# Implementierungsverfahren

## FlexPod

NetApp
January 21, 2025

This PDF was generated from https://docs.netapp.com/de-de/flexpod/express/express-c-series-aff220-deploy_cisco_nexus_3172p_deployment_procedure.html on January 21, 2025. Always check docs.netapp.com for the latest.

# Inhalt

Implementierungsverfahren . . . 1
Cisco Nexus 3172P-Implementierungsverfahren . . . 2
Verfahren zur NetApp Storage-Implementierung (Teil 1) . . . 12
Cisco UCS C-Serie Rack-Server-Implementierung Verfahren . . . 36
NetApp Verfahren zur Implementierung von AFF-Storage (Teil 2) . . . 48
Implementierungsverfahren für VMware vSphere 6.7 . . . 48
Installieren Sie VMware vCenter Server 6.7 . . . 64
Konfiguration von VMware vCenter Server 6.7 und vSphere Clustering . . . 72

# 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 |

| EIN Name | VLAN-Zweck | ID zur Validierung dieses Dokuments verwendet |
|---|---|---|
| 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.

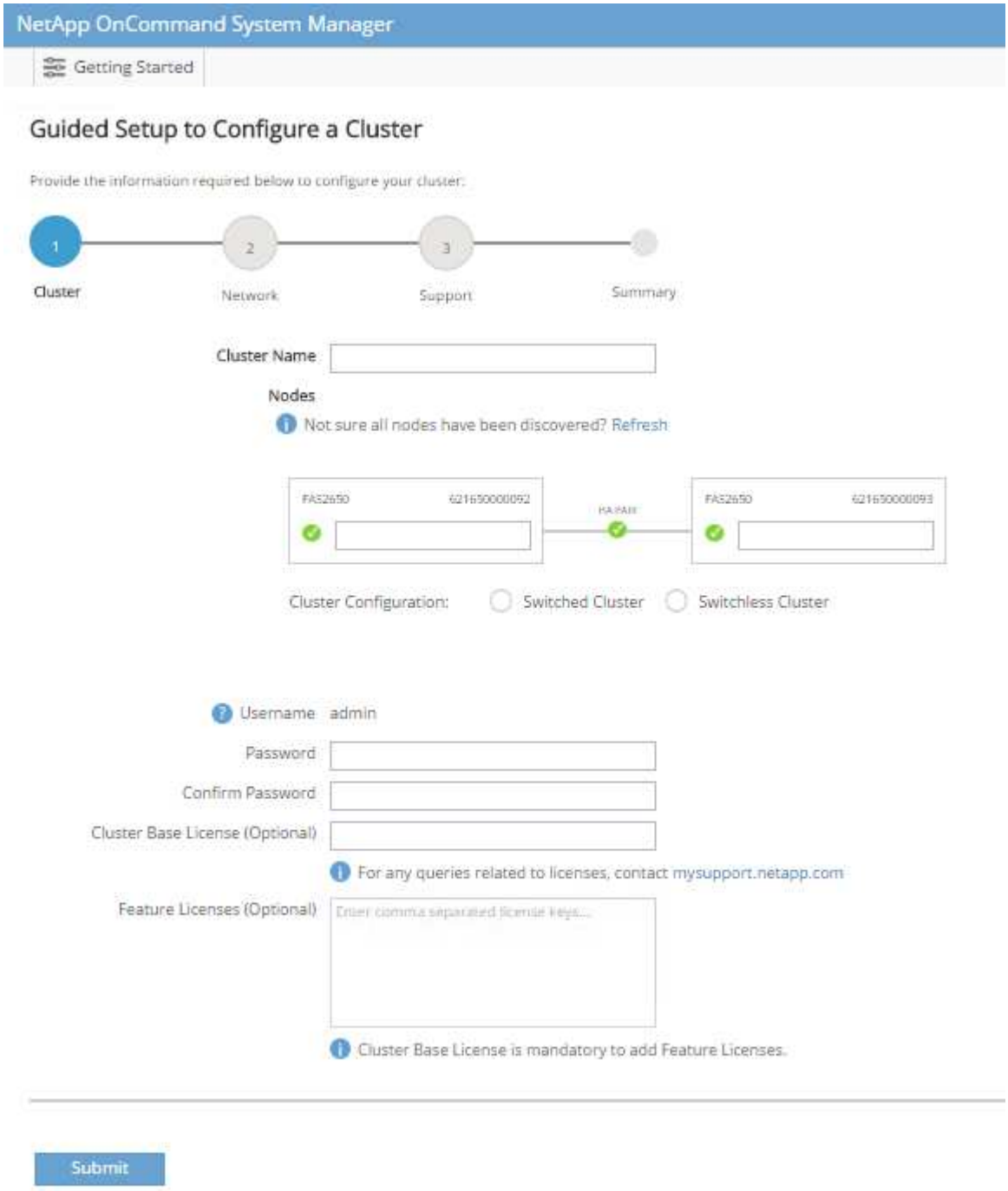
1. Befolgen Sie die Anweisungen zum Einrichten von Node A

```
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.

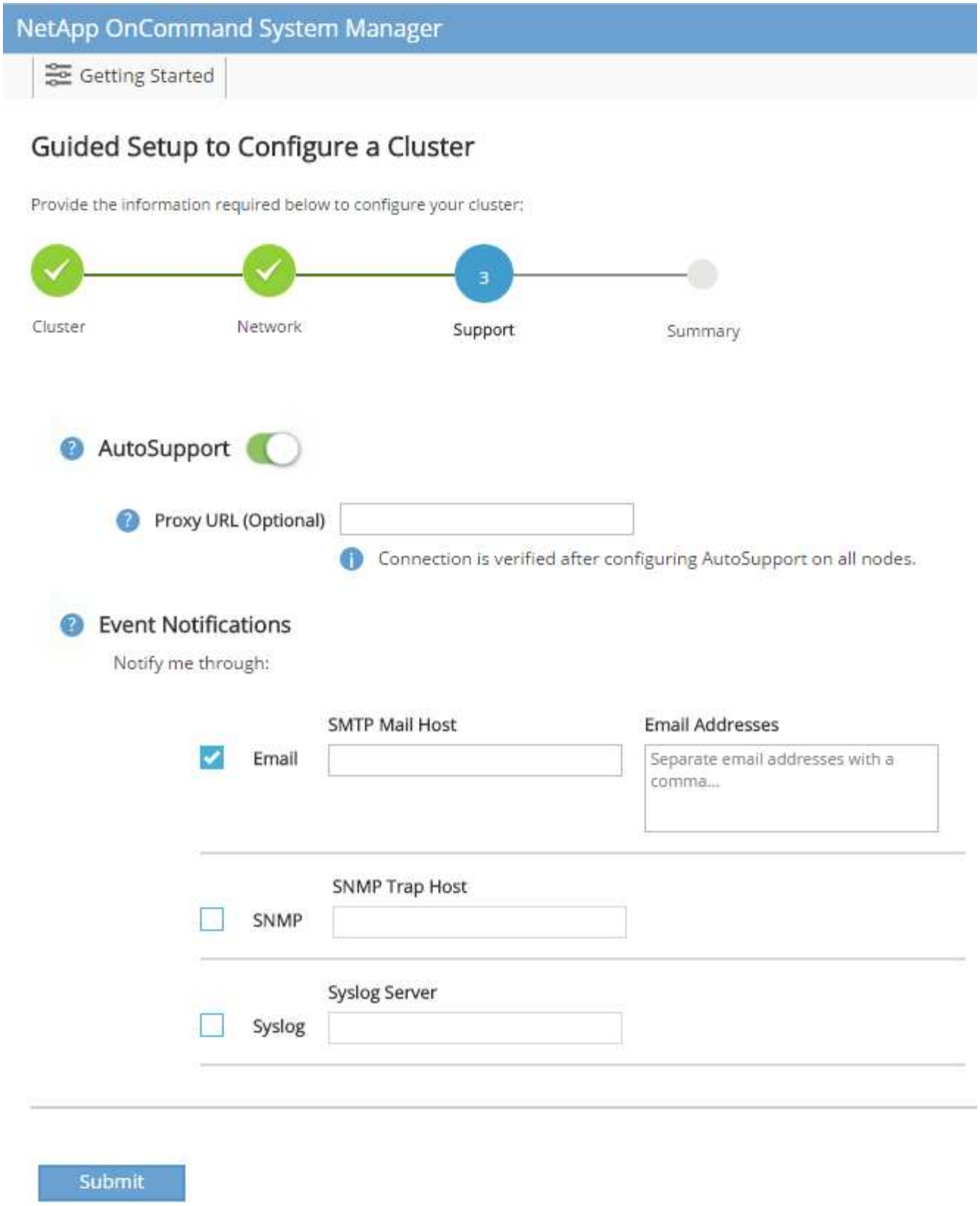
   Sie können auch einen alternativen NTP-Server eingeben.

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.

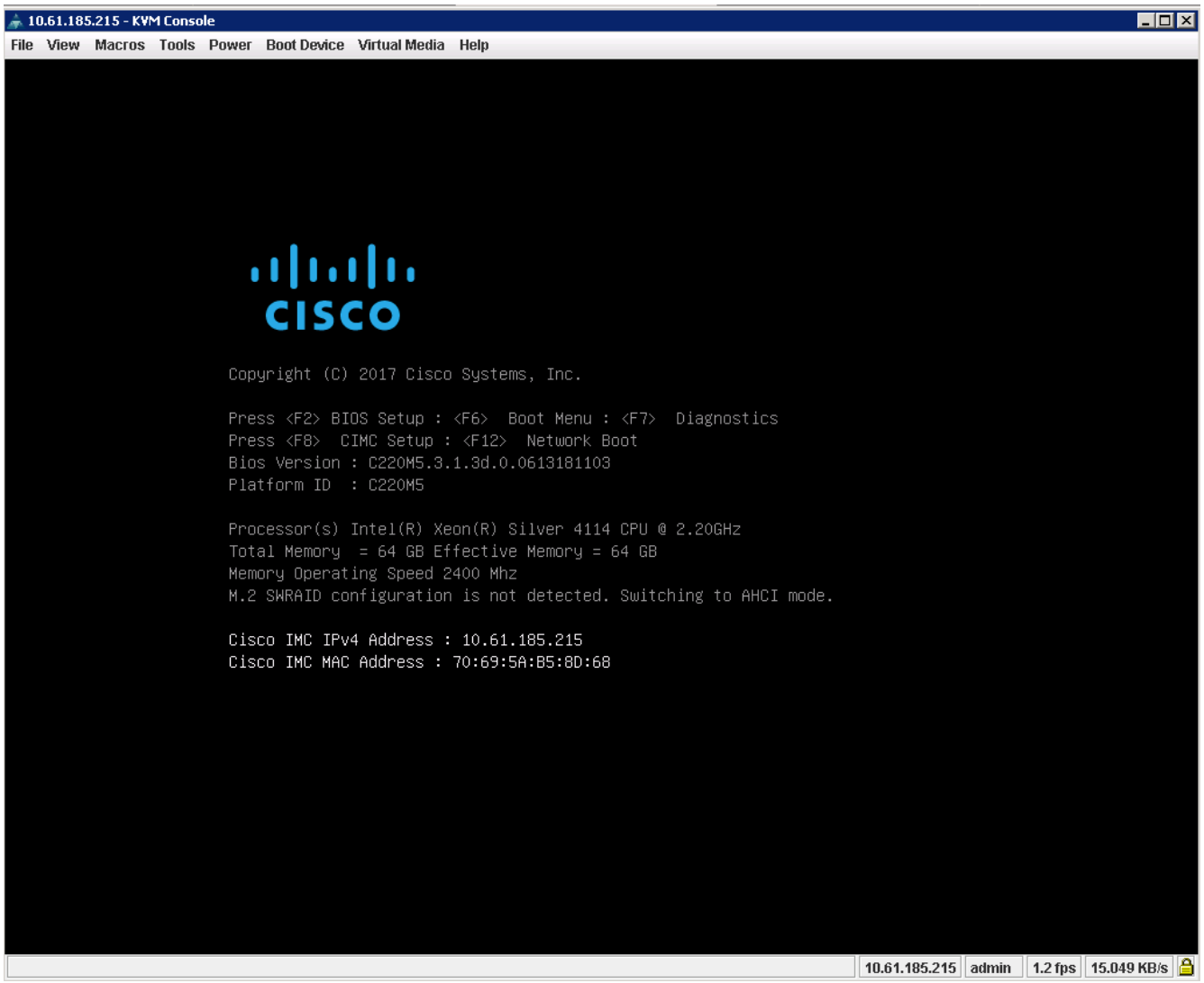
In der folgenden Tabelle sind die Informationen aufgeführt, die für die Konfiguration von CIMC für jeden Standalone-Server der Cisco UCS C-Serie erforderlich sind.

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

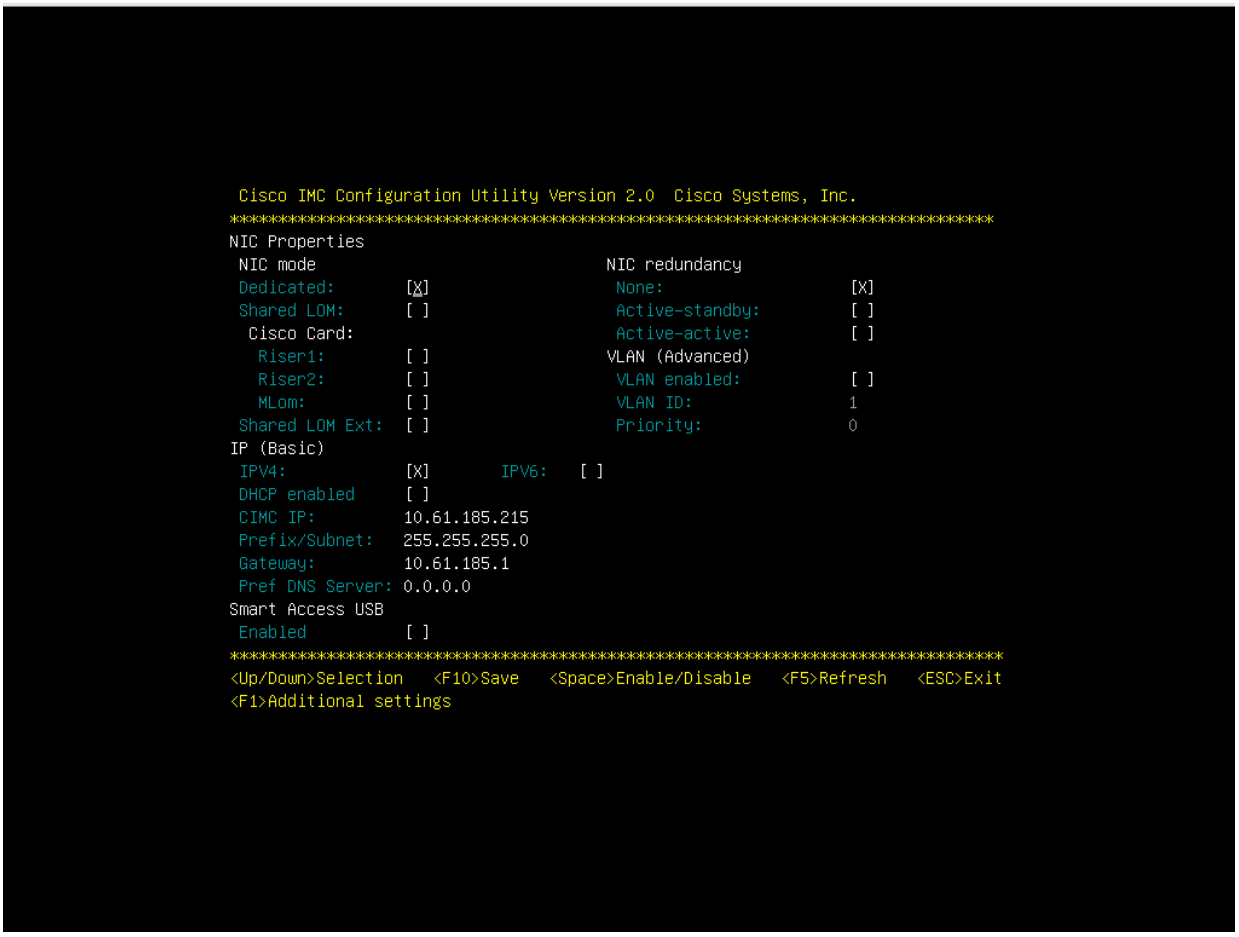
Die CIMC-Version, die in dieser Validierung verwendet wird, ist CIMC 3.1.3(g).

