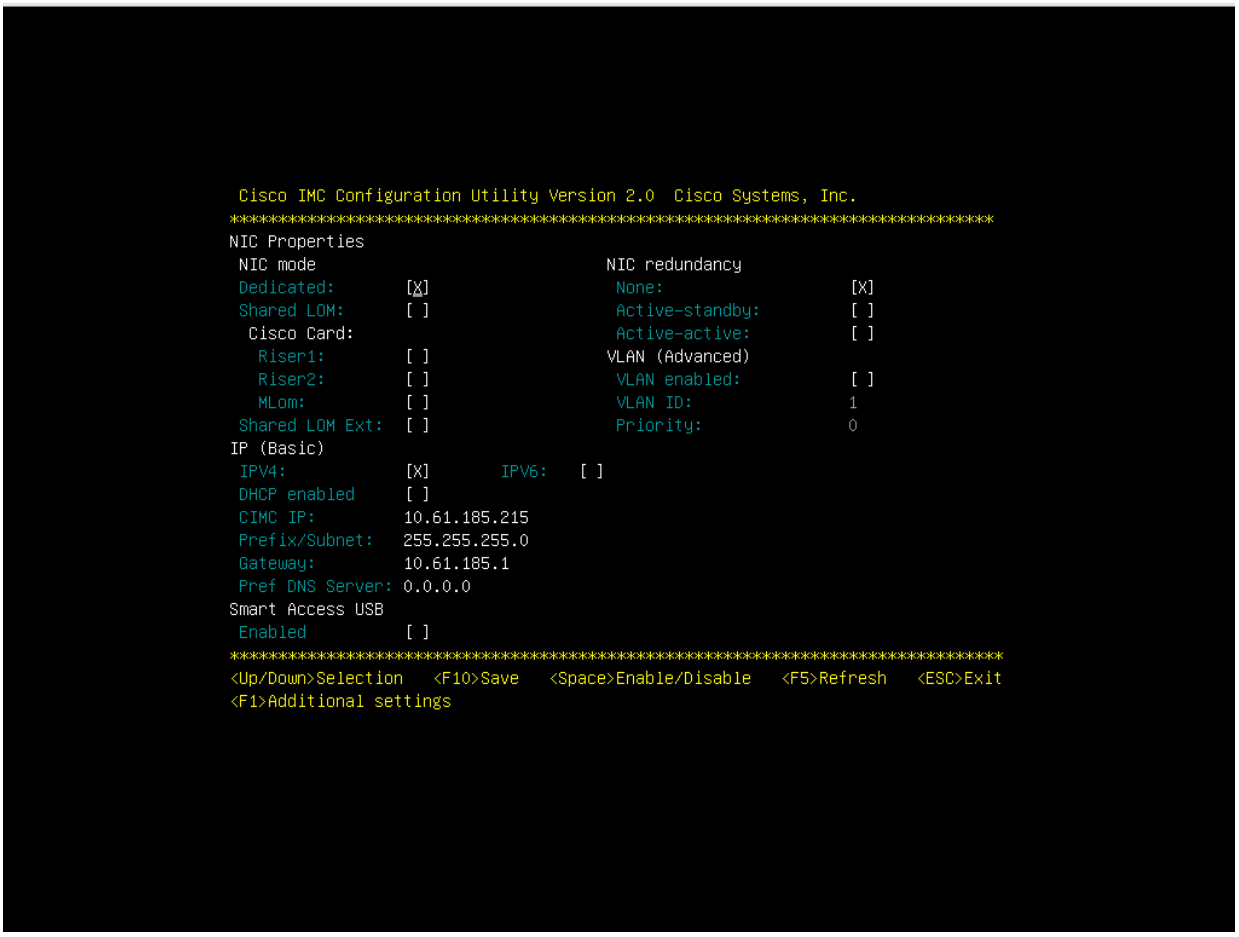
Die CIMC-Version, die in dieser Validierung verwendet wird, ist CIMC 3.1.3(g).

Alle Server

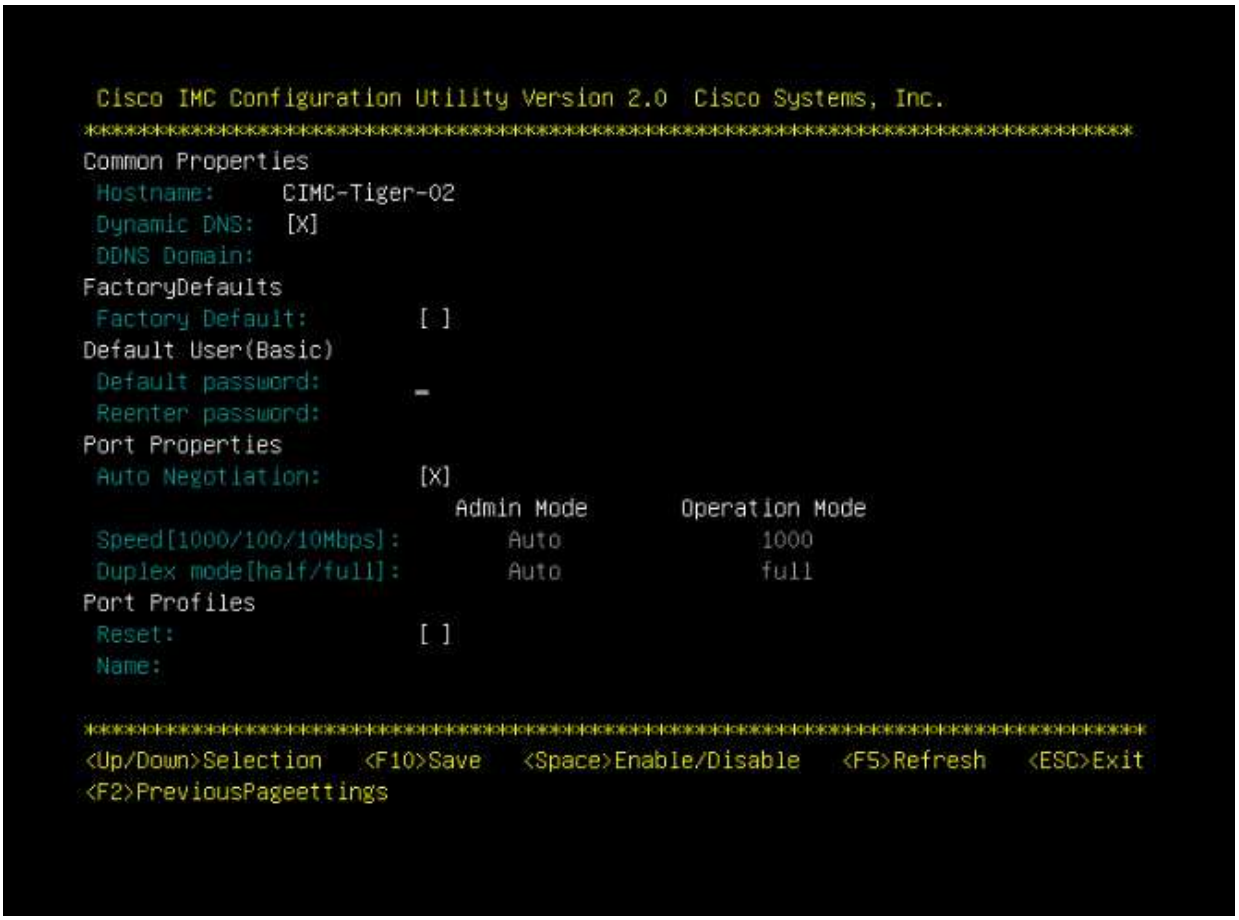
1. Schließen Sie den Cisco Keyboard-, Video- und Mausdongle (KVM) (im Lieferumfang des Servers enthalten) an den KVM-Port an der Vorderseite des Servers an. Schließen Sie einen VGA-Monitor und eine USB-Tastatur an die entsprechenden KVM-Dongle-Ports an.
2. Schalten Sie den Server ein, und drücken Sie 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.

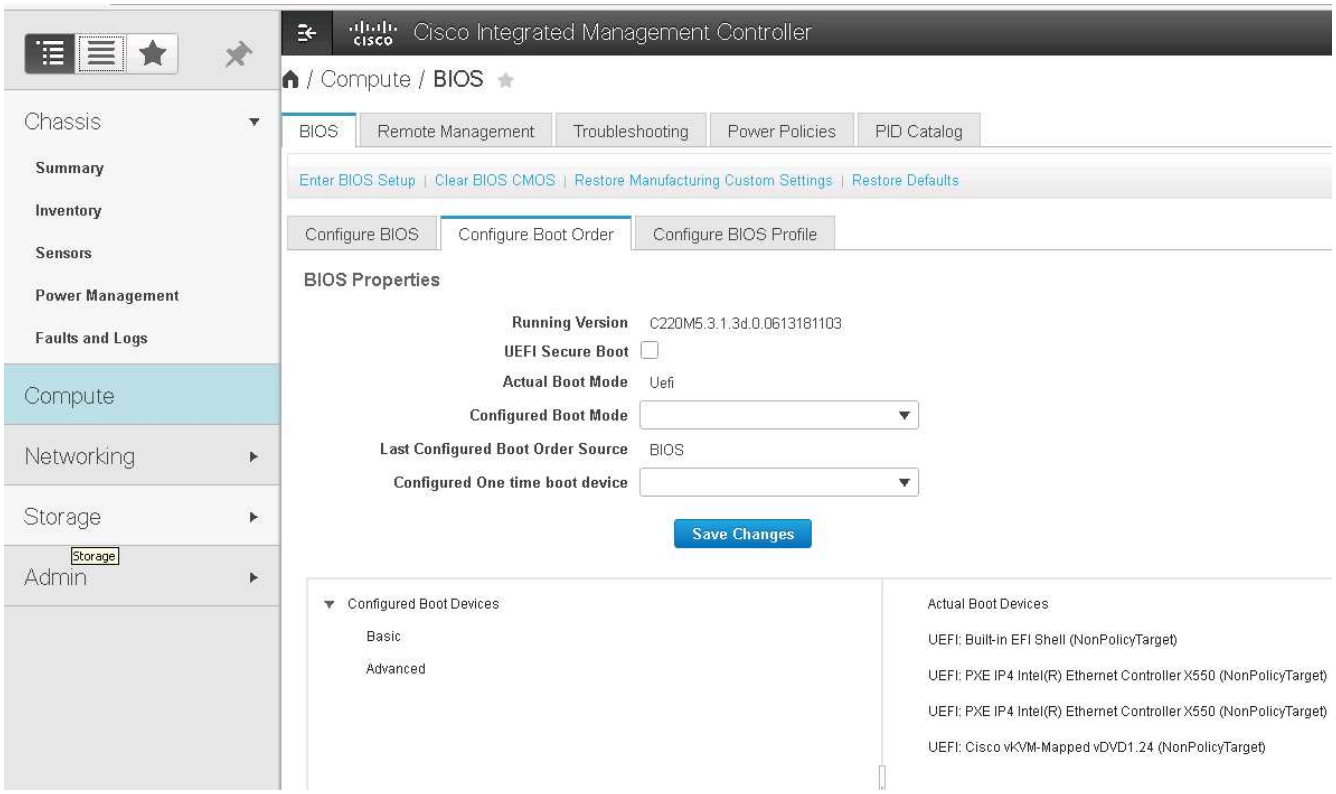
Details	Detailwert
ESXi Host-Initiator Ein Name	<<var_ucs_Initiator_Name_A>>
ESXi Host, iSCSI A IP	<<var_esxi_Host_iscsiA_ip>>
ESXi-Host, iSCSI-A-Netzwerkmaske	<<var_esxi_Host_iscsiA_Maska>>
ESXi Host iSCSI Ein Standard-Gateway	\<<var_esxi_Host_iscsiA_Gateway>
ESXi Host-Initiator B-Name	\<<var_ucs_Initiator_Name_B>
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.



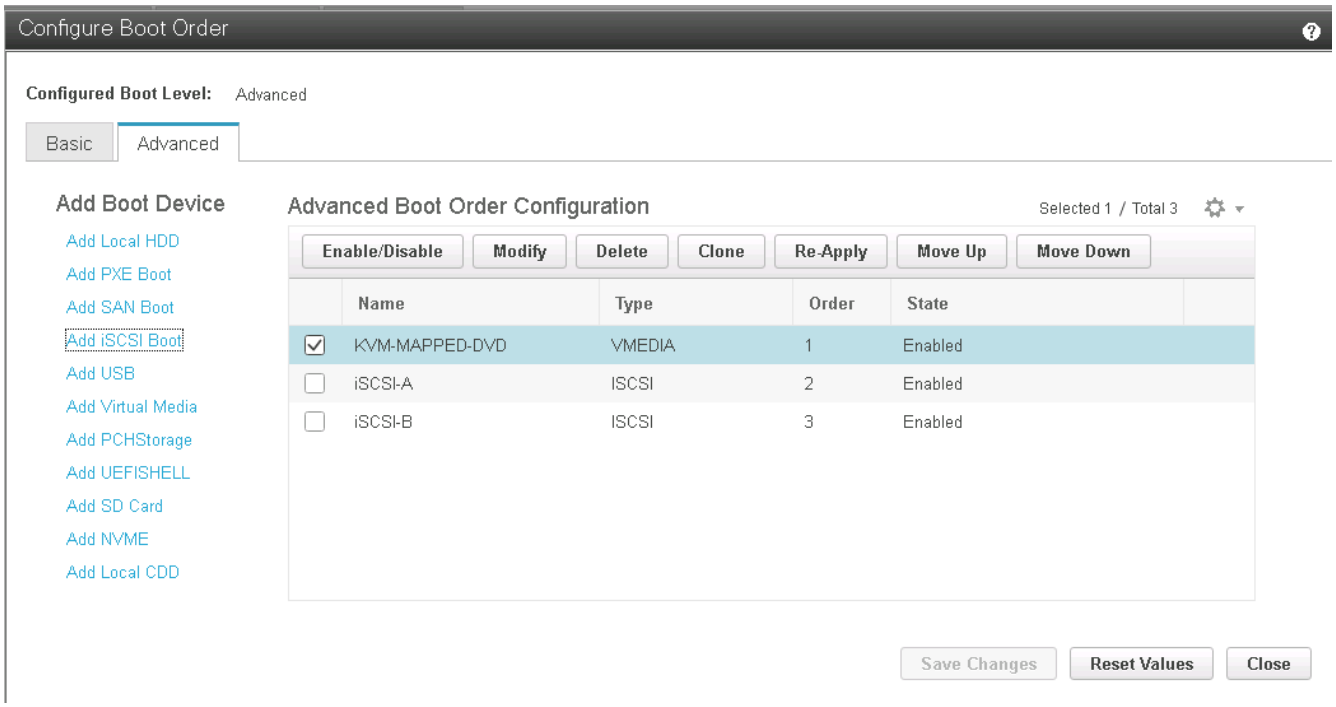
3. Konfigurieren Sie die folgenden Geräte, indem Sie unter Startgerät hinzufügen auf das Gerät klicken und zur Registerkarte Erweitert wechseln.
   - Fügen Sie Einen Virtuellen Datenträger Hinzu
     - NAME: KVM-CD-DVD
     - UNTERTYP: KVM GEMAPPTEN DVD
     - Status: Aktiviert
     - Bestellung: 1
   - 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.

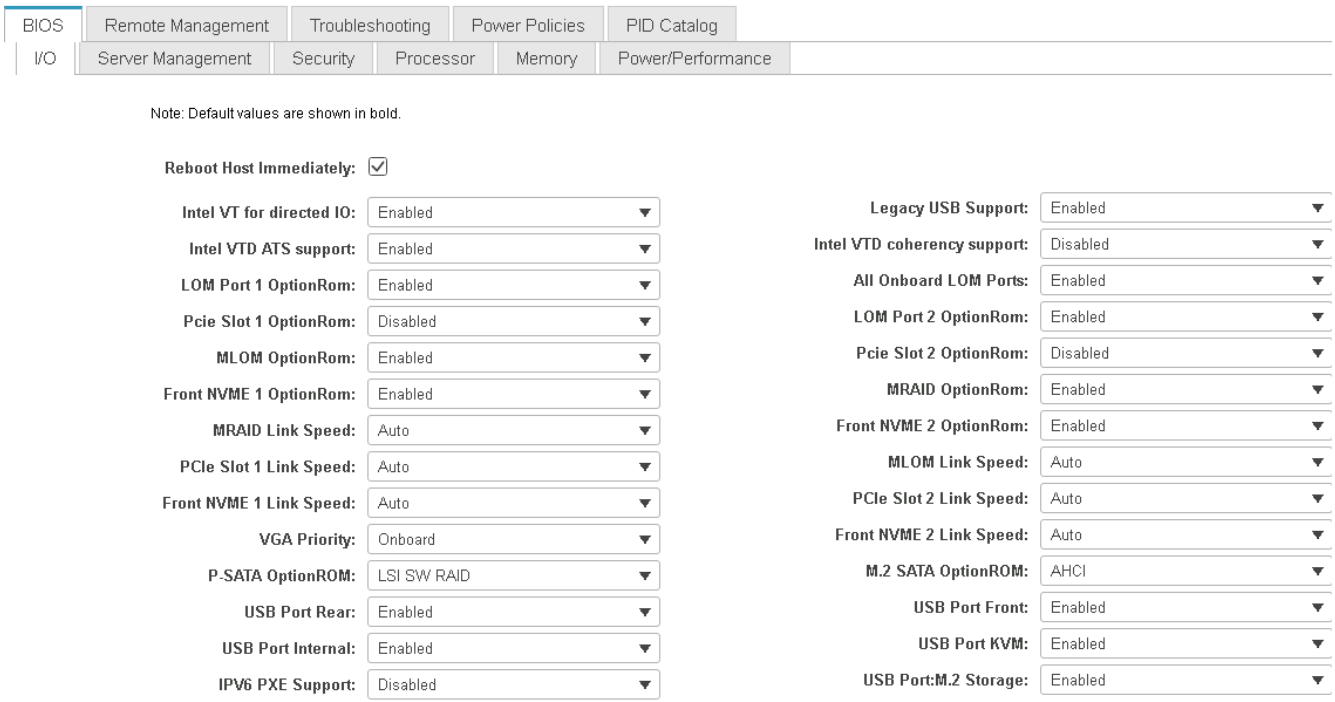


6. Starten Sie den Server neu, um mit Ihrer neuen Startreihenfolge zu starten.

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.



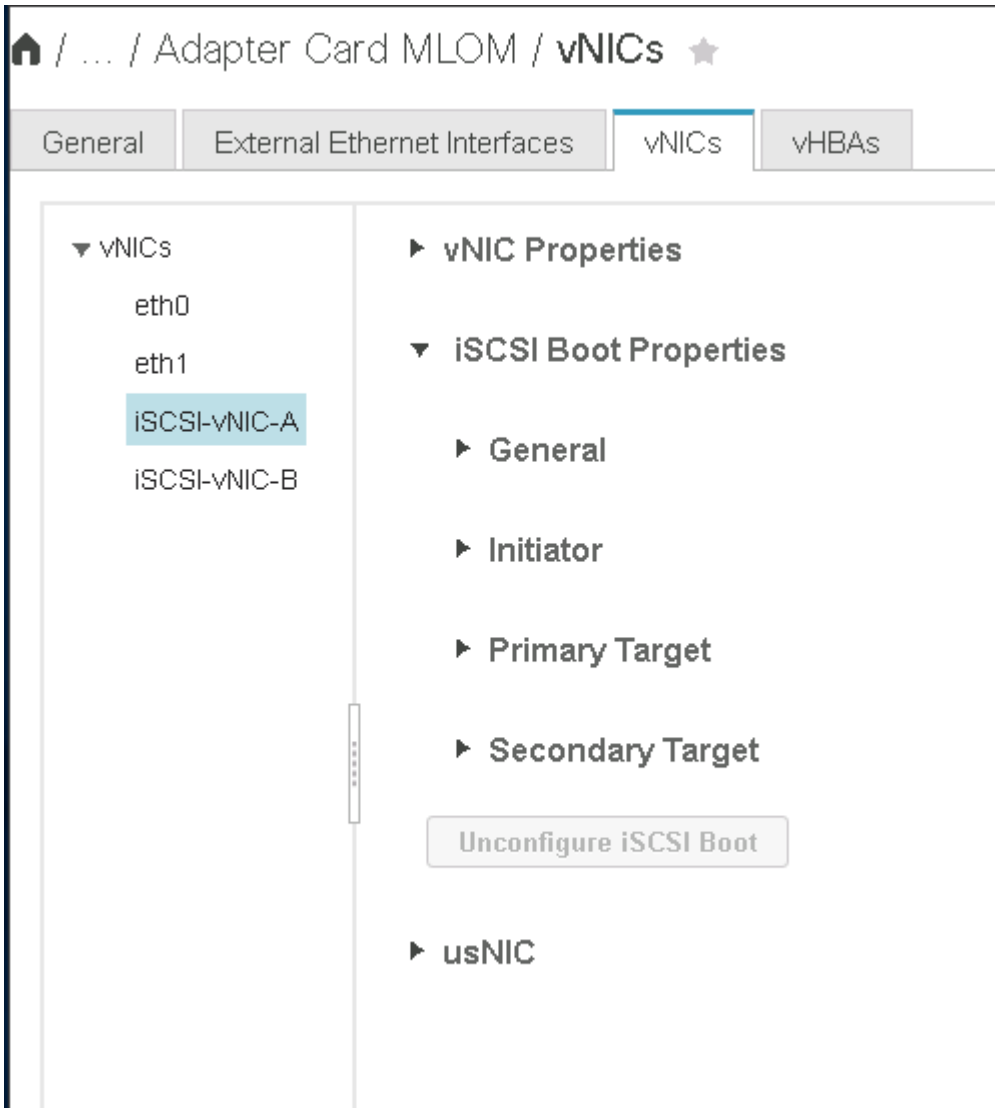
Konfigurieren Sie Cisco VIC1387 für iSCSI Boot

Die folgenden Konfigurationsschritte gelten für den Cisco VIC 1387 für iSCSI Boot.

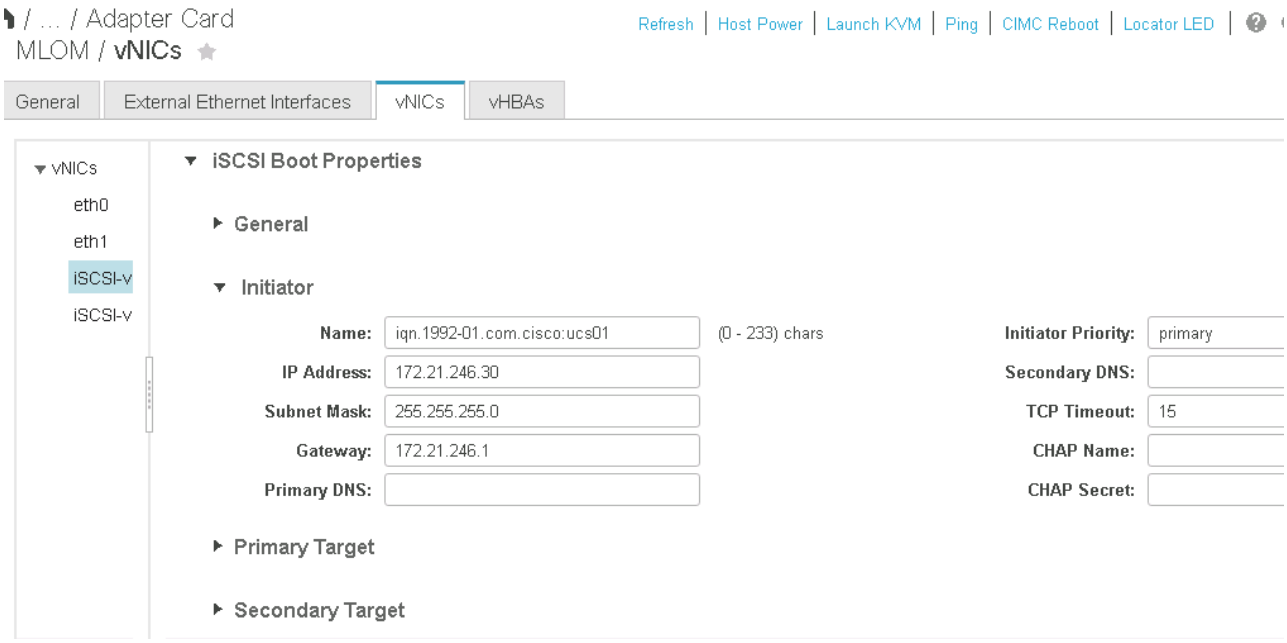
Erstellen von iSCSI-vNICs

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.



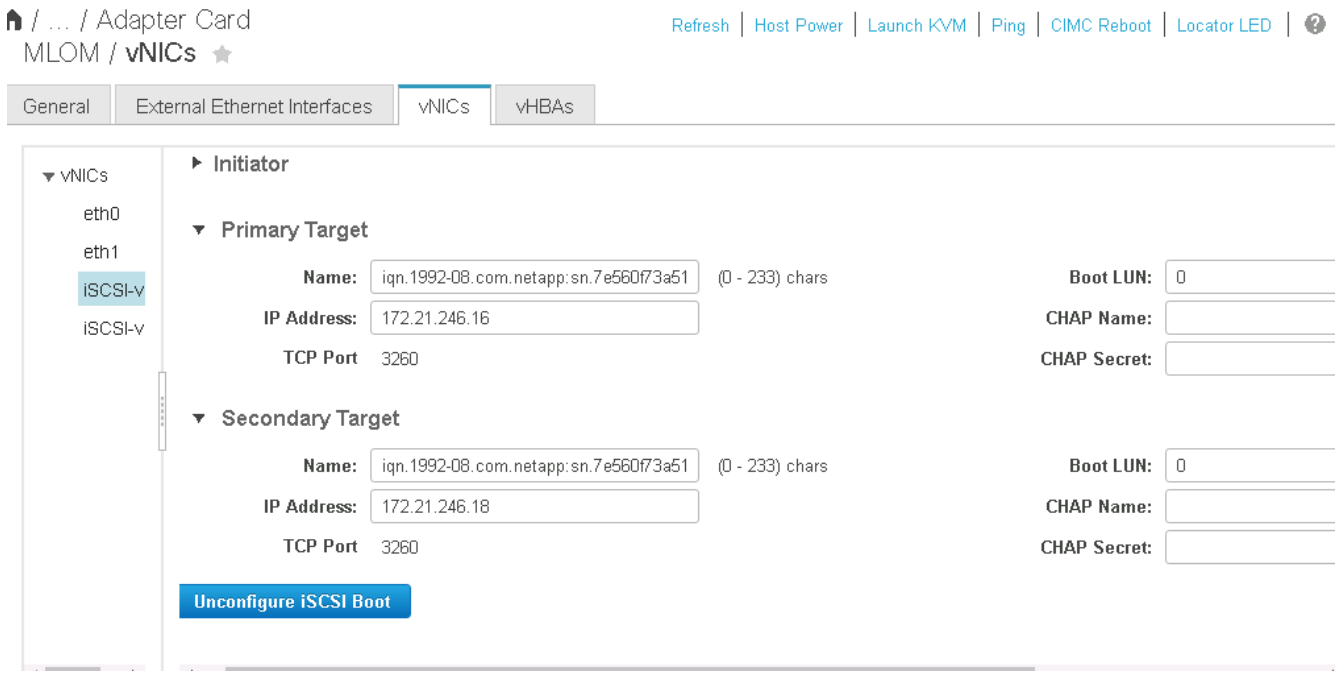
6. Geben Sie unter iSCSI Boot Properties die Initiator-Details ein:
   - Name: <<var_ucsa_Initiator_Name_a>>
   - IP-Adresse: <<var_esxi_hostA_iscsiA_ip>>
   - Subnetzmaske: <<var_esxi_hostA_iscsiA_maska>>
   - Gateway: <<var_esxi_hostA_iscsiA_Gateway>>



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

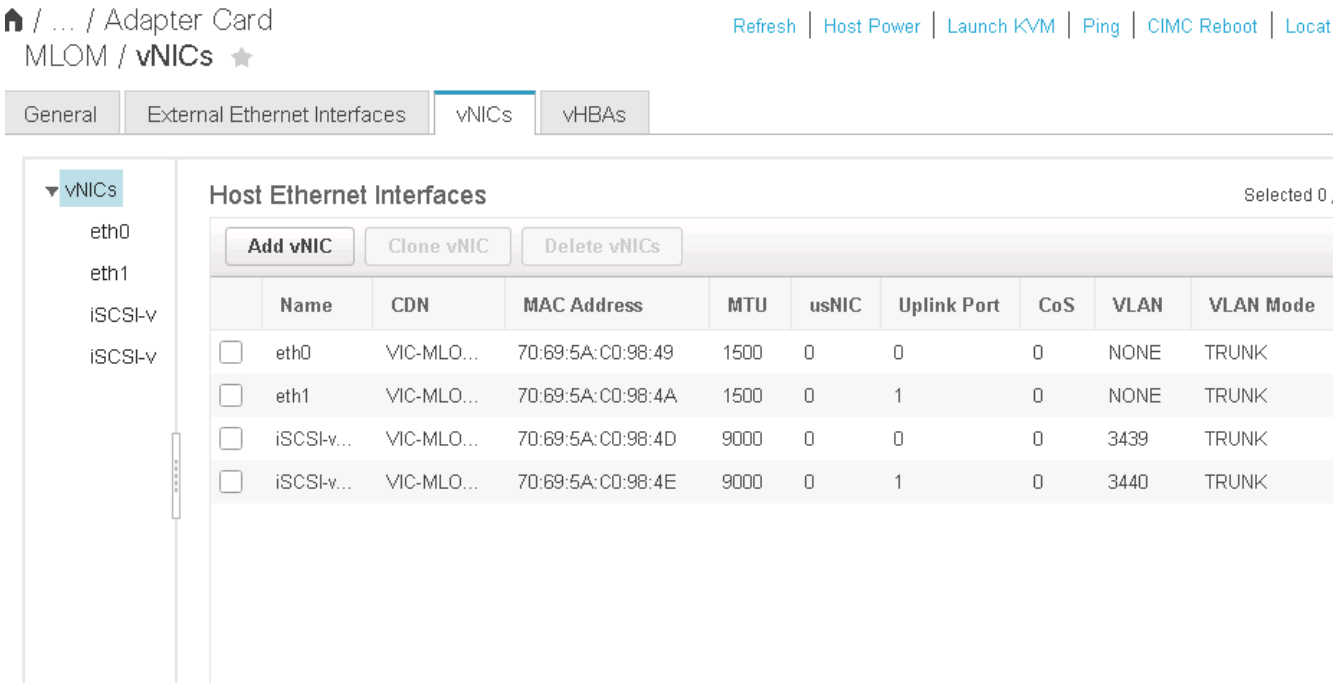
    Sie können die Speicher-IQN-Nummer mit dem abrufen `vserver iscsi show` Befehl.

    Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.
15. Klicken Sie auf ISCSI konfigurieren.

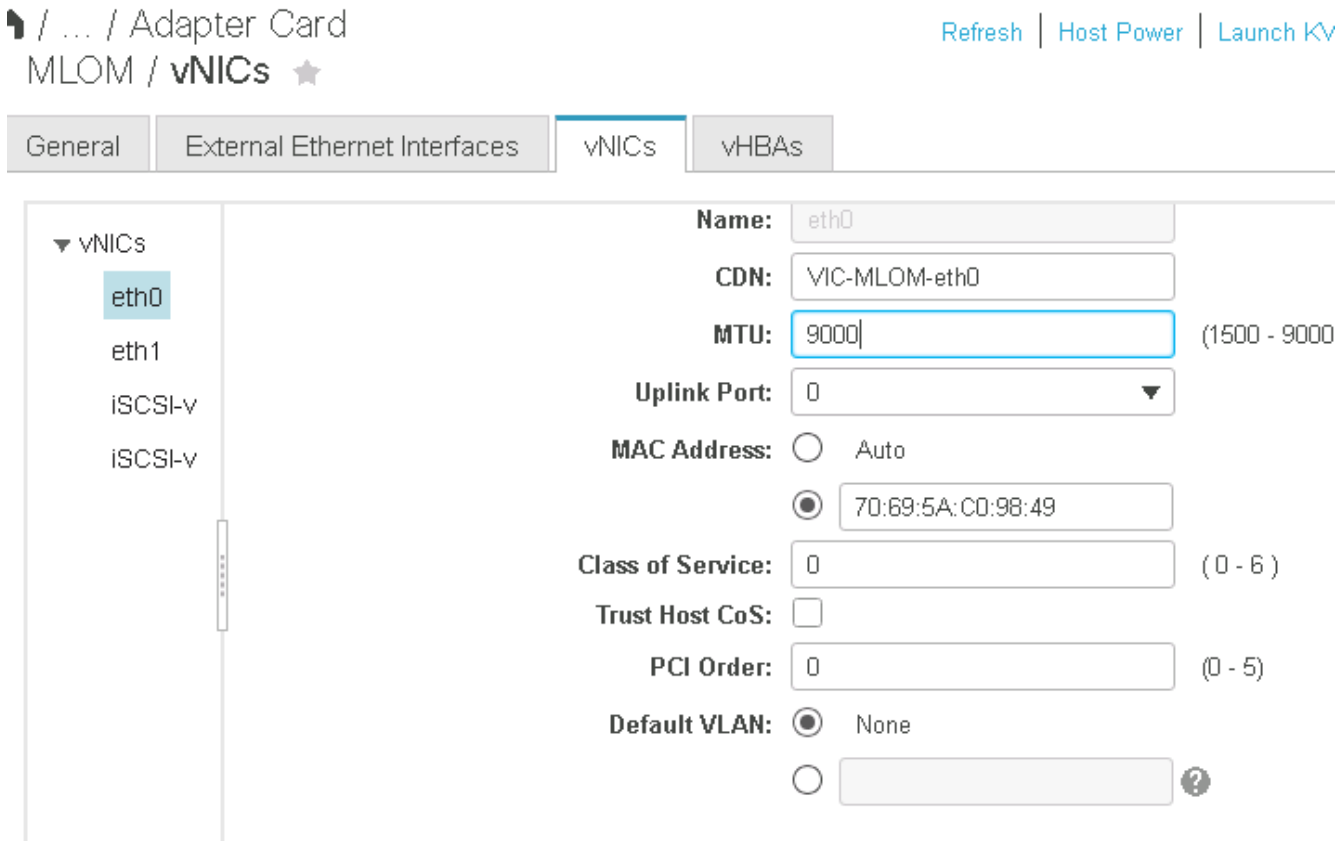
16. Wiederholen Sie diesen Vorgang, um iSCSI-Boot für Cisco UCS-Server B zu konfigurieren

Konfigurieren Sie vNICs für ESXi

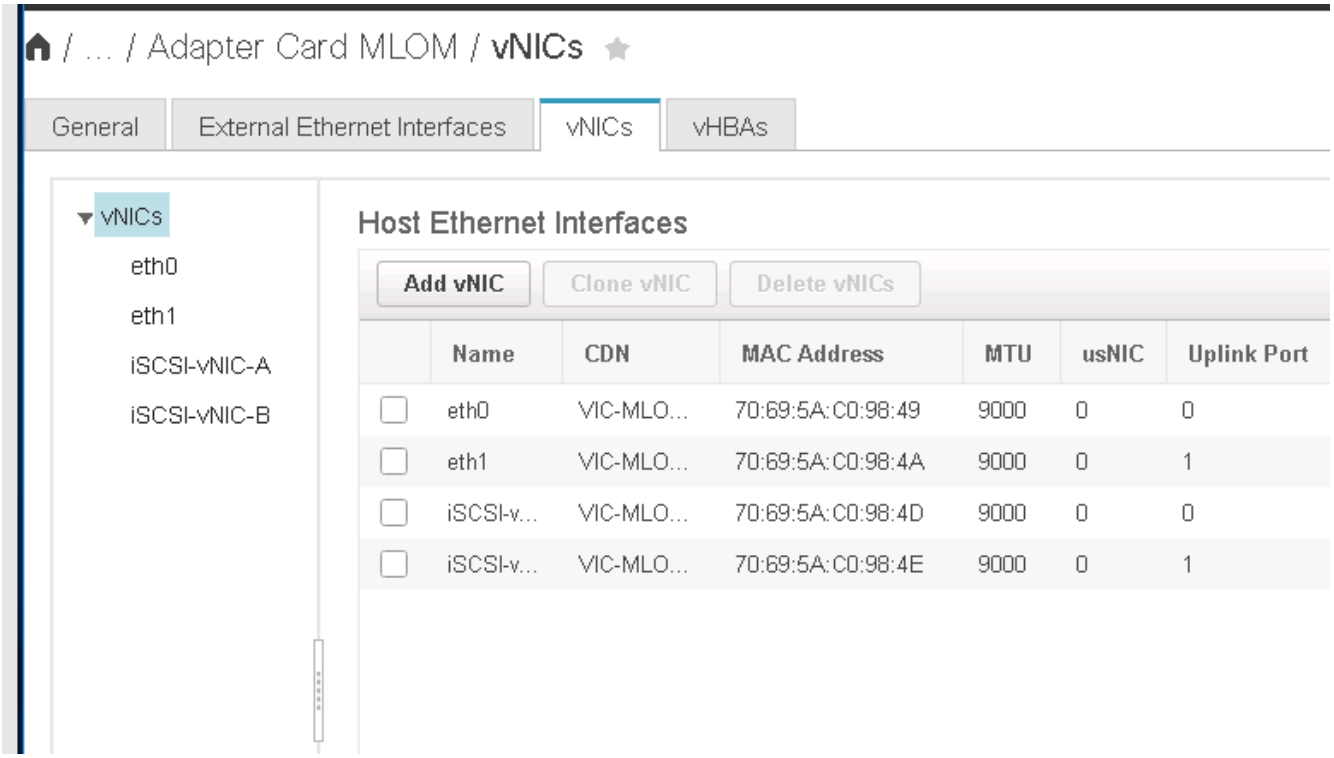
1. Klicken Sie im CIMC-Schnittstellenbrowser-Fenster auf Inventar und anschließend im rechten Fensterbereich auf Cisco VIC-Adapter.
2. Wählen Sie unter Adapterkarten Cisco UCS VIC 1387 aus und wählen Sie dann die darunter liegende vNICs aus.



