Procedure di implementazione

FlexPod

NetApp
March 25, 2024

Sommario

Procedure di implementazione

Questo documento fornisce informazioni dettagliate sulla configurazione di un sistema FlexPod Express completamente ridondante e ad alta disponibilità. Per riflettere questa ridondanza, i componenti configurati in ogni fase sono indicati come componente A o componente B. Ad esempio, i controller A e B identificano i due storage controller NetApp forniti in questo documento. Gli switch A e B identificano una coppia di switch Cisco Nexus.

Inoltre, questo documento descrive i passaggi per il provisioning di più host Cisco UCS, identificati in sequenza come server A, server B e così via.

Per indicare che è necessario includere in una fase le informazioni relative all'ambiente in uso, `<<text>>` viene visualizzato come parte della struttura dei comandi. Vedere l'esempio seguente per `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Questo documento consente di configurare completamente l'ambiente FlexPod Express. In questo processo, diversi passaggi richiedono l'inserimento di convenzioni di denominazione specifiche del cliente, indirizzi IP e schemi VLAN (Virtual Local Area Network). La tabella seguente descrive le VLAN richieste per l'implementazione, come descritto in questa guida. Questa tabella può essere completata in base alle variabili specifiche del sito e utilizzata per implementare le fasi di configurazione del documento.

> Se si utilizzano VLAN di gestione separate in-band e out-of-band, è necessario creare un percorso Layer-3 tra di esse. Per questa convalida, è stata utilizzata una VLAN di gestione comune.

UN Nome	Scopo della VLAN	ID utilizzato per la convalida di questo documento
VLAN di gestione	VLAN per le interfacce di gestione	3437
VLAN nativa	VLAN a cui sono assegnati frame senza tag	2
VLAN NFS	VLAN per traffico NFS	3438
VLAN VMware vMotion	VLAN designata per lo spostamento delle macchine virtuali da un host fisico a un altro	3441
VLAN del traffico delle macchine virtuali	VLAN per il traffico delle applicazioni delle macchine virtuali	3442
ISCSI-A-VLAN	VLAN per il traffico iSCSI sul fabric A.	3439
ISCSI-B-VLAN	VLAN per il traffico iSCSI sul fabric B.	3440

I numeri VLAN sono necessari per tutta la configurazione di FlexPod Express. Le VLAN sono indicate come

`<<var_xxxx_vlan>>`, dove `xxxx` È lo scopo della VLAN (ad esempio iSCSI-A).

La tabella seguente elenca le macchine virtuali VMware create.

Descrizione della macchina virtuale	Nome host
VMware vCenter Server	

Procedura di implementazione di Cisco Nexus 3172P

La sezione seguente descrive in dettaglio la configurazione dello switch Cisco Nexus 3172P utilizzata in un ambiente FlexPod Express.

Configurazione iniziale dello switch Cisco Nexus 3172P

Le seguenti procedure descrivono come configurare gli switch Cisco Nexus per l'utilizzo in un ambiente FlexPod Express di base.

> Questa procedura presuppone che si stia utilizzando un Cisco Nexus 3172P con software NX-OS versione 7.0(3)I7(5).

1. All'avvio iniziale e alla connessione alla porta della console dello switch, viene avviata automaticamente l'installazione di Cisco NX-OS. Questa configurazione iniziale riguarda le impostazioni di base, come il nome dello switch, la configurazione dell'interfaccia mgmt0 e l'installazione di Secure Shell (SSH).
2. La rete di gestione FlexPod Express può essere configurata in diversi modi. Le interfacce mgmt0 degli switch 3172P possono essere collegate a una rete di gestione esistente oppure le interfacce mgmt0 degli switch 3172P possono essere collegate in una configurazione back-to-back. Tuttavia, questo collegamento non può essere utilizzato per l'accesso alla gestione esterna, ad esempio il traffico SSH.

   In questa guida all'implementazione, gli switch Cisco Nexus 3172P FlexPod sono connessi a una rete di gestione esistente.

3. Per configurare gli switch Cisco Nexus 3172P, accendere lo switch e seguire le istruzioni visualizzate sullo schermo, come illustrato di seguito per la configurazione iniziale di entrambi gli switch, sostituendo i valori appropriati con le informazioni specifiche dello switch.

```
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. Viene visualizzato un riepilogo della configurazione e viene richiesto se si desidera modificarla. Se la configurazione è corretta, immettere `n`.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. Viene quindi richiesto se si desidera utilizzare questa configurazione e salvarla. In tal caso, immettere `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Ripetere questa procedura per lo switch Cisco Nexus B.

Abilitare le funzionalità avanzate

Alcune funzionalità avanzate devono essere attivate in Cisco NX-OS per fornire ulteriori opzioni di configurazione.

> Il `interface-vlan` la funzione è necessaria solo se si utilizza il back-to-back `mgmt0` opzione descritta in questo documento. Questa funzione consente di assegnare un indirizzo IP all'interfaccia VLAN (interfaccia virtuale dello switch), che consente la comunicazione di gestione in banda allo switch (ad esempio tramite SSH).

1. Per abilitare le funzioni appropriate sugli switch a e B di Cisco Nexus, accedere alla modalità di configurazione utilizzando il comando `(config t)` ed eseguire i seguenti comandi:

   ```
   feature interface-vlan
   feature lacp
   feature vpc
   ```

   L'hash predefinito per il bilanciamento del carico del canale della porta utilizza gli indirizzi IP di origine e di destinazione per determinare l'algoritmo di bilanciamento del carico tra le interfacce nel canale della porta. È possibile ottenere una migliore distribuzione tra i membri del canale delle porte fornendo più input all'algoritmo hash oltre agli indirizzi IP di origine e di destinazione. Per lo stesso motivo, NetApp consiglia vivamente di aggiungere le porte TCP di origine e di destinazione all'algoritmo hash.

2. Dalla modalità di configurazione (`config t`), immettere i seguenti comandi per impostare la configurazione del bilanciamento del carico del canale della porta globale sugli switch Cisco Nexus A e B:

   ```
   port-channel load-balance src-dst ip-l4port
   ```

Eseguire la configurazione spanning-tree globale

La piattaforma Cisco Nexus utilizza una nuova funzione di protezione chiamata Bridge Assurance. Bridge Assurance aiuta a proteggere da un collegamento unidirezionale o da altri errori software con un dispositivo che continua a inoltrare il traffico dati quando non esegue più l'algoritmo spanning-tree. Le porte possono essere posizionate in uno dei diversi stati, tra cui rete o edge, a seconda della piattaforma.

Per impostazione predefinita, NetApp consiglia di impostare il bridge assurance in modo che tutte le porte siano considerate porte di rete. Questa impostazione obbliga l'amministratore di rete a rivedere la configurazione di ciascuna porta. Inoltre, vengono visualizzati gli errori di configurazione più comuni, ad esempio porte edge non identificate o un vicino che non dispone della funzione di bridge assurance attivata. Inoltre, è più sicuro avere il blocco spanning tree molte porte piuttosto che troppo poche, il che consente allo stato di porta predefinito di migliorare la stabilità generale della rete.

Prestare particolare attenzione allo stato spanning tree quando si aggiungono server, storage e switch uplink, soprattutto se non supportano la funzione Bridge Assurance. In questi casi, potrebbe essere necessario modificare il tipo di porta per rendere attive le porte.

La protezione BPDU (Bridge Protocol Data Unit) è attivata per impostazione predefinita sulle porte edge come un altro livello di protezione. Per evitare loop nella rete, questa funzione arresta la porta se su questa interfaccia vengono visualizzate le BPDU di un altro switch.

Dalla modalità di configurazione (`config t`), eseguire i seguenti comandi per configurare le opzioni di spanning tree predefinite, tra cui il tipo di porta predefinita e BPDU Guard, sugli switch Cisco Nexus A e B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Definire le VLAN

Prima di configurare singole porte con VLAN diverse, è necessario definire le VLAN di livello 2 sullo switch. È inoltre consigliabile assegnare un nome alle VLAN per semplificare la risoluzione dei problemi in futuro.

Dalla modalità di configurazione (`config t`), eseguire i seguenti comandi per definire e descrivere le VLAN di livello 2 sugli switch Cisco Nexus A e B:

```
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
```

Configurare le descrizioni delle porte di accesso e di gestione

Come nel caso dell'assegnazione di nomi alle VLAN di livello 2, l'impostazione delle descrizioni per tutte le interfacce può essere utile sia per il provisioning che per la risoluzione dei problemi.

Dalla modalità di configurazione (`config t`) In ciascuno degli switch, immettere le seguenti descrizioni delle porte per la configurazione Large di FlexPod:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configurare le interfacce di gestione dello storage e del server

Le interfacce di gestione per il server e lo storage in genere utilizzano solo una singola VLAN. Pertanto, configurare le porte dell'interfaccia di gestione come porte di accesso. Definire la VLAN di gestione per ogni switch e modificare il tipo di porta spanning-tree in edge.

Dalla modalità di configurazione (`config t`), immettere i seguenti comandi per configurare le impostazioni delle porte per le interfacce di gestione dei server e dello storage:

Switch Cisco Nexus A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Eseguire la configurazione globale del canale della porta virtuale

Un VPC (Virtual Port Channel) consente ai collegamenti fisicamente collegati a due diversi switch Cisco Nexus di apparire come un singolo canale di porta su un terzo dispositivo. Il terzo dispositivo può essere uno switch, un server o qualsiasi altro dispositivo di rete. Un VPC è in grado di fornire il multipathing Layer-2, che consente di creare ridondanza aumentando la larghezza di banda, consentendo percorsi paralleli multipli tra i nodi e il traffico con bilanciamento del carico dove esistono percorsi alternativi.

Un VPC offre i seguenti vantaggi:

- Abilitazione di un singolo dispositivo all'utilizzo di un canale di porta su due dispositivi upstream
- Eliminazione delle porte bloccate dal protocollo spanning-tree
- Fornire una topologia senza loop
- Utilizzando tutta la larghezza di banda uplink disponibile
- Fornire una rapida convergenza in caso di guasto del collegamento o di un dispositivo
- Fornire resilienza a livello di collegamento
- Fornire alta disponibilità

La funzione VPC richiede alcune impostazioni iniziali tra i due switch Cisco Nexus per funzionare correttamente. Se si utilizza la configurazione mgmt0 back-to-back, utilizzare gli indirizzi definiti nelle interfacce e verificare che possano comunicare utilizzando il ping `[switch_A/B_mgmt0_ip_addr]vrf` comando di gestione.

Dalla modalità di configurazione (`config t`), eseguire i seguenti comandi per configurare la configurazione globale VPC per entrambi gli switch:

Switch Cisco Nexus 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
```

Switch Cisco Nexus 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
```

Configurare i canali delle porte di storage

I controller di storage NetApp consentono una connessione Active-Active alla rete utilizzando il protocollo LACP (link Aggregation Control Protocol). L'utilizzo di LACP è preferibile in quanto aggiunge sia la negoziazione che la registrazione tra gli switch. Poiché la rete è configurata per VPC, questo approccio consente di disporre di connessioni Active-Active dallo storage per separare gli switch fisici. Ciascun controller dispone di due collegamenti a ciascuno degli switch. Tuttavia, tutti e quattro i collegamenti fanno parte dello stesso VPC e dello stesso gruppo di interfacce (IFGRP).

Dalla modalità di configurazione (`config t`), eseguire i seguenti comandi su ciascuno switch per configurare le singole interfacce e la configurazione del canale di porta risultante per le porte collegate al controller NetApp AFF.

1. Eseguire i seguenti comandi sugli switch A e B per configurare i canali delle porte per lo storage controller A:

```
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. Eseguire i seguenti comandi sullo switch A e B per configurare i canali delle porte per lo storage controller B.

```
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
```

Nella convalida di questa soluzione, è stato utilizzato un MTU di 9000. Tuttavia, in base ai requisiti dell'applicazione, è possibile configurare un valore appropriato di MTU. È importante impostare lo stesso valore MTU nella soluzione FlexPod. Configurazioni MTU errate tra i componenti causeranno l'interruzione dei pacchetti e di questi pacchetti.

Configurare le connessioni al server

I server Cisco UCS dispongono di una scheda di interfaccia virtuale a due porte, VIC1387, utilizzata per il traffico dati e l'avvio del sistema operativo ESXi utilizzando iSCSI. Queste interfacce sono configurate per il failover reciproco, fornendo ridondanza aggiuntiva oltre un singolo collegamento. La diffusione di questi collegamenti su più switch consente al server di sopravvivere anche a un guasto completo dello switch.

Dalla modalità di configurazione (`config t`), eseguire i seguenti comandi per configurare le impostazioni delle porte per le interfacce collegate a ciascun server.

Cisco Nexus Switch A: Configurazione Cisco UCS Server-A e Cisco UCS Server-B.

```
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: Configurazione Cisco UCS Server-A e 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
```

Nella convalida di questa soluzione, è stato utilizzato un MTU di 9000. Tuttavia, in base ai requisiti dell'applicazione, è possibile configurare un valore appropriato di MTU. È importante impostare lo stesso valore MTU nella soluzione FlexPod. Le configurazioni MTU errate tra i componenti causeranno l'interruzione dei pacchetti e la loro nuova trasmissione. Questo influirà sulle prestazioni complessive della soluzione.

Per scalare la soluzione aggiungendo altri server Cisco UCS, eseguire i comandi precedenti con le porte dello switch a cui sono stati collegati i nuovi server aggiunti sugli switch A e B.

Uplink nell'infrastruttura di rete esistente

A seconda dell'infrastruttura di rete disponibile, è possibile utilizzare diversi metodi e funzionalità per eseguire l'uplink dell'ambiente FlexPod. Se è presente un ambiente Cisco Nexus esistente, NetApp consiglia di utilizzare VPC per eseguire l'uplink degli switch Cisco Nexus 3172P inclusi nell'ambiente FlexPod nell'infrastruttura. Gli uplink possono essere uplink 10 GbE per una soluzione di infrastruttura 10 GbE o 1 GbE per una soluzione di infrastruttura 1 GbE, se necessario. Le procedure descritte in precedenza possono essere utilizzate per creare un VPC uplink nell'ambiente esistente. Assicurarsi di eseguire l'avvio dell'esecuzione della

copia per salvare la configurazione su ogni switch dopo il completamento della configurazione.

"Pagina successiva: Procedura di implementazione dello storage NetApp (parte 1)"

Procedura di implementazione dello storage NetApp (parte 1)

Questa sezione descrive la procedura di implementazione dello storage NetApp AFF.

Installazione del controller di storage NetApp serie AFF2xx

NetApp Hardware Universe

L'applicazione NetApp Hardware Universe (HWU) fornisce componenti hardware e software supportati per qualsiasi versione specifica di ONTAP. Fornisce informazioni di configurazione per tutte le appliance di storage NetApp attualmente supportate dal software ONTAP. Fornisce inoltre una tabella delle compatibilità dei componenti.

Verificare che i componenti hardware e software che si desidera utilizzare siano supportati con la versione di ONTAP che si intende installare:

1. Accedere a. "HWU" per visualizzare le guide di configurazione del sistema. Fare clic sulla scheda Controller per visualizzare la compatibilità tra le diverse versioni del software ONTAP e le appliance di storage NetApp con le specifiche desiderate.
2. In alternativa, per confrontare i componenti in base all'appliance di storage, fare clic su Confronta sistemi di storage.

Prerequisiti della serie AFF2XX del controller
Per pianificare la posizione fisica dei sistemi storage, consultare la NetApp Hardware Universe. Fare riferimento alle seguenti sezioni: Requisiti elettrici, cavi di alimentazione supportati e porte e cavi integrati.

Controller di storage

Seguire le procedure di installazione fisica per i controller in "Documentazione di AFF A220".

NetApp ONTAP 9.4

Foglio di lavoro per la configurazione

Prima di eseguire lo script di installazione, completare il foglio di lavoro di configurazione contenuto nel manuale del prodotto. Il foglio di lavoro di configurazione è disponibile in "Guida alla configurazione del software ONTAP 9.4".

> Questo sistema viene configurato in una configurazione cluster senza switch a due nodi.

La seguente tabella mostra le informazioni di installazione e configurazione di ONTAP 9.4.

Dettaglio del cluster	Valore dei dettagli del cluster
Indirizzo IP del nodo cluster A.	[var_nodeA_mgmt_ip]

Dettaglio del cluster	Valore dei dettagli del cluster
Netmask del nodo cluster A.	[var_nodeA_mgmt_mask]
Nodo cluster A gateway	[var_nodeA_mgmt_gateway]
Nome del nodo cluster A.	[var_nodeA]
Indirizzo IP del nodo B del cluster	[var_nodeB_mgmt_ip]
Netmask del nodo B del cluster	[var_nodeB_mgmt_mask]
Gateway del nodo B del cluster	[var_nodeB_mgmt_gateway]
Nome del nodo B del cluster	[var_nodeB]
URL ONTAP 9.4	[var_url_boot_software]
Nome del cluster	[var_clustername]
Indirizzo IP di gestione del cluster	[var_clustermgmt_ip]
Gateway del cluster B.	[var_clustermgmt_gateway]
Netmask del cluster B.	[var_clustermgmt_mask]
Nome di dominio	[var_domain_name]
IP del server DNS (è possibile immettere più di uno)	[var_dns_server_ip]
IP server NTP (è possibile immettere più di un indirizzo)	[var_ntp_server_ip]

Configurare il nodo A.

Per configurare il nodo A, attenersi alla seguente procedura:

1. Connettersi alla porta della console del sistema di storage. Viene visualizzato un prompt Loader-A. Tuttavia, se il sistema di storage si trova in un loop di riavvio, premere Ctrl-C per uscire dal loop di avvio automatico quando viene visualizzato questo messaggio:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Consentire l'avvio del sistema.

   ```
   autoboot
   ```

3. Premere Ctrl-C per accedere al menu di avvio.

   Se ONTAP 9.4 non è la versione del software da avviare, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9.4 è la versione da avviare, selezionare l'opzione 8 e y per riavviare il nodo. Quindi, passare alla fase 14.

4. Per installare il nuovo software, selezionare l'opzione `7`.
5. Invio `y` per eseguire un aggiornamento.

6. Selezionare `e0M` per la porta di rete che si desidera utilizzare per il download.
7. Invio `y` per riavviare ora.
8. Inserire l'indirizzo IP, la netmask e il gateway predefinito per e0M nelle rispettive posizioni.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Inserire l'URL in cui è possibile trovare il software.

   Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

10. Premere Invio per il nome utente, che non indica alcun nome utente.
11. Invio `y` per impostare il software appena installato come predefinito da utilizzare per i riavvii successivi.
12. Invio `y` per riavviare il nodo.

    Durante l'installazione di un nuovo software, il sistema potrebbe eseguire aggiornamenti del firmware del BIOS e delle schede adattatore, causando riavvii e possibili arresti al prompt di Loader-A. Se si verificano queste azioni, il sistema potrebbe discostarsi da questa procedura.

13. Premere Ctrl-C per accedere al menu di avvio.
14. Selezionare l'opzione `4` Per la configurazione pulita e l'inizializzazione di tutti i dischi.
15. Invio `y` per azzerare i dischi, ripristinare la configurazione e installare un nuovo file system.
16. Invio `y` per cancellare tutti i dati presenti sui dischi.

    Il completamento dell'inizializzazione e della creazione dell'aggregato root può richiedere 90 minuti o più, a seconda del numero e del tipo di dischi collegati. Una volta completata l'inizializzazione, il sistema di storage si riavvia. Si noti che l'inizializzazione degli SSD richiede molto meno tempo. È possibile continuare con la configurazione del nodo B mentre i dischi del nodo A vengono azzerati.

17. Durante l'inizializzazione del nodo A, iniziare la configurazione del nodo B.

Configurare il nodo B.

Per configurare il nodo B, attenersi alla seguente procedura:

1. Connettersi alla porta della console del sistema di storage. Viene visualizzato un prompt Loader-A. Tuttavia, se il sistema di storage si trova in un loop di riavvio, premere Ctrl-C per uscire dal loop di avvio automatico quando viene visualizzato questo messaggio:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Premere Ctrl-C per accedere al menu di avvio.

```
autoboot
```

3. Premere Ctrl-C quando richiesto.

   Se ONTAP 9.4 non è la versione del software da avviare, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9.4 è la versione da avviare, selezionare l'opzione 8 e y per riavviare il nodo. Quindi, passare alla fase 14.

4. Per installare il nuovo software, selezionare l'opzione 7.
5. Invio `y` per eseguire un aggiornamento.
6. Selezionare `e0M` per la porta di rete che si desidera utilizzare per il download.
7. Invio `y` per riavviare ora.
8. Inserire l'indirizzo IP, la netmask e il gateway predefinito per e0M nelle rispettive posizioni.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Inserire l'URL in cui è possibile trovare il software.

   Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

10. Premere Invio per il nome utente, che non indica alcun nome utente.
11. Invio `y` per impostare il software appena installato come predefinito da utilizzare per i riavvii successivi.
12. Invio `y` per riavviare il nodo.

    Durante l'installazione di un nuovo software, il sistema potrebbe eseguire aggiornamenti del firmware del BIOS e delle schede adattatore, causando riavvii e possibili arresti al prompt di Loader-A. Se si verificano queste azioni, il sistema potrebbe discostarsi da questa procedura.

13. Premere Ctrl-C per accedere al menu di avvio.
14. Selezionare l'opzione 4 per Clean Configuration (pulizia configurazione) e Initialize All Disks (Inizializzazione di tutti
15. Invio `y` per azzerare i dischi, ripristinare la configurazione e installare un nuovo file system.
16. Invio `y` per cancellare tutti i dati presenti sui dischi.

    Il completamento dell'inizializzazione e della creazione dell'aggregato root può richiedere 90 minuti o più, a seconda del numero e del tipo di dischi collegati. Una volta completata l'inizializzazione, il sistema di storage si riavvia. Si noti che l'inizializzazione degli SSD richiede molto meno tempo.

Continuazione della configurazione del nodo A e della configurazione del cluster

Da un programma di porta della console collegato alla porta della console del controller di storage A (nodo A), eseguire lo script di configurazione del nodo. Questo script viene visualizzato quando ONTAP 9.4 viene avviato sul nodo per la prima volta.

> La procedura di configurazione del nodo e del cluster è stata leggermente modificata in ONTAP 9.4. La procedura guidata di installazione del cluster viene ora utilizzata per configurare il primo nodo di un cluster e System Manager viene utilizzato per configurare il cluster.

