Soluzioni FlexPod

FlexPod

NetApp
March 25, 2024

Sommario

Soluzioni FlexPod

Definizione FlexPod

Specifiche tecniche di FlexPod Express

TR-4293: Specifiche tecniche di FlexPod

Karthick Radhakrishnan, Arvind Ramakrishnan, Lindsey Street, Savita Kumari, NetApp

FlexPod Express è un'architettura pre-progettata e basata su Best practice, basata sul sistema di calcolo unificato Cisco e sulla famiglia di switch Cisco Nexus, e il layer di storage è costruito utilizzando NetApp FAS o lo storage NetApp e-Series. FlexPod Express è una piattaforma adatta per l'esecuzione di vari hypervisor di virtualizzazione, sistemi operativi bare metal e carichi di lavoro aziendali.

FlexPod offre non solo una configurazione di base, ma anche la flessibilità di essere dimensionati e ottimizzati per adattarsi a diversi casi di utilizzo e requisiti. Questo documento classifica le configurazioni FlexPod Express in base al sistema storage utilizzato, FlexPod Express con NetApp FAS e FlexPod Express con e-Series.

Piattaforme FlexPod

Esistono tre piattaforme FlexPod:

- **FlexPod Datacenter.** questa piattaforma è un'infrastruttura di data center virtuale estremamente scalabile, ideale per applicazioni aziendali con carichi di lavoro, virtualizzazione, VDI e cloud pubblico e privato. FlexPod Datacenter dispone di specifiche specifiche proprie, documentate in "TR-4036: Specifiche tecniche del data center FlexPod".
- **FlexPod Express.** questa piattaforma è un'infrastruttura convergente compatta, destinata a uffici remoti e casi di utilizzo edge.

Questo documento fornisce le specifiche tecniche della piattaforma FlexPod Express.

Regole FlexPod

Il design di FlexPod consente un'infrastruttura flessibile che comprende diversi componenti e versioni software.

Utilizzare i set di regole come guida per la creazione o l'assemblaggio di una configurazione FlexPod valida. I numeri e le regole elencati in questo documento rappresentano i requisiti minimi per FlexPod; possono essere ampliati nelle famiglie di prodotti incluse, in base alle esigenze di ambienti e casi di utilizzo diversi.

Configurazioni FlexPod supportate e validate

L'architettura di FlexPod è definita dall'insieme di regole descritte in questo documento. I componenti hardware e le configurazioni software devono essere supportati da Cisco hardware Compatibility List (HCL) e da "Tool di matrice di interoperabilità NetApp (IMT)".

Ogni Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) è una possibile configurazione FlexPod. Cisco e NetApp documentano queste combinazioni di configurazione e le convalidano con test

completi end-to-end. Le implementazioni FlexPod che si discostano da queste configurazioni sono pienamente supportate se seguono le linee guida di questo documento e tutti i componenti sono elencati come compatibili in Cisco HCL e NetApp "IMT".

Ad esempio, l'aggiunta di controller di storage aggiuntivi o server Cisco UCS e l'aggiornamento del software alle versioni più recenti sono completamente supportati se il software, l'hardware e le configurazioni soddisfano le linee guida definite in questo documento.

Software per lo storage

FlexPod supporta sistemi storage che eseguono sistemi operativi NetApp ONTAP o SANtricity.

NetApp ONTAP

Il software NetApp ONTAP è il sistema operativo che viene eseguito sui sistemi storage AFF e FAS. ONTAP offre un'architettura di storage altamente scalabile che consente operazioni senza interruzioni, aggiornamenti senza interruzioni e un'infrastruttura dati agile.

Per ulteriori informazioni su ONTAP, consultare "Pagina del prodotto ONTAP".

Software e-Series SANtricity

Il software e-Series SANtricity è il sistema operativo in esecuzione sui sistemi storage e-Series. SANtricity offre un sistema altamente flessibile che soddisfa le diverse esigenze applicative e offre alta disponibilità integrata e un'ampia gamma di funzionalità di protezione dei dati.

Per ulteriori informazioni, consultare "Pagina del prodotto SANtricity".

Requisiti hardware minimi

In questa sezione vengono descritti i requisiti hardware minimi per le diverse versioni di FlexPod Express.

FlexPod Express con NetApp FAS

I requisiti hardware per le soluzioni FlexPod Express che utilizzano i controller NetApp FAS per lo storage sottostante includono le configurazioni descritte in questa sezione.

Configurazione basata su CIMC (server rack standalone)

La configurazione di Cisco Integrated Management Controller (CIMC) include i seguenti componenti hardware:

- Due switch Ethernet standard da 10 Gbps in una configurazione ridondante (Cisco Nexus 31108 è consigliato, con i modelli Cisco Nexus 3000 e 9000 supportati)
- Server rack standalone Cisco UCS C-Series
- Due controller AFF serie C190, AFF A250, FAS2600 o FAS 2700 in una configurazione a coppia ad alta disponibilità (ha) implementata come cluster a due nodi

Configurazione gestita da Cisco UCS

La conferma gestita da Cisco UCS include i seguenti componenti hardware:

- Due switch Ethernet standard a 10 Gbps in una configurazione ridondante (si consiglia Cisco Nexus 3524)
- Uno chassis per server blade Cisco UCS 5108 a corrente alternata (CA)
- Due interconnessioni fabric Cisco UCS 6324
- Server Cisco UCS B-Series (almeno quattro server blade Cisco UCS B200 M5)
- Due controller AFF C190, AFF A250, FAS2750 o FAS2720 in una configurazione a coppia ha (richiede due adattatori di destinazione unificati disponibili, 2 porte [UTA2] per controller)

FlexPod Express con e-Series

I requisiti hardware per la configurazione iniziale di FlexPod Express con e-Series includono:

- Due interconnessioni fabric Cisco UCS 6324
- Uno chassis Cisco UCS Mini 5108 AC2 o DC2 (le interconnessioni fabric Cisco UCS 6324 sono supportate solo nello chassis AC2 e DC2)
- Server Cisco UCS B-Series (almeno due server blade Cisco UCS B200 M4)
- Configurazione a coppia ha di un sistema storage e-Series E2824 con un minimo di 12 dischi
- Due switch Ethernet standard a 10 Gbps in una configurazione ridondante (è possibile utilizzare gli switch esistenti nel data center)

Questi componenti hardware sono necessari per creare una configurazione iniziale della soluzione; è possibile aggiungere ulteriori blade server e dischi in base alle esigenze. Il sistema storage e-Series E2824 può essere sostituito con una piattaforma superiore e può essere eseguito anche come sistema all-flash.

Requisiti software minimi

In questa sezione vengono descritti i requisiti software minimi per le diverse versioni di FlexPod Express.

Requisiti software per FlexPod Express con NetApp AFF o FAS

I requisiti software per FlexPod Express con NetApp FAS includono:

- ONTAP 9.1 o versione successiva
- Cisco NX-OS versione 7.0(3)I6(1) o successiva
- Nella configurazione gestita da Cisco UCS, Cisco UCS Manager UCS 4.0(1b)

Tutti i software devono essere elencati e supportati in "NetApp IMT". Alcune funzionalità software potrebbero richiedere versioni di codice più recenti rispetto ai valori minimi elencati nelle architetture precedenti.

Requisiti software per FlexPod Express con e-Series

I requisiti software per FlexPod Express con e-Series includono:

- Software e-Series SANtricity 11.30 o superiore
- Cisco UCS Manager 4.0(1b).

Tutti i software devono essere elencati e supportati in "NetApp IMT".

Requisiti di connettività

In questa sezione vengono descritti i requisiti di connettività per le diverse versioni di FlexPod Express.

Requisiti di connettività per FlexPod Express con NetApp FAS

I requisiti di connettività per FlexPod Express con NetApp FAS includono:

- I controller di storage NetApp FAS devono essere collegati direttamente agli switch Cisco Nexus, ad eccezione della configurazione gestita da Cisco UCS, in cui i controller di storage sono collegati alle interconnessioni fabric.
- Non è possibile posizionare in linea apparecchiature aggiuntive tra i componenti principali di FlexPod.
- I Virtual Port channel (VPC) sono necessari per collegare gli switch Cisco Nexus serie 3000/9000 ai controller di storage NetApp.
- Sebbene non sia necessario, si consiglia di abilitare il supporto dei frame jumbo in tutto l'ambiente.

Requisiti di connettività per FlexPod Express con NetApp e-Series

I requisiti di connettività per FlexPod Express con e-Series includono:

- I controller di storage e-Series devono essere collegati direttamente alle interconnessioni fabric.
- Non è necessario posizionare apparecchiature aggiuntive inline tra i componenti principali di FlexPod.
- Tra le interconnessioni fabric e gli switch Ethernet sono richiesti VPC.

Requisiti di connettività per FlexPod Express con NetApp AFF

I requisiti di connettività per FlexPod Express con NetApp AFF includono:

- I controller di storage NetApp AFF devono essere collegati direttamente agli switch Cisco Nexus, ad eccezione della configurazione gestita da Cisco UCS, in cui i controller di storage sono collegati al fabric. interconnessioni.
- Non è possibile posizionare in linea apparecchiature aggiuntive tra i componenti principali di FlexPod.
- I Virtual Port channel (VPC) sono necessari per collegare gli switch Cisco Nexus serie 3000/9000 ai controller di storage NetApp.
- Sebbene non sia necessario, si consiglia di abilitare il supporto dei frame jumbo in tutto l'ambiente.

Altri requisiti

I requisiti aggiuntivi per FlexPod Express includono:

- Sono richiesti contratti di supporto validi per tutte le apparecchiature, tra cui:
  - Supporto SMARTnet per apparecchiature Cisco
  - Supporto SupportEdge Advisor o SupportEdge Premium per le apparecchiature NetApp
- Tutti i componenti software devono essere elencati e supportati in "NetApp IMT".
- Tutti i componenti hardware NetApp devono essere elencati e supportati su "NetApp Hardware Universe".
- Tutti i componenti hardware Cisco devono essere elencati e supportati su "Cisco HCL".

Funzionalità opzionali

In questa sezione vengono descritte le funzioni opzionali di FlexPod Express.

Opzione di boot iSCI

L'architettura FlexPod utilizza l'avvio iSCSI. I requisiti minimi per l'opzione di boot iSCSI includono:

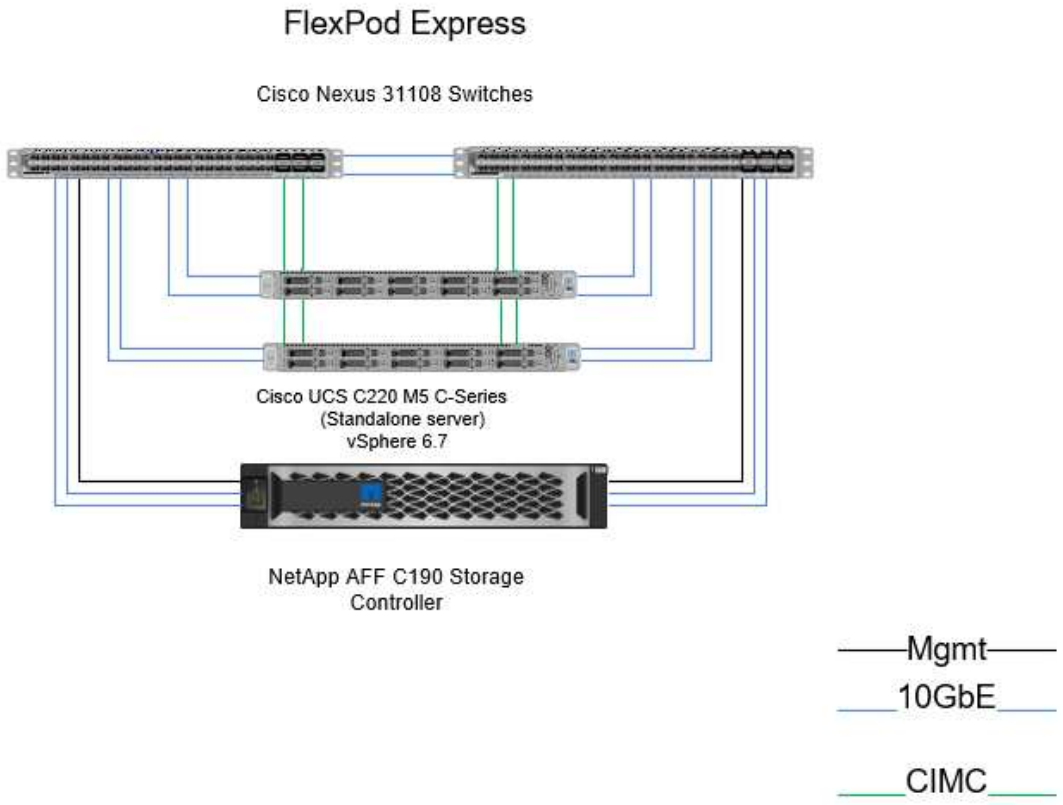
- Una licenza/funzione iSCSI attivata sul controller di storage NetApp
- Un adattatore Ethernet a due porte da 10 Gbps su ciascun nodo della coppia ha del controller di storage NetApp
- Un adattatore nel server Cisco UCS in grado di eseguire l'avvio iSCSI

Opzioni di configurazione

Questa sezione fornisce ulteriori informazioni sulla configurazione richiesta e validata nell'architettura FlexPod Express.

FlexPod Express con Cisco UCS serie C e AFF serie C190

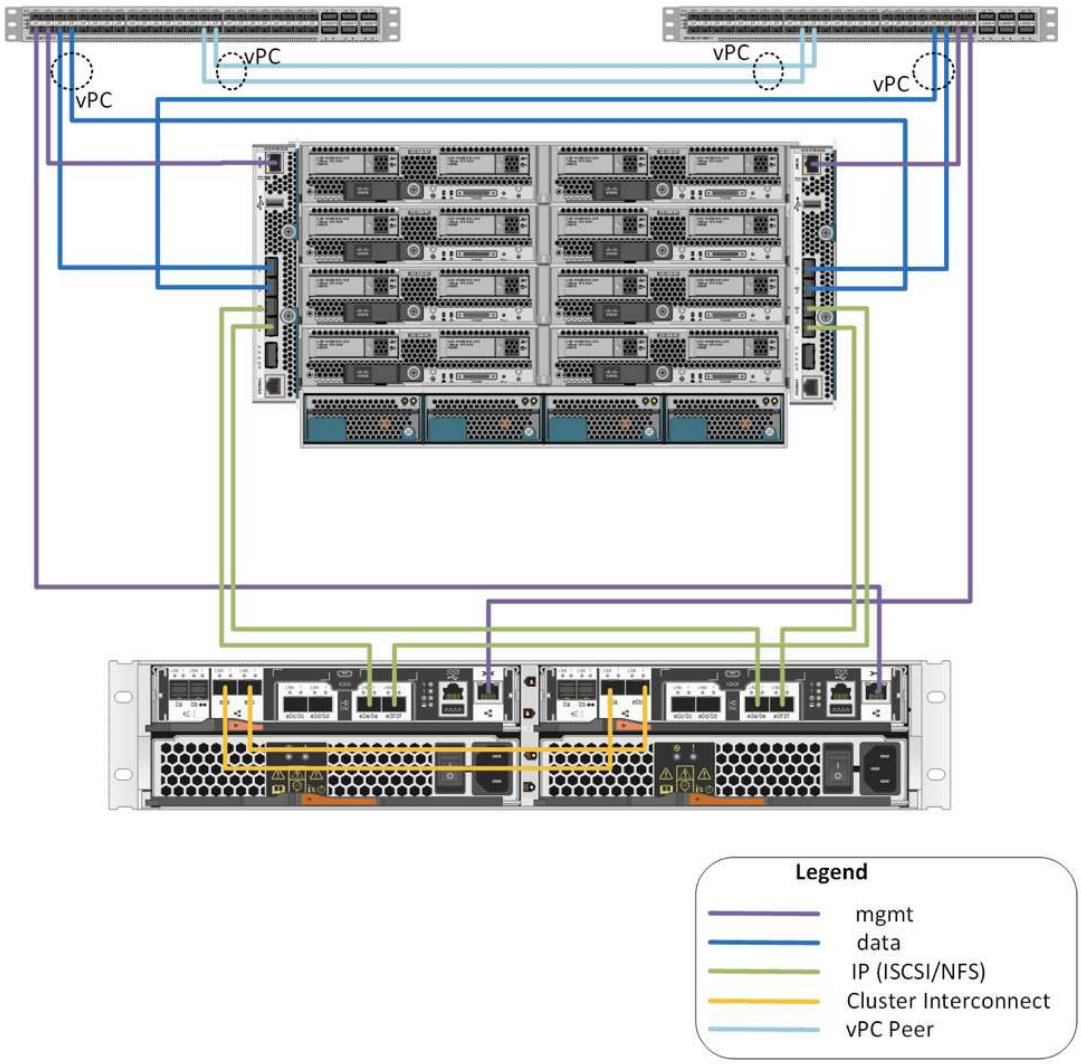
La figura seguente illustra la soluzione FlexPod Express con Cisco UCS serie C e AFF serie C190. Questa soluzione supporta entrambi gli uplink da 10 GbE.



Per ulteriori informazioni su questa configurazione, consultare la Guida all'implementazione di FlexPod con VMware vSphere 6.7 e NetApp AFF C190 NVA (in corso).

FlexPod Express con Cisco UCS Mini e AFF A220 e FAS 2750/2720

La figura seguente illustra la configurazione gestita da FlexPod con Cisco UCS.



Per ulteriori informazioni su questa configurazione, vedere "FlexPod Express con VMware vSphere 6.7U1 e NetApp AFF A220 con storage basato su IP collegato direttamente".

Componenti Cisco

Cisco contribuisce in modo sostanziale alla progettazione e all'architettura di FlexPod Express e contribuisce ai livelli di calcolo e di rete della soluzione. Questa sezione descrive i componenti Cisco UCS e Cisco Nexus disponibili per FlexPod Express.

Opzioni dei server blade Cisco UCS B-Series

I blade Cisco UCS B-Series attualmente supportati nella piattaforma Cisco UCS Mini sono B200 M5 e B420 M4. Gli altri blade verranno elencati nella tabella seguente man mano che diventano supportati nella piattaforma Cisco UCS Mini.

Server Cisco UCS B-Series	Codice del ricambio	Specifiche tecniche
CISCO UCS B200 M5	UCSB-B200-M5	https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-m5-blade-server/model.html
CISCO UCS B200 M4	UCSB-B200-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m4-specsheet.pdf
CISCO UCS B420 M4	UCSB-B420-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b420m4-spec-sheet.pdf

Opzioni dei server rack Cisco UCS C-Series

I blade Cisco UCS C-Series sono disponibili in unità a un rack e due rack (RU), con diverse opzioni di CPU, memoria e i/O. I numeri di parte elencati nella tabella seguente si riferiscono al server di base; non includono CPU, memoria, dischi, schede PCIe o Cisco FEX. In FlexPod sono disponibili e supportate diverse opzioni di configurazione.

Server rack Cisco UCS C-Series	Codice del ricambio	Specifiche tecniche
CISCO UCS C220 M4	UCSC-C220-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
CISCO UCS C240 M4	UCSC-C240-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m4-sff-spec-sheet.pdf
CISCO UCS C460 M4	UCSC-C460-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c460m4_specsheet.pdf

Switch Cisco Nexus

Per tutte le architetture FlexPod Express sono richiesti switch ridondanti.

FlexPod Express con architettura NetApp AFF o FAS è costruito con lo switch Cisco Nexus 31108. FlexPod Express con l'architettura Cisco UCS Mini (gestita da Cisco UCS) viene validata utilizzando lo switch Cisco Nexus 3524. Questa configurazione può essere implementata anche con uno switch standard.

FlexPod Express con e-Series può essere implementato con uno switch standard.

La seguente tabella elenca i codici dei componenti per lo chassis della serie Cisco Nexus; non includono moduli aggiuntivi o SFP.

Switch Cisco Nexus Series	Codice del ricambio	Specifiche tecniche
Cisco Nexus 3048	N3K-C3048TP-1GE	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-685363.html
Cisco Nexus 31108	N3K-C31108PC-V.	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 9396	N9K-C9396PX	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729405.html
Cisco Nexus 3172	N3K-C3172	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-729483.html

Opzioni di licenza del supporto Cisco

Sono richiesti contratti di supporto SMARTnet validi per tutte le apparecchiature Cisco nell'architettura FlexPod Express.

> Le licenze richieste e i numeri di parte per tali licenze devono essere verificati dal rappresentante commerciale in quanto possono differire per i diversi prodotti.

La seguente tabella elenca le opzioni di licenza per il supporto Cisco.

Licenze Cisco Support	Guida alla licenza
SMARTnet 24x7x4	http://www.cisco.com/web/services/portfolio/product-technical-support/smartnet/index.html

Componenti NetApp

I controller di storage NetApp forniscono la base dello storage nell'architettura FlexPod Express per l'avvio e lo storage dei dati delle applicazioni. Questa sezione elenca le diverse opzioni NetApp nell'architettura FlexPod Express.

Opzioni di storage controller NetApp

NetApp FAS

L'architettura FlexPod richiede controller AFF serie C190, AFF A220 o FAS2750 ridondanti. I controller eseguono il software ONTAP. Quando si ordinano i controller di storage, è possibile precaricare la versione software preferita sui controller. Per ONTAP, il cluster può essere implementato con una coppia di switch di interconnessione del cluster o in una configurazione del cluster senza switch.

I numeri di parte elencati nella seguente tabella si riferiscono a un controller vuoto. Sono disponibili diverse opzioni e configurazioni in base alla piattaforma di storage selezionata. Per ulteriori informazioni su questi componenti aggiuntivi, rivolgersi al rappresentante di vendita.

Controller dello storage	Codice ricambio FAS	Specifiche tecniche
FAS2750	In base alle singole opzioni scelte	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
FAS2720	In base alle singole opzioni scelte	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
AFF C190	In base alle singole opzioni scelte	https://www.netapp.com/us/products/entry-level-aff.aspx
AFF A220	In base alle singole opzioni scelte	https://www.netapp.com/us/documentation/all-flash-fas.aspx
FAS2620	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2650	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx

Storage e-Series

Nell'architettura FlexPod Express è richiesta una coppia ha di controller della serie E2800. I controller eseguono il sistema operativo SANtricity.

I numeri di parte elencati nella seguente tabella si riferiscono a un controller vuoto. Sono disponibili diverse opzioni e configurazioni in base alla piattaforma di storage selezionata. Per ulteriori informazioni su questi componenti aggiuntivi, rivolgersi al rappresentante di vendita.

Controller dello storage	Codice del ricambio	Specifiche tecniche
E2800	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/e2800/e2800-tech-specs.aspx

Moduli di espansione Ethernet di NetApp

NetApp FAS

La seguente tabella elenca le opzioni della scheda di rete NetApp FAS10GbE.

Componente	Codice del ricambio	Specifiche tecniche
NetApp X1117A	X1117A-R6	https://library.netapp.com/ecm/ecm_download_file/ECMM1280307

> I sistemi storage della serie FAS2500 e 2600 dispongono di porte 10GbE integrate.
>
> L'adattatore NetApp X1117A è per i sistemi storage FAS8020.

Storage e-Series

La seguente tabella elenca le opzioni della scheda di rete e-Series 10GbE.

Componente	Codice del ricambio
ISCSI 10 GbE/FC 16 GB a 4 porte	X-56025-00-0E-C.
ISCSI 10 GbE/FC 16 GB a 2 porte	X-56024-00-0E-C.

> I sistemi storage della serie E2824 dispongono di porte 10GbE integrate.
>
> La scheda HIC (host Interface Card) FC a 4 porte da 10 GbE iSCSI/16 GB può essere utilizzata per una maggiore densità di porte.

Le porte integrate e l'HIC possono funzionare come adattatori iSCSI o FC a seconda della funzione attivata in SANtricity OS.

Per ulteriori informazioni sulle opzioni della scheda di rete supportate, consultare la sezione adattatore di "NetApp Hardware Universe".

Shelf di dischi e dischi NetApp

NetApp FAS

Per i controller di storage è necessario almeno uno shelf di dischi NetApp. Il tipo di shelf NetApp selezionato determina i tipi di dischi disponibili all'interno di tale shelf.

Le serie di controller FAS2700 e FAS2600 sono offerte come configurazione che include doppi controller di storage e dischi alloggiati nello stesso chassis. Questa configurazione viene offerta con unità SATA o SAS; pertanto, non sono necessari shelf di dischi esterni aggiuntivi a meno che i requisiti di performance o capacità non impongano più spindle.

> Tutti i numeri di parte degli shelf di dischi si riferiscono allo shelf vuoto con due PSU CA. Per ulteriori codici ricambio, rivolgersi al rappresentante di vendita.
>
> I numeri di parte dei dischi variano in base alle dimensioni e al fattore di forma del disco che si intende acquistare. Per ulteriori codici ricambio, rivolgersi al rappresentante di vendita.

La seguente tabella elenca le opzioni di shelf di dischi NetApp, insieme ai dischi supportati per ciascun tipo di shelf, disponibili su NetApp Hardware Universe. Seguire il link Hardware Universe, selezionare la versione di ONTAP in uso, quindi selezionare il tipo di shelf. Sotto l'immagine shelf, fare clic su Supported Drives (unità supportate) per visualizzare le unità supportate per versioni specifiche di ONTAP e gli shelf di dischi.

Shelf di dischi	Codice del ricambio	Specifiche tecniche
DS212C	DS212C-0-12	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"
DS224C	DS224C-0-24	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"

Shelf di dischi	Codice del ricambio	Specifiche tecniche
DS460C	DS460C-0-60	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"
DS2246	X559A-R6	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"
DS4246	X24M-R6	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"
DS4486	DS4486-144 TB-R5-C.	"Shelf di dischi e supporti di storage specifiche tecniche unità supportate su NetApp Hardware Universe"

Storage e-Series

Per i controller di storage che non ospitano dischi nel proprio chassis è necessario almeno uno shelf di dischi NetApp. Il tipo di shelf NetApp selezionato determina i tipi di dischi disponibili all'interno di tale shelf.

I controller della serie E2800 sono offerti come configurazione che include doppi controller di storage e dischi alloggiati in uno shelf di dischi supportato. Questa configurazione viene offerta con unità SSD o SAS.

> I numeri di parte dei dischi variano in base alle dimensioni e al fattore di forma del disco che si intende acquistare. Per ulteriori codici ricambio, rivolgersi al rappresentante di vendita.

La seguente tabella elenca le opzioni di shelf di dischi NetApp e le unità supportate per ciascun tipo di shelf, disponibili su NetApp Hardware Universe. Seguire il link Hardware Universe, selezionare la versione di ONTAP in uso, quindi selezionare il tipo di shelf. Sotto l'immagine shelf, fare clic su Supported Drives (unità supportate) per visualizzare le unità supportate per versioni specifiche di ONTAP e gli shelf di dischi.

Shelf di dischi	Codice del ricambio	Specifiche tecniche
DE460C	E-X5730A-DM-0E-C.	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"
DE224C	E-X5721A-DM-0E-C.	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"
DE212C	E-X5723A-DM-0E-C.	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"

Opzioni di licenza software NetApp

NetApp FAS

La seguente tabella elenca le opzioni di licenza software NetApp FAS.

Licenze software NetApp	Codice ricambio	Specifiche tecniche
Licenza cluster di base	Per ulteriori informazioni sulle licenze, consulta il tuo team di vendita NetApp.	

Storage e-Series

La seguente tabella elenca le opzioni di licenza software e-Series.

Licenze software NetApp	Codice del ricambio	Specifiche tecniche
Funzionalità standard	Per ulteriori informazioni sulle licenze, consulta il tuo team di vendita NetApp.	
Funzionalità Premium		

Opzioni di licenza del supporto NetApp

Sono necessarie licenze SupportEdge Premium e i codici prodotto di tali licenze variano in base alle opzioni selezionate nella progettazione FlexPod.

NetApp FAS

La seguente tabella elenca le opzioni di licenza per il supporto NetApp per NetApp FAS.

Licenze NetApp Support	Codice del ricambio	Specifiche tecniche
SupportEdge Premium4 ore on-site; mesi: 36	CS-O2-4HR	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf

Storage e-Series

La seguente tabella elenca le opzioni di licenza del supporto NetApp per lo storage e-Series.

Licenze NetApp Support	Codice del ricambio	Specifiche tecniche
Supporto hardware Premium 4 ore on-site; mesi: 36	SVC-O2-4HR-E.	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf
Supporto software	SW-SSP-O2-4HR-E.	
Installazione iniziale	SVC-INST-O2-4HR-E.	

Requisiti di alimentazione e cablaggio

In questa sezione vengono descritti i requisiti di alimentazione e di cablaggio minimi per un design FlexPod Express.

Requisiti di alimentazione

I requisiti di alimentazione sono basati su U.S. E si presume l'utilizzo dell'alimentazione CA. Altri paesi potrebbero avere requisiti di alimentazione diversi. Per la maggior parte dei componenti sono disponibili anche opzioni di alimentazione a corrente continua (CC). Per ulteriori informazioni sulla potenza massima richiesta e altre informazioni dettagliate sull'alimentazione, consultare le specifiche tecniche dettagliate di ciascun componente hardware.

Per informazioni dettagliate sull'alimentazione di Cisco UCS, consultare la "Cisco UCS Power Calculator".

La seguente tabella elenca le porte di alimentazione richieste per ciascuna periferica.

Switch Cisco Nexus	Cavi di alimentazione necessari
Cisco Nexus 3048	2 cavi di alimentazione C13/C14 per ciascuno switch Cisco Nexus serie 3000
Cisco Nexus 3524	2 cavi di alimentazione C13/C14 per ciascuno switch Cisco Nexus serie 3000
Cisco Nexus 9396	2 cavi di alimentazione C13/C14 per ciascuno switch Cisco Nexus serie 9000

Chassis Cisco UCS	Cavi di alimentazione necessari
Cisco UCS 5108	2 CAB-US515P-C19-US/CAB-US520-C19-US per ogni chassis Cisco UCS

Server Cisco UCS B-Series	Cavi di alimentazione necessari
CISCO UCS B200 M4	N/D; il server blade è alimentato dallo chassis
CISCO UCS B420 M4	N/D; il server blade è alimentato dallo chassis
CISCO UCS B200 M5	N/D; il server blade è alimentato dallo chassis
CISCO UCS B480 M5	N/D; il server blade è alimentato dallo chassis

Server Cisco UCS C-Series	Porte di alimentazione richieste
CISCO UCS C220 M4	2 cavi di alimentazione C13/C14 per ciascun server Cisco UCS
CISCO UCS C240 M4	
CISCO UCS C460 M4 CISCO UCS C220 M5 CISCO UCS C240 M5 CISCO UCS C480 M5	

Controller NetApp FAS	Porte di alimentazione richieste (per coppia ha)
FAS2554	2 x C13/C14
FAS2552	2 x C13/C14
FAS2520	2 x C13/C14
FAS8020	2 x C13/C14

Controller e-Series	Porte di alimentazione richieste (per coppia ha)
E2824	2 x C14/C20

Shelf di dischi NetApp FAS	Porte di alimentazione richieste
DS212C	2 x C13/C14
DS224C	2 x C13/C14

Shelf di dischi NetApp FAS	Porte di alimentazione richieste
DS460C	2 x C13/C14
DS2246	2 x C13/C14
DS4246	4 x C13/C14

Shelf di dischi e-Series	Porte di alimentazione richieste
DE460C	2 x C14/C20
DE224C	2 x C14/C20
DE212C	2 x C14/C20

Requisiti minimi per i cavi

In questa sezione vengono descritti i requisiti minimi per i cavi per un design FlexPod Express. La maggior parte delle implementazioni FlexPod richiede cavi aggiuntivi, ma il numero varia in base alle dimensioni e all'ambito dell'implementazione.

La seguente tabella elenca il numero minimo di cavi necessari per ciascun dispositivo.

Switch Cisco Nexus serie 3000	Cavi necessari
Cisco Nexus 31108	Almeno due cavi 10 GbE in fibra o Twinax per switch
Cisco Nexus 3172PQ	
Cisco Nexus 3048	
Cisco Nexus 3524	
Cisco Nexus 9396	
DS212C	
DS2246	Il numero di cavi SAS dipende dalla configurazione specifica degli shelf di dischi
DS460C	
DS224C	
DS4246	
E2800	• Almeno un cavo Gigabit Ethernet (1 GbE) per la gestione per controller • Almeno due cavi 10GbE per controller (per iSCSI) o due cavi FC che soddisfano i requisiti di velocità
DE460C	2 cavi mini-SAS HD per shelf di dischi
DE224C	2 cavi mini-SAS HD per shelf di dischi
DE212C	2 cavi mini-SAS HD per shelf di dischi

Specifiche tecniche e riferimenti

Questa sezione descrive specifiche tecniche importanti aggiuntive per ciascun componente FlexPod Express.

Server blade Cisco UCS B-Series

La seguente tabella elenca le opzioni del server blade Cisco UCS B-Series.

Componente	CISCO UCS B200 M4	CISCO UCS B420 M4	CISCO UCS B200 M5
Supporto del processore	Intel Xeon E5-2600	Intel Xeon E5-4600	Processori scalabili Intel Xeon
Capacità massima di memoria	24 DIMM per un massimo di 768 GB	48 DIMM per un massimo di 3 TB	24 DIMM per un massimo di 3072 GB
Dimensioni e velocità della memoria	32 GB di DDR4; 2133 MHz	64 GB DDR4; 2400 MHz	16 GB, 32 GB, 64 GB e 128 GB DDR4; 2666 MHz
Supporto per l'avvio SAN	Sì	Sì	Sì
Slot per adattatori i/o mezzanino	2	3	2, anteriore e posteriore, incluso il supporto GPU
Throughput i/o massimo	80 Gbps	160 Gbps	80 Gbps

Server rack Cisco UCS C-Series

La seguente tabella elenca le opzioni dei server rack Cisco UCS C-Series.

Componente	CISCO UCS C220 M4	CISCO UCS C240 M4	CISCO UCS C460 M4	CISCO UCS C220 M5
Supporto del processore	1 o 2 processori Intel serie E5-2600	1 o 2 processori Intel Xeon serie E5-2600	2 o 4 processori Intel Xeon serie E7-4800/8800	Processori scalabili Intel Xeon (1 o 2)
Capacità massima di memoria	1,5 GB	1,5 TB	6 TB	3072 GB
Slot PCIe	2	6	10	2
Fattore di forma	1 RU	2 RU	4 RU	1 RU

La seguente tabella elenca le schede tecniche per le opzioni del server rack Cisco UCS C-Series.

Componente	Scheda informativa Cisco UCS
CISCO UCS C220 M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
CISCO UCS C240 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m4-rack-server/datasheet-c78-732455.html

Componente	Scheda informativa Cisco UCS
CISCO UCS C460 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c460-m4-rack-server/datasheet-c78-730907.html
CISCO UCS C220 M5	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf

Switch Cisco Nexus serie 3000

La seguente tabella elenca le opzioni degli switch Cisco Nexus serie 3000.

Componente	Cisco Nexus 3048	Cisco Nexus 3524	Cisco Nexus 31108	Cisco Nexus 3172PQ
Fattore di forma	1 RU	1 RU	1 RU	1 RU
Numero massimo di porte 1 Gbps	48	24	48 (10/40/100 Gbps)	72 porte 1/10GbE o 48 porte 1/10GbE più sei porte 40GbE
Velocità di inoltro	132 Mbps	360 Mbps	1,2 Bpps	1 Bpps
Supporto Jumbo Frame	Sì	Sì	Sì	Sì

La seguente tabella elenca le schede tecniche per le opzioni dello switch Cisco Nexus serie 3000.

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus 31108	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 3172PQ	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3048	https://www.cisco.com/c/en/us/products/switches/nexus-3048-switch/index.html
Cisco Nexus 3172PQ-XL	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3548 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html
Cisco Nexus 3548	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html

La seguente tabella elenca le opzioni degli switch Cisco Nexus serie 9000.

Componente	Cisco Nexus 9396	Cisco Nexus 9372
Fattore di forma	2 RU	1 RU
Numero massimo di porte	60	54
Porte uplink SFP+ a 10 Gbps	48	48

La seguente tabella elenca le schede tecniche delle opzioni degli switch Cisco Nexus serie 9000.

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus 9396	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Cisco Nexus 9372	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Nexus 9396X	https://www.cisco.com/c/en/us/products/switches/nexus-9396px-switch/index.html?dtid=osscdc000283

Storage controller NetApp FAS

La seguente tabella elenca le opzioni attuali del controller di storage NetApp FAS.

Componente corrente	FAS2620	FAS2650
Configurazione	2 controller in uno chassis 2U	2 controller in uno chassis 4U
Capacità massima raw	1440 TB	1243 TB
Dischi interni	12	24
Numero massimo di dischi (interni ed esterni)	144	144
Dimensione massima del volume	100 TB	
Dimensione massima dell'aggregato	4 TB	
Numero massimo di LUN	2,048 per controller	
Supporto dello storage di rete	ISCSI, FC, FCoE, NFS e CIFS	
Numero massimo di volumi NetApp FlexVol	1,000 per controller.	
Numero massimo di copie Snapshot di NetApp	255,000 per controller	
Massimo caching dei dati intelligente di NetApp Flash Pool	24 TB	

Per ulteriori informazioni sull'opzione del controller di storage FAS, consultare "Modelli FAS" Della Hardware Universe. Per AFF, vedere "Modelli AFF" sezione.

La seguente tabella elenca le caratteristiche di un sistema di controller FAS8020.

Componente	FAS8020
Configurazione	2 controller in uno chassis 3U
Capacità massima raw	2880 TB
Numero massimo di dischi	480
Dimensione massima del volume	70 TB
Dimensione massima dell'aggregato	324 TB
Numero massimo di LUN	8,192 per controller
Supporto dello storage di rete	ISCSI, FC, NFS e CIFS
Numero massimo di volumi FlexVol	1,000 per controller
Numero massimo di copie Snapshot	255,000 per controller
Caching dei dati intelligente NetApp Flash cache massimo	3 TB
Caching massimo dei dati di Flash Pool	24 TB

La seguente tabella elenca le schede tecniche per i controller di storage NetApp.

Componente	Scheda informativa sullo storage controller
Serie FAS2600	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
Serie FAS2500	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
Serie FAS8000	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

Adattatori Ethernet NetApp FAS

La seguente tabella elenca le schede di rete NetApp FAS 10GbE.

Componente	X1117A-R6
Numero di porte	2
Tipo di adattatore	SFP+ con fibra

L'adattatore SFP+ X1117A-R6 è supportato dai controller della serie FAS8000.

I sistemi storage delle serie FAS2600 e FAS2500 dispongono di porte 10GbE integrate. Per ulteriori informazioni, consultare "Scheda informativa sulla scheda di rete NetApp 10GbE".

> Per ulteriori informazioni sull'adattatore in base al modello AFF o FAS, consultare "Sezione adattatore" Nel Hardware Universe.

Shelf di dischi NetApp FAS

La seguente tabella elenca le opzioni correnti dello shelf di dischi NetApp FAS.

Componente	DS460C	DS224C	DS212C	DS2246	DS4246
Fattore di forma	4 RU	2 RU	2 RU	2 RU	4 RU
Dischi per enclosure	60	24	12	24	24
Fattore di forma del disco	grande fattore di forma da 3.5"	fattore di forma ridotto da 2.5"	grande fattore di forma da 3.5"	fattore di forma ridotto da 2.5"	grande fattore di forma da 3.5"
Moduli i/o shelf	Doppi moduli IOM12	Doppi moduli IOM12	Doppi moduli IOM12	Doppi moduli IOM6	Doppi moduli IOM6

Per ulteriori informazioni, consulta la scheda informativa sugli shelf di dischi NetApp.

> Per ulteriori informazioni sugli shelf di dischi, consultare NetApp Hardware Universe "Sezione shelf di dischi".

Dischi NetApp FAS

Le specifiche tecniche per i dischi NetApp includono dimensioni del fattore di forma, capacità del disco, rpm del disco, controller di supporto e requisiti di versione Data ONTAP e sono disponibili nella sezione Drives (unità) a "NetApp Hardware Universe".

Storage controller e-Series

La seguente tabella elenca le opzioni correnti dei controller di storage e-Series.

Componente corrente	E2812	E2824	E2860
Configurazione	2 controller in uno chassis 2U	2 controller in uno chassis 2U	2 controller in uno chassis 4U
Capacità massima raw	1800 TB	1756,8 TB	1800 TB
Dischi interni	12	24	60
Numero massimo di dischi (interni ed esterni)	180		
SSD massimo	120		
Dimensione massima del volume per il volume del pool di dischi	1024 TB		
Numero massimo di pool di dischi	20		
Supporto dello storage di rete	ISCSI e FC		
Numero massimo di volumi	512		

La seguente tabella elenca le schede tecniche per il controller di storage e-Series corrente.

Componente	Scheda informativa sullo storage controller
E2800	http://www.netapp.com/us/media/ds-3805.pdf

Adattatori e-Series

La seguente tabella elenca gli adattatori e-Series.

Componente	X-56023-00-0E-C.	X-56025-00-0E-C.	X-56027-00-0E-C.	X-56024-00-0E-C.	X-56026-00-0E-C.
Numero di porte	2	4	4	2	2
Tipo di adattatore	10 GB base-T.	16 G FC e 10 GbE iSCSI	SAS	16 G FC e 10 GbE iSCSI	SAS

Shelf di dischi e-Series

La seguente tabella elenca le opzioni di shelf di dischi e-Series.

Componente	DE212C	DE224C	DE460C
Fattore di forma	2 RU	2 RU	4 RU
Dischi per enclosure	12	24	60
Fattore di forma del disco	fattore di forma ridotto da 2.5" 3.5"	2.5"	fattore di forma ridotto da 2.5" 3.5"
Moduli i/o shelf	IOM12	IOM12	IOM12

Dischi e-Series

Le specifiche tecniche per i dischi NetApp includono dimensioni del fattore di forma, capacità del disco, giri/min del disco, controller di supporto e requisiti di versione SANtricity e sono disponibili nella sezione dischi a "NetApp Hardware Universe".

Architetture e apparecchiature precedenti

FlexPod è una soluzione flessibile che consente ai clienti di utilizzare sia le apparecchiature nuove che quelle esistenti per la vendita da parte di Cisco e NetApp. Talvolta, alcuni modelli di apparecchiature di Cisco e NetApp sono stati progettati per essere utilizzati al termine del ciclo di vita.

Anche se questi modelli di apparecchiature non sono più disponibili, i clienti che hanno acquistato uno di questi modelli prima della data di fine vendita possono utilizzare l'apparecchiatura in una configurazione FlexPod.

Inoltre, le architetture FlexPod Express vengono periodicamente aggiornate per introdurre l'hardware e il software più recenti di Cisco e NetApp nella soluzione FlexPod Express. In questa sezione sono elencate le architetture e l'hardware FlexPod precedenti utilizzati al loro interno.

Architetture FlexPod Express precedenti

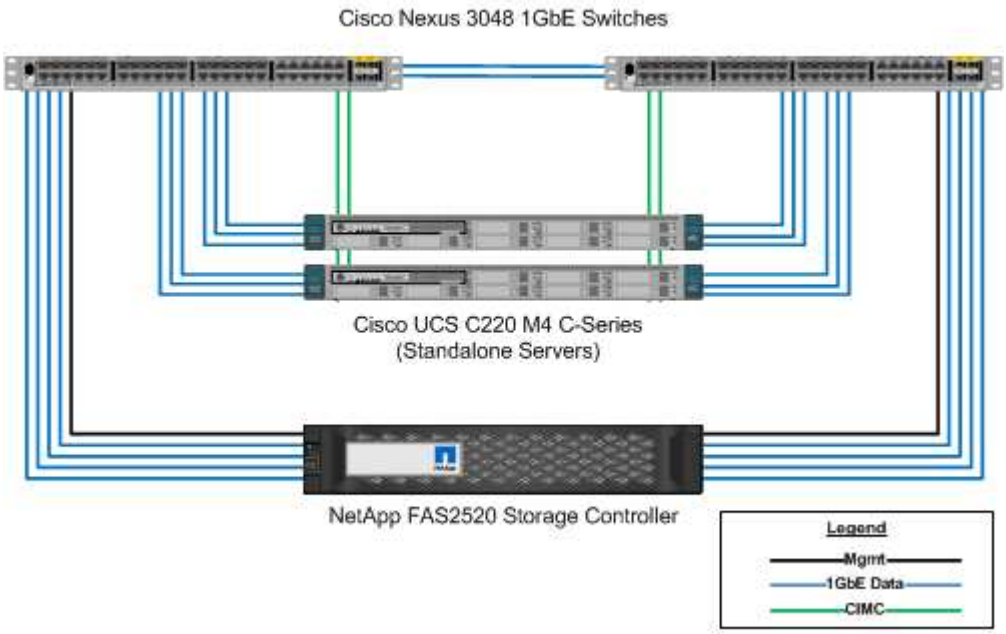
In questa sezione vengono descritte le architetture FlexPod Express precedenti.

FlexPod Express configurazioni piccole e medie

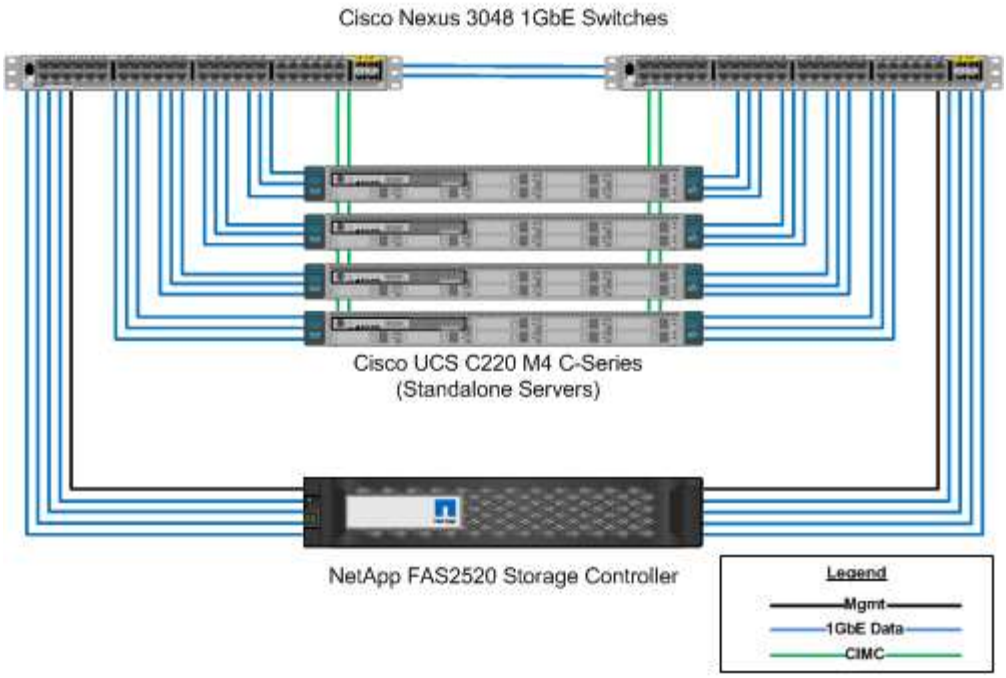
Le configurazioni FlexPod Express di piccole e medie dimensioni includono i seguenti componenti:

- Due switch Cisco Nexus 3048 in una configurazione ridondante
- Almeno due server Cisco UCS C-Series con montaggio in rack
- Due controller della serie FAS2200 o FAS2500 in una configurazione a coppia ha

La figura seguente illustra la configurazione di FlexPod Express Small.



La seguente figura illustra la configurazione del supporto FlexPod Express.

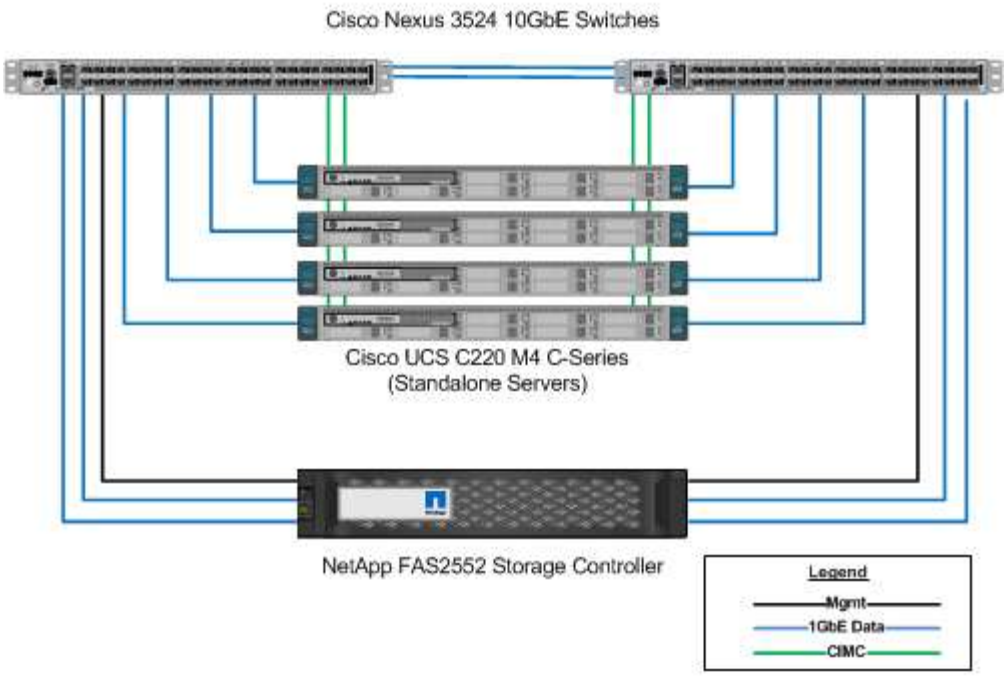


Configurazione di grandi dimensioni di FlexPod Express

La configurazione FlexPod Express Large include i seguenti componenti:

- Due switch Cisco Nexus serie 3500 o Cisco Nexus serie 9300 in una configurazione ridondante
- Almeno due server Cisco UCS C-Series con montaggio in rack
- Due controller FAS2552, FAS2554 o FAS8020 in una configurazione a coppia ha (richiede due porte 10 GbE per controller)
- Uno shelf di dischi NetApp con qualsiasi tipo di disco supportato (quando si utilizza FAS8020)

La seguente figura illustra la configurazione di FlexPod Express Large.



Precedenti architetture verificate con FlexPod Express

Le precedenti architetture verificate con FlexPod Express sono ancora supportate. I documenti relativi all'architettura e all'implementazione includono:

- "FlexPod Express con Cisco UCS serie C e NetApp serie FAS2500"
- "FlexPod Express con VMware vSphere 6.0: Configurazioni piccole e medie"
- "FlexPod Express con VMware vSphere 6.0: Configurazione di grandi dimensioni"
- "FlexPod Express con Microsoft Windows Server 2012 R2 Hyper-V: Configurazioni piccole e medie"
- "FlexPod Express con Microsoft Windows Server 2012 R2 Hyper-V: Configurazione di grandi dimensioni"

Hardware precedente

La seguente tabella elenca l'hardware utilizzato nelle architetture FlexPod Express precedenti.

Hardware utilizzato nelle architetture precedenti	Specifiche tecniche (se disponibili)
CISCO UCS C220 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m3-rack-server/data_sheet_c78-700626.html
CISCO UCS C24 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706103.html
CISCO UCS C22 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706101.html
CISCO UCS C240 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m3-rack-server/data_sheet_c78-700629.html
CISCO UCS C260 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/c260m2_specsheet.pdf

Hardware utilizzato nelle architetture precedenti	Specifiche tecniche (se disponibili)
CISCO UCS C420 M3	http://www.cisco.com/en/US/products/ps12770/index.html
CISCO UCS C460 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf
CISCO UCS B200 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m3-blade-server/data_sheet_c78-700625.html
CISCO UCS B420 M3	N/A.
CISCO UCS B22 M3	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b22m3_specsheet.pdf
Cisco Nexus 3524	http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
FAS2240	
FAS2220	http://www.netapp.com/us/products/storage-systems/fas2200/fas2200-tech-specs.aspx
DS4243	N/A.

Apparecchiature legacy

La seguente tabella elenca le opzioni del controller di storage legacy di NetApp.

Controller dello storage	Codice ricambio FAS	Specifiche tecniche
FAS2520	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	In base alle singole opzioni scelte	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

La seguente tabella elenca le opzioni di shelf di dischi legacy NetApp per NetApp FAS.

Shelf di dischi	Codice del ricambio	Specifiche tecniche
DE1600	E-X5682A-DM-0E-R6-C.	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"

Shelf di dischi	Codice del ricambio	Specifiche tecniche
DE5600	E-X4041A-12-R6	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"
DE6600	X-48564-00-R6	"Shelf di dischi specifiche tecniche unità supportate su NetApp Hardware Universe"

Controller FAS legacy di NetApp

La seguente tabella elenca le opzioni del controller FAS di NetApp legacy.

Componente corrente	FAS2554	FAS2552	FAS2520
Configurazione	2 controller in uno chassis 4U	2 controller in uno chassis 2U	2 controller in uno chassis 2U
Capacità massima raw	576 TB	509 TB	336 TB
Dischi interni	24	24	12
Numero massimo di dischi (interni ed esterni)	144	144	84
Dimensione massima del volume	60 TB		
Dimensione massima dell'aggregato	120 TB		
Numero massimo di LUN	2,048 per controller		
Supporto dello storage di rete	ISCSI, FC, FCoE, NFS e CIFS		ISCSI, NFS e CIFS
Numero massimo di volumi NetApp FlexVol	1,000 per controller		
Numero massimo di copie Snapshot di NetApp	255,000 per controller		

Per ulteriori modelli NetApp FAS, vedere "Sezione modelli FAS" Nel Hardware Universe.

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"

- Pagina delle risorse di documentazione di AFF

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- Pagina delle risorse di documentazione per i sistemi storage FAS

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- Documentazione NetApp

  "https://docs.netapp.com"

Specifiche tecniche del data center FlexPod

TR-4036: Specifiche tecniche del data center FlexPod

Arvind Ramakrishnan e Jyh-shing Chen, NetApp

La piattaforma FlexPod 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 sui controller di storage NetApp (sistemi AFF, ASA o FAS).

FlexPod è una piattaforma adatta per l'esecuzione di una vasta gamma di hypervisor di virtualizzazione, sistemi operativi bare-metal e carichi di lavoro aziendali. FlexPod offre non solo una configurazione di base, ma anche la flessibilità di essere dimensionati e ottimizzati per adattarsi a diversi casi di utilizzo e requisiti.

> Prima di ordinare una configurazione FlexPod completa, consultare "Infrastruttura convergente FlexPod" pagina su netapp.com per la versione più recente di queste specifiche tecniche.

"Successivo: Piattaforme FlexPod."

Piattaforme FlexPod

Esistono due piattaforme FlexPod:

- **FlexPod Datacenter.** questa piattaforma è un'infrastruttura di data center virtuale estremamente scalabile, adatta per applicazioni aziendali con carichi di lavoro, virtualizzazione, infrastruttura di desktop virtuale (VDI) e carichi di lavoro di cloud pubblico, privato e ibrido.
- **FlexPod Express.** questa piattaforma è un'infrastruttura convergente compatta, destinata a uffici remoti e casi di utilizzo edge. Le specifiche di FlexPod Express sono documentate in "Specifiche tecniche di FlexPod Express."

Questo documento fornisce le specifiche tecniche della piattaforma FlexPod Datacenter.

Regole FlexPod

Il design di FlexPod consente un'infrastruttura flessibile che comprende diversi componenti e versioni software.

Utilizzare i set di regole come guida per la creazione o l'assemblaggio di una configurazione FlexPod valida. I numeri e le regole elencati in questo documento rappresentano i requisiti minimi per una configurazione

FlexPod. Possono essere ampliati nelle famiglie di prodotti incluse, in base alle esigenze di ambienti e casi di utilizzo diversi.

Configurazioni FlexPod supportate e validate

L'architettura di FlexPod è definita dall'insieme di regole descritte in questo documento. I componenti hardware e le configurazioni software devono essere supportati da "Elenco di compatibilità hardware e software Cisco UCS" e a. "Tool di matrice di interoperabilità NetApp (IMT)".

Ogni Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) è una possibile configurazione FlexPod. Cisco e NetApp documentano queste combinazioni di configurazione e le convalidano con test completi end-to-end. Le implementazioni FlexPod che si discostano da queste configurazioni sono pienamente supportate se seguono le linee guida contenute in questo documento e se tutti i componenti sono elencati come compatibili nell'elenco di compatibilità hardware e software di Cisco UCS e in NetApp "IMT".

Ad esempio, l'aggiunta di più controller di storage o Cisco UCS Server e l'aggiornamento del software alle versioni più recenti sono completamente supportati se il software, l'hardware e le configurazioni soddisfano le linee guida definite in questo documento.

NetApp ONTAP

Il software NetApp ONTAP viene installato su tutti i sistemi NetApp FAS, AFF e AFF All SAN Array (ASA). FlexPod è validato con il software ONTAP, fornendo un'architettura di storage altamente scalabile che consente operazioni senza interruzioni, aggiornamenti senza interruzioni e un'infrastruttura dati agile.

Per ulteriori informazioni su ONTAP, consultare "Software per la gestione dei dati ONTAP" pagina del prodotto.

Switching delle modalità operative di Cisco Nexus

È possibile utilizzare una vasta gamma di prodotti Cisco Nexus come componente di switching di una determinata implementazione FlexPod. La maggior parte di queste opzioni sfrutta il tradizionale sistema operativo Cisco Nexus o il software NX-OS. La famiglia di switch Cisco Nexus offre diverse funzionalità all'interno delle sue linee di prodotti. Queste funzionalità sono descritte in dettaglio più avanti in questo documento.

L'offerta di Cisco nell'ambito del networking software-defined è chiamata Application Centric Infrastructure (ACI). La linea di prodotti Cisco Nexus che supporta la modalità ACI, chiamata anche modalità fabric, è la serie Cisco Nexus 9300. Questi switch possono essere implementati anche in modalità NX-OS o standalone.

Cisco ACI è destinato alle implementazioni del data center che si concentrano sui requisiti di un'applicazione specifica. Le applicazioni vengono instanziate attraverso una serie di profili e contratti che consentono la connettività dall'host o dalla macchina virtuale (VM) fino allo storage attraverso la rete.

FlexPod è validato con entrambe le modalità operative degli switch Cisco Nexus. Per ulteriori informazioni sulle modalità ACI e NX-OS, consultare le seguenti pagine Cisco:

- "Cisco Application Centric Infrastructure"
- "Software Cisco NX-OS"

Requisiti hardware minimi

Una configurazione di FlexPod Datacenter ha requisiti hardware minimi, inclusi, a titolo esemplificativo ma non esaustivo, switch, fabric interconnects, server e storage controller NetApp.

È necessario utilizzare Cisco UCS Server. I server C-Series e B-Series sono stati utilizzati nei progetti validati. I Cisco Nexus Fabric Extender (FEX) sono opzionali con i server C-Series.

Una configurazione FlexPod ha i seguenti requisiti hardware minimi:

- Due switch Cisco Nexus in una configurazione ridondante. Questa configurazione può essere costituita da due switch ridondanti della serie Cisco Nexus 5000, 7000 o 9000. I due switch devono essere dello stesso modello e devono essere configurati nella stessa modalità operativa.

  Se si sta implementando un'architettura ACI, è necessario rispettare i seguenti requisiti aggiuntivi:

  - Implementare gli switch Cisco Nexus serie 9000 in una topologia Leaf-spine.
  - Utilizzare tre Cisco Application Policy Infrastructure Controller (APIC).
- Due Cisco UCS 6200, 6300 o 6400 Series Fabric Interconnect in una configurazione ridondante.
- Server Cisco UCS:
  - Se la soluzione utilizza server B-Series, uno chassis per server blade Cisco UCS 5108 B-Series più due server blade Cisco UCS B-Series più due moduli i/o (IOM) 2104, 2204/8, 2408 o 2304.
  - Se la soluzione utilizza server C-Series, due server rack Cisco UCS C-Series.

    Per implementazioni più estese di server rack Cisco UCS C-Series, è possibile scegliere una coppia di moduli FEX 2232PP. Tuttavia, il modello 2232PP non è un requisito hardware.
- Due storage controller NetApp in una configurazione di coppia ad alta disponibilità (ha):

  Questa configurazione può essere costituita da qualsiasi controller di storage NetApp FAS, AFF o ASA supportato. Vedere "NetApp Hardware Universe" Applicazione per un elenco aggiornato dei modelli di controller FAS, AFF e ASA supportati.

  - La configurazione ha richiede due interfacce ridondanti per controller per l'accesso ai dati; le interfacce possono essere FCoE, FC o 10/25/100GB Ethernet (GbE).
  - Se la soluzione utilizza NetApp ONTAP, è necessaria una topologia di interconnessione cluster approvata da NetApp. Per ulteriori informazioni, consultare "Switch" Scheda di NetApp Hardware Universe.
  - Se la soluzione utilizza ONTAP, per l'accesso ai dati sono necessarie almeno due porte 10/25/100GbE aggiuntive per controller.
  - Per i cluster ONTAP con due nodi, è possibile configurare un cluster senza switch a due nodi.
  - Per i cluster ONTAP con più di due nodi, è necessaria una coppia di switch di interconnessione del cluster.
- Uno shelf di dischi NetApp con qualsiasi tipo di disco supportato. Consultare la scheda Shelf di "NetApp Hardware Universe" per un elenco aggiornato dei modelli di shelf di dischi supportati.

Requisiti software minimi

Una configurazione FlexPod ha i seguenti requisiti software minimi:

- ONTAP di NetApp:
  - La versione del software ONTAP richiede ONTAP 9.1 o versione successiva
- Release di Cisco UCS Manager:
  - Cisco UCS 6200 Series Fabric Interconnect - 2.2(8a)
  - Cisco UCS 6300 Series Fabric Interconnect - 3.1(1e)
  - Cisco UCS 6400 Series Fabric Interconnect - 4.0(1)
- Cisco Intersight Managed Mode:
  - Cisco UCS 6400 Series Fabric Interconnect – 4.1(2)
- Per gli switch Cisco Nexus serie 5000, software Cisco NX-OS versione 5.0(3)N1(1c) o successiva, incluso NX-OS 5.1.x.
- Per gli switch Cisco Nexus serie 7000:
  - Lo chassis a 4 slot richiede il software Cisco NX-OS versione 6.1(2) o successiva
  - Lo chassis a 9 slot richiede il software Cisco NX-OS versione 5.2 o successiva
  - Lo chassis a 10 slot richiede il software Cisco NX-OS versione 4.0 o successiva
  - Lo chassis a 18 slot richiede il software Cisco NX-OS versione 4.1 o successiva
- Per gli switch Cisco Nexus serie 9000, software Cisco NX-OS versione 6.1(2) o successiva

> Il software utilizzato in una configurazione FlexPod deve essere elencato e supportato in NetApp "IMT". Alcune funzionalità potrebbero richiedere versioni più recenti del software rispetto a quelle elencate.

