



FlexPod Express

FlexPod

NetApp
March 25, 2024

Sommario

- FlexPod Express 1
 - Guida alla progettazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190 1
 - Guida all'implementazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190..... 8
 - Guida alla progettazione di FlexPod Express con Cisco UCS serie C e AFF serie A220 103
 - Guida all'implementazione di FlexPod Express con Cisco UCS serie C e AFF serie A220..... 113
 - FlexPod Express con VMware vSphere 6.7U1 e NetApp AFF A220 con storage basato su IP direct-attached 194
 - FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e NetApp AFF/FAS - NVA - implementazione 304

FlexPod Express

Guida alla progettazione di FlexPod Express con Cisco UCS serie C e NetApp AFF serie C190

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

Savita Kumari, NetApp

In collaborazione con:[Errore: Immagine grafica mancante]

Le tendenze del settore indicano una vasta 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 la tecnologia che conoscono nel proprio data center.

FlexPod è un'architettura di data center pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco, sulla famiglia di switch Cisco Nexus e sui sistemi NetApp AFF. I componenti di 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.

["Avanti: Riepilogo del programma."](#)

Riepilogo del programma

Portfolio di infrastrutture convergenti FlexPod

Le architetture di riferimento FlexPod vengono fornite come Cisco Validated Design (CVD) o come NetApp Verified Architectures (NVA). Le deviazioni basate sui requisiti del cliente rispetto a un determinato CVD o NVA sono consentite se tali variazioni non comportano l'implementazione di configurazioni non supportate.

Come illustrato nella figura seguente, il portfolio FlexPod include le seguenti soluzioni: FlexPod Express e FlexPod Datacenter.

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

[Errore: Immagine grafica mancante]

Programma NetApp Verified Architecture

Il programma NetApp Verified Architecture offre ai clienti un'architettura verificata per le soluzioni NetApp. Una soluzione NVA ha le seguenti qualità:

- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione

- Accelera il time-to-market questa guida illustra in dettaglio la progettazione di FlexPod con VMware vSphere.

Inoltre, questo design sfrutta il nuovissimo sistema AFF C190, che esegue il software NetApp ONTAP 9.6, gli switch Cisco Nexus 31108 e i server Cisco UCS C220 M5 come nodi hypervisor.

Panoramica della soluzione

FlexPod Express è progettato per eseguire carichi di lavoro di virtualizzazione misti. È destinato alle filiali e alle filiali e alle piccole e medie imprese. È inoltre ottimale per le aziende più grandi che desiderano implementare una soluzione dedicata per uno scopo specifico. Questa nuova soluzione per FlexPod aggiunge nuove tecnologie come NetApp ONTAP 9.6, il sistema NetApp AFF C190 e VMware vSphere 6.7U2.

La figura seguente mostra i componenti hardware inclusi nella soluzione FlexPod Express.

[Errore: Immagine grafica mancante]

Pubblico di riferimento

Questo documento è destinato a coloro che desiderano sfruttare un'infrastruttura costruita per garantire l'efficienza DELL'IT e consentire l'innovazione DELL'IT. I destinatari di questo documento includono, a titolo esemplificativo ma non esaustivo, tecnici di vendita, consulenti sul campo, personale di servizi professionali, responsabili IT, partner engineer e clienti.

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. È dotato del nuovo sistema NetApp AFF C190, che esegue il software ONTAP 9.6, due switch Cisco Nexus 31108 e server rack Cisco UCS C220 M5 che eseguono VMware vSphere 6.7U2. Questa soluzione validata, illustrata nella figura seguente, utilizza la tecnologia 10 Gigabit Ethernet (10 GbE). Viene inoltre fornita una guida su come scalare aggiungendo due nodi hypervisor alla volta, in modo che l'architettura FlexPod Express possa adattarsi alle esigenze di business in evoluzione di un'organizzazione.

[Errore: Immagine grafica mancante]

["Successivo: Requisiti tecnologici."](#)

Requisiti tecnologici

FlexPod richiede una combinazione di componenti hardware e software che dipende dall'hypervisor selezionato e dalla velocità di rete. Inoltre, FlexPod Express definisce 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 questa configurazione FlexPod Express e per implementare questa soluzione. I componenti hardware utilizzati in qualsiasi implementazione della soluzione possono variare in base ai requisiti del cliente.

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

Requisiti software

La seguente tabella elenca i componenti software necessari per implementare le architetture della soluzione FlexPod Express.

Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	4.0.4	Per server rack C220 M5
Sistema operativo Cisco NX	7.0(3)I7(6)	Per switch Cisco Nexus 31108
NetApp ONTAP	9.6	Per i controller NetApp AFF C190

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

Software	Versione
Appliance server VMware vCenter	6.7U2
VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI per ESXi	1.1.2
Virtual Storage Console di NetApp	9.6

"Avanti: [Scelte di progettazione.](#)"

Scelte di progettazione

Le tecnologie elencate in questa sezione sono state scelte durante la fase di progettazione architetturale. Ogni tecnologia ha uno scopo specifico nella soluzione di infrastruttura FlexPod Express.

NetApp AFF serie C190 con ONTAP 9.6

Questa soluzione sfrutta due dei più recenti prodotti NetApp: Il sistema NetApp AFF C190 e il software ONTAP 9.6.

Sistema AFF C190

Il gruppo di destinazione è costituito dai clienti che desiderano modernizzare la propria infrastruttura IT con tecnologia all-flash a un prezzo conveniente. Il sistema AFF C190 viene fornito con il nuovo ONTAP 9.6 e le licenze del bundle flash, il che significa che sono integrate le seguenti funzioni:

- CIFS, NFS, iSCSI e FCP
- Software di replica dei dati NetApp SnapMirror, software di backup NetApp SnapVault, software di ripristino dei dati NetApp SnapRestore, suite di prodotti software per la gestione dello storage NetApp SnapManager e software NetApp SnapCenter
- Tecnologia FlexVol
- Deduplica, compressione e compattazione
- Thin provisioning
- QoS dello storage
- Tecnologia NetApp RAID DP
- Tecnologia Snapshot di NetApp
- FabricPool

Le seguenti figure mostrano le due opzioni per la connettività host.

La figura seguente illustra le porte UTA 2 in cui è possibile inserire il modulo SFP+.

[Errore: Immagine grafica mancante]

La figura seguente illustra le porte 10GBASE-T per il collegamento tramite cavi Ethernet RJ-45 convenzionali.

[Errore: Immagine grafica mancante]



Per l'opzione della porta 10GBASE-T, è necessario disporre di uno switch uplink basato su 10GBASE-T.

Il sistema AFF C190 è offerto esclusivamente con SSD da 960 GB. È possibile scegliere tra quattro fasi di espansione:

- 8x 960 GB
- 12x 960 GB
- 18x 960 GB
- 24x 960 GB

Per informazioni complete sul sistema hardware AFF C190, consultare ["Pagina dell'array all-flash NetApp AFF C190"](#).

Software ONTAP 9.6

I sistemi NetApp AFF C190 utilizzano il nuovo software per la gestione dei dati ONTAP 9.6. ONTAP 9.6 è il software per la gestione dei dati aziendali leader del settore. Combina nuovi livelli di semplicità e flessibilità con potenti funzionalità di gestione dei dati, efficienza dello storage e integrazione cloud leader del settore.

ONTAP 9.6 dispone di diverse funzionalità adatte alla soluzione FlexPod Express. In primo luogo, l'impegno di NetApp per l'efficienza dello storage, che può essere una delle funzionalità più importanti per le piccole implementazioni. Le caratteristiche di efficienza dello storage di NetApp come deduplica, compressione, compattazione e thin provisioning sono disponibili in ONTAP 9.6. Il sistema NetApp WAFL scrive sempre blocchi da 4 KB; pertanto, la compattazione combina più blocchi in un blocco da 4 KB quando i blocchi non utilizzano lo spazio allocato di 4 KB. La seguente figura illustra questo processo.

[Errore: Immagine grafica mancante]

ONTAP 9.6 ora supporta una dimensione del blocco opzionale da 512 byte per i volumi NVMe. Questa funzionalità funziona bene con VMware Virtual Machine file System (VMFS), che utilizza in modo nativo un blocco da 512 byte. È possibile mantenere la dimensione predefinita del 4K o, se si desidera, impostare la dimensione del blocco di 512 byte.

Altri miglioramenti delle funzionalità di ONTAP 9.6 includono:

- **NetApp aggregate Encryption (NAE).** NAE assegna le chiavi a livello di aggregato, crittografando così tutti i volumi nell'aggregato. Questa funzione consente di crittografare e deduplicare i volumi a livello di aggregato.
- **Ottimizzazione dei volumi NetApp ONTAP FlexGroup.** In ONTAP 9.6, è possibile rinominare facilmente un volume FlexGroup. Non è necessario creare un nuovo volume in cui migrare i dati. Le dimensioni del volume possono essere ridotte anche utilizzando Gestione di sistema o CLI di ONTAP.
- **Miglioramento FabricPool.** ONTAP 9.6 ha aggiunto il supporto aggiuntivo per gli archivi di oggetti come Tier cloud. All'elenco è stato aggiunto anche il supporto per Google Cloud e Alibaba Cloud Object Storage Service (OSS). FabricPool supporta diversi archivi di oggetti, tra cui AWS S3, Azure Blob, IBM Cloud Object Storage e il software di storage basato su oggetti NetApp StorageGRID.
- **Miglioramento di SnapMirror.** in ONTAP 9.6, una nuova relazione di replica del volume viene crittografata per impostazione predefinita prima di lasciare l'array di origine e viene decrittografata nella destinazione di SnapMirror.

Cisco Nexus serie 3000

Cisco Nexus 31108PC-V è uno switch top-of-rack (Tor) basato su SFP+ a 10 Gbps con 48 porte SFP+ e 6 porte QSFP28. Ciascuna porta SFP+ può funzionare a 100 Mbps, 10 Gbps e ciascuna porta QSFP28 può funzionare in modalità nativa a 100 Gbps o 40 Gbps o in modalità 4x 10 Gbps, offrendo opzioni di migrazione flessibili. Questo switch è un vero switch senza PHY ottimizzato per bassa latenza e basso consumo energetico.

La specifica Cisco Nexus 31108PC-V include i seguenti componenti:

- Capacità di switching di 2,16 Tbps e velocità di inoltro fino a 1,2 Tbps per 31108 PC-V.
- 48 porte SFP supportano 1 e 10 Gigabit Ethernet (10 GbE); 6 porte QSFP28 supportano 4 porte 10 GbE o 40 GbE ciascuna o 100 GbE

La figura seguente illustra lo switch Cisco Nexus 31108PC-V.

[Errore: Immagine grafica mancante]

Per ulteriori informazioni sugli switch Cisco Nexus 31108PC-V, vedere "[Scheda tecnica degli switch Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL e 3172TQ-XL](#)".

Cisco UCS C-Series

Il server rack Cisco UCS C-Series è stato scelto per FlexPod Express perché le sue numerose opzioni di configurazione consentono di adattarlo a requisiti specifici in un'implementazione FlexPod Express.

I server rack Cisco UCS C-Series offrono computing unificato in un fattore di forma standard di settore per ridurre il TCO e aumentare l'agilità.

I server rack Cisco UCS C-Series offrono i seguenti vantaggi:

- Un punto di ingresso indipendente dal fattore di forma in Cisco UCS

- Implementazione semplificata e rapida delle applicazioni
- Estensione delle innovazioni e dei vantaggi di Unified Computing ai server rack
- Maggiore scelta per i clienti con vantaggi esclusivi in un pacchetto rack familiare

[Errore: Immagine grafica mancante]

Il server rack Cisco UCS C220 M5, mostrato nella figura precedente, è tra i server per applicazioni e infrastrutture aziendali generici più versatili del settore. Si tratta di un server rack a due socket ad alta densità che offre performance ed efficienza leader di settore per un'ampia gamma di carichi di lavoro, tra cui virtualizzazione, collaborazione e applicazioni bare-metal. I server rack Cisco UCS C-Series possono essere implementati come server standalone o come parte di Cisco UCS per sfruttare le innovazioni di Unified Computing basate su standard di Cisco che aiutano a ridurre il TCO dei clienti e ad aumentare l'agilità del business.

Per ulteriori informazioni sui server C220 M5, vedere ["Scheda informativa sul server rack Cisco UCS C220 M5"](#).

Connettività Cisco UCS VIC 1457 per server rack C220 M5

L'adattatore Cisco UCS VIC 1457 mostrato nella figura seguente è una scheda modulare SFP (Small Form Factor Pluggable) a quattro porte su scheda madre (mLOM) progettata per la generazione M5 dei server Cisco UCS C-Series. La scheda supporta Ethernet a 10/25Gbps o FCoE. La scheda può presentare all'host interfacce conformi agli standard PCIe, che possono essere configurate dinamicamente come schede di rete o HBA.

[Errore: Immagine grafica mancante]

Per informazioni complete sull'adattatore Cisco UCS VIC 1457, vedere ["Scheda informativa Cisco UCS Virtual Interface Card serie 1400"](#).

VMware vSphere 6.7U2

VMware vSphere 6.7U2 è una delle opzioni di hypervisor da utilizzare con FlexPod Express. VMware vSphere consente alle organizzazioni di ridurre l'impatto di energia e raffreddamento, confermando che la capacità di calcolo acquistata viene utilizzata al massimo. Inoltre, VMware vSphere consente la protezione dai guasti hardware (VMware High Availability o VMware ha) e il bilanciamento del carico delle risorse di calcolo in un cluster di host vSphere (VMware Distributed Resource Scheduler in modalità di manutenzione o VMware DRS-MM).

Poiché riavvia solo il kernel, VMware vSphere 6.7U2 consente ai clienti di eseguire un avvio rapido, caricando vSphere ESXi senza riavviare l'hardware. Il client vSphere 6.7U2 (client basato su HTML5) presenta alcuni nuovi miglioramenti, come Developer Center con cattura del codice e API Explore. Con Code Capture, puoi registrare le tue azioni nel client vSphere per fornire un output di codice semplice e utilizzabile. VSphere 6.7U2 contiene anche nuove funzionalità come DRS in modalità di manutenzione (DRS-MM).

VMware vSphere 6.7U2 offre le seguenti funzionalità:

- VMware sta deprecando il modello di implementazione di VMware Platform Services Controller (PSC) esterno.



A partire dalla prossima release principale di vSphere, PSC esterno non sarà un'opzione disponibile.

- Nuovo supporto del protocollo per il backup e il ripristino di un'appliance server vCenter. Introduzione di NFS e SMB come protocolli supportati, fino a 7 in totale (HTTP, HTTPS, FTP, FTPS, SCP, NFS e SMB) durante la configurazione di vCenter Server per operazioni di backup o ripristino basate su file.
- Nuovo dal punto di vista funzionale quando si utilizza la libreria di contenuti. La sincronizzazione di un modello VM nativo tra le librerie di contenuti è ora disponibile quando vCenter Server è configurato per la modalità link avanzata.
- Eseguire l'aggiornamento a "[Pagina Plug-in client](#)".
- VMware vSphere Update Manager aggiunge inoltre miglioramenti al client vSphere. È possibile eseguire la conformità con il controllo degli attach-check e le azioni correttive da un'unica schermata.

Per ulteriori informazioni su VMware vSphere 6.7 U2, consultare "[Pagina del blog VMware vSphere](#)".

Per ulteriori informazioni sugli aggiornamenti di VMware vCenter Server 6.7 U2, vedere "[Note di rilascio](#)".



Sebbene questa soluzione sia stata validata con vSphere 6.7U2, supporta qualsiasi versione vSphere qualificata con gli altri componenti da "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)". NetApp consiglia di implementare la versione successiva di vSphere per le correzioni e le funzionalità avanzate.

Architettura di boot

Le opzioni supportate per l'architettura di boot FlexPod Express includono:

- LUN SAN iSCSI
- Scheda SD Cisco FlexFlash
- Disco locale

FlexPod Datacenter viene avviato da LUN iSCSI; pertanto, la gestibilità della soluzione viene migliorata utilizzando anche l'avvio iSCSI per FlexPod Express.

Layout della scheda di interfaccia di rete virtuale host ESXi

Cisco UCS VIC 1457 dispone di quattro porte fisiche. Questa convalida della soluzione include queste quattro porte fisiche nell'utilizzo dell'host ESXi. Se si dispone di un numero inferiore o superiore di schede di rete, è possibile che siano presenti numeri VMNIC diversi.

In un'implementazione di boot iSCSI, l'avvio iSCSI richiede schede di interfaccia di rete virtuali (vNIC) separate per l'avvio iSCSI. Queste vNIC utilizzano la VLAN iSCSI del fabric appropriata come VLAN nativa e sono collegate agli vSwitch di avvio iSCSI, come mostrato nella figura seguente.

[Errore: Immagine grafica mancante]

["Prossimo: Conclusione."](#)

Conclusione

Il design convalidato FlexPod Express è una soluzione semplice ed efficace che utilizza componenti leader del settore. Grazie alla scalabilità e all'offerta di opzioni per la piattaforma hypervisor, FlexPod Express può essere personalizzato in base alle specifiche esigenze di business. FlexPod Express è stato progettato per le piccole e medie imprese, le filiali e le filiali remote e altre aziende che richiedono soluzioni

dedicate.

"Avanti: Dove trovare ulteriori informazioni."

Dove trovare ulteriori informazioni

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

- Centro di documentazione dei sistemi AFF e FAS

["https://docs.netapp.com/platstor/index.jsp"](https://docs.netapp.com/platstor/index.jsp)

- Pagina delle risorse di documentazione di AFF

["https://www.netapp.com/us/documentation/all-flash-fas.aspx"](https://www.netapp.com/us/documentation/all-flash-fas.aspx)

- Guida all'implementazione di FlexPod con VMware vSphere 6.7 e NetApp AFF C190 (in corso)
- Documentazione NetApp

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

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

Programma NetApp Verified Architecture

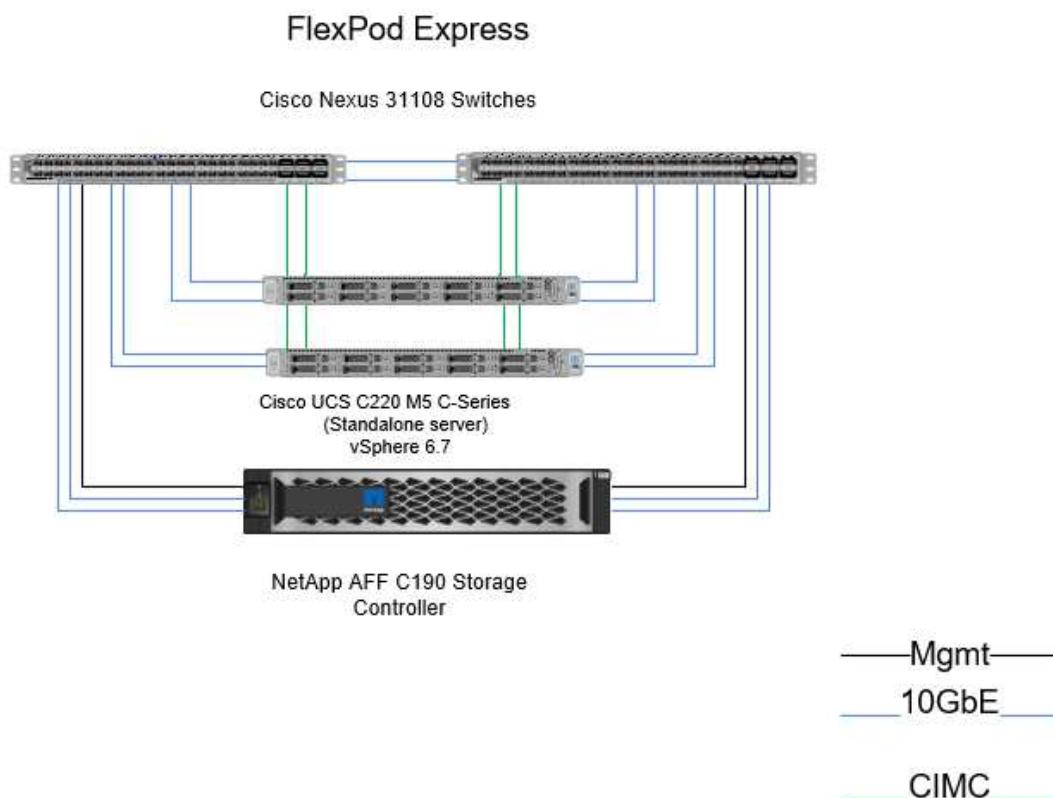
Il programma NetApp Verified Architecture offre ai clienti un'architettura verificata per le soluzioni NetApp. Un'architettura verificata di NetApp offre un'architettura della soluzione NetApp con le seguenti qualità:

- 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 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
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.

Cisco Nexus
31108PC-V A



Cisco Nexus
31108PC-V B



Cisco UCS
C220 M5 A



Cisco UCS
C220 M5 B



NetApp
AFF C190 A

NetApp
AFF C190 B

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
```

Eseguire la configurazione globale del canale della porta virtuale

Un VPC (Virtual Port Channel) consente ai collegamenti fisicamente collegati a due diversi switch Cisco Nexus di apparire come un singolo canale di porta su un terzo dispositivo. Il terzo dispositivo può essere uno switch, un server o qualsiasi altro dispositivo di rete. Un VPC è in grado di fornire il multipathing 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:

<input checked="" type="checkbox"/>	Email	SMTP Mail Host <input type="text"/>	Email Addresses <input type="text" value="Separate email addresses with a comma..."/>
<hr/>			
<input type="checkbox"/>	SNMP	SNMP Trap Host <input type="text"/>	
<hr/>			
<input type="checkbox"/>	Syslog	Syslog Server <input type="text"/>	
<hr/>			

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.

Eseguire 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 ☒ [X]

b. IP (di base):

IPV4: ☒ [X]

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: ☒ [X]

```

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 ▼

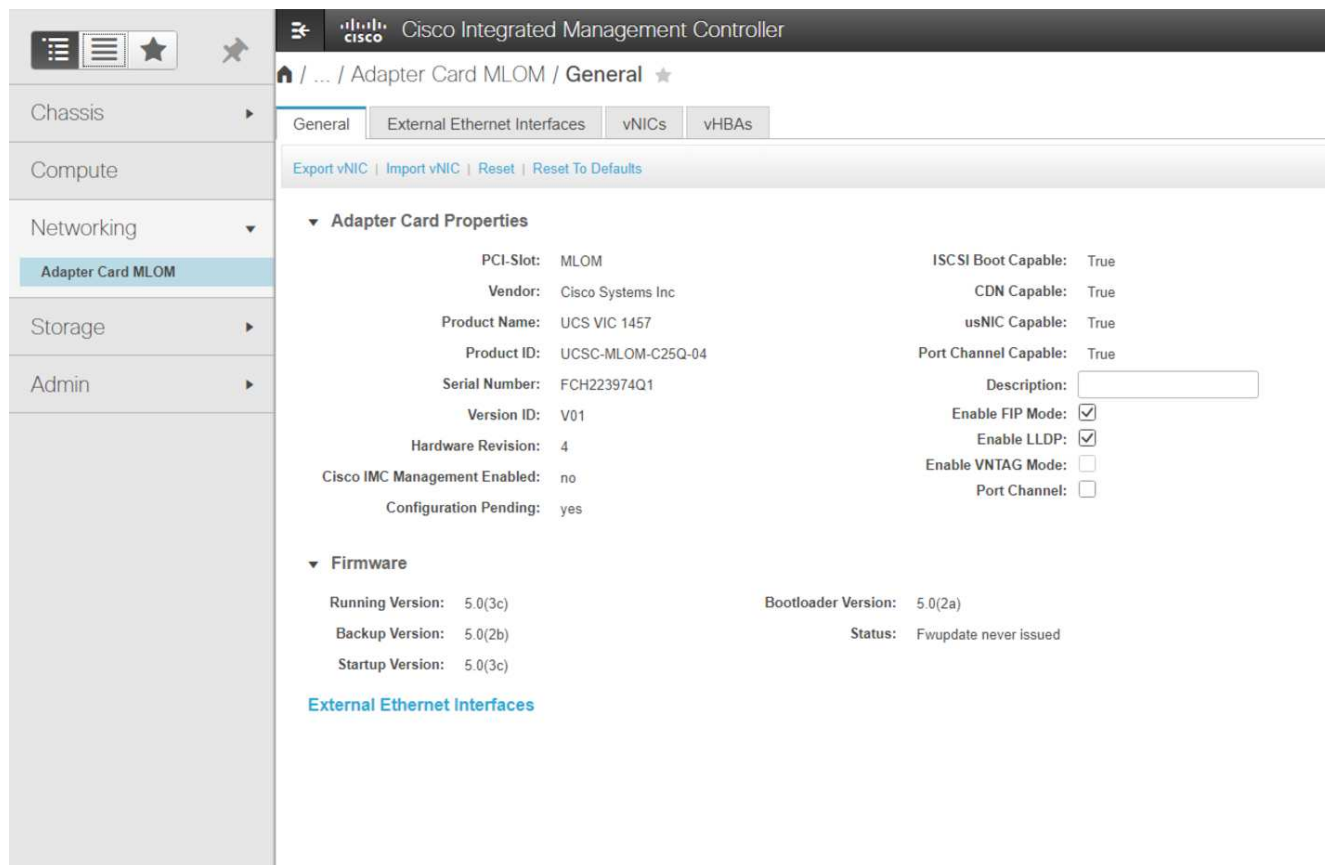
Configurare Cisco VIC1457 per l'avvio iSCSI

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>>

The screenshot shows the 'iSCSI Boot Properties' configuration window for vNIC 'eth1'. The 'Initiator' section contains fields for Name (iqn.1992-01.com.cisco.ucsa-01), IP Address (172.21.183.110), Subnet Mask (255.255.255.0), Gateway (172.21.183.1), and Primary DNS. The 'Primary Target' section contains fields for Name (iqn.1992-08.com.netapp.sn.e42fa6b2d2), IP Address (172.21.183.105), and TCP Port (3260). The 'Secondary Target' section contains fields for Name (iqn.1992-08.com.netapp.sn.e42fa6b2d2), IP Address (172.21.183.106), and TCP Port (3260). On the right, there are fields for Initiator Priority (primary), Secondary DNS, TCP Timeout (15), CHAP Name, CHAP Secret, Boot LUN (0), and CHAP Name/Secret for both primary and secondary targets. A blue button at the bottom left says '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>>

Adapter Card MLOM / vNICs

General External Ethernet Interfaces vNICs vHBAs

vNIC Properties

iSCSI Boot Properties

General

Initiator

Name: iqn.1992-01.com.cisco.ucsa-02 (0 - 222) chars

IP Address: 172.21.184.110

Subnet Mask: 255.255.255.0

Gateway: 172.21.184.1

Primary DNS:

Initiator Priority: primary

Secondary DNS:

TCP Timeout: 15 (0 - 255)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

Primary Target

Name: iqn.1992-08.com.netapp.sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.184.105

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

Secondary Target

Name: iqn.1992-08.com.netapp.sn.e42fa6b2d2 (0 - 222) chars

IP Address: 172.21.184.106

TCP Port: 3260

Boot LUN: 0 (0 - 65535)

CHAP Name: (0 - 49) chars

CHAP Secret: (0 - 49) chars

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

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.



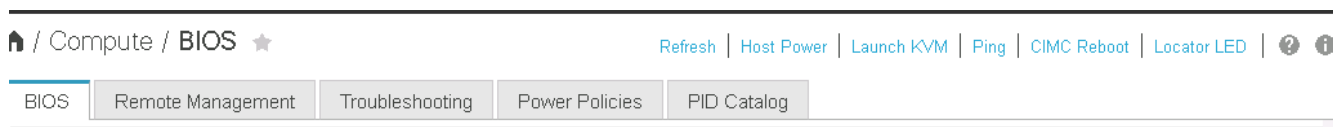
Questa procedura deve essere completata per tutti i nodi aggiuntivi aggiunti al cluster.

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.

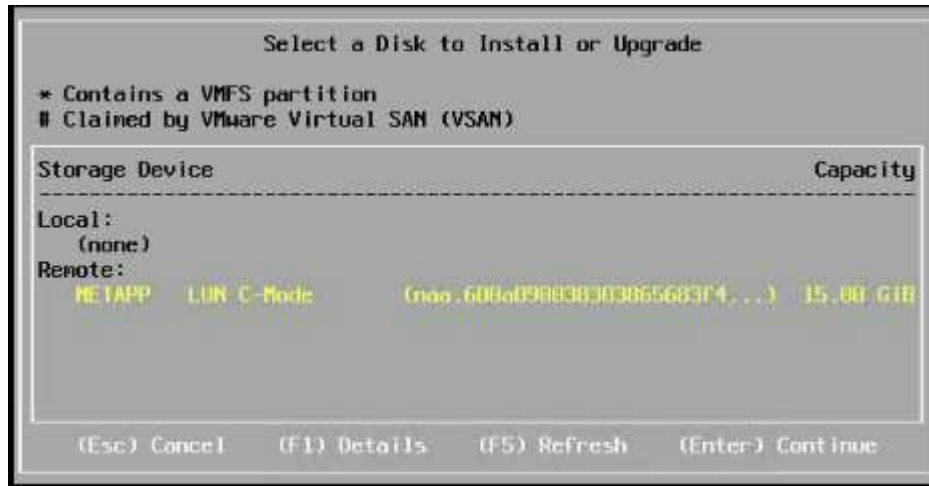
Installare VMware ESXi

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 deselegionando 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

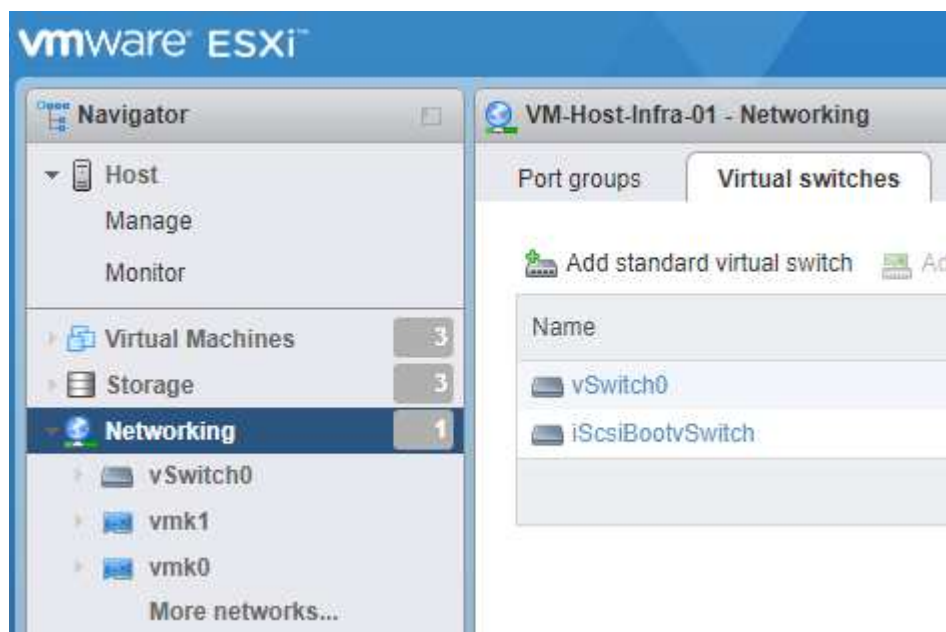
Per accedere all'host ESXi, attenersi alla seguente procedura:

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

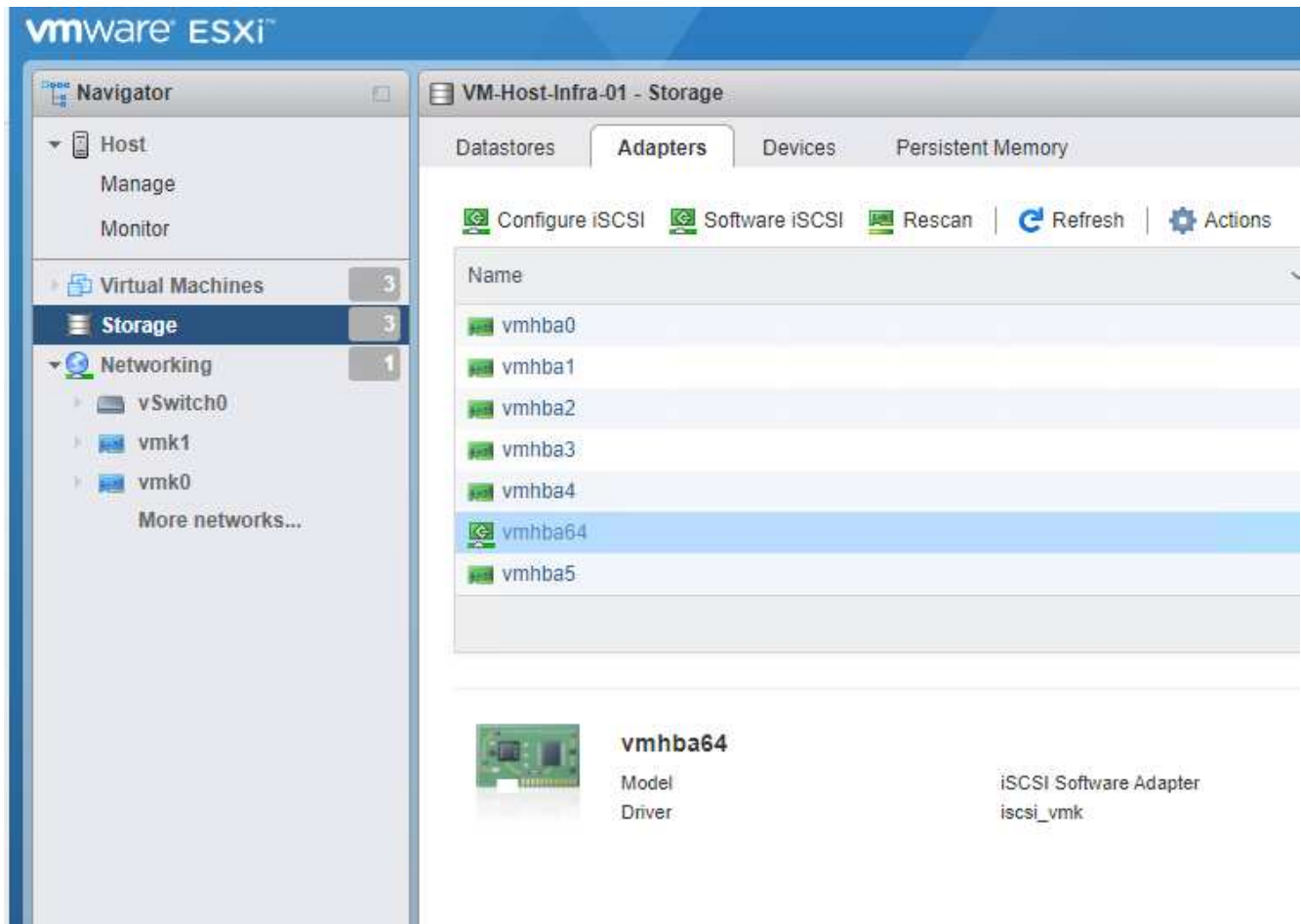
 vmnic5

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



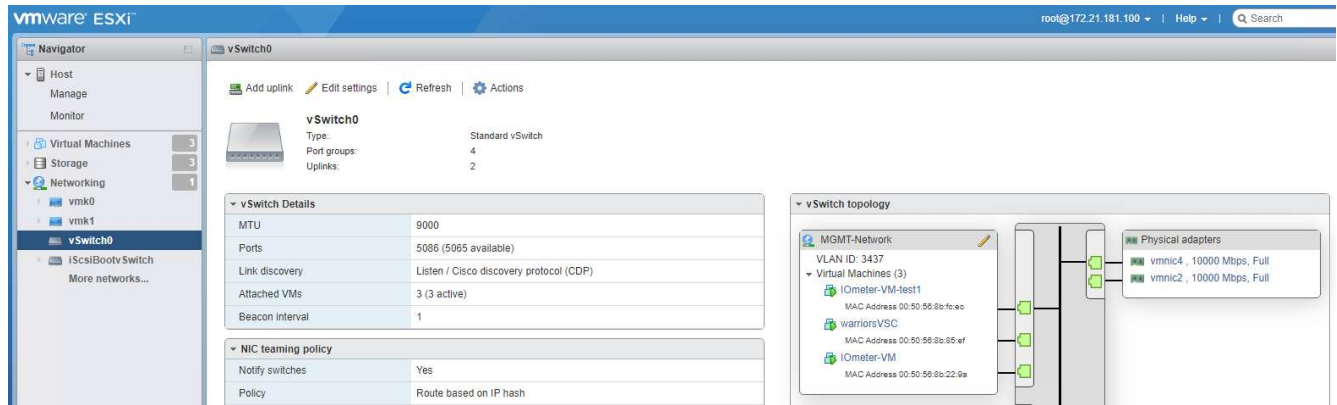
È possibile trovare gli indirizzi IP LIF iSCSI eseguendo il comando di visualizzazione dell'interfaccia di rete sul cluster NetApp o osservando la scheda Network Interfaces (interfacce di rete) in System Manager.

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.

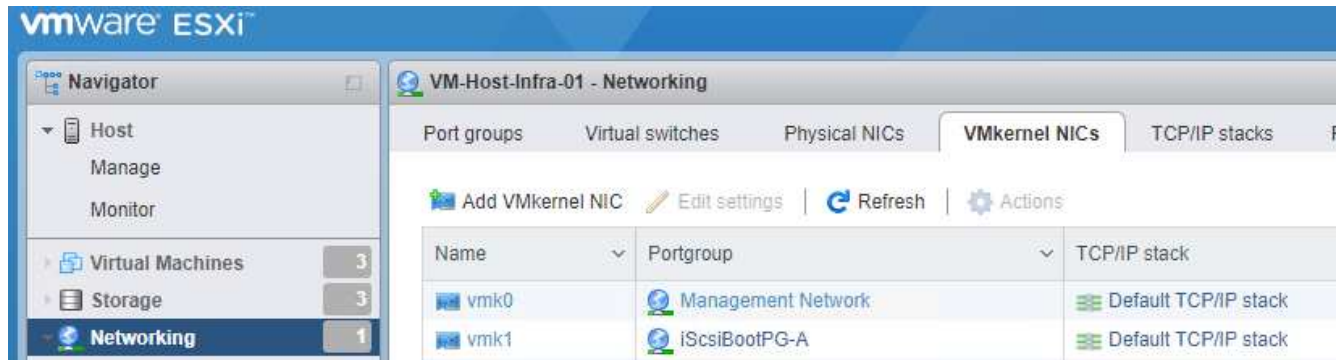
Configurare i gruppi di porte e le NIC VMkernel

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
<div>Create Cancel</div>	

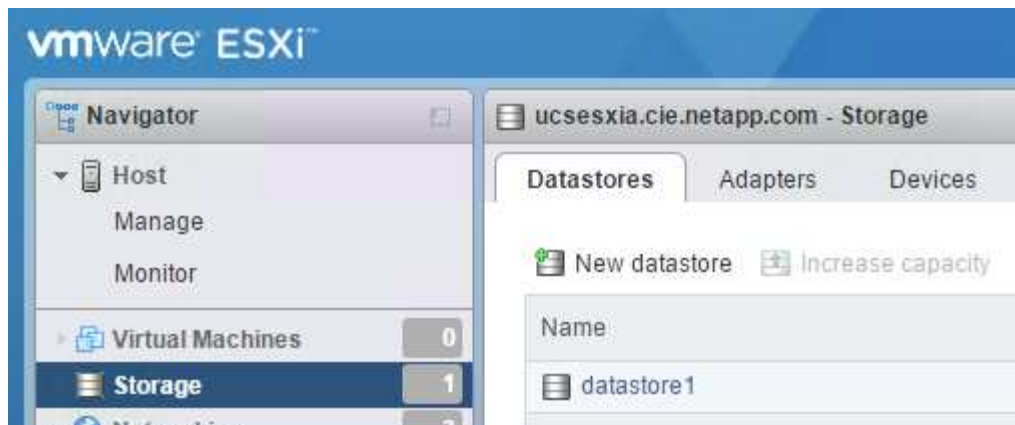


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

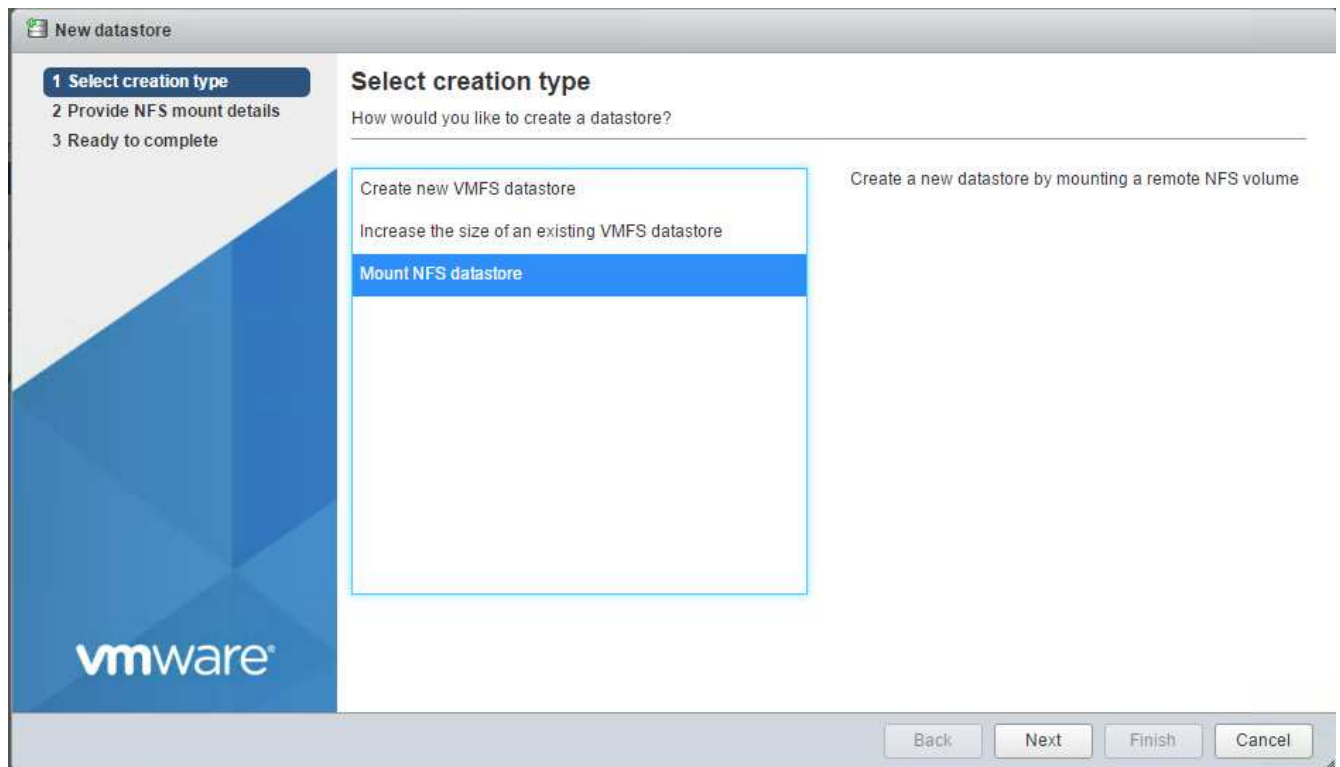
Montare i primi datastore

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:

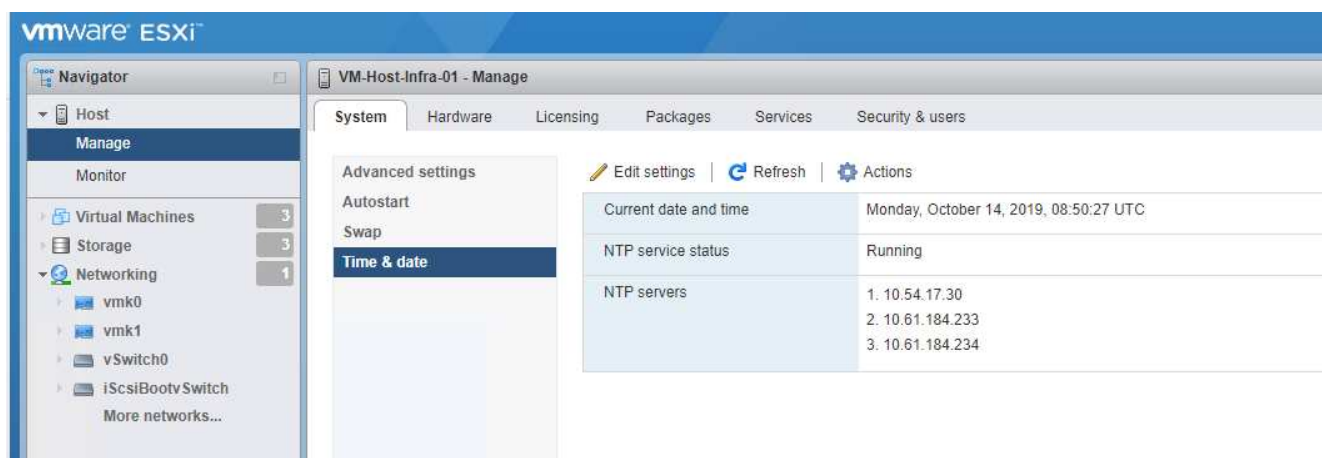
- Nome: `infra_swap`
- Server NFS: `<<var_nodea_nfs_lif>>`
- Condividere: `/infra_swap`

- Assicurarsi che sia selezionato NFS 3.

Configurare NTP

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

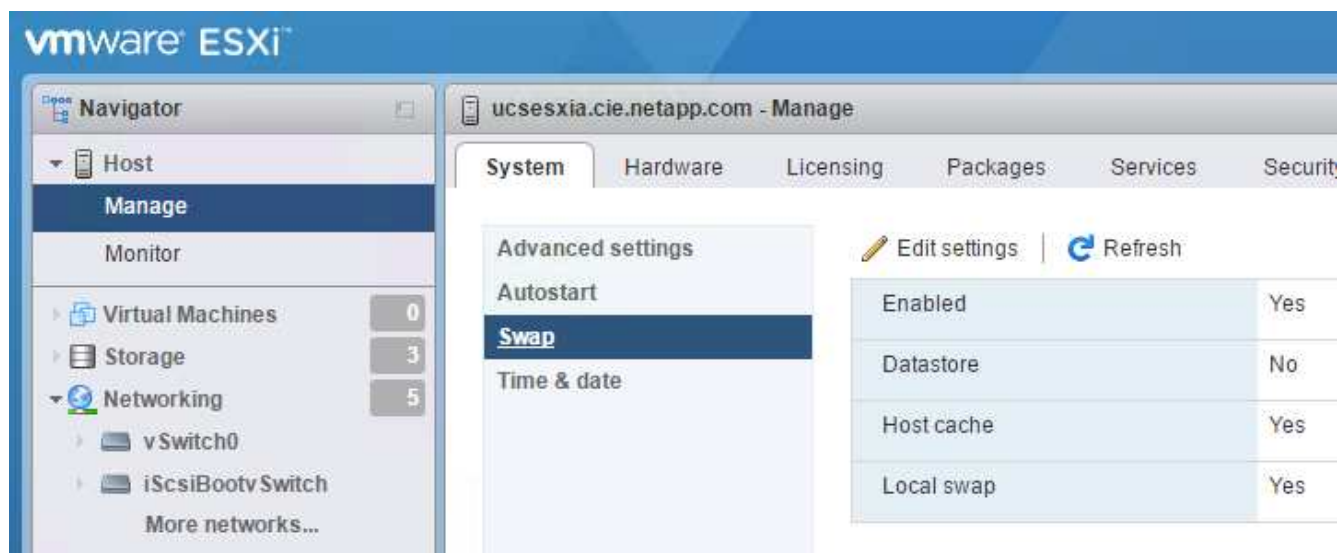
1. Fare clic su Manage (Gestisci) nel riquadro di navigazione a sinistra. Selezionare sistema nel riquadro di destra, quindi fare clic su Data e ora.
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio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

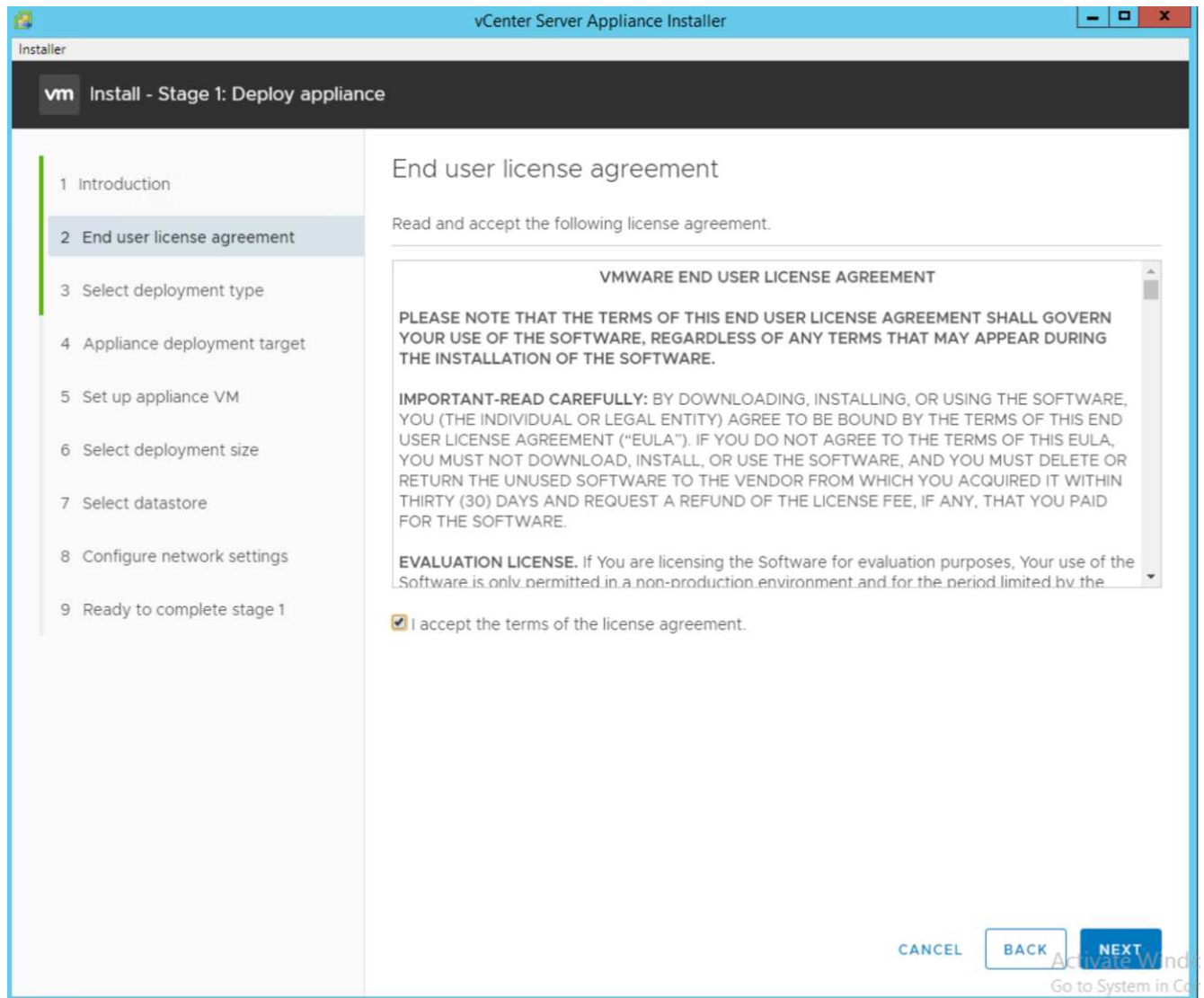


FlexPod utilizza l'appliance server vCenter (VCSA).