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.

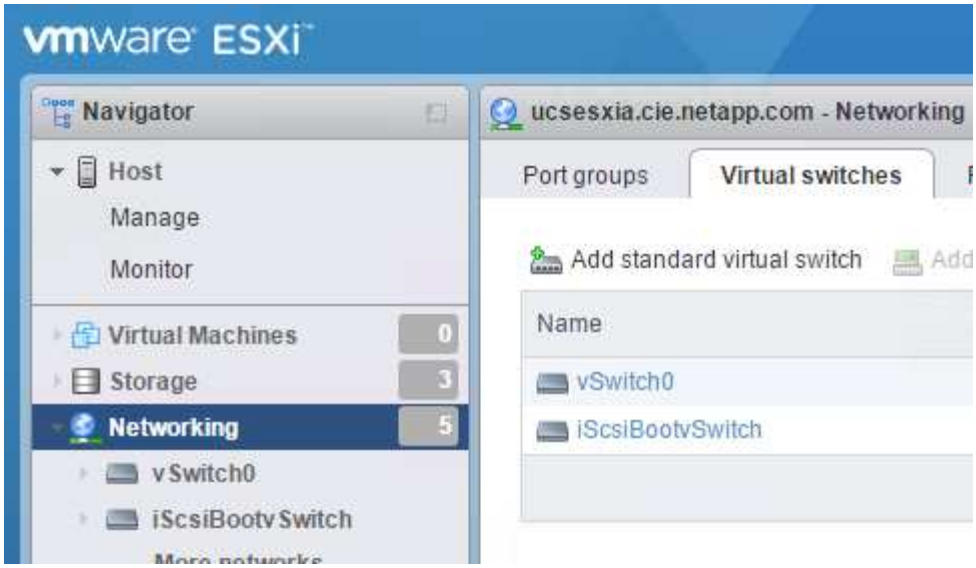
Details	Wert
ESXi Hostname	
ESXi Host-Management-IP	
ESXi Host-Managementmaske	
ESXi Host-Management-Gateway	
ESXi Host, NFS-IP	
ESXi Host-NFS-Maske	
ESXi Host-NFS-Gateway	
ESXi Host vMotion IP	
ESXi Host vMotion Maske	
ESXi Host vMotion Gateway	
ESXi Host, iSCSI A IP	
ESXi Host iSCSI-A-Maske	
ISCSI-A-Gateway 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.

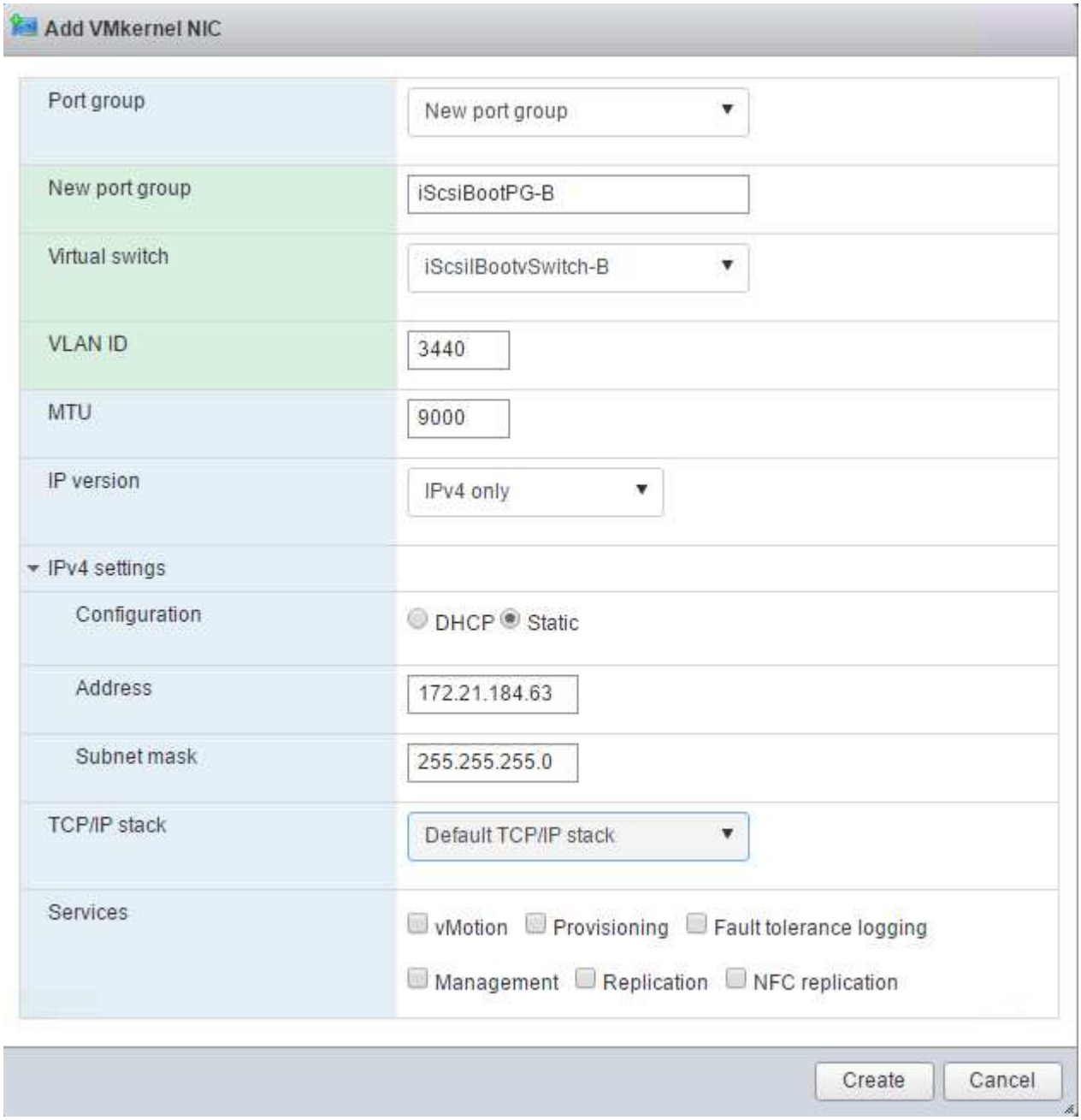


3. Klicken Sie auf iScsiBootvSwitch.
4. Wählen Sie Einstellungen bearbeiten aus.
5. Ändern Sie die MTU in 9000, und klicken Sie auf Speichern.
6. Klicken Sie im linken Navigationsbereich auf Netzwerk, um zur Registerkarte Virtuelle Switches zurückzukehren.
7. Klicken Sie Auf Standard-Virtuellen Switch 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 .

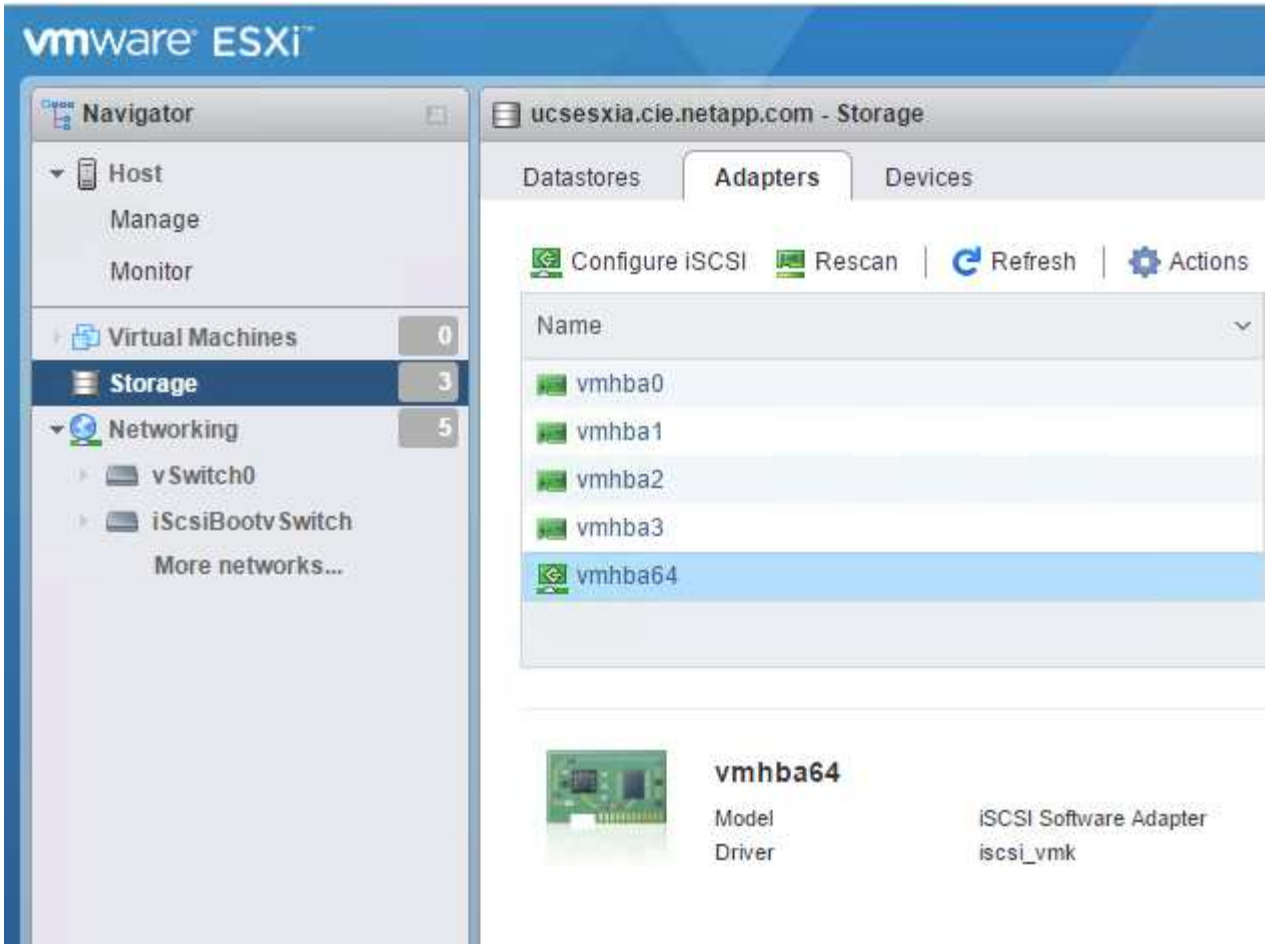


Setzen Sie die MTU auf 9000 auf `iScsiBootPG- A.`

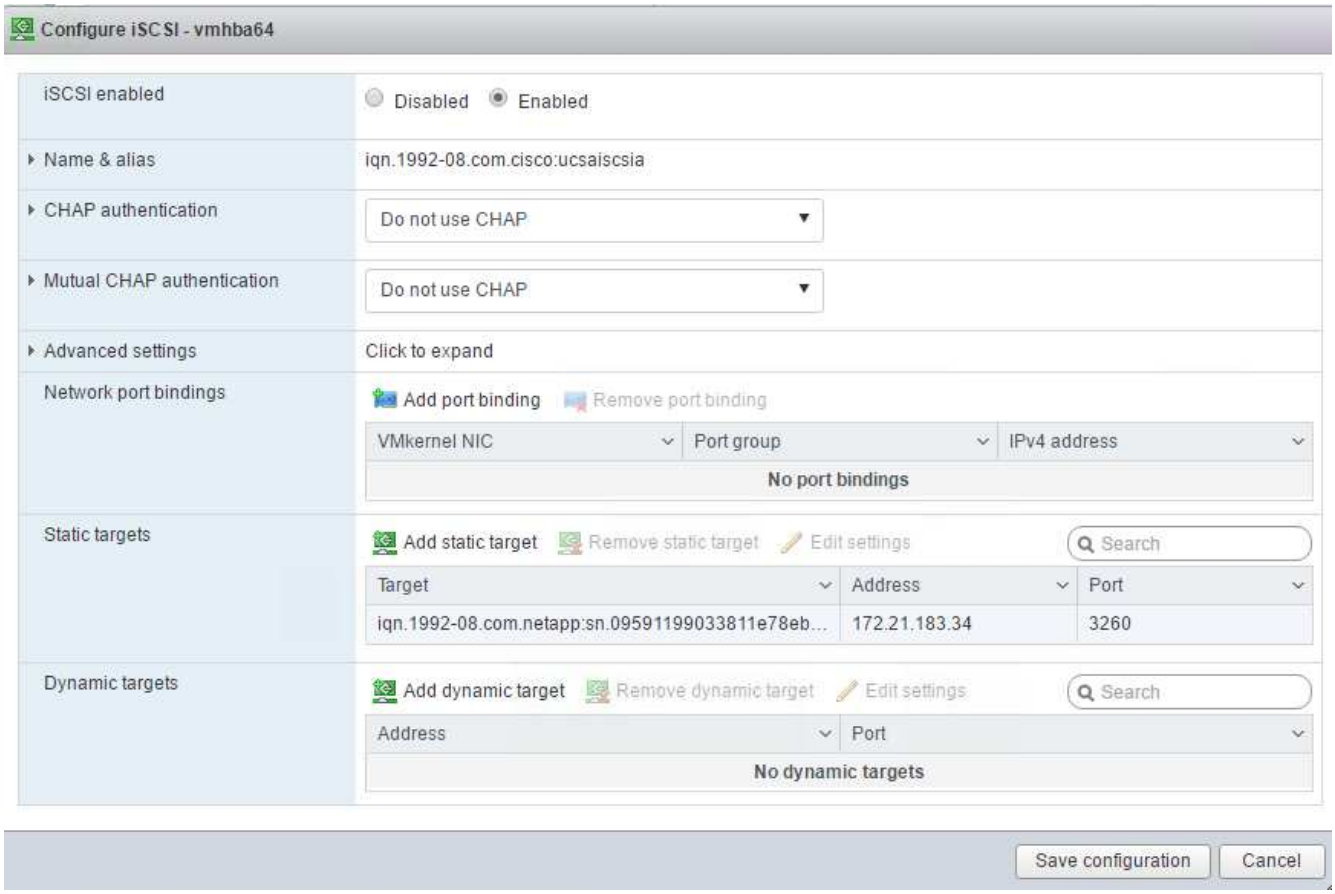
Konfigurieren Sie iSCSI-Multipathing

Gehen Sie wie folgt vor, um iSCSI-Multipathing auf den ESXi-Hosts einzurichten:

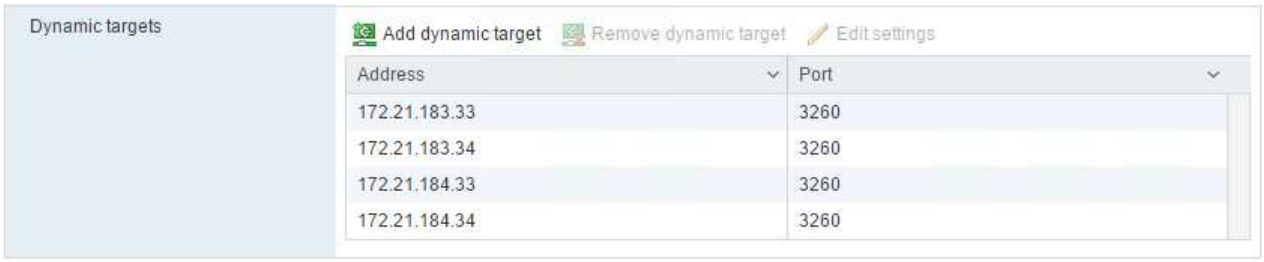
1. Wählen Sie im linken Navigationsbereich Storage aus. Klicken Sie Auf Adapter.
2. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf iSCSI konfigurieren.



3. Klicken Sie unter dynamische Ziele auf dynamische Ziele hinzufügen.



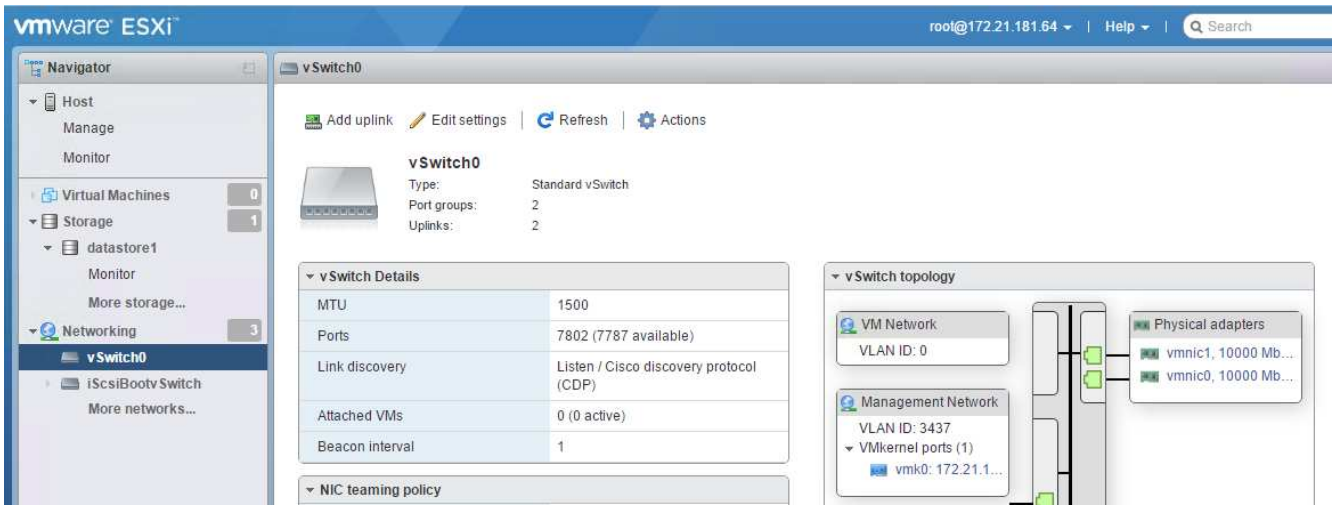
4. Geben Sie die IP-Adresse ein `iscsi_lif01a`.
   - Wiederholen Sie diesen Vorgang mit den IP-Adressen `iscsi_lif01b`, `iscsi_lif02a`, und `iscsi_lif02b`.
   - Klicken Sie Auf Konfiguration Speichern.



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.

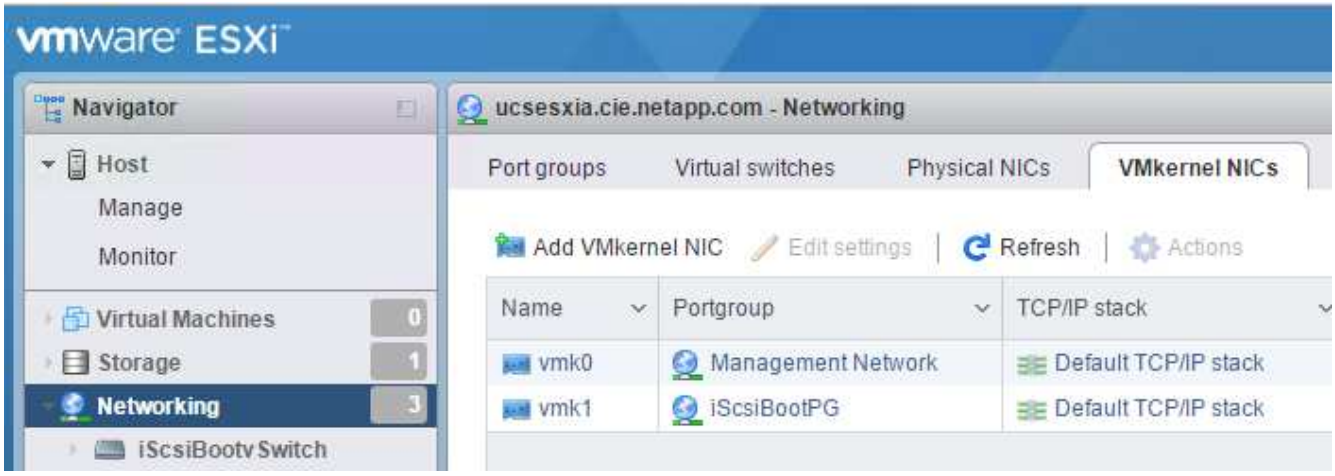
Konfigurieren Sie die Portgruppen und VMkernel NICs

1. Wählen Sie im linken Navigationsbereich die Option Netzwerk.
2. Klicken Sie mit der rechten Maustaste auf die Registerkarte Portgruppen.

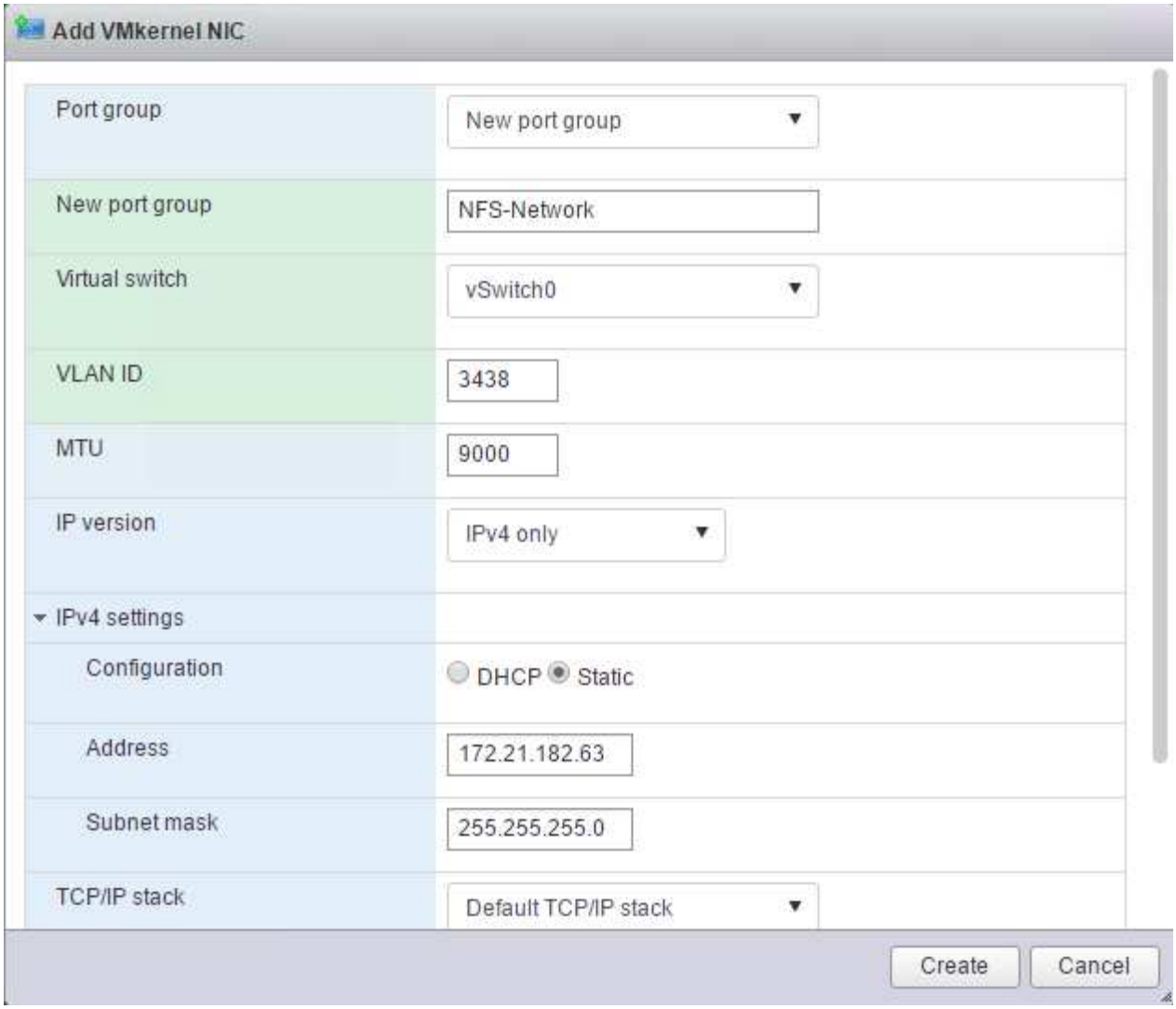
3. Klicken Sie mit der rechten Maustaste auf VM Network, und wählen Sie Bearbeiten aus. Ändern Sie die VLAN-ID in `<<var_vm_traffic_vlan>>`.
4. Klicken Sie Auf Portgruppe Hinzufügen.
   - Benennen Sie die Portgruppe `MGMT-Network`.
   - Eingabe `<<mgmt_vlan>>` Für die VLAN-ID.
   - Stellen Sie sicher, dass vSwitch0 ausgewählt ist.

- Klicken Sie Auf Hinzufügen.

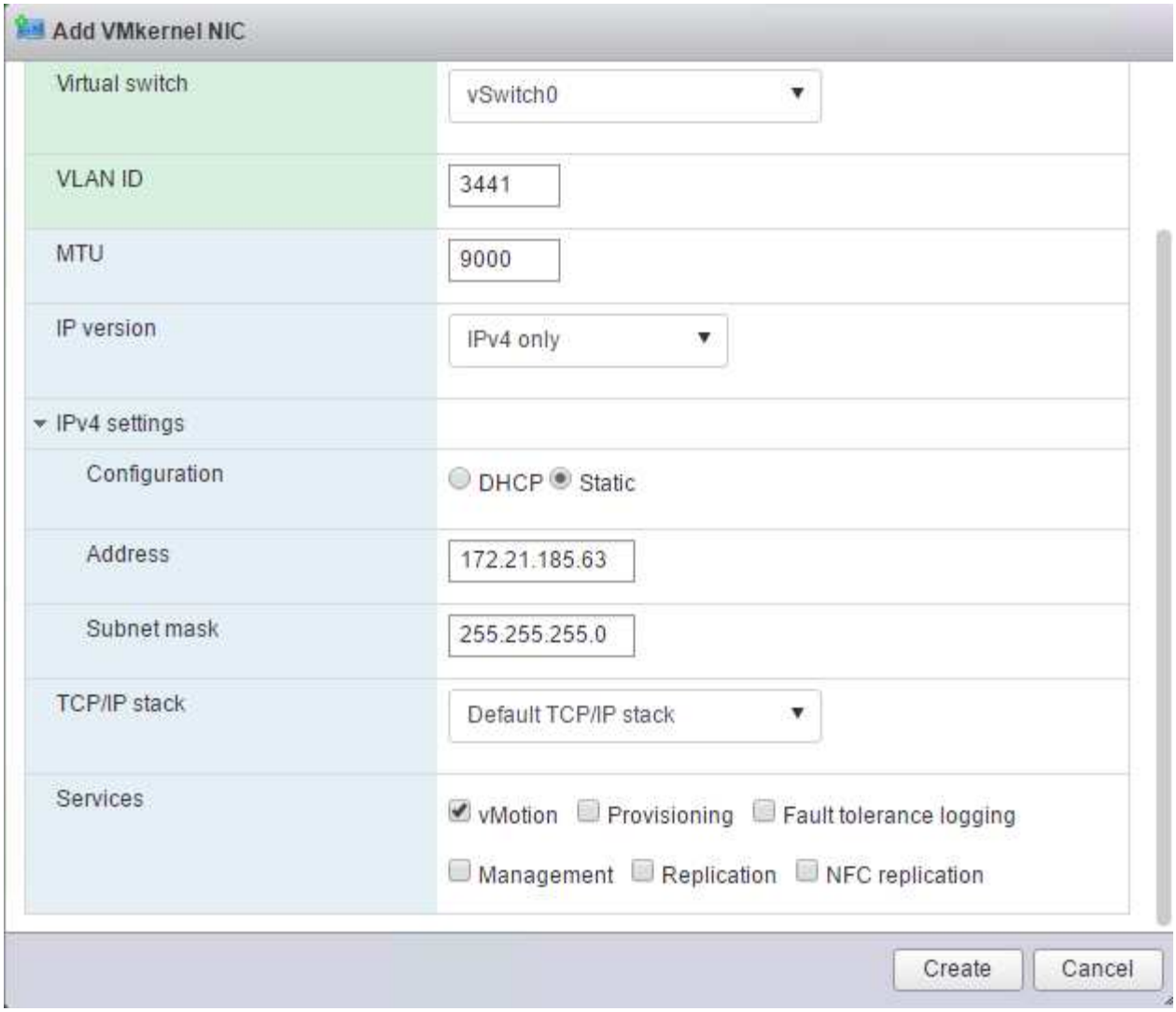
5. Klicken Sie auf die Registerkarte VMkernel NICs.



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.

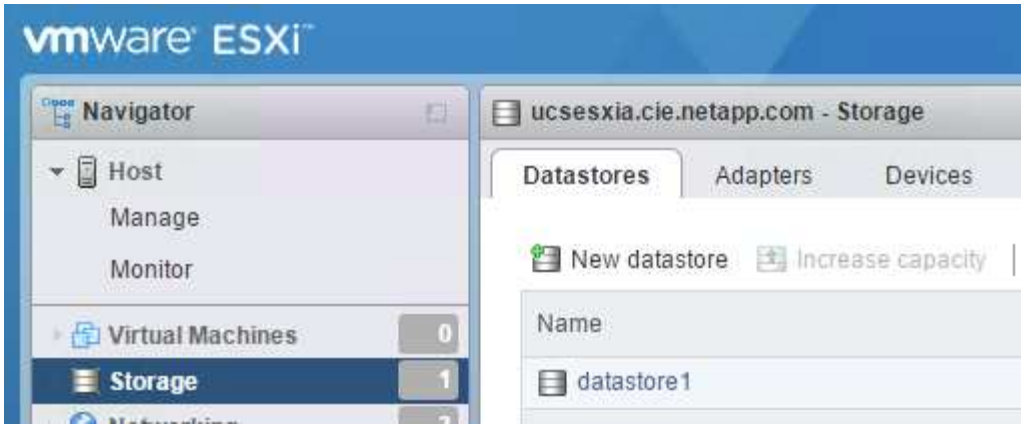


Es gibt viele Möglichkeiten, ESXi Networking zu konfigurieren, einschließlich der Verwendung des VMware vSphere Distributed Switches, wenn Ihre Lizenzierung es zulässt. In FlexPod Express werden alternative Netzwerkkonfigurationen unterstützt, wenn sie zur Erfüllung der geschäftlichen Anforderungen erforderlich sind.

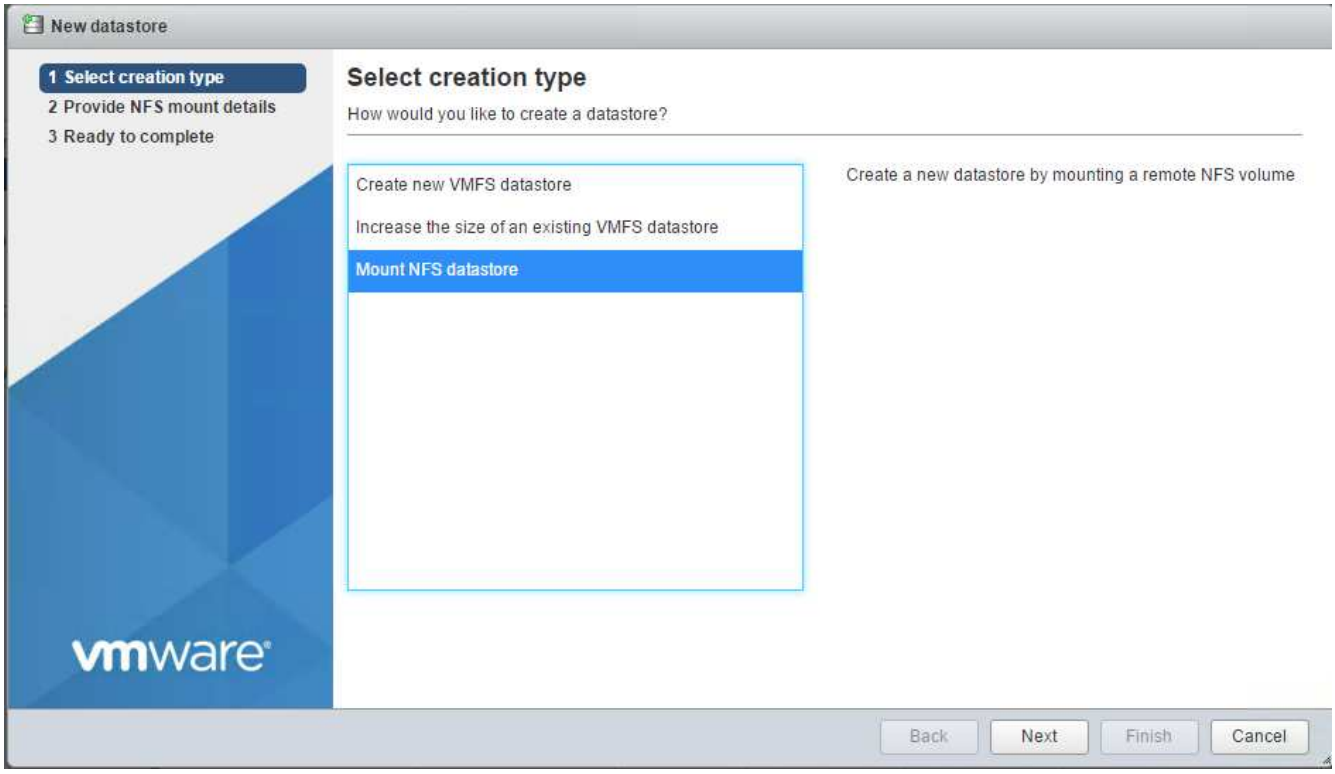
Erste Datastores mounten

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.



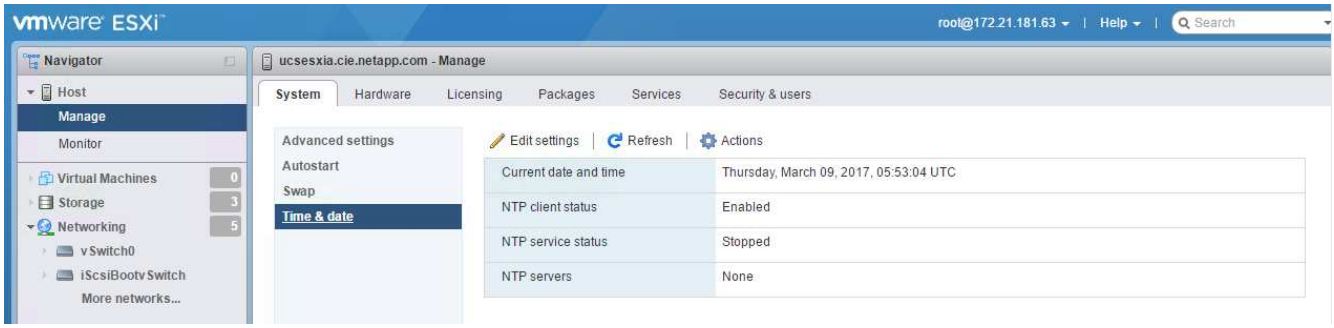
3. Geben Sie als Nächstes die folgenden Informationen auf der Seite „NFS Mount Details angeben“ ein:
   - Name: `infra_datastore_1`
   - NFS-Server: `<<var_nodea_nfs_lif>>`
   - Freigabe: /Infra_Datastore_1
   - Stellen Sie sicher, dass NFS 3 ausgewählt ist.
4. Klicken Sie Auf Fertig Stellen. Die Aufgabe 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.