Requisiti di connettività

Una configurazione FlexPod ha i seguenti requisiti di connettività:

- Per tutti i componenti è necessaria una rete di gestione out-of-band Ethernet a 100 Mbps/1 GB separata.
- NetApp consiglia di abilitare il supporto jumbo frame in tutto l'ambiente, ma non è necessario.
- Le porte dell'appliance Cisco UCS Fabric Interconnect sono consigliate solo per le connessioni iSCSI e NAS.
- Non è possibile posizionare apparecchiature aggiuntive in linea tra i componenti principali di FlexPod.

Connessioni uplink:

- Le porte dei controller di storage NetApp devono essere collegate agli switch Cisco Nexus serie 5000, 7000 o 9000 per consentire il supporto dei VPC (Virtual Port Channel).
- Gli switch Cisco Nexus serie 5000, 7000 o 9000 sono necessari per i VPC ai controller di storage NetApp.
- Gli switch Cisco Nexus serie 5000, 7000 o 9000 richiedono VPC per le interconnessioni fabric.
- Per un VPC sono necessarie almeno due connessioni. Il numero di connessioni all'interno di un VPC può essere aumentato in base al carico dell'applicazione e ai requisiti di performance.

Connessioni dirette:

- È possibile raggruppare le porte dei controller di storage NetApp direttamente connesse alle interconnessioni fabric per abilitare un canale di porta. VPC non è supportato per questa configurazione.
- I canali di porta FCoE sono consigliati per i progetti FCoE end-to-end.

Boot SAN:

- Le soluzioni FlexPod sono progettate in base a un'architettura DI avvio SAN che utilizza protocolli iSCSI, FC o FCoE. L'utilizzo delle tecnologie boot-from-SAN offre la configurazione più flessibile per l'infrastruttura del data center e abilita le ricche funzionalità disponibili all'interno di ciascun componente dell'infrastruttura. Sebbene l'avvio da SAN sia la configurazione più efficiente, l'avvio dallo storage del server locale è una configurazione valida e supportata.
- L'avvio SAN su FC-NVME non è supportato.

Altri requisiti

Un'architettura FlexPod presenta i seguenti requisiti aggiuntivi di interoperabilità e di supporto:

- Tutti i componenti hardware e software devono essere elencati e supportati su NetApp "IMT", il "Elenco di compatibilità hardware e software Cisco UCS"E Cisco UCS hardware and Software Interoperability Matrix Tool.
- Sono richiesti contratti di supporto validi per tutte le apparecchiature, tra cui:
  - Supporto Smart Net Total Care (SmartNet) per apparecchiature Cisco
  - Supporto SupportEdge Advisor o SupportEdge Premium per le apparecchiature NetApp

Per ulteriori informazioni, consulta NetApp "IMT".

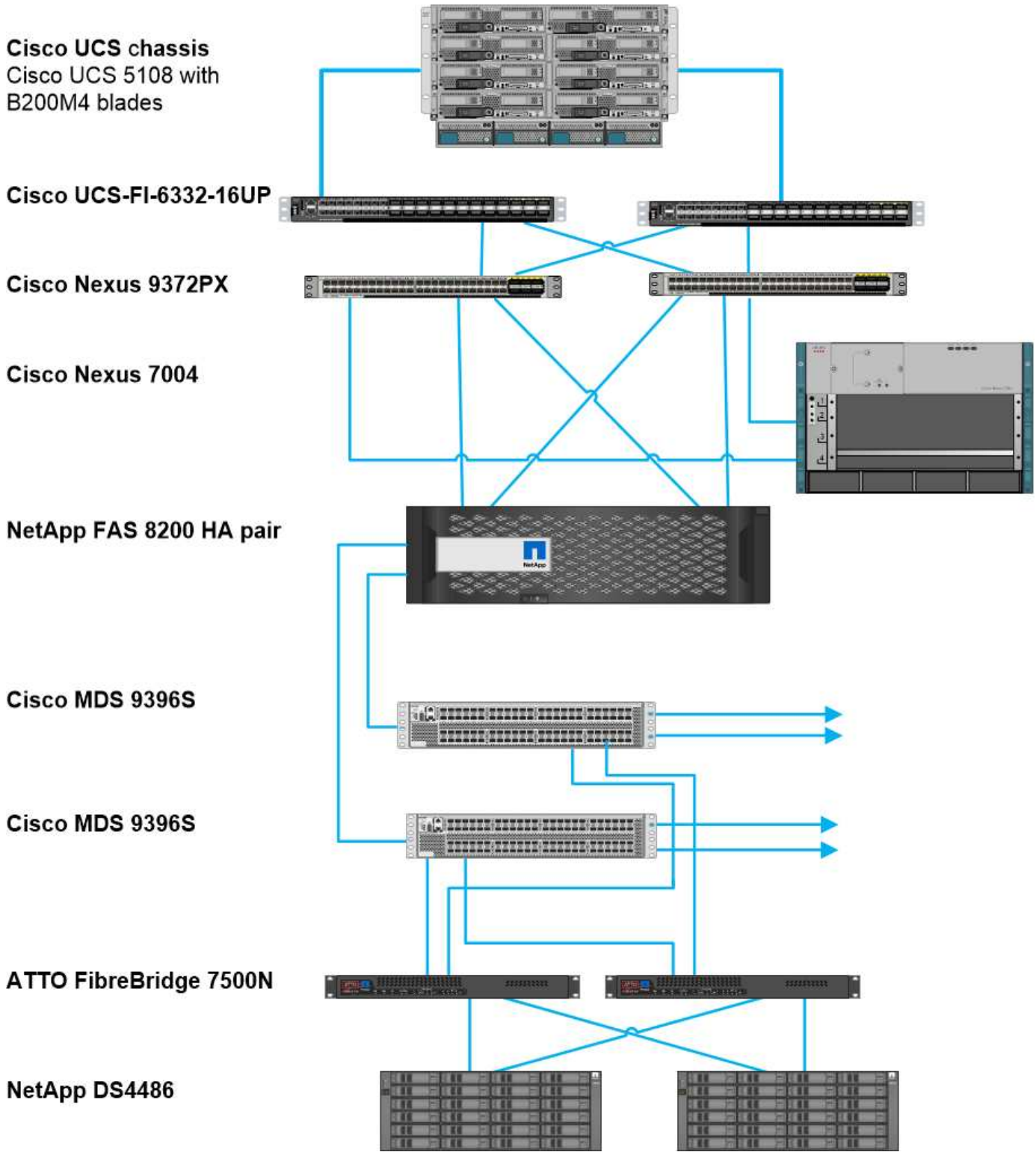
Funzionalità opzionali

NetApp supporta diversi componenti opzionali per migliorare ulteriormente le architetture dei data center FlexPod. I componenti opzionali sono descritti nelle seguenti sottosezioni.

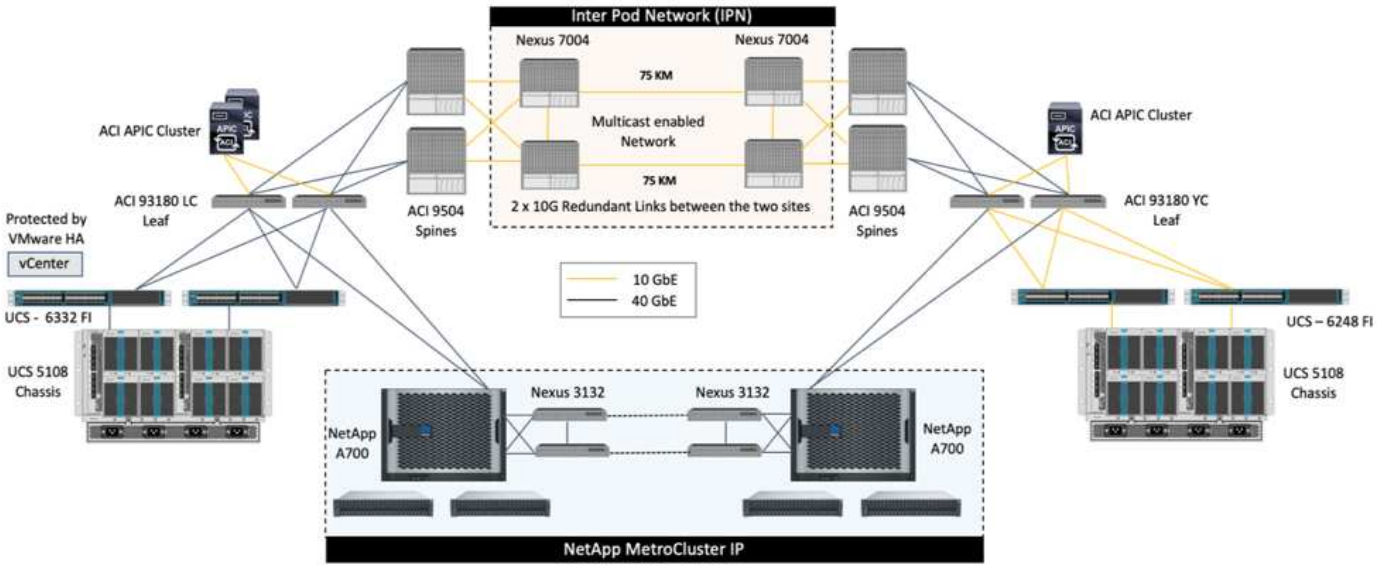
MetroCluster

FlexPod supporta entrambe le varianti del software NetApp MetroCluster per una disponibilità continua, in configurazioni cluster a due o quattro nodi. MetroCluster offre la replica sincrona per i carichi di lavoro critici. Richiede una configurazione a doppio sito connessa allo switch Cisco. La distanza massima supportata tra i siti è di circa 300 km (186 miglia) per MetroCluster FC e aumenta fino a circa 435 km per MetroCluster IP. Le seguenti figure illustrano un data center FlexPod con architettura NetApp MetroCluster e un data center FlexPod con architettura IP NetApp MetroCluster.

La figura seguente mostra il data center FlexPod con architettura NetApp MetroCluster.

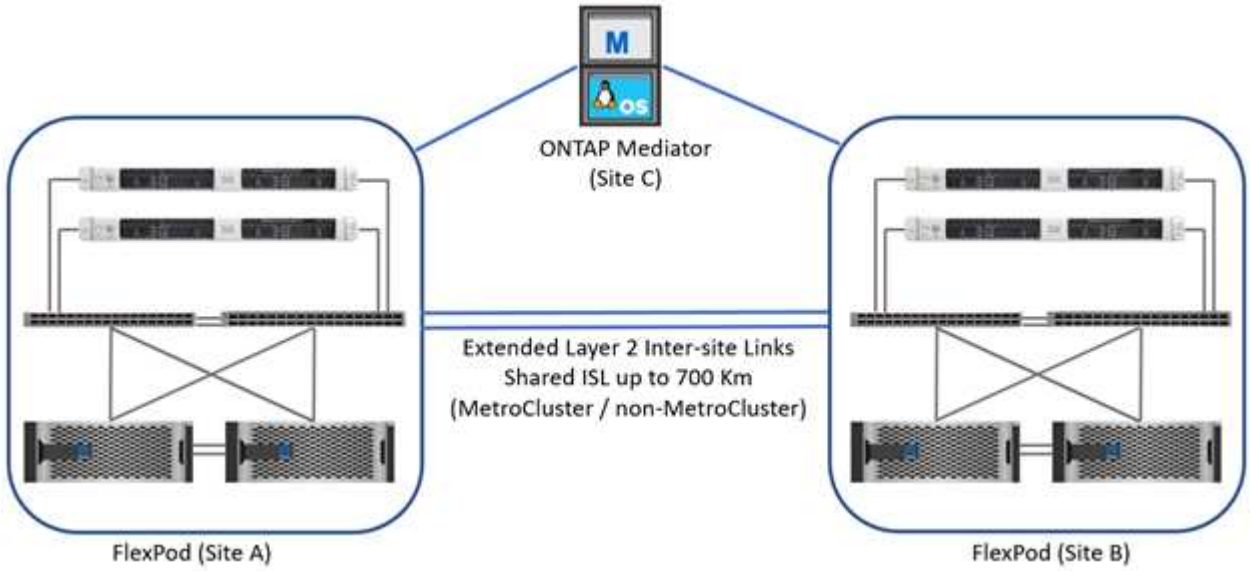


La figura seguente mostra il data center FlexPod con architettura IP NetApp MetroCluster.



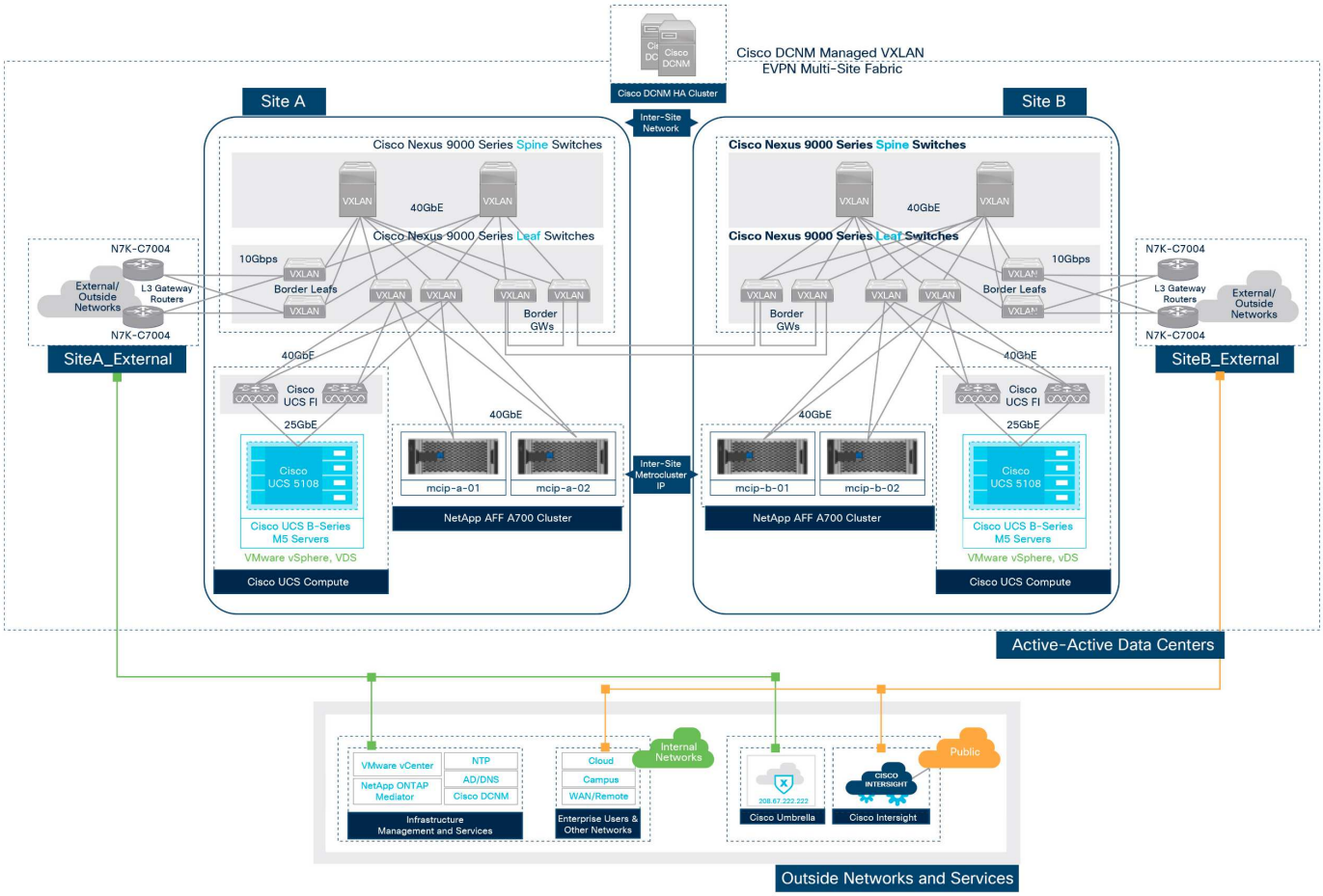
A partire da ONTAP 9.8, è possibile implementare ONTAP Mediator in un terzo sito per monitorare la soluzione IP di MetroCluster e facilitare lo switchover automatizzato non pianificato in caso di disastro del sito.

Per l'implementazione di una soluzione IP FlexPod MetroCluster con connettività estesa di livello 2 da sito a sito, è possibile ottenere risparmi sui costi condividendo ISL e utilizzando switch FlexPod come switch IP MetroCluster conformi se la larghezza di banda della rete e gli switch soddisfano i requisiti come illustrato nella figura seguente, Che raffigura la soluzione IP di FlexPod MetroCluster con condivisione ISL e switch conformi.

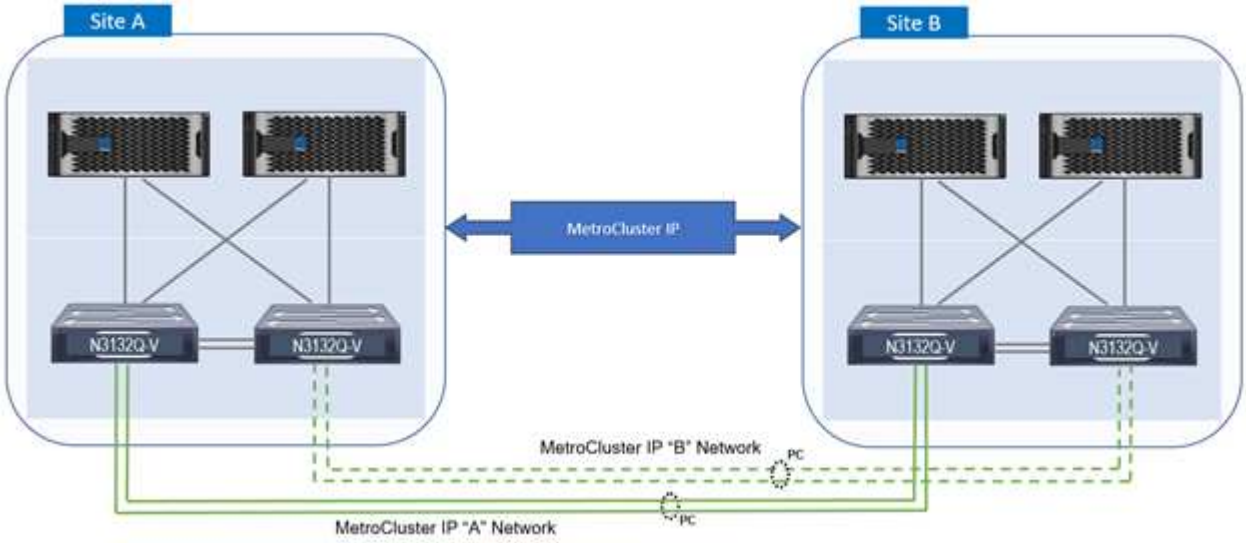


Le due figure seguenti illustrano il fabric VXLAN multi-sito e il fabric di storage IP MetroCluster per una soluzione IP FlexPod MetroCluster con implementazione del fabric VXLAN multi-sito.

- Fabric VXLAN multi-sito per soluzione IP FlexPod MetroCluster



- Fabric di storage IP MetroCluster per soluzione IP FlexPod MetroCluster



FC-NVMe end-to-end

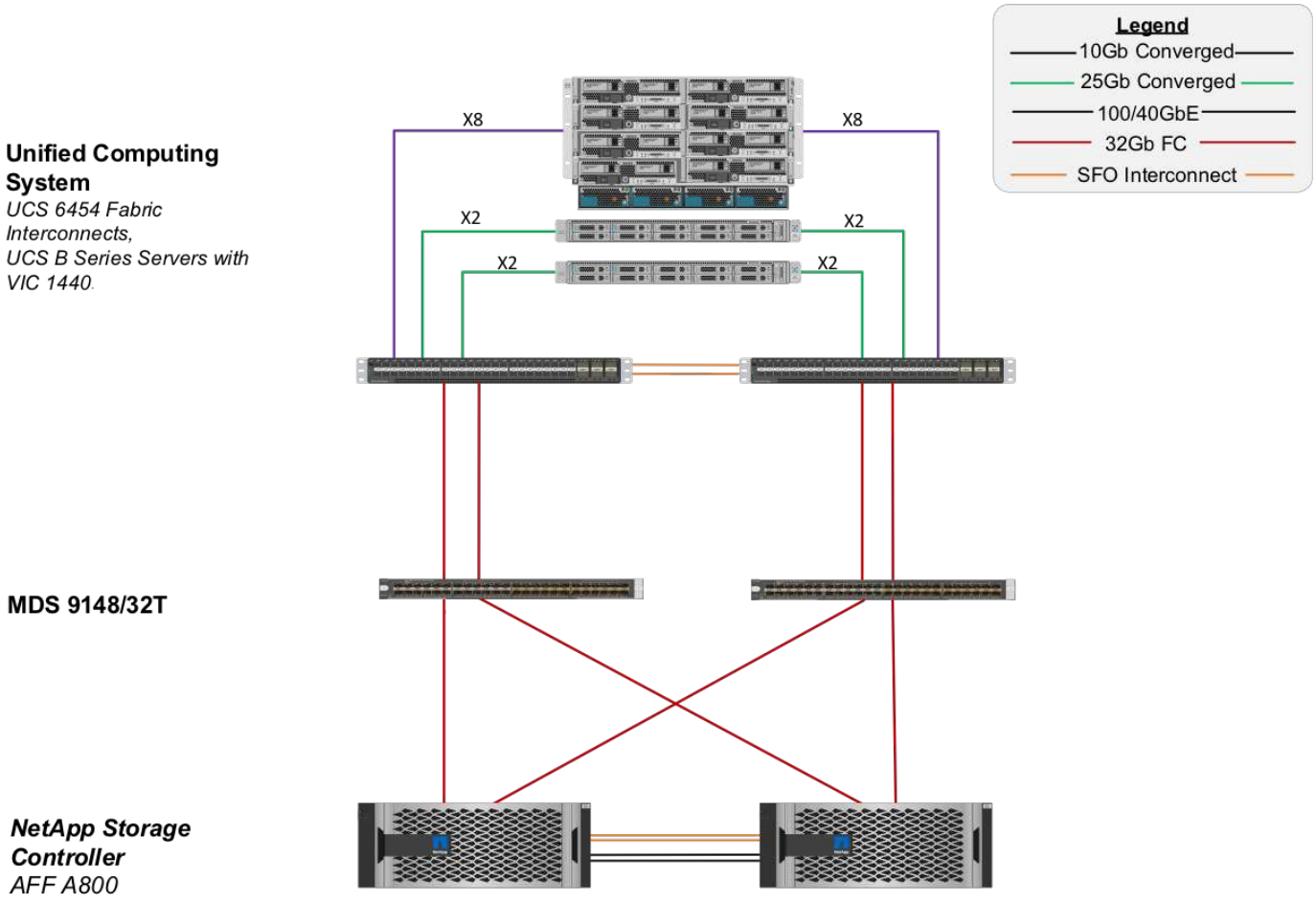
Un FC-NVMe end-to-end estende perfettamente l'infrastruttura SAN esistente di un cliente per le applicazioni in tempo reale, offrendo al contempo IOPS e throughput migliorati con latenza ridotta.

È possibile utilizzare un trasporto SAN FC 32G esistente per trasportare contemporaneamente carichi di lavoro NVMe e SCSI.

La figura seguente illustra il data center FlexPod per FC con Cisco MDS.

Per ulteriori informazioni sulle configurazioni FlexPod e sui vantaggi in termini di prestazioni, vedere "Presentazione del white paper NVMe end-to-end per FlexPod."

Per ulteriori informazioni sull'implementazione di ONTAP, vedere "TR-4684: Implementazione e configurazione di SAN moderne con NVMe".



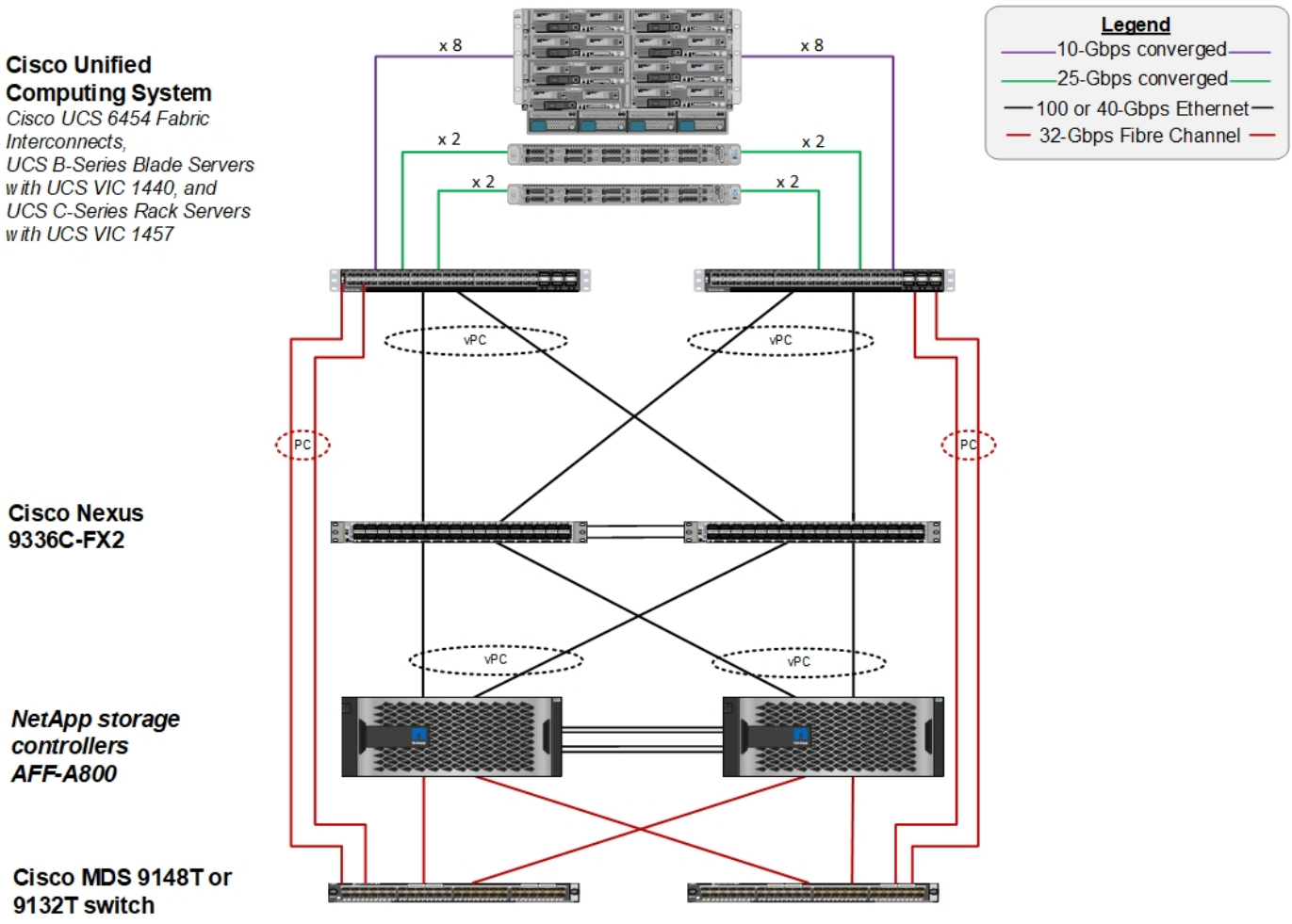
Avvio SAN FC tramite Cisco MDS

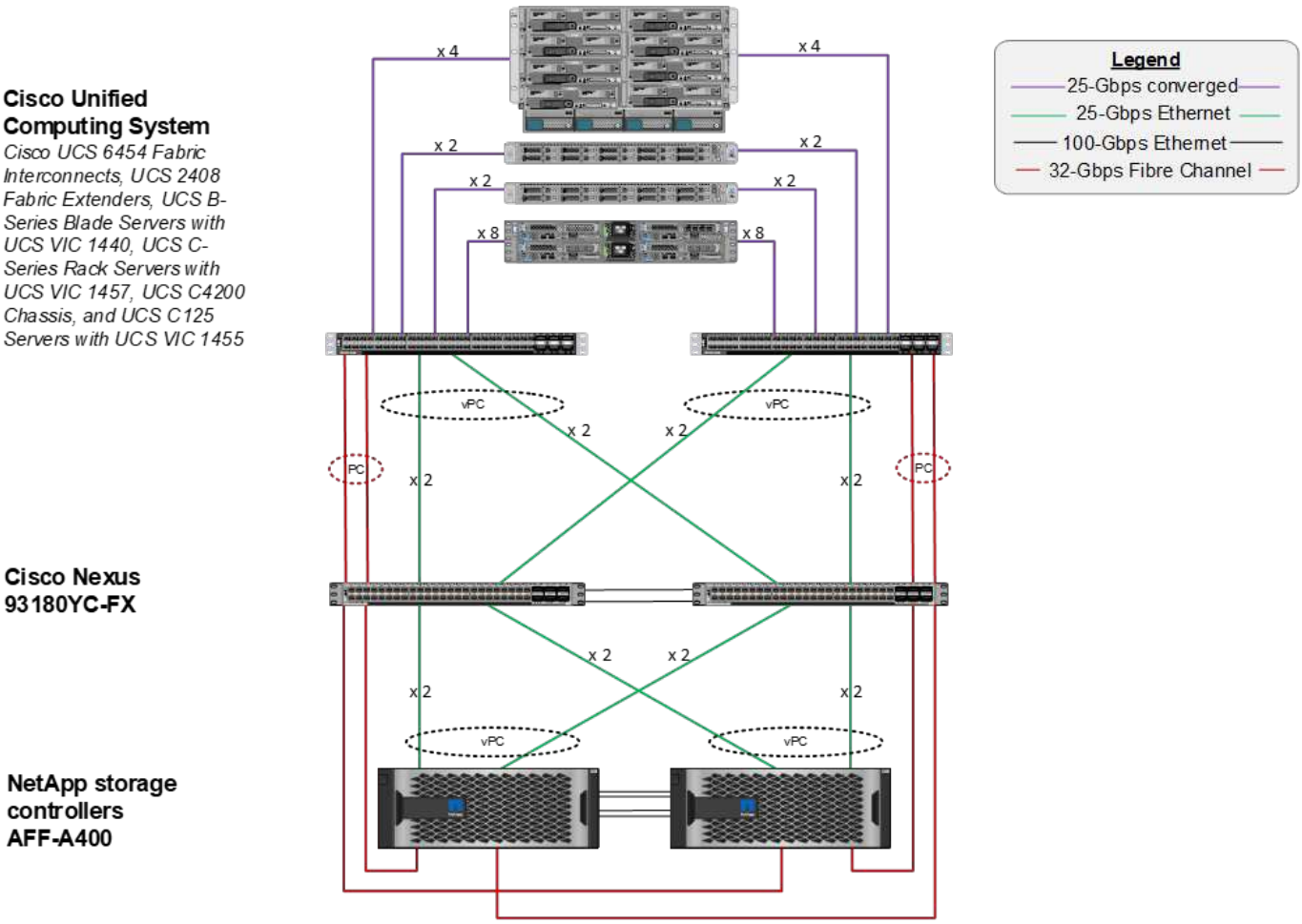
Per fornire una maggiore scalabilità utilizzando una rete SAN dedicata, FlexPod supporta switch FC tramite Cisco MDS e switch Nexus con supporto FC come Cisco Nexus 93108TC-FX. L'opzione di boot FC SAN tramite Cisco MDS ha i seguenti requisiti hardware e di licenza:

- Un minimo di due porte FC per controller di storage NetApp; una porta per ciascun fabric SAN
- Una licenza FC per ciascun controller di storage NetApp
- Switch Cisco MDS e versioni firmware supportate da NetApp "IMT"

Per ulteriori informazioni su una progettazione basata su MDS, vedere CVD "Guida all'implementazione di FlexPod Datacenter con VMware vSphere 6.7U1 Fibre Channel e iSCSI".

Le figure seguenti mostrano un esempio di data center FlexPod per FC con connettività MDS e data center FlexPod per FC con Cisco Nexus 93180YC-FX, rispettivamente.


Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects,
UCS B-Series Blade Servers with UCS VIC 1440, and
UCS C-Series Rack Servers with UCS VIC 1457
Cisco Nexus 9336C-FX2
NetApp storage controllers AFF-A800
Cisco MDS 9148T or 9132T switch
x 8
x 8
x 2
x 2
x 2
x 2
vPC
vPC
PC
PC
vPC
vPC
Legend
10-Gbps converged
25-Gbps converged
100 or 40-Gbps Ethernet
32-Gbps Fibre Channel



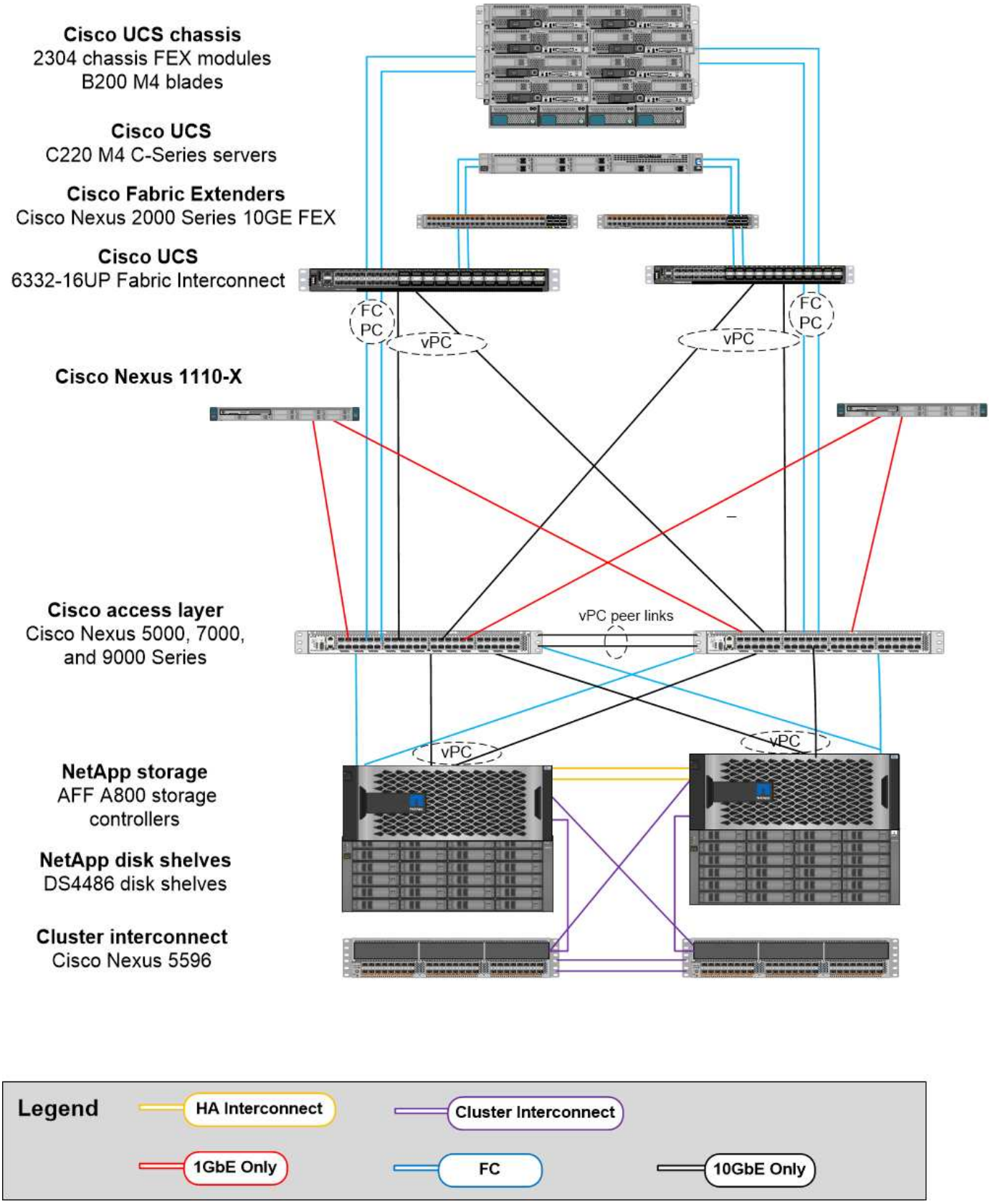
Boot FC SAN con Cisco Nexus

La classica opzione di boot FC SAN ha i seguenti requisiti hardware e di licenza:

- Quando lo zoning FC viene eseguito nello switch Cisco Nexus serie 5000, è necessaria una licenza Storage Protocols Service Package per gli switch Cisco Nexus serie 5000 (FC_FEATURES_PKG).
- Quando lo zoning FC viene eseguito nello switch Cisco Nexus serie 5000, sono necessari collegamenti SAN tra l'interconnessione fabric e lo switch Cisco Nexus serie 5000. Per una ridondanza aggiuntiva, si consiglia DI utilizzare canali di porta SAN tra i collegamenti.
- Gli switch Cisco Nexus 5010, 5020 e 5548P richiedono un modulo FC o Universal Port (UP) separato per la connettività all'interconnessione fabric Cisco UCS e al controller di storage NetApp.
- Cisco Nexus 93180YC-FX richiede una licenza per funzionalità FC per abilitare FC.
- Ogni storage controller NetApp richiede almeno due porte FC da 8/16/32GB per la connettività.
- È necessaria una licenza FC per lo storage controller NetApp.

> L'utilizzo della famiglia di switch Cisco Nexus 7000 o 9000 preclude l'utilizzo di FC tradizionali a meno che non venga eseguito lo zoning FC nell'interconnessione fabric. In tal caso, gli uplink SAN verso lo switch non sono supportati.

La figura seguente mostra una configurazione della connettività FC.



Opzione di boot SAN FCoE

L'opzione di boot SAN FCoE ha i seguenti requisiti hardware e di licenza:

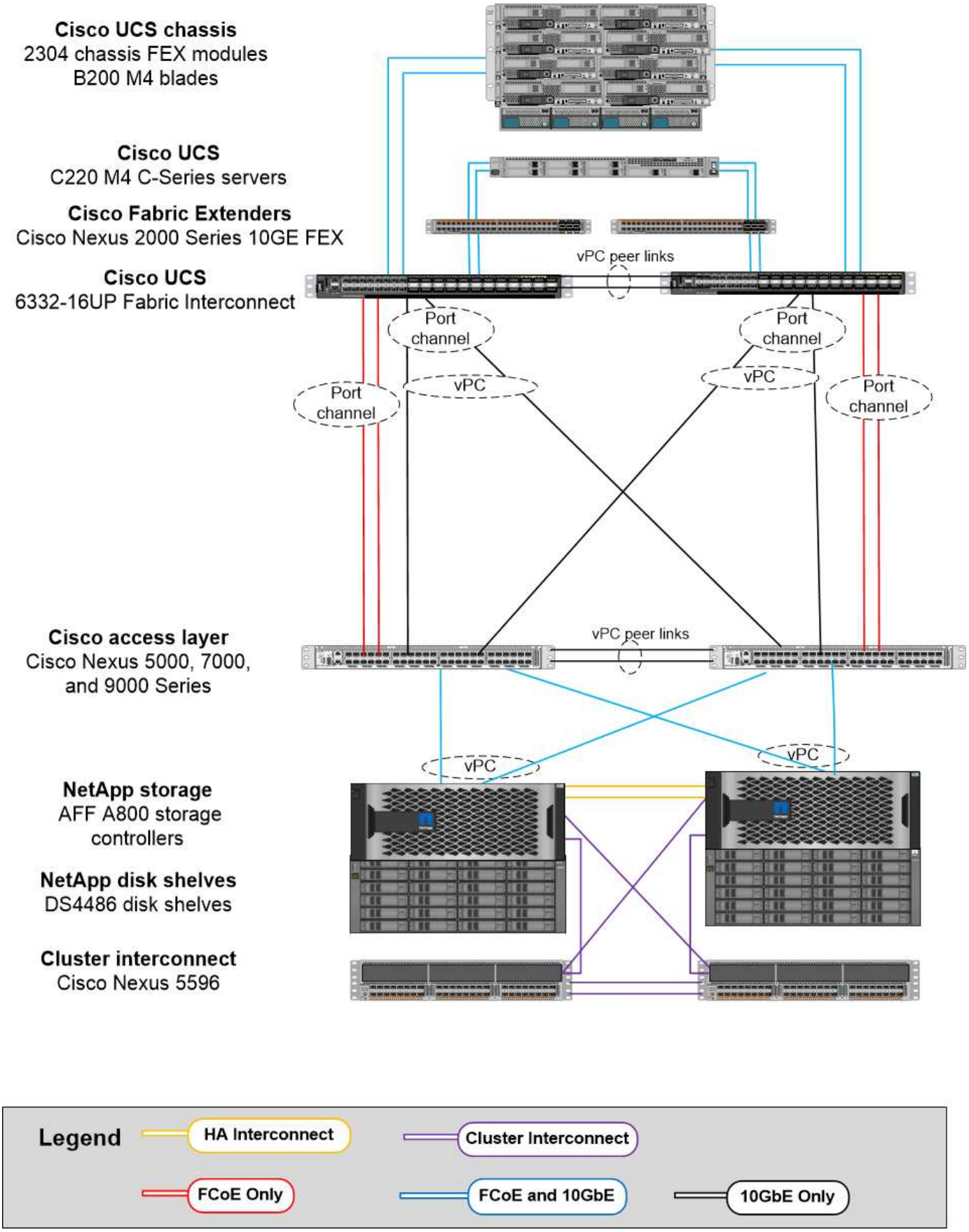
- Quando lo zoning FC viene eseguito nello switch, una licenza Storage Protocols Service Package per gli

switch Cisco Nexus serie 5000 o 7000 (`FC_FEATURES_PKG`) è obbligatorio.

- Quando lo zoning FC viene eseguito nello switch, sono necessari gli uplink FCoE tra l'interconnessione fabric e gli switch Cisco Nexus serie 5000 o 7000. Per un'ulteriore ridondanza, si consiglia di utilizzare anche i canali di porta FCoE tra i collegamenti.
- Ogni storage controller NetApp richiede almeno una scheda add-on UTA (Unified Target Adapter) a due porte per la connettività FCoE, a meno che non siano presenti porte UTA2 (Unified Target Adapter 2) integrate.
- Questa opzione richiede una licenza FC sul controller di storage NetApp.
- Se si utilizzano gli switch Cisco Nexus serie 7000 e lo zoning FC viene eseguito nello switch, è necessaria una scheda di linea in grado di supportare FCoE.

> L'utilizzo degli switch Cisco Nexus 9000 Series impedisce l'utilizzo di FCoE, a meno che non venga eseguito lo zoning FC nell'interconnessione fabric e lo storage non sia connesso all'interconnessione fabric con le porte dell'appliance. In tal caso, gli uplink FCoE verso lo switch non sono supportati.

La figura seguente mostra uno scenario di avvio FCoE.

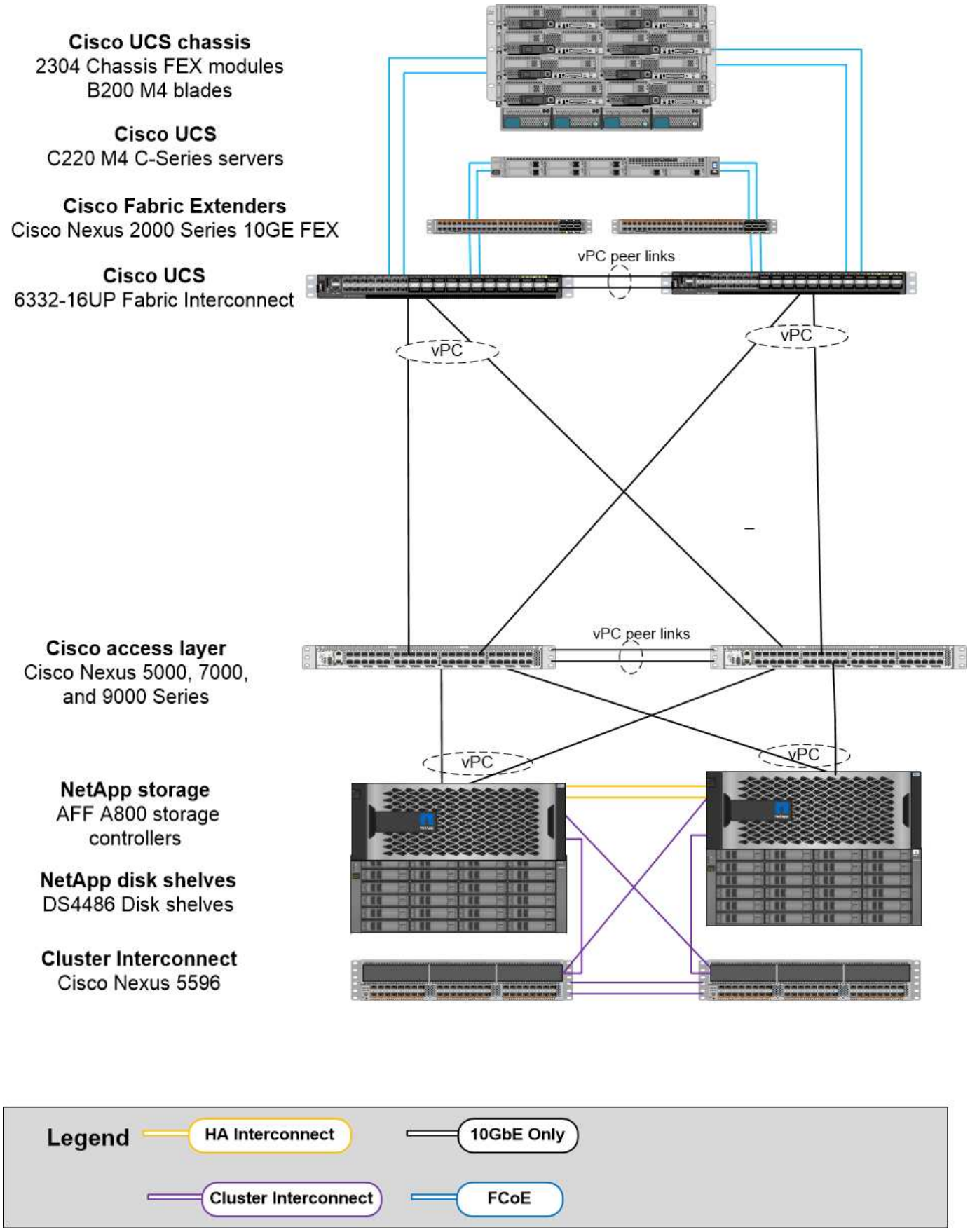

Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
vPC
Port channel
vPC
Port channel
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

Opzione di boot iSCI

L’opzione di boot iSCSI ha i seguenti requisiti hardware e di licenza:

- È necessaria una licenza iSCSI per lo storage controller NetApp.
- Nel Cisco UCS Server è necessario un adattatore in grado di eseguire l’avvio iSCSI.
- È necessario un adattatore Ethernet a due porte da 10 Gbps sul controller di storage NetApp.

La figura seguente mostra una configurazione solo Ethernet avviata mediante iSCSI.


Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage
controllers
NetApp disk shelves
DS4486 Disk shelves
Cluster Interconnect
Cisco Nexus 5596
Legend
HA Interconnect
10GbE Only
Cluster Interconnect
FCoE

Connessione diretta Cisco UCS con lo storage NetApp

I controller NetApp AFF e FAS possono essere collegati direttamente alle interconnessioni fabric UCS di Cisco senza switch SAN upstream.

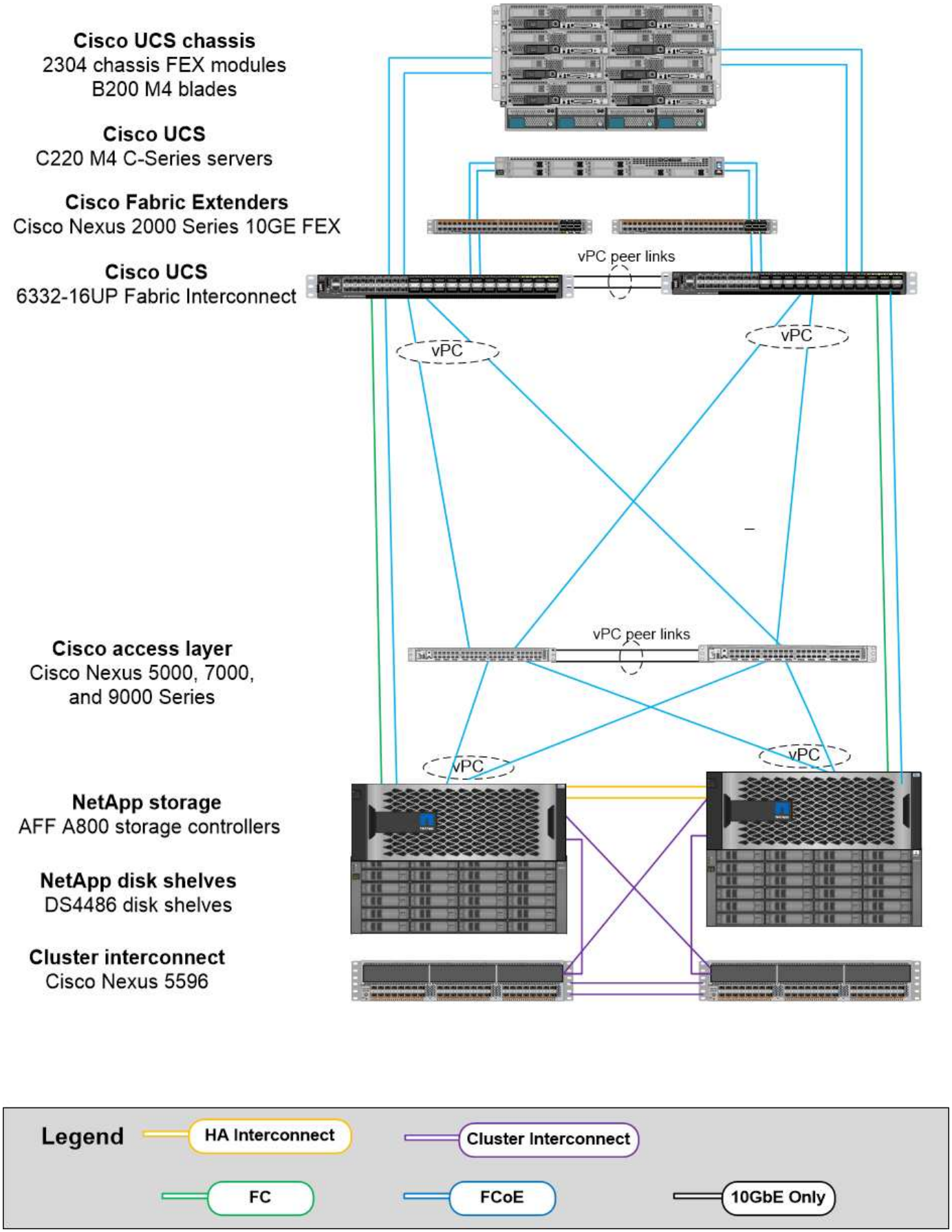
È possibile utilizzare quattro tipi di porte Cisco UCS per connettersi direttamente allo storage NetApp:

- **Porta FC dello storage.** collegare direttamente questa porta a una porta FC sullo storage NetApp.
- **Porta Storage FCoE.** collega direttamente questa porta a una porta FCoE sullo storage NetApp.
- **Appliance port.** collega direttamente questa porta a una porta 10 GbE sullo storage NetApp.
- **Unified storage port.** collega direttamente questa porta a un NetApp UTA.

I requisiti hardware e di licenza sono i seguenti:

- È richiesta una licenza di protocollo per lo storage controller NetApp.
- Sul server è richiesto un adattatore Cisco UCS (Initiator). Per un elenco degli adattatori Cisco UCS supportati, consultare NetApp "IMT".
- È necessario un adattatore di destinazione sul controller di storage NetApp.

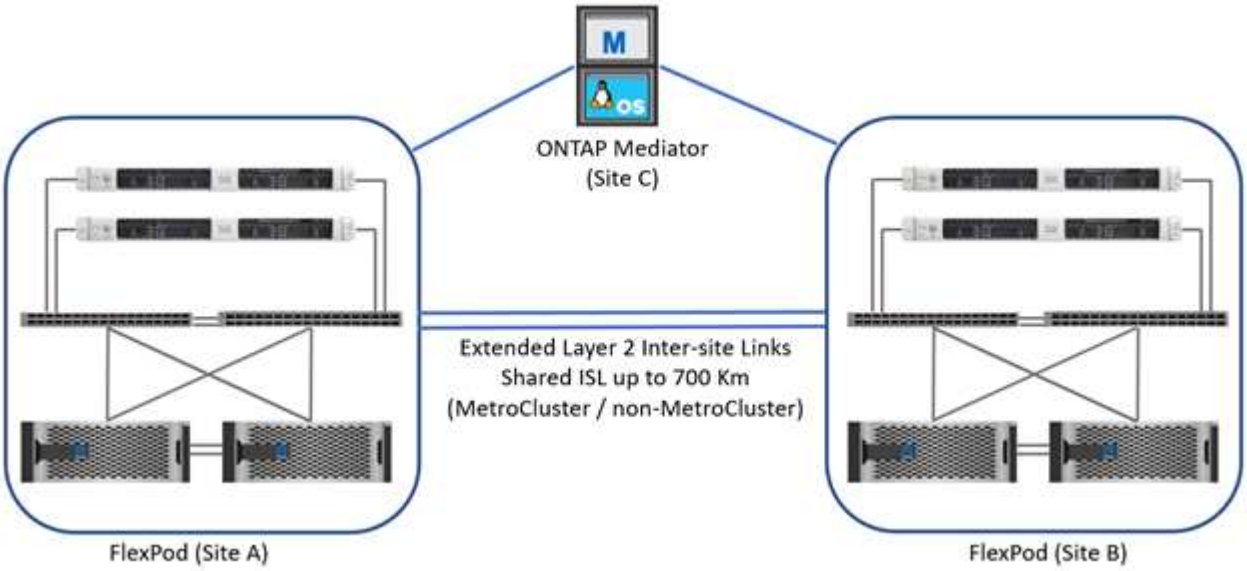
La figura seguente mostra una configurazione FC a connessione diretta.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

Note:

- Cisco UCS è configurato in modalità di commutazione FC.
- Le porte FCoE dalla destinazione alle interconnessioni fabric sono configurate come porte storage FCoE.
- Le porte FC dalla destinazione alle interconnessioni fabric sono configurate come porte di storage FC.

La figura seguente mostra una configurazione di connessione diretta iSCSI/Unified IP.



Note:

- Cisco UCS è configurato in modalità di commutazione Ethernet.
- Le porte iSCSI dalla destinazione alle interconnessioni fabric sono configurate come porte di storage Ethernet per i dati iSCSI.
- Le porte Ethernet dalla destinazione alle interconnessioni fabric sono configurate come porte di storage Ethernet per i dati CIFS/NFS.

Componenti Cisco

Cisco ha contribuito in modo sostanziale alla progettazione e all'architettura di FlexPod, coprendo sia i livelli di calcolo che quelli di rete della soluzione. Questa sezione descrive le opzioni Cisco UCS e Cisco Nexus disponibili per FlexPod. FlexPod supporta server Cisco UCS serie B e C-Series.

Opzioni di interconnessione fabric Cisco UCS

L'architettura FlexPod richiede interconnessioni fabric ridondanti. Quando si aggiungono più chassis Cisco UCS a una coppia di interconnessioni fabric, tenere presente che il numero massimo di chassis in un ambiente è determinato sia da un limite di architettura che da un limite di porta.

I numeri di parte riportati nella tabella seguente si riferiscono alle interconnessioni fabric di base. Non includono l'alimentatore (PSU), i moduli SFP+, QSFP+ o di espansione. Sono supportate ulteriori interconnessioni fabric; vedere "NetApp IMT" per un elenco completo.

Cisco UCS Fabric Interconnect	Codice del ricambio	Specifiche tecniche
Cisco UCS 6332UP	UCS-FI-6332-UP	"Cisco UCS 6332 Fabric Interconnect"
Cisco UCS 6454	UCS-FI-6454-U.	"Cisco UCS 6454 Fabric Interconnect"

Cisco UCS 6454

La serie Cisco UCS 6454 offre connettività Ethernet 10/25/40/100GbE lossless, a bassa latenza e velocità di linea e FCoE, oltre a porte unificate in grado di funzionare sia Ethernet che FC. Le porte a 44 10 Gbps possono funzionare come Ethernet convergente a 10 Gbps o 25 Gbps, di cui otto sono porte unificate in grado di funzionare a 8/16/32 Gbps per FC. Quattro porte operano a 1/10/25Gbps per la connettività legacy, mentre sei porte QSFP fungono da porte uplink o porte di breakout a 40/100Gbps. È possibile stabilire una connettività di rete end-to-end a 100 Gbps con i controller di storage NetApp che supportano gli adattatori a 100 Gbps. Per adattatori e supporto della piattaforma, vedere "NetApp Hardware Universe".

Per ulteriori informazioni sulle porte, consultare "Cisco UCS 6454 Fabric Interconnect" Scheda informativa.

Per le specifiche tecniche relative ai moduli dati QSFP da 100 GB, consultare "Scheda informativa sui moduli Cisco 100GBASE QSFP".

Opzione chassis Cisco UCS B-Series

Per utilizzare i blade Cisco UCS B-Series, è necessario disporre di uno chassis Cisco UCS B-Series. La tabella seguente descrive l'opzione chassis Cisco UCS BSeries.

Chassis Cisco UCS serie B.	Codice del ricambio	Specifiche tecniche
Cisco UCS 5108	N20-C6508	"Chassis per server blade Cisco UCS serie 5100"

Ogni chassis blade Cisco UCS 5108 deve disporre di due IOM Cisco UCS serie 2200/2300/2400 per fornire una connettività ridondante alle interconnessioni fabric.

Opzioni dei server blade Cisco UCS B-Series

I server blade Cisco UCS B-Series sono disponibili in varietà half-width e full-width, con diverse opzioni di CPU, memoria e i/O. I codici ricambio elencati nella tabella seguente si riferiscono al server di base. Non includono la CPU, la memoria, i dischi o le schede mezzanine. Sono disponibili diverse opzioni di configurazione supportate nell'architettura FlexPod.

Blade Cisco UCS serie B.	Codice del ricambio	Specifiche tecniche
CISCO UCS B200 M6	UCSB-B200-M6	"Server blade Cisco UCS B200 M6"

Le generazioni precedenti di blade Cisco UCS B-Series possono essere utilizzate nell'architettura FlexPod, se supportati su "Elenco di compatibilità hardware e software Cisco UCS". Anche i server blade Cisco UCS B-Series devono disporre di un contratto di supporto SmartNet valido.

Opzione chassis Cisco UCS X-Series

Per utilizzare i nodi di calcolo Cisco UCS X-Series, è necessario disporre di uno chassis Cisco UCS X-Series. La seguente tabella descrive l'opzione chassis di Cisco UCS X-Series.

Blade Cisco UCS X-Series	Codice del ricambio	Specifiche tecniche
Cisco UCS 9508 M6	UCSX-9508	"Chassis Cisco UCX9508 X-Series"

Ogni chassis Cisco UCS 9508 deve disporre di due Cisco UCS 9108 Intelligent Fabric Modules (IFM) per fornire una connettività ridondante alle interconnessioni fabric.

Opzioni dei dispositivi Cisco UCS X-Series

I nodi di calcolo Cisco UCS X-Series sono disponibili con diverse opzioni di CPU, memoria e i/O. I numeri di parte elencati nella tabella seguente si riferiscono al nodo di base. Non includono la CPU, la memoria, i dischi o le schede mezzanine. Sono disponibili diverse opzioni di configurazione supportate nell'architettura FlexPod.

Nodi di calcolo Cisco UCS X-Series	Codice del ricambio	Specifiche tecniche
Cisco UCS X210c M6	UCSX-210C-M6	"Nodo di calcolo M6 Cisco UCS X210c"

Opzioni dei server rack Cisco UCS C-Series

I server rack Cisco UCS C-Series sono disponibili in una e due varietà di unità rack (RU), con diverse opzioni di CPU, memoria e i/O. I codici ricambio elencati nella seconda tabella sono relativi al server di base. Non includono CPU, memoria, dischi, schede PCIe (Peripheral Component Interconnect Express) o Cisco Fabric Extender. Sono disponibili diverse opzioni di configurazione supportate nell'architettura FlexPod.

La seguente tabella elenca le opzioni di Cisco UCS C-Series rack Server.

Server rack Cisco UCS C-Series	Codice del ricambio	Specifiche tecniche
CISCO UCS C220 M6	UCSC-C220-M6	"Server rack Cisco UCS C220 M6"
CISCO UCS C225 M6	UCSC-C225-M6	"Server rack Cisco UCS C225 M6"
CISCO UCS C240 M6	UCSC-C240-M6	"Server rack Cisco UCS C240 M6"
CISCO UCS C245 M6	UCSC-C245-M6	"Server rack Cisco UCS C245 M6"

Le generazioni precedenti di server Cisco UCS C-Series possono essere utilizzate nell'architettura FlexPod, se supportati su "Elenco di compatibilità hardware e software Cisco UCS". Anche i server Cisco UCS C-Series devono disporre di un contratto di supporto SmartNet valido.

Opzioni switch Cisco Nexus serie 5000

L'architettura FlexPod richiede switch ridondanti Cisco Nexus serie 5000, 7000 o 9000. I codici ricambio elencati nella tabella seguente si riferiscono allo chassis Cisco Nexus serie 5000; non includono moduli SFP, moduli FC aggiuntivi o moduli Ethernet.

Switch Cisco Nexus serie 5000	Codice del ricambio	Specifiche tecniche
Cisco Nexus 56128P	N5K-C56128P	"Switch per piattaforma Cisco Nexus 5600"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	

Switch Cisco Nexus serie 5000	Codice del ricambio	Specifiche tecniche
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Switch Cisco Nexus 5548 e 5596"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Opzioni switch Cisco Nexus serie 7000

L'architettura FlexPod richiede switch ridondanti Cisco Nexus serie 5000, 7000 o 9000. I numeri di parte elencati nella tabella seguente si riferiscono allo chassis Cisco Nexus serie 7000; non includono moduli SFP, schede di linea o alimentatori, ma includono alloggiamenti per ventole.

