



Guida all'implementazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190

FlexPod

NetApp
March 25, 2024

This PDF was generated from https://docs.netapp.com/it-it/flexpod/express/express-c-series-c190-deploy_program_summary_overview.html on March 25, 2024. Always check docs.netapp.com for the latest.

Sommario

- Guida all'implementazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190 1
 - NVA-1142-DEPLOY: FlexPod Express con Cisco UCS C-Series e NetApp AFF C190 Series - implementazione NVA 1
 - Panoramica della soluzione 1
 - Requisiti tecnologici 4
 - Informazioni di cablaggio FlexPod Express 5
 - Procedure di implementazione 8
 - Conclusione 95
 - Ringraziamenti 96
 - Dove trovare ulteriori informazioni 96
 - Cronologia delle versioni 96

Guida all'implementazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190

NVA-1142-DEPLOY: FlexPod Express con Cisco UCS C-Series e NetApp AFF C190 Series - implementazione NVA

Savita Kumari, NetApp

Le tendenze del settore indicano che sta avvenendo una grande trasformazione del data center verso l'infrastruttura condivisa e il cloud computing. Inoltre, le organizzazioni cercano una soluzione semplice ed efficace per uffici remoti e filiali che utilizzi tecnologie che conoscono nel proprio data center.

FlexPod® Express è un'architettura di data center pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco (Cisco UCS), sulla famiglia di switch Cisco Nexus e sulle tecnologie di storage NetApp®. I componenti di un sistema FlexPod Express sono simili alle controparti del data center FlexPod, consentendo sinergie di gestione nell'intero ambiente dell'infrastruttura IT su scala ridotta. FlexPod Datacenter e FlexPod Express sono piattaforme ottimali per la virtualizzazione e per i sistemi operativi bare-metal e i carichi di lavoro aziendali.

FlexPod Datacenter e FlexPod Express offrono una configurazione di base e hanno la flessibilità di essere dimensionati e ottimizzati per adattarsi a diversi casi di utilizzo e requisiti. Gli attuali clienti di FlexPod Datacenter possono gestire il proprio sistema FlexPod Express con gli strumenti a cui sono abituati. I nuovi clienti FlexPod Express possono facilmente passare alla gestione del data center FlexPod man mano che il loro ambiente cresce.

FlexPod Express è una base infrastrutturale ottimale per uffici remoti e filiali e per piccole e medie imprese. Si tratta inoltre di una soluzione ottimale per i clienti che desiderano fornire un'infrastruttura per un carico di lavoro dedicato.

FlexPod offre un'infrastruttura facile da gestire, adatta a quasi tutti i carichi di lavoro.

Panoramica della soluzione

Questa soluzione FlexPod Express fa parte del programma di infrastruttura convergente FlexPod.

Programma di infrastruttura convergente FlexPod

Le architetture di riferimento FlexPod vengono fornite come Cisco Validated Design (CVD) o NetApp Verified Architectures (NVA). Sono consentite deviazioni in base ai requisiti del cliente rispetto a un determinato CVD o NVA se queste variazioni non creano una configurazione non supportata.

Il programma FlexPod include due soluzioni: FlexPod Express e FlexPod Datacenter.

- **FlexPod Express.** offre ai clienti una soluzione entry-level con tecnologie Cisco e NetApp.
- **FlexPod Datacenter.** offre una base polivalente ottimale per diversi carichi di lavoro e applicazioni.

The FlexPod Portfolio

A prevalidated, flexible platform that features



FlexPod® Express

Remote office or branch office, retail, small and midsize business, and edge



FlexPod Datacenter

Enterprise apps, unified infrastructure, and virtualization

11

Programma NetApp Verified Architecture

Il programma NetApp Verified Architecture offre ai clienti un'architettura verificata per le soluzioni NetApp. Un'architettura verificata di NetApp offre un'architettura della soluzione NetApp con le seguenti qualità:

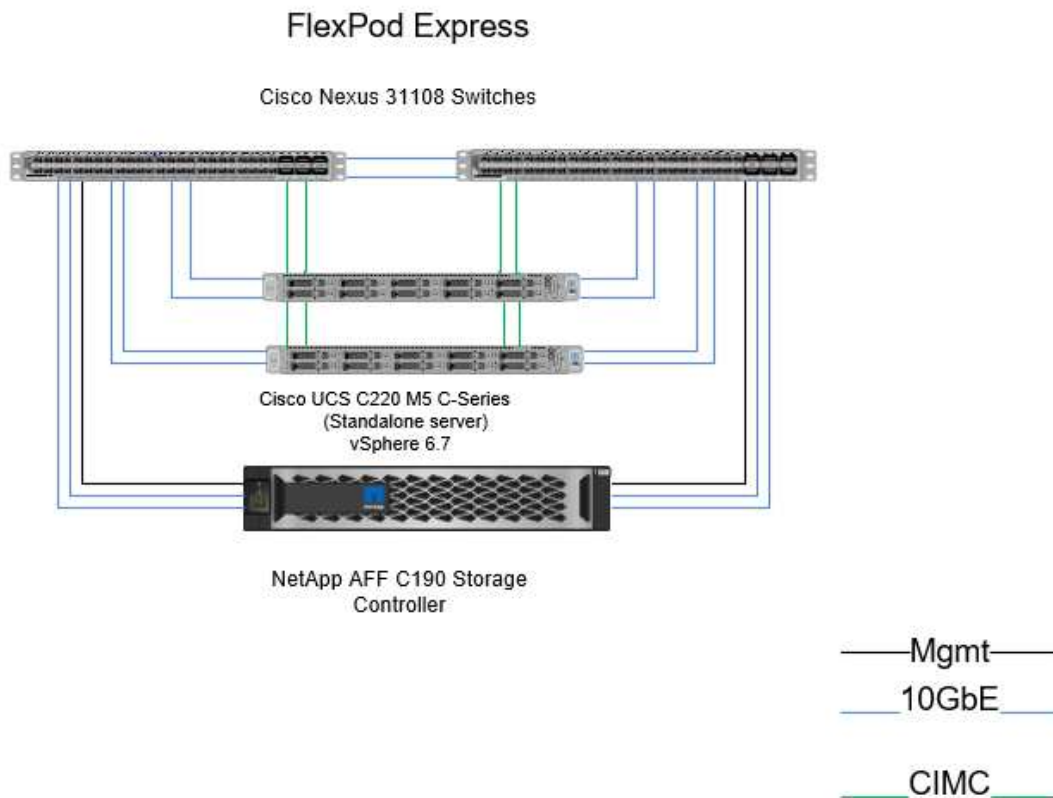
- Testato a fondo
- Prescrittivo in natura
- Rischi di implementazione ridotti al minimo
- Accelerazione del time-to-market

In questa guida viene illustrato in dettaglio il design di FlexPod con VMware vSphere. Inoltre, questo design utilizza il nuovissimo sistema AFF C190 (con NetApp ONTAP® 9.6), Cisco Nexus 31108 e i server Cisco UCS C-Series C220 M5 come nodi hypervisor.

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. Questa soluzione include il nuovo NetApp AFF C190 con ONTAP 9.6, due switch Cisco Nexus 31108 e server rack Cisco UCS C220 M5

con VMware vSphere 6.7U2. Questa soluzione validata utilizza la tecnologia 10 GbE. Viene inoltre fornita una guida su come scalare la capacità di calcolo aggiungendo due nodi hypervisor alla volta, in modo che l'architettura FlexPod Express possa adattarsi alle esigenze di business in evoluzione di un'organizzazione.



Per utilizzare in modo efficiente le quattro porte 10GbE fisiche del VIC 1457, creare due collegamenti aggiuntivi da ciascun server agli switch rack superiori.

Riepilogo del caso d'utilizzo

La soluzione FlexPod Express può essere applicata a diversi casi di utilizzo, tra cui:

- Uffici remoti o filiali
- Piccole e medie imprese
- Ambienti che richiedono una soluzione dedicata e conveniente

FlexPod Express è la soluzione ideale per carichi di lavoro misti e virtualizzati. Sebbene questa soluzione sia stata validata con vSphere 6.7U2, supporta qualsiasi versione vSphere qualificata con gli altri componenti dal NetApp Interoperability Matrix Tool. NetApp consiglia di implementare vSphere 6.7U2 per via delle correzioni e delle funzionalità avanzate, come ad esempio:

- Nuovo supporto del protocollo per il backup e il ripristino di un'appliance server vCenter, inclusi HTTP, HTTPS, FTP, FTPS, SCP, NFS E SMB.
- Nuovo dal punto di vista funzionale quando si utilizza la libreria di contenuti. La sincronizzazione dei modelli VM nativi tra le librerie di contenuti è ora disponibile quando vCenter Server è configurato per la

modalità link avanzata.

- Una pagina aggiornata del plug-in del client.
- Miglioramenti aggiunti in vSphere Update Manager (VUM) e nel client vSphere. È ora possibile eseguire le azioni di collegamento, verifica della conformità e correzione, il tutto da un'unica schermata.

Per ulteriori informazioni su questo argomento, vedere ["Pagina vSphere 6.7U2"](#) e a. ["VCenter Server 6.7U2 - Note di release"](#).

Requisiti tecnologici

Un sistema FlexPod richiede una combinazione di componenti hardware e software. FlexPod Express descrive inoltre i componenti hardware necessari per aggiungere nodi hypervisor al sistema in unità di due.

Requisiti hardware

Indipendentemente dall'hypervisor scelto, tutte le configurazioni FlexPod utilizzano lo stesso hardware. Pertanto, anche se i requisiti di business cambiano, è possibile utilizzare un hypervisor diverso sullo stesso hardware FlexPod Express.

La seguente tabella elenca i componenti hardware necessari per la configurazione e l'implementazione di FlexPod Express. I componenti hardware utilizzati in qualsiasi implementazione della soluzione possono variare in base ai requisiti del cliente.

Hardware	Quantità
Cluster a due nodi AFF C190	1
Server Cisco C220 M5	2
Switch Cisco Nexus 31108PC-V.	2
Cisco UCS Virtual Interface Card (VIC) 1457 per server rack Cisco UCS C220 M5	2

Questa tabella elenca l'hardware richiesto oltre alla configurazione di base per l'implementazione di 10GbE.

Hardware	Quantità
Server Cisco UCS C220 M5	2
Cisco VIC 1457	2

Requisiti software

La seguente tabella elenca i componenti software necessari per implementare le architetture delle soluzioni FlexPod Express.

Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	4.0.4	Per server rack Cisco UCS C220 M5

Software	Versione	Dettagli
Driver Cisco Nenic	1.0.0.29	Per le schede di interfaccia VIC 1457
Sistema operativo Cisco NX	7.0(3)I7(6)	Per switch Cisco Nexus 31108PC-V.
NetApp ONTAP	9.6	Per controller AFF C190

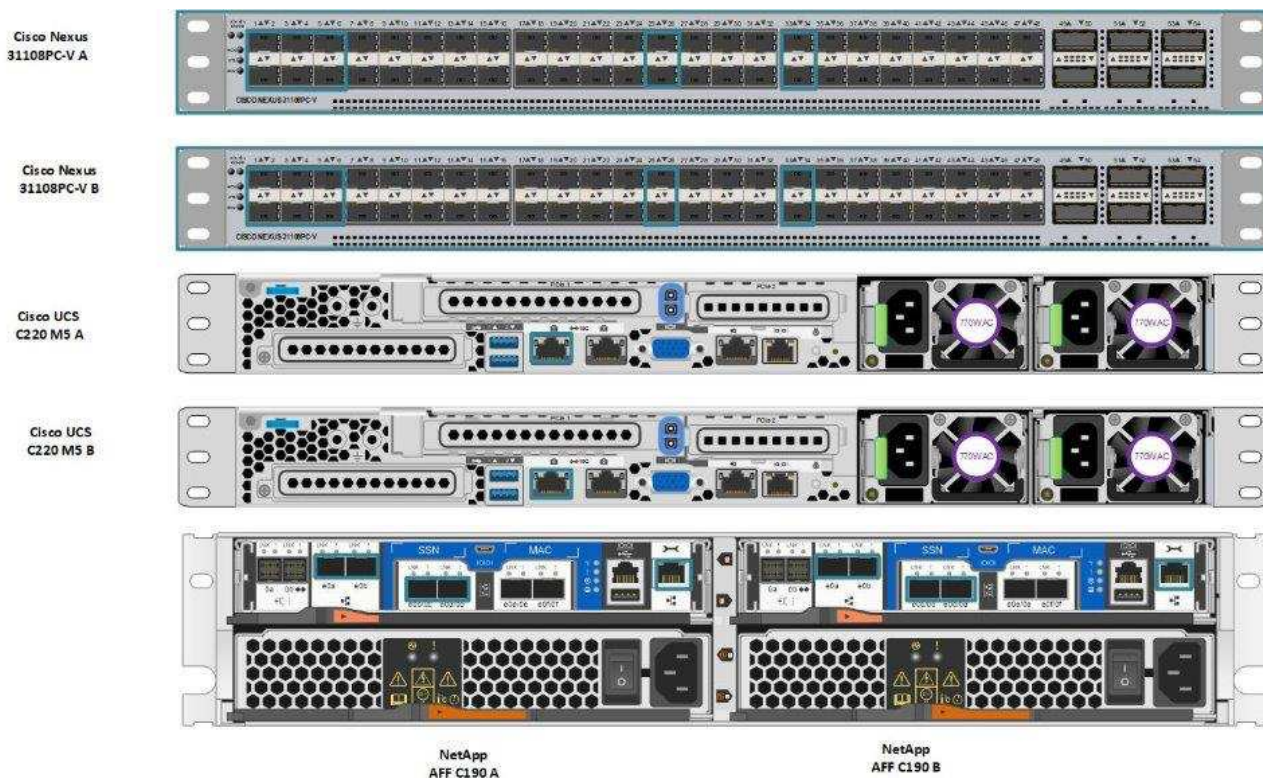
Questa tabella elenca il software necessario per tutte le implementazioni di VMware vSphere su FlexPod Express.

Software	Versione
Appliance server VMware vCenter	6.7U2
Hypervisor VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI per ESXi	1.1.2
NetApp VSC	9.6

Informazioni di cablaggio FlexPod Express

Questa convalida di riferimento è cablata come mostrato nelle figure e nelle tabelle seguenti.

Questa figura mostra il cablaggio di convalida di riferimento.



La seguente tabella elenca le informazioni di cablaggio per lo switch Cisco Nexus 31108PC-V-A.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 31108PC-V A	Eth1/1	Storage controller NetApp AFF C190 A	e0c
	Eth1/2	Storage controller NetApp AFF C190 B	e0c
	Eth1/3	Server standalone Cisco UCS C220 C-Series A	MLOM0
	Eth1/4	Server standalone Cisco UCS C220 C-Series B	MLOM0
	Eth1/5	Server standalone Cisco UCS C220 C-Series A	MLOM1
	Eth1/6	Server standalone Cisco UCS C220 C-Series B	MLOM1
	Eth1/25	Switch Cisco Nexus 31108PC-V B	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108PC-V B	Eth1/26
	Eth1/33	Storage controller NetApp AFF C190 A	E0M
	Eth1/34	Server standalone Cisco UCS C220 C-Series A	CIMC (FEX135/1/25)

Questa tabella elenca le informazioni di cablaggio per lo switch Cisco Nexus 31108PC-V- B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 31108PC-V B	Eth1/1	Storage controller NetApp AFF C190 A	e0d
	Eth1/2	Storage controller NetApp AFF C190 B	e0d
	Eth1/3	Server standalone Cisco UCS C220 C-Series A	MLOM2
	Eth1/4	Server standalone Cisco UCS C220 C-Series B	MLOM2
	Eth1/5	Server standalone Cisco UCS C220 C-Series A	MLOM3
	Eth1/6	Server standalone Cisco UCS C220 C-Series B	MLOM3
	Eth1/25	Switch Cisco Nexus 31108 A.	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108 A.	Eth1/26
	Eth1/33	Storage controller NetApp AFF C190 B	E0M
	Eth1/34	Server standalone Cisco UCS C220 C-Series B	CIMC (FEX135/1/26)

Questa tabella elenca le informazioni di cablaggio per lo storage controller NetApp AFF C190 A.

Dispositivo locale	Local Port (porta locale)	Dispositivo remoto	Porta remota
Storage controller NetApp AFF C190 A	e0a	Storage controller NetApp AFF C190 B	e0a
	e0b	Storage controller NetApp AFF C190 B	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/1
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/1
	E0M	Switch Cisco Nexus 31108PC-V A	Eth1/33

Questa tabella elenca le informazioni di cablaggio per il controller di storage NetApp AFF C190 B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Storage controller NetApp AFF C190 B	e0a	Storage controller NetApp AFF C190 A	e0a
	e0b	Storage controller NetApp AFF C190 A	e0b
	e0c	Switch Cisco Nexus 31108PC-V A	Eth1/2
	e0d	Switch Cisco Nexus 31108PC-V B	Eth1/2
	E0M	Switch Cisco Nexus 31108PC-V B	Eth1/33

Procedure di implementazione

Panoramica

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> network port vlan create -node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

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 seguente tabella 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.

Nome VLAN	Scopo della VLAN	ID VLAN	
VLAN di gestione	VLAN per le interfacce di gestione	3437	VSwitch0
VLAN NFS	VLAN per traffico NFS	3438	VSwitch0
VLAN VMware vMotion	VLAN designata per lo spostamento delle macchine virtuali (VM) da un host fisico all'altro	3441	VSwitch0
VLAN del traffico delle macchine virtuali	VLAN per il traffico delle applicazioni VM	3442	VSwitch0
ISCSI-A-VLAN	VLAN per il traffico iSCSI sul fabric A.	3439	IScsiBootvSwitch
ISCSI-B-VLAN	VLAN per il traffico iSCSI sul fabric B.	3440	IScsiBootvSwitch
VLAN nativa	VLAN a cui sono assegnati frame senza tag	2	

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).

In questa convalida sono stati creati due vSwitch.

La seguente tabella elenca i vSwitch della soluzione.

Nome vSwitch	Adattatori attivi	Porte	MTU	Bilanciamento del carico
VSwitch0	Vmnic2, vmnic4	predefinito (120)	9000	Routing basato su hash IP
IScsiBootvSwitch	Vmnic3, vmnic5	predefinito (120)	9000	Routing basato sull'ID della porta virtuale di origine.



Il metodo hash IP per il bilanciamento del carico richiede una configurazione appropriata per lo switch fisico sottostante utilizzando SRC-DST-IP EtherChannel con un canale porta statico (mode on). In caso di connettività intermittente a causa di una possibile errata configurazione dello switch, chiudere temporaneamente una delle due porte uplink associate sullo switch Cisco per ripristinare la comunicazione con la porta vmkernel di gestione ESXi, durante la risoluzione dei problemi relativi alle impostazioni del canale porta.