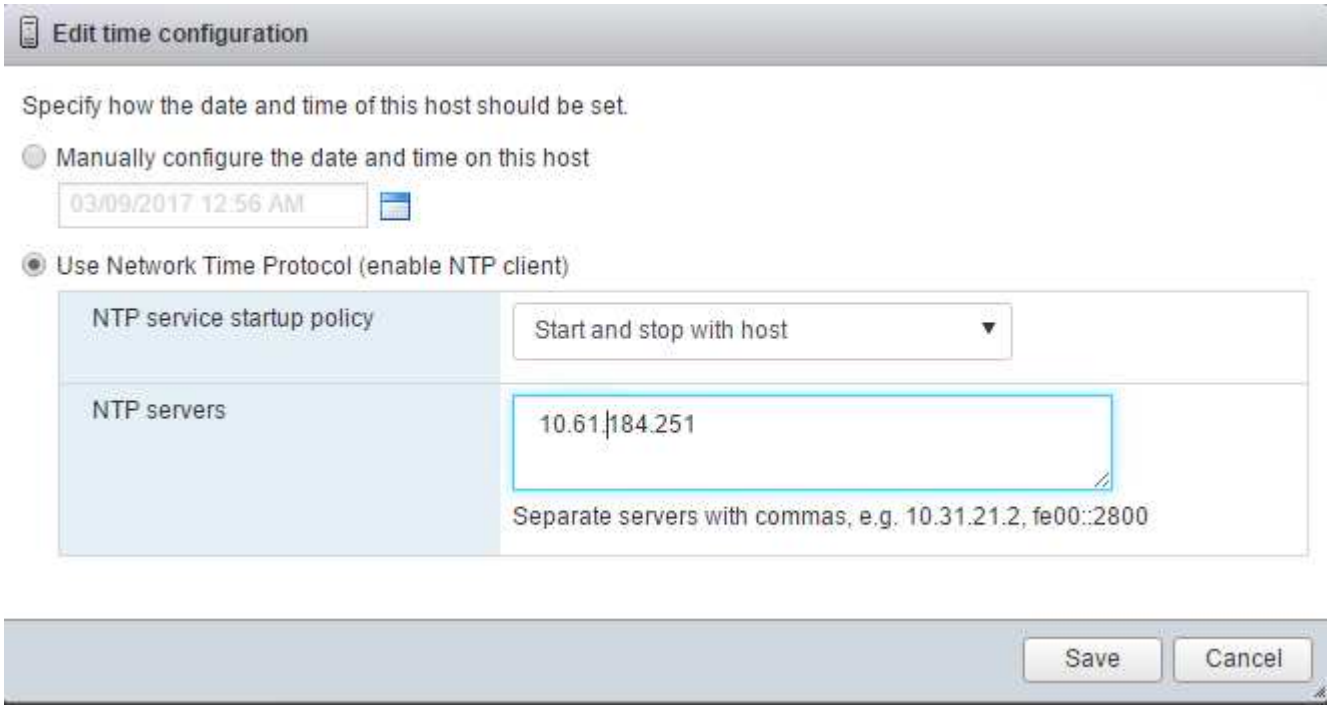
Konfigurieren Sie NTP

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.



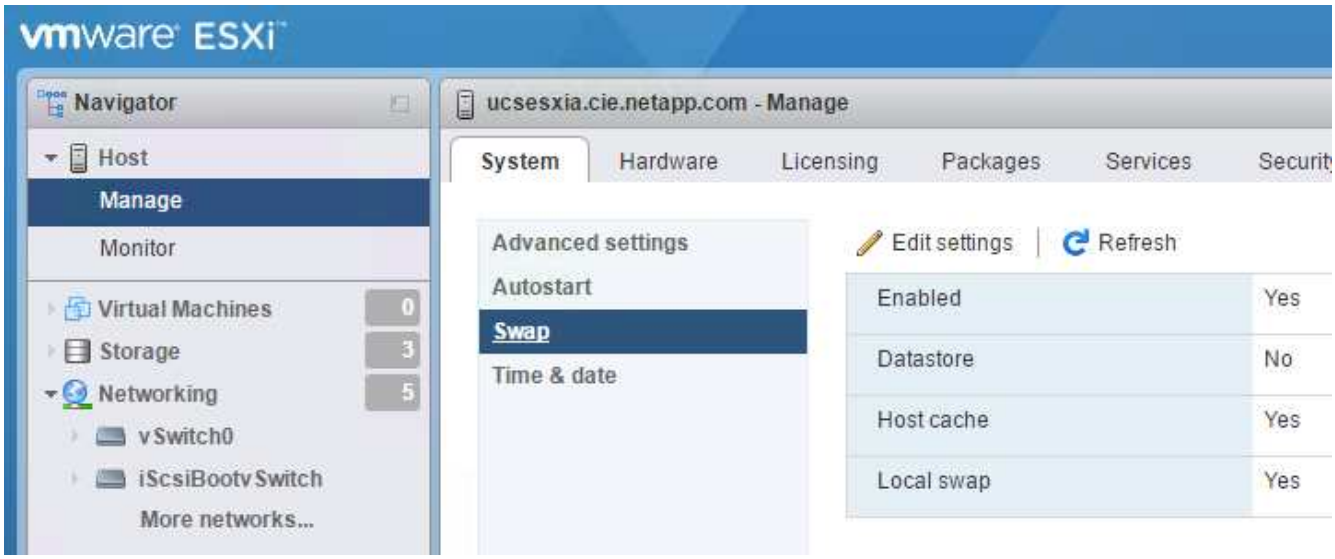
2. Wählen Sie Network Time Protocol (Network Time Protocol verwenden) (NTP Client aktivieren) aus.
3. Wählen Sie Start und Stopp mit Host als Startrichtlinie für den NTP-Dienst aus.
4. Eingabe `<<var_ntp>>` Als NTP-Server. Sie können mehrere NTP-Server festlegen.
5. Klicken Sie auf Speichern .



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"

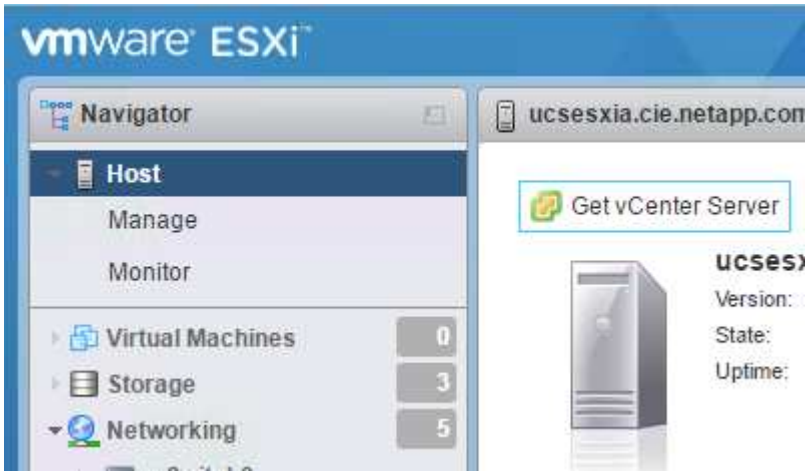
Installieren Sie VMware vCenter Server 6.7

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

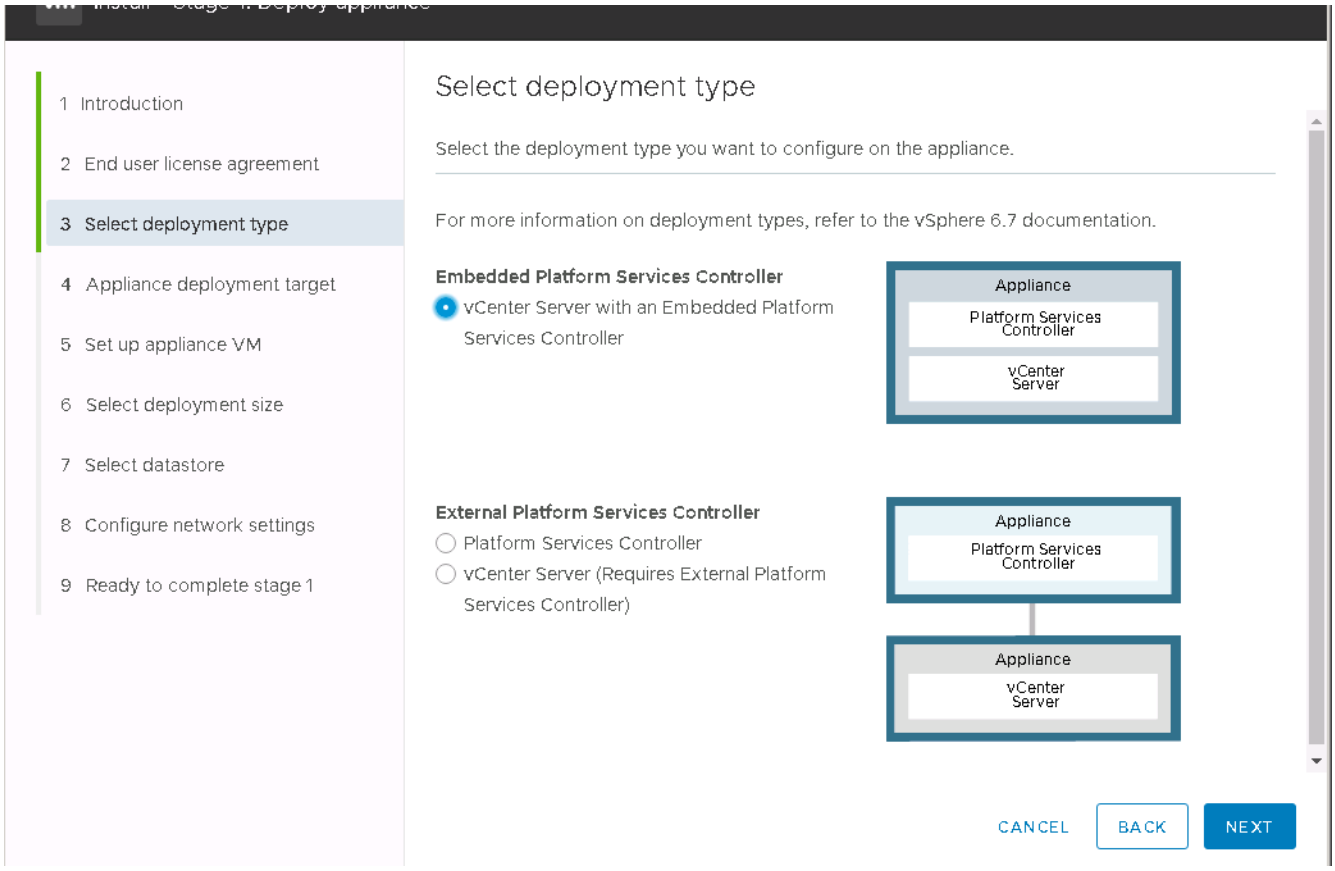
1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.



2. Laden Sie die VCSA von der VMware-Website herunter.

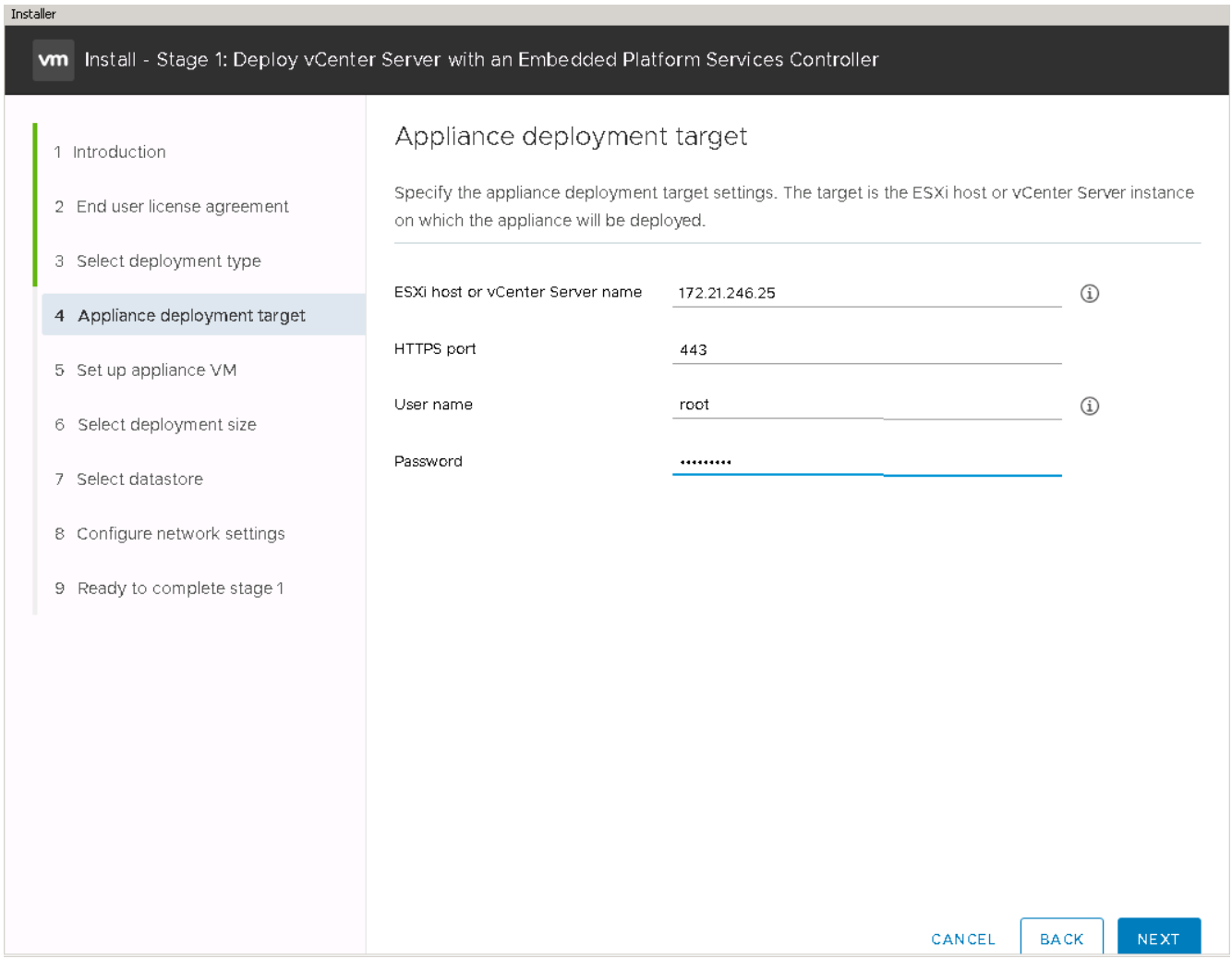
> Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.

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.

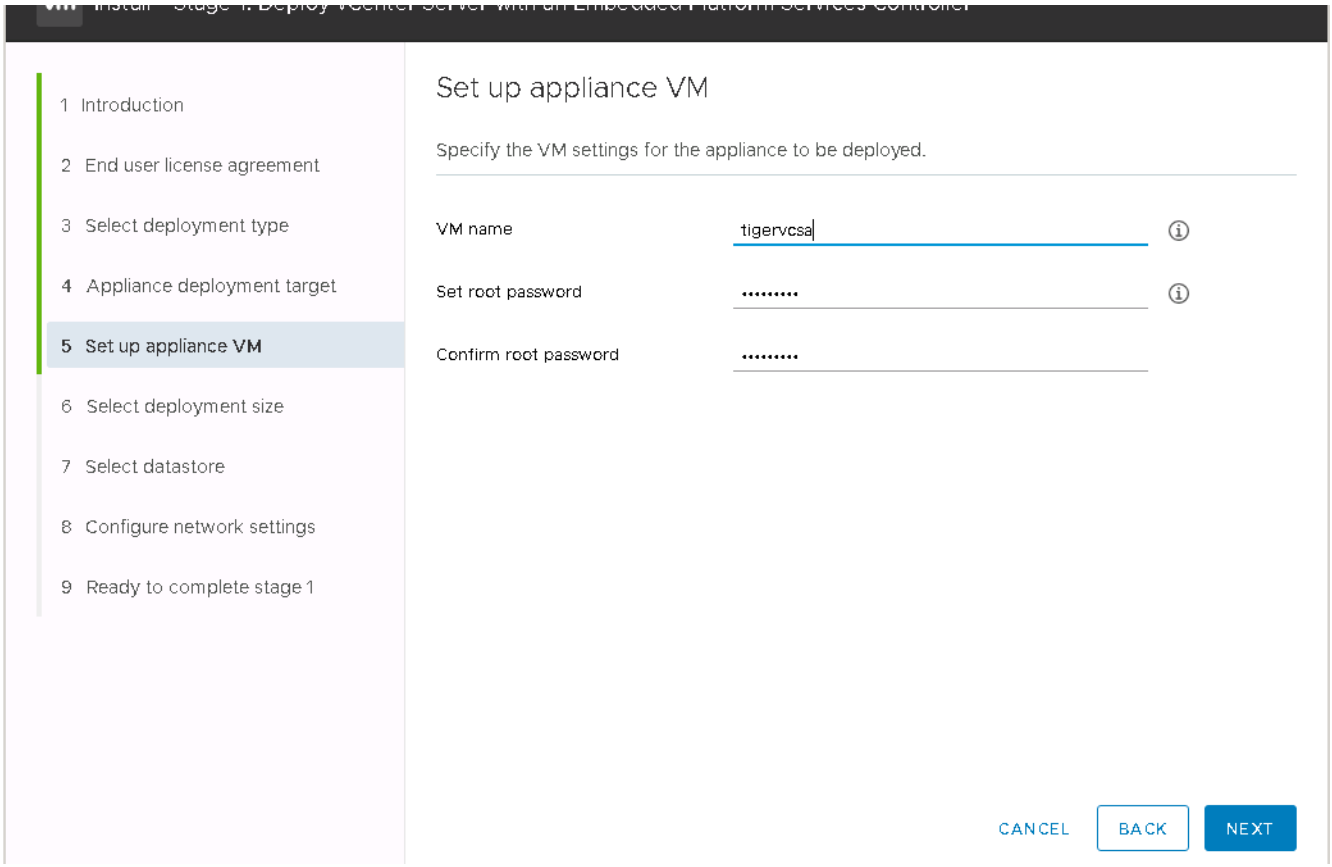


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

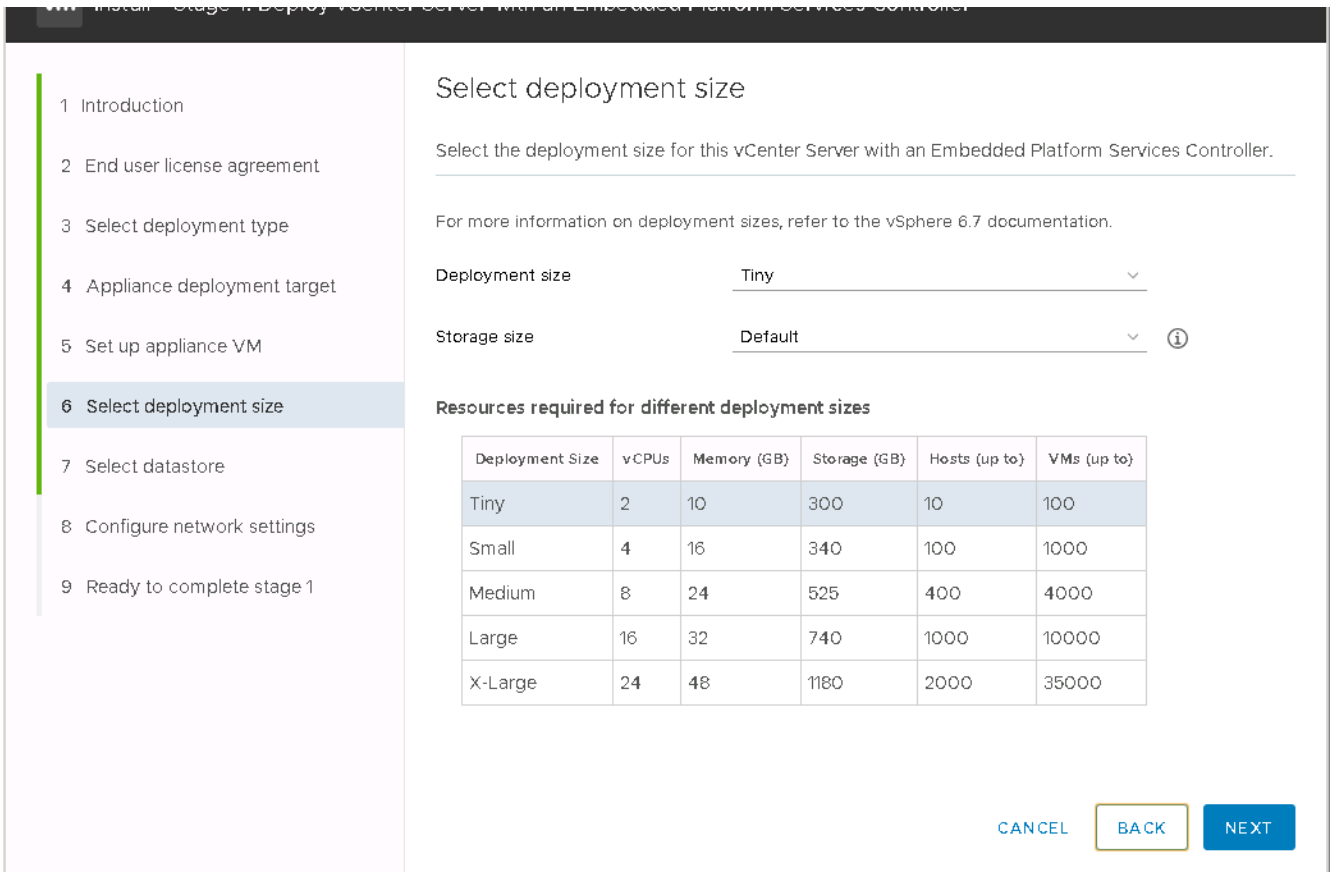
9. Geben Sie im Bereitstellungsziel der Appliance die IP-Adresse eines bereitgestellten ESXi-Hosts sowie den Root-Benutzernamen und das Root-Passwort ein.



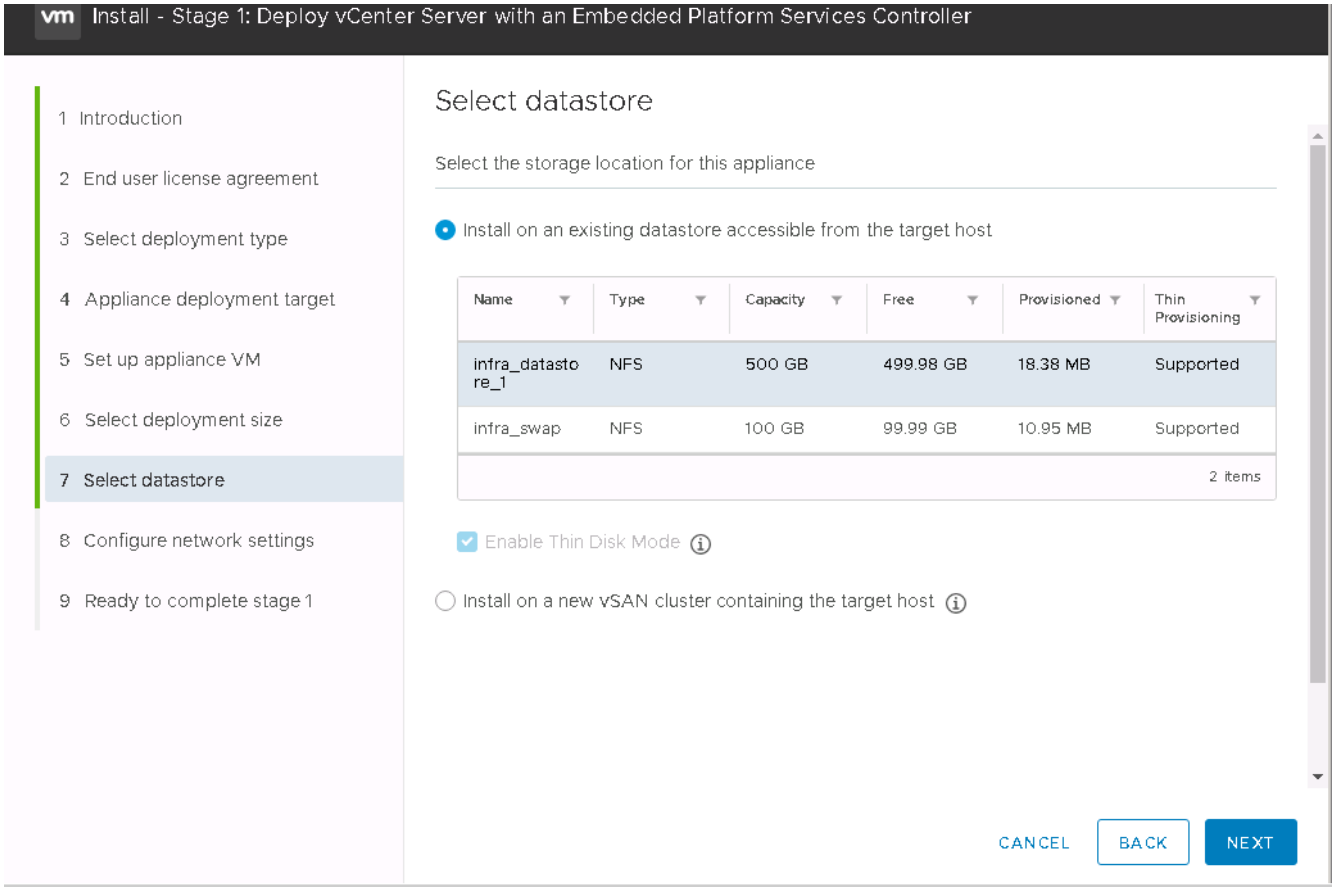
10. Legen Sie die Appliance-VM fest, indem Sie eingeben `VCSA` Als VM-Name und das Root-Passwort, das Sie für den VCSA verwenden möchten.



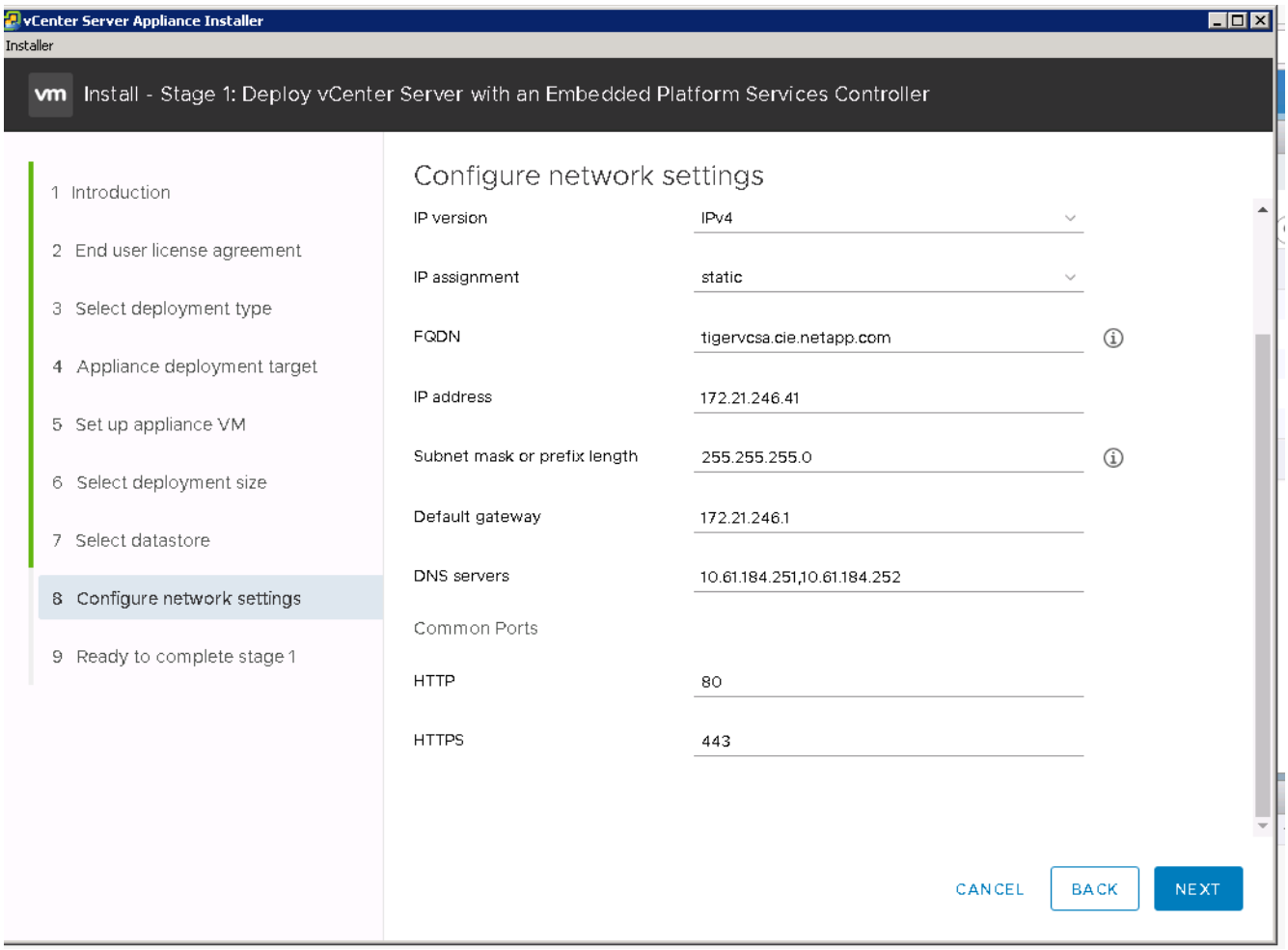
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



12. Wählen Sie den Infra_Datastore_1 aus. Klicken Sie Auf Weiter.

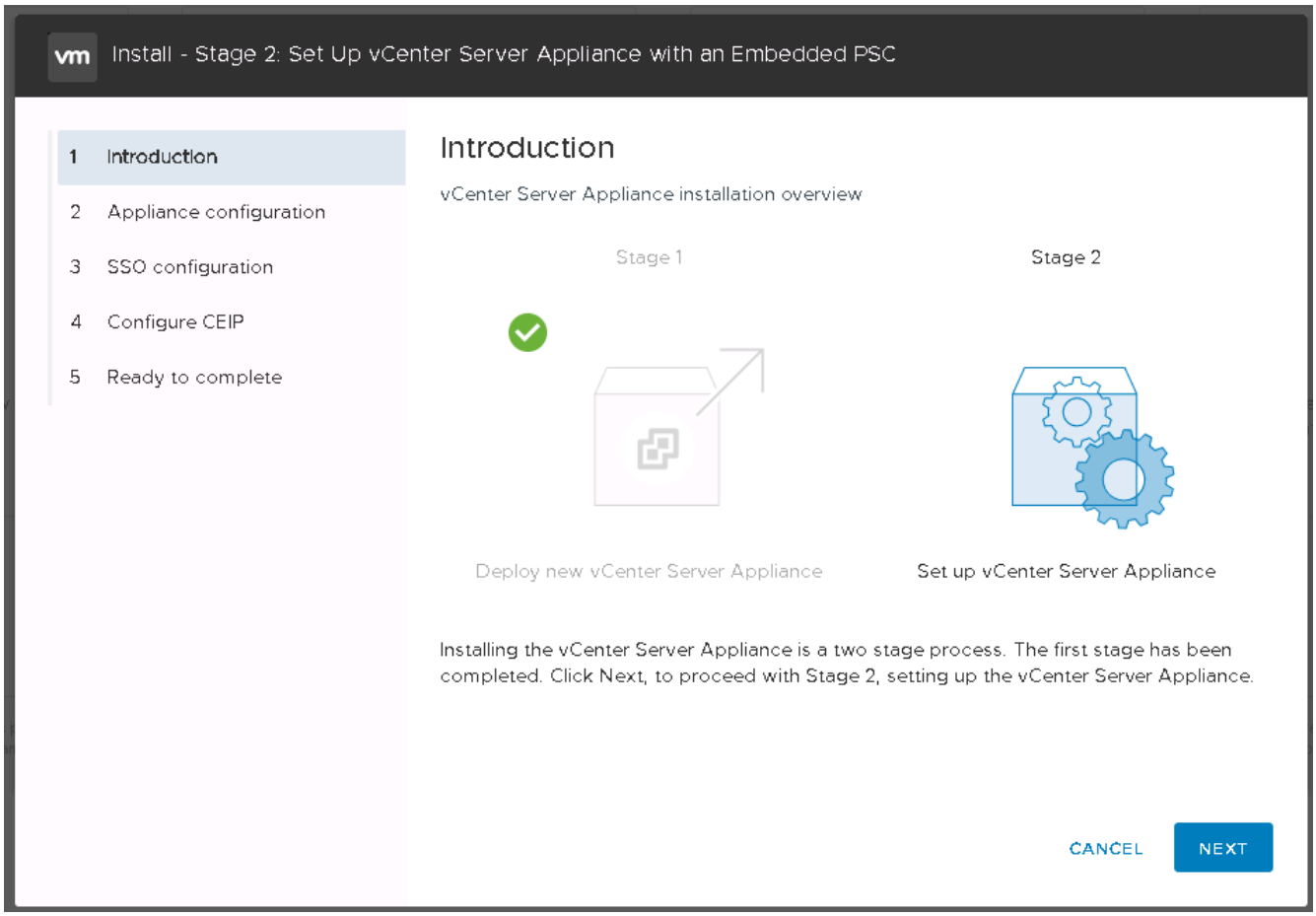


13. Geben Sie die folgenden Informationen auf der Seite Netzwerkeinstellungen konfigurieren ein, und klicken Sie auf Weiter.
    a. Wählen Sie MGMT-Network für Netzwerk.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse 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

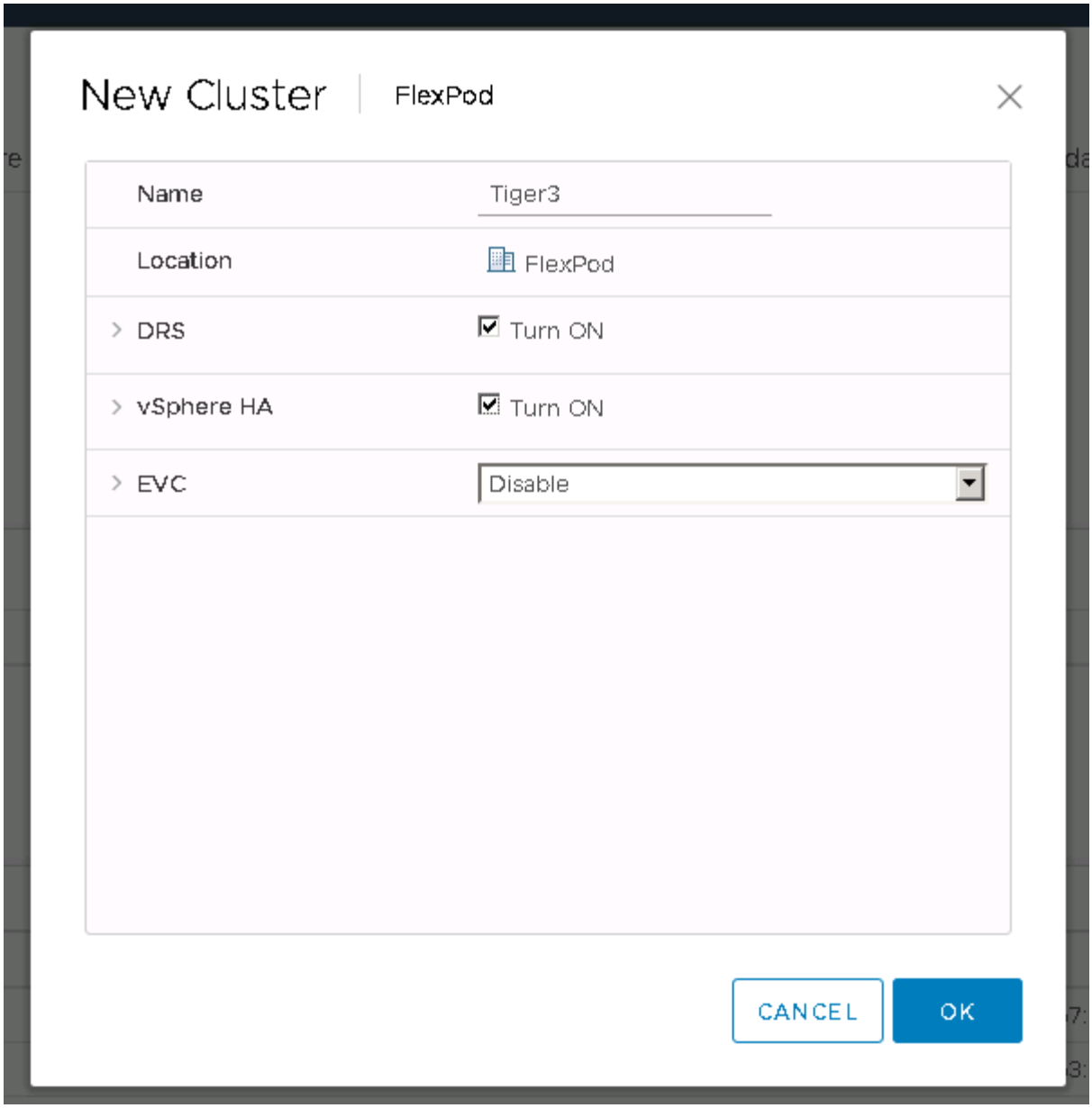
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

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

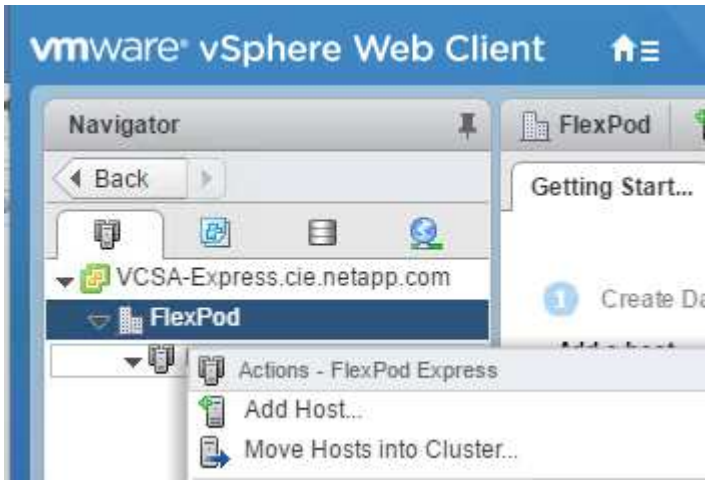
Führen Sie die folgenden Schritte aus, um einen vSphere-Cluster zu erstellen:

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.