**Alle Server**

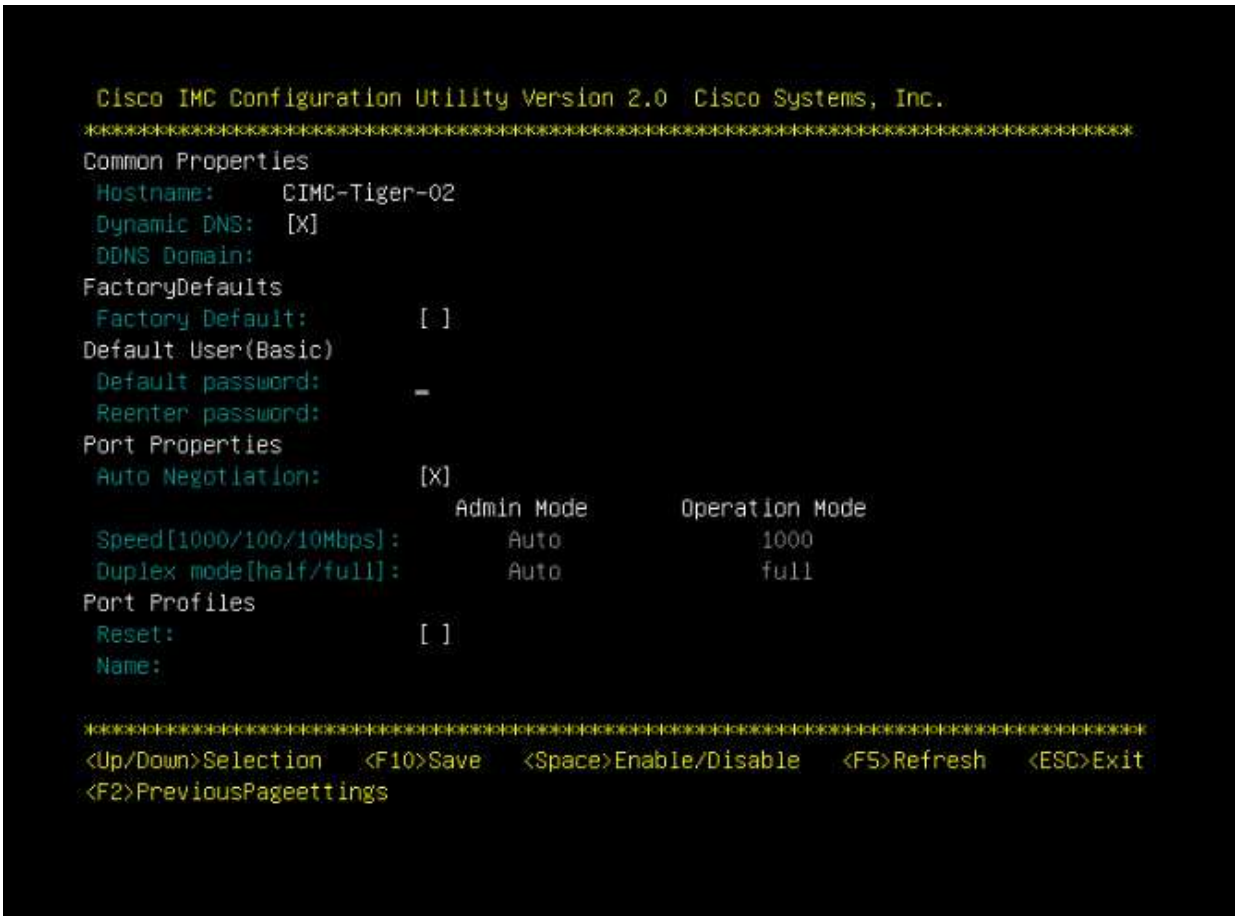
1. Schließen Sie den Cisco Keyboard-, Video- und Mausdongle (KVM) (im Lieferumfang des Servers enthalten) an den KVM-Port an der Vorderseite des Servers an. Schließen Sie einen VGA-Monitor und eine USB-Tastatur an die entsprechenden KVM-Dongle-Ports an.
2. Schalten Sie den Server ein, und drücken Sie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

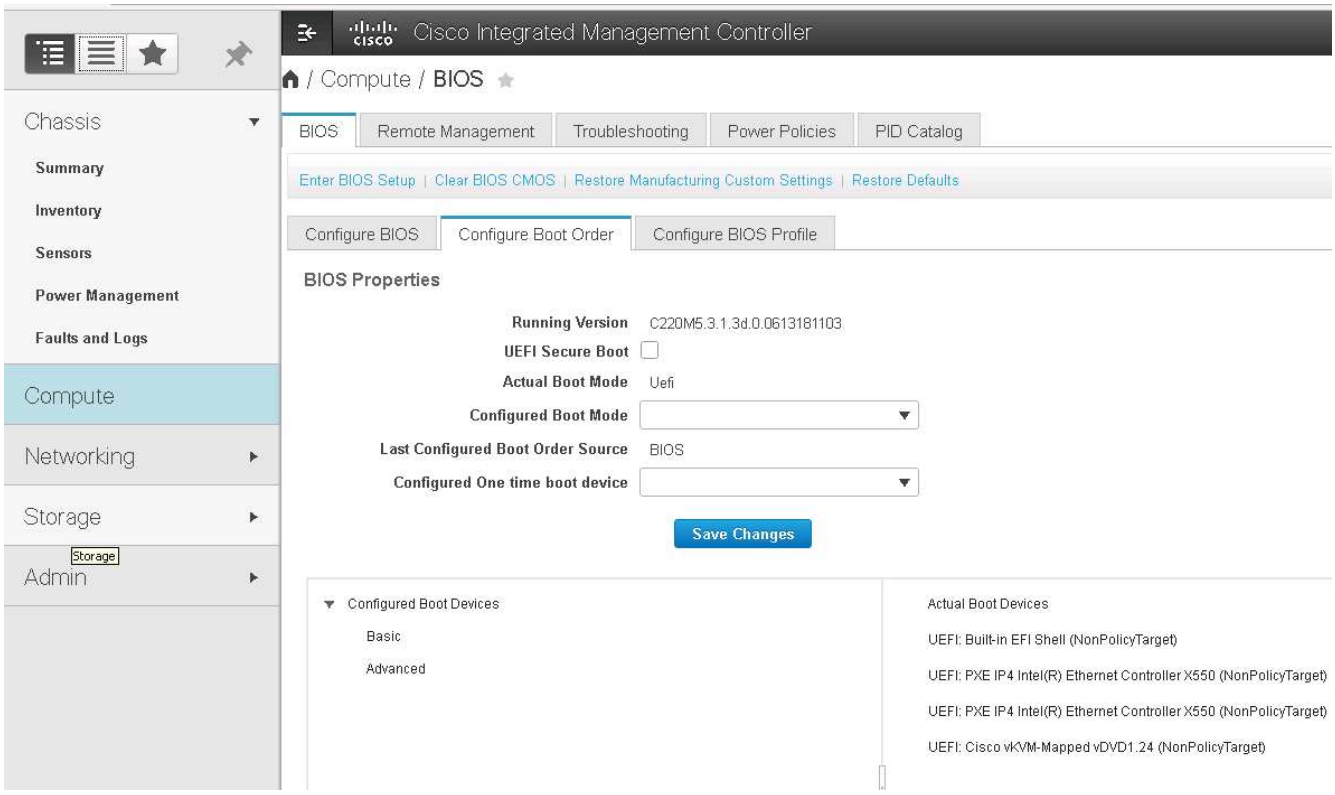
| Details | Detailwert |
|---|---|
| ESXi Host-Initiator Ein Name | <<var_ucs_Initiator_Name_A>> |
| ESXi Host, iSCSI A IP | <<var_esxi_Host_iscsiA_ip>> |
| ESXi-Host, iSCSI-A-Netzwerkmaske | <<var_esxi_Host_iscsiA_Maska>> |
| ESXi Host iSCSI Ein Standard-Gateway | \<<var_esxi_Host_iscsiA_Gateway> |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

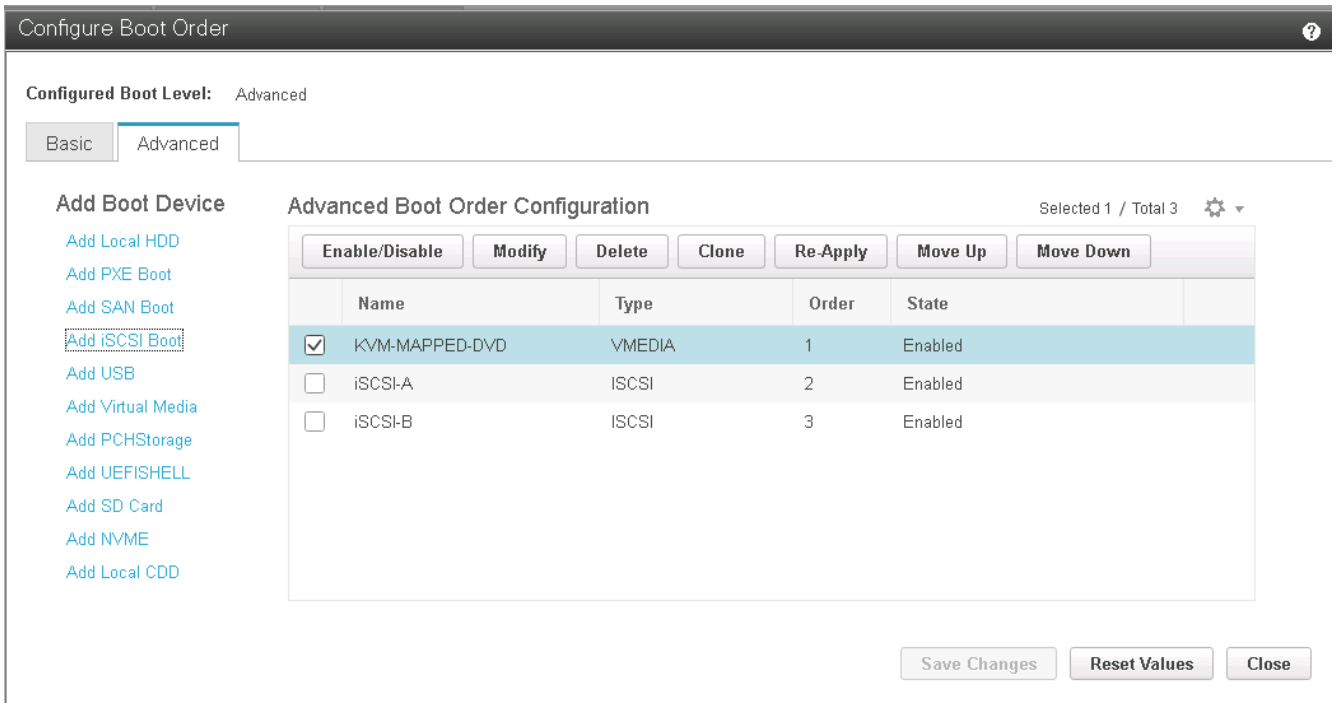
Gehen Sie wie folgt vor, um die Konfiguration der Startreihenfolge festzulegen:

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.

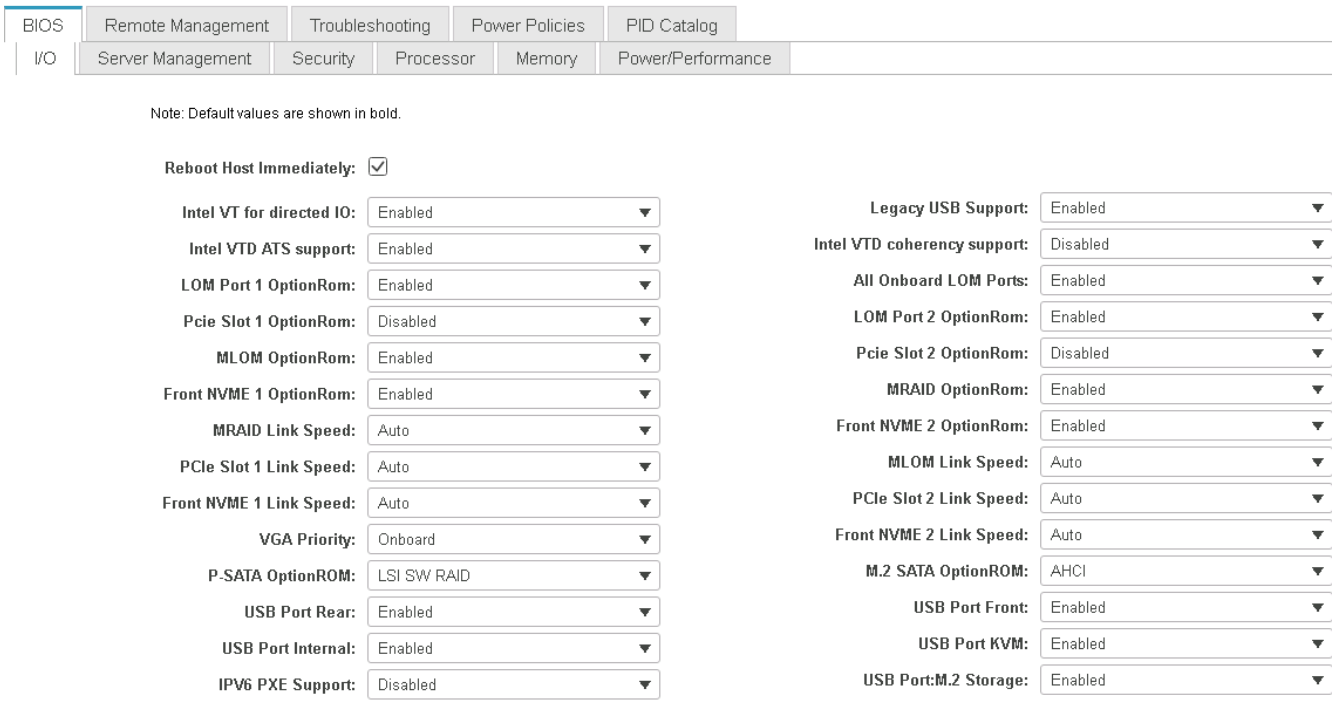



6. Starten Sie den Server neu, um mit Ihrer neuen Startreihenfolge zu starten.