La tabella seguente elenca le macchine virtuali VMware create.

Descrizione della macchina virtuale	Nome host
VMware vCenter Server	FlexPod-VCSA
Virtual Storage Console	FlexPod-VSC

Implementare Cisco Nexus 31108PC-V.

Questa sezione descrive in dettaglio la configurazione dello switch Cisco Nexus 31108PC-V utilizzata in un ambiente FlexPod Express.

Configurazione iniziale dello switch Cisco Nexus 31108PC-V.

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 31108PC-V con la versione software NX-OS 7.0(3)I7(6).

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 31108PC-V possono essere collegate a una rete di gestione esistente oppure le interfacce mgmt0 degli switch 31108PC-V 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 31108PC-V FlexPod Express sono collegati a una rete di gestione esistente.

3. Per configurare gli switch Cisco Nexus 31108PC-V, 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 : 31108PC-V-B

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: y

Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>

Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>

Configure advanced IP options? (yes/no) [n]: n

Enable the telnet service? (yes/no) [n]: n

Enable the ssh service? (yes/no) [y]: y

Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

Number of rsa key bits <1024-2048> [1024]: <enter>

Configure the ntp server? (yes/no) [n]: y

NTP server IPv4 address : <<var_ntp_ip>>

Configure default interface layer (L3/L2) [L2]: <enter>

Configure default switchport interface state (shut/noshut) [noshut]: <enter>

Configure CoPP system profile (strict/moderate/lenient/dense) [strict]: <enter>

4. 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.

Attivare le funzioni avanzate

Alcune funzionalità avanzate devono essere attivate in Cisco NX-OS per fornire ulteriori opzioni di configurazione. Per abilitare le funzioni appropriate sugli switch Cisco Nexus A e B, 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.

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
```

Configurare lo 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 predefinito e BPDU Guard, sugli switch Cisco Nexus A e B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

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) di ciascuno switch, immettere le seguenti descrizioni delle porte per la configurazione grande di FlexPod Express:

Switch Cisco Nexus A

```

int eth1/1
    description AFF C190-A e0c
int eth1/2
    description AFF C190-B e0c
int eth1/3
    description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
    description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
    description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
    description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
    description vPC peer-link 31108PC-V-B 1/25
int eth1/26
    description vPC peer-link 31108PC-V-B 1/26
int eth1/33
    description AFF C190-A e0M
int eth1/34
    description UCS Server A: CIMC

```

Switch Cisco Nexus B

```

int eth1/1
    description AFF C190-A e0d
int eth1/2
    description AFF C190-B e0d
int eth1/3
    description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
    description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
    description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
    description vPC peer-link 31108PC-V-A 1/25
int eth1/26
    description vPC peer-link 31108PC-V-A 1/26
int eth1/33
    description AFF C190-B e0M
int eth1/34
    description UCS Server B: CIMC

```


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
```

Eeguire 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 di livello 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 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-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

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
  delay-restore 150
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start

```

Configurare i canali della porta 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 sugli 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

```

Configurare le connessioni del server

I server Cisco UCS dispongono di una scheda di interfaccia virtuale a quattro porte, VIC1457, 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 della porta per le interfacce collegate a ciascun server.

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

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

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

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Configurare i canali delle porte del server

Eeguire i seguenti comandi sullo switch A e B per configurare i canali delle porte per il server-A:

```

int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut

```

Eseguire i seguenti comandi sullo switch A e B per configurare i canali delle porte per il server B:

```

int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut

```



Per la convalida di questa soluzione è stato utilizzato un MTU di 9000. Tuttavia, è possibile configurare un valore diverso per la MTU appropriato per i requisiti dell'applicazione. È importante impostare lo stesso valore MTU nella soluzione FlexPod. Le configurazioni MTU errate tra i componenti comportano l'interruzione dei pacchetti e la loro nuova trasmissione, con un conseguente impatto 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 in un'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 31108 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 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 AFF serie C190

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:

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.

In alternativa, per confrontare i componenti in base all'appliance di storage, fare clic su Confronta sistemi di storage.

Prerequisiti della serie AFFC190 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
- Porte e cavi integrati

Controller di storage

Seguire le procedure di installazione fisica per i controller in AFF ["C190"](#) Documentazione.

NetApp ONTAP 9.6

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 per la configurazione è disponibile nella Guida all'installazione del software ONTAP 9.6.



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

La seguente tabella fornisce informazioni sull'installazione e sulla configurazione di ONTAP 9.6.

Dettaglio del cluster	Valore dei dettagli del cluster
Indirizzo IP del nodo cluster A.	[var_nodeA_mgmt_ip]
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 9.6	[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...
```

Consentire l'avvio del sistema.

```
autoboot
```

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



Se ONTAP 9.6 non è la versione del software da avviare, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9.6 è la versione da avviare, selezionare l'opzione 8 e y per riavviare il nodo. Quindi, passare alla fase 14.

3. Per installare il nuovo software, selezionare l'opzione 7.
4. Immettere y per eseguire un aggiornamento.
5. Selezionare e0M come porta di rete da utilizzare per il download.
6. Immettere y per riavviare ora.
7. 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>>
```

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



Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

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

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

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 9.6 non è la versione del software da avviare, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9.6 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.A.
5. Immettere y per eseguire un aggiornamento.
6. Selezionare e0M come porta di rete da utilizzare per il download.
7. Immettere 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. Immettere y per impostare il software appena installato come predefinito da utilizzare per i riavvii successivi.
12. Immettere 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. Immettere y per azzerare i dischi, ripristinare la configurazione e installare un nuovo file system.
16. Inserire 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 9.6 viene avviato sul nodo per la prima volta.



La procedura di configurazione del nodo e del cluster è stata leggermente modificata in ONTAP 9.6. La configurazione guidata del cluster viene ora utilizzata per configurare il primo nodo di un cluster e per configurare il cluster viene utilizzato il gestore di sistema NetApp ONTAP (in precedenza OnCommand® System Manager).

1. Seguire le istruzioni per configurare 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 mediante la configurazione guidata di 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 10.63.172.162 Nel campo Primary NTP Server (Server NTP primario).



È inoltre possibile inserire un server NTP alternativo. L'indirizzo IP 10.63.172.162 da <<var_ntp_server_ip>> È l'IP di gestione Nexus.

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.

Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:



? AutoSupport ☒

? Proxy URL (Optional)

i Connection is verified after configuring AutoSupport on all nodes.

? Event Notifications

Notify me through:



Email

SMTP Mail Host

Email Addresses

Separate email addresses with a comma...



SNMP

SNMP Trap Host



Syslog

Syslog Server

Submit

Quando il sistema indica 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 integrate

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

```
AFF C190::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
AFF C190_A	0c	cna	target	-	-	online
AFF C190_A	0d	cna	target	-	-	online
AFF C190_A	0e	cna	target	-	-	online
AFF C190_A	0f	cna	target	-	-	online
AFF C190_B	0c	cna	target	-	-	online
AFF C190_B	0d	cna	target	-	-	online
AFF C190_B	0e	cna	target	-	-	online
AFF C190_B	0f	cna	target	-	-	online

8 entries were displayed.

2. Verificare che la modalità corrente delle porte in uso sia `cna` e che il tipo corrente sia impostato su destinazione. 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

Per rinominare le LIF (Management Logical Interface), 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 C190_B_1 -newname AFF C190-02_mgmt1
```

Impostare il revert automatico sulla gestione del cluster

Impostare il parametro di 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 processore di servizio

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:` indica che uno dei controller non ha ricevuto gli avvisi `hwassist keep alive` dal proprio partner, indicando 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 il gruppo di interfacce LACP in ONTAP

Questo tipo di gruppo di interfacce richiede due o più interfacce Ethernet e uno switch che supporti LACP. assicurarsi che sia configurato in base ai passaggi descritti in questa guida nella sezione 5.1.

Dal prompt del cluster, completare i seguenti passaggi:

```

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 ONTAP

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

```

AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
        this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
        this network port.
Do you want to continue? {y|n}: y

```

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 di dati 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 quando `aggr1_NodeA` non sarà 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 di 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,fc
```

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 precediti da `vserver` Nella riga di comando perché le SVM erano precedentemente chiamate Vserver.

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	<code>[var_esxi_hostA_nfs_ip]</code>
ESXi host B NFS IP address (Indirizzo IP NFS host B ESXi)	<code>[var_esxi_hostB_nfs_ip]</code>

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 il servizio iSCSI in ONTAP

Per creare il servizio iSCSI su SVM, eseguire il seguente comando. 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

Per creare un mirror di condivisione del carico del volume root SVM in ONTAP, attenersi alla seguente procedura:

1. Creare un volume come mirror per la 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 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Per ottenere i valori dei parametri richiesti nella fase successiva, eseguire il comando `show` del certificato di protezione.
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 -ssl3-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 alla SVM di essere disponibile sul web.

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

Creare un volume NetApp FlexVol in ONTAP

Per creare un volume NetApp FlexVol®, immettere il nome, le dimensioni e l'aggregato del volume 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 -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

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]

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]

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 un amministratore SVM dell'infrastruttura

La seguente tabella elenca le informazioni necessarie per aggiungere un amministratore SVM.

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
```

"Implementazione del server rack Cisco UCS C-Series."

Implementare il server rack Cisco UCS C-Series

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

Eeguire la configurazione iniziale del server standalone Cisco UCS C-Series per CIMC

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 4.0.(4).

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.

Accendere il server e premere F8 quando richiesto per accedere alla configurazione CIMC.



Copyright (c) 2019 Cisco Systems, Inc.

Press <F2> BIOS Setup : <F6> Boot Menu : <F7> Diagnostics
Press <F8> CIMC Setup : <F12> Network Boot
Bios Version : C220M5.4.0.4g.0.0712190011
Platform ID : C220M5

Processor(s) Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Total Memory = 64 GB Effective Memory = 64 GB
Memory Operating Speed 2400 Mhz
M.2 SWRAID configuration is not detected. Switching to AHCI mode.

Cisco IMC IPv4 Address : 10.63.172.160
Cisco IMC MAC Address : 70:69:5A:B5:8D:68

Entering CIMC Configuration Utility ...

92

2. Nell'utility di configurazione di CIMC, impostare le seguenti opzioni:

a. Modalità scheda di interfaccia di rete (NIC):

Dedicato ☒

b. IP (di base):

IPV4: ☒

DHCP attivato: ☐

IP CIMC: <<cimc_ip>>

Prefisso/sottorete: <<cimc_netmask>>

Gateway: <<cimc_gateway>>

c. VLAN (Advanced): Lasciare deselezionato per disattivare il tagging VLAN.

Ridondanza della NIC

Nessuno: ☒

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:          [X]
Shared LOM:     [ ]                   Active-standby: [ ]
Cisco Card:     [ ]                   Active-active:  [ ]
  Riser1:       [ ]                   VLAN (Advanced)
  Riser2:       [ ]                   VLAN enabled:   [ ]
  MLom:         [ ]                   VLAN ID:       1
  Shared LOM Ext: [ ]                   Priority:      0
IP (Basic)
IPv4:           [X]                   IPv6:          [ ]
DHCP enabled    [ ]
CIMC IP:        10.63.172.160
Prefix/Subnet:  255.255.255.0
Gateway:        10.63.172.1
Pref DNS Server: 0.0.0.0
Smart Access USB
Enabled         [ ]
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings

```

3. Premere F1 per visualizzare le impostazioni aggiuntive:

a. Proprietà comuni:

Nome host: <<esxi_host_name>>

DNS dinamico: []

Impostazioni predefinite: Lasciare deselezionato.

b. 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.

4. Premere F10 per salvare la configurazione dell'interfaccia CIMC.

5. Una volta salvata la configurazione, premere Esc per uscire.

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

In questa configurazione FlexPod Express, VIC1457 viene utilizzato per l'avvio iSCSI.

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



Un font corsivo indica le variabili univoche per ogni 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]
Indirizzo IP iscsi_lif01a	[var_iscsi_lif01a]
Indirizzo IP iscsi_lif02a	[var_iscsi_lif02a]
Indirizzo IP iscsi_lif01b	[var_iscsi_lif01b]
Indirizzo IP iscsi_lif02b	[var_iscsi_lif02b]
Infra_SVM IQN	[var_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 Compute (calcolo) e selezionare BIOS.
2. Fare clic su Configure Boot Order (Configura ordine di avvio), quindi su OK.

Cisco Integrated Management Controller

[Home](#) / [Compute](#) / [BIOS](#) ★

[BIOS](#)
[Remote Management](#)
[Troubleshooting](#)
[Power Policies](#)
[PID Catalog](#)

[Enter BIOS Setup](#) | [Clear BIOS CMOS](#) | [Restore Manufacturing Custom Settings](#) | [Restore Defaults](#)

[Configure BIOS](#)
[Configure Boot Order](#)
[Configure BIOS Profile](#)

BIOS Properties

Running Version

C220M5.4.0.4g.0.0712190011

UEFI Secure Boot

☐

Actual Boot Mode

Uefi

Configured Boot Mode

▼

Last Configured Boot Order Source

BIOS

Configured One time boot device

▼

Save Changes

▼ Configured Boot Devices

Basic

▶

Advanced

Actual Boot Devices

UEFI: Built-in EFI Shell (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

UEFI: PXE IP4 Intel(R) Ethernet Controller X550 (NonPolicyTarget)

Configure Boot Order

3. Configurare i seguenti dispositivi facendo clic su Device (dispositivo) sotto Add Boot Device (Aggiungi dispositivo di avvio) e selezionando la scheda Advanced (Avanzate):

a. Aggiungi supporti virtuali:

NOME: KVM-CD-DVD

SOTTOTIPO: DVD MAPPATO KVM

Stato: Attivato

Ordine: 1

b. Aggiunta dell'avvio iSCSI:

Nome: ISCSI-A.

Stato: Attivato

Ordine: 2

Slot: MLOM

Porta: 1

c. Fare clic su Add iSCSI Boot:

Nome: iSCSI-B.

Stato: Attivato

Ordine: 3

Slot: MLOM

Porta: 3

4. Fare clic su Aggiungi dispositivo.

5. Fare clic su Save Changes (Salva modifiche), quindi su Close (Chiudi)

Configure Boot Order

Configured Boot Level: Advanced

Basic Advanced

Add Boot Device

- Add Local HDD
- Add PXE Boot
- Add SAN Boot
- Add iSCSI Boot
- Add USB
- Add Virtual Media
- Add PCHStorage
- Add UEFISHELL
- Add SD Card
- Add NVME
- Add Local CDD

Advanced Boot Order Configuration

Selected 1 / Total 3

	Name	Type	Order	State
<input checked="" type="checkbox"/>	KVM-MAPPED-DVD	VMEDIA	1	Enabled
<input type="checkbox"/>	iSCSI-A	ISCSI	2	Enabled
<input type="checkbox"/>	iSCSI-B	ISCSI	3	Enabled

Save Changes Reset Values Close

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. Nella scheda Compute (calcolo), 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).

BIOS	Remote Management	Troubleshooting	Power Policies	PID Catalog	
I/O	Server Management	Security	Processor	Memory	Power/Performance

Note: Default values are shown in bold.

Reboot Host Immediately: ☒

Intel VT for directed IO:	Enabled ▼
Intel VTD ATS support:	Enabled ▼
LOM Port 1 OptionRom:	Enabled ▼
Pcie Slot 1 OptionRom:	Disabled ▼
MLOM OptionRom:	Enabled ▼
Front NVME 1 OptionRom:	Enabled ▼
MRAID Link Speed:	Auto ▼
PCIe Slot 1 Link Speed:	Auto ▼
Front NVME 1 Link Speed:	Auto ▼
VGA Priority:	Onboard ▼
P-SATA OptionROM:	LSI SW RAID ▼
USB Port Rear:	Enabled ▼
USB Port Internal:	Enabled ▼
IPv6 PXE Support:	Disabled ▼

Legacy USB Support:	Enabled ▼
Intel VTD coherency support:	Disabled ▼
All Onboard LOM Ports:	Enabled ▼
LOM Port 2 OptionRom:	Enabled ▼
Pcie Slot 2 OptionRom:	Disabled ▼
MRAID OptionRom:	Enabled ▼
Front NVME 2 OptionRom:	Enabled ▼
MLOM Link Speed:	Auto ▼
PCIe Slot 2 Link Speed:	Auto ▼
Front NVME 2 Link Speed:	Auto ▼
M.2 SATA OptionROM:	AHCI ▼
USB Port Front:	Enabled ▼
USB Port KVM:	Enabled ▼
USB Port:M.2 Storage:	Enabled ▼

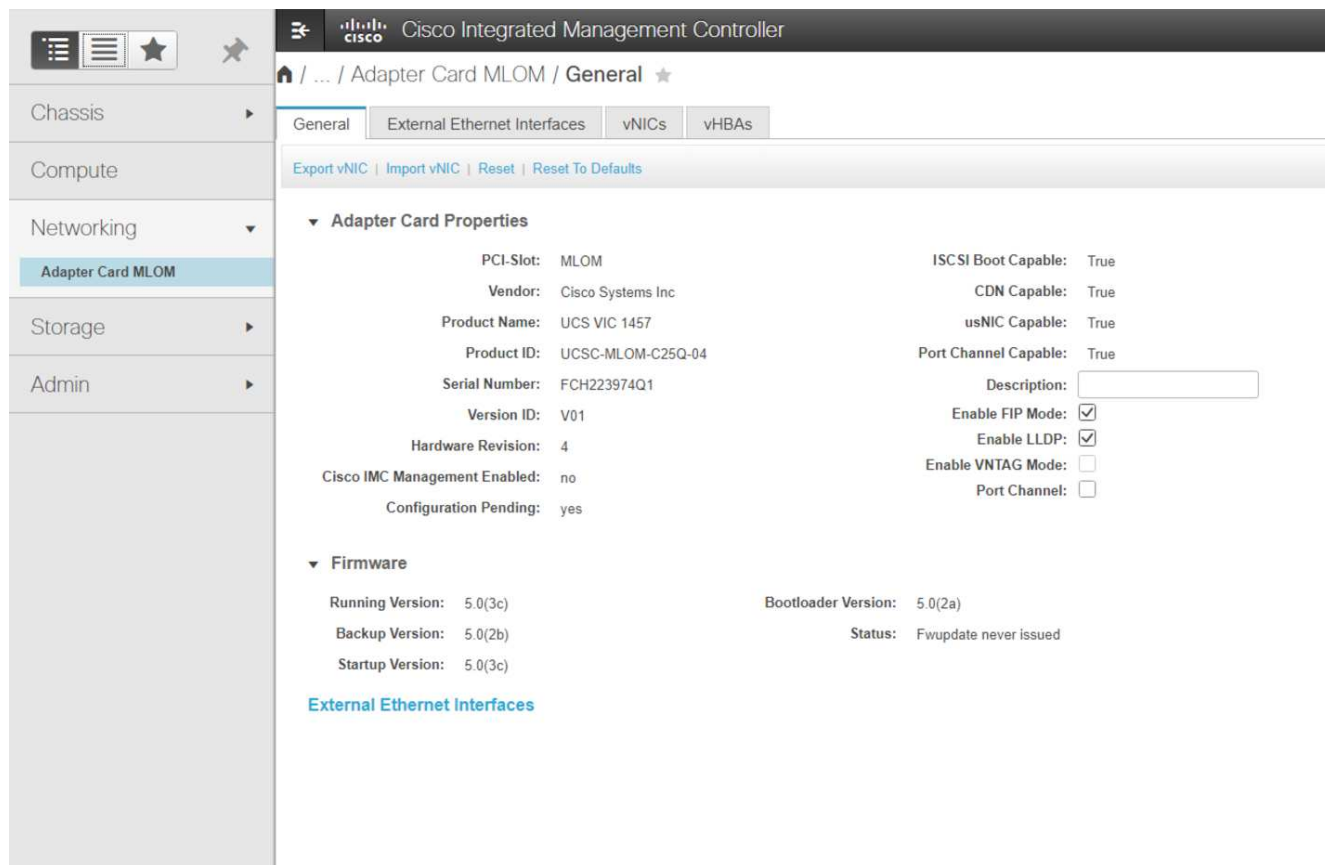
Configurare Cisco VIC1457 per l'avvio iSCSI

La seguente procedura di configurazione riguarda Cisco VIC 1457 per l'avvio iSCSI.