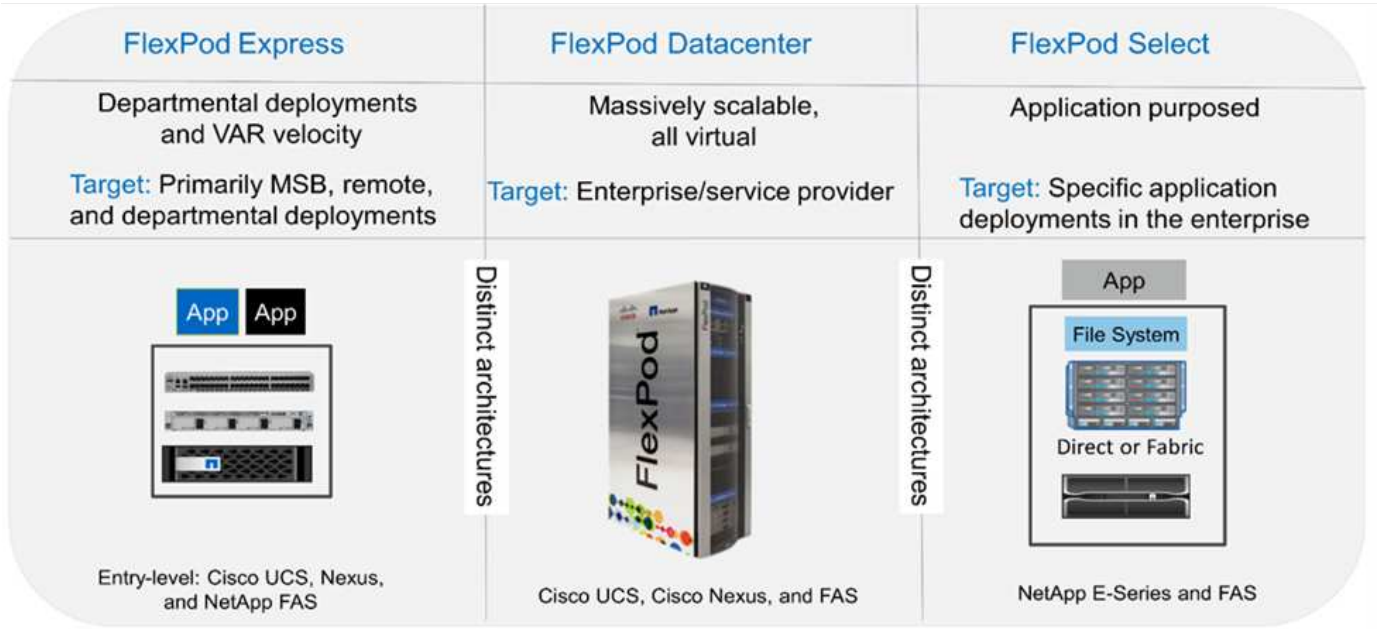
FlexPod Converged Infrastructure Programm

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

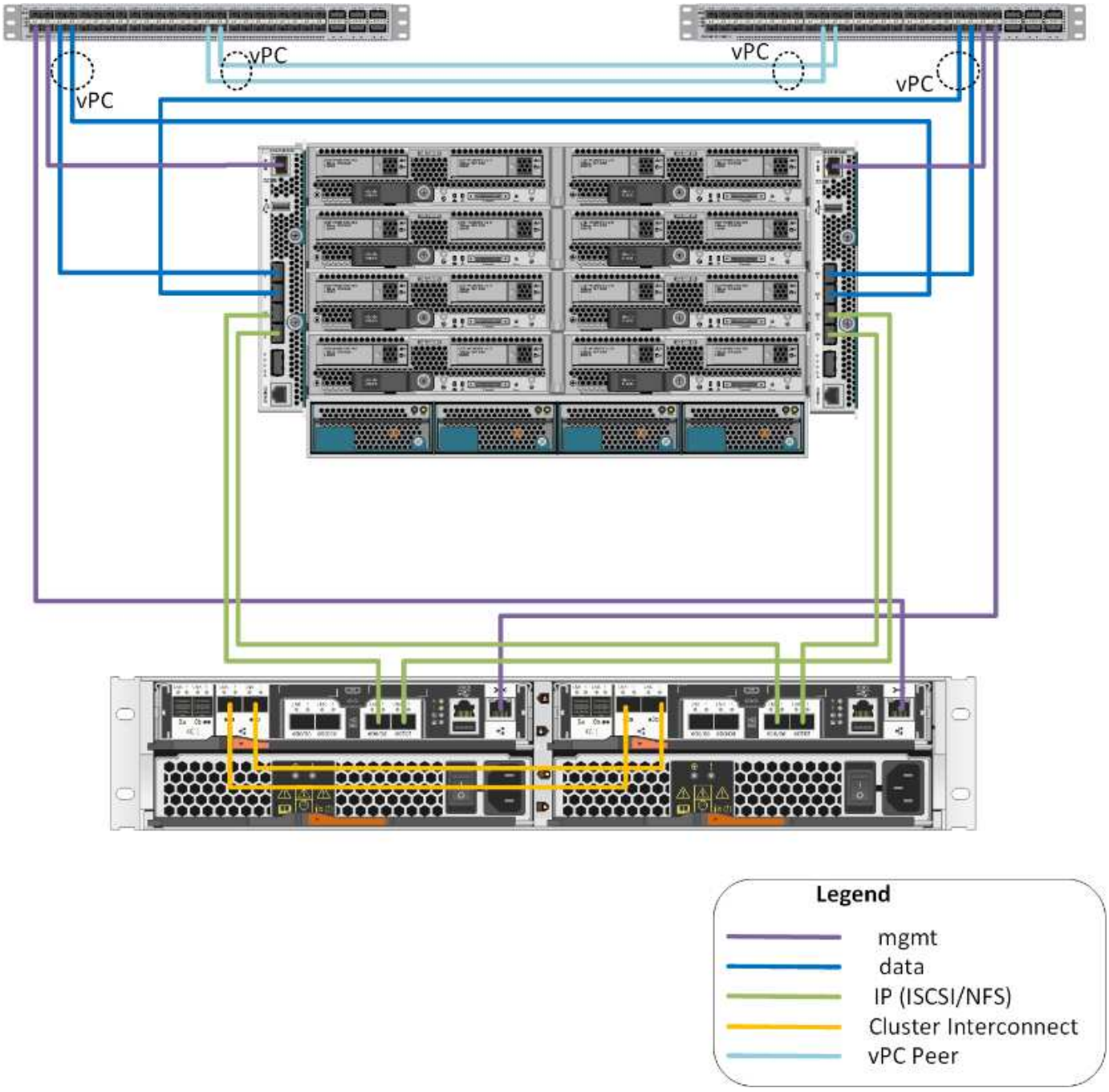
Softwarekomponenten

- 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

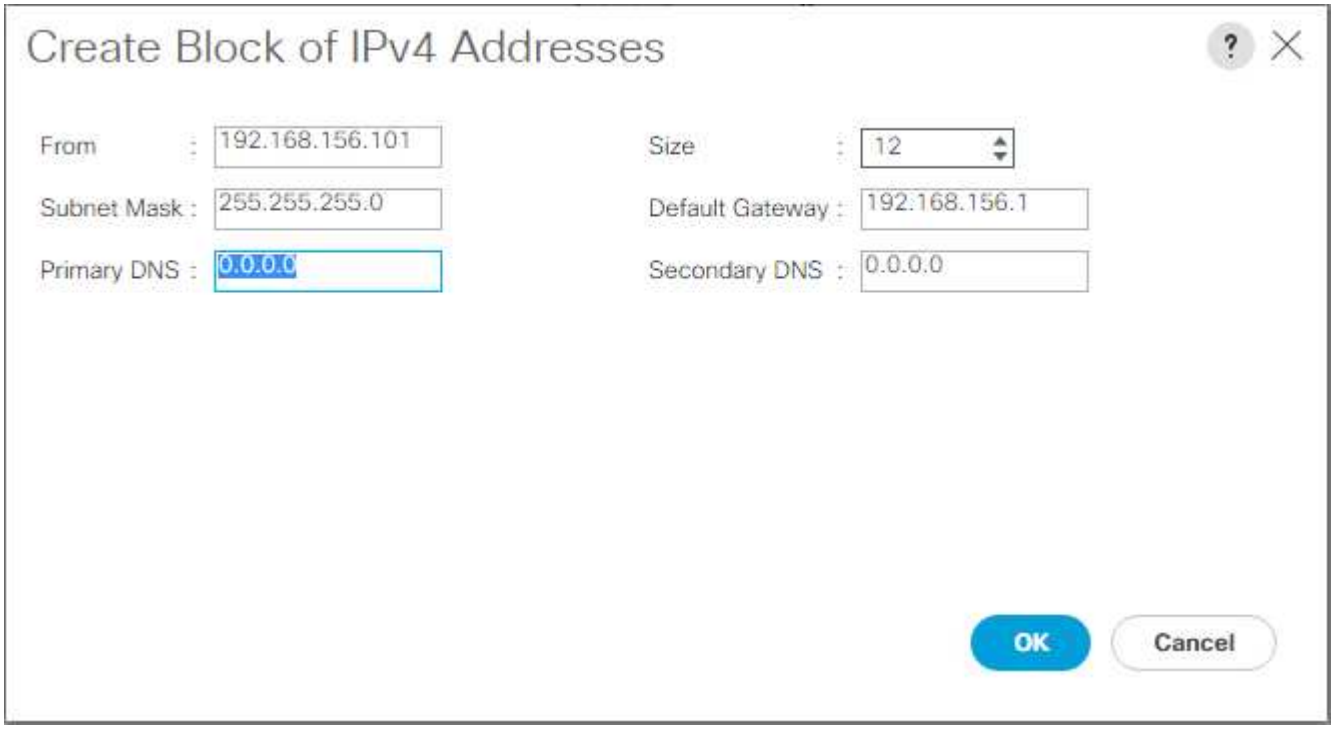
Cisco empfiehlt ausdrücklich die Konfiguration von „Call Home“ in Cisco UCS Manager. Die Konfiguration von „Call Home“ beschleunigt die Lösung von Support-Fällen. Gehen Sie wie folgt vor, um Call Home zu konfigurieren:

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.



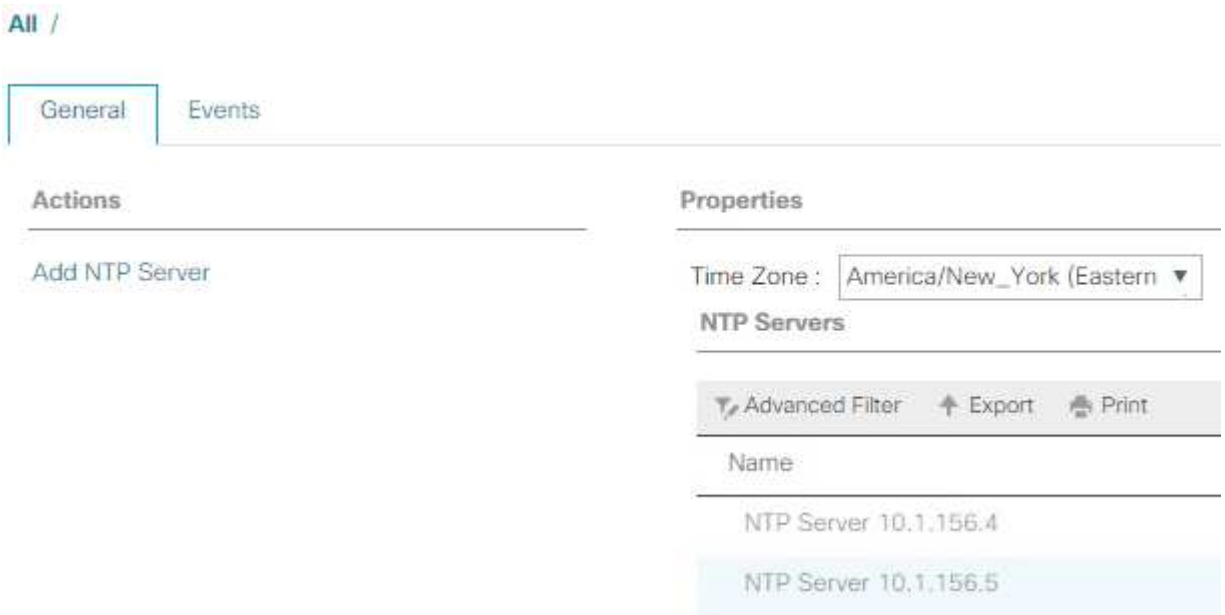
5. Klicken Sie auf OK, um den Block zu erstellen.
6. Klicken Sie in der Bestätigungsmeldung auf OK.

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

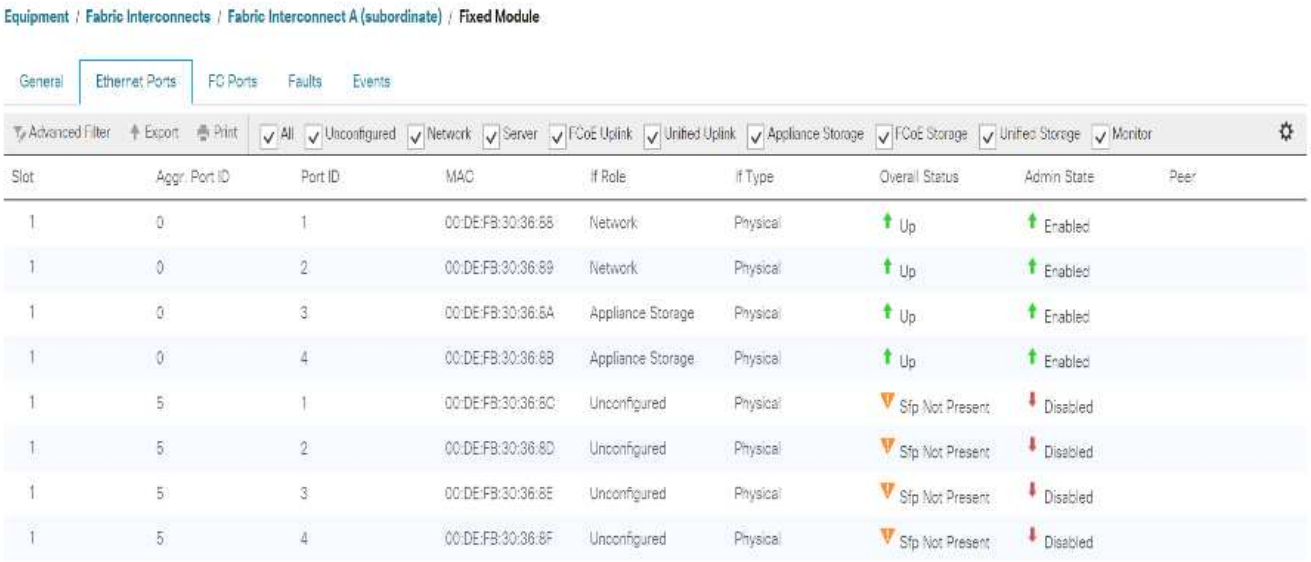
Durch die Festlegung der Erkennungsrichtlinie wird das Hinzufügen eines Cisco UCS B-Series Gehäuses und von zusätzlichen Fabric Extendern für weitere Cisco UCS C-Serie-Konnektivität vereinfacht. Gehen Sie wie folgt vor, um die Richtlinie zur Chassis-Erkennung zu ändern:

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.

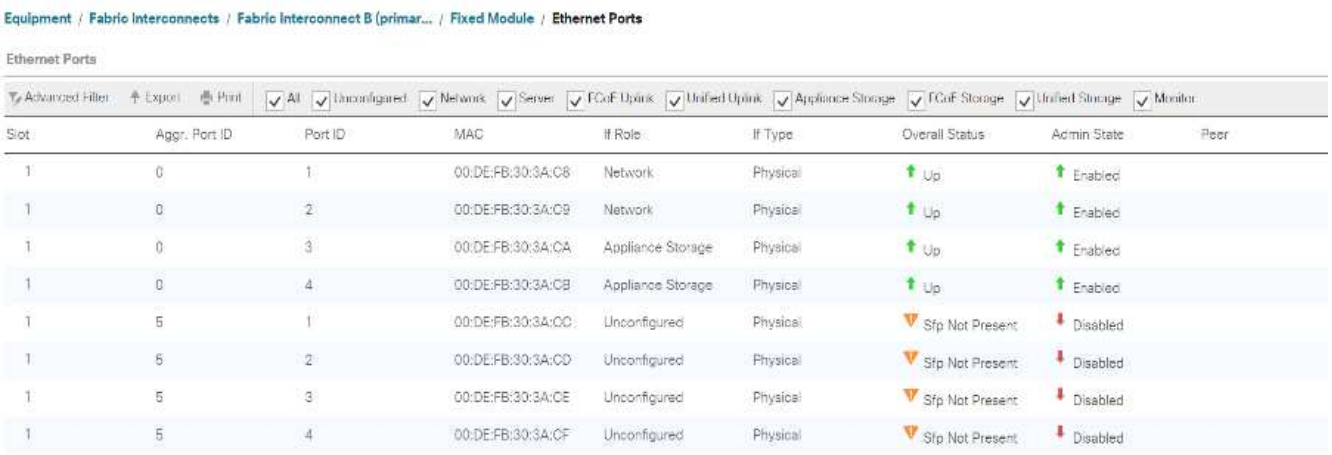
Unterstützung von Server-, Uplink- und Storage-Ports

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.



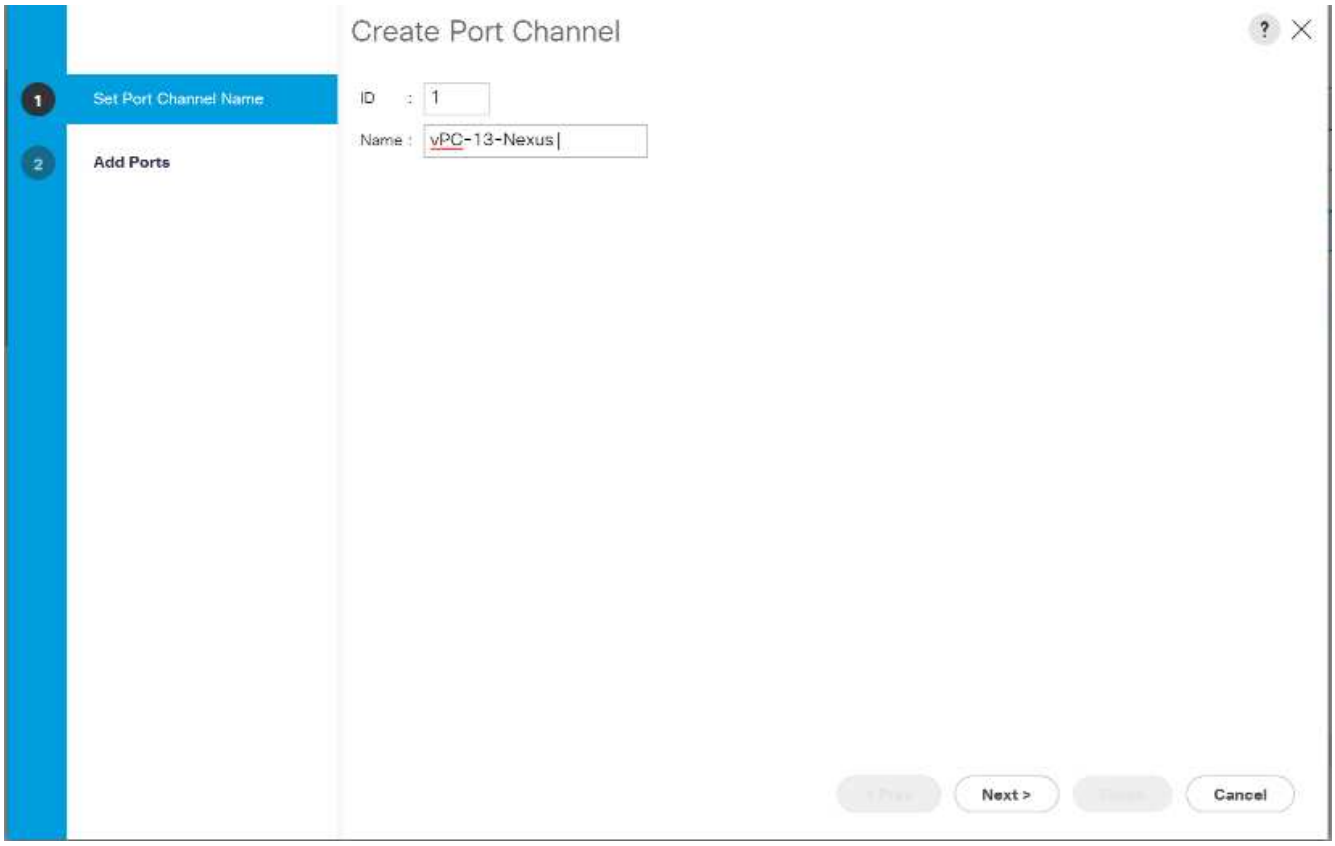
Erstellen von Uplink-Port-Kanälen zu Cisco Nexus 31108 Switches

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:

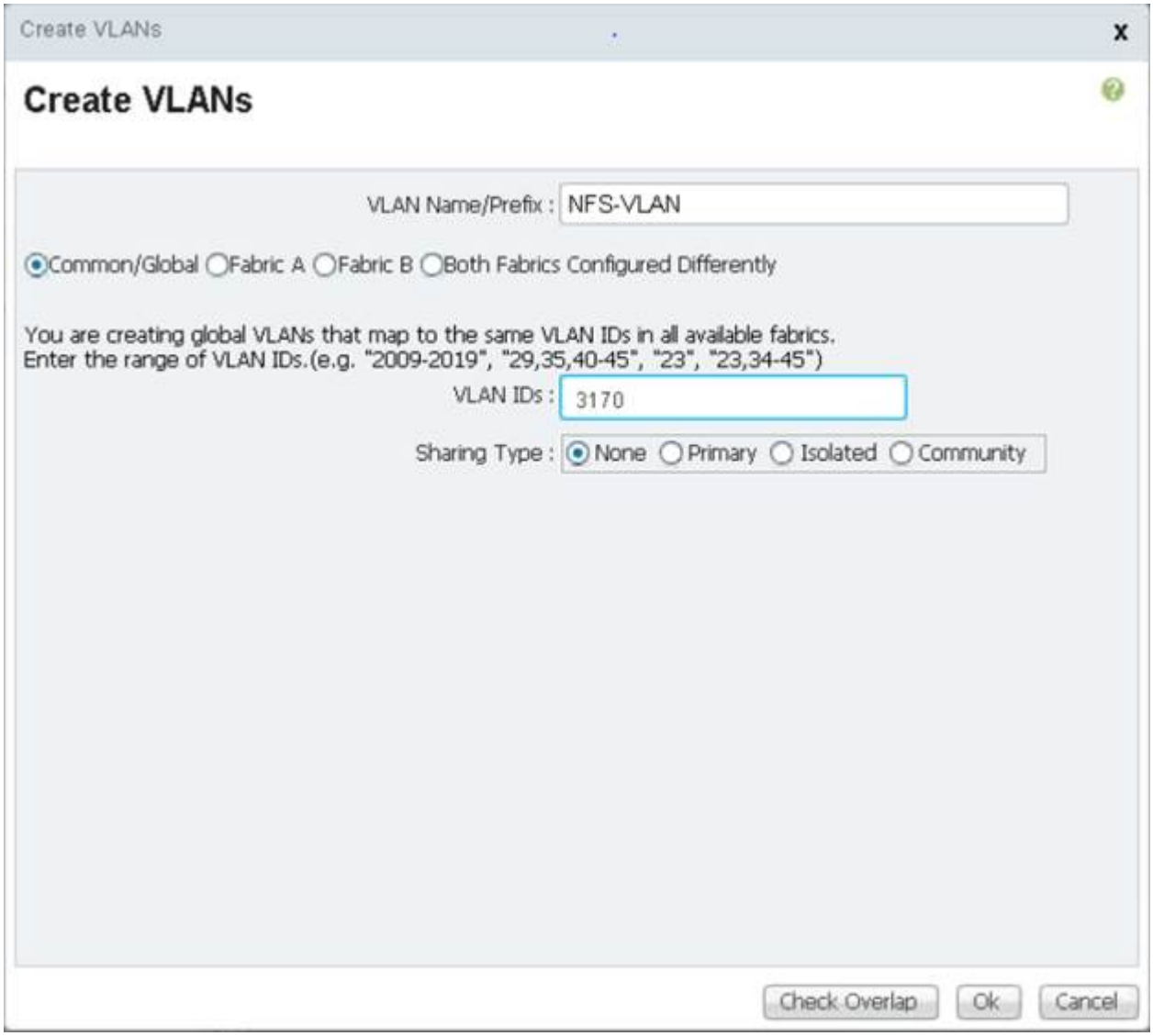
1. Wählen Sie im Cisco UCS Manager im Menü Neu in der Symbolleiste oben im Fenster die Option Organisation erstellen aus.
2. Geben Sie einen Namen für die Organisation ein.
3. Optional: Geben Sie eine Beschreibung für die Organisation ein. Klicken Sie auf OK.
4. Klicken Sie in der Bestätigungsmeldung 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:

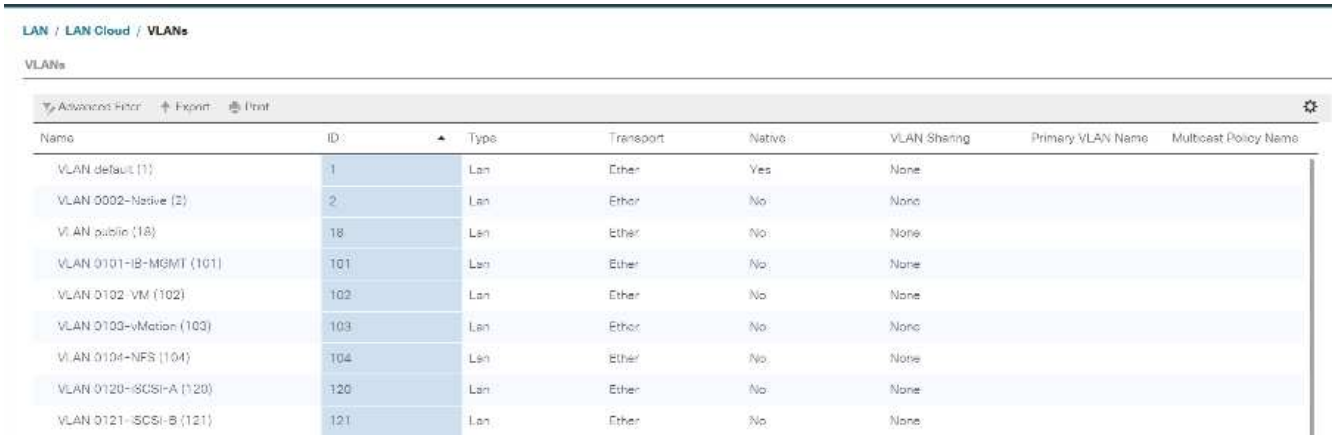
1. Wählen Sie im Cisco UCS Manager die Registerkarte LAN aus.
2. Erweitern Sie die Cloud der Appliances.
3. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
4. Wählen Sie VLANs erstellen aus.
5. Geben Sie NFS-VLAN als Name für das NFS-VLAN für die Infrastruktur ein.
6. Lassen Sie „Allgemein/global“ ausgewählt.
7. Eingabe `<<var_nfs_vlan_id>>` Für die VLAN-ID.

8. Den Freigabetyp auf Keine setzen lassen.

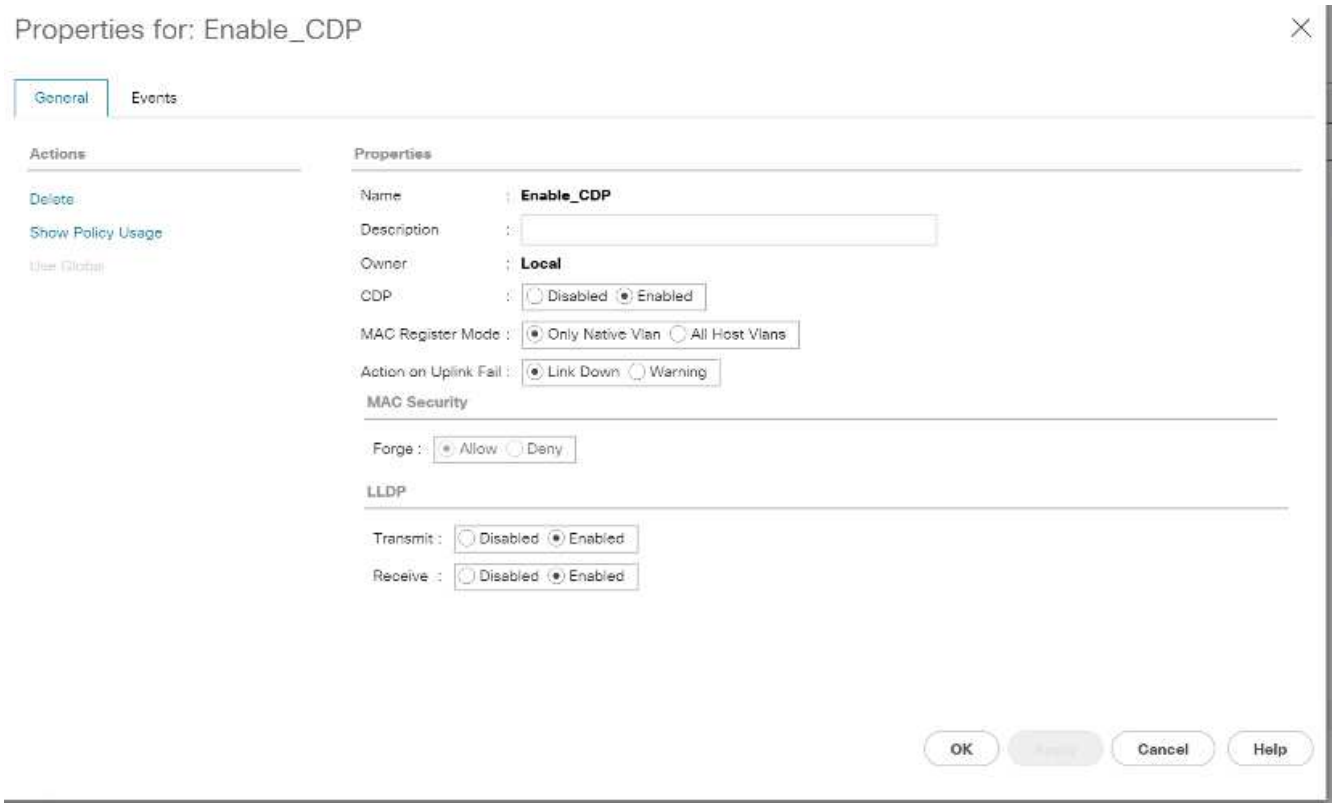


9. Klicken Sie auf OK, und klicken Sie erneut auf OK, um das VLAN zu erstellen.
10. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
11. Wählen Sie VLANs erstellen aus.
12. Geben Sie das iSCSI-A-VLAN als Namen für die iSCSI-Fabric-Infrastruktur Ein VLAN ein.
13. Lassen Sie „Allgemein/global“ 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.

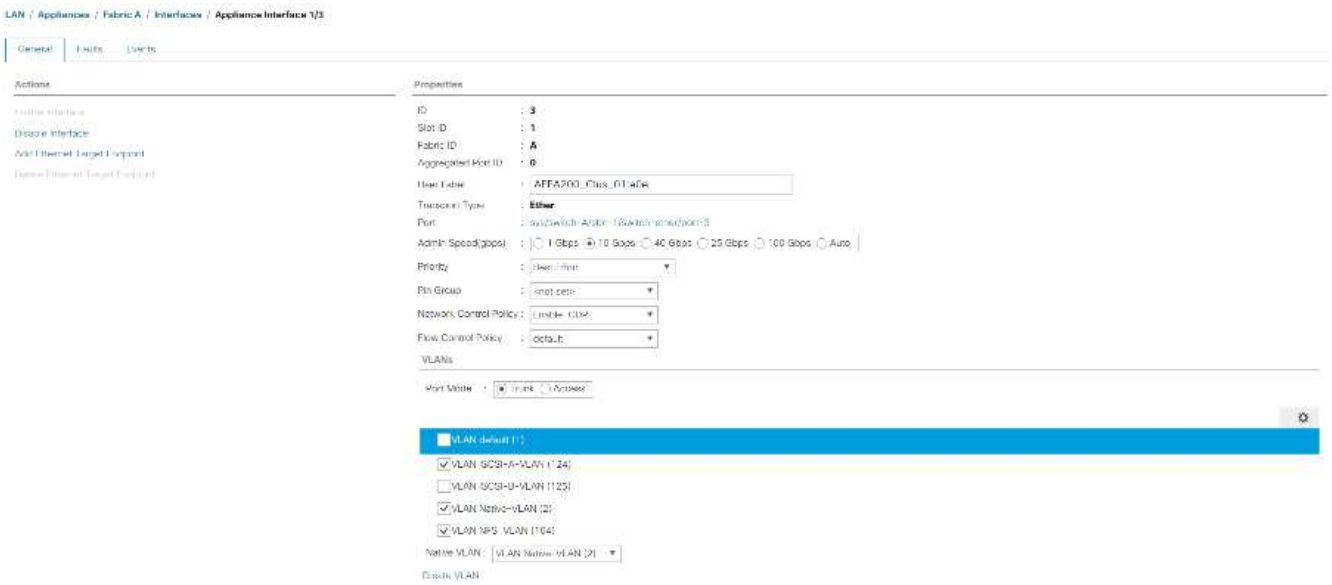
22. Klicken Sie mit der rechten Maustaste auf VLANs unter Appliances „Cloud“.
23. Wählen Sie VLANs erstellen aus.
24. Geben Sie Native-VLAN als Namen für das Native VLAN ein.
25. Lassen Sie „Allgemein/global“ ausgewählt.
26. Eingabe `<<var_native_vlan_id>>` Für die VLAN-ID.
27. Klicken Sie auf OK, und 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.

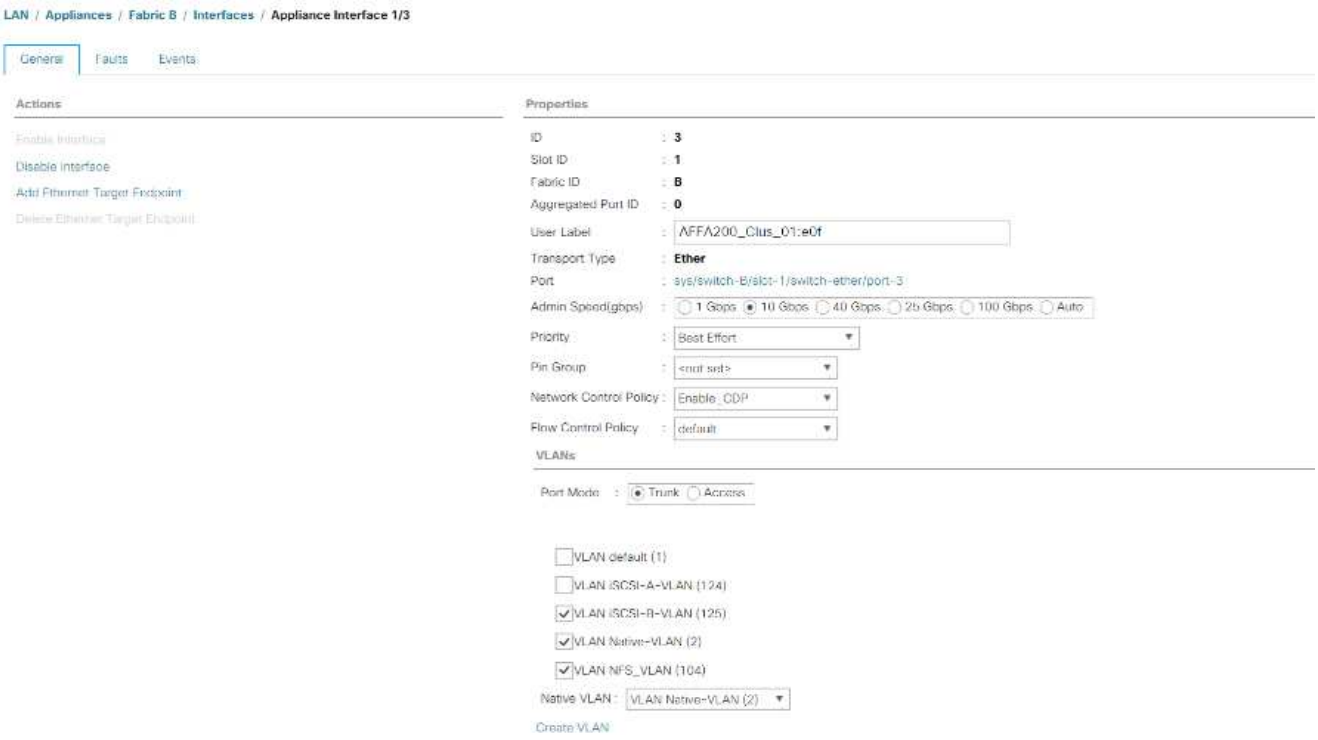


32. Klicken Sie auf OK und anschließend erneut auf OK, um die Richtlinie zu erstellen.
33. Erweitern Sie im Navigationsbereich unter LAN > Appliances Cloud die Struktur Fabric A.
34. Erweitern Sie Schnittstellen.
35. Wählen Sie Die Appliance-Schnittstelle 1/3.
36. Geben Sie im Feld „Benutzerbeschriftung“ 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.