### 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.



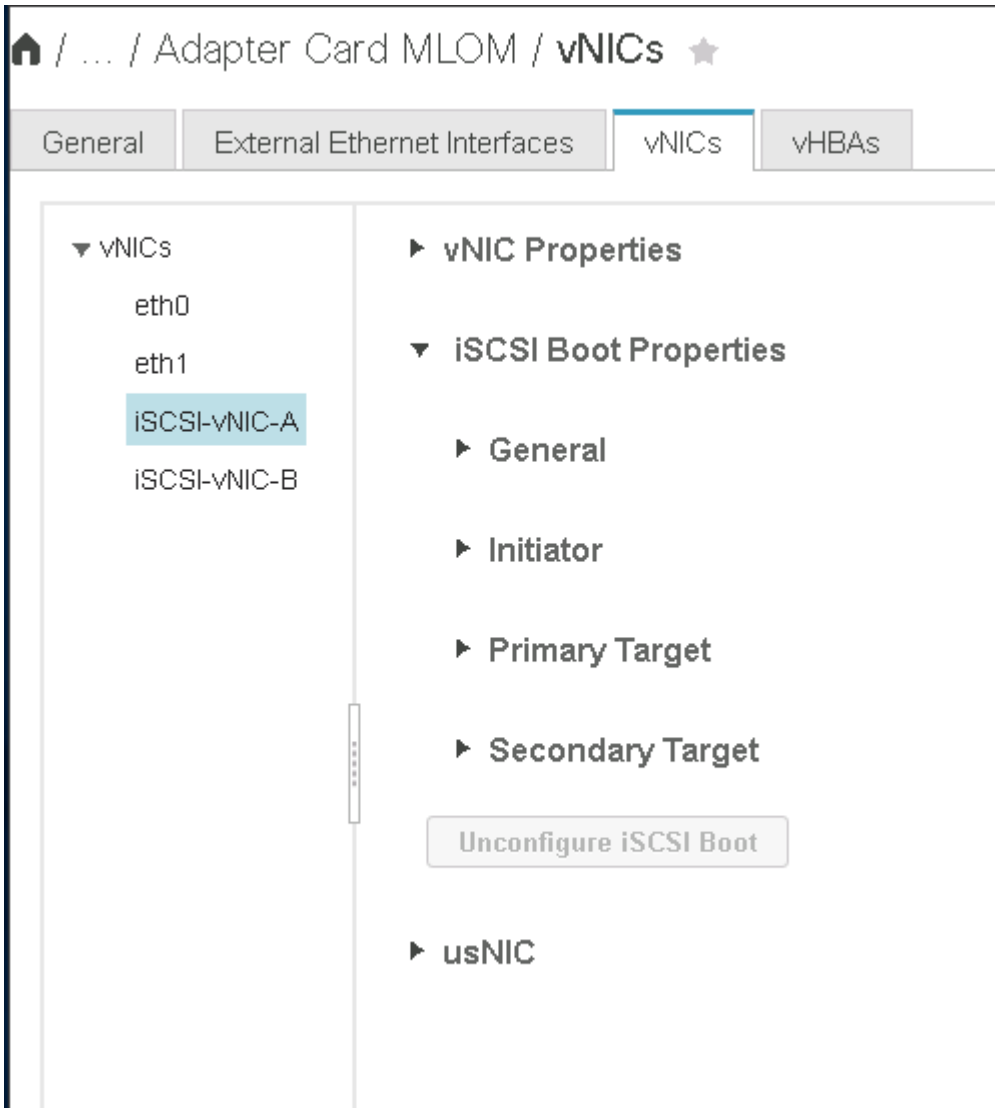

## Konfigurieren Sie Cisco VIC1387 für iSCSI Boot

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

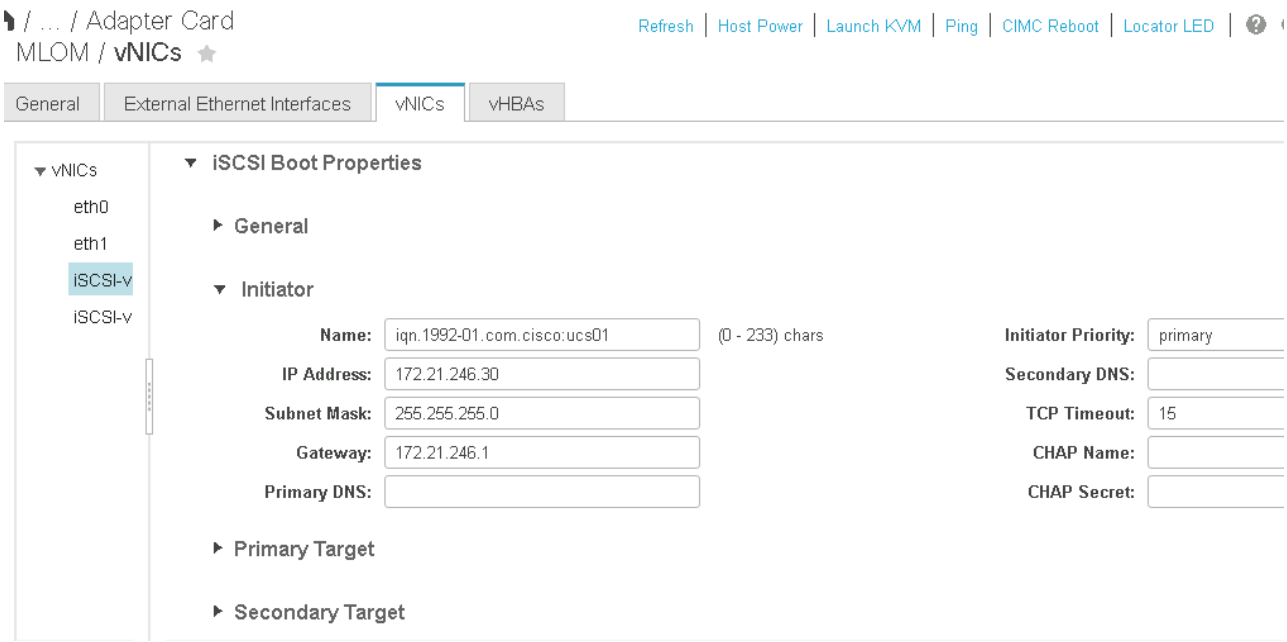
### Erstellen von iSCSI-vNICs

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.



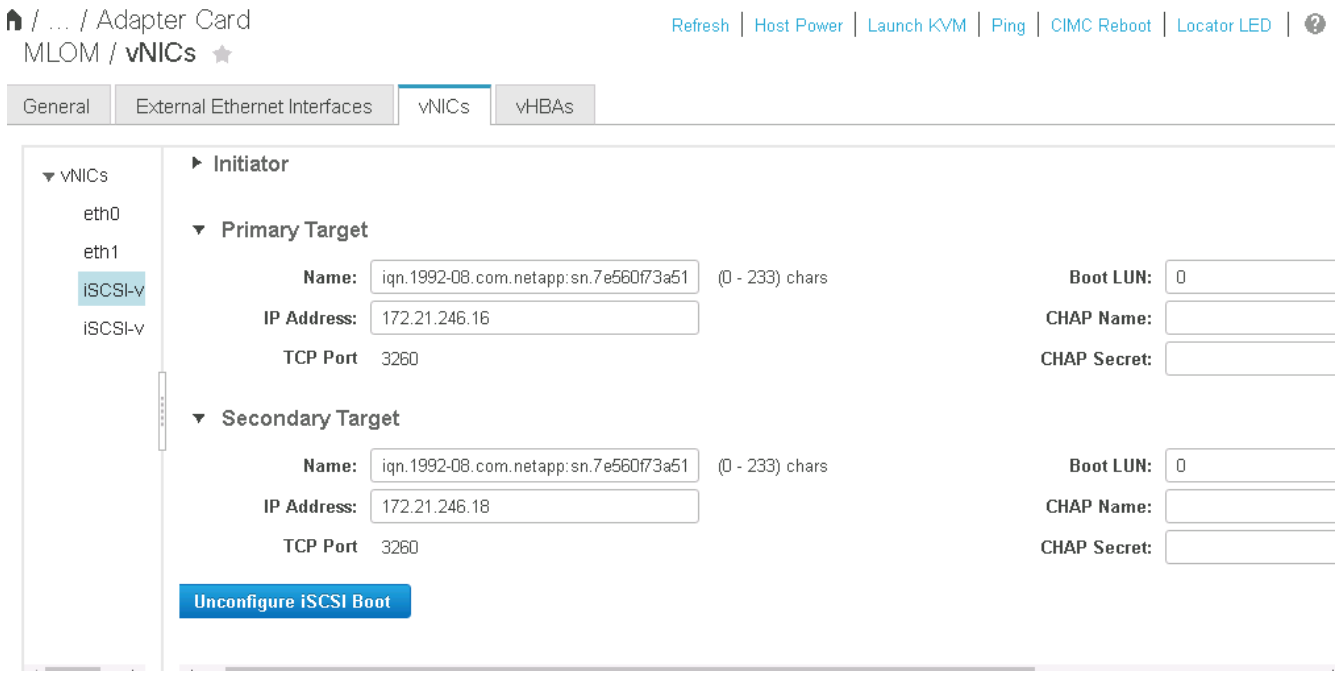

6. Geben Sie unter iSCSI Boot Properties die Initiator-Details ein:
   - Name: <<var_ucsa_Initiator_Name_a>>
   - IP-Adresse: <<var_esxi_hostA_iscsiA_ip>>
   - Subnetzmaske: <<var_esxi_hostA_iscsiA_maska>>
   - Gateway: <<var_esxi_hostA_iscsiA_Gateway>>




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.

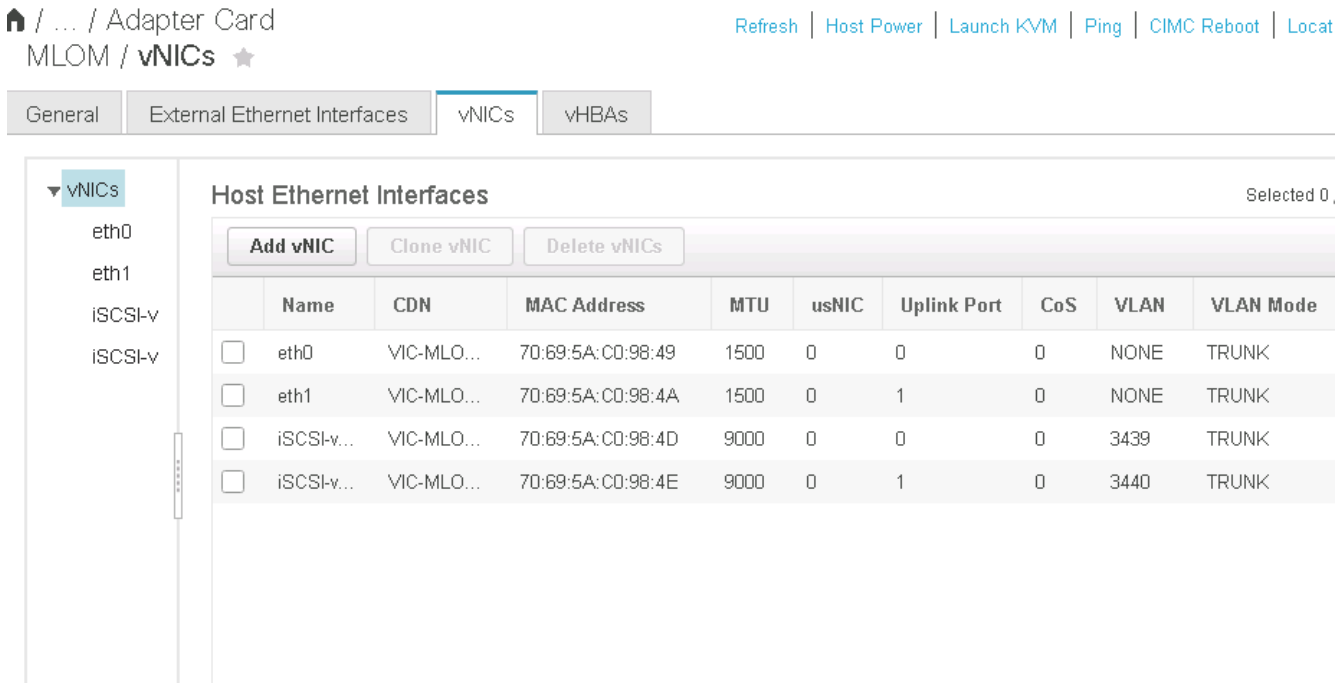
    > Achten Sie darauf, die IQN-Namen für jede vNIC aufzuzeichnen. Sie brauchen sie für einen späteren Schritt.

15. Klicken Sie auf ISCSI konfigurieren.

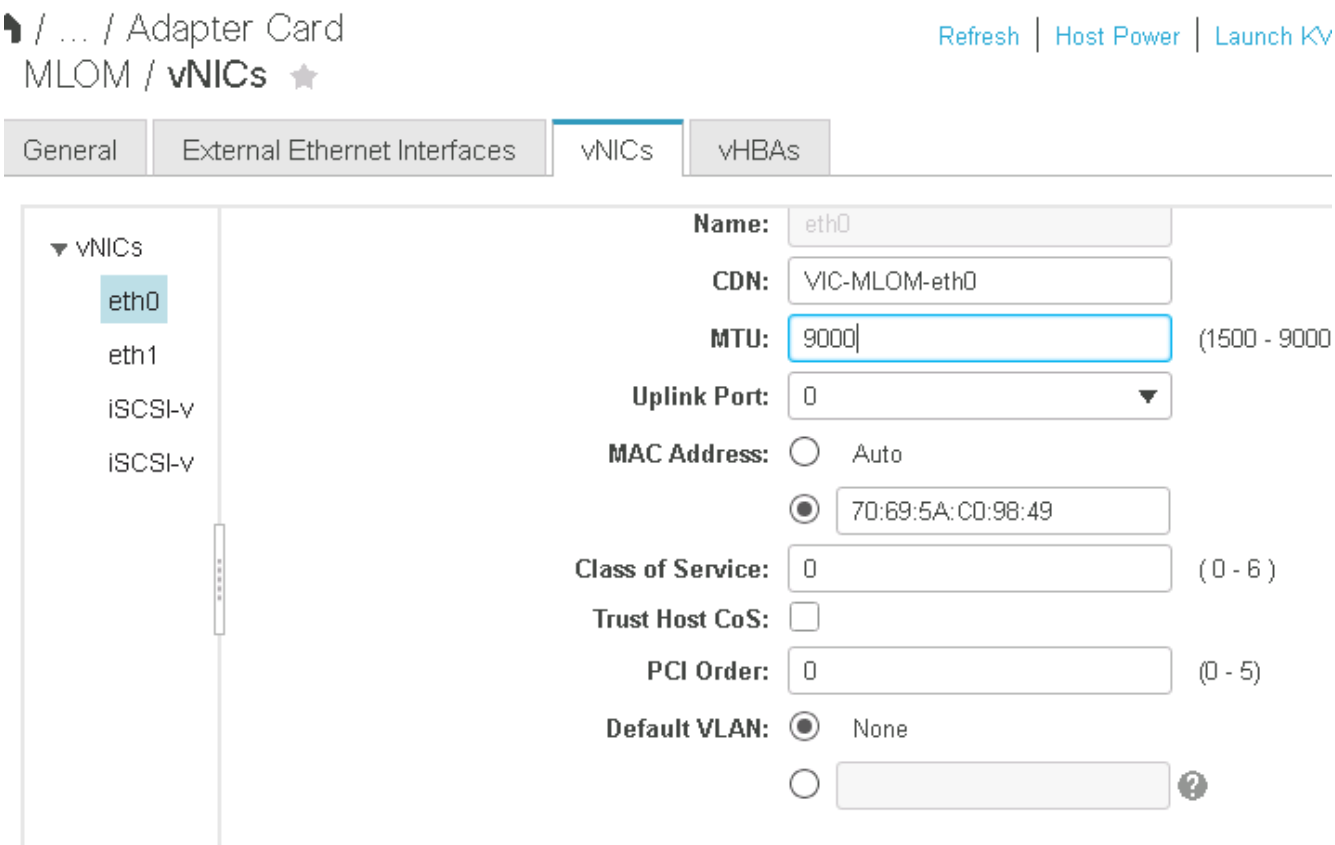
16. Wiederholen Sie diesen Vorgang, um iSCSI-Boot für Cisco UCS-Server B zu konfigurieren

### Konfigurieren Sie vNICs für ESXi

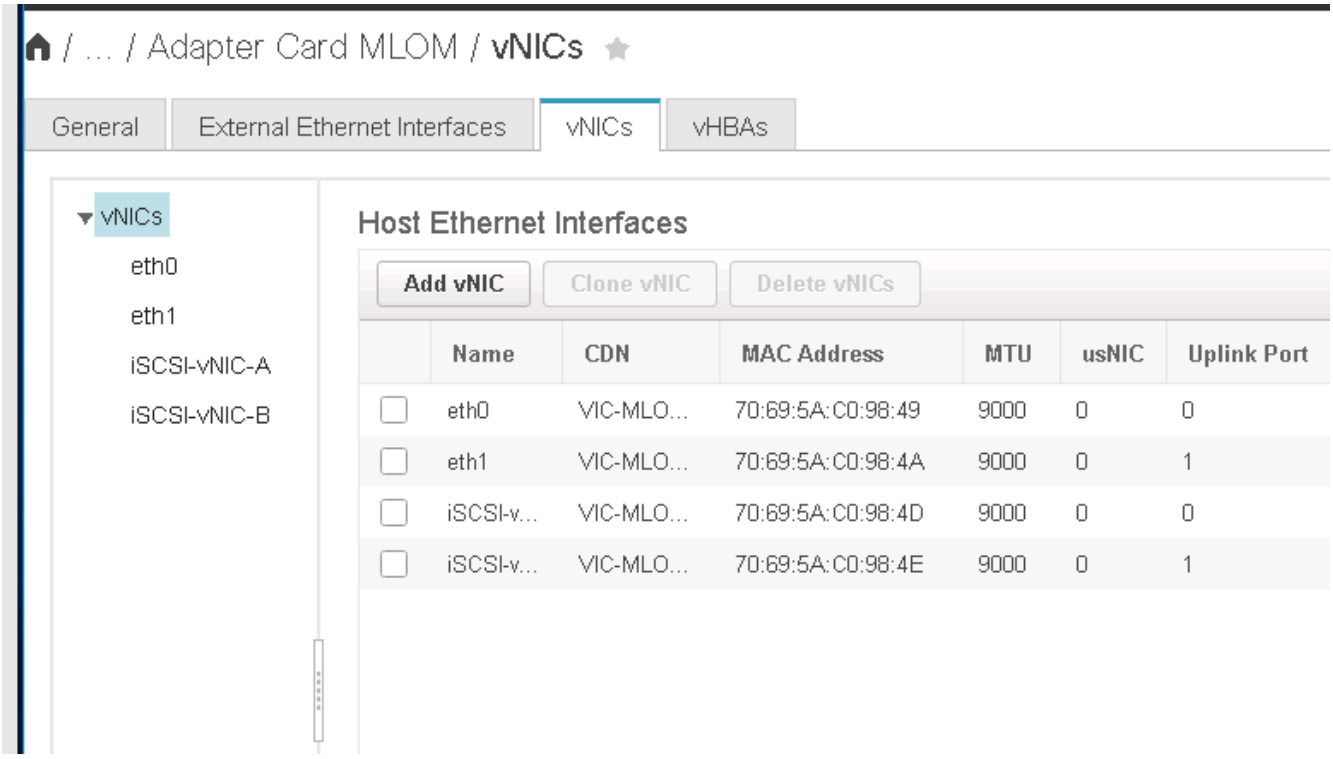
1. Klicken Sie im CIMC-Schnittstellenbrowser-Fenster auf Inventar und anschließend im rechten Fensterbereich auf Cisco VIC-Adapter.