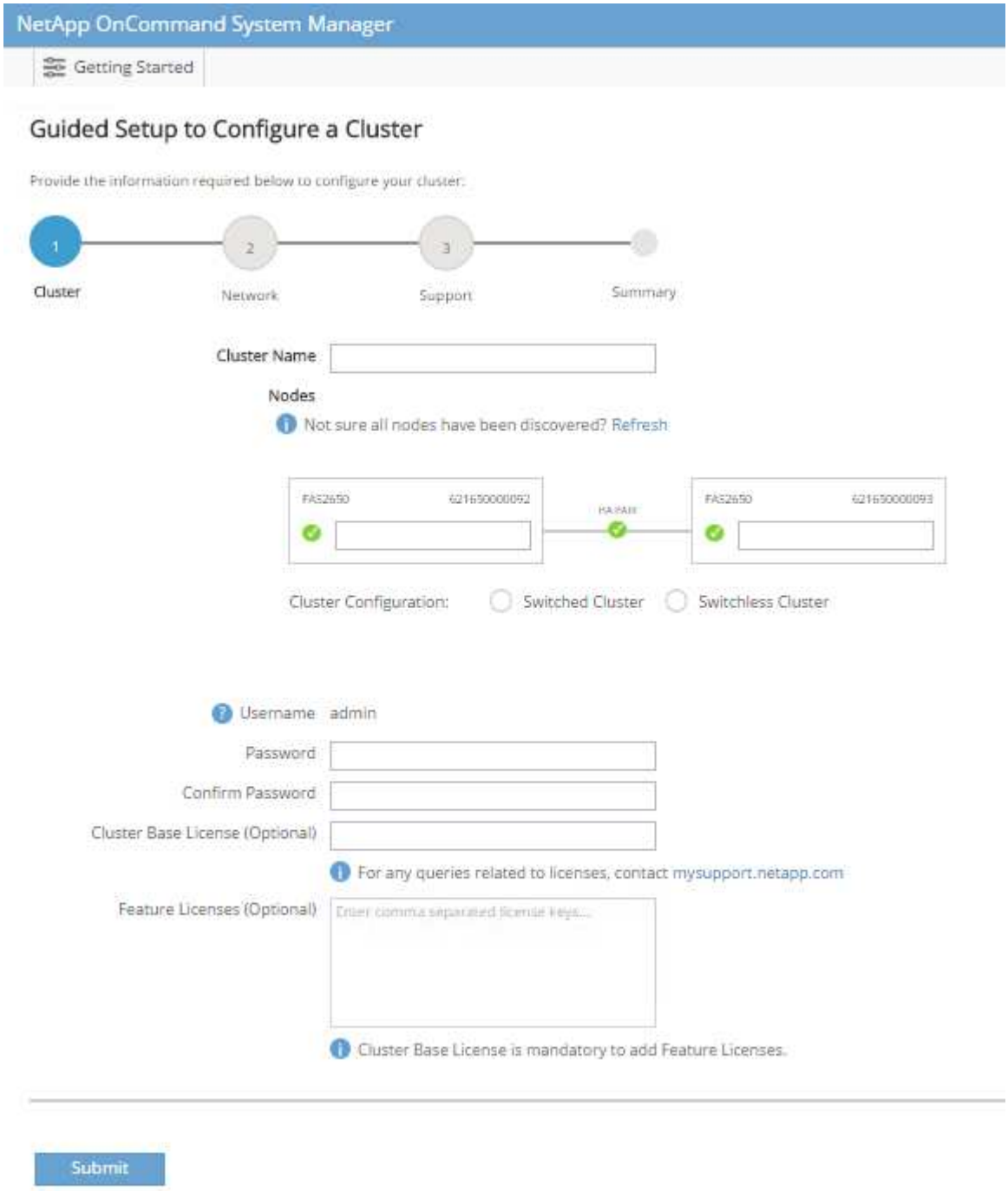
1. Seguire le istruzioni per impostare il nodo A.

```
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. Accedere all'indirizzo IP dell'interfaccia di gestione del nodo.

   L'installazione del cluster può essere eseguita anche utilizzando l'interfaccia CLI. Questo documento descrive la configurazione del cluster utilizzando la configurazione guidata di NetApp System Manager.

3. Fare clic su Guided Setup (Configurazione guidata) per configurare il cluster.
4. Invio `<<var_clustername>>` per il nome del cluster e. `<<var_nodeA>>` e. `<<var_nodeB>>` per ciascuno dei nodi che si sta configurando. Inserire la password che si desidera utilizzare per il sistema di storage. Selezionare Switchless Cluster (Cluster senza switch) per il tipo di cluster. Inserire la licenza di base del cluster.



5. È inoltre possibile inserire licenze delle funzionalità per Cluster, NFS e iSCSI.
6. Viene visualizzato un messaggio di stato che indica che il cluster è in fase di creazione. Questo messaggio di stato passa in rassegna diversi stati. Questo processo richiede alcuni minuti.
7. Configurare la rete.
   a. Deselezionare l'opzione IP Address Range (intervallo indirizzi IP).

b. Invio `<<var_clustermgmt_ip>>` Nel campo Cluster Management IP Address (Indirizzo IP di gestione cluster), `<<var_clustermgmt_mask>>` Nel campo Netmask, e. `<<var_clustermgmt_gateway>>` Nel campo Gateway. Utilizzare il … Nel campo Port (porta) per selezionare e0M del nodo A.

c. L'IP di gestione dei nodi per il nodo A è già popolato. Invio `<<var_nodeA_mgmt_ip>>` Per il nodo B.

d. Invio `<<var_domain_name>>` Nel campo DNS Domain Name (Nome dominio DNS). Invio `<<var_dns_server_ip>>` Nel campo DNS Server IP Address (Indirizzo IP server DNS).

   È possibile immettere più indirizzi IP del server DNS.

e. Invio `<<var_ntp_server_ip>>` Nel campo Primary NTP Server (Server NTP primario).

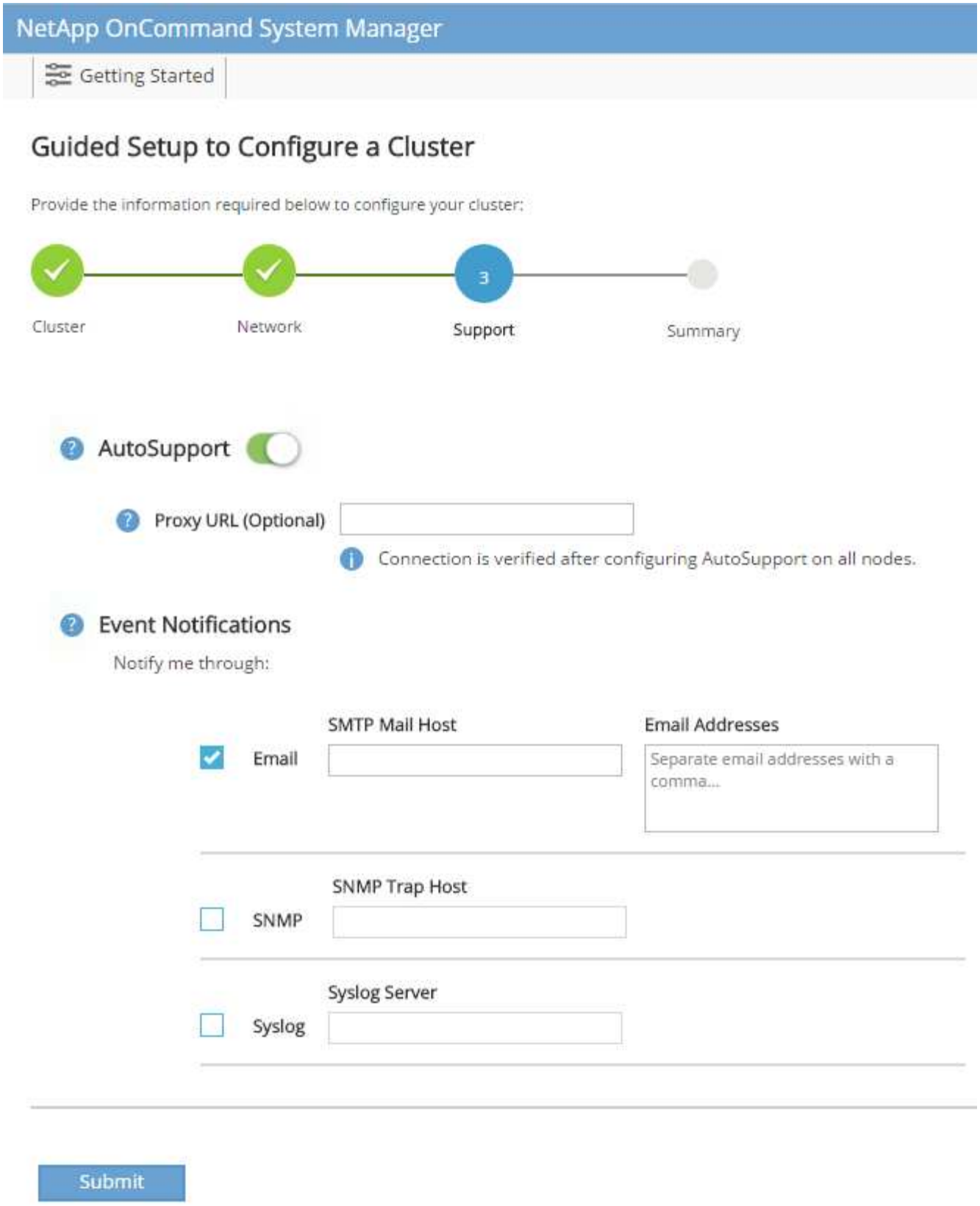
   È inoltre possibile inserire un server NTP alternativo.

8. Configurare le informazioni di supporto.

   a. Se l'ambiente richiede un proxy per accedere a AutoSupport, inserire l'URL nel campo URL proxy.

   b. Inserire l'host di posta SMTP e l'indirizzo di posta elettronica per le notifiche degli eventi.

      Prima di procedere, è necessario impostare almeno il metodo di notifica degli eventi. È possibile selezionare uno dei metodi.



9. Quando viene indicato che la configurazione del cluster è stata completata, fare clic su Manage Your Cluster (Gestisci cluster) per configurare lo storage.

Continuazione della configurazione del cluster di storage

Dopo la configurazione dei nodi di storage e del cluster di base, è possibile continuare con la configurazione del cluster di storage.

Azzerare tutti i dischi spare

Per azzerare tutti i dischi di riserva nel cluster, eseguire il seguente comando:

```
disk zerospares
```

Impostare la personalità delle porte UTA2 a bordo scheda

1. Verificare la modalità corrente e il tipo corrente di porte eseguendo `ucadmin show` comando.

```
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. Verificare che la modalità corrente delle porte in uso sia `cna` e che il tipo corrente sia impostato su `target`. In caso contrario, modificare il linguaggio della porta utilizzando il seguente comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

Per eseguire il comando precedente, le porte devono essere offline. Per disattivare una porta, eseguire il seguente comando:

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

> Se è stata modificata la personalità della porta, è necessario riavviare ciascun nodo per rendere effettiva la modifica.

Rinominare le interfacce logiche di gestione (LIF)

Per rinominare le LIF di gestione, attenersi alla seguente procedura:

1. Mostra i nomi LIF di gestione correnti.

```
network interface show –vserver <<clustername>>
```

2. Rinominare la LIF di gestione del cluster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Rinominare la LIF di gestione del nodo B.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

Impostare il revert automatico sulla gestione del cluster

Impostare `auto-revert` sull'interfaccia di gestione del cluster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configurare l'interfaccia di rete del Service Processor

Per assegnare un indirizzo IPv4 statico al processore di servizio su ciascun nodo, eseguire i seguenti comandi:

```
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>>
```

Gli indirizzi IP del processore di servizi devono trovarsi nella stessa sottorete degli indirizzi IP di gestione dei nodi.

Abilitare il failover dello storage in ONTAP

Per confermare che il failover dello storage è attivato, eseguire i seguenti comandi in una coppia di failover:

1. Verificare lo stato del failover dello storage.

```
storage failover show
```

Entrambi `<<var_nodeA>>` e. `<<var_nodeB>>` deve essere in grado di eseguire un takeover. Andare al passaggio 3 se i nodi possono eseguire un Takeover.

2. Attivare il failover su uno dei due nodi.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

L'attivazione del failover su un nodo lo abilita per entrambi i nodi.

3. Verificare lo stato ha del cluster a due nodi.

Questo passaggio non è applicabile ai cluster con più di due nodi.

```
cluster ha show
```

4. Andare al passaggio 6 se è configurata la disponibilità elevata. Se è configurata la disponibilità elevata, all'emissione del comando viene visualizzato il seguente messaggio:

```
High Availability Configured: true
```

5. Attivare la modalità ha solo per il cluster a due nodi.

> Non eseguire questo comando per i cluster con più di due nodi perché causa problemi di failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Verificare che l'assistenza hardware sia configurata correttamente e, se necessario, modificare l'indirizzo IP del partner.

```
storage failover hwassist show
```

Il messaggio `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica che l'assistenza hardware non è configurata. Eseguire i seguenti comandi per configurare l'assistenza hardware.

```
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>>
```

Creare un dominio di trasmissione MTU con frame jumbo in ONTAP

Per creare un dominio di trasmissione dati con un MTU di 9000, eseguire i seguenti comandi:

```
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
```

Rimuovere le porte dati dal dominio di trasmissione predefinito

Le porte dati 10GbE vengono utilizzate per il traffico iSCSI/NFS e devono essere rimosse dal dominio predefinito. Le porte e0e e e0f non vengono utilizzate e devono essere rimosse anche dal dominio predefinito.

Per rimuovere le porte dal dominio di trasmissione, eseguire il seguente comando:

```
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
```

Disattiva il controllo di flusso sulle porte UTA2

È una Best practice di NetApp disattivare il controllo di flusso su tutte le porte UTA2 collegate a dispositivi esterni. Per disattivare il controllo di flusso, eseguire il seguente comando:

```
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
```

Configurare IFGRP LACP in ONTAP

Questo tipo di gruppo di interfacce richiede due o più interfacce Ethernet e uno switch che supporti LACP. Assicurarsi che lo switch sia configurato correttamente.

Dal prompt del cluster, completare la seguente procedura.

```
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
```

Configurare i frame jumbo in NetApp ONTAP

Per configurare una porta di rete ONTAP per l'utilizzo di frame jumbo (che in genere hanno una MTU di 9,000 byte), eseguire i seguenti comandi dalla shell del cluster:

```
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
```

Creare VLAN in ONTAP

Per creare VLAN in ONTAP, attenersi alla seguente procedura:

1. Creare porte VLAN NFS e aggiungerle al dominio di trasmissione dati.

   ```
   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. Creare porte VLAN iSCSI e aggiungerle al dominio di trasmissione dati.

```
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. Creare porte MGMT-VLAN.

```
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>>
```

Creare aggregati in ONTAP

Durante il processo di installazione di ONTAP viene creato un aggregato contenente il volume root. Per creare aggregati aggiuntivi, determinare il nome dell'aggregato, il nodo su cui crearlo e il numero di dischi in esso contenuti.

Per creare aggregati, eseguire i seguenti comandi:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Conservare almeno un disco (selezionare il disco più grande) nella configurazione come spare. Una buona pratica consiste nell'avere almeno uno spare per ogni tipo e dimensione di disco.

Iniziare con cinque dischi; è possibile aggiungere dischi a un aggregato quando è richiesto storage aggiuntivo.

Impossibile creare l'aggregato fino al completamento dell'azzeramento del disco. Eseguire `aggr show` per visualizzare lo stato di creazione dell'aggregato. Non procedere fino a. `aggr1`_`nodeA` è online.

Configurare il fuso orario in ONTAP

Per configurare la sincronizzazione dell'ora e impostare il fuso orario sul cluster, eseguire il seguente comando:

```
timezone <<var_timezone>>
```

> Ad esempio, negli Stati Uniti orientali, il fuso orario è `America/New York`. Dopo aver digitato il nome del fuso orario, premere il tasto Tab per visualizzare le opzioni disponibili.

Configurare SNMP in ONTAP

Per configurare SNMP, attenersi alla seguente procedura:

1. Configurare le informazioni di base SNMP, ad esempio la posizione e il contatto. Quando viene eseguito il polling, queste informazioni vengono visualizzate come `sysLocation` e. `sysContact` Variabili in SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configurare i trap SNMP da inviare agli host remoti.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configurare SNMPv1 in ONTAP

Per configurare SNMPv1, impostare la password di testo normale segreta condivisa denominata community.

```
snmp community add ro <<var_snmp_community>>
```

> Utilizzare `snmp community delete all` comando con cautela. Se vengono utilizzate stringhe di comunità per altri prodotti di monitoraggio, questo comando le rimuove.

Configurare SNMPv3 in ONTAP

SNMPv3 richiede la definizione e la configurazione di un utente per l'autenticazione. Per configurare SNMPv3, attenersi alla seguente procedura:

1. Eseguire `security snmpusers` Per visualizzare l'ID del motore.
2. Creare un utente chiamato `snmpv3user`.

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Inserire l'ID del motore dell'entità autorevole e selezionare `md5` come protocollo di autenticazione.
4. Quando richiesto, immettere una password di lunghezza minima di otto caratteri per il protocollo di autenticazione.
5. Selezionare `des` come protocollo per la privacy.
6. Quando richiesto, immettere una password di lunghezza minima di otto caratteri per il protocollo di privacy.

Configurare HTTPS AutoSupport in ONTAP

Il tool NetApp AutoSupport invia a NetApp informazioni riepilogative sul supporto tramite HTTPS. Per configurare AutoSupport, eseguire il seguente comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Creare una macchina virtuale per lo storage

Per creare una SVM (Infrastructure Storage Virtual Machine), attenersi alla seguente procedura:

1. Eseguire `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Aggiungere l'aggregato di dati all'elenco di aggregati infra-SVM per NetApp VSC.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Rimuovere i protocolli di storage inutilizzati da SVM, lasciando NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Abilitare ed eseguire il protocollo NFS nella SVM infra-SVM.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. Accendere il `SVM vstorage` Parametro per il plug-in NetApp NFS VAAI. Quindi, verificare che NFS sia stato configurato.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

> I comandi sono preceduti da `vserver` nella riga di comando, perché le macchine virtuali dello storage erano precedentemente chiamate server.

Configurare NFSv3 in ONTAP

La seguente tabella elenca le informazioni necessarie per completare questa configurazione.

Dettaglio	Valore di dettaglio
ESXi ospita Un indirizzo IP NFS	[var_esxi_hostA_nfs_ip]
ESXi host B NFS IP address (Indirizzo IP NFS host B ESXi)	[var_esxi_hostB_nfs_ip]

Per configurare NFS su SVM, eseguire i seguenti comandi:

1. Creare una regola per ciascun host ESXi nel criterio di esportazione predefinito.
2. Per ogni host ESXi creato, assegnare una regola. Ogni host dispone di un proprio indice delle regole. Il primo host ESXi dispone dell'indice delle regole 1, il secondo host ESXi dell'indice delle regole 2 e così via.

```
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. Assegnare il criterio di esportazione al volume root SVM dell'infrastruttura.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

> NetApp VSC gestisce automaticamente le policy di esportazione se si sceglie di installarle dopo la configurazione di vSphere. Se non viene installato, è necessario creare regole dei criteri di esportazione quando vengono aggiunti altri server Cisco UCS C-Series.

Creare un servizio iSCSI in ONTAP

Per creare il servizio iSCSI, completare la seguente fase:

1. Creare il servizio iSCSI sulla SVM. Questo comando avvia anche il servizio iSCSI e imposta l'IQN iSCSI per SVM. Verificare che iSCSI sia stato configurato.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Creare un mirror di condivisione del carico del volume root SVM in ONTAP

1. Creare un volume come mirror di condivisione del carico del volume root SVM dell'infrastruttura su ciascun nodo.

```
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. Creare una pianificazione del processo per aggiornare le relazioni del mirror del volume root ogni 15 minuti.

```
job schedule interval create -name 15min -minutes 15
```

3. Creare le relazioni di mirroring.

```
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. Inizializzare la relazione di mirroring e verificare che sia stata creata.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configurare l'accesso HTTPS in ONTAP

Per configurare l'accesso sicuro al controller di storage, attenersi alla seguente procedura:

1. Aumentare il livello di privilegio per accedere ai comandi del certificato.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. In genere, è già in uso un certificato autofirmato. Verificare il certificato eseguendo il seguente comando:

```
security certificate show
```

3. Per ogni SVM mostrato, il nome comune del certificato deve corrispondere al nome FQDN DNS dell'SVM. I quattro certificati predefiniti devono essere cancellati e sostituiti da certificati autofirmati o certificati di un'autorità di certificazione.

   È consigliabile eliminare i certificati scaduti prima di creare i certificati. Eseguire `security certificate delete` comando per eliminare i certificati scaduti. Nel seguente comando, utilizzare LA SCHEDA completamento per selezionare ed eliminare ogni certificato predefinito.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Per generare e installare certificati autofirmati, eseguire i seguenti comandi come comandi una tantum. Generare un certificato server per infra-SVM e SVM del cluster. Di nuovo, utilizzare IL COMPLETAMENTO DELLA SCHEDA per facilitare il completamento di questi comandi.

```
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. Per ottenere i valori dei parametri richiesti nella fase successiva, eseguire `security certificate show` comando.
6. Attivare ciascun certificato appena creato utilizzando `-server-enabled true` e. `-client-enabled false` parametri. Di nuovo, utilizzare IL COMPLETAMENTO DELLA SCHEDA.

```
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. Configurare e abilitare l'accesso SSL e HTTPS e disattivare l'accesso HTTP.

```
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>>
```

Alcuni di questi comandi restituiscono normalmente un messaggio di errore che indica che la voce non esiste.

8. Ripristinare il livello di privilegio admin e creare la configurazione per consentire a SVM di essere disponibile sul web.

```
set -privilege admin
vserver services web modify -name spi|ontapi|compat -vserver * -enabled
true
```

Creare un volume NetApp FlexVol in ONTAP

Per creare un volume NetApp FlexVol, immettere il nome del volume, le dimensioni e l'aggregato in cui si trova. Creare due volumi di datastore VMware e un volume di boot del server.

```
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
```

Attiva la deduplica in ONTAP

Per attivare la deduplica sui volumi appropriati, eseguire i seguenti comandi:

```
volume efficiency on -vserver Infra-SVM -volume infra_datastore_1
volume efficiency on -vserver Infra-SVM -volume esxi_boot
```

Creare LUN in ONTAP

Per creare due LUN di avvio, eseguire i seguenti comandi:

```
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
```

Quando si aggiunge un server Cisco UCS C-Series aggiuntivo, è necessario creare un LUN di avvio aggiuntivo.

Creazione di LIF iSCSI in ONTAP

La seguente tabella elenca le informazioni necessarie per completare questa configurazione.

Dettaglio	Valore di dettaglio
Nodo di storage A iSCSI LIF01A	[var_nodeA_iscsi_lif01a_ip]
Nodo di storage A iSCSI LF01A network mask	[var_nodeA_iscsi_lif01a_mask]
Nodo di storage A iSCSI LF01B	[var_nodeA_iscsi_lif01b_ip]
Nodo di storage A iSCSI LF01B network mask	[var_nodeA_iscsi_lif01b_mask]
Nodo di storage B iSCSI LF01A	[var_nodeB_iscsi_lif01a_ip]
Nodo di storage B iSCSI LF01A Network mask	[var_nodeB_iscsi_lif01a_mask]
Nodo di storage B iSCSI LF01B	[var_nodeB_iscsi_lif01b_ip]
Nodo di storage B iSCSI LF01B Network mask	[var_nodeB_iscsi_lif01b_mask]

1. Creare quattro LIF iSCSI, due su ciascun nodo.

```
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
```

Creare LIF NFS in ONTAP

La seguente tabella elenca le informazioni necessarie per completare questa configurazione.

Dettaglio	Valore di dettaglio
Nodo di storage A NFS LIF 01 IP	[var_nodeA_nfs_lif_01_ip]
Nodo di storage: Una maschera di rete NFS LIF 01	[var_nodeA_nfs_lif_01_mask]
Nodo di storage B NFS LIF 02 IP	[var_nodeB_nfs_lif_02_ip]
Network mask NFS LIF 02 del nodo di storage B.	[var_nodeB_nfs_lif_02_mask]

1. Creare una LIF NFS.

```
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
```

Aggiungere l'amministratore SVM dell'infrastruttura

La seguente tabella elenca le informazioni necessarie per completare questa configurazione.

Dettaglio	Valore di dettaglio
IP Vsmgmt	[var_svm_mgmt_ip]
Maschera di rete Vsmgmt	[var_svm_mgmt_mask]
Gateway predefinito Vsmgmt	[var_svm_mgmt_gateway]

Per aggiungere l'amministratore SVM dell'infrastruttura e l'interfaccia logica di amministrazione SVM alla rete di gestione, attenersi alla seguente procedura:

1. Eseguire il seguente comando:

```
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
```

> L'IP di gestione SVM deve trovarsi nella stessa sottorete dell'IP di gestione del cluster di storage.

2. Creare un percorso predefinito per consentire all'interfaccia di gestione SVM di raggiungere il mondo esterno.