Prima di poter configurare le quattro porte singole, è necessario disattivare il canale predefinito delle porte 0, 1, 2 e 3. Se il port channeling non è disattivato, vengono visualizzate solo due porte per il VIC 1457. Per attivare il canale della porta sul CIMC, attenersi alla procedura riportata di seguito:

1. Nella scheda rete, fare clic su MLOM scheda adattatore.
2. Nella scheda General (Generale), deselezionare il canale della porta.
3. Salvare le modifiche e riavviare CIMC.



Creare vNIC iSCSI

Per creare vNIC iSCSI, attenersi alla seguente procedura:

1. Nella scheda rete, fare clic su scheda adattatore MLOM.
2. Fare clic su Add vNIC (Aggiungi vNIC) per creare una vNIC.
3. Nella sezione Add vNIC (Aggiungi vNIC), immettere le seguenti impostazioni:
 - Nome: Eth1
 - Nome CDN: iSCSI-vNIC-A.
 - MTU: 9000
 - VLAN predefinita: <<var_iscsi_vlan_a>>
 - Modalità VLAN: TRUNK
 - Enable PXE boot (attiva avvio PXE): Controllare
4. Fare clic su Add vNIC (Aggiungi vNIC), quindi su OK.
5. Ripetere la procedura per aggiungere una seconda vNIC:
 - Assegnare un nome alla vNIC eth3.
 - Nome CDN: iSCSI-vNIC-B.
 - Invio <<var_iscsi_vlan_b>> Come VLAN.
 - Impostare la porta uplink su 3.

▼ General

Name:

CDN:

MTU: (1500 - 9000)

Uplink Port: ▼

MAC Address: ☐ Auto
☒

Class of Service: (0 - 6)

Trust Host CoS: ☐

PCI Order: (0 - 7)

Default VLAN: ☐ None
☒ ?

6. Selezionare la vNIC eth1 a sinistra.

General External Ethernet Interfaces **vNICs** vHBAs

▼ vNICs

- eth0
- eth1**
- eth2
- eth3

► vNIC Properties

▼ iSCSI Boot Properties

► General

▼ Initiator

Name: (0 - 222) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

► Primary Target

► Secondary Target

Unconfigure iSCSI Boot

7. 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>>

▼ vNICs
eth0
eth1
eth2
eth3

► vNIC Properties

▼ iSCSI Boot Properties

► General

▼ Initiator

Name: (0 - 222) chars

IP Address:

Subnet Mask:

Gateway:

Primary DNS:

Initiator Priority:

Secondary DNS:

TCP Timeout: (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Primary Target

Name: (0 - 222) chars

IP Address:

TCP Port:

Boot LUN: (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

▼ Secondary Target

Name: (0 - 222) chars

IP Address:

TCP Port:

Boot LUN: (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

[Unconfigure iSCSI Boot](#)

8. 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

9. Inserire i dettagli del target secondario:

- 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. Inoltre, i nomi IQN per gli iniziatori devono essere univoci per ciascun server e per iSCSI vNIC.

10. Fare clic su Salva modifiche.

11. Selezionare vNIC eth3 e fare clic sul pulsante iSCSI Boot (Avvio iSCSI) situato nella parte superiore della sezione host Ethernet Interfaces (interfacce Ethernet host).

12. Ripetere la procedura per configurare eth3.

13. 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>>

The screenshot shows the 'vNIC Properties' configuration page for vNIC eth3. The 'iSCSI Boot Properties' section is expanded, showing the 'Initiator' and 'Primary Target' configurations. The 'Initiator' section includes fields for Name (iqn.1992-01.com.cisco.ucsa-02), IP Address (172.21.184.110), Subnet Mask (255.255.255.0), Gateway (172.21.184.1), and Primary DNS. The 'Primary Target' section includes fields for Name (iqn.1992-08.com.netapp.sn.e42fa6b2d2), IP Address (172.21.184.105), and TCP Port (3260). The 'Secondary Target' section is also visible with similar fields. On the right side, there are dropdown menus for Initiator Priority (set to 'primary') and checkboxes for Boot LUN, CHAP Name, and CHAP Secret.

14. 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

15. Inserire i dettagli del target secondario:

- 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.

16. Fare clic su Salva modifiche.

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

Configurare vNIC per ESXi

Per configurare le vNIC per ESXi, attenersi alla seguente procedura:

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 rete > scheda adattatore MLOM, selezionare la scheda vNIC, quindi selezionare le vNIC sottostanti.
3. Selezionare eth0 e fare clic su Proprietà.
4. Impostare MTU su 9000. Fare clic su Salva modifiche.
5. Impostare la VLAN sulla VLAN 2 nativa.

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

vNICs

- eth0
- eth1
- eth2
- eth3

vNIC Properties

General

Name: eth0

CDN: VIC-MLOM-eth0

MTU: 9000 (1500 - 9000)

Uplink Port: 0

MAC Address: ☐ Auto ☒ F8:0F:6F:89:26:CE

Class of Service: 0 (0 - 6)

Trust Host CoS: ☐

PCI Order: 0 (0 - 7)

Default VLAN: ☐ None ☒ 2

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

Cisco Integrated Management Controller

Home / ... / Adapter Card MLOM / vNICs

General External Ethernet Interfaces **vNICs** vHBAs

vNICs

- eth0
- eth1
- eth2
- eth3

Host Ethernet Interfaces

Selected 0 / Total 4

Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode	iSCSI Boot	PXE Boot	Channel	Port Profile	Uplink Failover
<input type="checkbox"/> eth0	VIC-MLO...	F8:0F:6F:89:26:CE	9000	0	0	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth1	VIC-ISC...	F8:0F:6F:89:26:CF	9000	0	1	0	3439	TRUNK	enabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth2	VIC-MLO...	F8:0F:6F:89:26:D0	9000	0	2	0	2	TRUNK	disabled	enabled	N/A	N/A	N/A
<input type="checkbox"/> eth3	VIC-ISC...	F8:0F:6F:89:26:D1	9000	0	3	0	3440	TRUNK	enabled	enabled	N/A	N/A	N/A



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

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

Procedura di implementazione dello storage NetApp AFF (parte 2)

Configurare lo storage di boot SAN ONTAP

Creare igroups iSCSI



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

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

```
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

To map boot LUNs to igroups, run the following commands from the cluster management SSH connection:

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -igroup
VM-Host-Infra-A -lun-id 0
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -igroup
VM-Host-Infra-B -lun-id 0
```



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

["Procedura di implementazione di VMware vSphere 6.7U2."](#)

Procedura di implementazione di VMware vSphere 6.7U2

Questa sezione fornisce procedure dettagliate per l'installazione di VMware ESXi 6.7U2 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 6.7U2 e fare clic su Open (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.

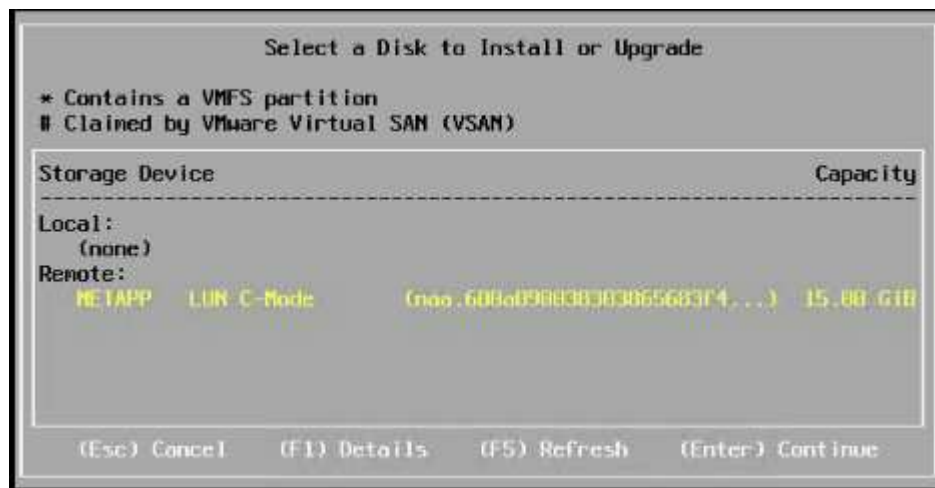
Installare VMware ESXi

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

Scarica L'immagine personalizzata Cisco ESXi 6.7U2

1. Passare a ["Pagina di download di VMware vSphere"](#) Per ISO personalizzati.
2. Fare clic su Vai a Download accanto all'immagine personalizzata Cisco per il CD di installazione ESXi 6.7U2.
3. Scaricare l'immagine personalizzata Cisco per il CD di installazione ESXi 6.7U2 (ISO).
4. All'avvio del sistema, il computer rileva la presenza del supporto di installazione di VMware ESXi.
5. Selezionare il programma di installazione di VMware ESXi dal menu visualizzato. Il programma di installazione viene caricato, che può richiedere alcuni minuti.
6. Una volta completato il caricamento del programma di installazione, premere Invio per continuare l'installazione.
7. Dopo aver letto il contratto di licenza con l'utente finale, accettarlo e continuare con l'installazione premendo F11.

8. Selezionare il LUN NetApp precedentemente configurato come disco di installazione per ESXi e premere Invio per continuare l'installazione.



9. Selezionare il layout di tastiera appropriato e premere Invio.
10. Inserire e confermare la password root e premere Invio.
11. 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.
6. Selezionare le porte corrispondenti a eth0 e eth1 in CIMC.

Network Adapters

Select the adapters for this host's default management network connection. Use two or more adapters for fault-tolerance and load-balancing.

Device Name	Hardware Label (MAC Address)	Status
<input type="checkbox"/> vmnic0	LOM Port 1 (...:5a:b5:8d:6e)	Connected
<input type="checkbox"/> vmnic1	LOM Port 2 (...:5a:b5:8d:6f)	Disconnected
<input checked="" type="checkbox"/> vmnic2	VIC-MLOM-eth0 (...:70:6c:cc)	Connected (...)
<input type="checkbox"/> vmnic3	VIC-iSCSI-A (...:3c:70:6c:cd)	Connected (...)
<input checked="" type="checkbox"/> vmnic4	VIC-MLOM-eth2 (...:70:6c:ce)	Connected (...)
<input type="checkbox"/> vmnic5	VIC-iSCSI-B (...:3c:70:6c:cf)	Connected (...)

<D> View Details <Space> Toggle Selected <Enter> OK <Esc> Cancel

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

25. Selezionare Troubleshooting Options (Opzioni di risoluzione dei problemi), quindi Enable ESXi Shell and SSH (attiva shell ES



Queste opzioni di troubleshooting possono essere disattivate dopo la convalida in base alla policy di sicurezza del cliente.

26. Premere due volte Esc per tornare alla schermata principale della console.
27. Fare clic su Alt-F1 dal menu a discesa CIMC Macros > Static Macros > Alt-F nella parte superiore della schermata.
28. Accedere con le credenziali appropriate per l'host ESXi.
29. Al prompt, immettere il seguente elenco di comandi esxcli in sequenza per abilitare la connettività di rete.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

Configurare l'host ESXi

Utilizzare le informazioni contenute nella seguente tabella per configurare ciascun host ESXi.

Dettaglio	Valore di dettaglio
Nome host ESXi	[esxi_host_fqdn]
IP di gestione host ESXi	[esxi_host_mgmt_ip]
Maschera di gestione host ESXi	[esxi_host_mgmt_netmask]
Gateway di gestione host ESXi	[esxi_host_mgmt_gateway]
IP NFS host ESXi	[esxi_host_NFS_ip]
ESXi host NFS mask	[esxi_host_NFS_netmask]
Gateway NFS host ESXi	[esxi_host_NFS_gateway]
IP vMotion host ESXi	[esxi_host_vMotion_ip]
Host ESXi vMotion mask	[esxi_host_vMotion_netmask]
Gateway vMotion host ESXi	[esxi_host_vMotion_gateway]
IP iSCSI-A host ESXi	[esxi_host_iSCSI-A_ip]
Host ESXi iSCSI-A mask	[esxi_host_iSCSI-A_netmask]
Gateway iSCSI-A host ESXi	[esxi_host_iSCSI-A_gateway]
IP iSCSI-B host ESXi	[esxi_host_iSCSI-B_ip]
Host ESXi iSCSI-B mask	[esxi_host_iSCSI-B_netmask]
Gateway iSCSI-B host ESXi	[esxi_host_SCSI-B_gateway]

Accedere all'host ESXi

Per accedere all'host ESXi, attenersi alla seguente procedura:

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. Leggere 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

Per configurare l'avvio iSCSI, attenersi alla seguente procedura:

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. Rinominare la porta iSCSIBootPG in iSCSIBootPG-A.



Vmnic3 e vmnic5 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.

7. Nel riquadro centrale, selezionare la scheda NIC VMkernel.
8. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel).
 - a. Specificare un nuovo nome di gruppo di porte di iScsiBootPG-B.
 - b. Selezionare iScsiBootvSwitch per lo switch virtuale.
 - c. Invio <<iScsiB_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_iscsib_ip>> Per Indirizzo.
- h. Invio <<var_hosta_iscsib_mask>> Per Subnet Mask.
- i. Fare clic su Crea.



Impostare la MTU su 9000 su iScsiBootPG-A.

9. Per impostare il failover, attenersi alla seguente procedura:

- a. Fare clic su Edit Settings (Modifica impostazioni) in iSCSIBootPG-A > Tiering and failover > failover order > vmnic3. Vmnic3 deve essere attivo e vmnic5 deve essere inutilizzato.
- b. Fare clic su Edit Settings (Modifica impostazioni) in iSCSIBootPG-B > Teaming and failover (Teaming e failover) > failover Order (Ordine di failover) > Vmnic5. Vmnic5 deve essere attivo e vmnic3 deve essere inutilizzato.

iScsiBootPG-A - Edit Settings

Properties

Security

Traffic shaping

Teaming and failover

Load balancing

Network failure detection

Notify switches

Failback

Failover order

☒ Override



Active adapters

 vmnic3

Standby adapters

Unused adapters

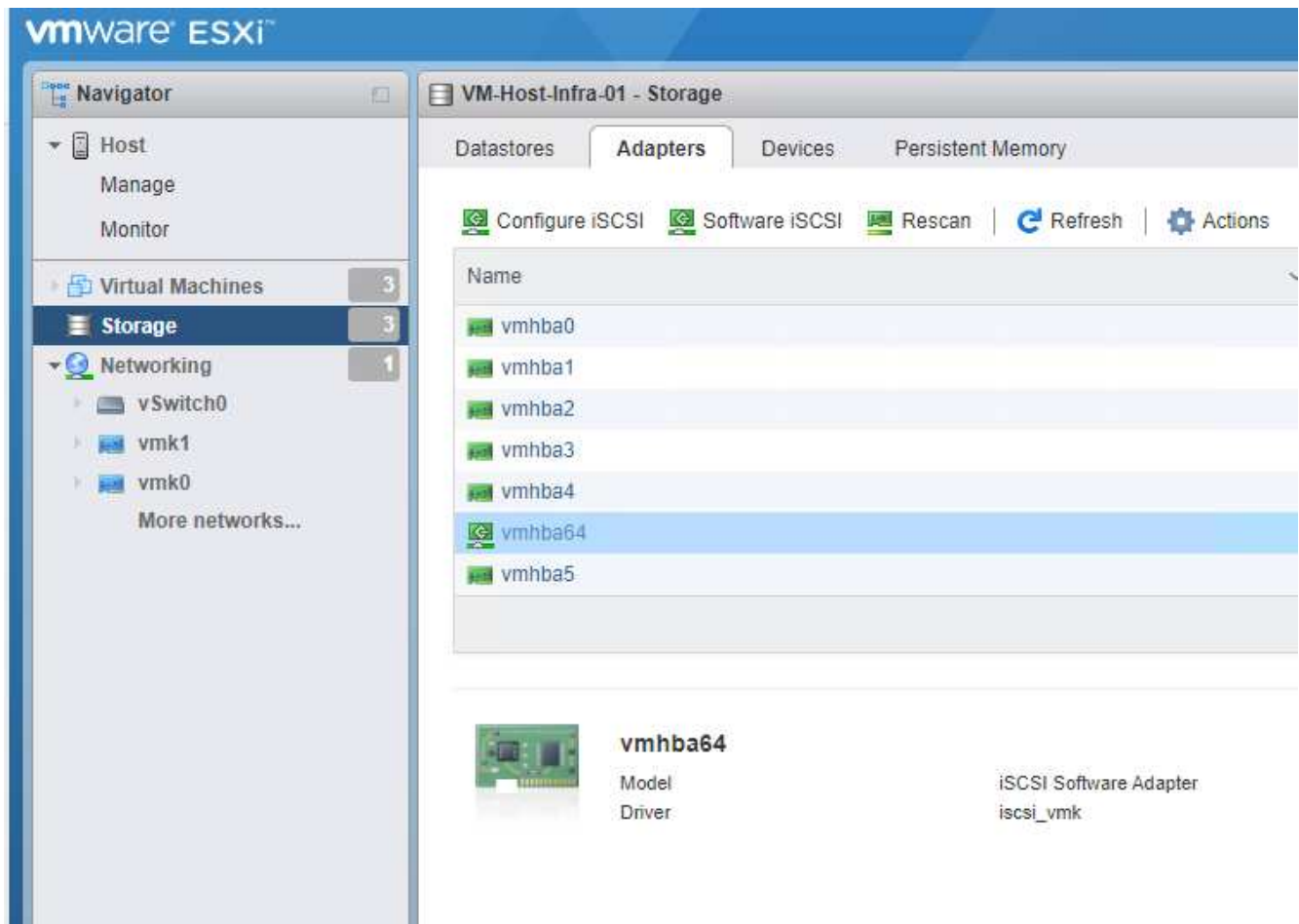
 vmnic5

Select active and standby adapters

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)

Configure iSCSI - vmhba64

iSCSI enabled ☐ Disabled ☒ Enabled

▶ Name & alias `iqn.1992-01.com.cisco:ucsA-01`

▶ CHAP authentication Do not use CHAP

▶ Mutual CHAP authentication Do not use CHAP

▶ Advanced settings Click to expand

Network port bindings No port bindings

Static targets

Add static target Remove static target Edit settings Search

Target	Address	Port
<code>iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...</code>	172.21.183.105	3260
<code>iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...</code>	172.21.184.106	3260
<code>iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...</code>	172.21.183.106	3260
<code>iqn.1992-08.com.netapp:sn.e42fa6b2d2e011e9a68d00a098f...</code>	172.21.184.105	3260

Dynamic targets

Add dynamic target Remove dynamic target Edit settings Search

Address	Port
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260

Save configuration Cancel

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**.