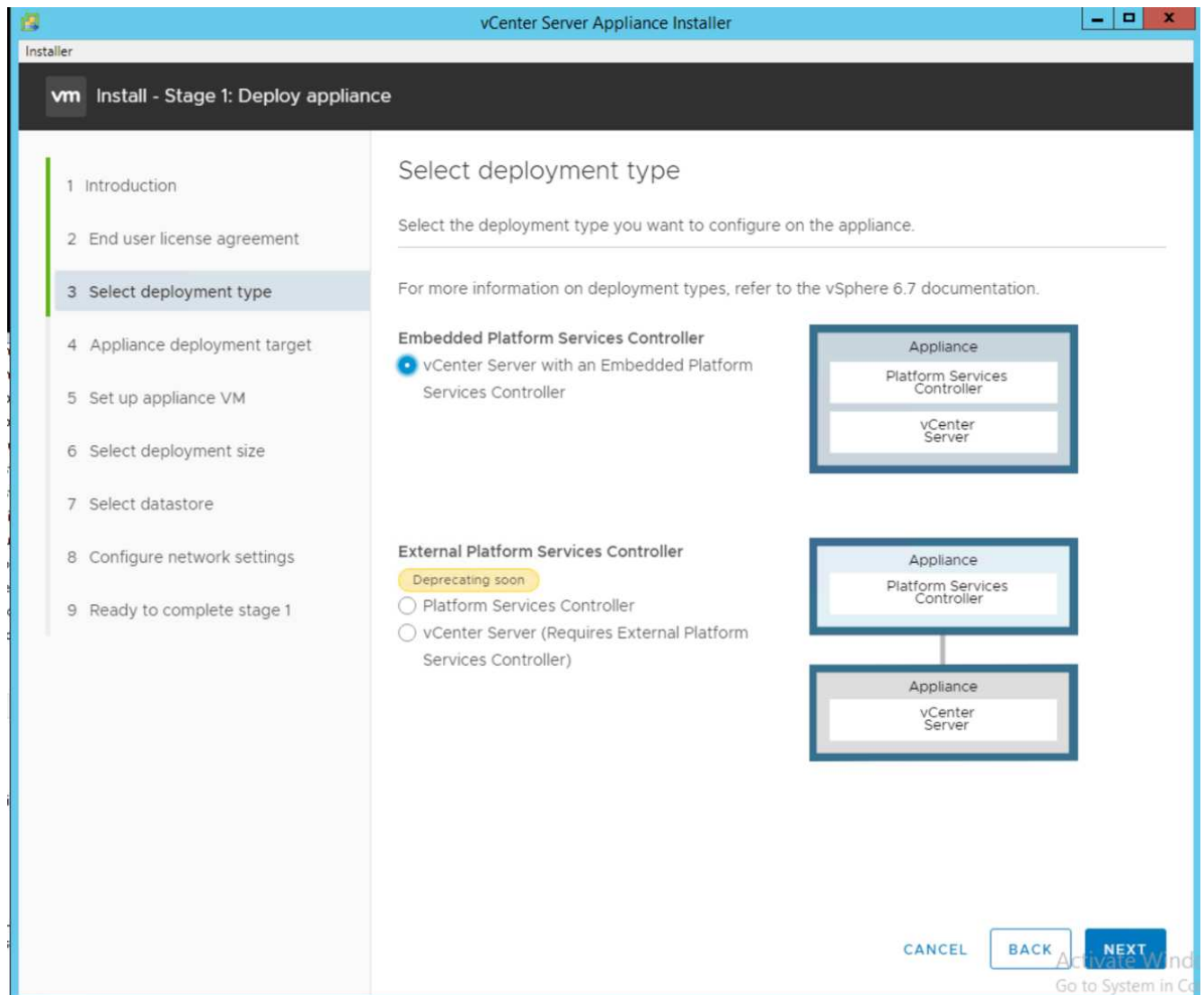
Scarica VMware vCenter Server Appliance

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

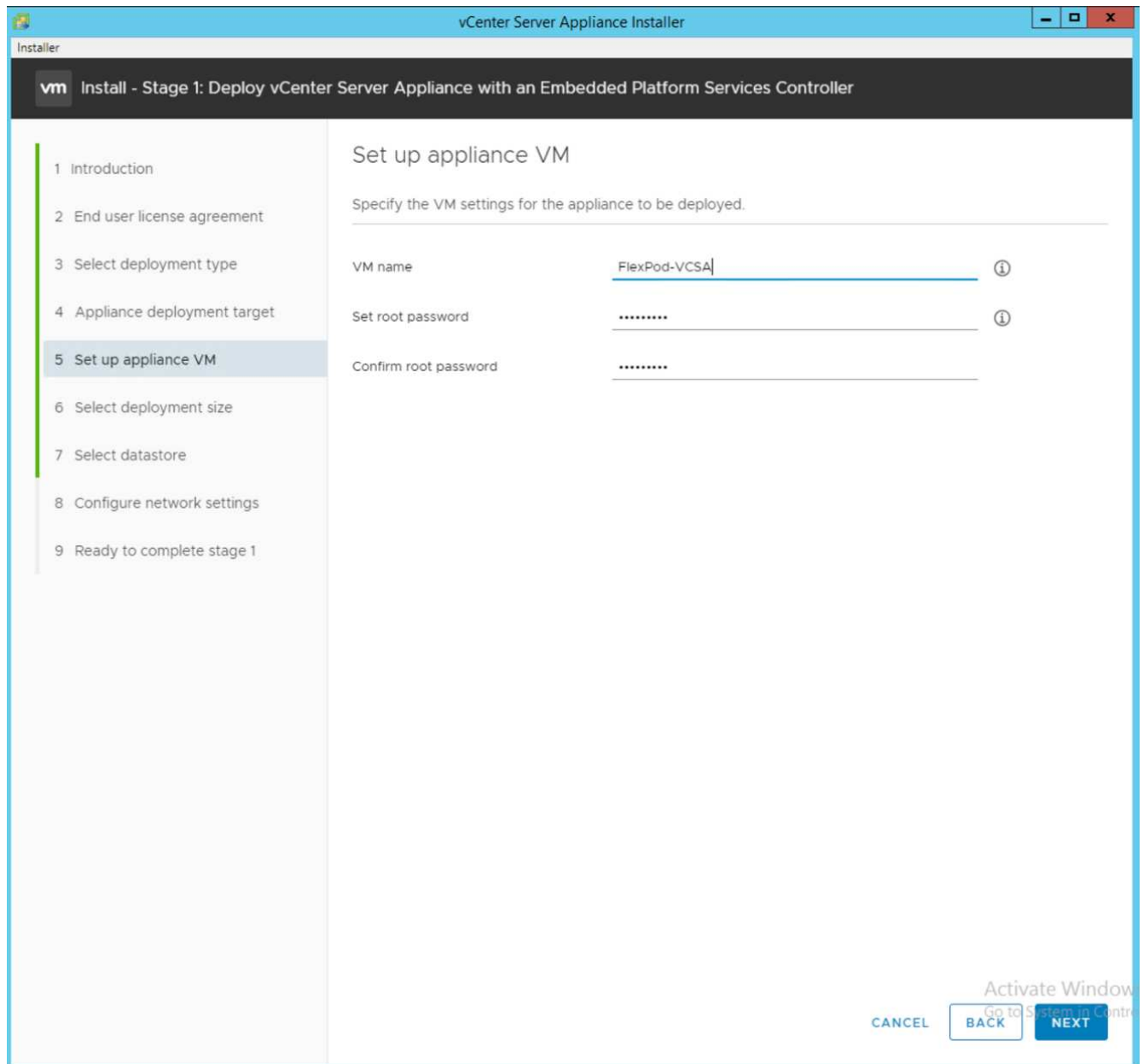
Specify the appliance deployment target settings. The target is the ESXi host or vCenter Server instance on which the appliance will be deployed.

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

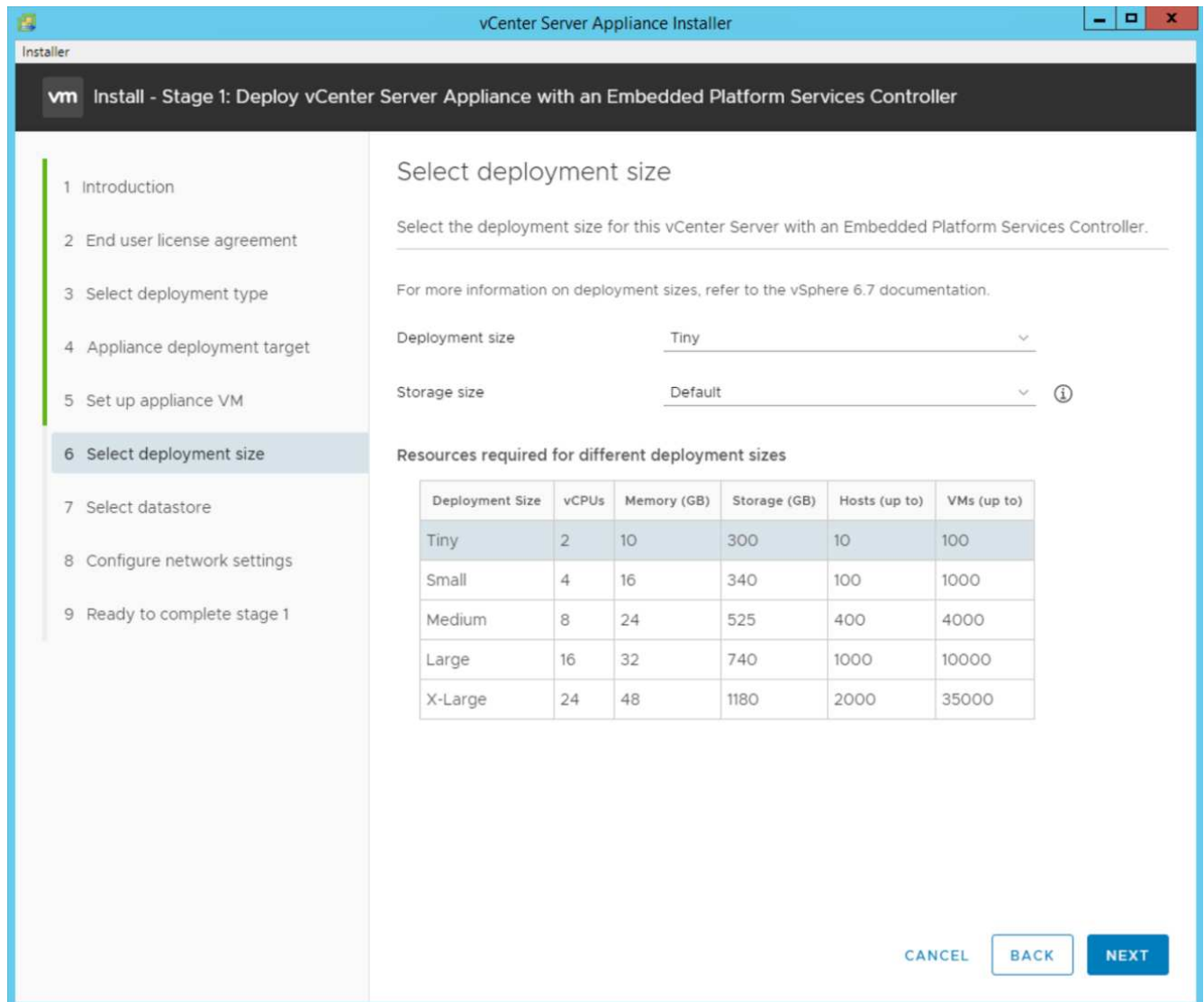
CANCEL BACK NEXT

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

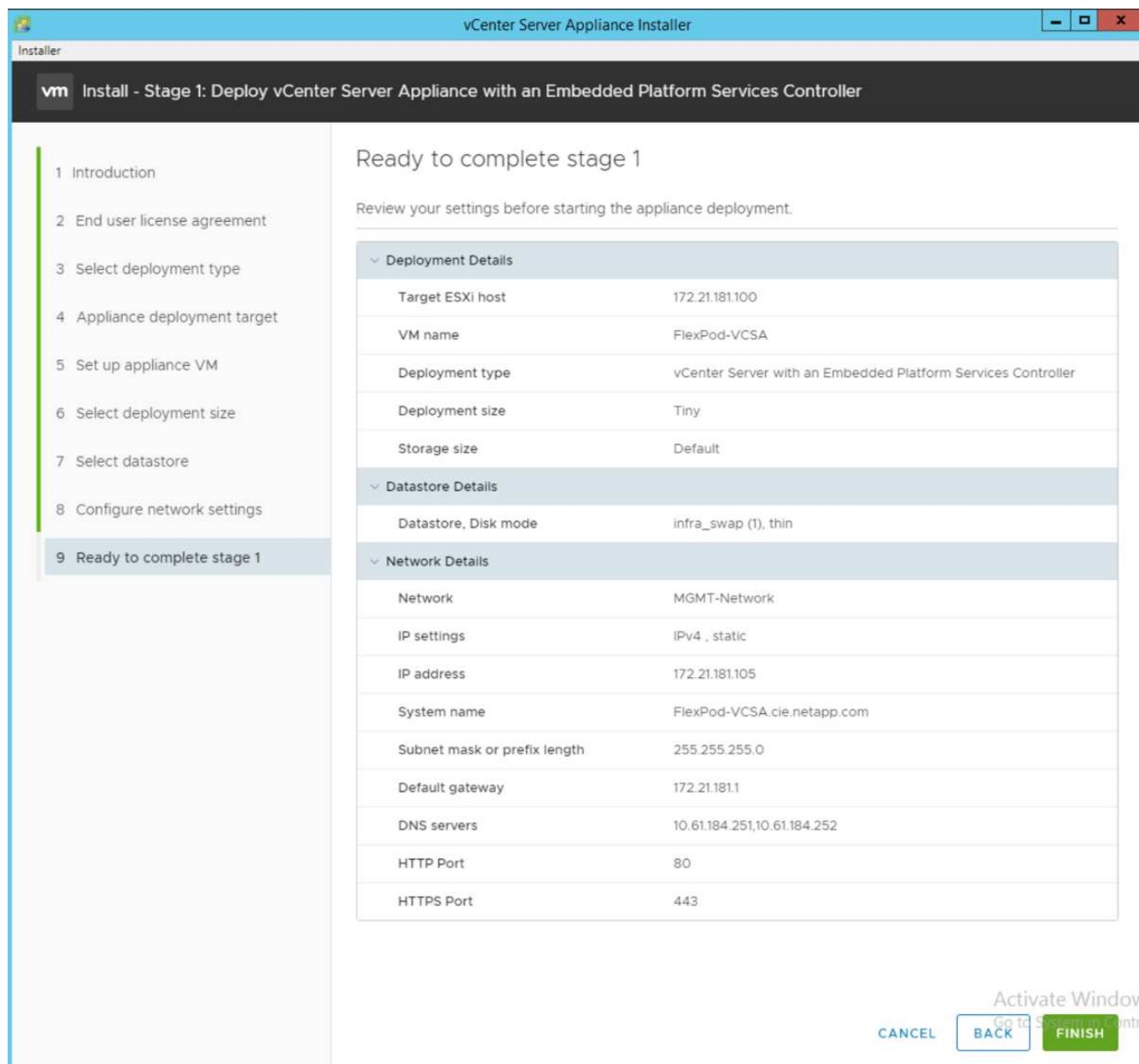
Configure network settings for this appliance

Network	MGMT-Network	ⓘ
IP version	IPv4	
IP assignment	static	
FQDN	FlexPod-VCSA.cie.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

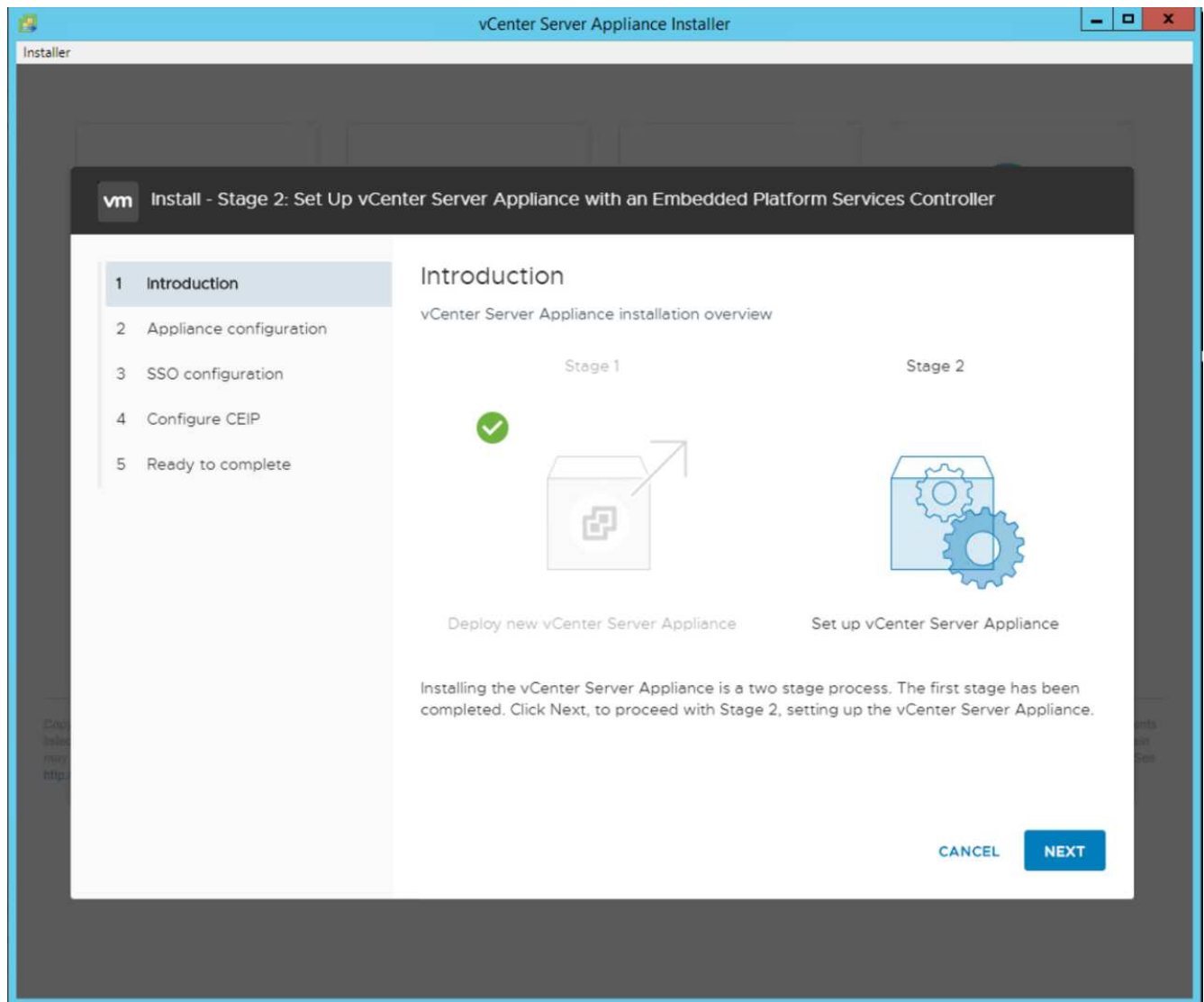
Activate Windows
Go to System in Control

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

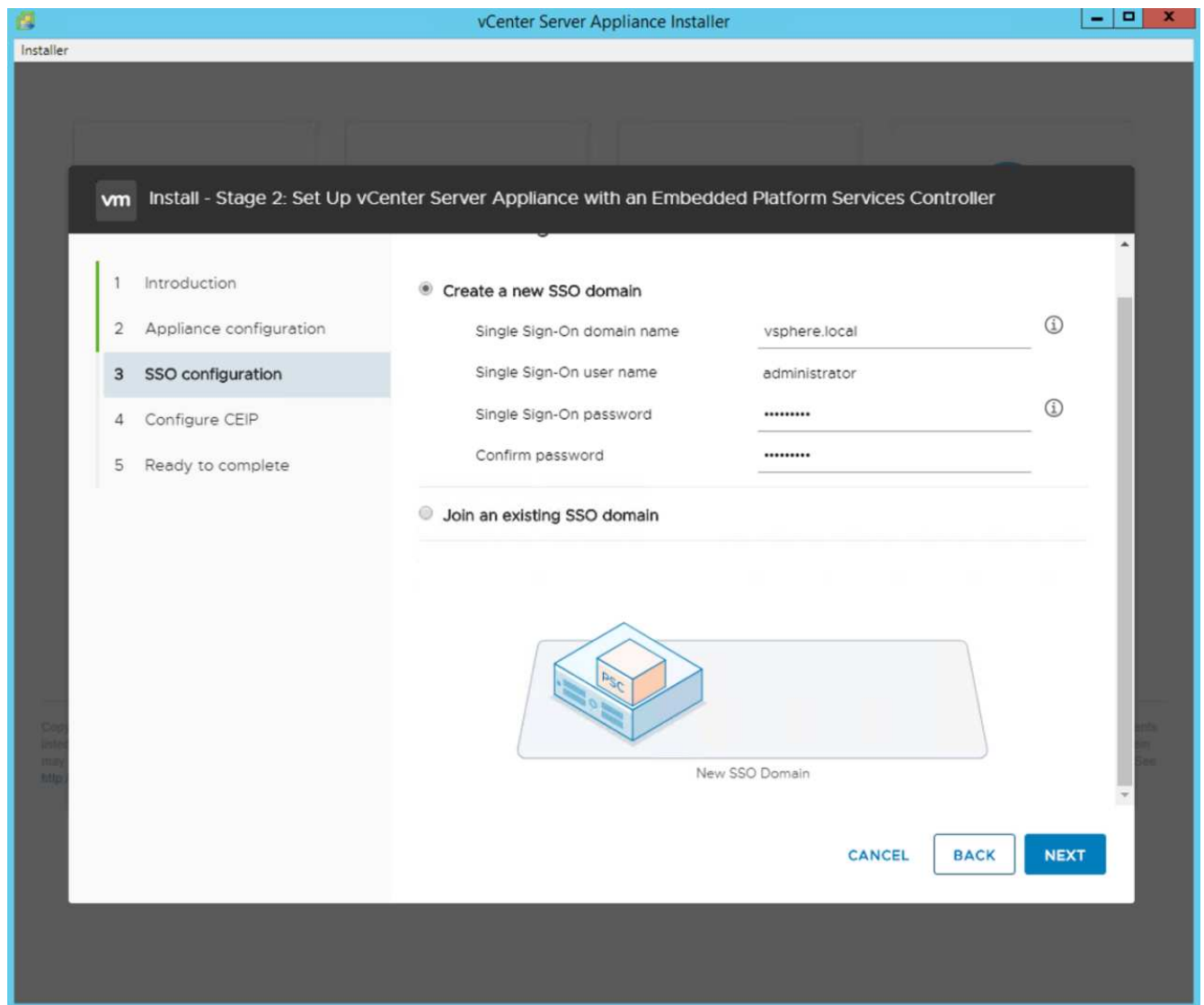


VCSA viene installato ora. Questo processo richiede alcuni minuti.

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.

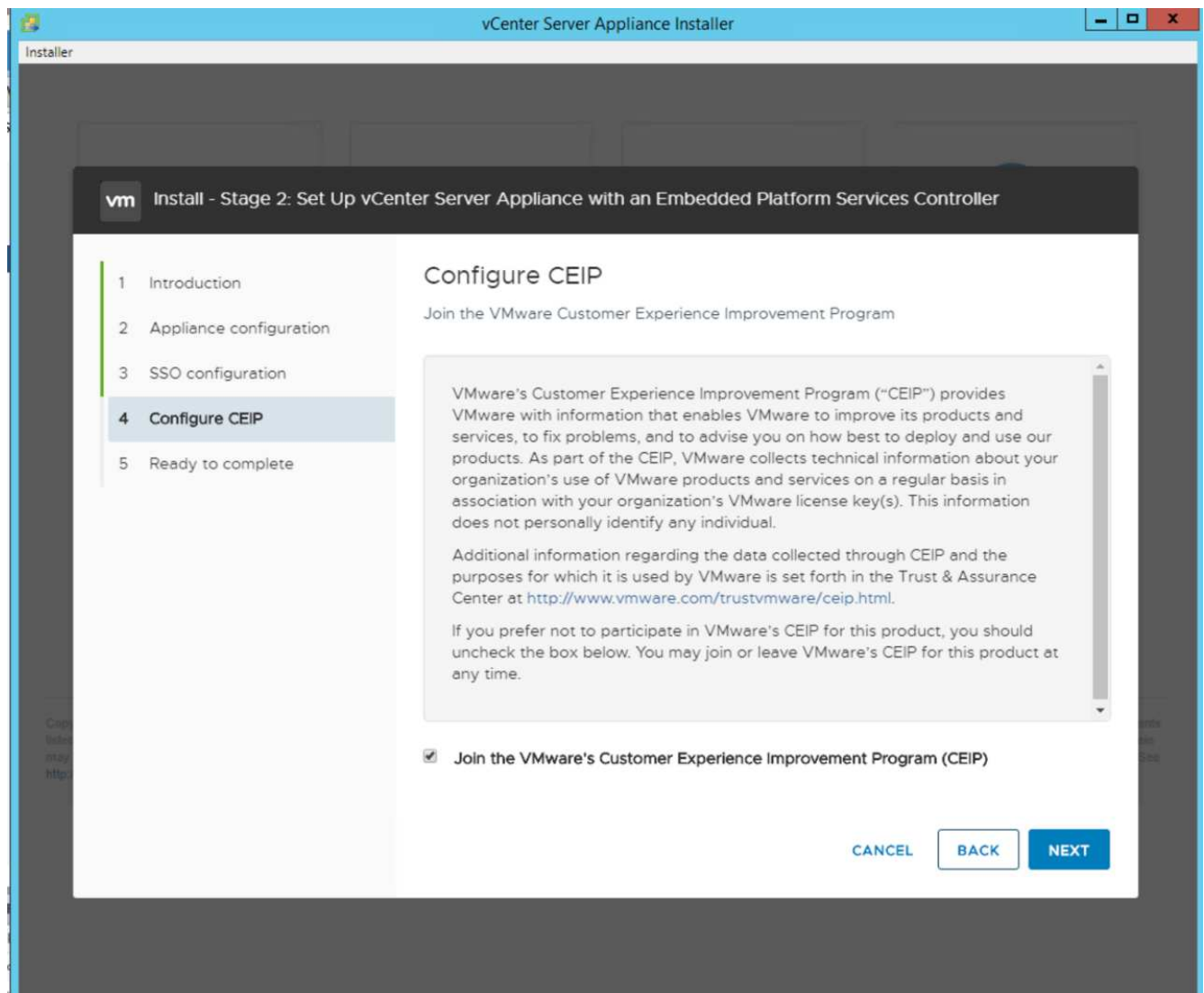


18. Invio <<var_ntp_id>> Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.
19. Se si intende utilizzare vCenter Server High Availability (ha), assicurarsi che l'accesso SSH sia attivato.
20. Configurare il nome di dominio SSO, la password e il nome del sito. Fare clic su Avanti.

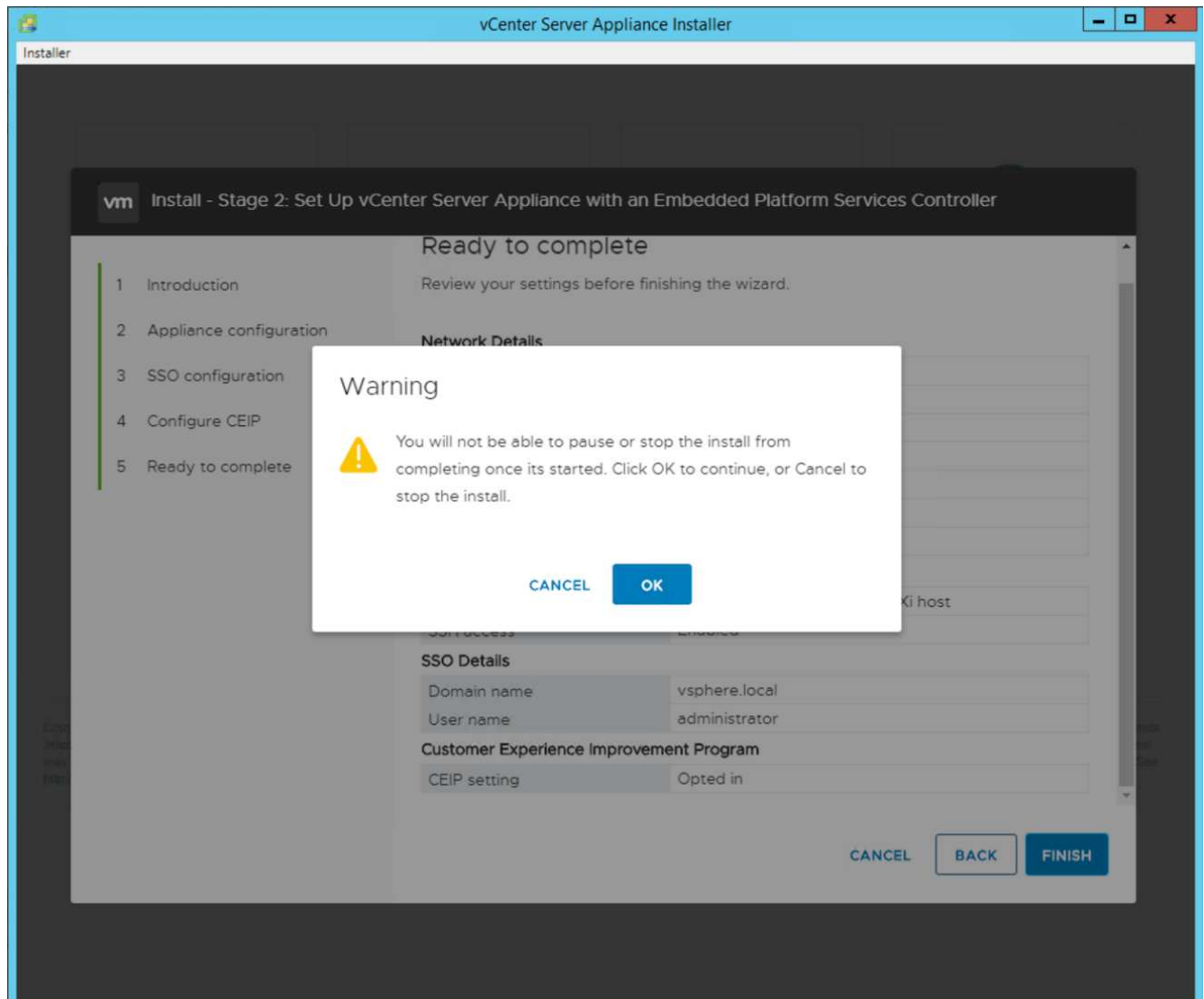


Registrare questi valori come riferimento, in particolare se si discosta da `vsphere.local` nome di dominio.

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"/>

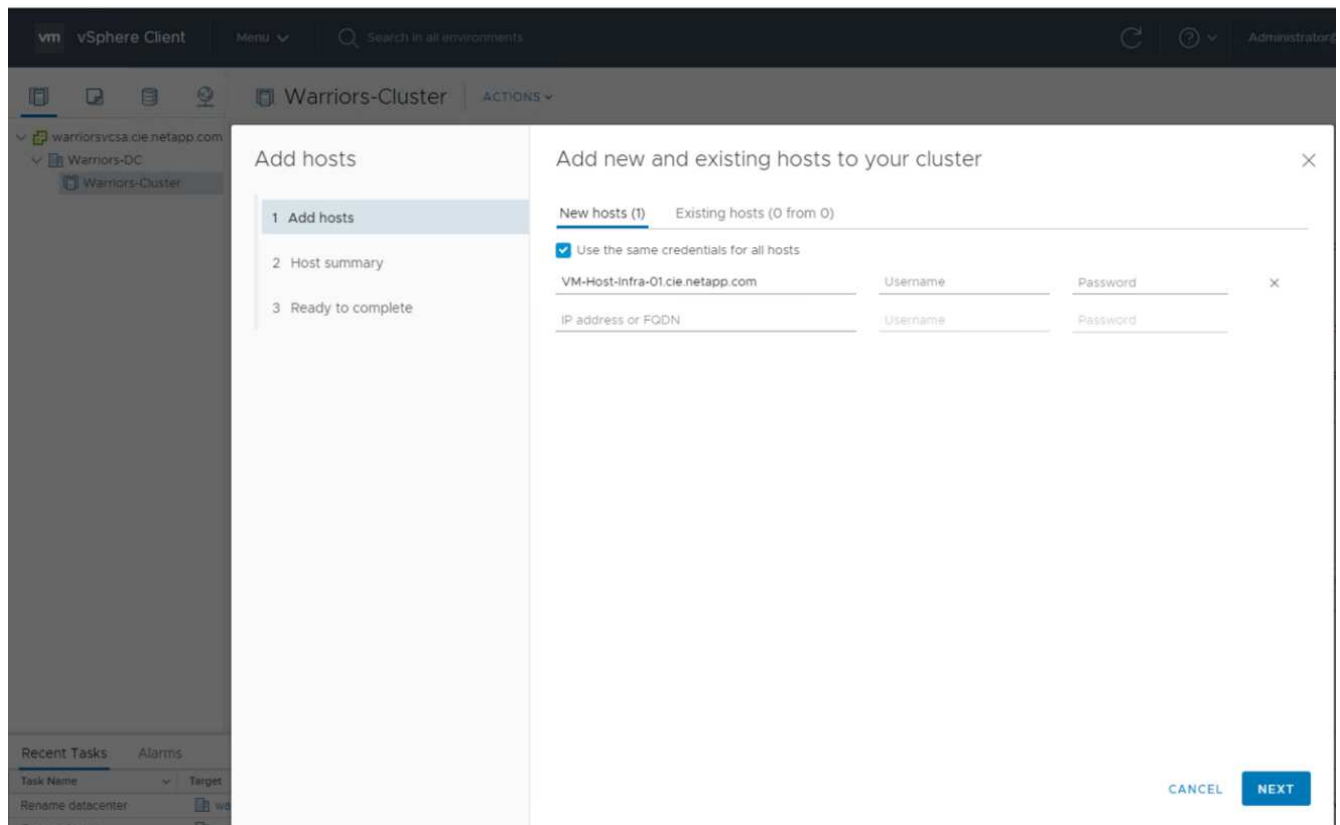
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

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.



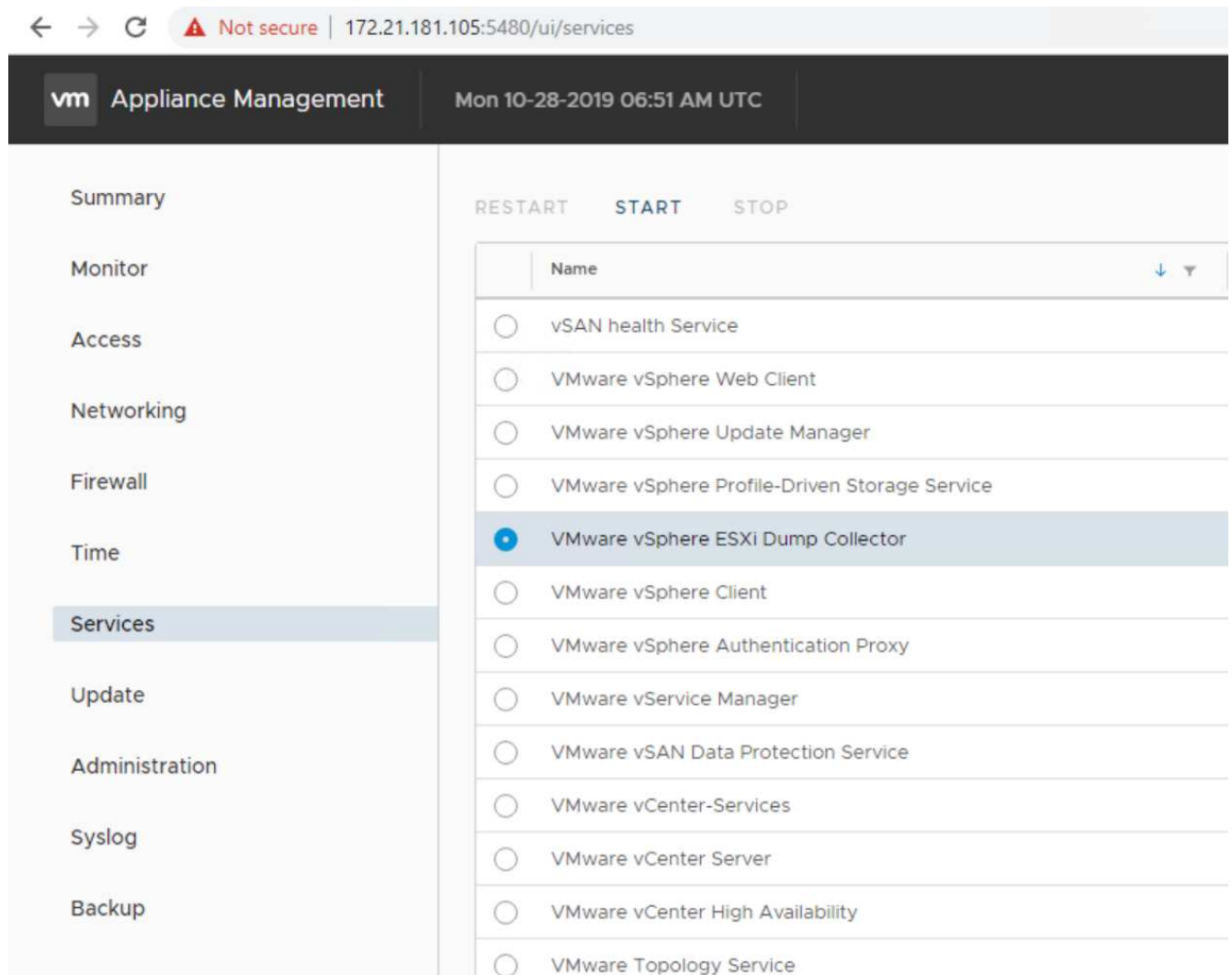
Questo processo deve essere completato per tutti gli host aggiuntivi aggiunti alla configurazione di FlexPod Express.

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."

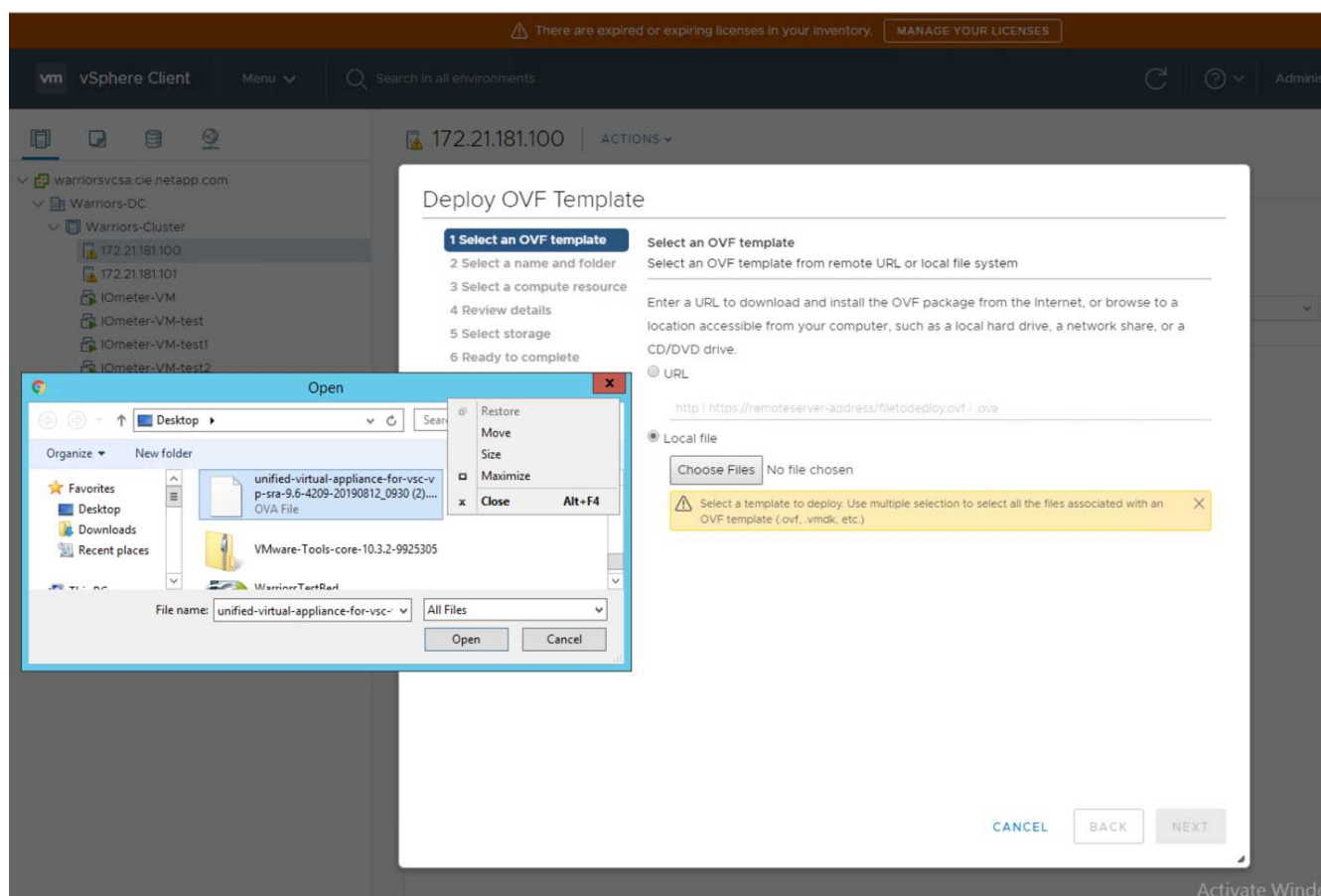
Procedure di implementazione di NetApp Virtual Storage Console 9.6

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.

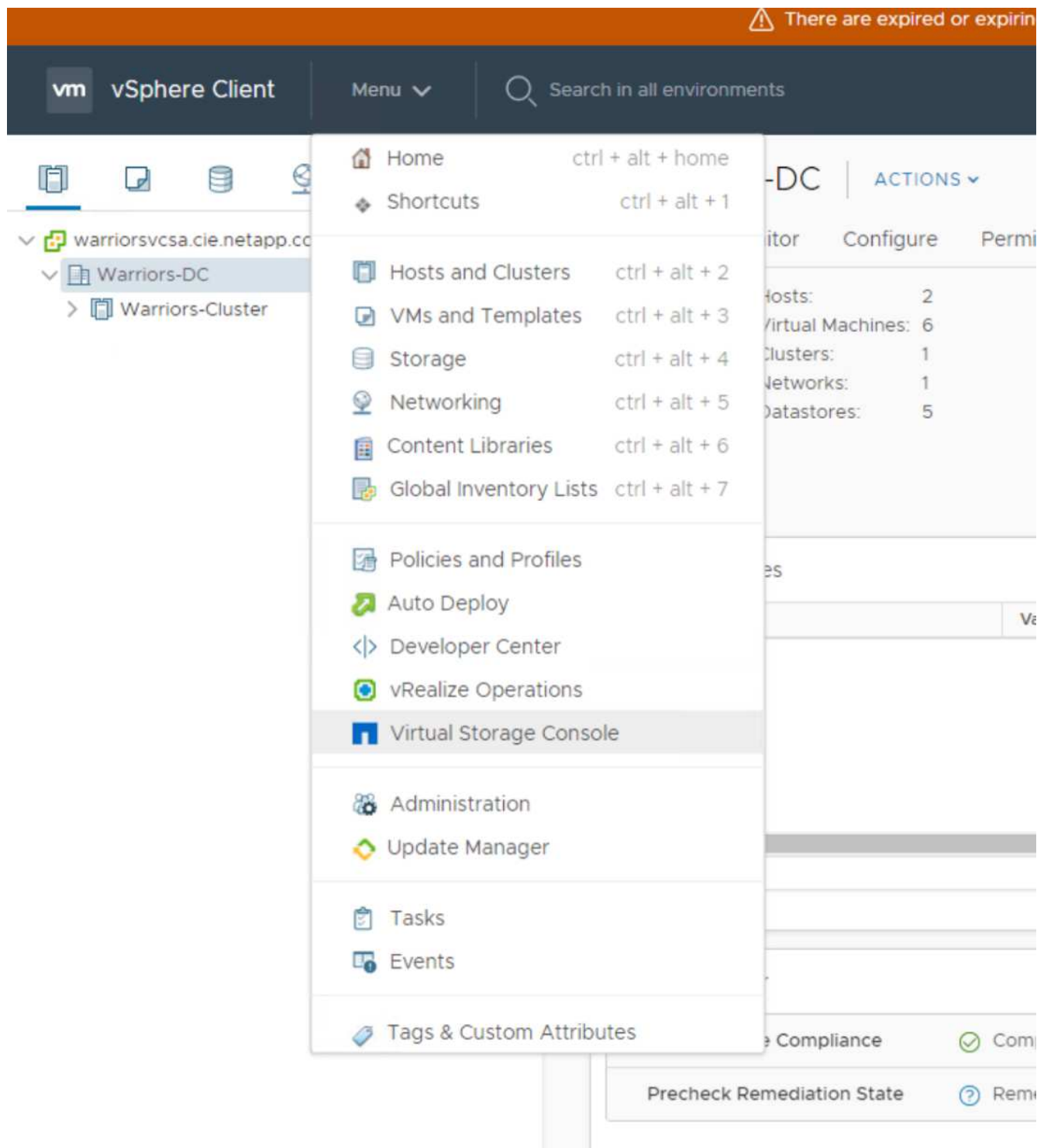
OR

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.

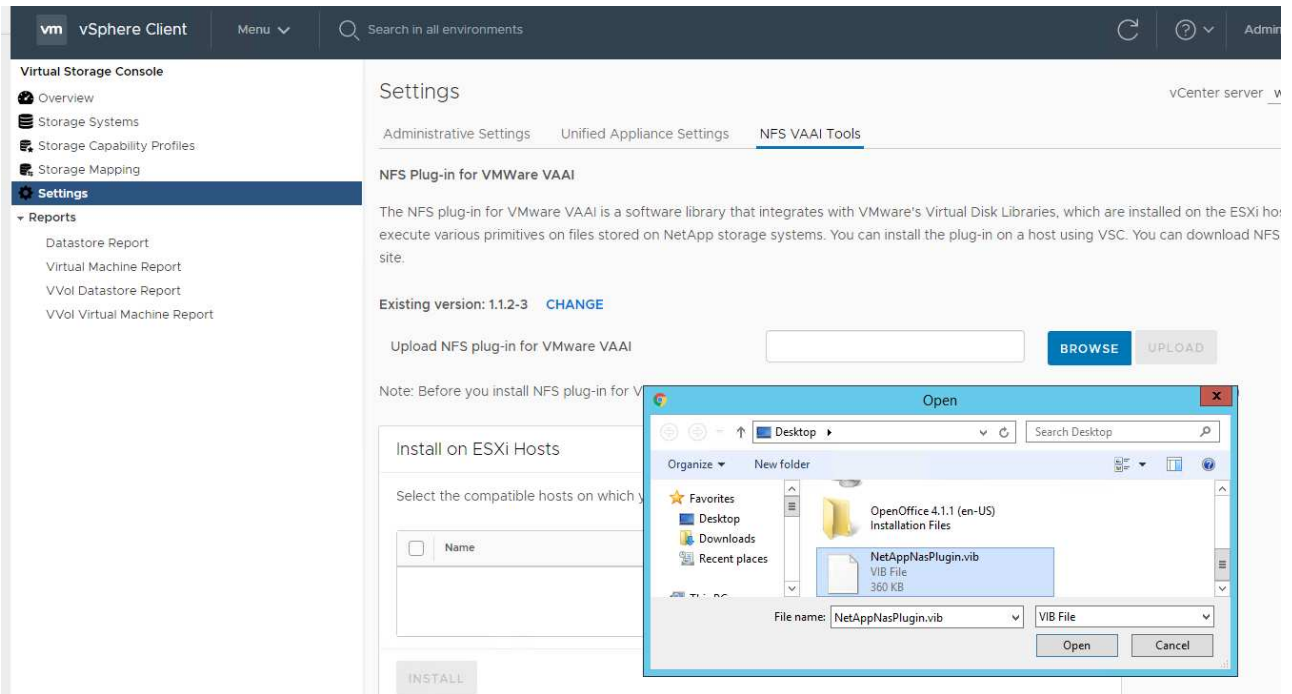


Scarica e installa il plug-in NetApp NFS VAAI

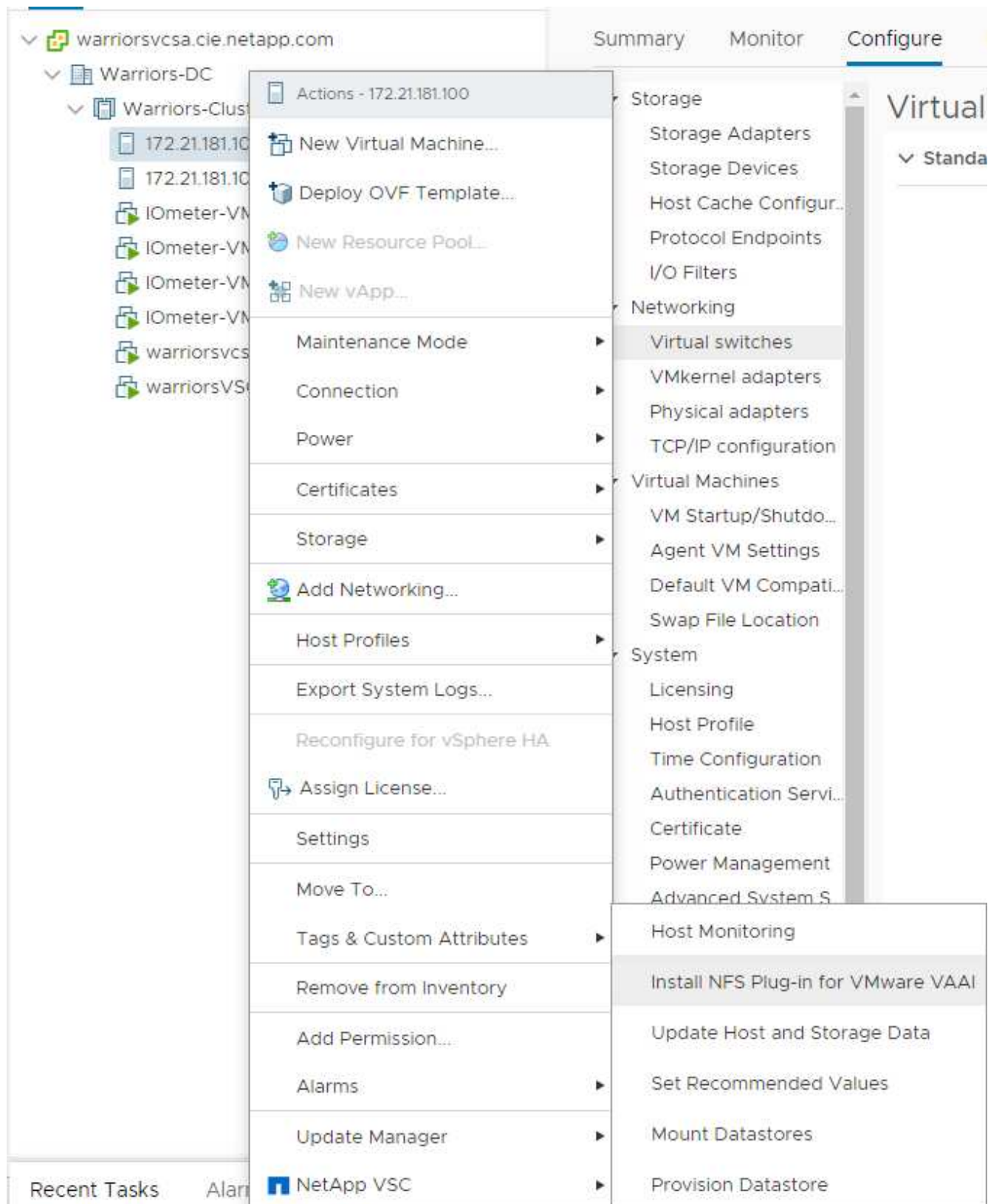
Per scaricare e installare il plug-in NetApp NFS VAAI, attenersi alla seguente procedura:

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.



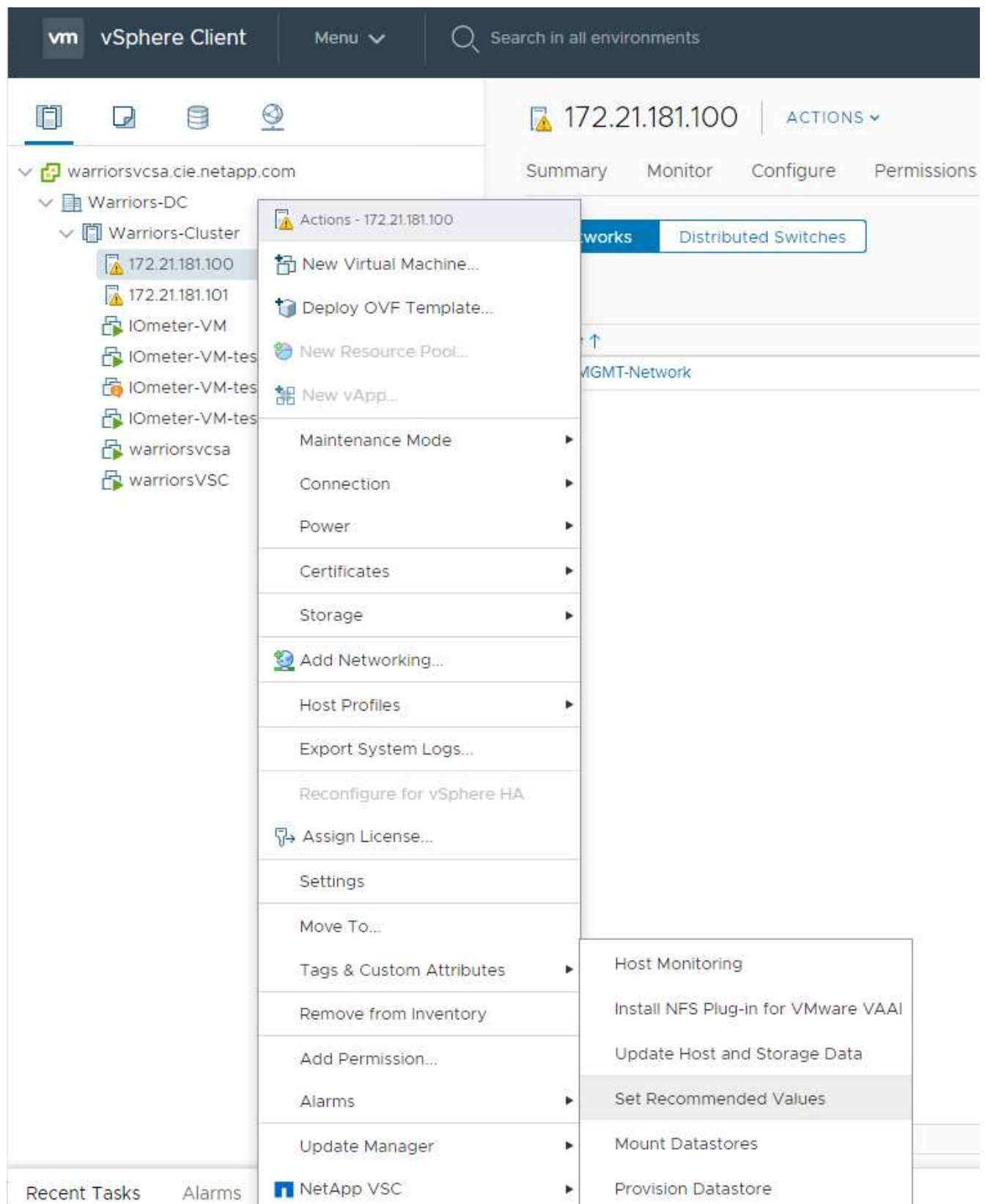
3. Fare clic su Upload (carica) per trasferire il plug-in a vCenter.
4. Selezionare l'host, quindi scegliere NetApp VSC > Install NFS Plug-in for VMware VAAI.