```
network route create -vserver Infra-SVM -destination 0.0.0.0/0 -gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Impostare una password per l'utente vsadmin di SVM e sbloccare l'utente.

```
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
```

"Avanti: Procedura di implementazione del server rack Cisco UCS C-Series"

Procedura di implementazione dei server rack Cisco UCS C-Series

La sezione seguente fornisce una procedura dettagliata per la configurazione di un server rack standalone Cisco UCS C-Series da utilizzare nella configurazione FlexPod Express.

Eseguire la configurazione iniziale del server standalone Cisco UCS C-Series per Cisco Integrated Management Server

Completare questa procedura per la configurazione iniziale dell'interfaccia CIMC per i server standalone Cisco UCS C-Series.

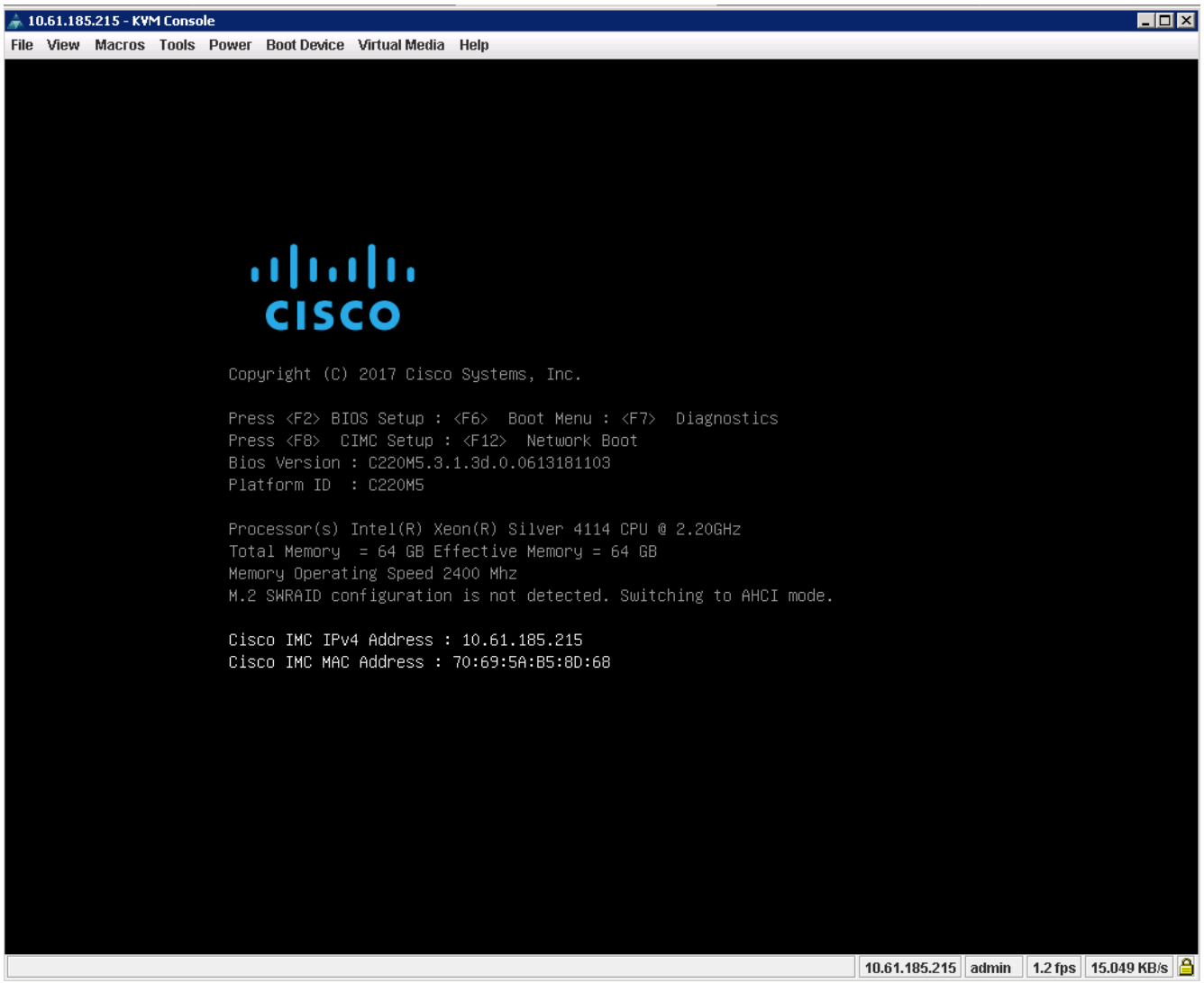
La seguente tabella elenca le informazioni necessarie per configurare CIMC per ogni server standalone Cisco UCS C-Series.

Dettaglio	Valore di dettaglio
Indirizzo IP CIMC	[cimc_ip]
Subnet mask CIMC	[cimc_netmask]
Gateway predefinito CIMC	[cimc_gateway]

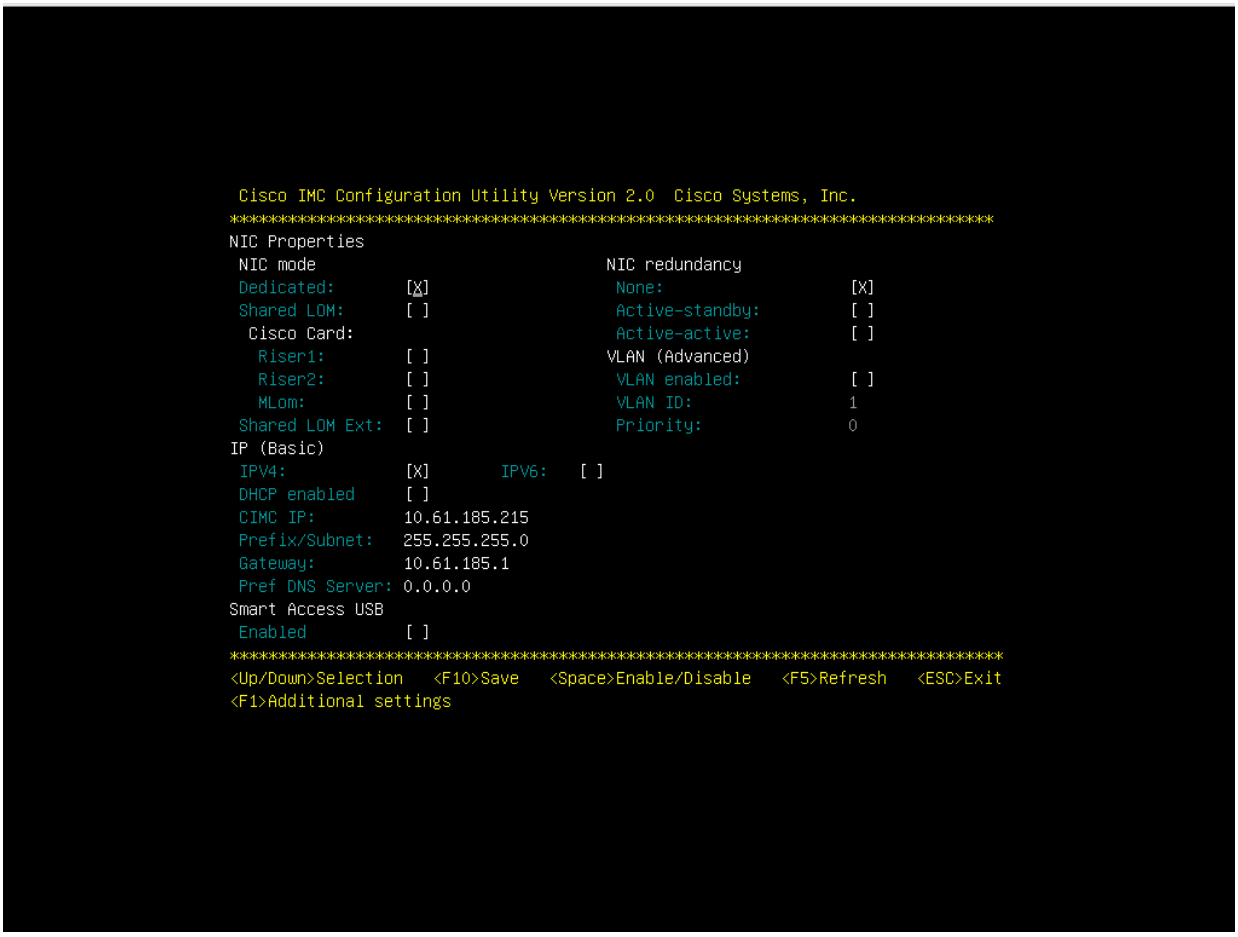
La versione di CIMC utilizzata per questa convalida è CIMC 3.1.3(g).

Tutti i server

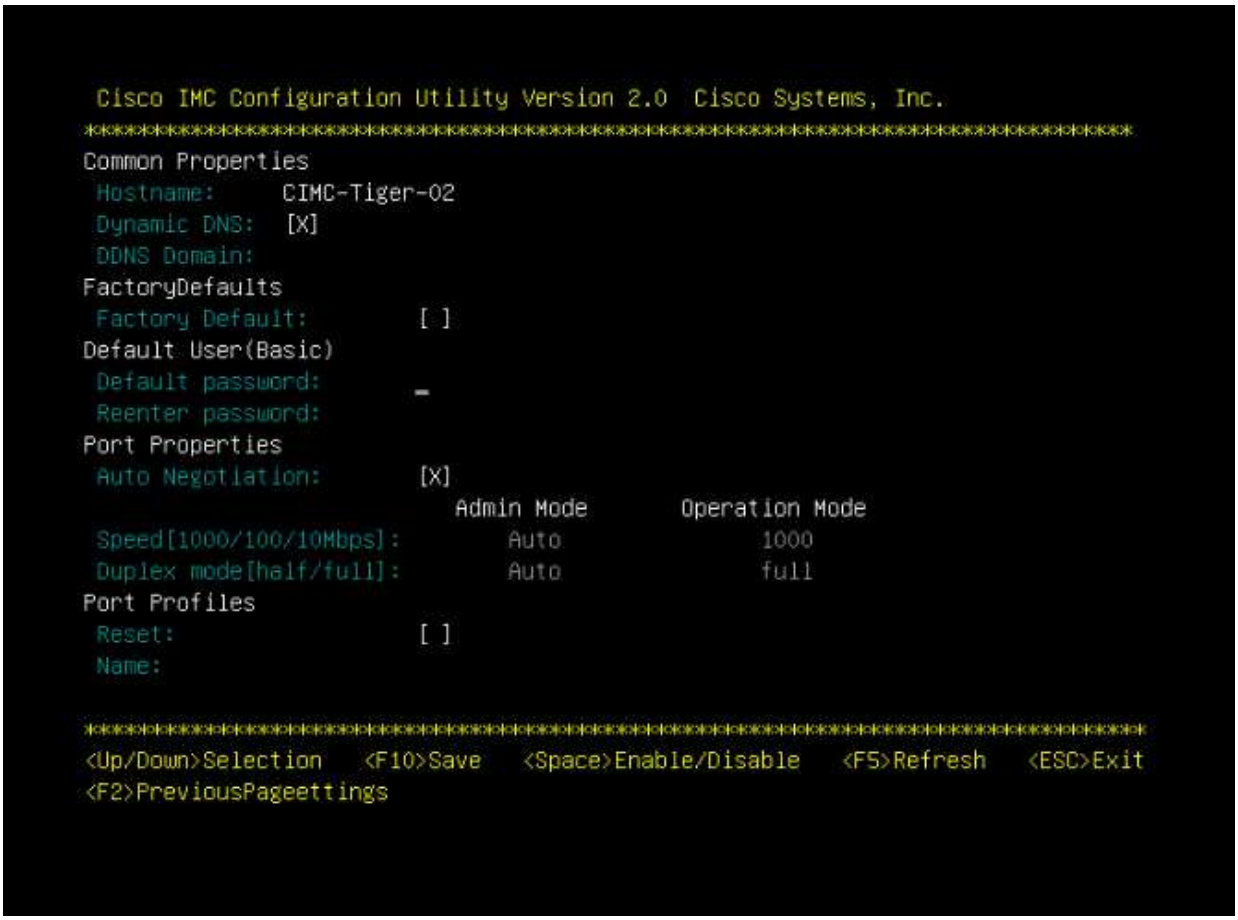
1. Collegare il dongle KVM (tastiera, video e mouse) Cisco (fornito con il server) alla porta KVM sulla parte anteriore del server. Collegare un monitor VGA e una tastiera USB alle porte dongle KVM appropriate.
2. Accendere il server e premere F8 quando richiesto per accedere alla configurazione CIMC.



3. Nell'utility di configurazione di CIMC, impostare le seguenti opzioni:
   - Modalità scheda di interfaccia di rete (NIC):
     - Dedicato [X]
   - IP (di base):
     - IPV4: [X]
     - DHCP abilitato: [ ]
     - IP CIMC:[cimc_ip]
     - Prefisso/sottorete:[cimc_netmask]
     - Gateway:[cimc_gateway]
   - VLAN (Advanced): Lasciare deselezionato per disattivare il tagging VLAN.
     - Ridondanza della NIC
     - Nessuno: [X]



4. Premere F1 per visualizzare ulteriori impostazioni.
   - Proprietà comuni:
     - Nome host:[esxi_host_name]
     - DNS dinamico: [ ]
     - Impostazioni predefinite: Lasciare deselezionato.
   - Utente predefinito (di base):
     - Password predefinita:[admin_password]
     - Immettere nuovamente la password:[admin_password]
     - Port properties (Proprietà porta): Utilizzare i valori predefiniti.
     - Port profiles (profili porta): Lasciare deselezionato.



5. Premere F10 per salvare la configurazione dell'interfaccia CIMC.
6. Una volta salvata la configurazione, premere Esc per uscire.

Configurare l'avvio iSCSI dei server Cisco UCS C-Series

In questa configurazione FlexPod Express, VIC1387 viene utilizzato per l'avvio iSCSI.

La seguente tabella elenca le informazioni necessarie per configurare l'avvio iSCSI.

> Il carattere corsivo indica le variabili univoche per ciascun host ESXi.

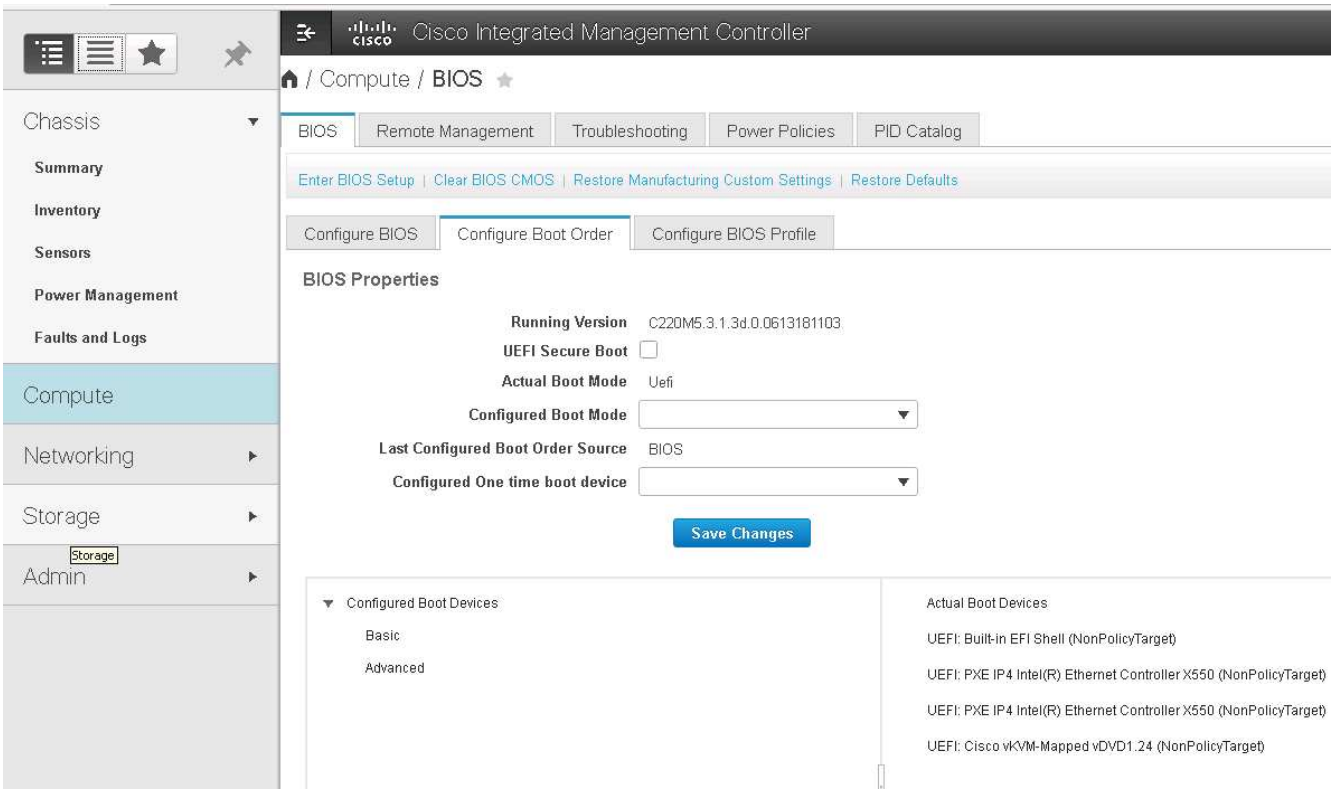
Dettaglio	Valore di dettaglio
Nome dell'iniziatore host ESXi	[var_ucs_initiator_name_A]
IP iSCSI-A host ESXi	[var_esxi_host_iscsiA_ip]
Host ESXi iSCSI-A network mask	[var_esxi_host_iscsiA_mask]
ESXi host iSCSI Un gateway predefinito	[var_esxi_host_iscsiA_gateway]
Nome B dell'iniziatore host ESXi	[var_ucs_initiator_name_B]
IP iSCSI-B host ESXi	[var_esxi_host_iscsiB_ip]
Maschera di rete iSCSI-B host ESXi	[var_esxi_host_iscsiB_mask]
Gateway iSCSI-B host ESXi	[var_esxi_host_iscsiB_gateway]

Dettaglio	Valore di dettaglio
Indirizzo IP iscsi_lif01a	
Indirizzo IP iscsi_lif02a	
Indirizzo IP iscsi_lif01b	
Indirizzo IP iscsi_lif02b	
Infra_SVM IQN	

Configurazione dell'ordine di avvio

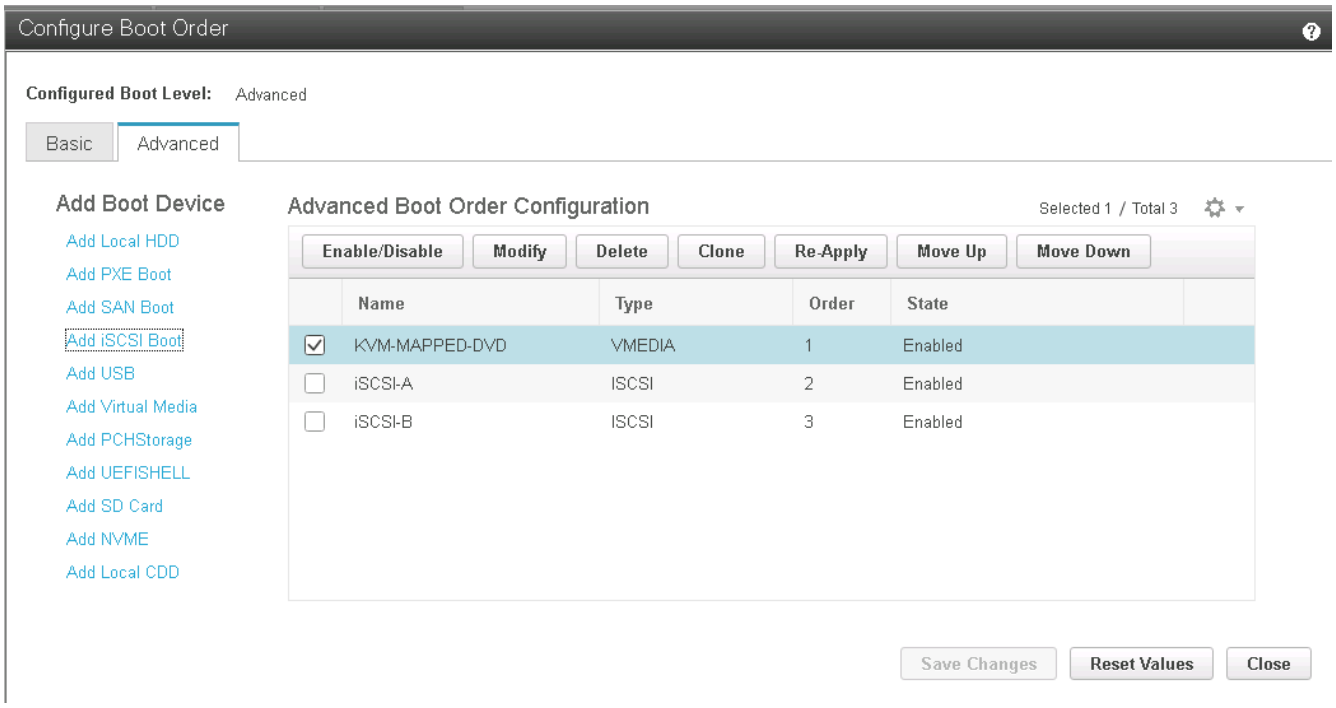
Per impostare la configurazione dell'ordine di avvio, attenersi alla seguente procedura:

1. Dalla finestra del browser dell'interfaccia CIMC, fare clic sulla scheda Server e selezionare BIOS.
2. Fare clic su Configure Boot Order (Configura ordine di avvio), quindi su OK.



3. Configurare i seguenti dispositivi facendo clic su dispositivo in Add Boot Device (Aggiungi dispositivo di avvio) e selezionando la scheda Advanced (Avanzate).
   - Aggiungere supporti virtuali
     - NOME: KVM-CD-DVD
     - SOTTOTIPO: DVD MAPPATO KVM
     - Stato: Attivato
     - Ordine: 1
   - Aggiungere l'avvio iSCSI.
     - Nome: ISCSI-A.