Dynamic targets

Add dynamic target Remove dynamic target Edit settings Search

Address	Port
172.21.183.105	3260
172.21.184.105	3260
172.21.183.106	3260
172.21.184.106	3260

Save configuration Cancel



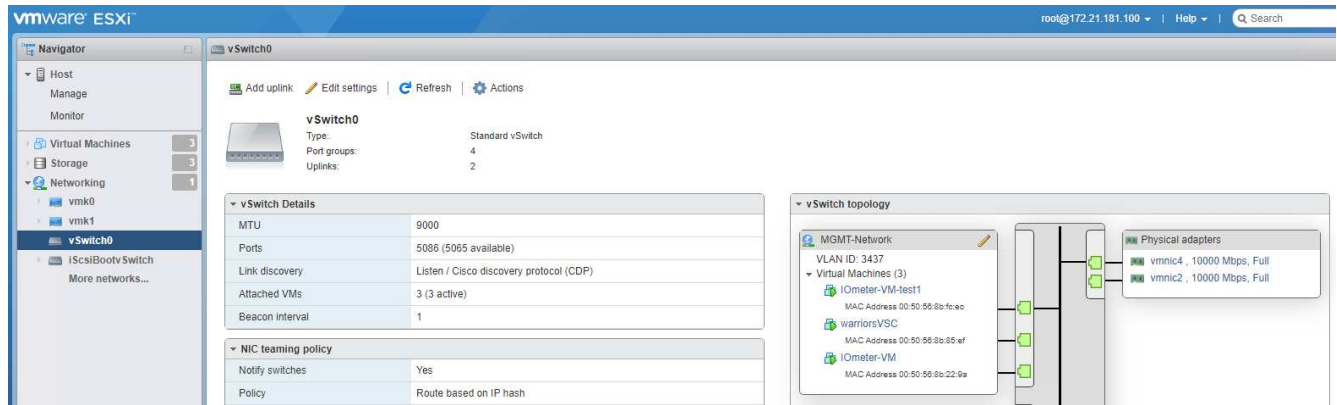
È possibile trovare gli indirizzi IP LIF iSCSI eseguendo il comando di visualizzazione dell'interfaccia di rete sul cluster NetApp o osservando la scheda Network Interfaces (interfacce di rete) in System Manager.

Configurare l'host ESXi

Per configurare l'avvio di ESXi, attenersi alla seguente procedura:

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 il raggruppamento NIC e verificare che vmnic2 e vmnic4 siano impostati su Active e che il raggruppamento NIC e il failover siano impostati su Route in base all'hash IP.



Il metodo hash IP per il bilanciamento del carico richiede che lo switch fisico sottostante sia configurato correttamente utilizzando SRC-DST-IP EtherChannel con un canale di porta statico (mode-on). La connessione potrebbe essere intermittente a causa di possibili errori di configurazione dello switch. In tal caso, chiudere temporaneamente una delle due porte di uplink associate sullo switch Cisco per ripristinare la comunicazione con la porta vmkernel di gestione ESXi durante la risoluzione dei problemi relativi alle impostazioni del canale della porta.

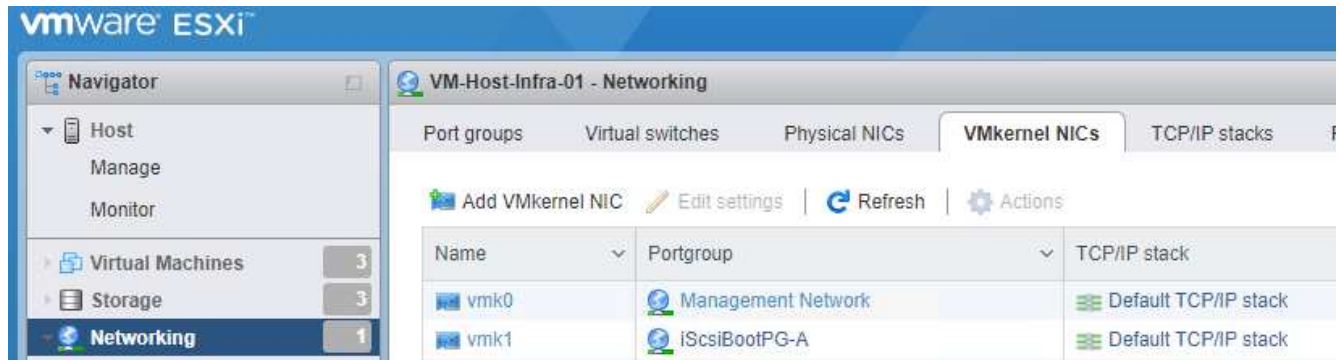
Configurare i gruppi di porte e le NIC VMkernel

Per configurare i gruppi di porte e le NIC VMkernel, attenersi alla seguente procedura:

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.
 - a. Assegnare un nome al gruppo di porte MGMT-Network.
 - b. Invio <<mgmt_vlan>> Per l'ID VLAN.
 - c. Assicurarsi che vSwitch0 sia selezionato.
 - d. Fare clic su Save (Salva)
5. Fare clic sulla scheda NIC VMkernel.



6. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel).
 - a. Selezionare New Port Group (nuovo gruppo di porte).
 - b. Assegnare un nome al gruppo di porte NFS-Network.
 - c. Invio <<nfs_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_nfs_ip>> Per Indirizzo.
 - h. Invio <<var_hosta_nfs_mask>> Per Subnet Mask.
 - i. 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.

Virtual switch	vSwitch0
VLAN ID	3441
MTU	9000
IP version	IPv4 only
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.185.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack
Services	<input checked="" type="checkbox"/> vMotion <input type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel

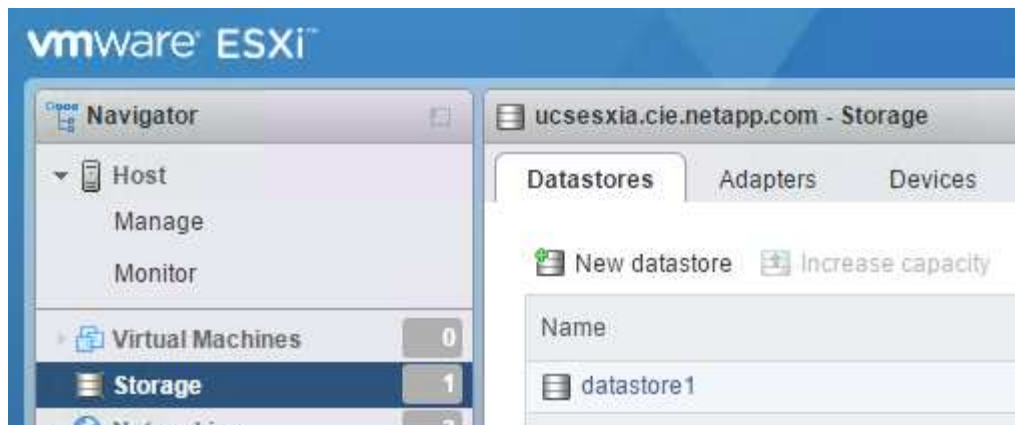


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

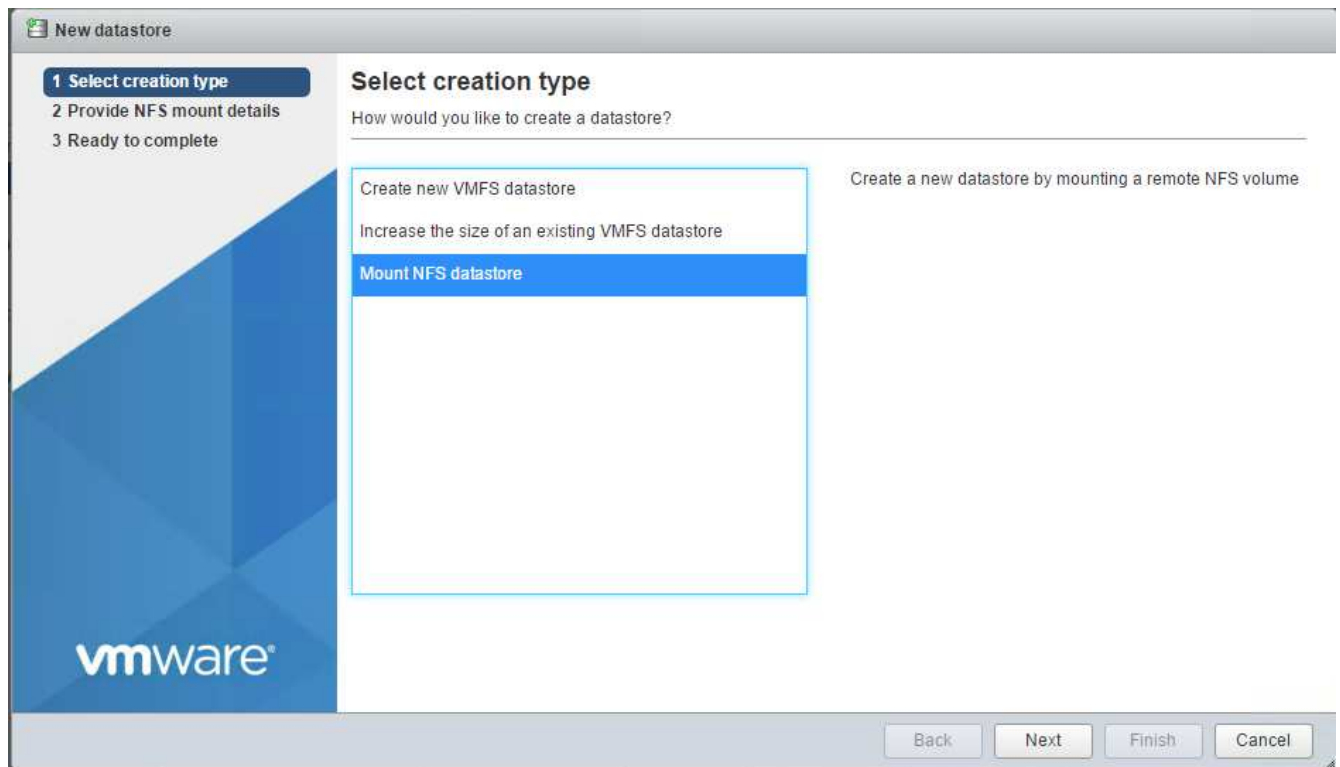
Montare i primi datastore

I primi datastore da montare sono `infra_datastore` Datastore per macchine virtuali e `infra_swap` Datastore 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. Inserire le seguenti informazioni nella pagina fornire dettagli sull'installazione NFS:

- Nome: `infra_datastore`
- Server NFS: `<<var_nodea_nfs_lif>>`
- Condividere: `/infra_datastore`
- 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 `infra_swap` datastore:

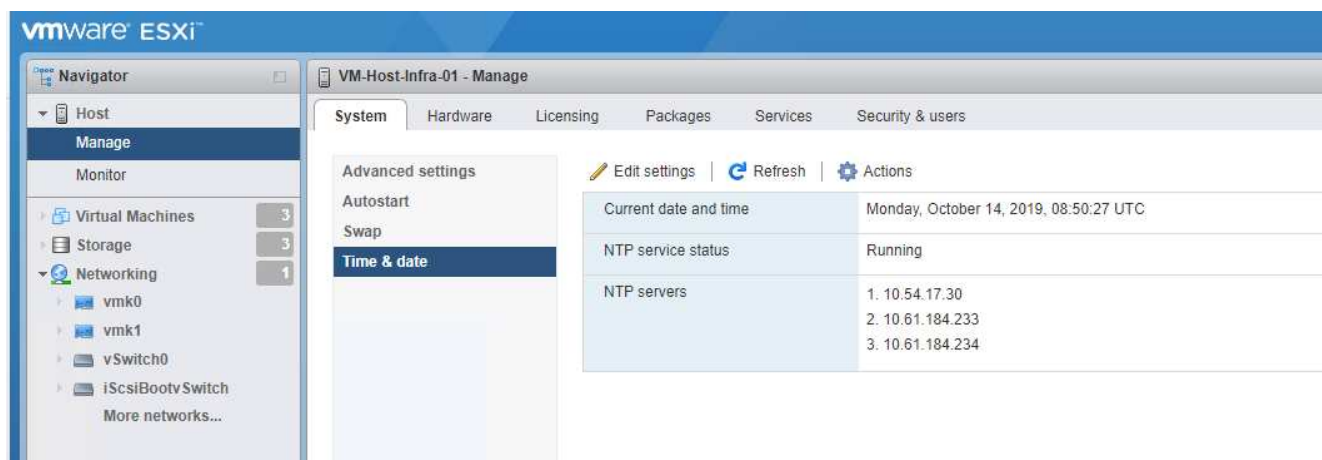
- Nome: `infra_swap`
- Server NFS: `<<var_nodea_nfs_lif>>`
- Condividere: `/infra_swap`

- Assicurarsi che sia selezionato NFS 3.

Configurare NTP

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

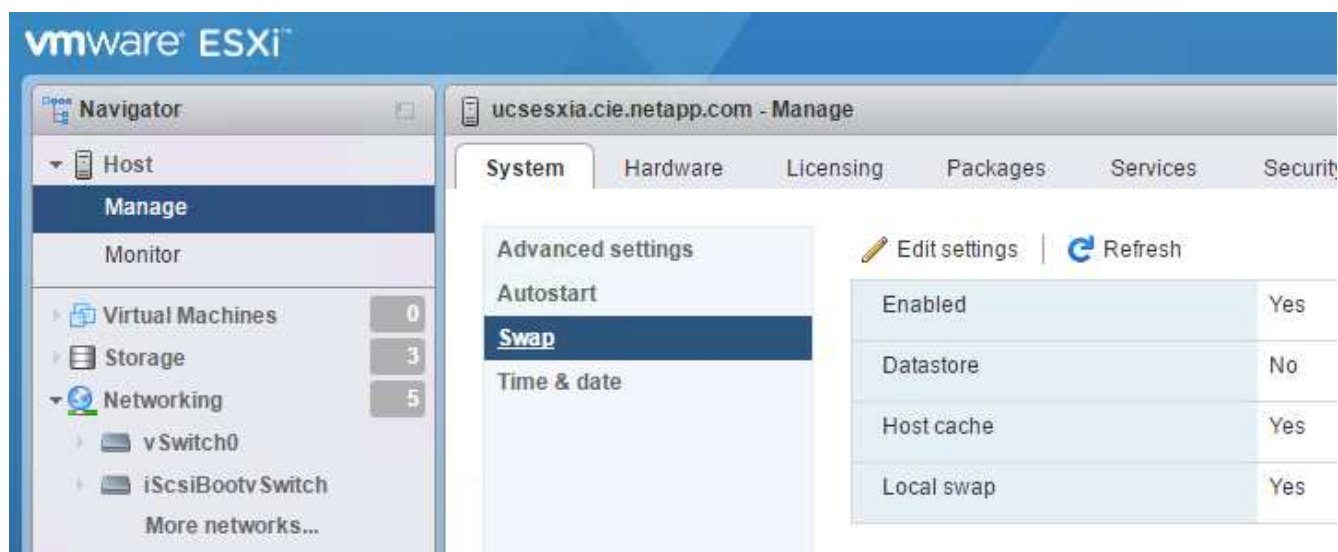
1. Fare clic su Manage (Gestisci) nel riquadro di navigazione a sinistra. Selezionare sistema nel riquadro di destra, quindi fare clic su Data e ora.
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio 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.