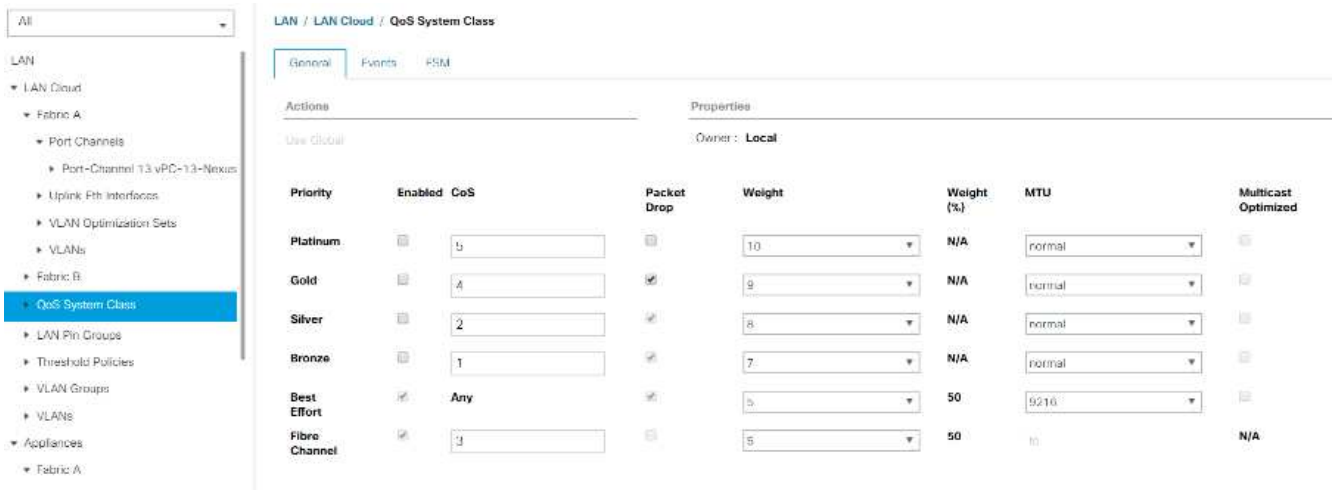


53. Klicken Sie auf Änderungen speichern und OK.
54. Wählen Sie unter Fabric B Appliance Interface 1/4 aus
55. Geben Sie im Feld „Benutzerbeschriftung“ Informationen ein, die den Port des Speichercontrollers angeben, z. B. `<storage_controller_02_name>:e0f`. Klicken Sie auf Änderungen speichern und OK.
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)

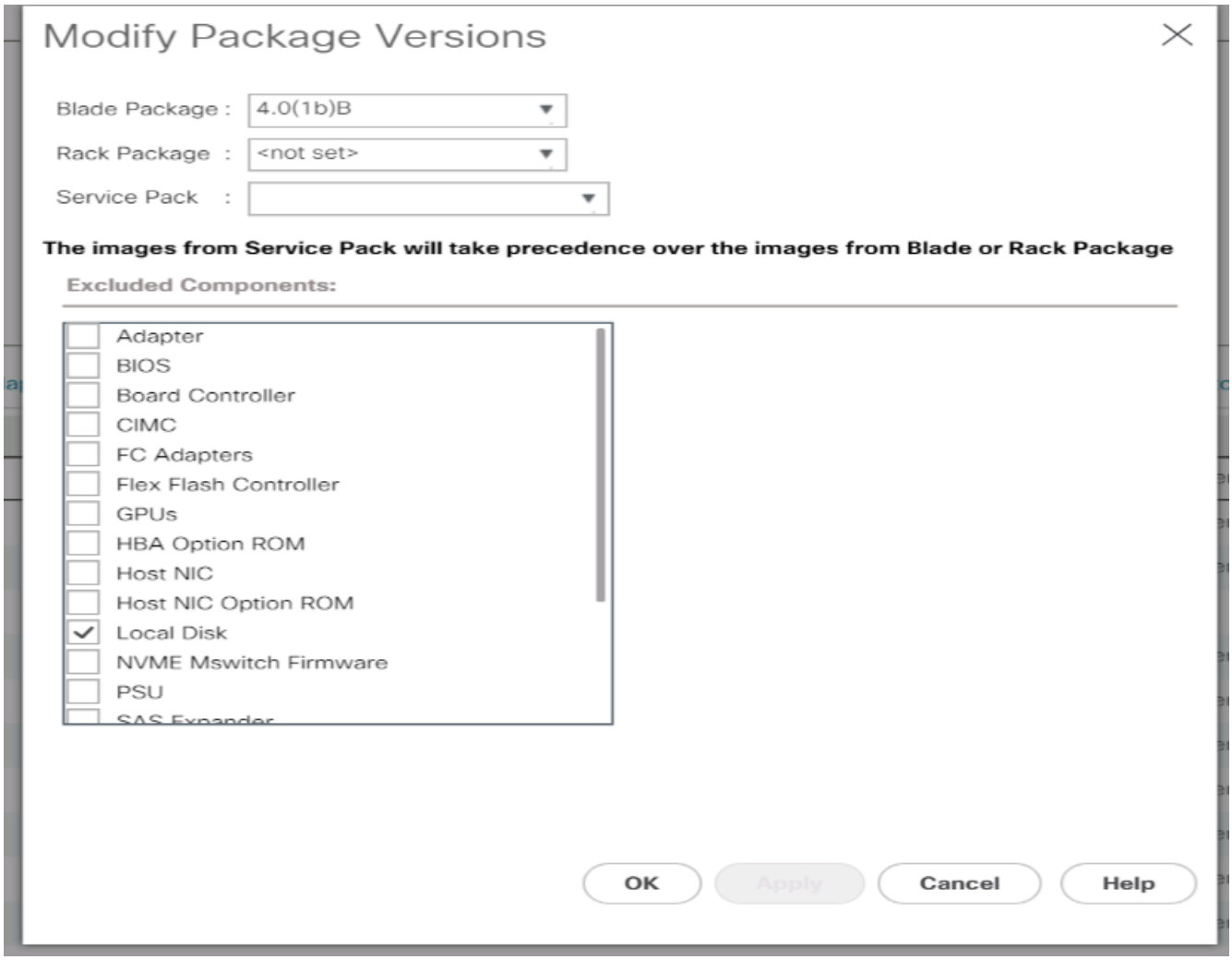
Informationen zum Upgrade der Cisco UCS Manager Software und der Cisco UCS Fabric Interconnect Software auf Version 4.0(1b) finden Sie unter "Cisco UCS Manager – Installations- und Upgrade-Leitfäden".

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:

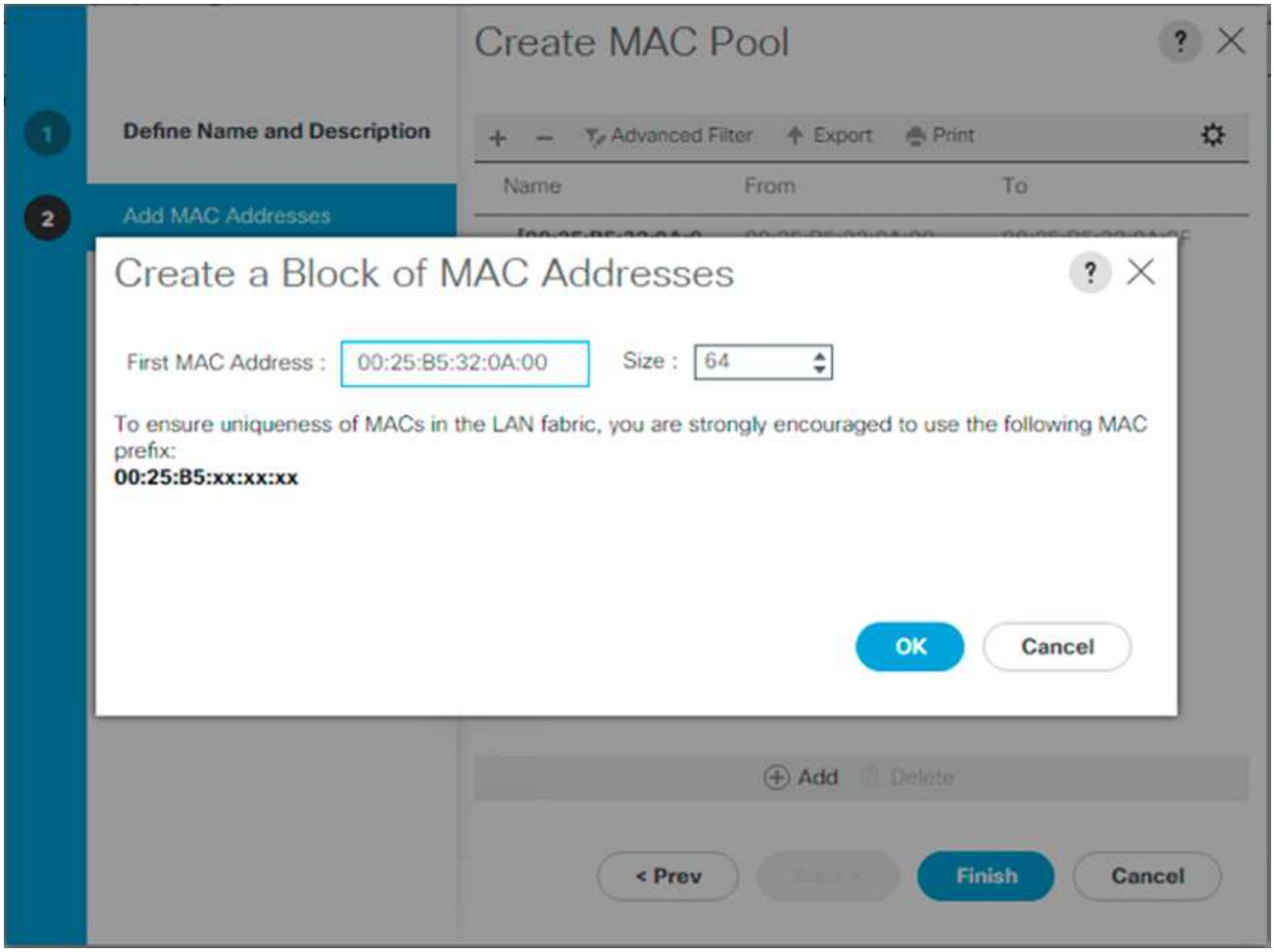
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Pools > Root aus.

   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.

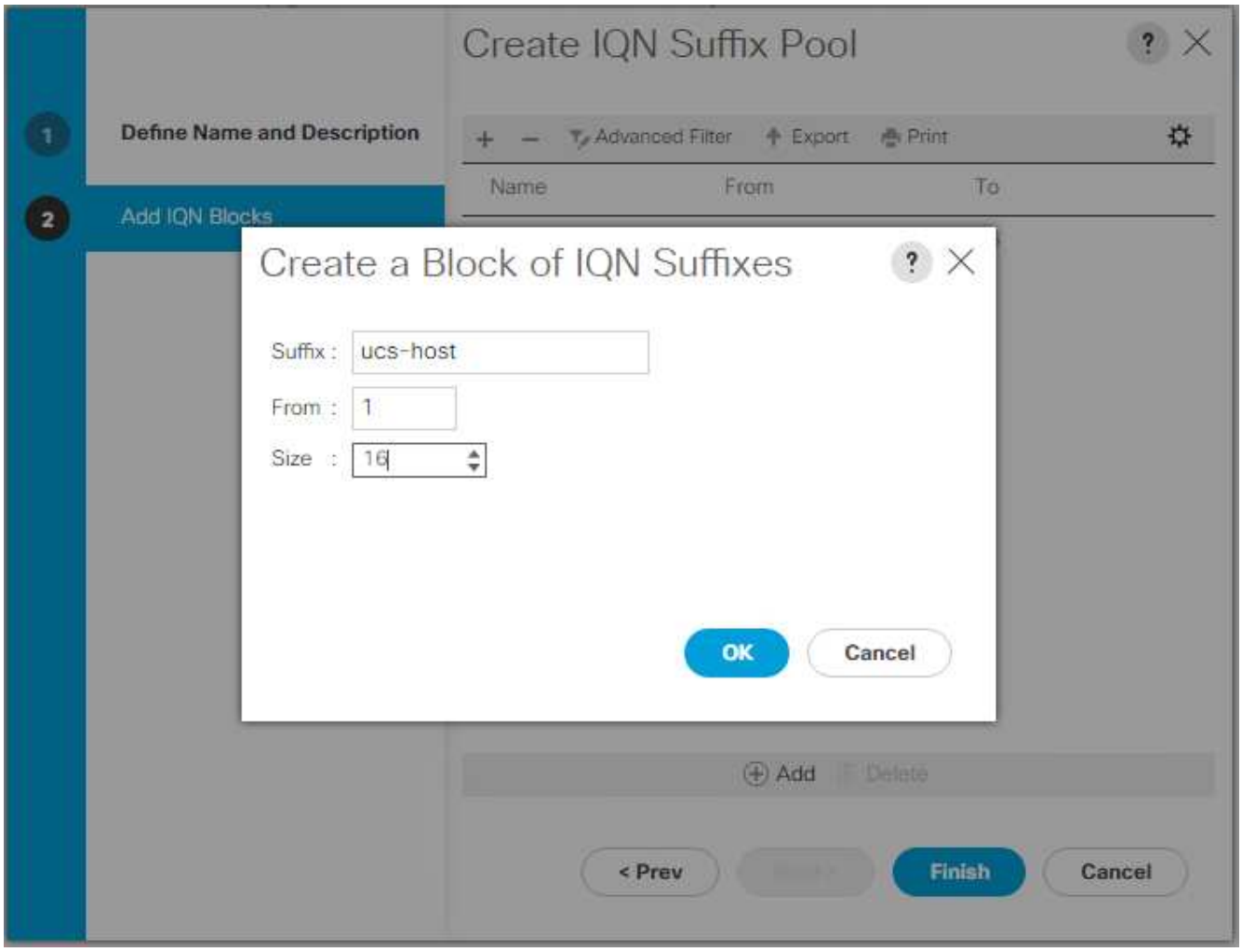
ISCSI-IQN-Pool erstellen

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.

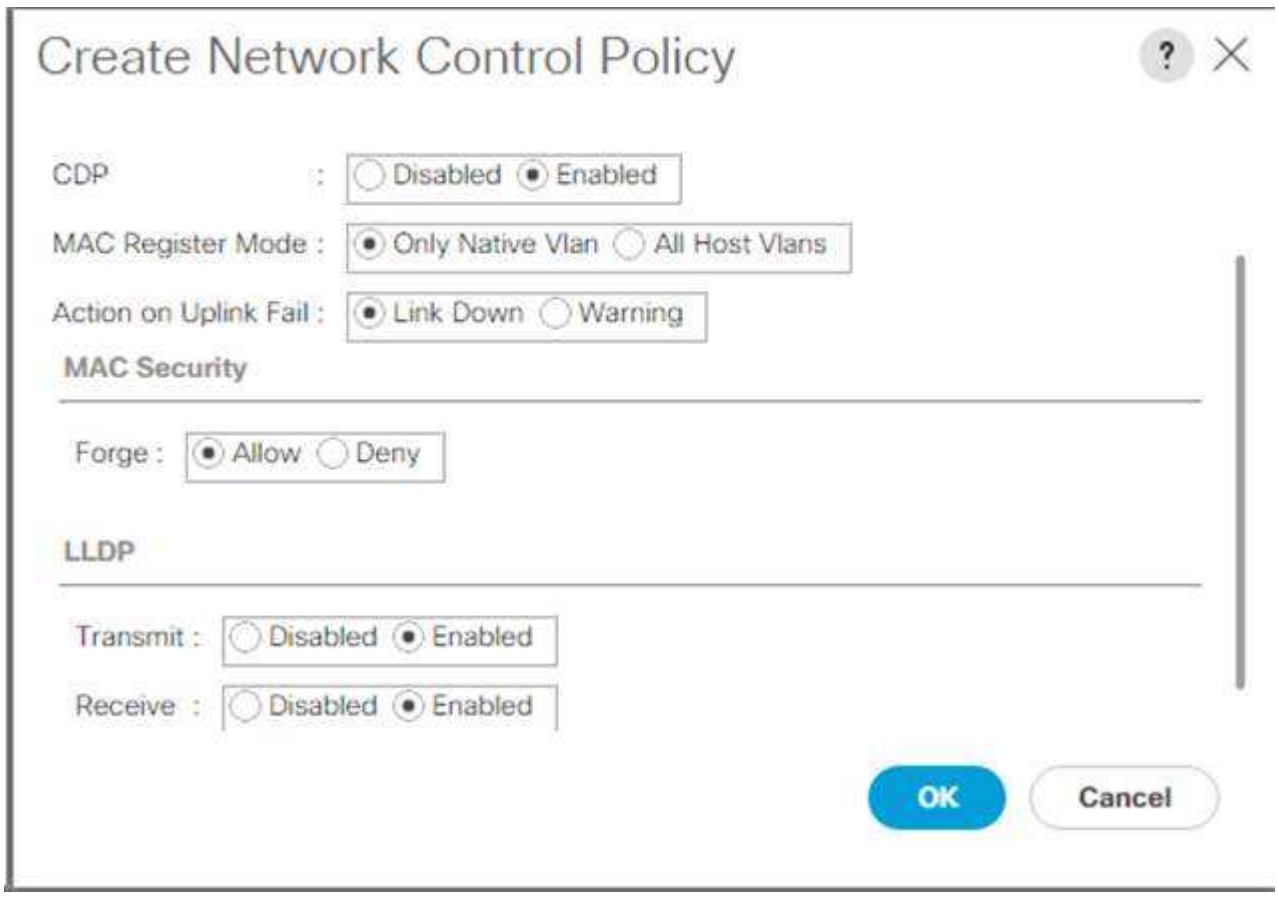
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Pools > Root aus.
3. Klicken Sie mit der rechten Maustaste auf Server Pools.

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:

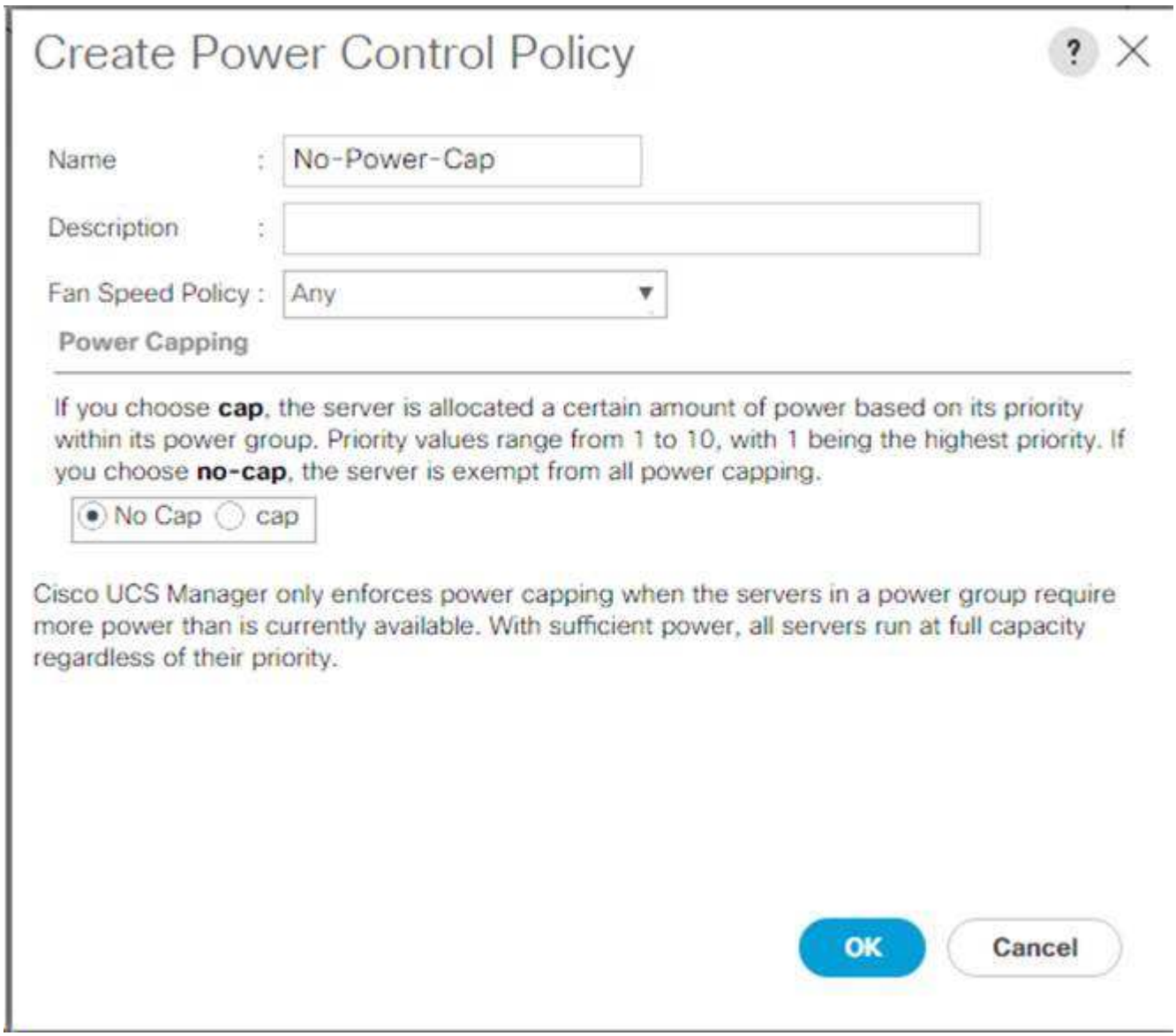
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf Network Control Policies.
4. Wählen Sie Netzwerksteuerungsrichtlinie Erstellen.
5. Geben Sie den Namen der Enable-CDP-LLDP-Richtlinie ein.
6. Wählen Sie bei CDP die Option 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.

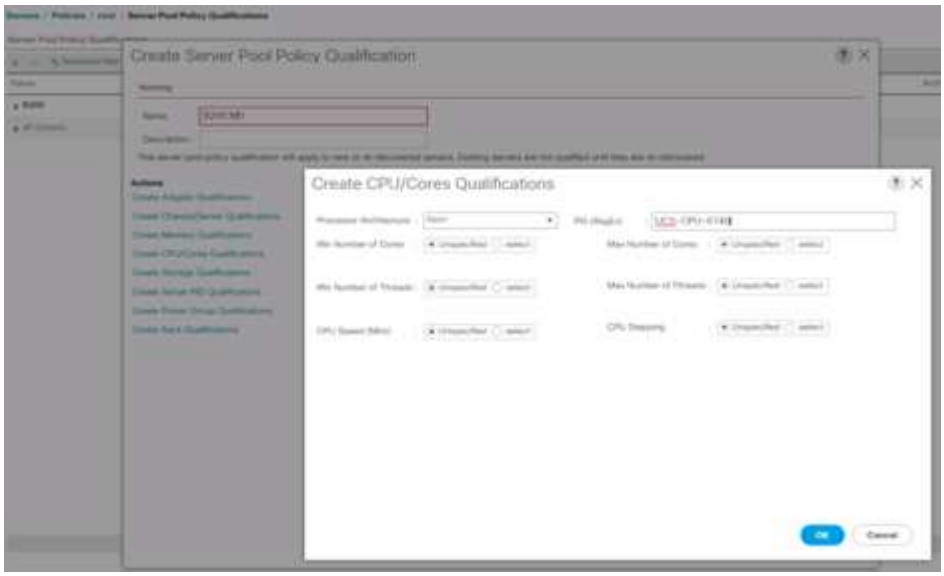


Serverpool-Qualifikationsrichtlinie erstellen (optional)

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.

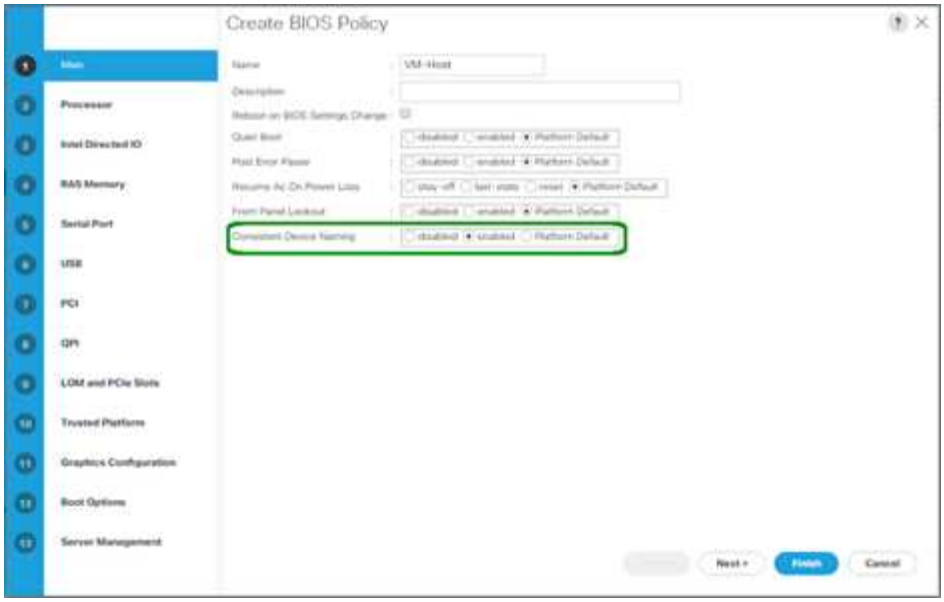
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Wählen Sie Die Qualifikationen Für Die Serverpool-Richtlinie Aus.
4. Wählen Sie Create Server Pool Policy Qualification oder Add aus.
5. Benennen Sie die Richtlinie Intel.
6. Wählen Sie CPU/Cores erstellen Qualifizierungen 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.



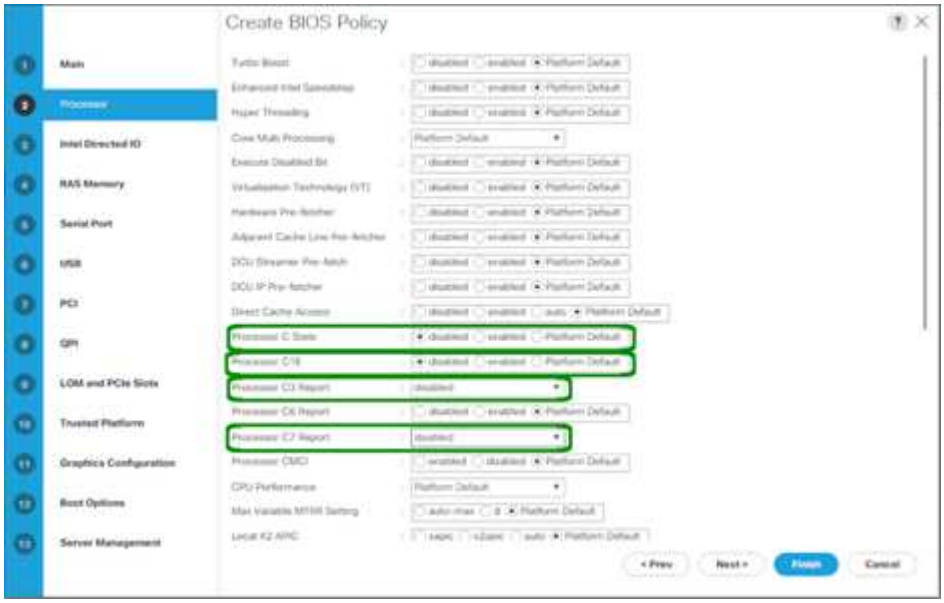
Erstellen der Server-BIOS-Richtlinie

Gehen Sie wie folgt vor, um eine Server-BIOS-Richtlinie für die Cisco UCS-Umgebung zu erstellen:

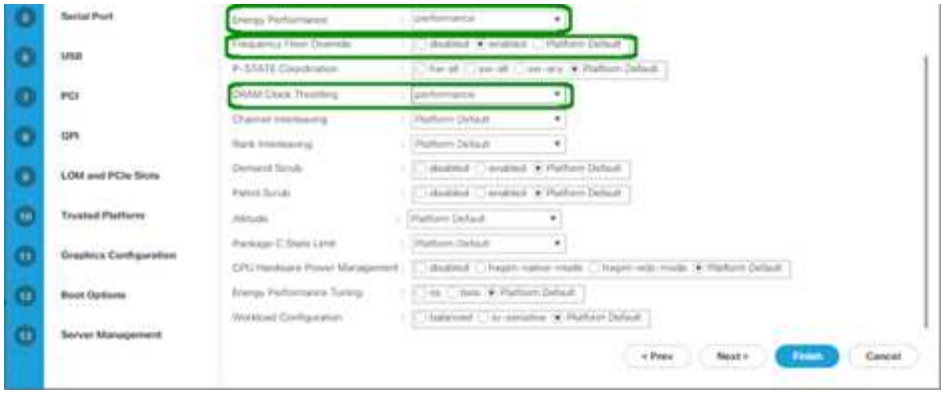
1. Klicken Sie im Cisco UCS Manager links auf Server.
2. Wählen Sie Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf BIOS-Richtlinien.
4. Wählen Sie BIOS-Richtlinie erstellen.
5. Geben Sie den VM-Host als Namen der BIOS-Richtlinie ein.
6. Ändern Sie die Einstellung für den stillen Start auf deaktiviert.
7. Ändern Sie die konsistente Gerätenennung in aktiviert.



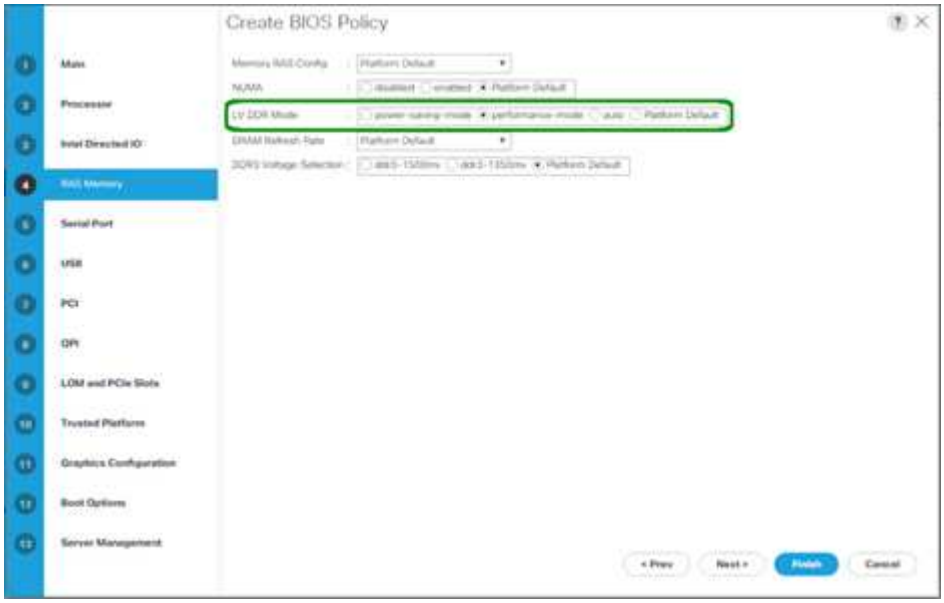
8. Wählen Sie die Registerkarte Prozessor aus, und legen Sie die folgenden Parameter fest:
   - Prozessor-C-Status: Deaktiviert
   - Prozessor C1E: Deaktiviert
   - Prozessor-C3-Bericht: Deaktiviert
   - Prozessor-C7-Bericht: Deaktiviert



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

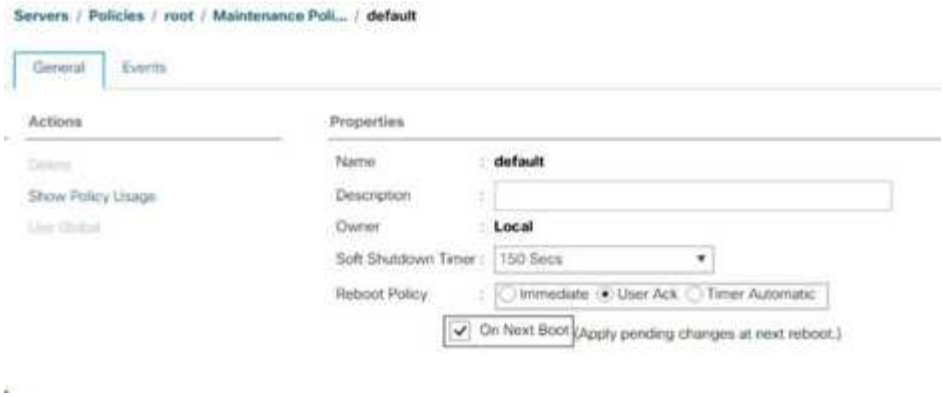


11. Klicken Sie auf Fertig stellen, um die BIOS-Richtlinie zu erstellen.
12. Klicken Sie auf OK.

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.

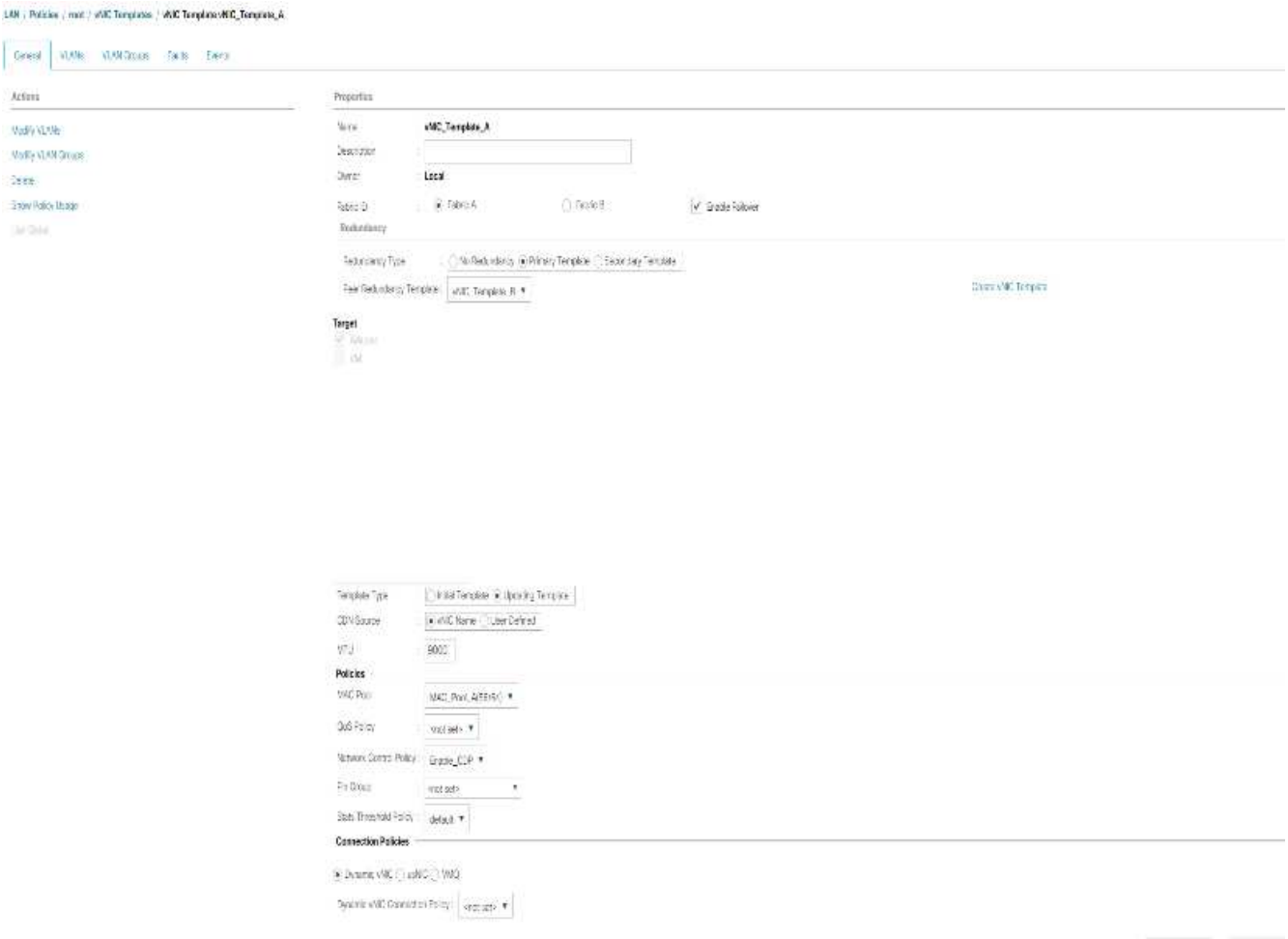
Es werden insgesamt vier vNIC-Vorlagen erstellt.

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.