Switch Cisco Nexus serie 7000	Codice del ricambio	Specifiche tecniche
Cisco Nexus 7004	N7K-C7004	"Switch Cisco Nexus 7000 a 4 slot"
Cisco Nexus 7009	N7K-C7009	"Switch Cisco Nexus 7000 a 9 slot"
Cisco Nexus 7702	N7K-C7702	"Switch Cisco Nexus 7700 a 2 slot"
Cisco Nexus 7706	N77-C7706	"Switch Cisco Nexus 7700 a 6 slot"

Opzioni switch Cisco Nexus serie 9000

L'architettura FlexPod richiede switch ridondanti Cisco Nexus serie 5000, 7000 o 9000. I codici ricambio elencati nella tabella seguente si riferiscono allo chassis Cisco Nexus serie 9000 e non includono moduli SFP o Ethernet.

Switch Cisco Nexus serie 9000	Codice ricambio	Specifiche tecniche
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Switch Cisco Nexus serie 9300"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Colonna Cisco Nexus 9336PQ ACI	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	
Cisco Nexus 92304QC	N9K-C92304QC	"Switch Cisco Nexus serie 9200"
Cisco Nexus 9236C	N9K-9236C	

Alcuni switch Cisco Nexus serie 9000 dispongono di varianti aggiuntive. Queste varianti sono supportate come parte della soluzione FlexPod. Per l'elenco completo degli switch Cisco Nexus serie 9000, vedere "Switch Cisco Nexus serie 9000" Sul sito Web di Cisco.

Opzioni Cisco APIC

Durante l'implementazione di Cisco ACI, è necessario configurare i tre Cisco APIC oltre agli elementi della sezione "Switch Cisco Nexus serie 9000". Per ulteriori informazioni sulle dimensioni di Cisco APIC, consultare "Scheda informativa sull'infrastruttura Cisco Application Centric."

Per ulteriori informazioni sulle specifiche dei prodotti APIC, fare riferimento alla Tabella 1 fino alla Tabella 3 del "Scheda informativa su Cisco Application Policy Infrastructure Controller".

Opzioni di Cisco Nexus Fabric Extender

I FEX ridondanti Cisco Nexus serie 2000 montati su rack sono consigliati per le architetture FlexPod di grandi dimensioni che utilizzano server C-Series. La tabella seguente descrive alcune opzioni di Cisco Nexus FEX. Sono supportati anche modelli FEX alternativi. Per ulteriori informazioni, consultare "Elenco di compatibilità hardware e software Cisco UCS".

Cisco Nexus rack-mount FEX	Codice del ricambio	Specifiche tecniche
Cisco Nexus 2232PP	N2K-C2232PP	"Cisco Nexus 2000 Series Fabric Extender"
Cisco Nexus 2232TM-E.	N2K-C2232TM-E.	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Cisco Nexus 2300 Platform Fabric Extender"
Cisco Nexus 2348TQCisco Nexus 2348TQ-E.	N2K-C2348TQN2K-C2348TQ-E.	

Opzioni Cisco MDS

Gli switch Cisco MDS sono un componente opzionale dell'architettura FlexPod. I fabric switch SAN ridondanti sono necessari quando si implementa lo switch Cisco MDS per FC SAN. La tabella seguente elenca i numeri di parte e i dettagli di un sottoinsieme di switch Cisco MDS supportati. Vedere "NetApp IMT" e. "Elenco di compatibilità hardware e software Cisco" Per un elenco completo degli switch SAN supportati.

Switch Cisco MDS serie 9000	Codice del ricambio	Descrizione
Cisco MDS 9148T	DS-C9148T-24IK	"Switch Cisco MDS serie 9100"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Switch Cisco MDS serie 9300"

Opzioni di licenza software Cisco

Le licenze sono necessarie per abilitare i protocolli di storage sugli switch Cisco Nexus. Gli switch Cisco Nexus serie 5000 e 7000 richiedono tutti una licenza per i servizi di storage per abilitare il protocollo FC o FCoE per le implementazioni DI boot SAN. Gli switch Cisco Nexus serie 9000 attualmente non supportano FC o FCoE.

Le licenze richieste e i numeri di parte per tali licenze variano a seconda delle opzioni selezionate per ciascun componente della soluzione FlexPod. Ad esempio, i numeri parte delle licenze software variano a seconda del numero di porte e degli switch Cisco Nexus serie 5000 o 7000 scelti. Consultare il proprio rappresentante commerciale per conoscere i codici ricambio esatti. La tabella seguente elenca le opzioni di licenza software Cisco.

Licenze software Cisco	Codice del ricambio	Informazioni sulla licenza
Cisco Nexus 5500 Storage License, 8, 48 e 96 porte	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Licenze delle funzionalità del software Cisco NX-OS"
Licenza per protocolli di storage Cisco Nexus 5010/5020	N5010-SSK9/N5020-SSK9	
Licenza per protocolli di storage Cisco Nexus 5600	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Licenza Cisco Nexus 7000 Storage Enterprise	N7K-SAN1K9	
Licenza Cisco Nexus 9000 Enterprise Services	N95-LAN1K9/N93-LAN1K9	

Opzioni di licenza di supporto Cisco

Per tutte le apparecchiature Cisco nell'architettura FlexPod sono richiesti contratti di supporto SmartNet validi.

Le licenze richieste e i numeri di parte per tali licenze devono essere verificati dal rappresentante commerciale in quanto possono variare per i diversi prodotti. La tabella seguente elenca le opzioni di licenza per il supporto Cisco.

Licenze Cisco Support	Guida alla licenza
Smart Net Total Care Onsite Premium	"Cisco Smart Net Total Care Service"

Componenti NetApp

I controller di storage NetApp forniscono la base dello storage nell'architettura FlexPod sia per l'avvio che per lo storage dei dati delle applicazioni. I componenti NetApp includono storage controller, switch di interconnessione cluster, shelf di dischi e dischi e opzioni di licenza.

Opzioni di storage controller NetApp

L'architettura FlexPod richiede controller NetApp FAS, AFF o AFF ASA ridondanti. I controller eseguono il software ONTAP. Una volta ordinati i controller storage, è possibile precaricare la versione software preferita sui controller. Per ONTAP, viene ordinato un cluster completo. Un cluster completo include una coppia di storage controller e un'interconnessione cluster (switch o switchless).

Sono disponibili diverse opzioni e configurazioni, a seconda della piattaforma di storage selezionata. Per ulteriori informazioni su questi componenti aggiuntivi, rivolgersi al rappresentante di vendita.

Le famiglie di controller elencate nella tabella seguente sono adatte per l'utilizzo in una soluzione FlexPod Datacenter, in quanto la loro connessione agli switch Cisco Nexus è perfetta. Vedere "NetApp Hardware Universe" per informazioni specifiche sulla compatibilità di ciascun modello di controller.

Famiglia di controller storage	Specifiche tecniche
AFF Serie A.	"Documentazione di AFF A-Series"
AFF ASA Serie A.	"Documentazione di AFF ASA A-Series"

Famiglia di controller storage	Specifiche tecniche
Serie FAS	"Documentazione della serie FAS"

Opzioni switch di interconnessione cluster

La seguente tabella elenca gli switch di interconnessione del cluster Nexus disponibili per le architetture FlexPod. Inoltre, FlexPod supporta tutti gli switch cluster supportati da ONTAP, inclusi gli switch non Cisco, purché siano compatibili con la versione di ONTAP implementata. Vedere "NetApp Hardware Universe" per ulteriori informazioni sulla compatibilità per modelli di switch specifici.

Switch di interconnessione del cluster	Specifiche tecniche
Cisco Nexus 3132Q-V.	"Documentazione NetApp: Switch Cisco Nexus 3132Q-V."
Cisco Nexus 9336C-FX2	"Documentazione NetApp: Switch Cisco Nexus 9336C-FX2"

Shelf di dischi e opzioni di dischi NetApp

Per tutti i controller di storage è richiesto un minimo di uno shelf di dischi NetApp.

Il tipo di shelf NetApp selezionato determina i tipi di dischi disponibili all'interno di tale shelf.

> Per tutti gli shelf di dischi e i codici dei dischi, rivolgersi al rappresentante commerciale.

Per ulteriori informazioni sulle unità supportate, fare clic sul collegamento NetApp Hardware Universe nella tabella seguente, quindi selezionare unità supportate.

Shelf di dischi	Specifiche tecniche
DS224C	"Shelf di dischi e supporti di storage supportati su NetApp Hardware Universe"
DS212C	
DS460C	
NS224	

Opzioni di licenza software NetApp

La seguente tabella elenca le opzioni di licenza software NetApp disponibili per l'architettura del data center FlexPod. Il software NetApp viene concesso in licenza a livello di controller FAS e AFF.

Licenze software NetApp	Codice del ricambio	Specifiche tecniche
SW, BUNDLE completo (controller), -C	SW-8XXX-COMP-BNDL-C.	"Libreria di prodotti A–Z"
SW, ONTAP Essentials (controller), -C	SW-8XXX-ONTAP9-C.	

Opzioni di licenza di supporto NetApp

Le licenze NetApp SupportEdge Premium sono necessarie per l'architettura FlexPod, ma i numeri di parte per tali licenze variano in base alle opzioni selezionate nella progettazione FlexPod. Ad esempio, i numeri di parte delle licenze software sono diversi a seconda del controller FAS scelto. Per informazioni sui numeri di parte esatti delle singole licenze di supporto, rivolgersi al rappresentante commerciale. La tabella seguente mostra un esempio di licenza SupportEdge.

Licenze per il supporto NetApp	Codice del ricambio	Specifiche tecniche
SupportEdge Premium 4 ore on-site - mesi: 36	CS-O2-4HR	"NetApp SupportEdge Premium"

Requisiti di alimentazione e cablaggio

Un design FlexPod presenta requisiti minimi per l'alimentazione e il cablaggio.

Requisiti di alimentazione

I requisiti di alimentazione per il data center FlexPod variano in base alla posizione in cui è installata la configurazione del data center FlexPod.

Per ulteriori informazioni sulla potenza massima richiesta e per altre informazioni dettagliate sull'alimentazione, consultare le specifiche tecniche di ciascun componente hardware elencato nella sezione "Specifiche tecniche e riferimenti: Componenti hardware".

Per informazioni dettagliate sull'alimentazione di Cisco UCS, consultare la "Calcolatore di alimentazione Cisco UCS".

Per i dati sull'alimentazione dei controller di storage NetApp, consultare "NetApp Hardware Universe". In piattaforme, selezionare la piattaforma di storage che si desidera utilizzare nella configurazione (FAS/V-Series o AFF). Selezionare la versione di ONTAP e lo storage controller, quindi fare clic sul pulsante Mostra risultati.

Requisiti minimi per i cavi

Il numero e il tipo di cavi e adattatori richiesti variano in base all'implementazione del data center FlexPod. Il tipo di cavo, il tipo di ricetrasmettitore e il numero vengono determinati durante il processo di progettazione in base alle proprie esigenze. La tabella seguente elenca il numero minimo di cavi necessari.

Hardware	Numero di modello	Cavi necessari
Chassis Cisco UCS	Cisco UCS 5108	Almeno due cavi twinaxial per ogni modulo Cisco UCS 2104XP, 2204XP o 2208XP

Hardware	Numero di modello	Cavi necessari
Cisco UCS Fabric Interconnects	Cisco UCS 6248UP	• Due cavi Cat5e per le porte di gestione • Due cavi Cat5e per le interconnessioni L1, L2, per coppia di interconnessioni fabric • Almeno quattro cavi twinaxial per interconnessione fabric • Almeno quattro cavi FC per interconnessione fabric
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• Due cavi Cat5e per le porte di gestione • Due cavi Cat5e per le interconnessioni L1, L2, per coppia di interconnessioni fabric • Almeno quattro cavi twinaxial per interconnessione fabric	Cisco UCS 6324
	• Due porte di gestione a 10/100/1000Mbps • Almeno due cavi twinaxial per interconnessione fabric	Switch Cisco Nexus serie 5000 e 7000
	Cisco Nexus serie 5000	
• Almeno due cavi 10 GbE in fibra o twinaxial per switch • Almeno due cavi FC per switch (se è richiesta la connettività FC/FCoE)	Cisco Nexus serie 7000	Switch Cisco Nexus serie 9000

Hardware	Numero di modello	Cavi necessari
Cisco Nexus serie 9000	Almeno due cavi da 10 GbE per switch	Controller NetApp FAS
AFF Serie A.	• Una coppia di cavi SAS o SATA per controller di storage • Almeno due cavi FC per controller, se si utilizza un FC legacy • Almeno due cavi da 10 GbE per controller • Almeno un cavo GbE per la gestione per controller • Per ONTAP, sono necessari otto cavi twinaxial corti per ogni coppia di switch di interconnessione del cluster	
Serie FAS	Shelf di dischi NetApp	DS212C
Due cavi SAS, SATA o FC per shelf di dischi		DS224C
		DS460C
		NS224

Specifiche tecniche e riferimenti

Le specifiche tecniche forniscono dettagli sui componenti hardware di una soluzione FlexPod, come chassis, FEX, server, switch, e storage controller.

Chassis per server blade Cisco UCS serie B.

Le specifiche tecniche dello chassis del server blade Cisco UCS B-Series, come mostrato nella tabella seguente, includono i seguenti componenti:

- Numero di unità rack
- Numero massimo di blade
- Funzionalità Unified Fabric
- Larghezza di banda i/o midplane per server
- Numero di alloggiamenti i/o per FEX

Componente	Chassis per server blade Cisco UCS serie 5100
Unità rack	6
Massima larghezza delle lame	4
Massimo di blade a mezza larghezza	8
Capacità di Unified Fabric	Sì

Componente	Chassis per server blade Cisco UCS serie 5100
I/o midplane	Fino a 80 Gbps di larghezza di banda i/o per server
Alloggiamenti i/o per FEXs	Due alloggiamenti per Cisco UCS 2104XP, 2204/8XP, 2408XP e 2304 FEX

Per ulteriori informazioni, consultare "Scheda informativa sullo chassis per server blade Cisco UCS serie 5100".

Server blade Cisco UCS B-Series

Le specifiche tecniche dei server blade Cisco UCS B-Series, come mostrato nella tabella seguente, includono i seguenti componenti:

- Numero di socket del processore
- Supporto del processore
- Capacità di memoria
- Dimensioni e velocità
- Supporto per l'avvio SAN
- Numero di slot per schede mezzanine
- Throughput i/o massimo
- Fattore di forma
- Numero massimo di server per chassis

Componente	Scheda informativa Cisco UCS
CISCO UCS B200 M6	"Server blade Cisco UCS B200 M6"

Server rack Cisco UCS C-Series

Le specifiche tecniche dei server rack Cisco UCS C-Series includono il supporto del processore, la capacità massima di memoria, il numero di slot PCIe e le dimensioni del fattore di forma. Per ulteriori informazioni sui modelli di server UCS compatibili, consultare "Compatibilità hardware Cisco" elenco. Le seguenti tabelle illustrano rispettivamente le schede tecniche di C-Series rack Server e l'opzione chassis Cisco UCS C-Series.

Componente	Scheda informativa Cisco UCS
CISCO UCS C220 M6	"Server rack Cisco UCS C220 M6"
CISCO UCS C225 M6	"Server rack Cisco UCS C225 M6"
CISCO UCS C240 M6	"Server rack Cisco UCS C240 M6"
CISCO UCS C245 M6	"Server rack Cisco UCS C245 M6"

Chassis Cisco UCS X-Series

Le specifiche tecniche dello chassis Cisco UCS X-Series, come mostrato nella tabella seguente, includono i seguenti componenti:

- Numero di unità rack

- Numero massimo di nodi
- Funzionalità Unified Fabric
- Numero di alloggiamenti i/o per gli IFM

Componente	Chassis con nodo di calcolo Cisco UCS 9508 X-Series
Unità rack	7
Numero massimo di nodi	8
Capacità di Unified Fabric	Sì
Alloggiamenti i/o per IFM	Due alloggiamenti per Cisco UCS 9108 Intelligent Fabric Modules (IFM)

Per ulteriori informazioni, consultare "Scheda informativa sullo chassis Cisco UCS X9508 X-Series".

Nodo di calcolo Cisco UCS X-Series

Le specifiche tecniche per il nodo di calcolo Cisco UCS X-Series, come mostrato nella seguente tabella, includono i seguenti componenti:

- Numero di socket del processore
- Supporto del processore
- Capacità di memoria
- Dimensioni e velocità
- Supporto per l'avvio SAN
- Numero di slot per schede mezzanine
- Throughput i/o massimo
- Fattore di forma
- Numero massimo di nodi di calcolo per chassis

Componente	Scheda informativa Cisco UCS
Cisco UCS X210c M6	"Nodo di calcolo M6 Cisco UCS X210c"

Raccomandazione GPU per FlexPod ai, ML e DL

I server rack Cisco UCS C-Series elencati nella tabella seguente possono essere utilizzati in un'architettura FlexPod per l'hosting di carichi di lavoro ai, ML e DL. I server Cisco UCS C480 ML M5 sono progettati appositamente per i carichi di lavoro ai, ML e DL e utilizzano GPU NVIDIA basate su SXM2, mentre gli altri server utilizzano GPU basate su PCIe.

La tabella seguente elenca anche le GPU consigliate che possono essere utilizzate con questi server.

Server	GPU
CISCO UCS C220 M6	NVIDIA T4
CISCO UCS C225 M6	NVIDIA T4

Server	GPU
CISCO UCS C240 M6	NVIDIA TESLA A10, A100
CISCO UCS C245 M6	NVIDIA TESLA A10, A100

Adattatori Cisco UCS VIC per server blade Cisco UCS B-Series

Le specifiche tecniche degli adattatori Cisco UCS Virtual Interface Card (VIC) per i server blade Cisco UCS B-Series includono i seguenti componenti:

- Numero di porte uplink
- Performance per porta (IOPS)
- Potenza
- Numero di porte blade
- Offload dell'hardware
- Supporto della virtualizzazione single root input/output (SR-IOV)

Tutte le architetture FlexPod attualmente validate utilizzano un VIC Cisco UCS. Altri adattatori sono supportati se sono elencati su NetApp "IMT" E sono compatibili con l'implementazione di FlexPod, ma potrebbero non offrire tutte le funzionalità delineate nelle architetture di riferimento corrispondenti. La seguente tabella illustra le schede tecniche dell'adattatore VIC Cisco UCS.

Componente	Scheda informativa Cisco UCS
Cisco UCS Virtual Interface Adapter	"Schede informative Cisco UCS VIC"

Cisco UCS Fabric Interconnects

Le specifiche tecniche per le interconnessioni fabric Cisco UCS includono le dimensioni del fattore di forma, il numero totale di porte e slot di espansione e la capacità di throughput. La seguente tabella illustra le schede tecniche di interconnessione fabric Cisco UCS.

Componente	Scheda informativa Cisco UCS
Cisco UCS 6248UP	"Cisco UCS 6200 Series Fabric Interconnect"
Cisco UCS 6296UP	
Cisco UCS 6324	"Cisco UCS 6324 Fabric Interconnect"
Cisco UCS 6300	"Cisco UCS 6300 Series Fabric Interconnect"
Cisco UCS 6454	"Cisco UCS 6400 Series Fabric Interconnect"

Switch Cisco Nexus serie 5000

Le specifiche tecniche degli switch Cisco Nexus serie 5000, incluse le dimensioni del fattore di forma, il numero totale di porte e il supporto per il modulo Layer-3 e la scheda figlia, sono contenute nella scheda informativa per ciascuna famiglia di modelli. Queste schede tecniche sono disponibili nella seguente tabella.

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus 5548UP	"Switch Cisco Nexus 5548UP"

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus 5596UP (2U)	"Switch Cisco Nexus 5596UP"
Cisco Nexus 56128P	"Switch Cisco Nexus 56128P"
Cisco Nexus 5672UP	"Switch Cisco Nexus 5672UP"

Switch Cisco Nexus serie 7000

Le specifiche tecniche degli switch Cisco Nexus serie 7000, incluse le dimensioni del fattore di forma e il numero massimo di porte, sono contenute nella scheda informativa per ciascuna famiglia di modelli. Queste schede tecniche sono disponibili nella seguente tabella.

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus 7004	"Switch Cisco Nexus serie 7000"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Switch Cisco Nexus serie 7700"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Switch Cisco Nexus serie 9000

Le specifiche tecniche degli switch Cisco Nexus serie 9000 sono contenute nella scheda tecnica di ciascun modello. Le specifiche includono le dimensioni del fattore di forma, il numero di supervisori, moduli fabric e slot per schede di linea e il numero massimo di porte. Queste schede tecniche sono disponibili nella seguente tabella.

Componente	Scheda informativa su Cisco Nexus
Cisco Nexus serie 9000	"Switch Cisco Nexus serie 9000"
Cisco Nexus serie 9500	"Switch Cisco Nexus serie 9500"
Cisco Nexus serie 9300	"Switch Cisco Nexus serie 9300"
Switch Cisco Nexus 9336PQ ACI spine	"Switch Cisco Nexus 9336PQ ACI spine"
Cisco Nexus serie 9200	"Switch per piattaforma Cisco Nexus 9200"

Controller Cisco Application Policy Infrastructure

Quando si implementa Cisco ACI, oltre agli elementi della sezione "Switch Cisco Nexus serie 9000", È necessario configurare tre Cisco APIC. La seguente tabella elenca la scheda informativa di Cisco APIC.

Componente	Scheda informativa di Cisco Application Policy Infrastructure
Cisco Application Policy Infrastructure Controller	"Scheda informativa di Cisco APIC"

Dettagli di Cisco Nexus Fabric Extender

Le specifiche tecniche di Cisco Nexus FEX includono velocità, numero di porte e collegamenti fissi e dimensioni del fattore di forma.

La seguente tabella elenca la scheda informativa di Cisco Nexus 2000 Series FEX.

Componente	Scheda informativa di Cisco Nexus Fabric Extender
Cisco Nexus 2000 Series Fabric Extender	"Scheda informativa su Nexus 2000 Series FEX"

Moduli SFP

Per informazioni sui moduli SFP, consultare le seguenti risorse:

- Per informazioni su Cisco 10Gb SFP, vedere "Moduli Cisco 10 Gigabit".
- Per informazioni su Cisco 25GB SFP, vedere "Moduli Cisco 25 Gigabit".
- Per informazioni sul modulo Cisco QSFP, consultare "Scheda informativa sui moduli Cisco 40GBASE QSFP".
- Per informazioni su Cisco 100GB SFP, vedere "Moduli Cisco 100 Gigabit".
- Per informazioni sul modulo Cisco FC SFP, consultare "Scheda informativa sulla famiglia di ricetrasmettitori collegabili Cisco MDS 9000".
- Per informazioni su tutti i moduli Cisco SFP e transceiver supportati, vedere "Note sull'installazione del modulo ricetrasmettitore SFP e SFP+ Cisco" e. "Cisco Transceiver Module".

Storage controller NetApp

Le specifiche tecniche dei controller di storage NetApp includono i seguenti componenti:

- Configurazione dello chassis
- Numero di unità rack
- Quantità di memoria
- Caching NetApp FlashCache
- Dimensione dell'aggregato
- Dimensione del volume
- Numero di LUN
- Storage di rete supportato
- Numero massimo di volumi NetApp FlexVol
- Numero massimo di host SAN supportati
- Numero massimo di copie Snapshot

Serie FAS

Tutti i modelli disponibili di controller di storage FAS sono supportati per l'utilizzo in un data center FlexPod. Le specifiche dettagliate per tutti i controller storage della serie FAS sono disponibili nella "NetApp Hardware Universe". Per informazioni dettagliate su un modello FAS specifico, consultare la documentazione specifica per la piattaforma riportata nella tabella seguente.

Componente	Documentazione sulla piattaforma controller della serie FAS
Serie FAS9000	"Scheda informativa della serie FAS9000"
Serie FAS8700	"Scheda informativa della serie FAS8700"
Serie FAS8300	"Scheda informativa della serie FAS8300"
Serie FAS500f	"Scheda informativa della serie FAS500f"
Serie FAS2700	"Scheda informativa della serie FAS2700"

AFF Serie A.

Tutti gli attuali modelli di storage controller NetApp AFF Serie A sono supportati per l'utilizzo in FlexPod. Per ulteriori informazioni, consultare "Specifiche tecniche di AFF" scheda tecnica e nella "NetApp Hardware Universe". Per informazioni dettagliate su un modello AFF specifico, consultare la documentazione specifica per la piattaforma riportata nella tabella seguente.

Componente	Documentazione sulla piattaforma del controller AFF Serie A.
NetApp AFF A800	"Documentazione sulla piattaforma AFF A800"
NetApp AFF A700	"Documentazione sulla piattaforma AFF A700"
NetApp AFF A700	"Documentazione sulla piattaforma AFF A700s"
NetApp AFF A400	"Documentazione sulla piattaforma AFF A400"
NetApp AFF A250	"Documentazione sulla piattaforma AFF A250"

AFF ASA Serie A.

Tutti gli attuali modelli di storage controller NetApp AFF ASA Serie A sono supportati per l'utilizzo in FlexPod. Ulteriori informazioni sono disponibili nelle risorse di documentazione di tutti gli array SAN, nel report tecnico del sistema array ONTAP AFF All SAN e nel NetApp Hardware Universe. Per informazioni dettagliate su un modello AFF specifico, consultare la documentazione specifica per la piattaforma riportata nella tabella seguente.

Componente	Documentazione sulla piattaforma del controller AFF Serie A.
NetApp AFF ASA A800	"Documentazione sulla piattaforma AFF ASA A800"
NetApp AFF ASA A700	"Documentazione sulla piattaforma AFF ASA A700"
NetApp AFF ASA A400	"Documentazione sulla piattaforma AFF ASA A400"
NetApp AFF ASA A250	"Documentazione sulla piattaforma AFF ASA A250"
NetApp AFF ASA A220	"Documentazione sulla piattaforma AFF ASA A220"

Shelf di dischi NetApp

Le specifiche tecniche per gli shelf di dischi NetApp includono le dimensioni del fattore di forma, il numero di dischi per enclosure e i moduli i/o per shelf; questa documentazione è disponibile nella seguente tabella. Per ulteriori informazioni, consultare "Shelf di dischi e supporti di storage NetApp - specifiche tecniche" e a. "NetApp Hardware Universe".

Componente	Documentazione sugli shelf di dischi NetApp FAS/AFF
Shelf di dischi NetApp DS212C	"Documentazione shelf di dischi DS212C"
Shelf di dischi NetApp DS224C	"Documentazione sugli shelf di dischi DS224C"
Shelf di dischi NetApp DS460C	"Documentazione sugli shelf di dischi DS460C"
Shelf di dischi NVMe-SSD NetApp NS224	"Documentazione shelf di dischi NS224"

Dischi NetApp

Le specifiche tecniche dei dischi NetApp includono dimensioni del fattore di forma, capacità del disco, rpm del disco, controller di supporto e requisiti di versione ONTAP. Queste specifiche sono disponibili nella sezione Drives (unità) di "NetApp Hardware Universe".

Apparecchiature legacy

FlexPod è una soluzione flessibile che consente di utilizzare le apparecchiature esistenti e le nuove apparecchiature attualmente in vendita da Cisco e NetApp. Occasionalmente, alcuni modelli di apparecchiature di Cisco e NetApp sono indicati come EOL (End of Life).

Anche se questi modelli di apparecchiature non sono più disponibili, se si è acquistato uno di questi modelli prima della data di fine disponibilità (EOA), è possibile utilizzare l'apparecchiatura in una configurazione FlexPod. È possibile fare riferimento a un elenco completo dei modelli di apparecchiature legacy supportati in FlexPod che non sono più in vendita sul "Indice di fine disponibilità dei programmi di assistenza e supporto NetApp".

Per ulteriori informazioni sulle apparecchiature Cisco legacy, consultare gli avvisi Cisco EOL e EOA per "Server rack Cisco UCS C-Series", "Server blade Cisco UCS serie B.", e. "Switch Nexus".

Il supporto del fabric FC legacy include quanto segue:

- Fabric da 2 GB
- Fabric da 4 GB

Il software legacy include:

- NetApp Data ONTAP funziona in 7-Mode, 7.3.5 e versioni successive
- Da ONTAP 8.1.x a 9.0.x
- Cisco UCS Manager 1.3 e versioni successive
- Cisco UCS Manager da 2.1 a 2.2.7

Dove trovare ulteriori informazioni

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

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com/"

- Comunicazioni di supporto NetApp

  "https://mysupport.netapp.com/info/communications/index.html"

- Tool di matrice di interoperabilità NetApp (IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe

  "https://hwu.netapp.com/"

- Supporto NetApp

  "https://mysupport.netapp.com/"

Data center FlexPod

FlexPod DataCenter con NetApp SnapMirror Business Continuity e ONTAP 9.10

TR-4920: Data center FlexPod con NetApp SnapMirror Business Continuity e ONTAP 9.10

Jyh-ishing Chen, NetApp

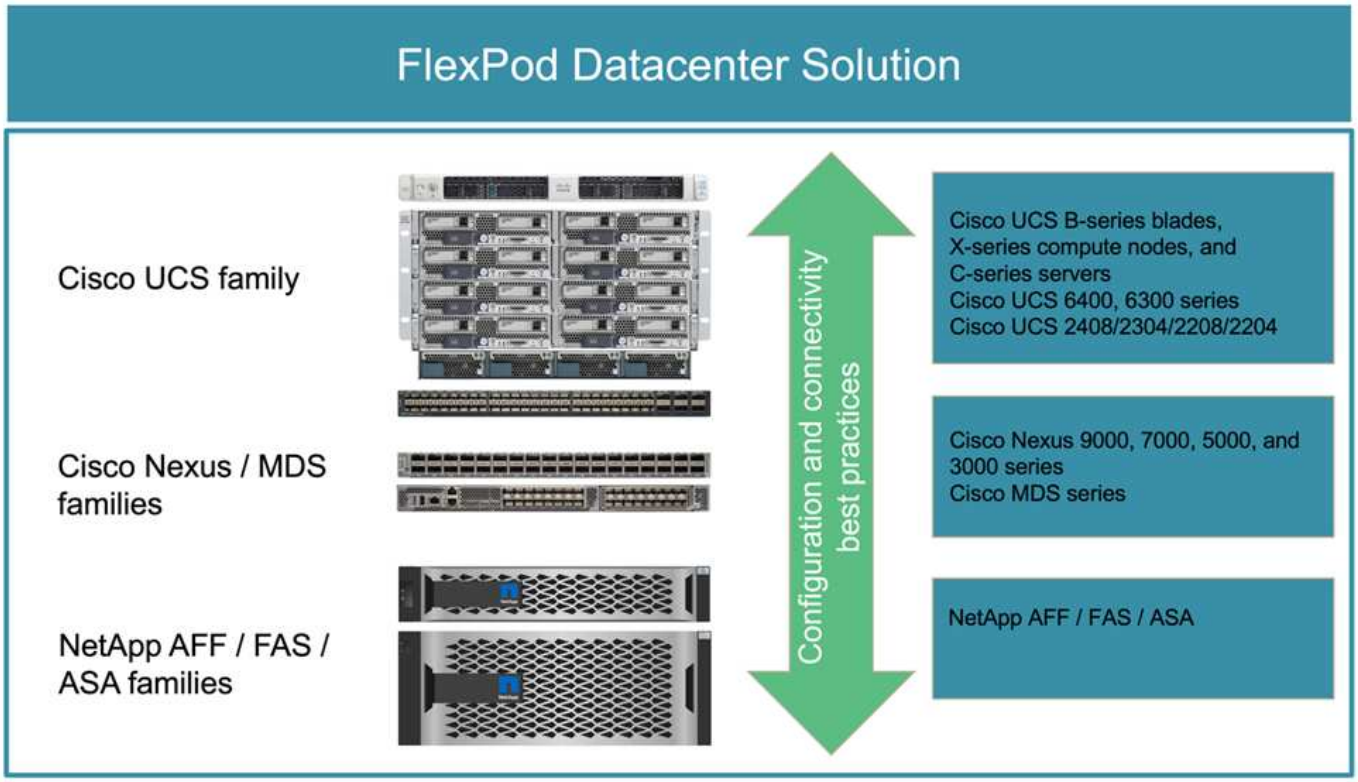
Introduzione

Soluzione FlexPod

FlexPod è un'architettura per data center con infrastruttura convergente basata su Best practice che include i seguenti componenti di Cisco e NetApp:

- Cisco Unified Computing System (Cisco UCS)
- Famiglie di switch Cisco Nexus e MDS
- Sistemi NetApp FAS, NetApp AFF e NetApp All SAN Array (ASA)

La figura seguente mostra alcuni dei componenti utilizzati per la creazione di soluzioni FlexPod. Questi componenti sono collegati e configurati in base alle Best practice di Cisco e NetApp per fornire una piattaforma ideale per l'esecuzione sicura di una vasta gamma di workload aziendali.



È disponibile un ampio portfolio di Cisco Validated Designs (CVD) e NetApp Verified Architectures (NVA). Questi CVD e NVA coprono tutti i principali carichi di lavoro dei data center e sono il risultato di continue

collaborazioni e innovazioni tra NetApp e Cisco sulle soluzioni FlexPod.

Incorporando test e validazioni estesi nel processo di creazione, i CVD e gli NVA di FlexPod offrono progetti di architettura di soluzioni di riferimento e guide di implementazione passo per aiutare partner e clienti a implementare e adottare le soluzioni FlexPod. Utilizzando questi CVD e NVA come guide per la progettazione e l'implementazione, le aziende possono ridurre i rischi, ridurre il downtime della soluzione e aumentare la disponibilità, la scalabilità, la flessibilità e la sicurezza delle soluzioni FlexPod che implementano.

Ciascuna delle famiglie di componenti FlexPod illustrate (Cisco UCS, switch Cisco Nexus/MDS e storage NetApp) offre opzioni di piattaforma e risorse per scalare l'infrastruttura in verticale o in orizzontale, supportando al contempo le funzionalità e le funzionalità richieste dalle Best practice di configurazione e connettività di FlexPod. FlexPod può anche scalare verso l'esterno per ambienti che richiedono implementazioni multiple e coerenti, implementando ulteriori stack FlexPod.

Disaster recovery e business continuity

Le aziende possono adottare diversi metodi per garantire che possano ripristinare rapidamente le applicazioni e i servizi dati in caso di disastri. La disponibilità di un piano di disaster recovery (DR) e business continuity (BC), l'implementazione di una soluzione che soddisfi gli obiettivi di business e l'esecuzione di test regolari degli scenari di disastro consente alle aziende di eseguire il ripristino da un disastro e di continuare i servizi business critici in seguito a una situazione di disastro.

Le aziende potrebbero avere requisiti di DR e BC diversi per diversi tipi di applicazioni e servizi dati. Alcune applicazioni e alcuni dati potrebbero non essere necessari in situazioni di emergenza o di emergenza, mentre altri potrebbero dover essere continuamente disponibili per supportare i requisiti di business.

Per applicazioni mission-critical e servizi dati che potrebbero interrompere il business quando non sono disponibili, è necessaria una valutazione accurata per rispondere a domande come il tipo di manutenzione e scenari di disastro che l'azienda deve prendere in considerazione, la quantità di dati che l'azienda può permettersi di perdere in caso di disastro e la rapidità con cui il ripristino può e deve avvenire.

Per le aziende che si affidano ai servizi dati per la generazione di ricavi, potrebbe essere necessario proteggere i servizi dati da una soluzione in grado di resistere non solo a diversi scenari di guasto singolo punto di errore, ma anche a uno scenario di disastro di interruzione del sito per garantire operazioni di business continue.

Obiettivo del punto di ripristino e obiettivo del tempo di ripristino

L'RPO (Recovery Point Objective) misura la quantità di dati, in termini di tempo, che è possibile permettersi di perdere, o il punto in cui è possibile ripristinare i dati. Con un piano di backup giornaliero, un'azienda potrebbe perdere un giorno di dati perché le modifiche apportate ai dati dall'ultimo backup potrebbero andare perse in caso di disastro. Per i servizi dati business-critical e mission-critical, potrebbe essere necessario un RPO zero e un piano e infrastrutture associati per proteggere i dati senza alcuna perdita di dati.

L'RTO (Recovery Time Objective) misura il tempo che è possibile dedicare a non disporre dei dati o la rapidità con cui i servizi dati devono essere ripristinati. Ad esempio, un'azienda potrebbe disporre di un'implementazione di backup e ripristino che utilizza nastri tradizionali per determinati set di dati a causa delle sue dimensioni. Di conseguenza, il ripristino dei dati dai nastri di backup potrebbe richiedere diverse ore o persino giorni in caso di guasto dell'infrastruttura. Le considerazioni sul tempo devono includere anche il tempo necessario per eseguire il backup dell'infrastruttura oltre al ripristino dei dati. Per i servizi dati mission-critical, potrebbe essere necessario un RTO molto basso e quindi tollerare solo un tempo di failover di secondi o minuti per riportare rapidamente i servizi dati online per la business continuity.

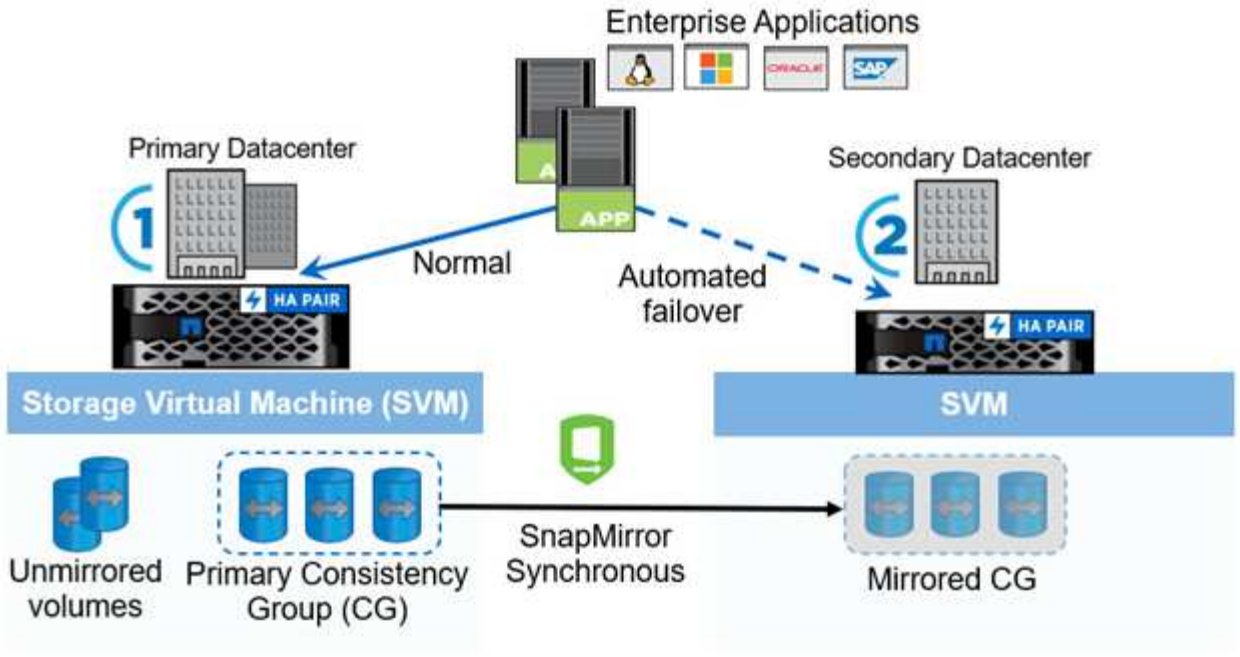
SM-BC

A partire da ONTAP 9.8, è possibile proteggere i carichi di lavoro SAN per il failover trasparente delle applicazioni con NetApp SM-BC. È possibile creare relazioni di gruppo di coerenza tra due cluster AFF o due cluster ASA per la replica dei dati in modo da ottenere un RPO pari a zero e un RTO pari quasi a zero.

La soluzione SM-BC replica i dati utilizzando la tecnologia SnapMirror Synchronous su una rete IP. Offre granularità a livello di applicazione e failover automatico per proteggere i servizi dati business-critical come Microsoft SQL Server, Oracle e così via con LUN SAN basate su protocollo iSCSI o FC. Un mediatore ONTAP implementato in un terzo sito monitora la soluzione SM-BC e consente il failover automatico in caso di disastro del sito.

Un gruppo di coerenza (CG) è un insieme di volumi FlexVol che fornisce una garanzia di coerenza dell'ordine di scrittura per il carico di lavoro dell'applicazione che deve essere protetto per la business continuity. Consente copie Snapshot simultanee coerenti con il crash di un insieme di volumi in un momento specifico. Una relazione SnapMirror, nota anche come relazione CG, viene stabilita tra un CG di origine e un CG di destinazione. Il gruppo di volumi scelto come parte di un CG può essere mappato a un'istanza dell'applicazione, a un gruppo di istanze dell'applicazione o a un'intera soluzione. Inoltre, le relazioni del gruppo di coerenza SM-BC possono essere create o eliminate su richiesta in base ai requisiti e alle modifiche aziendali.

Come illustrato nella figura seguente, i dati del gruppo di coerenza vengono replicati in un secondo cluster ONTAP per il disaster recovery e la business continuity. Le applicazioni sono dotate di connettività ai LUN in entrambi i cluster ONTAP. L'i/o viene normalmente gestito dal cluster primario e riprende automaticamente dal cluster secondario se si verifica un disastro sul primario. Durante la progettazione di una soluzione SM-BC, è necessario osservare i conteggi degli oggetti supportati per le relazioni CG (ad esempio, un massimo di 20 CGS e 200 endpoint) per evitare di superare i limiti supportati.



"Avanti: Soluzione FlexPod SM-BC."

Soluzione FlexPod SM-BC

"Precedente: Introduzione."

Panoramica della soluzione

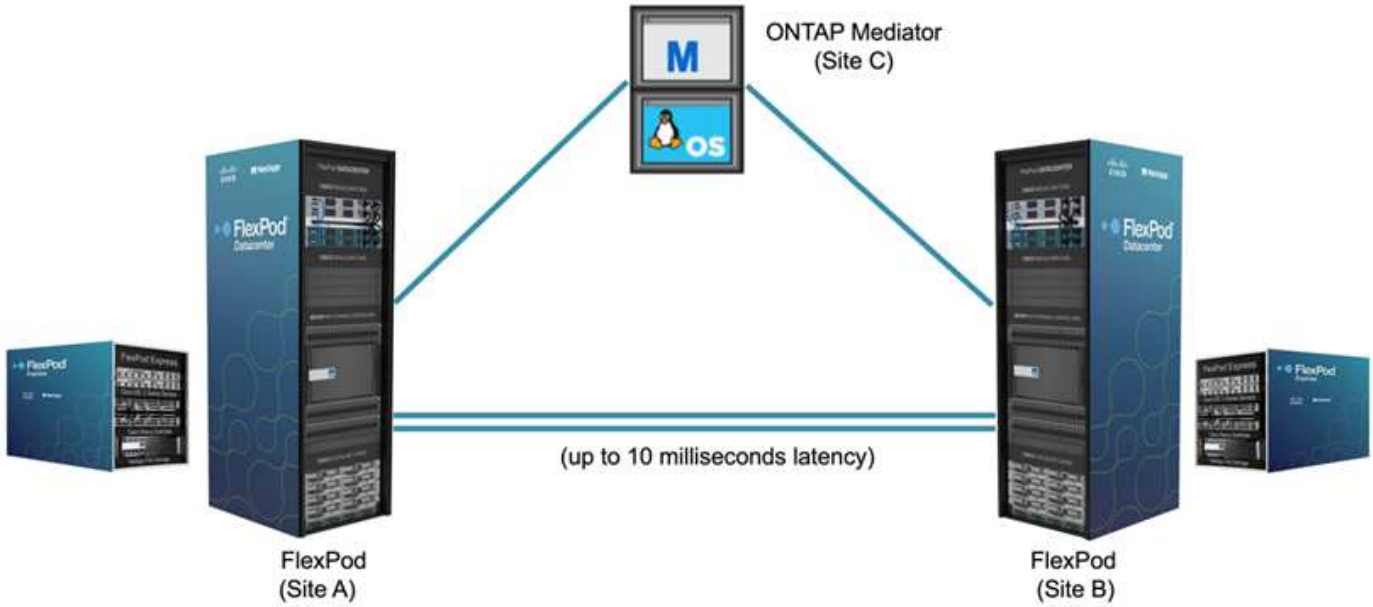
Ad alto livello, una soluzione FlexPod SM-BC è costituita da due sistemi FlexPod, situati in due siti separati da una certa distanza, collegati e accoppiati tra loro per fornire una soluzione di data center altamente disponibile, altamente flessibile e altamente affidabile in grado di garantire la continuità del business nonostante un guasto del sito.

Oltre a implementare due nuove infrastrutture FlexPod per creare una soluzione FlexPod SM-BC, la soluzione può essere implementata anche su due infrastrutture FlexPod esistenti compatibili con SM-BC o aggiungendo un nuovo FlexPod per il peer con un FlexPod esistente.

I due sistemi FlexPod in una soluzione FlexPod SM-BC non devono necessariamente essere identici nelle configurazioni. Tuttavia, i due cluster ONTAP devono essere delle stesse famiglie di storage, due sistemi AFF o due sistemi ASA, ma non necessariamente lo stesso modello hardware. La soluzione SM-BC non supporta i sistemi FAS.

I due siti FlexPod richiedono una connettività di rete che soddisfi la larghezza di banda della soluzione e i requisiti di qualità del servizio e che abbia una latenza di andata e ritorno inferiore a 10 millisecondi (10 ms) tra i siti, come richiesto dalla soluzione ONTAP SM-BC. Per la convalida di questa soluzione FlexPod SM-BC, i due siti FlexPod sono interconnessi tramite una rete Layer-2 estesa nello stesso laboratorio.

La soluzione NetApp ONTAP SM-BC offre la replica sincrona tra i due cluster di storage NetApp per l'alta disponibilità e il disaster recovery in un campus o in un'area metropolitana. Il mediatore ONTAP implementato in un terzo sito monitora la soluzione e consente il failover automatizzato in caso di disastro del sito. La figura seguente fornisce una vista di alto livello dei componenti della soluzione.



Con la soluzione FlexPod SM-BC, puoi implementare un cloud privato basato su VMware vSphere su un'infrastruttura distribuita ma integrata. La soluzione integrata consente di coordinare più siti come un'unica infrastruttura di soluzione per proteggere i servizi dati da una varietà di scenari di singolo punto di errore e da un guasto completo del sito.

Questo report tecnico evidenzia alcune considerazioni di progettazione end-to-end della soluzione FlexPod SM-BC. I professionisti sono incoraggiati a fare riferimento alle informazioni disponibili nei vari FlexPod CVD e NVA per ulteriori dettagli sull'implementazione della soluzione FlexPod.

Sebbene la soluzione sia stata validata implementando due sistemi FlexPod basati sulle Best practice FlexPod

documentate nei CVD, prende in conto i requisiti della soluzione SM-BC. La soluzione FlexPod SM-BC implementata descritta in questo report è stata validata per la resilienza e la tolleranza agli errori durante diversi scenari di guasto, nonché per uno scenario di guasto simulato del sito.

Requisiti della soluzione

La soluzione FlexPod SM-BC è progettata per soddisfare i seguenti requisiti chiave:

- Business continuity per applicazioni business-critical e servizi dati in caso di guasto di un data center completo (sito)
- Posizionamento flessibile e distribuito dei carichi di lavoro con mobilità dei carichi di lavoro nei data center
- Affinità del sito in cui l'accesso ai dati delle macchine virtuali avviene localmente, dallo stesso sito del data center, durante le normali operazioni
- Ripristino rapido senza perdita di dati in caso di guasto di un sito

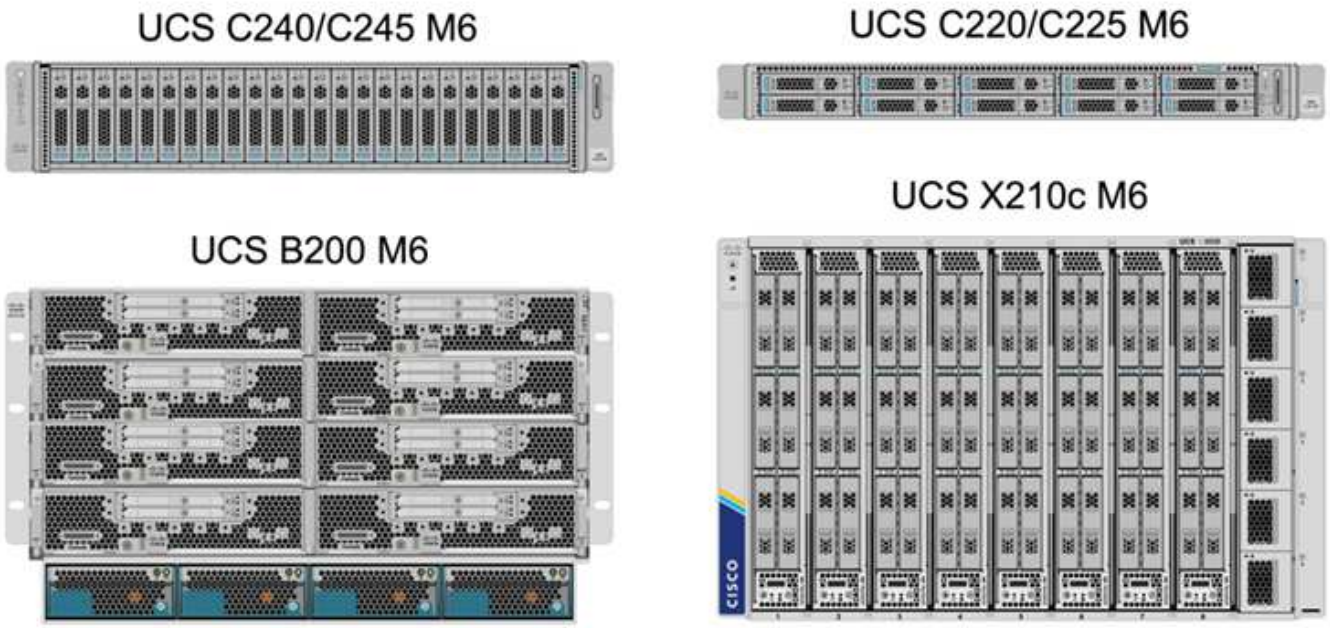
Componenti della soluzione

Componenti di calcolo Cisco

Cisco UCS è un'infrastruttura di calcolo integrata per fornire risorse di calcolo unificate, Unified Fabric e gestione unificata. Consente alle aziende di automatizzare e accelerare l'implementazione delle applicazioni, tra cui la virtualizzazione e i carichi di lavoro bare-metal. Cisco UCS supporta un'ampia gamma di casi di utilizzo dell'implementazione, tra cui sedi remote e filiali, data center e casi di utilizzo del cloud ibrido. A seconda dei requisiti specifici della soluzione, l'implementazione di calcolo di FlexPod può utilizzare una vasta gamma di componenti a diverse scale. Le seguenti sottosezioni forniscono informazioni aggiuntive su alcuni componenti UCS.

Server UCS e nodo di calcolo

La figura seguente mostra alcuni esempi dei componenti server UCS, tra cui i server rack UCS C- Series, lo chassis UCS 5108 con server blade B-Series e il nuovo chassis UCS X9508 con nodi di calcolo X-Series. I server rack Cisco UCS C-Series sono disponibili in un fattore di forma a una e due unità rack (RU), modelli basati su CPU Intel e AMD e con diverse velocità della CPU e core, memoria e opzioni di i/O. I server blade Cisco UCS B-Series e i nuovi nodi di calcolo X-Series sono inoltre disponibili con diverse opzioni di CPU, memoria e i/o e sono tutti supportati nell'architettura FlexPod per soddisfare i diversi requisiti di business.



Oltre ai server rack M6 C220/C225/C240/C245 di ultima generazione, ai server blade M6 B200 e ai nodi di calcolo X210c mostrati in questa figura, è possibile utilizzare anche le generazioni precedenti di server rack e blade, se ancora supportate.

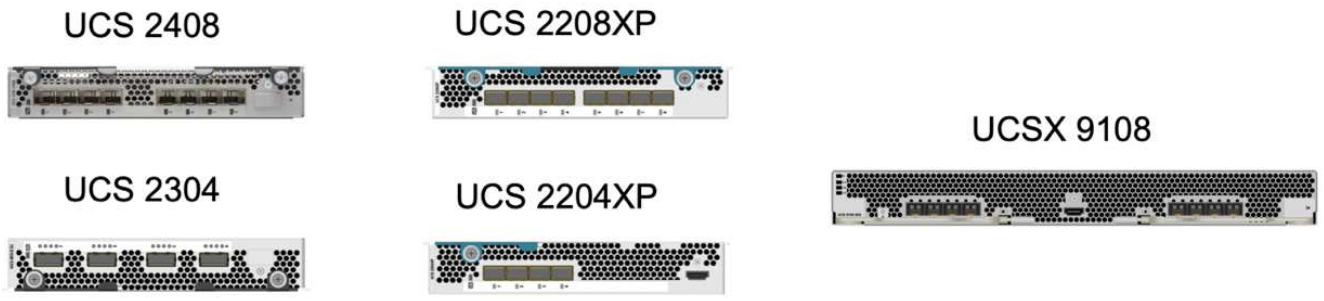
Modulo i/o e Intelligent Fabric Module

I/o Module (IOM)/Fabric Extender e Intelligent Fabric Module (IFM) forniscono connettività fabric unificata per lo chassis del server blade Cisco UCS 5108 e per lo chassis Cisco UCS X9508 X-Series, rispettivamente.

UCS IOM 2408 di quarta generazione dispone di otto porte 25-G Unified Ethernet per il collegamento dello chassis UCS 5108 con Fabric Interconnect (Fi). Ogni 2408 dispone di quattro connessioni Ethernet 10-G per il backplane tramite la scheda madre per ciascun server blade nello chassis.

UCSX 9108 25G IFM dispone di otto porte 25-G Unified Ethernet per il collegamento dei server blade nello chassis UCS X9508 con fabric interconnects. Ogni 9108 dispone di quattro connessioni 25-G verso ciascun nodo di calcolo UCS X210c nello chassis X9108. 9108 IFM funziona anche in combinazione con l'interconnessione fabric per gestire l'ambiente dello chassis.

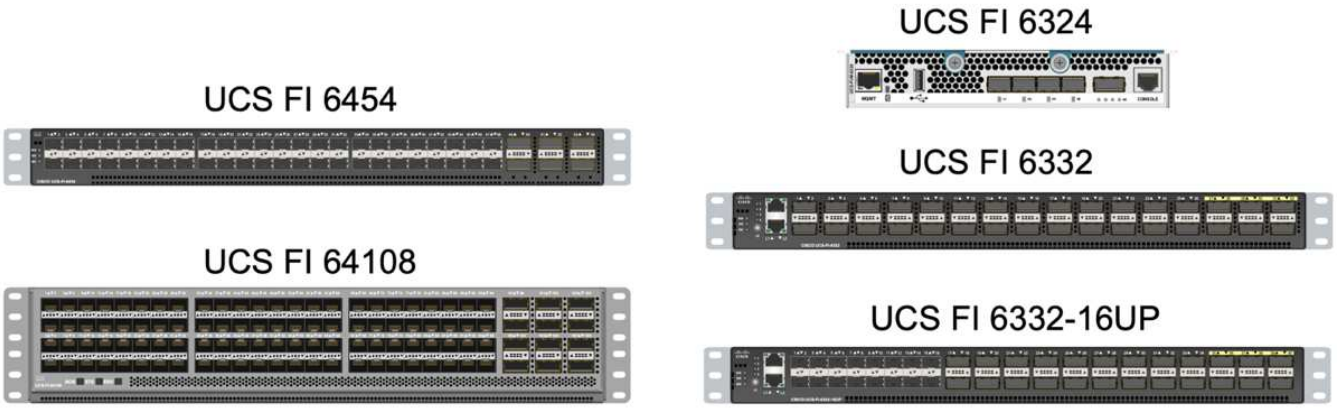
La figura seguente mostra UCS 2408 e le generazioni IOM precedenti per lo chassis UCS 5108 e 9108 IFM per lo chassis X9508.



Interconnessioni fabric UCS

Cisco UCS Fabric Interconnects (Fi) fornisce connettività e gestione per l'intero Cisco UCS. Generalmente implementato come coppia attiva/attiva, gli IF del sistema integrano tutti i componenti in un singolo dominio di gestione altamente disponibile controllato da Cisco UCS Manager o Cisco Intersight. Cisco UCS IF offre un singolo fabric unificato per il sistema con bassa latenza e switch cut-through senza perdita di dati che supporta LAN, SAN e traffico di gestione utilizzando un singolo set di cavi.

Sono disponibili due varianti per le IF Cisco UCS di quarta generazione: UCS Fi 6454 e 64108. Includono il supporto per porte Ethernet a 10/25 Gbps, porte Ethernet a 1/10/25 Gbps, porte up-link Ethernet a 40/100 Gbps e porte unificate in grado di supportare 10/25 Gigabit Ethernet o 8/16/32 Gbps Fibre Channel. La figura seguente mostra le IF Cisco UCS di quarta generazione insieme ai modelli di terza generazione supportati.

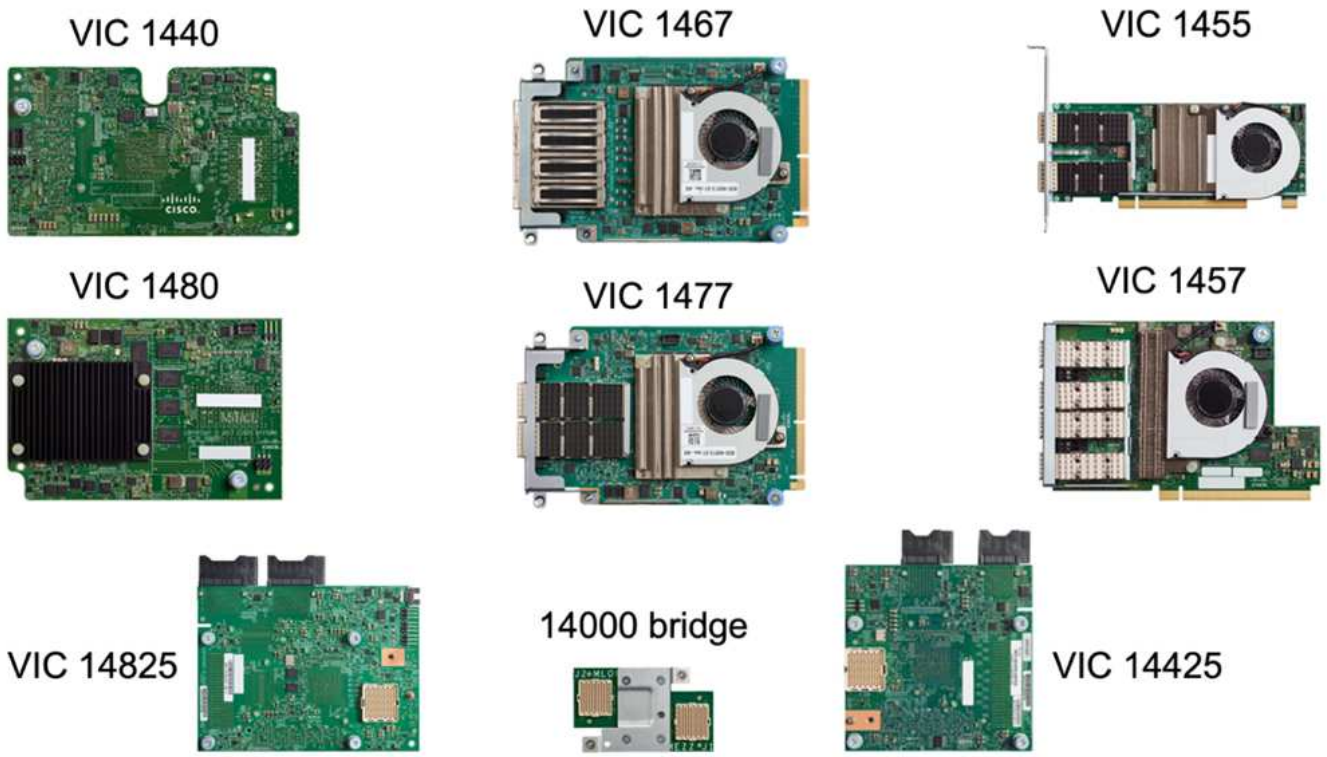


Per supportare lo chassis Cisco UCS X-Series, sono necessarie interconnessioni fabric di quarta generazione configurate in Intersight Managed Mode (IMM). Tuttavia, lo chassis Cisco UCS 5108 serie B può essere supportato sia in modalità IMM che in modalità gestita UCSM.

UCS Fi 6324 utilizza il fattore di forma IOM ed è integrato in uno chassis UCS Mini per le implementazioni che richiedono solo un piccolo dominio UCS.

Schede di interfaccia virtuale UCS

Cisco UCS Virtual Interface Card (VICS) unifica la gestione del sistema e la connettività LAN e SAN per server rack e blade. Supporta fino a 256 dispositivi virtuali, come vNIC (Virtual Network Interface Card) o vHBA (Virtual host Bus Adapter) utilizzando la tecnologia Cisco SingleConnect. Grazie alla virtualizzazione, le schede VIC semplificano notevolmente la connettività di rete e riducono il numero di adattatori di rete, cavi e porte switch necessari per l'implementazione della soluzione. La figura seguente mostra alcuni dei Cisco UCS VICS disponibili per i server B-Series e C-Series e i nodi di calcolo X-Series.



I diversi modelli di adattatori supportano diversi server blade e rack con diversi numeri di porte, velocità delle porte e fattori di forma di LAN modulare su scheda madre (mLOM), schede mezzanine e interfacce PCIe. Gli adattatori possono supportare alcune combinazioni di Ethernet 10/25/40/100-G e Fibre Channel over Ethernet (FCoE). Incorporano la tecnologia Converged Network Adapter (CNA) di Cisco, supportano un set completo di funzionalità e semplificano la gestione dell'adattatore e l'implementazione dell'applicazione. Ad esempio, il VIC supporta la tecnologia Data Center Virtual Machine Fabric Extender (VM-FEX) di Cisco, che estende le porte di interconnessione del fabric Cisco UCS alle macchine virtuali, semplificando così l'implementazione della virtualizzazione dei server.