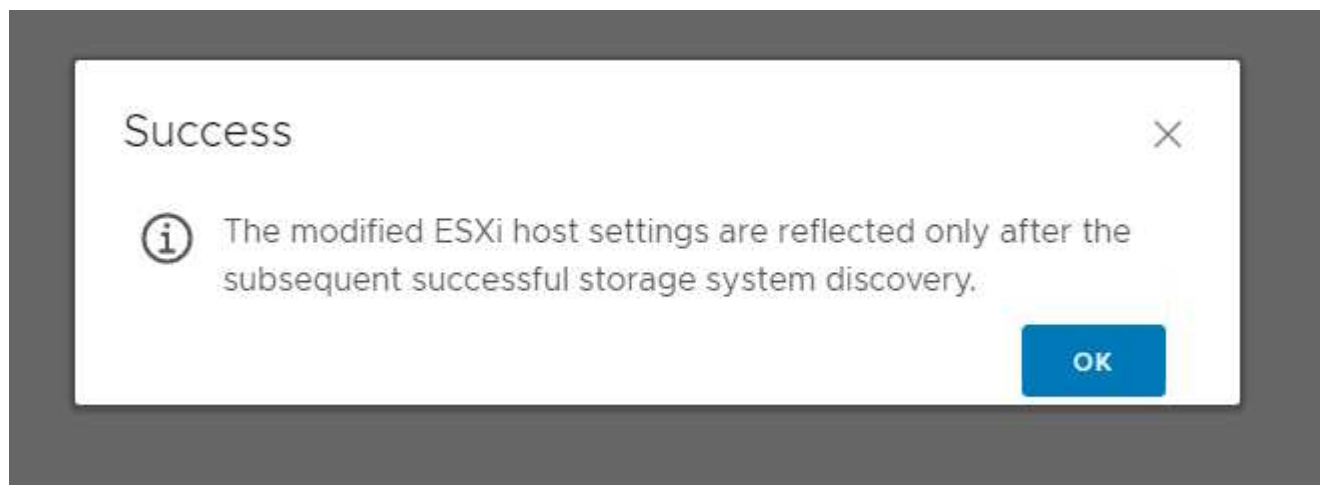
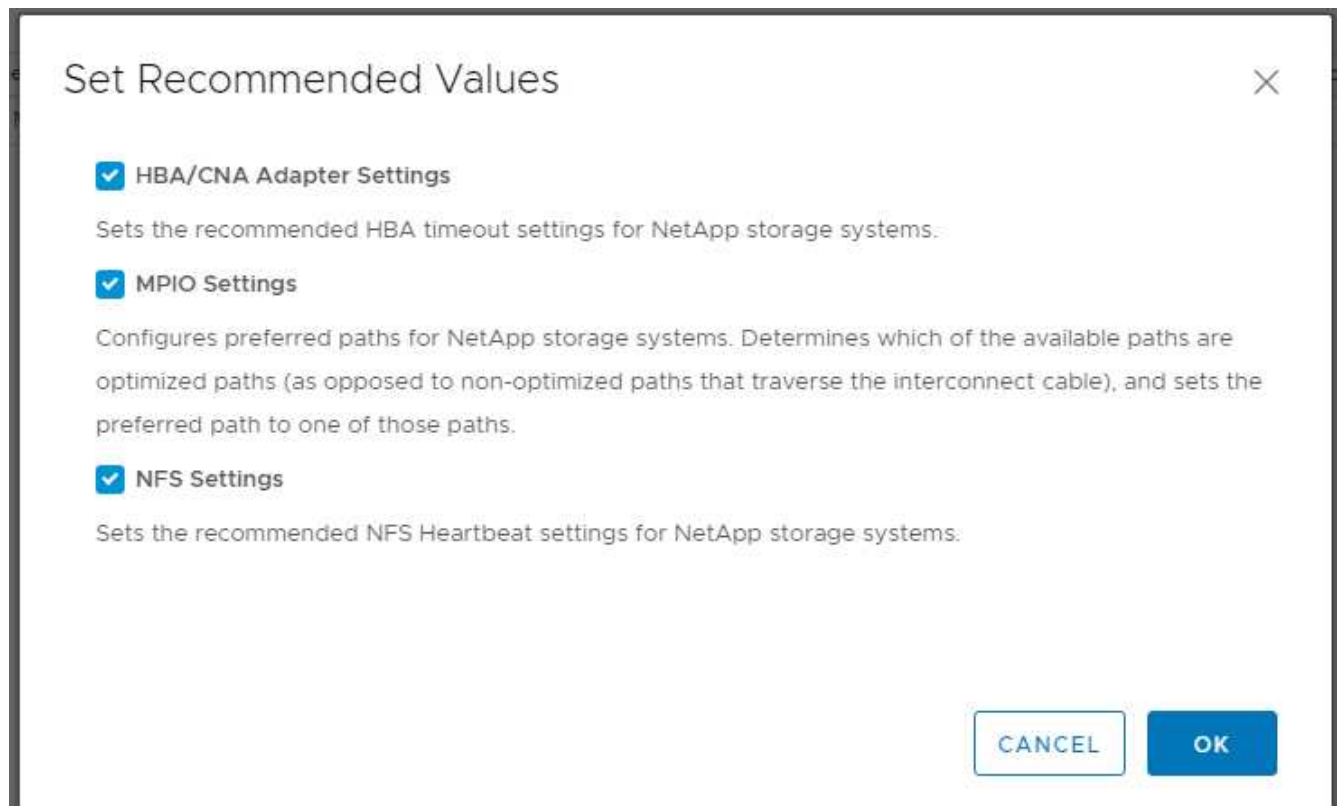
Utilizzare le impostazioni di storage ottimali per gli host ESXi

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.

Conclusione

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.

Guida alla progettazione di FlexPod Express con Cisco UCS serie C e AFF serie A220

NVA-1125-DESIGN: FlexPod Express con Cisco UCS serie C e AFF serie A220



Savita Kumari, NetApp in partnership con:

Le tendenze del settore indicano una vasta 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, sfruttando la tecnologia che conoscono nel proprio data center.

FlexPod è un'architettura di data center pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco, sulla famiglia di switch Cisco Nexus e su NetApp AFF. I componenti di 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.

["Avanti: Riepilogo del programma."](#)

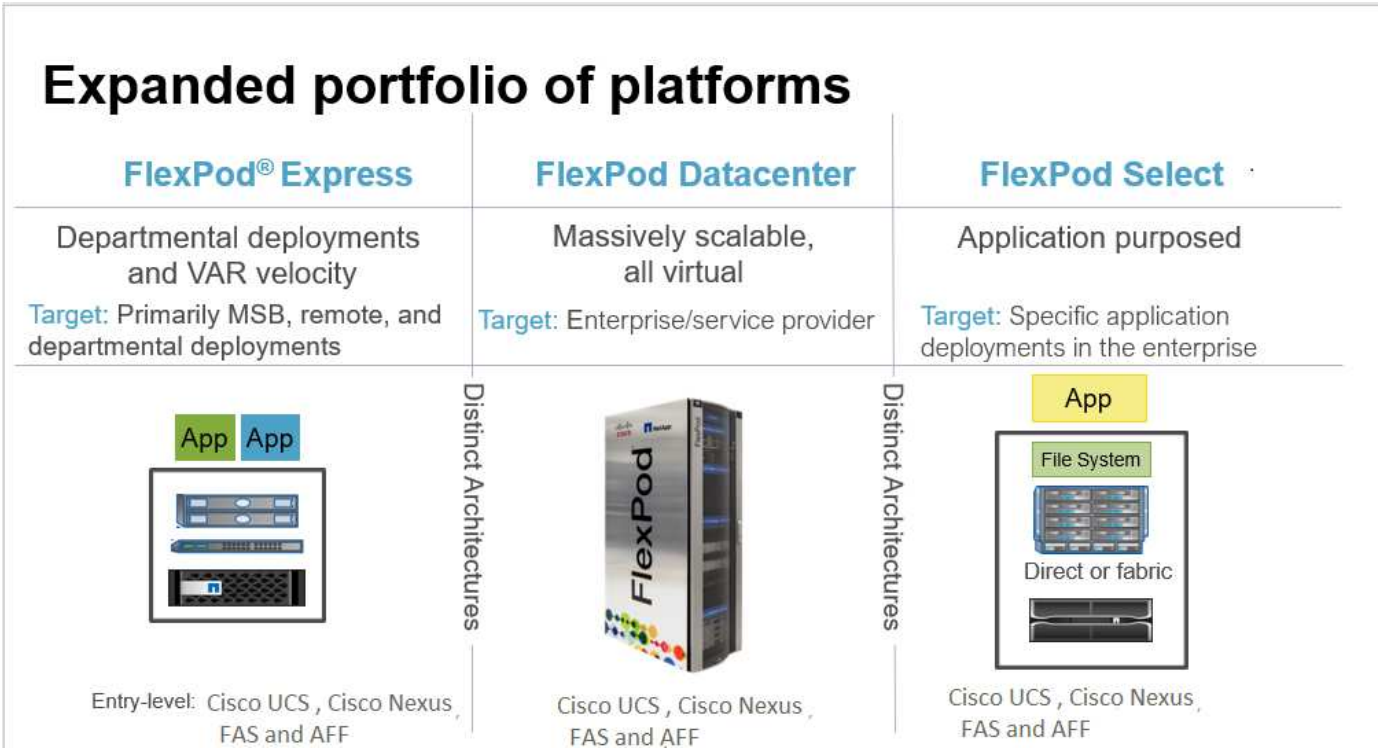
Riepilogo del programma

Portfolio di infrastrutture convergenti FlexPod

Le architetture di riferimento FlexPod vengono fornite come Cisco Validated Design (CVD) o come NetApp Verified Architectures (NVA). Le deviazioni basate sui requisiti del cliente rispetto a un determinato CVD o NVA sono consentite se le variazioni non comportano l'implementazione di configurazioni non supportate.

Come illustrato nella figura seguente, il portfolio FlexPod include tre soluzioni: FlexPod Express, FlexPod Datacenter e FlexPod Select:

- **FlexPod Express.** offre una soluzione entry-level costituita da tecnologie Cisco e NetApp.
- **FlexPod Datacenter.** offre una base polivalente ottimale per diversi carichi di lavoro e applicazioni.
- **FlexPod Select.** incorpora gli aspetti migliori del data center FlexPod e adatta l'infrastruttura a una determinata applicazione.



Programma NetApp Verified Architecture

Il programma NVA offre ai clienti un'architettura verificata per le soluzioni NetApp. Un NVA significa che la soluzione NetApp ha le seguenti qualità:

- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione
- Accelera il time-to-market

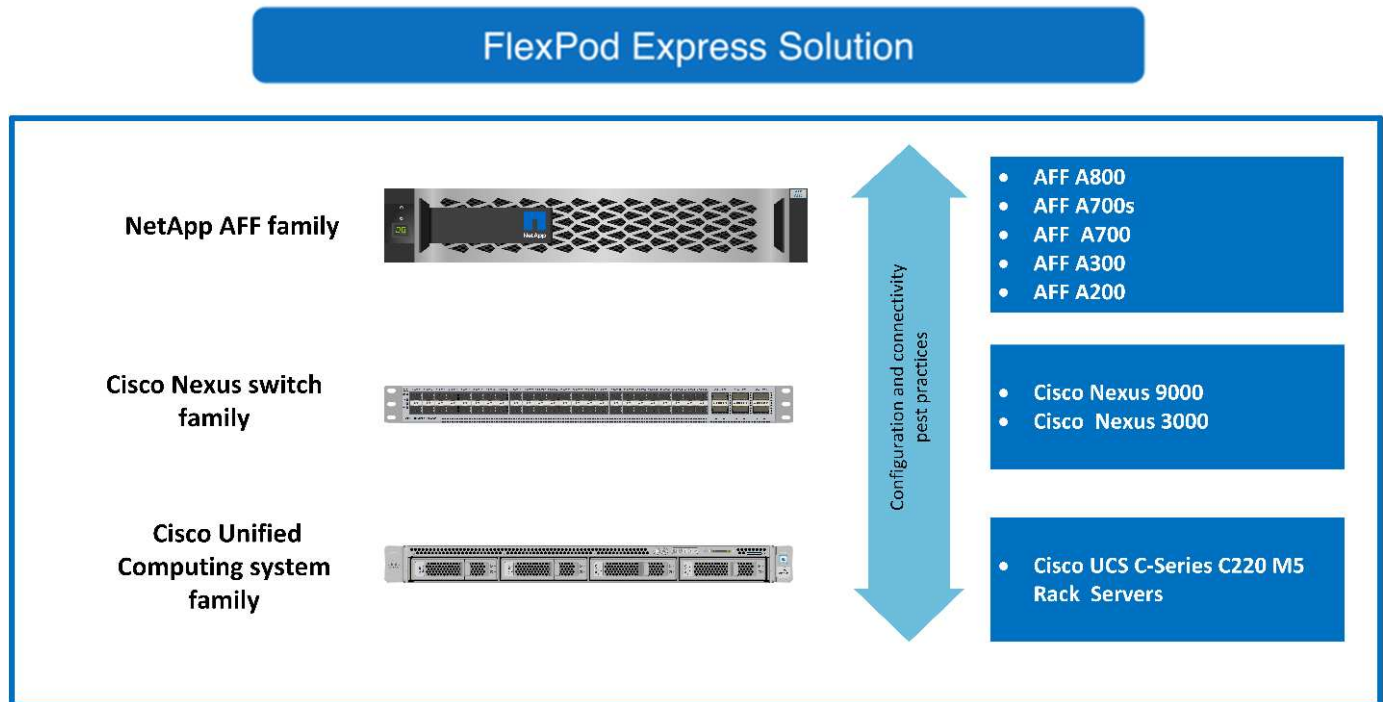
In questa guida viene illustrato in dettaglio il design di FlexPod con VMware vSphere. Inoltre, questo design sfrutta il nuovissimo sistema AFF A220, che esegue il software NetApp ONTAP 9.4, gli switch Cisco Nexus 3172P e i server Cisco UCS C220 M5 come nodi hypervisor.

Sebbene questo documento sia validato per AFF A220, questa soluzione supporta anche FAS2700.

Panoramica della soluzione

FlexPod Express è progettato per eseguire carichi di lavoro di virtualizzazione misti. È destinato alle filiali e alle filiali e alle piccole e medie imprese. È inoltre ottimale per le aziende più grandi che desiderano implementare una soluzione dedicata a uno scopo specifico. Questa nuova soluzione per FlexPod Express aggiunge nuove tecnologie come NetApp ONTAP 9.4, NetApp AFF A220 e VMware vSphere 6.7.

La figura seguente mostra i componenti hardware inclusi nella soluzione FlexPod Express.



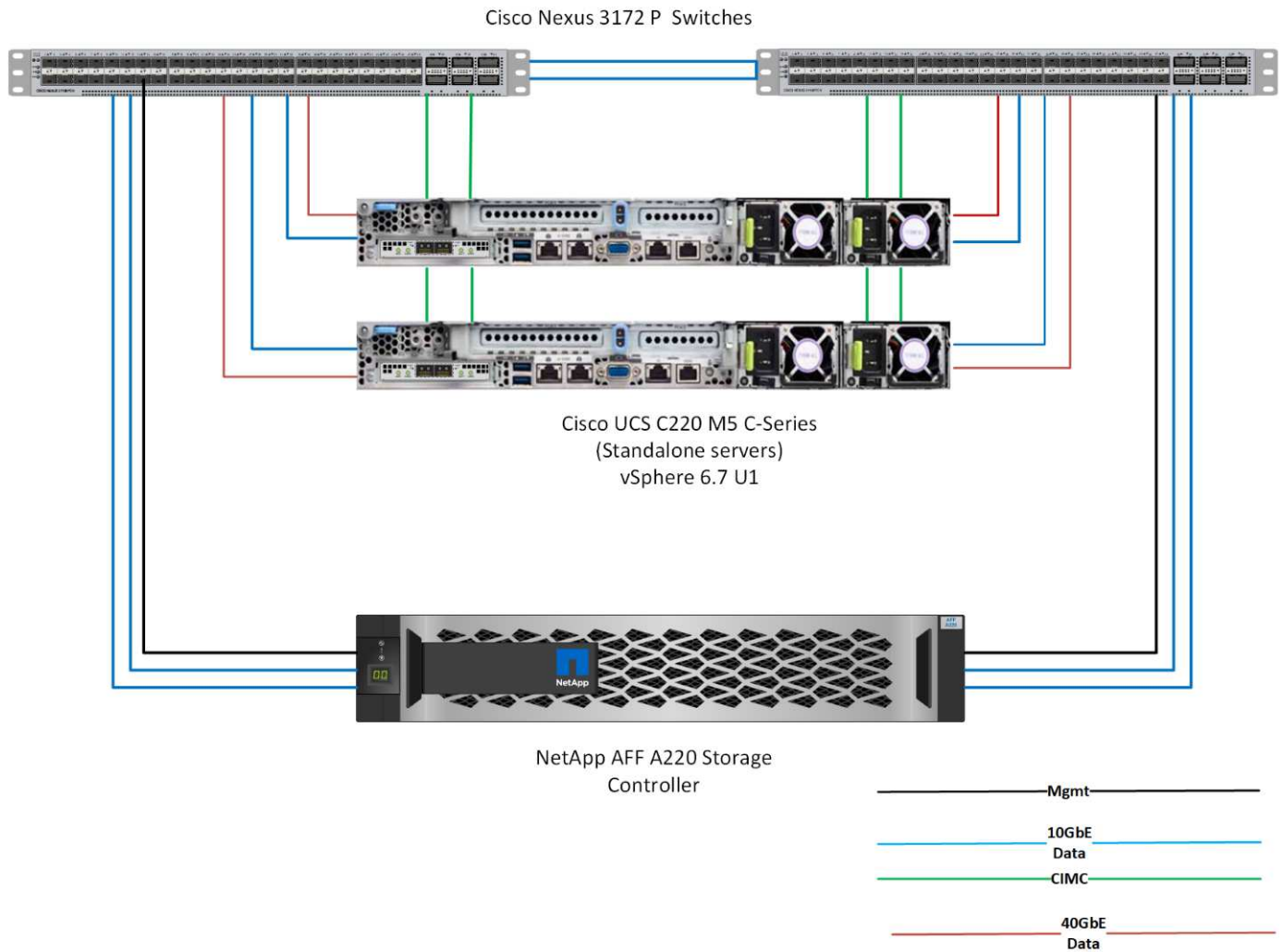
Pubblico di riferimento

Questo documento è destinato a coloro che desiderano sfruttare un'infrastruttura costruita per garantire l'efficienza DELL'IT e consentire l'innovazione DELL'IT. I destinatari di questo documento includono, a titolo esemplificativo ma non esaustivo, tecnici di vendita, consulenti sul campo, personale di servizi professionali, responsabili IT, partner engineer e clienti.

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. Questa soluzione include il nuovo sistema NetApp AFF A220, che esegue il software ONTAP 9.4, due switch Cisco Nexus 3172P e server rack Cisco UCS C220 M5 con VMware vSphere 6.7. Questa soluzione validata utilizza la tecnologia 10-Gigabit Ethernet (10 GbE). La figura seguente presenta una panoramica. Viene inoltre fornita una guida su come scalare aggiungendo due nodi hypervisor alla volta, in modo che l'architettura FlexPod Express possa adattarsi alle esigenze di business in evoluzione di un'organizzazione.

FlexPod Express



40 GbE non è validato, ma è un'infrastruttura supportata.

"Successivo: Requisiti tecnologici."

Requisiti tecnologici

FlexPod richiede una combinazione di componenti hardware e software che dipende dall'hypervisor selezionato e dalla velocità di rete. Inoltre, FlexPod Express definisce 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, entrambi gli hypervisor possono essere eseguiti sullo stesso hardware FlexPod Express.

La seguente tabella elenca i componenti hardware necessari per tutte le configurazioni FlexPod Express e per

implementare la soluzione. I componenti hardware utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Hardware	Quantità
Cluster a due nodi AFF A220	1
Server Cisco UCS C220 M5	2
Switch Cisco Nexus 3172P	2
Cisco UCS Virtual Interface Card (VIC) 1387 per server rack Cisco UCS C220 M5	2
Adattatore Cisco CVR-QSFP-SFP10G	4

Requisiti software

Le seguenti tabelle elencano i componenti software necessari per implementare le architetture della soluzione FlexPod Express.

La seguente tabella elenca i requisiti software per l'implementazione FlexPod Express di base.

Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	3.1.3	Per rack server C220 M5
Sistema operativo Cisco NX	nxos.7.0.3.17.5.bin	Per switch Cisco Nexus 3172P
NetApp ONTAP	9.4	Per controller AFF A220

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

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

["Avanti: Scelte di progettazione."](#)

Scelte di progettazione

Durante il processo di progettazione sono state scelte le seguenti tecnologie. Ogni tecnologia ha uno scopo specifico nella soluzione di infrastruttura FlexPod Express.

NetApp AFF serie A220 con ONTAP 9.4

Questa soluzione sfrutta due dei più recenti prodotti NetApp: Il software NetApp AFF A220 e ONTAP 9.4.

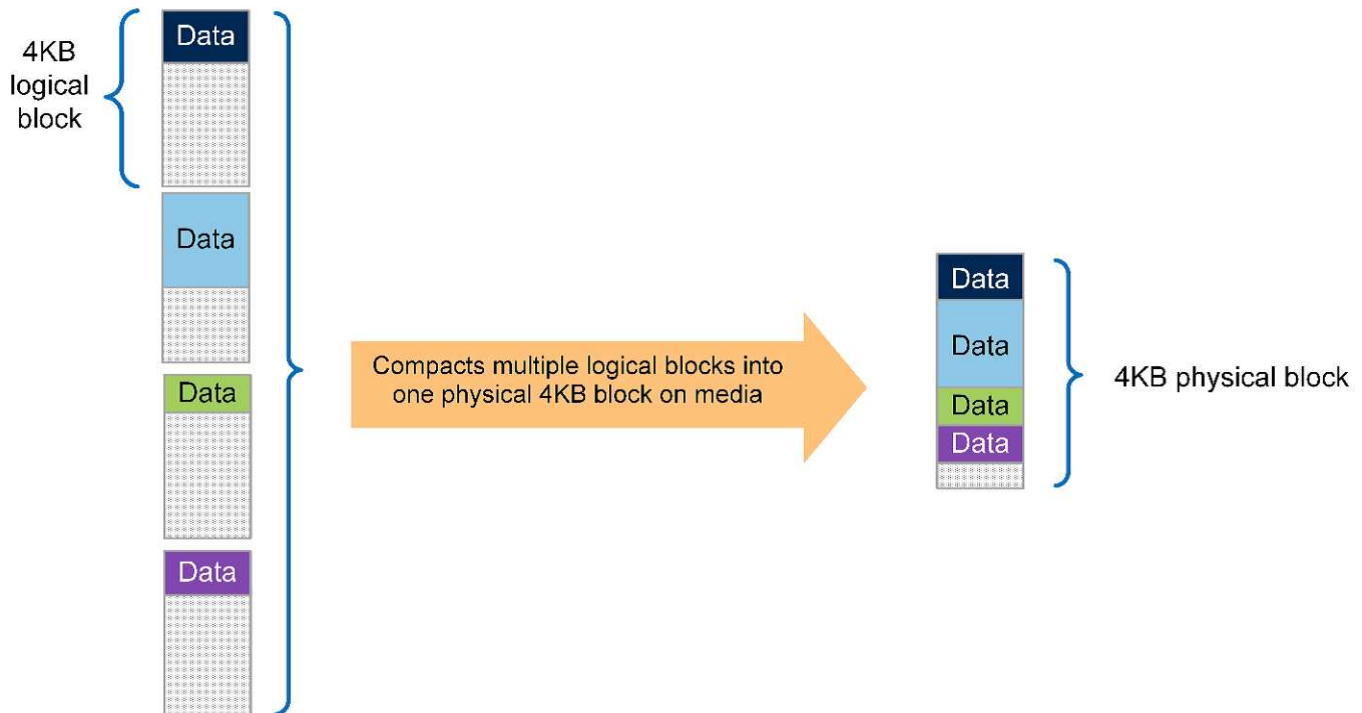
Sistema AFF A220

Per ulteriori informazioni sul sistema hardware AFF A220, consultare ["Pagina principale di AFF A-Series"](#).

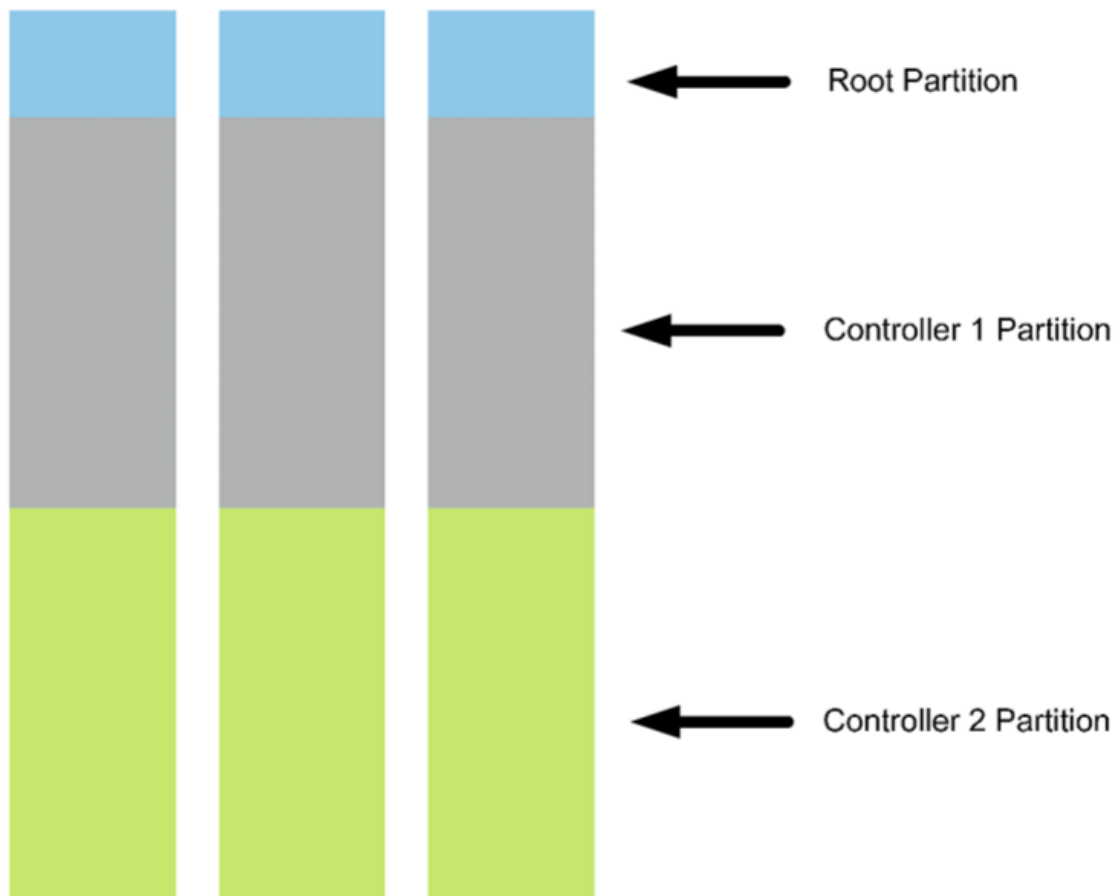
Software ONTAP 9.4

I sistemi NetApp AFF A220 utilizzano il nuovo software ONTAP 9.4. ONTAP 9.4 è il software per la gestione dei dati aziendali leader del settore. Combina nuovi livelli di semplicità e flessibilità con potenti funzionalità di gestione dei dati, efficienza dello storage e integrazione cloud leader del settore.

ONTAP 9.4 dispone di diverse funzionalità adatte alla soluzione FlexPod Express. In primo luogo, l'impegno di NetApp per l'efficienza dello storage, che può essere una delle funzionalità più importanti per le piccole implementazioni. Le caratteristiche di efficienza dello storage di NetApp come deduplica, compressione e thin provisioning sono disponibili in ONTAP 9.4 con una nuova aggiunta, la compattazione. Poiché il sistema NetApp WAFL scrive sempre blocchi da 4 KB, la compattazione combina più blocchi in un blocco da 4 KB quando i blocchi non utilizzano lo spazio allocato di 4 KB. La seguente figura illustra questo processo.



Inoltre, è possibile sfruttare la partizione dei dati root sul sistema AFF A220. Questa partizione consente di eseguire lo striping dell'aggregato root e di due aggregati di dati tra i dischi del sistema. Pertanto, entrambi i controller di un cluster AFF A220 a due nodi possono sfruttare le prestazioni di tutti i dischi dell'aggregato. Vedere la figura seguente.



Queste sono solo alcune funzionalità chiave che integrano la soluzione FlexPod Express. Per ulteriori informazioni sulle funzionalità aggiuntive di ONTAP 9.4, vedere ["Scheda informativa sul software di gestione dei dati ONTAP 9"](#). Inoltre, consulta NetApp ["Centro documentazione di ONTAP 9"](#), che è stato aggiornato per includere ONTAP 9.4.

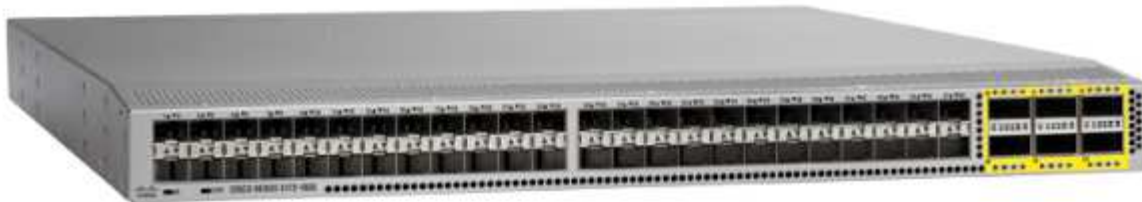
Cisco Nexus serie 3000

Cisco Nexus 3172P è uno switch robusto e conveniente che offre switching a 1/10/40/100Gbps. Lo switch Cisco Nexus 3172PQ, parte della famiglia Unified Fabric, è uno switch compatto a 1 unità rack (1RU) per implementazioni top-of-rack di data center. (Vedere la figura seguente). Offre fino a settantadue porte 1/10GbE in 1RU o quarantotto 1/10GbE più sei porte 40GbE in 1RU. Inoltre, per la massima flessibilità del livello fisico, supporta anche 1/10/40 Gbps.

Poiché tutti i vari modelli della serie Cisco Nexus utilizzano lo stesso sistema operativo sottostante, NX-OS, sono supportati più modelli Cisco Nexus nelle soluzioni FlexPod Express e FlexPod Datacenter.

Le specifiche delle performance includono:

- Throughput del traffico line-rate (entrambi i livelli 2 e 3) su tutte le porte
- MTU (Maximum Transmission Unit) configurabile fino a 9216 byte (frame jumbo)



Per ulteriori informazioni sugli switch Cisco Nexus 3172, consultare ["Scheda tecnica degli switch Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL e 3172TQ-XL"](#).

Cisco UCS C-Series

Il server rack Cisco UCS C-Series è stato scelto per FlexPod Express perché le sue numerose opzioni di configurazione consentono di adattarlo a requisiti specifici in un'implementazione FlexPod Express.

I server rack Cisco UCS C-Series offrono computing unificato in un fattore di forma standard di settore per ridurre il TCO e aumentare l'agilità.

I server rack Cisco UCS C-Series offrono i seguenti vantaggi:

- Un punto di ingresso indipendente dal fattore di forma in Cisco UCS
- Implementazione semplificata e rapida delle applicazioni
- Estensione delle innovazioni e dei vantaggi di Unified Computing ai server rack
- Maggiore scelta per i clienti con vantaggi esclusivi in un pacchetto rack familiare



Il server rack Cisco UCS C220 M5 (nella figura precedente) è tra i server per applicazioni e infrastrutture aziendali generici più versatili del settore. Si tratta di un server rack a due socket ad alta densità che offre performance ed efficienza leader di settore per un'ampia gamma di carichi di lavoro, tra cui virtualizzazione, collaborazione e applicazioni bare-metal. I server rack Cisco UCS C-Series possono essere implementati come server standalone o come parte di Cisco UCS per sfruttare le innovazioni di Unified Computing basate su standard di Cisco che aiutano a ridurre il TCO dei clienti e ad aumentare l'agilità del business.

Per ulteriori informazioni sui server C220 M5, consultare ["Scheda informativa sul server rack Cisco UCS C220 M5"](#).

Opzioni di connettività per i server rack C220 M5

Le opzioni di connettività per i server rack C220 M5 sono le seguenti:

• Cisco UCS VIC 1387

Cisco UCS VIC 1387 (nella figura seguente) offre QSFP+ 40GbE e FC over Ethernet (FCoE) dual-port Enhanced in un fattore di forma modulare LAN-on-motherboard (mLOM). Lo slot mLOM può essere utilizzato per installare Cisco VIC senza utilizzare uno slot PCIe (Component Interconnect Express) periferico, garantendo una maggiore espandibilità I/O.



Per ulteriori informazioni sull'adattatore Cisco UCS VIC 1387, consultare ["Cisco UCS Virtual Interface Card 1387"](#) scheda tecnica.

• ADATTATORE CVR-QSFP-SFP10G

Il modulo Cisco QSA converte una porta QSFP in una porta SFP o SFP+. Con questo adattatore, i clienti hanno la flessibilità di utilizzare qualsiasi modulo o cavo SFP+ o SFP per il collegamento a una porta a velocità inferiore sull'altra estremità della rete. Questa flessibilità consente una transizione conveniente a 40 GbE massimizzando l'utilizzo di piattaforme QSFP a 40 GbE ad alta densità. Questo adattatore supporta tutte le ottiche SFP+ e i cavi e supporta diversi moduli SFP da 1 GbE. Poiché questo progetto è stato validato utilizzando la connettività 10GbE e poiché il VIC 1387 utilizzato è 40 GbE, l'adattatore CVR-QSFP-SFP10G (nella figura seguente) viene utilizzato per la conversione.



VMware vSphere 6.7

VMware vSphere 6.7 è un hypervisor opzionale da utilizzare con FlexPod Express. VMware vSphere consente alle organizzazioni di ridurre l'impatto di energia e raffreddamento, confermando che la capacità di calcolo acquistata viene utilizzata al massimo. Inoltre, VMware vSphere consente la protezione dai guasti hardware (VMware High Availability o VMware ha) e il bilanciamento del carico delle risorse di calcolo in un cluster di host vSphere (VMware Distributed Resource Scheduler o VMware DRS).

Poiché riavvia solo il kernel, VMware vSphere 6.7 consente ai clienti di eseguire un "boot rapido" dove carica

vSphere ESXi senza riavviare l'hardware. Questa funzione è disponibile solo con le piattaforme e i driver presenti nell'elenco di avvio rapido. vSphere 6.7 amplia le funzionalità del client vSphere, che può fare circa il 90% di ciò che il client Web vSphere può fare.

In vSphere 6.7, VMware ha esteso questa funzionalità per consentire ai clienti di impostare Enhanced vMotion Compatibility (EVC) per macchina virtuale (VM) piuttosto che per host. In vSphere 6.7, VMware ha anche esposto le API che possono essere utilizzate per creare cloni istantanei.

Di seguito sono riportate alcune delle funzionalità di vSphere 6.7 U1:

- vSphere Client basato su Web HTML5 con funzionalità complete
- vMotion per VM NVIDIA GRID vGPU. Supporto per Intel FPGA.
- vCenter Server Converge Tool per passare da PSC esterno a PC interni.
- Miglioramenti per vSAN (aggiornamenti HCI).
- Libreria di contenuti migliorata.

Per ulteriori informazioni su vSphere 6.7 U1, vedere ["Novità di vCenter Server 6.7 Update 1"](#). Sebbene questa soluzione sia stata validata con vSphere 6.7, supporta qualsiasi versione vSphere qualificata con gli altri componenti dal NetApp Interoperability Matrix Tool. NetApp consiglia di implementare vSphere 6.7U1 per le correzioni e le funzionalità avanzate.

Architettura di boot

Di seguito sono riportate le opzioni supportate per l'architettura di avvio di FlexPod:

- LUN SAN iSCSI
- Scheda SD FlexFlash Cisco
- Disco locale

Poiché il data center FlexPod viene avviato da LUN iSCSI, la gestibilità della soluzione viene migliorata anche utilizzando l'avvio iSCSI per FlexPod Express.

["Avanti: Verifica della soluzione."](#)

Verifica della soluzione

Cisco e NetApp hanno progettato e costruito FlexPod Express per fungere da piattaforma infrastrutturale di prim'ordine per i propri clienti. Poiché è stato progettato con componenti leader del settore, i clienti possono affidarsi a FlexPod Express come base dell'infrastruttura. In linea con i principi fondamentali del portfolio FlexPod, l'architettura FlexPod Express è stata testata a fondo dagli architetti e dagli ingegneri dei data center Cisco e NetApp. Dalla ridondanza e disponibilità a ogni singola funzionalità, l'intera architettura FlexPod Express viene validata per infondere fiducia nei nostri clienti e per creare fiducia nel processo di progettazione.

VMware vSphere 6.7 è stato verificato sui componenti dell'infrastruttura FlexPod Express. Questa convalida includeva opzioni di connettività uplink 10 GbE per l'hypervisor.

["Prossimo: Conclusione."](#)

Conclusione

FlexPod offre una soluzione semplice ed efficace grazie a un design validato che utilizza componenti leader del settore. Grazie alla scalabilità e all'offerta di opzioni per la piattaforma hypervisor, FlexPod Express può essere personalizzato in base alle specifiche esigenze di business. FlexPod Express è stato progettato tenendo conto delle piccole e medie imprese, delle filiali e delle filiali remote e di altre aziende che richiedono soluzioni dedicate.

"Avanti: Dove trovare ulteriori informazioni."

Dove trovare ulteriori informazioni

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

- Documentazione NetApp

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

- Guida all'implementazione di FlexPod con VMware vSphere 6.7 e NetApp AFF A220

["https://www.netapp.com/us/media/nva-1123-deploy.pdf"](https://www.netapp.com/us/media/nva-1123-deploy.pdf)

Guida all'implementazione di FlexPod Express con Cisco UCS serie C e AFF serie A220

NVA-1123-DEPLOY: Guida all'implementazione di FlexPod con VMware vSphere 6.7 e NetApp AFF A220

Savita Kumari, NetApp



In collaborazione con:

Le tendenze del settore indicano una vasta 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, sfruttando la tecnologia con cui hanno familiarità nel proprio data center.

FlexPod è un'architettura di data center pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco, sulla famiglia di switch Cisco Nexus e sulle tecnologie 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 possono facilmente adattarsi 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

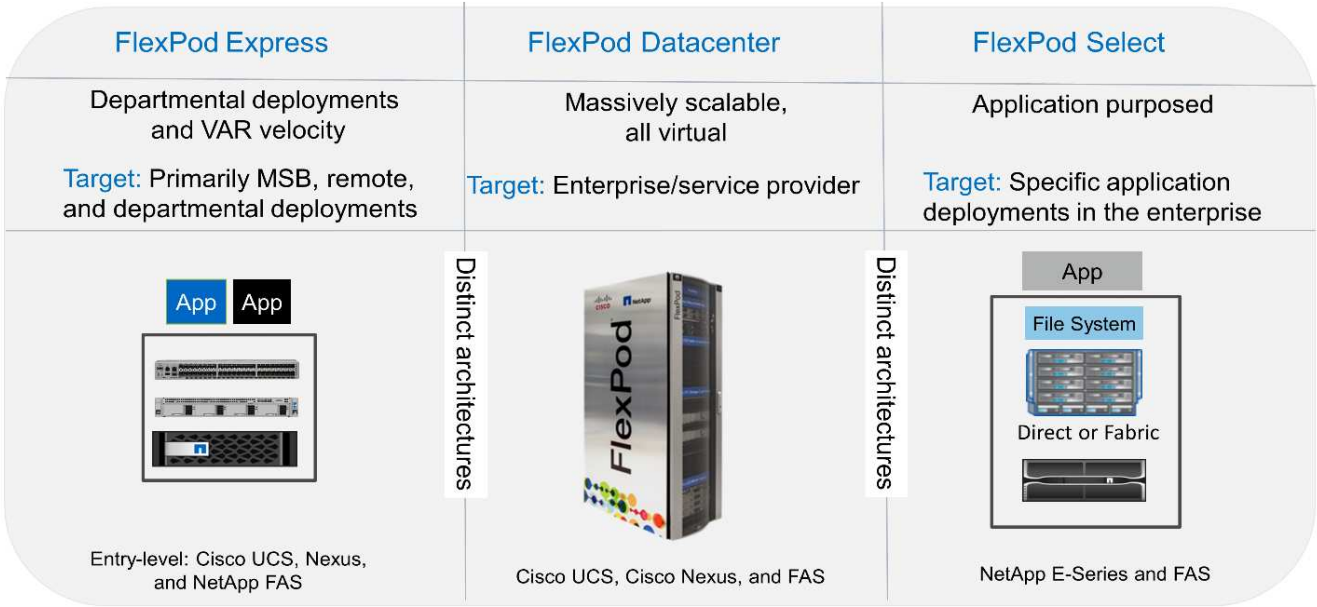
Questa soluzione FlexPod Express fa parte del programma di infrastruttura convergente FlexPod.

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.

Come illustrato nella figura seguente, il programma FlexPod include tre soluzioni: FlexPod Express, FlexPod Datacenter e FlexPod Select:

- **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.
- **FlexPod Select.** incorpora gli aspetti migliori del data center FlexPod e adatta l'infrastruttura a una determinata applicazione.



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:

- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione
- Accelera il time-to-market

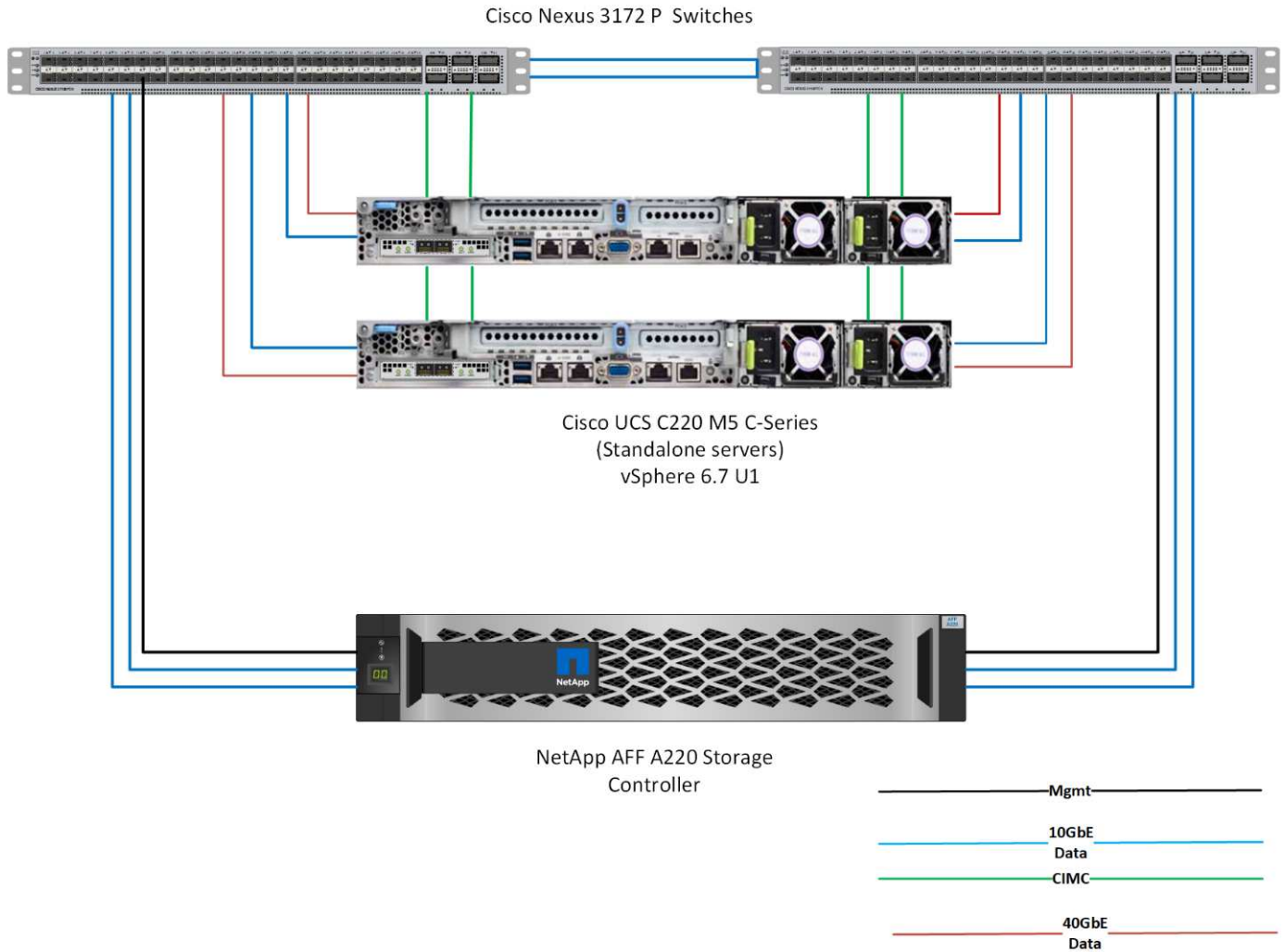
In questa guida viene illustrato in dettaglio il design di FlexPod con VMware vSphere. Inoltre, questo design utilizza il nuovissimo sistema AFF A220, che esegue NetApp ONTAP 9.4, Cisco Nexus 3172P e i server Cisco UCS C-Series C220 M5 come nodi hypervisor.

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. Questa soluzione include il nuovo NetApp AFF A220 con ONTAP 9.4, due switch Cisco Nexus 3172P e server rack Cisco UCS C220 M5 con VMware vSphere 6.7. 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.

La figura seguente mostra FlexPod Express con architettura VMware vSphere 10GbE.

FlexPod Express



Questa convalida utilizza la connettività 10 GbE e un Cisco UCS VIC 1387, che è 40 GbE. Per ottenere una connettività 10 GbE, viene utilizzato l'adattatore CVR-QSFP-SFP10G.

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 6.7, supporta qualsiasi versione vSphere qualificata con gli altri componenti dal NetApp Interoperability Matrix Tool. NetApp consiglia di implementare vSphere 6.7U1 per le correzioni e le funzionalità avanzate.

Di seguito sono riportate alcune funzionalità di vSphere 6.7 U1:

- Client vSphere basato su Web HTML5 con funzionalità complete
- VMotion per VM NVIDIA GRID vGPU. Supporto per Intel FPGA
- VCenter Server Converge Tool per passare da PSC esterno a PC interni
- Miglioramenti per vSAN (aggiornamenti HCI)
- Libreria di contenuti migliorata

Per ulteriori informazioni su vSphere 6.7 U1, vedere ["Novità di vCenter Server 6.7 Update 1"](#).

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, entrambi gli hypervisor possono essere eseguiti sullo stesso hardware FlexPod Express.

La seguente tabella elenca i componenti hardware necessari per tutte le configurazioni FlexPod Express.

Hardware	Quantità
Coppia AFF A220 ha	1
Server Cisco C220 M5	2
Switch Cisco Nexus 3172P	2
Cisco UCS Virtual Interface Card (VIC) 1387 per il server C220 M5	2
ADATTATORE CVR-QSFP-SFP10G	4

La seguente 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 1387	2
ADATTATORE CVR-QSFP-SFP10G	4

Requisiti software

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

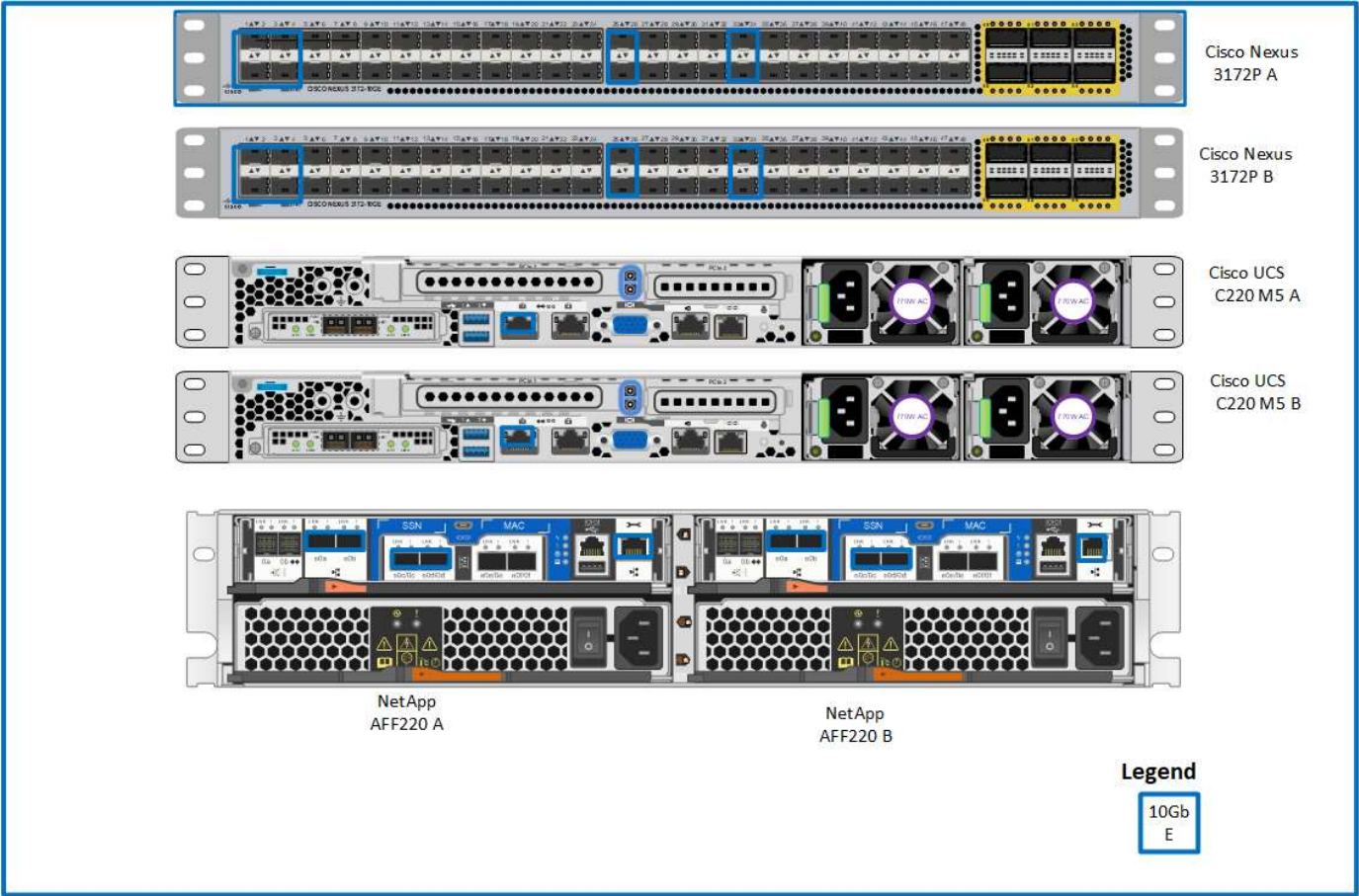
Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	3.1 (3g)	Per server rack Cisco UCS C220 M5
Driver Cisco Nenic	1.0.25.0	Per le schede di interfaccia VIC 1387
Sistema operativo Cisco NX	nxos.7.0.3.17.5.bin	Per switch Cisco Nexus 3172P
NetApp ONTAP	9.4	Per controller AFF A220

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

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

Informazioni di cablaggio FlexPod Express

La figura seguente mostra il cablaggio di convalida di riferimento.



La seguente tabella mostra le informazioni relative al cablaggio dello switch Cisco Nexus 3172P A.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 2P 317a	Eth1/1	Storage controller NetApp AFF A220 A	e0c
	Eth1/2	Storage controller NetApp AFF A220 B	e0c
	Eth1/3	Server standalone Cisco UCS C220 C-Series A	MLOM1 con adattatore CVR-QSFP-SFP10G
	Eth1/4	Server standalone Cisco UCS C220 C-Series B	MLOM1 con adattatore CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P B	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P B	Eth1/26
	Eth1/33	Storage controller NetApp AFF A220 A	E0M
	Eth1/34	Server standalone Cisco UCS C220 C-Series A	CIMC

La seguente tabella mostra le informazioni sul cablaggio per lo switch Cisco Nexus 3172P B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 3172P B	Eth1/1	Storage controller NetApp AFF A220 A	e0d
	Eth1/2	Storage controller NetApp AFF A220 B	e0d
	Eth1/3	Server standalone Cisco UCS C220 C-Series A	MLOM2 con adattatore CVR-QSFP-SFP10G
	Eth1/4	Server standalone Cisco UCS C220 C-Series B	MLOM2 con adattatore CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 2P 317a	Eth1/25
	Eth1/26	Switch Cisco Nexus 2P 317a	Eth1/26
	Eth1/33	Storage controller NetApp AFF A220 B	E0M
	Eth1/34	Server standalone Cisco UCS C220 C-Series B	CIMC

La seguente tabella mostra le informazioni di cablaggio per il controller storage NetApp AFF A220 A.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Storage controller NetApp AFF A220 A	e0a	Storage controller NetApp AFF A220 B	e0a

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
	e0b	Storage controller NetApp AFF A220 B	e0b
	e0c	Switch Cisco Nexus 2P 317a	Eth1/1
	e0d	Switch Cisco Nexus 3172P B	Eth1/1
	E0M	Switch Cisco Nexus 2P 317a	Eth1/33

La seguente tabella mostra le informazioni relative al cablaggio del controller di storage NetApp AFF A220 B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Storage controller NetApp AFF A220 B	e0a	Storage controller NetApp AFF A220 A	e0a
	e0b	Storage controller NetApp AFF A220 A	e0b
	e0c	Switch Cisco Nexus 2P 317a	Eth1/2
	e0d	Switch Cisco Nexus 3172P B	Eth1/2
	E0M	Switch Cisco Nexus 3172P B	Eth1/33

Procedure di implementazione

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

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

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

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

Questo documento consente di configurare completamente l'ambiente FlexPod Express. In questo processo, diversi passaggi richiedono l'inserimento di convenzioni di denominazione specifiche del cliente, indirizzi IP e schemi VLAN (Virtual Local Area Network). La tabella seguente descrive le VLAN richieste per

l'implementazione, come descritto in questa guida. Questa tabella può essere completata in base alle variabili specifiche del sito e utilizzata per implementare le fasi di configurazione del documento.



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

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

I numeri VLAN sono necessari per tutta la configurazione di FlexPod Express. Le VLAN sono indicate come `<<var_XXXX_vlan>>`, dove `XXXX` È lo scopo della VLAN (ad esempio iSCSI-A).

La tabella seguente elenca le macchine virtuali VMware create.

Descrizione della macchina virtuale	Nome host
VMware vCenter Server	

Procedura di implementazione di Cisco Nexus 3172P

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

Configurazione iniziale dello switch Cisco Nexus 3172P

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



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

1. All'avvio iniziale e alla connessione alla porta della console dello switch, viene avviata automaticamente l'installazione di Cisco NX-OS. Questa configurazione iniziale riguarda le impostazioni di base, come il nome dello switch, la configurazione dell'interfaccia mgmt0 e l'installazione di Secure Shell (SSH).

2. La rete di gestione FlexPod Express può essere configurata in diversi modi. Le interfacce mgmt0 degli switch 3172P possono essere collegate a una rete di gestione esistente oppure le interfacce mgmt0 degli switch 3172P possono essere collegate in una configurazione back-to-back. Tuttavia, questo collegamento non può essere utilizzato per l'accesso alla gestione esterna, ad esempio il traffico SSH.