    - Stato: Attivato
    - Ordine: 2
    - Slot: MLOM
    - Porta: 0
  - Fare clic su Add iSCSI Boot.
    - Nome: ISCSI-B.
    - Stato: Attivato
    - Ordine: 3
    - Slot: MLOM
    - Porta: 1
4. Fare clic su Aggiungi dispositivo.
5. Fare clic su Save Changes (Salva modifiche), quindi su Close (Chiudi)

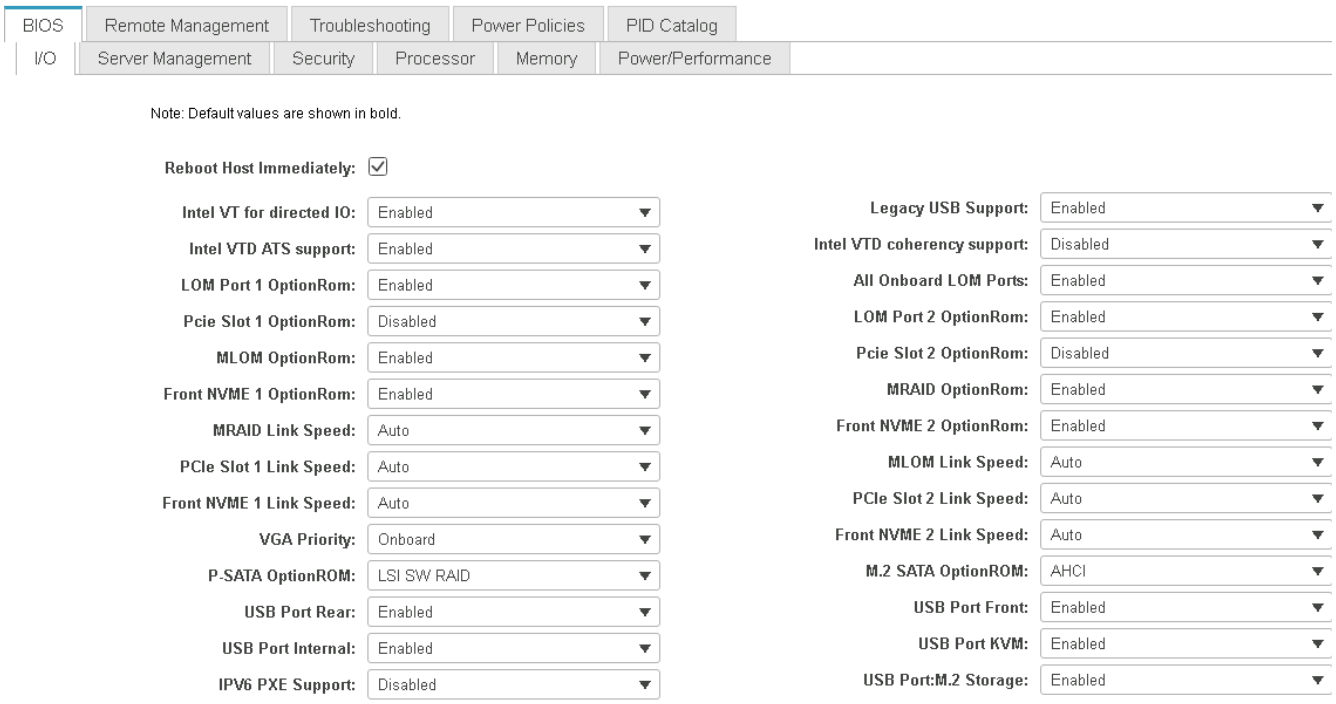


6. Riavviare il server per eseguire l'avvio con il nuovo ordine di avvio.

Disattivazione del controller RAID (se presente)

Se il server C-Series contiene un controller RAID, attenersi alla seguente procedura. Non è necessario un controller RAID per l'avvio dalla configurazione SAN. In alternativa, è anche possibile rimuovere fisicamente il controller RAID dal server.

1. Fare clic su BIOS nel riquadro di navigazione sinistro di CIMC.
2. Selezionare Configure BIOS (Configura BIOS).
3. Scorrere verso il basso fino a PCIe slot:HBA Option ROM.
4. Se il valore non è già disattivato, impostarlo su Disabled (Disattivato).



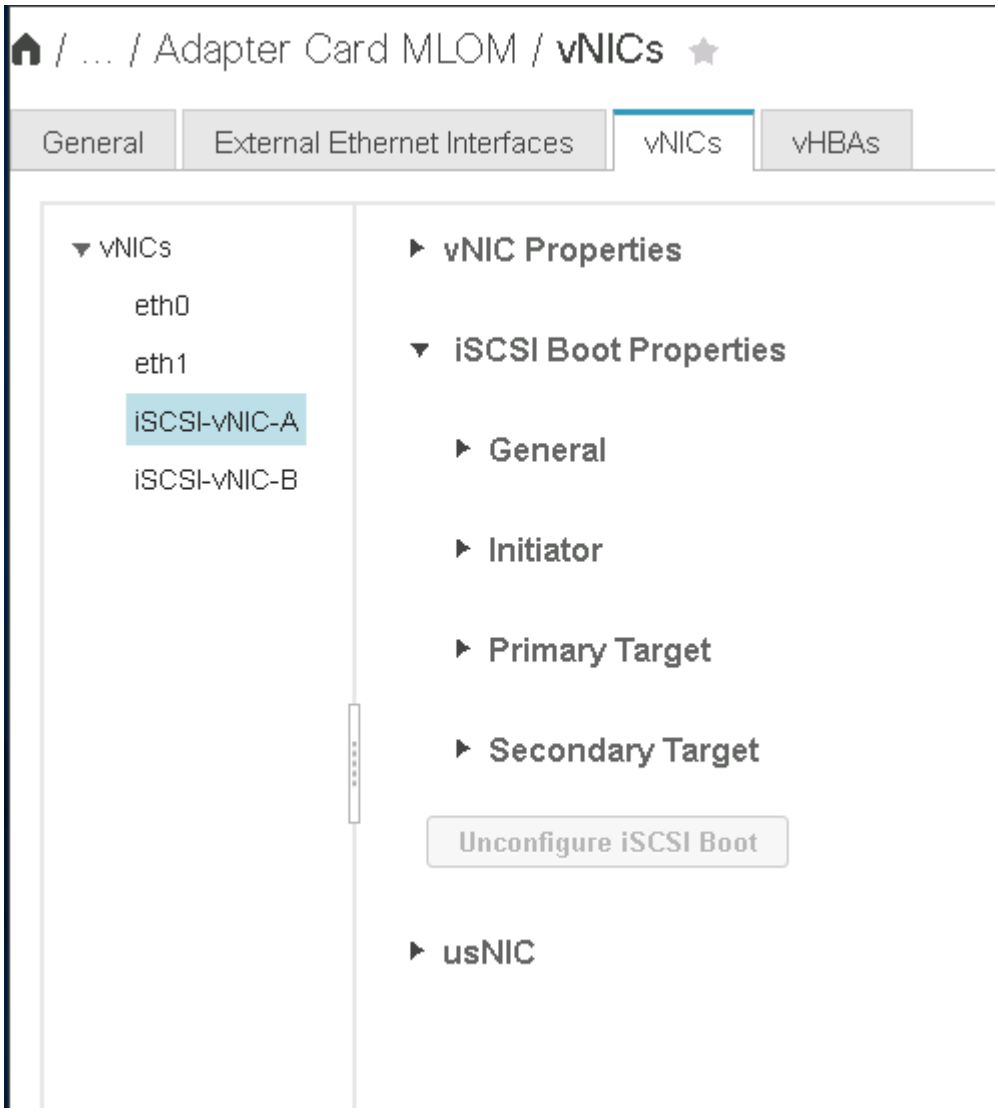
Configurare Cisco VIC1387 per l'avvio iSCSI

La seguente procedura di configurazione riguarda Cisco VIC 1387 per l'avvio iSCSI.

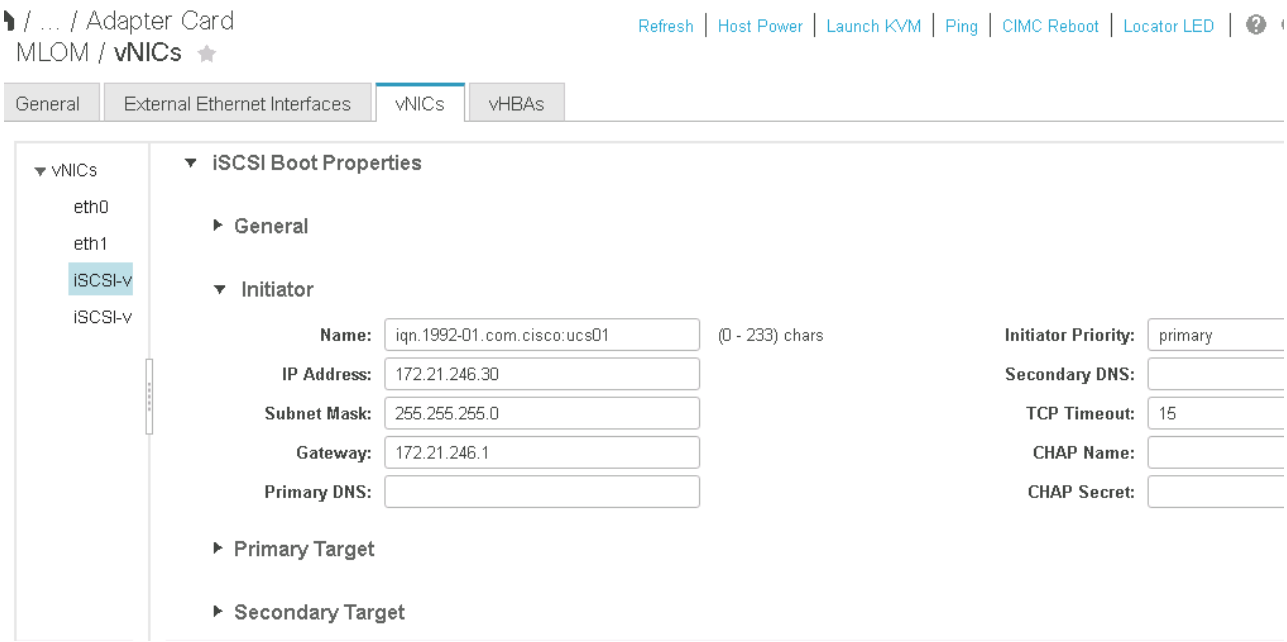
Creare vNIC iSCSI

1. Fare clic su Add (Aggiungi) per creare una vNIC.
2. Nella sezione Add vNIC (Aggiungi vNIC), immettere le seguenti impostazioni:
   - Nome: ISCSI-vNIC-A.
   - MTU: 9000
   - VLAN predefinita: `<<var_iscsi_vlan_a>>`
   - Modalità VLAN: TRUNK
   - Enable PXE boot (attiva avvio PXE): Controllare

3. Fare clic su Add vNIC (Aggiungi vNIC), quindi su OK.
4. Ripetere la procedura per aggiungere una seconda vNIC.
   a. Assegnare un nome alla vNIC `iSCSI-vNIC-B`.
   b. Invio `<<var_iscsi_vlan_b>>` Come VLAN.
   c. Impostare la porta uplink su `1`.
5. Selezionare la vNIC `iSCSI-vNIC-A` sulla sinistra.



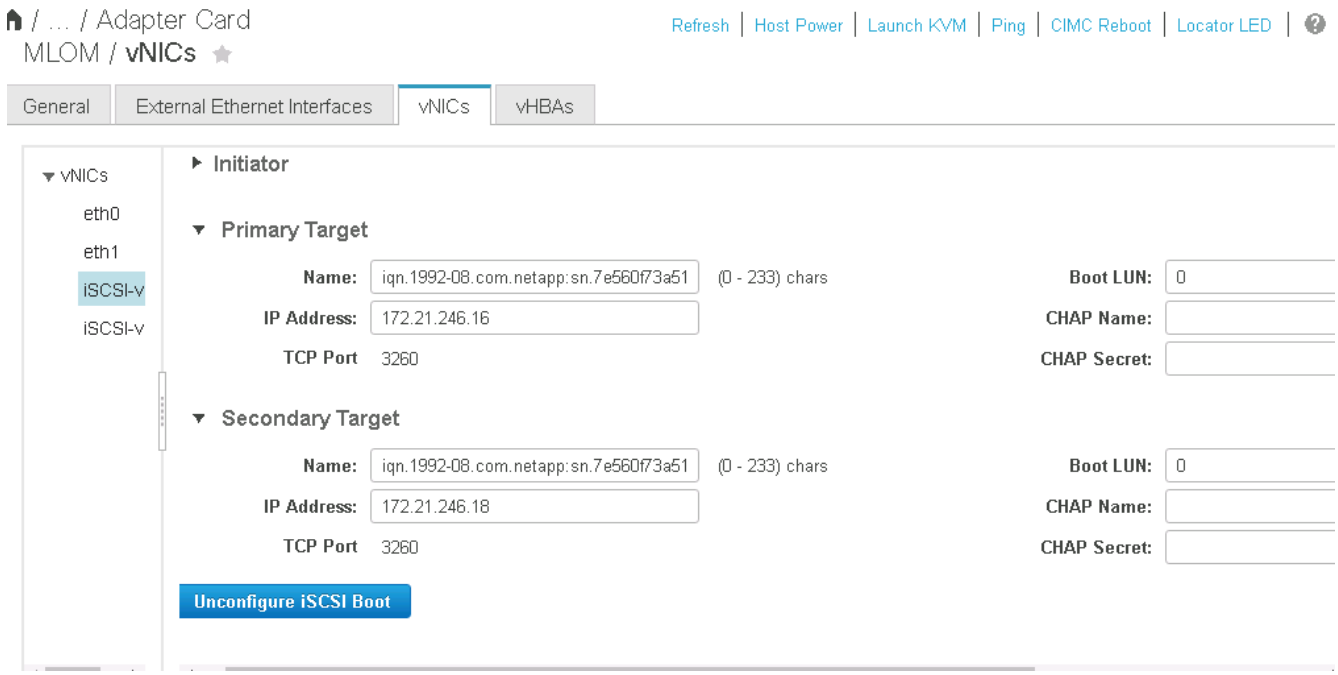
6. In iSCSI Boot Properties (Proprietà di avvio iSCSI), immettere i dettagli dell'iniziatore:
   - Nome:[var_ucsa_initiator_name_a]
   - Indirizzo IP:[var_esxi_hostA_iscsiA_ip]
   - Subnet mask:[var_esxi_hostA_iscsiA_mask]
   - Gateway:[var_esxi_hostA_iscsiA_gateway]



7. Inserire i dettagli principali del target.
   - Name (Nome): Numero IQN di infra-SVM
   - IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif01a`
   - LUN di boot: 0
8. Inserire i dettagli della destinazione secondaria.
   - Name (Nome): Numero IQN di infra-SVM
   - IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif02a`
   - LUN di boot: 0

   È possibile ottenere il numero IQN dello storage eseguendo `vserver iscsi show` comando.

   > Assicurarsi di registrare i nomi IQN per ogni vNIC. Sono necessari per un passaggio successivo.



9. Fare clic su Configura iSCSI.
10. Selezionare la vNIC `iSCSI-vNIC- B` E fare clic sul pulsante iSCSI Boot (Avvio iSCSI) situato nella parte superiore della sezione host Ethernet Interfaces (interfacce Ethernet host).
11. Ripetere la procedura da configurare `iSCSI-vNIC-B`.
12. Inserire i dettagli dell'iniziatore.
    - Nome: `<<var_ucsa_initiator_name_b>>`
    - Indirizzo IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Subnet mask: `<<var_esxi_hostb_iscsib_mask>>`
    - Gateway: `<<var_esxi_hostb_iscsib_gateway>>`
13. Inserire i dettagli principali del target.
    - Name (Nome): Numero IQN di infra-SVM
    - IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif01b`
    - LUN di boot: 0
14. Inserire i dettagli della destinazione secondaria.
    - Name (Nome): Numero IQN di infra-SVM
    - IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif02b`
    - LUN di boot: 0

    È possibile ottenere il numero IQN dello storage utilizzando `vserver iscsi show` comando.

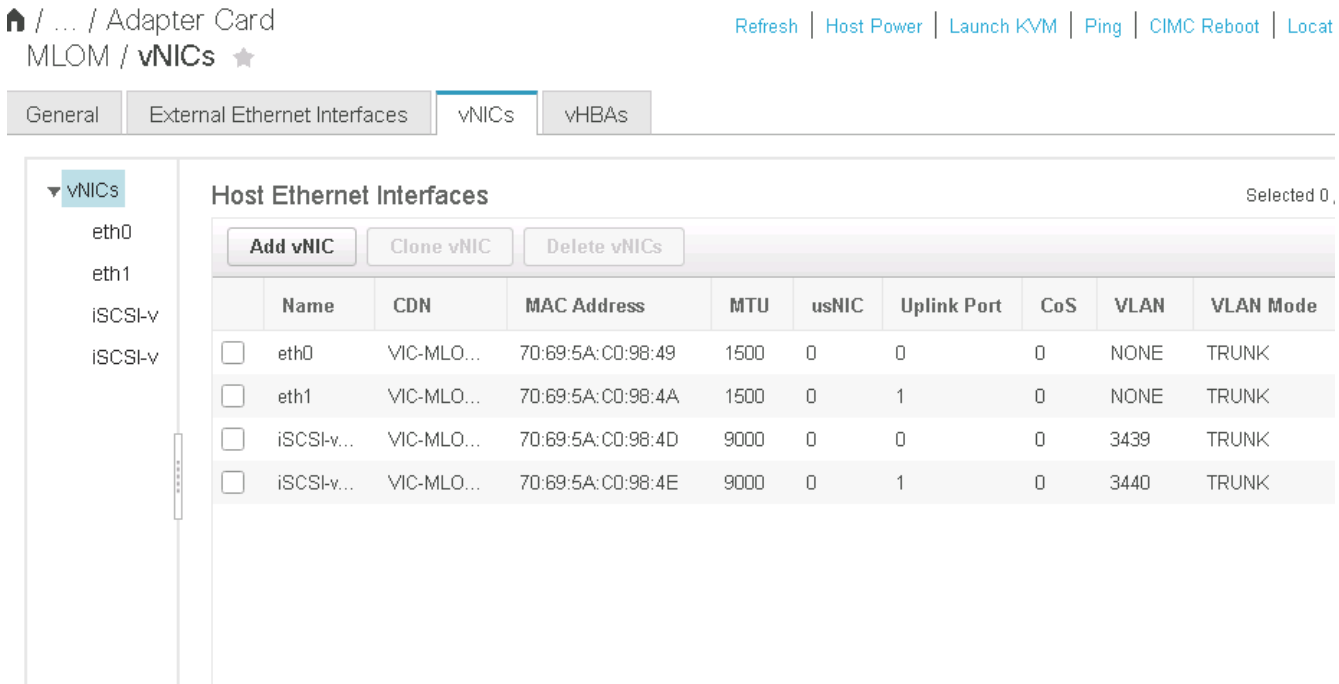
    > Assicurarsi di registrare i nomi IQN per ogni vNIC. Sono necessari per un passaggio successivo.

15. Fare clic su Configura ISCSI.

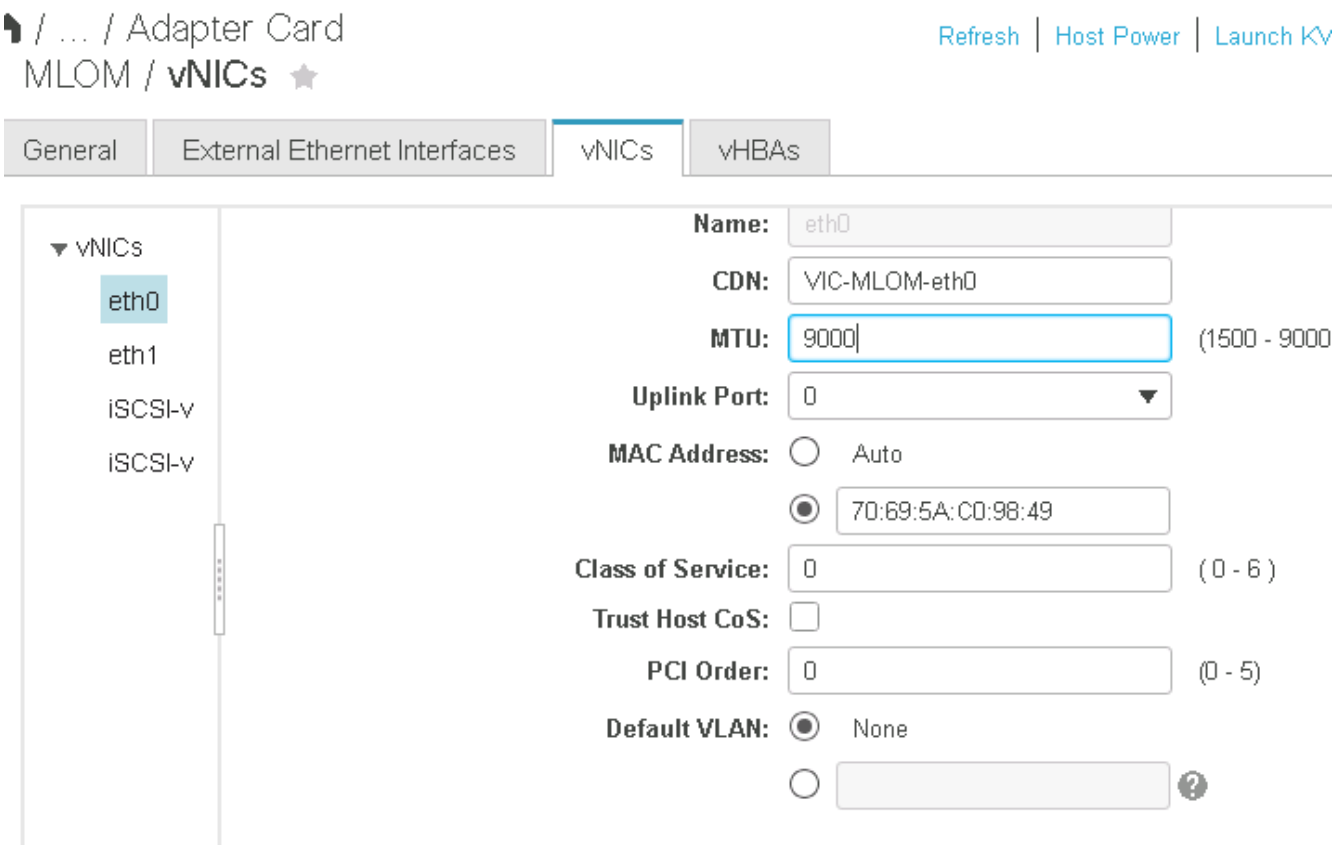
16. Ripetere questa procedura per configurare l'avvio iSCSI per il server Cisco UCS B.

Configurare vNIC per ESXi

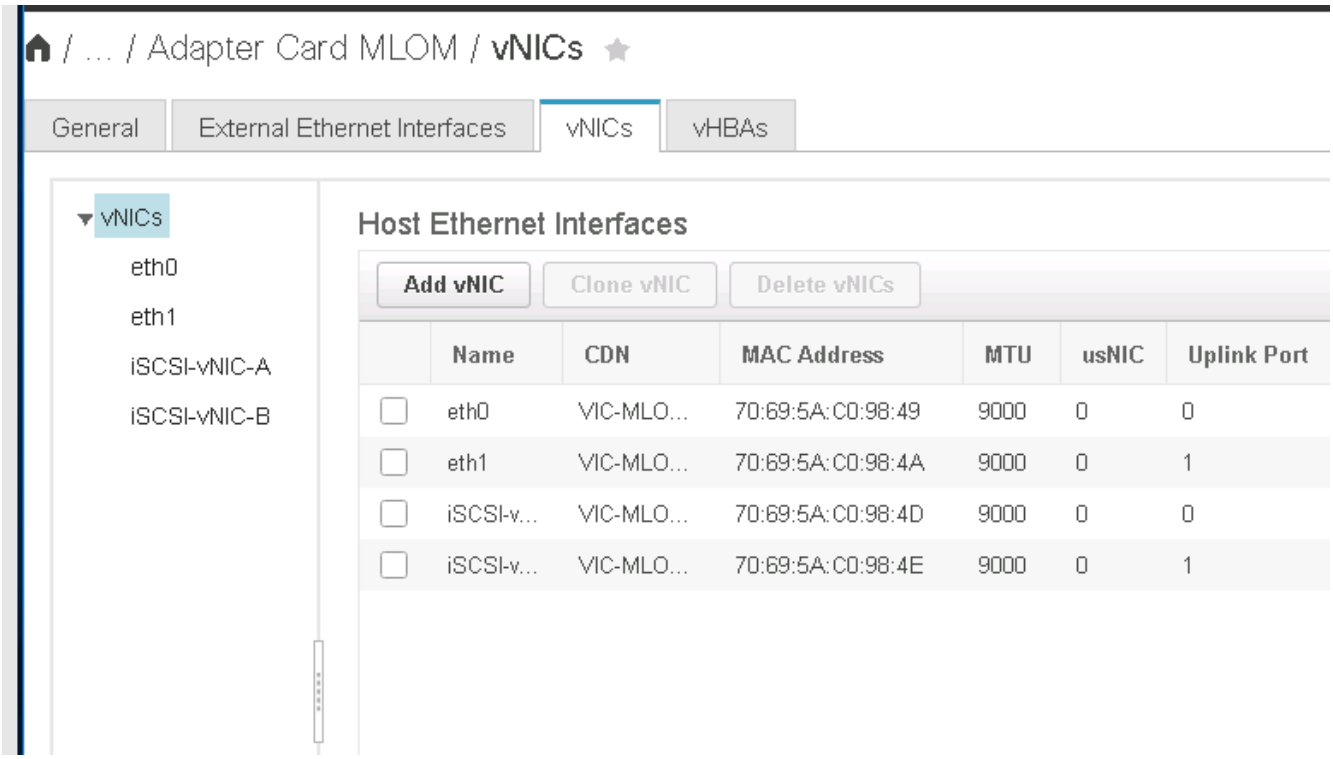
1. Dalla finestra del browser dell'interfaccia CIMC, fare clic su Inventory (inventario), quindi su Cisco VIC adapter (adattatori VIC Cisco) nel riquadro destro.
2. In schede adattatore, selezionare Cisco UCS VIC 1387, quindi selezionare le vNIC sottostanti.