2. Wählen Sie unter Adapterkarten Cisco UCS VIC 1387 aus und wählen Sie dann die darunter liegende vNICs aus.




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

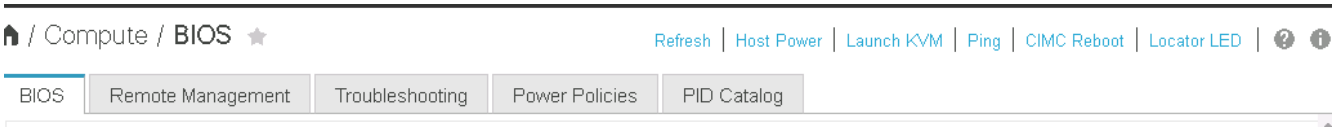
Für alle zusätzlichen Nodes, die dem Cluster hinzugefügt werden, muss dieser Vorgang abgeschlossen sein.

## 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.

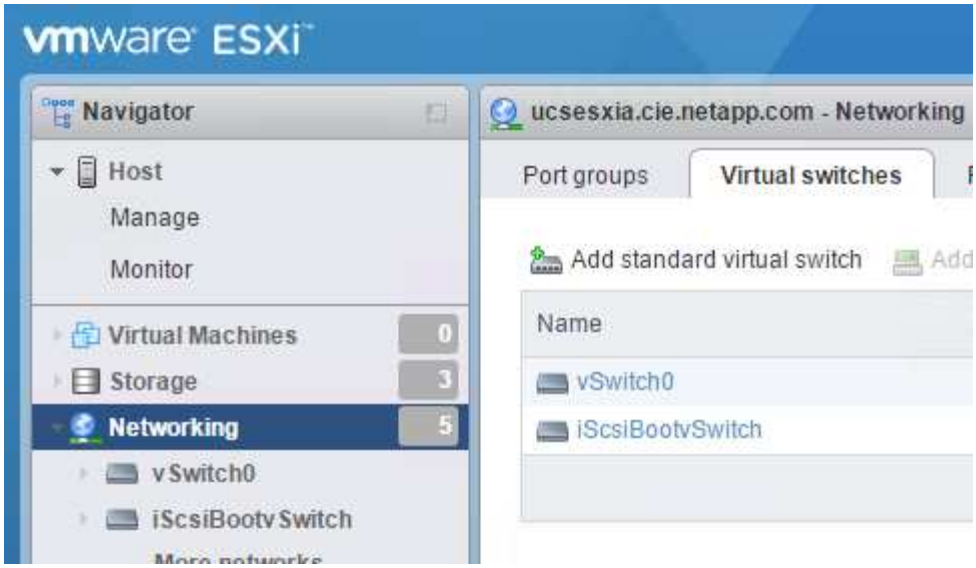
| Details | Wert |
|---|---|
| ESXi Hostname | |
| ESXi Host-Management-IP | |
| ESXi Host-Managementmaske | |
| ESXi Host-Management-Gateway | |
| ESXi Host, NFS-IP | |
| ESXi Host-NFS-Maske | |
| ESXi Host-NFS-Gateway | |
| ESXi Host vMotion IP | |
| ESXi Host vMotion Maske | |
| ESXi Host vMotion 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.

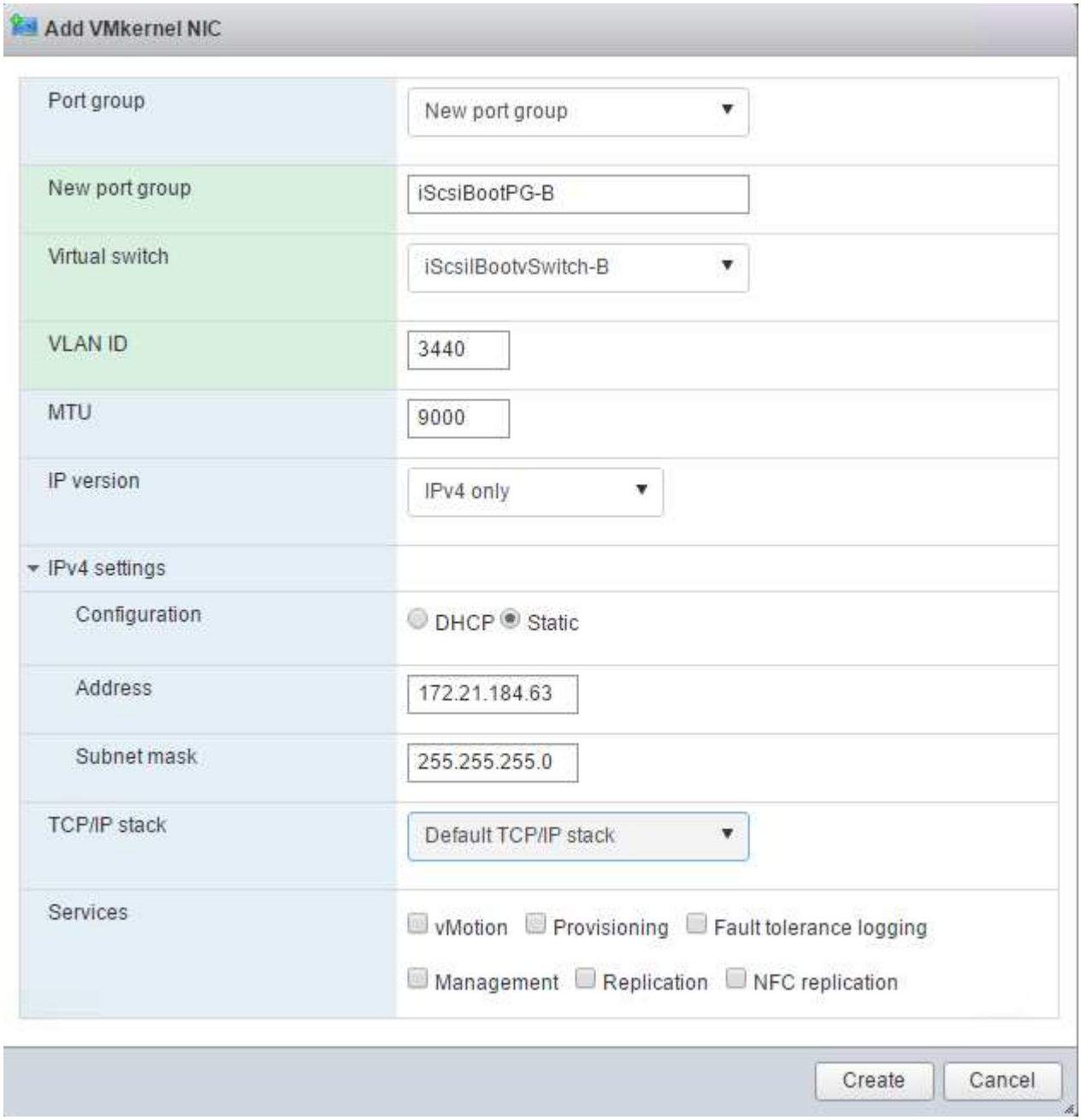



3. Klicken Sie auf iScsiBootvSwitch.
4. Wählen Sie Einstellungen bearbeiten aus.
5. Ändern Sie die MTU in 9000, und klicken Sie auf Speichern.
6. Klicken Sie im linken Navigationsbereich auf Netzwerk, um zur Registerkarte Virtuelle Switches zurückzukehren.
7. Klicken Sie Auf Standard-Virtuellen Switch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

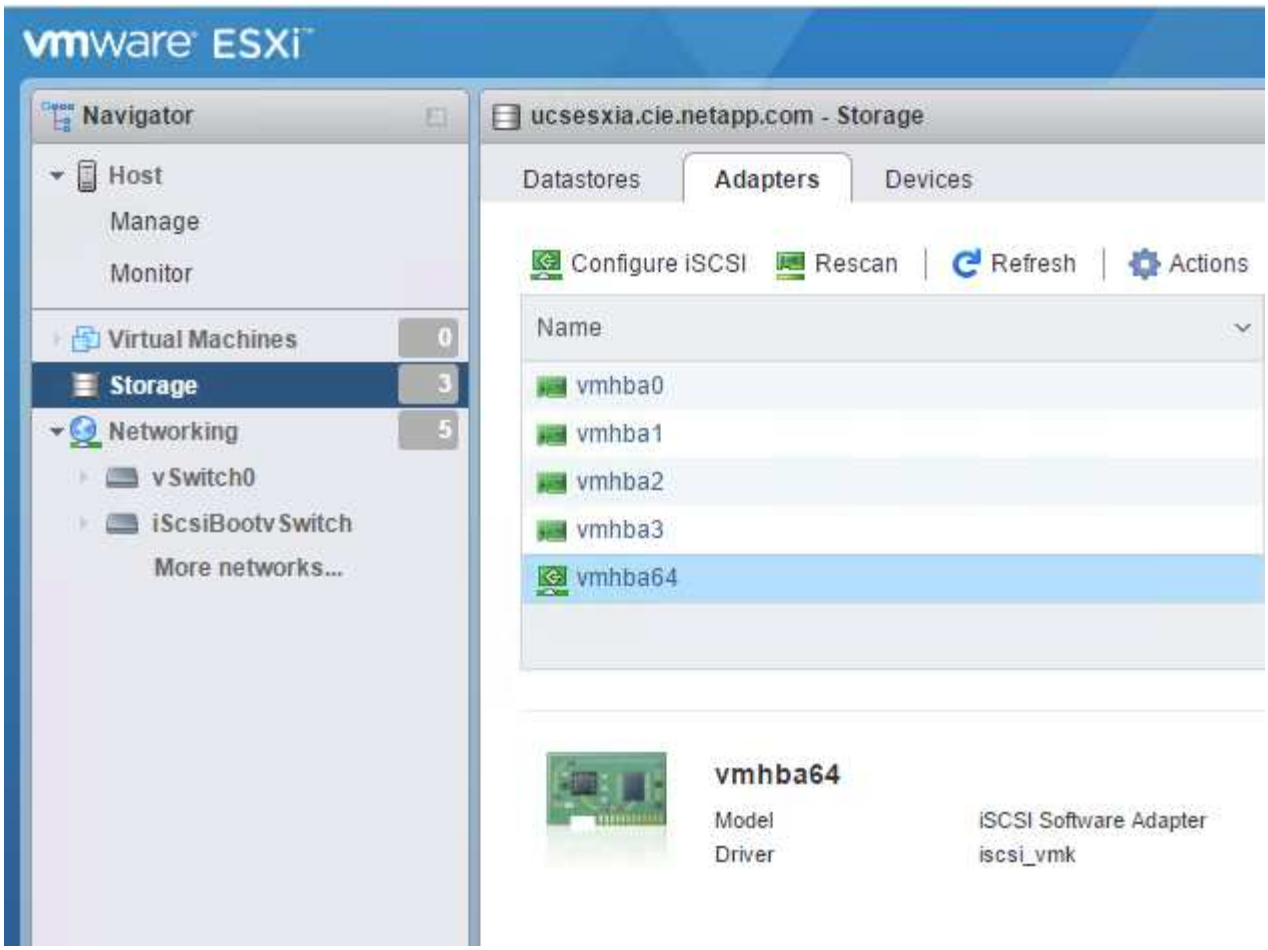



Setzen Sie die MTU auf 9000 auf `iScsiBootPG- A.`

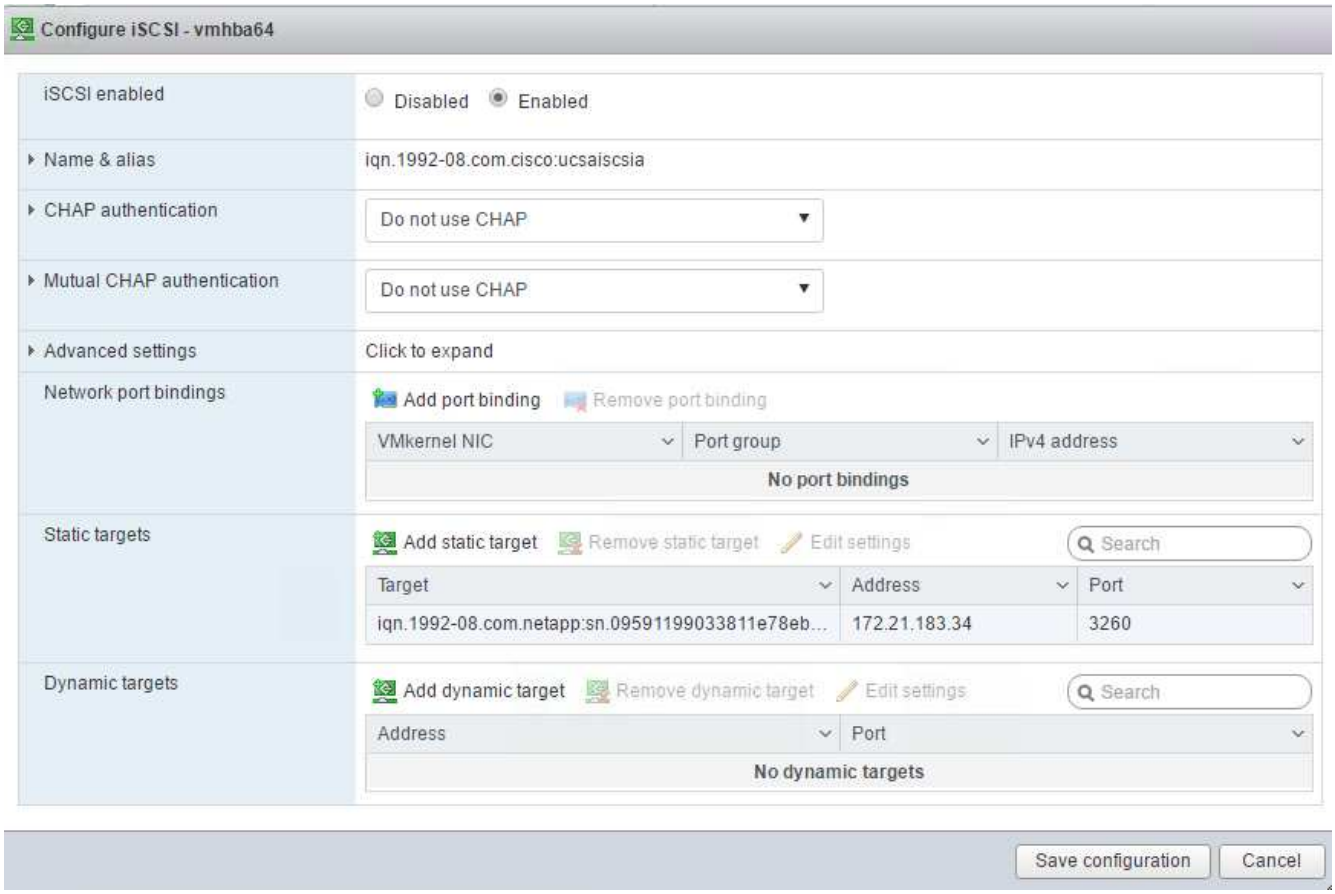
### Konfigurieren Sie iSCSI-Multipathing

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