Grazie alla combinazione di Cisco VIC nelle configurazioni mLOM, mezzanine, port expander e bridge card, è possibile sfruttare appieno la larghezza di banda e la connettività disponibili per i server blade. Ad esempio, utilizzando i due collegamenti 25-G sul VIC 14825 (mLOM), 14425 (mezzanino) e 14000 (scheda bridge) per il nodo di calcolo X210c, la larghezza di banda combinata del VIC è 2 x 50-G + 2 x 50-G, 100 G per fabric/IFM e 200 G in totale per server con configurazione IFM doppia.

Per informazioni dettagliate sulle famiglie di prodotti Cisco UCS, le specifiche tecniche e la documentazione, consultare "Cisco UCS" sito web per informazioni.

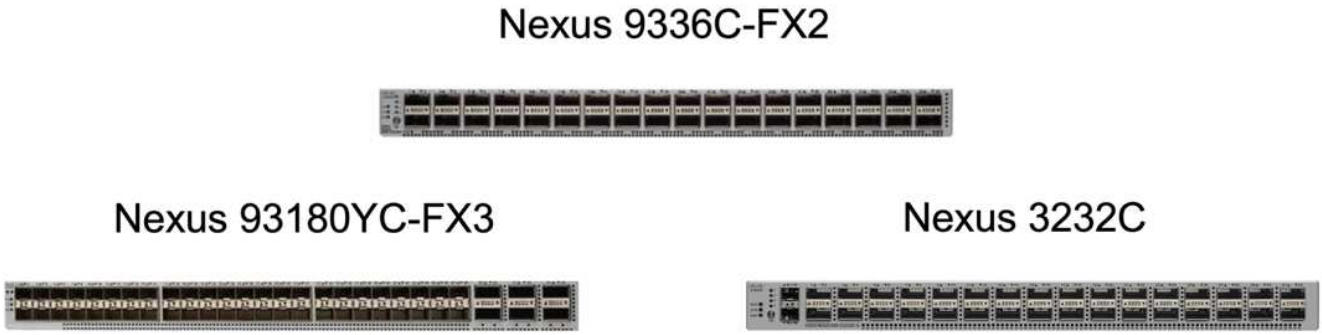
Componenti di switching Cisco

Switch Nexus

FlexPod utilizza gli switch della serie Cisco Nexus per fornire fabric di switching Ethernet per le comunicazioni tra Cisco UCS e i controller di storage NetApp. Tutti i modelli di switch Cisco Nexus attualmente supportati, inclusi Cisco Nexus serie 3000, 5000, 7000 e 9000, sono supportati per l'implementazione di FlexPod.

Quando si seleziona un modello di switch per l'implementazione di FlexPod, è necessario prendere in considerazione molti fattori, ad esempio performance, velocità delle porte, densità delle porte, latenza dello switching, E protocolli come ACI e VXLAN, per gli obiettivi di progettazione e per la durata del supporto degli switch.

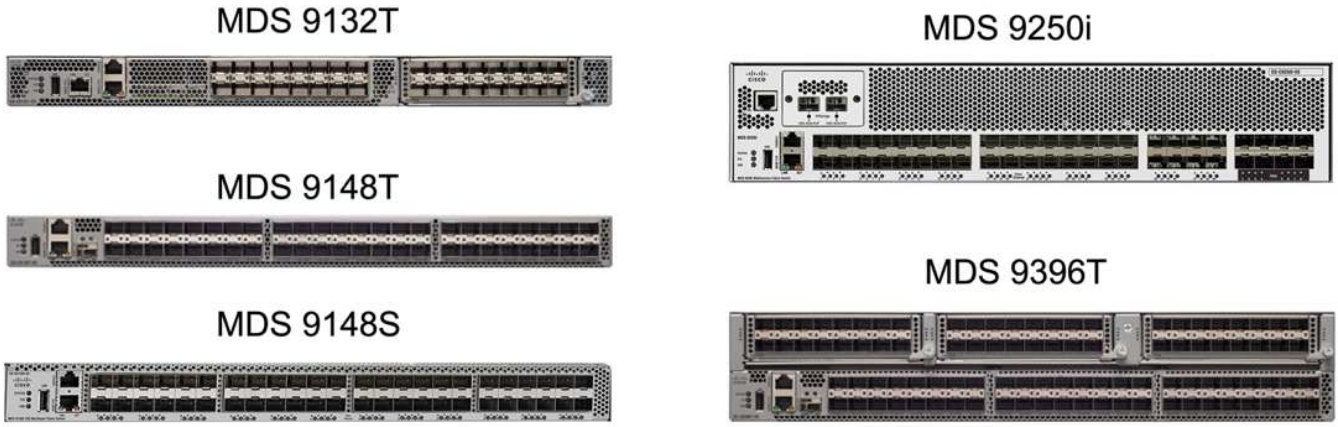
La convalida per molti CVD FlexPod recenti utilizza switch Cisco Nexus serie 9000 come Nexus 9336C-FX2 e Nexus 93180YC-FX3, che offrono porte 40/100G e 10/25G dalle performance elevate, bassa latenza ed eccezionale efficienza energetica in un form factor compatto 1U. Sono supportate velocità aggiuntive tramite porte uplink e cavi breakout. La figura seguente mostra alcuni switch Cisco Nexus 9k e 3k, tra cui Nexus 9336C-FX2 e Nexus 3232C utilizzati per questa convalida.



Vedere "Switch Cisco Data Center" Per ulteriori informazioni sugli switch Nexus disponibili e sulle relative specifiche e documentazione.

Switch MDS

Gli switch fabric Cisco MDS serie 9100/9200/9300 sono un componente opzionale dell'architettura FlexPod. Questi switch sono altamente affidabili, altamente flessibili, sicuri e possono fornire visibilità nel flusso di traffico nel fabric. La figura seguente mostra alcuni switch MDS di esempio che possono essere utilizzati per creare fabric FC SAN ridondanti per una soluzione FlexPod in grado di soddisfare i requisiti di business e delle applicazioni.



Gli switch fabric multistrato 32G ad alte prestazioni Cisco MDS 9132T/9148T/9396T sono convenienti e altamente affidabili, flessibili e scalabili. Le funzioni e le funzionalità avanzate di storage networking sono semplici da gestire e sono compatibili con l'intero portfolio della famiglia Cisco MDS 9000 per un'implementazione SAN affidabile.

Questa piattaforma hardware di prossima generazione integra funzionalità AVANZATE DI analisi E telemetria SAN. I dati di telemetria estratti dall'ispezione delle intestazioni dei frame possono essere trasmessi a una piattaforma di visualizzazione analitica, incluso Cisco Data Center Network Manager. Gli switch MDS che supportano FC 16G, come MDS 9148S, sono supportati anche in FlexPod. Inoltre, gli switch MDS multiservice, come MDS 9250i, che supporta i protocolli FCoE e FCIP oltre al protocollo FC, fanno parte del portfolio di soluzioni FlexPod.

Su switch MDS semomodibili come 9132T e 9396T, è possibile aggiungere ulteriori licenze di porte e moduli di espansione per supportare la connettività di dispositivi aggiuntivi. Sugli switch fissi, come 9148T, è possibile aggiungere ulteriori licenze per le porte in base alle necessità. Questa flessibilità pay-as-you-grow offre una componente delle spese operative per contribuire a ridurre le spese di capitale per l'implementazione e il funzionamento dell'infrastruttura SAN basata su switch MDS.

Vedere "Switch Cisco MDS Fabric" Per ulteriori informazioni sugli switch MDS Fabric disponibili, consultare "NetApp IMT" e. "Elenco di compatibilità hardware e software Cisco" Per un elenco completo degli switch SAN supportati.

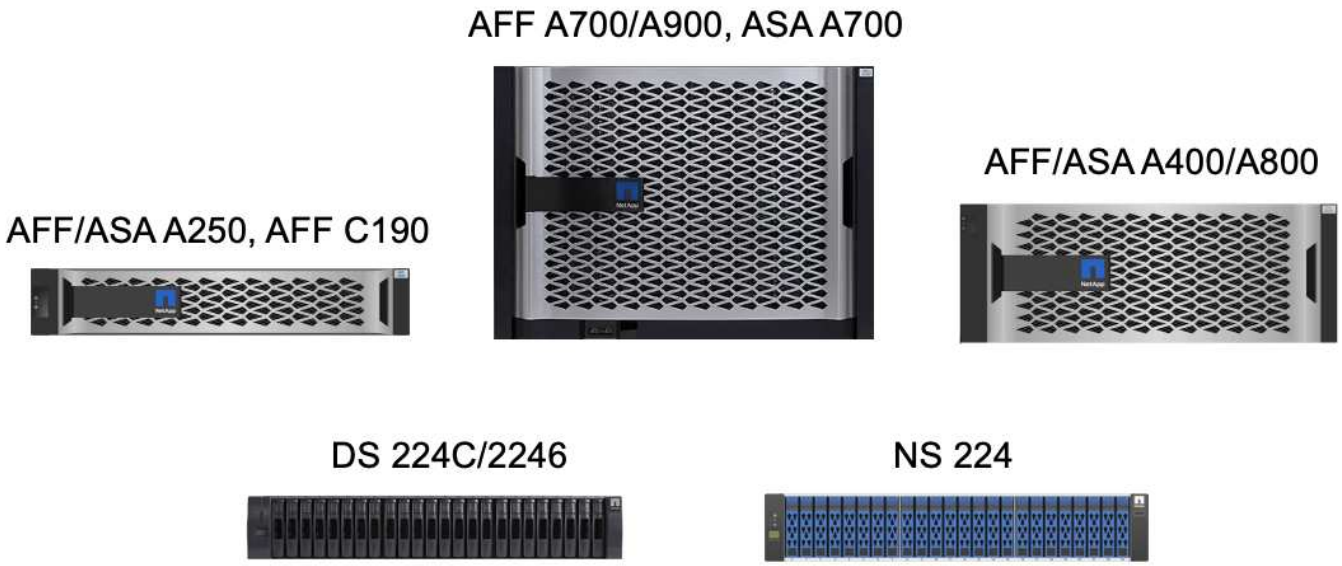
Componenti NetApp

Per creare una soluzione FlexPod SM-BC, sono necessari controller NetApp AFF o ASA ridondanti con software ONTAP 9.8 o versioni successive. L'ultima release di ONTAP, attualmente 9.10.1, è consigliata per l'implementazione di SM-BC per sfruttare le continue innovazioni ONTAP, le performance e i miglioramenti di qualità e il maggior numero massimo di oggetti per il supporto di SM-BC.

I controller NetApp AFF e ASA con performance e innovazioni leader del settore offrono protezione dei dati aziendali e funzionalità di gestione dei dati ricche di funzionalità. I sistemi AFF e ASA supportano le tecnologie NVMe end-to-end, tra cui SSD NVMe-attached e connettività host front-end NVMe over Fibre Channel (NVMe/FC). È possibile migliorare il throughput del carico di lavoro e ridurre la latenza di i/o adottando un'infrastruttura SAN basata su NVMe/FC. Tuttavia, i datastore basati su NVMe/FC possono attualmente essere utilizzati solo per carichi di lavoro non protetti da SM-BC, poiché la soluzione SM-BC attualmente supporta solo i protocolli iSCSI e FC.

I controller di storage NetApp AFF e ASA offrono inoltre ai clienti una base di cloud ibrido per sfruttare i vantaggi della perfetta mobilità dei dati resa possibile dal NetApp Data Fabric. Con il Data Fabric, puoi facilmente ottenere i dati dall'edge in cui vengono generati al core in cui vengono utilizzati e al cloud per sfruttare il calcolo elastico on-demand e le funzionalità ai e ML per ottenere informazioni di business attuabili.

Come mostrato nella figura seguente, NetApp offre una vasta gamma di storage controller e shelf di dischi per soddisfare i requisiti di performance e capacità. Per informazioni sulle funzionalità e le specifiche dei controller NetApp AFF e ASA, consultare la seguente tabella per i collegamenti alle pagine dei prodotti.

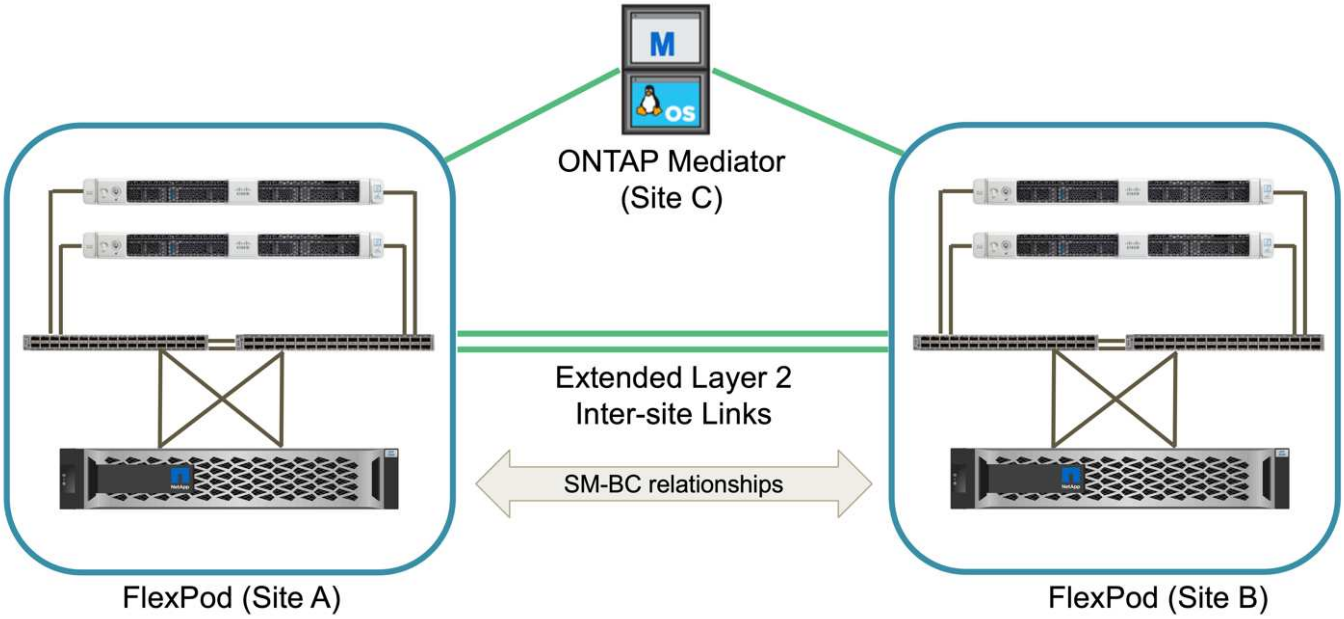


Famiglia di prodotti	Specifiche tecniche
Serie AFF	"Documentazione della serie AFF"
Serie ASA	"Documentazione della serie ASA"

Consultare "Shelf di dischi NetApp e documentazione sui supporti di storage" e. "NetApp Hardware Universe" per informazioni dettagliate sugli shelf di dischi e sugli shelf di dischi supportati per ciascun modello di controller di storage.

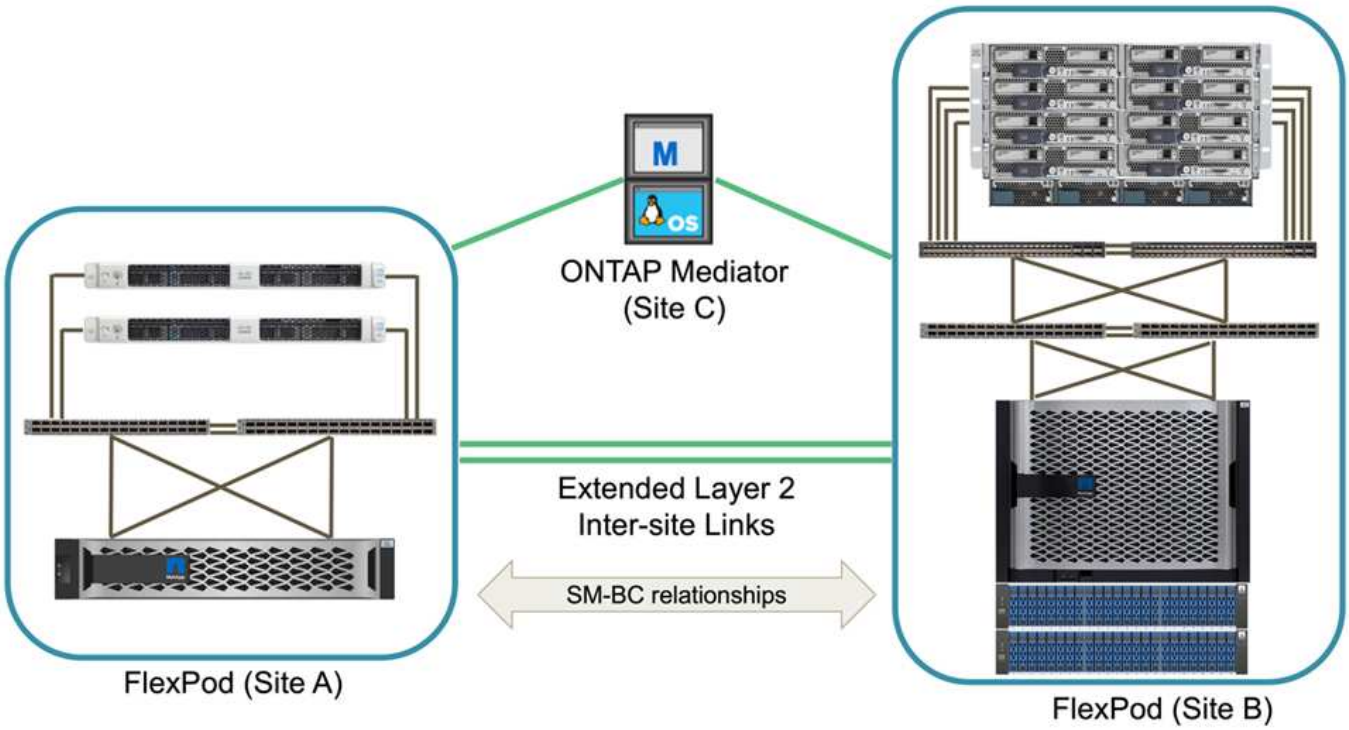
Topologie delle soluzioni

Le soluzioni FlexPod sono flessibili in termini di topologia e possono essere scalate in verticale o in orizzontale per soddisfare diversi requisiti di soluzione. Una soluzione che richiede la protezione della business continuity e solo risorse di calcolo e storage minime può utilizzare una semplice topologia di soluzione, come illustrato nella figura seguente. Questa semplice topologia utilizza i server rack UCS C-Series e i controller AFF/ASA con SSD nel controller senza shelf di dischi aggiuntivi.



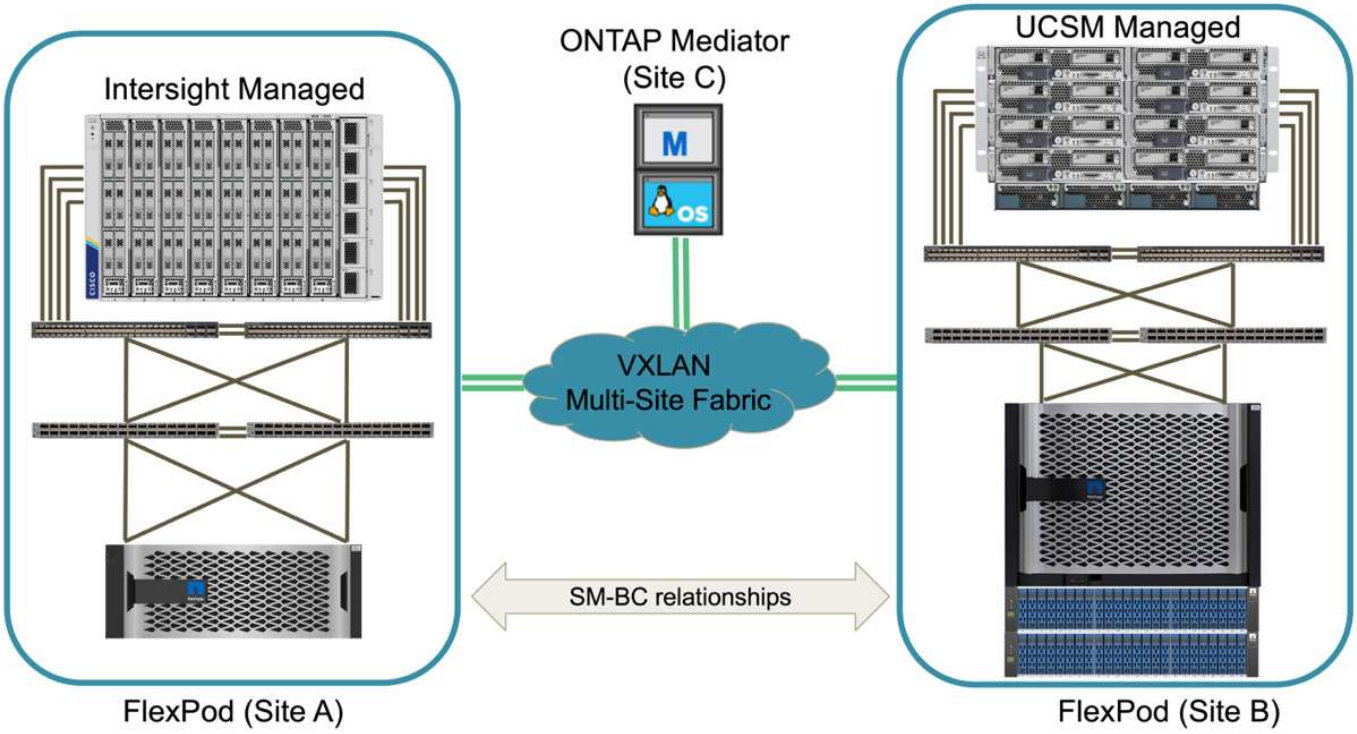
I componenti ridondanti di calcolo, rete e storage sono interconnessi con una connettività ridondante tra i componenti. Questo design ad alta disponibilità offre resilienza della soluzione e consente all'IT di resistere a scenari di singolo punto di errore. Il design multi-sito e le relazioni di replica sincrona dei dati di ONTAP SM-BC offrono servizi dati business-critical nonostante il potenziale guasto dello storage a singolo sito.

Una topologia di implementazione asimmetrica che potrebbe essere utilizzata dalle aziende tra un data center e una filiale in un'area metropolitana potrebbe essere simile alla seguente figura. Per questo design asimmetrico, il data center richiede un FlexPod dalle performance più elevate con più risorse di calcolo e storage. Tuttavia, il requisito della filiale è inferiore e può essere soddisfatto da un FlexPod molto più piccolo.

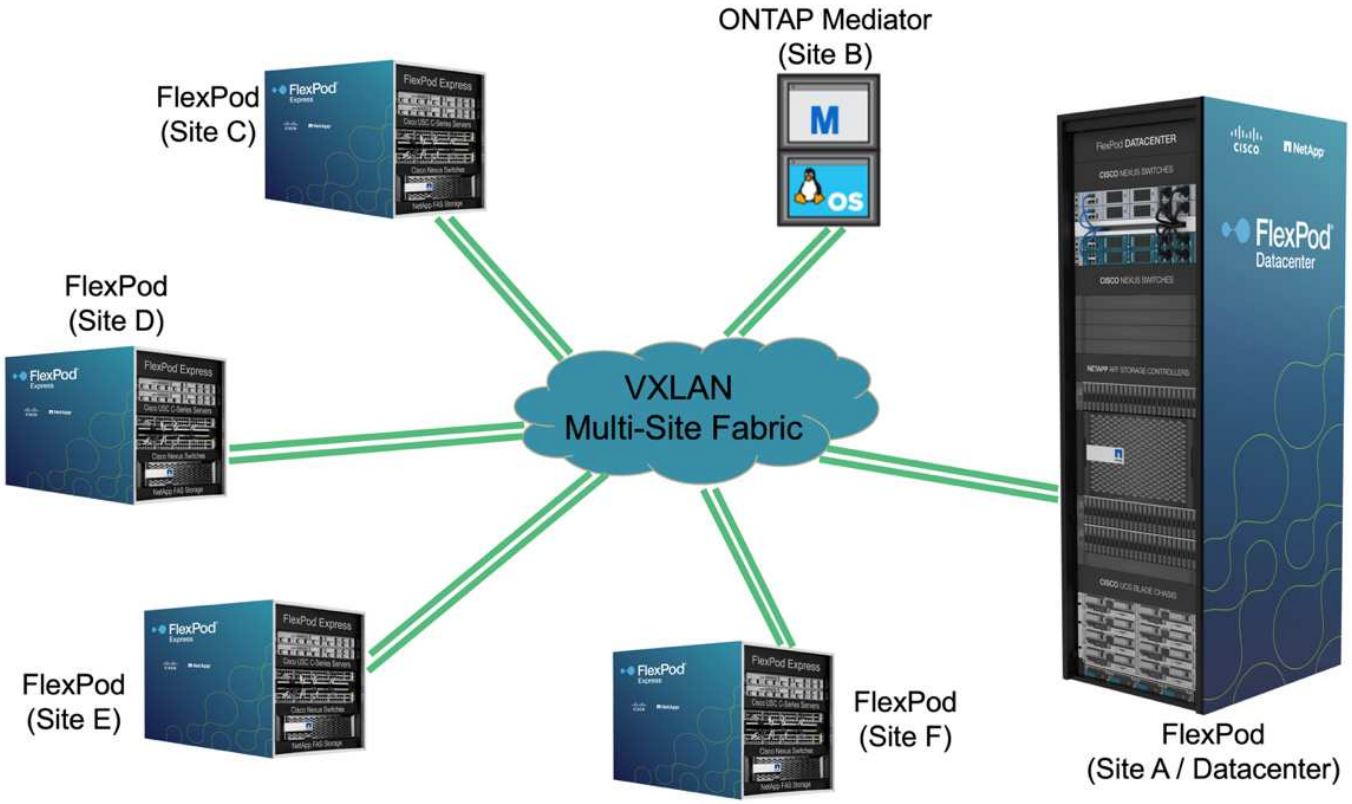


Per le aziende con requisiti di risorse di calcolo e storage più elevati e con più siti, un fabric multi-sito basato su VXLAN consente a più siti di disporre di un fabric di rete perfetto per facilitare la mobilità delle applicazioni, in modo che un'applicazione possa essere servita da qualsiasi sito.

Potrebbe esistere una soluzione FlexPod che utilizza lo chassis Cisco UCS 5108 e i server blade B-Series che deve essere protetta da una nuova istanza di FlexPod. La nuova istanza di FlexPod può utilizzare il più recente chassis UCS X9508 con nodi di calcolo X210c gestiti da Cisco Intersight, come mostrato nella figura seguente. In questo caso, i sistemi FlexPod di ciascun sito sono collegati a un fabric di data center più grande e i siti sono collegati tramite una rete di interconnessione per formare un fabric multisito VXLAN.



Per le aziende che dispongono di un data center e di diverse filiali in un'area metropolitana che devono essere protette per garantire la business continuity, La topologia di implementazione di FlexPod SM-BC illustrata nella figura seguente può essere implementata per proteggere i servizi dati e le applicazioni critiche per raggiungere obiettivi RPO pari a zero e RTO pari a zero per tutti i siti delle filiali.



Per questo modello di implementazione, ogni filiale stabilisce le relazioni SM-BC e i gruppi di coerenza richiesti con il data center. È necessario tenere in considerazione i limiti degli oggetti SM-BC supportati, in modo che le relazioni di gruppo di coerenza e i conteggi degli endpoint non superino i massimi supportati nel data center.

"Pagina successiva: Panoramica sulla convalida della soluzione."

Convalida della soluzione

Convalida della soluzione - Panoramica

"Precedente: Soluzione FlexPod SM-BC."

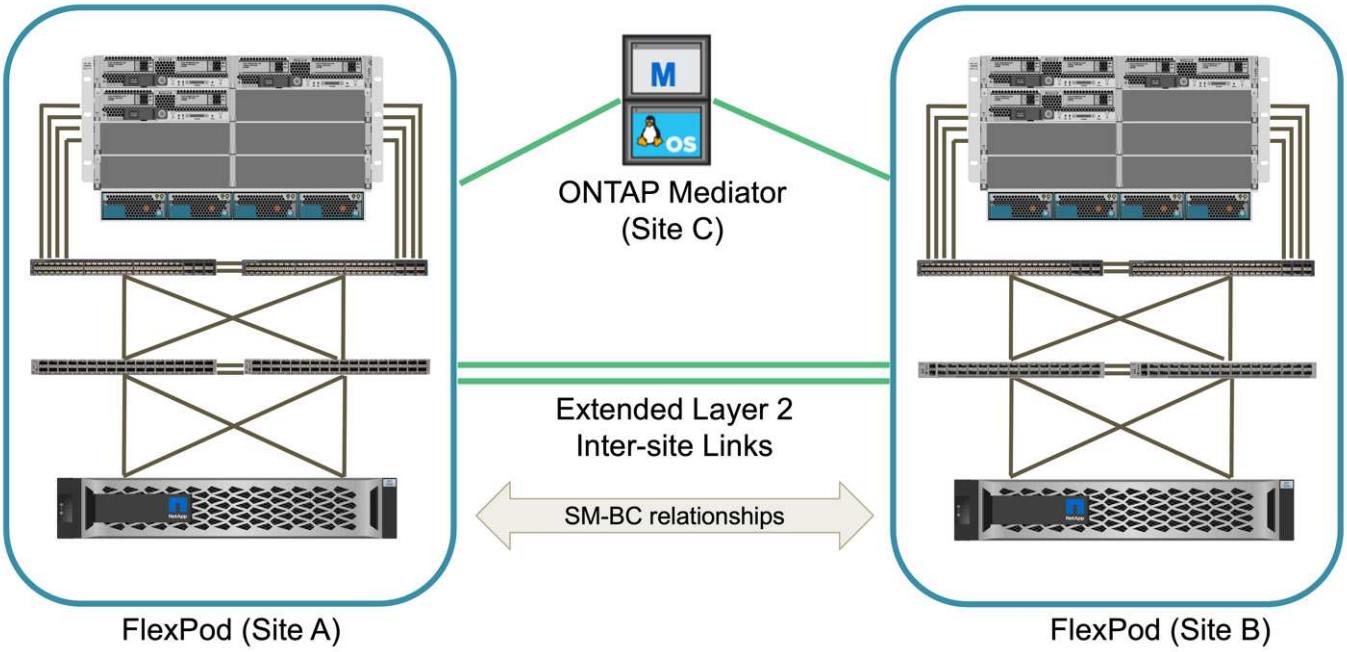
I dettagli di progettazione e implementazione della soluzione FlexPod SM-BC dipendono dalla configurazione specifica della situazione FlexPod e dagli obiettivi della soluzione. Una volta definiti i requisiti generali di business continuity, è possibile creare la soluzione FlexPod SM-BC implementando una soluzione completamente nuova con due nuovi sistemi FlexPod, aggiungendo un nuovo FlexPod in un altro sito per l'associazione con un FlexPod esistente o associando due sistemi FlexPod esistenti.

Poiché le soluzioni FlexPod sono di natura flessibile nelle relative configurazioni, è possibile utilizzare potenzialmente tutte le configurazioni e i componenti FlexPod supportati. Il resto di questa sezione fornisce informazioni sulle validazioni di implementazione eseguite per una soluzione di infrastruttura virtuale basata su VMware. Ad eccezione degli aspetti correlati a SM-BC, l'implementazione segue i processi di implementazione

standard di FlexPod. Per informazioni generali sull'implementazione di FlexPod, consultare i CVD e gli NVA FlexPod disponibili per le configurazioni specifiche.

Topologia di convalida

Per la convalida della soluzione FlexPod SM-BC, vengono utilizzati i componenti tecnologici supportati da NetApp, Cisco e VMware. La soluzione include coppie ha NetApp AFF A250 con ONTAP 9.10.1, due switch Cisco Nexus 9336C-FX2 nel sito A e due switch Cisco Nexus 3232C nel sito B, Cisco UCS 6454 Fi in entrambi i siti, E tre server Cisco UCS B200 M5 in ogni sito che esegue VMware vSphere 7.0u2 e gestiti da UCS Manager e dal server VMware vCenter. La figura seguente mostra la topologia di convalida della soluzione a livello di componente con due sistemi FlexPod in esecuzione nel sito A e nel sito B collegati tramite collegamenti intersito Layer-2 estesi e mediatore ONTAP in esecuzione nel sito C.



Hardware e software

La seguente tabella elenca l'hardware e il software utilizzati per la convalida della soluzione. È importante notare che Cisco, NetApp e VMware dispongono di matrici di interoperabilità utilizzate per determinare il supporto per qualsiasi implementazione specifica di FlexPod:

- "http://support.netapp.com/matrix/"
- "Cisco UCS hardware and Software Interoperability Tool"
- "http://www.vmware.com/resources/compatibility/search.php"

Categoria	Componente	Versione del software	Quantità
Calcolo	Cisco UCS Fabric Interconnect 6454	4.2(1f)	4 (2 per sito)
	Server Cisco UCS B200 M5	4.2(1f)	6 (3 per sito)
	CISCO UCS IOM 2204XP	4.2(1f)	4 (2 per sito)

Categoria	Componente	Versione del software	Quantità
	CISCO VIC 1440 (PID: UCSB-MLOM-40G-04)	5.2 (1a)	2 (1 per sito)
	CISCO VIC 1340 (PID: UCSB-MLOM-40G-03)	4.5 (1a)	4 (2 per sito)
Rete	Cisco Nexus 9336C-FX2	9.3(6)	2 (sito A)
	Cisco Nexus 3232C	9.3(6)	2 (sito B)
Storage	NetApp AFF A250	9.10.1	4 (2 per sito)
	System Manager di NetApp	9.10.1	2 (1 per sito)
	NetApp Active IQ Unified Manager	9.10	1
	Strumenti NetApp ONTAP per VMware vSphere	9.10	1
	Plug-in NetApp SnapCenter per VMware vSphere	4.6	1
	Mediatore NetApp ONTAP	1.3	1
	NAbox	3.0.2	1
	NetApp Harvest	21.11.1-1	1
Virtualizzazione	VMware ESXi	7.0U2	6 (3 per sito)
	Driver Ethernet Nenico VMware ESXi	1.0.35.0	6 (3 per sito)
	VMware vCenter	7.0U2	1
	Plug-in NetApp NFS per VMware VAAI	2.0	6 (3 per sito)
Test	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18.10	1
	HammerDB	4.3	1
	Microsoft Windows	10	6 (3 per sito)
	Iometro	1.1.0	6 (3 per sito)

"Successivo: Convalida della soluzione - calcolo."

Convalida della soluzione - calcolo

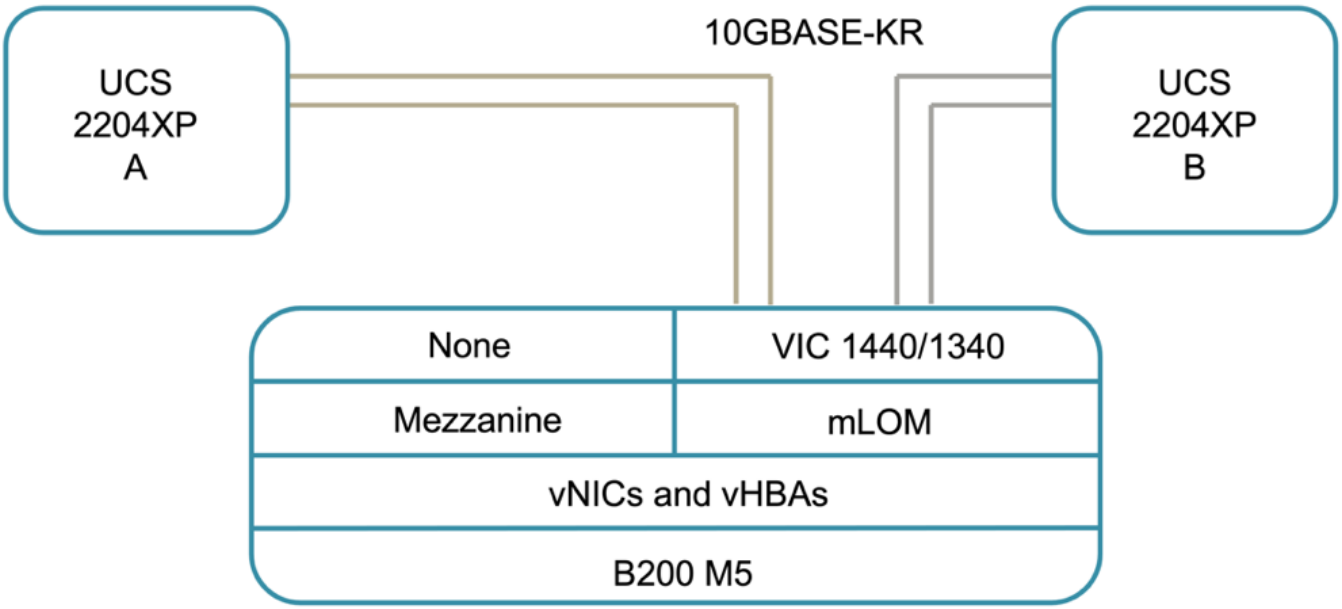
"Preivous: Convalida della soluzione - Panoramica."

La configurazione di calcolo per la soluzione FlexPod SM-BC segue le Best practice

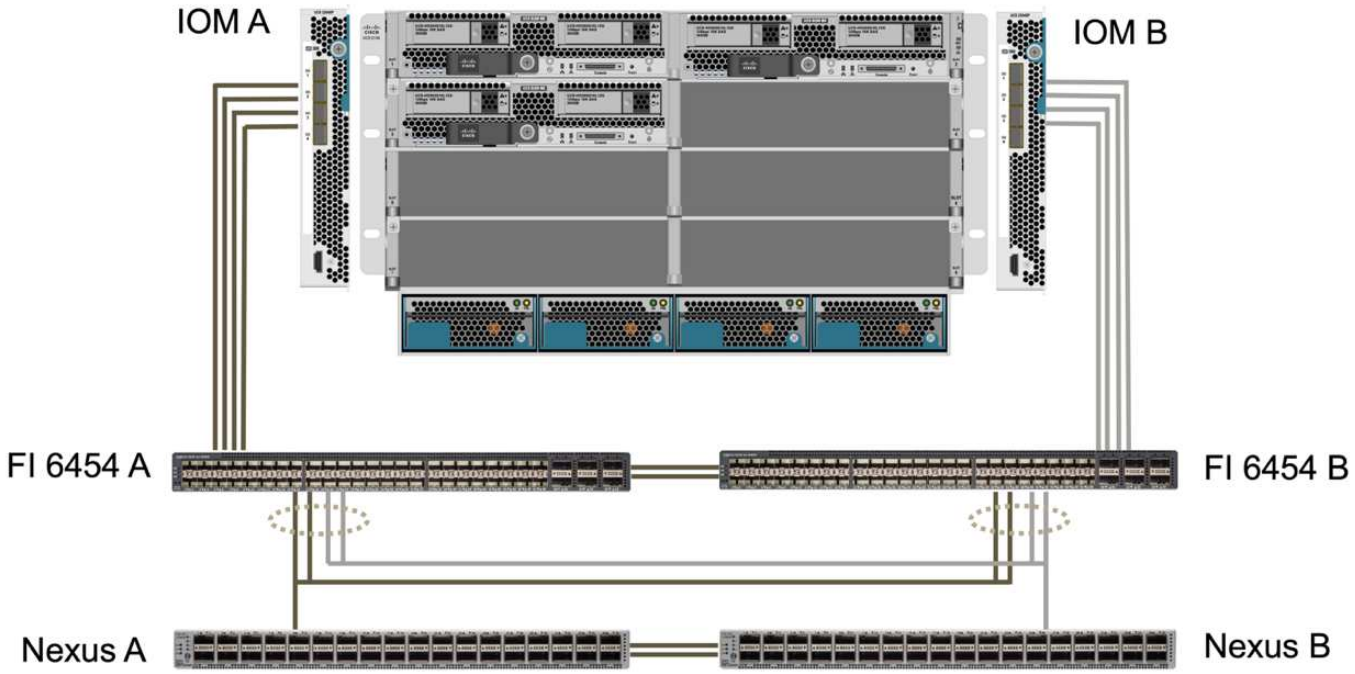
tipiche delle soluzioni FlexPod. Nelle sezioni seguenti vengono illustrate alcune delle configurazioni e della connettività utilizzate per la convalida. Vengono inoltre evidenziate alcune considerazioni relative a SM-BC per fornire riferimenti e indicazioni per l'implementazione.

Connettività

La connettività tra i server blade UCS B200 e gli IOM viene fornita dalla scheda VIC UCS attraverso le connessioni del backplane dello chassis UCS 5108. Gli UCS 2204XP Fabric Extender utilizzati per la convalida dispongono di sedici porte 10G ciascuna per connettersi agli otto server blade half-width, ad esempio due per ciascun server. Per aumentare la larghezza di banda della connettività del server, è possibile aggiungere un VIC aggiuntivo basato su mezzanino per collegare il server all'IOM UCS 2408 alternativo, che fornisce quattro connessioni 10G a ciascun server.



La connettività tra lo chassis UCS 5108 e gli UCS 6454 IF utilizzati per la convalida è fornita da IOM 2204XP che utilizza quattro connessioni 10G. Le porte Fi da 1 a 4 sono configurate come porte server per queste connessioni. Le porte Fi da 25 a 28 sono configurate come porte di uplink di rete verso lo switch Nexus A e B nel sito locale. La figura e la tabella riportate di seguito forniscono lo schema di connettività e i dettagli di connessione delle porte per i Fi UCS 6454 da collegare allo chassis UCS 5108 e agli switch Nexus.



Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
UCS 6454 FI A	1	IOM A.	1
	2		2
	3		3
	4		4
	25	Nexus A.	1/13/1
	26		1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus A.	1/13/3
	26		1/13/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
	L2		L2

Le connessioni descritte in precedenza sono simili per entrambi i siti A e B, nonostante il sito A utilizzi switch Nexus 9336C-FX2e il sito B con switch Nexus 3232C. I cavi breakout DA 40 G a 4 x 10 G sono utilizzati per le connessioni Nexus-Fi. Le connessioni Fi a Nexus utilizzano il canale di porta e i canali di porta virtuale sono configurati sugli switch Nexus per aggregare le connessioni a ciascun Fi.

Quando si utilizza una diversa combinazione di componenti IOM, Fi e switch Nexus, assicurarsi di utilizzare i cavi e la velocità della porta appropriati per la combinazione di ambienti.

È possibile ottenere un'ulteriore larghezza di banda utilizzando componenti che supportano connessioni a velocità superiore o più connessioni. È possibile ottenere una ridondanza aggiuntiva aggiungendo connessioni aggiuntive con componenti che li supportano.

Profili di servizio

Uno chassis per server blade con interconnessioni fabric gestite da UCS Manager (UCSM) o Cisco Intersight può astrarre i server utilizzando i profili di servizio disponibili in UCSM e i profili server in Intersight. Questa convalida utilizza UCSM e profili di servizio per semplificare la gestione del server. Con i profili di servizio, è possibile sostituire o aggiornare un server semplicemente associando il profilo di servizio originale al nuovo hardware.

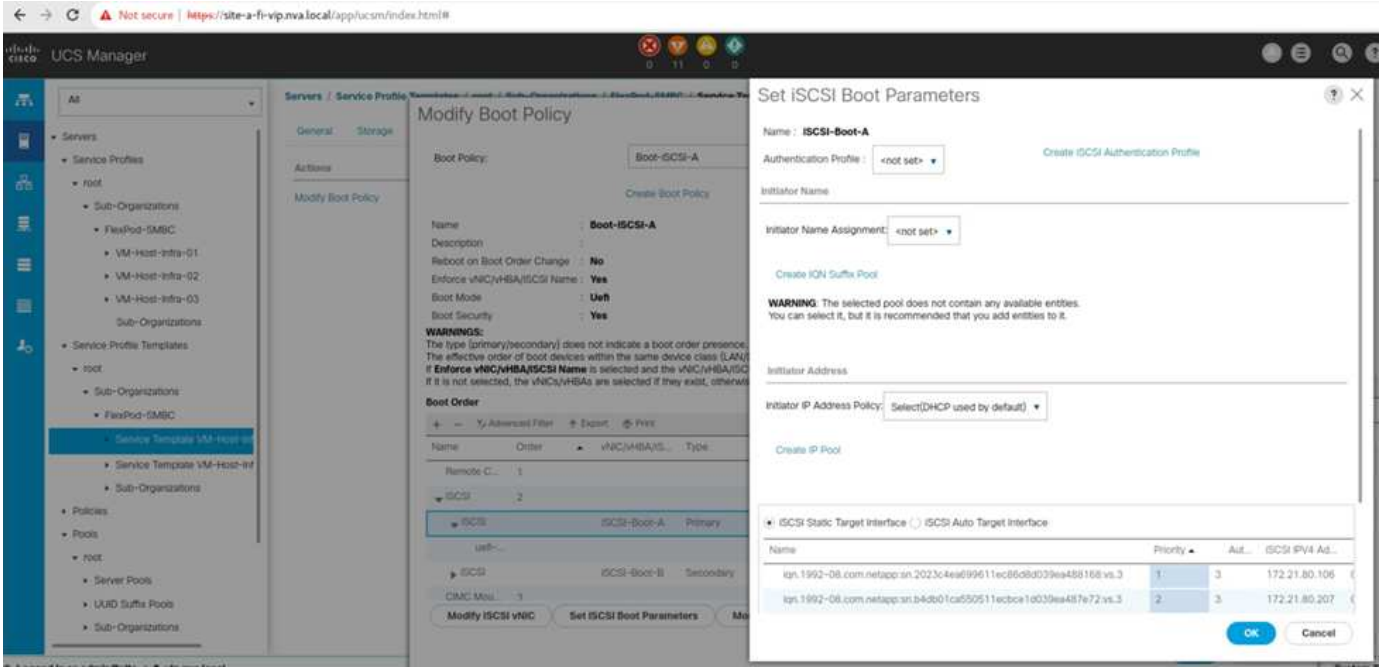
I profili di servizio creati supportano i seguenti elementi per gli host VMware ESXi:

- Eseguire l'avvio SAN dallo storage AFF A250 in entrambi i siti utilizzando il protocollo iSCSI.
- Vengono create sei vNIC per i server in cui:
  - Due vNIC ridondanti (vSwitch0-A e vSwitch0-B) trasportano traffico di gestione in banda. Facoltativamente, questi vNIC possono essere utilizzati anche dai dati del protocollo NFS non protetti da SM-BC.
  - Lo switch distribuito vSphere utilizza due vNIC ridondanti (VDS-A e VDS-B) per trasportare il traffico VMware vMotion e altre applicazioni.
  - ISCSI-A vNIC utilizzato da iSCSI-A vSwitch per fornire l'accesso al percorso iSCSI-A.
  - VNIC iSCSI-B utilizzata da iSCSI-B vSwitch per fornire l'accesso al percorso iSCSI-B.

Boot SAN

Per la configurazione di boot SAN iSCSI, i parametri di boot iSCSI sono impostati in modo da consentire l'avvio iSCSI da entrambi i fabric iSCSI. Per adattarsi allo scenario di failover SM-BC in cui un LUN di avvio SAN iSCSI viene servito dal cluster secondario quando il cluster primario non è disponibile, la configurazione di destinazione statica iSCSI deve includere destinazioni sia dal sito A che dal sito B. Inoltre, per massimizzare la disponibilità del LUN di avvio, configurare le impostazioni dei parametri di avvio iSCSI per l'avvio da tutti i controller di storage.

La destinazione statica iSCSI può essere configurata nella policy di avvio dei modelli di profilo del servizio nella finestra di dialogo Set iSCSI Boot Parameter (Imposta parametro di avvio iSCSI), come mostrato nella figura seguente. La configurazione consigliata per l'impostazione dei parametri di avvio iSCSI è illustrata nella tabella seguente, che implementa la strategia di avvio descritta in precedenza per ottenere una disponibilità elevata.



Fabric iSCSI	Priorità	Destinazione iSCSI	LIF iSCSI
ISCSI A.	1	Sito Di destinazione iSCSI	Site A Controller 1 iSCSI A LIF
	2	Destinazione iSCSI del sito B.	Site B Controller 2 iSCSI A LIF
ISCSI B	1	Destinazione iSCSI del sito B.	LIF iSCSI B controller 1 sito B
	2	Sito Di destinazione iSCSI	LIF B iSCSI controller 2 sito A

"Pagina successiva: Convalida della soluzione - rete."

Convalida della soluzione - rete

"Precedente: Convalida della soluzione - calcolo."

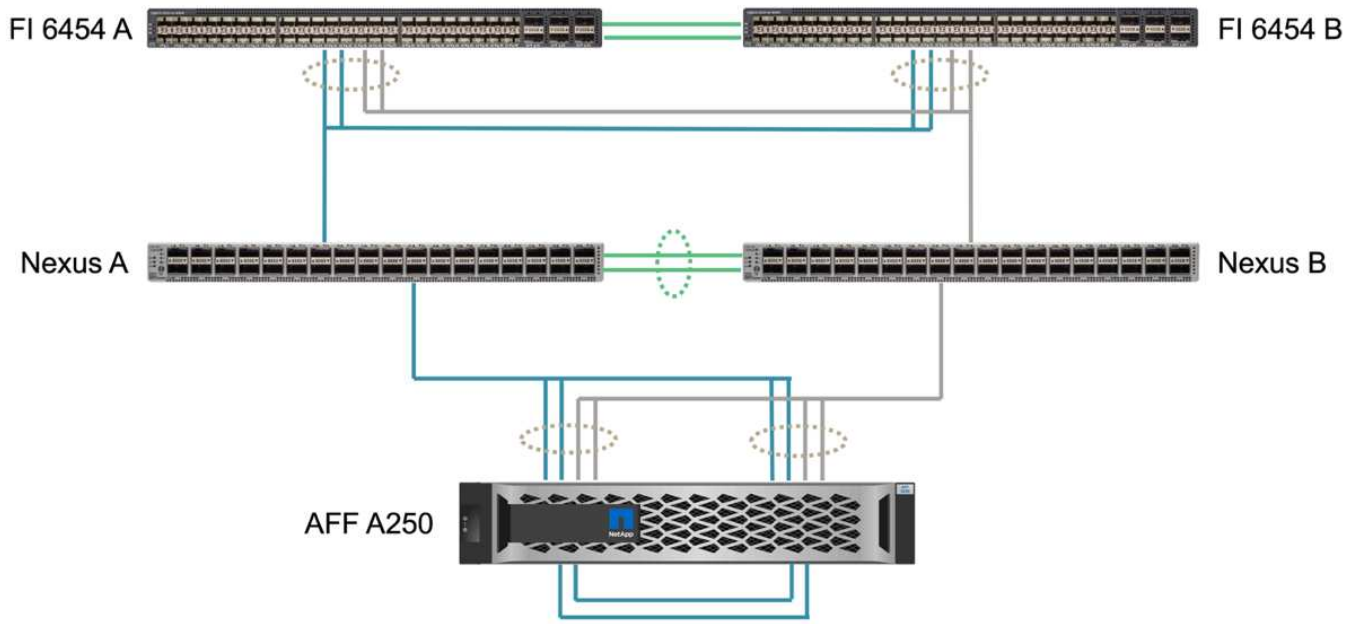
La configurazione di rete per la soluzione FlexPod SM-BC segue le Best practice tipiche delle soluzioni FlexPod in ogni sito. Per la connettività tra siti, la configurazione di convalida della soluzione collega gli switch FlexPod Nexus nei due siti per fornire una connettività tra siti che estende le VLAN tra i due siti. Nelle sezioni seguenti vengono illustrate alcune delle configurazioni e della connettività utilizzate per la convalida.

Connettività

Gli switch FlexPod Nexus di ogni sito forniscono la connettività locale tra il calcolo UCS e lo storage ONTAP in una configurazione ad alta disponibilità. I componenti ridondanti e la connettività ridondante offrono la resilienza rispetto a scenari con singolo punto di errore.

Il seguente diagramma mostra la connettività locale dello switch Nexus in ogni sito. Oltre a quanto mostrato nel diagramma, sono disponibili anche connessioni di console e di rete di gestione per ciascun componente non

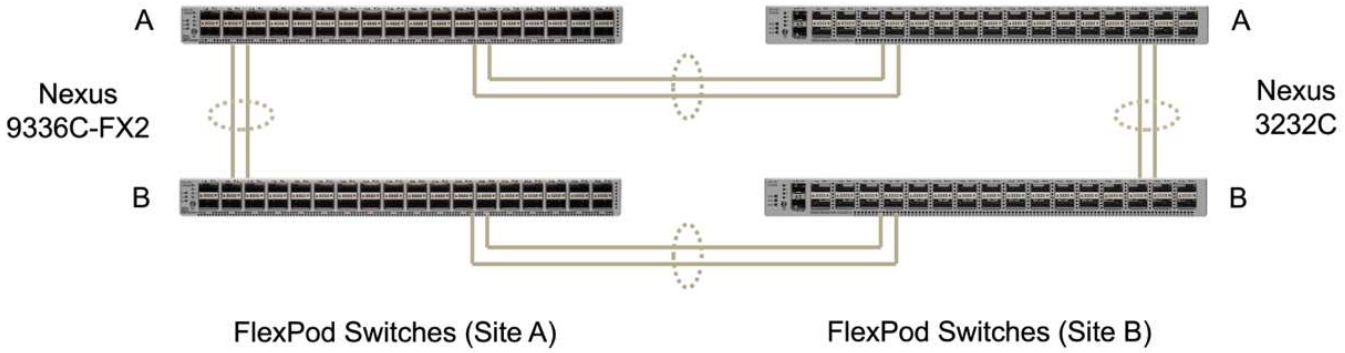
mostrate. I cavi breakout da 40 G a 4 x 10 G vengono utilizzati per collegare gli switch Nexus ai Fi UCS e ai controller di storage ONTAP AFF A250. In alternativa, i cavi breakout DA 100 G a 4 x 25 G possono essere utilizzati per aumentare la velocità di comunicazione tra gli switch Nexus e i controller di storage AFF A250. Per semplicità, i due controller AFF A250 sono mostrati logicamente come uno accanto all'altro per l'illustrazione del cablaggio. Le due connessioni tra i due controller storage consentono allo storage di formare un cluster senza switch.



La seguente tabella mostra la connettività tra gli switch Nexus e i controller di storage AFF A250 in ogni sito.

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Nexus A.	1/10/1	AFF A250 A.	e1a
	1/10/2		e1b
	1/10/3	AFF A250 B	e1a
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A.	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B	e1c
	1/10/4		e1d

La connettività tra gli switch FlexPod del sito A e del sito B è illustrata nella seguente figura con i dettagli relativi al cablaggio elencati nella tabella allegata. Le connessioni tra i due switch di ciascun sito sono relative ai collegamenti peer VPC. D'altra parte, le connessioni tra gli switch tra i siti forniscono i collegamenti tra siti. I collegamenti estendono le VLAN tra i siti per la comunicazione tra cluster, la replica dei dati SM-BC, la gestione in-band e l'accesso ai dati per le risorse del sito remoto.



Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
Switch a del sito A.	33	Punto B interruttore A	31
	34		32
	25	Switch B del sito A	25
	26		26
Switch B del sito A	33	Switch B del sito B.	31
	34		32
	25	Switch a del sito A.	25
	26		26
Punto B interruttore A	31	Switch a del sito A.	33
	32		34
	25	Switch B del sito B.	25
	26		26
Switch B del sito B.	31	Switch B del sito A	33
	32		34
	25	Punto B interruttore A	25
	26		26

La tabella precedente elenca la connettività dal punto di vista di ogni switch FlexPod. Di conseguenza, la tabella contiene informazioni duplicate per la leggibilità.

Port Channel e Virtual Port Channel

Il canale delle porte consente l'aggregazione dei collegamenti utilizzando il protocollo LACP (link Aggregation Control Protocol) per l'aggregazione della larghezza di banda e la resilienza del collegamento in caso di guasto. Virtual Port Channel (VPC) consente di visualizzare logicamente le connessioni del canale di porta tra due switch Nexus. Ciò migliora ulteriormente la resilienza dei guasti per scenari come un guasto di un singolo collegamento o un guasto di un singolo switch.

Il traffico del server UCS allo storage prende i percorsi di IOM A a Fi A e IOM B a Fi B prima di raggiungere gli switch Nexus. Poiché le connessioni Fi agli switch Nexus utilizzano il canale della porta sul lato Fi e il canale

della porta virtuale sul lato dello switch Nexus, il server UCS può utilizzare efficacemente i percorsi attraverso entrambi gli switch Nexus e può sopravvivere a scenari di singolo punto di errore. Tra i due siti, gli switch Nexus sono interconnessi come illustrato nella figura precedente. Sono disponibili due collegamenti ciascuno per collegare le coppie di switch tra i siti e utilizzano anche una configurazione port-channel.

La gestione in-band, la connettività tra cluster e il protocollo di storage dei dati iSCSI / NFS viene fornita interconnettendo i controller di storage di ogni sito agli switch Nexus locali in una configurazione ridondante. Ogni controller di storage è collegato a due switch Nexus. Le quattro connessioni sono configurate come parte di un gruppo di interfacce sullo storage per una maggiore resilienza. Sul lato dello switch Nexus, queste porte fanno anche parte di un VPC tra gli switch.

La seguente tabella elenca l'ID del canale della porta e l'utilizzo in ciascun sito.

ID canale porta	Utilizzo
10	Link Nexus peer locale
15	Collegamenti a di interconnessione fabric
16	Collegamenti B di interconnessione fabric
27	Link al controller dello storage A.
28	Collegamenti del controller di storage B.
100	Collegamenti switch A tra siti
200	Collegamenti switch B tra siti

VLAN

La seguente tabella elenca le VLAN configurate per la configurazione dell'ambiente di convalida della soluzione FlexPod SM-BC insieme al relativo utilizzo.

Nome	ID VLAN	Utilizzo
VLAN nativa	2	VLAN 2 utilizzata come VLAN nativa invece della VLAN predefinita (1)
OOB-MGMT-VLAN	3333	VLAN di gestione out-of-band per i dispositivi
IB-MGMT-VLAN	3334	VLAN di gestione in-band per host ESXi, gestione delle macchine virtuali e così via
NFS-VLAN	3335	VLAN NFS opzionale per il traffico NFS
ISCSI-A-VLAN	3336	ISCSI-A Fabric VLAN per il traffico iSCSI
ISCSI-B-VLAN	3337	VLAN del fabric iSCSI-B per il traffico iSCSI
VLAN VMotion	3338	VLAN di traffico VMware vMotion
VM-Traffic-VLAN	3339	VLAN del traffico VMware VM

Nome	ID VLAN	Utilizzo
VLAN intercluster	3340	VLAN intercluster per comunicazioni peer cluster ONTAP

> Anche se SM-BC non supporta i protocolli NFS o CIFS per la business continuity, è comunque possibile utilizzarli per carichi di lavoro che non devono essere protetti per la business continuity. Gli archivi dati NFS non sono stati creati per questa convalida.

"Successivo: Convalida della soluzione - Storage."

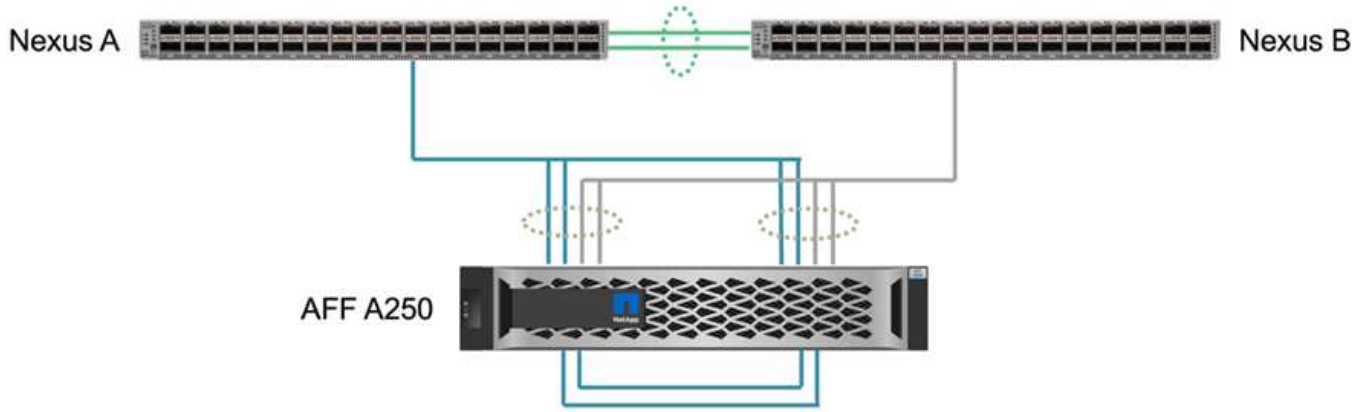
Convalida della soluzione - Storage

"Precedente: Convalida della soluzione - rete."

La configurazione dello storage per la soluzione FlexPod SM-BC segue le Best practice tipiche delle soluzioni FlexPod in ogni sito. Per il peering del cluster SM-BC e la replica dei dati, utilizzano i collegamenti tra siti stabiliti tra gli switch FlexPod di entrambi i siti. Nelle sezioni seguenti vengono illustrate alcune delle configurazioni e della connettività utilizzate per la convalida.

Connettività

La connettività dello storage alle IFI UCS locali e ai server blade viene fornita dagli switch Nexus del sito locale. Attraverso la connettività dello switch Nexus tra i siti, è possibile accedere allo storage anche dai blade server UCS remoti. La figura e la tabella seguenti mostrano il diagramma di connettività dello storage e un elenco di connessioni per i controller dello storage in ogni sito.