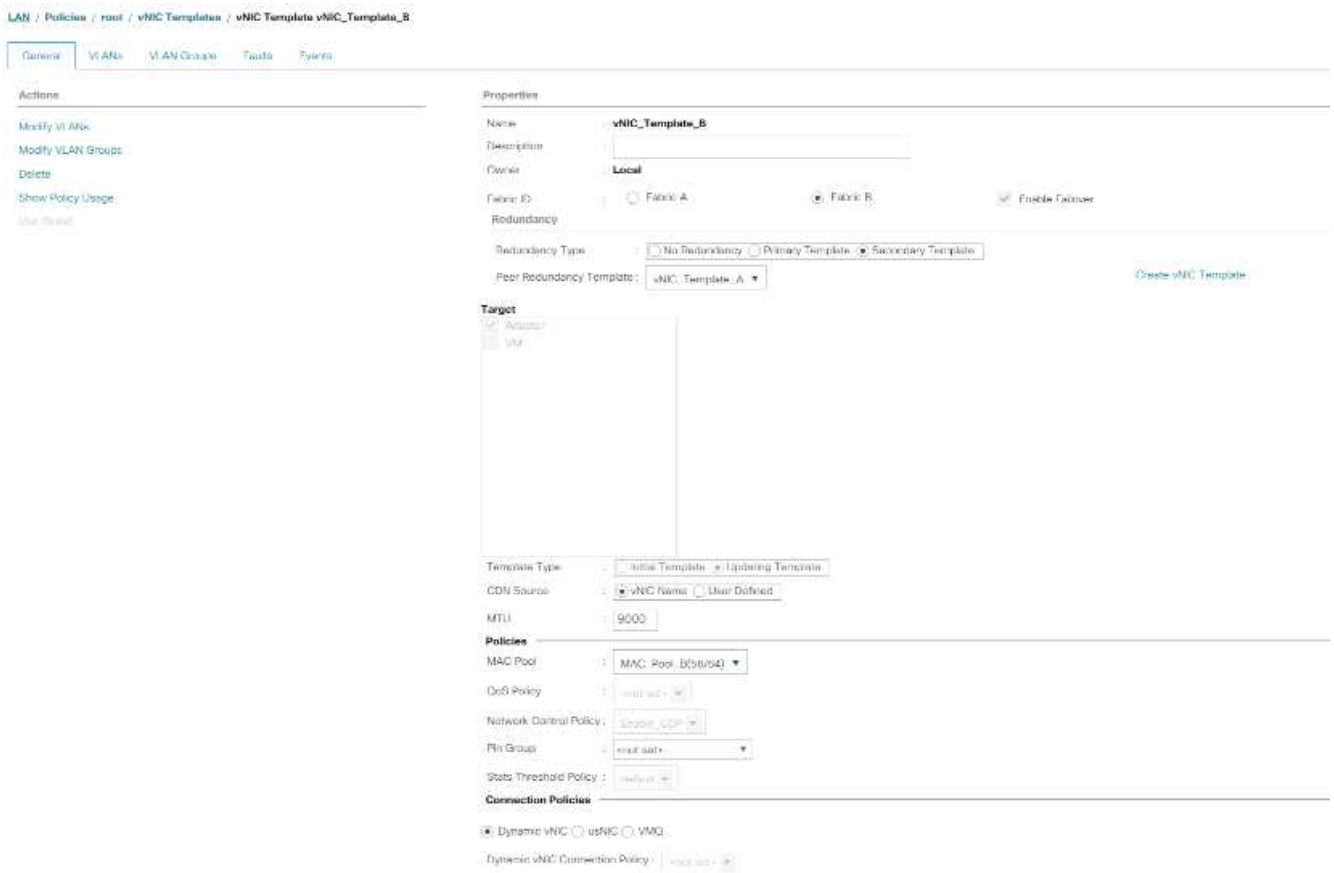


Gehen Sie wie folgt vor, um die sekundäre Redundanzvorlage Infra-B zu erstellen:

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.

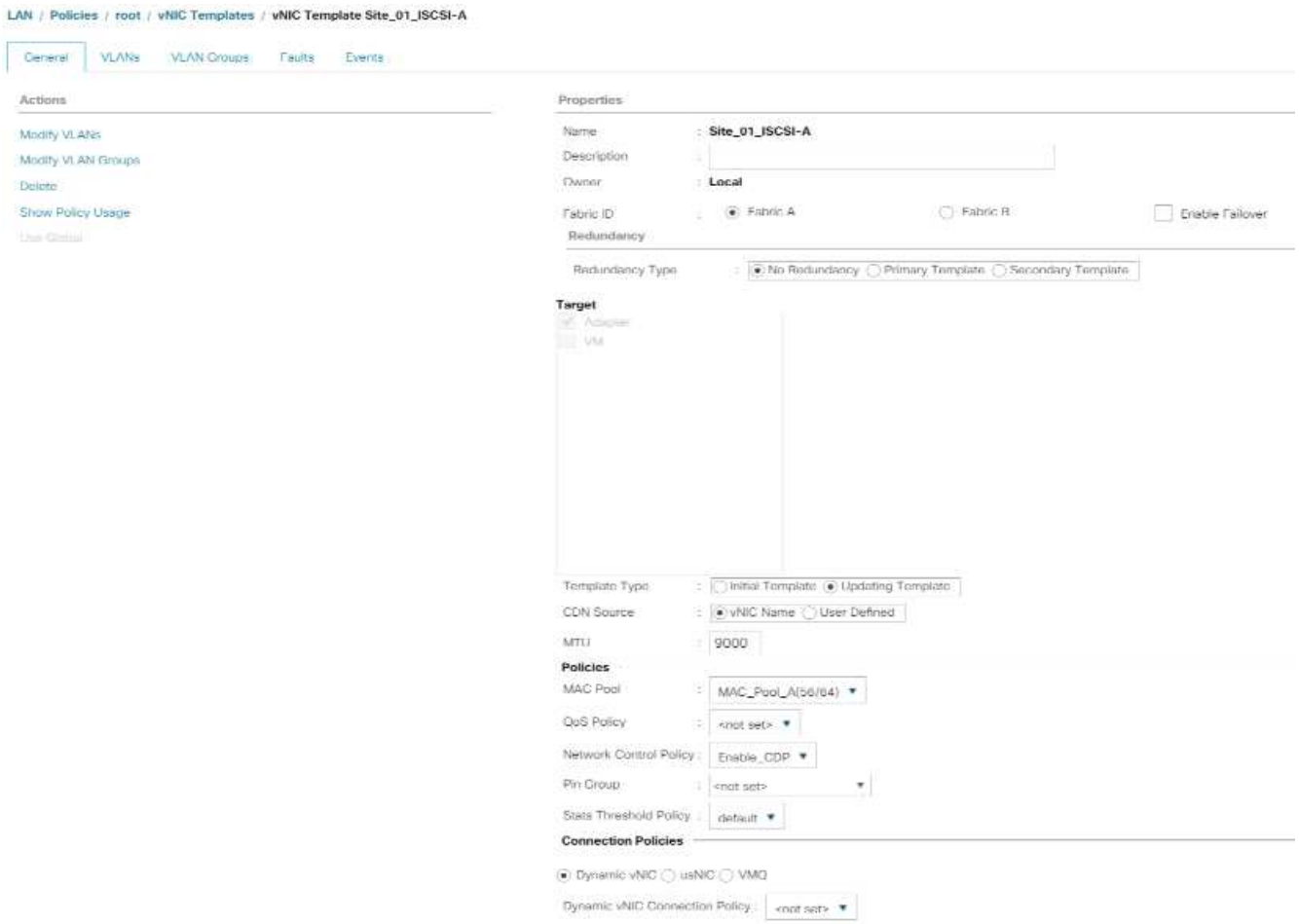
9. Primäre Vorlage für Redundanztyp auswählen.
10. Lassen Sie die Vorlage für Peer-Redundanz auf gesetzt `vNIC_Template_A`.
11. Stellen Sie unter Target sicher, dass nur die Adapteroption ausgewählt ist.
12. Einstellen `Native-VLAN` Als natives VLAN.
13. Wählen Sie vNIC-Name für die CDN-Quelle aus.
14. 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.



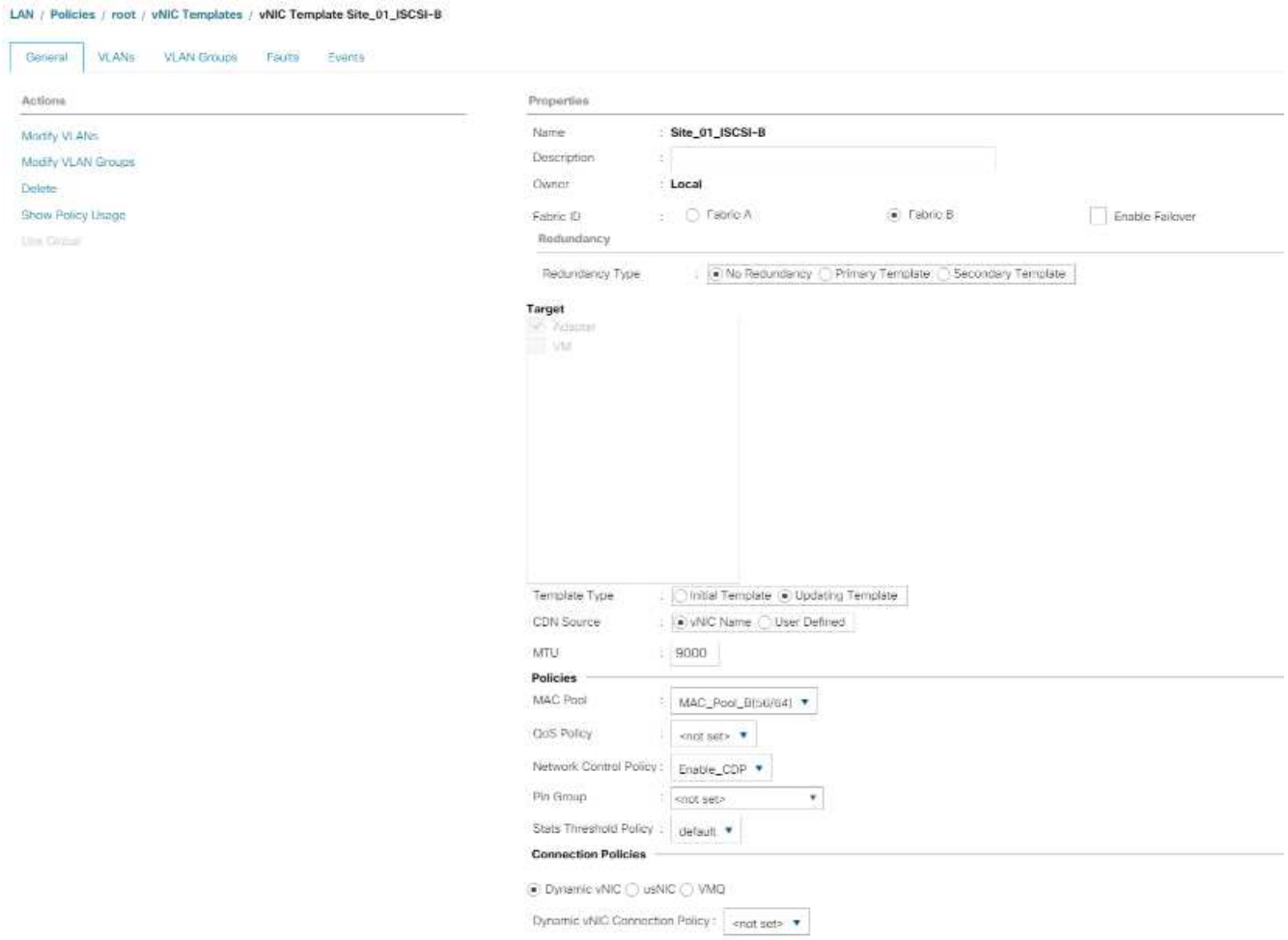
Erstellen von iSCSI-vNICs

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.



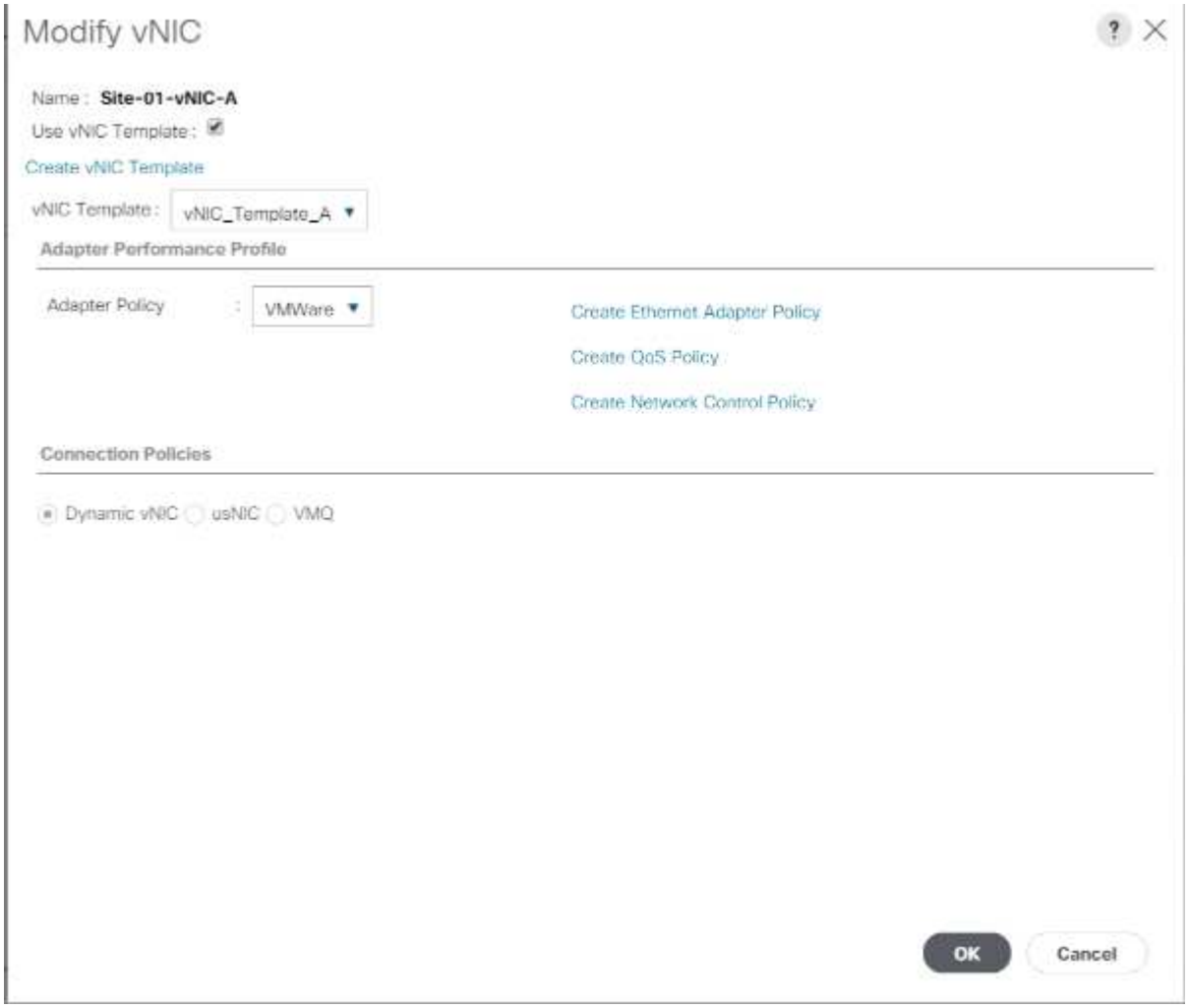
LAN-Konnektivitätsrichtlinie für iSCSI-Boot erstellen

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:

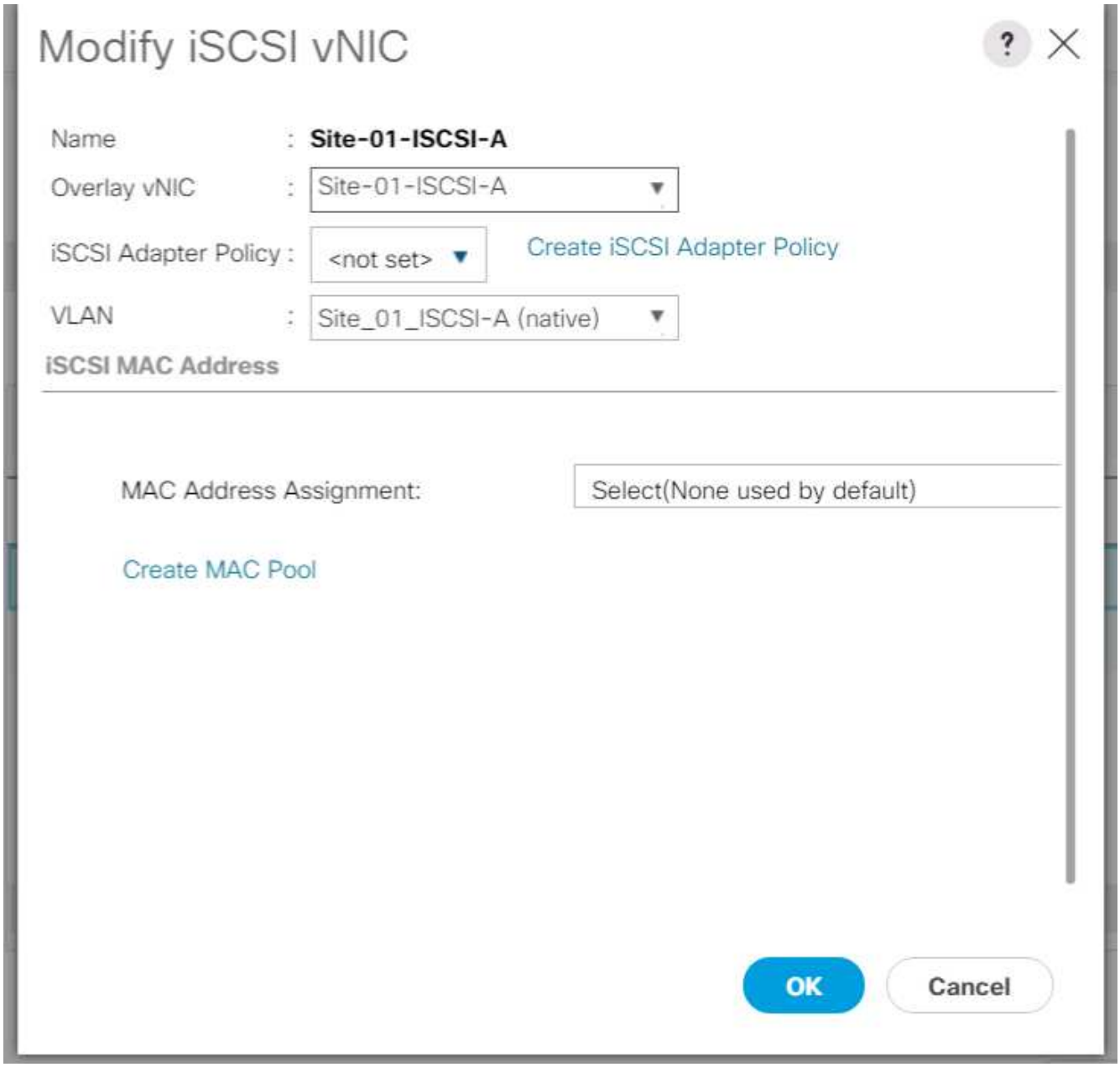
1. Klicken Sie in Cisco UCS Manager links auf LAN.
2. Wählen Sie LAN > Richtlinien > Root.
3. Klicken Sie mit der rechten Maustaste auf LAN Connectivity Policies.
4. Wählen Sie LAN-Verbindungsrichtlinie erstellen.
5. Eingabe `Site-XX-Fabric-A` Als Name der Richtlinie.
6. Klicken Sie oben auf Hinzufügen, 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.

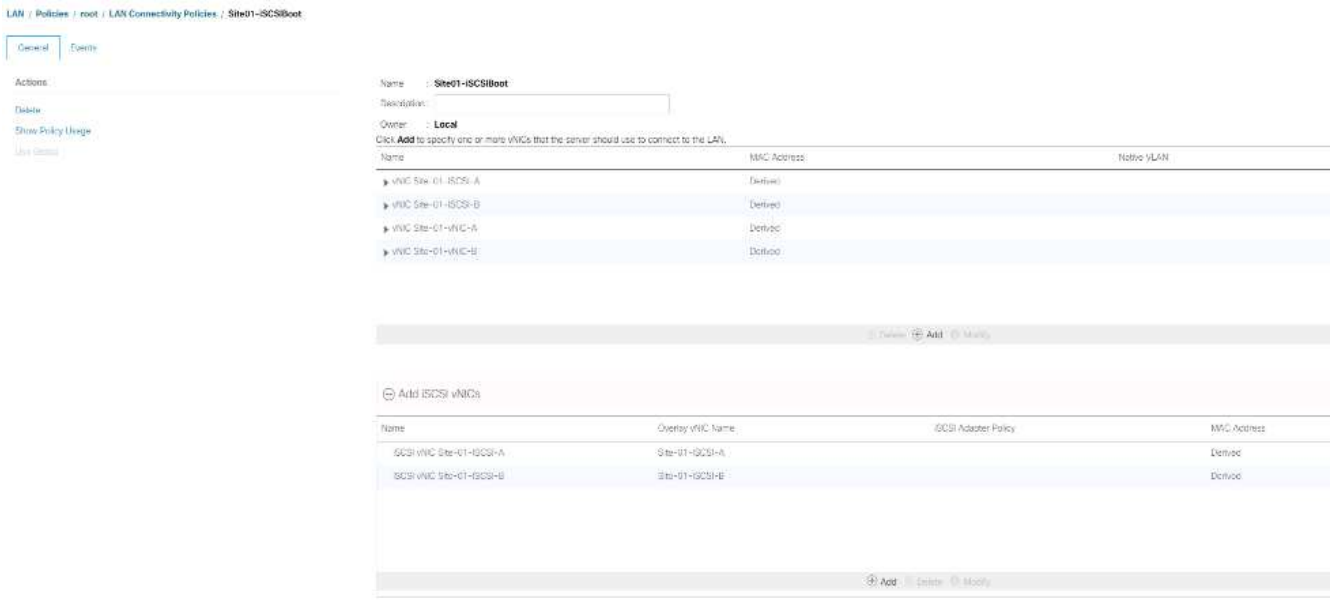


12. Klicken Sie oben auf Hinzufügen, um einen vNIC hinzuzufügen.
13. Geben Sie im Dialogfeld vNIC erstellen ein `Site-01-vNIC-B` Als Name der vNIC.
14. Wählen Sie die Option vNIC-Vorlage verwenden aus.
15. Wählen Sie in der Liste vNIC-Vorlage die Option aus `vNIC_Template_B`.
16. Wählen Sie aus der Dropdown-Liste 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.

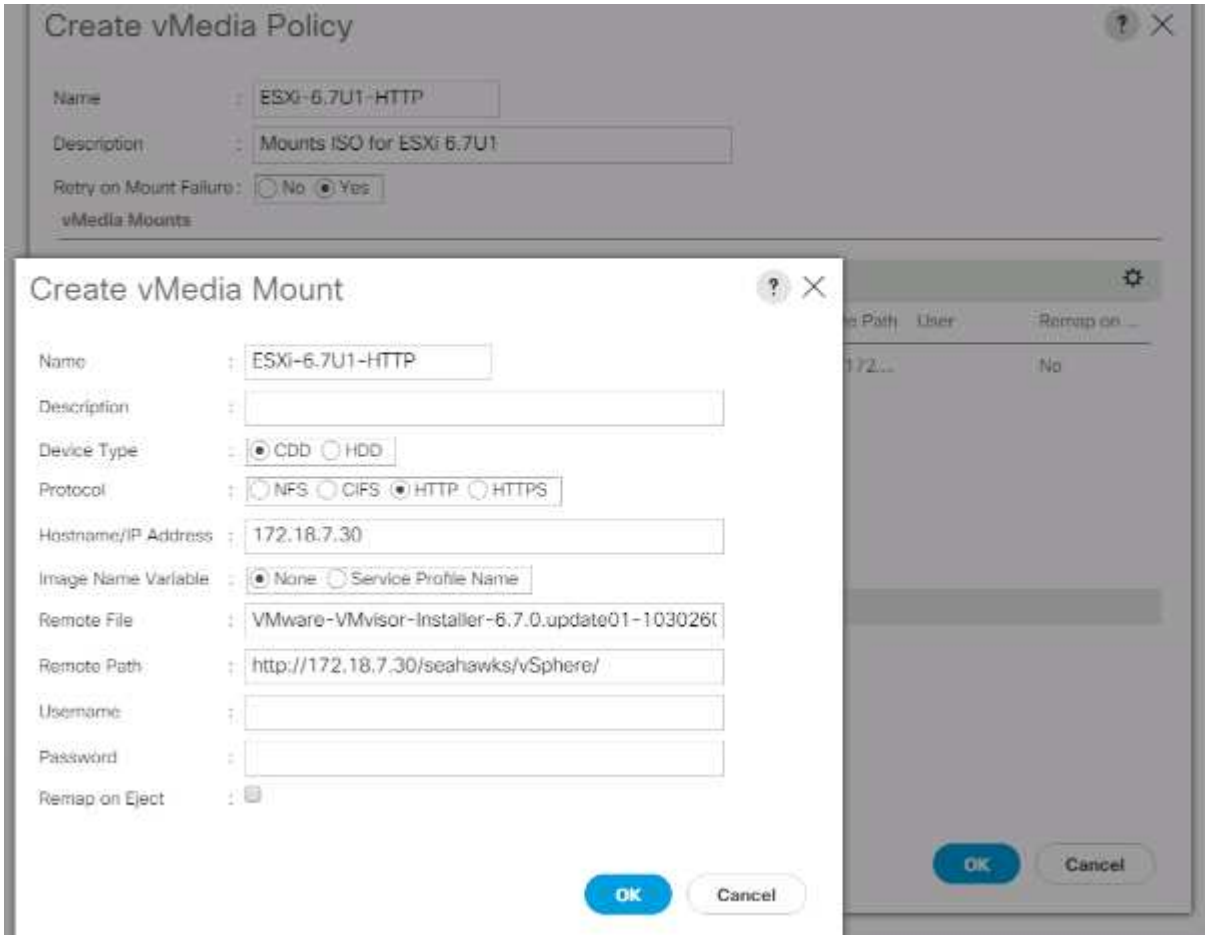
13. Eingabe `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Als Name der Remote-Datei.

    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

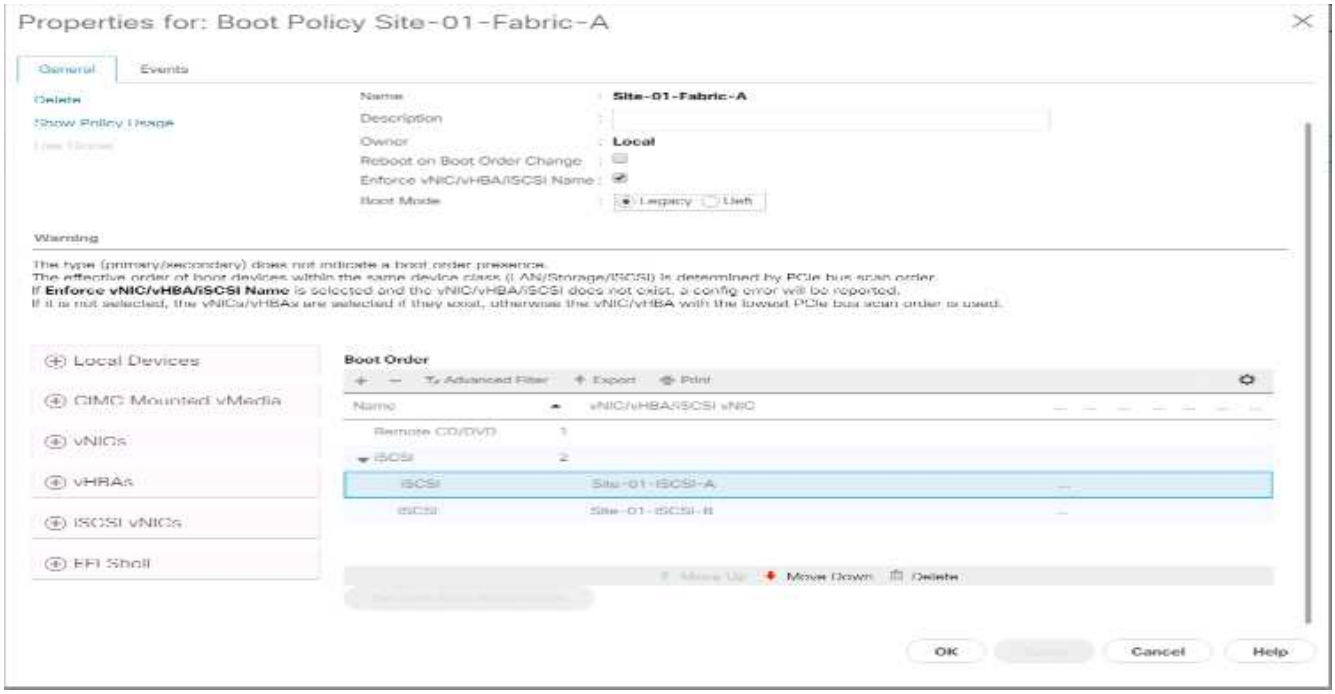
Das Verfahren in diesem Abschnitt gilt für eine Cisco UCS-Umgebung, in der sich zwei logische iSCSI-Schnittstellen (LIFs) auf Cluster-Node 1 befinden (`iscsi_lif01a` Und `iscsi_lif01b`) Und zwei iSCSI LIFs befinden sich auf Cluster Node 2 (`iscsi_lif02a` Und `iscsi_lif02b`). Es wird außerdem davon ausgegangen, 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.



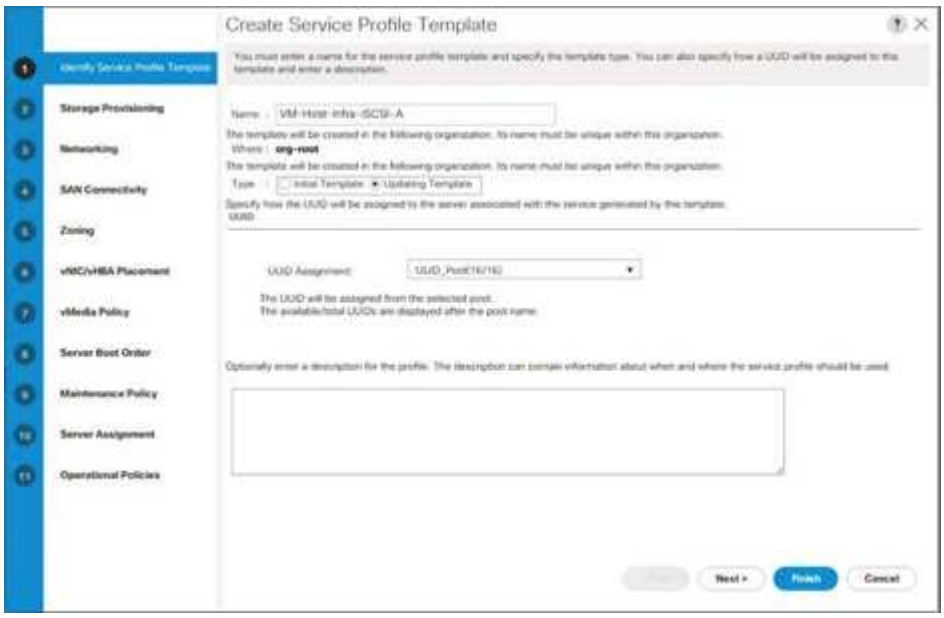
Erstellen einer Service-Profilvorlage

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

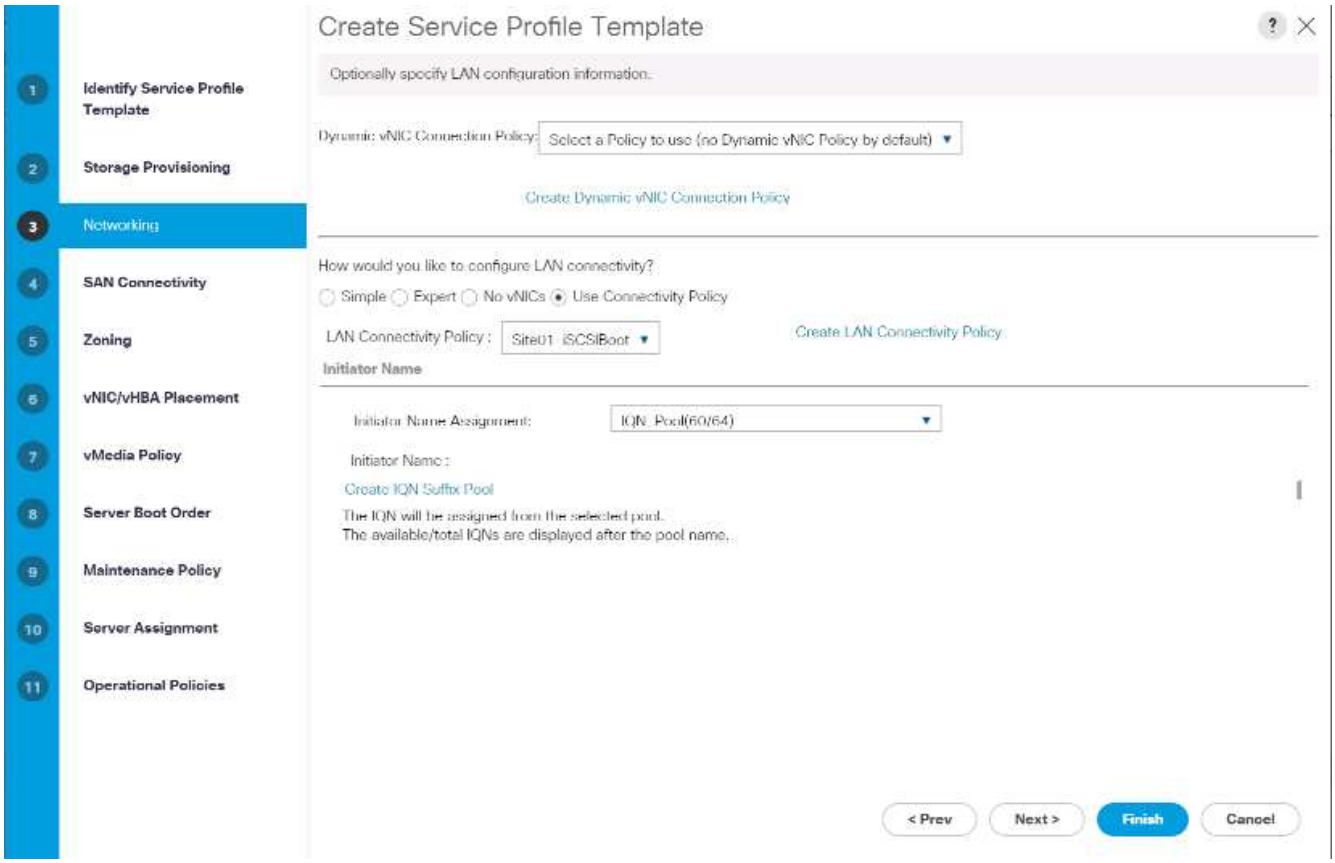
Gehen Sie wie folgt vor, um die Speicherbereitstellung zu konfigurieren:

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

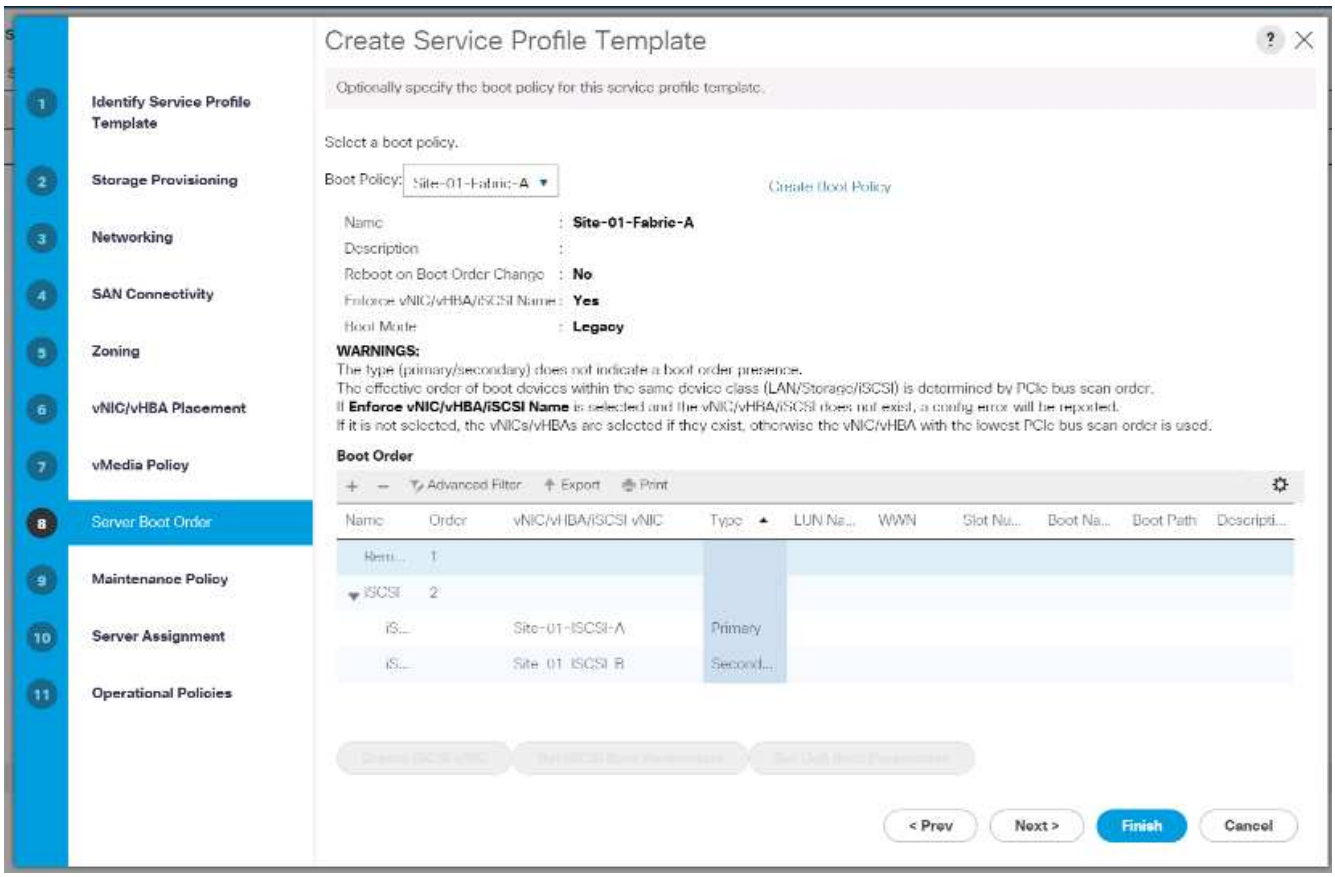
Gehen Sie wie folgt vor, um die vMedia-Richtlinie zu konfigurieren:

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.