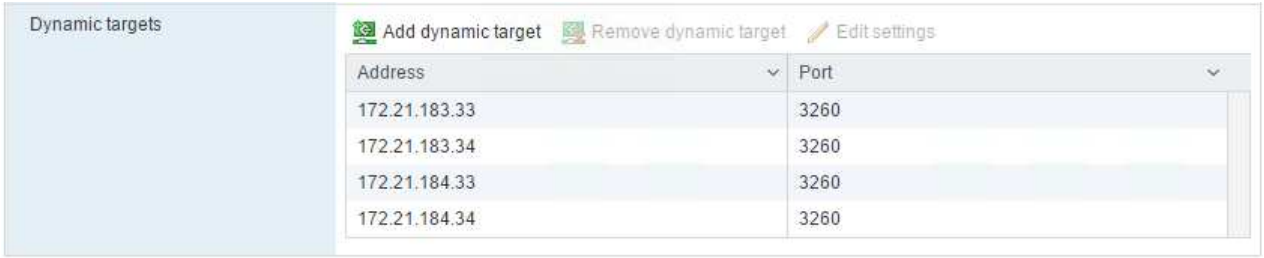
1. Wählen Sie im linken Navigationsbereich Storage aus. Klicken Sie Auf Adapter.
2. Wählen Sie den iSCSI-Software-Adapter aus, und klicken Sie auf iSCSI konfigurieren.




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



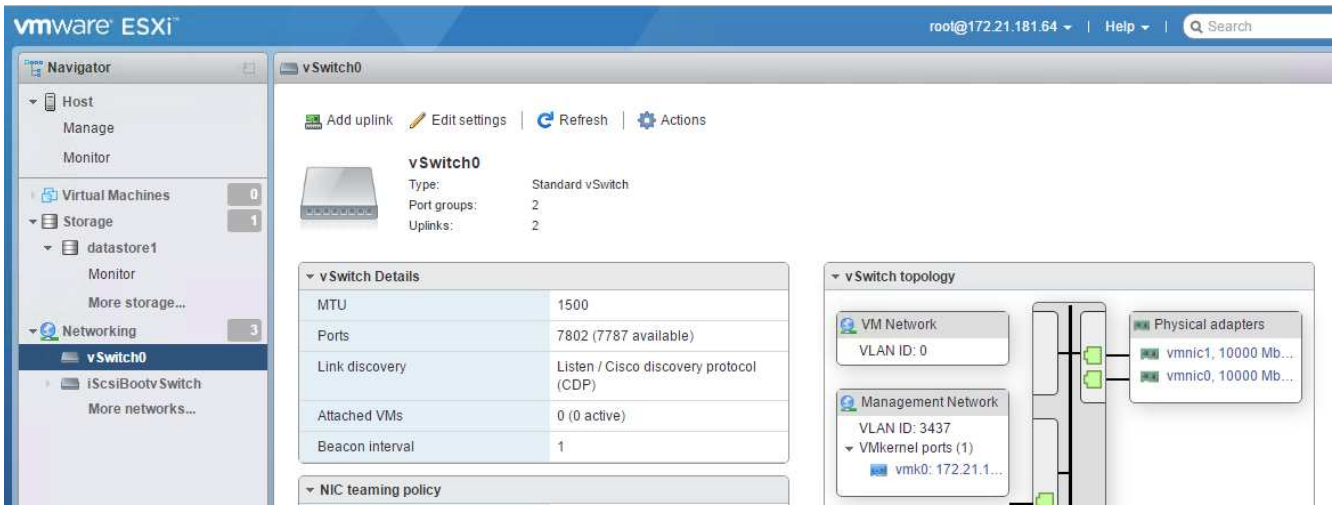

4. Geben Sie die IP-Adresse ein `iscsi_lif01a`.
   - Wiederholen Sie diesen Vorgang mit den IP-Adressen `iscsi_lif01b`, `iscsi_lif02a`, und `iscsi_lif02b`.
   - Klicken Sie Auf Konfiguration Speichern.




> 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.

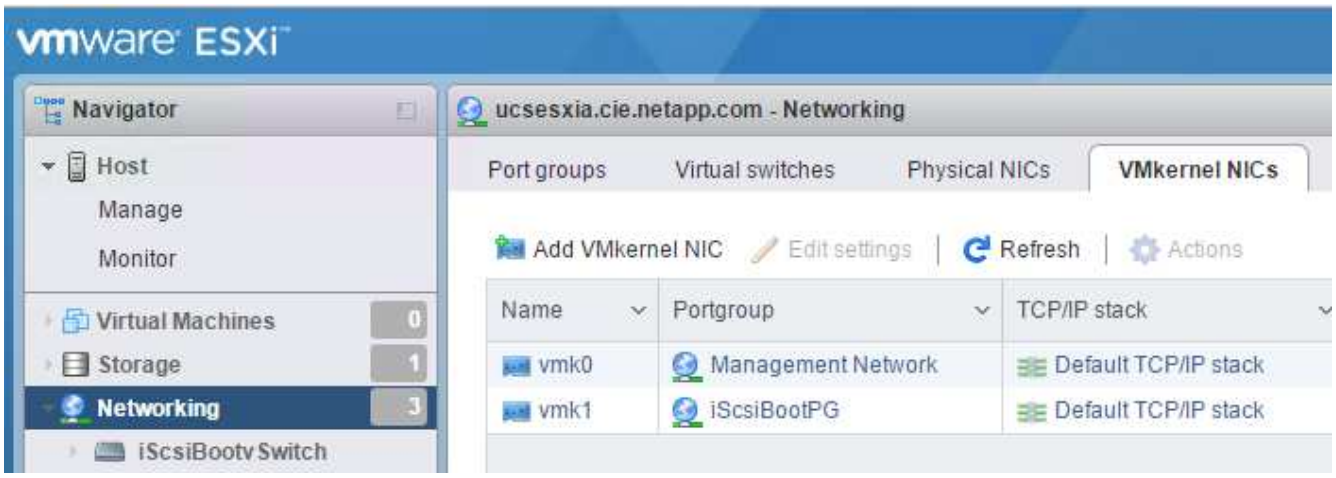
### Konfigurieren Sie die Portgruppen und VMkernel NICs

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

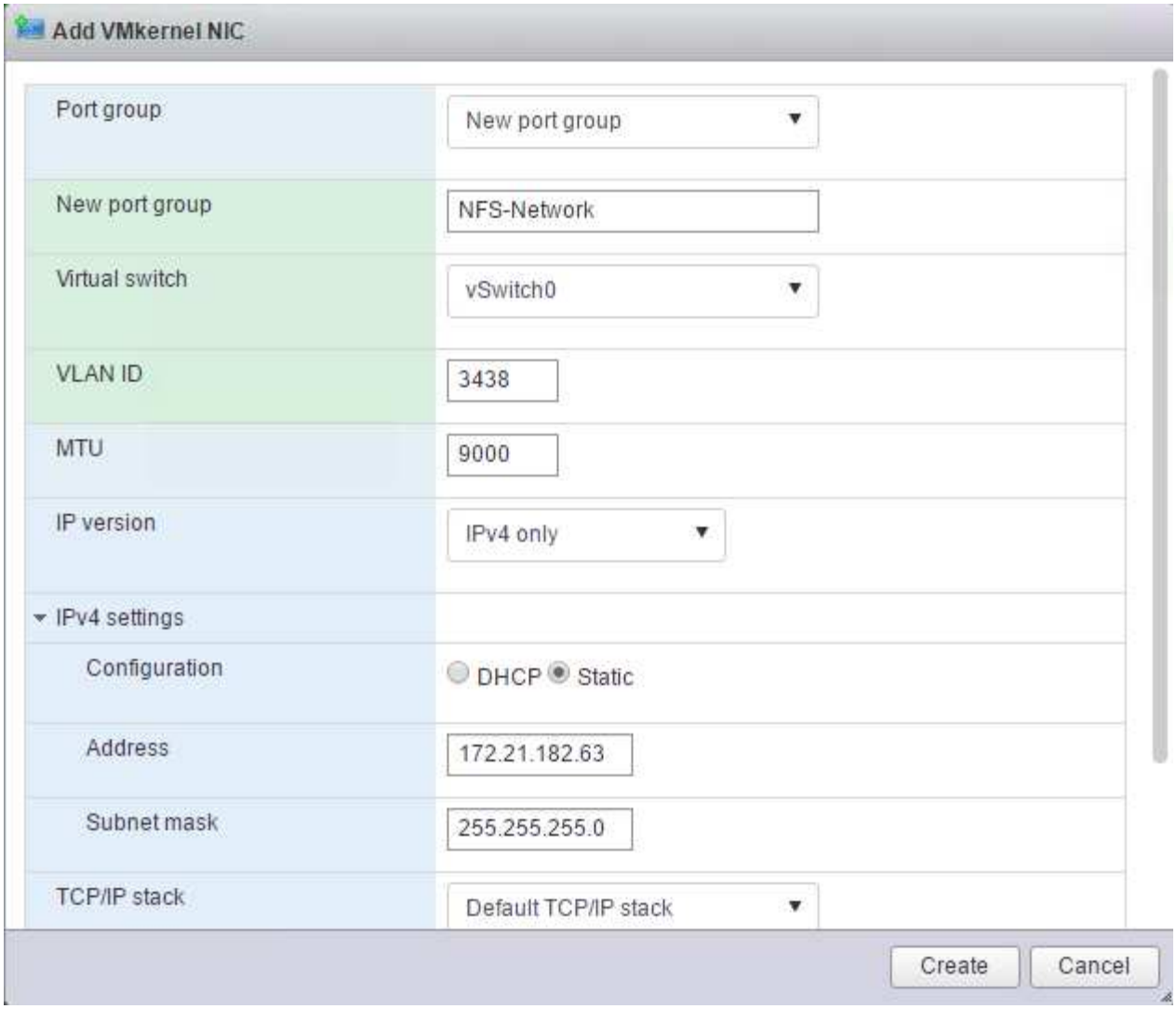
3. Klicken Sie mit der rechten Maustaste auf VM Network, und wählen Sie Bearbeiten aus. Ändern Sie die VLAN-ID in `<<var_vm_traffic_vlan>>`.
4. Klicken Sie Auf Portgruppe Hinzufügen.
   - Benennen Sie die Portgruppe `MGMT-Network`.
   - Eingabe `<<mgmt_vlan>>` Für die VLAN-ID.
   - Stellen Sie sicher,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

- Klicken Sie Auf Hinzufügen.

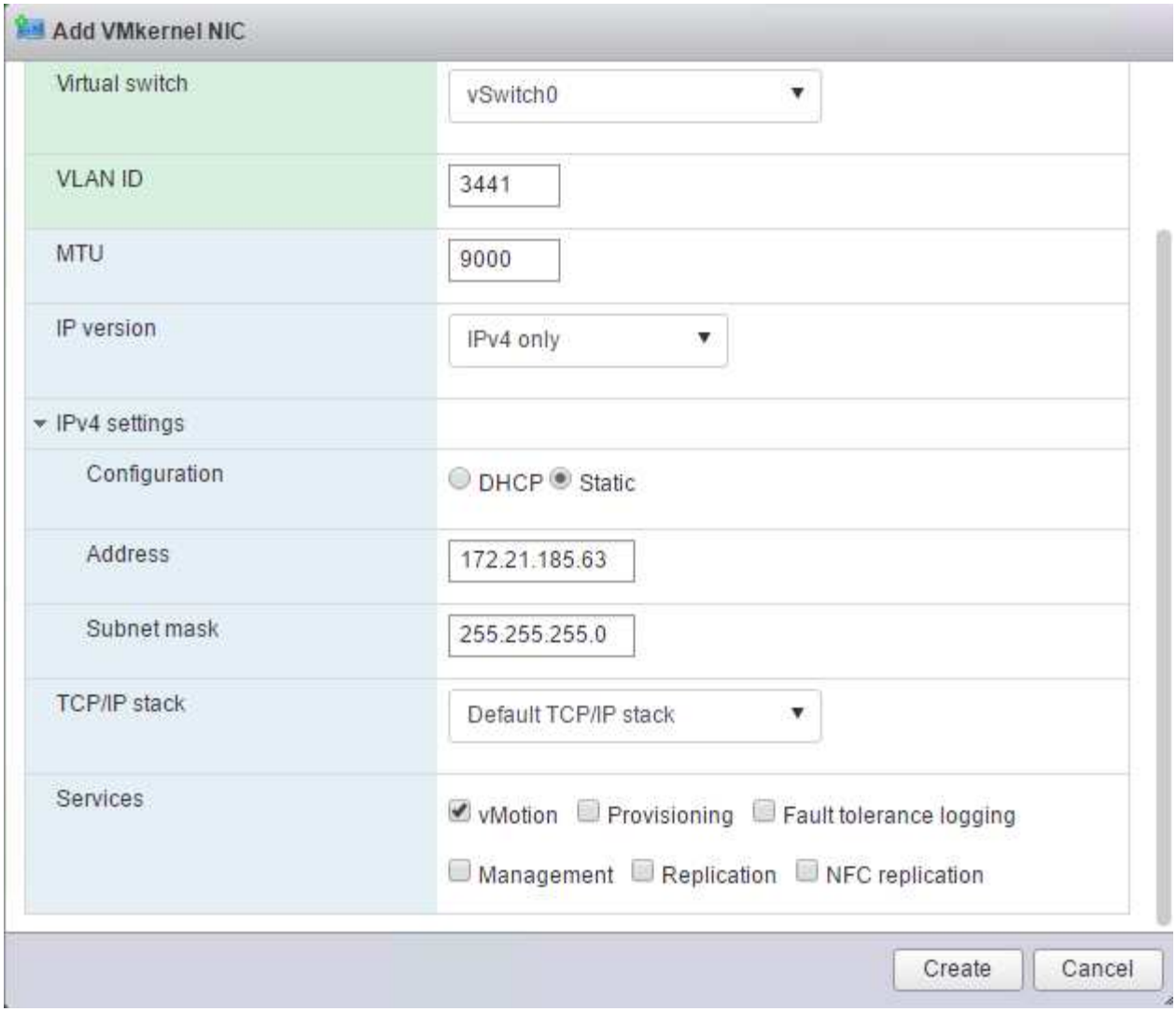
5. Klicken Sie auf die Registerkarte VMkernel NICs.




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.