Edit swap configuration	
Enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Datastore	infra_swap ▼
Local swap enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
Host cache enabled	<input checked="" type="radio"/> Yes <input type="radio"/> No
<div>Save Cancel</div>	

3. Fare clic su Salva.

["Procedura di installazione di VMware vCenter Server 6.7U2."](#)

Procedura di installazione di VMware vCenter Server 6.7U2

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

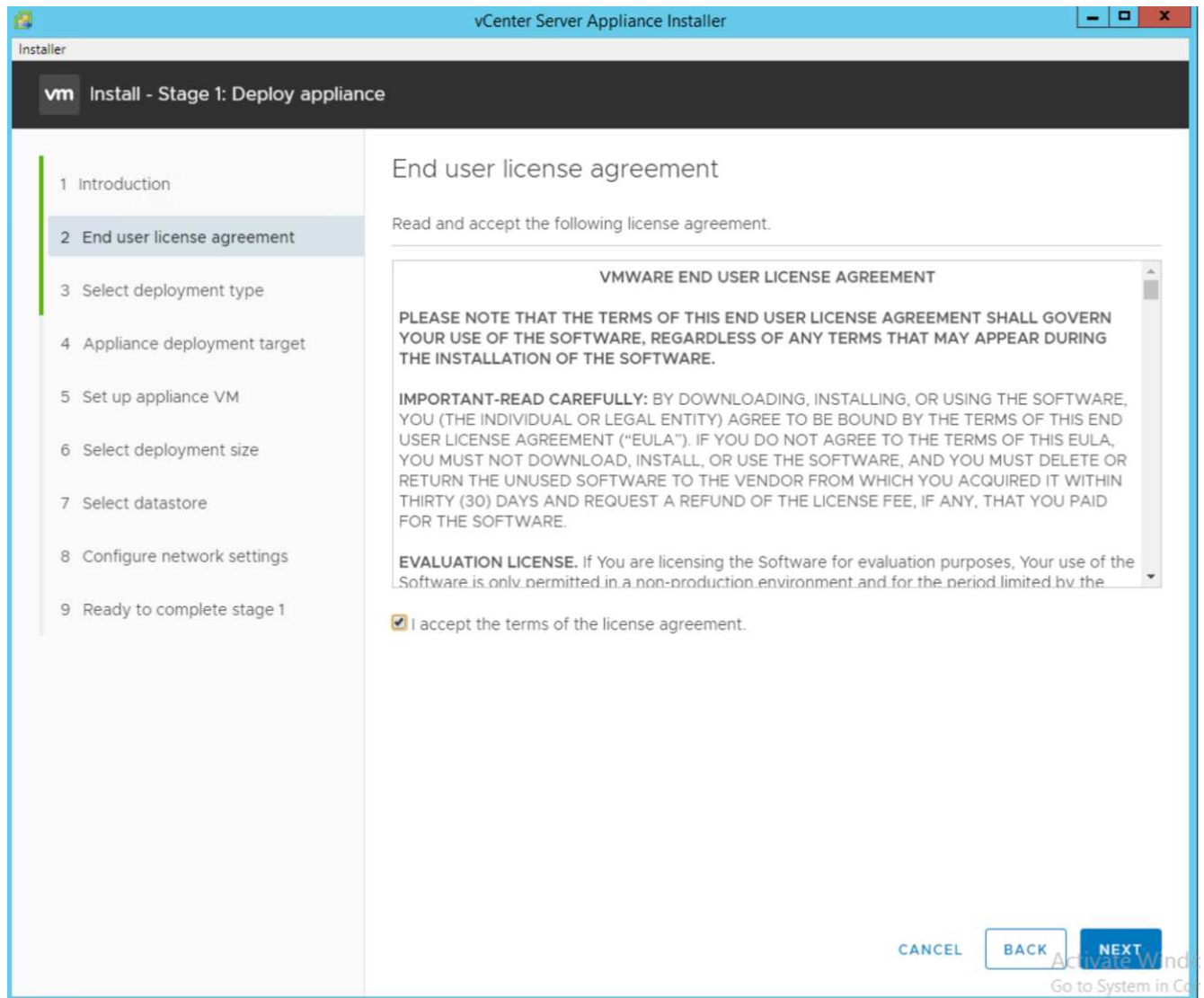


FlexPod utilizza l'appliance server vCenter (VCSA).

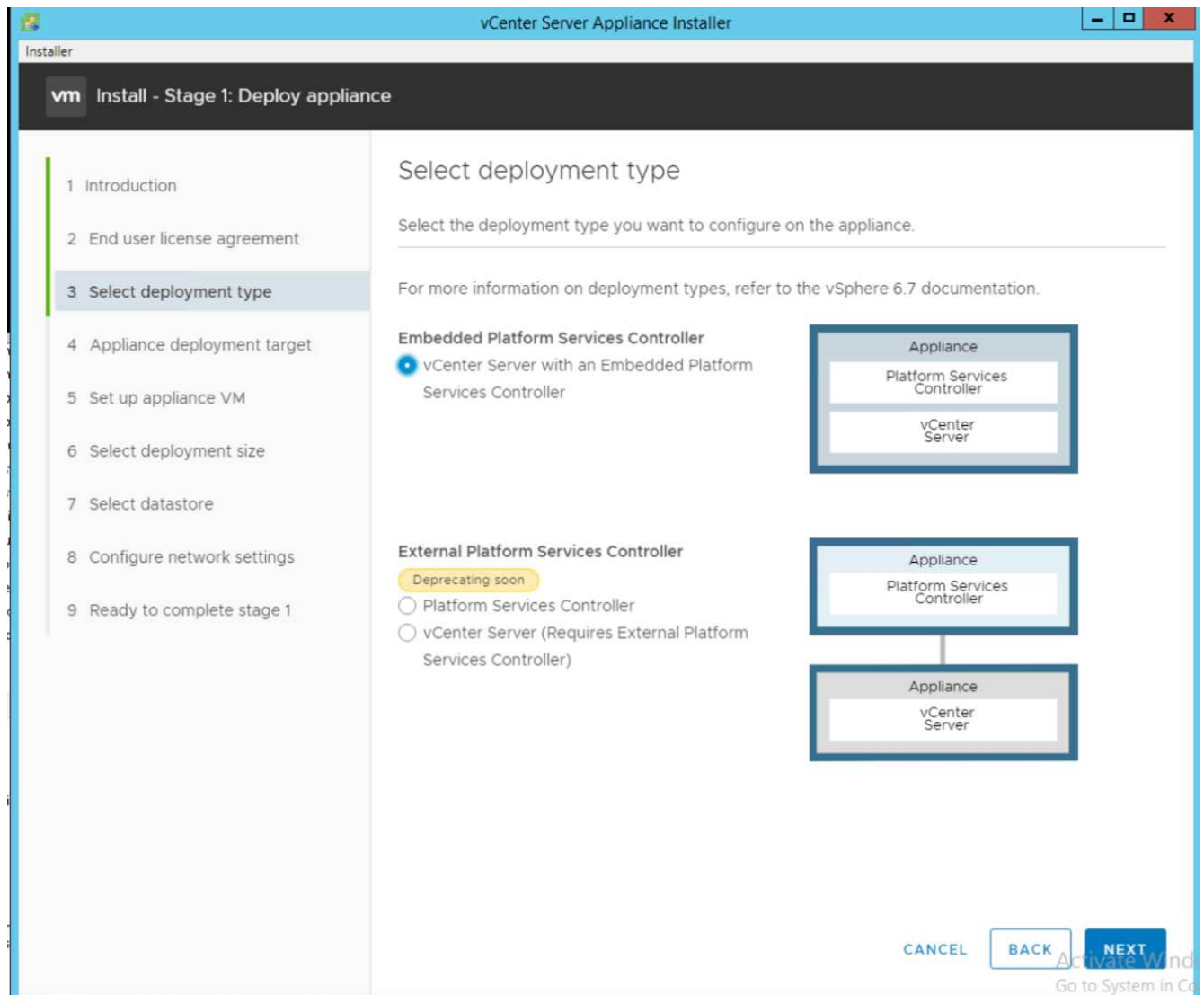
Scarica VMware vCenter Server Appliance

Per scaricare VMware vCenter Server Appliance (VCSA), attenersi alla seguente procedura:

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.
3. Sebbene sia supportato l'installabile di Microsoft Windows vCenter Server, VMware consiglia VCSA per le nuove implementazioni.
4. Montare l'immagine ISO.
5. Accedere alla directory `vcsa- ui-installer > win32`. Fare doppio clic `installer.exe`.
6. Fare clic su Installa.
7. Fare clic su Avanti nella pagina Introduzione.



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 implementazione appliance), immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root.

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

Appliance deployment target

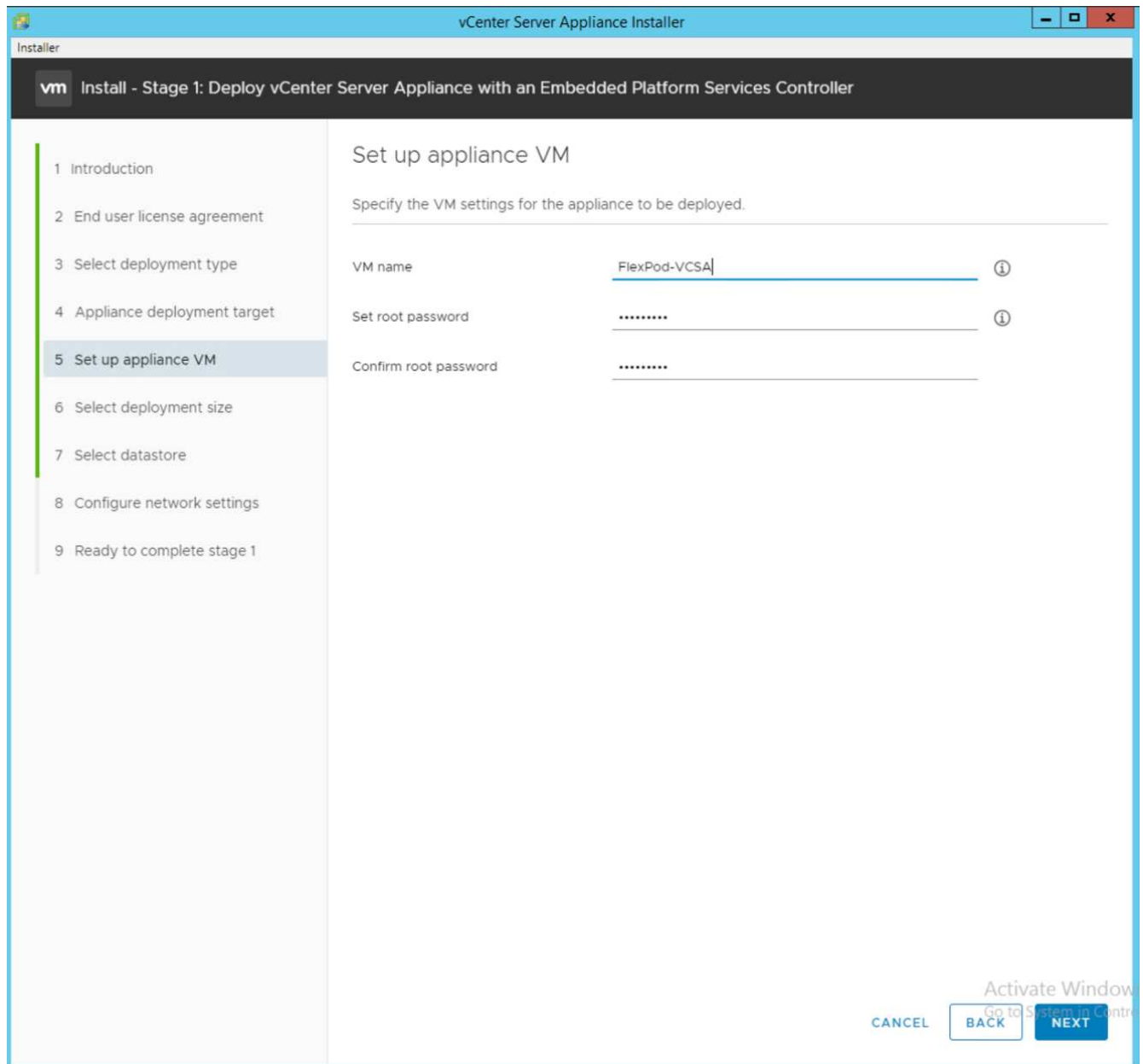
Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

ESXi host or vCenter Server name	172.21.181.100	?
HTTPS port	443	
User name	root	?
Password	

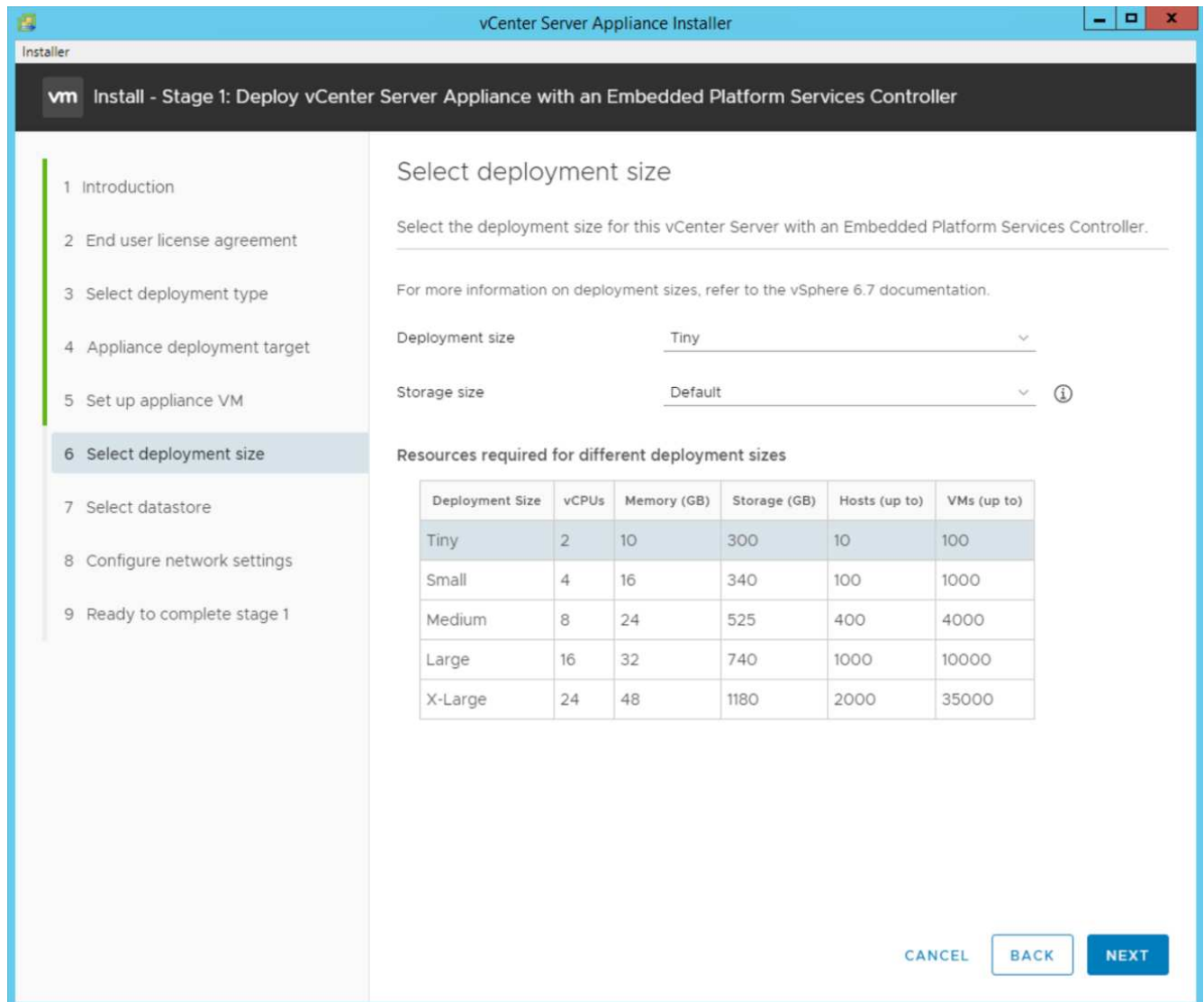
CANCEL BACK NEXT

Activate Windows
Go to System in Settings

10. Impostare la macchina virtuale 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 `infra_datastore` datastore. 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.

Installer

vCenter Server Appliance Installer

vm Install - Stage 1: Deploy vCenter Server Appliance with an Embedded Platform Services Controller

1 Introduction

2 End user license agreement

3 Select deployment type

4 Appliance deployment target

5 Set up appliance VM

6 Select deployment size

7 Select datastore

8 Configure network settings

9 Ready to complete stage 1

Configure network settings

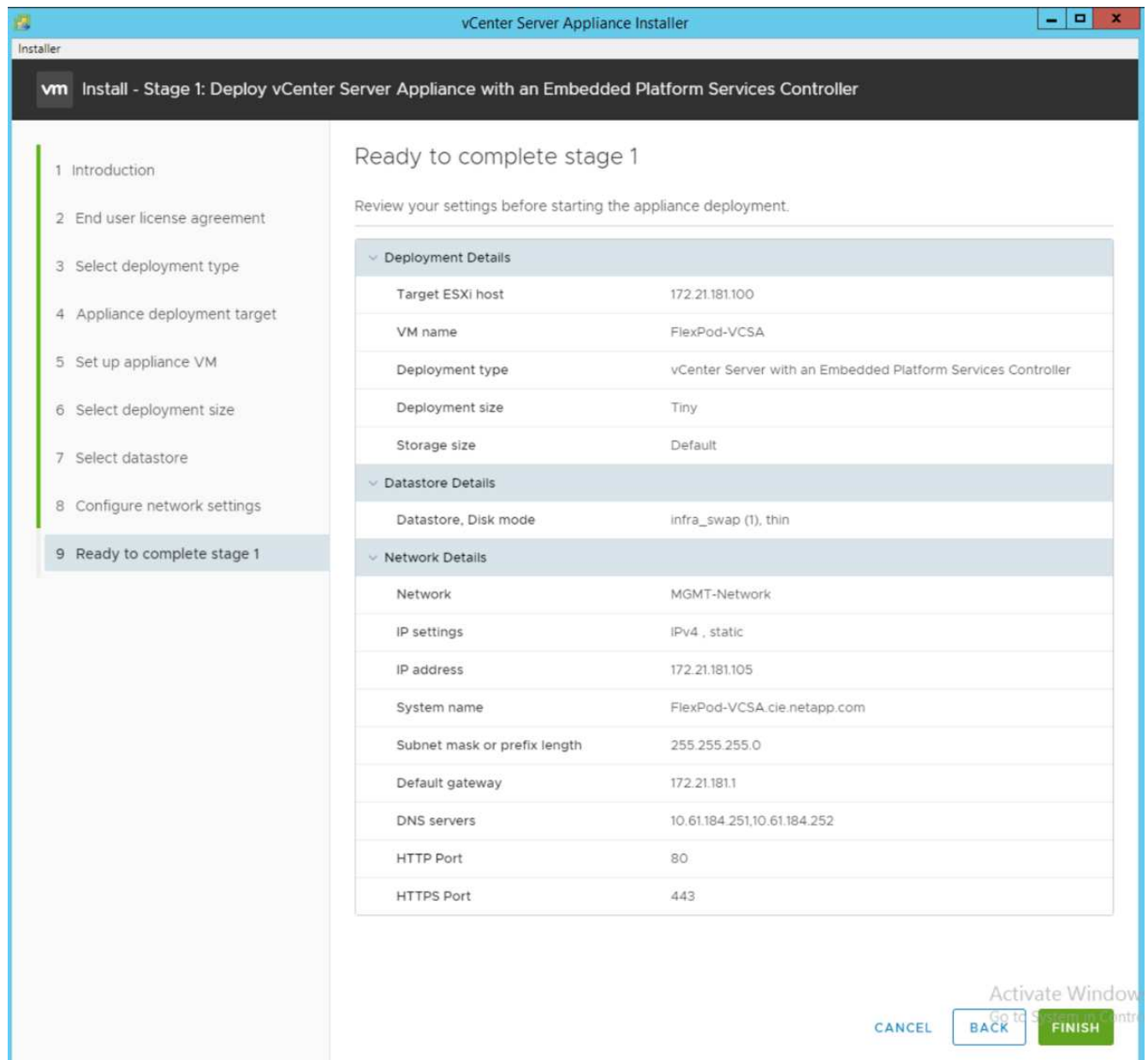
Configure network settings for this appliance