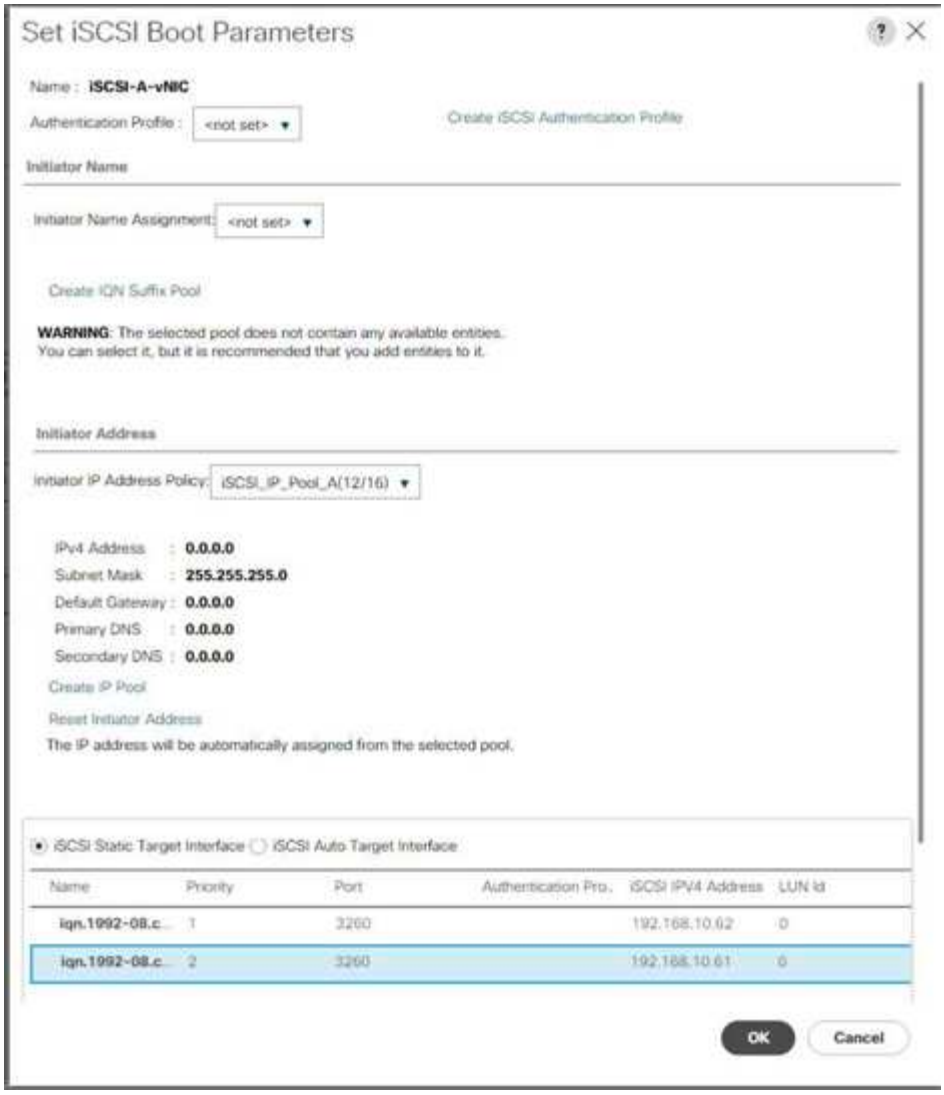
2. Wählen Sie in der Boor-Reihenfolge aus `Site-01- iSCSI-A`.
3. Klicken Sie auf iSCSI-Startparameter festlegen.
4. Lassen Sie im Dialogfeld iSCSI-Boot-Parameter festlegen die Option Authentication Profile nicht auf gesetzt, es sei denn, Sie haben unabhängig eine für Ihre Umgebung geeignete Option erstellt.
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.

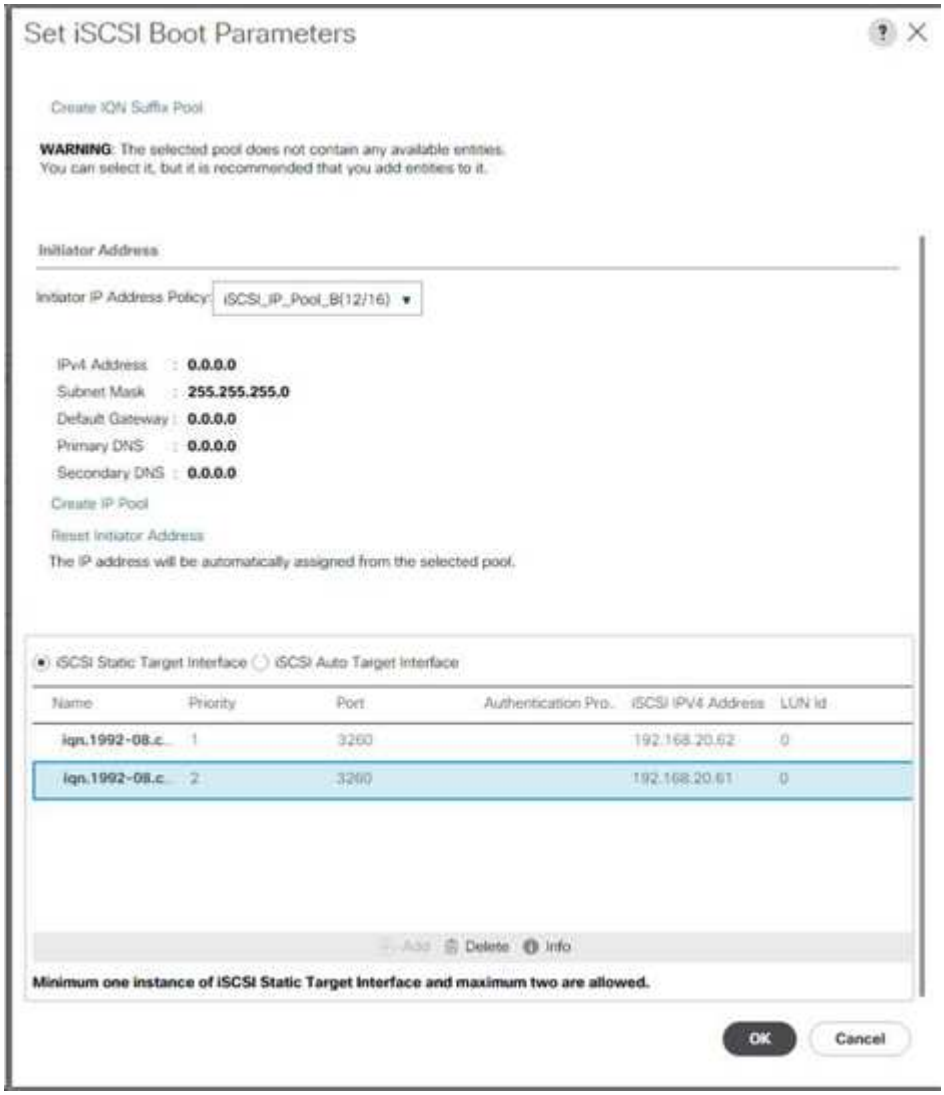
16. Wählen Sie in der Startreihenfolge iSCSI-B-vNIC aus.
17. Klicken Sie auf iSCSI-Startparameter festlegen.
18. Lassen Sie im Dialogfeld iSCSI-Boot-Parameter festlegen die Option Authentication Profile nicht als festgelegt, es sei denn, Sie haben unabhängig eine für Ihre Umgebung geeignete Option erstellt.
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.

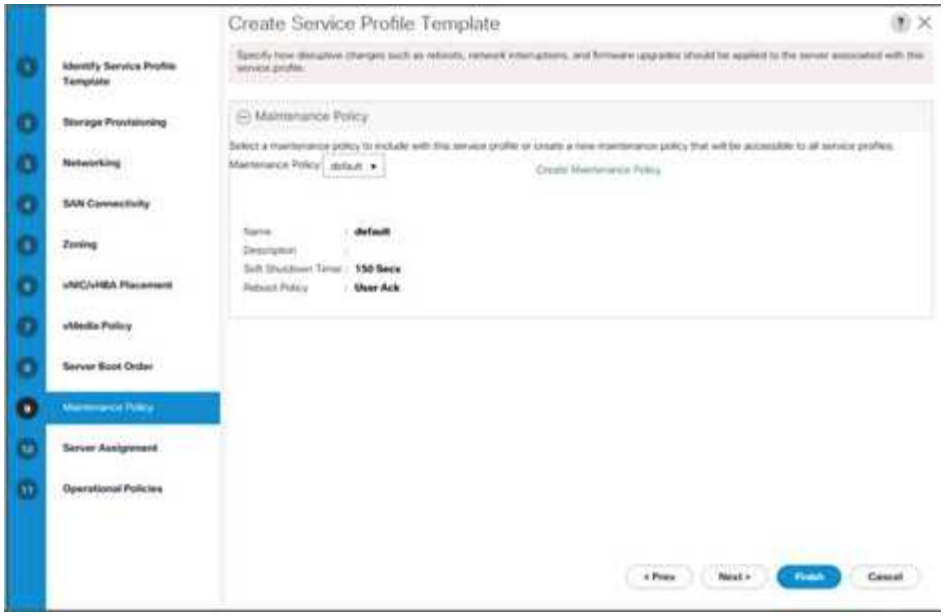


30. Klicken Sie Auf Weiter.

Wartungsrichtlinie konfigurieren

Gehen Sie wie folgt vor, um die Wartungsrichtlinie zu konfigurieren:

1. Ändern Sie die Wartungsrichtlinie in den Standardwert.

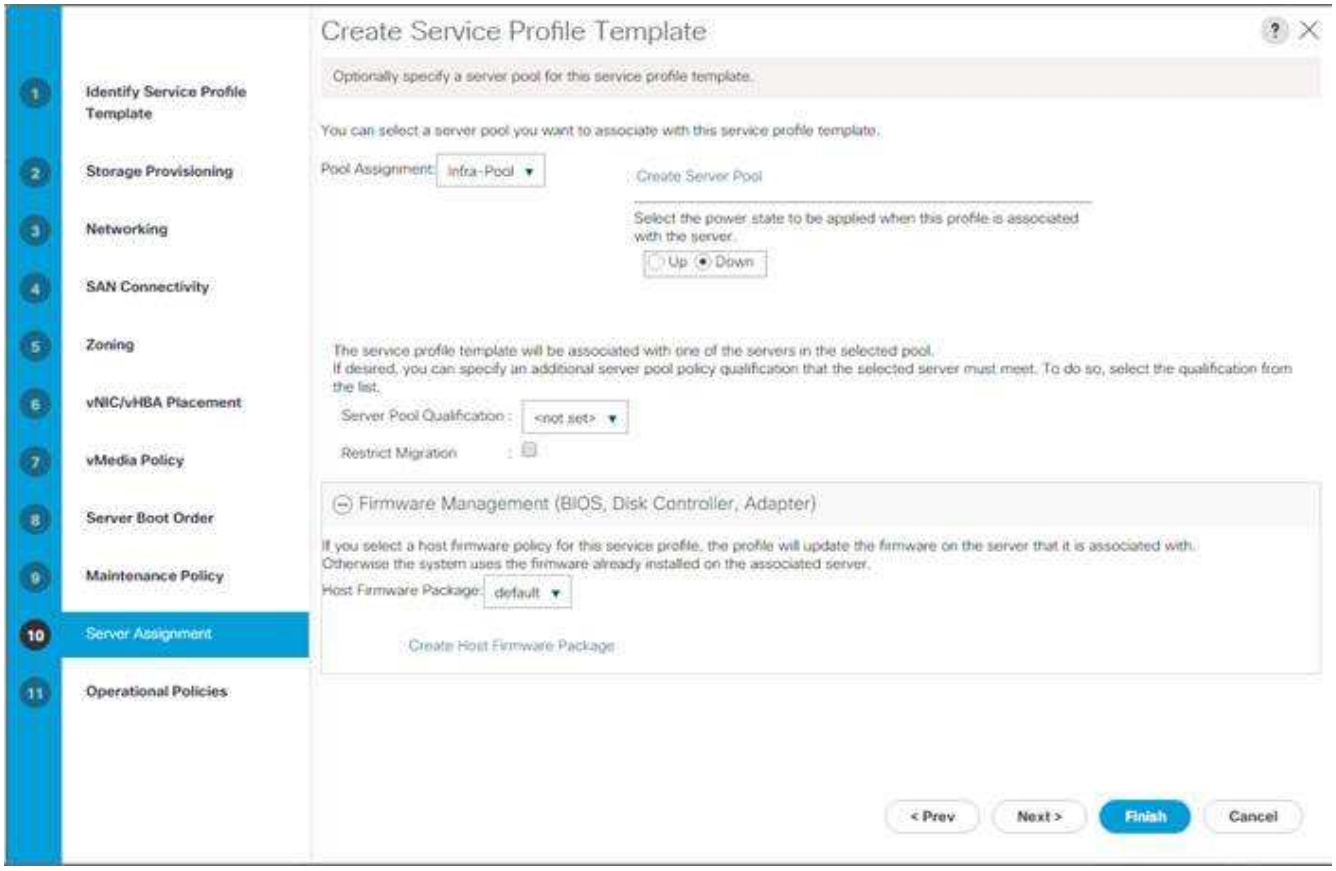


2. Klicken Sie Auf Weiter.

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.

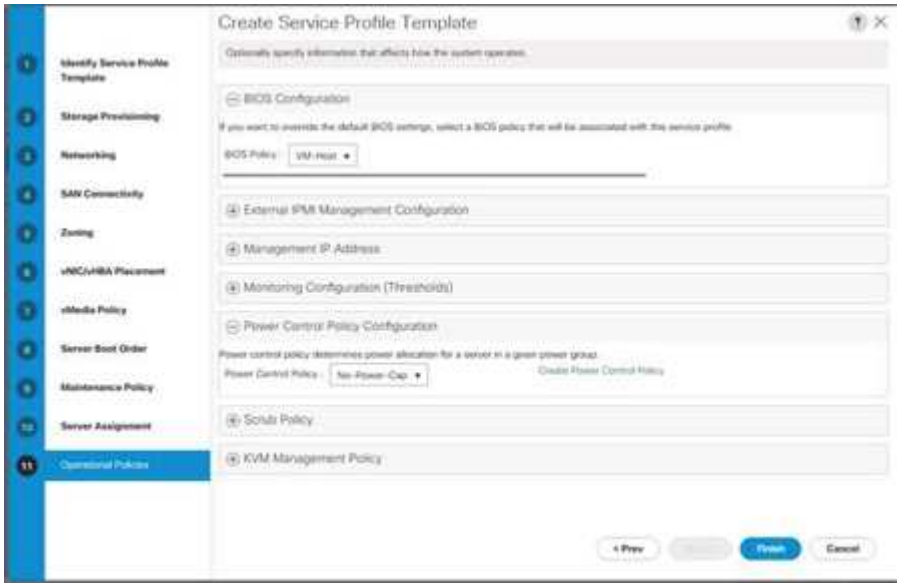


4. Klicken Sie Auf Weiter.

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

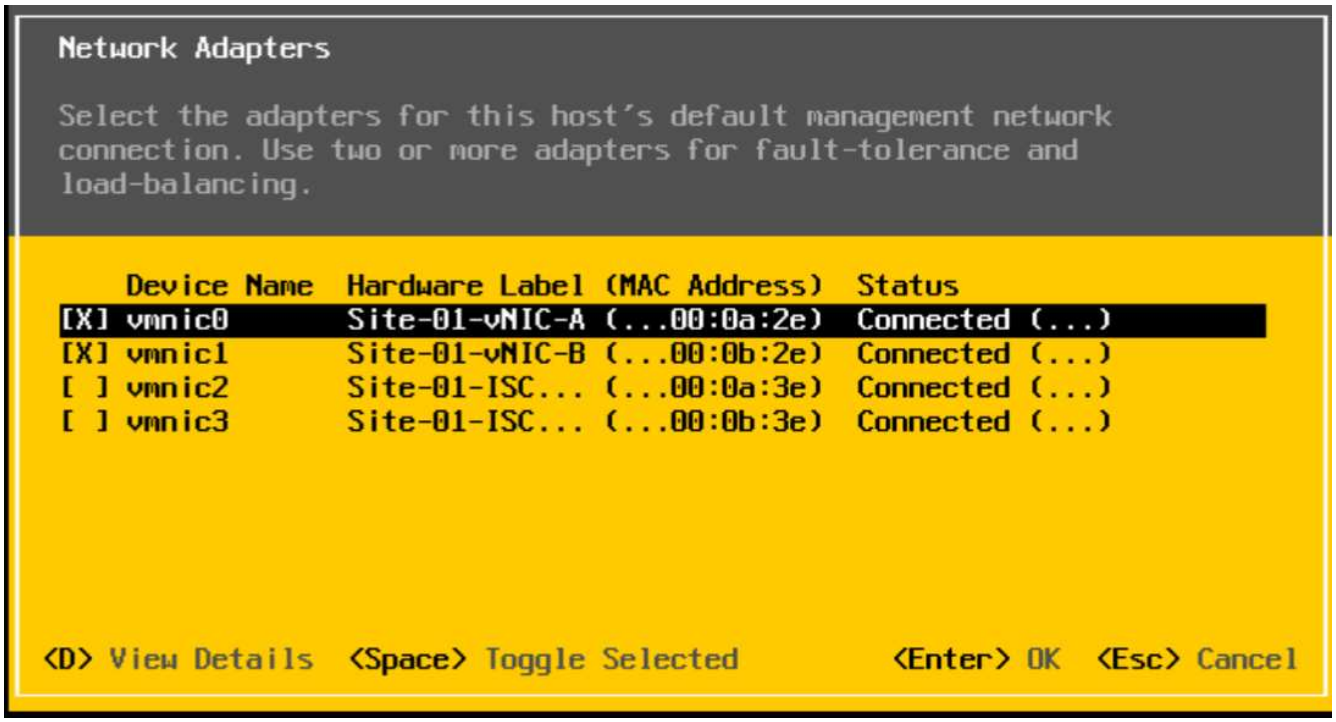
Für jeden VMware Host ist das Hinzufügen eines Managementnetzwerks erforderlich, um den Host zu verwalten. Um ein Management-Netzwerk für die VMware-Hosts hinzuzufügen, führen Sie die folgenden Schritte auf jedem ESXi-Host aus:

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.

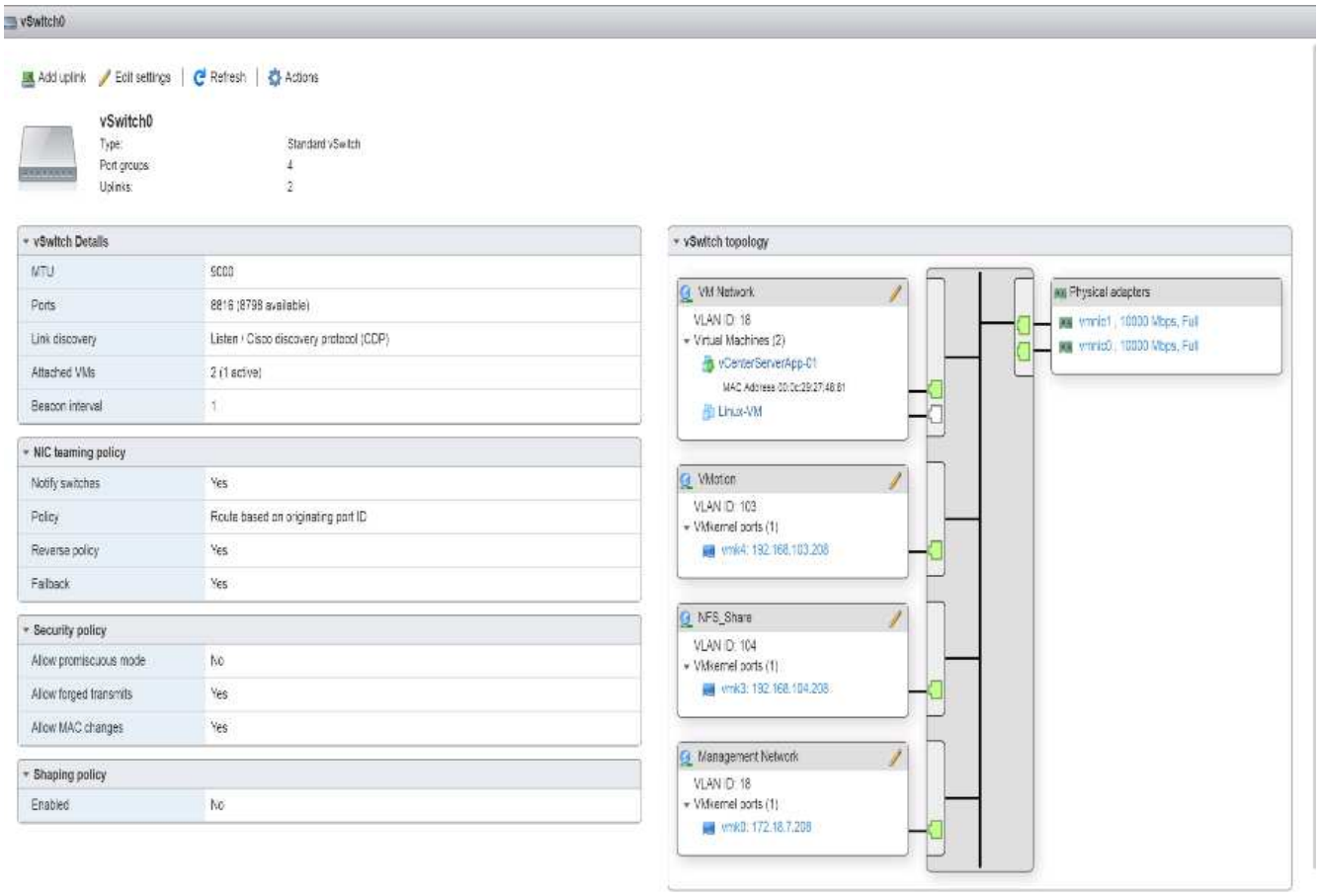
21. Klicken Sie auf Speichern .
22. Wählen Sie die Registerkarte Virtuelle Switches aus.
23. Wählen Sie den virtuellen Standard-Switch hinzufügen aus.
24. Geben Sie einen Namen von an `iScsciBootvSwitch-B` Für den vSwitch-Namen.
25. Setzen Sie die MTU auf 9000.
26. Wählen Sie vmnic3 aus dem Dropdown-Menü 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.

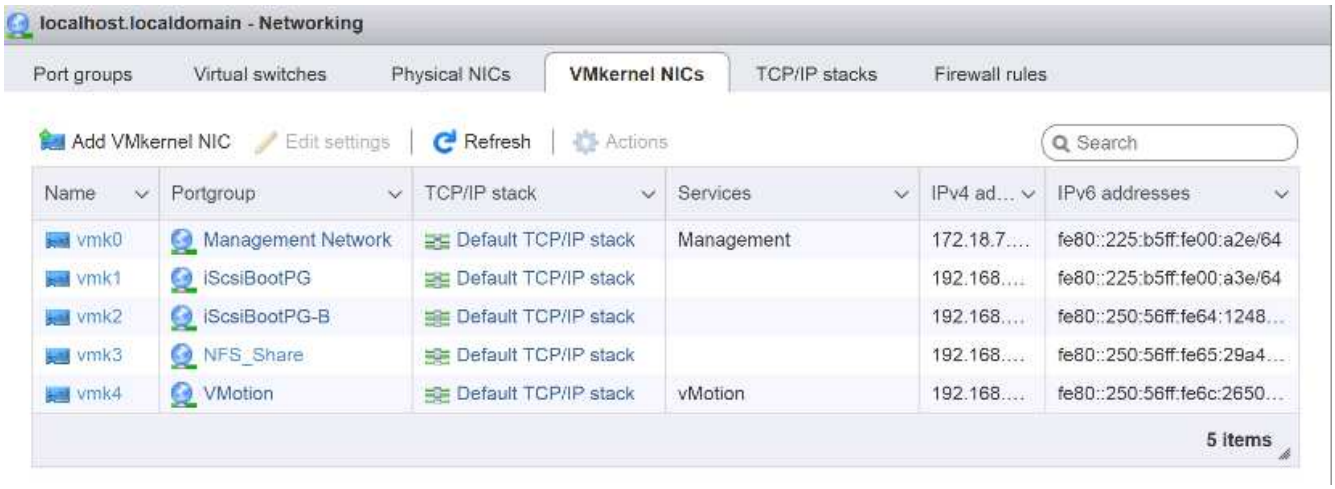
Um IP-Adressenkonflikte zu vermeiden, sollten die Cisco UCS iSCSI IP-Pool-Adressen neu zugewiesen werden, wird empfohlen, für die iSCSI VMkernel-Ports unterschiedliche IP-Adressen im gleichen Subnetz zu verwenden.

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:

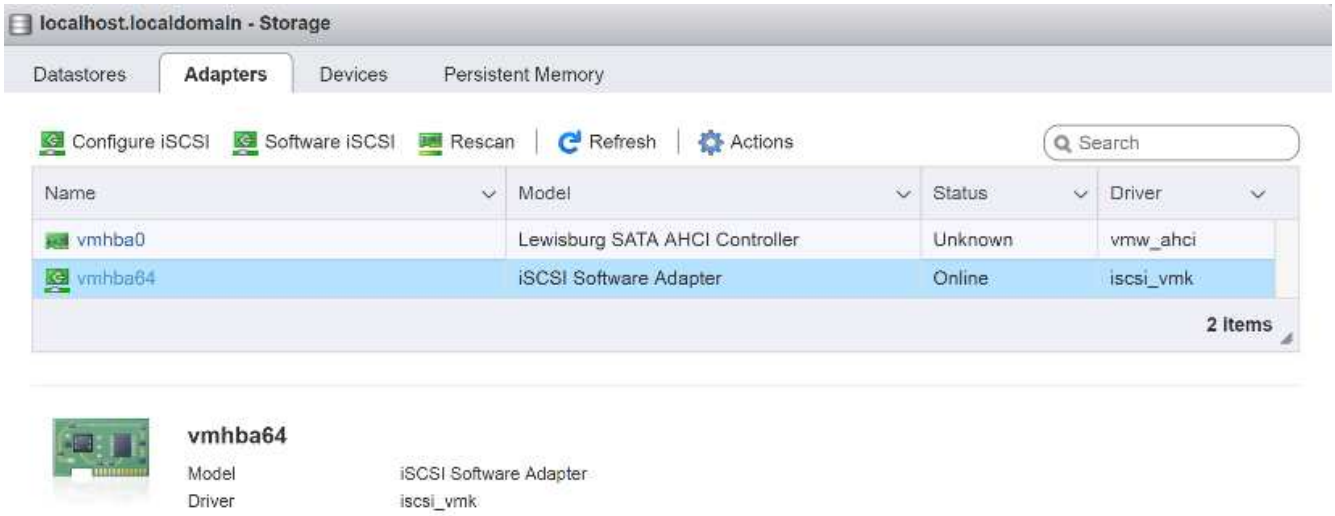


ISCSI-Multipathing einrichten

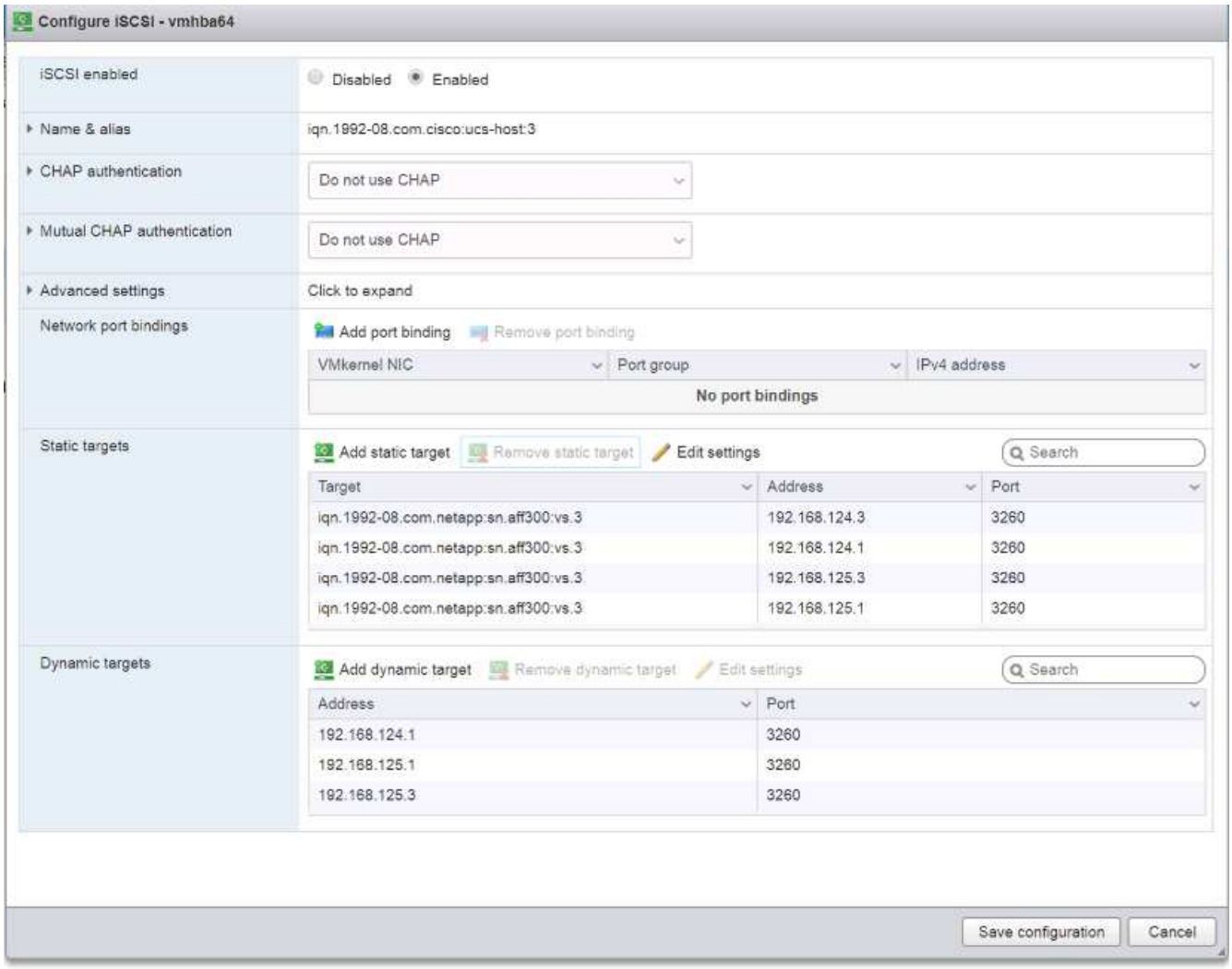
ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

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.

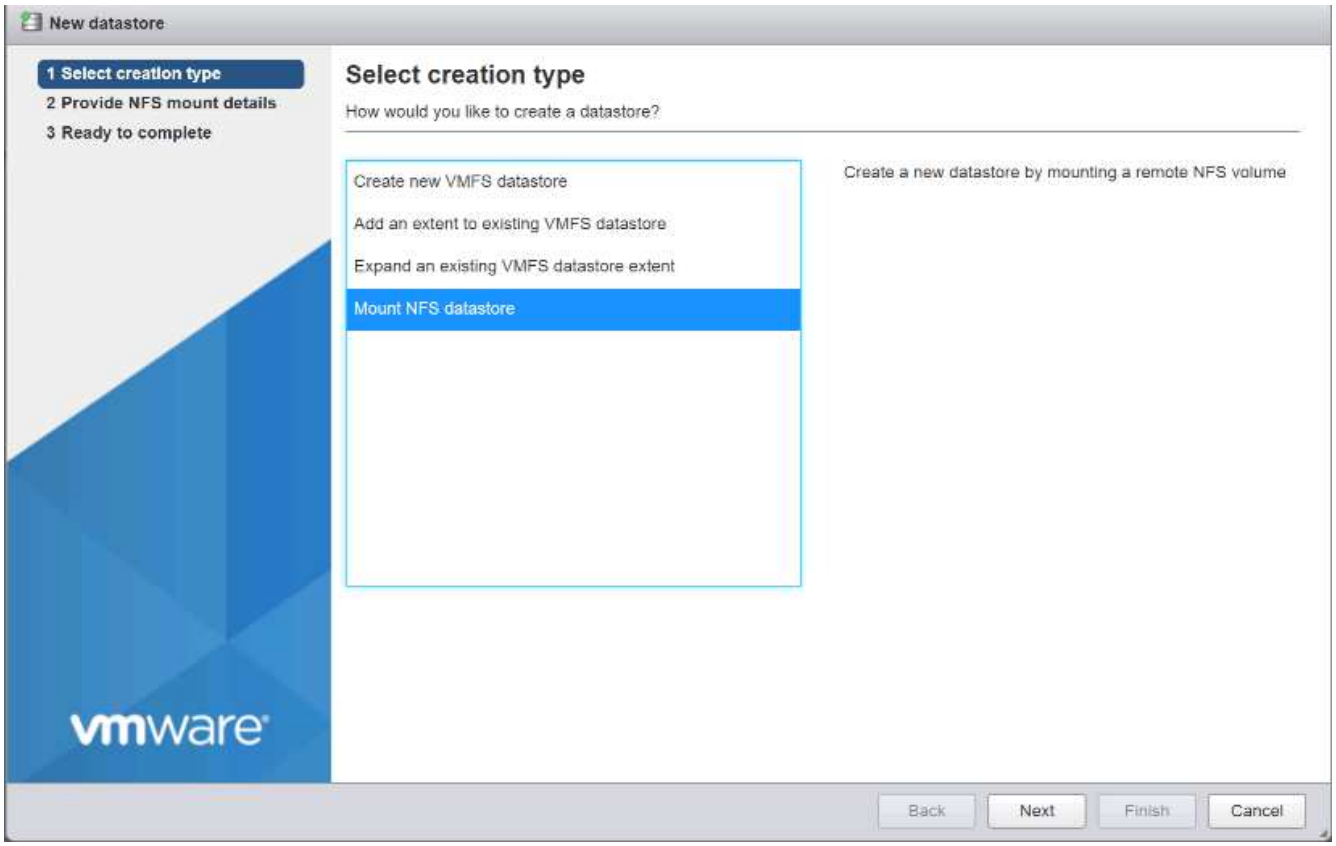
Der Host liest den Speicheradapter automatisch wieder ein, und die Ziele werden statischen Zielen hinzugefügt.

Bereitstellung erforderlicher Datastores

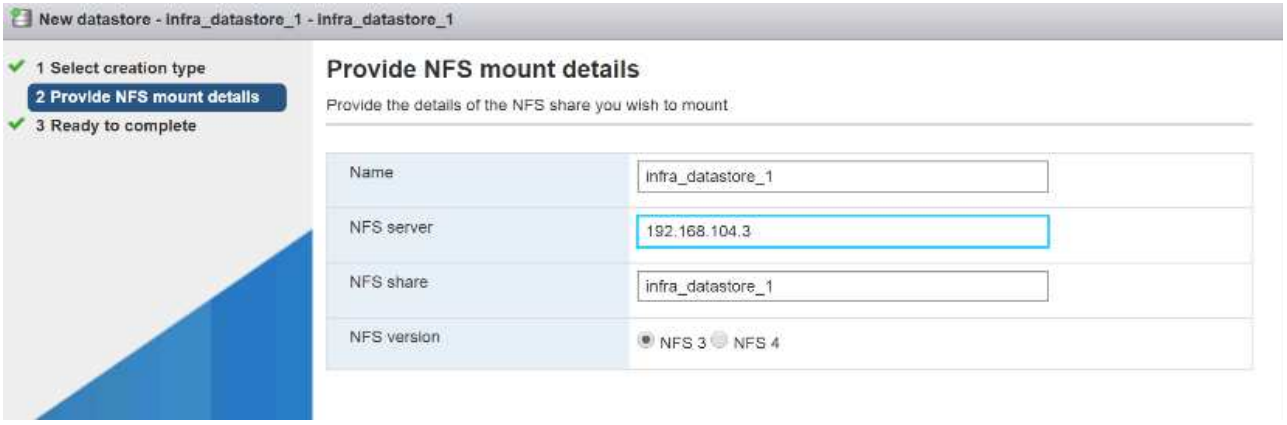
ESXi hostet VM-Host-Infra-01 und VM-Host-Infra-02

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.