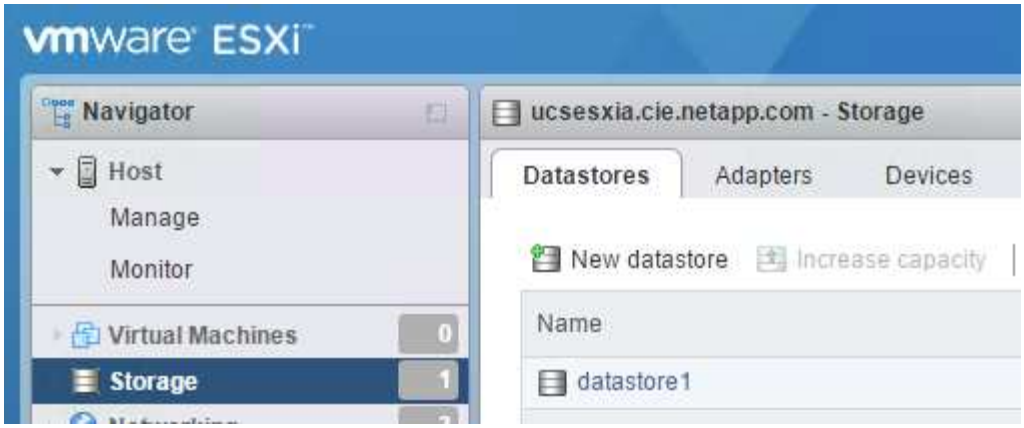



Es gibt viele Möglichkeiten, ESXi Networking zu konfigurieren, einschließlich der Verwendung des VMware vSphere Distributed Switches, wenn Ihre Lizenzierung es zulässt. In FlexPod Express werden alternative Netzwerkkonfigurationen unterstützt, wenn sie zur Erfüllung der geschäftlichen Anforderungen erforderlich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

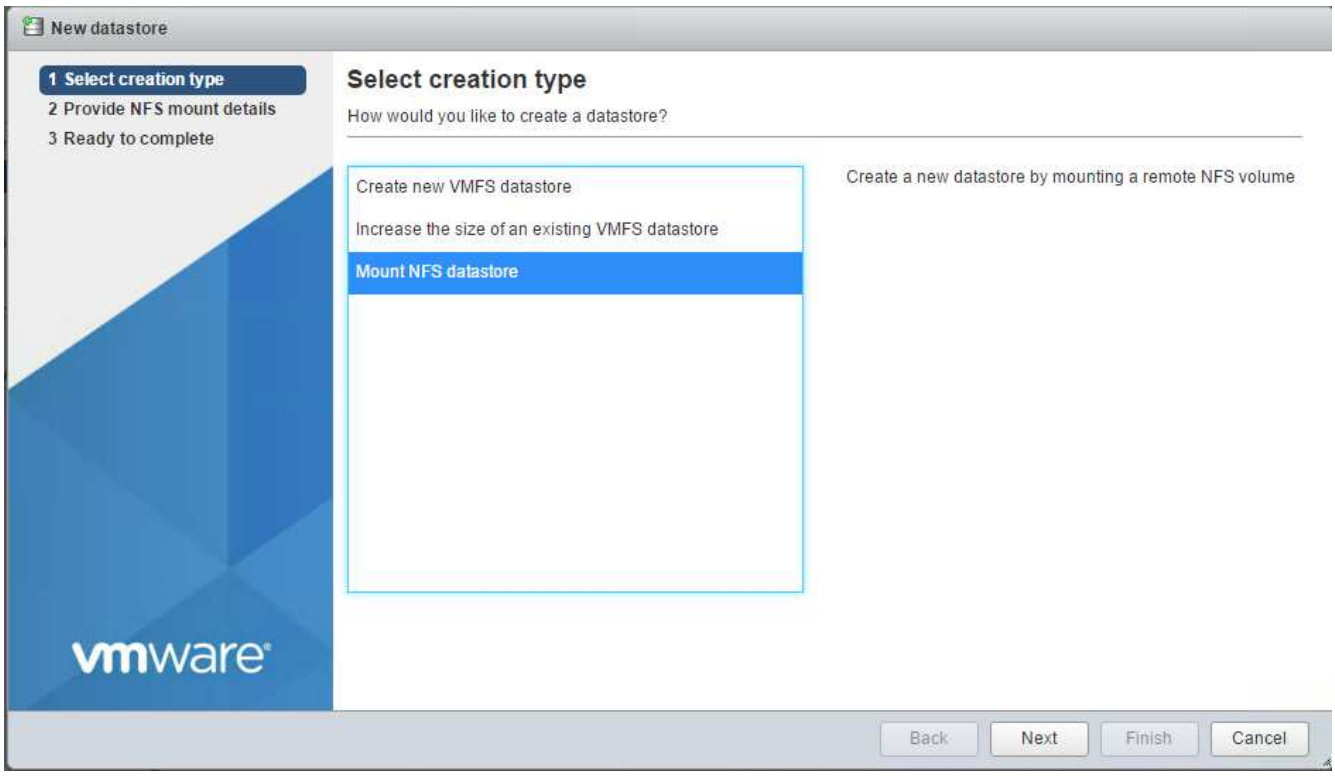
**Erste Datastores mounten**

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.



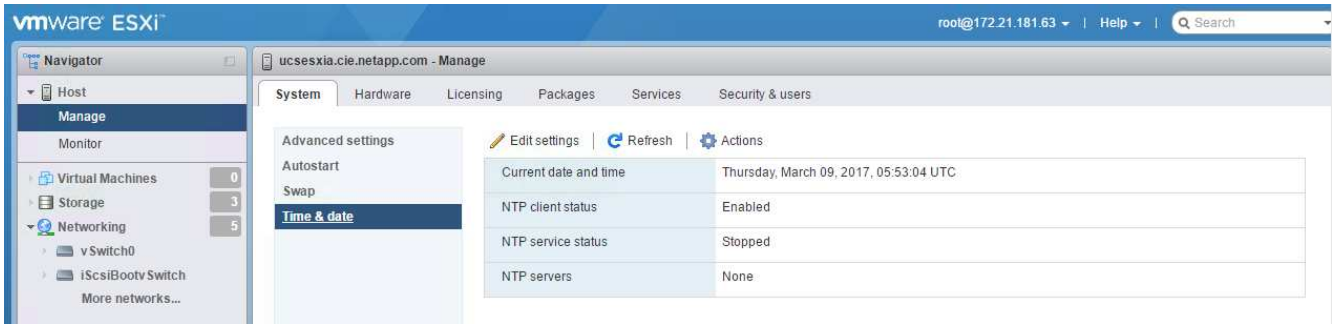

3. Geben Sie als Nächstes die folgenden Informationen auf der Seite „NFS Mount Details angeben“ ein:
   - Name: `infra_datastore_1`
   - NFS-Server: `<<var_nodea_nfs_lif>>`
   - Freigabe: /Infra_Datastore_1
   - Stellen Sie sicher, dass NFS 3 ausgewählt ist.
4. Klicken Sie Auf Fertig Stellen. Die Aufgabe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

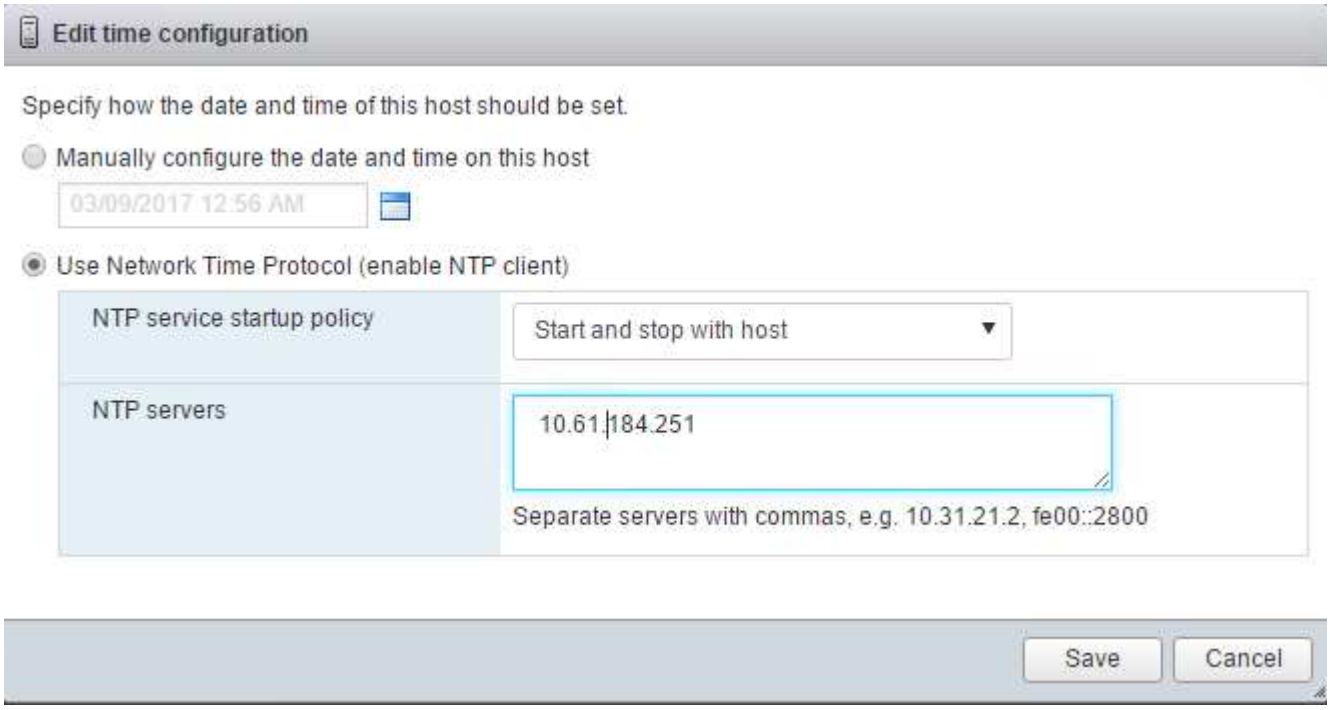
### Konfigurieren Sie NTP

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.



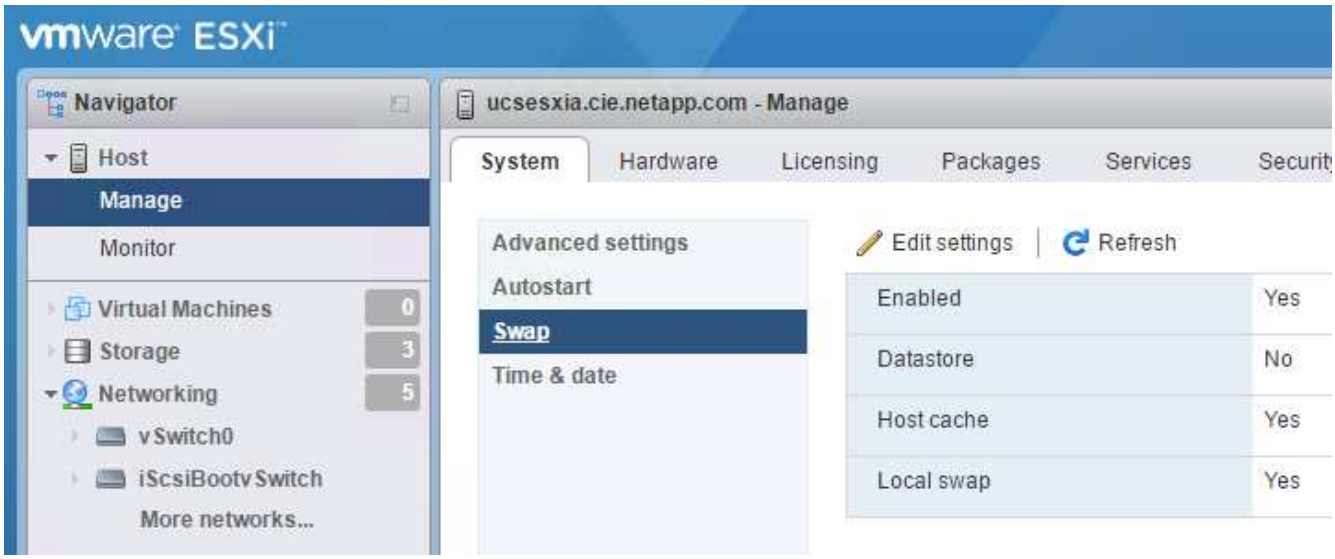