Network	MGMT-Network	ⓘ
IP version	IPv4	
IP assignment	static	
FQDN	FlexPod-VCSA.cle.netapp.com	ⓘ
IP address	172.21.181.105	
Subnet mask or prefix length	255.255.255.0	ⓘ
Default gateway	172.21.181.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

CANCEL BACK NEXT

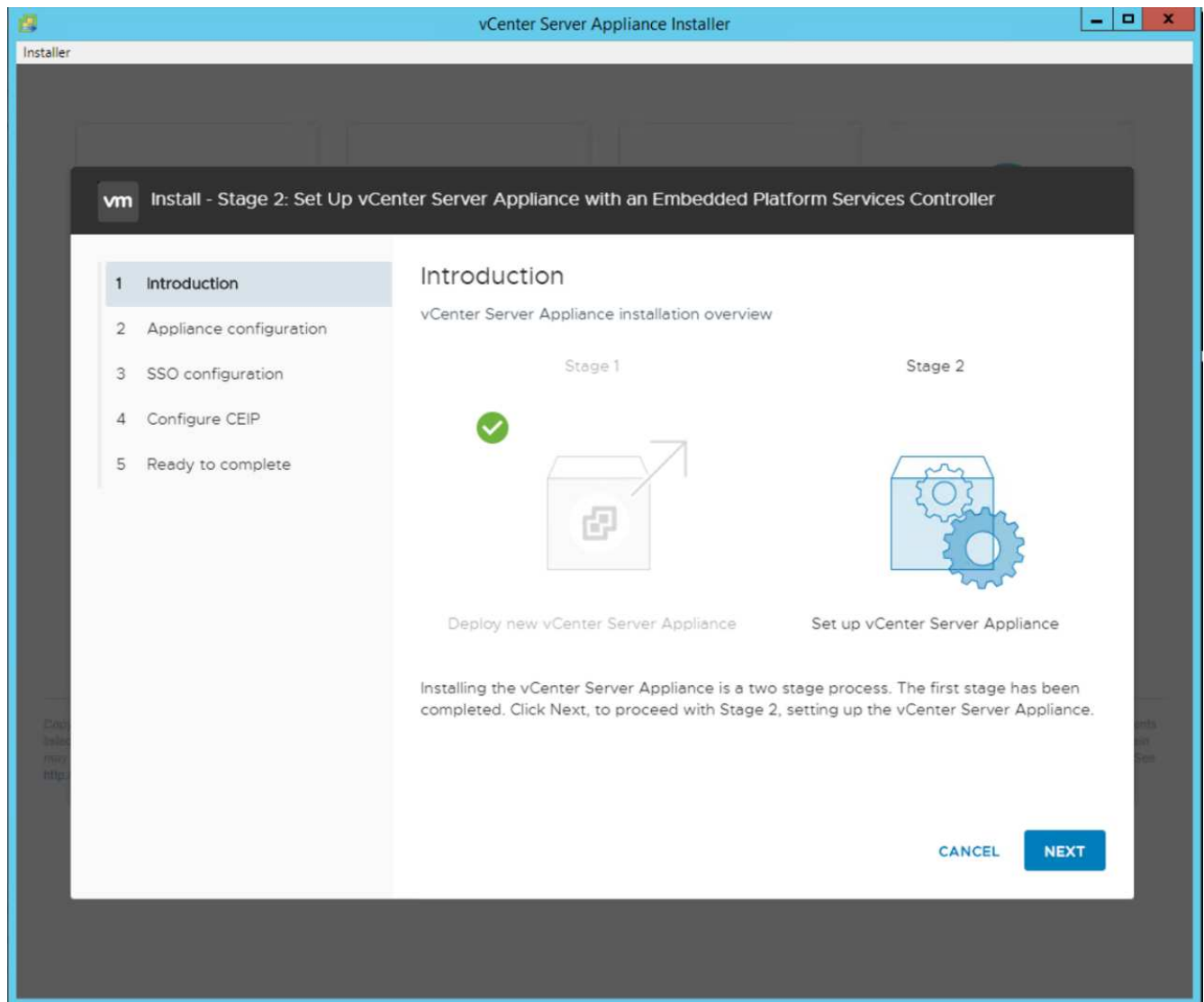
Activate Windows
Go to System in Control

15. Rivedere le impostazioni nella fase 1 prima di avviare l'implementazione dell'appliance.

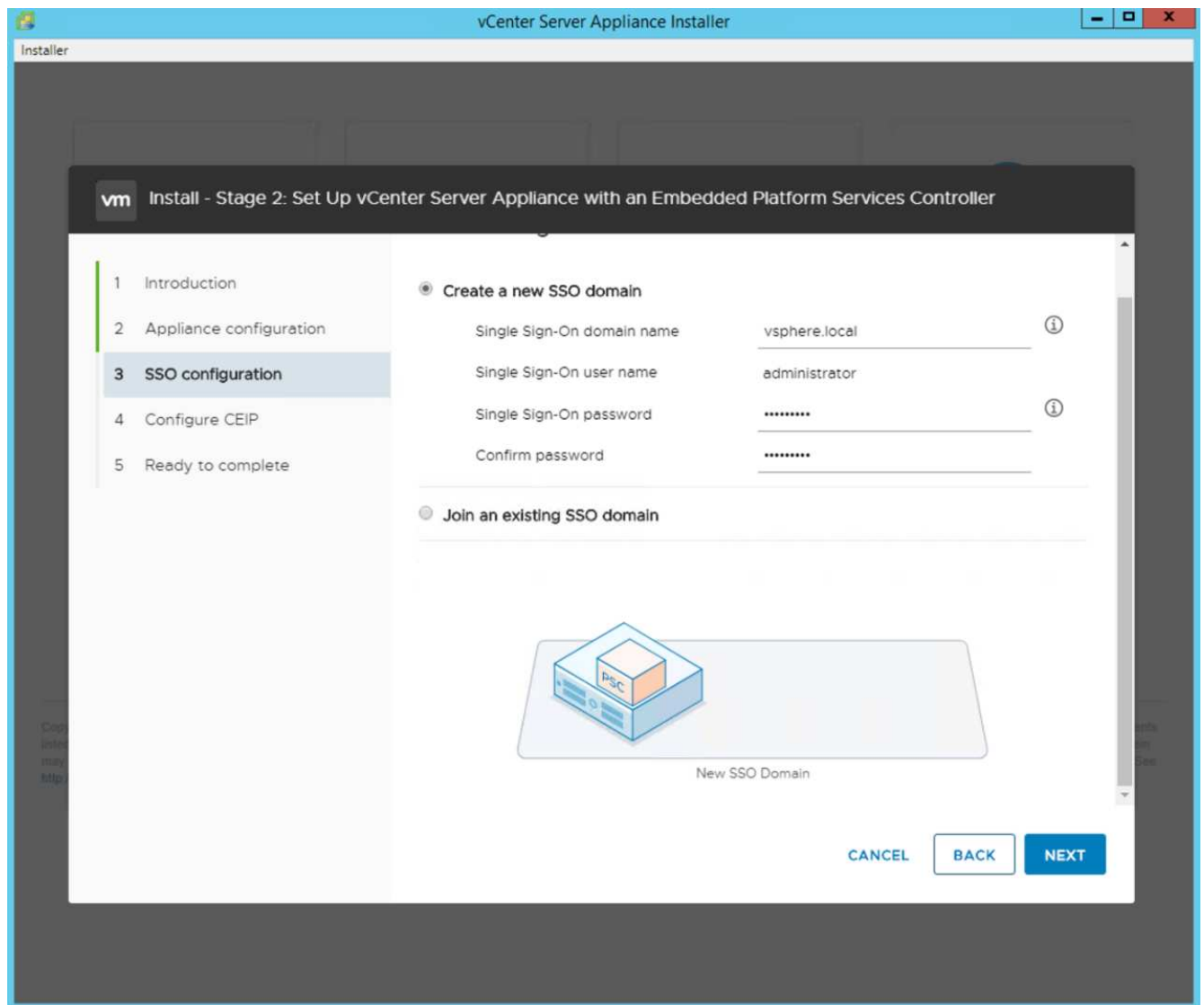


VCSA viene installato ora. Questo processo richiede alcuni minuti.

16. 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.
17. Nella pagina Introduzione alla fase 2, fare clic su Avanti.

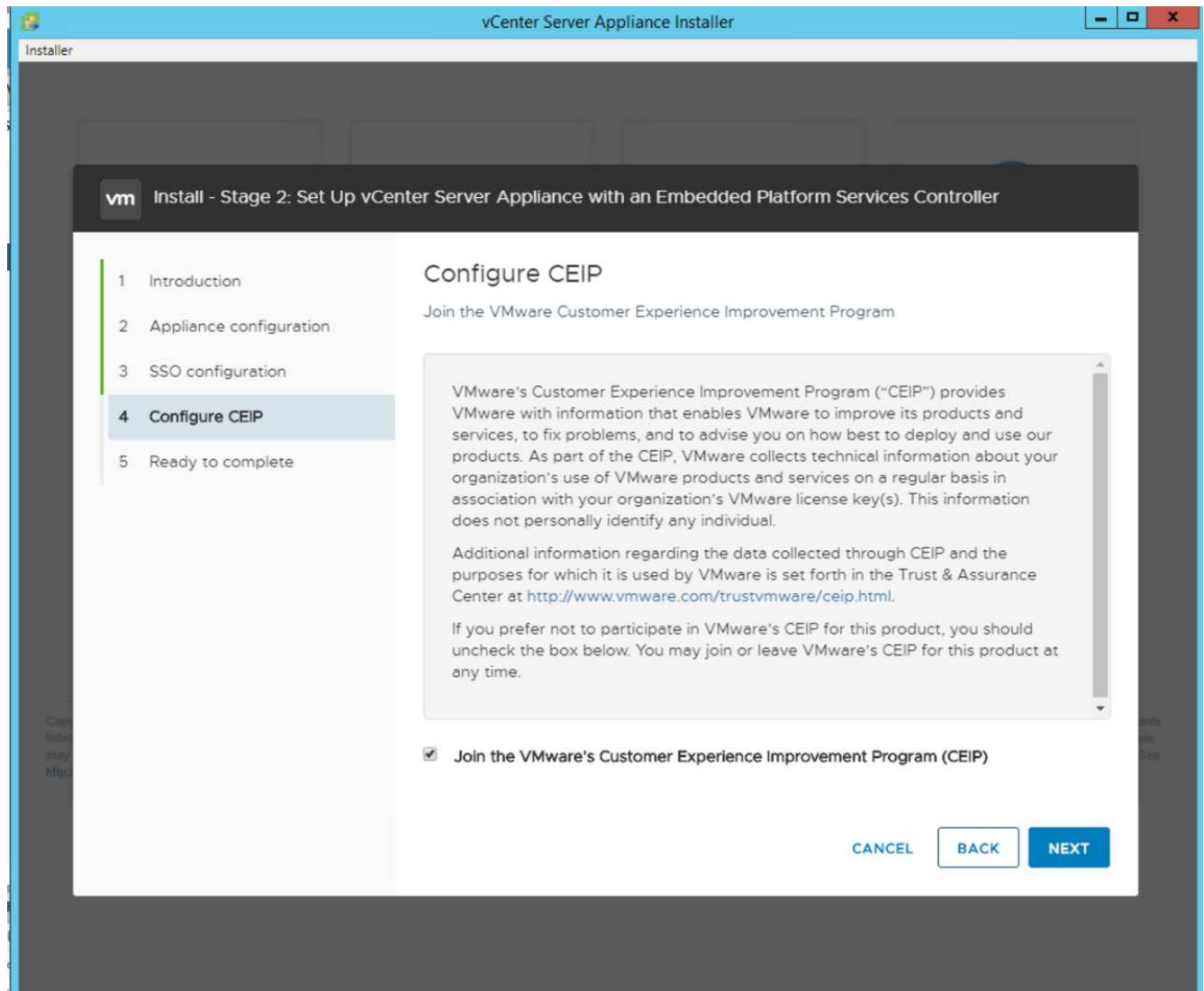


18. Invio <<var_ntp_id>> Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.
19. Se si intende utilizzare vCenter Server High Availability (ha), assicurarsi che l'accesso SSH sia attivato.
20. Configurare il nome di dominio SSO, la password e il nome del sito. Fare clic su Avanti.

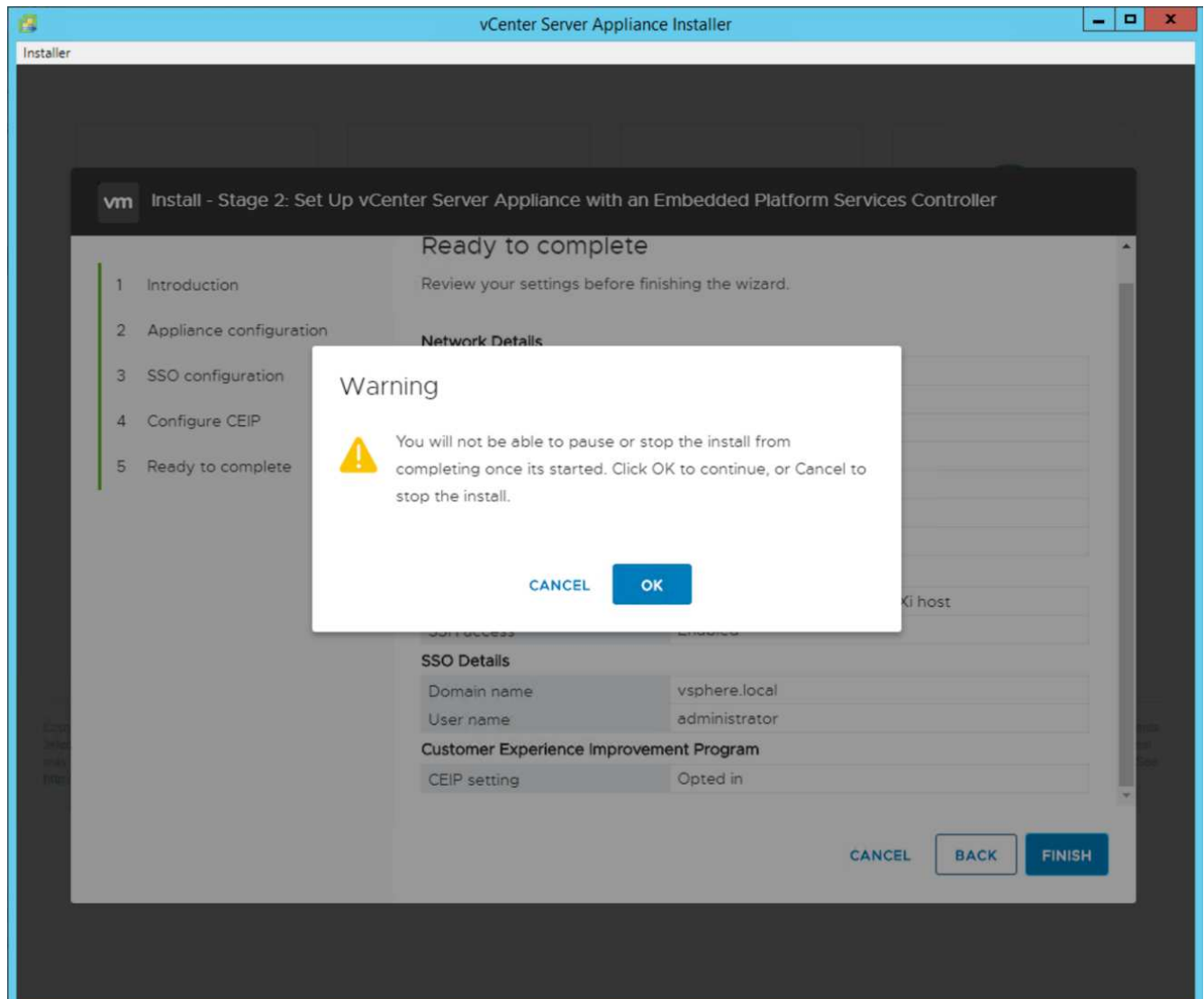


Registrare questi valori come riferimento, in particolare se si discosta da `vsphere.local` nome di dominio.

21. Se lo desideri, partecipa al programma VMware Customer Experience. Fare clic su Avanti.



22. Visualizzare il riepilogo delle impostazioni. Fare clic su fine o utilizzare il pulsante Indietro per modificare le impostazioni.
23. 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.

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

"Pagina successiva: Configurazione del clustering di VMware vCenter Server 6.7U2 e vSphere."

Configurazione del clustering di VMware vCenter Server 6.7U2 e vSphere

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

1. Selezionare `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 un 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.