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

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

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

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

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

- 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
```

- Ripetere questa procedura per lo switch Cisco Nexus B.

Abilitare le funzionalità avanzate

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



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

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

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

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

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

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

Eseguire la configurazione spanning-tree globale

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

Per impostazione predefinita, NetApp consiglia di impostare il bridge assurance in modo che tutte le porte siano considerate porte di rete. Questa impostazione obbliga l'amministratore di rete a rivedere la configurazione di ciascuna porta. Inoltre, vengono visualizzati gli errori di configurazione più comuni, ad

esempio porte edge non identificate o un vicino che non dispone della funzione di bridge assurance attivata. Inoltre, è più sicuro avere il blocco spanning tree molte porte piuttosto che troppo poche, il che consente allo stato di porta predefinito di migliorare la stabilità generale della rete.

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

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

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

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

Definire le VLAN

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

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

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurare le descrizioni delle porte di accesso e di gestione

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

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

Switch Cisco Nexus A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configurare le interfacce di gestione dello storage e del server

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

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

Switch Cisco Nexus A

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

Switch Cisco Nexus B

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

Eseguire la configurazione globale del canale della porta virtuale

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

Un VPC offre i seguenti vantaggi:

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

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

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

Switch Cisco Nexus A

```
vpc domain 1
  role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Switch Cisco Nexus B

```

vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start

```

Configurare i canali delle porte di storage

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

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

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

```

int eth1/1
    channel-group 11 mode active
int Po11
    description vPC to Controller-A
    switchport
    switchport mode trunk
    switchport trunk native vlan <<native_vlan_id>>
    switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
    spanning-tree port type edge trunk
    mtu 9216
    vpc 11
    no shut

```

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

```

int eth1/2
    channel-group 12 mode active
int Po12
    description vPC to Controller-B
    switchport
    switchport mode trunk
    switchport trunk native vlan <<native_vlan_id>>
    switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
    spanning-tree port type edge trunk
    mtu 9216
    vpc 12
    no shut
exit
copy run start

```



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

Configurare le connessioni al server

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

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

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

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

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

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

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

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

Uplink nell'infrastruttura di rete esistente

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

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

["Pagina successiva: Procedura di implementazione dello storage NetApp \(parte 1\)"](#)

Procedura di implementazione dello storage NetApp (parte 1)

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

Installazione del controller di storage NetApp serie AFF2xx

NetApp Hardware Universe

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

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

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

Prerequisiti della serie AFF2XX del controller

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

Controller di storage

Seguire le procedure di installazione fisica per i controller in ["Documentazione di AFF A220"](#).

NetApp ONTAP 9.4

Foglio di lavoro per la configurazione

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



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

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

Dettaglio del cluster	Valore dei dettagli del cluster
Indirizzo IP del nodo cluster A.	[var_nodeA_mgmt_ip]
Netmask del nodo cluster A.	[var_nodeA_mgmt_mask]
Nodo cluster A gateway	[var_nodeA_mgmt_gateway]

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

Configurare il nodo A.

Per configurare il nodo A, attenersi alla seguente procedura:

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

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

2. Consentire l'avvio del sistema.

```
autoboot
```

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

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

4. Per installare il nuovo software, selezionare l'opzione 7.
5. Invio y per eseguire un aggiornamento.
6. Selezionare e0M per la porta di rete che si desidera utilizzare per il download.
7. Invio y per riavviare ora.

8. Inserire l'indirizzo IP, la netmask e il gateway predefinito per e0M nelle rispettive posizioni.

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

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



Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

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

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

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

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

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

Configurare il nodo B.

Per configurare il nodo B, attenersi alla seguente procedura:

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

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

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

```
autoboot
```

3. Premere Ctrl-C quando richiesto.

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

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

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

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



Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

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

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

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

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

Continuazione della configurazione del nodo A e della configurazione del cluster

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



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

1. Seguire le istruzioni per impostare il nodo A.

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
    "help" or "?" - if you want to have a question clarified,
    "back" - if you want to change previously answered questions, and
    "exit" or "quit" - if you want to quit the cluster setup wizard.
    Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

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

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

3. Fare clic su Guided Setup (Configurazione guidata) per configurare il cluster.

4. Invio <<var_clustername>> per il nome del cluster e. <<var_nodeA>> e. <<var_nodeB>> per ciascuno dei nodi che si sta configurando. Inserire la password che si desidera utilizzare per il sistema di storage. Selezionare Switchless Cluster (Cluster senza switch) per il tipo di cluster. Inserire la licenza di base del cluster.

Guided Setup to Configure a Cluster

Provide the information required below to configure your cluster:

Cluster Name

Nodes
 ⓘ Not sure all nodes have been discovered? [Refresh](#)

Cluster Configuration: ☐ Switched Cluster ☐ Switchless Cluster

ⓘ Username admin

Password

Confirm Password

Cluster Base License (Optional)

ⓘ For any queries related to licenses, contact mysupport.netapp.com

Feature Licenses (Optional)

ⓘ Cluster Base License is mandatory to add Feature Licenses.

5. È inoltre possibile inserire licenze delle funzionalità per Cluster, NFS e iSCSI.
6. Viene visualizzato un messaggio di stato che indica che il cluster è in fase di creazione. Questo messaggio di stato passa in rassegna diversi stati. Questo processo richiede alcuni minuti.
7. Configurare la rete.
 - a. Deselezionare l'opzione IP Address Range (intervallo indirizzi IP).
 - b. Invio `<<var_clustermgmt_ip>>` Nel campo Cluster Management IP Address (Indirizzo IP di gestione cluster), `<<var_clustermgmt_mask>>` Nel campo Netmask, e, `<<var_clustermgmt_gateway>>` Nel campo Gateway. Utilizzare il ... Nel campo Port (porta) per selezionare e0M del nodo A.
 - c. L'IP di gestione dei nodi per il nodo A è già popolato. Invio `<<var_nodeA_mgmt_ip>>` Per il nodo B.

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

È possibile immettere più indirizzi IP del server DNS.

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

È inoltre possibile inserire un server NTP alternativo.

8. Configurare le informazioni di supporto.

- a. Se l'ambiente richiede un proxy per accedere a AutoSupport, inserire l'URL nel campo URL proxy.
- b. Inserire l'host di posta SMTP e l'indirizzo di posta elettronica per le notifiche degli eventi.

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

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

Continuazione della configurazione del cluster di storage

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

Azzerare tutti i dischi spare

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

```
disk zerospares
```

Impostare la personalità delle porte UTA2 a bordo scheda

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

```
AFF A220::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status
AFF A220_A	0c	fc	target	-	-	online
AFF A220_A	0d	fc	target	-	-	online
AFF A220_A	0e	fc	target	-	-	online
AFF A220_A	0f	fc	target	-	-	online
AFF A220_B	0c	fc	target	-	-	online
AFF A220_B	0d	fc	target	-	-	online
AFF A220_B	0e	fc	target	-	-	online
AFF A220_B	0f	fc	target	-	-	online

8 entries were displayed.

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

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

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

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



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

Rinominare le interfacce logiche di gestione (LIF)

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

1. Mostra i nomi LIF di gestione correnti.

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

2. Rinominare la LIF di gestione del cluster.

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

3. Rinominare la LIF di gestione del nodo B.

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

Impostare il revert automatico sulla gestione del cluster

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

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

Configurare l'interfaccia di rete del Service Processor

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

```
system service-processor network modify -node <<var_nodeA>> -address  
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeA_sp_ip>>  
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>  
system service-processor network modify -node <<var_nodeB>> -address  
-family IPv4 -enable true -dhcp none -ip-address <<var_nodeB_sp_ip>>  
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```



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

Abilitare il failover dello storage in ONTAP

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

1. Verificare lo stato del failover dello storage.

```
storage failover show
```

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

2. Attivare il failover su uno dei due nodi.

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

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

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

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

```
cluster ha show
```

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

```
High Availability Configured: true
```

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



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

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

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

```
storage failover hwassist show
```

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

```
storage failover modify -hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify -hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Creare un dominio di trasmissione MTU con frame jumbo in ONTAP

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

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Rimuovere le porte dati dal dominio di trasmissione predefinito

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

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

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Disattiva il controllo di flusso sulle porte UTA2

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


```

net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y

```

Configurare IFGRP LACP in ONTAP

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

Dal prompt del cluster, completare la seguente procedura.

```

ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d

```

Configurare i frame jumbo in NetApp ONTAP

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

```

AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
        this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
        this network port.
Do you want to continue? {y|n}: y

```

Creare VLAN in ONTAP

Per creare VLAN in ONTAP, attenersi alla seguente procedura:

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

```

network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>

```

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

```

network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>

```

3. Creare porte MGMT-VLAN.

```

network port vlan create -node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>

```

Creare aggregati in ONTAP

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

Per creare aggregati, eseguire i seguenti comandi:

```

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

```

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

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

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

Configurare il fuso orario in ONTAP

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

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



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

Configurare SNMP in ONTAP

Per configurare SNMP, attenersi alla seguente procedura:

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

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

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

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

Configurare SNMPv1 in ONTAP

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

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



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

Configurare SNMPv3 in ONTAP

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

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

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

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

Configurare HTTPS AutoSupport in ONTAP

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

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

Creare una macchina virtuale per lo storage

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

1. Eseguire `vserver create` comando.

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

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

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

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

```
vserver remove-protocols -vserver Infra-SVM -protocols cifs,ndmp,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 macchine virtuali dello storage erano precedentemente chiamate `server`.

Configurare NFSv3 in ONTAP

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

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

Per configurare NFS su SVM, eseguire i seguenti comandi:

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

```
vserver export-policy rule create -vserver Infra-SVM -policyname default  
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>  
-rorule sys -rwrule sys -superuser sys -allow-suid false  
vserver export-policy rule create -vserver Infra-SVM -policyname default  
-ruleindex 2 -protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>  
-rorule sys -rwrule sys -superuser sys -allow-suid false  
vserver export-policy rule show
```

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

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



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

Creare un servizio iSCSI in ONTAP

Per creare il servizio iSCSI, completare la seguente fase:

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

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

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

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

```
volume create -vserver Infra_Vserver -volume rootvol_m01 -aggregate
aggr1_nodeA -size 1GB -type DP
volume create -vserver Infra_Vserver -volume rootvol_m02 -aggregate
aggr1_nodeB -size 1GB -type DP
```

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

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

3. Creare le relazioni di mirroring.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

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

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

Configurare l'accesso HTTPS in ONTAP

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

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

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

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

```
security certificate show
```

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

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

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

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

```
security certificate create [TAB] ...  
Example: security certificate create -common-name infra-svm. netapp.com  
-type server -size 2048 -country US -state "North Carolina" -locality  
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr  
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256  
-vserver Infra-SVM
```

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

```
security ssl modify [TAB] ...  
Example: security ssl modify -vserver Infra-SVM -server-enabled true  
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common  
-name infra-svm.netapp.com
```

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


```
system services web modify -external true -sslsv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
        interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```



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

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

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

Creare un volume NetApp FlexVol in ONTAP

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

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Attiva la deduplica in ONTAP

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

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

Creare LUN in ONTAP

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

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```



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

Creazione di LIF iSCSI in ONTAP

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

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

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

```

network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> -status-admin up -failover-policy
disabled -firewall-policy data -auto-revert false
network interface show

```

Creare LIF NFS in ONTAP

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

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

1. Creare una LIF NFS.

```

network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up -failover-policy broadcast-
domain-wide -firewall-policy data -auto-revert true
network interface show

```

Aggiungere l'amministratore SVM dell'infrastruttura

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

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

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

1. Eseguire il seguente comando:

```

network interface create -vserver Infra-SVM -lif vsmgmt -role data
-data-protocol none -home-node <<var_nodeB>> -home-port e0M -address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
-failover-policy broadcast-domain-wide -firewall-policy mgmt -auto-
revert true

```



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

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

```

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

```

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

```
security login password -username vsadmin -vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock -username vsadmin -vserver Infra-SVM
```

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

Procedura di implementazione dei server rack Cisco UCS C-Series

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

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

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

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

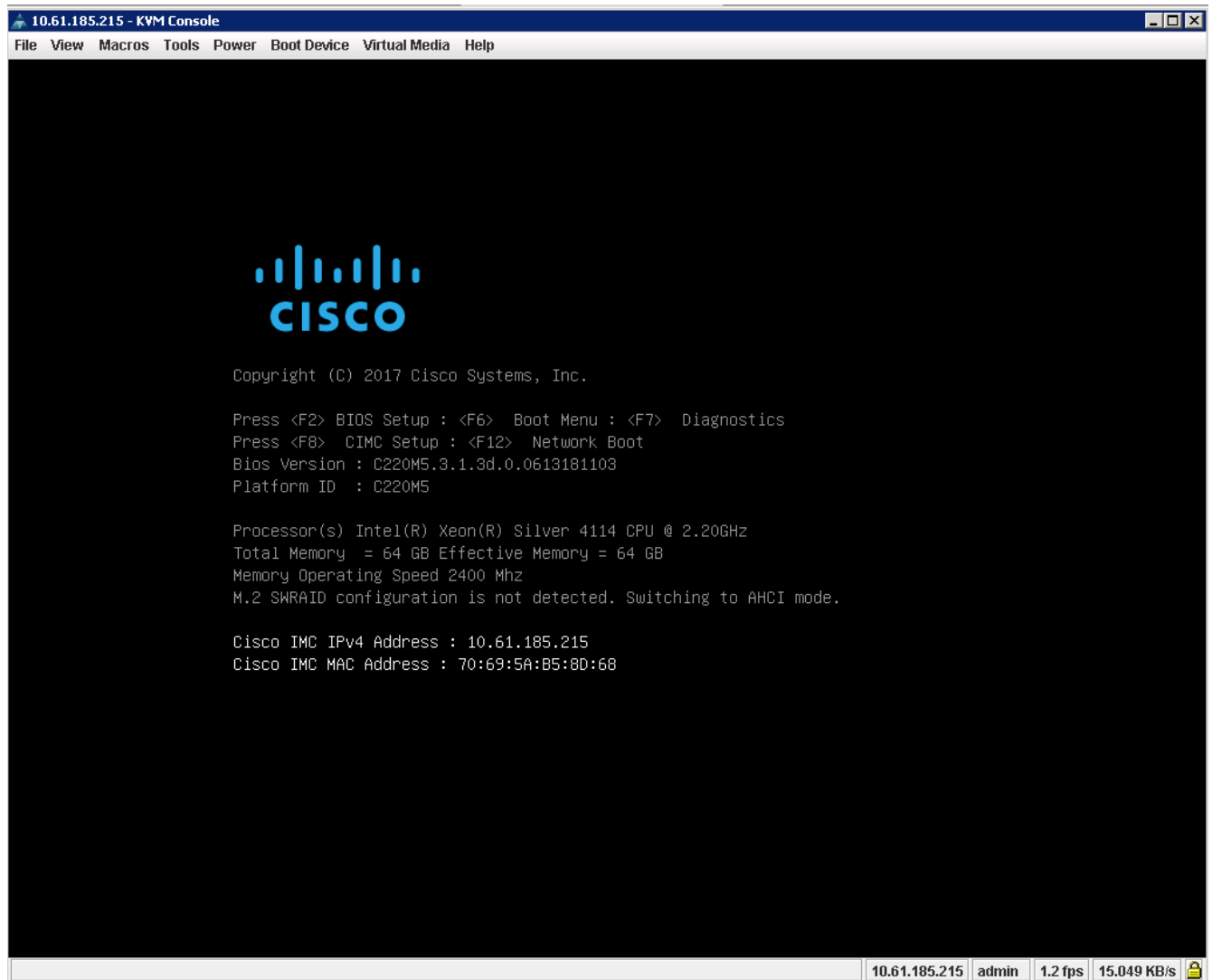
Dettaglio	Valore di dettaglio
Indirizzo IP CIMC	[cimc_ip]
Subnet mask CIMC	[cimc_netmask]
Gateway predefinito CIMC	[cimc_gateway]



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

Tutti i server

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



3. Nell'utilità di configurazione di CIMC, impostare le seguenti opzioni:

- Modalità scheda di interfaccia di rete (NIC):
 - Dedicato ☒ [X]
- IP (di base):
 - IPV4: ☒ [X]
 - DHCP abilitato: ☐ []
 - IP CIMC:
 - Prefisso/sottorete:
 - Gateway:
- VLAN (Advanced): Lasciare deselezionato per disattivare il tagging VLAN.
 - Ridondanza della NIC
 - Nessuno: ☒ [X]

```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode
Dedicated:      [X]          NIC redundancy
Shared LOM:     [ ]          None: [X]
Cisco Card:     [ ]          Active-standby: [ ]
Riser1:        [ ]          Active-active: [ ]
Riser2:        [ ]          VLAN (Advanced)
MLom:          [ ]          VLAN enabled: [ ]
Shared LOM Ext: [ ]          VLAN ID: 1
Priority: 0
IP (Basic)
IPv4: [X]          IPv6: [ ]
DHCP enabled [ ]
CIMC IP: 10.61.185.215
Prefix/Subnet: 255.255.255.0
Gateway: 10.61.185.1
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
```

4. Premere F1 per visualizzare ulteriori impostazioni.

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


```
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
  Hostname:      CIMC-Tiger-02
  Dynamic DNS:   [X]
  DDNS Domain:
FactoryDefaults
  Factory Default:      [ ]
Default User(Basic)
  Default password:      -
  Reenter password:
Port Properties
  Auto Negotiation:      [X]
                                Admin Mode      Operation Mode
  Speed[1000/100/10Mbps]:      Auto              1000
  Duplex mode[half/full]:      Auto              full
Port Profiles
  Reset:                  [ ]
  Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettings
```

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

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

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

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



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

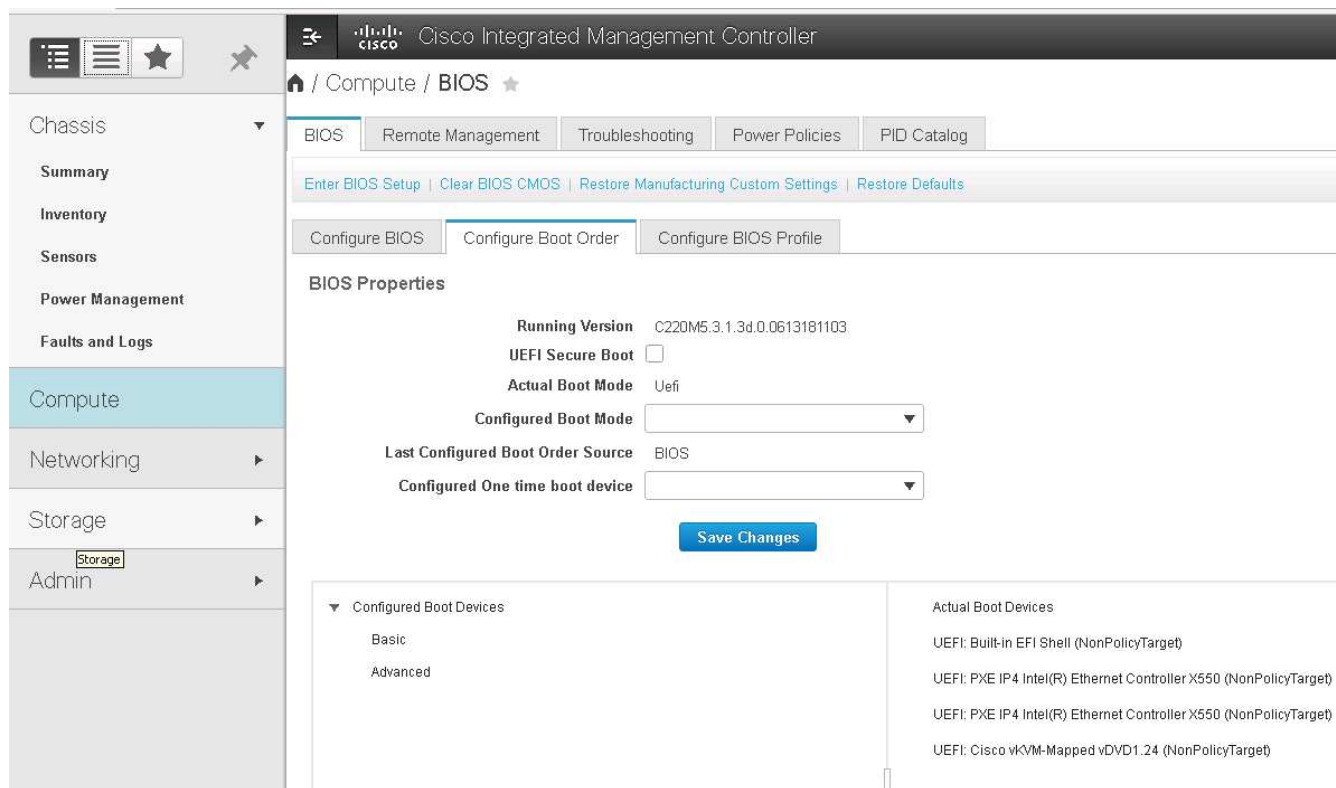
Dettaglio	Valore di dettaglio
Nome dell'iniziatore host ESXi	[var_ucs_initiator_name_A]
IP iSCSI-A host ESXi	[var_esxi_host_iscsiA_ip]
Host ESXi iSCSI-A network mask	[var_esxi_host_iscsiA_mask]
ESXi host iSCSI Un gateway predefinito	[var_esxi_host_iscsiA_gateway]
Nome B dell'iniziatore host ESXi	[var_ucs_initiator_name_B]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

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

Configurazione dell'ordine di avvio

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

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



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

- Stato: Attivato
- Ordine: 2
- Slot: MLOM
- Porta: 0
- Fare clic su Add iSCSI Boot.
 - Nome: iSCSI-B.
 - Stato: Attivato
 - Ordine: 3
 - Slot: MLOM
 - Porta: 1

4. Fare clic su Aggiungi dispositivo.

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

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. 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 VIC1387 per l'avvio iSCSI

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

Creare vNIC iSCSI

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

vNIC Properties

General

Name: iSCSI-vNIC-A

CDN: VIC-MLOM-iSCSI-vNIC-A

MTU: 9000 (1500 - 9000)

Uplink Port: 0

MAC Address:
☐ Auto
☒ 70:69:5A:C0:98:ED

Class of Service: 0 (0 - 6)

Trust Host CoS: ☒

PCI Order: 4 (0 - 5)

Default VLAN:
☐ None
☒ 3439

VLAN Mode: Trunk

Rate Limit: ☒ OFF
☐ (1 - 1000)

Channel Number: N/A (1 - 1000)

PCI Link: 0 (0 - 1)

Enable NVGRE: ☐

Enable VXLAN: ☐

Advanced Filter: ☐

Port Profile: N/A

Enable PXE Boot: ☒

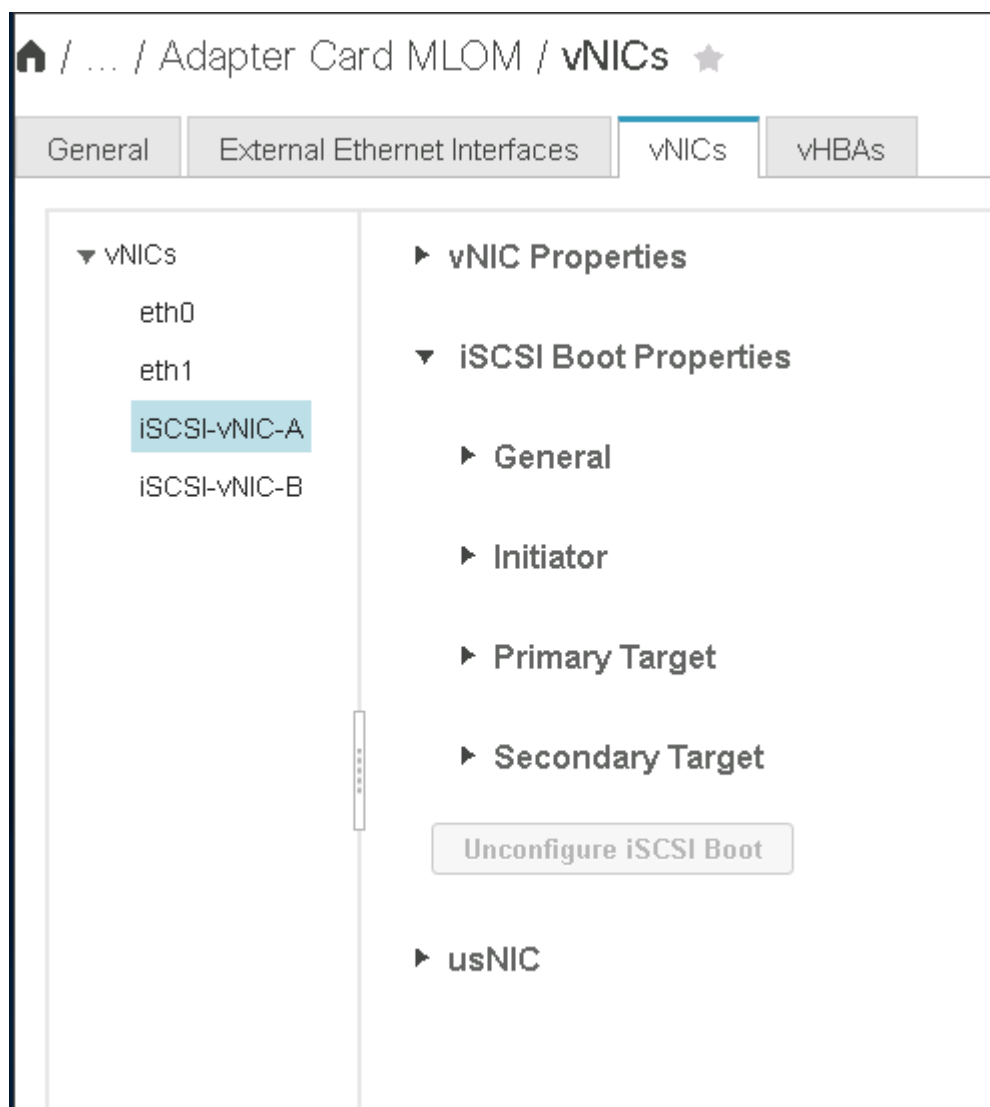
Enable VMQ: ☐

Enable aRFS: ☐

Enable Uplink Failover: ☐

Failback Timeout: N/A (0 - 600)

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



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

vNICs

eth0
eth1
ISCSI-v
ISCSI-v

ISCSI Boot Properties

General

Initiator

Name: (0 - 233) chars
Initiator Priority:

IP Address:
Secondary DNS:

Subnet Mask:
TCP Timeout:

Gateway:
CHAP Name:

Primary DNS:
CHAP Secret:

Primary Target

Secondary Target

7. Inserire i dettagli principali del target.

- Name (Nome): Numero IQN di infra-SVM
- IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif01a`
- LUN di boot: 0

8. Inserire i dettagli della destinazione secondaria.

- Name (Nome): Numero IQN di infra-SVM
- IP address (Indirizzo IP): Indirizzo IP di `iscsi_lif02a`
- LUN di boot: 0

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



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

General

External Ethernet Interfaces

vNICs

vHBAs

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

► Initiator

▼ Primary Target

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars

IP Address: 172.21.246.16

TCP Port: 3260

Boot LUN: 0

CHAP Name:

CHAP Secret:

▼ Secondary Target

Name: iqn.1992-08.com.netapp:sn.7e560f73a51 (0 - 233) chars

IP Address: 172.21.246.18

TCP Port: 3260

Boot LUN: 0

CHAP Name:

CHAP Secret:

Unconfigure iSCSI Boot

9. Fare clic su Configura iSCSI.

10. Selezionare la vNIC iSCSI-vNIC- B E fare clic sul pulsante iSCSI Boot (Avvio iSCSI) situato nella parte superiore della sezione host Ethernet Interfaces (interfacce Ethernet host).

11. Ripetere la procedura da configurare iSCSI-vNIC-B.

12. Inserire i dettagli dell'iniziatore.

- Nome: <<var_ucsa_initiator_name_b>>
- Indirizzo IP: <<var_esxi_hostb_iscsib_ip>>
- Subnet mask: <<var_esxi_hostb_iscsib_mask>>
- Gateway: <<var_esxi_hostb_iscsib_gateway>>

13. Inserire i dettagli principali del target.

- Name (Nome): Numero IQN di infra-SVM
- IP address (Indirizzo IP): Indirizzo IP di iscsi_lif01b
- LUN di boot: 0

14. Inserire i dettagli della destinazione secondaria.

- Name (Nome): Numero IQN di infra-SVM
- IP address (Indirizzo IP): Indirizzo IP di iscsi_lif02b
- LUN di boot: 0

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



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

15. Fare clic su Configura iSCSI.

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

Configurare vNIC per ESXi

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

🏠 / ... / Adapter Card [Refresh](#) | [Host Power](#) | [Launch KVM](#) | [Ping](#) | [CIMC Reboot](#) | [Locat](#)

MLOM / vNICs ★

General External Ethernet Interfaces **vNICs** vHBAs

▼ vNICs

- eth0
- eth1
- iSCSI-v
- iSCSI-v

Host Ethernet Interfaces Selected 0,

Add vNIC Clone vNIC Delete vNICs

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port	CoS	VLAN	VLAN Mode
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	1500	0	0	0	NONE	TRUNK
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	1500	0	1	0	NONE	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0	0	3439	TRUNK
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	1	0	3440	TRUNK

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

General

External Ethernet Interfaces

vNICs

vHBAs

▼ vNICs

eth0

eth1

ISCSI-v

ISCSI-v

Name:

eth0

CDN:

VIC-MLOM-eth0

MTU:

9000

(1500 - 9000)

Uplink Port:

0

MAC Address:

☐ Auto
 ☒ 70:69:5A:C0:98:49

Class of Service:

0

(0 - 6)

Trust Host CoS:

☐

PCI Order:

0

(0 - 5)

Default VLAN:

☒ None
 ☐ ?

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

[/ ... / Adapter Card MLOM / vNICs](#) ★

General

External Ethernet Interfaces

vNICs

vHBAs

▼ vNICs

eth0

eth1

ISCSI-vNIC-A

ISCSI-vNIC-B

Host Ethernet Interfaces

Add vNIC

Clone vNIC

Delete vNICs

	Name	CDN	MAC Address	MTU	usNIC	Uplink Port
<input type="checkbox"/>	eth0	VIC-MLO...	70:69:5A:C0:98:49	9000	0	0
<input type="checkbox"/>	eth1	VIC-MLO...	70:69:5A:C0:98:4A	9000	0	1
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4D	9000	0	0
<input type="checkbox"/>	iSCSI-v...	VIC-MLO...	70:69:5A:C0:98:4E	9000	0	1



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

Procedura di implementazione dello storage NetApp AFF (parte 2)

Configurazione dello storage di boot SAN ONTAP

Creare igroups iSCSI

Per creare igroups, completare il seguente passaggio:

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

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

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-A -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-B -protocol iscsi
-ostype vmware -initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```



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

Mappare le LUN di avvio a igroups

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

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



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

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

Procedura di implementazione di VMware vSphere 6.7

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

Esistono diversi metodi per l'installazione di VMware ESXi in un ambiente di questo tipo. Questa procedura

utilizza la console KVM virtuale e le funzioni dei supporti virtuali dell'interfaccia CIMC per i server Cisco UCS C-Series per mappare i supporti di installazione remota su ciascun server.



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

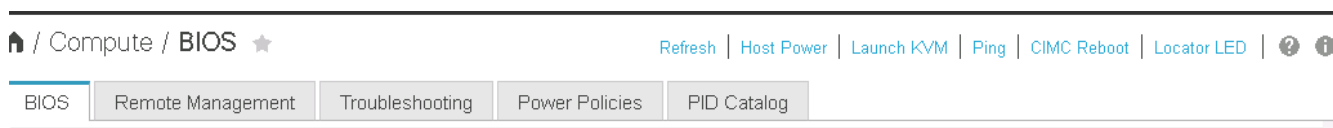
Questa procedura deve essere completata per tutti i nodi aggiuntivi aggiunti al cluster.

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

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

Tutti gli host

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



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



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

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

Installare VMware ESXi

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

Scarica L'immagine personalizzata di ESXi 6.7 Cisco

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

Tutti gli host

1. All'avvio del sistema, il computer rileva la presenza del supporto di installazione di VMware ESXi.

2. Selezionare il programma di installazione di VMware ESXi dal menu visualizzato.

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

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



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

Configurare il networking per la gestione degli host VMware ESXi

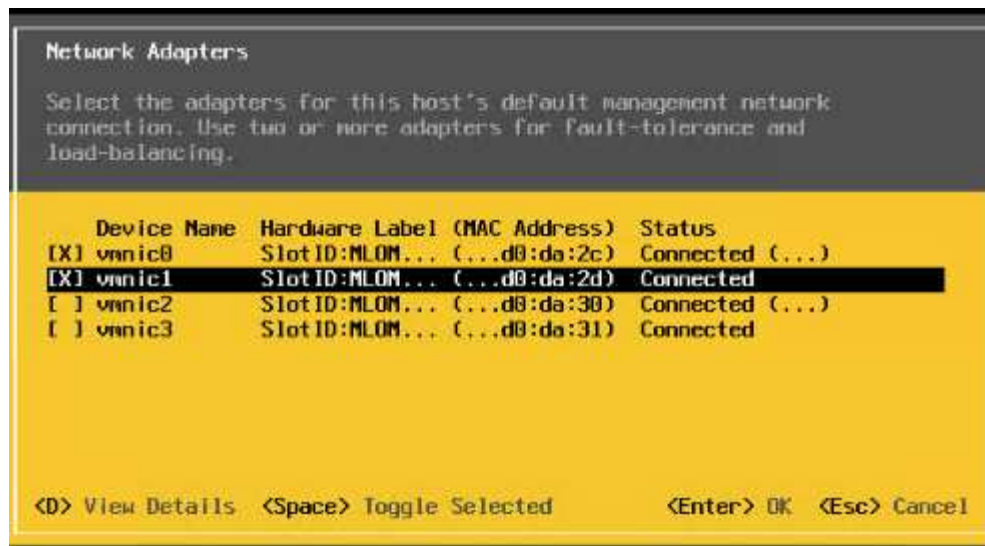
La seguente procedura descrive come aggiungere la rete di gestione per ciascun host VMware ESXi.

Tutti gli host

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



Selezionare le porte corrispondenti a eth0 e eth1 in CIMC.



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

Configurare l'host ESXi

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

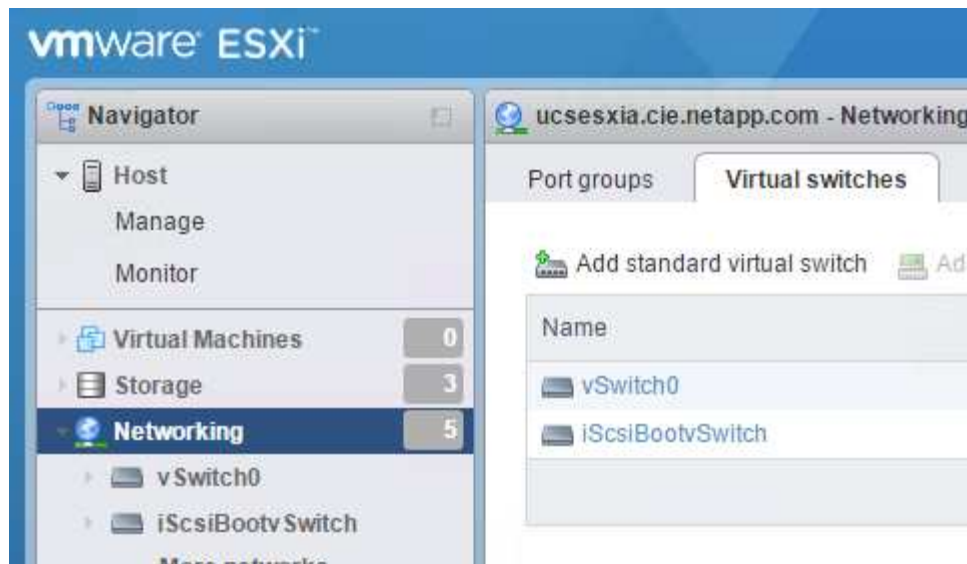
Dettaglio	Valore
Nome host ESXi	
IP di gestione host ESXi	
Maschera di gestione host ESXi	
Gateway di gestione host ESXi	
IP NFS host ESXi	
ESXi host NFS mask	
Gateway NFS host ESXi	
IP vMotion host ESXi	
Host ESXi vMotion mask	
Gateway vMotion host ESXi	
IP iSCSI-A host ESXi	
Host ESXi iSCSI-A mask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

Accedere all'host ESXi

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

Configurare l'avvio iSCSI

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



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



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

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

Add VMkernel NIC

Port group	New port group ▼
New port group	iScsiBootPG-B
Virtual switch	iScsiBootvSwitch-B ▼
VLAN ID	3440
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.184.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼
Services	<input checked="" type="checkbox"/> vMotion <input checked="" type="checkbox"/> Provisioning <input type="checkbox"/> Fault tolerance logging <input checked="" type="checkbox"/> Management <input type="checkbox"/> Replication <input type="checkbox"/> NFC replication

Create Cancel

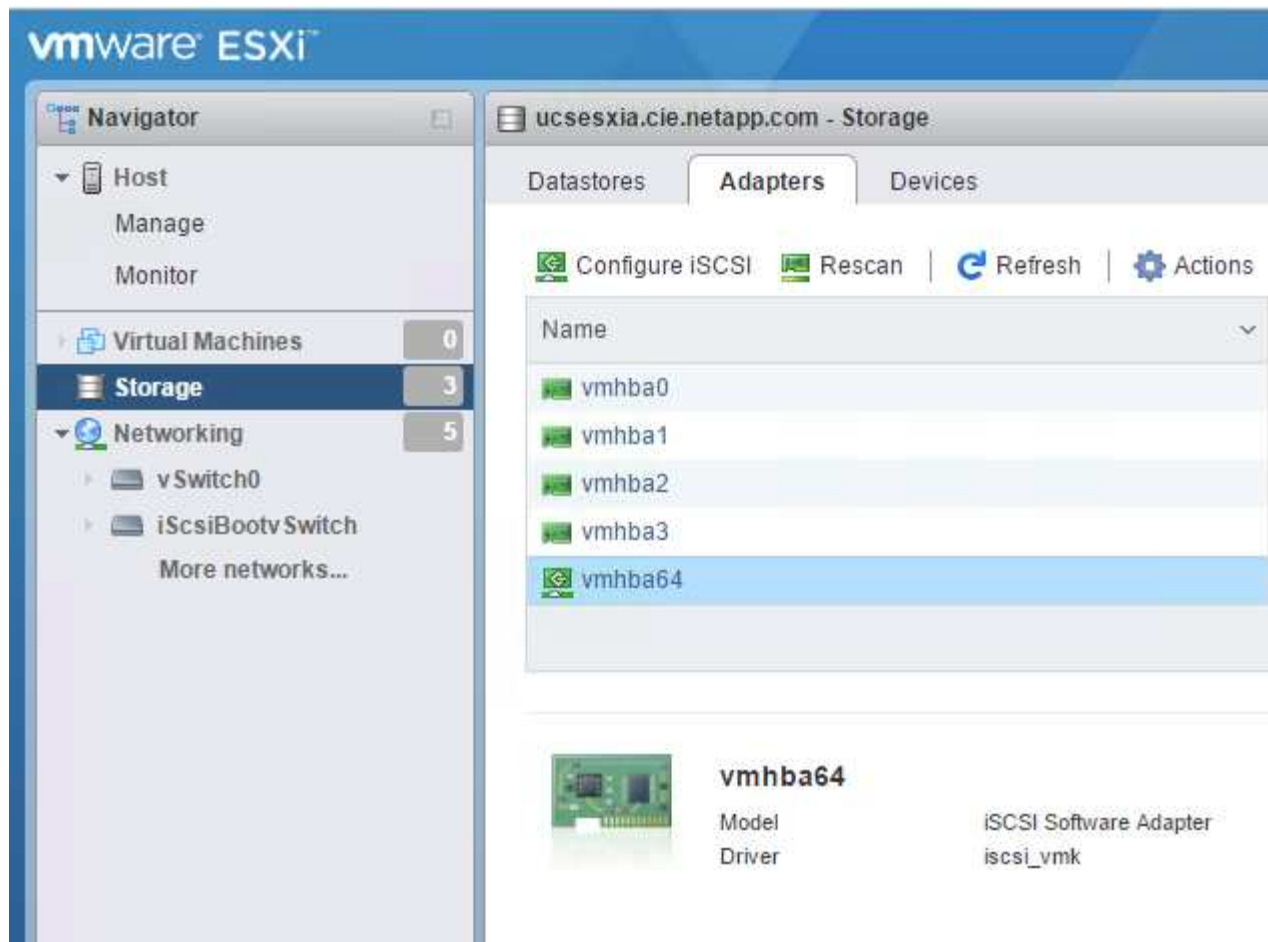


Impostare MTU su 9000 ON iScsiBootPG- A.

Configurare il multipathing iSCSI

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

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



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

Configure iSCSI - vmhba64

iSCSI enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled								
▶ Name & alias	iqn.1992-08.com.cisco:ucsaiscsia								
▶ CHAP authentication	Do not use CHAP ▼								
▶ Mutual CHAP authentication	Do not use CHAP ▼								
▶ Advanced settings	Click to expand								
Network port bindings	<div> Add port binding Remove port binding </div> <table border="1"> <thead> <tr> <th>VMkernel NIC</th> <th>Port group</th> <th>IPv4 address</th> </tr> </thead> <tbody> <tr> <td colspan="3">No port bindings</td> </tr> </tbody> </table>			VMkernel NIC	Port group	IPv4 address	No port bindings		
VMkernel NIC	Port group	IPv4 address							
No port bindings									
Static targets	<div> Add static target Remove static target Edit settings <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Target</th> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td>iqn.1992-08.com.netapp:sn.09591199033811e78eb...</td> <td>172.21.183.34</td> <td>3260</td> </tr> </tbody> </table>			Target	Address	Port	iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260
Target	Address	Port							
iqn.1992-08.com.netapp:sn.09591199033811e78eb...	172.21.183.34	3260							
Dynamic targets	<div> Add dynamic target Remove dynamic target Edit settings <input type="text" value="Search"/> </div> <table border="1"> <thead> <tr> <th>Address</th> <th>Port</th> </tr> </thead> <tbody> <tr> <td colspan="2">No dynamic targets</td> </tr> </tbody> </table>			Address	Port	No dynamic targets			
Address	Port								
No dynamic targets									

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**.

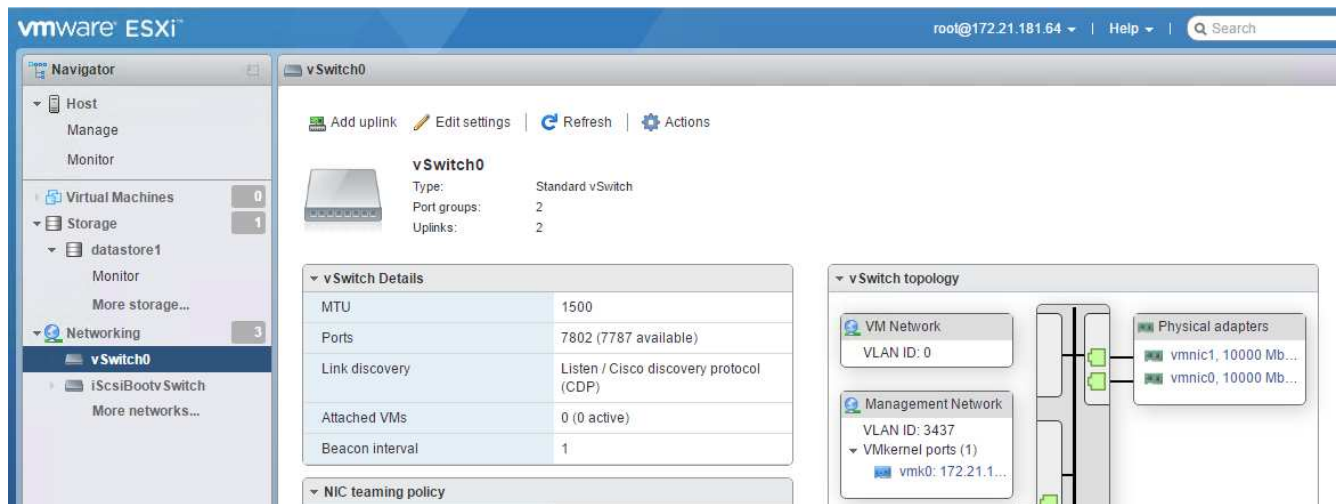
Dynamic targets	Add dynamic target Remove dynamic target Edit settings
Address	Port
172.21.183.33	3260
172.21.183.34	3260
172.21.184.33	3260
172.21.184.34	3260



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

Configurare l'host ESXi

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



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

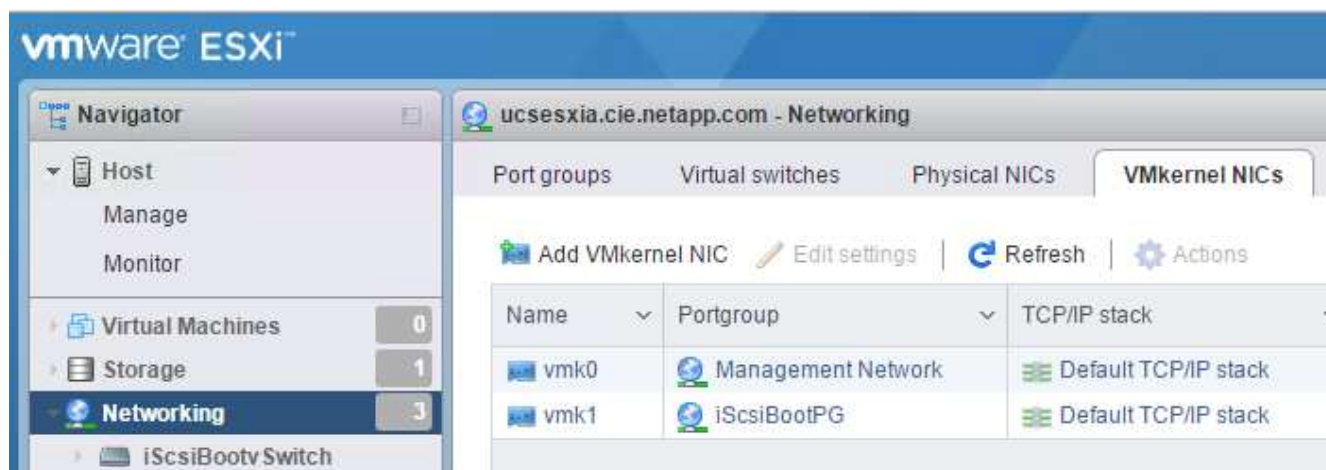
Configurare i gruppi di porte e le NIC VMkernel

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



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

5. Fare clic sulla scheda NIC VMkernel.



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

Port group	New port group ▼
New port group	NFS-Network
Virtual switch	vSwitch0 ▼
VLAN ID	3438
MTU	9000
IP version	IPv4 only ▼
▼ IPv4 settings	
Configuration	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Address	172.21.182.63
Subnet mask	255.255.255.0
TCP/IP stack	Default TCP/IP stack ▼

Create Cancel

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

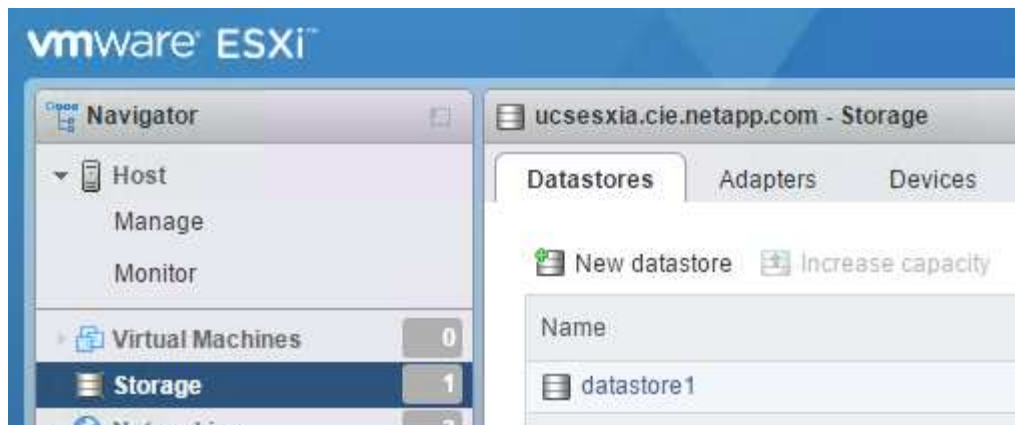


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

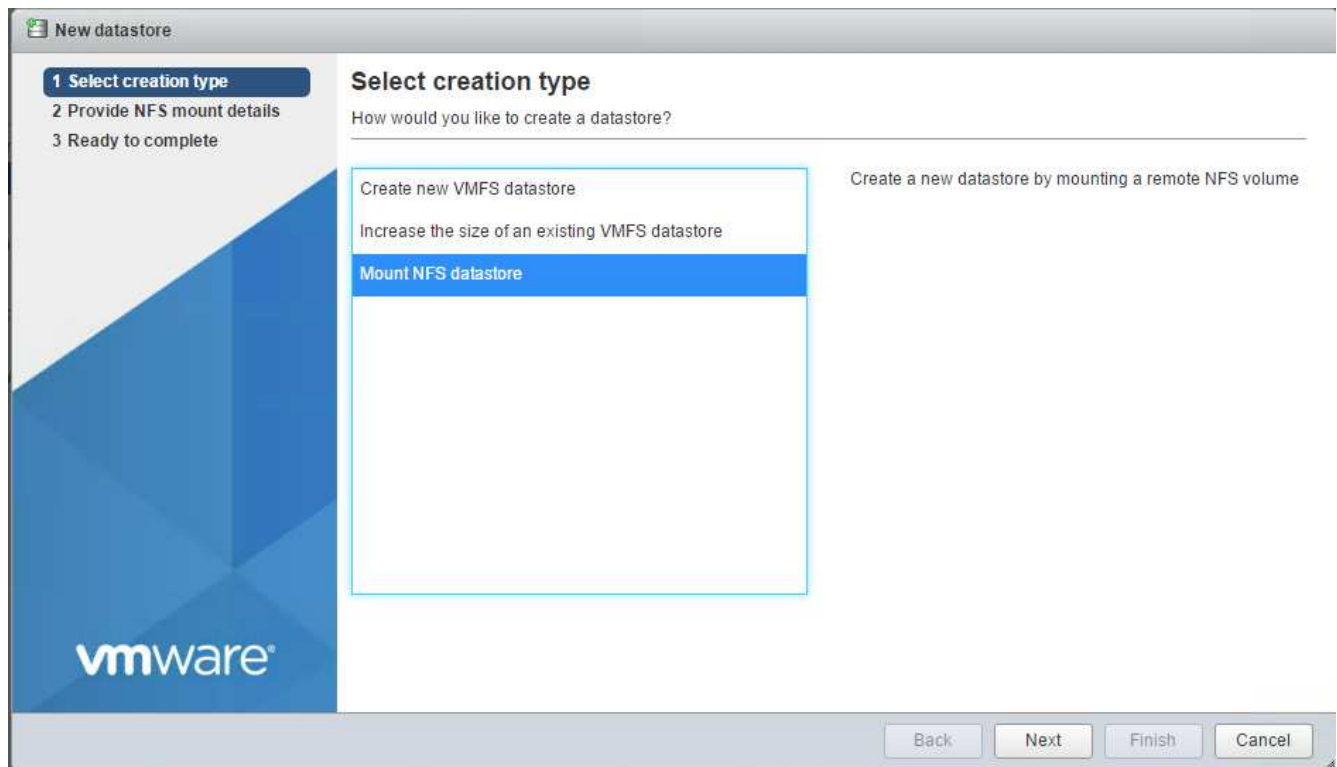
Montare i primi datastore

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

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



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



3. Quindi, inserire le seguenti informazioni nella pagina fornire i dettagli del montaggio NFS:

- Nome: `infra_datastore_1`
- Server NFS: `<<var_nodea_nfs_lif>>`
- Share: `/Infra_datastore_1`
- Assicurarsi che sia selezionato NFS 3.

4. Fare clic su fine. È possibile visualizzare il completamento dell'attività nel riquadro attività recenti.

5. Ripetere questa procedura per montare il datastore `infra_swap`:

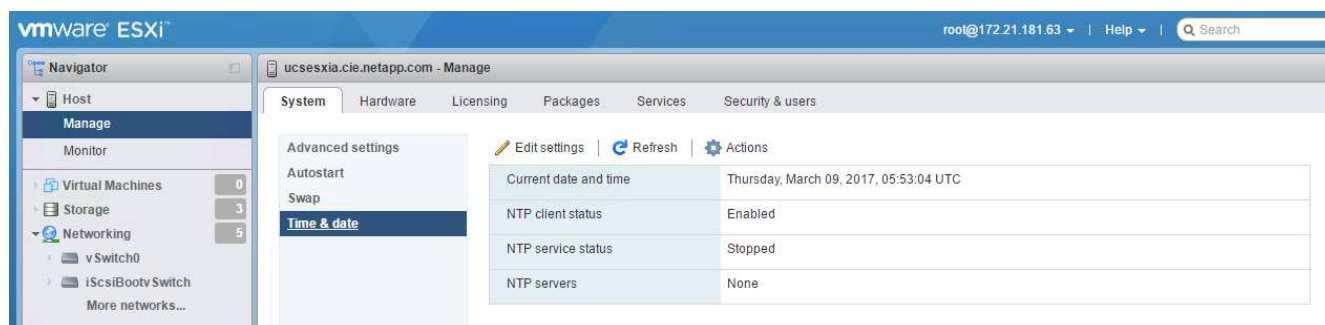
- Nome: `infra_swap`
- Server NFS: `<<var_nodea_nfs_lif>>`
- Condividere: `/infra_swap`

- Assicurarsi che sia selezionato NFS 3.

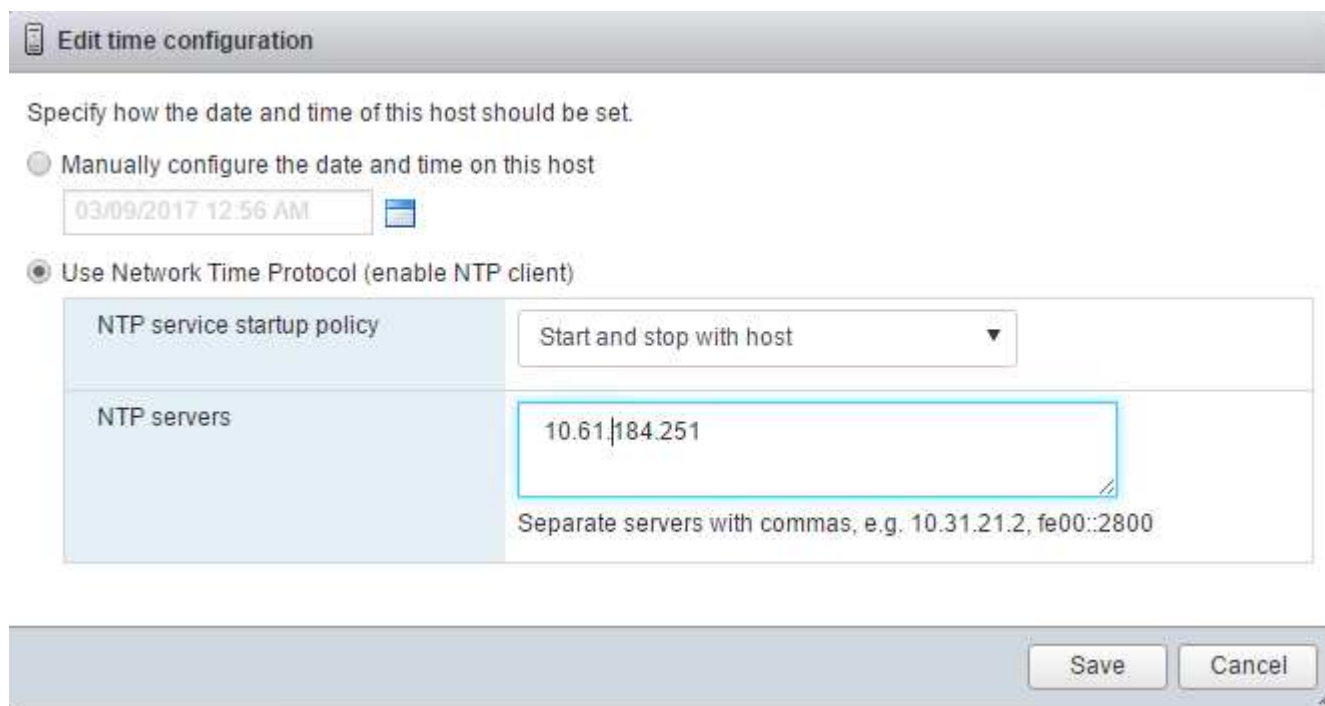
Configurare NTP

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

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



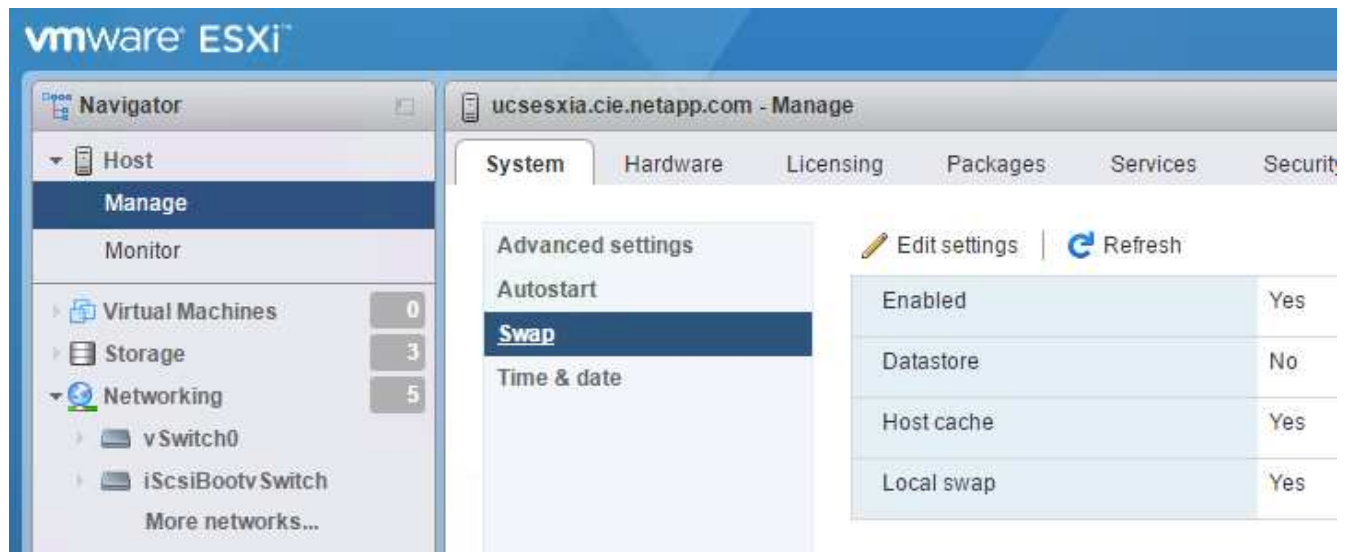
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio del servizio NTP.
4. Invio <<var_ntp>> Come server NTP. È possibile impostare più server NTP.
5. Fare clic su Salva.



Spostare la posizione del file di swap della macchina virtuale

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

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



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



3. Fare clic su Salva.

Installare il plug-in NetApp NFS 1.0.20 per VMware VAAI

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

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

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

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


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

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

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

Questi comandi producono il seguente output:

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

3. Scarica il plug-in NetApp NFS per VMware VAAI:

- Accedere alla ["pagina di download del software"](#).
- Scorrere verso il basso e fare clic su NetApp NFS Plug-in for VMware VAAI.
- Selezionare la piattaforma ESXi.
- Scarica il bundle offline (.zip) o il bundle online (.vib) del plug-in più recente.

4. Installare il plug-in sull'host ESXi utilizzando ESX CLI.

5. Riavviare l'host ESXi.

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
  Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
  Reboot Required: true
  VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
  VIBs Removed:
  VIBs Skipped:
```

"Installazione di VMware vCenter Server 6.7"

Installare VMware vCenter Server 6.7

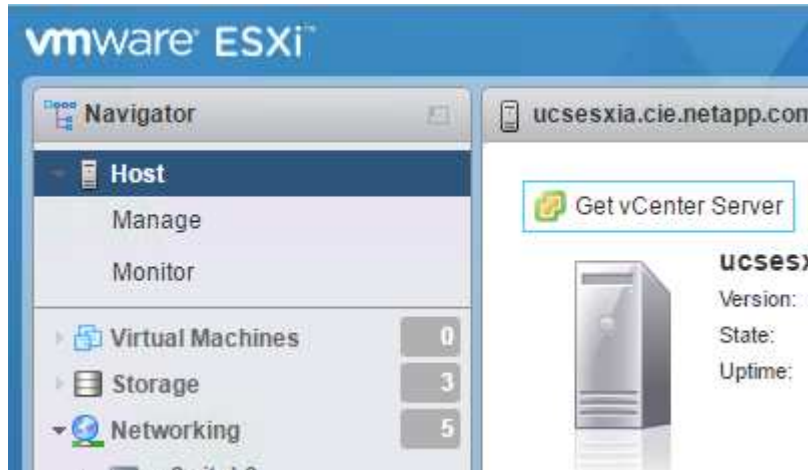
Questa sezione fornisce procedure dettagliate per l'installazione di VMware vCenter Server 6.7 in una configurazione FlexPod Express.