3. Selezionare eth0 e fare clic su Proprietà.
4. Impostare MTU su 9000. Fare clic su Salva modifiche.



5. Ripetere i passaggi 3 e 4 per eth1, verificando che la porta uplink sia impostata su `1` per eth1.



Questa procedura deve essere ripetuta per ogni nodo iniziale di Cisco UCS Server e per ogni nodo aggiuntivo di Cisco UCS Server aggiunto all'ambiente.

"Pagina successiva: Procedura di implementazione dello storage NetApp AFF (parte 2)"

Procedura di implementazione dello storage NetApp AFF (parte 2)

Configurazione dello storage di boot SAN ONTAP

Creare igroups iSCSI

Per creare igroups, completare il seguente passaggio:

Per questa fase, sono necessari gli IQN iSCSI Initiator della configurazione del server.

1. Dalla connessione SSH del nodo di gestione del cluster, eseguire i seguenti comandi. Per visualizzare i tre igroups creati in questa fase, eseguire il comando igroup show.

```
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>>
```

> Questa fase deve essere completata quando si aggiungono altri server Cisco UCS C-Series.

Mappare le LUN di avvio a igroups

Per mappare le LUN di avvio a igroups, eseguire i seguenti comandi dalla connessione SSH di gestione del cluster:

```
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
```

> Questa fase deve essere completata quando si aggiungono altri server Cisco UCS C-Series.

"Procedura di implementazione di VMware vSphere 6.7."

Procedura di implementazione di VMware vSphere 6.7

Questa sezione fornisce procedure dettagliate per l'installazione di VMware ESXi 6.7 in una configurazione FlexPod Express. Le procedure di implementazione che seguono sono personalizzate per includere le variabili di ambiente descritte nelle sezioni

precedenti.

Esistono diversi metodi per l'installazione di VMware ESXi in un ambiente di questo tipo. Questa procedura utilizza la console KVM virtuale e le funzioni dei supporti virtuali dell'interfaccia CIMC per i server Cisco UCS C-Series per mappare i supporti di installazione remota su ciascun server.

> Questa procedura deve essere completata per il server Cisco UCS A e il server Cisco UCS B.

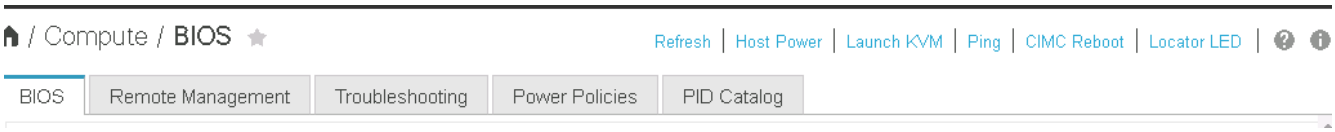
Questa procedura deve essere completata per tutti i nodi aggiuntivi aggiunti al cluster.

Accedere all'interfaccia CIMC per i server standalone Cisco UCS C-Series

La procedura riportata di seguito illustra in dettaglio il metodo di accesso all'interfaccia CIMC per i server standalone Cisco UCS C-Series. È necessario accedere all'interfaccia CIMC per eseguire il KVM virtuale, che consente all'amministratore di avviare l'installazione del sistema operativo tramite supporti remoti.

Tutti gli host

1. Accedere a un browser Web e immettere l'indirizzo IP dell'interfaccia CIMC per Cisco UCS C-Series. Questa fase avvia l'applicazione GUI CIMC.
2. Accedere all'interfaccia utente CIMC utilizzando il nome utente e le credenziali admin.
3. Nel menu principale, selezionare la scheda Server.
4. Fare clic su Avvia console KVM.



5. Dalla console KVM virtuale, selezionare la scheda Virtual Media (supporti virtuali).
6. Selezionare Map CD/DVD (Mappa CD/DVD).

> Potrebbe essere necessario fare clic su Activate Virtual Devices (attiva dispositivi virtuali). Selezionare Accetta questa sessione, se richiesto.

7. Accedere al file di immagine ISO del programma di installazione di VMware ESXi 6.7 e fare clic su Apri. Fare clic su Map Device (Connetti dispositivo)
8. Selezionare il menu Power (alimentazione) e scegliere Power Cycle System (Avvio a freddo). Fare clic su Sì.

Installare VMware ESXi

La seguente procedura descrive come installare VMware ESXi su ciascun host.

Scarica L'immagine personalizzata di ESXI 6.7 Cisco

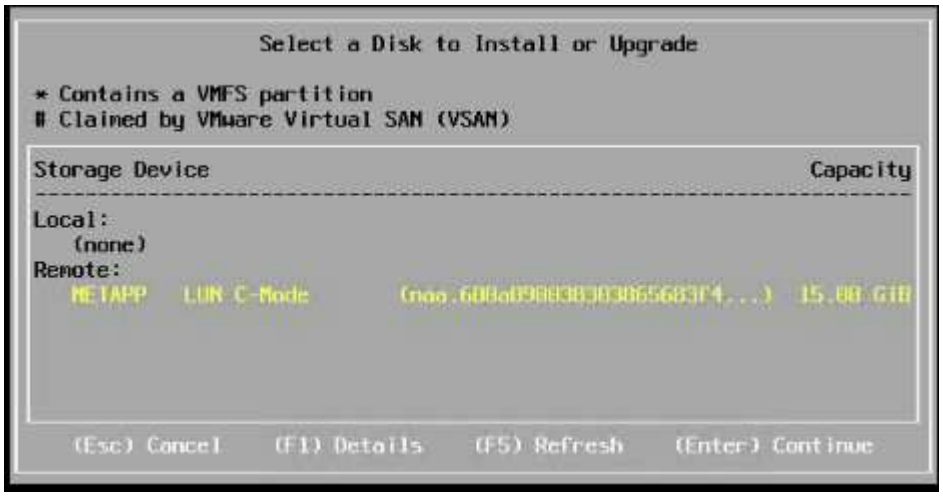
1. Passare a. "Pagina di download di VMware vSphere" Per ISO personalizzati.
2. Fare clic su Vai a Download accanto al CD di installazione Cisco Custom Image for ESXi 6.7 GA.
3. Scaricare il CD di installazione Cisco Custom Image per ESXi 6.7 GA (ISO).

Tutti gli host

1. All'avvio del sistema, il computer rileva la presenza del supporto di installazione di VMware ESXi.
2. Selezionare il programma di installazione di VMware ESXi dal menu visualizzato.

   Il programma di installazione viene caricato. Questa operazione richiede alcuni minuti.

3. Una volta completato il caricamento del programma di installazione, premere Invio per continuare l'installazione.
4. Dopo aver letto il contratto di licenza con l'utente finale, accettarlo e continuare con l'installazione premendo F11.
5. Selezionare il LUN NetApp precedentemente configurato come disco di installazione per ESXi e premere Invio per continuare l'installazione.



6. Selezionare il layout di tastiera appropriato e premere Invio.
7. Inserire e confermare la password root e premere Invio.
8. Il programma di installazione avvisa che le partizioni esistenti vengono rimosse nel volume. Continuare con l'installazione premendo F11. Il server si riavvia dopo l'installazione di ESXi.

Configurare il networking per la gestione degli host VMware ESXi

La seguente procedura descrive come aggiungere la rete di gestione per ciascun host VMware ESXi.

Tutti gli host

1. Una volta riavviato il server, immettere l'opzione per personalizzare il sistema premendo F2.
2. Effettuare l'accesso con root come nome di accesso e password root precedentemente inserita durante il processo di installazione.
3. Selezionare l'opzione Configure Management Network (Configura rete di gestione).
4. Selezionare Network Adapter (adattatori di rete) e premere Invio.
5. Selezionare le porte desiderate per vSwitch0. Premere Invio.

   Selezionare le porte corrispondenti a eth0 e eth1 in CIMC.

6. Selezionare VLAN (opzionale) e premere Invio.
7. Inserire l'ID VLAN `<<mgmt_vlan_id>>`. Premere Invio.
8. Dal menu Configure Management Network (Configura rete di gestione), selezionare IPv4 Configuration (Configurazione IPv4) per configurare l'indirizzo IP dell'interfaccia di gestione. Premere Invio.
9. Utilizzare i tasti freccia per evidenziare Set Static IPv4 address (Imposta indirizzo IPv4 statico) e utilizzare la barra spaziatrice per selezionare questa opzione.
10. Inserire l'indirizzo IP per la gestione dell'host VMware ESXi `<<esxi_host_mgmt_ip>>`.
11. Inserire la subnet mask per l'host VMware ESXi `<<esxi_host_mgmt_netmask>>`.
12. Immettere il gateway predefinito per l'host VMware ESXi `<<esxi_host_mgmt_gateway>>`.
13. Premere Invio per accettare le modifiche apportate alla configurazione IP.
14. Accedere al menu di configurazione IPv6.
15. Utilizzare la barra spaziatrice per disattivare IPv6 deselezionando l'opzione Enable IPv6 (riavvio richiesto). Premere Invio.
16. Accedere al menu per configurare le impostazioni DNS.
17. Poiché l'indirizzo IP viene assegnato manualmente, le informazioni DNS devono essere inserite anche manualmente.
18. Inserire l'indirizzo IP del server DNS primario[nameserver_ip].
19. (Facoltativo) inserire l'indirizzo IP del server DNS secondario.
20. Inserire l'FQDN per il nome host VMware ESXi:[esxi_host_fqdn].
21. Premere Invio per accettare le modifiche apportate alla configurazione DNS.
22. Uscire dal sottomenu Configure Management Network (Configura rete di gestione) premendo Esc.
23. Premere Y per confermare le modifiche e riavviare il server.
24. Disconnettersi dalla console VMware premendo Esc.

Configurare l'host ESXi

Per configurare ciascun host ESXi, sono necessarie le informazioni riportate nella seguente tabella.

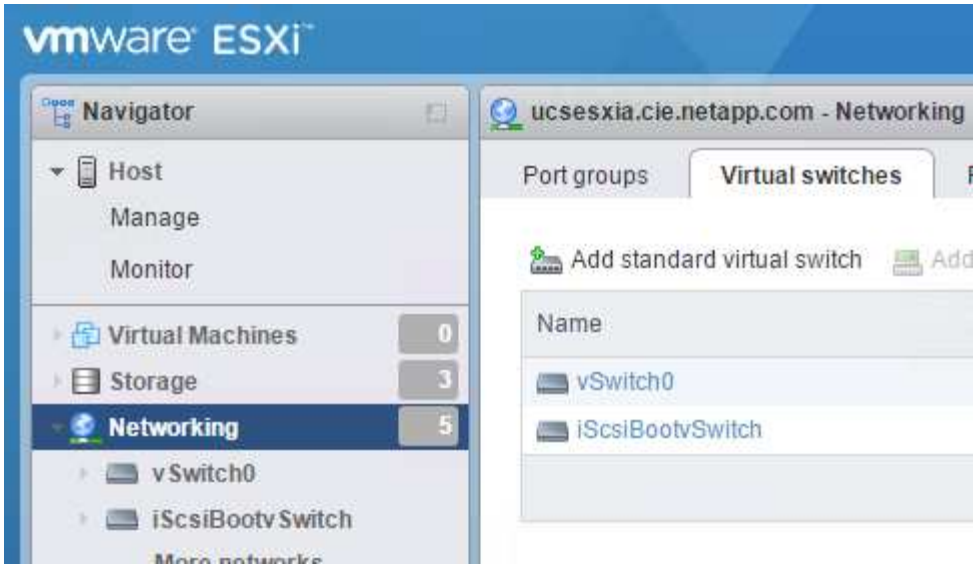
Dettaglio	Valore
Nome host ESXi	
IP di gestione host ESXi	
Maschera di gestione host ESXi	
Gateway di gestione host ESXi	
IP NFS host ESXi	
ESXi host NFS mask	
Gateway NFS host ESXi	
IP vMotion host ESXi	
Host ESXi vMotion mask	
Gateway vMotion host ESXi	
IP iSCSI-A host ESXi	
Host ESXi iSCSI-A mask	
Gateway iSCSI-A host ESXi	
IP iSCSI-B host ESXi	
Host ESXi iSCSI-B mask	
Gateway iSCSI-B host ESXi	

Accedere all’host ESXi

1. Aprire l’indirizzo IP di gestione dell’host in un browser Web.
2. Accedere all’host ESXi utilizzando l’account root e la password specificati durante il processo di installazione.
3. Leggi la dichiarazione sul programma di miglioramento basato sull’esperienza dei clienti VMware. Dopo aver selezionato la risposta corretta, fare clic su OK.

Configurare l’avvio iSCSI

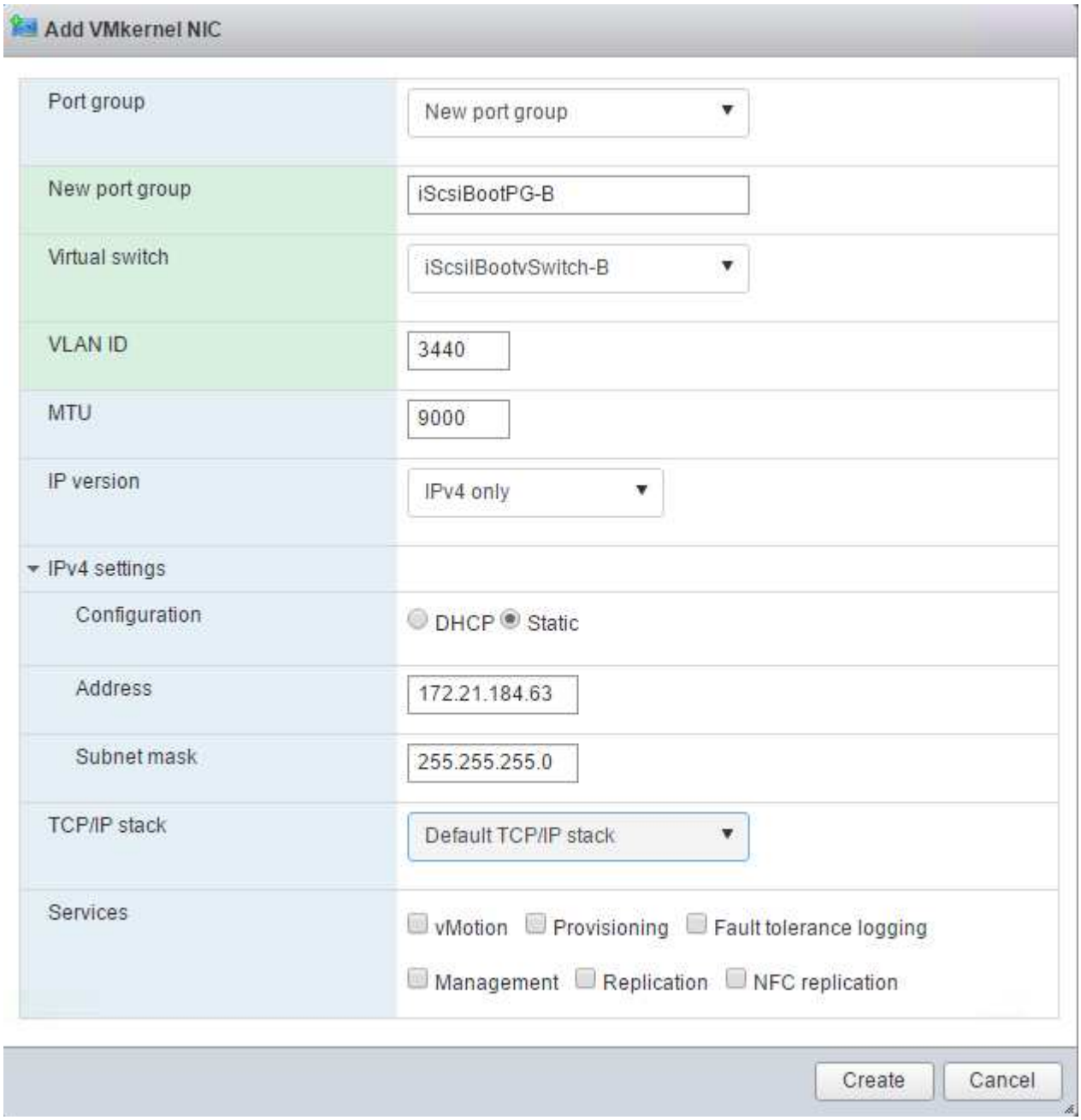
1. Selezionare Networking (rete) a sinistra.
2. A destra, selezionare la scheda Virtual Switches (interruttori virtuali).



3. Fare clic su iScsiBootvSwitch.
4. Selezionare Modifica impostazioni.
5. Impostare la MTU su 9000 e fare clic su Save (Salva).
6. Fare clic su Networking (rete) nel riquadro di navigazione a sinistra per tornare alla scheda Virtual Switches (Switch virtuali).
7. Fare clic su Add Standard Virtual Switch.
8. Fornire il nome `iScsiBootvSwitch-B` Per il nome vSwitch.
   - Impostare MTU su 9000.
   - Selezionare vmnic3 dalle opzioni Uplink 1.
   - Fare clic su Aggiungi.

> Vmnic2 e vmnic3 vengono utilizzati per l'avvio iSCSI in questa configurazione. Se si dispone di schede di rete aggiuntive nell'host ESXi, è possibile che siano presenti numeri vmnic diversi. Per confermare quali NIC vengono utilizzate per l'avvio iSCSI, associare gli indirizzi MAC sulle vNIC iSCSI in CIMC alle vmniche in ESXi.

9. Nel riquadro centrale, selezionare la scheda NIC VMkernel.
10. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel).
    - Specificare un nuovo nome di gruppo di porte di `iScsiBootPG-B`.
    - Selezionare iScsiBootvSwitch-B per lo switch virtuale.
    - Invio `<<iscsib_vlan_id>>` Per l'ID VLAN.
    - Impostare la MTU su 9000.
    - Espandere Impostazioni IPv4.
    - Selezionare Static Configuration (Configurazione statica).
    - Invio `<<var_hosta_iscsib_ip>>` Per Indirizzo.
    - Invio `<<var_hosta_iscsib_mask>>` Per Subnet Mask.
    - Fare clic su Crea.

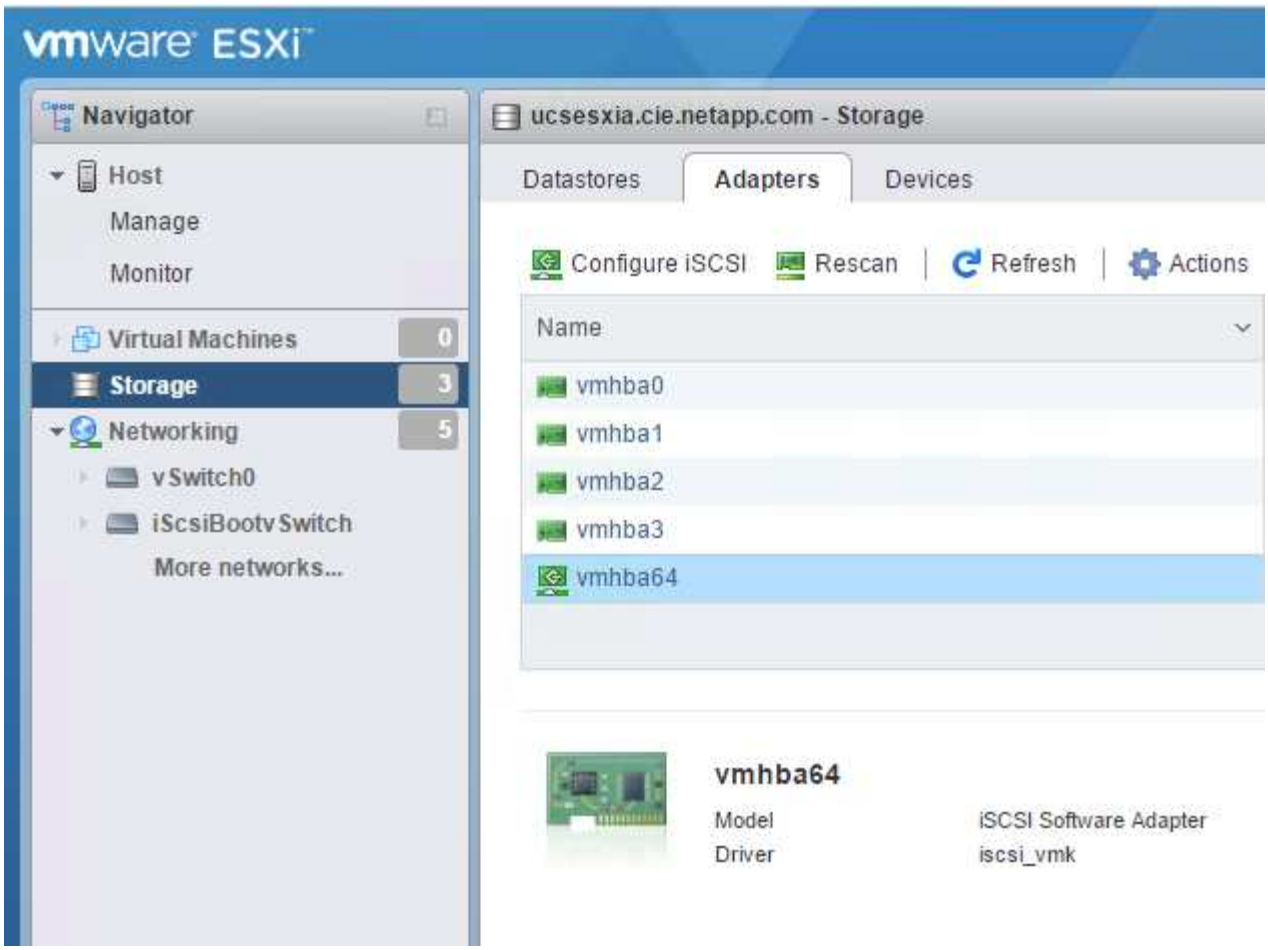


Impostare MTU su 9000 ON `iScsiBootPG- A.`

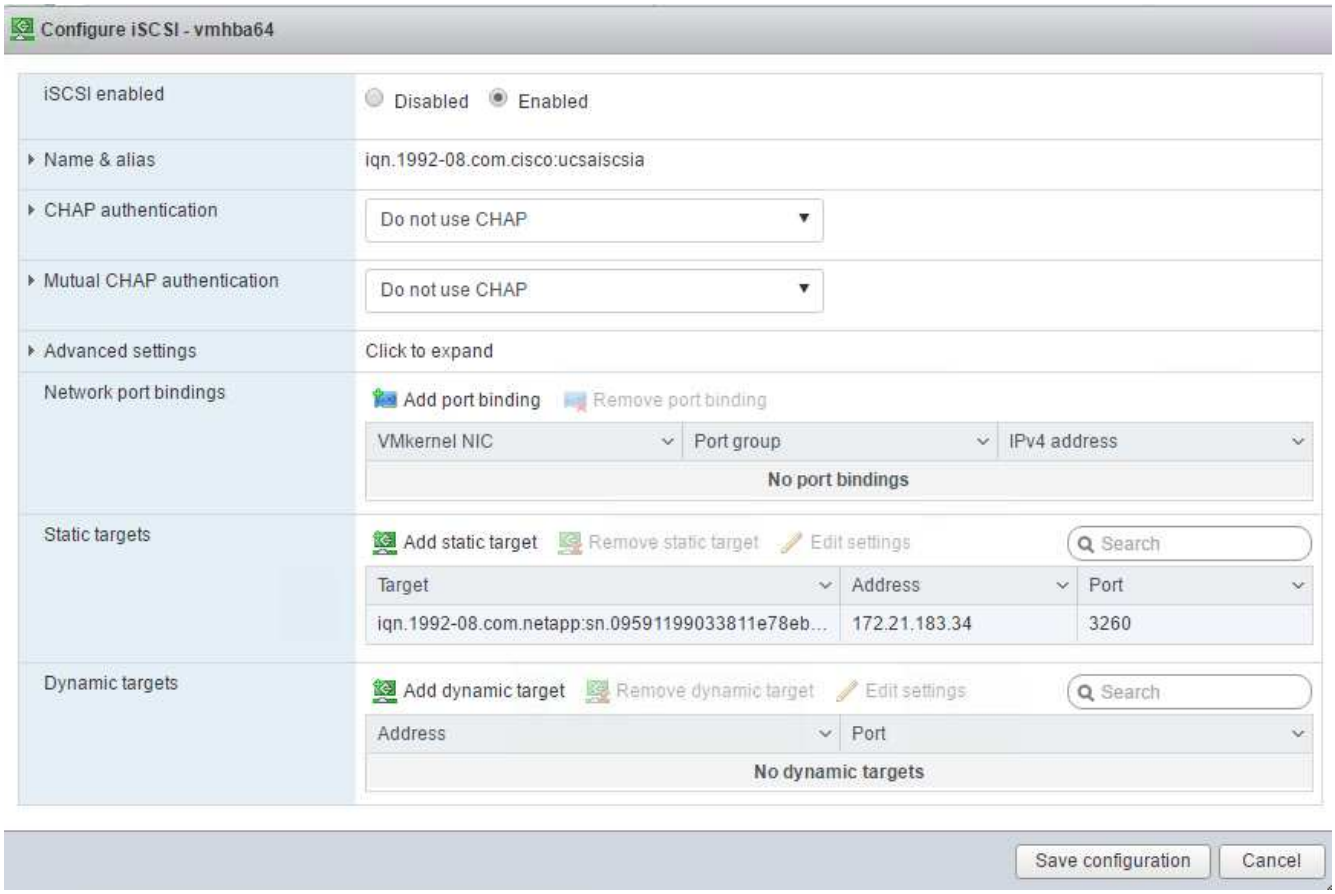
Configurare il multipathing iSCSI

Per configurare il multipathing iSCSI sugli host ESXi, attenersi alla seguente procedura:

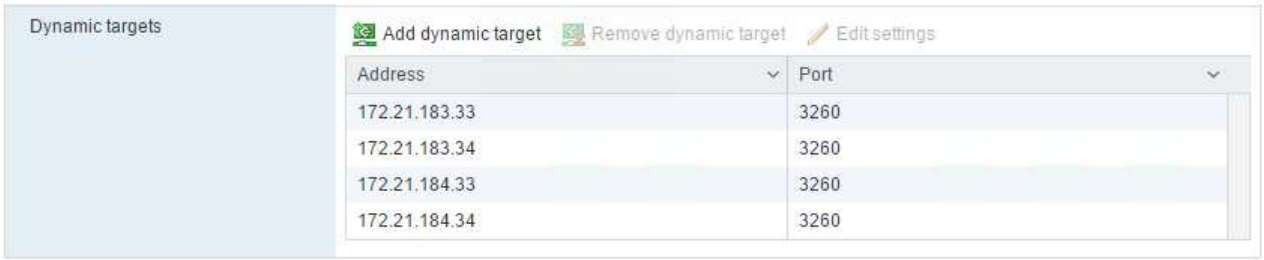
1. Selezionare Storage (archiviazione) nel riquadro di navigazione a sinistra. Fare clic su adattatori.
2. Selezionare l'adattatore software iSCSI e fare clic su Configure iSCSI (Configura iSCSI).



3. In Dynamic Targets (destinazioni dinamiche), fare clic su Add Dynamic Target (Aggiungi destinazione dinamica



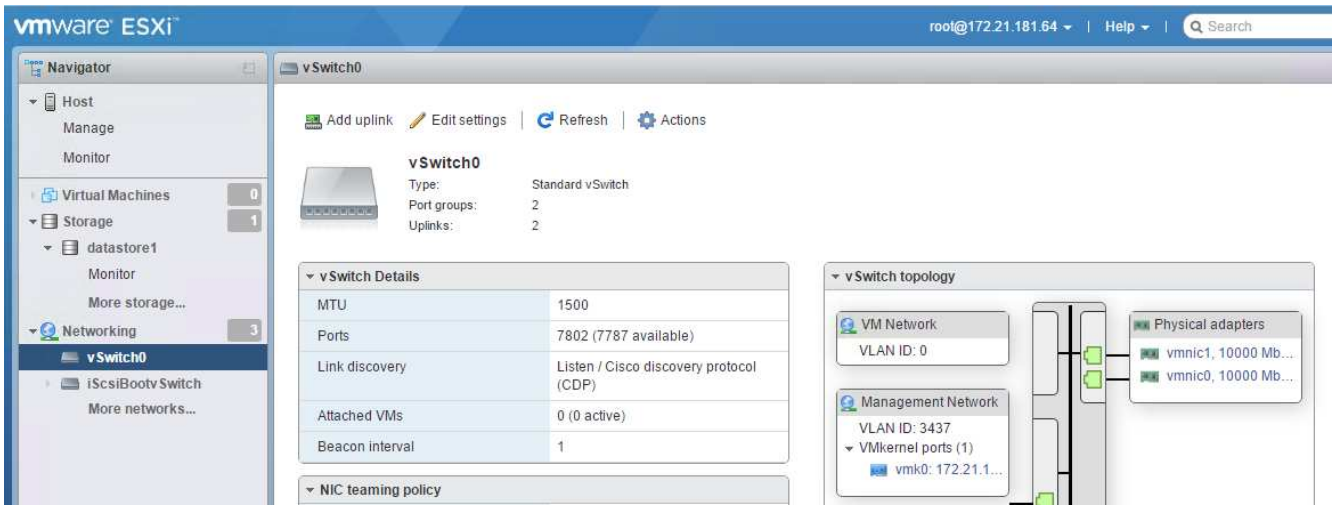
4. Inserire l'indirizzo IP `iscsi_lif01a`.
   - Ripetere l'operazione con gli indirizzi IP `iscsi_lif01b`, `iscsi_lif02a`, e. `iscsi_lif02b`.
   - Fare clic su Salva configurazione.



> È possibile trovare gli indirizzi IP LIF iSCSI eseguendo il comando `Network interface show `(Mostra interfaccia di rete) sul cluster NetApp o osservando la scheda Network Interfaces (interfacce di rete) in Gestore di sistema OnCommand.

Configurare l'host ESXi

1. Nel riquadro di spostamento a sinistra, selezionare rete.
2. Selezionare vSwitch0.



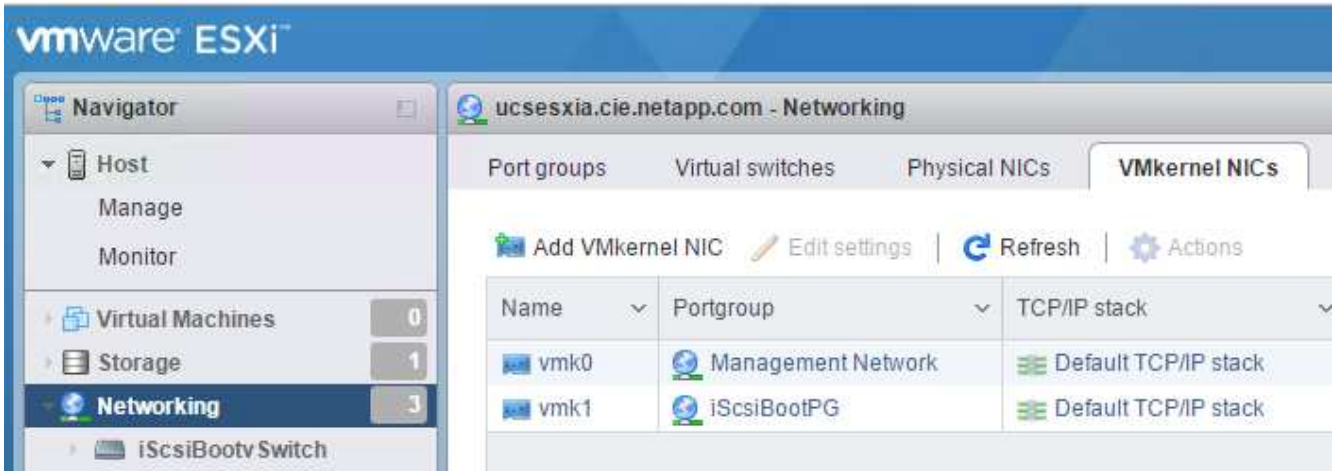
3. Selezionare Edit Settings (Modifica impostazioni).
4. Impostare la MTU su 9000.
5. Espandere NIC Teaming e verificare che vmnic0 e vmnic1 siano impostati su Active.

Configurare i gruppi di porte e le NIC VMkernel

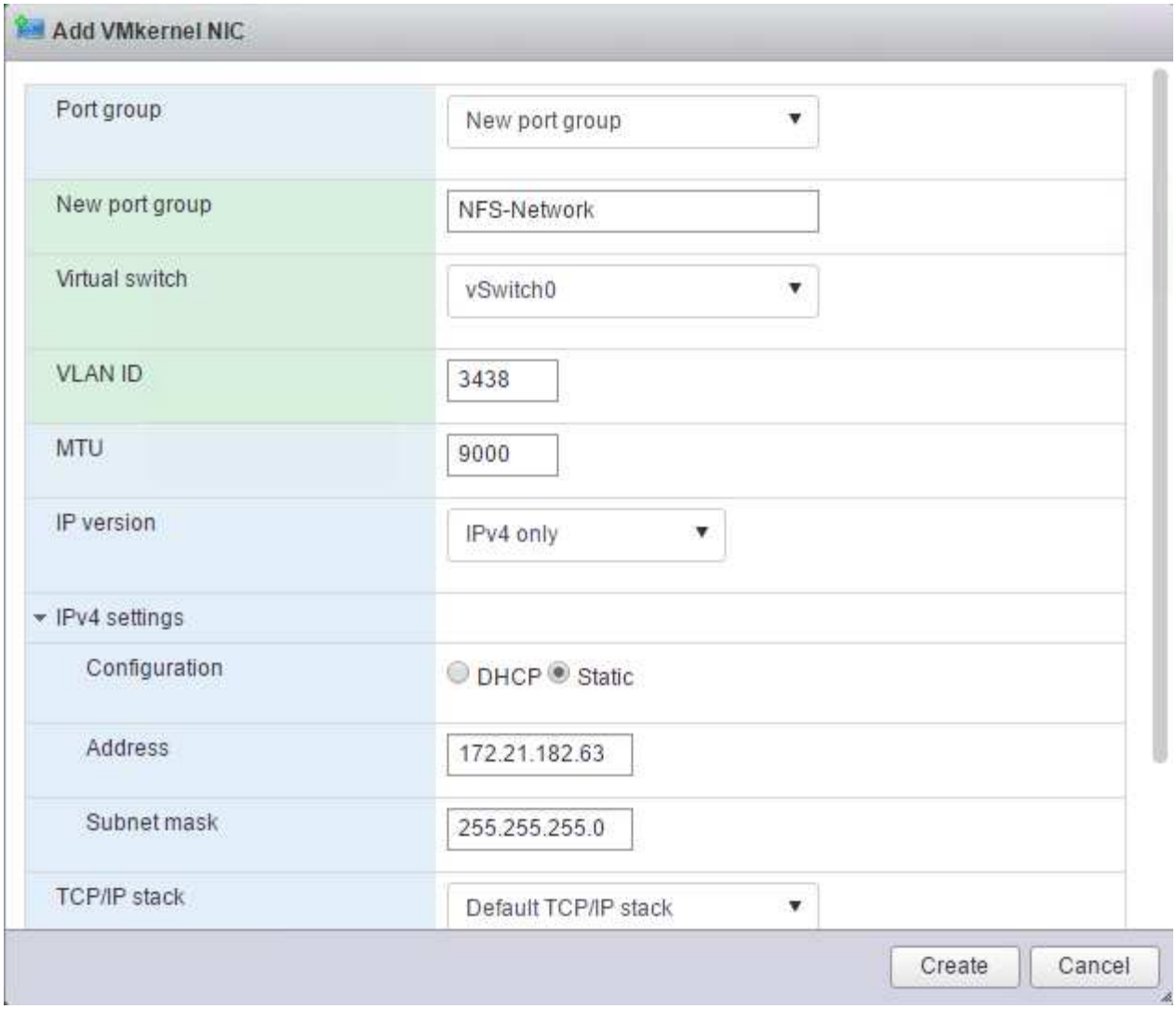
1. Nel riquadro di spostamento a sinistra, selezionare rete.
2. Fare clic con il pulsante destro del mouse sulla scheda gruppi di porte.

3. Fare clic con il pulsante destro del mouse su rete VM e selezionare Modifica. Impostare l'ID VLAN su `<<var_vm_traffic_vlan>>`.
4. Fare clic su Aggiungi gruppo di porte.
   - Assegnare un nome al gruppo di porte `MGMT-Network`.
   - Invio `<<mgmt_vlan>>` Per l'ID VLAN.
   - Assicurarsi che vSwitch0 sia selezionato.
   - Fare clic su Aggiungi.

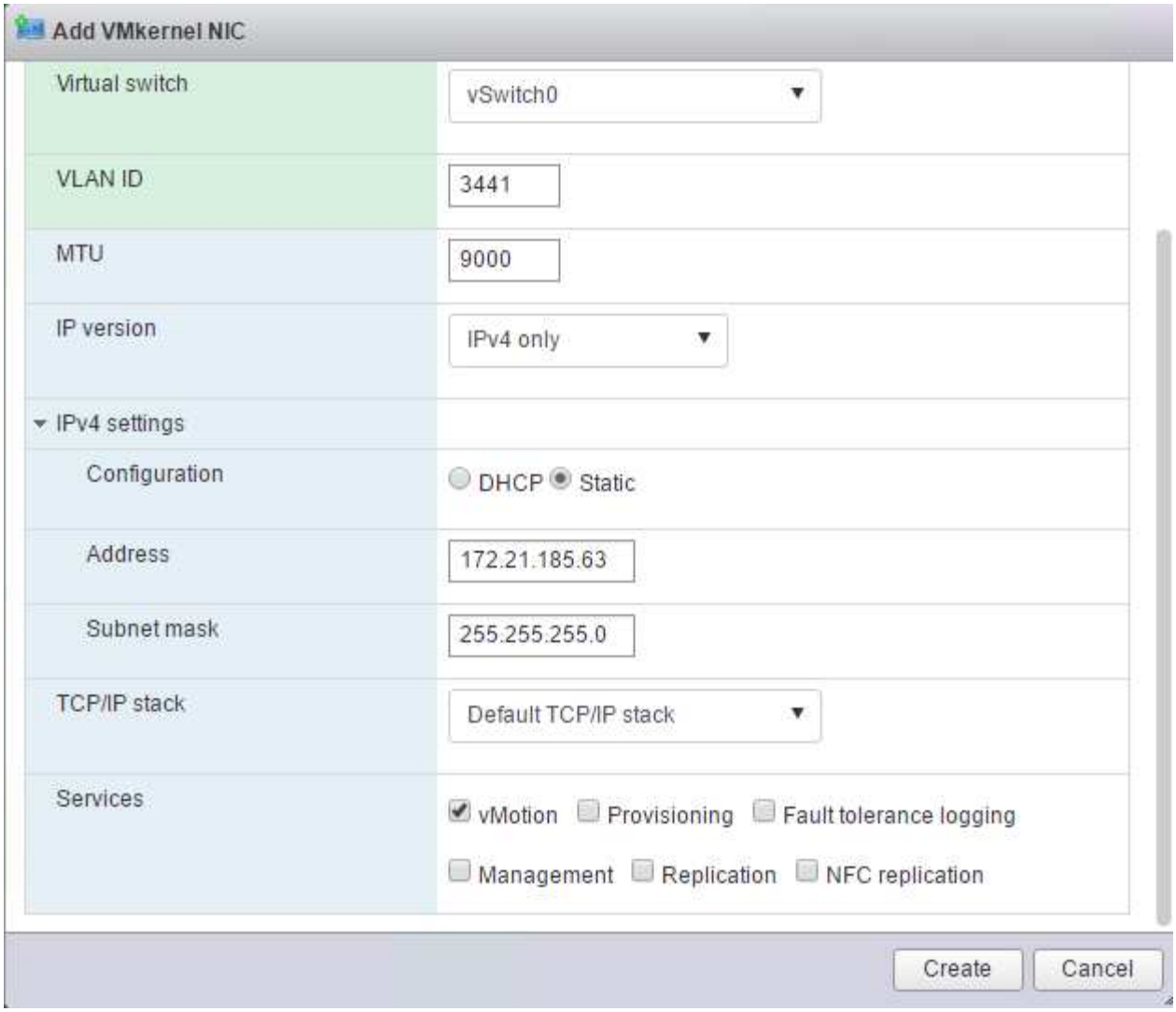
5. Fare clic sulla scheda NIC VMkernel.



6. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel).
   - Selezionare New Port Group (nuovo gruppo di porte).
   - Assegnare un nome al gruppo di porte `NFS-Network`.
   - Invio `<<nfs_vlan_id>>` Per l'ID VLAN.
   - Impostare la MTU su 9000.
   - Espandere Impostazioni IPv4.
   - Selezionare Static Configuration (Configurazione statica).
   - Invio `<<var_hosta_nfs_ip>>` Per Indirizzo.
   - Invio `<<var_hosta_nfs_mask>>` Per Subnet Mask.
   - Fare clic su Crea.



7. Ripetere questa procedura per creare la porta VMkernel vMotion.
8. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel).
    a. Selezionare New Port Group (nuovo gruppo di porte).
    b. Assegnare un nome al gruppo di porte vMotion.
    c. Invio `<<vmotion_vlan_id>>` Per l'ID VLAN.
    d. Impostare la MTU su 9000.
    e. Espandere Impostazioni IPv4.
    f. Selezionare Static Configuration (Configurazione statica).
    g. Invio `<<var_hosta_vmotion_ip>>` Per Indirizzo.
    h. Invio `<<var_hosta_vmotion_mask>>` Per Subnet Mask.
    i. Assicurarsi che la casella di controllo vMotion sia selezionata dopo Impostazioni IPv4.

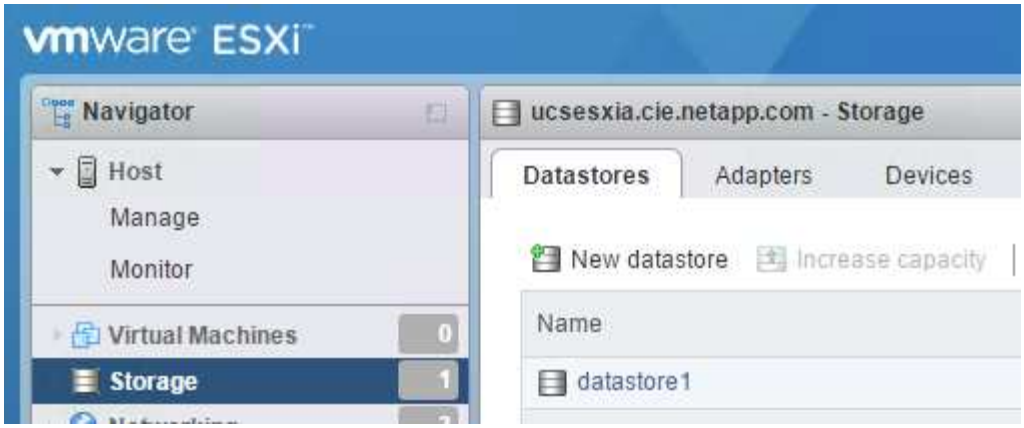


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

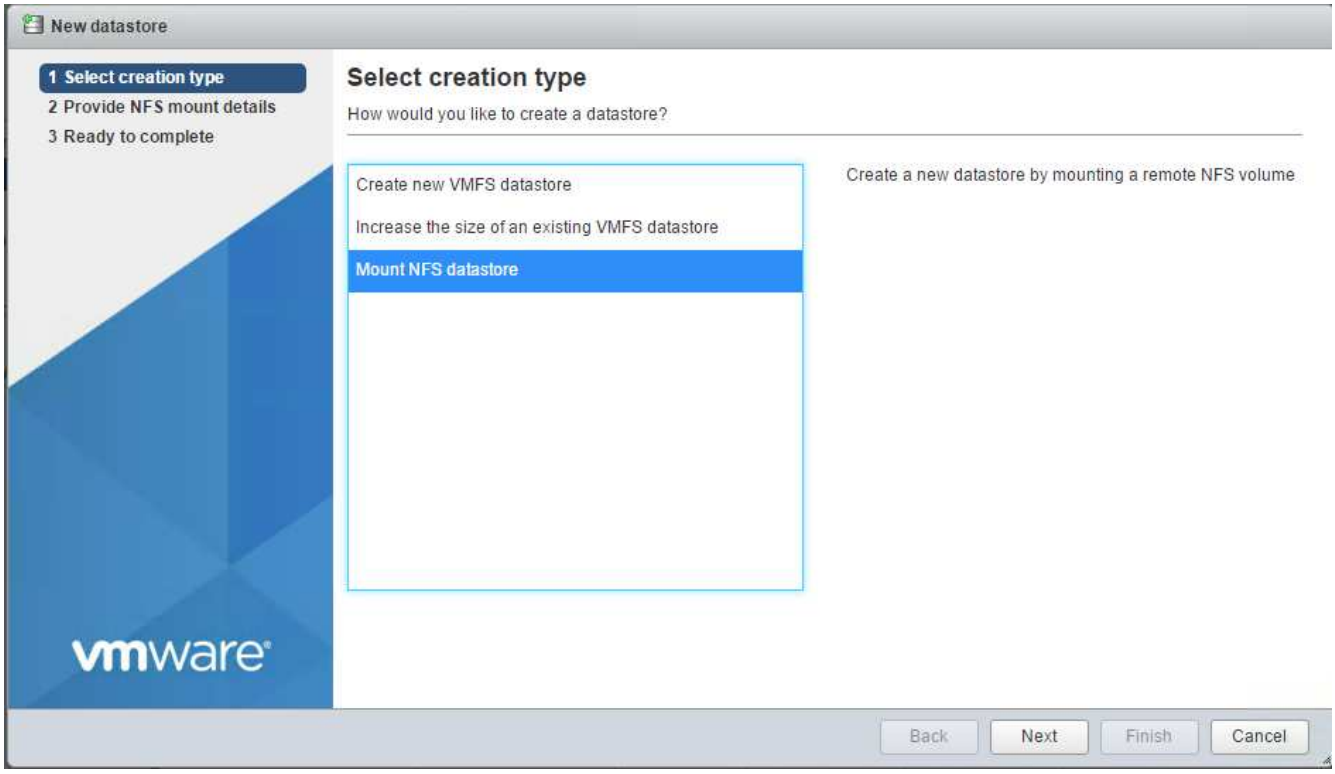
Montare i primi datastore

I primi datastore da montare sono il datastore infra_datastore_1 per le macchine virtuali e il datastore infra_swap per i file di swap delle macchine virtuali.

1. Fare clic su Storage (archiviazione) nel riquadro di spostamento di sinistra, quindi su New Datastore (nuovo archivio dati).