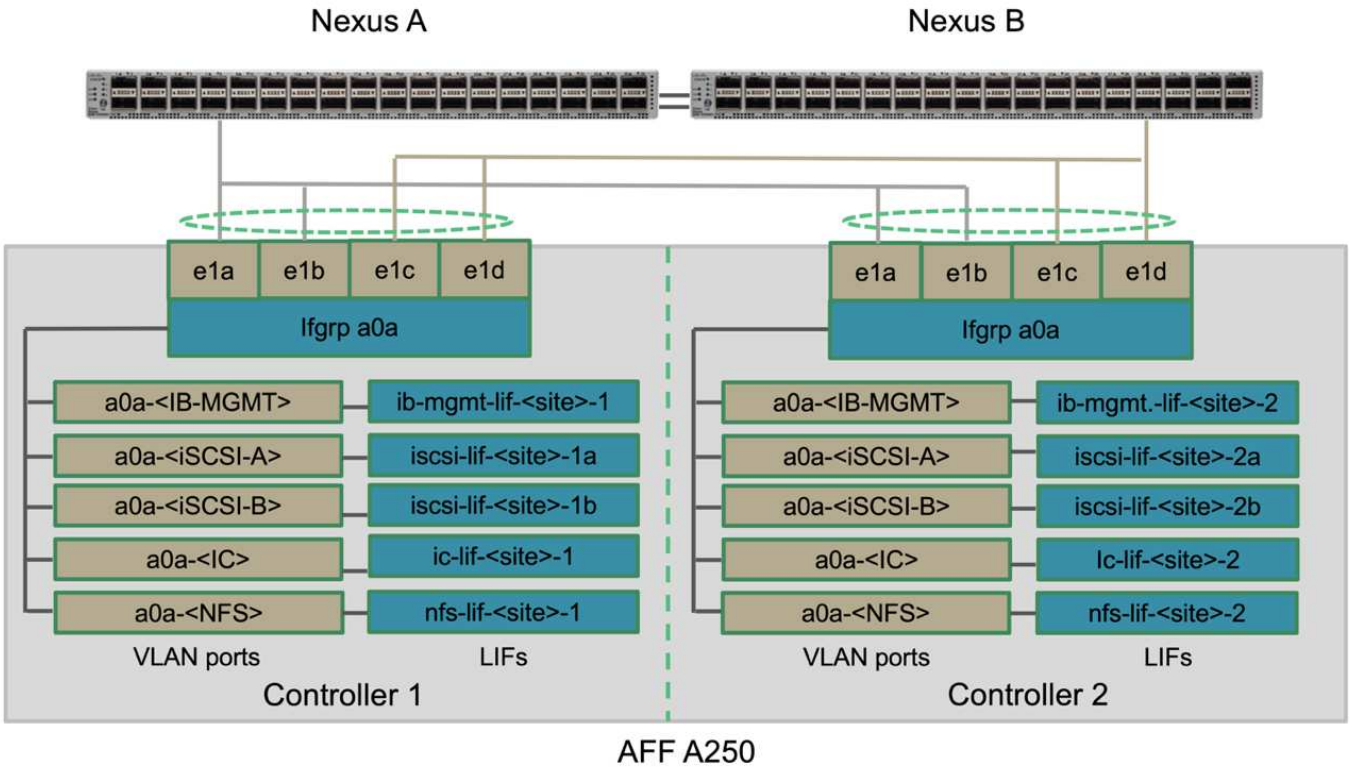
Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
AFF A250 A.	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A.	1/10/1
	e1b		1/10/2
	e1c	Nexus B	1/10/1

Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
	e1d		1/10/2
AFF A250 B	e0c	AFF A250 A.	e0c
	e0d		e0d
	e1a	Nexus A.	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

Connessioni e interfacce

Due porte fisiche su ciascun controller di storage sono collegate a ciascuno switch Nexus per l'aggregazione della larghezza di banda e la ridondanza per questa convalida. Queste quattro connessioni partecipano a una configurazione di gruppo di interfacce sullo storage. Le porte corrispondenti sugli switch Nexus partecipano a un VPC per l'aggregazione e la resilienza del collegamento.

I protocolli di gestione in-band, inter-cluster e storage dei dati NFS/iSCSI utilizzano VLAN. Le porte VLAN vengono create sul gruppo di interfacce per separare i diversi tipi di traffico. Le interfacce logiche (LIF) per le rispettive funzioni vengono create sulla parte superiore delle porte VLAN corrispondenti. La figura seguente mostra la relazione tra connessioni fisiche, gruppi di interfacce, porte VLAN e interfacce logiche.



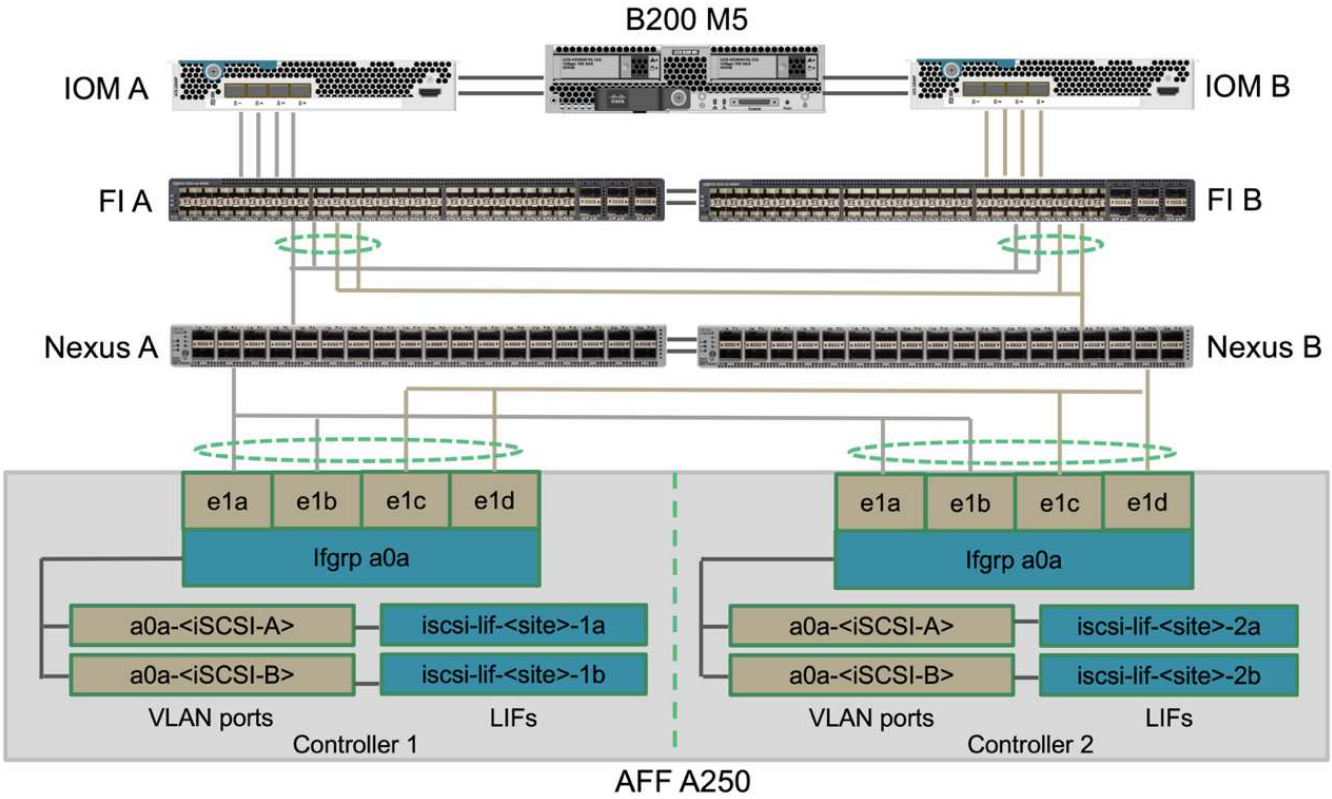
Boot SAN

NetApp consiglia di implementare l'avvio SAN per i server Cisco UCS nella soluzione FlexPod. L'implementazione dell'avvio SAN consente di proteggere in modo sicuro il sistema operativo all'interno del sistema di storage NetApp, fornendo migliori performance e flessibilità. Per questa soluzione, è stato validato

l'avvio SAN iSCSI.

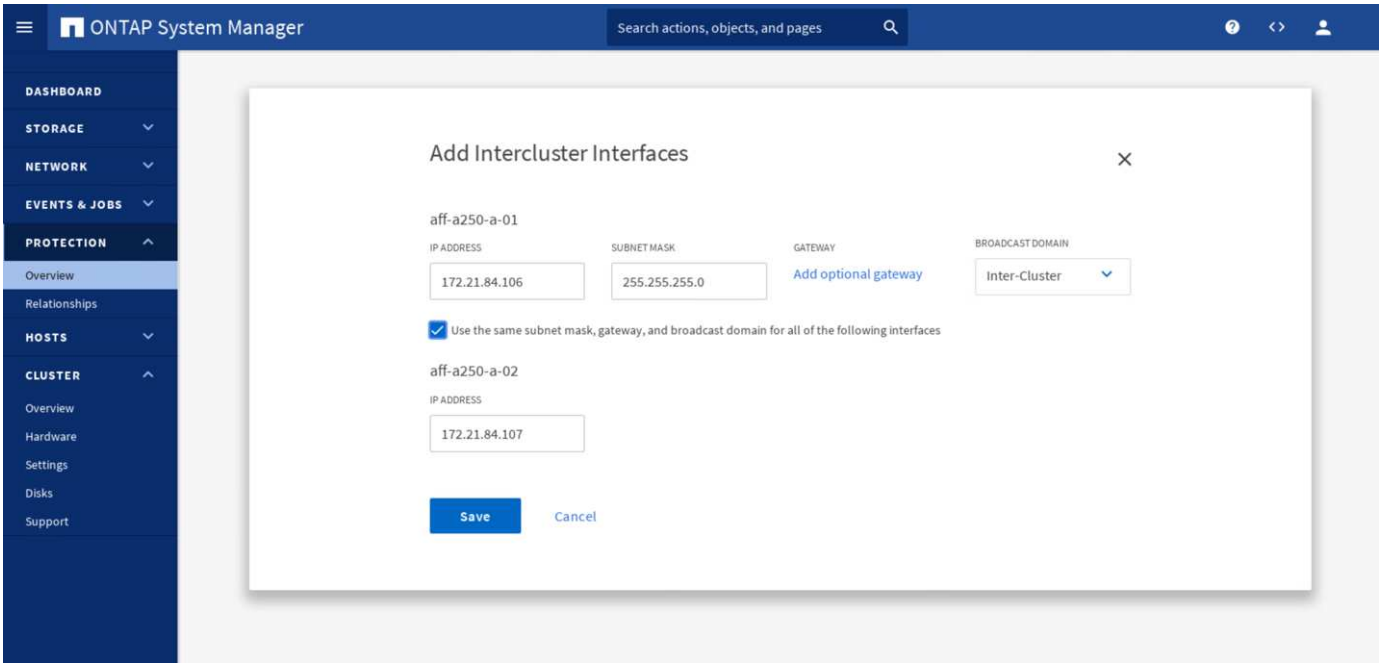
La figura seguente mostra la connettività per l'avvio SAN iSCSI del server Cisco UCS dallo storage NetApp. Nell'avvio SAN iSCSI, a ciascun server Cisco UCS vengono assegnate due vNIC iSCSI (una per ciascun fabric SAN) che forniscono una connettività ridondante dal server fino allo storage. Le porte di storage Ethernet 10/25-G collegate agli switch Nexus (in questo esempio e1a, e1b, e1c e e1d) sono raggruppate in modo da formare un gruppo di interfacce (ifgrp) (in questo esempio, a0a). Le porte VLAN iSCSI vengono create su ifgrp e le LIF iSCSI vengono create sulle porte VLAN iSCSI.

Ogni LUN di boot iSCSI viene mappato al server che si avvia da esso attraverso le LIF iSCSI associando il LUN di boot con i nomi iSCSI qualificati del server (IQN) nel relativo igroup di boot. L'igroup di boot del server contiene due IQN, uno per ogni fabric vNIC/SAN. Questa funzione consente solo al server autorizzato di accedere al LUN di avvio creato appositamente per tale server.



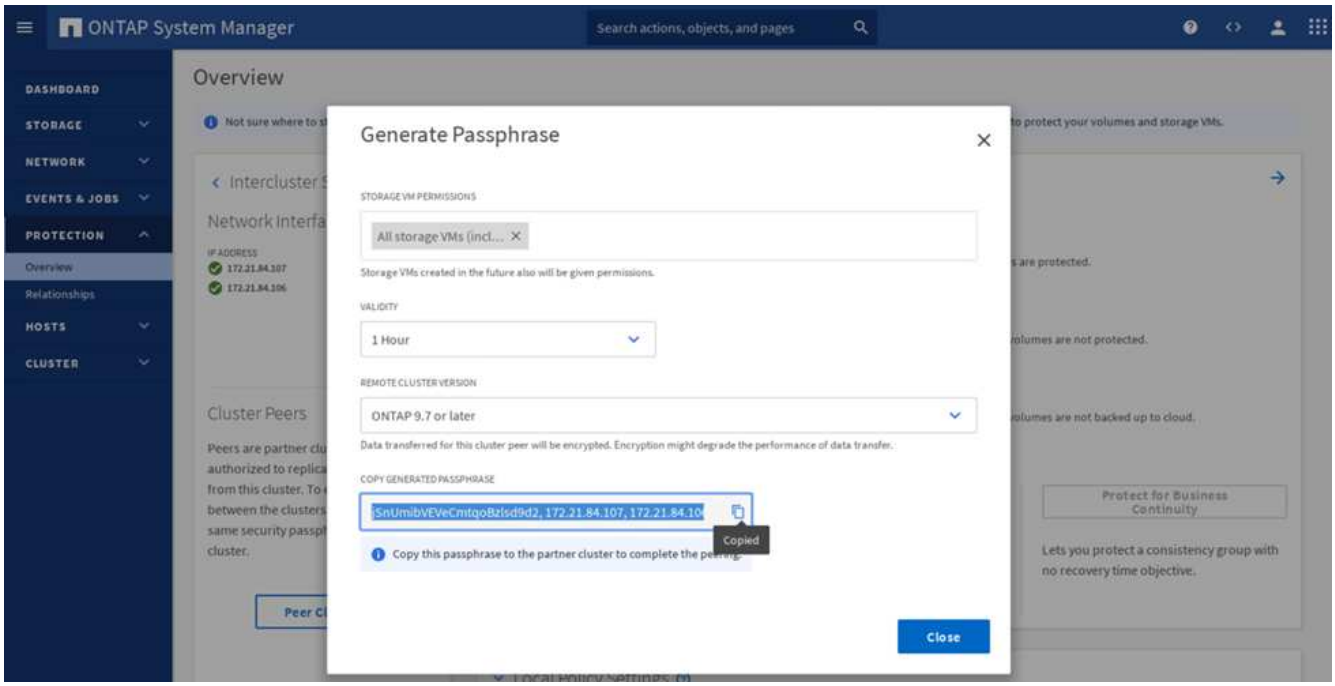
Peering dei cluster

I peer del cluster ONTAP comunicano tramite le LIF dell'intercluster. Utilizzando Gestione di sistema di ONTAP per i due cluster, è possibile creare le LIF di intercluster necessarie nel pannello protezione > Panoramica.

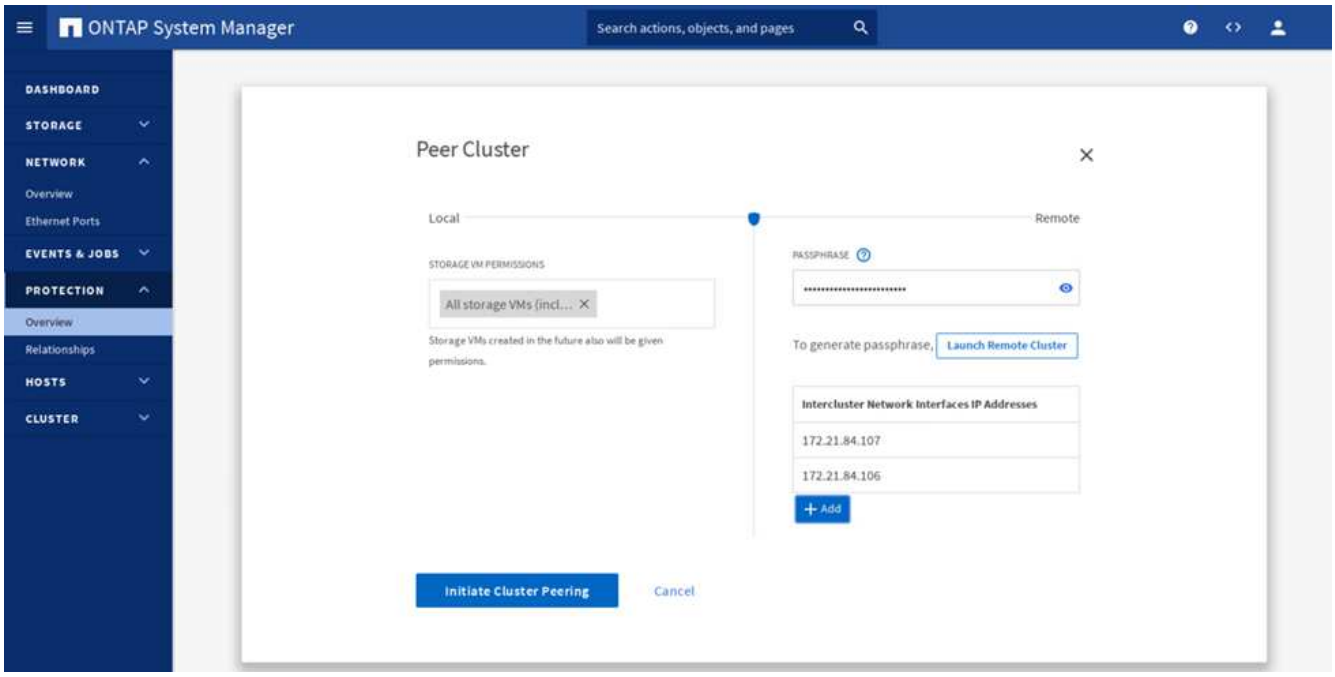


Per unire i due cluster, completare i seguenti passaggi:

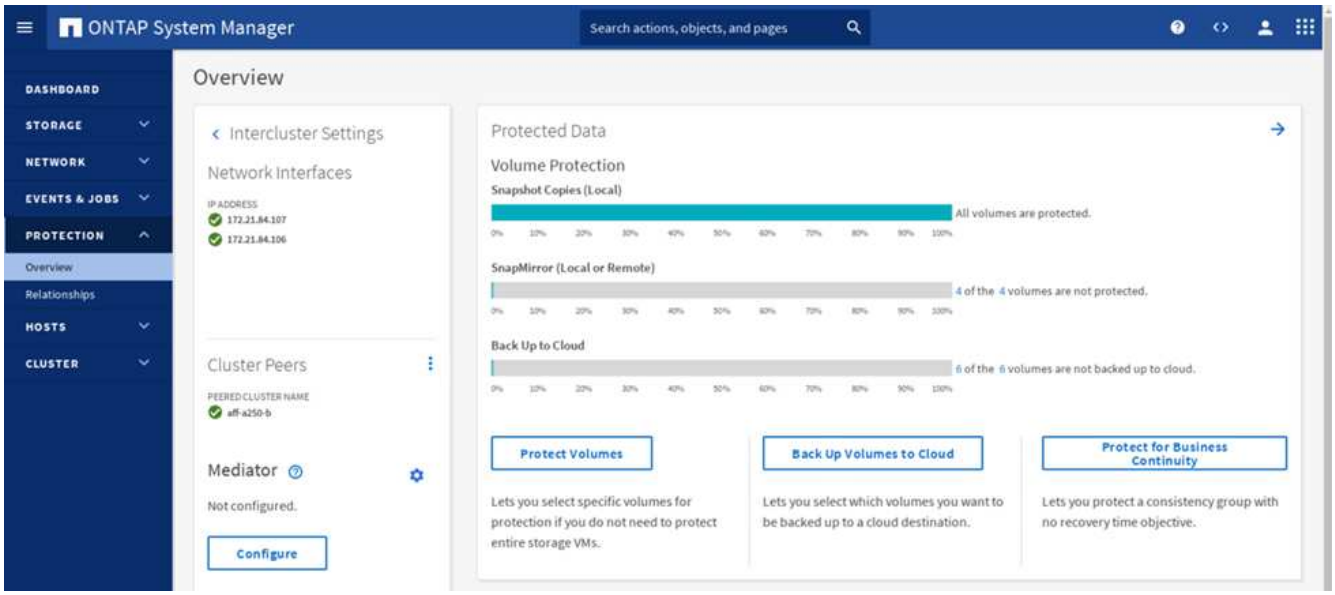
1. Generare la passphrase di peering del cluster nel primo cluster.



2. Richiamare l’opzione Peer Cluster nel secondo cluster e fornire la passphrase e le informazioni LIF dell’intercluster.



3. Il pannello System Manager Protection > Overview (protezione > Panoramica di System Manager) mostra le informazioni relative ai peer del cluster.

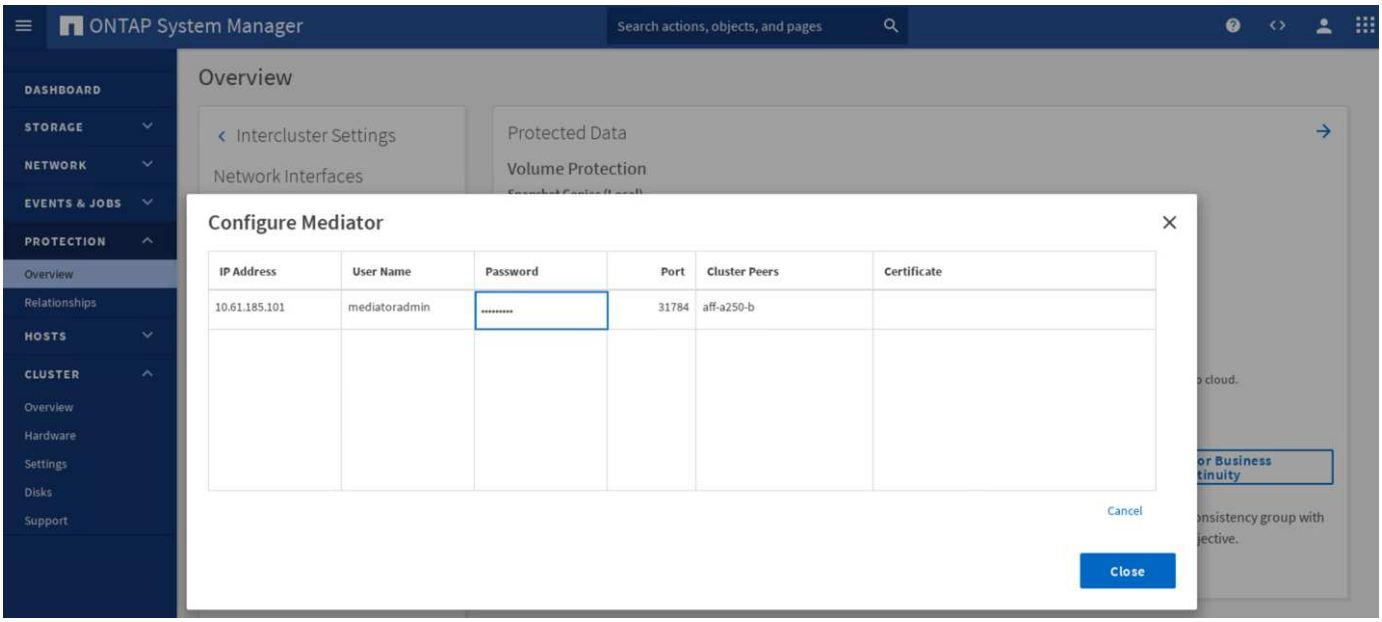


Installazione e configurazione del mediatore ONTAP

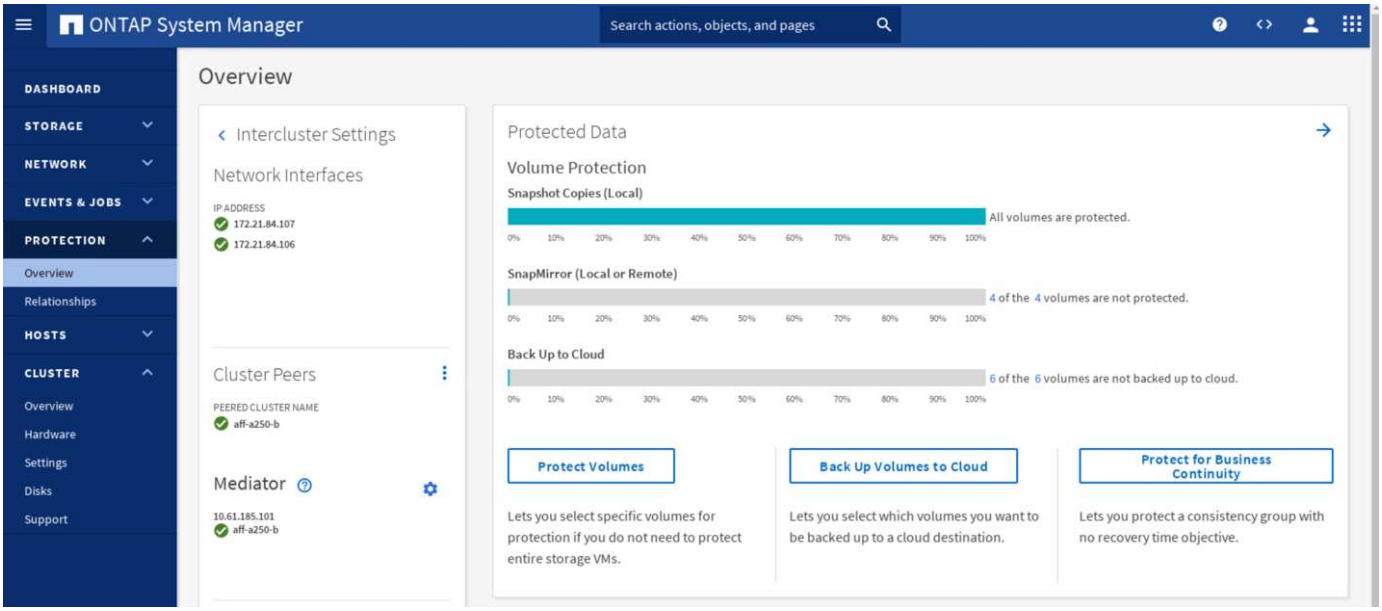
Il mediatore ONTAP stabilisce un quorum per i cluster ONTAP in una relazione SM-BC. Coordina il failover automatizzato quando viene rilevato un guasto e aiuta a evitare scenari di split-brain quando ogni cluster tenta contemporaneamente di stabilire il controllo come cluster primario.

Prima di installare il mediatore ONTAP, consultare "Installare o aggiornare il servizio di supporto ONTAP" Pagina per i prerequisiti, le versioni di Linux supportate e le procedure per l'installazione sui vari sistemi operativi Linux supportati.

Una volta installato il mediatore ONTAP, è possibile aggiungere il certificato di sicurezza del mediatore ONTAP ai cluster ONTAP e configurare il mediatore ONTAP nel pannello protezione > Panoramica di Gestione sistema. La seguente schermata mostra la GUI di configurazione del mediatore ONTAP.



Dopo aver fornito le informazioni necessarie, il mediatore ONTAP configurato viene visualizzato nel pannello protezione > Panoramica di Gestione sistema.



Gruppo di coerenza SM-BC

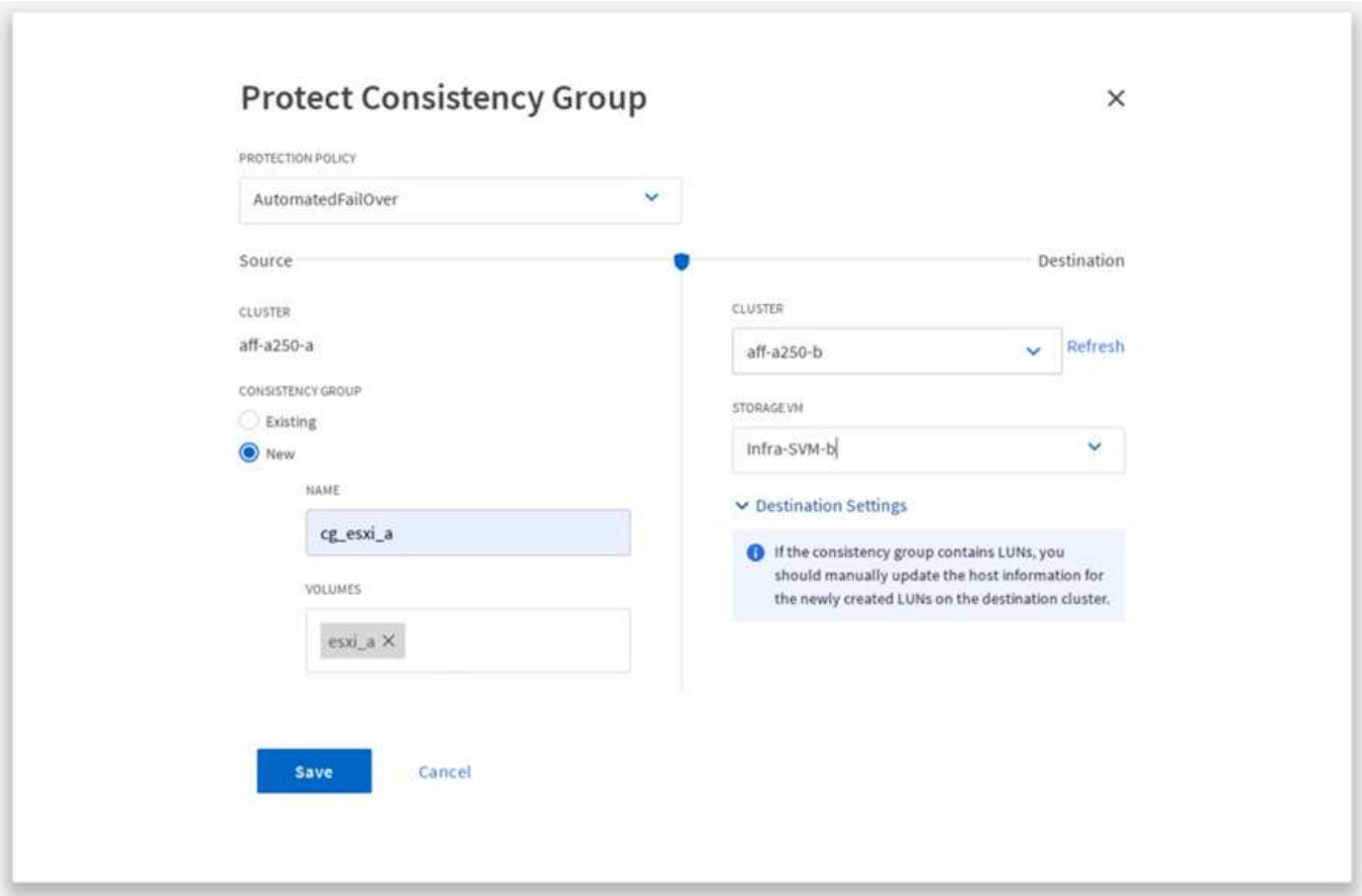
Un gruppo di coerenza offre una garanzia di coerenza dell'ordine di scrittura per un workload dell'applicazione che copre un insieme di volumi specificati. Per ONTAP 9.10.1, ecco alcune delle limitazioni e delle limitazioni più importanti.

- Il numero massimo di relazioni di gruppo di coerenza SM-BC in un cluster è 20.
- Il numero massimo di volumi supportati per relazione SM-BC è 16.
- Il numero massimo di endpoint totali di origine e destinazione in un cluster è 200.

Per ulteriori informazioni, consultare la documentazione di ONTAP SM-BC sul "restrizioni e limitazioni".

Per la configurazione della convalida, è stato utilizzato Gestore di sistema di ONTAP per creare i gruppi di

coerenza per proteggere le LUN di avvio ESXi e le LUN degli archivi dati condivisi per entrambi i siti. La finestra di dialogo per la creazione di gruppi di coerenza è accessibile selezionando protezione > Panoramica > protezione per la business continuity > Proteggi gruppo di coerenza. Per creare un gruppo di coerenza, fornire i volumi di origine, il cluster di destinazione e le informazioni sulla macchina virtuale di storage di destinazione necessari per la creazione.

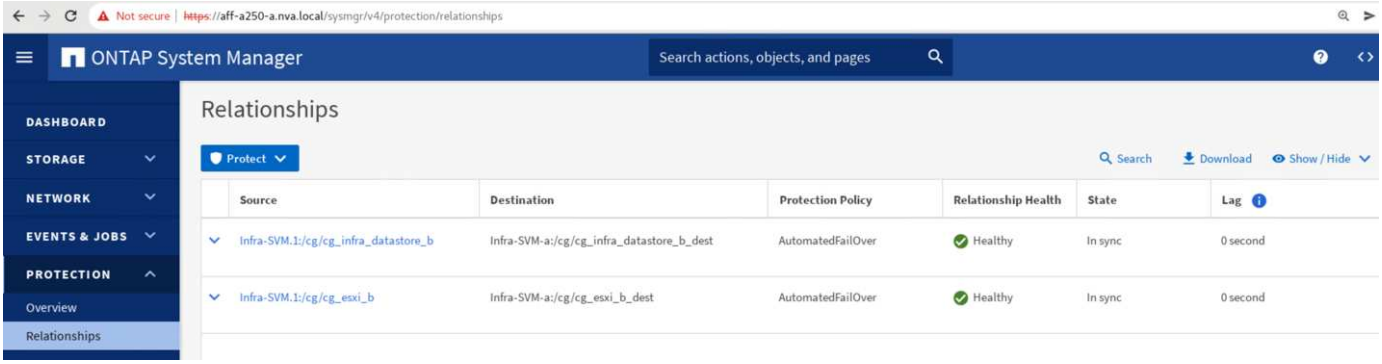


Nella tabella seguente sono elencati i quattro gruppi di coerenza creati e i volumi inclusi in ciascun gruppo di coerenza per il test di convalida.

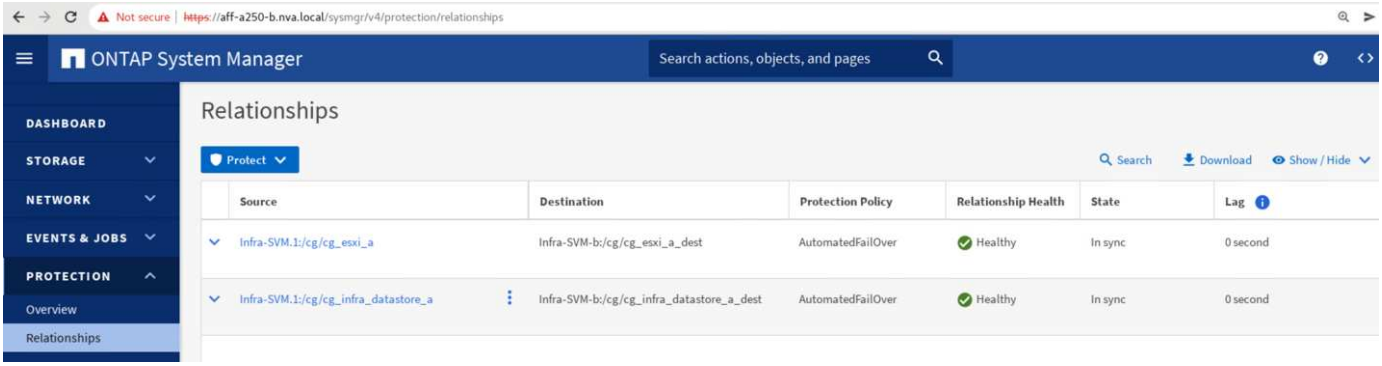
System Manager	Gruppo di coerenza	Volumi
Sito A	cg_esxi_a.	esxi_a.
Sito A	cg_infra_datastore_a.	infra_datastore_a_01 infra_datastore_a_02
Sito B	cg_esxi_b	esxi_b
Sito B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

Una volta creati, i gruppi di coerenza vengono visualizzati sotto le rispettive relazioni di protezione nel sito A e nel sito B.

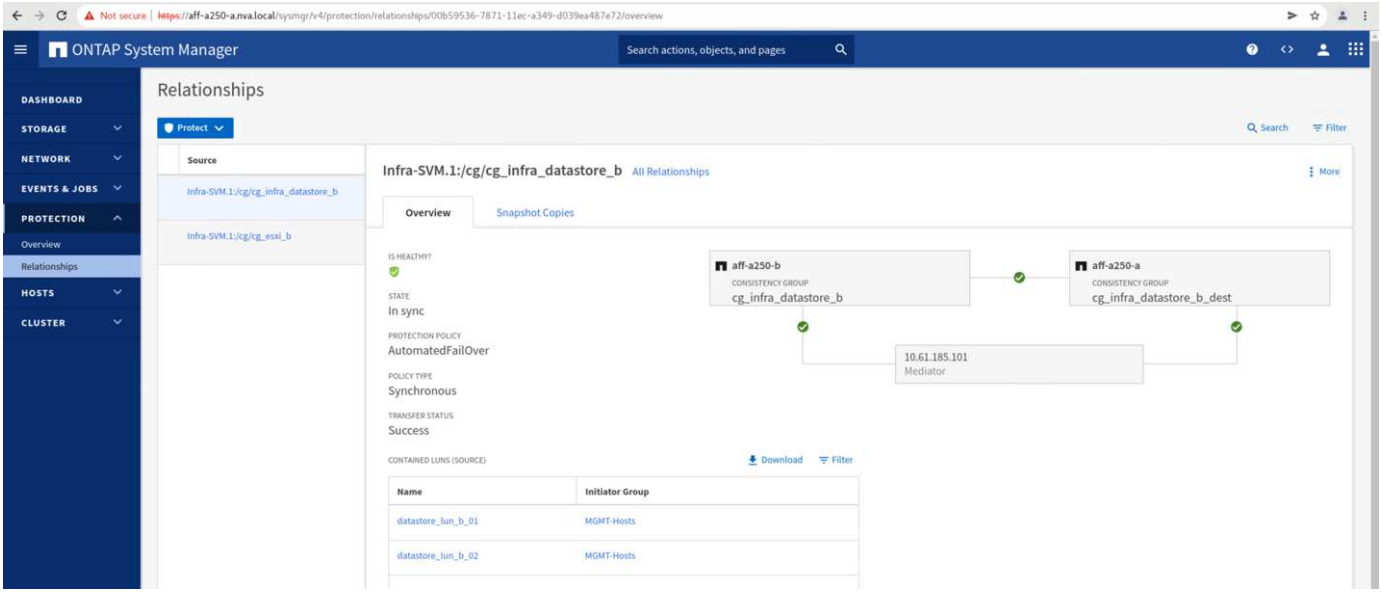
Questa schermata mostra le relazioni dei gruppi di coerenza nel sito A.



Questa schermata mostra le relazioni dei gruppi di coerenza nel sito B.



Questa schermata mostra i dettagli delle relazioni del gruppo di coerenza per il gruppo cg_infra_datastore_b.



Volumi, LUN e mappature host

Una volta creati i gruppi di coerenza, SnapMirror sincronizza i volumi di origine e di destinazione in modo che i dati possano essere sempre sincronizzati. I volumi di destinazione del sito remoto riportano i nomi dei volumi con il _dest end (fine destinazione). Ad esempio, per il volume esxi_a nel cluster del sito A, nel sito B è presente un volume esxi_a_dest Data Protection (DP) corrispondente

Questa schermata mostra le informazioni sul volume per il sito A.

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Questa schermata mostra le informazioni sul volume per il sito B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Per facilitare il failover trasparente delle applicazioni, è necessario mappare anche i LUN SM-BC mirrorati agli host dal cluster di destinazione. In questo modo, gli host possono visualizzare correttamente i percorsi verso le LUN dai cluster di origine e di destinazione. Il `igroup show` e. `lun show` Le uscite per il sito A e il sito B vengono acquisite nelle due schermate seguenti. Con le mappature create, ogni host ESXi nel cluster vede il proprio LUN di avvio SAN come ID 0 e tutte e quattro le LUN degli archivi dati iSCSI condivisi.

Questa schermata mostra la mappatura di igroups e LUN host per un cluster del sito A.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01           VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02           VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03           VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                   MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01      VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02      VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03      VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b              MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

Questa schermata mostra la mappatura di igroups e LUN host per il cluster del sito B.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Successivo: Convalida della soluzione - virtualizzazione."

Convalida della soluzione - virtualizzazione

"Precedente: Convalida della soluzione - Storage."

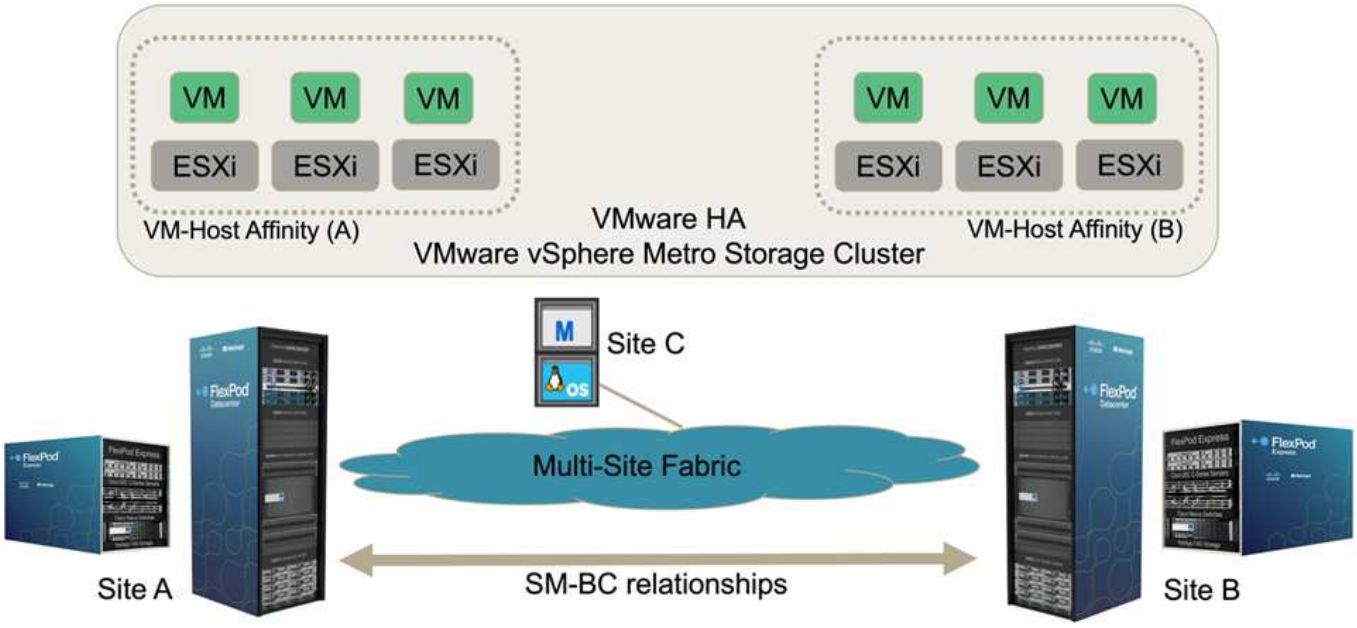
Nella soluzione multi-sito FlexPod SM-BC, un singolo VMware vCenter gestisce le risorse dell'infrastruttura virtuale per l'intera soluzione. Gli host di entrambi i data center partecipano al singolo cluster VMware ha che copre entrambi i data center. Gli host hanno accesso alla soluzione NetApp SM-BC, in cui è possibile accedere allo storage con relazioni SM-BC definite da entrambi i siti.

Lo storage della soluzione SM-BC è conforme al modello di accesso uniforme della funzionalità vMSC (VMware vSphere Metro Storage Cluster) per evitare disastri e downtime. Per ottenere performance ottimali delle macchine virtuali, i dischi delle macchine virtuali devono essere ospitati sui sistemi NetApp AFF A250 locali per ridurre al minimo la latenza e il traffico tra i collegamenti WAN durante il normale funzionamento.

Nell'ambito dell'implementazione della progettazione, è necessario determinare la distribuzione delle macchine virtuali tra i due siti. È possibile determinare l'affinità del sito della macchina virtuale e la distribuzione delle applicazioni tra i due siti in base alle preferenze del sito e ai requisiti dell'applicazione. I gruppi VM/host del cluster VMware e le regole VM/host vengono utilizzati per configurare l'affinità VM/host per assicurarsi che le VM siano in esecuzione sugli host del sito desiderato.

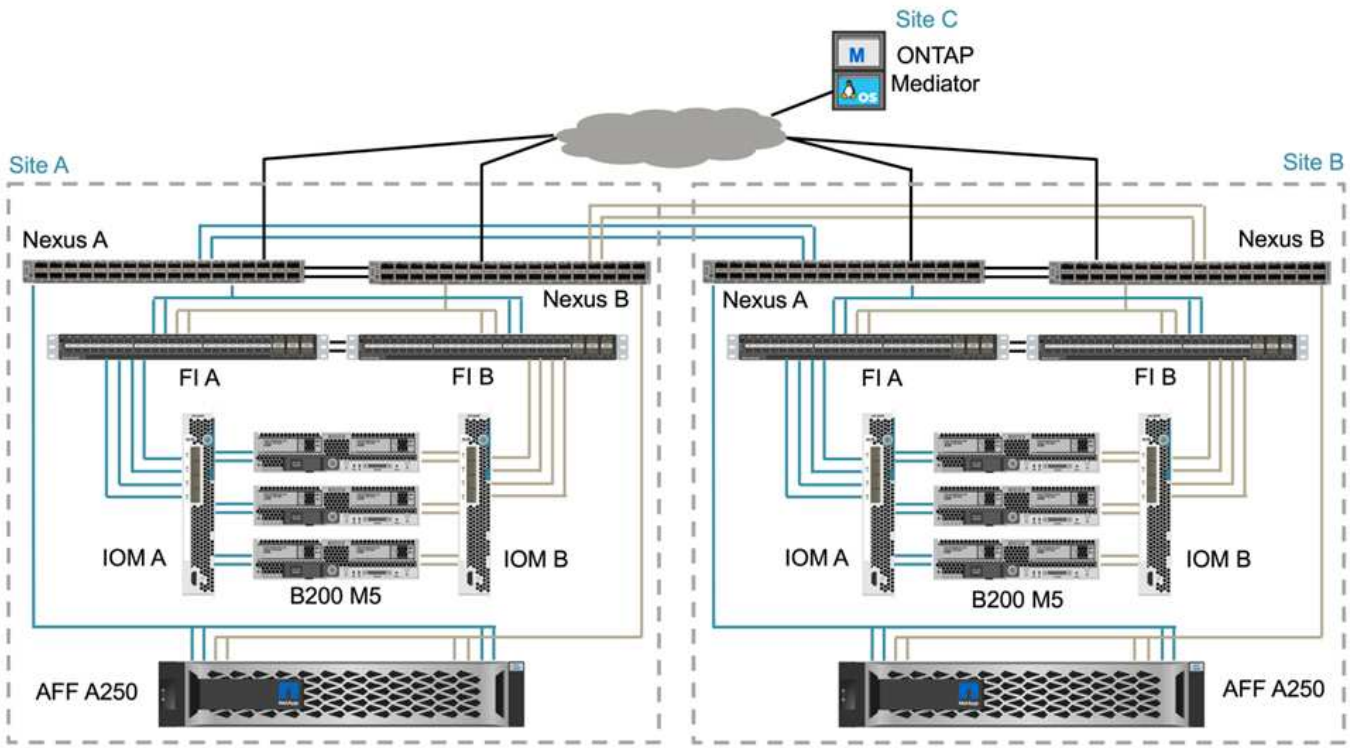
Tuttavia, le configurazioni che consentono l'esecuzione delle macchine virtuali in entrambi i siti garantiscono che le macchine virtuali possano essere riavviate da VMware ha negli host del sito remoto per fornire la resilienza della soluzione. Per consentire l'esecuzione delle macchine virtuali in entrambi i siti, tutti gli archivi dati condivisi iSCSI devono essere montati su tutti gli host ESXi per garantire un funzionamento vMotion fluido delle macchine virtuali tra i siti.

La figura seguente mostra una vista di alto livello sulla virtualizzazione della soluzione FlexPod SM-BC che include sia le funzionalità VMware ha che vMSC per fornire un'elevata disponibilità per i servizi di calcolo e storage. L'architettura della soluzione di data center Active-Active consente la mobilità dei carichi di lavoro tra i siti e fornisce protezione DR/BC.



Connettività di rete end-to-end

La soluzione FlexPod SM-BC include infrastrutture FlexPod in ogni sito, connettività di rete tra siti e mediatore ONTAP implementato in un terzo sito per soddisfare gli obiettivi RPO e RTO richiesti. La figura seguente mostra la connettività di rete end-to-end tra i server Cisco UCS B200M5 di ciascun sito e lo storage NetApp con funzionalità SM-BC all'interno di un sito e tra siti.



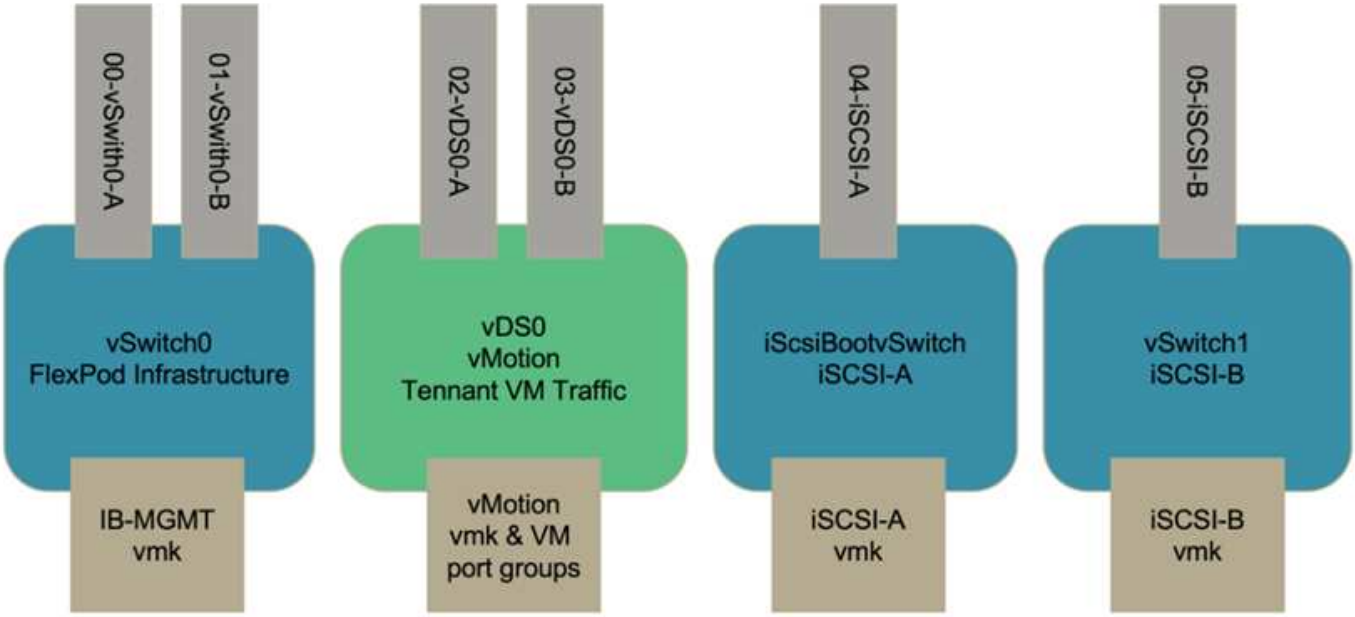
L'architettura di implementazione di FlexPod è identica in ogni sito per la convalida di questa soluzione. Tuttavia, la soluzione supporta implementazioni asimmetriche e può essere aggiunta a soluzioni FlexPod esistenti se soddisfano i requisiti.

L'architettura Layer-2 estesa viene utilizzata per un data fabric multi-sito perfetto che fornisce connettività tra il calcolo Cisco UCS con canale di porta e lo storage NetApp in ogni data center, oltre alla connettività tra i data center. La configurazione del canale delle porte e la configurazione del canale delle porte virtuali, se appropriato, vengono utilizzate per l'aggregazione della larghezza di banda e la tolleranza agli errori tra i livelli di calcolo, rete e storage, nonché per i collegamenti tra siti. Di conseguenza, i blade server UCS dispongono di connettività e accesso multipath allo storage NetApp locale e remoto.

Networking virtuale

Ciascun host del cluster viene implementato utilizzando reti virtuali identiche, indipendentemente dalla sua posizione. La progettazione separa i diversi tipi di traffico utilizzando gli switch virtuali VMware (vSwitch) e VMware Virtual Distributed Switch (VDS). VMware vSwitch viene utilizzato principalmente per le reti dell'infrastruttura FlexPod e VDS per le reti applicative, ma non è necessario.

Gli switch virtuali (vSwitch, VDS) vengono implementati con due uplink per switch virtuale; gli uplink a livello di hypervisor ESXi vengono definiti vmnics e vNIC virtuali (vNIC) sul software Cisco UCS. Le vNIC vengono create sull'adattatore VIC Cisco UCS in ciascun server utilizzando i profili di servizio Cisco UCS. Sono definite sei vNIC, due per vSwitch0, due per vDS0, due per vSwitch1 e due per gli uplink iSCSI, come mostrato nella figura seguente.



VSwitch0 viene definito durante la configurazione dell'host VMware ESXi e contiene la VLAN di gestione dell'infrastruttura FlexPod e le porte VMkernel (VMK) dell'host ESXi per la gestione. Su vSwitch0 è disponibile anche un gruppo di porte delle macchine virtuali per la gestione dell'infrastruttura per qualsiasi macchina virtuale per la gestione dell'infrastruttura critica necessaria.

È importante posizionare tali macchine virtuali dell'infrastruttura di gestione su vSwitch0 invece che su VDS, perché se l'infrastruttura FlexPod viene spenta o spenta e si tenta di attivare la macchina virtuale di gestione su un host diverso dall'host su cui era originariamente in esecuzione, Si avvia correttamente sulla rete su vSwitch0. Questo processo è particolarmente importante se VMware vCenter è la macchina virtuale di gestione. Se vCenter si trovasse sul VDS e si spostasse su un altro host e poi si avviasse, non sarebbe connesso alla rete dopo l'avvio.

In questa progettazione vengono utilizzati due vSwitch di avvio iSCSI. L'avvio iSCSI di Cisco UCS richiede vNIC separate per l'avvio iSCSI. Queste vNIC utilizzano la VLAN iSCSI del fabric appropriato come VLAN nativa e sono collegate al vSwitch di boot iSCSI appropriato. Facoltativamente, è possibile implementare reti iSCSI su VDS implementando un nuovo VDS o utilizzando un VDS esistente.

Regole e gruppi di affinità VM-host

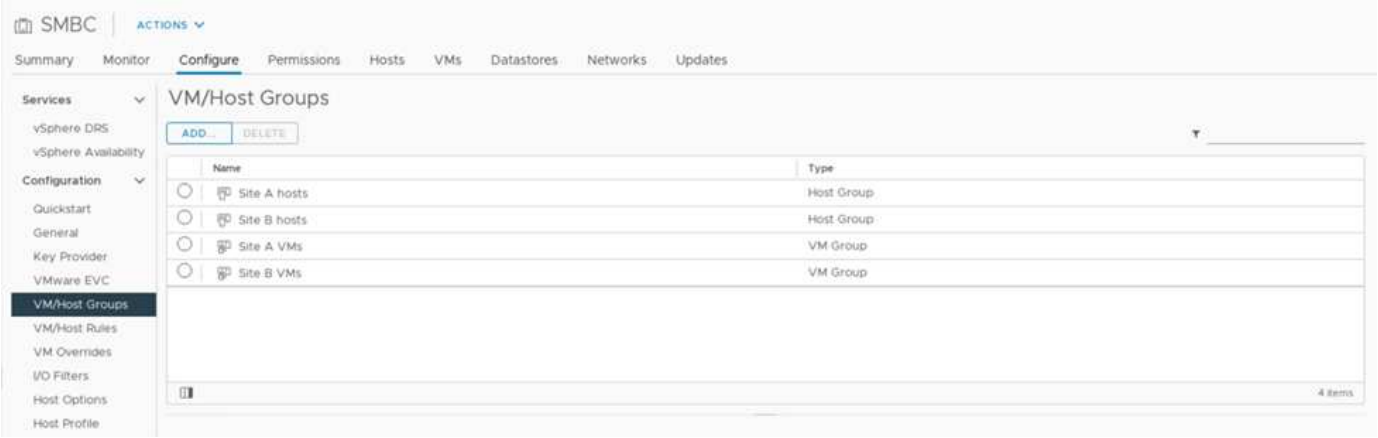
Per consentire l'esecuzione delle macchine virtuali su qualsiasi host ESXi in entrambi i siti SM-BC, tutti gli host ESXi devono montare gli archivi dati iSCSI da entrambi i siti. Se gli archivi dati di entrambi i siti sono montati correttamente da tutti gli host ESXi, è possibile migrare una macchina virtuale tra qualsiasi host con vMotion e la macchina virtuale mantiene comunque l'accesso a tutti i dischi virtuali creati da tali archivi dati.

Per una macchina virtuale che utilizza datastore locali, l'accesso ai dischi virtuali diventa remoto se viene migrato a un host nel sito remoto e quindi aumenta la latenza delle operazioni di lettura a causa della distanza fisica tra i siti. Pertanto, è consigliabile mantenere le macchine virtuali sugli host locali e utilizzare lo storage locale nel sito.

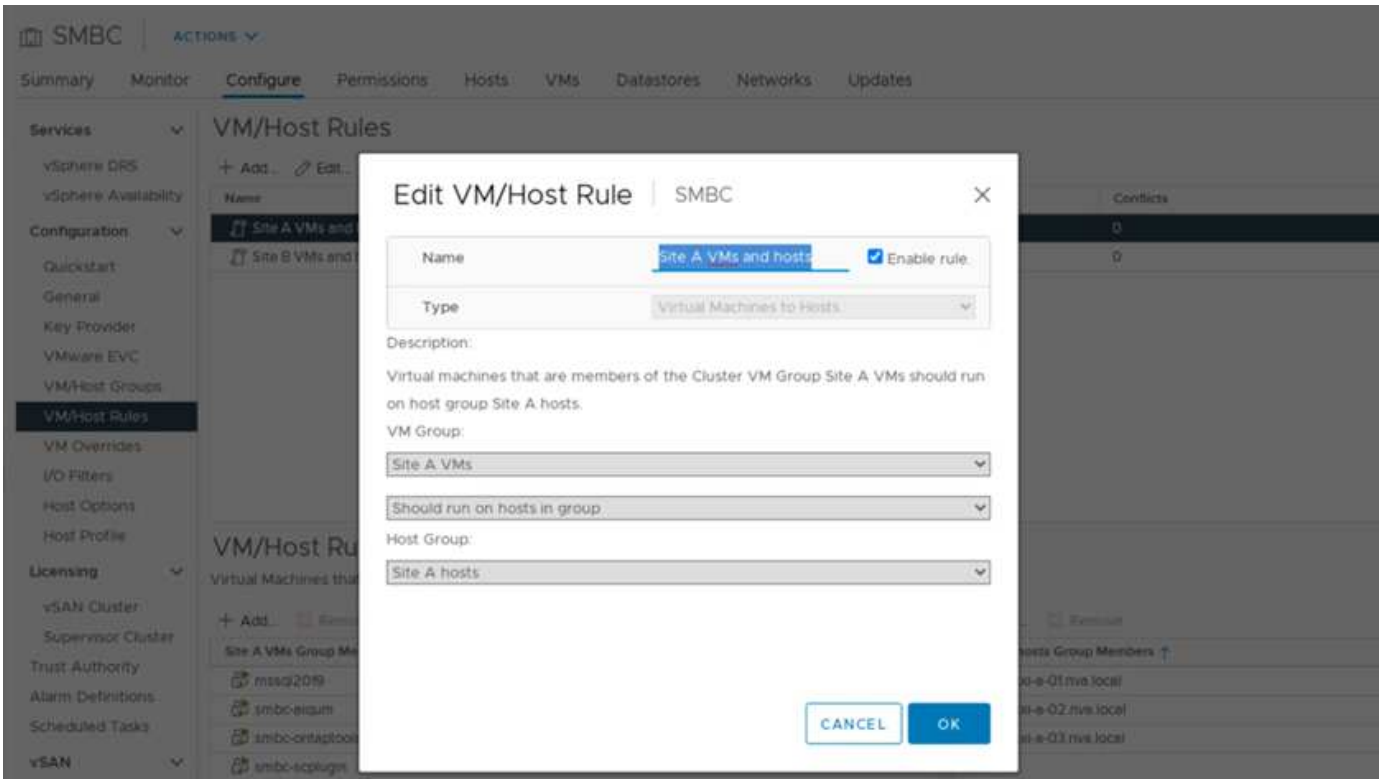
Utilizzando un meccanismo di affinità VM/host, è possibile utilizzare i gruppi VM/host per creare un gruppo VM e un gruppo host per macchine virtuali e host situati in un determinato sito. Utilizzando le regole VM/host, è possibile specificare il criterio per le macchine virtuali e gli host da seguire. Per consentire la migrazione delle macchine virtuali tra i siti durante la manutenzione del sito o uno scenario di emergenza, utilizzare la specifica della policy "dovrebbe essere eseguita sugli host nel gruppo" per ottenere tale flessibilità.

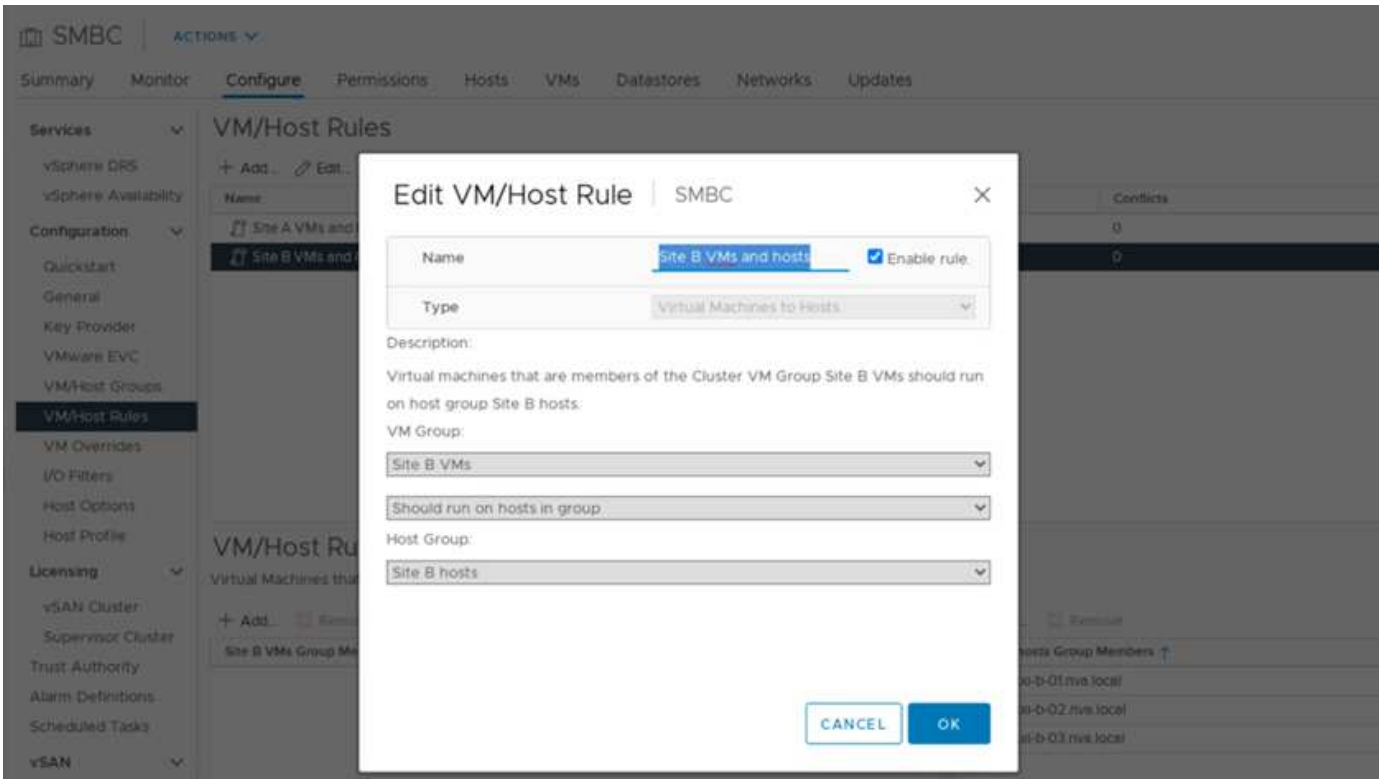
La seguente schermata mostra che vengono creati due gruppi di host e due gruppi di macchine virtuali per

host e macchine virtuali del sito A e del sito B.