FlexPod utilizza l'appliance server vCenter (VCSA).

Scarica l'appliance server VMware vCenter

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

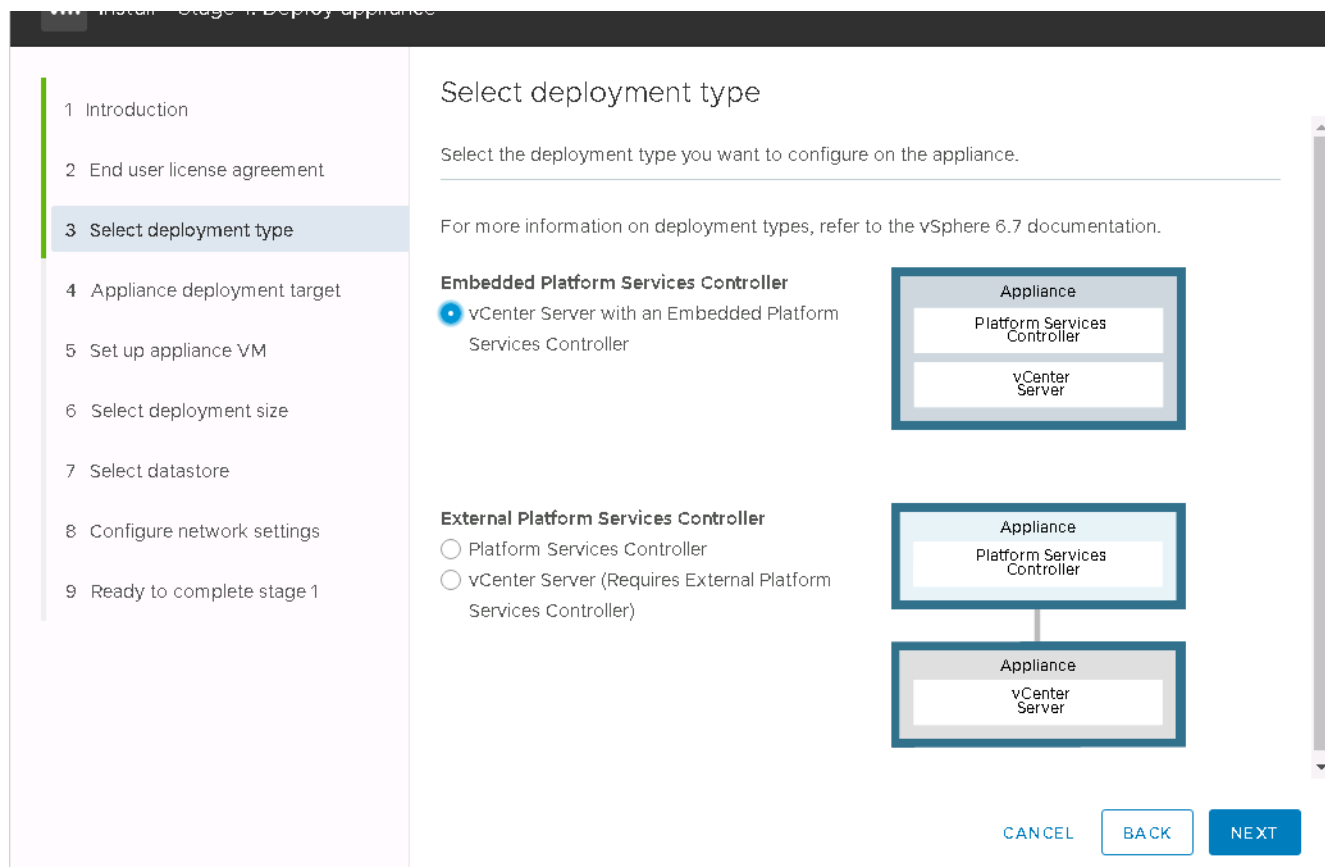


2. Scaricare VCSA dal sito VMware.



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

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



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

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

Installer

vm Install - Stage 1: Deploy vCenter Server 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	172.21.246.25	i
HTTPS port	443	
User name	root	i
Password	*****	

CANCEL

BACK

NEXT

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

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

vm Install - Stage 1: Deploy vCenter Server 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

Select datastore

Select the storage location for this appliance

☒ Install on an existing datastore accessible from the target host

Name	Type	Capacity	Free	Provisioned	Thin Provisioning
infra_datastore_1	NFS	500 GB	499.98 GB	18.38 MB	Supported
infra_swap	NFS	100 GB	99.99 GB	10.95 MB	Supported

2 items

☒ Enable Thin Disk Mode ⓘ

☐ Install on a new vSAN cluster containing the target host ⓘ

CANCEL

BACK

NEXT

13. Inserire le seguenti informazioni nella pagina Configure network settings (Configura impostazioni di rete) e fare clic su Next (Avanti).

- Selezionare MGMT-Network for Network (rete MGMT per rete).
- Inserire l'FQDN o l'IP da utilizzare per VCSA.
- Inserire l'indirizzo IP da utilizzare.
- Inserire la subnet mask da utilizzare.
- Inserire il gateway predefinito.
- Inserire il server DNS.

14. Nella pagina Pronto per completare la fase 1, verificare che le impostazioni immesse siano corrette. Fare clic su fine.

vCenter Server Appliance Installer

Installer

vm Install - Stage 1: Deploy vCenter Server 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

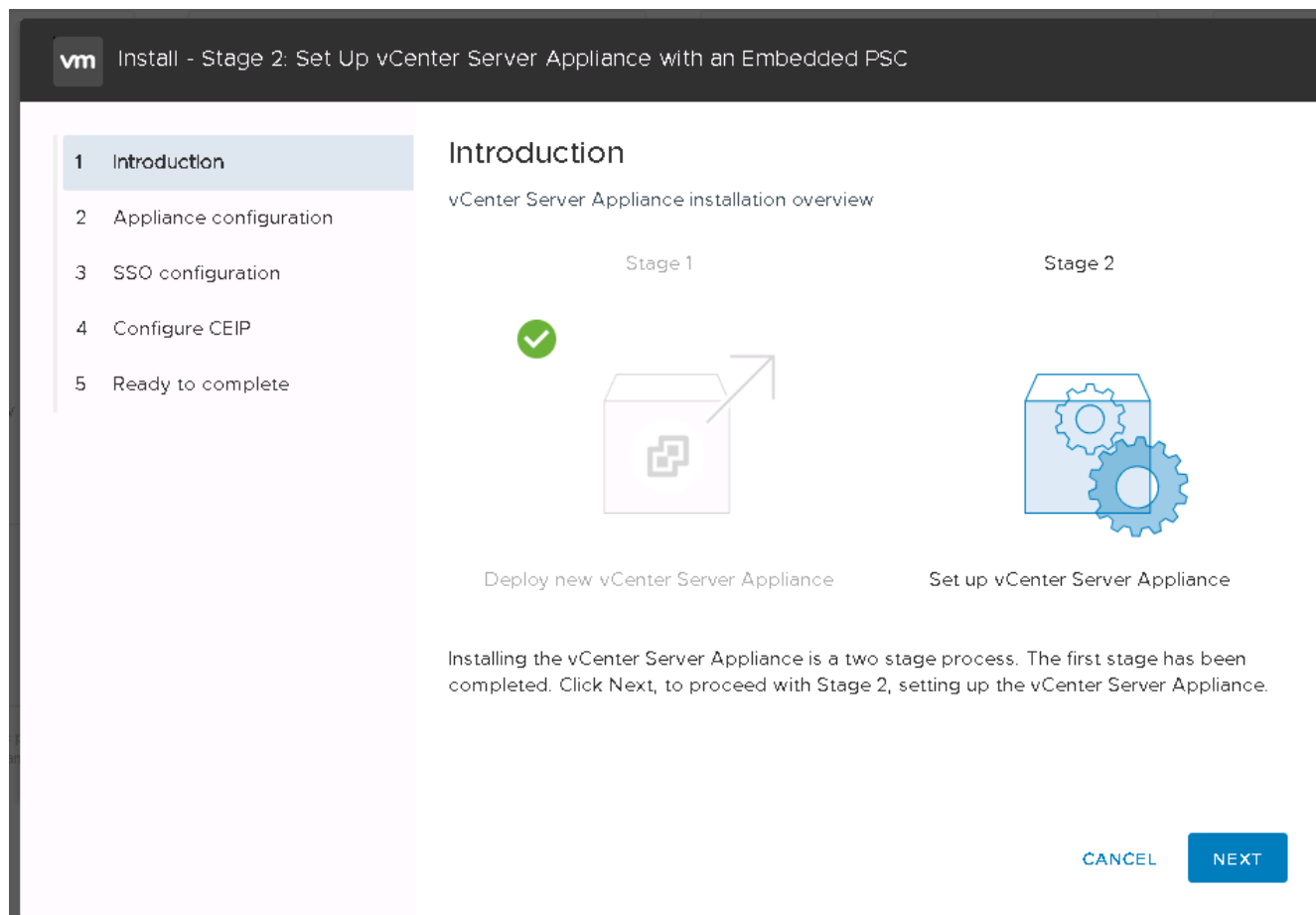
Configure network settings

IP version	IPv4	
IP assignment	static	
FQDN	tigervcsa.cle.netapp.com	i
IP address	172.21.246.41	
Subnet mask or prefix length	255.255.255.0	i
Default gateway	172.21.246.1	
DNS servers	10.61.184.251,10.61.184.252	
Common Ports		
HTTP	80	
HTTPS	443	

CANCEL BACK NEXT

VCSA viene installato ora. Questo processo richiede alcuni minuti.

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



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

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

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

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

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

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

21. Viene visualizzato un messaggio che indica che non sarà possibile sospendere o interrompere il completamento dell'installazione dopo l'avvio. Fare clic su OK per continuare.

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

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

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

["Configurazione del clustering di VMware vCenter Server 6.7 e vSphere."](#)

Configurare il clustering di VMware vCenter Server 6.7 e vSphere

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

seguente procedura:

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

Creare il cluster vSphere

Per creare un cluster vSphere, attenersi alla seguente procedura:

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

New Cluster

FlexPod

✕

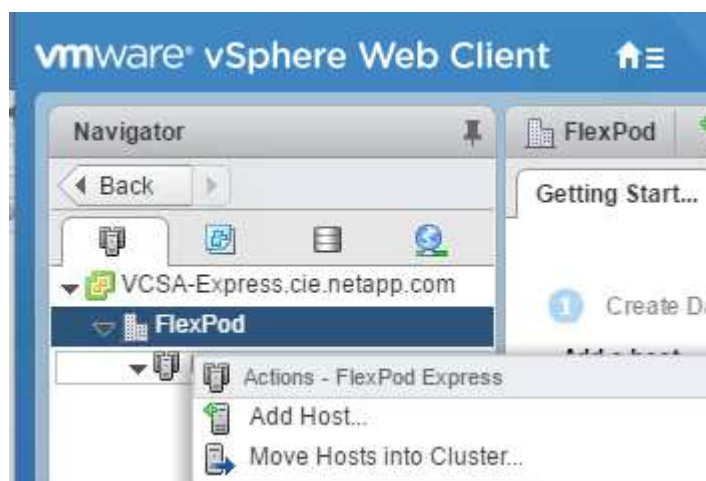
Name	Tiger3
Location	FlexPod
> DRS	<input checked="" type="checkbox"/> Turn ON
> vSphere HA	<input checked="" type="checkbox"/> Turn ON
> EVC	Disable

CANCEL

OK

Aggiungere host ESXi al cluster

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



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



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

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

Configurare il coredump sugli host ESXi

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

```
esxcli system coredump network set -i ip_address_of_core_dump_collector  
-v vmk0 -o 6500  
esxcli system coredump network set --enable=true  
esxcli system coredump network check
```

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

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

Conclusione

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 aggiuntivi, FlexPod può essere personalizzato in base alle specifiche esigenze aziendali. FlexPod Express è stato progettato tenendo conto delle piccole e medie imprese, delle ROBOs e di altre aziende che richiedono soluzioni dedicate.

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)

- Guida alla progettazione di FlexPod Express con VMware vSphere 6.7 e NetApp AFF A220

["https://www.netapp.com/us/media/nva-1125-design.pdf"](https://www.netapp.com/us/media/nva-1125-design.pdf)

FlexPod Express con VMware vSphere 6.7U1 e NetApp AFF A220 con storage basato su IP direct-attached

NVA-1131-DEPLOY: FlexPod Express con VMware vSphere 6.7U1 e NetApp AFF A220 con storage basato su IP direct-attached

SREE Lakshmi Lanka, NetApp

Le tendenze del settore indicano una vasta 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, sfruttando la tecnologia con cui hanno familiarità nel proprio data center.

FlexPod è un'architettura pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco, sulla famiglia di switch Cisco Nexus e sulle tecnologie 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 la versatilità 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 possono facilmente adattarsi 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 (ROBOS) 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

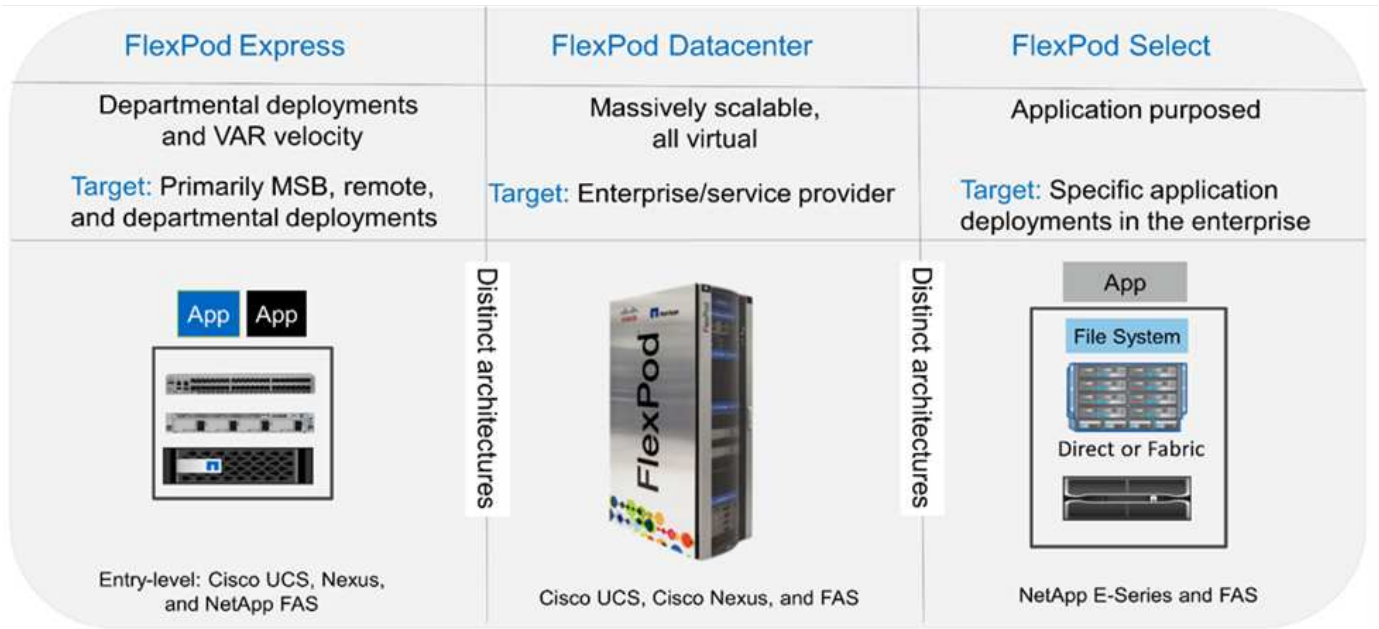
Le architetture di riferimento FlexPod vengono fornite come Cisco Validated Design (CVD) o NetApp Verified Architectures (NVA). Sono consentite deviazioni in base ai requisiti del cliente rispetto a un determinato CVD o NVA se queste variazioni non creano una configurazione non supportata.

Come illustrato nella figura seguente, il programma FlexPod include tre soluzioni: FlexPod Express, FlexPod

Datacenter e FlexPod Select:

- **FlexPod** 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.
- **FlexPod Select** incorpora gli aspetti migliori del data center FlexPod e adatta l'infrastruttura a una determinata applicazione.

La figura seguente mostra i componenti tecnici della soluzione.



Programma NetApp Verified Architecture

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

- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione
- Accelera il time-to-market

In questa guida viene illustrato in dettaglio il design di FlexPod Express con storage NetApp direct-attached. Le sezioni seguenti elencano i componenti utilizzati per la progettazione di questa soluzione.

Componenti hardware

- NetApp AFF A220
- Cisco UCS Mini
- CISCO UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Switch Cisco Nexus serie 3000

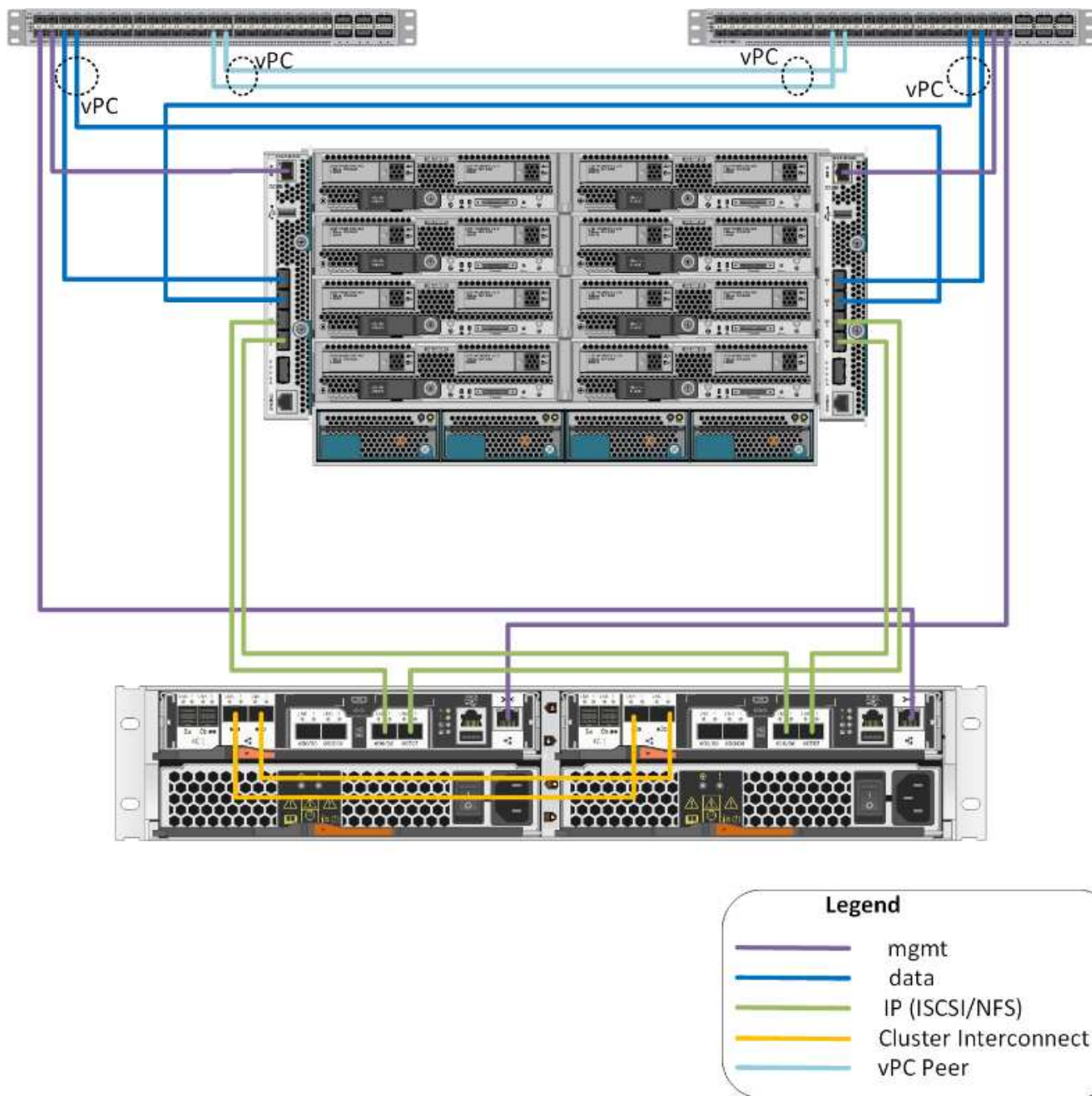
Componenti software

- NetApp ONTAP 9. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4.0(1b)
- Firmware Cisco NXOS 7.0(3)I6(1)

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. Include il nuovo NetApp AFF A220 con ONTAP 9.5, due switch Cisco Nexus 31108PCV e server Cisco UCS B200 M5 con VMware vSphere 6.7U1. Questa soluzione validata utilizza lo storage IP Direct Connect su tecnologia 10 GbE.

La figura seguente illustra FlexPod Express con architettura di connessione diretta basata su IP VMware vSphere 6.7U1.



Riepilogo del caso d'utilizzo

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

- Robot
- 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.

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, entrambi gli hypervisor possono essere eseguiti sullo stesso hardware FlexPod Express.

La seguente tabella elenca i componenti hardware necessari per tutte le configurazioni FlexPod Express.

Hardware	Quantità
Coppia AFF A220 ha	1
Server Cisco UCS B200 M5	2
Switch Cisco Nexus 31108PCV	2
Cisco UCS Virtual Interface Card (VIC) 1440 per il server Cisco UCS B200 M5	2
Cisco UCS Mini con due interconnessioni fabric UCS-Fi-M-6324 integrate	1

Requisiti software

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

Software	Versione	Dettagli
Cisco UCS Manager	4.0(1b)	Per Cisco UCS Fabric Interconnect Fi-6324UP
Software Cisco Blade	4.0(1b)	Per server Cisco UCS B200 M5
Driver Cisco Nenic	1.0.25.0	Per schede di interfaccia Cisco VIC 1440
Sistema operativo Cisco NX	7.0(3)I6(1)	Per switch Cisco Nexus 31108PCV
NetApp ONTAP	9.5	Per controller AFF A220

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

Software	Versione
Appliance server VMware vCenter	6.7U1
Hypervisor VMware vSphere ESXi	6.7U1

Informazioni di cablaggio rapido FlexPod

Il cablaggio di convalida di riferimento è documentato nelle tabelle seguenti.

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

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 31108PCV A.	Eth1/1	Storage controller NetApp AFF A220 A	E0M
	Eth1/2	Cisco UCS-mini Fi-A.	mgmt0
	Eth1/3	Cisco UCS-mini Fi-A.	Eth1/1
	ETH 1/4	Cisco UCS-mini Fi-B.	Eth1/1
	ETH 1/13	CISCO NX 31108PCV B	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV B	ETH 1/14

La seguente tabella elenca le informazioni di cablaggio per lo switch Cisco Nexus 31108PCV B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch Cisco Nexus 31108PCV B	Eth1/1	Storage controller NetApp AFF A220 B	E0M
	Eth1/2	Cisco UCS-mini Fi-B.	mgmt0
	Eth1/3	Cisco UCS-mini Fi-A.	Eth1/2
	ETH 1/4	Cisco UCS-mini Fi-B.	Eth1/2
	ETH 1/13	CISCO NX 31108PCV A.	ETH 1/13
	ETH 1/14	CISCO NX 31108PCV A.	ETH 1/14

La seguente tabella elenca le informazioni di cablaggio per il controller di storage NetApp AFF A220 A.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Storage controller NetApp AFF A220 A	e0a	Storage controller NetApp AFF A220 B	e0a
	e0b	Storage controller NetApp AFF A220 B	e0b
	e0e	Cisco UCS-mini Fi-A.	Eth1/3
	e0f	Cisco UCS-mini Fi-B.	Eth1/3
	E0M	CISCO NX 31108PCV A.	Eth1/1

La seguente tabella elenca le informazioni di cablaggio per il controller di storage NetApp AFF A220 B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Storage controller NetApp AFF A220 B	e0a	Storage controller NetApp AFF A220 B	e0a
	e0b	Storage controller NetApp AFF A220 B	e0b
	e0e	Cisco UCS-mini Fi-A.	Eth1/4
	e0f	Cisco UCS-mini Fi-B.	Eth1/4
	E0M	CISCO NX 31108PCV B	Eth1/1

La seguente tabella elenca le informazioni di cablaggio per Cisco UCS Fabric Interconnect A.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Cisco UCS Fabric Interconnect A.	Eth1/1	CISCO NX 31108PCV A.	Eth1/3
	Eth1/2	CISCO NX 31108PCV B	Eth1/3
	Eth1/3	Storage controller NetApp AFF A220 A	e0e
	Eth1/4	Storage controller NetApp AFF A220 B	e0e
	mgmt0	CISCO NX 31108PCV A.	Eth1/2

La seguente tabella elenca le informazioni di cablaggio per Cisco UCS Fabric Interconnect B.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Cisco UCS Fabric Interconnect B	Eth1/1	CISCO NX 31108PCV A.	Eth1/4
	Eth1/2	CISCO NX 31108PCV B	Eth1/4
	Eth1/3	Storage controller NetApp AFF A220 A	e0f
	Eth1/4	Storage controller NetApp AFF A220 B	e0f
	mgmt0	CISCO NX 31108PCV B	Eth1/2

Procedure di implementazione

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


Inoltre, questo documento descrive i passaggi per il provisioning di più host Cisco UCS, identificati in sequenza

come server A, server B e così via.

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

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

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



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

Nome VLAN	Scopo della VLAN	ID utilizzato per la convalida di questo documento
VLAN di gestione	VLAN per le interfacce di gestione	18
VLAN nativa	VLAN a cui sono assegnati frame senza tag	2
VLAN NFS	VLAN per traffico NFS	104
VLAN VMware vMotion	VLAN designata per lo spostamento delle macchine virtuali (VM) da un host fisico all'altro	103
VLAN del traffico delle macchine virtuali	VLAN per il traffico delle applicazioni VM	102
ISCSI-A-VLAN	VLAN per il traffico iSCSI sul fabric A.	124
ISCSI-B-VLAN	VLAN per il traffico iSCSI sul fabric B.	125

I numeri VLAN sono necessari per tutta la configurazione di FlexPod Express. Le VLAN sono indicate come <<var_xxxx_vlan>>, dove `xxxx` È lo scopo della VLAN (ad esempio iSCSI-A).

La tabella seguente elenca le macchine virtuali VMware create.

Descrizione della macchina virtuale	Host Name (Nome host)
VMware vCenter Server	Seahawks-vcsa.cie.netapp.com

Procedura di implementazione di Cisco Nexus 31108PCV

Questa sezione descrive in dettaglio la configurazione dello switch Cisco Nexus 31308PCV utilizzata in un ambiente FlexPod Express.

Configurazione iniziale dello switch Cisco Nexus 31108PCV

Questa procedura descrive 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 31108PCV con la versione software NX-OS 7.0(3)I6(1).

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

3. Per configurare gli switch Cisco Nexus 31108PCV, 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 : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>

```

- 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]: no

```

- 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

```

- Ripetere i passaggi da 1 a 5 per lo switch Cisco Nexus B.

Abilitare le funzionalità avanzate

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

configurazione.

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

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



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

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

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

Eseguire la configurazione spanning-tree globale

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

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

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

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

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

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

Definire le VLAN

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

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

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurare le descrizioni delle porte di accesso e di gestione

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

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

Switch Cisco Nexus A

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Switch Cisco Nexus B

```
int eth1/1
    description AFF A220-B e0M
int eth1/2
    description Cisco UCS FI-B mgmt0
int eth1/3
    description Cisco UCS FI-A eth1/2
int eth1/4
    description Cisco UCS FI-B eth1/2
int eth1/13
    description vPC peer-link 31108PVC-B 1/13
int eth1/14
    description vPC peer-link 31108PVC-B 1/14
```

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`), eseguire i seguenti comandi per configurare le impostazioni delle porte per le interfacce di gestione dei server e dello storage:

Switch Cisco Nexus A

```
int eth1/1-2
    switchport mode access
    switchport access vlan <<mgmt_vlan>>
    spanning-tree port type edge
    speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/1-2
    switchport mode access
    switchport access vlan <<mgmt_vlan>>
    spanning-tree port type edge
    speed 1000
exit
```

Aggiungere l'interfaccia di distribuzione NTP

Switch Cisco Nexus A

Dalla modalità di configurazione globale, eseguire i seguenti comandi.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Switch Cisco Nexus B

Dalla modalità di configurazione globale, eseguire i seguenti comandi.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

Eseguire la configurazione globale del canale della porta virtuale

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

Un VPC offre i seguenti vantaggi:

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

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

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

Switch Cisco Nexus A

```

vpc domain 1
  role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start

```

Switch Cisco Nexus B

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
    peer-gateway
    auto-recovery
    ip arp synchronize
    int eth1/13-14
    channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
    channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
channel-group 14 mode active
copy run start
```



Nella convalida di questa soluzione, è stata utilizzata un'unità di trasmissione massima (MTU) di 9000. Tuttavia, in base ai requisiti dell'applicazione, è possibile configurare un valore appropriato di MTU. È importante impostare lo stesso valore MTU nella soluzione FlexPod. Configurazioni MTU errate tra i componenti causano l'interruzione dei pacchetti.

Uplink nell'infrastruttura di rete esistente

A seconda dell'infrastruttura di rete disponibile, è possibile utilizzare diversi metodi e funzionalità per eseguire l'uplink dell'ambiente FlexPod. Se è presente un ambiente Cisco Nexus esistente, NetApp consiglia di utilizzare VPC per eseguire l'uplink degli switch Cisco Nexus 31108PVC inclusi nell'ambiente FlexPod nell'infrastruttura. Gli uplink possono essere uplink 10 GbE per una soluzione di infrastruttura 10 GbE o 1 GbE per una soluzione di infrastruttura 1 GbE, se necessario. Le procedure descritte in precedenza possono essere utilizzate per creare un VPC uplink nell'ambiente esistente. Assicurarsi di eseguire l'avvio dell'esecuzione della copia per salvare la configurazione su ogni switch dopo il completamento della configurazione.

Procedura di implementazione dello storage NetApp (parte 1)

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

Installazione del controller di storage NetApp serie AFF2xx

NetApp Hardware Universe

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

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

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

Prerequisiti della serie AFF2XX del controller

Per pianificare la posizione fisica dei sistemi storage, consultare le 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 ["Documentazione di AFF A220"](#).

NetApp ONTAP 9.5

Foglio di lavoro per la configurazione

Prima di eseguire lo script di installazione, completare il foglio di lavoro di configurazione contenuto nel manuale del prodotto. Il foglio di lavoro di configurazione è disponibile in "[Guida alla configurazione del software ONTAP 9.5](#)" (disponibile in "[Centro documentazione di ONTAP 9](#)"). La tabella seguente illustra le informazioni di installazione e configurazione di ONTAP 9.5.



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

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 9.5	[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 DEL SERVER NTP A.	<< switch-a-ntp-ip >>
IP SERVER NTP B.	<< switch-b-ntp-ip >>

Configurare il nodo A.

Per configurare il nodo A, attenersi alla seguente procedura:

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

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

2. Consentire l'avvio del sistema.

```
autoboot
```

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

Se ONTAP 9. 5 non è la versione del software che si sta avviando, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9. 5 è la versione da avviare, selezionare l'opzione 8 e y per riavviare il nodo. Quindi, passare alla fase 14.

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

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

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



Questo server Web deve essere ping-in.

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

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

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

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

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

Configurare il nodo B.

Per configurare il nodo B, attenersi alla seguente procedura:

1. Connettersi alla porta della console del sistema di storage. Viene visualizzato un prompt Loader-A.

Tuttavia, se il sistema di storage si trova in un loop di riavvio, premere Ctrl-C per uscire dal loop di avvio automatico quando viene visualizzato questo messaggio:

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

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

```
autoboot
```

3. Premere Ctrl-C quando richiesto.

Se ONTAP 9.5 non è la versione del software che si sta avviando, continuare con i passi seguenti per installare il nuovo software. Se ONTAP 9.4 è la versione da avviare, selezionare l'opzione 8 e y per riavviare il nodo. Quindi, passare alla fase 14.

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

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

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



Questo server Web deve essere ping-in.

```
<<var_url_boot_software>>
```

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

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

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

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

Configurazione del nodo di continuazione A e 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 9.5 viene avviato sul nodo per la prima volta.

La procedura di configurazione del nodo e del cluster è stata leggermente modificata in ONTAP 9.5. La procedura guidata di installazione del cluster viene ora utilizzata per configurare il primo nodo di un cluster e System Manager viene utilizzato per configurare il cluster.

1. Seguire le istruzioni per 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 utilizzando la configurazione guidata di NetApp System Manager.

3. Fare clic su Guided Setup (Configurazione guidata) per configurare il cluster.
4. Invio `<<var_clustername>>` per il nome del cluster e. `<<var_nodeA>>` e. `<<var_nodeB>>` per ciascuno dei nodi che si sta configurando. Inserire la password che si desidera utilizzare per il sistema di storage. Selezionare Switchless Cluster (Cluster senza switch) per il tipo di cluster. Inserire la licenza di base del cluster.
5. È inoltre possibile inserire licenze delle funzionalità per Cluster, NFS e iSCSI.
6. Viene visualizzato un messaggio di stato che indica che il cluster è in fase di creazione. Questo messaggio di stato passa in rassegna diversi stati. Questo processo richiede alcuni minuti.
7. Configurare la rete.
 - a. Deselezionare l'opzione IP Address Range (intervallo indirizzi IP).
 - b. Invio `<<var_clustermgmt_ip>>` Nel campo Cluster Management IP Address (Indirizzo IP di gestione cluster), `<<var_clustermgmt_mask>>` Nel campo Netmask, e. `<<var_clustermgmt_gateway>>` Nel campo Gateway. Utilizzare il ... Nel campo Port (porta) per selezionare e0M del nodo A.
 - c. L'IP di gestione dei nodi per il nodo A è già popolato. Invio `<<var_nodeA_mgmt_ip>>` Per il nodo B.
 - d. Invio `<<var_domain_name>>` Nel campo DNS Domain Name (Nome dominio DNS). Invio `<<var_dns_server_ip>>` Nel campo DNS Server IP Address (Indirizzo IP server DNS).

È possibile immettere più indirizzi IP del server DNS.
 - e. Invio `<<switch-a-ntp-ip>>` Nel campo Primary NTP Server (Server NTP primario).

È anche possibile immettere un server NTP alternativo come `<<switch-b-ntp-ip>>`.
8. Configurare le informazioni di supporto.
 - a. Se l'ambiente richiede un proxy per accedere a AutoSupport, inserire l'URL nel campo URL proxy.
 - b. Inserire l'host di posta SMTP e l'indirizzo di posta elettronica per le notifiche degli eventi.

Prima di procedere, è necessario impostare almeno il metodo di notifica degli eventi. È possibile selezionare uno dei metodi.
9. Quando viene indicato che la configurazione del cluster è stata completata, fare clic su Manage Your Cluster (Gestisci cluster) per configurare lo storage.

Continuazione della configurazione del cluster di storage

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

Azzerare tutti i dischi spare

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

```
disk zerospares
```

Impostare la personalità delle porte UTA2 a bordo scheda

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

```
AFFA220-Clus::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin Status

AFFA220-Clus-01	0c	cna	target	-	-	offline
AFFA220-Clus-01	0d	cna	target	-	-	offline
AFFA220-Clus-01	0e	cna	target	-	-	offline
AFFA220-Clus-01	0f	cna	target	-	-	offline
AFFA220-Clus-02	0c	cna	target	-	-	offline
AFFA220-Clus-02	0d	cna	target	-	-	offline
AFFA220-Clus-02	0e	cna	target	-	-	offline
AFFA220-Clus-02	0f	cna	target	-	-	offline

8 entries were displayed.

2. Verificare che la modalità corrente delle porte in uso sia `cna` e che il tipo corrente sia impostato su `target`. In caso contrario, modificare la personalità della porta eseguendo 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.

Abilitare il protocollo Cisco Discovery

Per attivare il protocollo Cisco Discovery Protocol (CDP) sui controller di storage NetApp, eseguire il seguente comando:

```
node run -node * options cdpd.enable on
```

Abilitare il protocollo link-Layer Discovery su tutte le porte Ethernet

Attivare lo scambio di informazioni adiacenti LLDP (link-Layer Discovery Protocol) tra lo switch di storage e di rete eseguendo il seguente comando. Questo comando attiva LLDP su tutte le porte di tutti i nodi del cluster.

```
node run * options lldp.enable on
```

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 A220_A_1 - newname AFF A220-01_mgmt1
```

Impostare il revert automatico sulla gestione del cluster

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

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

Configurare l'interfaccia di rete del Service Processor

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

```
system service-processor network modify -node <<var_nodeA>> -address  
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeA_sp_ip>>  
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>  
system service-processor network modify -node <<var_nodeB>> -address  
-family IPv4 -enable true - dhcp none -ip-address <<var_nodeB_sp_ip>>  
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```



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

Abilitare il failover dello storage in ONTAP

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

1. Verificare lo stato del failover dello storage.

```
storage failover show
```

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

2. Attivare il failover su uno dei due nodi.

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

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



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

```
cluster ha show
```

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

```
High Availability Configured: true
```

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

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

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

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

```
storage failover hwassist show
```

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

```
storage failover modify -hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify -hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Creare un dominio di trasmissione MTU con frame jumbo in ONTAP

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

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Rimuovere le porte dati dal dominio di trasmissione predefinito

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

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

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Disattiva il controllo di flusso sulle porte UTA2

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

```

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

```



La connessione diretta di Cisco UCS Mini a ONTAP non supporta LACP.

Configurare i frame jumbo in NetApp ONTAP

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

```

AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y

```

Create 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 e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>

```

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

```

network port vlan create -node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>

```

3. Creare porte MGMT-VLAN.

```

network port vlan create -node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create -node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>

```

Creare aggregati in ONTAP

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

Per creare aggregati, eseguire i seguenti comandi:

```

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

```

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

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

Impossibile creare l'aggregato fino al completamento dell'azzeramento del disco. Eseguire `aggr show` per visualizzare lo stato di creazione dell'aggregato. Non procedere fino a `aggr1_nodeA` è online.

Configurare il fuso orario in ONTAP

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

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



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

Configurare SNMP in ONTAP

Per configurare SNMP, attenersi alla seguente procedura:

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

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

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

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

Configurare SNMPv1 in ONTAP

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

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



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

Configurare SNMPv3 in ONTAP

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

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

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

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

Configurare HTTPS AutoSupport in ONTAP

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

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

Creare una macchina virtuale per lo storage

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

1. Eseguire `vserver create` comando.

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

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

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

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

```
vserver remove-protocols -vserver Infra-SVM -protocols cifs,ndmp,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 server

Configurare NFSv3 in ONTAP

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

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

Per configurare NFS su SVM, eseguire i seguenti comandi:

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

```
vserver export-policy rule create -vserver Infra-SVM -policyname default
-ruleindex 1 -protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys -rwrule sys -superuser sys -allow-suid falsevserver export-
policy rule create -vserver Infra-SVM -policyname default -ruleindex 2
-protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys -rwrule
sys -superuser sys -allow-suid false
vserver export-policy rule show
```

3. 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 B-Series.

Creare un servizio iSCSI in ONTAP

Per creare il servizio iSCSI, completare la seguente fase:

1. Creare il servizio iSCSI sulla SVM. Questo comando avvia anche il servizio iSCSI e imposta il nome qualificato iSCSI (IQN) 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 DPvolume 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 di dominio completo DNS (FQDN) 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 completamente per selezionare ed eliminare ogni certificato predefinito.

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

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

```
security certificate create [TAB] ...  
Example: security certificate create -common-name infra-svm.netapp.com  
-type server -size 2048 - country US -state "North Carolina" -locality  
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr  
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256  
-vserver Infra-SVM
```

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

```
security ssl modify [TAB] ...  
Example: security ssl modify -vserver Infra-SVM -server-enabled true  
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common  
-name infra-svm.netapp.com
```

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

```
system services web modify -external true -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 a SVM di essere disponibile sul web.

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

Creare un volume NetApp FlexVol in ONTAP

Per creare un volume NetApp FlexVol®, immettere il nome, 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_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Attiva la deduplica in ONTAP

Per attivare la deduplica sui volumi appropriati una volta al giorno, eseguire i seguenti comandi:

```

volume efficiency modify -vserver Infra-SVM -volume esxi_boot -schedule
sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_1
-schedule sun-sat@0
volume efficiency modify -vserver Infra-SVM -volume infra_datastore_2
-schedule sun-sat@0

```

Creare LUN in ONTAP

Per creare due LUN (Logical Unit Number) 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 tabella seguente elenca le informazioni necessarie per completare questa configurazione.

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

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

```

network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> -status-admin up - failover-policy
disabled -firewall-policy data -auto-revert false
network interface show

```

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 a IP	[var_nodeA_nfs_lif_01_a_ip]
Nodo di storage A NFS LIF 01 una maschera di rete	[var_nodeA_nfs_lif_01_a_mask]
Nodo di storage A NFS LIF 01 b IP	[var_nodeA_nfs_lif_01_b_ip]
Nodo di storage A NFS LIF 01 b network mask	[var_nodeA_nfs_lif_01_b_mask]
Nodo di storage B NFS LIF 02 a IP	[var_nodeB_nfs_lif_02_a_ip]
Nodo di storage B NFS LIF 02 una maschera di rete	[var_nodeB_nfs_lif_02_a_mask]
Nodo di storage B NFS LIF 02 b IP	[var_nodeB_nfs_lif_02_b_ip]
Nodo di storage B NFS LIF 02 b maschera di rete	[var_nodeB_nfs_lif_02_b_mask]

1. Creare una LIF NFS.


```

network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> -address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up -failover-policy
broadcast-domain-wide - firewall-policy data -auto-revert true
network interface show

```

Aggiungere l'amministratore SVM dell'infrastruttura

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

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

Per aggiungere l'amministratore SVM dell'infrastruttura e la LIF 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 SVM vsadmin 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
```

Configurazione del server Cisco UCS

Base Cisco UCS di FlexPod

Eseguire la configurazione iniziale di Cisco UCS 6324 Fabric Interconnect per ambienti FlexPod.

Questa sezione fornisce procedure dettagliate per configurare Cisco UCS per l'utilizzo in un ambiente ROBO FlexPod utilizzando Cisco UCS Manager.

Cisco UCS Fabric Interconnect 6324 A.

Cisco UCS utilizza server e reti a livello di accesso. Questo sistema server di nuova generazione dalle performance elevate offre un data center con un elevato grado di agilità e scalabilità dei carichi di lavoro.

Cisco UCS Manager 4.0(1b) supporta 6324 Fabric Interconnect che integra Fabric Interconnect nello chassis Cisco UCS e fornisce una soluzione integrata per un ambiente di implementazione più piccolo. Cisco UCS Mini semplifica la gestione del sistema e consente di risparmiare sui costi per le implementazioni su larga scala.

I componenti hardware e software supportano l'Unified Fabric di Cisco, che esegue diversi tipi di traffico del data center su un singolo adattatore di rete convergente.

Configurazione iniziale del sistema

La prima volta che si accede a un'interconnessione fabric in un dominio Cisco UCS, una procedura guidata di installazione richiede le seguenti informazioni necessarie per configurare il sistema:

- Metodo di installazione (GUI o CLI)
- Setup mode (modalità di installazione) (ripristino da backup completo del sistema o configurazione iniziale)
- Tipo di configurazione del sistema (configurazione standalone o cluster)
- Nome del sistema
- Password amministratore

- Indirizzo IPv4 della porta di gestione e subnet mask oppure indirizzo e prefisso IPv6
- Indirizzo IPv4 o IPv6 del gateway predefinito
- Indirizzo IPv4 o IPv6 del server DNS
- Nome di dominio predefinito

La seguente tabella elenca le informazioni necessarie per completare la configurazione iniziale di Cisco UCS su Fabric Interconnect A.

Dettaglio	Dettaglio/valore
System Name (Nome sistema)	[var_ucs_clustername]
Admin Password (Password amministratore)	[var_password]
Management IP Address (Indirizzo IP di gestione): Fabric Interconnect A	[var_ucsa_mgmt_ip]
Netmask di gestione: Fabric Interconnect A	[var_ucsa_mgmt_mask]
Gateway predefinito: Fabric Interconnect A.	[var_ucsa_mgmt_gateway]
Indirizzo IP del cluster	[var_ucs_cluster_ip]
Indirizzo IP del server DNS	[var_nameserver_ip]
Nome di dominio	[var_domain_name]

Per configurare Cisco UCS per l'utilizzo in un ambiente FlexPod, attenersi alla seguente procedura:

1. Connettersi alla porta console del primo Cisco UCS 6324 Fabric Interconnect A.

Enter the configuration method. (console/gui) ? console

Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

Enforce strong password? (y/n) [y]: Enter

Enter the password for "admin":<<var_password>>
Confirm the password for "admin":<<var_password>>

Is this Fabric interconnect part of a cluster(select 'no' for standalone)? (yes/no) [n]: yes

Enter the switch fabric (A/B) []: A

Enter the system name: <<var_ucs_clustername>>

Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

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

Cluster IPv4 address : <<var_ucs_cluster_ip>>

Configure the DNS Server IP address? (yes/no) [n]: y

DNS IP address : <<var_nameserver_ip>>

Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

Join centralized management environment (UCS Central)? (yes/no) [n]:
no

NOTE: Cluster IP will be configured only after both Fabric Interconnects are initialized. UCSM will be functional only after peer FI is configured in clustering mode.

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

Applying configuration. Please wait.

Configuration file - Ok

2. Esaminare le impostazioni visualizzate sulla console. Se sono corretti, rispondi `yes` per applicare e salvare la configurazione.
3. Attendere la richiesta di accesso per verificare che la configurazione sia stata salvata.

La seguente tabella elenca le informazioni necessarie per completare la configurazione iniziale di Cisco UCS su Fabric Interconnect B.

Dettaglio	Dettaglio/valore
System Name (Nome sistema)	[var_ucs_clustername]
Admin Password (Password amministratore)	[var_password]
Management IP Address-Fi B (Indirizzo IP di gestione)	[var_ucsb_mgmt_ip]
Gestione Netmask-Fi B	[var_ucsb_mgmt_mask]
Gateway-Fi B predefinito	[var_ucsb_mgmt_gateway]
Indirizzo IP del cluster	[var_ucs_cluster_ip]
Indirizzo IP del server DNS	[var_nameserver_ip]
Domain Name (Nome dominio)	[var_domain_name]

1. Connettersi alla porta console del secondo Cisco UCS 6324 Fabric Interconnect B.

```

Enter the configuration method. (console/gui) ? console

Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

Enter the admin password of the peer Fabric
interconnect:<<var_password>>
Connecting to peer Fabric interconnect... done
Retrieving config from peer Fabric interconnect... done
Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
Cluster IPv4 address: <<var_ucs_cluster_address>>

Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>

Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
Applying configuration. Please wait.

Configuration file - Ok

```

2. Attendere la richiesta di accesso per confermare che la configurazione è stata salvata.

Accedere a Cisco UCS Manager

Per accedere all'ambiente Cisco Unified Computing System (UCS), attenersi alla seguente procedura:

1. Aprire un browser Web e accedere all'indirizzo del cluster Cisco UCS Fabric Interconnect.

Potrebbe essere necessario attendere almeno 5 minuti dopo aver configurato la seconda interconnessione fabric per Cisco UCS Manager.

2. Fare clic sul collegamento Launch UCS Manager (Avvia UCS Manager) per avviare Cisco UCS Manager.
3. Accettare i certificati di sicurezza necessari.
4. Quando richiesto, immettere admin come nome utente e la password dell'amministratore.
5. Fare clic su Login (accesso) per accedere a Cisco UCS Manager.

Software Cisco UCS Manager versione 4.0(1b)

Il presente documento presuppone l'utilizzo del software Cisco UCS Manager versione 4.0(1b). Per aggiornare il software Cisco UCS Manager e il software Cisco UCS 6324 Fabric Interconnect, fare riferimento a. ["Guide all'installazione e all'aggiornamento di Cisco UCS Manager."](#)

Configurare Cisco UCS Call Home

Cisco consiglia vivamente di configurare Call Home in Cisco UCS Manager. La configurazione di Call Home accelera la risoluzione dei casi di supporto. Per configurare Call Home, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Admin (Amministratore) a sinistra.
2. Selezionare tutti > Gestione comunicazioni > Chiama casa.
3. Impostare lo stato su on.
4. Compilare tutti i campi in base alle preferenze di gestione, quindi fare clic su Save Changes (Salva modifiche) e su OK per completare la configurazione di Call Home.