2. Wählen Sie Network Time Protocol (Network Time Protocol verwenden) (NTP Client aktivieren) aus.
3. Wählen Sie Start und Stopp mit Host als Startrichtlinie für den NTP-Dienst aus.
4. Eingabe `<<var_ntp>>` Als NTP-Server. Sie können mehrere NTP-Server festlegen.
5. Klicken Sie auf Speichern .




### 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"

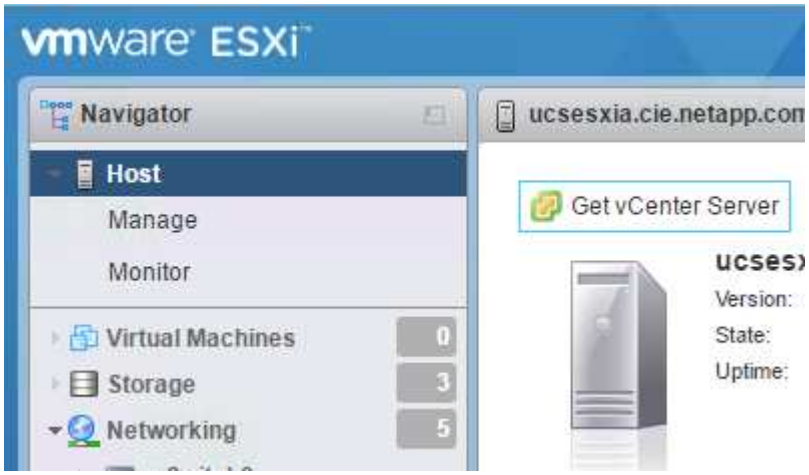
# Installieren Sie VMware vCenter Server 6.7

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

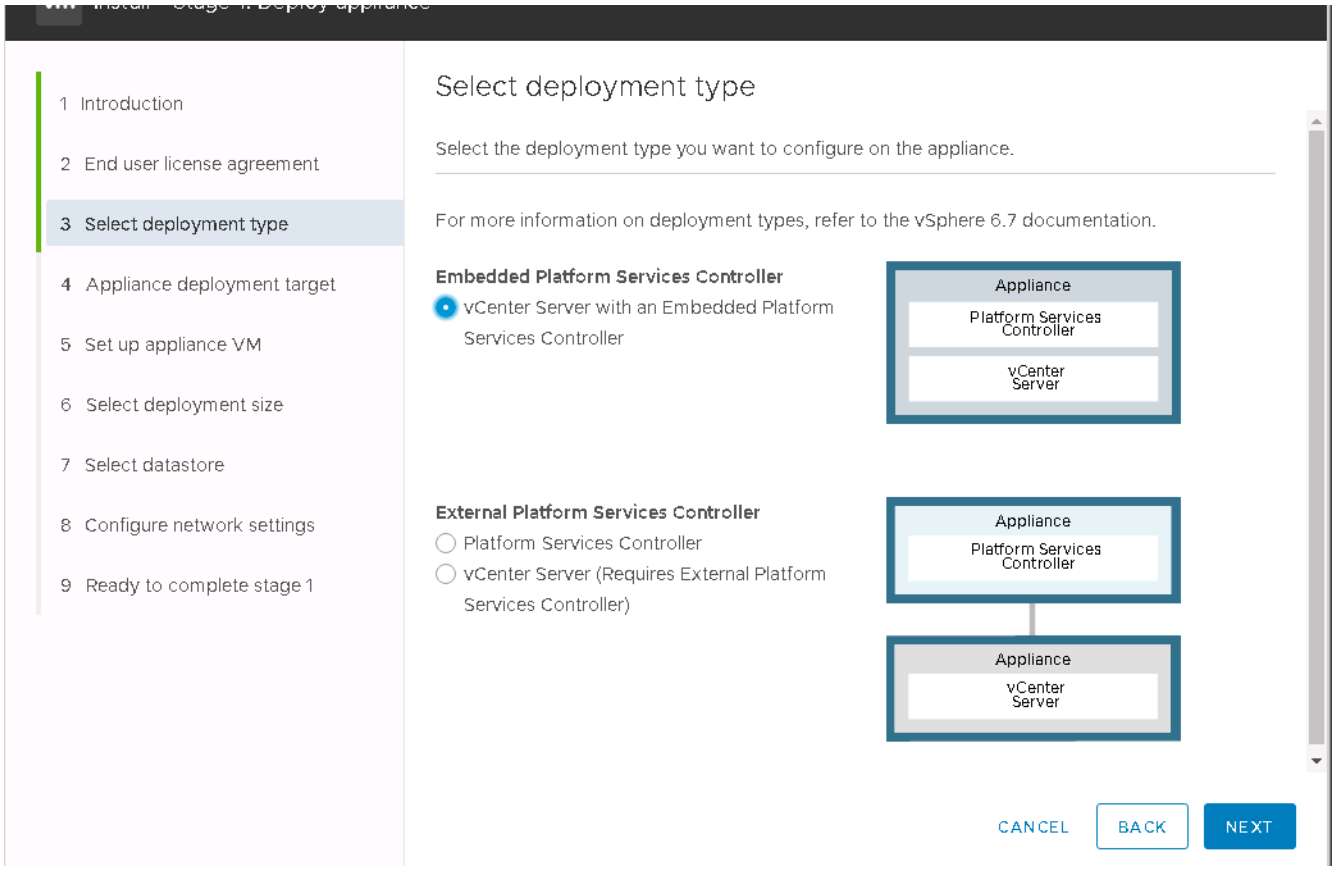
1. Laden Sie die VCSA herunter. Öffnen Sie den Download-Link, indem Sie bei der Verwaltung des ESXi-Hosts auf das Symbol vCenter Server abrufen klicken.




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

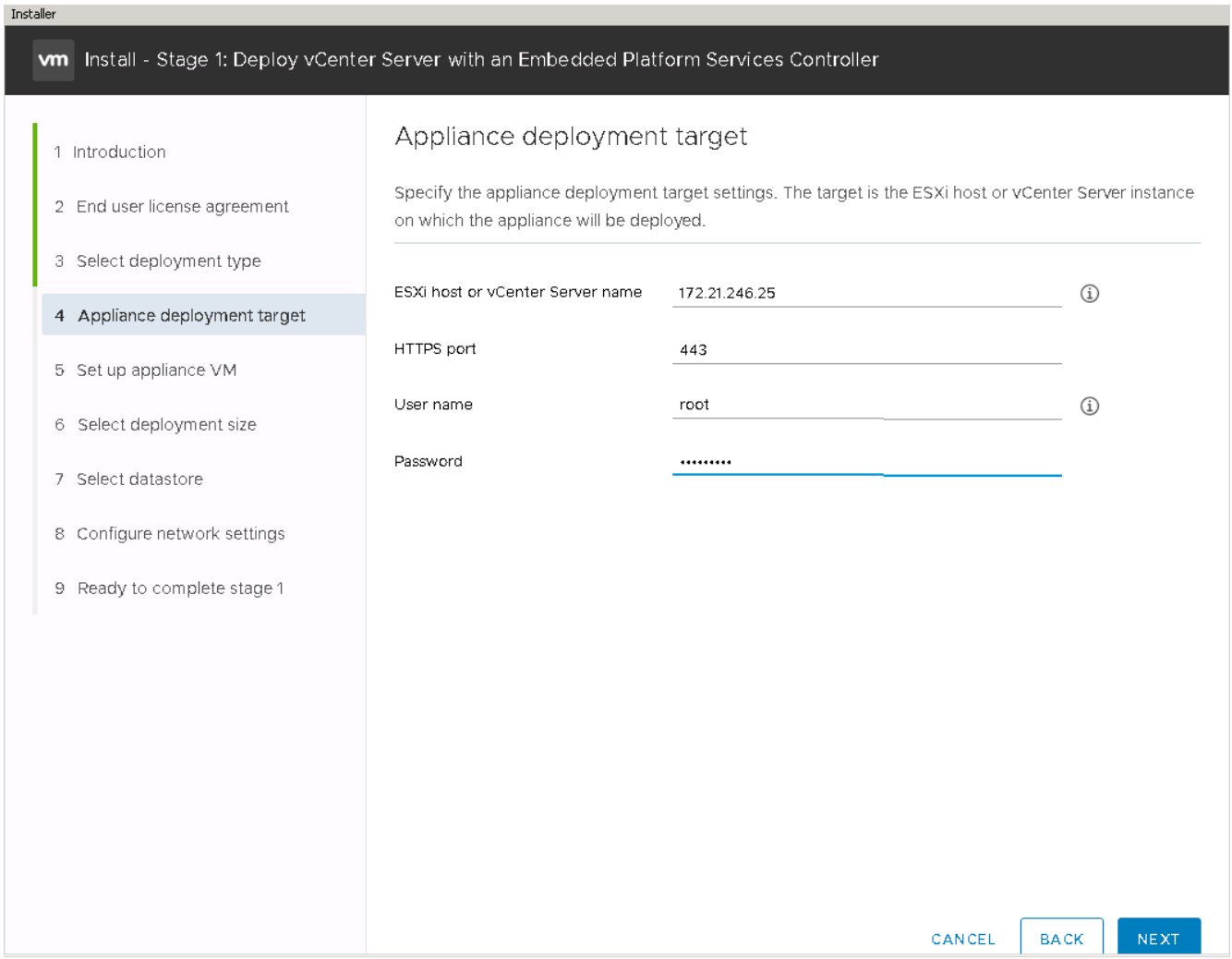
> Obwohl die installierbare Microsoft Windows vCenter Server unterstützt wird, empfiehlt VMware VCSA für neue Implementierungen.

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.

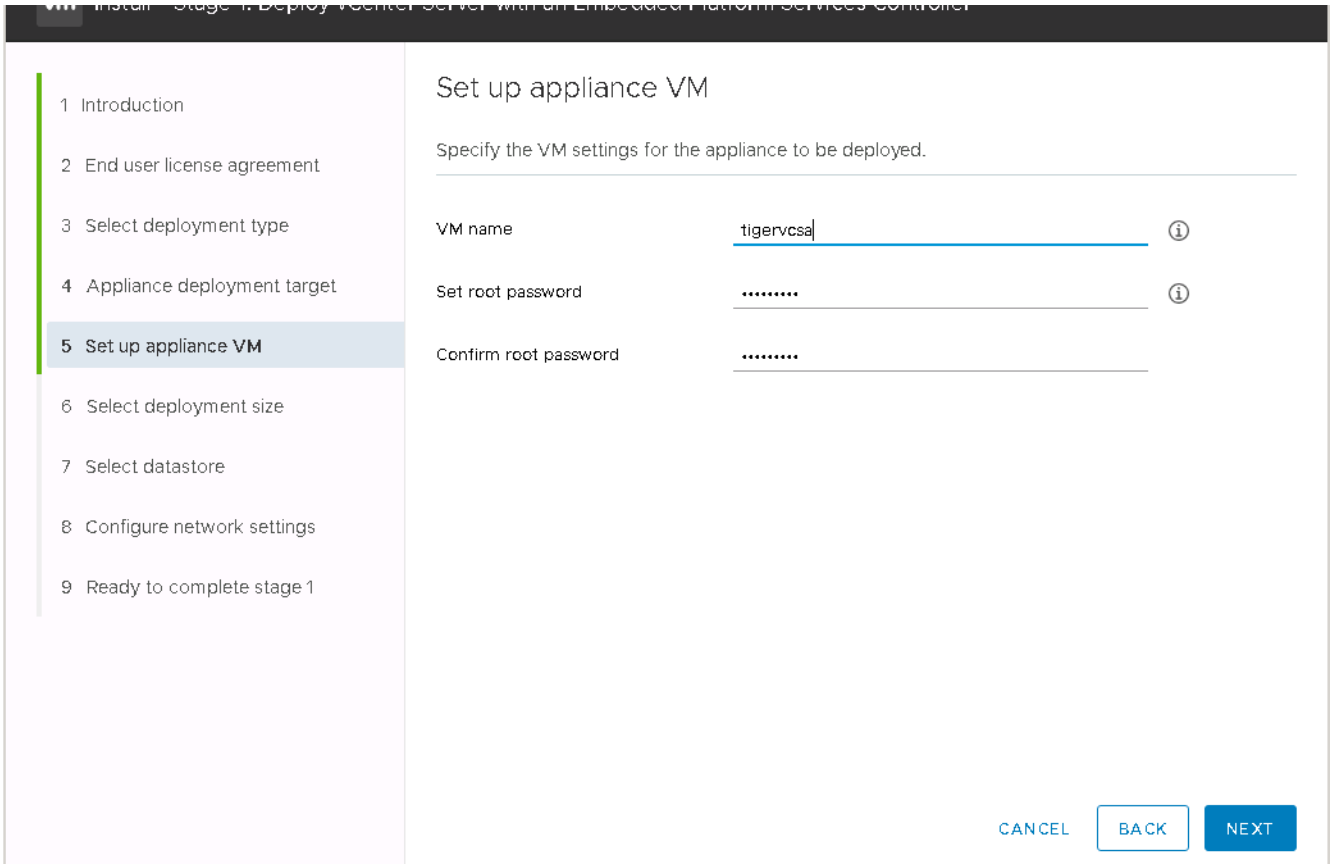



Falls erforderlich wird auch die Controller-Implementierung für externe Plattformen im Rahmen der FlexPod Express Lösung unterstützt.

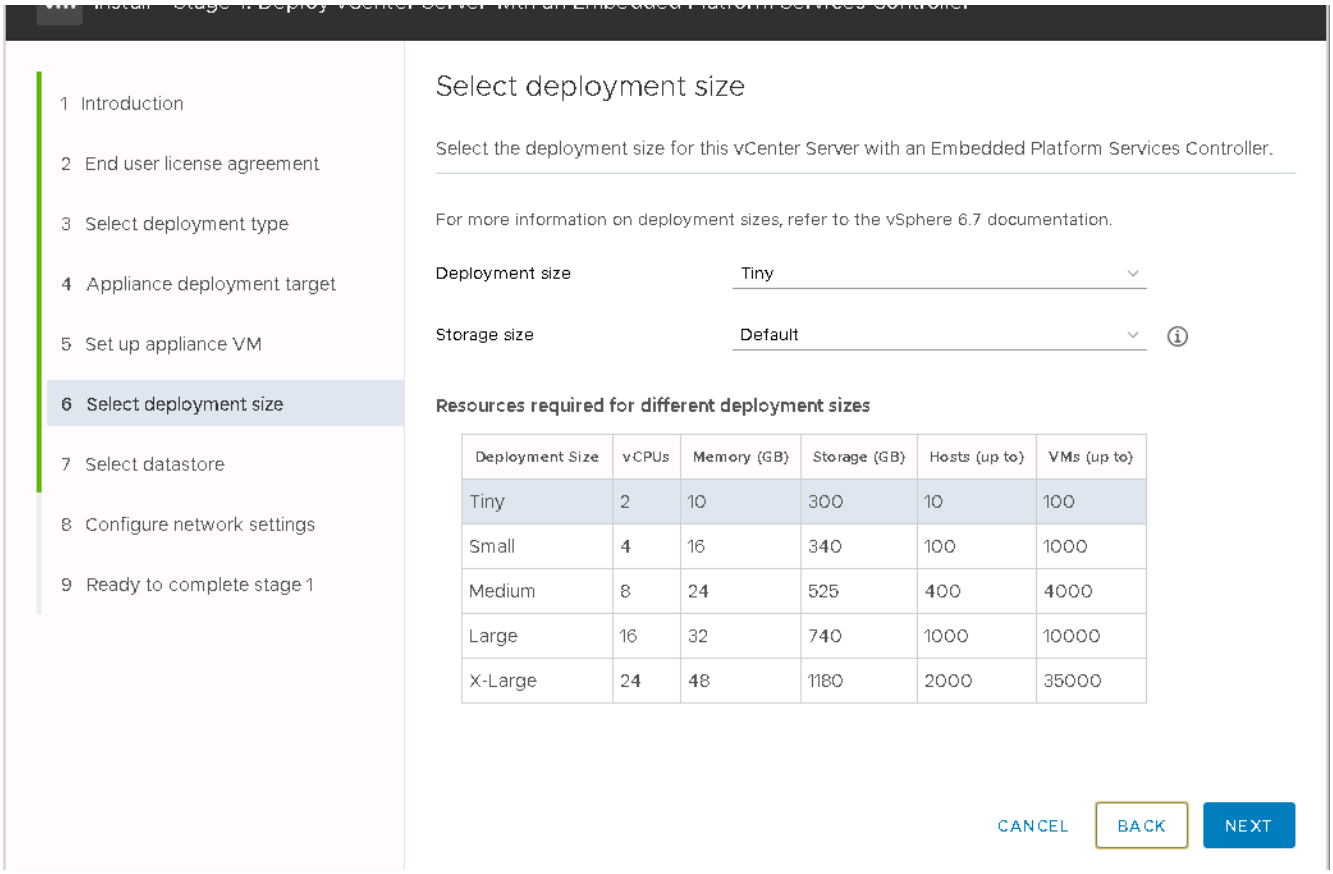
9. Geben Sie im Bereitstellungsziel der Appliance die IP-Adresse eines bereitgestellten ESXi-Hosts sowie den Root-Benutzernamen und das Root-Passwort ein.