Inoltre, le due figure seguenti mostrano le regole VM/host create per le VM del sito A e del sito B da eseguire sugli host dei rispettivi siti utilizzando il criterio "dovrebbe essere eseguito sugli host nel gruppo".

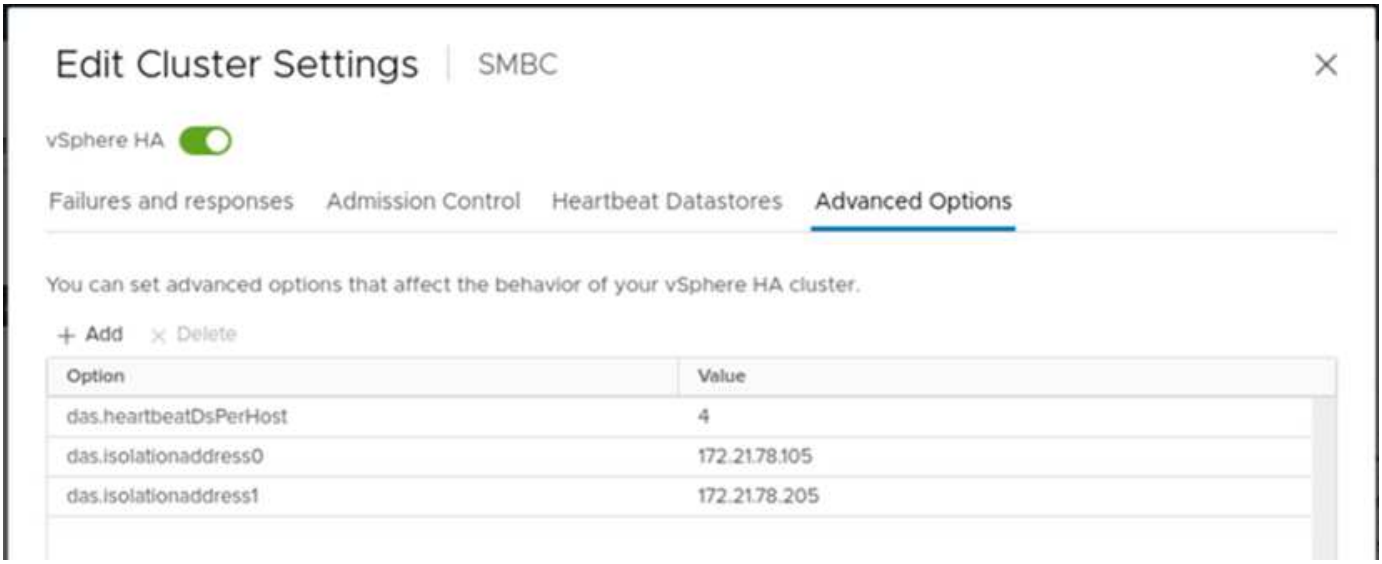




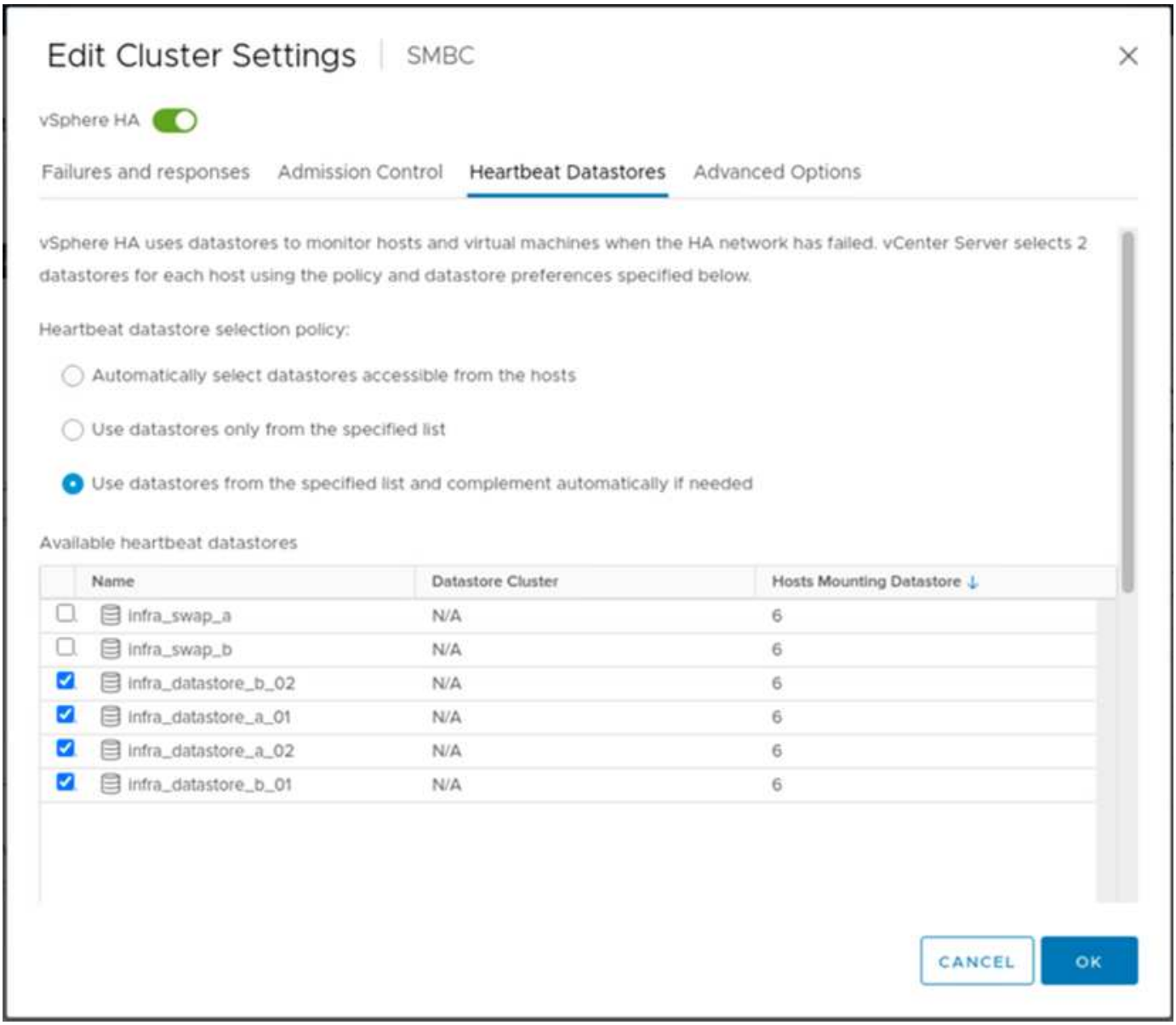
VSphere ha heartbeat

VMware vSphere ha dispone di un meccanismo heartbeat per la convalida dello stato dell'host. Il meccanismo heartbeat primario avviene attraverso la rete e il meccanismo heartbeat secondario attraverso il datastore. Se non vengono ricevuti heartbeat, decide se è isolato dalla rete eseguendo il ping del gateway predefinito o degli indirizzi di isolamento configurati manualmente. Per il battito cardiaco del datastore, VMware consiglia di aumentare i datastore heartbeat da un minimo di due a quattro per un cluster allungato.

Per la convalida della soluzione, vengono utilizzati i due indirizzi IP di gestione del cluster ONTAP come indirizzo di isolamento. Inoltre, l'opzione avanzata vSphere ha consigliata `ds.heartbeatDsPerHost` con un valore di 4 è stato aggiunto come mostrato nella figura seguente.



Per il datastore heartbeat, specificare automaticamente i quattro datastore condivisi dal cluster e il complemento, come mostrato nella figura seguente.



Per ulteriori Best practice e configurazioni per VMware ha Cluster e VMware vSphere Metro Storage Cluster, vedere "Creazione e utilizzo di cluster vSphere ha", "VMware vSphere Metro Storage Cluster (vMSC)" E la KB VMware per "NetApp ONTAP con NetApp SnapMirror Business Continuity (SM-BC) e VMware vSphere Metro Storage Cluster (vMSC)".

"Successivo: Convalida della soluzione - scenari validati."

Convalida della soluzione - scenari validati

"Precedente: Convalida della soluzione - virtualizzazione."

La soluzione FlexPod Datacenter SM-BC protegge i servizi dati per una vasta gamma di scenari a singolo punto di errore e in caso di disastro del sito. Il design ridondante implementato in ogni sito offre alta disponibilità e l'implementazione di SM-BC con replica sincrona dei dati tra i siti protegge i servizi dati da un disastro a livello di sito. La soluzione implementata è convalidata per le funzioni della soluzione desiderate e per i vari scenari di guasto per i quali la soluzione è progettata per proteggere.

Convalida delle funzioni della soluzione

Per verificare le funzioni della soluzione e simulare scenari di guasto parziale e completo del sito vengono utilizzati diversi casi di test. Per ridurre al minimo la duplicazione con i test già eseguiti nelle soluzioni FlexPod Datacenter esistenti nell'ambito del programma Cisco Validated Design, l'attenzione di questo report è incentrata sugli aspetti della soluzione correlati a SM-BC. Sono incluse alcune convalide FlexPod generali per i professionisti che devono eseguire le convalide di implementazione.

Per la convalida della soluzione, è stata creata una macchina virtuale Windows 10 per host ESXi su tutti gli host ESXi di entrambi i siti. Lo strumento IOMeter è stato installato e utilizzato per generare i/o su due dischi di dati virtuali mappati dagli archivi dati iSCSI locali condivisi. I parametri del carico di lavoro IOMeter configurati erano 8 KB di i/o, 75% di lettura e 50% di random, con 8 comandi i/o in sospeso per ciascun disco dati. Per la maggior parte degli scenari di test eseguiti, la continuazione dell'i/o di IOMeter indica che lo scenario non ha causato un'interruzione del servizio dati.

Poiché SM-BC è un fattore critico per le applicazioni di business come i server di database, L'istanza di Microsoft SQL Server 2019 su una macchina virtuale Windows Server 2022 è stata inclusa anche come parte del test per confermare che l'applicazione continua a funzionare quando lo storage nel sito locale non è disponibile e il servizio dati viene ripristinato nello storage del sito remoto senza applicazione interruzioni.

Test di boot SAN iSCSI host ESXi

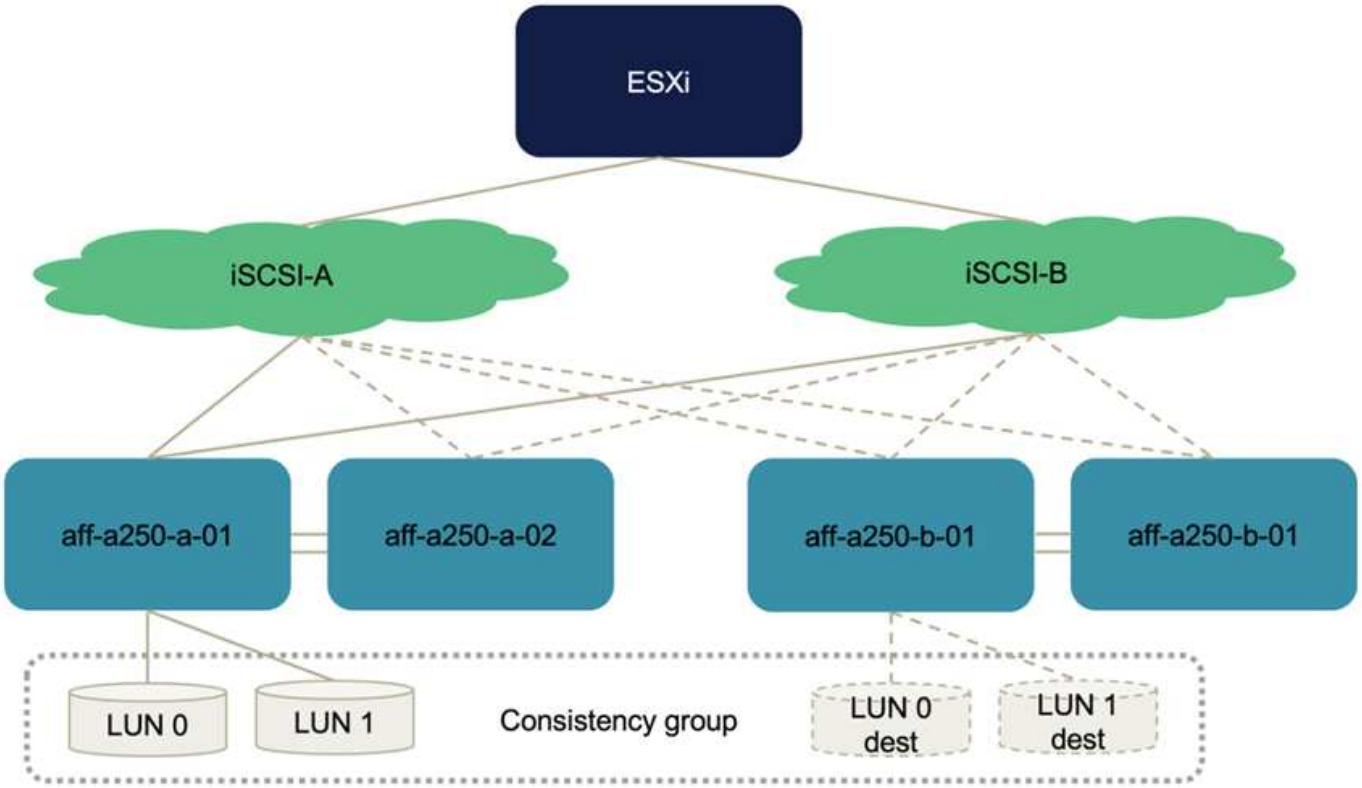
Gli host ESXi della soluzione sono configurati per l'avvio da SAN iSCSI. L'utilizzo dell'avvio SAN semplifica la gestione del server quando si sostituisce un server, in quanto il profilo di servizio del server può essere associato a un nuovo server per l'avvio senza apportare ulteriori modifiche alla configurazione.

Oltre all'avvio di un host ESXi situato in un sito dalla propria LUN di avvio iSCSI locale, sono stati eseguiti test anche per avviare l'host ESXi quando il controller dello storage locale si trova in uno stato di Takeover o quando il cluster di storage locale non è completamente disponibile. Questi scenari di convalida garantiscono che gli host ESXi siano configurati correttamente in base alla progettazione e possano avviarsi durante una manutenzione dello storage o uno scenario di emergenza per il disaster recovery per garantire la business continuity.

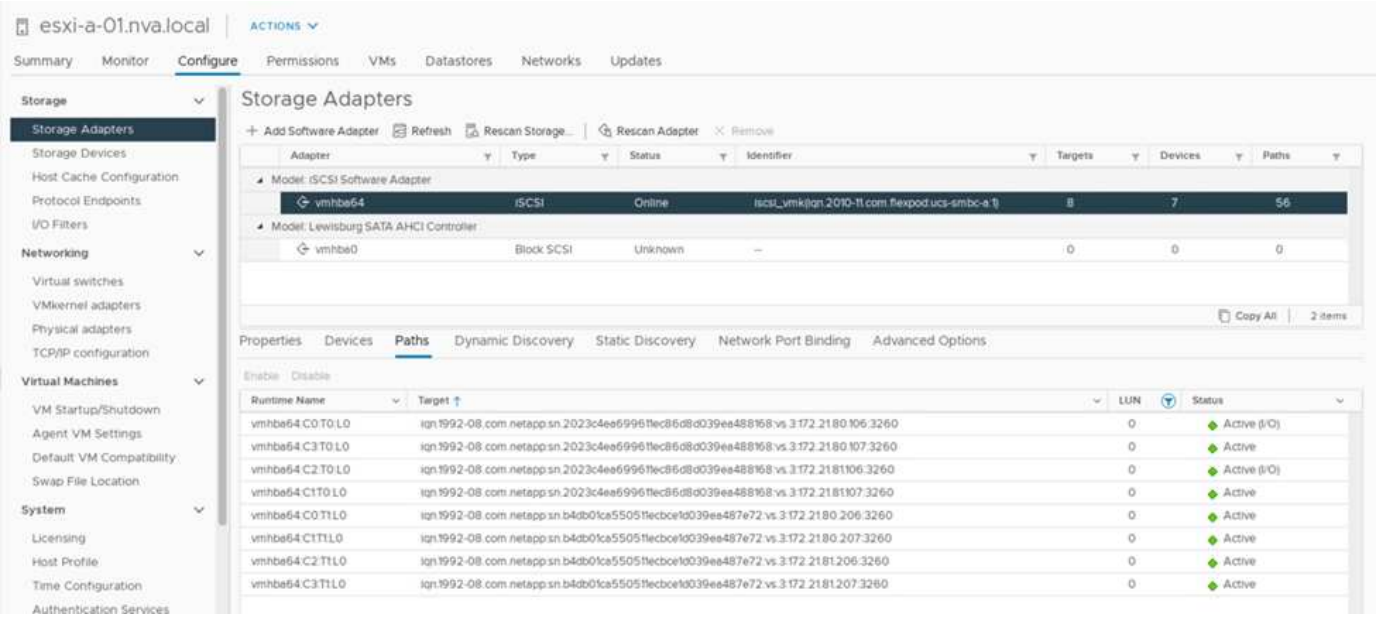
Prima di configurare la relazione del gruppo di coerenza SM-BC, un LUN iSCSI ospitato da una coppia ha di controller di storage dispone di quattro percorsi, due attraverso ogni fabric iSCSI, in base all'implementazione delle Best practice. Un host può accedere al LUN attraverso le due VLAN/fabric iSCSI al controller host LUN e attraverso il partner ad alta disponibilità del controller.

Dopo aver configurato la relazione del gruppo di coerenza SM-BC e aver mappato correttamente i LUN mirrorati agli iniziatori, il numero di percorsi per il LUN raddoppia. Per questa implementazione, si passa da due percorsi attivi/ottimizzati e due percorsi attivi/non ottimizzati a due percorsi attivi/ottimizzati e sei percorsi attivi/non ottimizzati.

La figura seguente illustra i percorsi che un host ESXi può utilizzare per accedere a un LUN, ad esempio LUN 0. Poiché il LUN è collegato al sito Un controller 01, solo i due percorsi che accedono direttamente al LUN tramite quel controller sono attivi/ottimizzati e tutti i sei percorsi rimanenti sono attivi/non ottimizzati.



La seguente schermata delle informazioni sul percorso del dispositivo di storage mostra come l'host ESXi vede i due tipi di percorsi del dispositivo. I due percorsi attivi/ottimizzati sono mostrati come aventi `active (I/O)` stato del percorso, mentre i sei percorsi attivi/non ottimizzati sono mostrati solo come `active`. Si noti inoltre che la colonna Target mostra le due destinazioni iSCSI e i rispettivi indirizzi IP LIF iSCSI per raggiungere le destinazioni.



Quando uno dei controller di storage non è più disponibile per la manutenzione o l'aggiornamento, i due percorsi che raggiungono il controller down non sono più disponibili e vengono visualizzati con uno stato di percorso di `dead` invece.

Se si verifica un failover del gruppo di coerenza sul cluster di storage primario, a causa di test di failover

manuali o failover automatico di emergenza, il cluster di storage secondario continua a fornire servizi dati per le LUN nel gruppo di coerenza SM-BC. Poiché le identità del LUN vengono preservate e i dati vengono replicati in modo sincrono, tutte le LUN di avvio degli host ESXi protette da gruppi di coerenza SM-BC rimangono disponibili dal cluster di storage remoto.

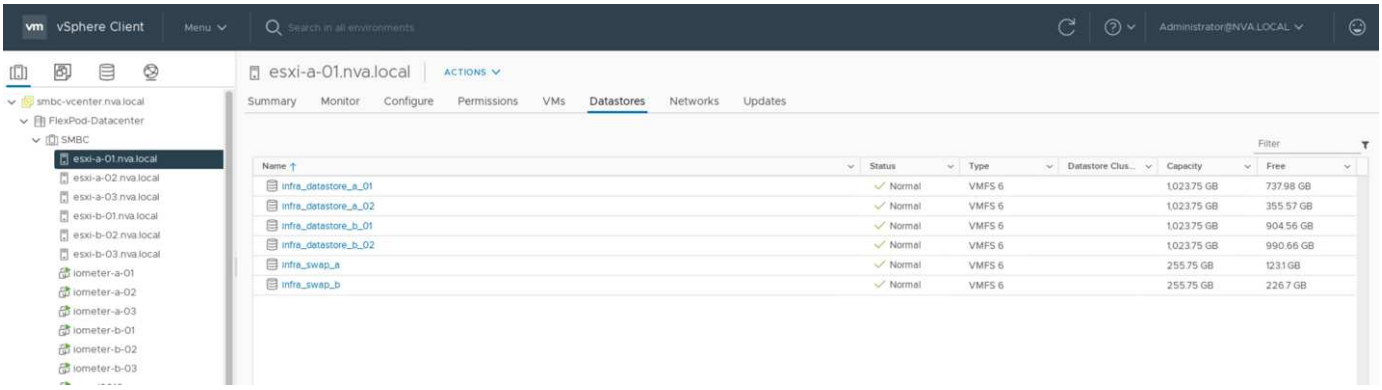
Test di affinità di VMware vMotion e VM/host

Sebbene una soluzione generica FlexPod per data center supporti multiprotocollo come FC, iSCSI, NVMe e NFS, la funzionalità della soluzione FlexPod SM-BC supporta i protocolli FC e iSCSI SAN generalmente utilizzati per le soluzioni business-critical. Questa convalida utilizza solo datastore basati su protocollo iSCSI e boot SAN iSCSI.

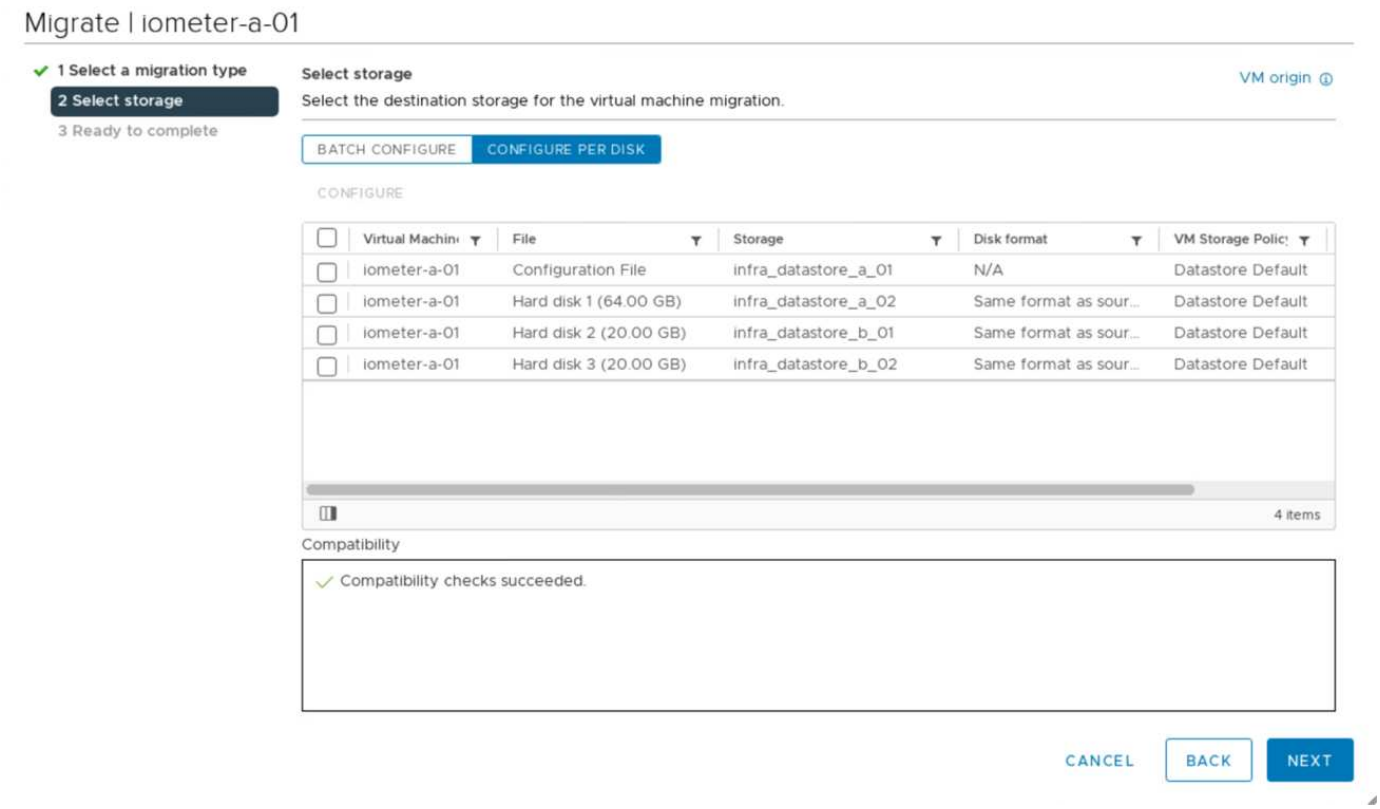
Per consentire alle macchine virtuali di utilizzare i servizi di storage da un sito SM-BC, gli archivi dati iSCSI di entrambi i siti devono essere montati da tutti gli host nel cluster per consentire la migrazione delle macchine virtuali tra i due siti e per gli scenari di disaster failover.

Per le applicazioni eseguite sull'infrastruttura virtuale che non richiedono la protezione del gruppo di coerenza SM-BC tra i siti, è possibile utilizzare anche il protocollo NFS e gli archivi dati NFS. In tal caso, è necessario prestare attenzione quando si allocano storage per le macchine virtuali in modo che le applicazioni business-critical utilizzino correttamente gli archivi dati SAN protetti dal gruppo di coerenza SM-BC per garantire la continuità del business.

La seguente schermata mostra che gli host sono configurati per montare datastore iSCSI da entrambi i siti.



È possibile eseguire la migrazione dei dischi delle macchine virtuali tra gli archivi dati iSCSI disponibili da entrambi i siti, come illustrato nella figura seguente. Per considerazioni sulle performance, è ottimale che le macchine virtuali utilizzino lo storage del cluster di storage locale per ridurre le latenze di i/o dei dischi. Ciò è particolarmente vero quando i due siti si trovano ad alcune distanze a causa della latenza fisica di andata e ritorno di circa 1 ms per 100 km di distanza.



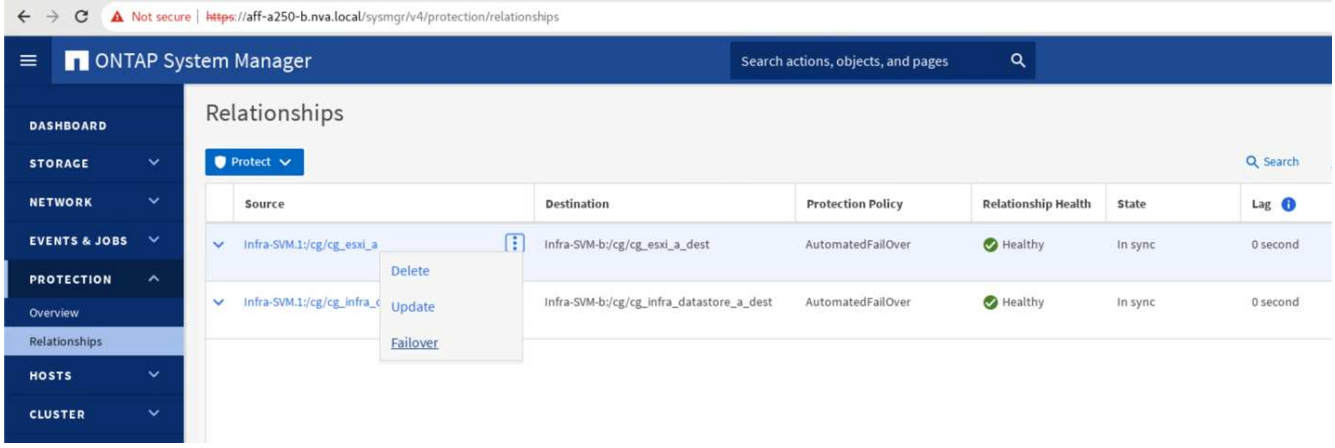
I test di vMotion delle macchine virtuali su un host diverso nello stesso sito e tra diversi siti sono stati eseguiti e sono stati eseguiti con successo. Dopo la migrazione manuale di una macchina virtuale tra i siti, la regola di affinità VM/host attiva e trasferisce nuovamente la macchina virtuale nel gruppo in cui appartiene in condizioni normali.

Failover dello storage pianificato

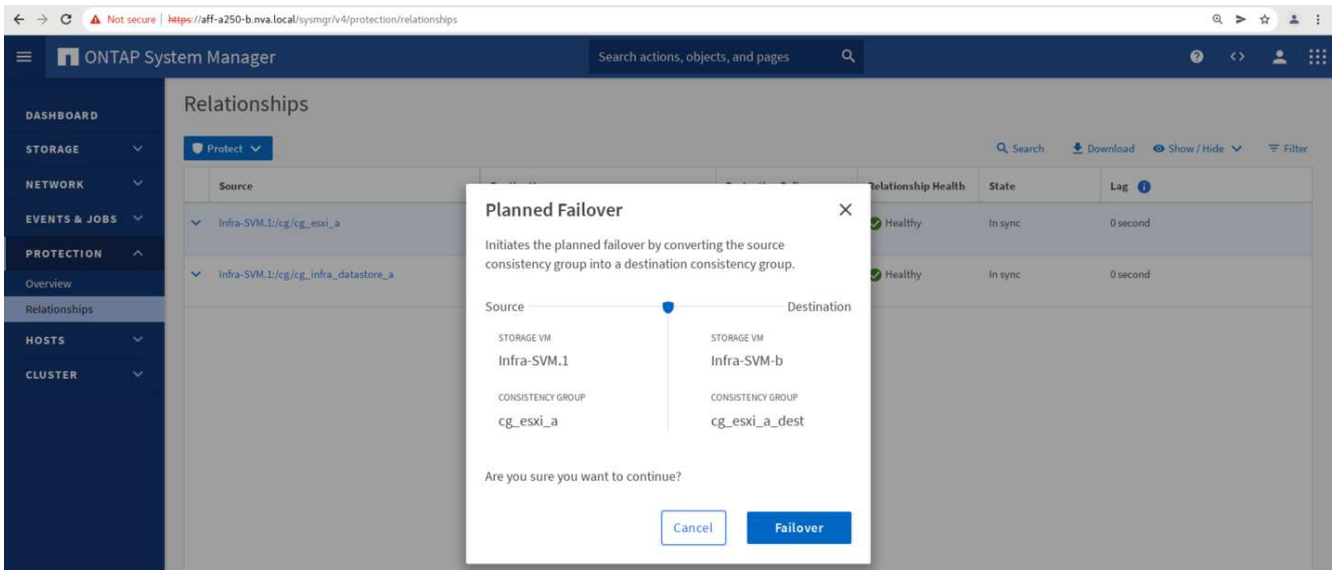
Le operazioni pianificate di failover dello storage devono essere eseguite sulla soluzione dopo la configurazione iniziale per determinare se la soluzione funziona correttamente dopo il failover dello storage. Il test può aiutare a identificare eventuali problemi di connettività o configurazione che potrebbero causare interruzioni i/O. Il test e la risoluzione regolari di qualsiasi problema di connettività o configurazione consentono di fornire servizi dati ininterrotti in caso di disastro reale del sito. Il failover dello storage pianificato può essere utilizzato anche prima di un'attività di manutenzione dello storage pianificata, in modo che i servizi dati possano essere serviti dal sito non interessato.

Per avviare un failover manuale dei servizi dati di storage del sito A verso il sito B, è possibile utilizzare il System Manager del sito B ONTAP per eseguire l'azione.

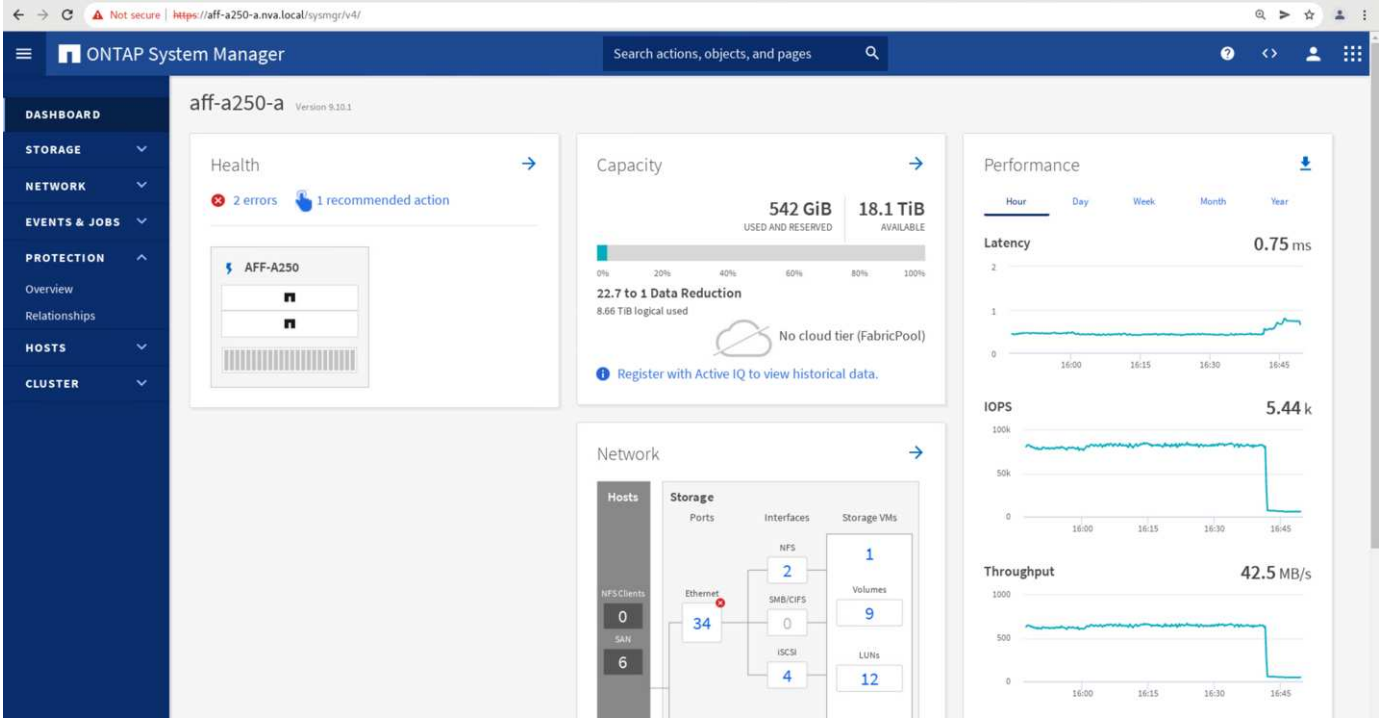
1. Accedere alla schermata protezione > Relazioni per verificare che lo stato della relazione del gruppo di coerenza sia `In Sync`. Se si trova ancora in `Synchronizing` state (stato), attendere che lo stato diventi `In Sync` prima di eseguire un failover.
2. Espandere i punti accanto al nome di origine e fare clic su failover.



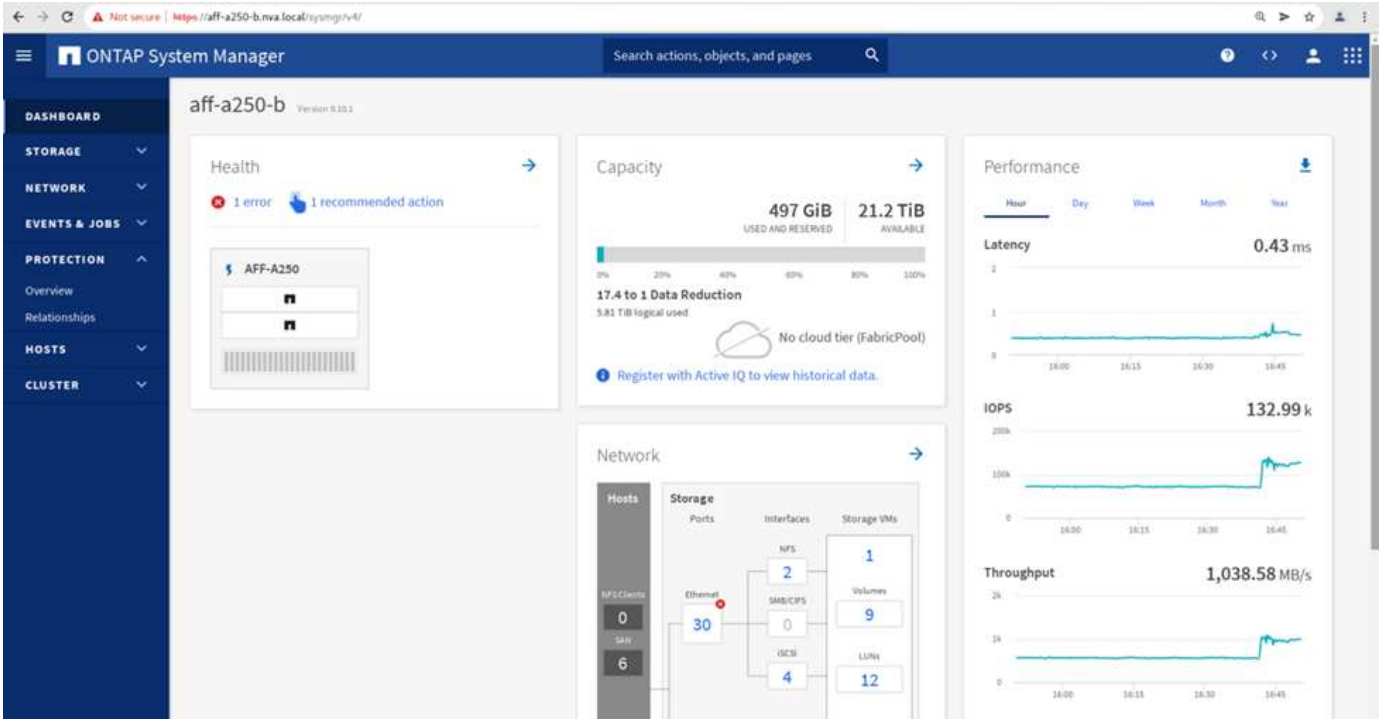
3. Confermare il failover per l'avvio dell'azione.



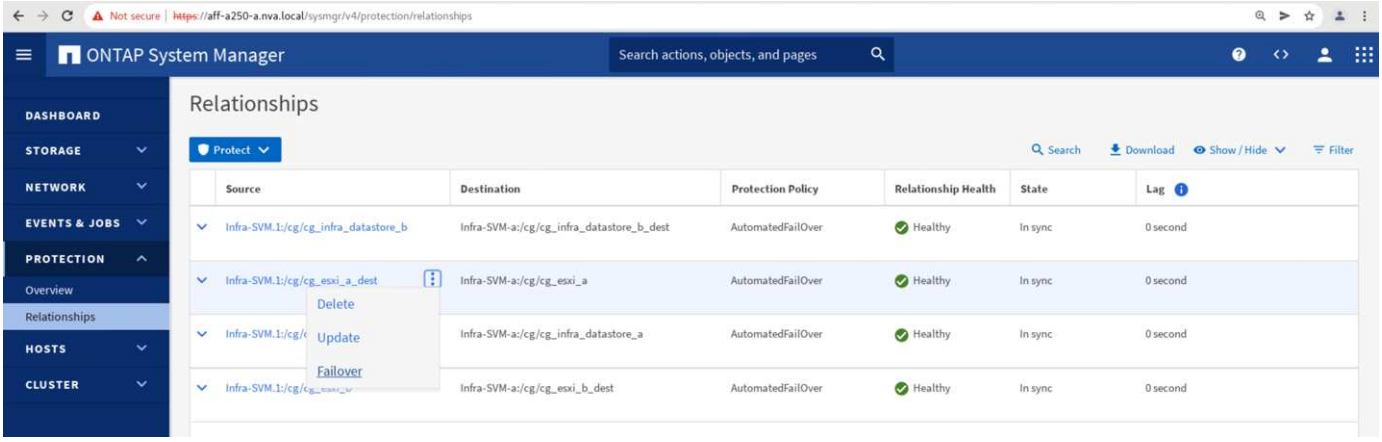
Subito dopo l'avvio del failover dei due gruppi di coerenza, `cg_esxi_a` e. `cg_infra_datastore_a`, Nella GUI di System Manager del sito B, l'i/o del sito A che serve questi due gruppi di coerenza si è spostato sul sito B. Di conseguenza, l'i/o presso il sito A si è ridotto in modo significativo, come mostrato nel riquadro delle performance di System Manager del sito.



D'altro canto, il pannello Performance del dashboard System Manager del sito B mostra un aumento significativo degli IOPS, dovuto alla fornitura di ulteriori i/o spostati dal sito A a circa 130.000 IOPS, E ha raggiunto un throughput di circa 1 GB/s mantenendo una latenza i/o inferiore a 1 millisecondo.

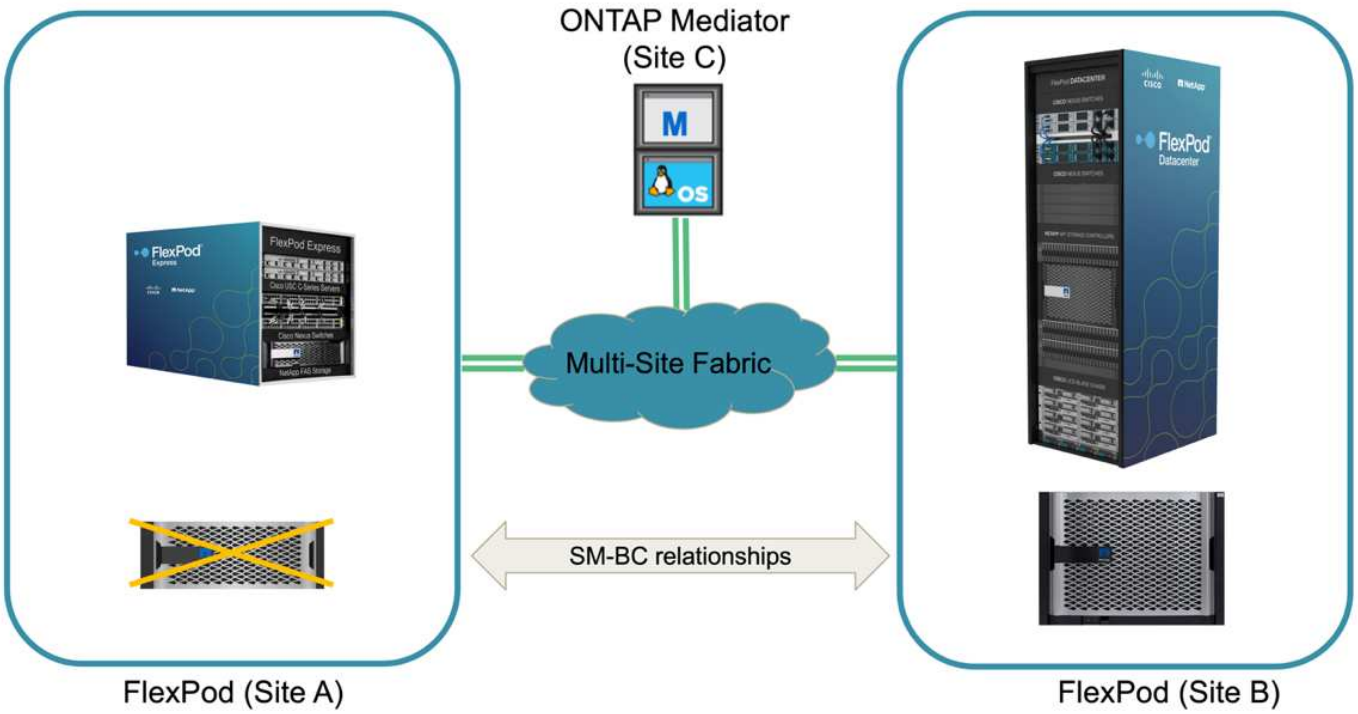


Con la migrazione trasparente dell'i/o dal sito A al sito B, i controller di storage del sito A possono ora essere messi fuori servizio per la manutenzione pianificata. Una volta completato il lavoro di manutenzione o il test e quando il sito Esegue il backup E il funzionamento Di Un cluster di storage, controllare e attendere che lo stato di protezione del gruppo di coerenza venga nuovamente impostato su `In sync` Prima di eseguire un failover per restituire l'i/o di failover dal sito B al sito A. Tenere presente che quanto più tempo un sito viene utilizzato per la manutenzione o il test, tanto più tempo occorre prima che i dati vengano sincronizzati e il gruppo di coerenza venga restituito a `In sync` stato.



Failover dello storage non pianificato

Un failover dello storage non pianificato può verificarsi quando si verifica un disastro reale o durante una simulazione di disastro. Ad esempio, vedere la figura seguente in cui il sistema di storage del sito A subisce un'interruzione dell'alimentazione, viene attivato un failover dello storage non pianificato e i servizi dati per le LUN del sito A, protette dalle relazioni SM-BC, continuano dal sito B.



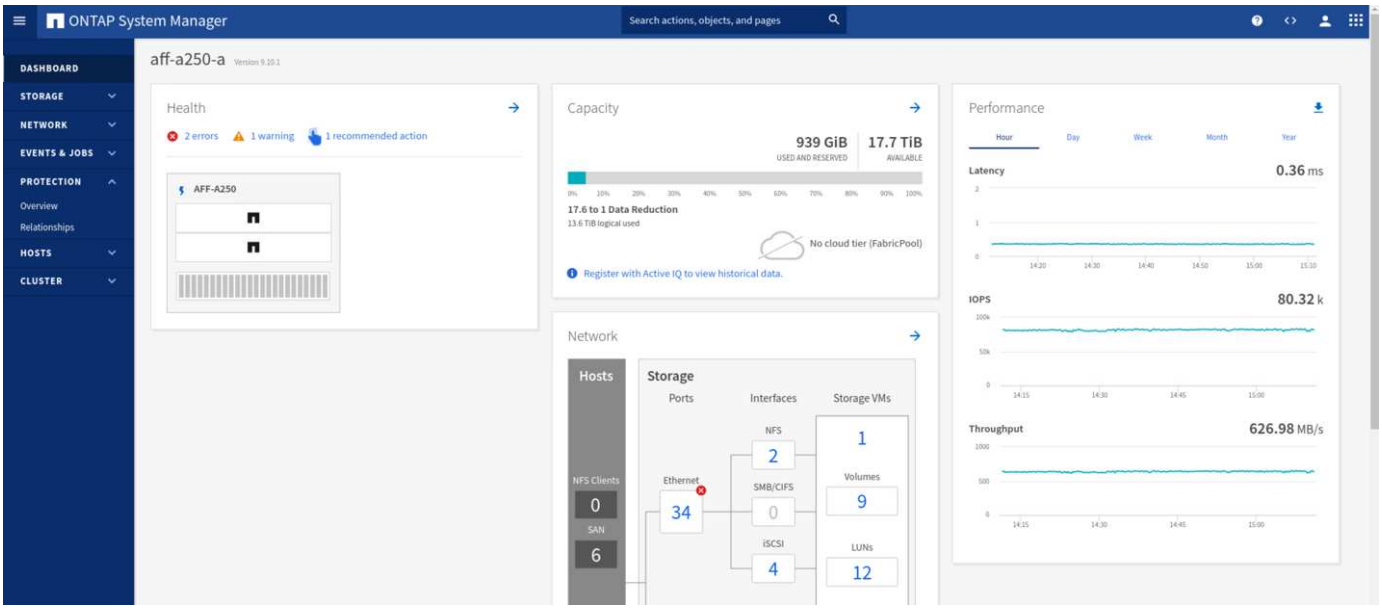
Per simulare un disastro dello storage nel sito A, è possibile spegnere entrambi i controller dello storage nel sito A spegnendo fisicamente l'interruttore di alimentazione per interrompere l'alimentazione dei controller. oppure utilizzando il comando di gestione dell'alimentazione del sistema dei processori del servizio del controller di storage per spegnere i controller.

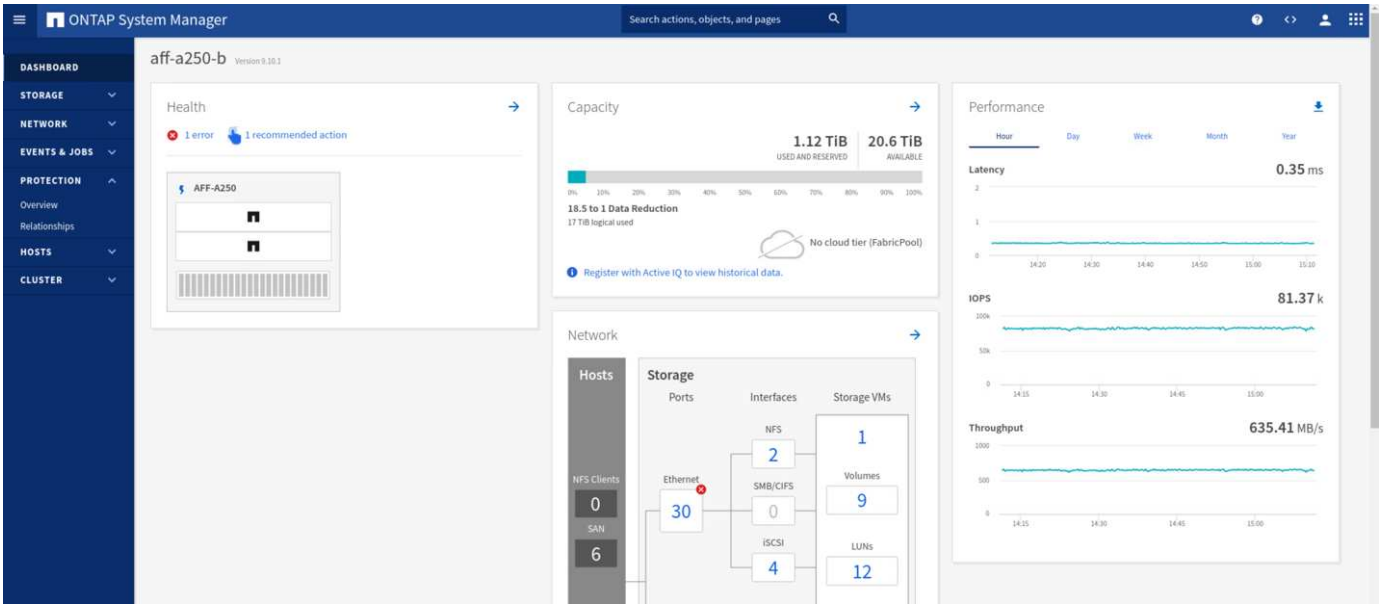
Quando il cluster di storage nel sito A viene interrotto, si verifica un arresto improvviso dei servizi dati forniti dal sito Di Un cluster di storage. Quindi, il mediatore ONTAP, che monitora la soluzione SM-BC da un terzo sito, rileva la condizione di guasto dello storage del sito A e consente alla soluzione SM-BC di eseguire un failover automatizzato non pianificato. Ciò consente ai controller di storage del sito B di continuare i servizi dati per le LUN configurate nelle relazioni del gruppo di coerenza SM-BC con il sito A.

Dal punto di vista dell'applicazione, i servizi dati si fermano brevemente mentre il sistema operativo controlla lo

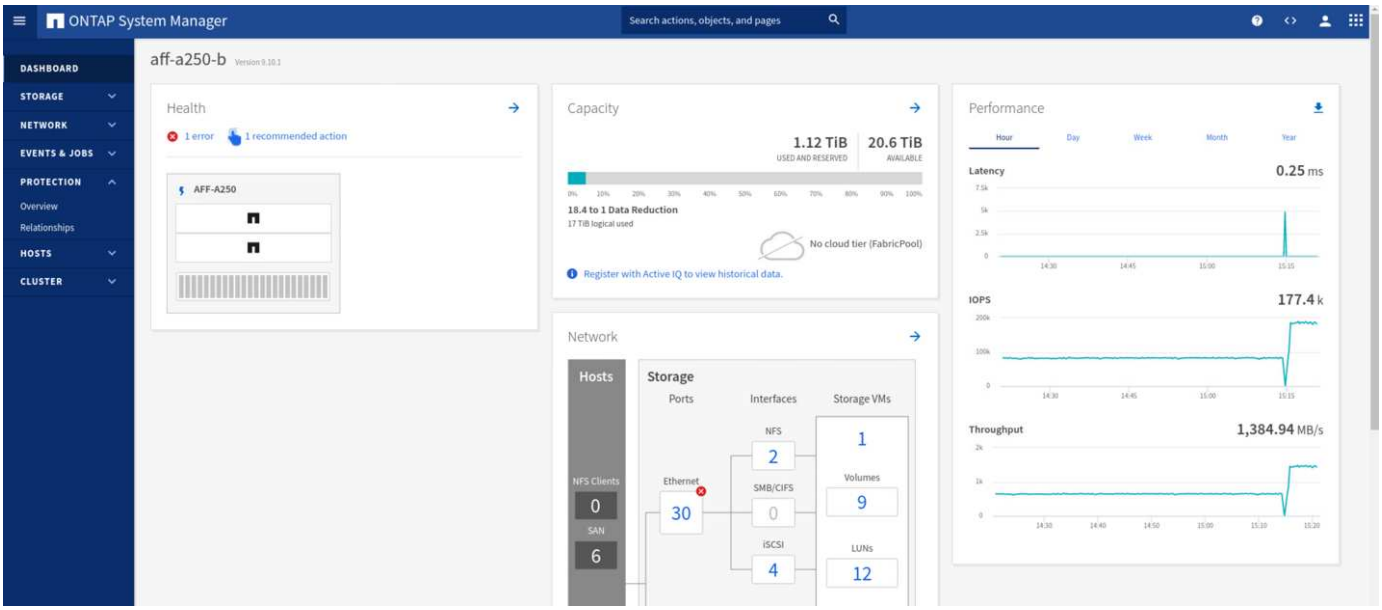
stato del percorso per i LUN e quindi riprende l'i/o sui percorsi disponibili per i controller di storage del sito B sopravvissuti.

Durante il test di convalida, lo strumento IOMeter sulle macchine virtuali di entrambi i siti genera i/o negli archivi dati locali. Una volta spento Il sito, Un cluster, i/o si è messo in pausa per un breve periodo e poi ripreso. Vedere le due figure seguenti per le dashboard del cluster di storage rispettivamente presso il sito A e il sito B prima del disastro, che mostrano circa 80.000 IOPS e un throughput di 600 MB/s in ogni sito.

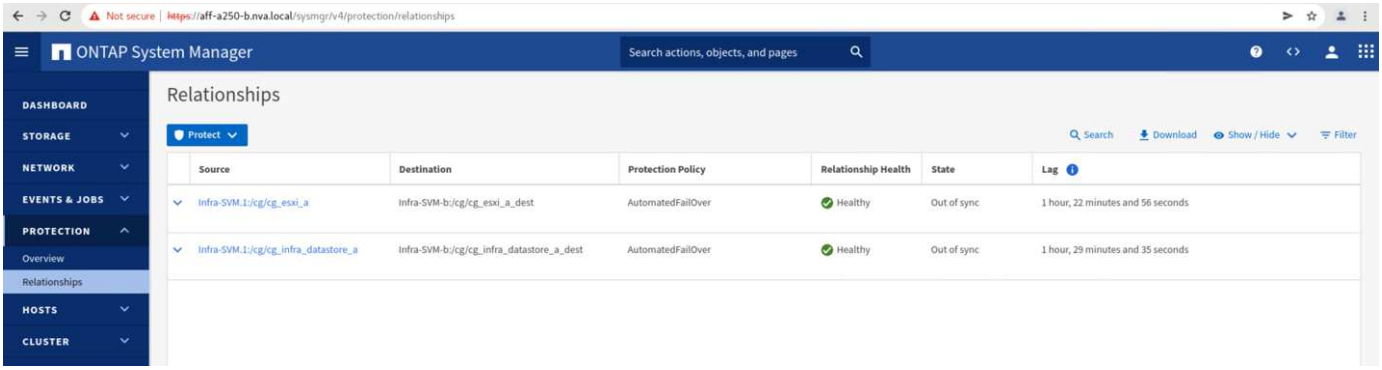




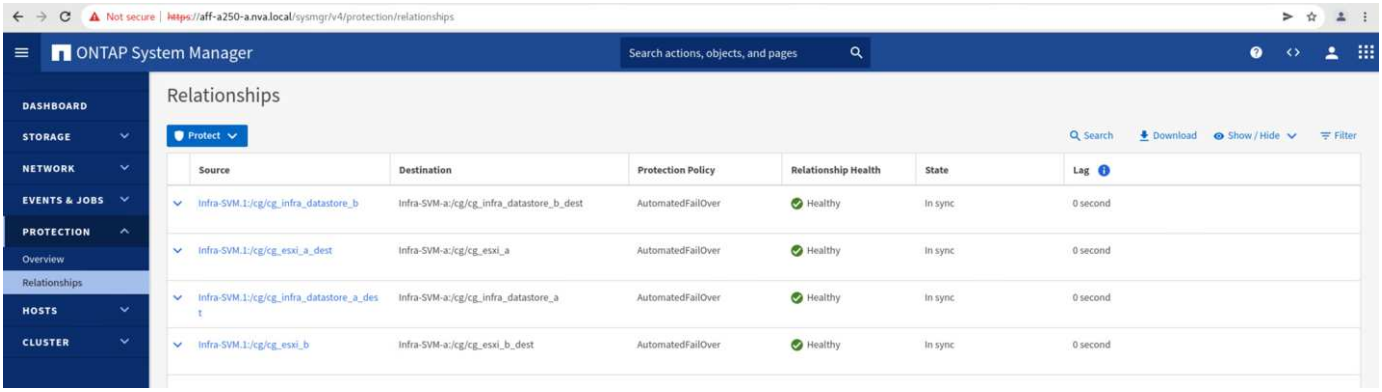
Dopo aver spento i controller di storage nel sito A, possiamo validare visivamente che l'i/o del controller di storage del sito B è aumentato drasticamente per fornire servizi dati aggiuntivi per conto del sito A (vedere la figura seguente). Inoltre, la GUI delle VM IOMeter ha dimostrato che l'i/o è continuato nonostante l'interruzione del cluster di storage del sito A. Se sono presenti archivi dati aggiuntivi supportati da LUN non protetti da relazioni SM-BC, tali archivi dati non saranno più accessibili in caso di disastro dello storage. Pertanto, è importante valutare le esigenze aziendali dei vari dati applicativi e inserirli correttamente in datastore protetti dalle relazioni SM-BC per garantire la continuità del business.



Mentre il sito Di Un cluster è inattivo, le relazioni dei gruppi coerenti mostrano `Out of sync` come mostrato nella figura seguente. Una volta riacceso l'alimentazione per i controller di storage nel sito A, il cluster di storage si avvia e la sincronizzazione dei dati tra il sito A e il sito B.



Prima di restituire i servizi dati dal sito B al sito A, è necessario controllare System Manager del sito A e assicurarsi che le relazioni SM-BC vengano ripristinati e che lo stato sia nuovamente sincronizzato. Dopo aver confermato che i gruppi di coerenza sono sincronizzati, è possibile avviare un'operazione di failover manuale per restituire i servizi dati nelle relazioni del gruppo di coerenza al sito A.



Manutenzione completa del sito o guasto del sito

Un sito potrebbe richiedere la manutenzione del sito, subire un'interruzione dell'alimentazione o essere colpito

da un disastro naturale, ad esempio un uragano o un terremoto. Pertanto, è fondamentale che tu eserciti scenari di guasto del sito pianificati e non pianificati per garantire che la tua soluzione FlexPod SM-BC sia configurata correttamente per sopravvivere a tali guasti per tutte le applicazioni business-critical e i servizi dati. Sono stati validati i seguenti scenari correlati al sito.

- Scenario di manutenzione pianificata del sito mediante la migrazione di macchine virtuali e servizi dati critici nell'altro sito
- Scenario di disservizio del sito non pianificato spegnendo server e controller storage per la simulazione di disastro

Per preparare un sito per la manutenzione pianificata del sito, è necessaria una combinazione di migrazione delle macchine virtuali interessate fuori sede con vMotion e un failover manuale delle relazioni del gruppo di coerenza SM-BC per migrare le macchine virtuali e i servizi dati critici nel sito alternativo. Il test è stato eseguito in due ordini diversi: VMotion prima seguito da SM-BC failover e SM-BC failover prima seguito da vMotion, per confermare che le macchine virtuali continuano a funzionare e i servizi dati non vengono interrotti.