Aggiunta di un blocco di indirizzi IP per l'accesso a tastiera, video e mouse

Per creare un blocco di indirizzi IP per l'accesso a tastiera, video e mouse (KVM) nel server in banda nell'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Espandere Pools > root > IP Pools.
3. Fare clic con il pulsante destro del mouse su IP Pool ext-mgmt e selezionare Create Block of IPv4 Addresses (Crea blocco di indirizzi IPv4).
4. Inserire l'indirizzo IP iniziale del blocco, il numero di indirizzi IP richiesti e le informazioni relative alla subnet mask e al gateway.

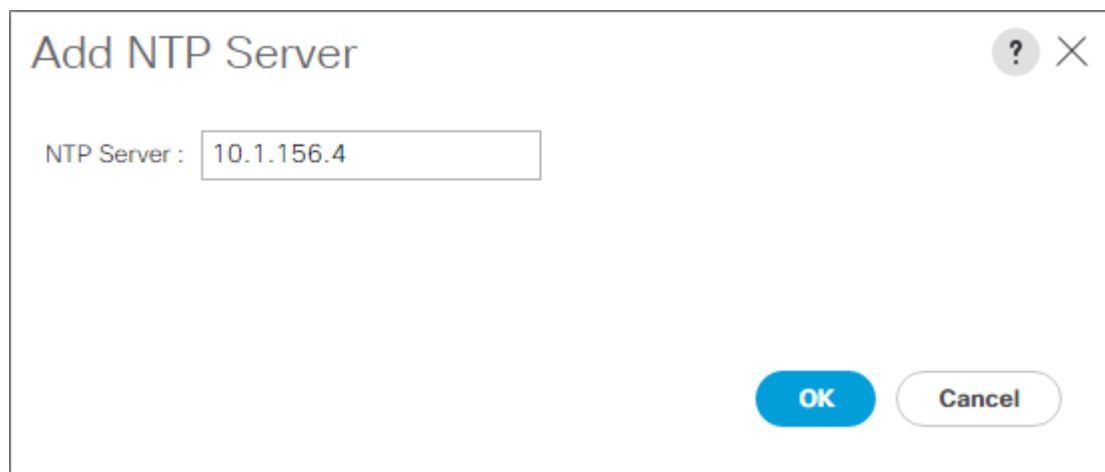
The screenshot shows a dialog box titled "Create Block of IPv4 Addresses". It has a question mark icon and a close button (X) in the top right corner. The dialog contains two columns of input fields. The left column has "From" (192.168.156.101), "Subnet Mask" (255.255.255.0), and "Primary DNS" (0.0.0.0). The right column has "Size" (12), "Default Gateway" (192.168.156.1), and "Secondary DNS" (0.0.0.0). At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).

5. Fare clic su OK per creare il blocco.
6. Fare clic su OK nel messaggio di conferma.

Sincronizzare Cisco UCS con NTP

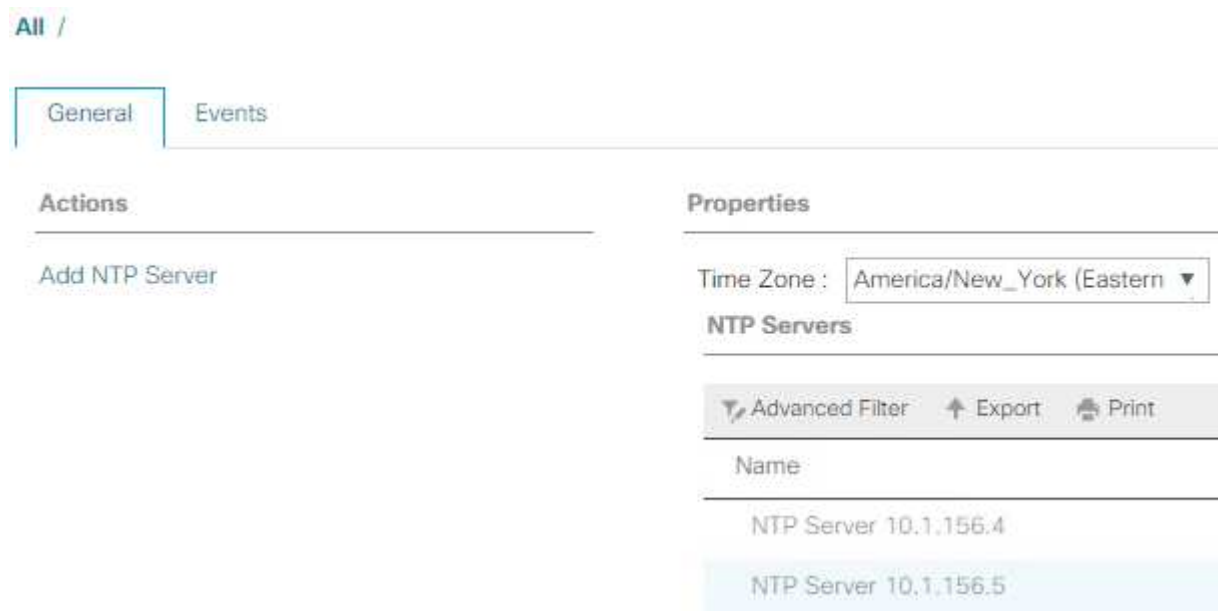
Per sincronizzare l'ambiente Cisco UCS con i server NTP negli switch Nexus, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Admin (Amministratore) a sinistra.
2. Espandere tutti > Gestione fuso orario.
3. Selezionare fuso orario.
4. Nel riquadro Proprietà, selezionare il fuso orario appropriato nel menu fuso orario.
5. Fare clic su Save Changes (Salva modifiche) e su OK.
6. Fare clic su Aggiungi server NTP.
7. Invio <switch-a-ntp-ip> or <Nexus-A-mgmt-IP> E fare clic su OK. Fare clic su OK.



The image shows a dialog box titled "Add NTP Server". It has a close button (X) and a help button (?) in the top right corner. Inside the dialog, there is a label "NTP Server :" followed by a text input field containing the IP address "10.1.156.4". At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white with a grey border).

8. Fare clic su Aggiungi server NTP.
9. Invio <switch-b-ntp-ip> or <Nexus-B-mgmt-IP> E fare clic su OK. Fare clic su OK nella conferma.



The image shows the "NTP Servers" configuration page in Cisco UCS Manager. At the top, there is a breadcrumb "All /". Below it, there are two tabs: "General" (selected) and "Events". The page is divided into two main sections: "Actions" and "Properties".

Actions: Contains a single button labeled "Add NTP Server".

Properties: Contains a "Time Zone" dropdown menu set to "America/New_York (Eastern)". Below this is a section titled "NTP Servers" which includes a table of configured servers. Above the table are buttons for "Advanced Filter", "Export", and "Print".

Name
NTP Server 10.1.156.4
NTP Server 10.1.156.5

Modificare la policy di rilevamento dello chassis


L'impostazione della policy di rilevamento semplifica l'aggiunta dello chassis Cisco UCS B-Series e di ulteriori fabric extender per ulteriore connettività Cisco UCS C-Series. Per modificare la policy di rilevamento dello chassis, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Equipment (apparecchiatura) a sinistra e selezionare Equipment (apparecchiatura) nel secondo elenco.
2. Nel riquadro di destra, selezionare la scheda Criteri.
3. In Global Policies (Criteri globali), impostare la policy di rilevamento chassis/FEX in modo che corrisponda al numero minimo di porte di uplink cablate tra lo chassis o i fabric extender (FEX) e le interconnessioni fabric.
4. Impostare la preferenza di raggruppamento dei collegamenti su Port Channel (canale porta). Se l'ambiente da configurare contiene una grande quantità di traffico multicast, impostare Multicast hardware Hash su Enabled (attivato).
5. Fare clic su Salva modifiche.
6. Fare clic su OK.


Abilitare le porte server, uplink e storage

Per abilitare le porte server e uplink, attenersi alla seguente procedura:

1. In Cisco UCS Manager, nel riquadro di navigazione, selezionare la scheda Equipment (strumentazione).
2. Espandere Equipment > Fabric Interconnect > Fabric Interconnect A > Fixed Module.
3. Espandere Porte Ethernet.
4. Selezionare le porte 1 e 2 collegate agli switch Cisco Nexus 31108, fare clic con il pulsante destro del mouse e selezionare Configure as Uplink Port (Configura come porta Uplink).
5. Fare clic su Yes (Sì) per confermare le porte di uplink e fare clic su OK.
6. Selezionare le porte 3 e 4 collegate ai controller di storage NetApp, fare clic con il pulsante destro del mouse e selezionare Configura come porta appliance.
7. Fare clic su Yes (Sì) per confermare le porte dell'appliance.
8. Nella finestra Configure as Appliance Port (Configura come porta appliance), fare clic su OK.
9. Fare clic su OK per confermare.
10. Nel riquadro di sinistra, selezionare Fixed Module (modulo fisso) in Fabric Interconnect A.
11. Nella scheda Porte Ethernet, verificare che le porte siano state configurate correttamente nella colonna ruolo If. Se sulla porta di scalabilità sono stati configurati server C-Series, fare clic su di essi per verificare la connettività della porta.

General Ethernet Ports FC Ports Faults Events									
Advanced Filter Export Print <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Unconfigured <input checked="" type="checkbox"/> Network <input checked="" type="checkbox"/> Server <input checked="" type="checkbox"/> FCoE Uplink <input checked="" type="checkbox"/> Unified Uplink <input checked="" type="checkbox"/> Appliance Storage <input checked="" type="checkbox"/> FCoE Storage <input checked="" type="checkbox"/> Unified Storage <input checked="" type="checkbox"/> Monitor 									
Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
1	0	1	00:DE:FB:30:36:88	Network	Physical	Up	Enabled		
1	0	2	00:DE:FB:30:36:89	Network	Physical	Up	Enabled		
1	0	3	00:DE:FB:30:36:8A	Appliance Storage	Physical	Up	Enabled		
1	0	4	00:DE:FB:30:36:8B	Appliance Storage	Physical	Up	Enabled		
1	5	1	00:DE:FB:30:36:8C	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	2	00:DE:FB:30:36:8D	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	3	00:DE:FB:30:36:8E	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	4	00:DE:FB:30:36:8F	Unconfigured	Physical	Sfp Not Present	Disabled		

12. Espandere Equipment > Fabric Interconnect > Fabric Interconnect B > Fixed Module.
13. Espandere Porte Ethernet.
14. Selezionare le porte Ethernet 1 e 2 collegate agli switch Cisco Nexus 31108, fare clic con il pulsante destro del mouse e selezionare Configura come porta Uplink.
15. Fare clic su Yes (Sì) per confermare le porte di uplink e fare clic su OK.
16. Selezionare le porte 3 e 4 collegate ai controller di storage NetApp, fare clic con il pulsante destro del mouse e selezionare Configura come porta appliance.
17. Fare clic su Yes (Sì) per confermare le porte dell'appliance.
18. Nella finestra Configure as Appliance Port (Configura come porta appliance), fare clic su OK.
19. Fare clic su OK per confermare.
20. Nel riquadro di sinistra, selezionare Fixed Module (modulo fisso) in Fabric Interconnect B.
21. Nella scheda Porte Ethernet, verificare che le porte siano state configurate correttamente nella colonna ruolo If. Se sulla porta di scalabilità sono stati configurati server C-Series, fare clic su di essa per verificare la connettività della porta.

Ethernet Ports									
Advanced Filter Export Print <input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Unconfigured <input checked="" type="checkbox"/> Network <input checked="" type="checkbox"/> Server <input checked="" type="checkbox"/> FCoE Uplink <input checked="" type="checkbox"/> Unified Uplink <input checked="" type="checkbox"/> Appliance Storage <input checked="" type="checkbox"/> FCoE Storage <input checked="" type="checkbox"/> Unified Storage <input checked="" type="checkbox"/> Monitor 									
Slot	Aggr. Port ID	Port ID	MAC	If Role	If Type	Overall Status	Admin State	Peer	
1	0	1	00:DE:FB:30:3A:C8	Network	Physical	Up	Enabled		
1	0	2	00:DE:FB:30:3A:C9	Network	Physical	Up	Enabled		
1	0	3	00:DE:FB:30:3A:CA	Appliance Storage	Physical	Up	Enabled		
1	0	4	00:DE:FB:30:3A:CB	Appliance Storage	Physical	Up	Enabled		
1	5	1	00:DE:FB:30:3A:CC	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	2	00:DE:FB:30:3A:CD	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	3	00:DE:FB:30:3A:CE	Unconfigured	Physical	Sfp Not Present	Disabled		
1	5	4	00:DE:FB:30:3A:CF	Unconfigured	Physical	Sfp Not Present	Disabled		

Creazione di canali di porte uplink per switch Cisco Nexus 31108

Per configurare i canali di porta necessari nell'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, selezionare la scheda LAN nel riquadro di navigazione.



In questa procedura, vengono creati due canali di porta: Uno dal fabric A agli switch Cisco Nexus 31108 e uno dal fabric B agli switch Cisco Nexus 31108. Se si utilizzano switch standard, modificare questa procedura di conseguenza. Se si utilizzano switch 1 Gigabit Ethernet (1 GbE) e SFP GLC-T sulle interconnessioni fabric, le velocità di interfaccia delle porte Ethernet 1/1 e 1/2 nelle interconnessioni fabric devono essere impostate su 1 Gbps.

2. In LAN > LAN Cloud, espandere la struttura Fabric A.
3. Fare clic con il pulsante destro del mouse su canali porta.
4. Selezionare Create Port Channel (Crea canale porta).
5. Inserire 13 come ID univoco del canale della porta.
6. Inserire VPC-13-Nexus come nome del canale della porta.
7. Fare clic su Avanti.

8. Selezionare le seguenti porte da aggiungere al canale della porta:
 - a. ID slot 1 e porta 1
 - b. ID slot 1 e porta 2
9. Fare clic su >> per aggiungere le porte al canale della porta.
10. Fare clic su Finish (fine) per creare il canale della porta. Fare clic su OK.

11. In Port Channels (canali porta), selezionare il canale della porta appena creato.

Il canale della porta deve avere uno stato generale di attivazione.

12. Nel riquadro di navigazione, in LAN > LAN Cloud, espandere la struttura Fabric B.

13. Fare clic con il pulsante destro del mouse su canali porta.

14. Selezionare Create Port Channel (Crea canale porta).

15. Inserire 14 come ID univoco del canale della porta.

16. Inserire VPC-14-Nexus come nome del canale della porta. Fare clic su Avanti.

17. Selezionare le seguenti porte da aggiungere al canale della porta:

a. ID slot 1 e porta 1

b. ID slot 1 e porta 2

18. Fare clic su >> per aggiungere le porte al canale della porta.

19. Fare clic su Finish (fine) per creare il canale della porta. Fare clic su OK.

20. In Port Channels (canali porta), selezionare il canale porta appena creato.

21. Il canale della porta deve avere uno stato generale di attivazione.

Creazione di un'organizzazione (opzionale)

Le organizzazioni vengono utilizzate per organizzare le risorse e limitare l'accesso a diversi gruppi all'interno dell'organizzazione IT, consentendo così la multi-tenancy delle risorse di calcolo.



Sebbene questo documento non preveda l'utilizzo di organizzazioni, questa procedura fornisce istruzioni per crearne una.

Per configurare un'organizzazione nell'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, dal menu New (nuovo) nella barra degli strumenti nella parte superiore della finestra, selezionare Create Organization (Crea organizzazione).
2. Immettere un nome per l'organizzazione.
3. Facoltativo: Inserire una descrizione per l'organizzazione. Fare clic su OK.
4. Fare clic su OK nel messaggio di conferma.

Configurare le porte dell'appliance di storage e le VLAN di storage

Per configurare le porte e le VLAN di storage dell'appliance di storage, attenersi alla seguente procedura:

1. In Cisco UCS Manager, selezionare la scheda LAN.
2. Espandere il cloud Appliances.
3. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.
4. Selezionare Create VLAN (Crea VLAN).
5. Inserire NFS-VLAN come nome della VLAN NFS dell'infrastruttura.
6. Lasciare selezionato Common/Global (comune/globale).
7. Invio <<var_nfs_vlan_id>> Per l'ID VLAN.

8. Lasciare l'opzione Sharing Type (tipo di condivisione) impostata su None

Create VLANs

VLAN Name/Prefix : NFS-VLAN

☒ Common/Global ☐ Fabric A ☐ Fabric B ☐ Both Fabrics Configured Differently

You are creating global VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")

VLAN IDs : 3170

Sharing Type : ☒ None ☐ Primary ☐ Isolated ☐ Community

Check Overlap Ok Cancel

9. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.

10. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.

11. Selezionare Create VLAN (Crea VLAN).

12. Inserire iSCSI-A-VLAN come nome per il fabric iSCSI infrastruttura A VLAN.

13. Lasciare selezionato Common/Global (comune/globale).

14. Invio <<var_iscsi-a_vlan_id>> Per l'ID VLAN.

15. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.

16. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.

17. Selezionare Create VLAN (Crea VLAN).

18. Inserire iSCSI-B-VLAN come nome della VLAN infrastruttura iSCSI Fabric B.

19. Lasciare selezionato Common/Global (comune/globale).

20. Invio <<var_iscsi-b_vlan_id>> Per l'ID VLAN.

21. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.

22. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.
23. Selezionare Create VLAN (Crea VLAN).
24. Inserire la VLAN nativa come nome della VLAN nativa.
25. Lasciare selezionato Common/Global (comune/globale).
26. Invio <<var_native_vlan_id>> Per l'ID VLAN.
27. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.

LAN / LAN Cloud / VLANs

VLANs

Advanced Filter Export Print

Name	ID	Type	Transport	Native	VLAN Sharing	Primary VLAN Name	Multicast Policy Name
VLAN default (1)	1	Lan	Ether	Yes	None		
VLAN 0002-Native (2)	2	Lan	Ether	No	None		
VLAN public (18)	18	Lan	Ether	No	None		
VLAN 0101-IB-MGMT (101)	101	Lan	Ether	No	None		
VLAN 0102-VM (102)	102	Lan	Ether	No	None		
VLAN 0103-vMotion (103)	103	Lan	Ether	No	None		
VLAN 0104-NFS (104)	104	Lan	Ether	No	None		
VLAN 0120-SCSI-A (120)	120	Lan	Ether	No	None		
VLAN 0121-SCSI-B (121)	121	Lan	Ether	No	None		

28. Nel riquadro di navigazione, in LAN > Policy, espandere Appliances e fare clic con il pulsante destro del mouse su Network Control Policies.
29. Selezionare Crea criterio di controllo di rete.
30. Assegnare un nome al criterio Enable_CDP_LLDP E selezionare Enabled (attivato) accanto a CDP.
31. Attivare le funzioni di trasmissione e ricezione per LLDP.

Properties for: Enable_CDP

General Events

Actions

Delete

Show Policy Usage

Use Global

Properties

Name: Enable_CDP

Description:

Owner: Local

CDP: ☐ Disabled ☒ Enabled

MAC Register Mode: ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail: ☒ Link Down ☐ Warning

MAC Security

Forge: ☒ Allow ☐ Deny

LLDP

Transmit: ☐ Disabled ☒ Enabled

Receive: ☐ Disabled ☒ Enabled

OK Cancel Help

32. Fare clic su OK, quindi fare nuovamente clic su OK per creare il criterio.
33. Nel riquadro di navigazione, sotto LAN > Appliances Cloud, espandere la struttura ad albero fabric A.
34. Espandere interfacce.
35. Selezionare Appliance Interface 1/3.
36. Nel campo User Label (etichetta utente), inserire le informazioni che indicano la porta dello storage controller, ad esempio <storage_controller_01_name>:e0e. Fare clic su Save Changes (Salva modifiche) e OK.
37. Selezionare Enable_CDP Network Control Policy (criterio di controllo di rete Enable_CDP), quindi Save Changes (Salva modifiche) e OK.
38. In VLAN, selezionare iSCSI-A-VLAN, NFS VLAN e Native VLAN. Impostare la VLAN nativa come VLAN nativa. Deselezionare la selezione della VLAN predefinita.
39. Fare clic su Save Changes (Salva modifiche) e OK.

LAN / Appliances / Fabric A / Interfaces / Appliance Interface 1/3

General | Ports | Details

Actions

- Create interface
- Disable interface
- Delete interface
- View Ethernet Target Properties
- Remove Ethernet Target Properties

Properties

ID: 3
Slot ID: 1
Fabric ID: A
Aggregated Port ID: 0
User Label: AFA200_Chic_01-e0e
Transceiver Type: Ether
Port: Switched-200G-100Gbps-200Gbps
Admin Speed(gbps): 1 Gbps 10 Gbps 40 Gbps 25 Gbps 100 Gbps Auto
Priority: High
Pin Group: not set
Network Control Policy: Enable_CDP
Flow Control Policy: disable
VLANs

Port Mode: trunk

☒ VLAN default (1)
☒ VLAN iSCSI-A-VLAN (124)
☐ VLAN iSCSI-B-VLAN (125)
☒ VLAN Native-VLAN (2)
☒ VLAN NFS-VLAN (104)
Native VLAN: VLAN Native-VLAN (2)
Disable VLAN

40. Selezionare Appliance Interface 1/4 in Fabric A.
41. Nel campo User Label (etichetta utente), inserire le informazioni che indicano la porta dello storage controller, ad esempio <storage_controller_02_name>:e0e. Fare clic su Save Changes (Salva modifiche) e OK.
42. Selezionare Enable_CDP Network Control Policy (criterio di controllo di rete Enable_CDP), quindi Save Changes (Salva modifiche) e OK.
43. In VLAN, selezionare iSCSI-A-VLAN, NFS VLAN e Native VLAN.
44. Impostare la VLAN nativa come VLAN nativa.
45. Deselezionare la selezione della VLAN predefinita.
46. Fare clic su Save Changes (Salva modifiche) e OK.
47. Nel riquadro di navigazione, sotto LAN > Appliances Cloud, espandere la struttura Fabric B.
48. Espandere interfacce.
49. Selezionare Appliance Interface 1/3.
50. Nel campo User Label (etichetta utente), inserire le informazioni che indicano la porta dello storage

controller, ad esempio <storage_controller_01_name>:e0f. Fare clic su Save Changes (Salva modifiche) e OK.

51. Selezionare Enable_CDP Network Control Policy (criterio di controllo di rete Enable_CDP), quindi Save Changes (Salva modifiche) e OK.
52. In VLAN, selezionare iSCSI-B-VLAN, NFS VLAN e Native VLAN. Impostare la VLAN nativa come VLAN nativa. Deselezionare la VLAN predefinita.

LAN / Appliances / Fabric B / Interfaces / Appliance Interface 1/3

General | Faults | Events

Actions

- Enable Interface
- Disable Interface
- Add Fibre Channel Target Endpoint
- Delete Fibre Channel Target Endpoint

Properties

ID : 3

Slot ID : 1

Fabric ID : B

Aggregated Port ID : 0

User Label : AFFA200_Clus_01:e0f

Transport Type : Ether

Port : sys/switch-B/slot-1/switch-ether/port-3

Admin Speed(gbps) : ☐ 1 Gbps ☒ 10 Gbps ☐ 40 Gbps ☐ 25 Gbps ☐ 100 Gbps ☐ Auto

Priority : Best Effort

Pin Group : <not set>

Network Control Policy : Enable_CDP

Flow Control Policy : default

VLANs

Port Mode : ☒ Trunk ☐ Access

☐ VLAN default (1)

☐ VLAN iSCSI-A-VLAN (124)

☒ VLAN iSCSI-B-VLAN (125)

☒ VLAN Native-VLAN (2)

☒ VLAN NFS_VLAN (104)

Native VLAN : VLAN Native-VLAN (2)

Create VLAN

53. Fare clic su Save Changes (Salva modifiche) e OK.
54. Selezionare Appliance Interface 1/4 in Fabric B.
55. Nel campo User Label (etichetta utente), inserire le informazioni che indicano la porta dello storage controller, ad esempio <storage_controller_02_name>:e0f. Fare clic su Save Changes (Salva modifiche) e OK.
56. Selezionare Enable_CDP Network Control Policy (criterio di controllo di rete Enable_CDP), quindi Save Changes (Salva modifiche) e OK.
57. In VLAN, selezionare iSCSI-B-VLAN, NFS VLAN e Native VLAN. Impostare la VLAN nativa come VLAN nativa. Deselezionare la VLAN predefinita.
58. Fare clic su Save Changes (Salva modifiche) e OK.

Impostare i frame jumbo nel fabric Cisco UCS

Per configurare i frame jumbo e abilitare la qualità del servizio nel fabric Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, nel riquadro di navigazione, fare clic sulla scheda LAN.
2. Selezionare LAN > LAN Cloud > QoS System Class.
3. Nel riquadro di destra, fare clic sulla scheda Generale.

4. Nella riga Best effort, inserire 9216 nella casella sotto la colonna MTU.

Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multicast Optimized
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	9	N/A	normal	<input type="checkbox"/>
Silver	<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	N/A	normal	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	50	9216	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	50	10	N/A

5. Fare clic su Salva modifiche.

6. Fare clic su OK.

Riconoscere lo chassis Cisco UCS

Per riconoscere tutti gli chassis Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, selezionare la scheda Equipment (apparecchiatura), quindi espandere la scheda Equipment (apparecchiatura) a destra.
2. Espandere Equipment > chassis.
3. In Actions for chassis 1 (azioni per chassis 1), selezionare Acknowledge chassis (Conferma chassis).
4. Fare clic su OK, quindi su OK per completare la conferma dello chassis.
5. Fare clic su Chiudi per chiudere la finestra Proprietà.

Caricare le immagini del firmware Cisco UCS 4.0(1b)

Per aggiornare il software Cisco UCS Manager e Cisco UCS Fabric Interconnect alla versione 4.0(1b), fare riferimento a. ["Guide all'installazione e all'aggiornamento di Cisco UCS Manager"](#).

Creare un pacchetto firmware host

I criteri di gestione del firmware consentono all'amministratore di selezionare i pacchetti corrispondenti per una determinata configurazione del server. Queste policy spesso includono pacchetti per schede di rete, BIOS, controller della scheda, adattatori FC, host bus adapter (HBA) Option ROM e proprietà dello storage controller.

Per creare una policy di gestione del firmware per una data configurazione del server nell'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Espandere host firmware Packages (pacchetti firmware host).
4. Selezionare default (predefinito).
5. Nel riquadro delle azioni, selezionare Modify Package Versions (Modifica versioni pacchetto).

6. Selezionare la versione 4.0(1b) per entrambi i pacchetti blade.

Modify Package Versions

Blade Package : 4.0(1b)B

Rack Package : <not set>

Service Pack :

The images from Service Pack will take precedence over the images from Blade or Rack Package

Excluded Components:

- ☐ Adapter
- ☐ BIOS
- ☐ Board Controller
- ☐ CIMC
- ☐ FC Adapters
- ☐ Flex Flash Controller
- ☐ GPUs
- ☐ HBA Option ROM
- ☐ Host NIC
- ☐ Host NIC Option ROM
- ☒ Local Disk
- ☐ NVME Mswitch Firmware
- ☐ PSU
- ☐ SAS Expander

OK Apply Cancel Help

7. Fare clic su OK, quindi di nuovo su OK per modificare il pacchetto firmware dell'host.

Creare pool di indirizzi MAC

Per configurare i pool di indirizzi MAC necessari per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Pools > root.

In questa procedura vengono creati due pool di indirizzi MAC, uno per ciascun fabric di switching.

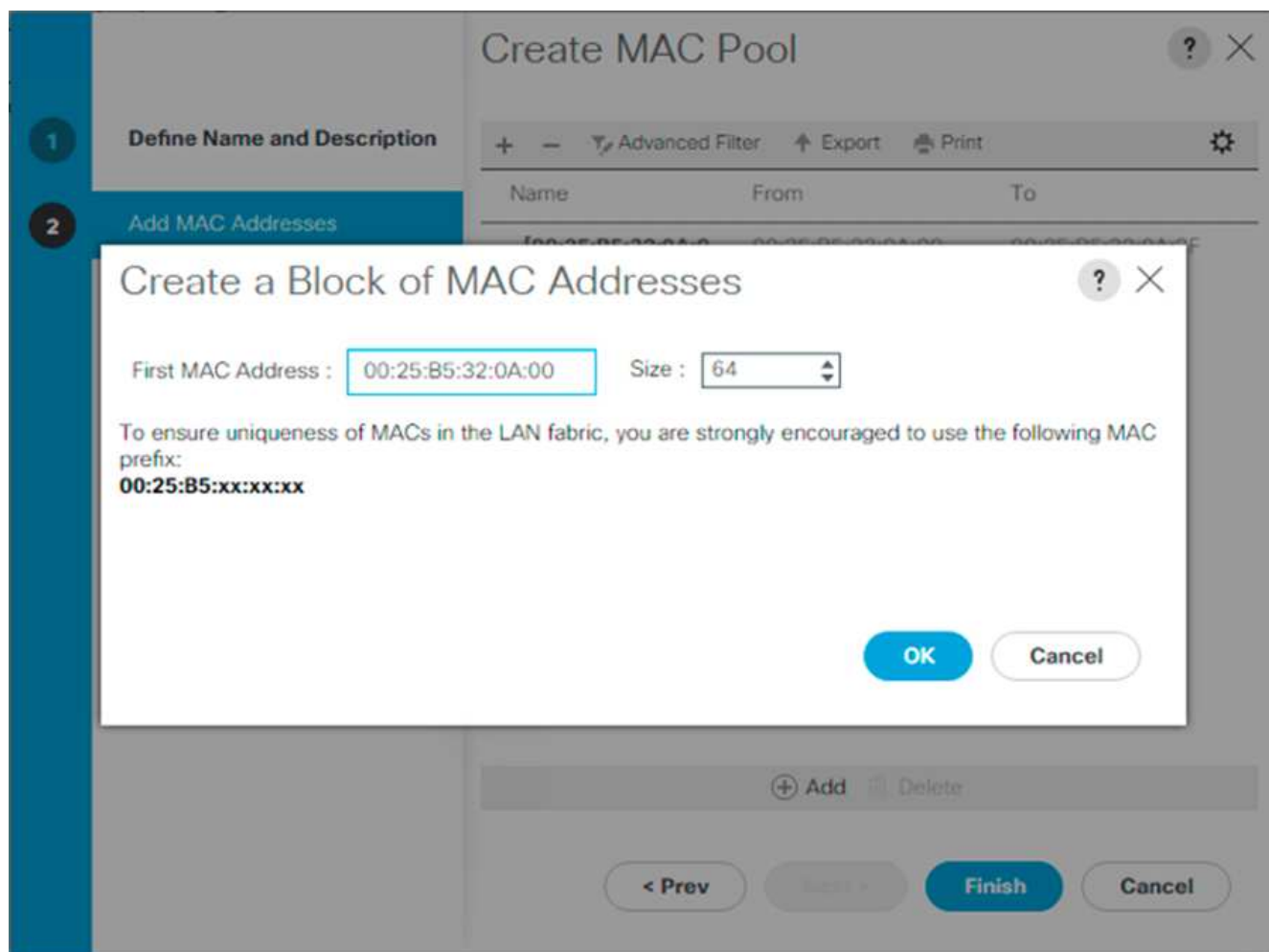
3. Fare clic con il pulsante destro del mouse su MAC Pools sotto l'organizzazione root.
4. Selezionare Create MAC Pool (Crea pool MAC) per creare il pool di indirizzi MAC.
5. Immettere MAC-Pool-A come nome del pool MAC.
6. Facoltativo: Inserire una descrizione per il pool MAC.
7. Selezionare Sequential (sequenziale) come opzione per Assignment Order (Ordine di assegnazione). Fare clic su Avanti.
8. Fare clic su Aggiungi.

9. Specificare un indirizzo MAC iniziale.



Per la soluzione FlexPod, si consiglia di inserire 0A nell'ottetto successivo all'ultimo dell'indirizzo MAC iniziale per identificare tutti gli indirizzi MAC come indirizzi fabric A. Nel nostro esempio, abbiamo portato avanti l'esempio di incorporare anche le informazioni sul numero di dominio Cisco UCS, fornendoci 00:25:B5:32:0A:00 come primo indirizzo MAC.

10. Specificare una dimensione per il pool di indirizzi MAC sufficiente a supportare le risorse blade o server disponibili. Fare clic su OK.



11. Fare clic su fine.

12. Nel messaggio di conferma, fare clic su OK.

13. Fare clic con il pulsante destro del mouse su MAC Pools sotto l'organizzazione root.

14. Selezionare Create MAC Pool (Crea pool MAC) per creare il pool di indirizzi MAC.

15. Inserire MAC-Pool-B come nome del pool MAC.

16. Facoltativo: Inserire una descrizione per il pool MAC.

17. Selezionare Sequential (sequenziale) come opzione per Assignment Order (Ordine di assegnazione). Fare clic su Avanti.

18. Fare clic su Aggiungi.

19. Specificare un indirizzo MAC iniziale.



Per la soluzione FlexPod, si consiglia di inserire 0B nell'ottetto successivo all'ultimo dell'indirizzo MAC iniziale per identificare tutti gli indirizzi MAC di questo pool come indirizzi fabric B. Ancora una volta, abbiamo fatto un esempio di integrazione delle informazioni sul numero di dominio Cisco UCS, che ci hanno fornito 00:25:B5:32:0B:00 come primo indirizzo MAC.

20. Specificare una dimensione per il pool di indirizzi MAC sufficiente a supportare le risorse blade o server disponibili. Fare clic su OK.
21. Fare clic su fine.
22. Nel messaggio di conferma, fare clic su OK.

Creare un pool IQN iSCSI

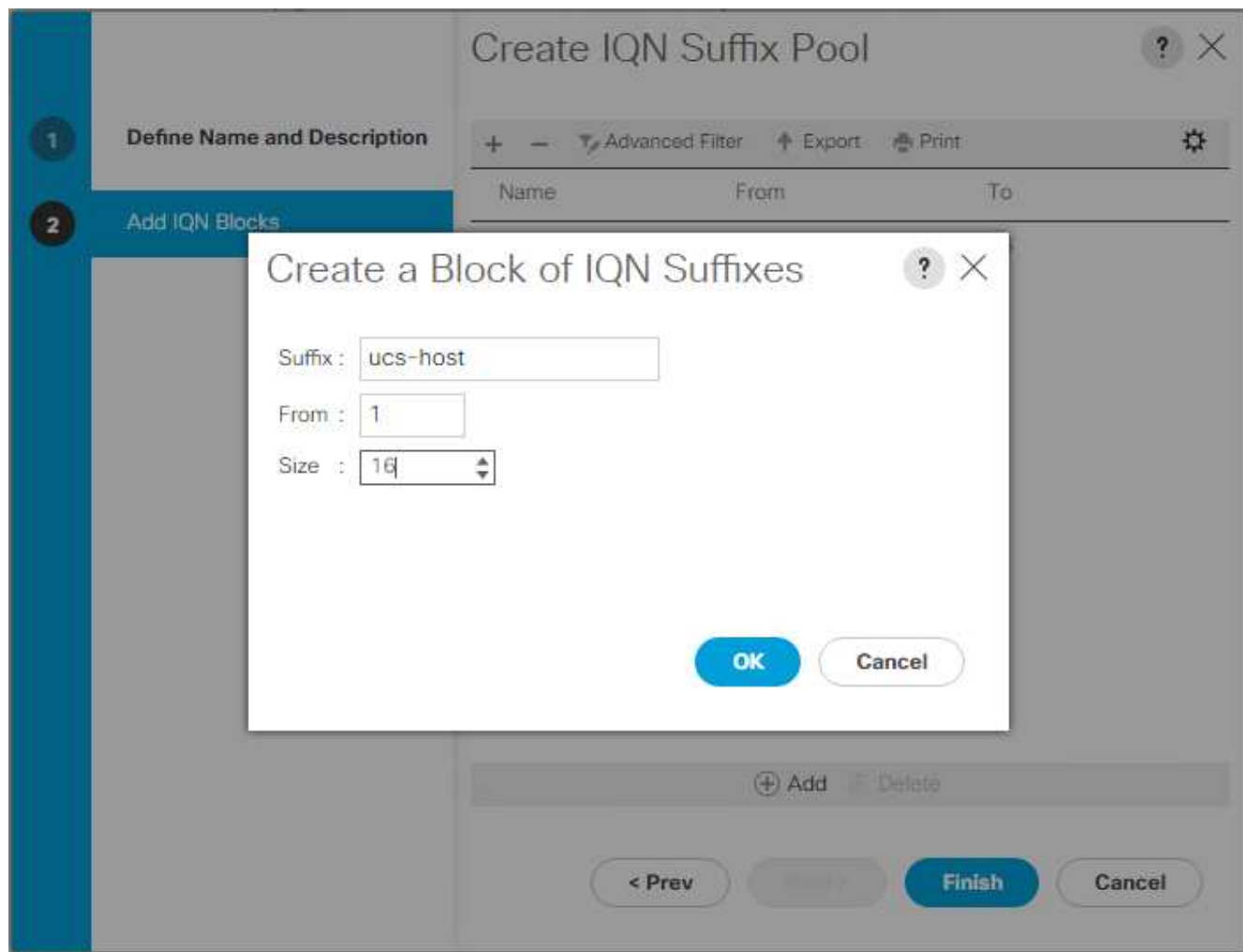
Per configurare i pool IQN necessari per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su SAN a sinistra.
2. Selezionare Pools > root.
3. Fare clic con il pulsante destro del mouse su IQN Pools.
4. Selezionare Create IQN Suffix Pool (Crea pool di suffissi IQN) per creare il pool IQN.
5. Immettere IQN-Pool come nome del pool IQN.
6. Facoltativo: Inserire una descrizione per il pool IQN.
7. Invio `iqn.1992-08.com.cisco` come prefisso.
8. Selezionare sequenziale per Ordine di assegnazione. Fare clic su Avanti.
9. Fare clic su Aggiungi.
10. Invio `ucs-host` come suffisso.



Se si utilizzano più domini Cisco UCS, potrebbe essere necessario utilizzare un suffisso IQN più specifico.

11. Immettere 1 nel campo da.
12. Specificare la dimensione del blocco IQN sufficiente per supportare le risorse server disponibili. Fare clic su OK.



13. Fare clic su fine.

Creare pool di indirizzi IP iSCSI Initiator

Per configurare l'avvio iSCSI dei pool IP necessari per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Pools > root.
3. Fare clic con il pulsante destro del mouse su IP Pools.
4. Selezionare Create IP Pool (Crea pool IP).
5. Immettere iSCSI-IP-Pool-A come nome del pool IP.
6. Facoltativo: Inserire una descrizione per il pool IP.
7. Selezionare Sequential (sequenziale) per l'ordine di assegnazione. Fare clic su Avanti.
8. Fare clic su Add (Aggiungi) per aggiungere un blocco di indirizzi IP.
9. Nel campo From (da), immettere l'inizio dell'intervallo da assegnare come indirizzi IP iSCSI.
10. Impostare la dimensione su un numero di indirizzi sufficiente per ospitare i server. Fare clic su OK.
11. Fare clic su Avanti.
12. Fare clic su fine.

13. Fare clic con il pulsante destro del mouse su IP Pools.
14. Selezionare Create IP Pool (Crea pool IP).
15. Inserire iSCSI-IP-Pool-B come nome del pool IP.
16. Facoltativo: Inserire una descrizione per il pool IP.
17. Selezionare Sequential (sequenziale) per l'ordine di assegnazione. Fare clic su Avanti.
18. Fare clic su Add (Aggiungi) per aggiungere un blocco di indirizzi IP.
19. Nel campo From (da), immettere l'inizio dell'intervallo da assegnare come indirizzi IP iSCSI.
20. Impostare la dimensione su un numero di indirizzi sufficiente per ospitare i server. Fare clic su OK.
21. Fare clic su Avanti.
22. Fare clic su fine.

Creare un pool di suffissi UUID

Per configurare il necessario pool di suffissi UUID (Universally Unique Identifier) per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Pools > root.
3. Fare clic con il pulsante destro del mouse su UUID Suffix Pools.
4. Selezionare Create UUID Suffix Pool (Crea pool di suffissi UUID).
5. Inserire UUID-Pool come nome del pool di suffissi UUID.
6. Facoltativo: Inserire una descrizione per il pool di suffissi UUID.
7. Mantenere il prefisso sull'opzione derivata.
8. Selezionare Sequential (sequenziale) per l'ordine di assegnazione.
9. Fare clic su Avanti.
10. Fare clic su Add (Aggiungi) per aggiungere un blocco di UUID.
11. Mantenere il campo da all'impostazione predefinita.
12. Specificare una dimensione per il blocco UUID sufficiente a supportare le risorse server o blade disponibili.
Fare clic su OK.
13. Fare clic su fine.
14. Fare clic su OK.

Creare un pool di server

Per configurare il pool di server necessario per l'ambiente Cisco UCS, attenersi alla seguente procedura:



Si consiglia di creare pool di server univoci per ottenere la granularità necessaria nel proprio ambiente.

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Pools > root.
3. Fare clic con il pulsante destro del mouse su Server Pools.

4. Selezionare Crea pool di server.
5. Immettere `Infra-Pool` come nome del pool di server.
6. Facoltativo: Inserire una descrizione per il pool di server. Fare clic su Avanti.
7. Selezionare due (o più) server da utilizzare per il cluster di gestione VMware e fare clic su >> per aggiungerli al pool di server `Infra-Pool`.
8. Fare clic su fine.
9. Fare clic su OK.

Creare Network Control Policy per Cisco Discovery Protocol e link Layer Discovery Protocol

Per creare un Network Control Policy per Cisco Discovery Protocol (CDP) e link Layer Discovery Protocol (LLDP), attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Criteri di controllo di rete.
4. Selezionare Crea criterio di controllo di rete.
5. Immettere il nome del criterio Enable-CDP-LLDP.
6. Per CDP, selezionare l'opzione Enabled (attivato).
7. Per LLDP, scorrere verso il basso e selezionare Enabled (attivato) per Transmit (trasmissione) e Receive (ricezione).
8. Fare clic su OK per creare il criterio di controllo di rete. Fare clic su OK.

Create Network Control Policy

CDP : ☐ Disabled ☒ Enabled

MAC Register Mode : ☒ Only Native Vlan ☐ All Host Vlans

Action on Uplink Fail : ☒ Link Down ☐ Warning

MAC Security

Forge : ☒ Allow ☐ Deny

LLDP

Transmit : ☐ Disabled ☒ Enabled

Receive : ☐ Disabled ☒ Enabled

OK **Cancel**

Creare una policy per il controllo del risparmio di energia

Per creare una policy di controllo dell'alimentazione per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic sulla scheda Server a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Power Control Policies.
4. Selezionare Create Power Control Policy (Crea policy di controllo del risparmio di
5. Inserire No-Power-Cap come nome del criterio di controllo dell'alimentazione.
6. Impostare il limite di alimentazione su No Cap.
7. Fare clic su OK per creare il criterio di controllo del risparmio di energia. Fare clic su OK.

Create Power Control Policy ? X

Name :

Description :

Fan Speed Policy :

Power Capping

If you choose **cap**, the server is allocated a certain amount of power based on its priority within its power group. Priority values range from 1 to 10, with 1 being the highest priority. If you choose **no-cap**, the server is exempt from all power capping.

☒ No Cap ☐ cap

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.

OK Cancel

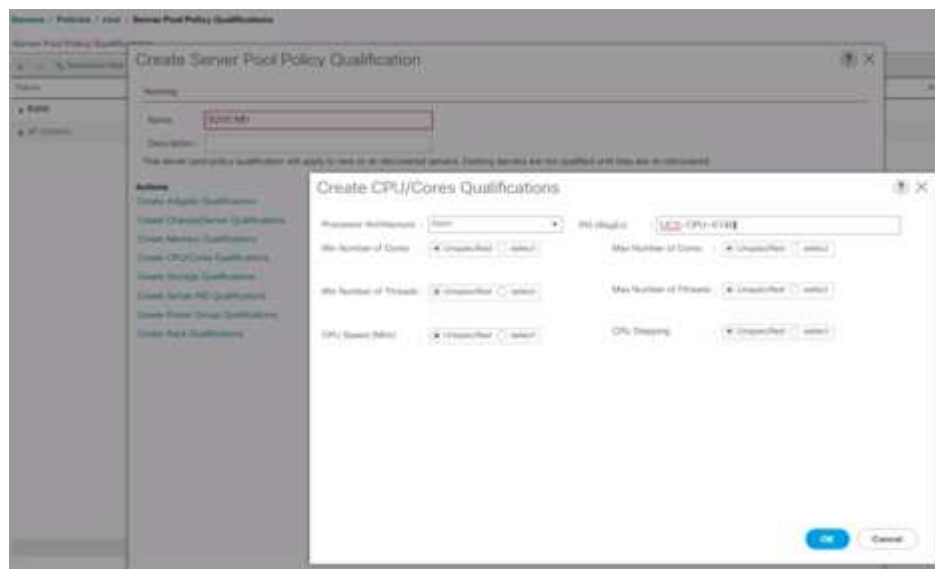
Crea policy di qualificazione del pool di server (opzionale)

Per creare un criterio di qualificazione del pool di server opzionale per l'ambiente Cisco UCS, attenersi alla seguente procedura:



In questo esempio viene creata una policy per i server Cisco UCS B-Series con processori Intel E2660 v4 Xeon Broadwell.

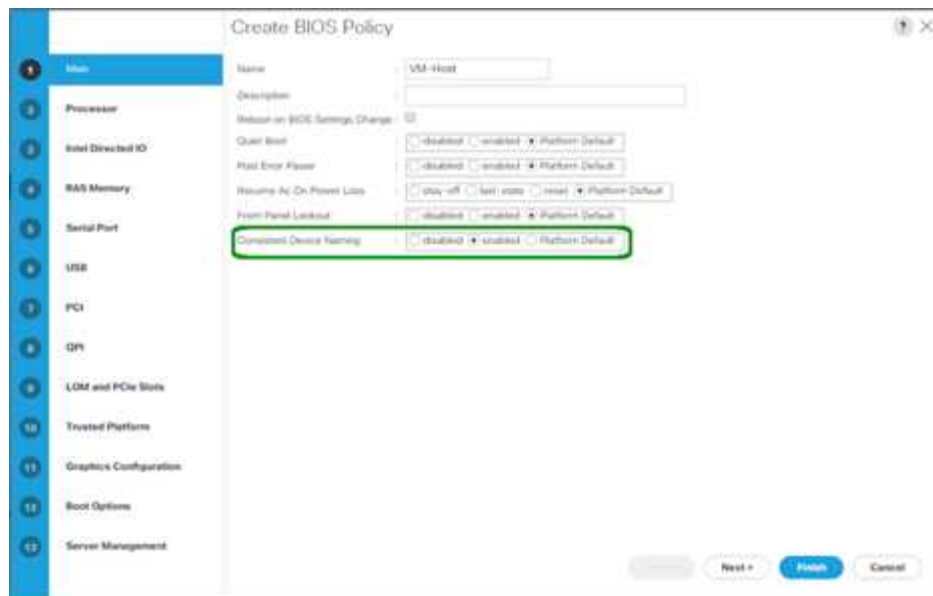
1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Selezionare Server Pool Policy Qualifications (Criteri policy pool server).
4. Selezionare Create Server Pool Policy Qualification (Crea criterio pool di server) o Add (Aggiungi).
5. Assegnare un nome al criterio Intel.
6. Selezionare Create CPU/Core Qualifications (Crea criteri CPU/core).
7. Scegli Xeon per il processore/architettura.
8. Invio <UCS-CPU- PID> Come ID di processo (PID).
9. Fare clic su OK per creare il criterio CPU/Core.
10. Fare clic su OK per creare il criterio, quindi fare clic su OK per confermare.



Creare una policy del BIOS del server

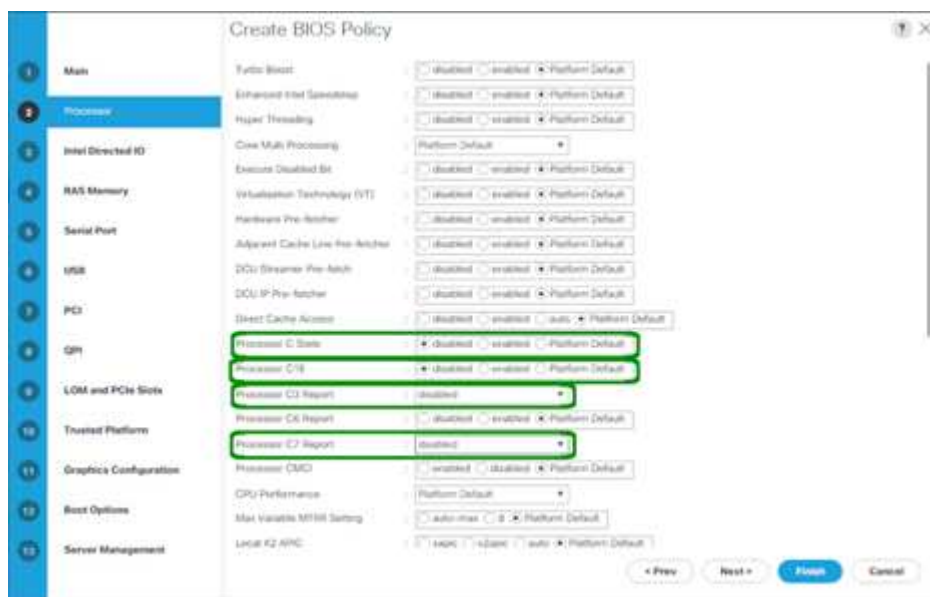
Per creare un criterio BIOS del server per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Criteri del BIOS.
4. Selezionare Create BIOS Policy (Crea policy BIOS).
5. Inserire VM-host come nome del criterio del BIOS.
6. Impostare l'opzione Quiet Boot su Disabled (Disattivato).
7. Impostare l'opzione Naming periferica coerente su attivato.



8. Selezionare la scheda Processor (processore) e impostare i seguenti parametri:

- Stato del processore C: Disattivato
- Processore C1E: Disattivato
- Report del processore C3: Disattivato
- Report processore C7: Disattivato



9. Scorrere verso il basso fino alle opzioni rimanenti del processore e impostare i seguenti parametri:

- Performance energetica: Performance
- Frequency Floor Override (Ignora frequenza)
- Rallentamento del clock della DRAM: Prestazioni



10. Fare clic su RAS Memory (memoria RAS) e impostare i seguenti parametri:

- LV DDR Mode (modalità LV DDR): Modalità Performance (prestazioni)



11. Fare clic su Finish (fine) per creare il criterio del BIOS.

12. Fare clic su OK.

Aggiornare la policy di manutenzione predefinita

Per aggiornare la policy di manutenzione predefinita, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Selezionare Maintenance Policies > default (Criteri di manutenzione).
4. Impostare il criterio di riavvio su User Ack.
5. Selezionare al prossimo avvio per delegare le finestre di manutenzione agli amministratori del server.

Servers / Policies / root / Maintenance Poli... / default

General Events

Actions

- Cancel
- Show Policy Usage
- Use Global

Properties

Name : default

Description :

Owner : Local

Soft Shutdown Timer : 150 Secs

Reboot Policy : ☐ Immediate ☒ User Ack ☐ Timer Automatic

☒ On Next Boot (Apply pending changes at next reboot.)

6. Fare clic su Salva modifiche.
7. Fare clic su OK per accettare la modifica.

Creare modelli vNIC

Per creare più modelli vNIC (Virtual Network Interface Card) per l'ambiente Cisco UCS, completare le procedure descritte in questa sezione.



Vengono creati in totale quattro modelli vNIC.

Creare vNIC dell'infrastruttura

Per creare una vNIC dell'infrastruttura, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su vNIC Templates.
4. Selezionare Create vNIC Template (Crea modello vNIC).
5. Invio Site-XX-vNIC_A Come nome del modello vNIC.
6. Selezionare Updating-template come tipo di modello.
7. Per Fabric ID (ID fabric), selezionare Fabric A.
8. Assicurarsi che l'opzione Enable failover (attiva failover) non sia selezionata.
9. Selezionare Primary Template (modello primario) per Redundancy Type (tipo di
10. Lasciare il modello di ridondanza peer impostato su <not set>.
11. In destinazione, assicurarsi che sia selezionata solo l'opzione adattatore.
12. Impostare Native-VLAN Come VLAN nativa.
13. Selezionare vNIC Name (Nome vNIC) per l'origine CDN.
14. Per MTU, immettere 9000.
15. In Permitted VLAN (VLAN consentite), selezionare `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic` E Site-XX-vMotion. Utilizzare il tasto Ctrl per effettuare questa selezione multipla.
16. Fare clic su Seleziona. Queste VLAN dovrebbero ora essere visualizzate in VLAN selezionate.
17. Nell'elenco MAC Pool, selezionare MAC_Pool_A.

18. Nell'elenco Network Control Policy (Criteri di controllo rete), selezionare Pool-A.
19. Nell'elenco Network Control Policy (Criteri di controllo di rete), selezionare Enable-CDP-LLDP.
20. Fare clic su OK per creare il modello vNIC.
21. Fare clic su OK.

LAN > Policies > root > vNIC Templates > vNIC_Template_A

General vNICs vNIC Groups Tasks Events

Actions

Modify vNICs
Modify vNIC Groups
Delete
Show Policy Usage
Get State

Properties

Name: vNIC_Template_A
Description:
Owner: Local
Fabric ID: ☒ Fabric A ☐ Fabric B ☒ Enable Failover
Redundancy: ☐ No Redundancy ☒ Primary Template ☐ Secondary Template
Peer Redundancy Template: vNIC_Template_B [Create vNIC Template](#)
Target: ☒ vNIC ☐ vNIC Group

Template Type: ☐ Initial Template ☒ Updating Template
QoS Source: ☒ vNIC Name ☐ User Defined
MTU: 9000
Policies
MAC Policy: MAC_Pool_Access
QoS Policy: vnic_def
Network Control Policy: Enable_CDP
Pre-Config: vnic_def
State Threshold Policy: default
Connection Policies
☒ Dynamic vNIC ☐ vNIC ☐ VNIC
Dynamic vNIC Connection Policy: vnic_def

Per creare il modello di ridondanza secondario Infra-B, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su vNIC Templates.
4. Selezionare Create vNIC Template (Crea modello vNIC).
5. Immettere `Site-XX-vNIC_B` come nome del modello vNIC.
6. Selezionare Updating-template come tipo di modello.
7. Per ID fabric, selezionare Fabric B.
8. Selezionare l'opzione Enable failover (attiva failover).



La scelta del failover è un passaggio critico per migliorare il tempo di failover del collegamento gestendolo a livello hardware e per evitare che lo switch virtuale non rilevi guasti alla scheda NIC.