New Cluster | FlexPod-Datacenter

Name	FlexPod-Cluster
Location	FlexPod-Datacenter
DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

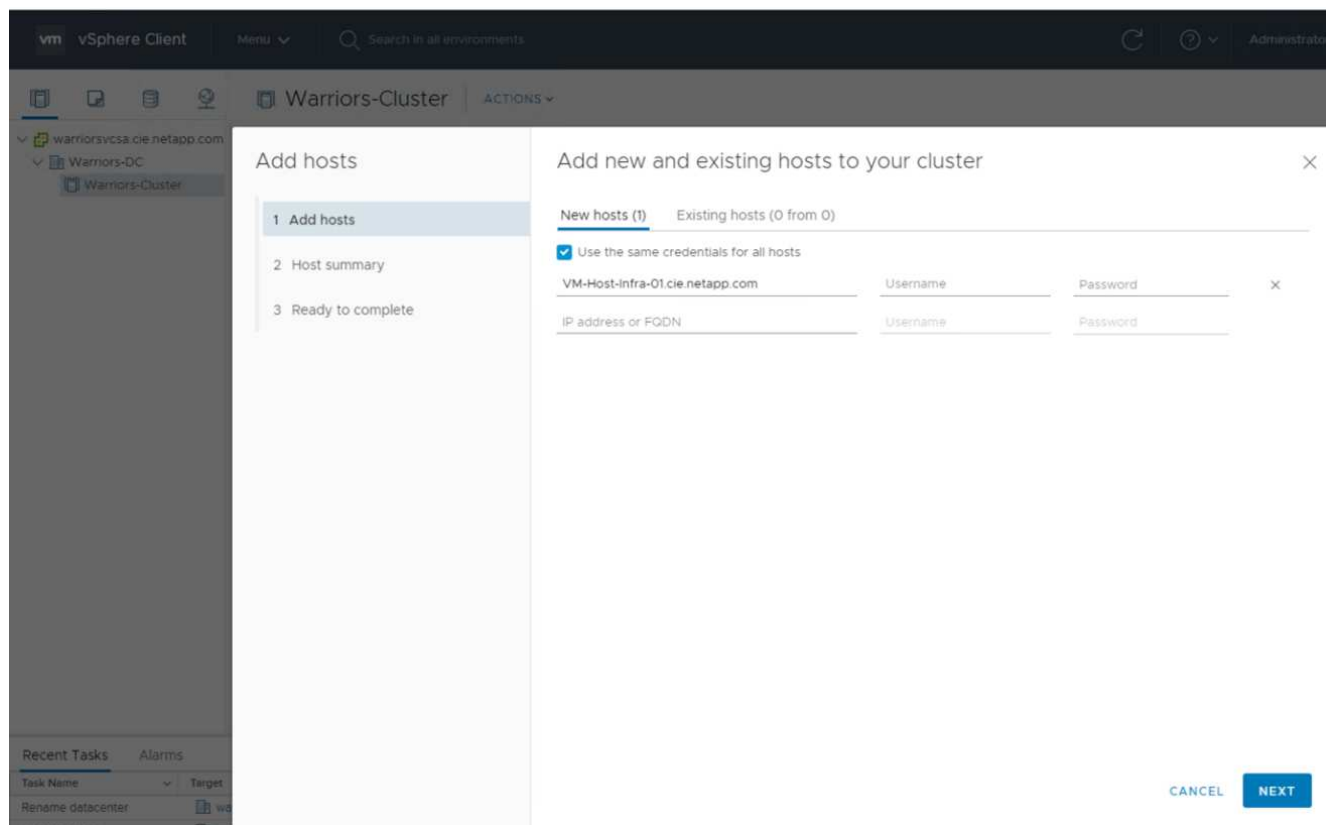
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

CANCEL **OK**

Aggiungere gli host ESXi al cluster

Per aggiungere gli host ESXi al cluster, attenersi alla seguente procedura:

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.
3. Questa fase può essere completata in un secondo momento, se lo si desidera.
 - a. Fare clic su Next (Avanti) per disattivare la modalità di blocco.
 - b. Fare clic su Next (Avanti) nella pagina VM location (posizione macchina virtuale).
 - c. Consultare la pagina Pronto per il completamento. Utilizzare il pulsante Indietro per apportare eventuali modifiche o selezionare fine.
4. Ripetere i passaggi 1 e 2 per l'host Cisco UCS B.



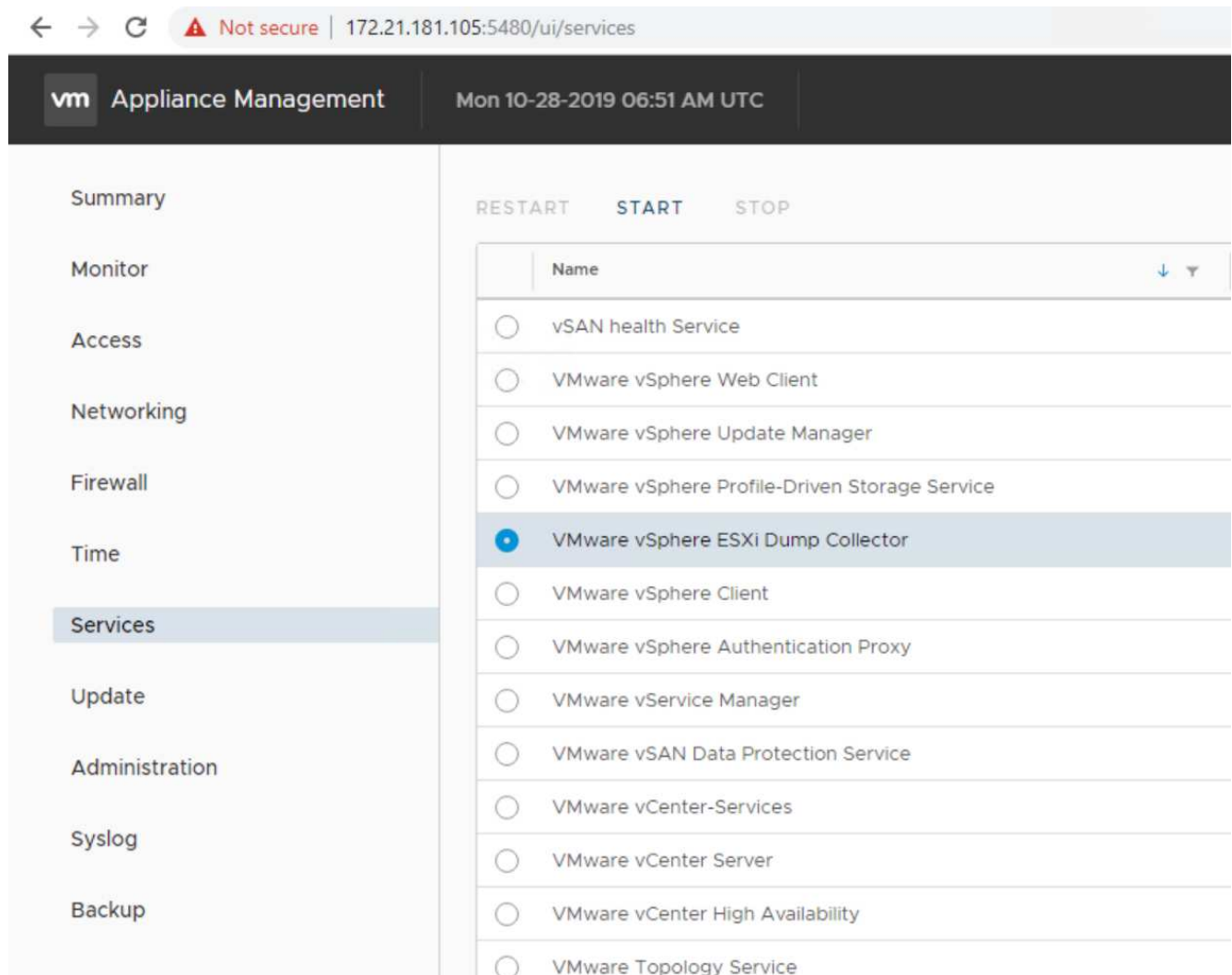
Questo processo deve essere completato per tutti gli host aggiuntivi aggiunti alla configurazione di FlexPod Express.

Configurare il coredump sugli host ESXi

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

1. Accedere a [https:// "VCenter"](https://VCenter) IP:5480/, inserire root come nome utente e la password root.
2. Fare clic su Services (servizi) e selezionare VMware vSphere ESXi Dump Collector.

3. Avviare il servizio VMware vSphere ESXi Dump Collector.



4. Utilizzando SSH, connettersi all'host ESXi IP di gestione, immettere root per il nome utente e la password root.
5. 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
```

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

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -  
vmk0 -o 6500  
root@VM-Host-Infra-01:~]  
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true  
root@VM-Host-Infra-01:~] esxcli system coredump network check  
Verified the configured netdump server is running
```



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



`ip_address_of_core_dump_collector` In questa convalida si trova l'IP vCenter.

"Pagina successiva: Procedure di implementazione di NetApp Virtual Storage Console 9.6."

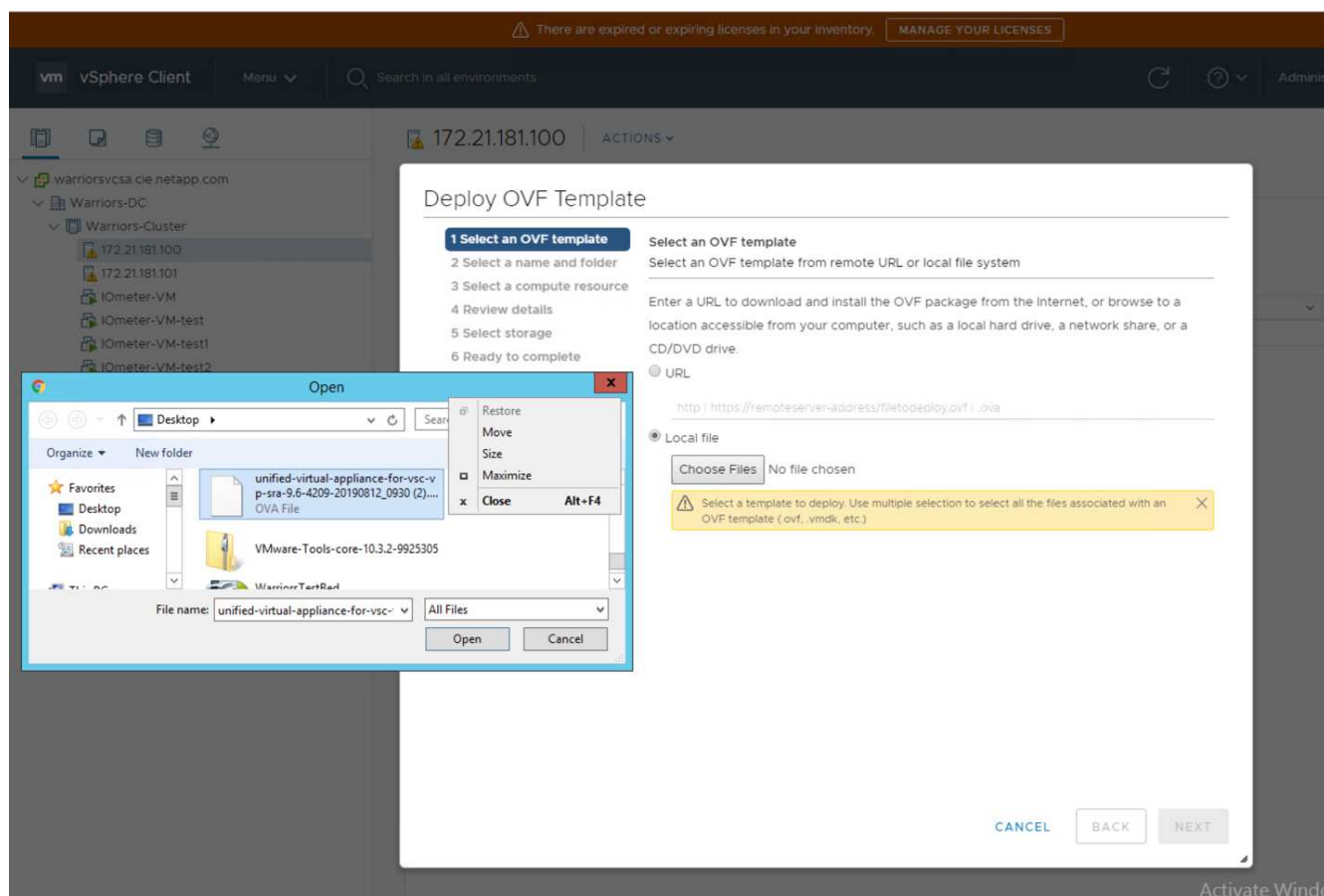
Procedure di implementazione di NetApp Virtual Storage Console 9.6

In questa sezione vengono descritte le procedure di implementazione di NetApp Virtual Storage Console (VSC).

Installare Virtual Storage Console 9.6

Per installare il software VSC 9.6 utilizzando un'implementazione Open Virtualization Format (OVF), attenersi alla seguente procedura:

1. Accedere a vSphere Web Client > host Cluster > Deploy OVF Template (implementa modello OVF).
2. Accedere al file VSC OVF scaricato dal sito del supporto NetApp.



3. Inserire il nome della macchina virtuale e selezionare un data center o una cartella in cui eseguire l'implementazione. Fare clic su Avanti.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements
- ✓ 6 Select storage
- 7 Select networks
- 8 Customize template

Select a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▼  warriorsvcsa.cie.netapp.com
- >  FlexPod-Datacenter

4. Selezionare il cluster ESXi FlexPod-Cluster e fare clic su Next (Avanti).
5. Esaminare i dettagli e fare clic su Next (Avanti).

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details

Verify the template details.

Publisher	No certificate present
Product	Virtual Appliance - NetApp VSC, VASA Provider and SRA for ONTAP
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp VSC, VASA Provider, and SRA virtual appliance for NetApp storage systems. For more information or support please visit http://www.netapp.com/
Download size	1.0 GB
Size on disk	2.1 GB (thin provisioned)
	53.0 GB (thick provisioned)

CANCEL

BACK

NEXT

6. Fare clic su Accept (Accetta) per accettare la licenza e fare clic su Next (Avanti).
7. Selezionare il formato del disco virtuale di thin provisioning e uno degli archivi dati NFS. Fare clic su Avanti.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Select storage**
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
infra_datastore	75 GB	360 KB	75 GB	NF
infra_datastore1	475 GB	639.9 GB	276.86 GB	NF
infra_swap (1)	100 GB	4.98 GB	95.02 GB	NF

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Da Select Networks (Seleziona reti), scegliere una rete di destinazione e fare clic su Next (Avanti).

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- 7 Select networks**
- 8 Customize template
- 9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	MGMT-Network
1 items	

IP Allocation Settings

IP allocation:

Static - Manual

IP protocol:

IPv4

CANCEL

BACK

NEXT

9. Da Customize Template (Personalizza modello), immettere la password dell'amministratore VSC, il nome vCenter o l'indirizzo IP e altri dettagli di configurazione, quindi fare clic su Next (Avanti).

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Select storage
- ✓ 7 Select networks
- ✓ 8 Customize template**
- 9 Ready to complete

vCenter Server Address (*)

Specify the IP address/hostname of an existing vCenter to register to.

172.21.181.105

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password:

Confirm Password:

✓ **Network Properties** 8 settings

Host Name

Specify the hostname for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

10. Esaminare i dettagli di configurazione immessi e fare clic su Finish (fine) per completare l'implementazione di NetApp-VSC VM.
11. Accendere la macchina virtuale NetApp-VSC e aprire la console della macchina virtuale.
12. Durante il processo di avvio delle macchine virtuali NetApp-VSC, viene visualizzato un messaggio che richiede di installare VMware Tools. Da vCenter, selezionare NetApp-VSC VM > sistema operativo guest > Installa VMware Tools.

Booting VSC, VASA Provider, and SRA virtual appliance...Please wait...

VMware Tools OVF vCenter configuration not found.

VMware Tools OVF vCenter configuration not found.

VMware Tools OVF vCenter configuration not found.

VMware Tools installation

Before you can continue the VSC, VASA Provider, and SRA virtual appliance installation, you must install the VMware Tools:

1. Select VM > Guest OS > Install VMware Tools.

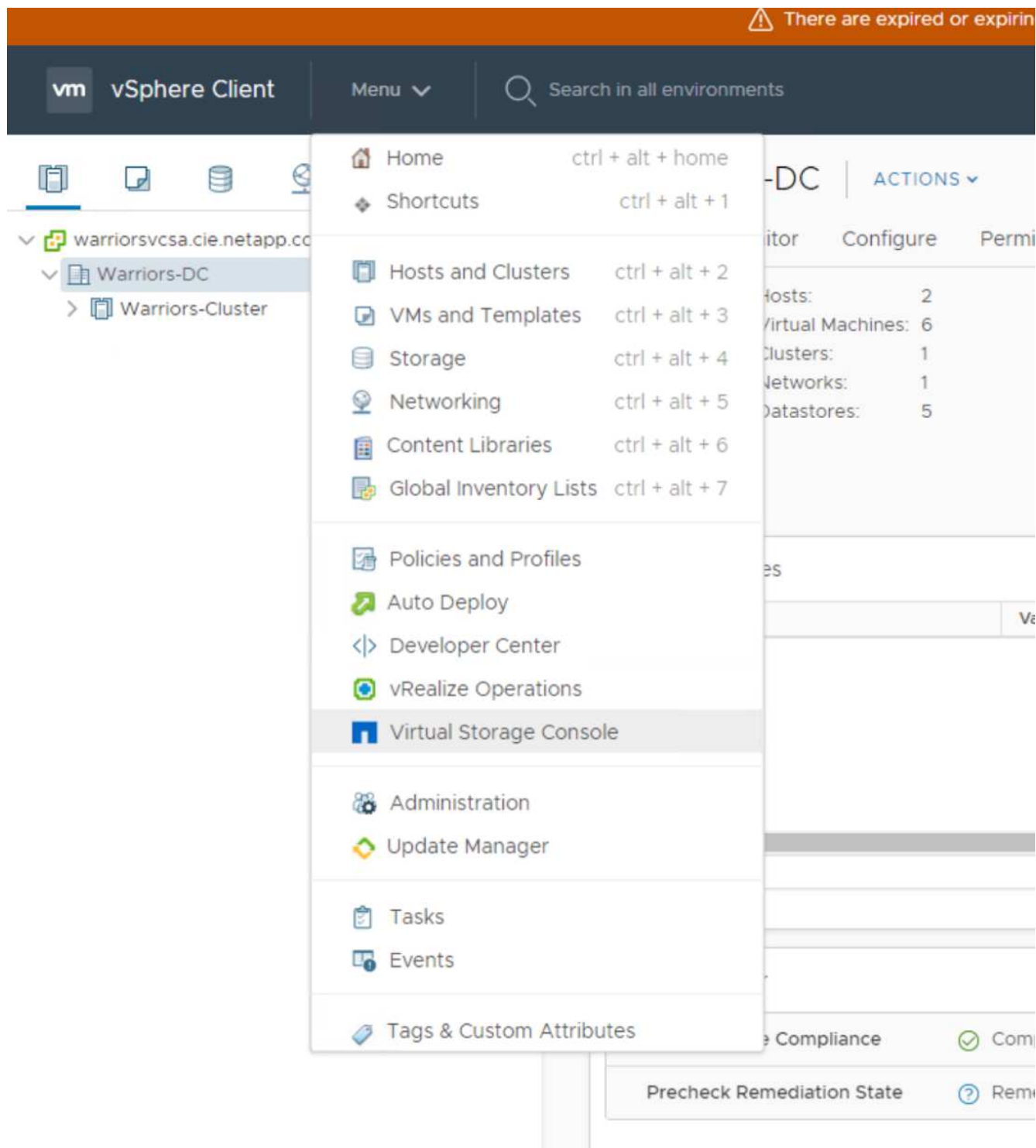
OR

Click on "Install VMware Tools" pop-up box on the vSphere Web Client.

2. Follow the prompts provided by the VMware Tools wizard.

Once you click on mount, the installation process will automatically continue.