2. Selezionare Mount NFS Datastore (monta archivio dati NFS).



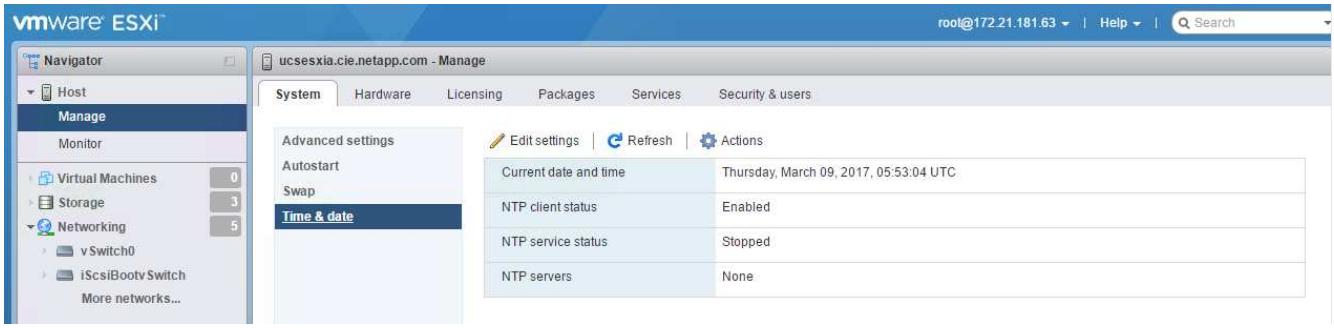
3. Quindi, inserire le seguenti informazioni nella pagina fornire i dettagli del montaggio NFS:
   - Nome: `infra_datastore_1`
   - Server NFS: `<<var_nodea_nfs_lif>>`
   - Share: /Infra_datastore_1
   - Assicurarsi che sia selezionato NFS 3.
4. Fare clic su fine. È possibile visualizzare il completamento dell'attività nel riquadro attività recenti.
5. Ripetere questa procedura per montare il datastore infra_swap:
   - Nome: `infra_swap`
   - Server NFS: `<<var_nodea_nfs_lif>>`
   - Condividere: `/infra_swap`

- Assicurarsi che sia selezionato NFS 3.

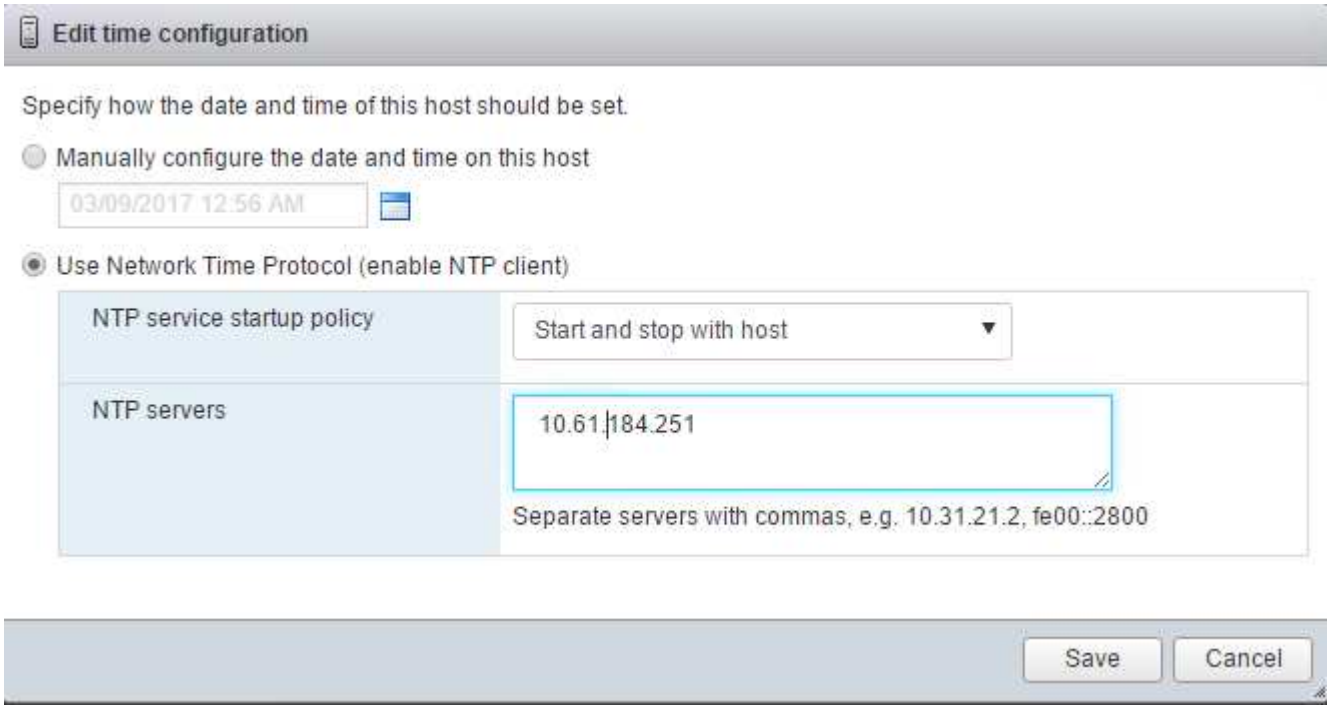
Configurare NTP

Per configurare NTP per un host ESXi, attenersi alla seguente procedura:

1. Fare clic su Manage (Gestisci) nel riquadro di navigazione a sinistra. Selezionare sistema nel riquadro di destra, quindi fare clic su Data e ora.



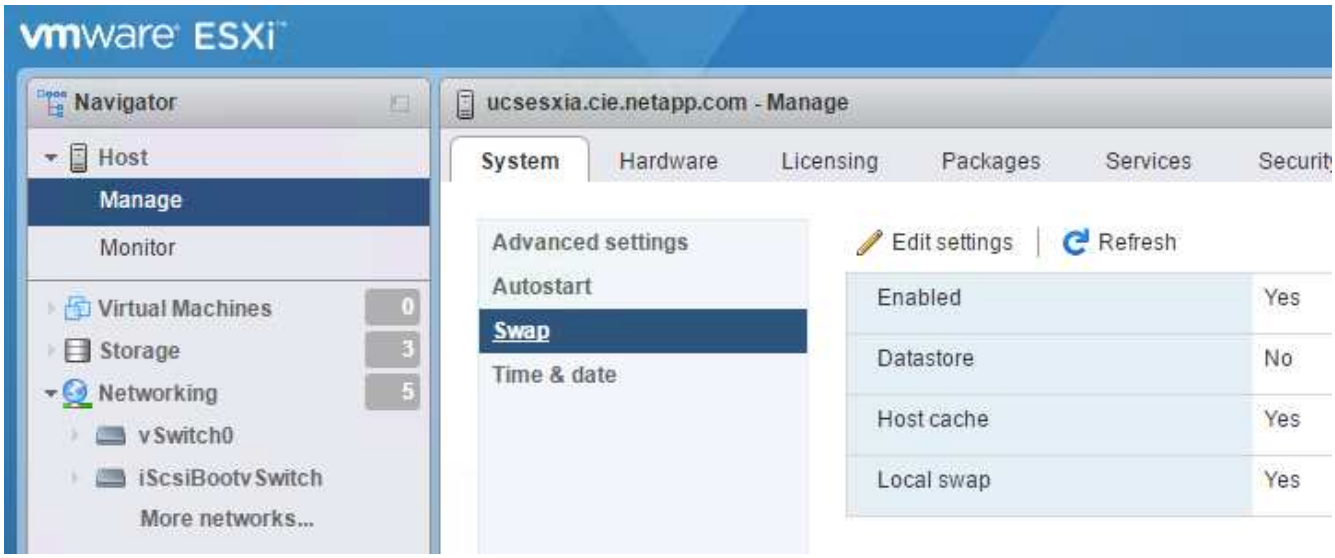
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio del servizio NTP.
4. Invio `<<var_ntp>>` Come server NTP. È possibile impostare più server NTP.
5. Fare clic su Salva.



Spostare la posizione del file di swap della macchina virtuale

Questi passaggi forniscono informazioni dettagliate sullo spostamento della posizione del file di swap della macchina virtuale.

1. Fare clic su Manage (Gestisci) nel riquadro di navigazione a sinistra. Selezionare System (sistema) nel riquadro di destra, quindi fare clic su Swap (Scambia).



2. Fare clic su Modifica impostazioni. Selezionare infra_swap dalle opzioni Datastore.

3. Fare clic su Salva.

Installare il plug-in NetApp NFS 1.0.20 per VMware VAAI

Per installare il plug-in NetApp NFS 1.0.20 per VMware VAAI, attenersi alla seguente procedura.

1. Immettere i seguenti comandi per verificare che VAAI sia attivato:

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Se VAAI è attivato, questi comandi producono il seguente output:

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Se VAAI non è abilitato, immettere i seguenti comandi per abilitare VAAI:

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Questi comandi producono il seguente output:

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Scarica il plug-in NetApp NFS per VMware VAAI:
   a. Accedere alla "pagina di download del software".
   b. Scorrere verso il basso e fare clic su NetApp NFS Plug-in for VMware VAAI.
   c. Selezionare la piattaforma ESXi.
   d. Scarica il bundle offline (.zip) o il bundle online (.vib) del plug-in più recente.
4. Installare il plug-in sull'host ESXi utilizzando ESX CLI.
5. Riavviare l'host ESXI.

```
[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:~]
```

"Installazione di VMware vCenter Server 6.7"

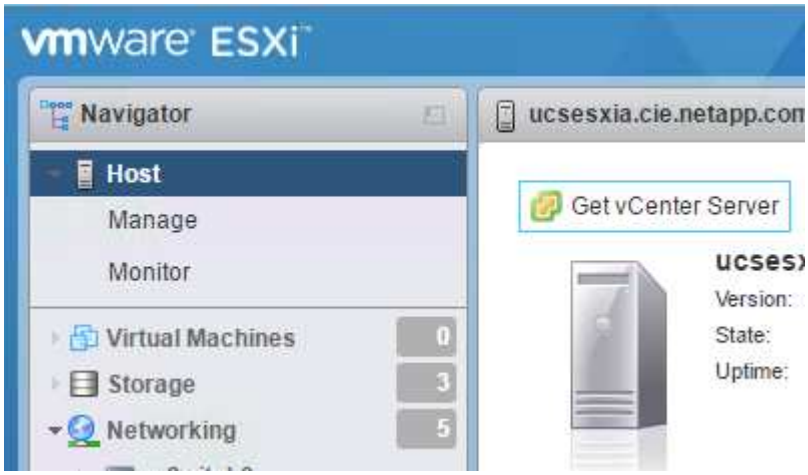
Installare VMware vCenter Server 6.7

Questa sezione fornisce procedure dettagliate per l'installazione di VMware vCenter Server 6.7 in una configurazione FlexPod Express.

FlexPod utilizza l'appliance server vCenter (VCSA).

Scarica l'appliance server VMware vCenter

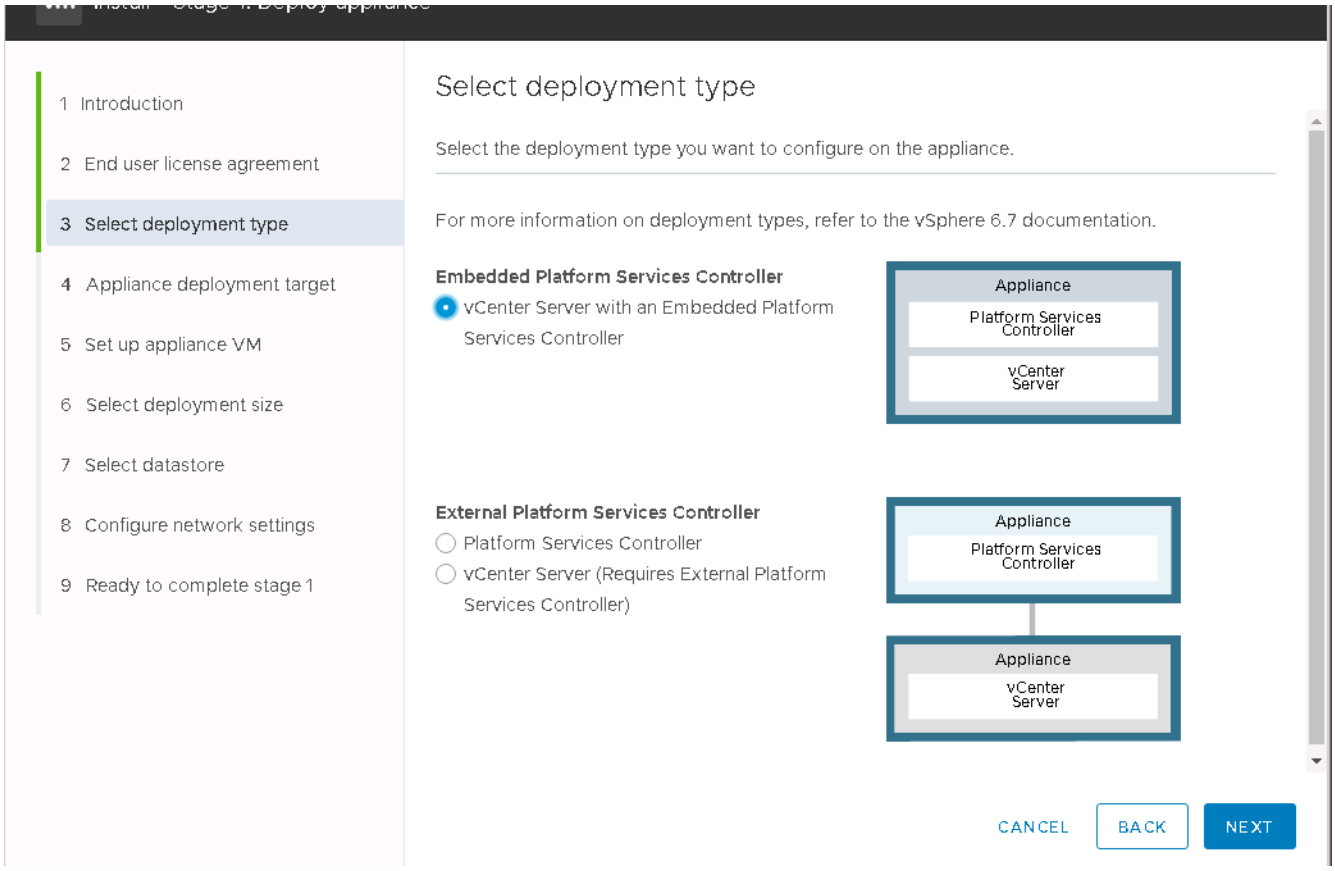
1. Scarica VCSA. Per accedere al collegamento per il download, fare clic sull'icona Get vCenter Server (Ottieni server vCenter) durante la gestione dell'host ESXi.



2. Scaricare VCSA dal sito VMware.

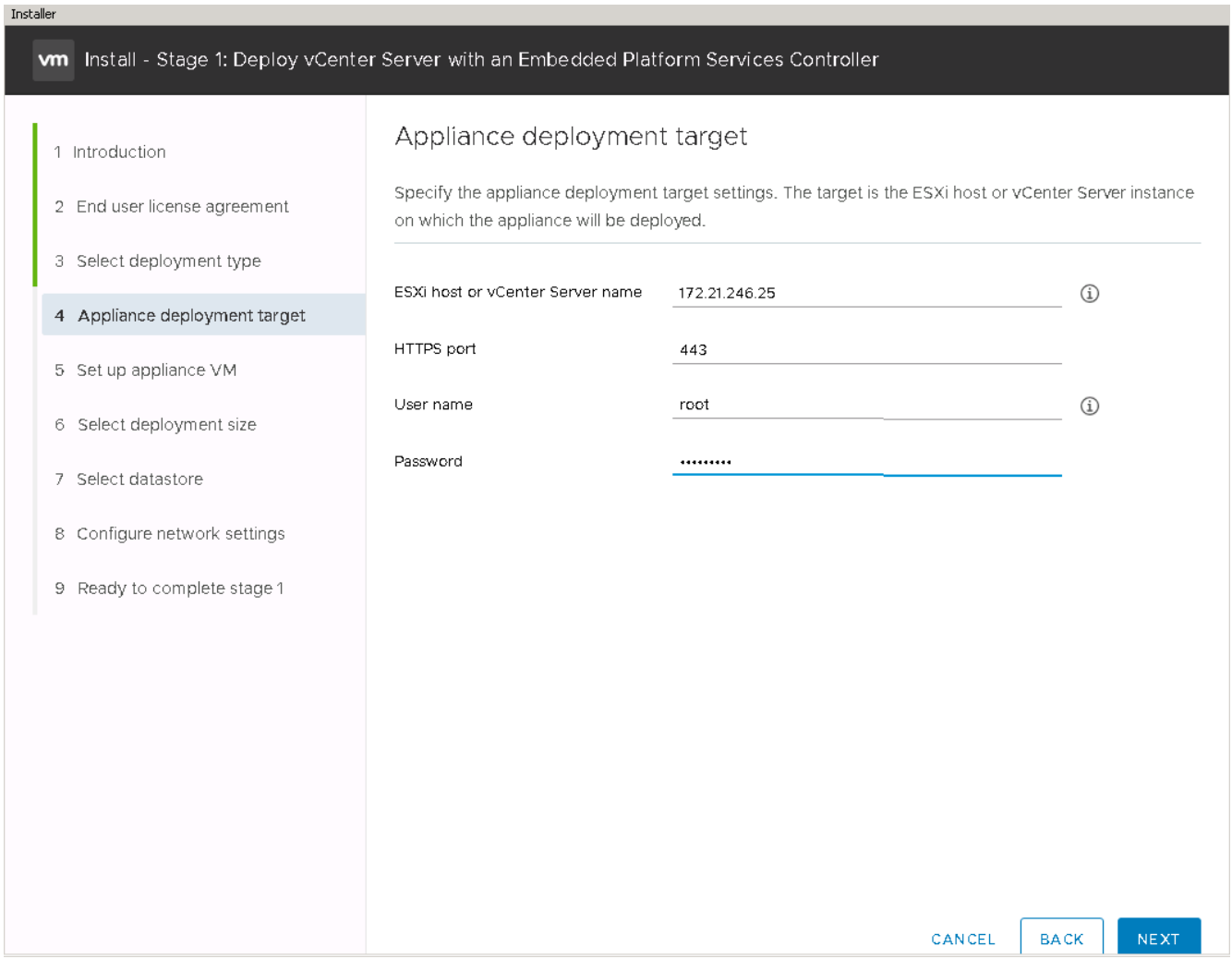
> Sebbene sia supportato l'installabile di Microsoft Windows vCenter Server, VMware consiglia VCSA per le nuove implementazioni.

3. Montare l'immagine ISO.
4. Accedere alla directory vcsa-ui-installer> win32. Fare doppio clic su installer.exe.
5. Fare clic su Installa.
6. Fare clic su Avanti nella pagina Introduzione.
7. Accettare il contratto di licenza con l'utente finale.
8. Selezionare Embedded Platform Services Controller come tipo di implementazione.

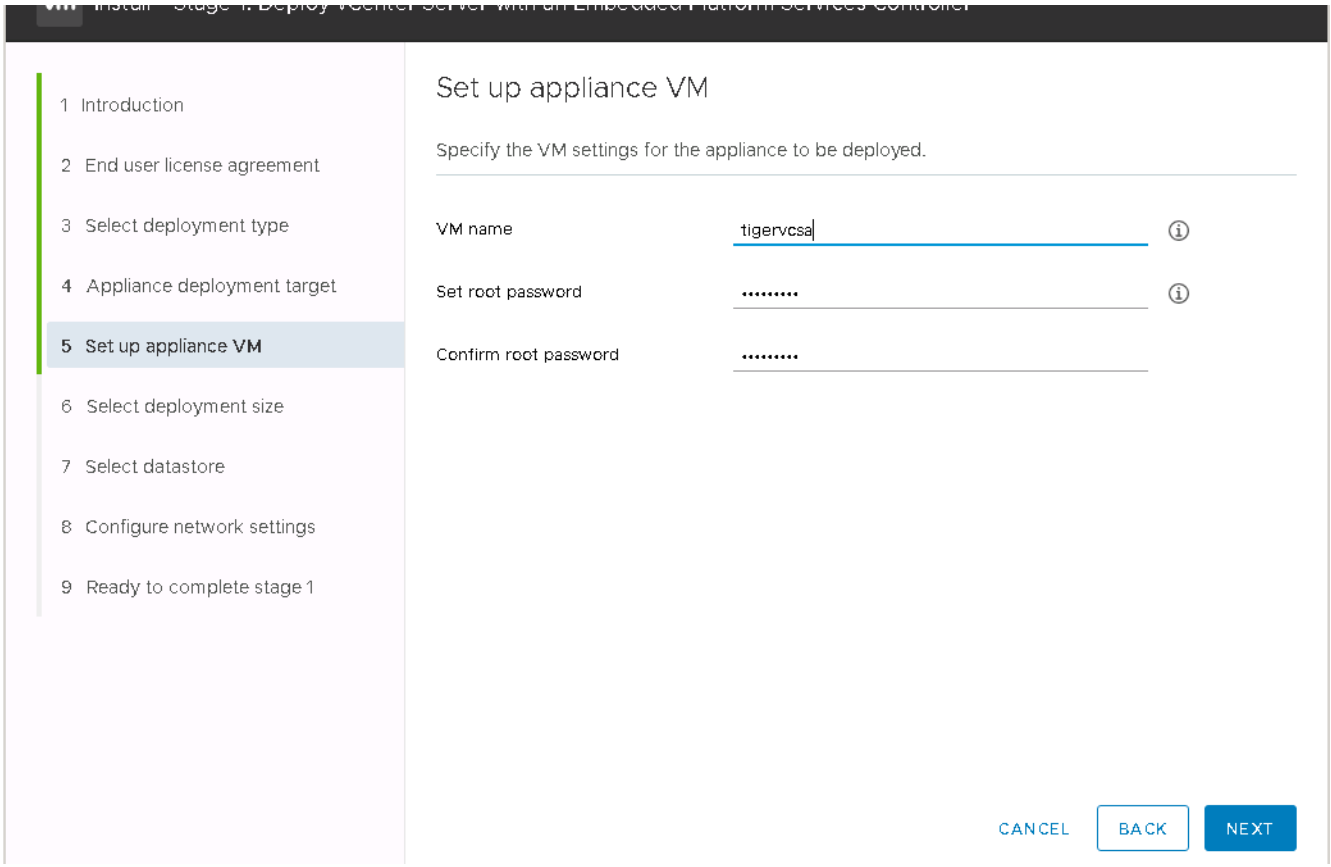


Se necessario, l'implementazione del controller dei servizi della piattaforma esterna è supportata anche come parte della soluzione FlexPod Express.