9. Selezionare Primary Template (modello primario) per Redundancy Type (tipo di
10. Lasciare il modello di ridondanza peer impostato su vNIC_Template_A.
11. In destinazione, assicurarsi che sia selezionata solo l'opzione adattatore.
12. Impostare Native-VLAN Come VLAN nativa.
13. Selezionare vNIC Name (Nome vNIC) per l'origine CDN.
14. Per MTU, immettere 9000.
15. In Permitted VLAN (VLAN consentite), selezionare `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic` E Site-XX-vMotion. Utilizzare il tasto Ctrl per effettuare questa selezione multipla.
16. Fare clic su Seleziona. Queste VLAN dovrebbero ora essere visualizzate in VLAN selezionate.
17. Nell'elenco MAC Pool, selezionare MAC_Pool_B.
18. Nell'elenco Network Control Policy (Criteri controllo rete), selezionare Pool-B.
19. Nell'elenco Network Control Policy (Criteri di controllo di rete), selezionare Enable-CDP-LLDP.
20. Fare clic su OK per creare il modello vNIC.
21. Fare clic su OK.

LAN / Policies / root / vNIC Templates / vNIC Template vNIC_Template_B

Templates VLANs VLAN Groups Trunks Profiles

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Default

Properties

Name: vNIC_Template_B

Description:

Owner: Local

Fabric ID: ☐ Fabric A ☒ Fabric B ☐ Enable Fabric

Redundancy

Redundancy Type: ☐ No Redundancy ☐ Primary Template ☒ Secondary Template

Peer Redundancy Template: vNIC_Template_A

Create vNIC Template

Target

Adapters

MTU

Template Type: ☐ Native Template ☒ Upstream Template

CDN Source: ☒ vNIC Name ☐ User Defined

MTU: 9000

Policies

MAC Pool: 1 MAC Pool_B(56/54)

QoS Policy: 1

Network Control Policy: 1 Enable_CDP

Pin Group: 1

Stats Threshold Policy: 1 default

Connection Policies

☒ Dynamic vNIC ☐ iSCSI ☐ VMQ

Dynamic vNIC Connection Policy: 1

Creare vNIC iSCSI

Per creare vNIC iSCSI, attenersi alla seguente procedura:

1. Selezionare LAN a sinistra.

2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su vNIC Templates.
4. Selezionare Create vNIC Template (Crea modello vNIC).
5. Invio Site- 01-iSCSI_A Come nome del modello vNIC.
6. Selezionare Fabric A. Non selezionare l'opzione Enable failover (attiva failover).
7. Lasciare il tipo di ridondanza impostato su No Redundancy (Nessuna ridondanza).
8. In destinazione, assicurarsi che sia selezionata solo l'opzione adattatore.
9. Selezionare Updating Template (aggiornamento modello) per Template Type (
10. In VLAN, selezionare solo sito- 01-iSCSI_A_VLAN.
11. Selezionare Site- 01-iSCSI_A_VLAN come VLAN nativa.
12. Lasciare il nome vNIC impostato per l'origine CDN.
13. In MTU, immettere 9000.
14. Dall'elenco MAC Pool, selezionare MAC-Pool-A.
15. Dall'elenco Network Control Policy (Criteri di controllo di rete), selezionare Enable-CDP-LLDP.
16. Fare clic su OK per completare la creazione del modello vNIC.
17. Fare clic su OK.

LAN / Policies / root / vNIC Templates / vNIC Template Site_01_iSCSI-A

General VLANs VLAN Groups Faults Events

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Global

Properties

Name : Site_01_iSCSI-A

Description :

Owner : Local

Fabric ID : ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Redundancy :

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

☒ Adapter ☐ VM

Template Type : ☐ Initial Template ☒ Updating Template

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

Policies

MAC Pool : MAC_Pool_A(56/64)

QoS Policy : <not set>

Network Control Policy : Enable_CDP

Pin Group : <not set>

Stats Threshold Policy : default

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set>

18. Selezionare LAN a sinistra.
19. Selezionare Policy > root.
20. Fare clic con il pulsante destro del mouse su vNIC Templates.
21. Selezionare Create vNIC Template (Crea modello vNIC).
22. Invio Site- 01-iSCSI_B Come nome del modello vNIC.
23. Selezionare Fabric B. Non selezionare l'opzione Enable failover (attiva failover).
24. Lasciare il tipo di ridondanza impostato su No Redundancy (Nessuna ridondanza).
25. In destinazione, assicurarsi che sia selezionata solo l'opzione adattatore.
26. Selezionare Updating Template (aggiornamento modello) per Template Type (
27. In VLAN, selezionare solo Site- 01-iSCSI_B_VLAN.
28. Selezionare Site- 01-iSCSI_B_VLAN Come VLAN nativa.
29. Lasciare il nome vNIC impostato per l'origine CDN.
30. In MTU, immettere 9000.
31. Dall'elenco MAC Pool, selezionare MAC-Pool-B.
32. Dall'elenco Network Control Policy (Criteri di controllo della rete), selezionare Enable-CDP-LLDP.
33. Fare clic su OK per completare la creazione del modello vNIC.
34. Fare clic su OK.

General VLANs VLAN Groups Faults Events

Actions

- Modify VNICs
- Modify VLAN Groups
- Delete
- Show Policy Usage
- Use Wizard

Properties

Name : Site_01_ISCSI-B

Description :

Owner : Local

Fabric ID : ☐ Fabric A ☒ Fabric B ☐ Enable Failover

Redundancy

Redundancy Type : ☒ No Redundancy ☐ Primary Template ☐ Secondary Template

Target

☒ Podster

☐ VM

Template Type : ☐ Initial Template ☒ Updating Template

CDN Source : ☒ vNIC Name ☐ User Defined

MTU : 9000

Policies

MAC Pool : MAC_Pool_B(56/64) ▼

QoS Policy : <not set> ▼

Network Control Policy : Enable_CDP ▼

Pin Group : <not set> ▼

Stats Threshold Policy : default ▼

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

Dynamic vNIC Connection Policy : <not set> ▼

Creare una policy di connettività LAN per l'avvio iSCSI

Questa procedura si applica a un ambiente Cisco UCS in cui due LIF iSCSI si trovano sul nodo cluster 1 (iscsi_lif01a e iscsi_lif01b) E due LIF iSCSI si trovano sul nodo cluster 2 (iscsi_lif02a e iscsi_lif02b). Inoltre, si presuppone che i LIF A siano collegati al fabric A (Cisco UCS 6324 A) e che i LIF B siano collegati al fabric B (Cisco UCS 6324 B).

Per configurare il criterio di connettività LAN dell'infrastruttura necessario, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare LAN > Policies > root.
3. Fare clic con il pulsante destro del mouse su Criteri di connettività LAN.
4. Selezionare Crea policy di connettività LAN.
5. Invio Site-XX-Fabric-A come nome del criterio.
6. Fare clic sull'opzione Add (Aggiungi) superiore per aggiungere una vNIC.
7. Nella finestra di dialogo Create vNIC (Crea vNIC), immettere Site-01-vNIC-A Come nome della vNIC.
8. Selezionare l'opzione Use vNIC Template (Usa modello vNIC).
9. Nell'elenco vNIC Template (modello vNIC), selezionare vNIC_Template_A.

10. Dall'elenco a discesa Adapter Policy (criterio adattatore), selezionare VMware.
11. Fare clic su OK per aggiungere questa vNIC al criterio.

Modify vNIC

Name : **Site-01-vNIC-A**

Use vNIC Template : ☒

[Create vNIC Template](#)

vNIC Template : vNIC_Template_A ▼

Adapter Performance Profile

Adapter Policy : VMWare ▼

[Create Ethernet Adapter Policy](#)

[Create QoS Policy](#)

[Create Network Control Policy](#)

Connection Policies

☒ Dynamic vNIC ☐ usNIC ☐ VMQ

OK **Cancel**

12. Fare clic sull'opzione Add (Aggiungi) superiore per aggiungere una vNIC.
13. Nella finestra di dialogo Create vNIC (Crea vNIC), immettere Site-01-vNIC-B Come nome della vNIC.
14. Selezionare l'opzione Use vNIC Template (Usa modello vNIC).
15. Nell'elenco vNIC Template (modello vNIC), selezionare vNIC_Template_B.
16. Dall'elenco a discesa Adapter Policy (criterio adattatore), selezionare VMware.
17. Fare clic su OK per aggiungere questa vNIC al criterio.
18. Fare clic sull'opzione Add (Aggiungi) superiore per aggiungere una vNIC.
19. Nella finestra di dialogo Create vNIC (Crea vNIC), immettere Site-01- iSCSI-A Come nome della vNIC.
20. Selezionare l'opzione Use vNIC Template (Usa modello vNIC).
21. Nell'elenco vNIC Template (modello vNIC), selezionare Site-01-iSCSI-A.
22. Dall'elenco a discesa Adapter Policy (criterio adattatore), selezionare VMware.
23. Fare clic su OK per aggiungere questa vNIC al criterio.
24. Fare clic sull'opzione Add (Aggiungi) superiore per aggiungere una vNIC.

25. Nella finestra di dialogo Create vNIC (Crea vNIC), immettere Site-01-iSCSI-B Come nome della vNIC.
26. Selezionare l'opzione Use vNIC Template (Usa modello vNIC).
27. Nell'elenco vNIC Template (modello vNIC), selezionare Site-01-iSCSI-B.
28. Dall'elenco a discesa Adapter Policy (criterio adattatore), selezionare VMware.
29. Fare clic su OK per aggiungere questa vNIC al criterio.
30. Espandere l'opzione Add iSCSI vNIC (Aggiungi vNIC iSCSI).
31. Fare clic sull'opzione Lower Add (Aggiungi) nello spazio Add iSCSI vNIC (Aggiungi vNIC iSCSI) per aggiungere iSCSI vNIC.
32. Nella finestra di dialogo Create iSCSI vNIC (Crea vNIC iSCSI), immettere Site-01-iSCSI-A Come nome della vNIC.
33. Selezionare Overlay vNIC As (Sovrapponi vNIC con nome) Site-01-iSCSI-A.
34. Lasciare l'opzione iSCSI Adapter Policy (criterio adattatore iSCSI) su Not Set (non impostato).
35. Selezionare la VLAN con nome Site-01-iSCSI-Site-A (nativo).
36. Selezionare None (Nessuno) (utilizzato per impostazione predefinita) come assegnazione dell'indirizzo MAC.
37. Fare clic su OK per aggiungere la vNIC iSCSI al criterio.

Modify iSCSI vNIC ? ✕

Name : **Site-01-ISCSI-A**

Overlay vNIC :

iSCSI Adapter Policy : [Create iSCSI Adapter Policy](#)

VLAN :

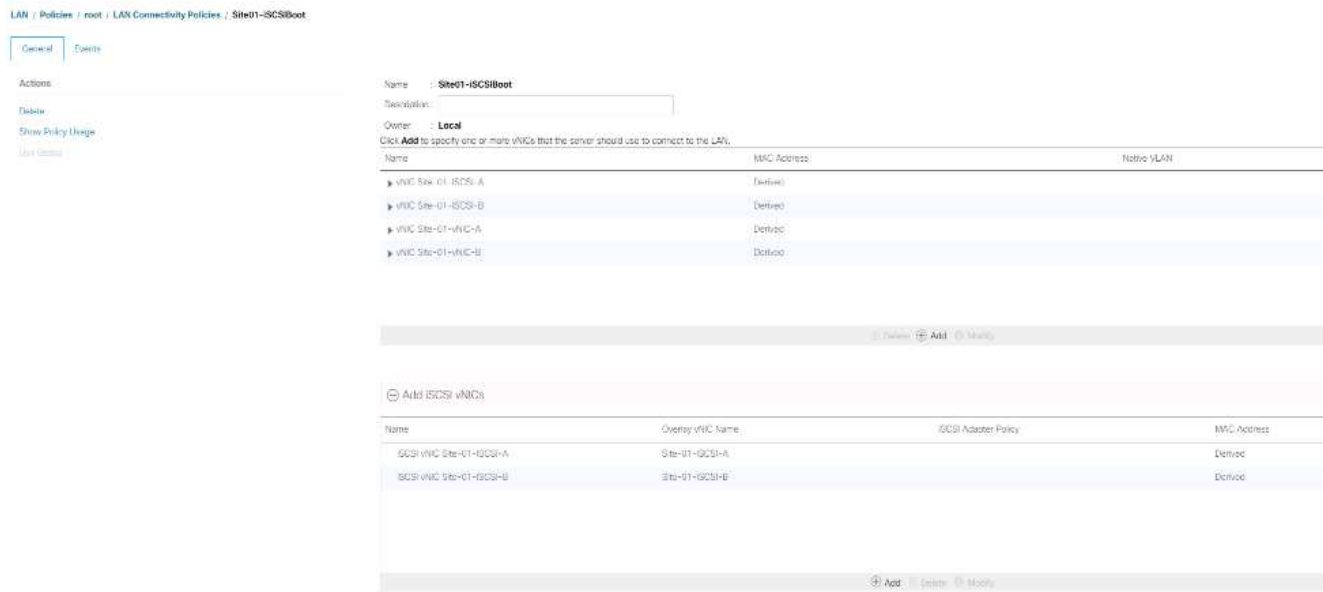
iSCSI MAC Address

MAC Address Assignment:

[Create MAC Pool](#)

OK **Cancel**

38. Fare clic sull'opzione Lower Add (Aggiungi) nello spazio Add iSCSI vNIC (Aggiungi vNIC iSCSI) per aggiungere iSCSI vNIC.
39. Nella finestra di dialogo Create iSCSI vNIC (Crea vNIC iSCSI), immettere Site-01-iSCSI-B Come nome della vNIC.
40. Selezionare Overlay vNIC come Site-01-iSCSI-B.
41. Lasciare l'opzione iSCSI Adapter Policy (criterio adattatore iSCSI) su Not Set (non impostato).
42. Selezionare la VLAN con nome Site-01-iSCSI-Site-B (nativo).
43. Selezionare None (Nessuno) (utilizzato per impostazione predefinita) come MAC Address Assignment (assegnazione indirizzo MAC).
44. Fare clic su OK per aggiungere la vNIC iSCSI al criterio.
45. Fare clic su Salva modifiche.



Creare una policy vMedia per l'avvio dell'installazione di VMware ESXi 6.7U1

Nelle fasi di configurazione di NetApp Data ONTAP è necessario un server web HTTP, utilizzato per ospitare NetApp Data ONTAP e il software VMware. La policy vMedia creata qui mappa VMware ESXi 6.7U1 ISO al server Cisco UCS per avviare l'installazione di ESXi. Per creare questo criterio, attenersi alla seguente procedura:

1. In Cisco UCS Manager, selezionare Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Selezionare i criteri vMedia.
4. Fare clic su Add (Aggiungi) per creare una nuova policy vMedia.
5. Assegnare un nome al criterio ESXi-6.7U1-HTTP.
6. Immettere Mounts ISO per ESXi 6.7U1 nel campo Description (Descrizione).
7. Selezionare Sì per Riprova in caso di errore di montaggio.
8. Fare clic su Aggiungi.
9. Assegnare un nome al mount ESXi-6.7U1-HTTP.
10. Selezionare il tipo di dispositivo CDD.
11. Selezionare il protocollo HTTP.
12. Inserire l'indirizzo IP del server Web.



Gli IP del server DNS non sono stati precedentemente immessi nell'IP KVM, pertanto è necessario inserire l'IP del server Web invece del nome host.

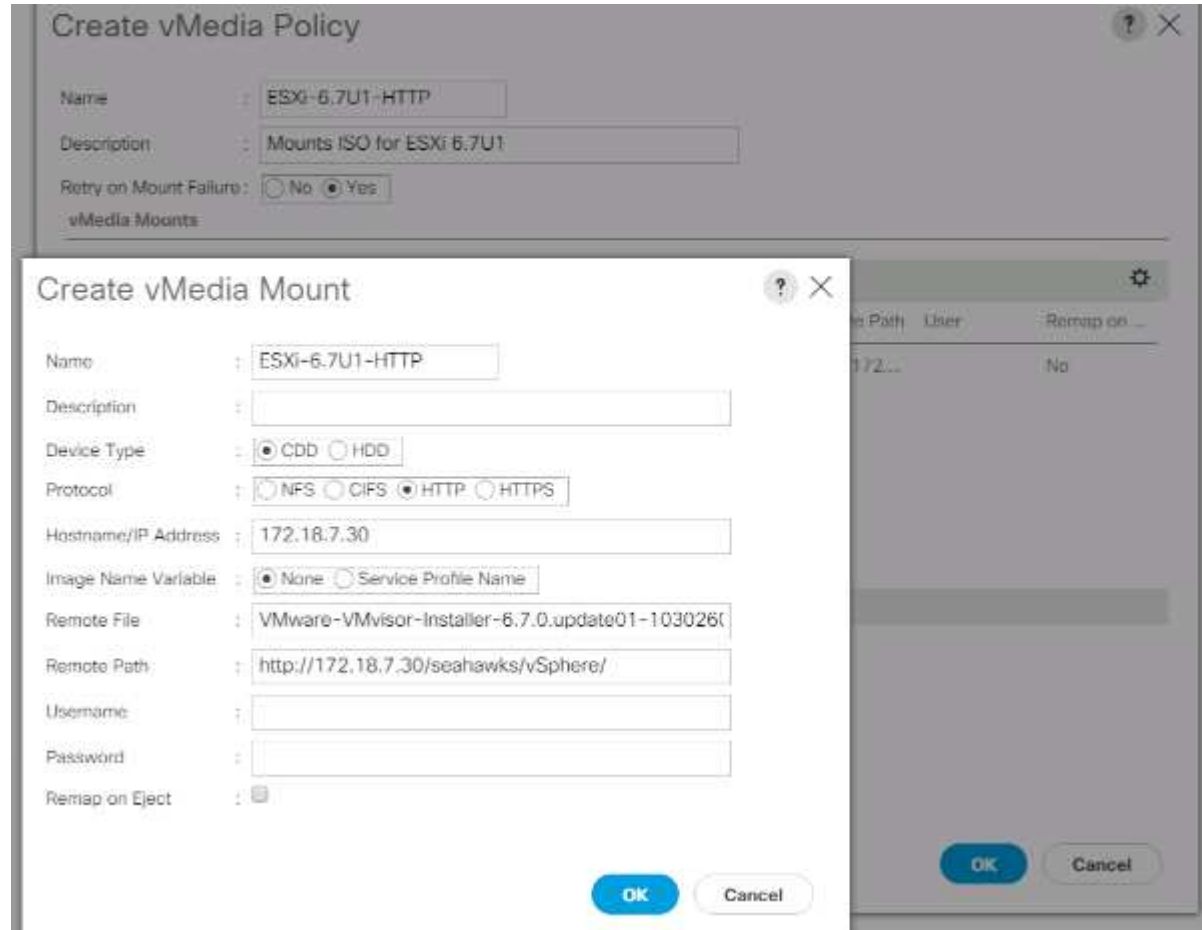
13. Invio VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso Come nome del file remoto.

Questo ISO VMware ESXi 6.7U1 può essere scaricato da ["Download VMware"](#).

14. Immettere il percorso del server Web al file ISO nel campo percorso remoto.

15. Fare clic su OK per creare vMedia Mount.
16. Fare clic su OK, quindi di nuovo su OK per completare la creazione del criterio vMedia.

Per i nuovi server aggiunti all'ambiente Cisco UCS, è possibile utilizzare il modello di profilo del servizio vMedia per installare l'host ESXi. Al primo avvio, l'host si avvia nel programma di installazione di ESXi poiché il disco montato SULLA SAN è vuoto. Dopo l'installazione di ESXi, il vMedia non viene referenziato finché il disco di avvio è accessibile.



Creare una policy di avvio iSCSI

La procedura descritta in questa sezione si applica a un ambiente Cisco UCS in cui due interfacce logiche iSCSI (LIF) si trovano sul nodo cluster 1 (`iscsi_lif01a` e `iscsi_lif01b`) e due LIF iSCSI si trovano sul nodo cluster 2 (`iscsi_lif02a` e `iscsi_lif02b`). Inoltre, si presuppone che i LIF A siano collegati al fabric A (Cisco UCS Fabric Interconnect A) e che i LIF B siano collegati al fabric B (Cisco UCS Fabric Interconnect B).

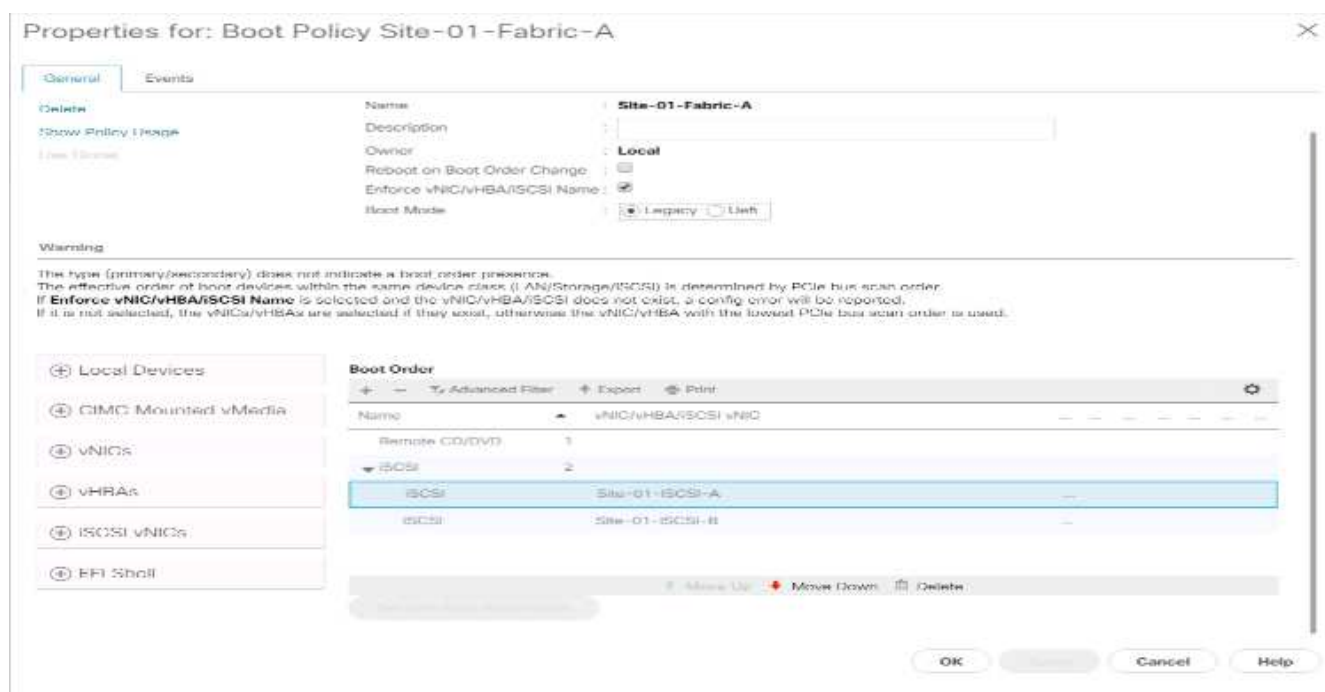


In questa procedura viene configurato un criterio di avvio. Il criterio configura la destinazione primaria in modo che sia `iscsi_lif01a`.

Per creare una policy di avvio per l'ambiente Cisco UCS, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Criteri di avvio.

4. Selezionare Create Boot Policy (Crea policy di avvio).
5. Invio Site-01-Fabric-A come nome della policy di boot.
6. Facoltativo: Inserire una descrizione per la policy di avvio.
7. Lasciare deselezionata l'opzione Reboot on Boot Order Change (Riavvia alla modifica dell'ordine di avvio).
8. La modalità di avvio è legacy.
9. Espandere il menu a discesa Local Devices (periferiche locali) e selezionare Add Remote CD/DVD (Aggiungi CD/DVD remoto).
10. Espandere il menu a discesa vNIC iSCSI e selezionare Add iSCSI Boot (Aggiungi avvio iSCSI).
11. Nella finestra di dialogo Add iSCSI Boot (Aggiungi avvio iSCSI), immettere Site-01-iSCSI-A. Fare clic su OK.
12. Selezionare Add iSCSI Boot (Aggiungi avvio iSCSI).
13. Nella finestra di dialogo Add iSCSI Boot (Aggiungi avvio iSCSI), immettere Site-01-iSCSI-B. Fare clic su OK.
14. Fare clic su OK per creare il criterio.



Creare un modello di profilo del servizio

In questa procedura, viene creato un modello di profilo di servizio per gli host ESXi dell'infrastruttura per l'avvio fabric A.

Per creare il modello di profilo del servizio, attenersi alla seguente procedura:

1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Service Profile Templates > root.
3. Fare clic con il pulsante destro del mouse su root.
4. Selezionare Create Service Profile Template (Crea modello profilo servizio) per aprire la procedura guidata Create Service Profile Template (Crea modello profilo servizio).

5. Invio VM-Host-Infra-iSCSI-A come nome del modello di profilo del servizio. Questo modello di profilo del servizio è configurato per l'avvio dal nodo di storage 1 sul fabric A.
6. Selezionare l'opzione Updating Template (aggiornamento modello).
7. In UUID, selezionare UUID_Pool Come pool UUID. Fare clic su Avanti.

Configurare il provisioning dello storage

Per configurare il provisioning dello storage, attenersi alla seguente procedura:

1. Se si dispone di server senza dischi fisici, fare clic su Criteri di configurazione disco locale e selezionare il criterio di storage locale di avvio SAN. In caso contrario, selezionare il criterio di storage locale predefinito.
2. Fare clic su Avanti.

Configurare le opzioni di rete

Per configurare le opzioni di rete, attenersi alla seguente procedura:

1. Mantenere l'impostazione predefinita per Dynamic vNIC Connection Policy (Criteri di connessione vNIC dinamici).
2. Selezionare l'opzione Use Connectivity Policy (Usa policy di connettività) per configurare la connettività LAN.
3. Selezionare iSCSI-Boot dal menu a discesa LAN Connectivity Policy (Criteri di connettività LAN).
4. Selezionare IQN_Pool In Initiator Name Assignment. Fare clic su Avanti.

Configurare la connettività SAN

Per configurare la connettività SAN, attenersi alla seguente procedura:

1. Per i vHBA, selezionare No nella casella come si desidera configurare la connettività SAN? opzione.
2. Fare clic su Avanti.

Configurare lo zoning

Per configurare lo zoning, fare clic su Next (Avanti).

Configurare il posizionamento di vNIC/HBA

Per configurare il posizionamento di vNIC/HBA, attenersi alla seguente procedura:

1. Nell'elenco a discesa Select Placement (Seleziona posizionamento), lasciare la policy di posizionamento come Let System Perform Placement (Consenti al sistema di eseguire il posizionamento).
2. Fare clic su Avanti.

Configurare il criterio vMedia

Per configurare il criterio vMedia, attenersi alla seguente procedura:

1. Non selezionare una policy vMedia.
2. Fare clic su Avanti.

Configurare l'ordine di avvio del server

Per configurare l'ordine di avvio del server, attenersi alla seguente procedura:

1. Selezionare `Boot-Fabric-A` Per la policy di avvio.

Create Service Profile Template

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: **Site-01-Fabric-A** [Create Boot Policy](#)

Name: **Site-01-Fabric-A**
Description:
Reboot on Boot Order Change: **No**
Enforce vNIC/vHBA/iSCSI Name: **Yes**
Boot Mode: **Legacy**

WARNINGS:
The type (primary/secondary) does not indicate a boot order preference.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs are selected if they exist, otherwise the vNIC/vHBA with the lowest PCIe bus scan order is used.

Boot Order

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	LUN Name	WWN	Slot Number	Boot Name	Boot Path	Description
HBA	1		Primary						
iSCSI	2		Primary						
iSCSI		Site-01-iSCSI-A	Primary						
iSCSI		Site-01-iSCSI-B	Secondary						

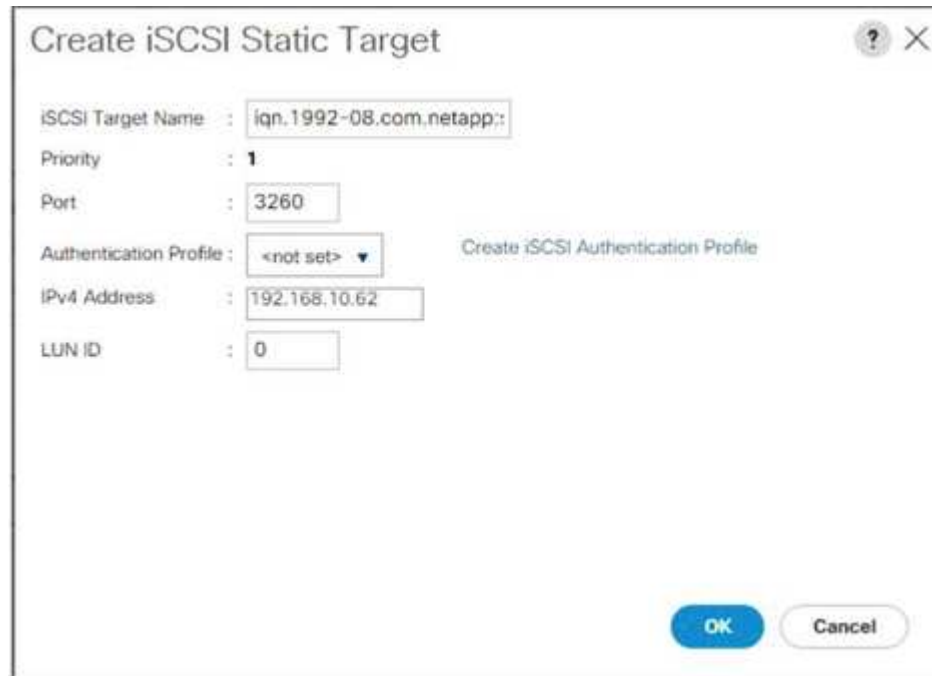
[Add iSCSI vNIC](#) [Add iSCSI Boot Parameters](#) [Set iSCSI Boot Parameters](#)

[< Prev](#) [Next >](#) [Finish](#) [Cancel](#)

2. Nell'ordine boot, selezionare `Site-01- iSCSI-A`.
3. Fare clic su `Set iSCSI Boot Parameters`.
4. Nella finestra di dialogo `Set iSCSI Boot Parameters` (Imposta parametri di avvio iSCSI), lasciare l'opzione `Authentication Profile` (Profilo di autenticazione) su `Not Set` (non impostato) a meno che non sia stata creata in modo indipendente una voce appropriata per l'ambiente in uso.
5. Lasciare la finestra di dialogo `Initiator Name Assignment` (assegnazione nome iniziatore) non impostata per utilizzare il nome iniziatore del profilo di servizio singolo definito nei passaggi precedenti.
6. Impostare `iSCSI_IP_Pool_A` Come policy dell'indirizzo IP iniziatore.
7. Selezionare l'opzione `iSCSI Static Target Interface` (interfaccia destinazione statica iSCSI).
8. Fare clic su `Aggiungi`.
9. Inserire il nome della destinazione iSCSI. Per ottenere il nome di destinazione iSCSI di `Infra-SVM`, accedere all'interfaccia di gestione del cluster di storage ed eseguire `iscsi show` comando.

```
bb04-aff300:> iscsi show
Target                Target                Status
Vserver Name          Alias                Admin
-----
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811a68d9d00a098a9fec2:vs.3
                        Infra-SVM
                        up
```

10. Immettere l'indirizzo IP di `iscsi_lif_02a` Per il campo IPv4 Address (Indirizzo IPv4).

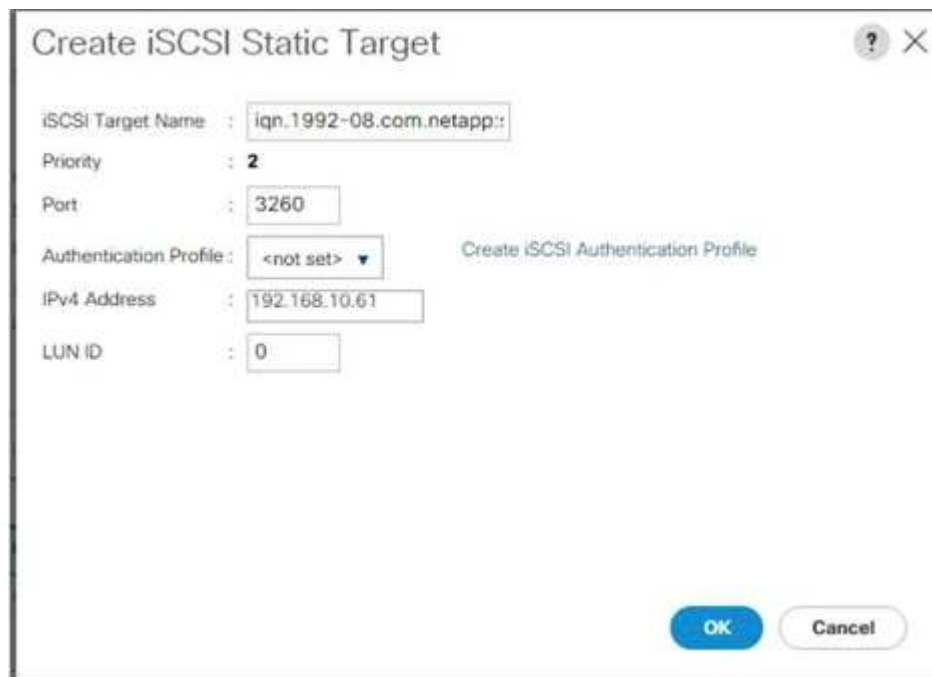


The dialog box is titled "Create iSCSI Static Target" and contains the following fields and options:

- iSCSI Target Name: `iqn.1992-08.com.netapp::`
- Priority: `1`
- Port: `3260`
- Authentication Profile: `<not set>` (with a dropdown arrow) and a link "Create iSCSI Authentication Profile"
- IPv4 Address: `192.168.10.62`
- LUN ID: `0`

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).

11. Fare clic su OK per aggiungere la destinazione statica iSCSI.
12. Fare clic su Aggiungi.
13. Inserire il nome della destinazione iSCSI.
14. Immettere l'indirizzo IP di `iscsi_lif_01a` Per il campo IPv4 Address (Indirizzo IPv4).



The dialog box is titled "Create iSCSI Static Target" and contains the following fields and options:

- iSCSI Target Name: `iqn.1992-08.com.netapp::`
- Priority: `2`
- Port: `3260`
- Authentication Profile: `<not set>` (with a dropdown arrow) and a link "Create iSCSI Authentication Profile"
- IPv4 Address: `192.168.10.61`
- LUN ID: `0`

At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).

15. Fare clic su OK per aggiungere la destinazione statica iSCSI.

Set iSCSI Boot Parameters

Name : **iSCSI-A-vNIC**

Authentication Profile : **<not set>** [Create iSCSI Authentication Profile](#)

Initiator Name

Initiator Name Assignment: **<not set>**

[Create IQN Suffix Pool](#)

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: **iSCSI_IP_Pool_A(12/16)**

IPv4 Address : **0.0.0.0**
 Subnet Mask : **255.255.255.0**
 Default Gateway : **0.0.0.0**
 Primary DNS : **0.0.0.0**
 Secondary DNS : **0.0.0.0**

[Create IP Pool](#)
[Reset Initiator Address](#)
 The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface ☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro.	iSCSI IPv4 Address	LUN id
iqn.1992-08.c...	1	3260		192.168.10.62	0
iqn.1992-08.c...	2	3260		192.168.10.61	0

OK **Cancel**



Gli IP di destinazione sono stati inseriti con il nodo di storage 02 IP per primo e il nodo di storage 01 IP per secondo. Questo presuppone che il LUN di avvio si trovi sul nodo 01. L'host si avvia utilizzando il percorso verso il nodo 01 se viene utilizzato l'ordine in questa procedura.

16. In Boot Order (Ordine di avvio), selezionare iSCSI-B-vNIC.
17. Fare clic su Set iSCSI Boot Parameters.
18. Nella finestra di dialogo Set iSCSI Boot Parameters (Imposta parametri di avvio iSCSI), lasciare l'opzione Authentication Profile (Profilo di autenticazione) come Not Set (non impostato), a meno che non sia stata creata in modo indipendente una voce appropriata per l'ambiente in uso.
19. Lasciare la finestra di dialogo Initiator Name Assignment (assegnazione nome iniziatore) non impostata per utilizzare il nome iniziatore del profilo di servizio singolo definito nei passaggi precedenti.
20. Impostare `iSCSI_IP_Pool_B` Come policy dell'indirizzo IP iniziatore.
21. Selezionare l'opzione iSCSI Static Target Interface (interfaccia destinazione statica iSCSI).
22. Fare clic su Aggiungi.
23. Inserire il nome della destinazione iSCSI. Per ottenere il nome di destinazione iSCSI di Infra-SVM, accedere all'interfaccia di gestione del cluster di storage ed eseguire `iscsi show` comando.

```
bb04-aff300::> iscsi show
```

Vserver	Target Name	Target Alias	Status Admin
Infra-SVM	iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3	Infra-SVM	up

24. Immettere l'indirizzo IP di `iscsi_lif_02b` Per il campo IPv4 Address (Indirizzo IPv4).

Create iSCSI Static Target

iSCSI Target Name :

Priority :

Port :

Authentication Profile : [Create iSCSI Authentication Profile](#)

IPv4 Address :

LUN ID :

25. Fare clic su OK per aggiungere la destinazione statica iSCSI.

26. Fare clic su Aggiungi.

27. Inserire il nome della destinazione iSCSI.

28. Immettere l'indirizzo IP di `iscsi_lif_01b` Per il campo IPv4 Address (Indirizzo IPv4).

Create iSCSI Static Target

iSCSI Target Name :

Priority :

Port :

Authentication Profile : [Create iSCSI Authentication Profile](#)

IPv4 Address :

LUN ID :

29. Fare clic su OK per aggiungere la destinazione statica iSCSI.

Set iSCSI Boot Parameters

Create IQN Suffix Pool

WARNING: The selected pool does not contain any available entities. You can select it, but it is recommended that you add entities to it.

Initiator Address

Initiator IP Address Policy: iSCSI_IP_Pool_B(12/16)

IPv4 Address : 0.0.0.0

Subnet Mask : 255.255.255.0

Default Gateway : 0.0.0.0

Primary DNS : 0.0.0.0

Secondary DNS : 0.0.0.0

Create IP Pool

Reset Initiator Address

The IP address will be automatically assigned from the selected pool.

☒ iSCSI Static Target Interface

☐ iSCSI Auto Target Interface

Name	Priority	Port	Authentication Pro..	iSCSI IPv4 Address	LUN Id
iqn.1992-08.c...	1	3260		192.168.20.62	0
iqn.1992-08.c...	2	3260		192.168.20.61	0

Add

Delete

Info

Minimum one instance of iSCSI Static Target Interface and maximum two are allowed.

OK

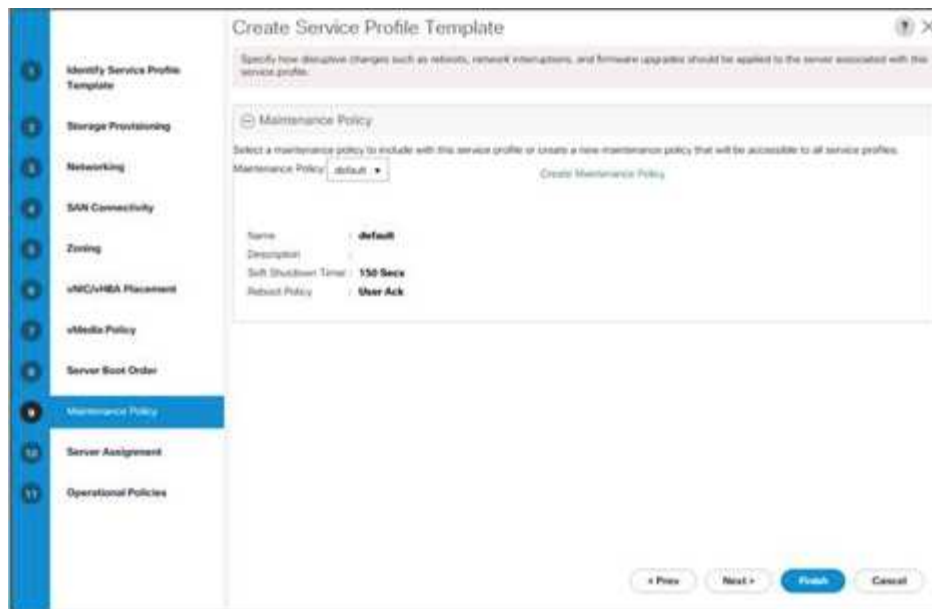
Cancel

30. Fare clic su Avanti.

Configurare la policy di manutenzione

Per configurare la policy di manutenzione, attenersi alla seguente procedura:

- 1. Impostare la policy di manutenzione su default.



2. Fare clic su Avanti.

Configurare l'assegnazione del server

Per configurare l'assegnazione del server, attenersi alla seguente procedura:

1. Nell'elenco Pool Assignment (assegnazione pool), selezionare Infra-Pool.
2. Selezionare inattivo come stato di alimentazione da applicare quando il profilo è associato al server.
3. Espandere firmware Management (Gestione firmware) nella parte inferiore della pagina e selezionare il criterio predefinito.

4. Fare clic su Avanti.

Configurare le policy operative

Per configurare le policy operative, attenersi alla seguente procedura:

1. Dall'elenco a discesa BIOS Policy (criterio BIOS), selezionare VM-host (host VM).
2. Espandere Power Control Policy Configuration e selezionare No-Power-Cap dall'elenco a discesa Power Control Policy (Criteri controllo alimentazione).

3. Fare clic su Finish (fine) per creare il modello di profilo del servizio.
4. Fare clic su OK nel messaggio di conferma.

Creare un modello di profilo del servizio abilitato per vMedia

Per creare un modello di profilo del servizio con vMedia attivato, attenersi alla seguente procedura:

1. Connettersi a UCS Manager e fare clic su Servers (Server) a sinistra.
2. Selezionare Service Profile Templates > root > Service Template VM-host-Infra-iSCSI-A.
3. Fare clic con il pulsante destro del mouse su VM-host-Infra-iSCSI-A e selezionare Create a Clone (Crea un clone).
4. Assegnare un nome al clone VM-Host-Infra-iSCSI-A-VM.
5. Selezionare la VM-host-Infra-iSCSI-A-VM appena creata e selezionare la scheda vMedia Policy (criterio vMedia) a destra.
6. Fare clic su Modify vMedia Policy.
7. Selezionare ESXi-6. 7U1-HTTP vMedia Policy e fare clic su OK.
8. Fare clic su OK per confermare.

Creare profili di servizio

Per creare profili di servizio dal modello di profilo di servizio, attenersi alla seguente procedura:

1. Connettersi a Cisco UCS Manager e fare clic su Servers (Server) a sinistra.
2. Espandere Server > modelli profilo servizio > root > <name> modello servizio.
3. In azioni, fare clic su Crea profilo di servizio dal modello e completare i seguenti passaggi:
 - a. Invio Site- 01-Infra-0 come prefisso di denominazione.
 - b. Invio 2 come numero di istanze da creare.
 - c. Selezionare root come org.
 - d. Fare clic su OK per creare i profili di servizio.



4. Fare clic su OK nel messaggio di conferma.

5. Verificare che i profili di servizio Site-01-Infra-01 e. Site-01-Infra-02 sono stati creati.



I profili di servizio vengono automaticamente associati ai server dei pool di server assegnati.

Configurazione dello storage - parte 2: LUN di avvio e gruppi di iniziatori

Configurazione dello storage di boot ONTAP

Creare gruppi di iniziatori

Per creare gruppi di iniziatori (igroups), attenersi alla seguente procedura:

1. Eseguire i seguenti comandi dalla connessione SSH del nodo di gestione del cluster:

```
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-01 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-01-iqn>
igroup create -vserver Infra-SVM -igroup VM-Host-Infra-02 -protocol
iscsi -ostype vmware -initiator <vm-host-infra-02-iqn>
igroup create -vserver Infra-SVM -igroup MGMT-Hosts -protocol iscsi
-ostype vmware -initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```



Utilizzare i valori elencati nella Tabella 1 e nella Tabella 2 per le informazioni IQN.

2. Per visualizzare i tre igroups appena creati, eseguire `igroup show` comando.

Mappare le LUN di avvio a igroups

Per mappare le LUN di avvio a igroups, completare la seguente fase:

1. Dalla connessione SSH di gestione del cluster di storage, eseguire i seguenti comandi:

```
lun map -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra- A
-igroup VM-Host-Infra-01 -lun-id 0lun map -vserver Infra-SVM -volume
esxi_boot -lun VM-Host-Infra- B -igroup VM-Host-Infra-02 -lun-id 0
```

Procedura di implementazione di VMware vSphere 6.7U1

Questa sezione fornisce procedure dettagliate per l'installazione di VMware ESXi 6.7U1 in una configurazione FlexPod Express. Al termine delle procedure, viene eseguito il provisioning di due host ESXi avviati.

Esistono diversi metodi per installare ESXi in un ambiente VMware. Queste procedure si concentrano su come utilizzare la console KVM integrata e le funzionalità dei supporti virtuali di Cisco UCS Manager per mappare i supporti di installazione remota ai singoli server e connettersi alle LUN di avvio.

Scarica l'immagine personalizzata Cisco per ESXi 6.7U1

Se l'immagine personalizzata VMware ESXi non è stata scaricata, completare i seguenti passaggi per

completare il download:

1. Fare clic sul seguente collegamento: [VMware vSphere Hypervisor \(ESXi\) 6.7U1](#).
2. Sono necessari un ID utente e una password su "[vmware.com](#)" per scaricare questo software.
3. Scaricare il .iso file.

Cisco UCS Manager

Cisco UCS IP KVM consente all'amministratore di avviare l'installazione del sistema operativo tramite supporti remoti. È necessario accedere all'ambiente Cisco UCS per eseguire il KVM IP.

Per accedere all'ambiente Cisco UCS, attenersi alla seguente procedura:

1. Aprire un browser Web e inserire l'indirizzo IP dell'indirizzo del cluster Cisco UCS. Questa fase avvia l'applicazione Cisco UCS Manager.
2. Fare clic sul collegamento Launch UCS Manager (Avvia UCS Manager) sotto HTML per avviare la GUI di HTML 5 UCS Manager.
3. Se viene richiesto di accettare i certificati di sicurezza, accettarli secondo necessità.
4. Quando richiesto, immettere `admin` come nome utente e inserire la password amministrativa.
5. Per accedere a Cisco UCS Manager, fare clic su Login (Accedi).
6. Dal menu principale, fare clic su Servers (Server) a sinistra.
7. Selezionare Server > profili di servizio > root > VM-Host-Infra-01.
8. Fare clic con il pulsante destro del mouse VM-Host-Infra-01 E selezionare KVM Console.
9. Seguire le istruzioni per avviare la console KVM basata su Java.
10. Selezionare Server > profili di servizio > root > VM-Host-Infra-02.
11. Fare clic con il pulsante destro del mouse VM-Host-Infra-02. E selezionare KVM Console.
12. Seguire le istruzioni per avviare la console KVM basata su Java.

Configurare l'installazione di VMware ESXi

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per preparare il server per l'installazione del sistema operativo, completare i seguenti passaggi su ciascun host ESXi:

1. Nella finestra KVM, fare clic su Virtual Media (supporti virtuali).
2. Fare clic su Activate Virtual Devices.
3. Se viene richiesto di accettare una sessione KVM non crittografata, accettarla secondo necessità.
4. Fare clic su Virtual Media e selezionare Map CD/DVD (Mappa CD/DVD).
5. Accedere al file di immagine ISO del programma di installazione di ESXi e fare clic su Open (Apri).
6. Fare clic su Map Device (Connetti dispositivo)
7. Fare clic sulla scheda KVM per monitorare l'avvio del server.

Installare ESXi

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per installare VMware ESXi sul LUN avviabile iSCSI degli host, attenersi alla seguente procedura per ciascun host:

1. Avviare il server selezionando Boot Server e facendo clic su OK. Quindi fare nuovamente clic su OK.
2. Al riavvio, il computer rileva la presenza del supporto di installazione ESXi. Selezionare il programma di installazione di ESXi dal menu di avvio visualizzato.
3. Al termine del caricamento del programma di installazione, premere Invio per continuare l'installazione.
4. Leggere e accettare il contratto di licenza con l'utente finale (EULA). Premere F11 per accettare e continuare.
5. Selezionare il LUN precedentemente configurato come disco di installazione per ESXi e premere Invio per continuare l'installazione.
6. Selezionare il layout di tastiera appropriato e premere Invio.
7. Inserire e confermare la password root e premere Invio.
8. Il programma di installazione visualizza un avviso che indica che il disco selezionato verrà ripartizionato. Premere F11 per continuare l'installazione.
9. Al termine dell'installazione, selezionare la scheda Virtual Media (supporti virtuali) e deselezionare il segno P accanto al supporto di installazione ESXi. Fare clic su Sì.



L'immagine di installazione di ESXi deve essere dismappata per assicurarsi che il server si riavvii in ESXi e non nel programma di installazione.

10. Al termine dell'installazione, premere Invio per riavviare il server.
11. In Cisco UCS Manager, associare il profilo di servizio corrente al modello di profilo di servizio non vMedia per impedire il montaggio dell'iso di installazione di ESXi su HTTP.

Configurare la rete di gestione per gli host ESXi

Per la gestione dell'host è necessario aggiungere una rete di gestione per ciascun host VMware. Per aggiungere una rete di gestione per gli host VMware, completare i seguenti passaggi su ciascun host ESXi:

ESXi host VM-host-Infra-01 e VM-host-Infra-02

Per configurare ciascun host ESXi con accesso alla rete di gestione, attenersi alla seguente procedura:

1. Una volta riavviato il server, premere F2 per personalizzare il sistema.
2. Accedere come `root`, Inserire la password corrispondente e premere Invio per accedere.
3. Selezionare Opzioni di risoluzione dei problemi e premere Invio.
4. Selezionare Enable ESXi Shell (attiva shell ESXi) e premere Invio.
5. Selezionare Enable SSH (attiva SSH) e premere Invio.
6. Premere Esc per uscire dal menu delle opzioni di risoluzione dei problemi.
7. Selezionare l'opzione Configure Management Network (Configura rete di gestione) e premere Invio.
8. Selezionare Network Adapter (adattatori di rete) e premere Invio.
9. Verificare che i numeri nel campo etichetta hardware corrispondano ai numeri nel campo Nome periferica.
10. Premere Invio.

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 checked="" type="checkbox"/> vmnic0	Site-01-vNIC-A (...00:0a:2e)	Connected (...)
<input checked="" type="checkbox"/> vmnic1	Site-01-vNIC-B (...00:0b:2e)	Connected (...)
<input type="checkbox"/> vmnic2	Site-01-ISC... (...00:0a:3e)	Connected (...)
<input type="checkbox"/> vmnic3	Site-01-ISC... (...00:0b:3e)	Connected (...)

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

11. Selezionare l'opzione VLAN (opzionale) e premere Invio.
12. Inserire il <ib-mgmt-vlan-id> E premere Invio.
13. Selezionare IPv4 Configuration (Configurazione IPv4) e premere Invio.
14. Selezionare l'opzione Set Static IPv4 Address (Imposta indirizzo IPv4 statico) e Network Configuration (Configurazione di rete) utilizzando la barra spaziatrice.
15. Inserire l'indirizzo IP per la gestione del primo host ESXi.
16. Inserire la subnet mask del primo host ESXi.
17. Immettere il gateway predefinito per il primo host ESXi.
18. Premere Invio per accettare le modifiche apportate alla configurazione IP.
19. Selezionare l'opzione Configurazione DNS e premere Invio.



Poiché l'indirizzo IP viene assegnato manualmente, le informazioni DNS devono essere inserite anche manualmente.

20. Inserire l'indirizzo IP del server DNS primario.
21. Facoltativo: Inserire l'indirizzo IP del server DNS secondario.
22. Inserire l'FQDN per il primo host ESXi.
23. Premere Invio per accettare le modifiche apportate alla configurazione DNS.
24. Premere Esc per uscire dal menu Configure Management Network (Configura rete di gestione).
25. Selezionare Test Management Network (Test rete di gestione) per verificare che la rete di gestione sia configurata correttamente e premere Invio.
26. Premere Invio per eseguire il test, premere nuovamente Invio una volta completato il test, esaminare l'ambiente in caso di errore.
27. Selezionare nuovamente Configure Management Network (Configura rete di gestione) e premere Invio.

28. Selezionare l'opzione IPv6 Configuration (Configurazione IPv6) e premere Invio.
29. Utilizzando la barra spaziatrice, selezionare Disable IPv6 (Restart required) (Disattiva IPv6 (riavvio richiesto) e premere Invio.
30. Premere Esc per uscire dal sottomenu Configure Management Network (Configura rete di gestione).
31. Premere Y per confermare le modifiche e riavviare l'host ESXi.

Reset VMware ESXi host VMkernel port vmk0 MAC address (opzionale)

ESXi host VM-host-Infra-01 e VM-host-Infra-02

Per impostazione predefinita, l'indirizzo MAC della porta VMkernel vmk0 di gestione corrisponde all'indirizzo MAC della porta Ethernet su cui è posizionata. Se il LUN di avvio dell'host ESXi viene rimappato a un server diverso con indirizzi MAC diversi, si verifica un conflitto di indirizzi MAC perché vmk0 conserva l'indirizzo MAC assegnato, a meno che la configurazione del sistema ESXi non venga reimpostata. Per reimpostare l'indirizzo MAC di vmk0 su un indirizzo MAC assegnato da VMware casuale, attenersi alla seguente procedura:

1. Dalla schermata principale del menu della console ESXi, premere Ctrl-Alt-F1 per accedere all'interfaccia della riga di comando della console VMware. In UCSM KVM, Ctrl-Alt-F1 viene visualizzato nell'elenco delle macro statiche.
2. Accedere come root.
3. Tipo `esxcfg-vmknic -l` per ottenere un elenco dettagliato dell'interfaccia vmk0. Vmk0 deve far parte del gruppo di porte della rete di gestione. Annotare l'indirizzo IP e la netmask di vmk0.
4. Per rimuovere vmk0, immettere il seguente comando:

```
esxcfg-vmknic -d "Management Network"
```

5. Per aggiungere nuovamente vmk0 con un indirizzo MAC casuale, immettere il seguente comando:

```
esxcfg-vmknic -a -i <vmk0-ip> -n <vmk0-netmask> "Management Network".
```

6. Verificare che vmk0 sia stato aggiunto nuovamente con un indirizzo MAC casuale