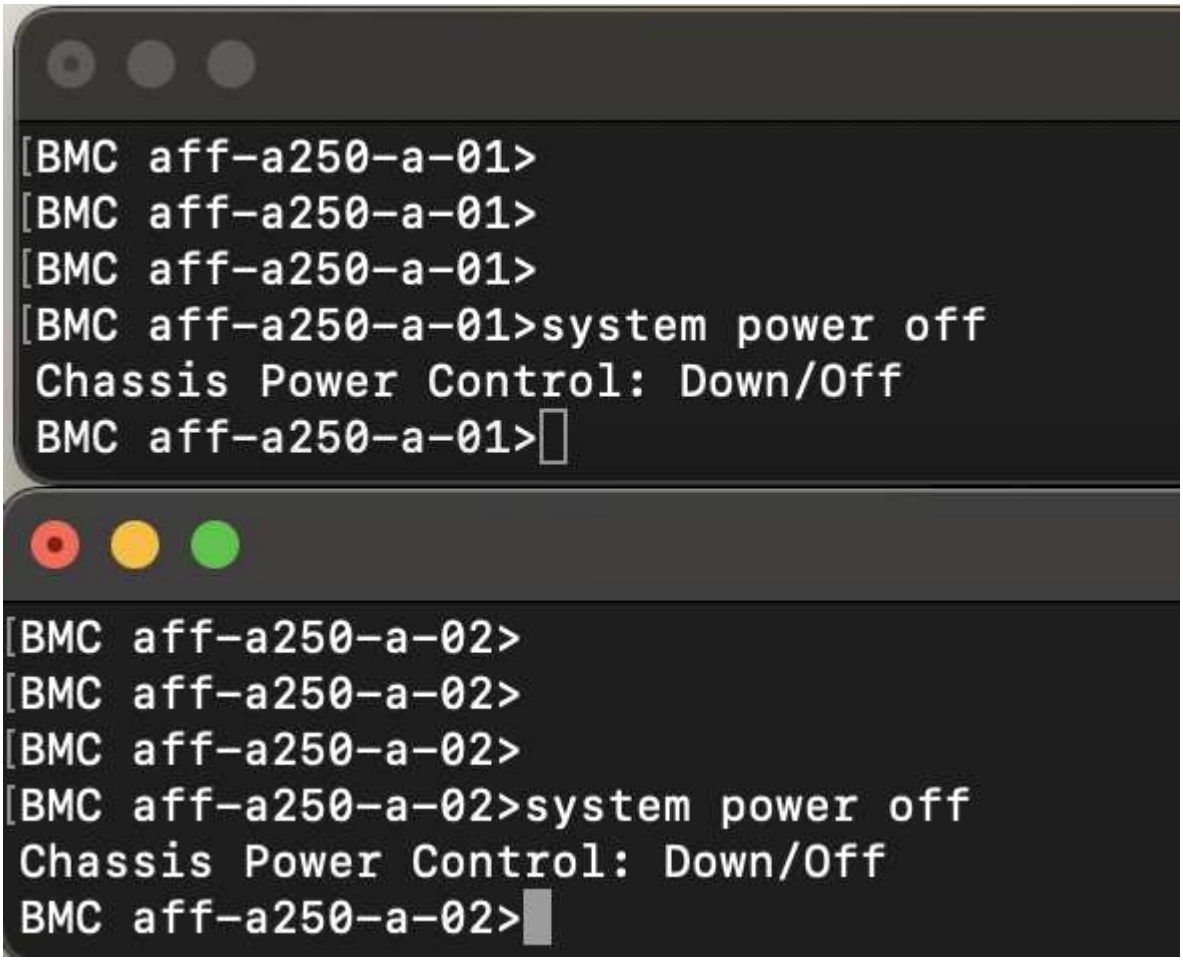
Prima di eseguire la migrazione pianificata, aggiornare la regola di affinità VM/host in modo che le macchine virtuali attualmente in esecuzione sul sito vengano migrate automaticamente fuori dal sito sottoposto a manutenzione. La seguente schermata mostra un esempio di modifica della regola di affinità VM/host del sito A per la migrazione automatica delle macchine virtuali dal sito A al sito B. Invece di specificare che le macchine virtuali devono essere eseguite sul sito B, è possibile anche scegliere di disattivare temporaneamente la regola di affinità in modo che le macchine virtuali possano essere migrate manualmente.

Una volta migrate le macchine virtuali e i servizi storage, è possibile spegnere server, controller storage, shelf di dischi e switch ed eseguire le attività di manutenzione del sito necessarie. Una volta completata la manutenzione del sito e riattivata l'istanza di FlexPod, è possibile modificare l'affinità del gruppo di host per il

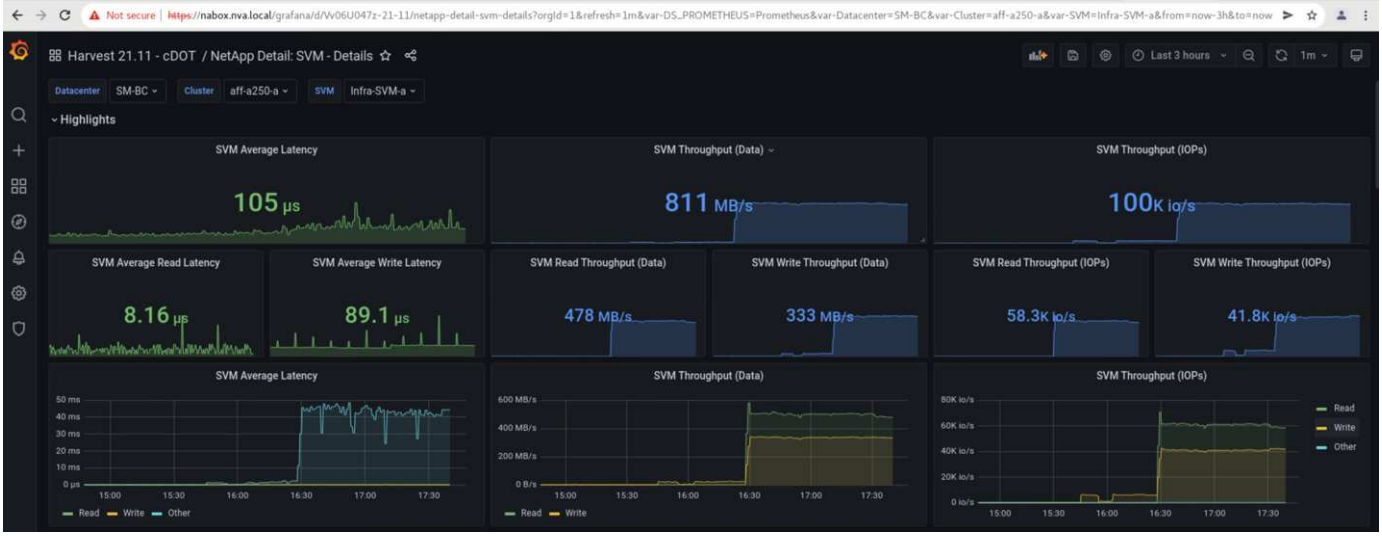
ritorno delle macchine virtuali al sito originale. In seguito, modificare nuovamente la regola di affinità del sito VM/host "must run on hosts in group" (deve essere eseguita su host in gruppo) in modo che le macchine virtuali possano essere eseguite sugli host dell'altro sito in caso di disastro. Per il test di convalida, tutte le macchine virtuali sono state migrate correttamente nell'altro sito e i servizi dati sono continuati senza problemi dopo l'esecuzione di un failover per le relazioni SM-BC.

Per la simulazione di disastro del sito non pianificata, i server e i controller dello storage sono stati spenti per simulare un disastro del sito. La funzionalità VMware ha rileva le macchine virtuali in downtime e le riavvia sul sito esistente. Inoltre, il mediatore ONTAP in esecuzione in un terzo sito rileva il guasto del sito e il sito sopravvissuto avvia un failover e inizia a fornire servizi dati per il sito inattivo come previsto.

La seguente schermata mostra che la CLI del processore di servizio dei controller di storge è stata utilizzata per spegnere il sito Di Un cluster in modo brusco per simulare un disastro dello storage nel sito.



Le dashboard delle macchine virtuali dello storage dei cluster acquisite dallo strumento di raccolta dati NetApp Harvest e visualizzate nella dashboard Grafana nello strumento di monitoraggio NAbox sono illustrate nelle due schermate seguenti. Come si può vedere sul lato destro dei grafici IOPS e throughput, il cluster del sito B rileva il carico di lavoro dello storage del cluster A subito dopo il downdown del cluster del sito A.

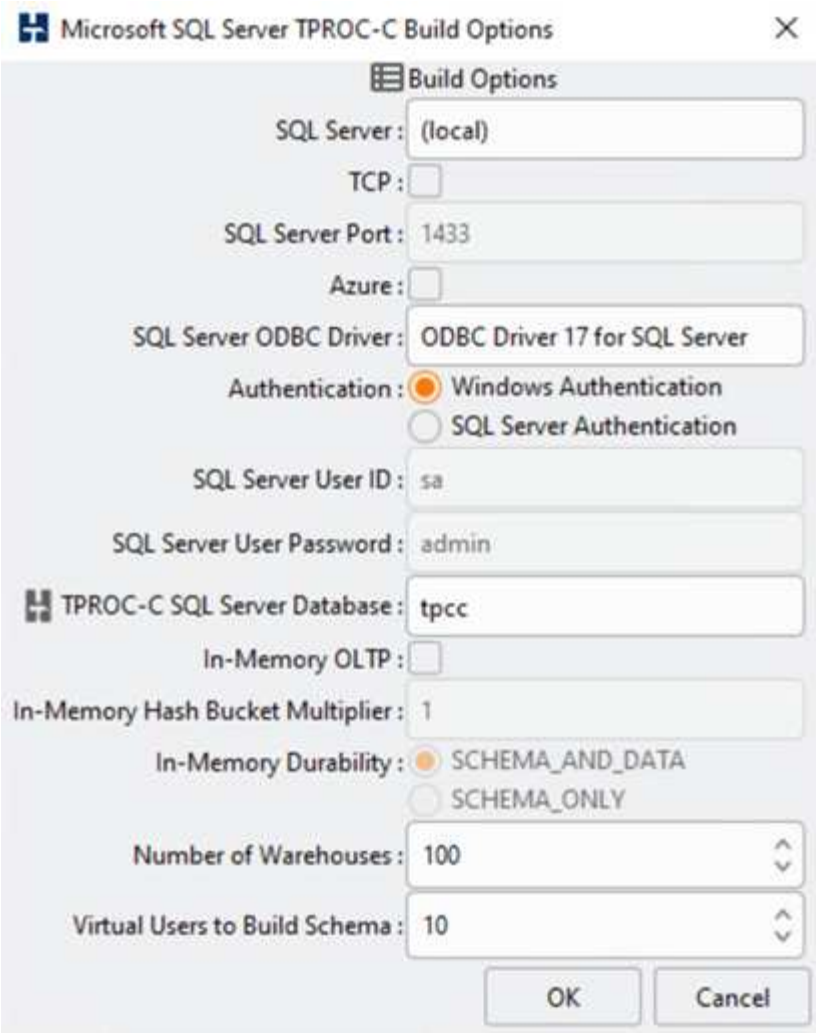


Microsoft SQL Server

Microsoft SQL Server è una piattaforma di database ampiamente adottata e implementata per L'IT aziendale. Microsoft SQL Server 2019 offre numerose nuove funzionalità e miglioramenti ai motori di analisi e relazionali. Supporta i carichi di lavoro con applicazioni in esecuzione on-premise, nel cloud e in modalità ibrida utilizzando una combinazione di questi due. Inoltre, può essere implementato su più piattaforme, tra cui Windows, Linux e container.

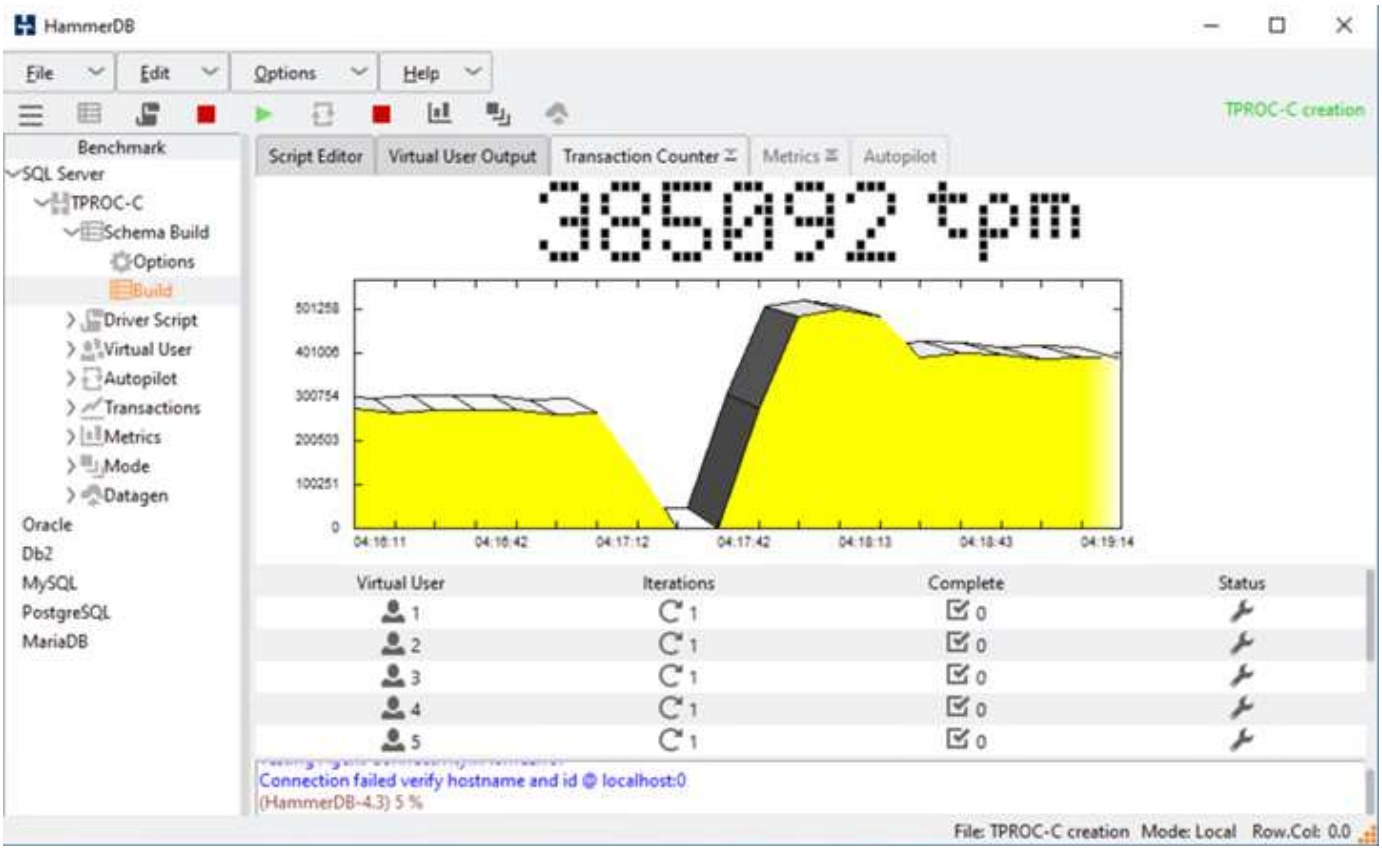
Come parte della convalida dei carichi di lavoro business-critical per la soluzione FlexPod SM-BC, Microsoft SQL Server 2019 installato su una macchina virtuale Windows Server 2022 è incluso insieme alle macchine virtuali IOMeter per il test di failover dello storage pianificato e non pianificato SM-BC. Sulla macchina virtuale Windows Server 2022, SQL Server Management Studio viene installato per gestire SQL Server. Per i test, il tool di database HammerDB viene utilizzato per generare transazioni di database.

Il tool di test del database HammerDB è stato configurato per il test con il carico di lavoro Microsoft SQL Server TPROC-C. Per le configurazioni di creazione dello schema, le opzioni sono state aggiornate per utilizzare 100 warehouse con 10 utenti virtuali, come mostrato nella seguente schermata.



Dopo l'aggiornamento delle opzioni di creazione dello schema, è stato avviato il processo di creazione dello schema. Pochi minuti dopo, è stato introdotto un errore simulato del cluster di storage del sito B non pianificato spegnendo entrambi i nodi del cluster di storage AFF A250 a due nodi circa contemporaneamente utilizzando i comandi CLI del processore di sistema.

Dopo una breve pausa delle transazioni del database, è stato attivato il failover automatico per la risoluzione dei problemi e le transazioni sono state riavviate. La seguente schermata mostra la schermata di HammerDB Transaction Counter. Poiché il database per Microsoft SQL Server risiede normalmente nel cluster di storage del sito B, la transazione si è interrotta brevemente quando lo storage del sito B è andato in pausa e poi ripresa dopo il failover automatico.



Le metriche del cluster di storge sono state acquisite utilizzando il tool NAbox con il tool di monitoraggio NetApp Harvest installato. I risultati vengono visualizzati nei dashboard Grafana predefiniti per la macchina virtuale di storage e altri oggetti di storage. La dashboard fornisce metrici per latenza, throughput, IOPS e dettagli aggiuntivi con statistiche di lettura e scrittura separate per il sito B e il sito A.

Questa schermata mostra la dashboard delle performance NAbox Grafana per il cluster di storage del sito B.

Gli IOPS per il cluster di storage del sito B erano circa 100.000 IOPS prima dell'introduzione del disastro. Quindi, le metriche delle performance hanno mostrato un netto calo fino a zero sul lato destro dei grafici a causa del disastro. Poiché il cluster di storage del sito B non era attivo, non era possibile raccogliere nulla dal cluster del sito B dopo l'introduzione del disastro.

D'altra parte, gli IOPS per il cluster di storage del sito A hanno raccolto i carichi di lavoro aggiuntivi dal sito B dopo il failover automatizzato. Il carico di lavoro aggiuntivo può essere facilmente visualizzato sul lato destro dei grafici IOPS e throughput nella seguente schermata, che mostra la dashboard delle performance NAbox Grafana per il cluster di storage del sito A.

Lo scenario di disaster test dello storage sopra riportato ha confermato che il carico di lavoro di Microsoft SQL Server può sopravvivere a un'interruzione completa del cluster di storage nel sito B in cui risiede il database. L'applicazione utilizzava in modo trasparente i servizi dati forniti dal sito Di Un cluster di storage dopo il rilevamento del disastro e il failover.

A livello di elaborazione, quando le macchine virtuali in esecuzione in un determinato sito subiscono un guasto all'host, le macchine virtuali sono progettate per essere riavviate automaticamente dalla funzionalità VMware ha. Per un'interruzione completa del calcolo del sito, le regole di affinità VM/host consentono il riavvio delle macchine virtuali nel sito sopravvissuto. Tuttavia, affinché un'applicazione business-critical fornisca servizi ininterrotti, è necessario un clustering basato su applicazioni come Microsoft failover Cluster o Kubernetes container-based application architecture per evitare il downtime dell'applicazione. Consultare il documento pertinente per l'implementazione del clustering basato sulle applicazioni, che esula dall'ambito di questo report tecnico.

"Prossimo: Conclusione."

Conclusione

"Precedente: Convalida della soluzione - scenari validati."

Il data center FlexPod con SM-BC utilizza un data center Active-Active per garantire la business continuity e il disaster recovery per i carichi di lavoro business-critical. La soluzione in genere collega due data center implementati in ubicazioni separate e geograficamente distribuite in un'area metropolitana. La soluzione NetApp SM-BC utilizza la replica sincrona per proteggere i servizi dati business-critical da guasti del sito. La soluzione richiede che i due siti di implementazione FlexPod abbiano una latenza di rete di andata e ritorno inferiore a 10 millisecondi.

Il mediatore NetApp ONTAP implementato in un terzo sito monitora la soluzione SM-BC e consente il failover automatizzato quando viene rilevato un disastro del sito. VMware vCenter con VMware ha e la configurazione estesa di VMware vSphere Metro Storage Cluster funzionano perfettamente con NetApp SM-BC per

consentire alla soluzione di soddisfare gli obiettivi RPO zero e RTO quasi zero desiderati.

La soluzione FlexPod SM-BC può essere implementata anche sulle infrastrutture FlexPod esistenti se soddisfano i requisiti o aggiungendo una soluzione FlexPod aggiuntiva a un FlexPod esistente per raggiungere gli obiettivi di business continuity. NetApp e Cisco offrono ulteriori strumenti di gestione, monitoraggio e automazione, come Cisco Intersight, Ansible e HashiCorp Terraform, in modo da poter monitorare facilmente la soluzione, ottenere informazioni sulle operazioni e automatizzare l'implementazione e le operazioni.

Dal punto di vista di un'applicazione business-critical come Microsoft SQL Server, un database che risiede in un datastore VMware protetto da una relazione ONTAP SM-BC CG continua a essere disponibile nonostante un'interruzione dello storage del sito. Come verificato durante il test di convalida, dopo un'interruzione dell'alimentazione del cluster di storage in cui risiede il database, si verifica un failover della relazione SM-BC CG e le transazioni Microsoft SQL Server vengono rieseguite senza interruzioni dell'applicazione.

Grazie alla protezione granulare dei dati delle applicazioni, è possibile creare relazioni ONTAP SM-BC CG per le applicazioni business-critical in modo da soddisfare i requisiti di RPO zero e RTO quasi zero. Affinché il cluster VMware su cui è in esecuzione l'applicazione Microsoft SQL Server possa sopravvivere a un'interruzione dello storage del sito, le LUN di avvio degli host ESXi di ogni sito sono protette anche da una relazione SM-BC CG.

La flessibilità e la scalabilità di FlexPod ti consentono di iniziare con un'infrastruttura delle giuste dimensioni, in grado di crescere e di evolversi in base ai tuoi requisiti di business. Questo design validato consente di implementare in modo affidabile il cloud privato basato su VMware vSphere su un'infrastruttura distribuita e integrata, offrendo una soluzione resiliente a molti scenari di singolo punto di errore e un guasto del sito per proteggere i servizi dati aziendali critici.

"Pagina successiva: Dove trovare informazioni aggiuntive e cronologia delle versioni."

Dove trovare informazioni aggiuntive e cronologia delle versioni

"Precedente: Conclusione."

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

FlexPod

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Server Cisco - Unified Computing System (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- Documentazione sui prodotti NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- FlexPod Datacenter con Cisco UCS 4.2(1) in modalità gestita UCS, VMware vSphere 7.0 U2 e guida alla

progettazione di NetApp ONTAP 9.9

"https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- FlexPod Datacenter con Cisco UCS 4.2(1) in modalità gestita UCS, VMware vSphere 7.0 U2 e guida all'implementazione di NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- Guida alla progettazione di FlexPod Datacenter con Cisco UCS X-Series, VMware 7.0 U2 e NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- Guida all'implementazione di FlexPod Datacenter con Cisco UCS X-Series, VMware 7.0 U2 e NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e Guida alla progettazione di NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- Guida all'implementazione di FlexPod Express per VMware vSphere 7.0 con Cisco UCS Mini e NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP con fabric front-end VXLAN multi-sito

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox

  "https://nabox.org"

- NetApp Harvest

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4878: Continuità aziendale SnapMirror (SM-BC) ONTAP 9.8

  https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Come eliminare correttamente una relazione SnapMirror ONTAP 9

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Nozioni di base sul disaster recovery sincrono di SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Nozioni di base sul disaster recovery asincrono di SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Protezione dei dati e disaster recovery

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Installare o aggiornare il servizio di supporto ONTAP

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere ha e vSphere Metro Storage Cluster

- Creazione e utilizzo di cluster vSphere ha

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage Cluster (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Procedure consigliate per VMware vSphere Metro Storage Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP con NetApp SnapMirror Business Continuity (SM-BC) con VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Proteggi le applicazioni e i database di Tier 1 con il cluster di storage metro VMware vSphere e ONTAP

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL e HammerDB

- Microsoft SQL Server 2019

  "https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Guida alle Best practice per l'architettura di Microsoft SQL Server su VMware vSphere

"https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- Sito web di HammerDB

  "https://www.hammerdb.com"

Matrice di compatibilità

- Matrice di compatibilità hardware Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Tool di matrice di interoperabilità NetApp

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- Guida alla compatibilità VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Aprile 2022	Release iniziale.

Data center FlexPod con VMware vSphere 7.0, fabric Cisco VXLAN a sito singolo e NetApp ONTAP 9.7 - progettazione

Ramesh Isaac, Cisco Abhinav Singh, NetApp

Cisco Validated Designs (CVD) è costituito da sistemi e soluzioni progettati, testati e documentati per facilitare e migliorare le implementazioni dei clienti. Questi design incorporano un'ampia gamma di tecnologie e prodotti in un portfolio di soluzioni sviluppate per soddisfare le esigenze di business dei clienti. Cisco e NetApp hanno collaborato per offrire FlexPod, che funge da base per una varietà di carichi di lavoro, e offrire design architetturali robusti, efficienti e scalabili per soddisfare i requisiti dei clienti. Una soluzione FlexPod è un approccio validato per l'implementazione di tecnologie e prodotti Cisco e NetApp per la creazione di un'infrastruttura di cloud pubblico e privato condivisa.

"Data center FlexPod con VMware vSphere 7.0, fabric Cisco VXLAN a sito singolo e NetApp ONTAP 9.7 - progettazione"

Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7 - implementazione

John George, Cisco Sree Lakshmi Lanka, NetApp

Questo documento descrive il data center FlexPod di Cisco e NetApp con NetApp ONTAP 9.7 su sistema storage all-flash NetApp AFF A400, la release software unificata 4.1(2) con processori scalabili Intel Xeon di seconda generazione e VMware vSphere 7.0. Cisco UCS Manager (UCSM) 4.1(2) offre il supporto consolidato di:

- Tutti gli attuali modelli Cisco UCS Fabric Interconnect: 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- Serie 2200/2300/2400 IOM
- Cisco UCS B-Series
- Cisco UCS C-Series

Sono incluse anche le piattaforme di gestione Cisco Intersight e NetApp Active IQ SaaS.

FlexPod Datacenter con NetApp ONTAP 9.7, Cisco UCS Unified Software release 4.1(2) e VMware vSphere 7.0 comprendono un'architettura data center pre-progettata e Best-practice basata sul sistema di calcolo unificato Cisco (Cisco UCS), sulla famiglia di switch Cisco Nexus 9000, switch fabric multistrato MDS 9000, E gli storage array NetApp AFF serie A con software per la gestione dei dati ONTAP 9.7.

"Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7 - implementazione"

Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - progettazione

John George, Cisco Scott Kovacs, NetApp

Questo documento descrive la soluzione Cisco e NetApp FlexPod, un approccio validato per l'implementazione delle tecnologie Cisco e NetApp come infrastruttura cloud condivisa. Questo design validato offre un framework per l'implementazione di VMware vSphere, la piattaforma di virtualizzazione più diffusa nei data center di livello Enterprise, su FlexPod.

"Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - progettazione"

Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - implementazione

John George, Cisco Scott Kovacs, NetApp

L'attuale tendenza del settore nella progettazione dei data center è verso le infrastrutture condivise. Utilizzando la virtualizzazione insieme alle piattaforme IT pre-validate, i clienti aziendali hanno intrapreso il percorso verso il cloud allontanandosi dai silos di applicazioni e verso un'infrastruttura condivisa che può essere implementata

rapidamente, aumentando in tal modo l'agilità e riducendo i costi. Cisco e NetApp hanno collaborato per offrire FlexPod, che utilizza i componenti di storage, server e rete migliori per fungere da base per una varietà di carichi di lavoro, consentendo progettazioni architetturali efficienti che possono essere implementate in modo rapido e sicuro.

"Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - implementazione"

Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - progettazione

John George, Cisco Scott Kovacs, NetApp

Questo documento descrive una soluzione validata per l'implementazione delle tecnologie Cisco e NetApp come infrastruttura cloud condivisa. Questo design validato offre un framework per l'implementazione di VMware vSphere, la piattaforma di virtualizzazione più diffusa nei data center di livello Enterprise, su FlexPod.

FlexPod è un'infrastruttura integrata leader del settore che supporta un'ampia gamma di carichi di lavoro e casi di utilizzo aziendali. Questa soluzione consente ai clienti di implementare in modo rapido e affidabile un cloud privato basato su VMware vSphere su un'infrastruttura integrata.

"Data center FlexPod con Cisco Intersight e NetApp ONTAP 9.7 - progettazione"

Data center FlexPod con VMware vSphere 6.7 U2, fabric Cisco UCS di fouth generation e NetApp ONTAP 9.6

John George, Cisco Sree Lakshmi Lanka, NetApp

Questo documento descrive il data center FlexPod di Cisco e NetApp con NetApp ONTAP 9.6, la versione software unificata 4.0(4) con processori scalabili Intel Xeon di seconda generazione e VMware vSphere 6.7 U2. Cisco UCS Manager (UCSM) 4.0(4) offre il supporto consolidato di:

- Tutti gli attuali modelli Cisco UCS Fabric Interconnect: 6200, 6300, 6324 (Cisco UCS Mini)
- 6454
- Serie 2200/2300/2400 IOM
- Cisco UCS B-Series
- Cisco UCS C-Series.

FlexPod Datacenter con NetApp ONTAP 9.6, Cisco UCS Unified Software release 4.0(4) e VMware vSphere 6.7 U2 è un'architettura di data center pre-progettata e Best-practice basata sul sistema di calcolo unificato Cisco (Cisco UCS), sulla famiglia di switch Cisco Nexus 9000, switch fabric multistrato MDS 9000, E gli storage array NetApp AFF Serie A con ONTAP 9.

"Data center FlexPod con VMware vSphere 6.7 U2, fabric Cisco UCS di quarta generazione e NetApp ONTAP 9.6"

Data center FlexPod con VMware vSphere 6.7 U1, fabric Cisco UCS di quarta generazione e progettazione NetApp AFF a-Series

John George, Cisco Sree Lakshmi Lanka, NetApp

Questo documento descrive la soluzione Cisco e NetApp FlexPod, un approccio validato per l'implementazione delle tecnologie Cisco e NetApp come infrastruttura cloud condivisa. Questo design validato offre un framework per l'implementazione di VMware vSphere, la piattaforma di virtualizzazione più diffusa nei data center di livello Enterprise, su FlexPod.

FlexPod è un'infrastruttura integrata leader del settore che supporta un'ampia gamma di carichi di lavoro e casi di utilizzo aziendali. Questa soluzione consente ai clienti di implementare in modo rapido e affidabile il cloud privato basato su VMware vSphere su un'infrastruttura integrata.

L'architettura della soluzione consigliata è basata su Cisco Unified Computing System (Cisco UCS) utilizzando la versione software unificata per supportare le piattaforme hardware Cisco UCS, inclusi i server blade Cisco UCS B-Series e rack C-Series, Cisco UCS 6454 Fabric Interconnect, switch Cisco Nexus 9000 Series, switch Cisco MDS Fibre Channel, E gli storage array della serie All Flash di NetApp. Inoltre, include VMware vSphere 6.7 Update 1, che offre una serie di nuove funzionalità per ottimizzare l'utilizzo dello storage e facilitare un cloud privato.

"Data center FlexPod con VMware vSphere 6.7 U1, fabric Cisco UCS di quarta generazione e progettazione NetApp AFF a-Series"

Data center FlexPod con VMware vSphere 6.7 U1, fabric Cisco UCS di quarta generazione e NetApp AFF A-Series

John George, Cisco Scott Kovacs, NetApp

Questo documento descrive il data center FlexPod di Cisco e NetApp con la versione software unificata 4.0(2) e VMware vSphere 6.7 U1. Cisco UCS Manager (UCSM) 4.0(2) fornisce il supporto consolidato di tutti gli attuali modelli Cisco UCS Fabric Interconnect (6200, 6300, 6324 (Cisco UCS Mini)), 6454,2200/2300 Series IOM, Cisco UCS B-Series e Cisco UCS C-Series. FlexPod Datacenter con Cisco UCS Unified Software release 4.0(2) e VMware vSphere 6.7 U1 è un'architettura di data center pre-progettata e basata su Best-practice, basata sul sistema di calcolo unificato Cisco (UCS), sulla famiglia di switch Cisco Nexus 9000, switch fabric multistrato MDS 9000, E gli storage array NetApp AFF Serie A con sistema operativo ONTAP 9.

"Data center FlexPod con VMware vSphere 6.7 U1, fabric Cisco UCS di quarta generazione e NetApp AFF A-Series"

FlexPod Datacenter con Cisco ACI Multi-Pod, NetApp MetroCluster IP e VMware vSphere 6.7 - progettazione

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Questo documento descrive l'integrazione del multi-pod Cisco ACI e della soluzione NetApp MetroCluster IP nel data center FlexPod per fornire una soluzione multi-data center altamente disponibile. L'architettura multi-data center offre la possibilità di bilanciare i carichi di lavoro tra due data center utilizzando la mobilità dei carichi di lavoro senza interruzioni, consentendo così la migrazione dei servizi tra siti senza la necessità di sostenere un'interruzione del servizio.

La soluzione FlexPod con multi-pod ACI e NetApp MetroCluster IP offre i seguenti vantaggi:

- Mobilità perfetta dei carichi di lavoro nei data center
- Policy coerenti in tutti i siti
- Estensione Layer-2 in data center geograficamente distribuiti
- Migliore prevenzione dei downtime durante la manutenzione
- Prevenzione e ripristino di disastri

"FlexPod Datacenter con Cisco ACI Multi-Pod, NetApp MetroCluster IP e VMware vSphere 6.7 - progettazione"

Data center FlexPod con multi-pod Cisco ACI con NetApp MetroCluster IP e VMware vSphere 6.7 - implementazione

Haseeb Niazi, Cisco Ramesh Issac, Cisco Arvind Ramakrishnan, NetApp

Cisco e NetApp hanno collaborato per offrire una serie di soluzioni FlexPod che consentono piattaforme strategiche per data center. La soluzione FlexPod offre un'architettura integrata che incorpora le Best practice di progettazione per il calcolo, lo storage e il networking, riducendo al minimo i rischi PER L'IT convalidando l'architettura integrata per garantire la compatibilità tra i vari componenti. La soluzione affronta anche i punti critici DELL'IT fornendo una guida documentata alla progettazione, una guida all'implementazione e un supporto che possono essere utilizzati in varie fasi (pianificazione, progettazione e implementazione) di un'implementazione.

"Data center FlexPod con multi-pod Cisco ACI con NetApp MetroCluster IP e VMware vSphere 6.7 - implementazione"

Cloud ibrido

Cloud ibrido FlexPod con Cloud Volumes ONTAP per Epic

TR-4960: Cloud ibrido FlexPod con Cloud Volumes ONTAP per Epic

In collaborazione con:

Kamini Singh, NetApp

La chiave per fare una trasformazione digitale è semplicemente fare di più con i dati. Gli ospedali generano e richiedono grandi quantità di dati per gestire la propria organizzazione e servire i pazienti in modo efficace. Le informazioni vengono raccolte ed elaborate durante il trattamento dei pazienti e la gestione dei programmi del personale e delle risorse mediche.

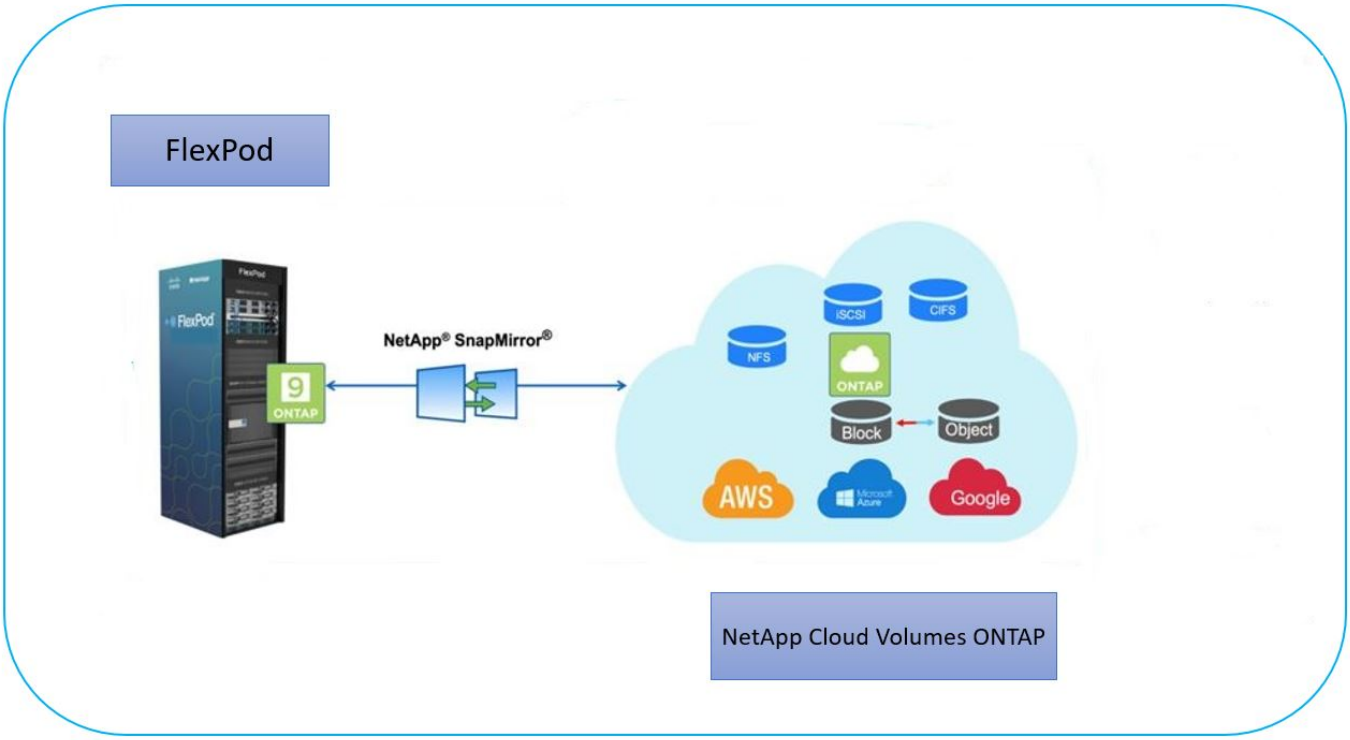
Le dimensioni in costante aumento dei dati sanitari e le preziose informazioni che questi dati possono fornire rendono i servizi dati sanitari e la protezione dei dati critici e impegnativi. Innanzitutto, i dati del settore sanitario devono essere sia disponibili che protetti per soddisfare i requisiti di ripristino dei dati, business continuity medica o conformità.

In secondo luogo, i dati sanitari devono essere resi prontamente disponibili per l'analisi. Spesso questa analisi utilizza approcci basati sull'intelligenza artificiale (ai) e sull'apprendimento automatico (ML) per aiutare le aziende mediche a migliorare le proprie soluzioni e creare valori di business.

In terzo luogo, le infrastrutture dei servizi dati e le metodologie di protezione dei dati devono adattarsi alla crescita dei dati sanitari man mano che un'azienda medica cresce. Inoltre, la mobilità dei dati sta diventando sempre più critica a causa della necessità di spostare i dati dall'edge in cui vengono creati al core e al cloud per utilizzare le risorse disponibili per l'analisi dei dati o l'archiviazione.

NetApp offre una singola soluzione di gestione dei dati per le applicazioni aziendali, inclusa l'assistenza sanitaria, e siamo in grado di guidare gli ospedali nel loro percorso verso la trasformazione digitale. NetApp Cloud Volumes ONTAP offre una soluzione per la gestione dei dati nel settore sanitario in cui i dati possono essere replicati in modo efficiente da un data center FlexPod a Cloud Volumes ONTAP implementato su un cloud pubblico come AWS.

Sfruttando risorse di cloud pubblico sicure e convenienti, Cloud Volumes ONTAP migliora il disaster recovery basato sul cloud con replica dei dati altamente efficiente, efficienze dello storage integrate e semplici test di DR. Questi sistemi sono gestiti con controllo unificato e semplicità di trascinamento, che offre una protezione conveniente e a prova di proiettile contro qualsiasi tipo di errore, guasto o disastro. Cloud Volumes ONTAP offre la tecnologia SnapMirror di NetApp come soluzione per la replica dei dati a livello di blocco che mantiene aggiornata la destinazione attraverso aggiornamenti incrementali.



Pubblico

Il presente documento è destinato a NetApp e ai partner Solutions Engineer (SES) e al personale dei servizi professionali. NetApp presuppone che il lettore disponga delle seguenti conoscenze di base:

- Una solida comprensione dei concetti SAN e NAS
- Familiarità tecnica con i sistemi storage NetApp ONTAP
- Familiarità tecnica con la configurazione e l'amministrazione del software ONTAP

Vantaggi della soluzione

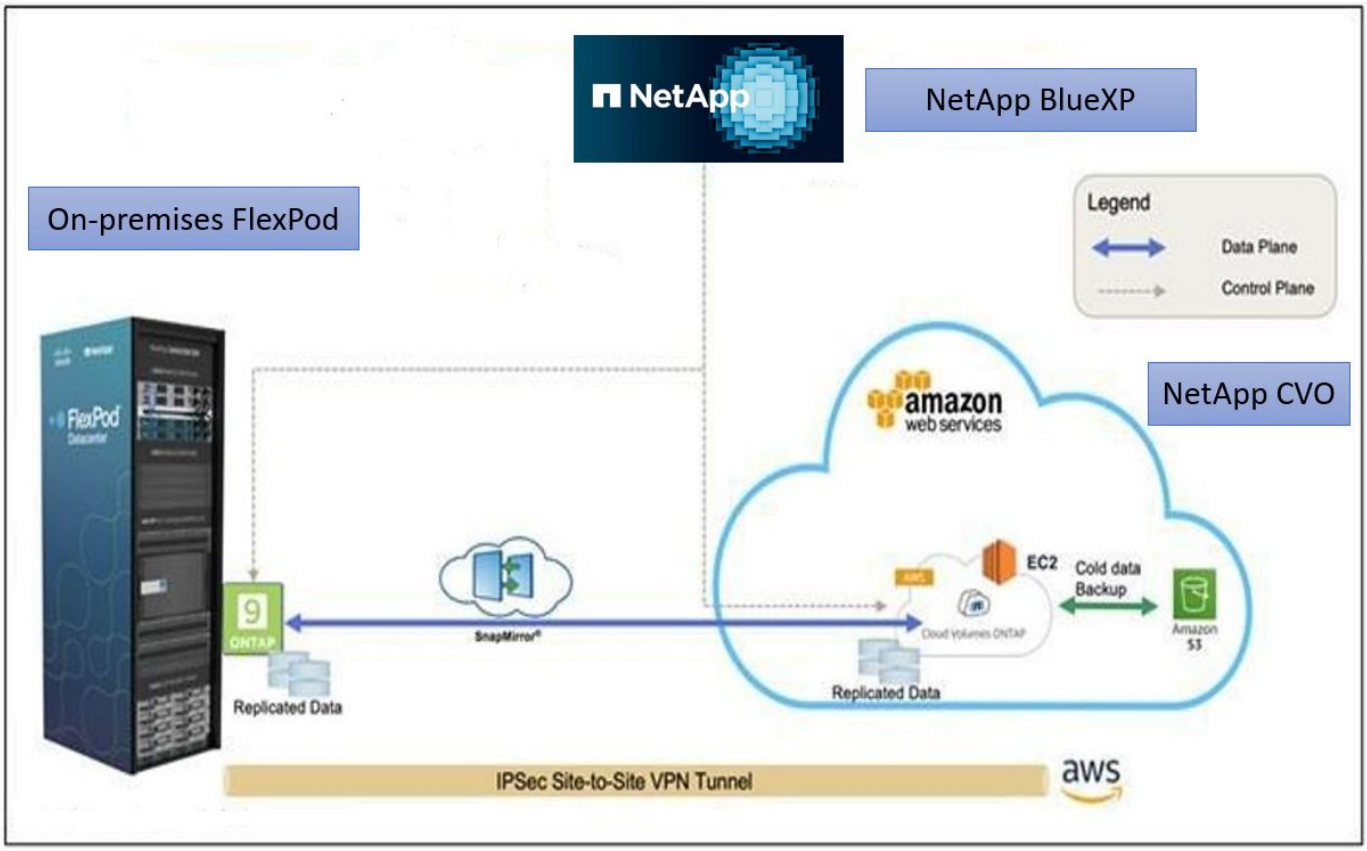
Il data center FlexPod integrato con NetApp Cloud Volumes ONTAP offre i seguenti vantaggi ai carichi di lavoro del settore sanitario:

- **Protezione personalizzata.** Cloud Volumes ONTAP offre replica dei dati a livello di blocco da ONTAP al cloud che mantiene aggiornata la destinazione attraverso aggiornamenti incrementali. Gli utenti possono specificare una pianificazione di sincronizzazione per determinare quando le modifiche all'origine vengono trasferite. In questo modo si ottiene una protezione personalizzata per tutti i tipi di dati sanitari.
- **Failover e failover.** in caso di disastro, gli amministratori dello storage possono impostare rapidamente il failover sui volumi cloud. Quando il sito primario viene ripristinato, i nuovi dati creati nell'ambiente DR vengono sincronizzati di nuovo con i volumi di origine, consentendo di ristabilire la replica dei dati secondari. In questo modo, i dati del settore sanitario possono essere facilmente ripristinati senza interruzioni.
- **Efficienza.** lo spazio di storage e i costi per la copia del cloud secondario sono ottimizzati mediante compressione dei dati, thin provisioning e deduplica. I dati del settore sanitario vengono trasferiti a livello di blocco in forma compressa e deduplicata, migliorando la velocità dei trasferimenti. Inoltre, i dati vengono automaticamente suddivisi in livelli per lo storage a oggetti a basso costo e riportati allo storage dalle performance elevate solo quando si accede, ad esempio in uno scenario di DR. In questo modo si riducono significativamente i costi di storage in corso.

- **Ransomware Protection.** la protezione ransomware NetApp BlueXP esegue la scansione delle origini dati in ambienti cloud e on-premise, rileva le vulnerabilità di sicurezza e fornisce il loro stato di sicurezza attuale e il punteggio dei rischi. Fornisce quindi consigli pratici che è possibile analizzare e seguire per rimediare. In questo modo, puoi proteggere i tuoi dati sanitari critici da attacchi ransomware.

Topologia della soluzione

In questa sezione viene descritta la topologia logica della soluzione. La figura seguente rappresenta la topologia della soluzione composta dall'ambiente on-premise di FlexPod, dal CVO (NetApp Cloud Volumes ONTAP) eseguito su Amazon Web Services (AWS) e dalla piattaforma NetApp BlueXP SaaS.



I piani di controllo e i piani di dati sono chiaramente indicati tra gli endpoint. Il piano dati viene eseguito tra l'istanza di ONTAP in esecuzione su FAS all-flash in FlexPod e l'istanza CVO di NetApp in AWS sfruttando una connessione VPN sicura sito-sito. La replica dei dati dei carichi di lavoro del settore sanitario dal data center FlexPod on-premise a NetApp Cloud Volumes ONTAP è gestita dalla replica di NetApp SnapMirror. Questa soluzione supporta anche il backup e il tiering opzionali dei dati cold che risiedono nell'istanza NetApp CVO in AWS S3.

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp ONTAP, networking Cisco Nexus, networking storage

Cisco MDS e Cisco Unified Computing System (Cisco UCS).

Le organizzazioni del settore sanitario sono alla ricerca di una soluzione per facilitare la loro trasformazione digitale e migliorare le esperienze e i risultati dei pazienti. Con FlexPod, otterrai una piattaforma sicura e scalabile che favorisce l'efficienza e consente al tuo staff di prendere decisioni più informate in modo più rapido, in modo da offrire una migliore assistenza ai pazienti.

FlexPod è la piattaforma ideale per le esigenze dei carichi di lavoro nel settore sanitario, in quanto offre i seguenti vantaggi:

- Ottimizzazione delle operazioni per ottenere informazioni più rapide e risultati migliori per i pazienti.
- Ottimizzazione delle applicazioni di imaging con un'infrastruttura scalabile e affidabile.
- Implementazione rapida ed efficiente con un approccio comprovato per applicazioni specifiche per il settore sanitario come EHR.

EHR

Electronic Health Records (EHR) crea software per gruppi medici di medie e grandi dimensioni, ospedali e organizzazioni sanitarie integrate. I clienti includono anche ospedali di comunità, strutture accademiche, organizzazioni per bambini, fornitori di reti di sicurezza e sistemi multi-ospedalieri. Il software integrato con EHR copre le funzioni cliniche, di accesso e di ricavo e si estende a casa.

Le organizzazioni di fornitori di servizi sanitari continuano a essere sotto pressione per massimizzare i benefici dei loro investimenti sostanziali in EHR leader del settore. Quando i clienti progettano i propri data center per le soluzioni EHR e le applicazioni mission-critical, spesso identificano i seguenti obiettivi per l'architettura del data center:

- Elevata disponibilità delle applicazioni EHR
- Performance elevate
- Facilità di implementazione dei sistemi EHR nel data center
- Agilità e scalabilità per consentire la crescita con nuove release o applicazioni EHR
- Convenienza
- Gestibilità, stabilità e facilità di supporto
- Solida protezione dei dati, backup, recovery e continuità del business

FlexPod è validato da EHR e supporta una piattaforma contenente Cisco UCS con processori Intel Xeon, Red Hat Enterprise Linux (RHEL) e virtualizzazione con VMware ESXi. Questa piattaforma, unita alla classifica di alto livello di comfort di EHR per lo storage NetApp che esegue ONTAP, offre ai clienti la sicurezza di eseguire le proprie applicazioni sanitarie in un cloud privato completamente gestito tramite FlexPod, che può anche essere connesso a qualsiasi provider di cloud pubblico.

NetApp BlueXP

BlueXP (in precedenza NetApp Cloud Manager) è una piattaforma di gestione di livello Enterprise basata su SaaS che consente agli esperti IT e agli architetti del cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud di NetApp. Fornisce un sistema centralizzato per la visualizzazione e la gestione dello storage on-premise e cloud, supportando account e provider di cloud ibridi e multipli. Per ulteriori informazioni, vedere "BlueXP".

Connettore

Un'istanza di connettore consente a BlueXP di gestire risorse e processi all'interno di un ambiente di cloud pubblico. Connector è necessario per molte delle funzionalità fornite da BlueXP e può essere implementato nel cloud o nella rete on-premise.

Il connettore è supportato nelle seguenti posizioni:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On-premise

Per ulteriori informazioni su Connector, consultare "Pagina del connettore".

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è un'offerta di storage software-defined che esegue il software di gestione dei dati ONTAP nel cloud per offrire una gestione avanzata dei dati per i carichi di lavoro di file e blocchi. Con Cloud Volumes ONTAP, puoi ottimizzare i costi di cloud storage e aumentare le performance applicative, migliorando al contempo protezione dei dati, sicurezza e conformità.

I vantaggi principali includono:

- * Efficienza dello storage.* sfrutta la deduplica dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione istantanea per ridurre al minimo i costi dello storage.
- **High Availability.** offre affidabilità Enterprise e operazioni continue in caso di guasti nel tuo ambiente cloud.
- **Protezione dei dati.** Cloud Volumes ONTAP utilizza SnapMirror, la tecnologia di replica leader del settore di NetApp, per replicare i dati on-premise nel cloud, in modo che sia facile disporre di copie secondarie per diversi casi di utilizzo. Cloud Volumes ONTAP si integra anche con il backup nel cloud per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati nel cloud.
- **Tiering dei dati.** consente di passare da un pool di storage ad alte e a basse performance on-demand senza portare le applicazioni offline.
- **Coerenza delle applicazioni.** garantire la coerenza delle copie Snapshot di NetApp utilizzando la tecnologia NetApp SnapCenter.
- **Sicurezza dei dati.** Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.
- **Controlli di conformità alla privacy.** l'integrazione con Cloud Data Sense ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

Per ulteriori informazioni, vedere "Cloud Volumes ONTAP".

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager consente il monitoraggio dei cluster di storage ONTAP da un'unica interfaccia, riprogettata e intuitiva, che offre intelligence basata su conoscenze della community e analytics ai. Fornisce informazioni complete sul funzionamento, sulle performance e sulle attività proattive dell'ambiente di storage e delle macchine virtuali in esecuzione. Quando si verifica un problema con l'infrastruttura di storage, Unified Manager può notificare i dettagli del problema per identificare la causa principale. La dashboard della macchina virtuale offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter

analizzare l'intero percorso di i/o dall'host vSphere fino alla rete e infine allo storage.

Alcuni eventi forniscono anche azioni correttive che possono essere intraprese per risolvere il problema. È possibile configurare avvisi personalizzati per gli eventi in modo che, quando si verificano problemi, venga inviata una notifica tramite e-mail e trap SNMP. Active IQ Unified Manager consente di pianificare i requisiti di storage degli utenti prevedendo le tendenze di capacità e utilizzo in modo da poter agire prima che si verifichino problemi, evitando decisioni reattive a breve termine che possono portare a ulteriori problemi a lungo termine.

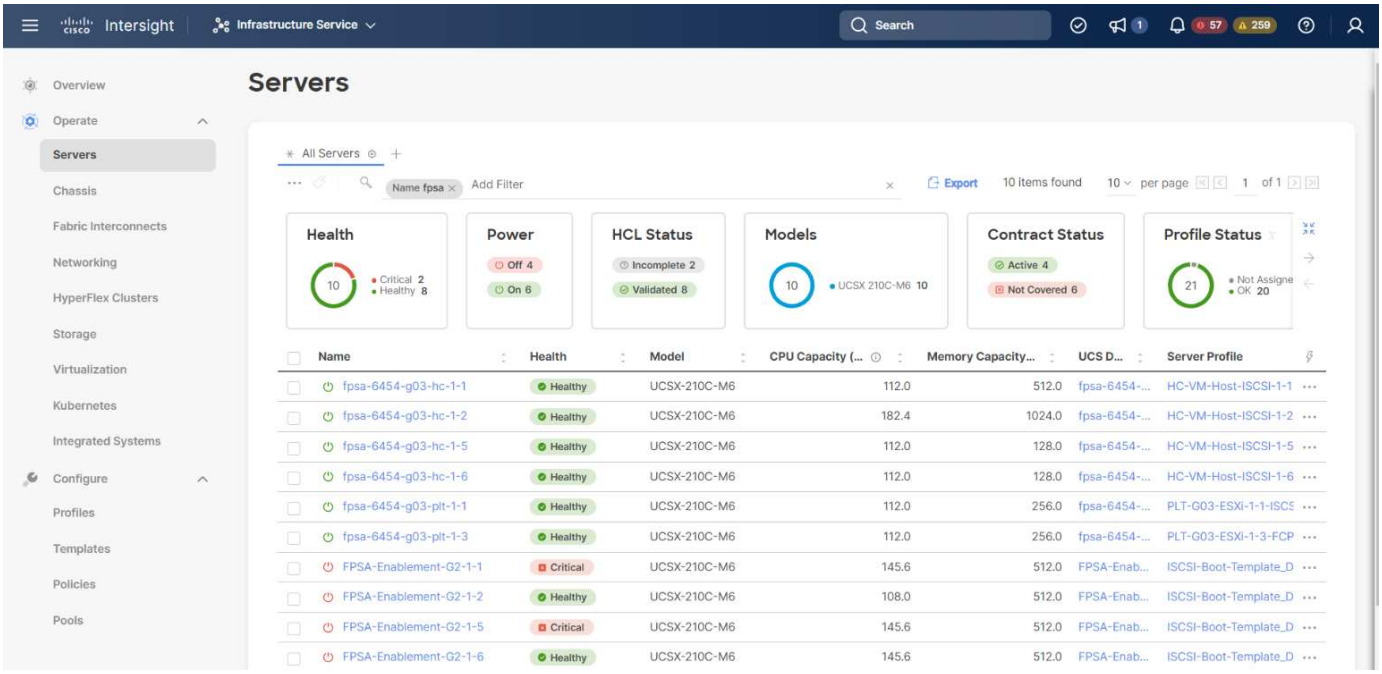
Per ulteriori informazioni, vedere "Active IQ Unified Manager".

Cisco Intersight

Cisco Intersight è una piattaforma SaaS che offre automazione, osservabilità e ottimizzazione intelligenti per infrastrutture e applicazioni tradizionali e native del cloud. La piattaforma aiuta a promuovere il cambiamento con i team IT e offre un modello operativo progettato per il cloud ibrido. Cisco Intersight offre i seguenti vantaggi:

- **Delivery più rapida.** Intersight viene fornito come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può concentrarsi sul supporto delle esigenze aziendali critiche.
- **Operazioni semplificate.** Intersight semplifica le operazioni utilizzando un singolo tool SaaS sicuro con inventario, autenticazione e API comuni per lavorare nell'intero stack e in tutte le ubicazioni, eliminando i silos tra i team. Questo consente di gestire server fisici e hypervisor on-premise, su macchine virtuali, K8s, serverless, automazione, ottimizzazione e controllo dei costi sia on-premise che nei cloud pubblici.
- **Ottimizzazione continua.** puoi ottimizzare continuamente il tuo ambiente utilizzando l'intelligence fornita da Cisco Intersight su ogni livello e da Cisco TAC. Questa intelligenza viene convertita in azioni consigliate e automatizzabili per consentirti di adattarsi in tempo reale a qualsiasi cambiamento: Dallo spostamento dei carichi di lavoro al monitoraggio dello stato di salute dei server fisici ai consigli per la riduzione dei costi per i cloud pubblici con cui lavori.

Cisco Intersight offre due modalità di gestione: UCSM Managed Mode (UMM) e Intersight Managed Mode (IMM). È possibile selezionare la modalità gestita UCSM (UMM) o la modalità gestita di Intersight (IMM) nativa per i sistemi Cisco UCS collegati al fabric durante la configurazione iniziale delle interconnessioni fabric. In questa soluzione viene utilizzato IMM nativo. La figura seguente mostra Cisco Intersight Dashboard.



VMware vSphere 7.0

VMware vSphere è una piattaforma di virtualizzazione per la gestione olistica di grandi insiemi di infrastrutture (incluse CPU, storage e networking) come ambiente operativo perfetto, versatile e dinamico. A differenza dei sistemi operativi tradizionali che gestiscono un singolo computer, VMware vSphere aggrega l'infrastruttura di un intero data center per creare un unico power house con risorse che possono essere allocate in modo rapido e dinamico a qualsiasi applicazione in necessità.

Per ulteriori informazioni su VMware vSphere e i relativi componenti, vedere "VMware vSphere".

VMware vCenter Server

VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da una singola console e aggrega il monitoraggio delle performance di cluster, host e macchine virtuali. VMware vCenter Server offre agli amministratori una panoramica approfondita dello stato e della configurazione di cluster di calcolo, host, macchine virtuali, storage, sistema operativo guest, e altri componenti critici di un'infrastruttura virtuale. VMware vCenter gestisce l'insieme completo di funzionalità disponibili in un ambiente VMware vSphere.

Per informazioni dettagliate, vedere "VMware vCenter".

Revisioni hardware e software

Questa soluzione di cloud ibrido può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware, come definito nella "Tool di matrice di interoperabilità NetApp", "Compatibilità hardware e software UCS", e. "Guida alla compatibilità VMware".

La seguente tabella mostra le revisioni hardware e software di FlexPod on-premise.

Componente	Prodotto	Versione
Calcolo	Cisco UCS X210c M6	5.0(1b)

Componente	Prodotto	Versione
	Cisco UCS Fabric Interconnects 6454	4.2(2a)
Rete	Sistema operativo Cisco Nexus 9336C-FX2 NX	9.3(9)
Storage	NetApp AFF A400	ONTAP 9.11.1P2
	Strumenti NetApp ONTAP per VMware vSphere	9.11
	Plug-in NetApp NFS per VMware VAAI	2.0
	NetApp Active IQ Unified Manager	9.11P1
Software	VMware vSphere	7.0 (U3)
	Driver Ethernet Nenico VMware ESXi	1.0.35.0
	Appliance VMware vCenter	7.0.3
	Appliance virtuale Cisco Intersight Assist	1.0.9-342

La seguente tabella mostra le versioni di NetApp BlueXP e Cloud Volumes ONTAP.

Vendor	Prodotto	Versione
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"Pagina successiva: Installazione e configurazione."

Installazione e configurazione

"Precedente: Componenti della soluzione."

Implementazione di NetApp Cloud Volumes ONTAP

Completare i seguenti passaggi per configurare l'istanza di Cloud Volumes ONTAP:

1. Preparare l'ambiente del provider di servizi cloud pubblico.

   È necessario acquisire i dettagli dell'ambiente del provider di servizi cloud pubblico per la configurazione della soluzione. Ad esempio, per la preparazione dell'ambiente Amazon Web Services (AWS), è necessario disporre della chiave di accesso AWS, della chiave segreta AWS e di altri dettagli di rete come regione, VPC, subnet e così via.

2. Configurare il gateway dell'endpoint VPC.

   Per abilitare la connessione tra il VPC e il servizio AWS S3 è necessario un gateway endpoint VPC. Viene utilizzato per attivare il backup su CVO, un endpoint con il tipo di gateway.

3. Accedi a NetApp BlueXP.

   Per accedere a NetApp BlueXP e ad altri servizi cloud, devi iscriverti a. "NetApp BlueXP". Per configurare le aree di lavoro e gli utenti nell'account BlueXP, fare clic su "qui". Devi disporre di un account che disponga dell'autorizzazione per implementare il connettore nel tuo cloud provider direttamente da BlueXP. È possibile scaricare il criterio BlueXP da "qui".