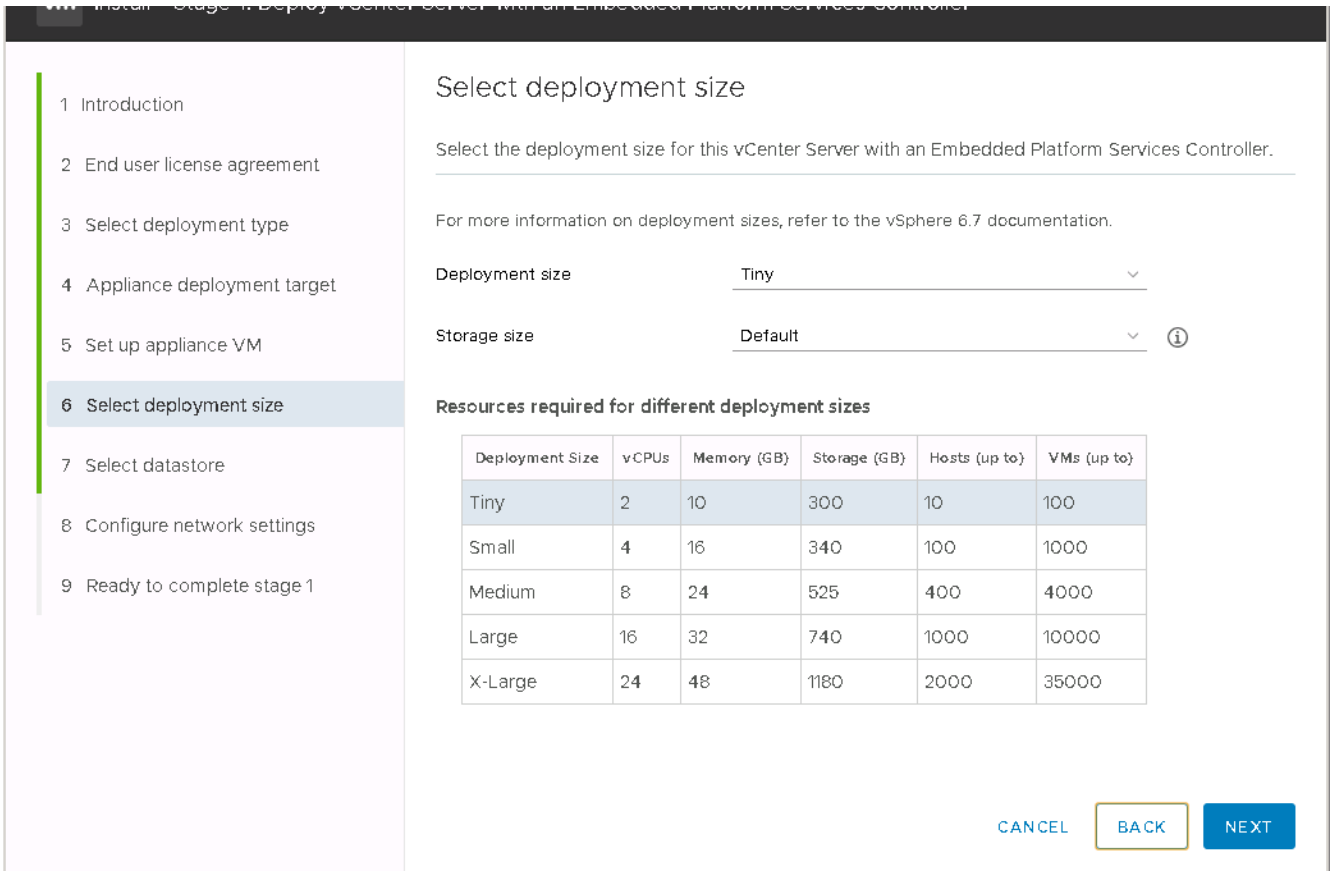
9. In Appliance Deployment Target (destinazione di implementazione dell'appliance), immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root.



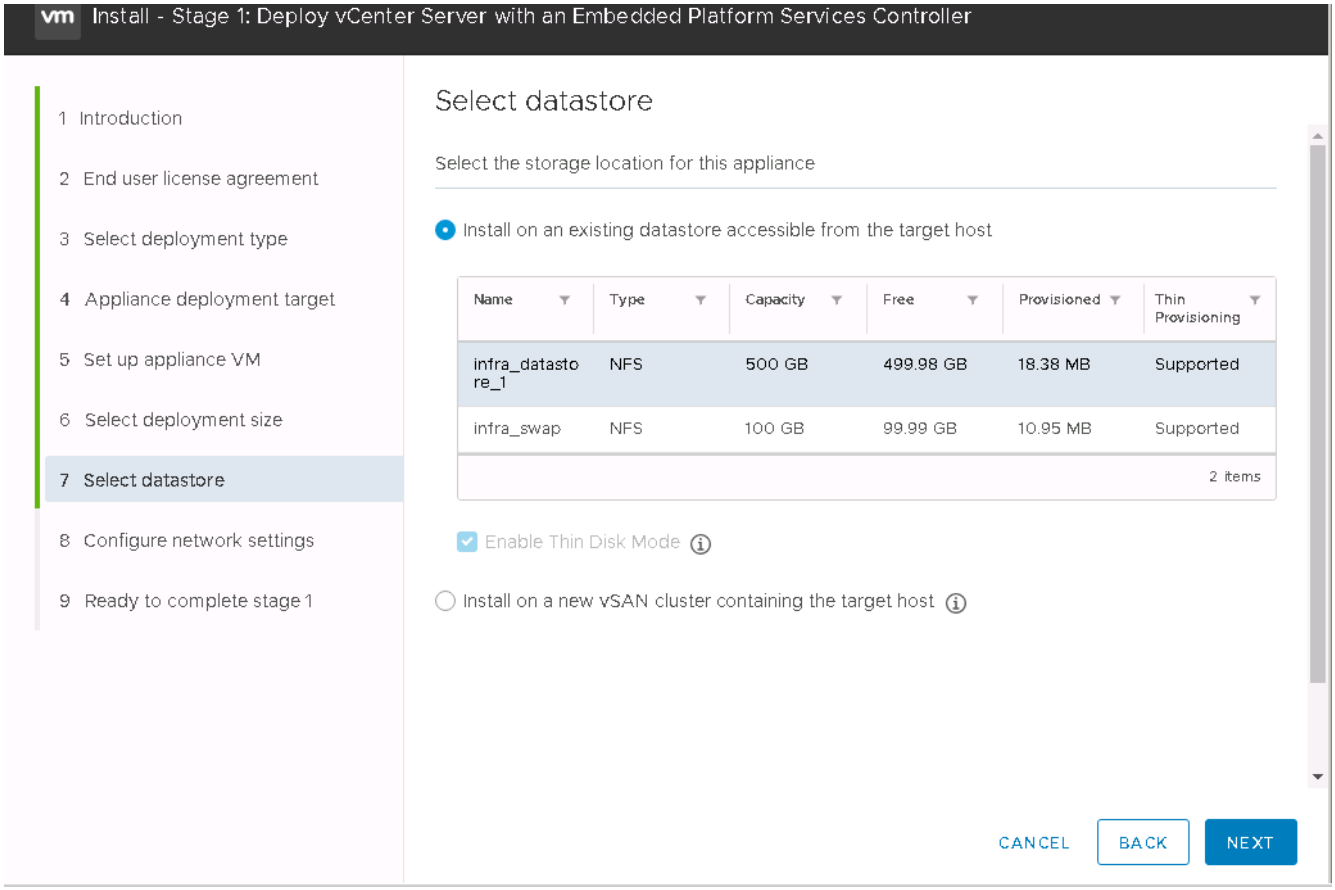
10. Impostare la VM dell'appliance immettendo `VCSA` Come nome della macchina virtuale e password root che si desidera utilizzare per VCSA.



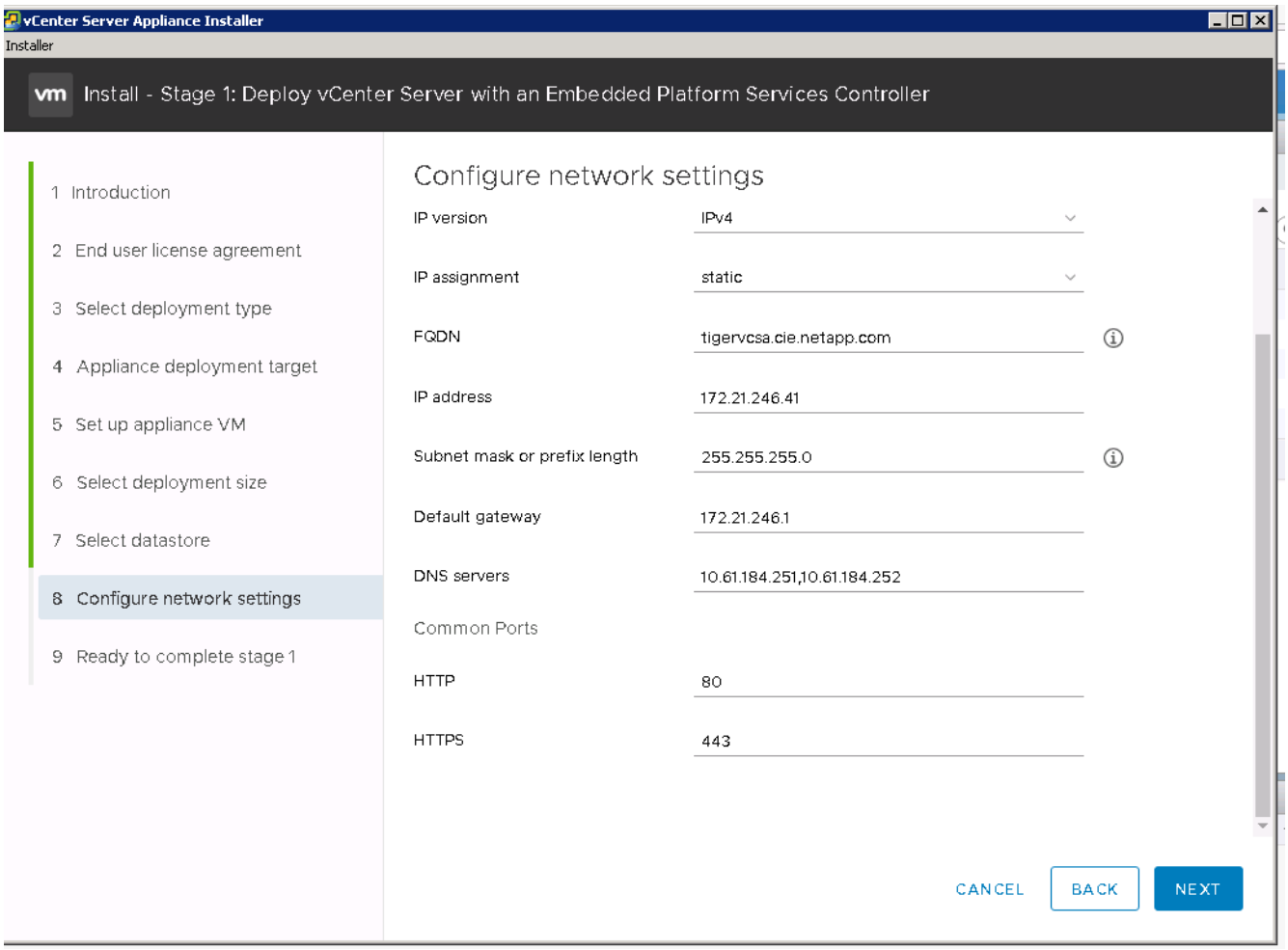
11. Selezionare la dimensione di implementazione più adatta al proprio ambiente. Fare clic su Avanti.



12. Selezionare il datastore infra_datastore_1. Fare clic su Avanti.

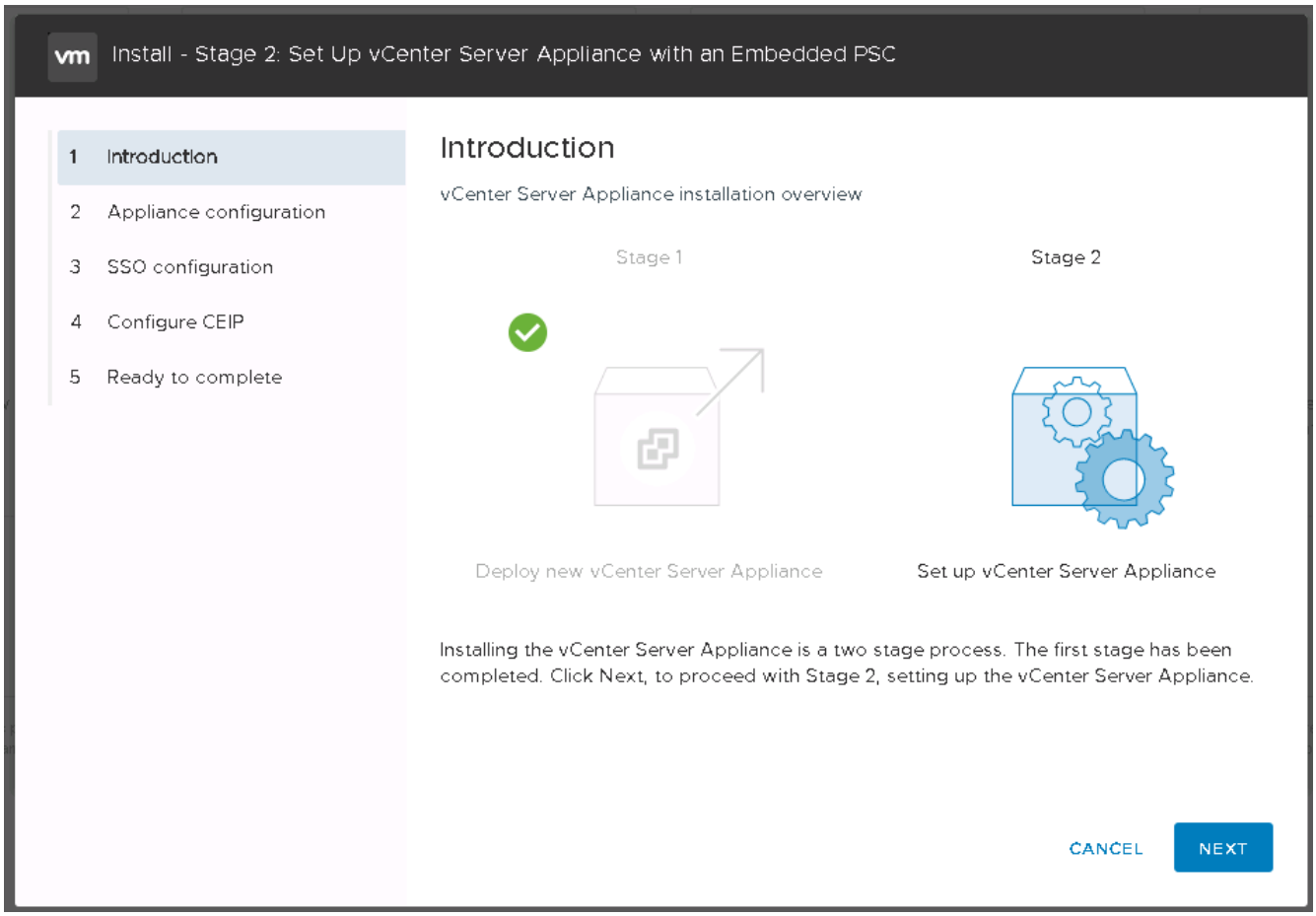


13. Inserire le seguenti informazioni nella pagina Configure network settings (Configura impostazioni di rete) e fare clic su Next (Avanti).
    a. Selezionare MGMT-Network for Network (rete MGMT per rete).
    b. Inserire l'FQDN o l'IP da utilizzare per VCSA.
    c. Inserire l'indirizzo IP da utilizzare.
    d. Inserire la subnet mask da utilizzare.
    e. Inserire il gateway predefinito.
    f. Inserire il server DNS.
14. Nella pagina Pronto per completare la fase 1, verificare che le impostazioni immesse siano corrette. Fare clic su fine.



VCSA viene installato ora. Questo processo richiede alcuni minuti.

15. Al termine della fase 1, viene visualizzato un messaggio che indica che il processo è stato completato. Fare clic su Continue (continua) per iniziare la configurazione della fase 2.
16. Nella pagina Introduzione alla fase 2, fare clic su Avanti.



17. Invio `<<var_ntp_id>>` Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.

    Se si intende utilizzare vCenter Server High Availability (ha), assicurarsi che l'accesso SSH sia attivato.

18. Configurare il nome di dominio SSO, la password e il nome del sito. Fare clic su Avanti.

    Registrare questi valori come riferimento, soprattutto se si discosta dal nome di dominio vsphere.local.

19. Se lo desideri, partecipa al programma VMware Customer Experience. Fare clic su Avanti.
20. Visualizzare il riepilogo delle impostazioni. Fare clic su fine o utilizzare il pulsante Indietro per modificare le impostazioni.
21. Viene visualizzato un messaggio che indica che non sarà possibile sospendere o interrompere il completamento dell'installazione dopo l'avvio. Fare clic su OK per continuare.

    La configurazione dell'appliance continua. Questa operazione richiede alcuni minuti.

    Viene visualizzato un messaggio che indica che la configurazione è stata eseguita correttamente.

    È possibile fare clic sui collegamenti forniti dal programma di installazione per accedere a vCenter Server.

"Configurazione del clustering di VMware vCenter Server 6.7 e vSphere."

Configurare il clustering di VMware vCenter Server 6.7 e vSphere

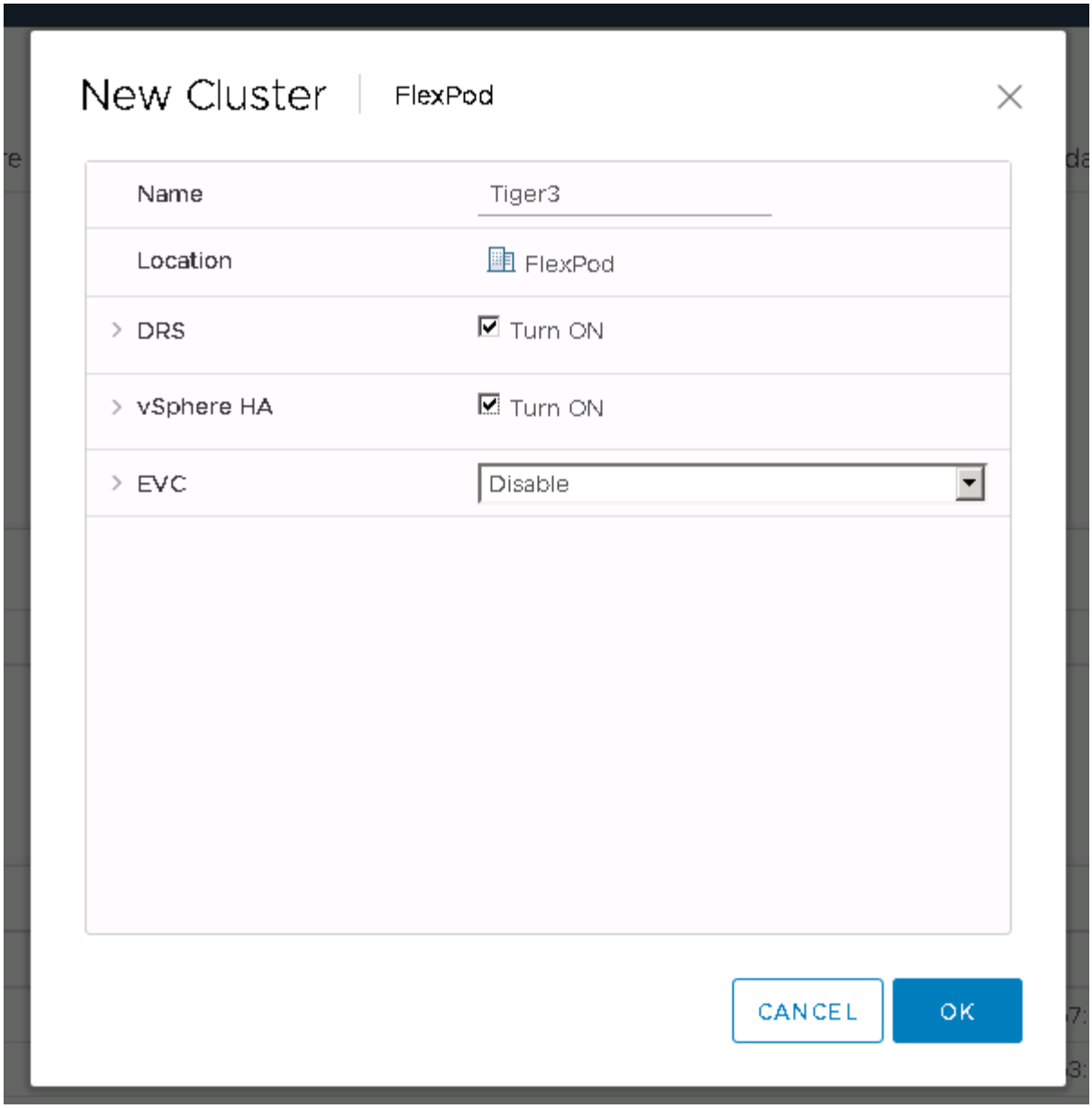
Per configurare VMware vCenter Server 6.7 e il clustering vSphere, attenersi alla seguente procedura:

1. Accedere a https://\<<FQDN or IP of vCenter>>/vsphere-client/.
2. Fare clic su Launch vSphere Client.
3. Accedere con il nome utente administrator@vsphere.local e la password SSO immessa durante il processo di configurazione di VCSA.
4. Fare clic con il pulsante destro del mouse sul nome di vCenter e selezionare New Datacenter (nuovo data center).
5. Inserire un nome per il data center e fare clic su OK.

Creare il cluster vSphere

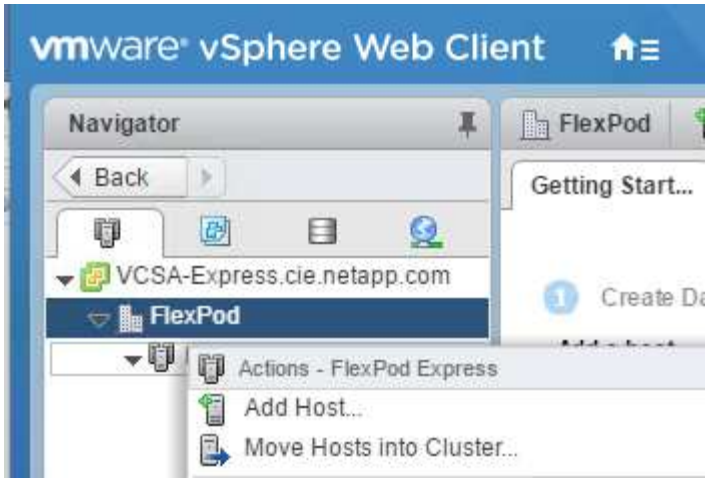
Per creare un cluster vSphere, attenersi alla seguente procedura:

1. Fare clic con il pulsante destro del mouse sul data center appena creato e selezionare New Cluster (nuovo cluster).
2. Inserire un nome per il cluster.
3. Attivare DR e vSphere ha selezionando le caselle di controllo.
4. Fare clic su OK.



Aggiungere host ESXi al cluster

1. Fare clic con il pulsante destro del mouse sul cluster e selezionare Add host (Aggiungi host).



2. Per aggiungere un host ESXi al cluster, attenersi alla seguente procedura:
   a. Inserire l'IP o l'FQDN dell'host. Fare clic su Avanti.
   b. Immettere il nome utente root e la password. Fare clic su Avanti.
   c. Fare clic su Yes (Sì) per sostituire il certificato dell'host con un certificato firmato dal server di certificazione VMware.
   d. Fare clic su Avanti nella pagina Riepilogo host.
   e. Fare clic sull'icona + verde per aggiungere una licenza all'host vSphere.

      Questa fase può essere completata in un secondo momento, se lo si desidera.

   f. Fare clic su Next (Avanti) per disattivare la modalità di blocco.
   g. Fare clic su Next (Avanti) nella pagina VM location (posizione macchina virtuale).
   h. Consultare la pagina Pronto per il completamento. Utilizzare il pulsante Indietro per apportare eventuali modifiche o selezionare fine.
3. Ripetere i passaggi 1 e 2 per l'host Cisco UCS B. Questo processo deve essere completato per tutti gli host aggiuntivi aggiunti alla configurazione di FlexPod Express.

Configurare il coredump sugli host ESXi

1. Utilizzando SSH, connettersi all'host ESXi IP di gestione, immettere root per il nome utente e la password root.
2. Eseguire i seguenti comandi:

```
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. Il messaggio `Verified the configured netdump server is running` viene visualizzato dopo l'immissione del comando finale.

Questo processo deve essere completato per tutti gli host aggiuntivi aggiunti a FlexPod Express.