```
esxcfg-vmknic -l
```

7. Tipo `exit` per disconnettersi dall'interfaccia della riga di comando.
8. Premere Ctrl-Alt-F2 per tornare all'interfaccia del menu della console ESXi.

Accedere agli host VMware ESXi con il client host VMware

ESXi host VM-host-Infra-01

Per accedere all'host VM-host-Infra-01 ESXi utilizzando VMware host Client, attenersi alla seguente procedura:

1. Aprire un browser Web sulla workstation di gestione e accedere a `VM-Host-Infra-01` Indirizzo IP di gestione.

2. Fare clic su Open the VMware host Client (Apri client host VMware).
3. Invio `root` per il nome utente.
4. Inserire la password `root`.
5. Fare clic su Login (accesso) per connettersi.
6. Ripetere questa procedura per accedere a `VM-Host-Infra-02` in una scheda o in una finestra separata del browser.

Installazione dei driver VMware per Cisco Virtual Interface Card (VIC)

Scaricare ed estrarre il bundle offline per il seguente driver VMware VIC sulla workstation di gestione:

- Driver Nenic versione 1.0.25.0

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per installare i driver VMware VIC sugli host ESXi VM-host-Infra-01 e VM-host-Infra-02, attenersi alla seguente procedura:

1. Da ciascun client host, selezionare Storage (archiviazione).
2. Fare clic con il pulsante destro del mouse su `datastore1` e selezionare Browse (Sfogliare).
3. Nel browser Datastore, fare clic su Upload (carica).
4. Individuare la posizione salvata per i driver VIC scaricati e selezionare `VMW-ESX-6.7.0-nenic-1.0.25.0-offline_bundle-11271332.zip`.
5. Nel browser Datastore, fare clic su Upload (carica).
6. Fare clic su Open (Apri) per caricare il file nel `datastore1`.
7. Assicurarsi che il file sia stato caricato su entrambi gli host ESXi.
8. Impostare ciascun host in modalità di manutenzione, se non lo è già.
9. Connettersi a ciascun host ESXi tramite ssh da una connessione shell o da un terminale putty.
10. Accedere come `root` con la password `root`.
11. Eseguire i seguenti comandi su ciascun host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. Una volta completato il riavvio, accedere al client host su ciascun host e uscire dalla modalità di manutenzione.

Configurare le porte VMkernel e lo switch virtuale

ESXi host VM-host-Infra-01 e VM-host-Infra-02

Per configurare le porte VMkernel e gli switch virtuali sugli host ESXi, attenersi alla seguente procedura:

1. Dal client host, selezionare Networking (rete) a sinistra.

2. Nel riquadro centrale, selezionare la scheda Virtual switches (interruttori virtuali).
3. Selezionare vSwitch0.
4. Selezionare Modifica impostazioni.
5. Impostare la MTU su 9000.
6. Espandere il raggruppamento NIC.
7. Nella sezione Ordine di failover, selezionare vmnic1 e fare clic su Contrassegna attivo.
8. Verificare che vmnic1 abbia ora lo stato attivo.
9. Fare clic su Salva.
10. Selezionare Networking (rete) a sinistra.
11. Nel riquadro centrale, selezionare la scheda Virtual switches (interruttori virtuali).
12. Selezionare iScsiBootvSwitch.
13. Selezionare Modifica impostazioni.
14. Impostare la MTU su 9000
15. Fare clic su Salva.
16. Selezionare la scheda NIC VMkernel.
17. Selezionare vmk1 iScsiBootPG.
18. Selezionare Modifica impostazioni.
19. Impostare la MTU su 9000.
20. Espandere le impostazioni IPv4 e modificare l'indirizzo IP in un indirizzo esterno a UCS iSCSI-IP-Pool-A.



Per evitare conflitti di indirizzi IP se gli indirizzi del pool IP iSCSI Cisco UCS devono essere riassegnati, si consiglia di utilizzare indirizzi IP diversi nella stessa subnet per le porte VMkernel iSCSI.

21. Fare clic su Salva.
22. Selezionare la scheda Virtual switches (interruttori virtuali).
23. Selezionare Add standard virtual switch (Aggiungi switch virtuale standard).
24. Specificare un nome di iScsciBootvSwitch-B Per il nome vSwitch.
25. Impostare MTU su 9000.
26. Selezionare vmnic3 dal menu a discesa Uplink 1.
27. Fare clic su Aggiungi.
28. Nel riquadro centrale, selezionare la scheda NIC VMkernel.
29. Selezionare Add VMkernel NIC (Aggiungi NIC VMkernel)
30. Specificare un nuovo nome di gruppo di porte di iScsiBootPG-B.
31. Selezionare iScsciBootvSwitch-B per Virtual Switch.
32. Impostare MTU su 9000. Non inserire un ID VLAN.
33. Selezionare Static (statico) per le impostazioni IPv4 ed espandere l'opzione per fornire l'indirizzo e la subnet mask all'interno della configurazione.



Per evitare conflitti di indirizzi IP, se gli indirizzi del pool IP iSCSI Cisco UCS devono essere riassegnati, si consiglia di utilizzare indirizzi IP diversi nella stessa subnet per le porte VMkernel iSCSI.

34. Fare clic su Crea.
35. A sinistra, selezionare rete, quindi selezionare la scheda gruppi di porte.
36. Nel riquadro centrale, fare clic con il pulsante destro del mouse su rete VM e selezionare Rimuovi.
37. Fare clic su Remove (Rimuovi) per completare la rimozione del gruppo di porte.
38. Nel riquadro centrale, selezionare Add port group (Aggiungi gruppo di porte).
39. Assegnare un nome al gruppo di porte Management Network (rete di gestione) e immettere `<ib-mgmt-vlan-id>` Nel campo VLAN ID (ID VLAN) e assicurarsi che sia selezionato Virtual switch vSwitch0 (interruttore virtuale vSwitch0).
40. Fare clic su Add (Aggiungi) per finalizzare le modifiche per la rete IB-MGMT.
41. Nella parte superiore, selezionare la scheda NIC VMkernel.
42. Fare clic su Add VMkernel NIC.
43. Per nuovo gruppo di porte, immettere VMotion.
44. Per Virtual switch, selezionare vSwitch0 Selected (vSwitch0 selezionato).
45. Invio `<vmotion-vlan-id>` Per l'ID VLAN.
46. Impostare la MTU su 9000.
47. Selezionare Static IPv4 settings (Impostazioni IPv4 statiche) ed espandere IPv4 settings (Impostazioni IPv4).
48. Inserire l'indirizzo IP e la netmask dell'host ESXi vMotion.
49. Selezionare lo stack TCP/IP vMotion.
50. Selezionare vMotion in servizi.
51. Fare clic su Crea.
52. Fare clic su Add VMkernel NIC.
53. Per nuovo gruppo di porte, immettere NFS_Share.
54. Per Virtual switch, selezionare vSwitch0 Selected (vSwitch0 selezionato).
55. Invio `<infra-nfs-vlan-id>` Per l'ID VLAN.
56. Impostare la MTU su 9000.
57. Selezionare Static IPv4 settings (Impostazioni IPv4 statiche) ed espandere IPv4 settings (Impostazioni IPv4).
58. Immettere l'indirizzo IP e la netmask NFS dell'infrastruttura host ESXi.
59. Non selezionare nessuno dei servizi.
60. Fare clic su Crea.
61. Selezionare la scheda Virtual Switches (interruttori virtuali), quindi vSwitch0. Le proprietà delle NIC VMkernel vSwitch0 devono essere simili al seguente esempio:

vSwitch0

Add uplink | Edit settings | Refresh | Actions

vSwitch0
 Type: Standard vSwitch
 Port groups: 4
 Uplinks: 2

vSwitch Details

MTU	SC00
Ports	8816 (8798 available)
Link discovery	Listen + Cisco discovery protocol (CDP)
Attached VMs	2 (1 active)
Beacon interval	1

NIC teaming policy

Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Fallback	Yes

Security policy

Allow promiscuous mode	No
Allow forged transmits	Yes
Allow MAC changes	Yes

Shaping policy

Enabled	No
---------	----

vSwitch topology

VM Network
 VLAN ID: 18
 Virtual Machines (2)
 vCenterServerApp-01
 MAC Address 00:0c:29:27:48:61
 Linux-VM

VMotion
 VLAN ID: 103
 VMkernel ports (1)
 vmk4: 192.168.103.208

NFS_Share
 VLAN ID: 104
 VMkernel ports (1)
 vmk3: 192.168.104.208

Management network
 VLAN ID: 18
 VMkernel ports (1)
 vmk0: 172.18.7.208

Physical adapters
 vmnic1: 10000 Mbps, Full
 vmnic0: 10000 Mbps, Full

62. Selezionare la scheda NIC VMkernel per confermare gli adattatori virtuali configurati. Gli adattatori elencati devono essere simili al seguente esempio:

localhost.localdomain - Networking

Port groups | Virtual switches | Physical NICs | **VMkernel NICs** | TCP/IP stacks | Firewall rules

Add VMkernel NIC | Edit settings | Refresh | Actions

Search

Name	Portgroup	TCP/IP stack	Services	IPv4 ad...	IPv6 addresses
vmk0	Management Network	Default TCP/IP stack	Management	172.18.7...	fe80::225:b5ff:fe00:a2e/64
vmk1	iScsiBootPG	Default TCP/IP stack		192.168...	fe80::225:b5ff:fe00:a3e/64
vmk2	iScsiBootPG-B	Default TCP/IP stack		192.168...	fe80::250:56ff:fe64:1248...
vmk3	NFS_Share	Default TCP/IP stack		192.168...	fe80::250:56ff:fe65:29a4...
vmk4	VMotion	Default TCP/IP stack	vMotion	192.168...	fe80::250:56ff:fe6c:2650...

5 items

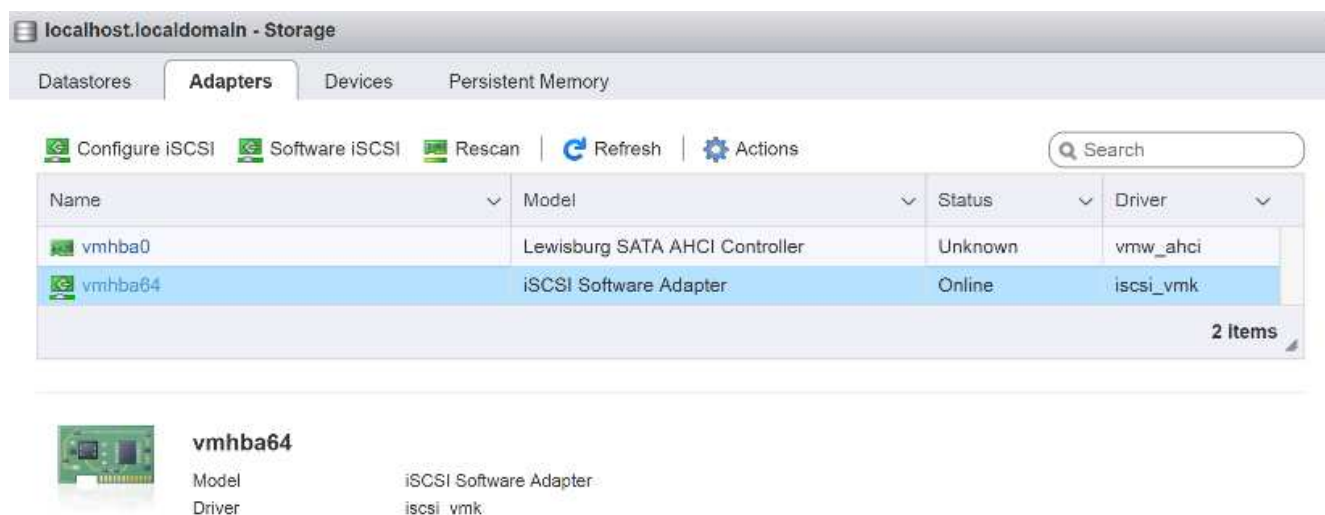
Configurare il multipathing iSCSI

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per configurare il multipathing iSCSI sull'host ESXi VM-host-Infra-01 e VM-host-Infra-02, attenersi alla seguente procedura:

1. Da ciascun client host, selezionare Storage (archiviazione) a sinistra.

2. Nel riquadro centrale, fare clic su adattatori.
3. Selezionare l'adattatore software iSCSI e fare clic su Configure iSCSI (Configura iSCSI).



4. In Dynamic Targets (destinazioni dinamiche), fare clic su Add Dynamic target (Aggiungi destinazione dinamica).
5. Immettere l'indirizzo IP di `iscsi_lif01a`.
6. Ripetere l'immissione di questi indirizzi IP: `iscsi_lif01b`, `iscsi_lif02a`, e `iscsi_lif02b`.
7. Fare clic su Salva configurazione.

Configure iSCSI - vmhba64

iSCSI enabled: ☐ Disabled ☒ Enabled

Name & alias: iqn.1992-08.com.cisco:ucs-host:3

CHAP authentication: Do not use CHAP

Mutual CHAP authentication: Do not use CHAP

Advanced settings: Click to expand

Network port bindings:

Add port binding Remove port binding

VMkernel NIC Port group IPv4 address

No port bindings

Static targets:

Add static target Remove static target Edit settings Search

Target	Address	Port
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.124.3	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.124.1	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.125.3	3260
iqn.1992-08.com.netapp:sn.aff300:vs.3	192.168.125.1	3260

Dynamic targets:

Add dynamic target Remove dynamic target Edit settings Search

Address	Port
192.168.124.1	3260
192.168.125.1	3260
192.168.125.3	3260

Save configuration Cancel

Per ottenere tutti i `iscsi_lif` indirizzi IP, accedere all'interfaccia di gestione del cluster di storage NetApp ed eseguire `network interface show` comando.



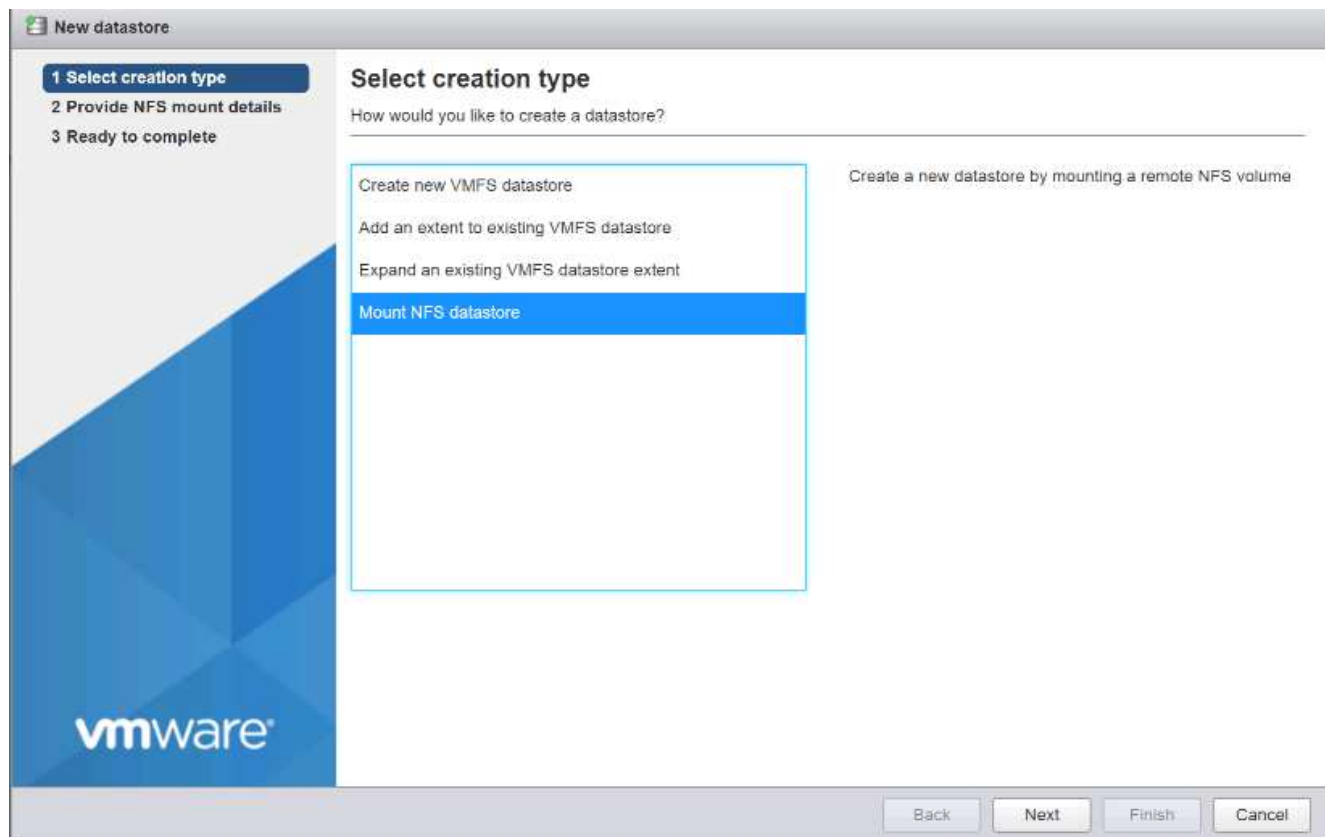
L'host esegue automaticamente una nuova scansione dell'adattatore di storage e le destinazioni vengono aggiunte a destinazioni statiche.

Montare gli archivi dati richiesti

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

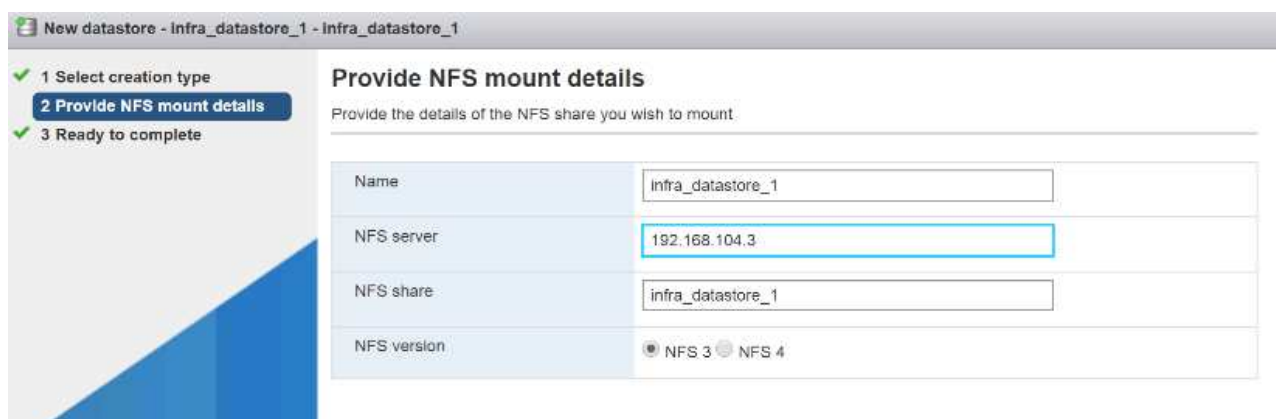
Per montare gli archivi dati richiesti, completare la seguente procedura su ciascun host ESXi:

1. Dal client host, selezionare Storage (archiviazione) a sinistra.
2. Nel riquadro centrale, selezionare Datastore.
3. Nel riquadro centrale, selezionare New Datastore (nuovo archivio dati) per aggiungere un nuovo archivio dati.
4. Nella finestra di dialogo nuovo datastore, selezionare Mount NFS datastore (Installa datastore NFS) e fare clic su Next (Avanti).



5. Nella pagina fornire dettagli sul montaggio NFS, completare la seguente procedura:

- a. Invio `infra_datastore_1` per il nome del datastore.
- b. Inserire l'indirizzo IP di `nfs_lif01_a` LIF per il server NFS.
- c. Invio `/infra_datastore_1` Per la condivisione NFS.
- d. Lasciare la versione di NFS impostata su NFS 3.
- e. Fare clic su Avanti.



6. Fare clic su fine. Il datastore dovrebbe ora apparire nell'elenco datastore.
7. Nel riquadro centrale, selezionare New Datastore (nuovo archivio dati) per aggiungere un nuovo archivio dati.
8. Nella finestra di dialogo New Datastore (nuovo archivio dati), selezionare Mount NFS Datastore (monta archivio dati NFS) e fare clic su Next (Avanti).

9. Nella pagina fornire dettagli sul montaggio NFS, completare la seguente procedura:
 - a. Invio `infra_datastore_2` per il nome del datastore.
 - b. Inserire l'indirizzo IP di `nfs_lif02_a` LIF per il server NFS.
 - c. Invio `/infra_datastore_2` Per la condivisione NFS.
 - d. Lasciare la versione di NFS impostata su NFS 3.
 - e. Fare clic su Avanti.
10. Fare clic su fine. Il datastore dovrebbe ora apparire nell'elenco datastore.

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin provision...	Access
datastore1	Non-SSD	7.5 GB	3.95 GB	3.55 GB	VMFS6	Supported	Single
infra_datastore_1	Unknown	500 GB	37.19 GB	462.81 GB	NFS	Supported	Single
infra_datastore_2	Unknown	500 GB	60.79 GB	439.21 GB	NFS	Supported	Single

11. Montare entrambi i datastore su entrambi gli host ESXi.

Configurare NTP sugli host ESXi

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per configurare NTP sugli host ESXi, completare i seguenti passaggi su ciascun host:

1. Dal client host, selezionare Manage (Gestisci) a sinistra.
2. Nel riquadro centrale, selezionare la scheda Time & Date (Data e ora).
3. Fare clic su Modifica impostazioni.
4. Assicurarsi che l'opzione Use Network Time Protocol (Enable NTP client) (Usa protocollo orario di rete (attiva client NTP) sia selezionata.
5. Utilizzare il menu a discesa per selezionare Start and Stop with host (Avvia e arresta con host).
6. Inserire i due indirizzi NTP dello switch Nexus nella casella Server NTP separati da una virgola.

Edit time configuration

Specify how the date and time of this host should be set.

☒ Manually configure the date and time on this host

10/13/2016 4:09 PM

☐ Use Network Time Protocol (enable NTP client)

NTP service startup policy: Start and stop with host

NTP servers: 10.1.156.4,10.1.156.5

Separate servers with commas, e.g. 10.31.21.2, fe00::2800

Save Cancel

7. Fare clic su Save (Salva) per salvare le modifiche di configurazione.
8. Selezionare Actions (azioni) > NTP service (Servizio NTP) > Start (Avvio)
9. Verificare che il servizio NTP sia in esecuzione e che l'orologio sia impostato approssimativamente sull'ora corretta



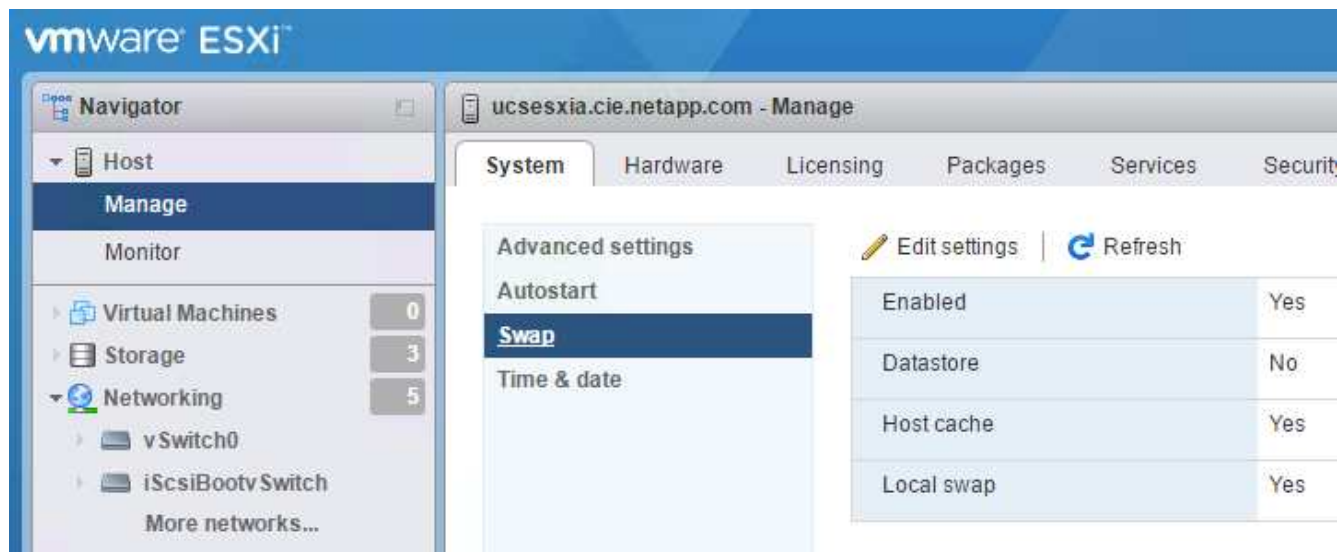
L'ora del server NTP potrebbe variare leggermente rispetto all'ora dell'host.

Configurare lo swap host ESXi

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

Per configurare lo swap degli host sugli host ESXi, attenersi alla seguente procedura per ciascun host:

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



2. Fare clic su Modifica impostazioni. Selezionare `infra_swap` Dalle opzioni Datastore.



3. Fare clic su Salva.

Installare il plug-in NetApp NFS 1.1.2 per VMware VAAI

Per installare il plug-in NetApp NFS 1. 1.2 per VMware VAAI, completare i seguenti passaggi.

1. Scarica il plug-in NetApp NFS per VMware VAAI:
 - a. Accedere alla "[Pagina di download del software NetApp](#)".
 - b. Scorrere verso il basso e fare clic su NetApp NFS Plug-in for VMware VAAI.
 - c. Selezionare la piattaforma ESXi.
 - d. Scarica il bundle offline (.zip) o il bundle online (.vib) del plug-in più recente.
2. Il plug-in NetApp NFS per VMware VAAI è in attesa di qualifica IMT con ONTAP 9.5 e i dettagli sull'interoperabilità saranno presto pubblicati su NetApp IMT.
3. Installare il plug-in sull'host ESXi utilizzando ESX CLI.
4. Riavviare l'host ESXi.

Installare VMware vCenter Server 6.7

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

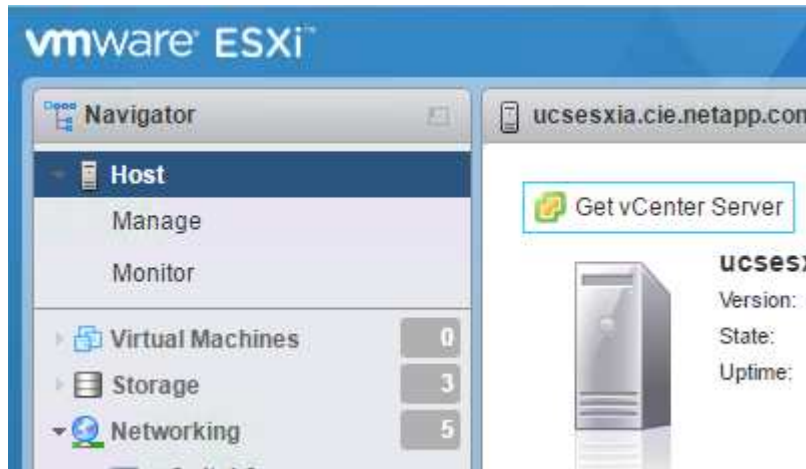


FlexPod utilizza l'appliance server vCenter (VCSA).

Installare l'appliance server VMware vCenter

Per installare 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.

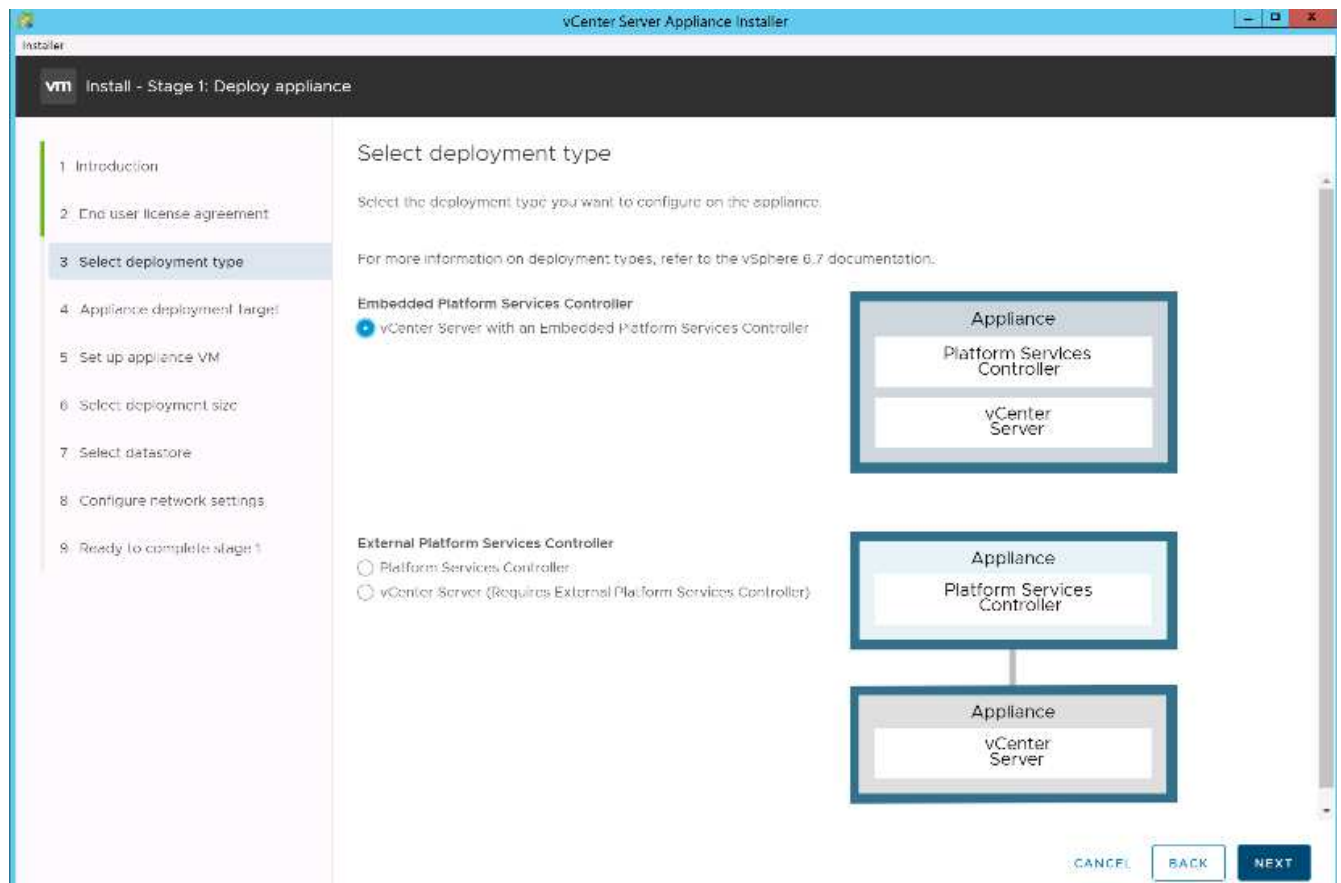


2. Scaricare VCSA dal sito VMware.



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

3. Montare l'immagine ISO.
4. Passare a `vcса-ui-installer > win32 directory`. Fare doppio clic `installer.exe`.
5. Fare clic su Installa.
6. Fare clic su Avanti nella pagina Introduzione.
7. Accettare l'EULA.
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. Nella pagina Appliance Deployment Target, immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root. Fare clic su Avanti.

Installer vCenter Server Appliance Installer

vm Install - Stage 1: Deploy appliance

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: 172.18.7.208 ⓘ

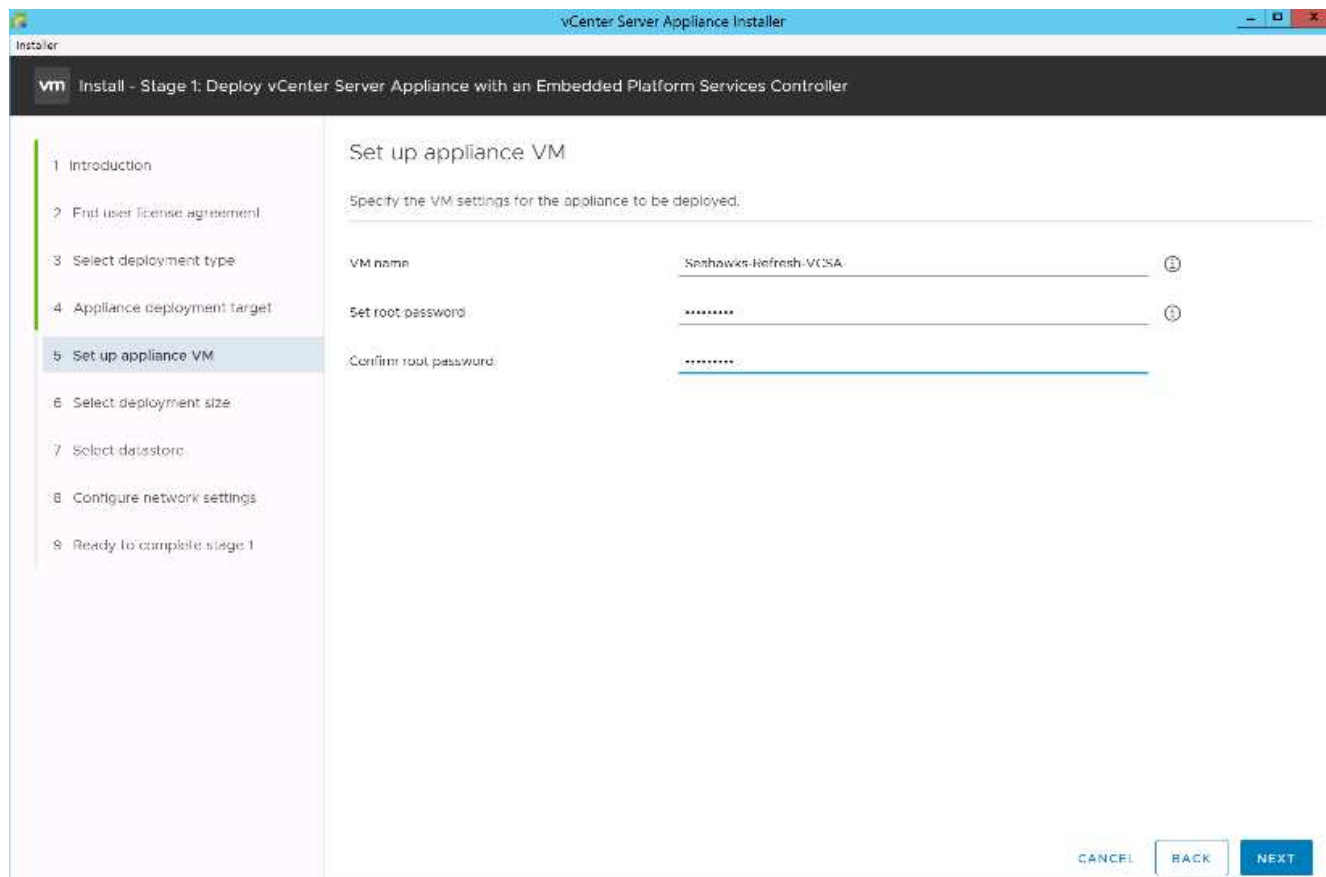
HTTPS port: 443

User name: root ⓘ

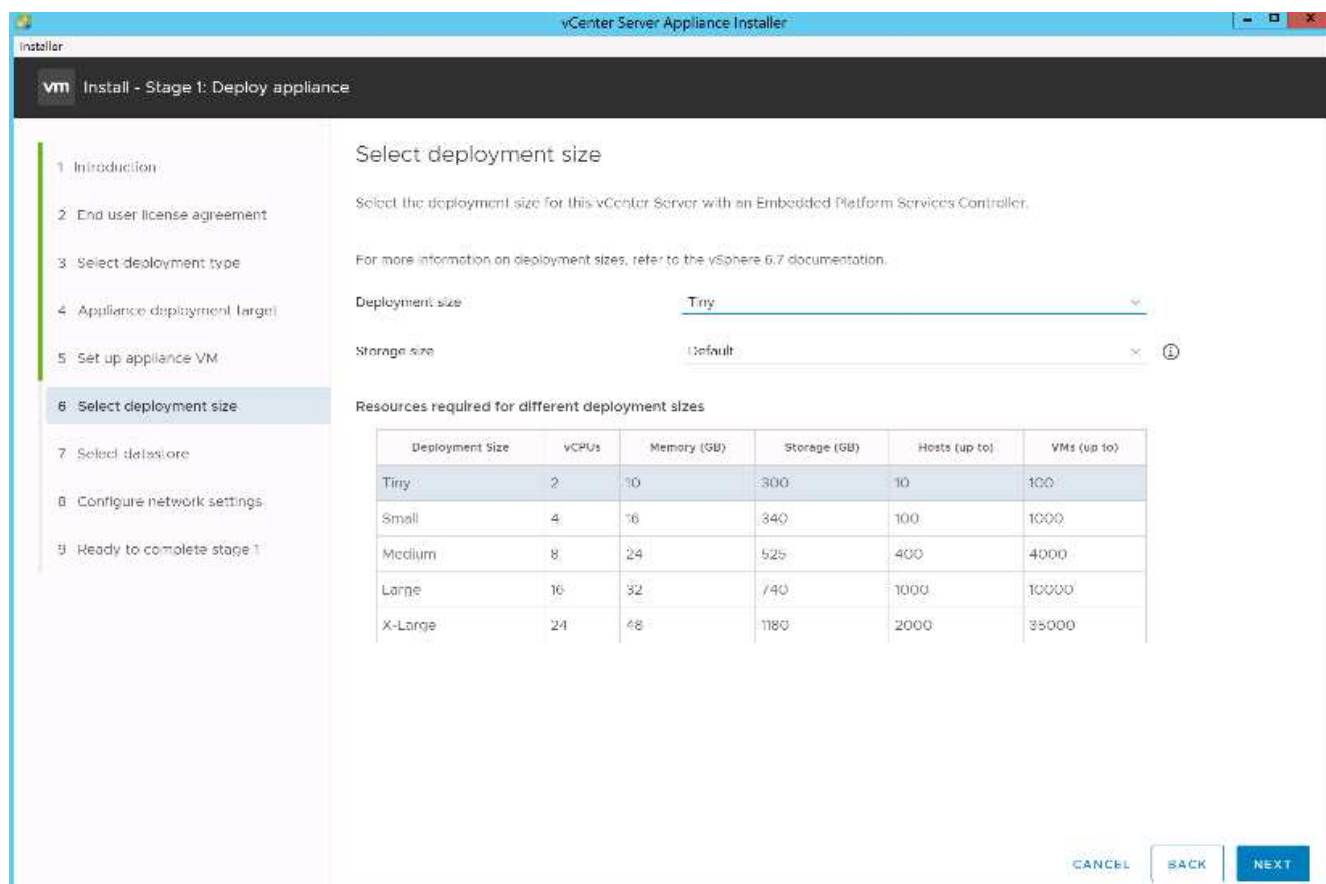
Password:

CANCEL BACK NEXT

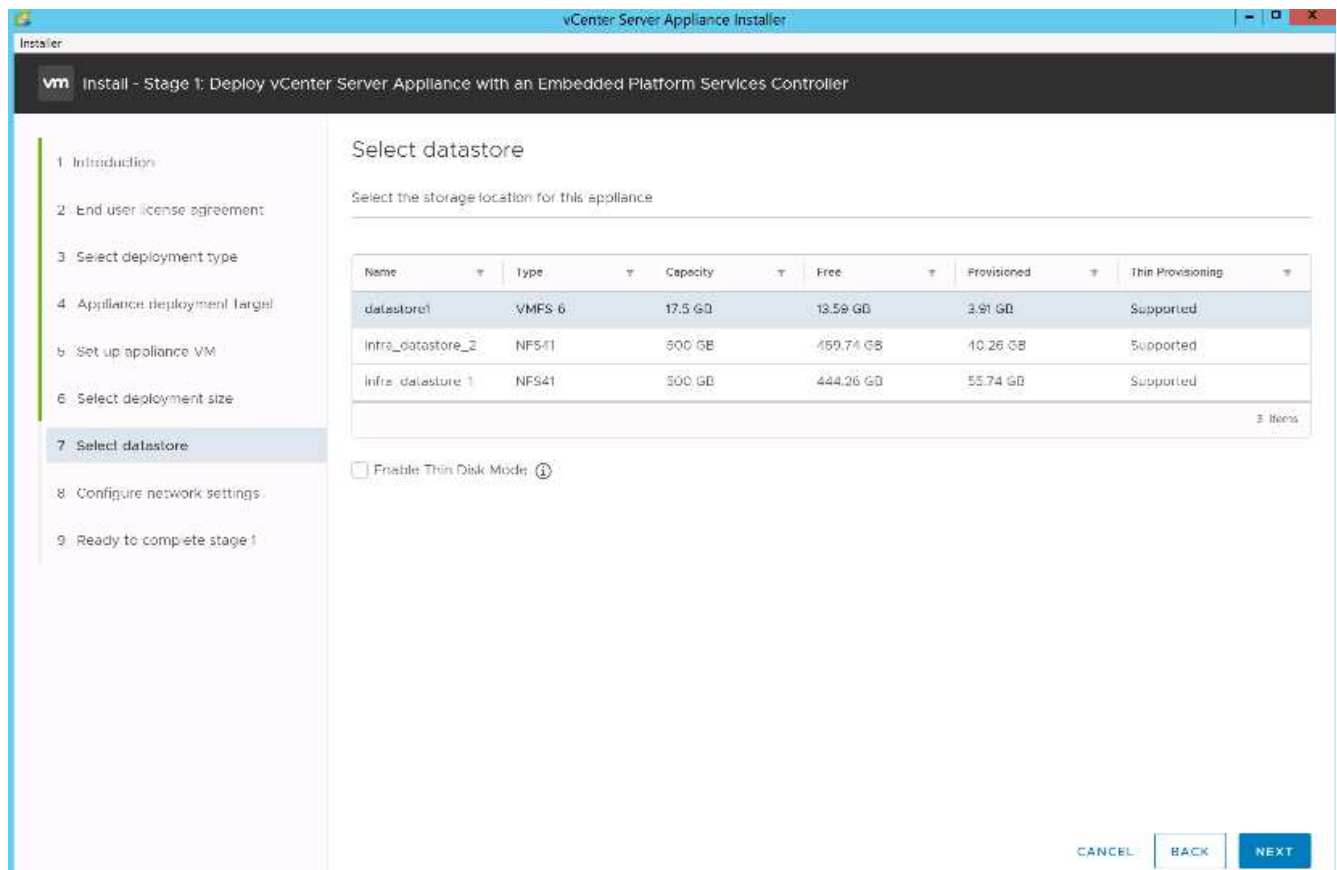
10. Impostare la macchina virtuale dell'appliance immettendo VCSA come nome della macchina virtuale e password root che si desidera utilizzare per VCSA. Fare clic su Avanti.



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

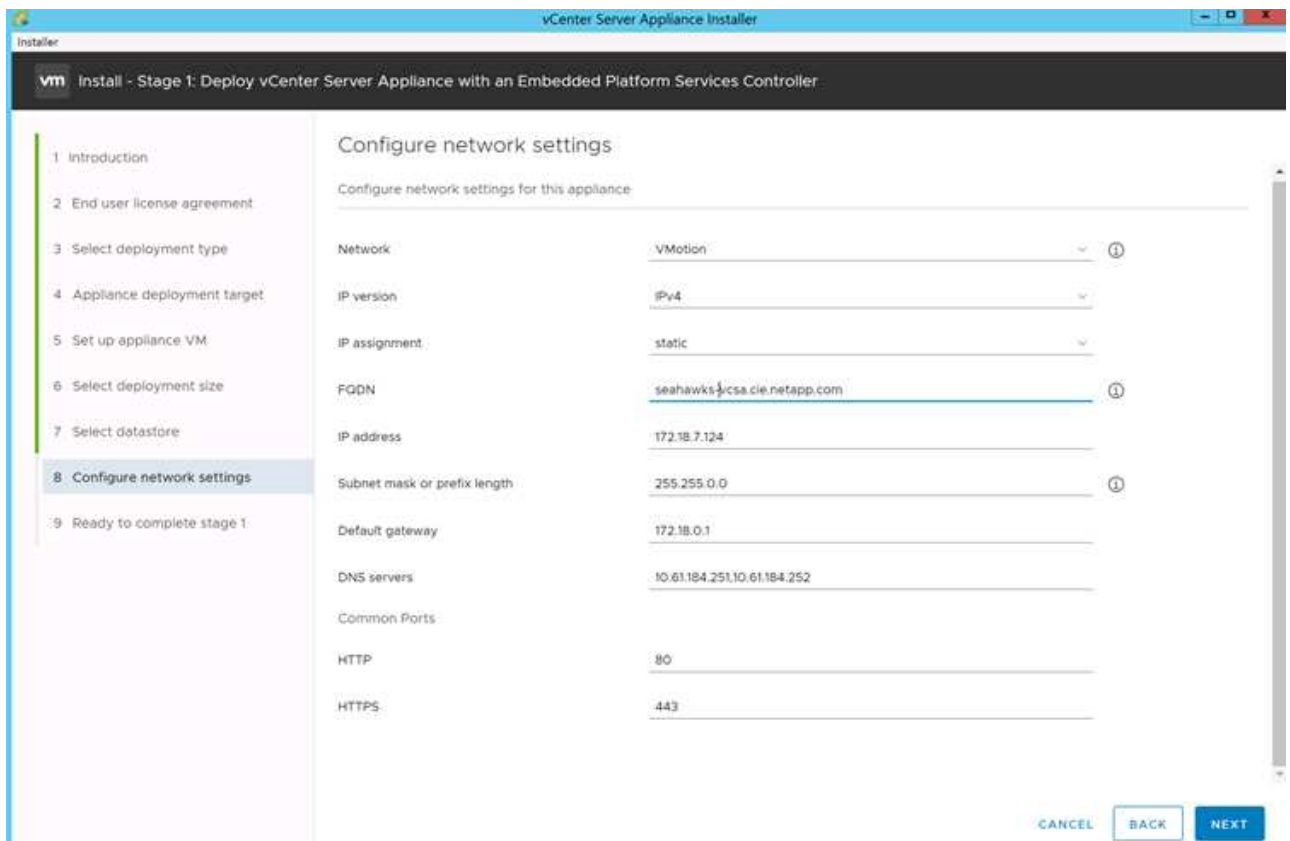


12. Selezionare infra_datastore_1 datastore. Fare clic su Avanti.



13. Inserire le seguenti informazioni nella pagina Configure Network Settings (Configura impostazioni di rete) e fare clic su Next (Avanti).

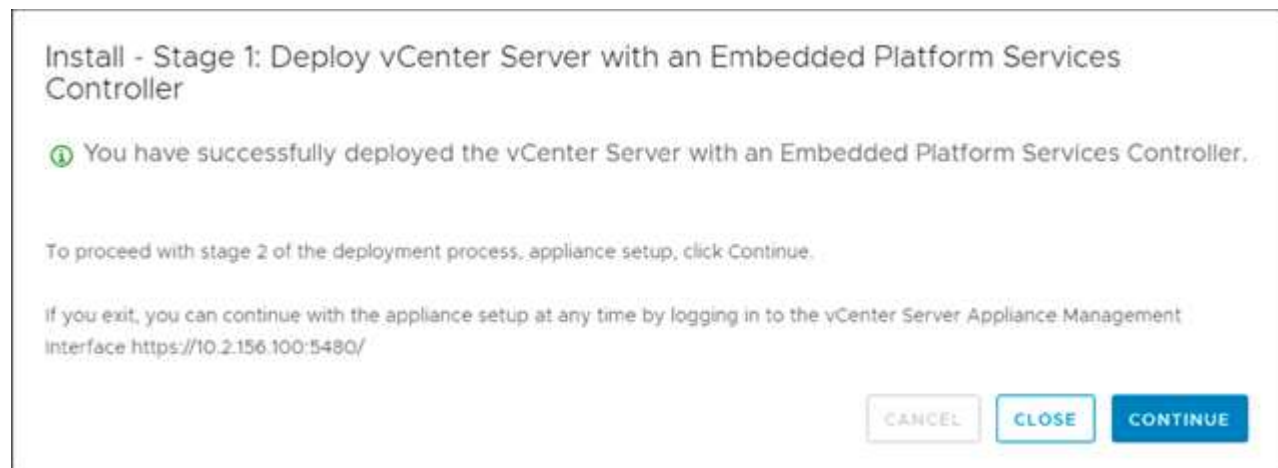
- Selezionare MGMT-Network come rete.
- Inserire l'FQDN o l'IP da utilizzare per VCSA.
- Inserire l'indirizzo IP da utilizzare.
- Inserire la subnet mask da utilizzare.
- Inserire il gateway predefinito.
- Inserire il server DNS.



14. Nella pagina Pronto per completare la fase 1, verificare che le impostazioni immesse siano corrette. Fare clic su fine.

VCSA viene installato ora. Questo processo richiede alcuni minuti.

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



16. Nella pagina Introduzione alla fase 2, fare clic su Avanti.
17. Invio <<var_ntp_id>> Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.

Se si intende utilizzare la disponibilità elevata di vCenter Server, assicurarsi che l'accesso SSH sia attivato.

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

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

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

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

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



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

Configurare il clustering di VMware vCenter Server 6.7 e vSphere

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

1. Accedere a <https://<FQDN or IP of vCenter>/vsphere-client/>.
2. Fare clic su Launch vSphere Client.
3. Accedere con il nome utente administrator@vsphere.local e la password SSO immessa durante la procedura di configurazione 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. Selezionare e attivare le opzioni DRS e vSphere ha.
4. Fare clic su OK.

Name	Express
Location	Flexpod_SeaHawks
DRS	<input checked="" type="checkbox"/>
vSphere HA	<input checked="" type="checkbox"/>
vSAN	<input type="checkbox"/>

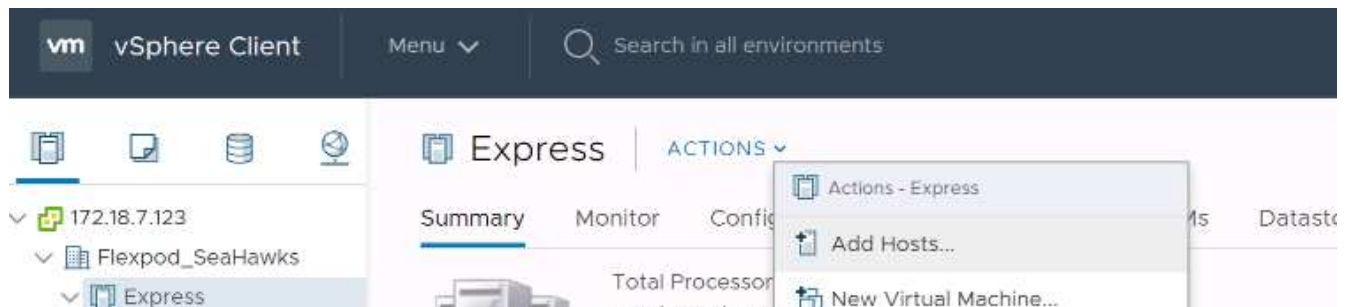
These services will have default settings - these can be changed later in the Cluster Quickstart workflow.

CANCEL OK

Aggiungere host ESXi al cluster

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

1. Selezionare Add host (Aggiungi host) nel menu Actions (azioni) del cluster.



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



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

- f. Fare clic su Next (Avanti) per disattivare la modalità di blocco.
- g. Fare clic su Next (Avanti) nella pagina VM location (posizione macchina virtuale).

h. Consultare la pagina Pronto per il completamento. Utilizzare il pulsante Indietro per apportare eventuali modifiche o selezionare fine.

3. Ripetere i passaggi 1 e 2 per l'host Cisco UCS B.

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

Configurare il coredump sugli host ESXi

ESXi Dump Collector Setup per host con avvio iSCSI

Gli host ESXi avviati con iSCSI utilizzando VMware iSCSI Software Initiator devono essere configurati per eseguire i core dump sul Dump Collector ESXi che fa parte di vCenter. Dump Collector non è attivato per impostazione predefinita su vCenter Appliance. Questa procedura deve essere eseguita alla fine della sezione relativa all'implementazione di vCenter. Per configurare ESXi Dump Collector, attenersi alla seguente procedura:

1. Accedere a vSphere Web Client come administrator@vsphere.local e selezionare Home.
2. Nel riquadro centrale, fare clic su Configurazione di sistema.
3. Nel riquadro di sinistra, selezionare servizi.
4. In servizi, fare clic su VMware vSphere ESXi Dump Collector.
5. Nel riquadro centrale, fare clic sull'icona verde di avvio per avviare il servizio.
6. Nel menu azioni, fare clic su Modifica tipo di avvio.
7. Selezionare Automatic (automatico).
8. Fare clic su OK.
9. Connettersi a ciascun host ESXi utilizzando ssh come root.
10. Eseguire i seguenti comandi:

```
esxcli system coredump network set -v vmk0 -j <vcenter-ip>
esxcli system coredump network set -e true
esxcli system coredump network check
```

Il messaggio `Verified the configured netdump server is running` viene visualizzato dopo aver eseguito il comando finale.



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

Conclusione

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 aggiuntivi, FlexPod può essere personalizzato in base alle specifiche esigenze aziendali. FlexPod Express è stato progettato tenendo conto delle piccole e medie imprese, delle ROBOs e di altre aziende che richiedono soluzioni dedicate.

Ulteriori informazioni

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

- NVA- 1130-DESIGN: FlexPod Express con VMware vSphere 6.7U1 e NetApp AFF A220 con NVA storage basato su IP direct-attached

["https://www.netapp.com/us/media/nva-1130-design.pdf"](https://www.netapp.com/us/media/nva-1130-design.pdf)

- Centro di documentazione per sistemi AFF e FAS

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

- Centro documentazione di ONTAP 9

["http://docs.netapp.com/ontap-9/index.jsp"](http://docs.netapp.com/ontap-9/index.jsp)

- Documentazione sui prodotti NetApp

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

FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e NetApp AFF/FAS - NVA - implementazione

Jyh-ishing Chen, NetApp

La soluzione FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e NetApp AFF/FAS sfrutta Cisco UCS Mini con server blade B200 M5, Cisco UCS 6324 in-chassis Fabric Interconnect, switch Cisco Nexus 31108PC-V o altri switch compatibili e la coppia di controller ha NetApp AFF A220, C190 o FAS2700, Che esegue il software di gestione dei dati NetApp ONTAP 9.7. Questo documento sull'implementazione dell'architettura verificata di NetApp fornisce le procedure dettagliate necessarie per configurare i componenti dell'infrastruttura e per implementare VMware vSphere 7.0 e i relativi strumenti per creare un'infrastruttura virtuale basata su FlexPod Express altamente affidabile e ad alta disponibilità.

["FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e NetApp AFF/FAS - NVA - implementazione"](#)

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.