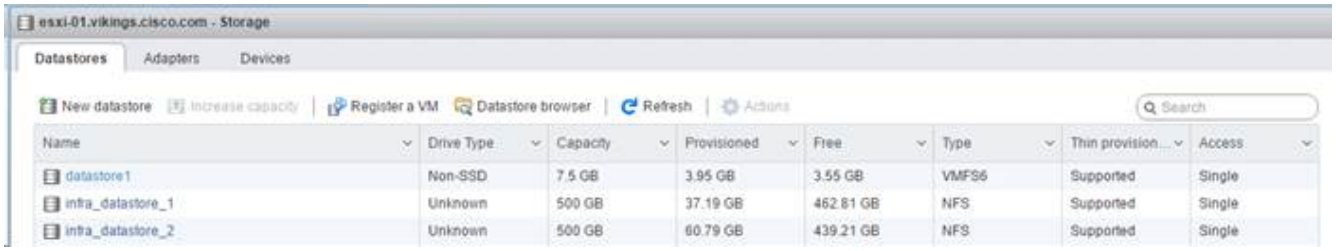


5. Führen Sie auf der Seite „NFS Mount Details angeben“ die folgenden Schritte aus:
   a. Eingabe `infra_datastore_1` Für den Namen des Datenspeichers.
   b. Geben Sie die IP-Adresse für das ein `nfs_lif01_a` LIF für den NFS-Server:
   c. Eingabe `/infra_datastore_1` Für den NFS-Share.
   d. NFS-Version 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.



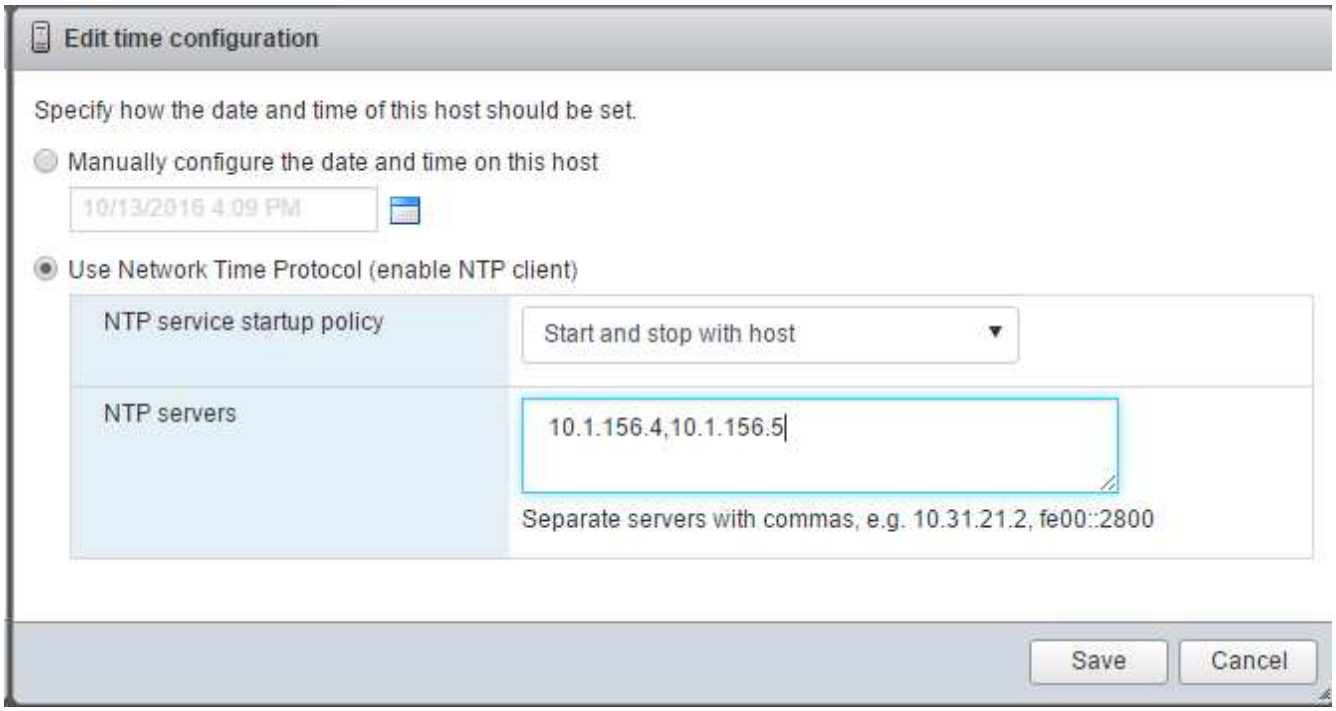
11. Mounten Sie beide Datenspeicher auf beiden ESXi Hosts.

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

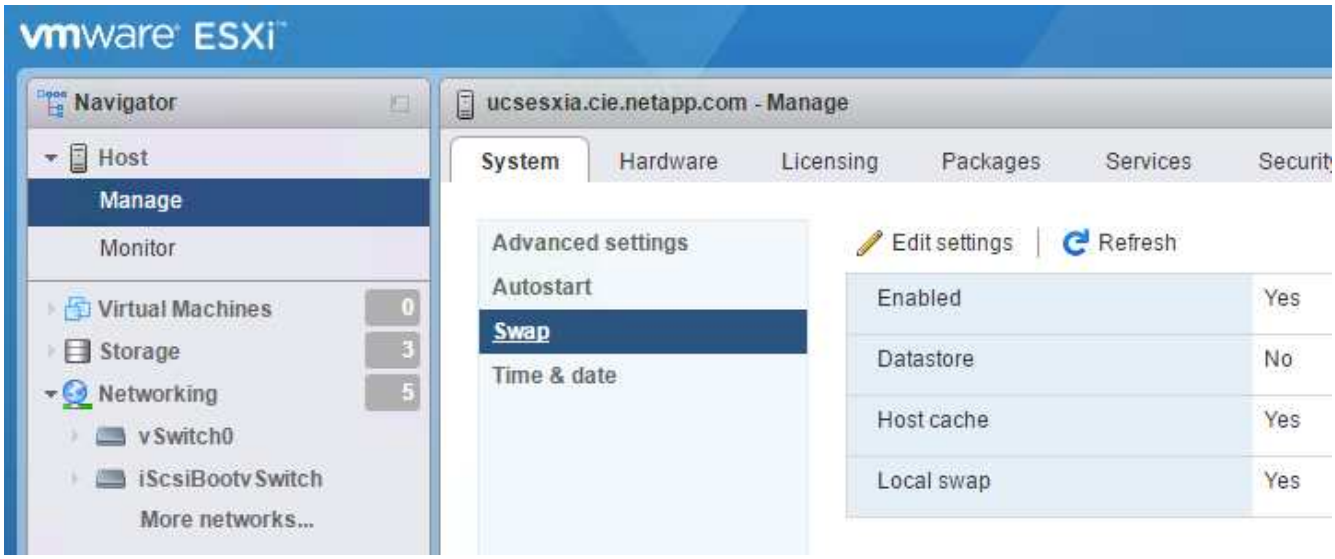
Die NTP-Serverzeit kann von der Hostzeit leicht abweichen.

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

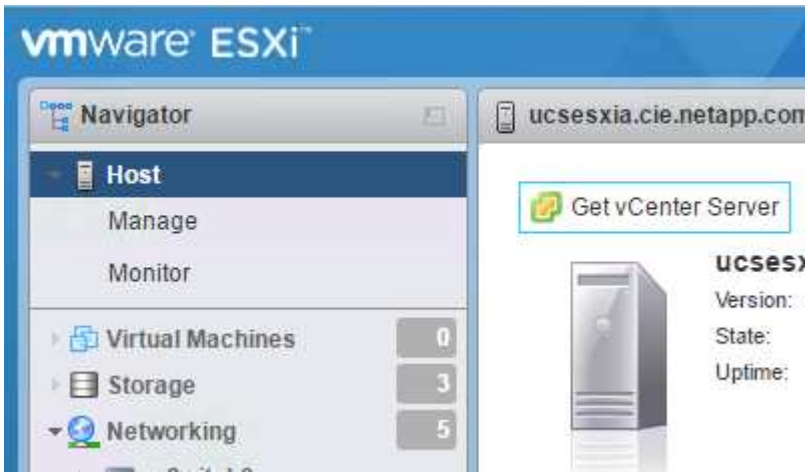
Dieser Abschnitt enthält ausführliche Verfahren zur Installation von VMware vCenter Server 6.7 in einer FlexPod Express-Konfiguration.

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:

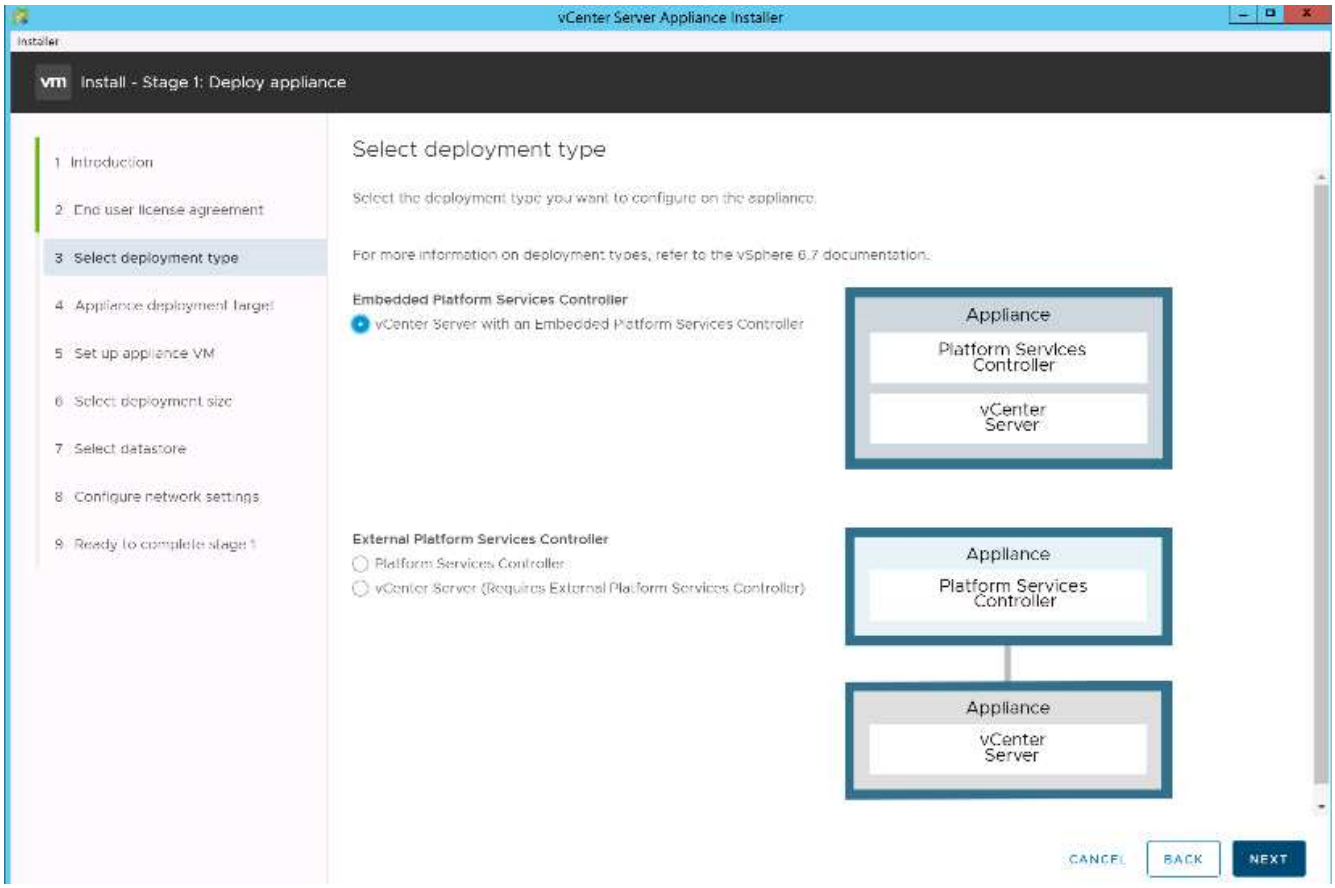
1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.



2. Laden Sie die VCSA von der VMware-Website herunter.

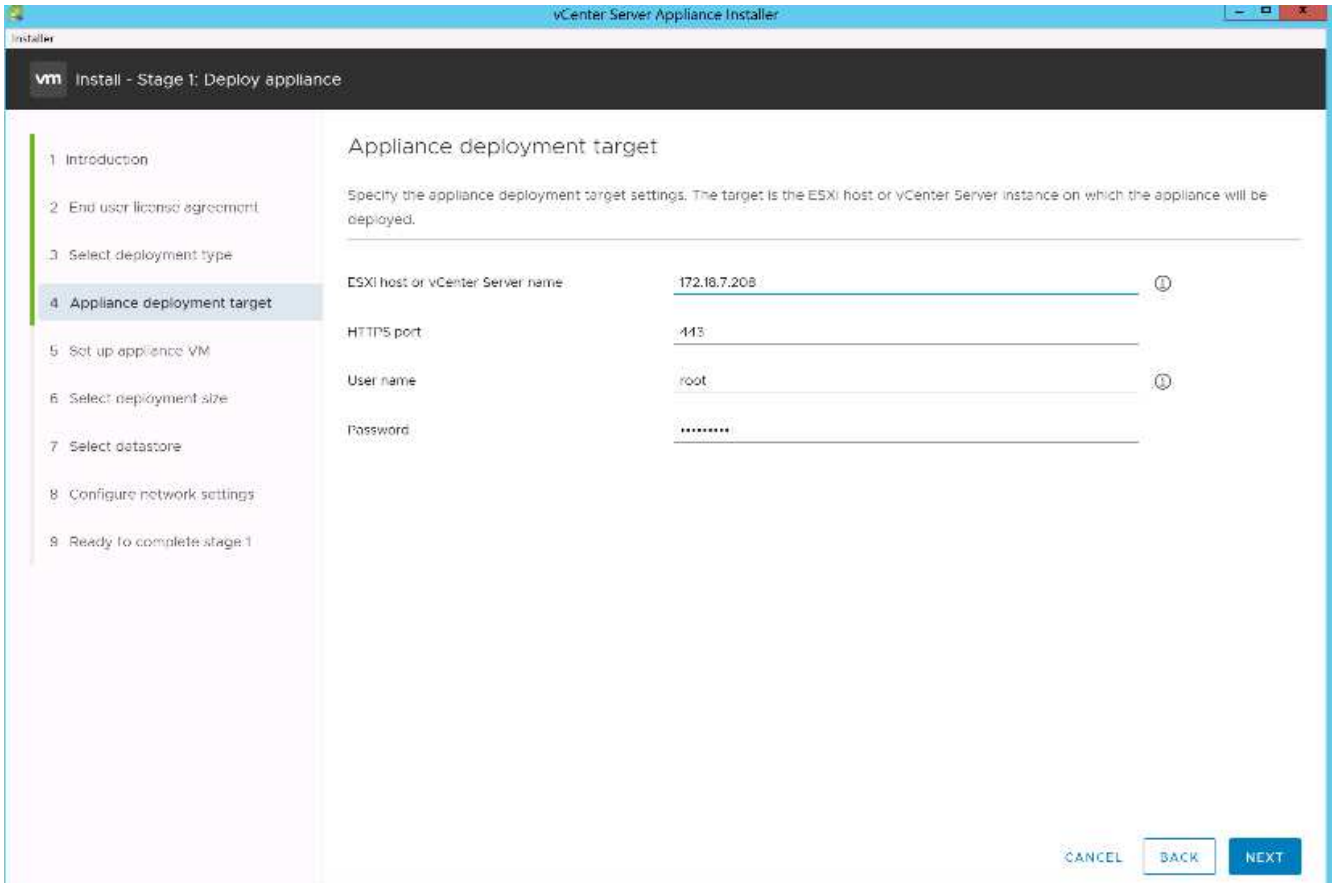
Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.

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.

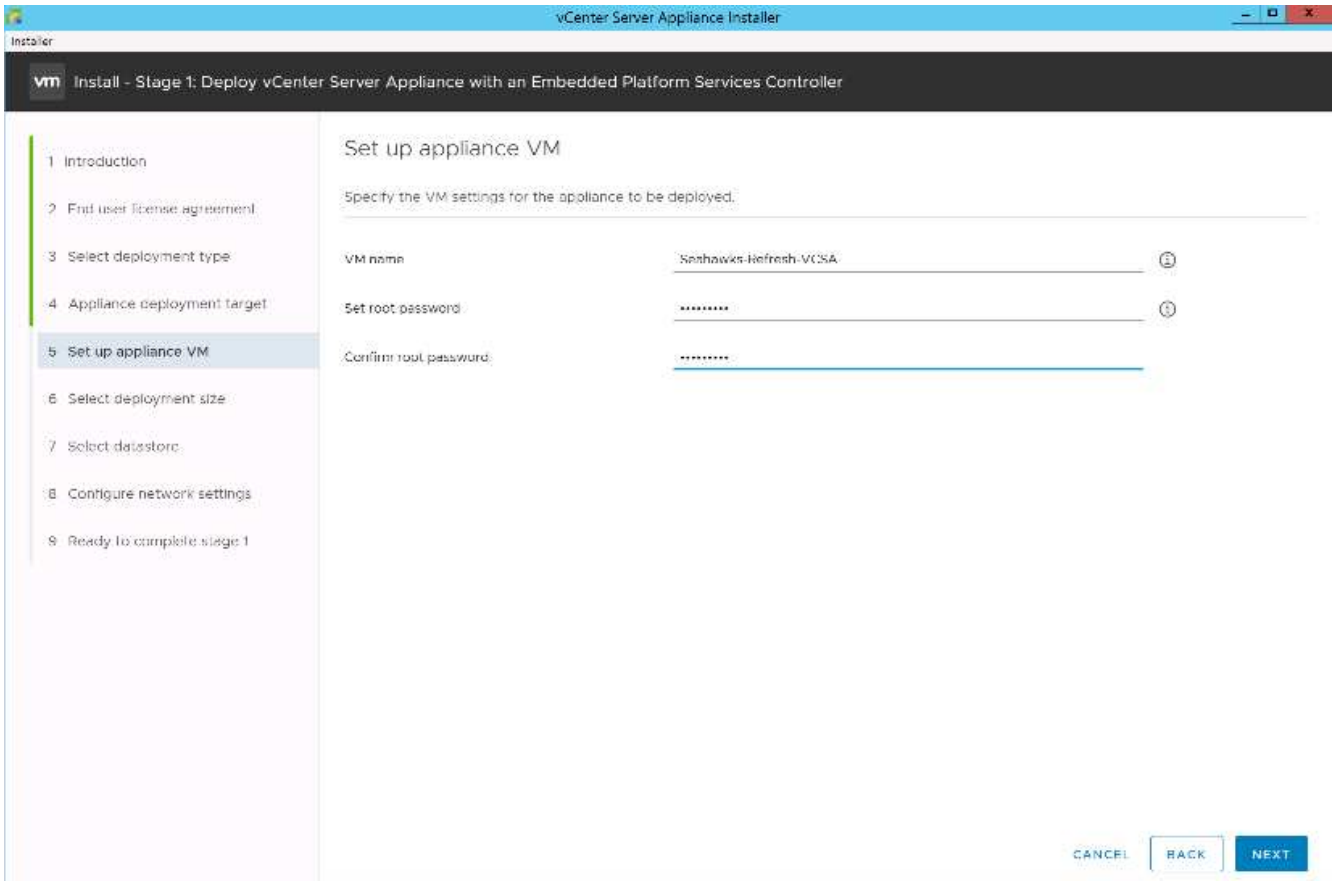


Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

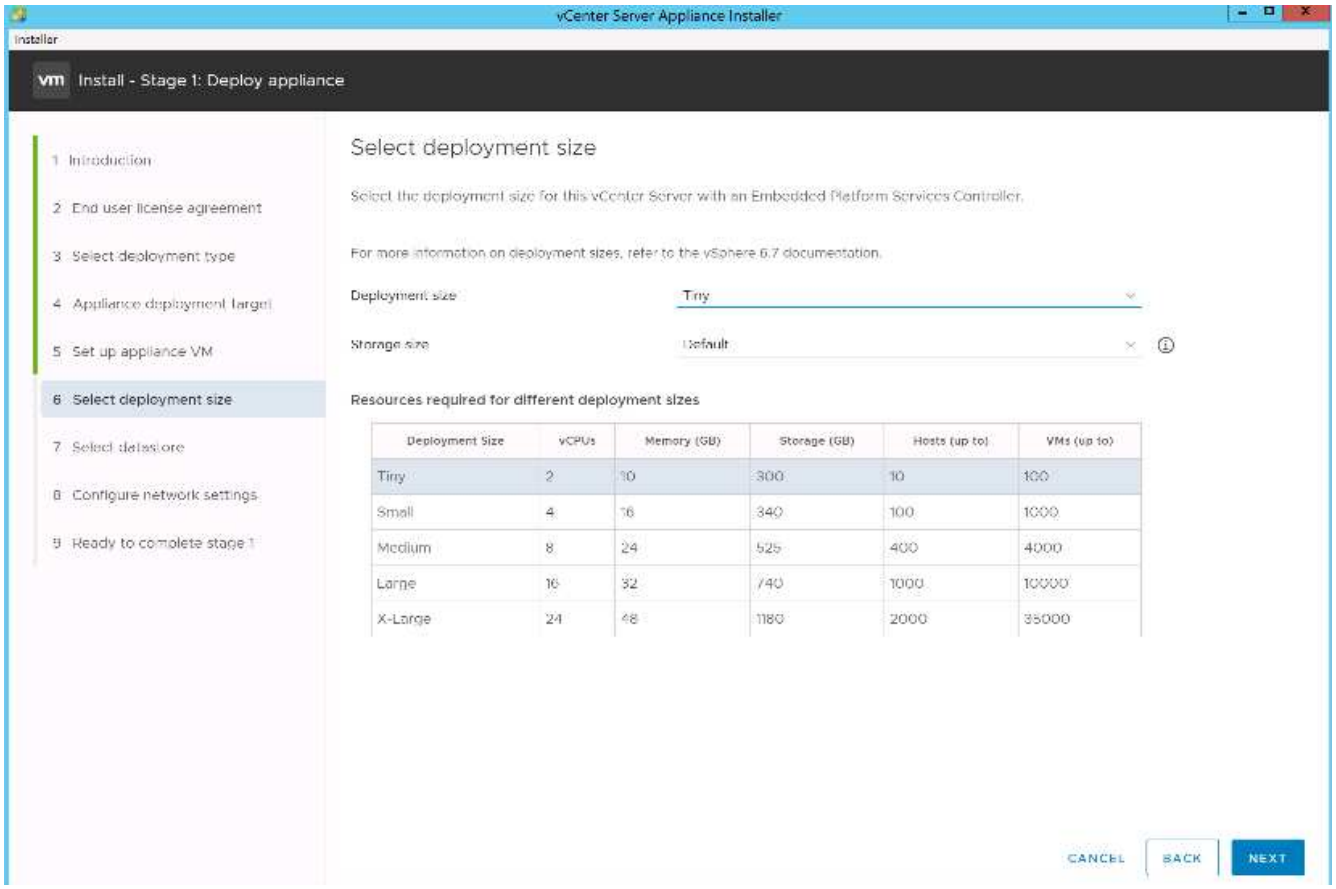
9. Geben Sie auf der Seite Appliance Deployment Target die IP-Adresse eines bereitgestellten ESXi-Hosts, den Root-Benutzernamen und das Root-Passwort ein. Klicken Sie Auf Weiter.



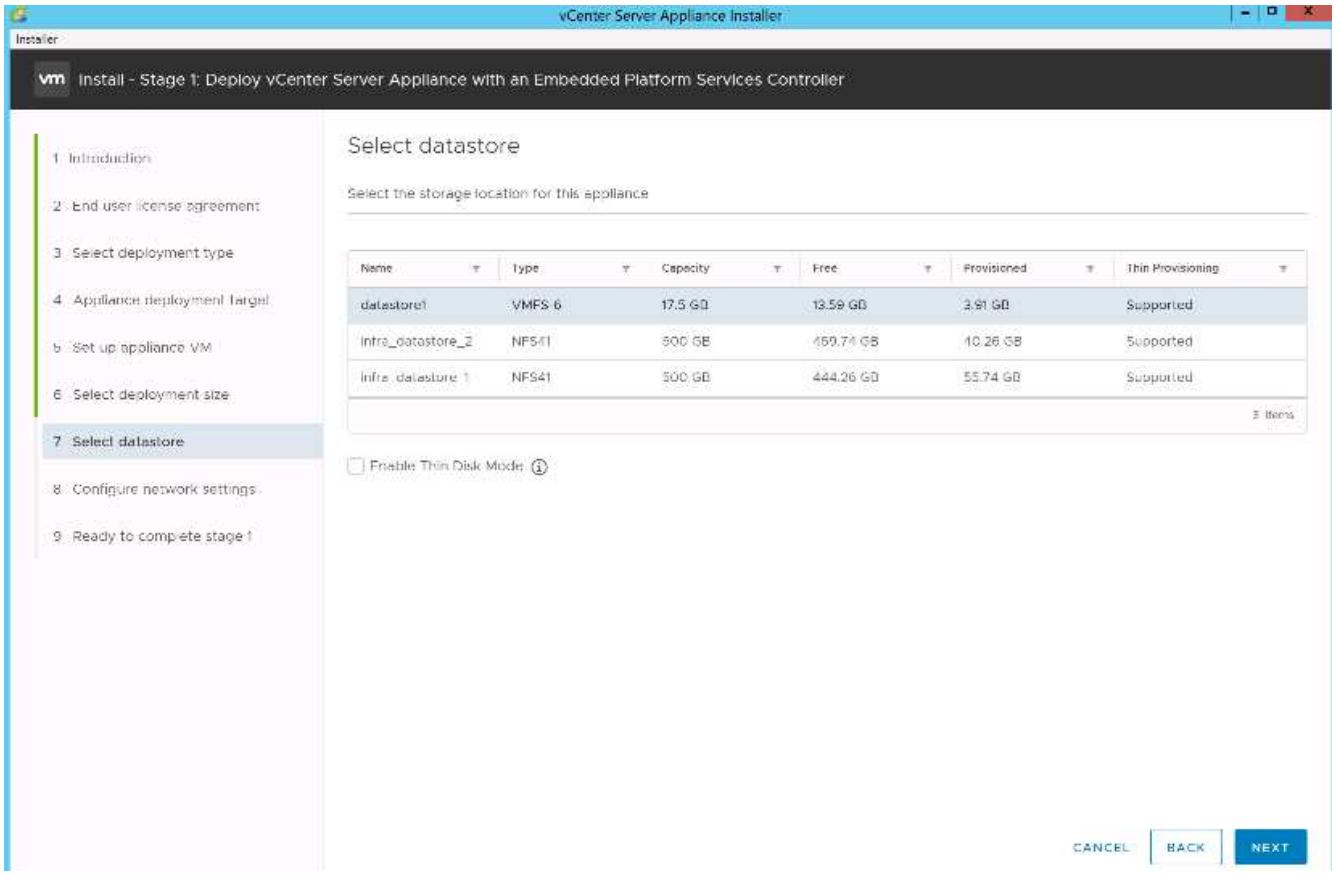
10. Legen Sie die Appliance-VM fest, indem Sie VCSA als VM-Name und das Root-Passwort eingeben, das Sie für VCSA verwenden möchten. Klicken Sie Auf Weiter.



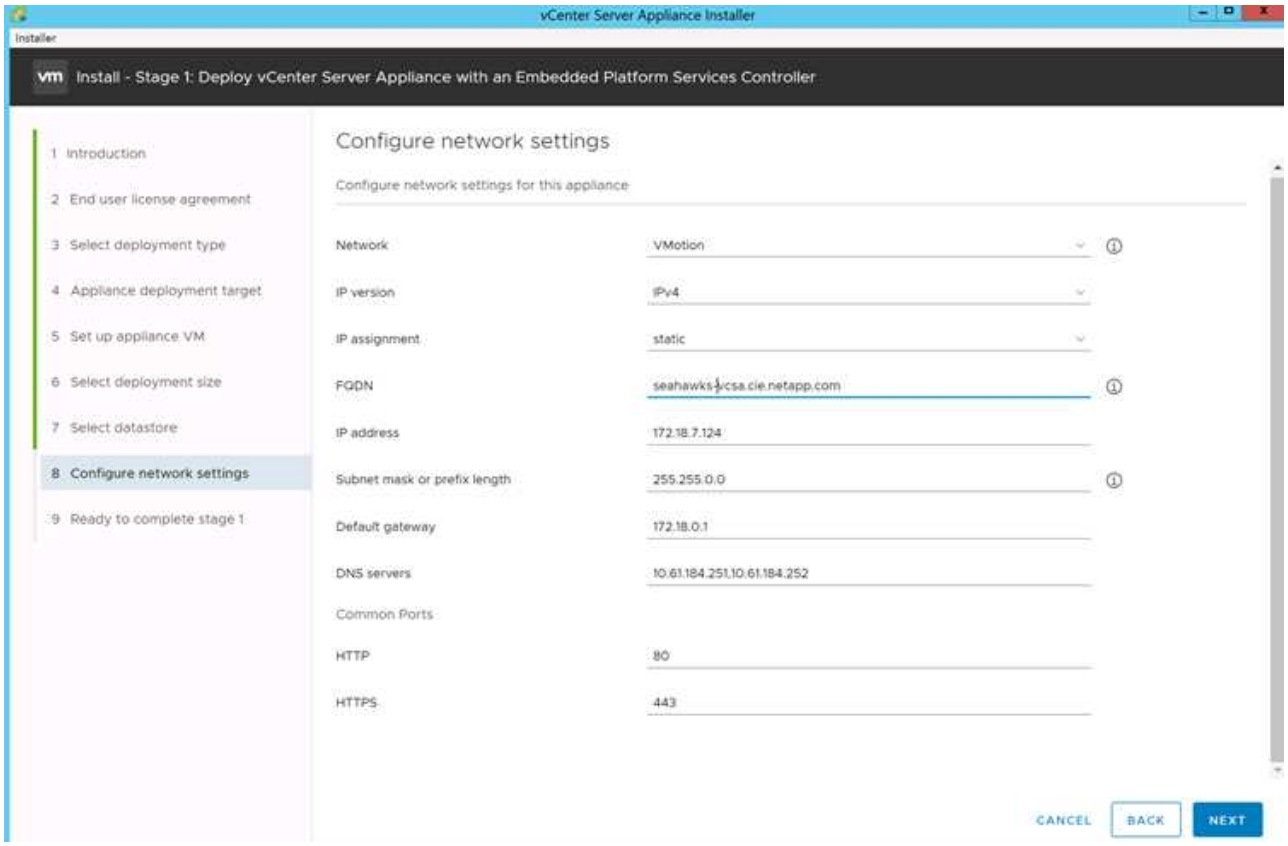
11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



12. Wählen Sie die aus `infra_datastore_1` Datenspeicher: Klicken Sie Auf Weiter.



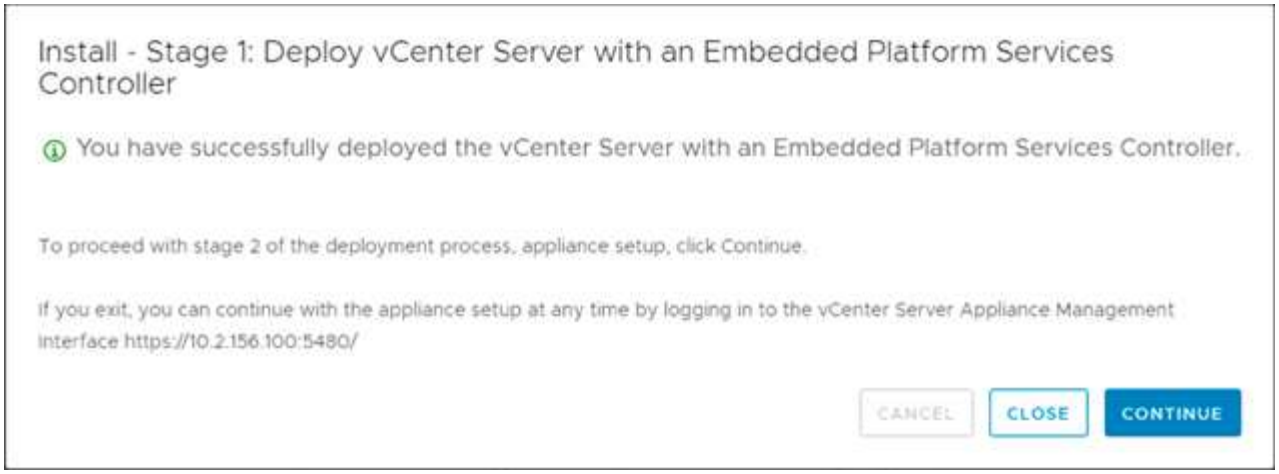
13. Geben Sie auf der Seite Netzwerkeinstellungen konfigurieren die folgenden Informationen ein, und klicken Sie auf Weiter.
    a. Wählen SIE MGMT-Network als Netzwerk aus.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse 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

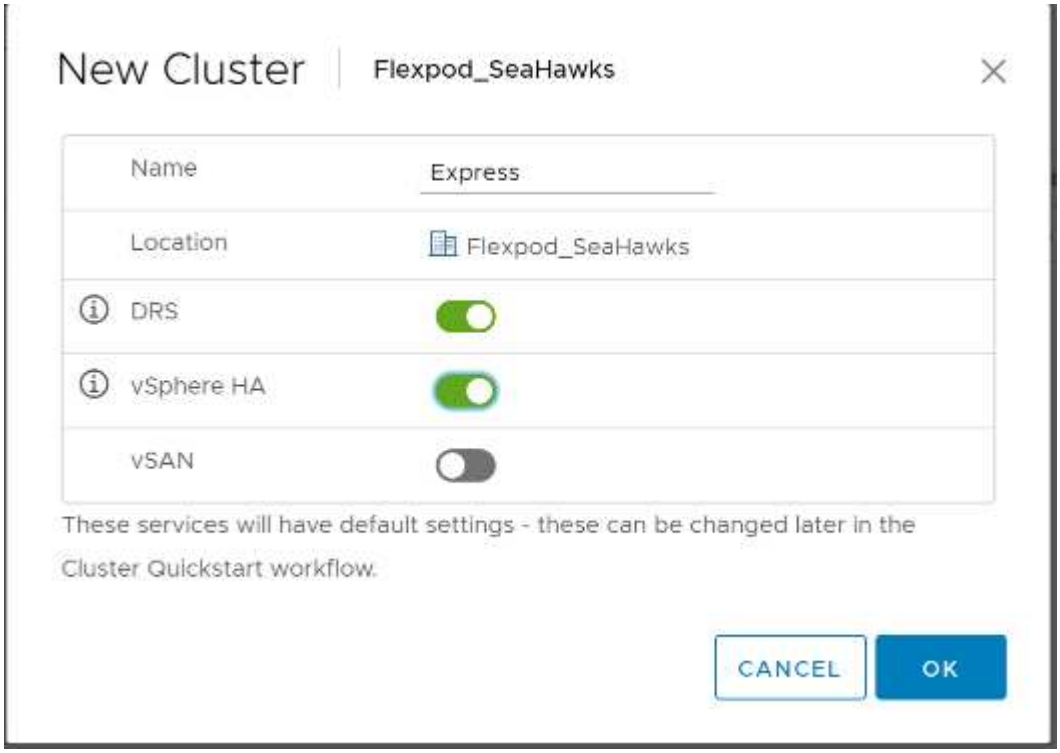
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

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:

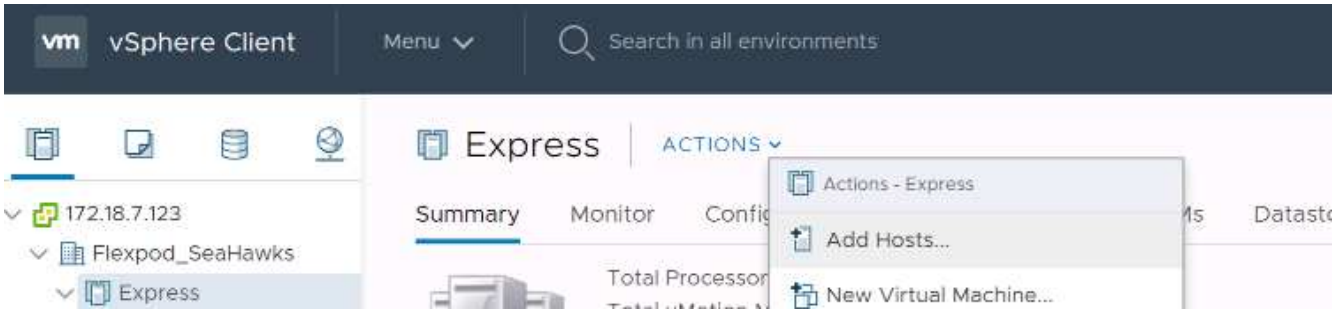
1. Klicken Sie mit der rechten Maustaste auf das neu erstellte Datacenter, und wählen Sie Neuer Cluster aus.
2. Geben Sie einen Namen für das Cluster ein.
3. Wählen Sie DRS und vSphere HA-Optionen aus und aktivieren Sie sie.
4. Klicken Sie auf OK.



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"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.