13. Le informazioni sulla configurazione di rete e sulla registrazione di vCenter sono state fornite durante la personalizzazione del modello OVF. Pertanto, dopo l'esecuzione della VM NetApp-VSC, VSC, vSphere API for Storage Awareness (VASA) e VMware Storage Replication Adapter (SRA) vengono registrati in vCenter.
14. Disconnettersi dal client vCenter e accedere nuovamente. Dal menu Home, verificare che NetApp VSC sia installato.

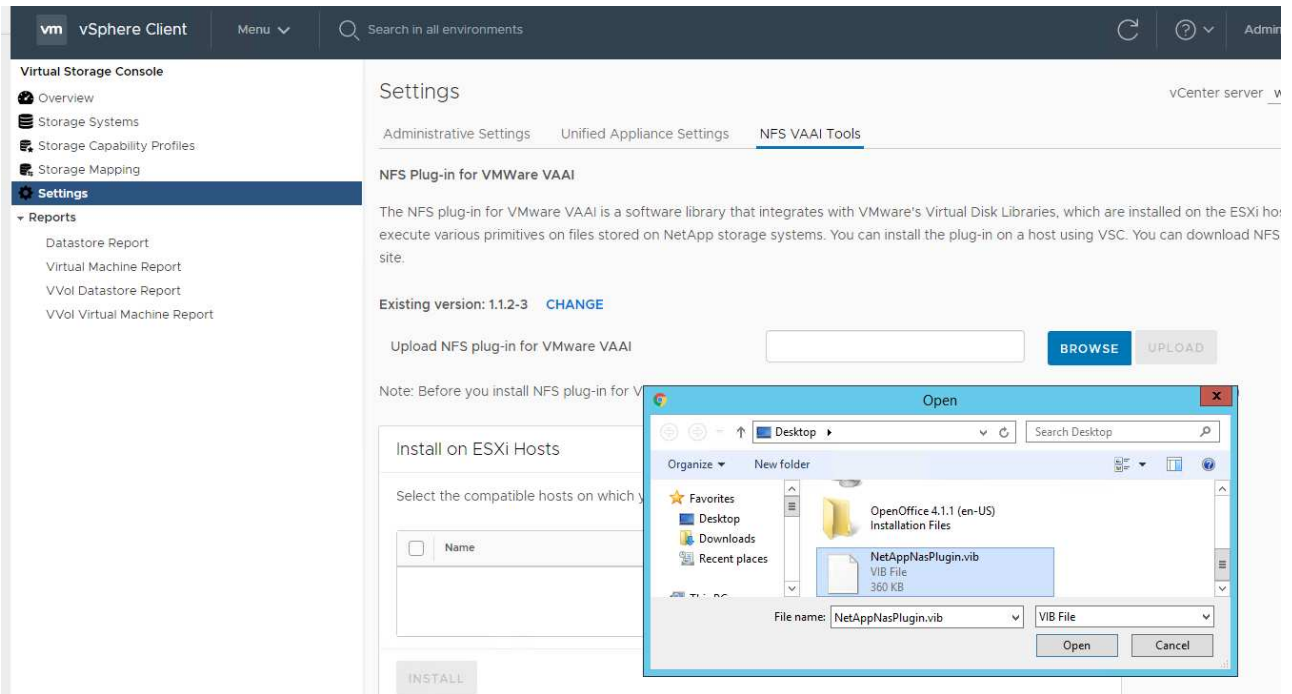


Scarica e installa il plug-in NetApp NFS VAAI

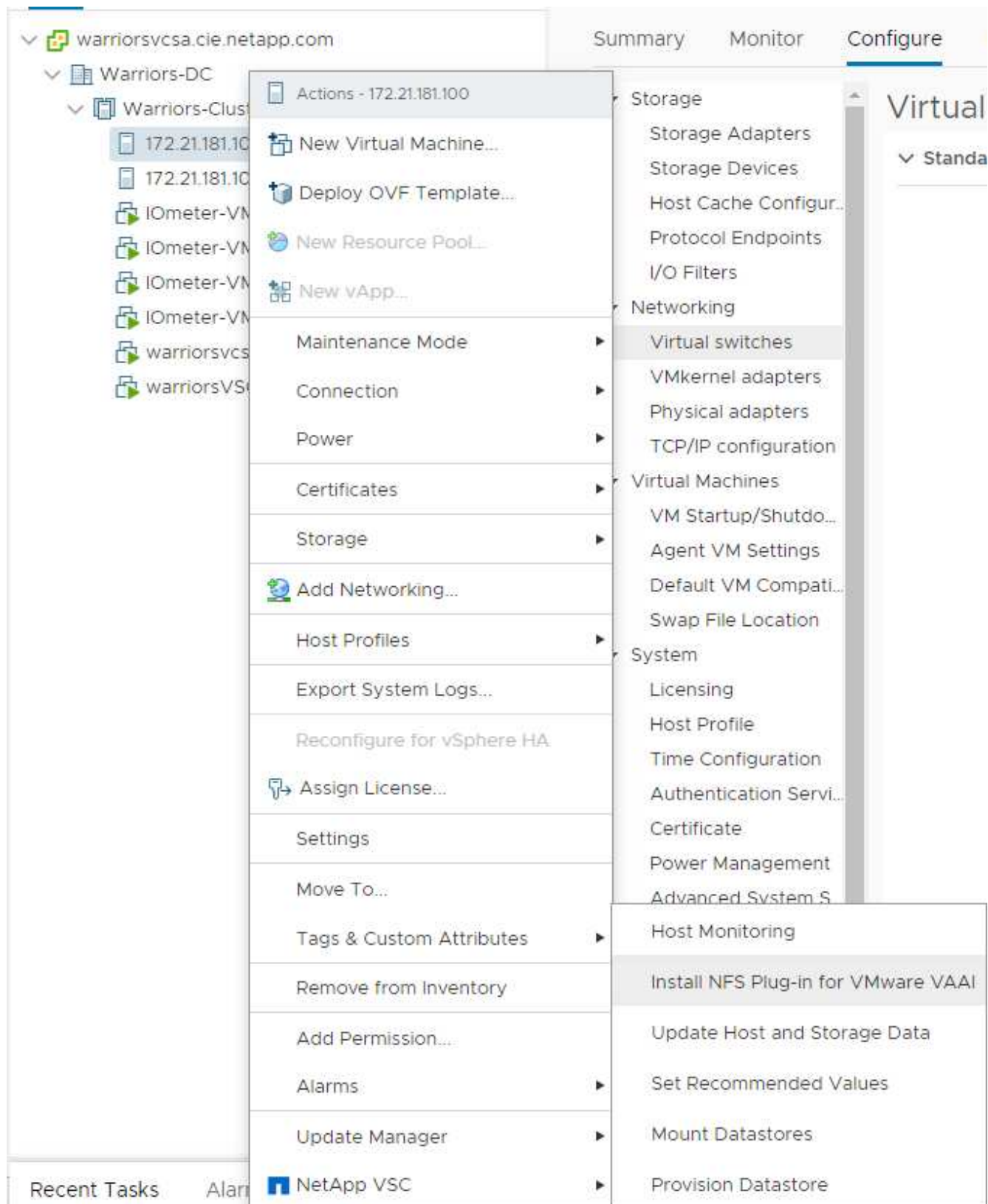
Per scaricare e installare il plug-in NetApp NFS VAAI, attenersi alla seguente procedura:

1. Scarica il plug-in NetApp NFS 1.1.2 per VMware .vib Dalla pagina di download del plug-in NFS e salvarlo sul computer locale o sull'host di amministrazione.
2. 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. Dalla schermata iniziale del client Web vSphere, selezionare Virtual Storage Console.
- d. In Virtual Storage Console > Settings > NFS VAAI Tools (Console di storage virtuale > Impostazioni > Strumenti NFS VAAI), caricare il plug-in NFS scegliendo Select file (Seleziona file) e selezionando la posizione in cui è memorizzato il plug-in scaricato.



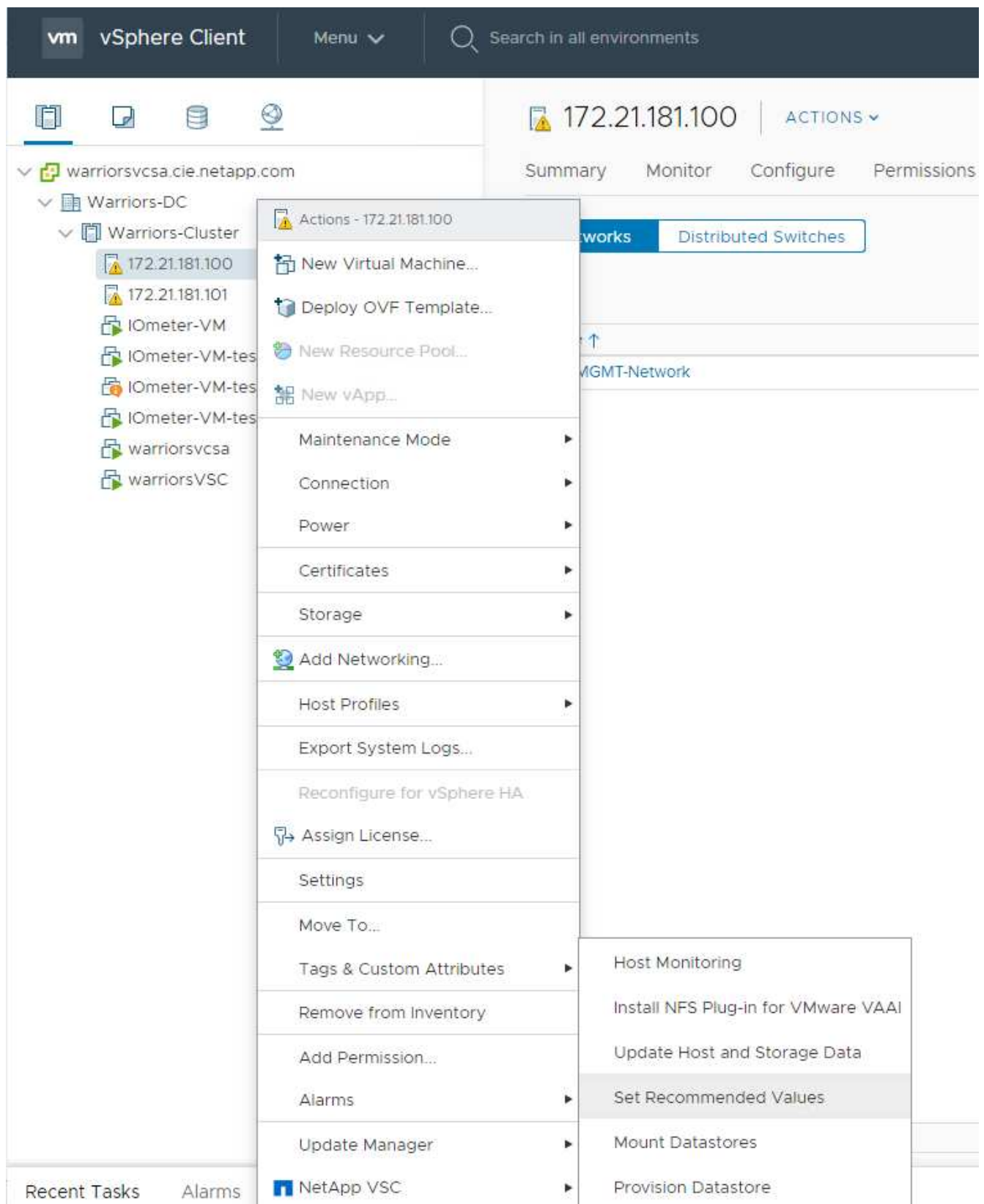
3. Fare clic su Upload (carica) per trasferire il plug-in a vCenter.
4. Selezionare l'host, quindi scegliere NetApp VSC > Install NFS Plug-in for VMware VAAI.



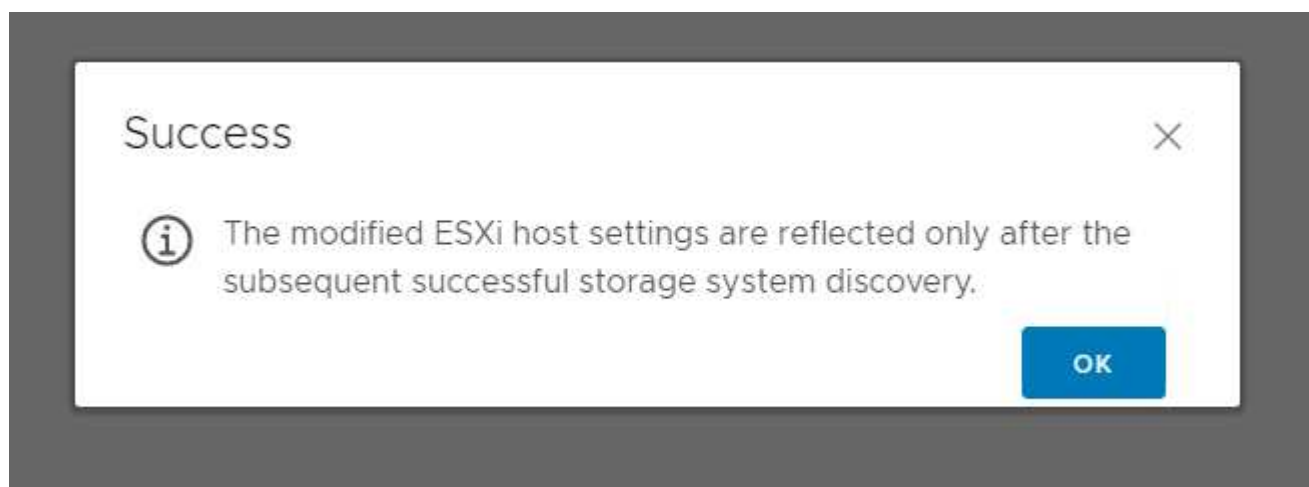
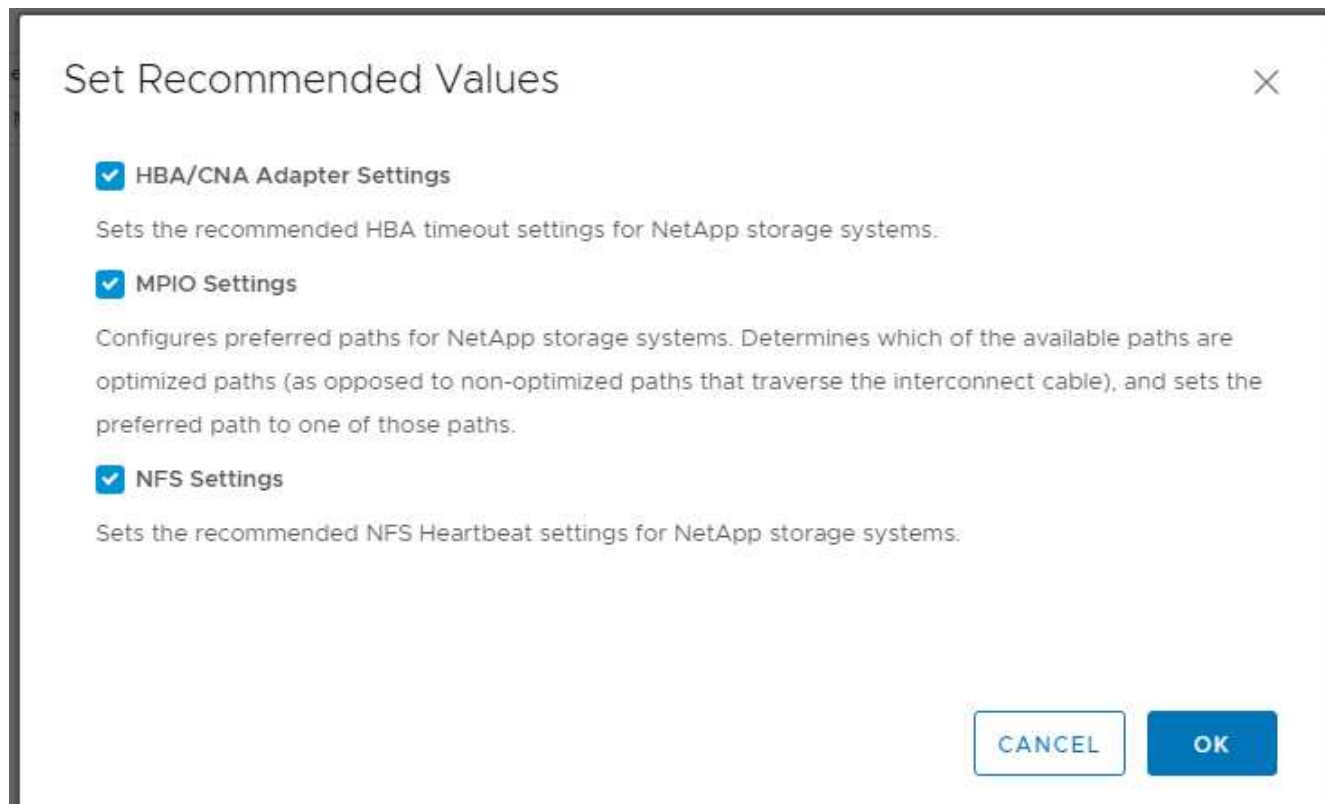
Utilizzare le impostazioni di storage ottimali per gli host ESXi

VSC consente la configurazione automatica delle impostazioni relative allo storage per tutti gli host ESXi connessi ai controller di storage NetApp. Per utilizzare queste impostazioni, attenersi alla seguente procedura:

1. Dalla schermata iniziale, selezionare vCenter > host e cluster. Per ciascun host ESXi, fare clic con il pulsante destro del mouse e selezionare NetApp VSC > Set Recommended Values (Imposta valori consigliati).



2. Controllare le impostazioni che si desidera applicare agli host vSphere selezionati. Fare clic su OK per applicare le impostazioni.



3. Riavviare L'host ESXi dopo aver applicato queste impostazioni.

Conclusion

FlexPod offre una soluzione semplice ed efficace grazie a un design validato che utilizza componenti leader del settore. Grazie alla scalabilità attraverso l'aggiunta di componenti, FlexPod può essere personalizzato in base alle specifiche esigenze di business. FlexPod Express è stato progettato per piccole e medie imprese, ROBOs e altre aziende che richiedono soluzioni dedicate.

Ringraziamenti

Gli autori desiderano ringraziare John George per il suo supporto e il suo contributo a questo progetto.

Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

Documentazione sui prodotti NetApp

[http://docs. "netapp"com](http://docs.netapp.com)

FlexPod Express con guida

NVA-1139-DESIGN: FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190

["https://www.netapp.com/us/media/nva-1139-design.pdf"](https://www.netapp.com/us/media/nva-1139-design.pdf)

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Novembre 2019	Release iniziale.

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.