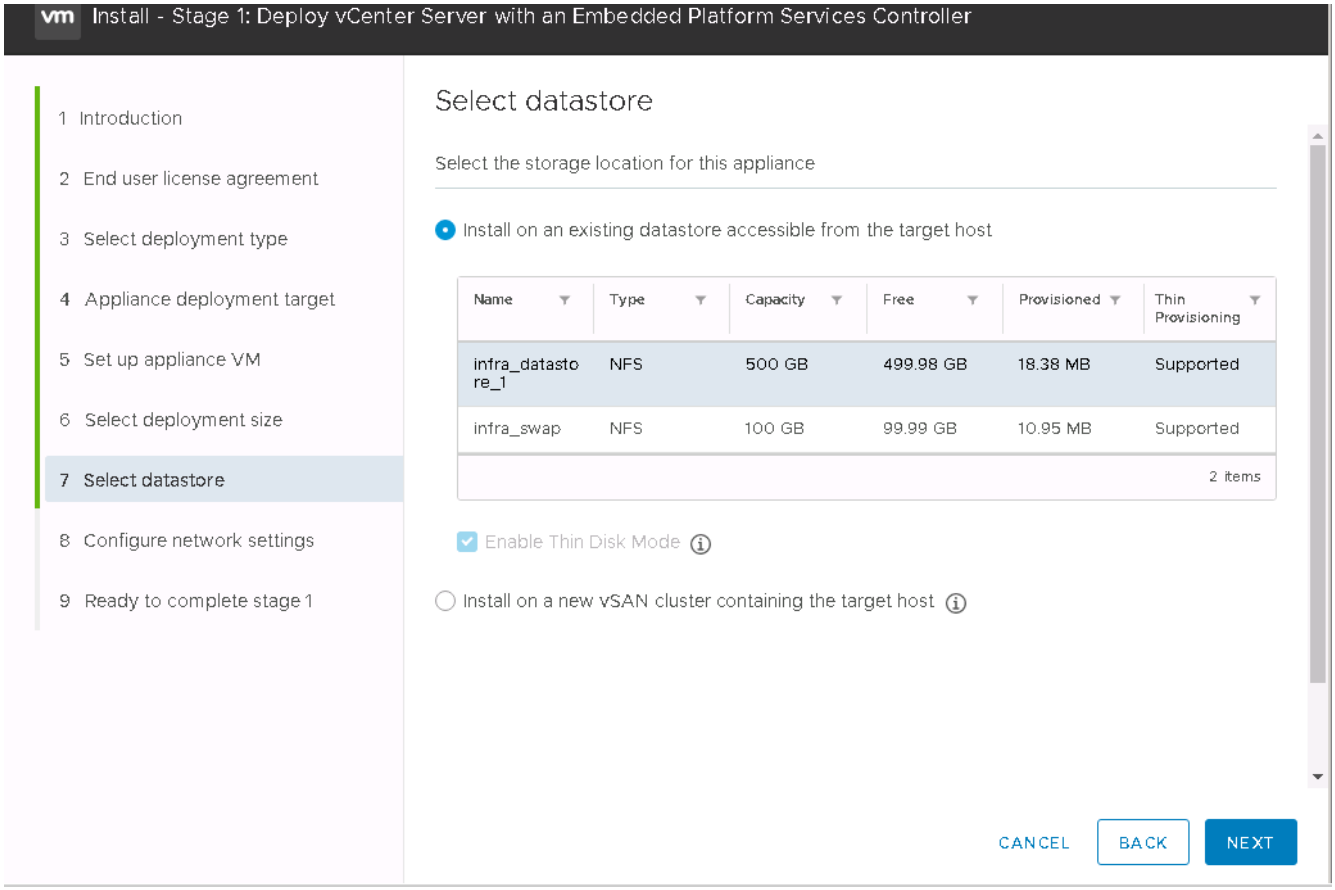

10. Legen Sie die Appliance-VM fest, indem Sie eingeben `VCSA` Als VM-Name und das Root-Passwort, das Sie für den VCSA verwenden möchten.



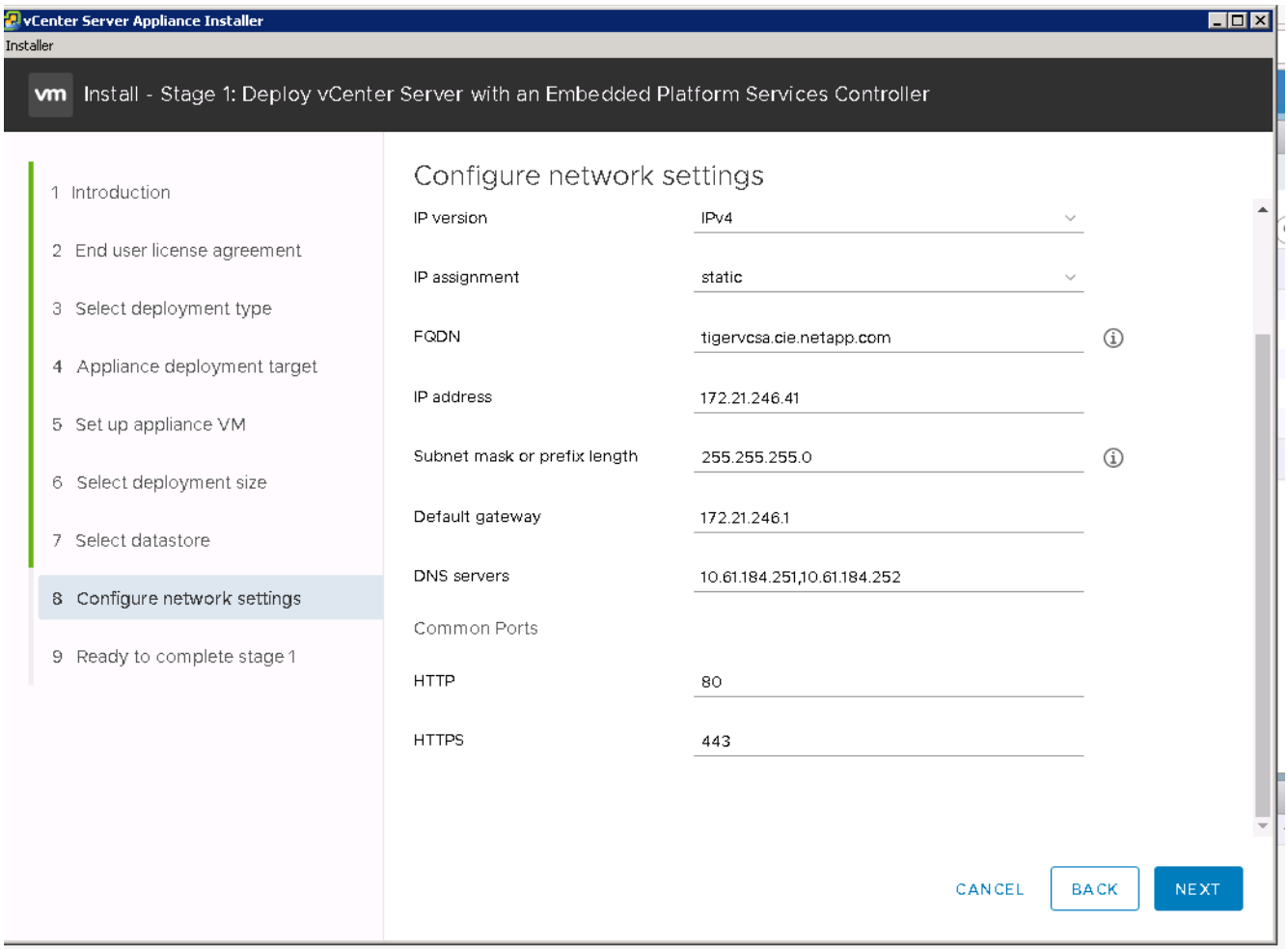

11. Wählen Sie die Implementierungsgröße aus, die am besten zu Ihrer Umgebung passt. Klicken Sie Auf Weiter.



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

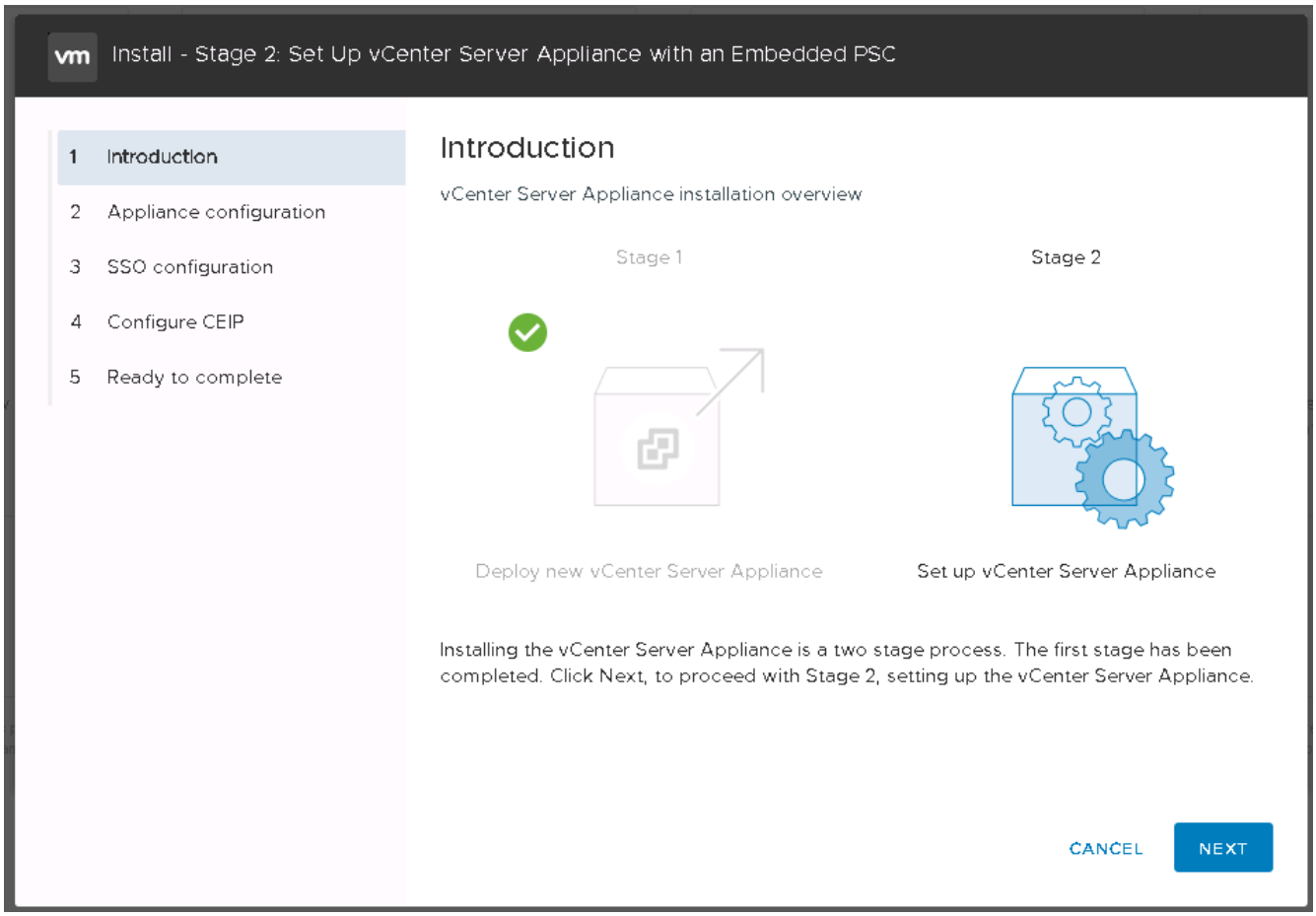



13. Geben Sie die folgenden Informationen auf der Seite Netzwerkeinstellungen konfigurieren ein, und klicken Sie auf Weiter.
    a. Wählen Sie MGMT-Network für Netzwerk.
    b. Geben Sie den FQDN oder die IP ein, die für den VCSA verwendet werden sollen.
    c. Geben Sie die zu verwendenden IP-Adresse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

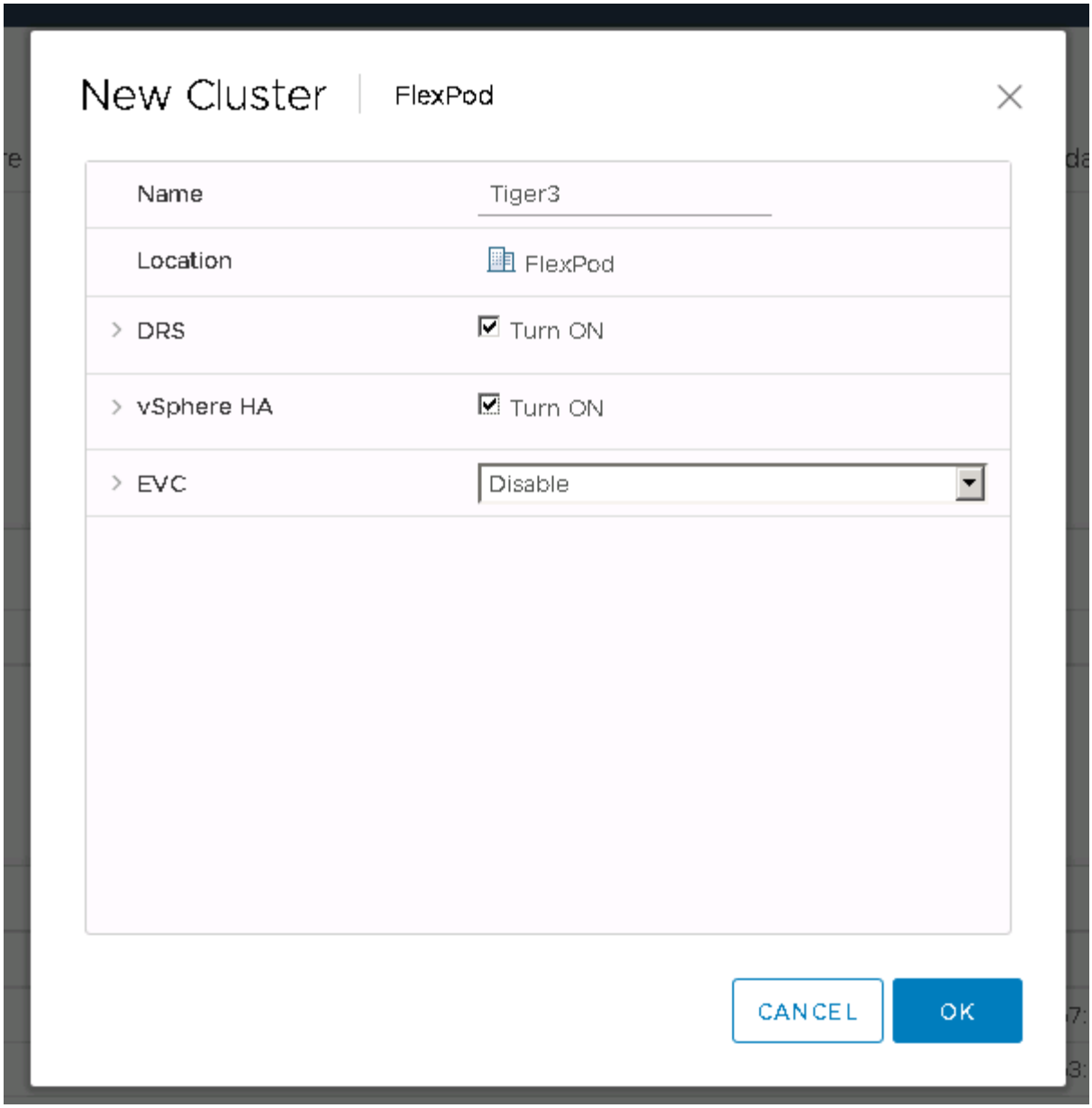
Gehen Sie wie folgt vor, um VMware vCenter Server 6.7- und vSphere-Clustering zu konfigurieren:

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

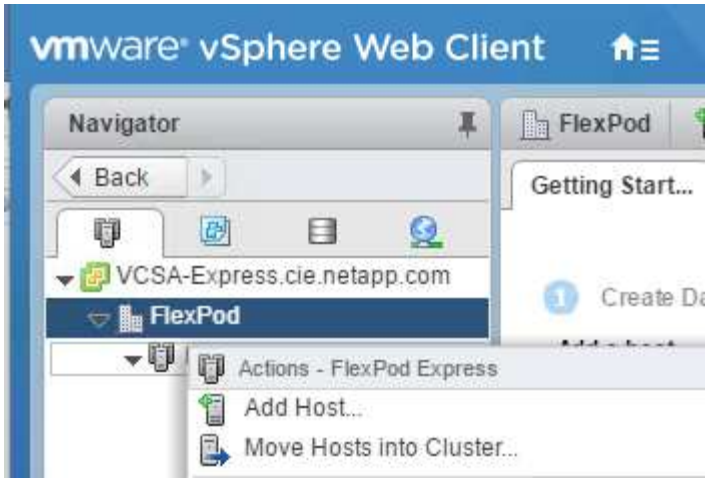
Führen Sie die folgenden Schritte aus, um einen vSphere-Cluster zu erstellen:

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.

**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.