4. Implementare il connettore.

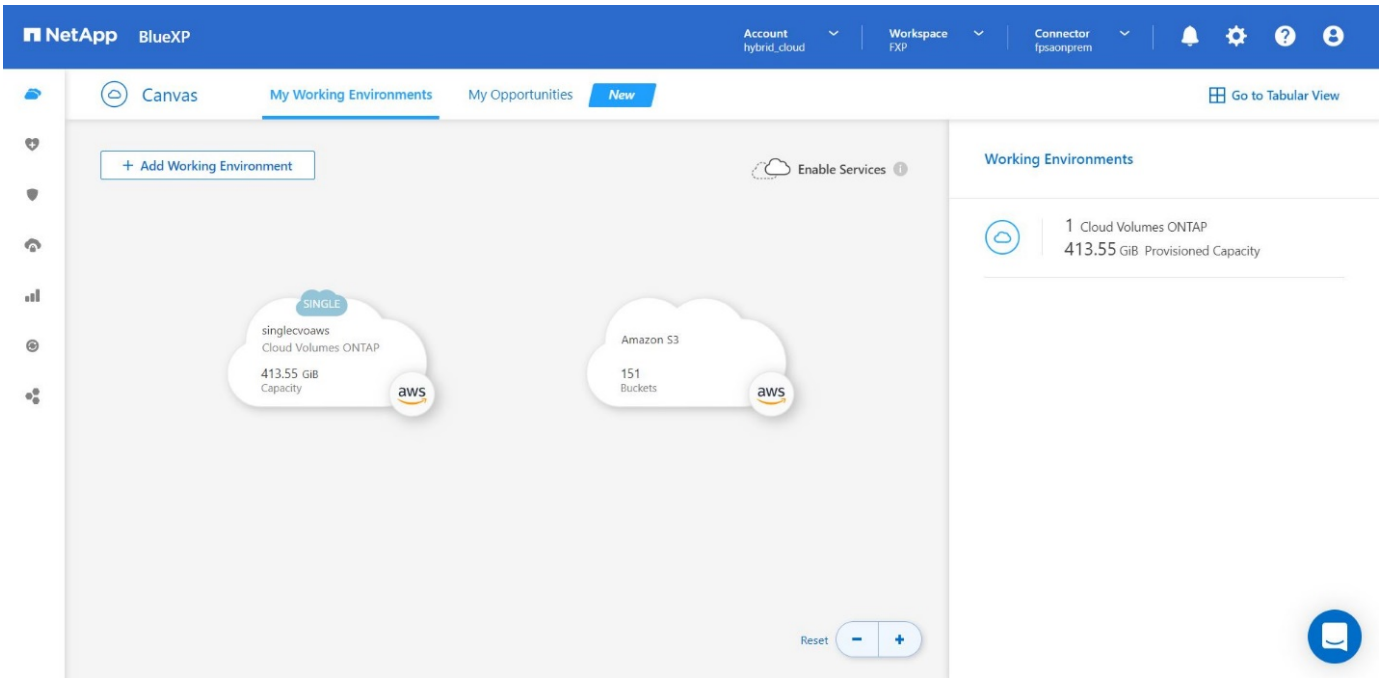
   Prima di aggiungere un ambiente di lavoro Cloud Volume ONTAP, è necessario implementare Connector. BlueXP richiede se si tenta di creare il primo ambiente di lavoro Cloud Volumes ONTAP senza il connettore. Per implementare il connettore in AWS da BlueXP, consulta questa sezione "collegamento".

5. Avviare Cloud Volumes ONTAP in AWS.

   È possibile avviare Cloud Volumes ONTAP in una configurazione a sistema singolo o come coppia ha in AWS. "Leggi le istruzioni dettagliate".

   Per informazioni dettagliate su questi passaggi, consultare "Guida rapida per Cloud Volumes ONTAP in AWS".

   In questa soluzione, abbiamo implementato un sistema Cloud Volumes ONTAP a nodo singolo in AWS. La figura seguente mostra NetApp BlueXP Dashboard con istanza CVO a nodo singolo.



Implementazione FlexPod on-premise

Per conoscere i dettagli di progettazione di FlexPod con UCS X-Series, VMware e NetApp ONTAP, vedere "Data center FlexPod con Cisco UCS serie X." guida alla progettazione. Questo documento fornisce indicazioni di progettazione per l'integrazione della piattaforma Cisco Intersight-Managed UCS X-Series nell'infrastruttura del data center FlexPod.

Per la distribuzione dell'istanza di FlexPod on-premise, vedere "questa guida all'implementazione".

Questo documento fornisce indicazioni per l'implementazione dell'integrazione della piattaforma UCS X-Series

gestita da Cisco Intersight all'interno di un'infrastruttura di data center FlexPod. Il documento tratta sia le configurazioni che le Best practice per un'implementazione di successo.

FlexPod può essere implementato sia in modalità gestita UCS che in modalità gestita di Cisco Intersight (IMM). Se si sta implementando FlexPod in modalità gestita UCS, vedere questa sezione "guida alla progettazione" e questo "guida all'implementazione".

L'implementazione di FlexPod può essere automatizzata con l'infrastruttura come codice utilizzando Ansible. Di seguito sono riportati i collegamenti ai repository di GitHub per l'implementazione end-to-end di FlexPod:

- È possibile visualizzare la configurazione Ansible di FlexPod con Cisco UCS in modalità gestita, NetApp ONTAP e VMware vSphere "qui".
- È possibile visualizzare la configurazione Ansible di FlexPod con Cisco UCS in IMM, NetApp ONTAP e VMware vSphere "qui".

Configurazione dello storage ONTAP on-premise

In questa sezione vengono descritte alcune importanti procedure di configurazione di ONTAP specifiche di questa soluzione.

1. Configurare una SVM con il servizio iSCSI in esecuzione.

```
1. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   Se la licenza iSCSI non è stata installata durante la configurazione del cluster, assicurarsi di installare la licenza prima di creare il servizio iSCSI.

2. Creare un volume FlexVol.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Aggiunta di interfacce per l'accesso iSCSI.

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> -status-admin up
```

In questa soluzione sono stati creati quattro LIF (Logical Interface) iSCSI, due su ciascun nodo.

Dopo che l'istanza di FlexPod è attiva e in esecuzione con vCenter implementato e tutti gli host ESXi aggiunti, è necessario implementare una macchina virtuale Linux che agisca come server che si connette e accede allo storage NetApp ONTAP. In questa soluzione, è stata installata un'istanza di CentOS 8 in vCenter.

4. Creare un LUN.

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

Per un database operativo EHR (ODB), un giornale e carichi di lavoro applicativi, EHR consiglia di presentare lo storage ai server come LUN iSCSI. NetApp supporta inoltre l'utilizzo di FCP e NVMe/FC se si dispone di versioni di AIX e dei sistemi operativi RHEL in grado di supportare, migliorando le performance. FCP e NVMe/FC possono coesistere sullo stesso fabric.

5. Creare un igroup.

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

Gli iGroups vengono utilizzati per consentire l'accesso al server alle LUN. Per l'host Linux, il server IQN si trova nel file `/etc/iscsi/initiatorname.iscsi`.

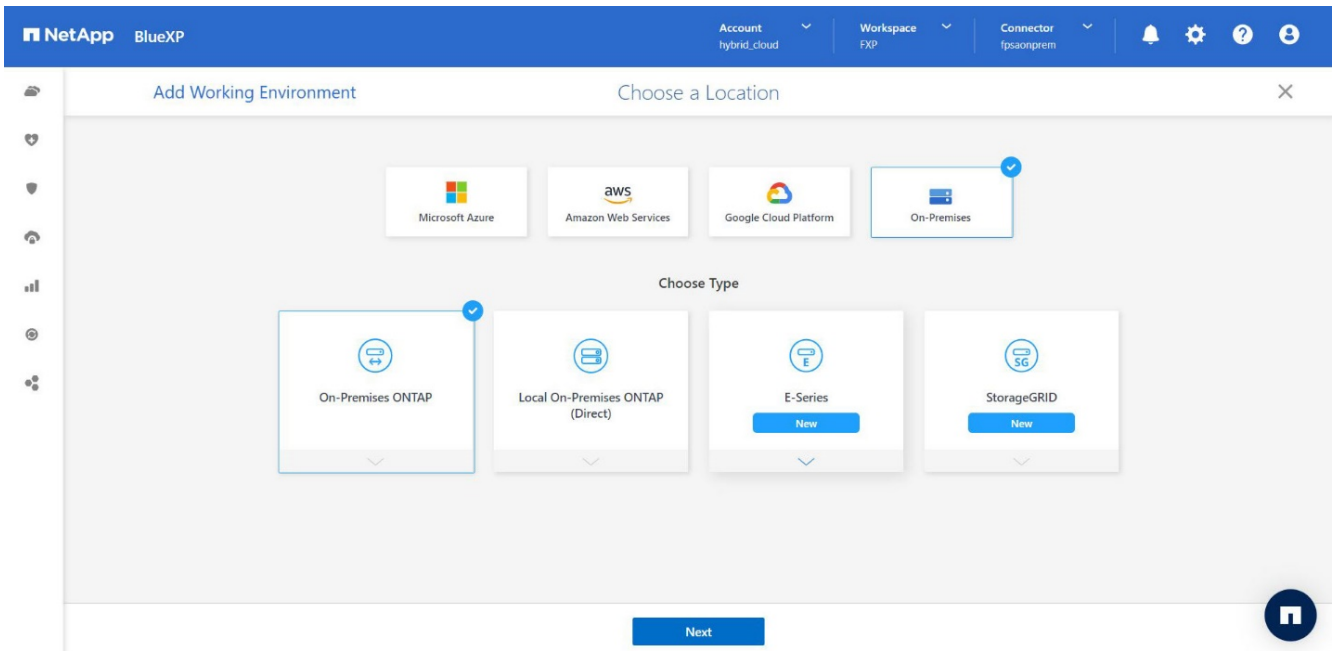
6. Mappare il LUN sull'igroup.

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

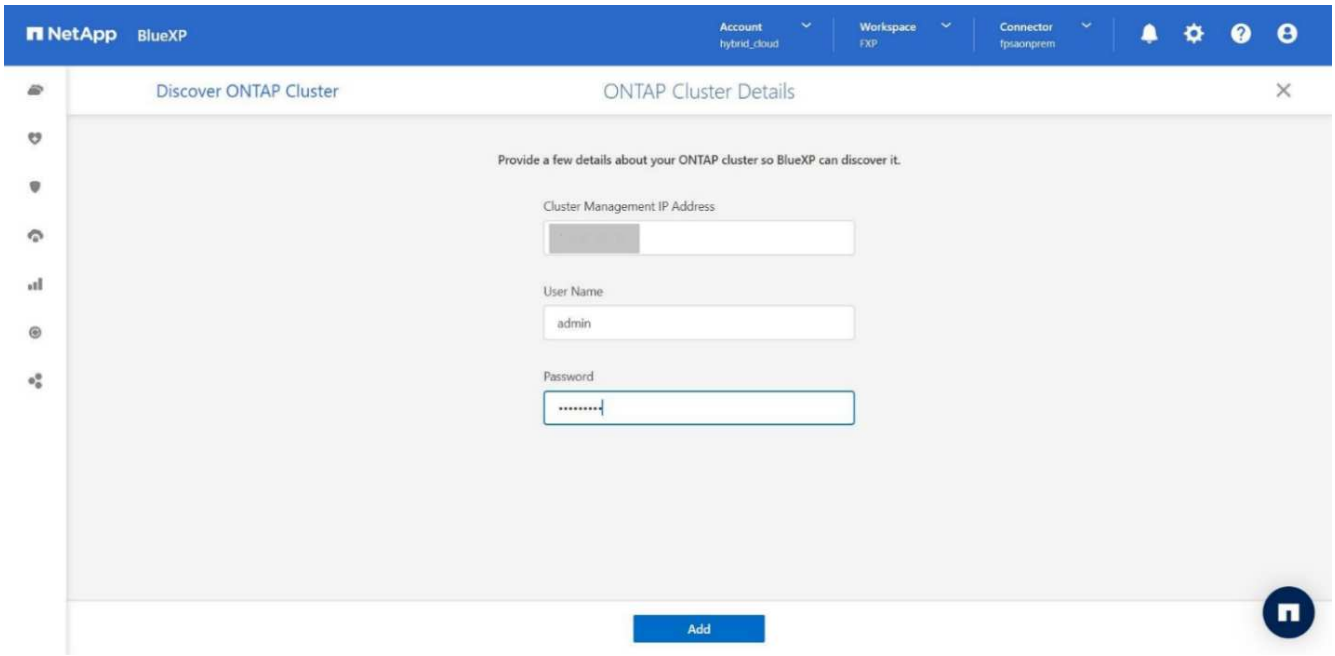
Aggiunta di storage FlexPod on-premise a BlueXP

Completare i seguenti passaggi per aggiungere lo storage FlexPod all'ambiente di lavoro utilizzando NetApp BlueXP.

1. Dal menu di navigazione, selezionare **Storage** > **Canvas**.
2. Nella pagina Canvas, fare clic su **Add Working Environment** (Aggiungi ambiente di lavoro) e selezionare **on-premise**.
3. Selezionare **ONTAP on-premise**. Fare clic su **Avanti**.

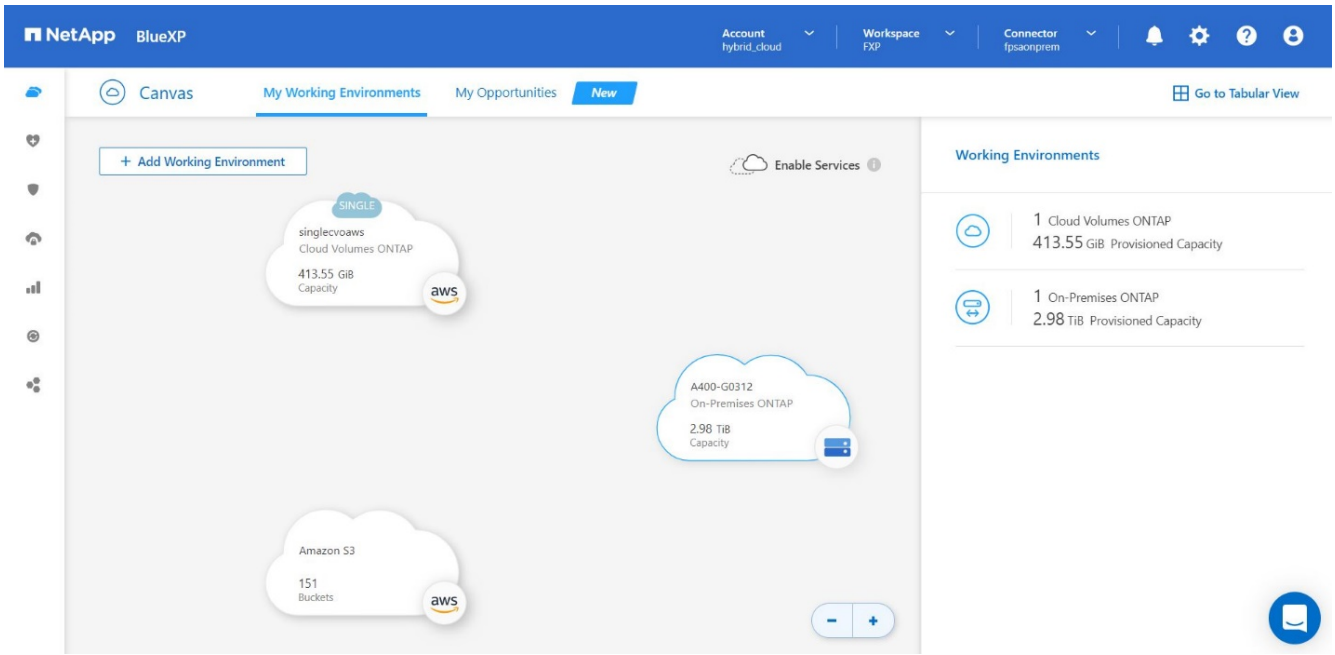


4. Nella pagina Dettagli cluster ONTAP, inserire l'indirizzo IP di gestione del cluster e la password per l'account utente admin. Quindi fare clic su **Aggiungi**.



5. Nella pagina Dettagli e credenziali, immettere un nome e una descrizione per l'ambiente di lavoro, quindi fare clic su **Go**.

   BlueXP rileva il cluster ONTAP e lo aggiunge come ambiente di lavoro su Canvas.



Per informazioni dettagliate, vedere la pagina "Scopri i cluster ONTAP on-premise".

"Pagina successiva: Configurazione SAN."

Configurazione SAN

"Precedente: Installazione e configurazione."

Questa sezione descrive la configurazione lato host richiesta da EHR per consentire al

software di integrarsi al meglio con lo storage NetApp. In questo segmento, discutiamo in modo specifico dell'integrazione degli host per i sistemi operativi Linux. Utilizzare "Tool di matrice di interoperabilità NetApp (IMT)" per convalidare tutte le versioni del software e del firmware.

> La seguente procedura di configurazione è specifica per l'host CentOS 8 utilizzato in questa soluzione.

Kit di utility host NetApp

NetApp consiglia di installare NetApp host Utility Kit (host Utilities) sui sistemi operativi degli host collegati ai sistemi storage NetApp e che accedono ad essi. È supportato Microsoft MPIO (Multipath i/o) nativo. Il sistema operativo deve essere compatibile con ALUA (Asymmetric Logical Unit Access) per il multipathing. L'installazione delle utility host configura le impostazioni dell'HBA (host Bus Adapter) per lo storage NetApp.

È possibile scaricare le utility host di NetApp "qui". In questa soluzione, abbiamo installato Linux host Utilities 7.1 sull'host.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

Scopri lo storage ONTAP

Assicurarsi che il servizio iSCSI sia in esecuzione quando si suppone che si verifichino i log-in. Per impostare la modalità di accesso per un portale specifico su una destinazione o per tutti i portali su una destinazione, utilizzare `iscsiadm` comando.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Ora puoi utilizzare `sanlun` Per visualizzare le informazioni relative ai LUN collegati all'host. Assicurarsi di aver effettuato l'accesso come root sull'host.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                     device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

Configurare il multipathing

Device Mapper Multipathing (DM-multipath) è un'utility di multipathing nativa in Linux. Può essere utilizzato per la ridondanza e per migliorare le performance. Aggrega o combina i percorsi di i/o multipli tra server e storage, in modo da creare un singolo dispositivo a livello di sistema operativo.

1. Prima di configurare DM-multipath sul sistema, assicurarsi che il sistema sia stato aggiornato e includa `device-mapper-multipath` pacchetto.

   ```
   [root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
   device-mapper-multipath-libs-0.8.4-31.el8.x86_64
   device-mapper-multipath-0.8.4-31.el8.x86_64
   ```

2. Il file di configurazione è `/etc/multipath.conf` file. Aggiornare il file di configurazione come mostrato di seguito.

   ```
   [root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
   defaults {
      path_checker      readsector0
      no_path_retry      fail
   }
   devices {
      device {
         vendor         "NETAPP  "
         product         "LUN.*"
         no_path_retry     queue
         path_checker      tur
      }
   }
   ```

3. Attivare e avviare i servizi multipath.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. Aggiungere il modulo kernel caricabile `dm-multipath` e riavviare il servizio multipath. Infine, controllare lo stato del multipathing.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

Per informazioni dettagliate su questi passaggi, vedere "qui".

Creare un volume fisico

Utilizzare `pvcreate` comando per inizializzare un dispositivo a blocchi da utilizzare come volume fisico. L'inizializzazione è analoga alla formattazione di un file system.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

Creare un gruppo di volumi

Per creare un gruppo di volumi da uno o più volumi fisici, utilizzare `vgcreate` comando. Questo comando crea un nuovo gruppo di volumi in base al nome e vi aggiunge almeno un volume fisico.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

Il `vgdisplay` il comando può essere utilizzato per visualizzare le proprietà dei gruppi di volumi (ad esempio dimensioni, estensioni, numero di volumi fisici e così via) in un formato fisso.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

Creare un volume logico

Quando si crea un volume logico, il volume logico viene ricavato da un gruppo di volumi utilizzando le estensioni libere sui volumi fisici che compongono il gruppo di volumi.

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Questo comando crea un volume logico chiamato `datalv` che utilizza tutto lo spazio non allocato nel gruppo di volumi `datavg`.

Creare il file system

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Creare la cartella da montare

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Montare il file system

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

Per informazioni dettagliate su queste attività, vedere la pagina "Amministrazione di LVM con comandi CLI".

Generazione di dati

```
`Dgen.pl` È un generatore di dati di script perl per il simulatore i/o di
EHR (GenerateIO). I dati all'interno dei LUN vengono generati con l'EHR
`Dgen.pl` script. Lo script è progettato per creare dati simili a quelli
che si trovano all'interno di un database EHR.
```

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

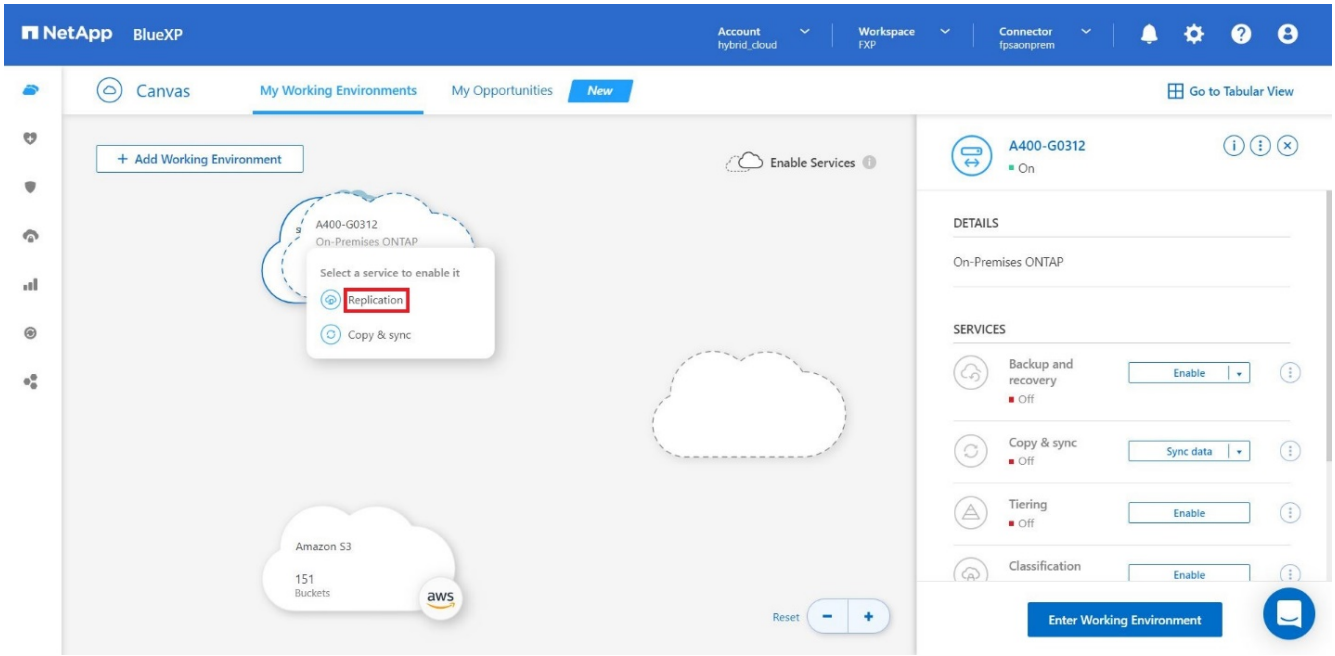
Durante la corsa `Dgen.pl` per impostazione predefinita, lo script utilizza il 85% del file system per la generazione dei dati.

Configurare la replica di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP

NetApp SnapMirror replica i dati a velocità elevate su LAN o WAN, in modo da ottenere un'elevata disponibilità dei dati e una replica rapida dei dati in ambienti virtuali e tradizionali. Quando si replicano i dati nei sistemi storage NetApp e si aggiornano continuamente i dati secondari, i dati vengono mantenuti aggiornati e rimangono disponibili ogni volta che ne hai bisogno. Non sono richiesti server di replica esterni.

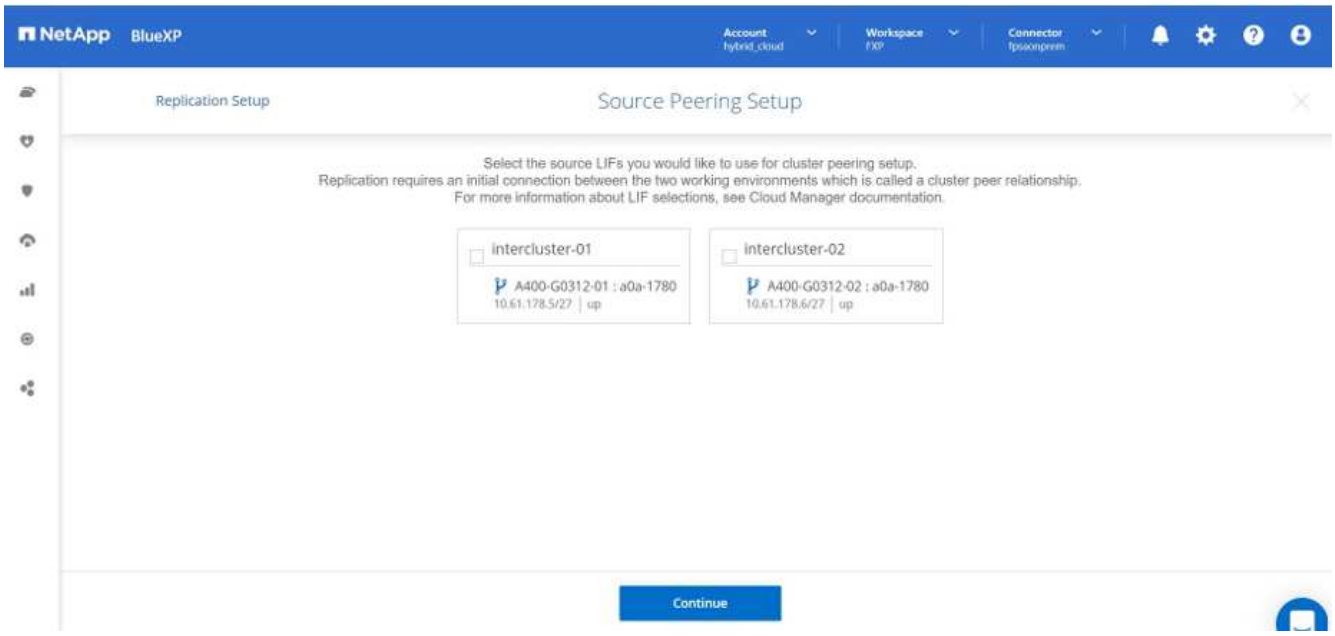
Completare i seguenti passaggi per configurare la replica di SnapMirror tra il sistema ONTAP on-premise e CVO.

1. Dal menu di navigazione, selezionare **Storage** > **Canvas**.
2. In Canvas, selezionare l'ambiente di lavoro che contiene il volume di origine, trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume, quindi selezionare **Replication**.

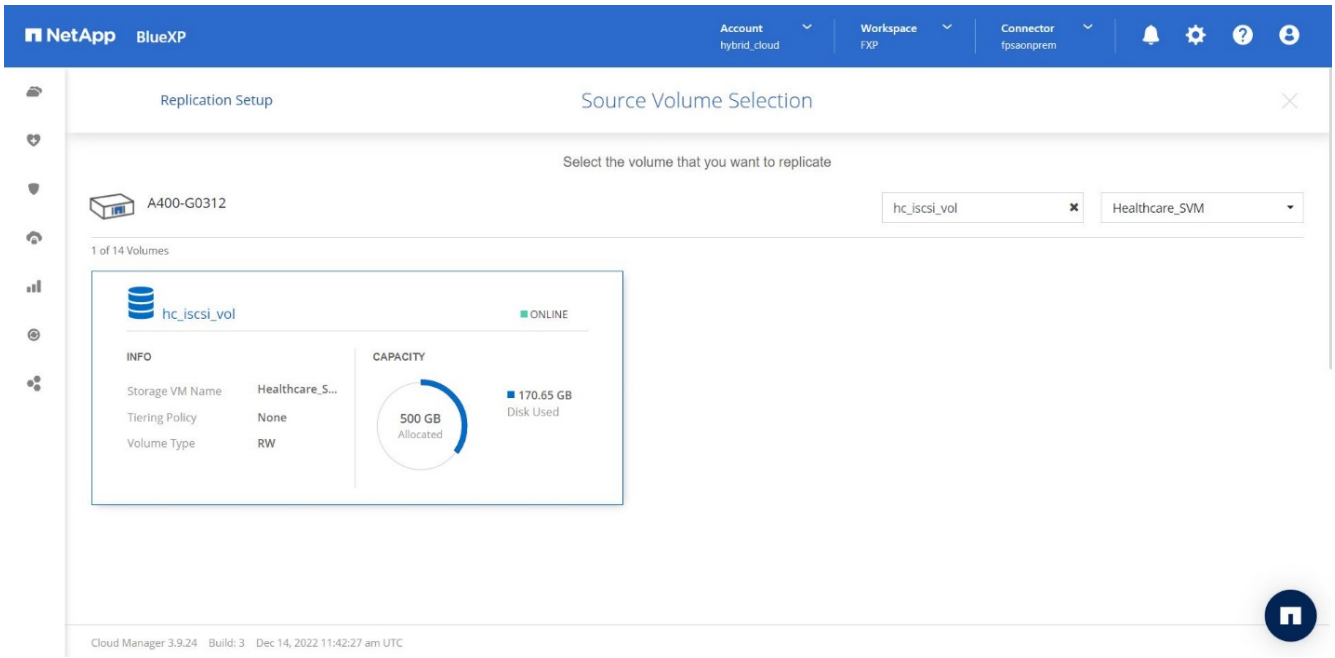


I passaggi rimanenti spiegano come creare una relazione sincrona tra cluster Cloud Volumes ONTAP e ONTAP on-premise.

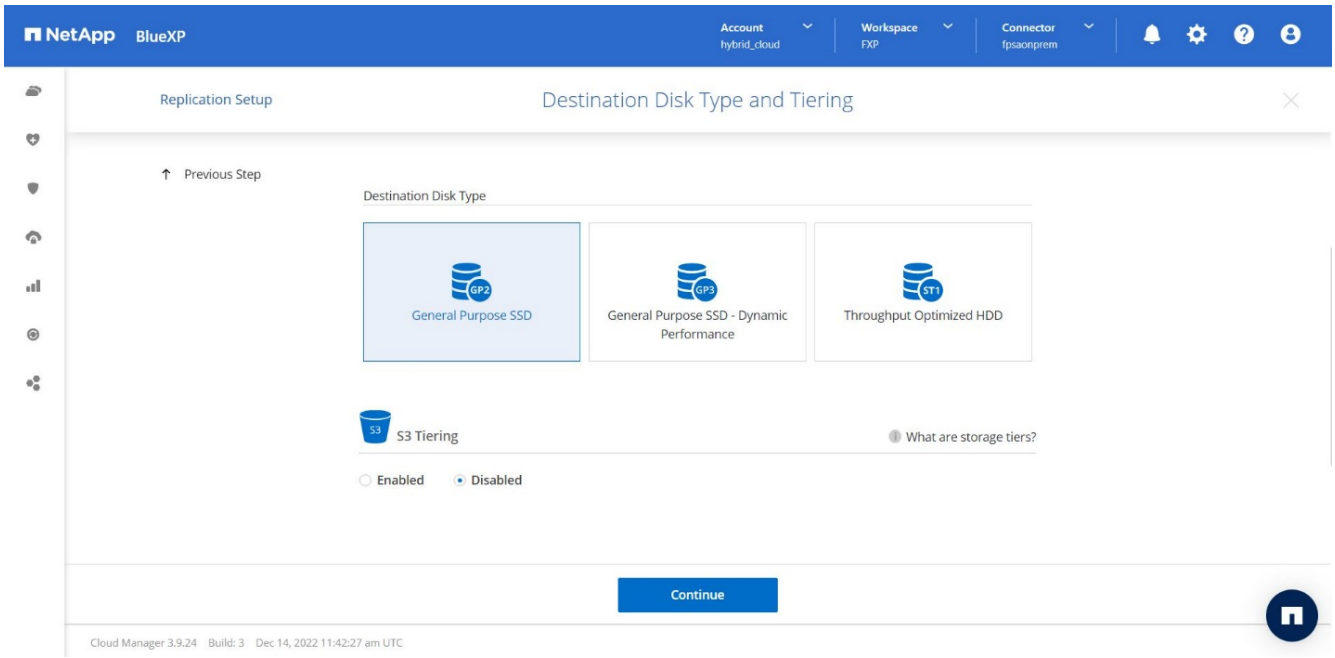
3. **Impostazione peering di origine e destinazione.** se viene visualizzata questa pagina, selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.



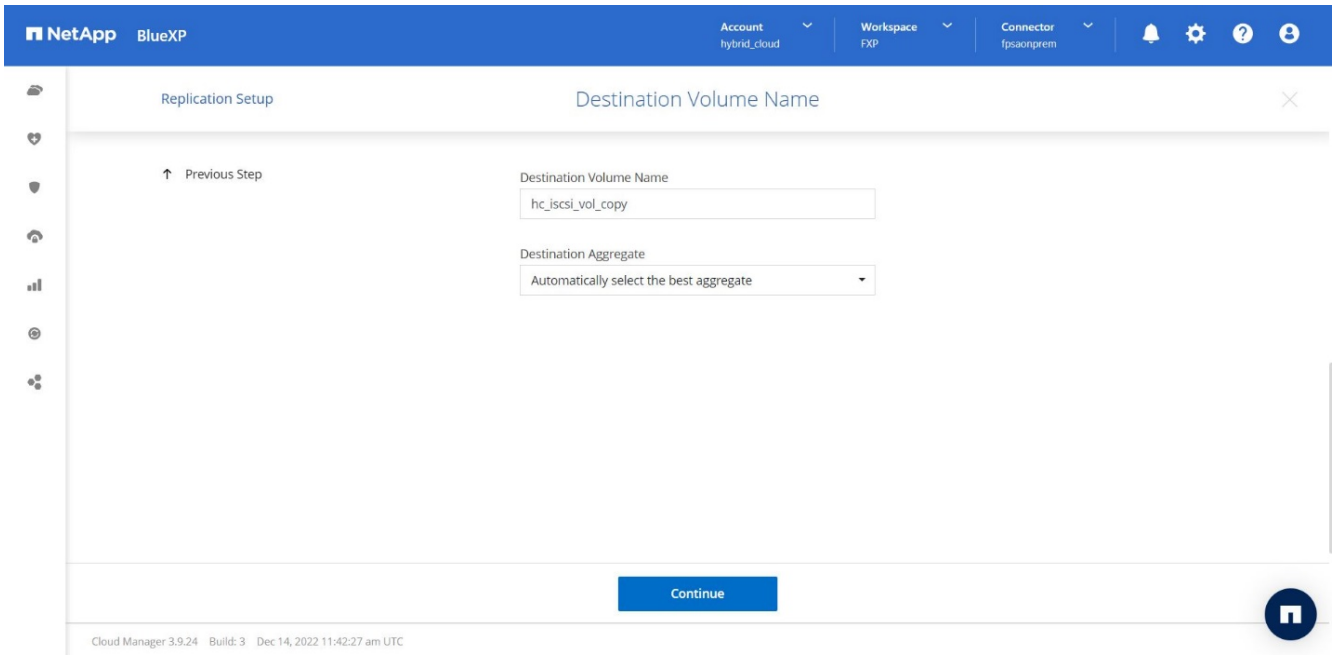
4. **Source Volume Selection.** selezionare il volume che si desidera replicare.



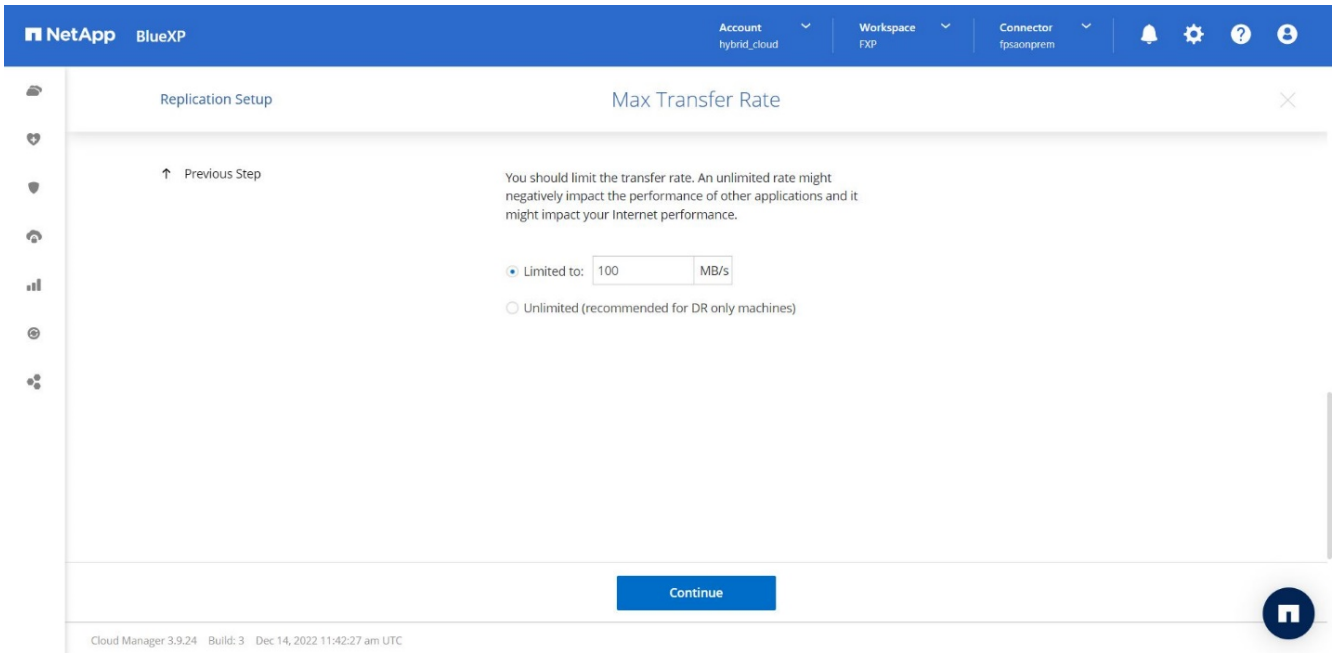
5. **Tipo di disco di destinazione e tiering.** se la destinazione è un sistema Cloud Volumes ONTAP, selezionare il tipo di disco di destinazione e scegliere se si desidera attivare il tiering dei dati.



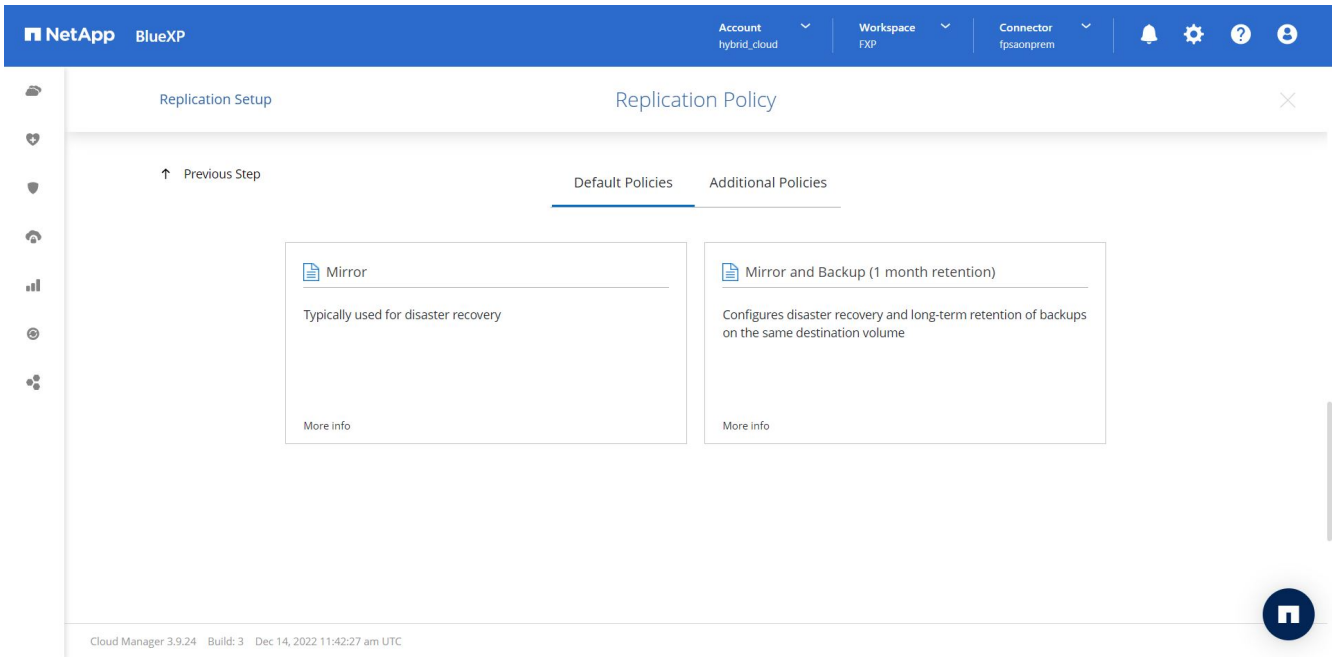
6. **Nome volume di destinazione:** specificare il nome del volume di destinazione e scegliere l'aggregato di destinazione. Se la destinazione è un cluster ONTAP, è necessario specificare anche la VM di storage di destinazione.



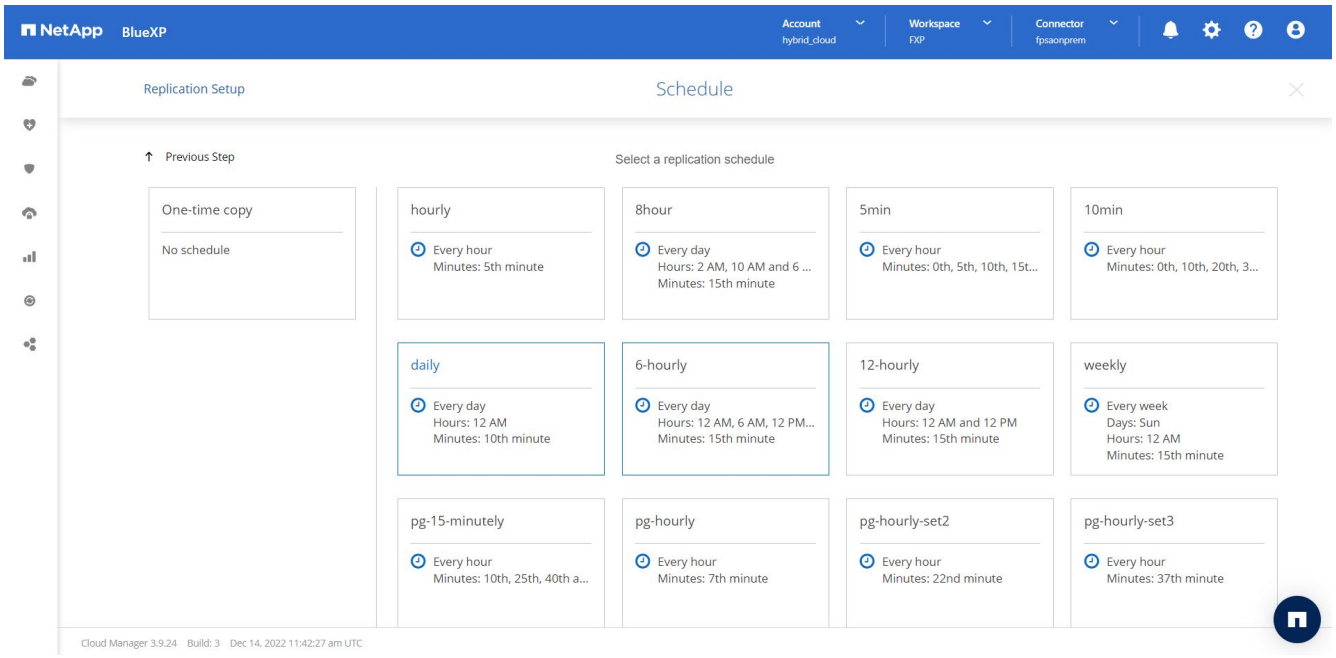
7. **Velocità di trasferimento massima.** specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.



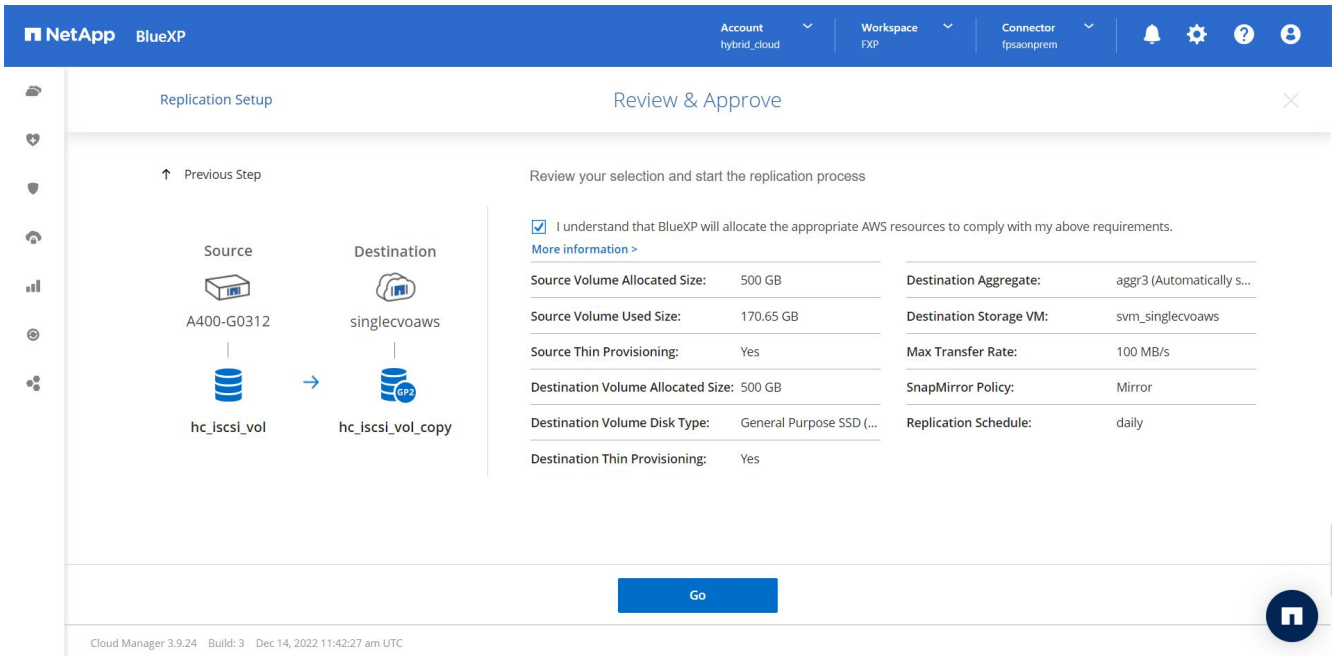
8. **Replication policy.** scegliere un criterio predefinito o fare clic su **Additional Policies**, quindi selezionare uno dei criteri avanzati. Per assistenza, "scopri le policy di replica".



9. **Pianificazione.** scegliere una copia singola o una pianificazione ricorrente. Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione su `destination cluster` Utilizzo di System Manager.

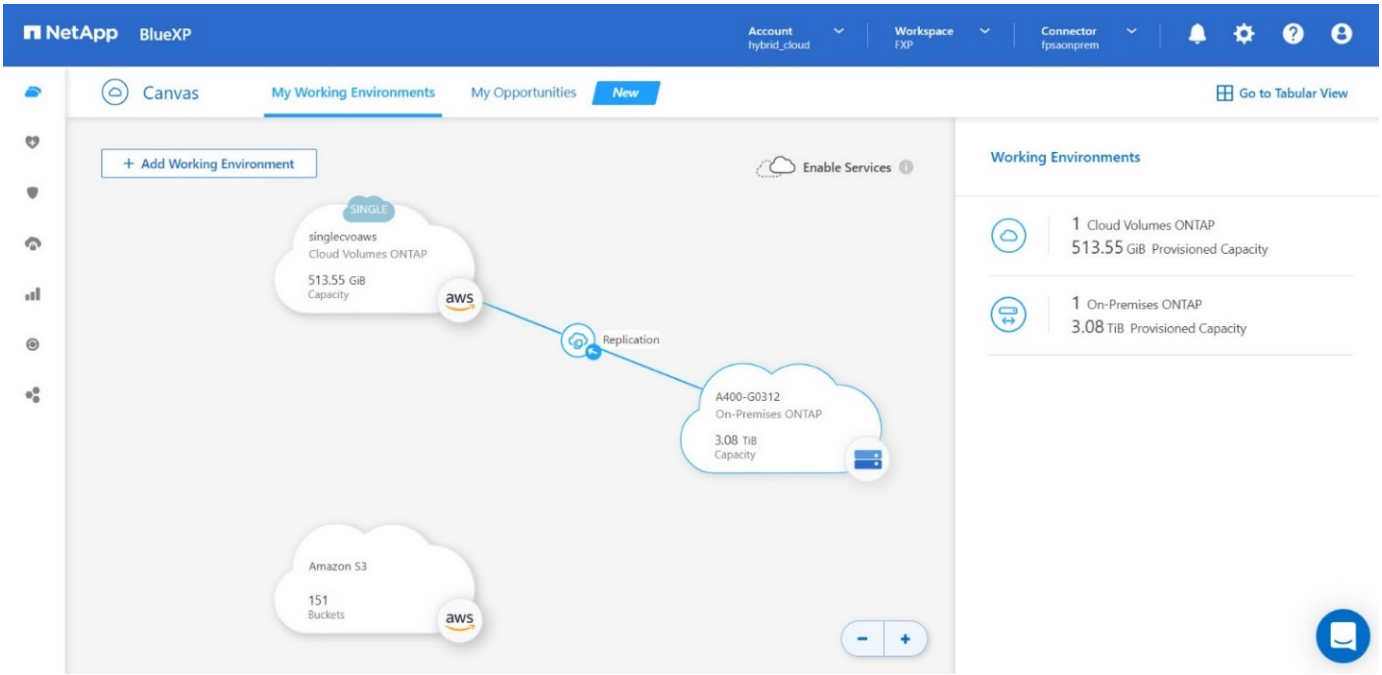


10. **Review.** Rivedi le tue selezioni e fai clic su **Go**.

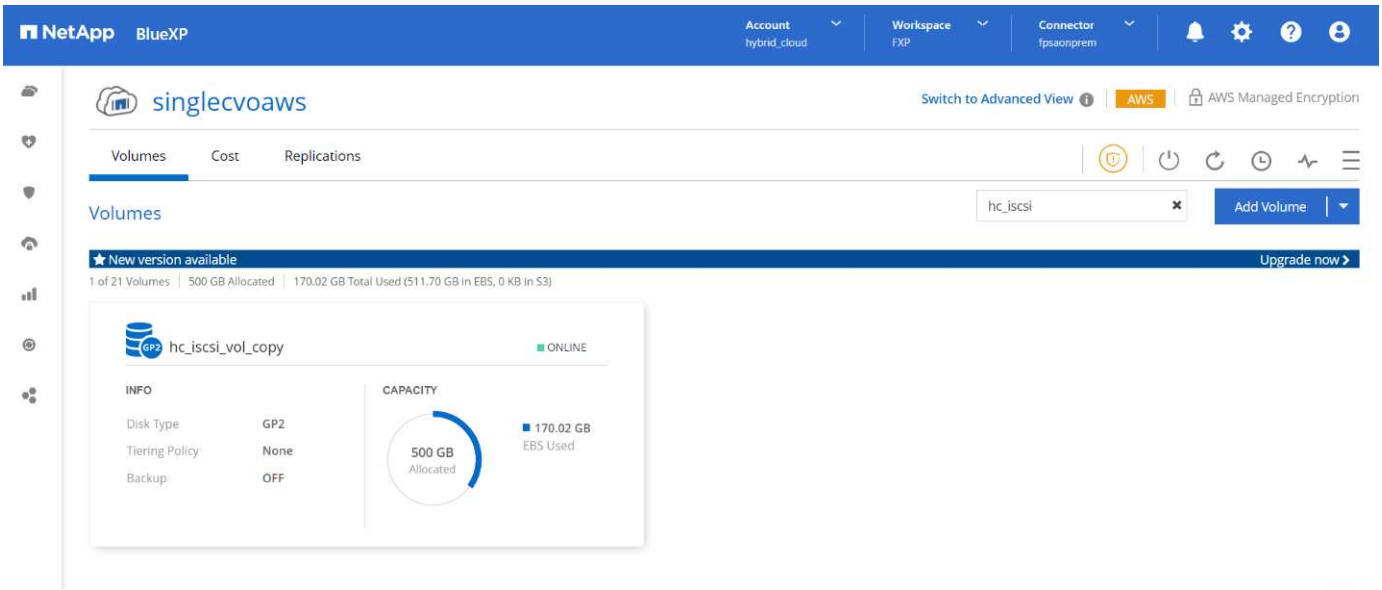


Per informazioni dettagliate su questi passaggi di configurazione, vedere "qui".

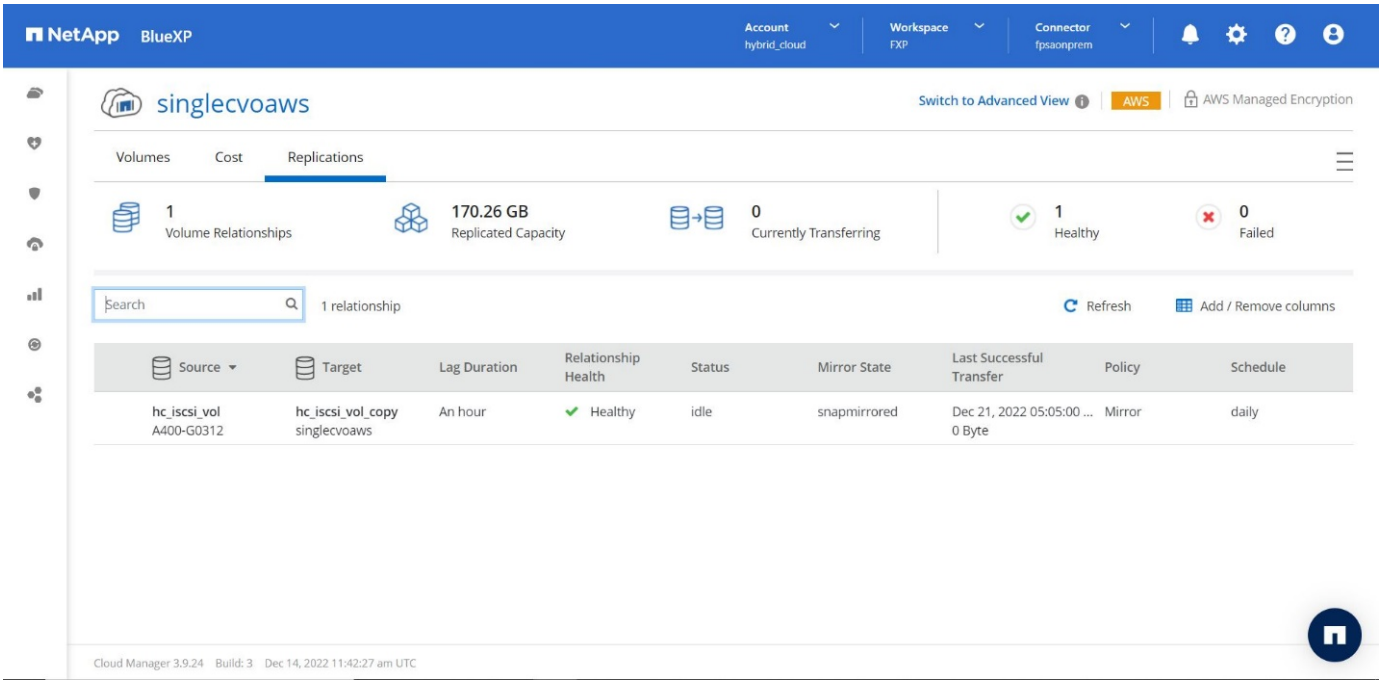
BlueXP avvia il processo di replica dei dati. A questo punto, è possibile visualizzare il servizio **Replication** stabilito tra il sistema ONTAP on-premise e Cloud Volumes ONTAP.



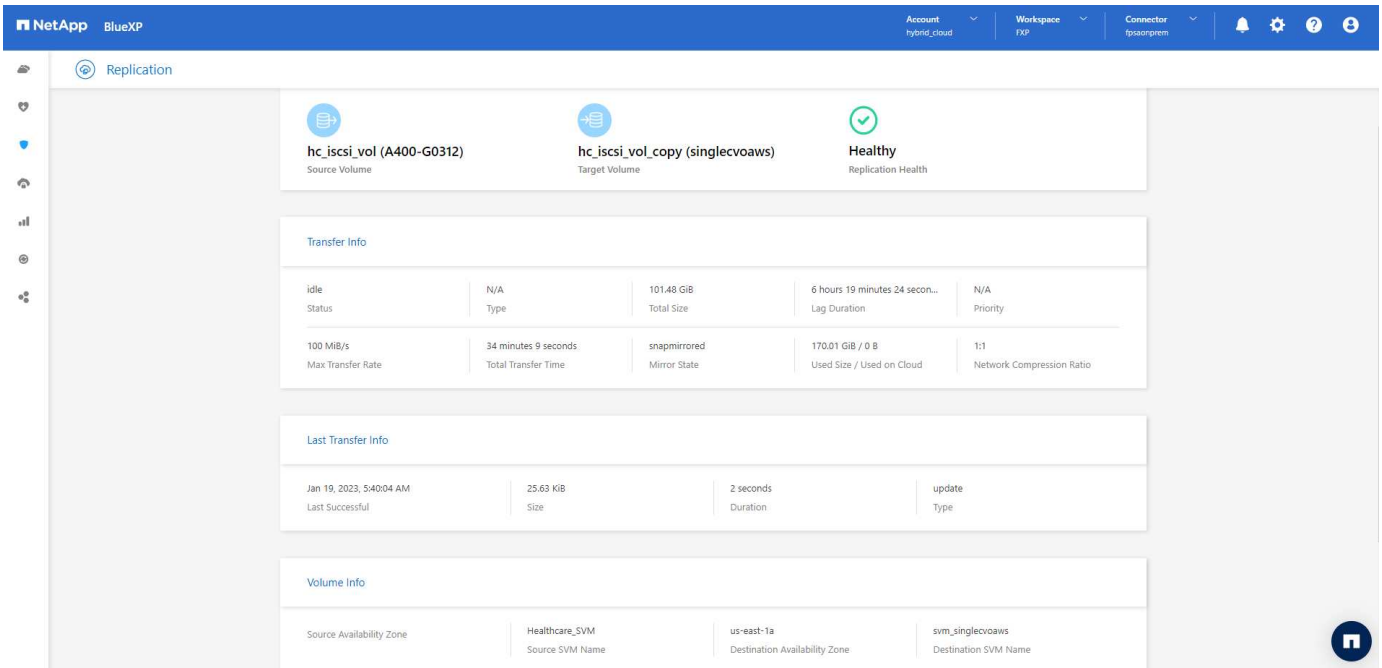
Nel cluster Cloud Volumes ONTAP, è possibile visualizzare il volume appena creato.



È inoltre possibile verificare che la relazione di SnapMirror sia stabilita tra il volume on-premise e il volume cloud.



Ulteriori informazioni sull'attività di replica sono disponibili nella scheda **Replication**.



"Successivo: Convalida della soluzione."

Convalida della soluzione

"Precedente: Configurazione SAN."

In questa sezione vengono esaminati alcuni casi di utilizzo della soluzione.

- Uno dei principali casi di utilizzo di SnapMirror è il backup dei dati. SnapMirror può essere utilizzato come strumento di backup primario replicando i dati all'interno dello stesso cluster o su destinazioni remote.
- Utilizzo dell'ambiente DR per eseguire test di sviluppo delle applicazioni (sviluppo/test).
- Dr in caso di disastro in produzione.
- Distribuzione dei dati e accesso remoto ai dati.

In particolare, i casi di utilizzo relativamente pochi validati in questa soluzione non rappresentano l'intera funzionalità della replica SnapMirror.

Sviluppo e test delle applicazioni (sviluppo/test)

Per accelerare lo sviluppo delle applicazioni, è possibile clonare rapidamente i dati replicati nel sito di DR e utilizzarli per lo sviluppo e il test delle applicazioni. La co-locazione degli ambienti di DR e di sviluppo/test può migliorare significativamente l'utilizzo delle strutture di backup o DR, mentre i cloni on-demand di sviluppo/test offrono il numero di copie di dati necessario per arrivare più rapidamente alla produzione.

La tecnologia FlexClone di NetApp consente di creare rapidamente una copia in lettura/scrittura di un volume FlexVol di destinazione SnapMirror nel caso in cui si desideri disporre dell'accesso in lettura/scrittura della copia secondaria per confermare la disponibilità di tutti i dati di produzione.

Completare i seguenti passaggi per utilizzare l'ambiente DR per eseguire lo sviluppo/test dell'applicazione:

1. Eseguire una copia dei dati di produzione. A tale scopo, eseguire un'istantanea applicativa di un volume on-premise. La creazione dello snapshot dell'applicazione prevede tre fasi: `Lock`, `Snap`, e. `Unlock`.

a. Interrompere il file system in modo che l'i/o venga sospeso e le applicazioni mantengano la coerenza. Qualsiasi applicazione scrive sul file system rimane in uno stato di attesa fino a quando non viene emesso il comando unquiesce nella fase c. I passaggi a, b e c vengono eseguiti attraverso un processo o un flusso di lavoro trasparente e che non influisce sullo SLA dell'applicazione.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

Questa opzione richiede il blocco del file system specificato in caso di nuove modifiche. Qualsiasi processo che tenta di scrivere nel file system bloccato viene bloccato fino a quando il file system non viene sbloccato.

b. Creare uno snapshot del volume on-premise.

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
hc_iscsi_vol -snapshot kamini
```

c. Riavviare i/o dal file system

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

Questa opzione viene utilizzata per sbloccare il file system e consentire il proseguimento delle operazioni. Tutte le modifiche al filesystem che sono state bloccate dal blocco vengono sbloccate e possono essere completate.

Lo snapshot coerente con l'applicazione può essere eseguito anche utilizzando NetApp SnapCenter, che ha l'orchestrazione completa del workflow descritto sopra come parte di SnapCenter. Per informazioni dettagliate, vedere "qui".

2. Eseguire un'operazione di aggiornamento di SnapMirror per mantenere sincronizzati i sistemi di produzione e DR.

```
singlecvoaws::> snapmirror update -destination-path
svm_singlecvoaws:hc_iscsi_vol_copy -source-path
Healthcare_SVM:hc_iscsi_vol

Operation is queued: snapmirror update of destination
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

È possibile eseguire un aggiornamento di SnapMirror anche tramite l'interfaccia utente grafica di BlueXP nella scheda **Replication**.

3. Creare un'istanza di FlexClone in base all'istantanea dell'applicazione acquisita in precedenza.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

Per l'attività precedente, è possibile creare anche una nuova snapshot, ma è necessario seguire le stesse procedure descritte in precedenza per garantire la coerenza dell'applicazione.

4. Attivare un volume FlexClone per visualizzare l'istanza EHR nel cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. Eseguire i seguenti comandi sull'istanza EHR nel cloud per accedere ai dati o al file system.
   a. Scopri lo storage ONTAP. Controllare lo stato del multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. Attivare il gruppo di volumi.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. Montare il file system e visualizzare il riepilogo delle informazioni sul file system.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

In questo modo è possibile utilizzare l'ambiente DR per lo sviluppo/test delle applicazioni. L'esecuzione di test/sviluppo dell'applicazione sullo storage DR consente di utilizzare più risorse che altrimenti potrebbero rimanere inattive per gran parte del tempo.

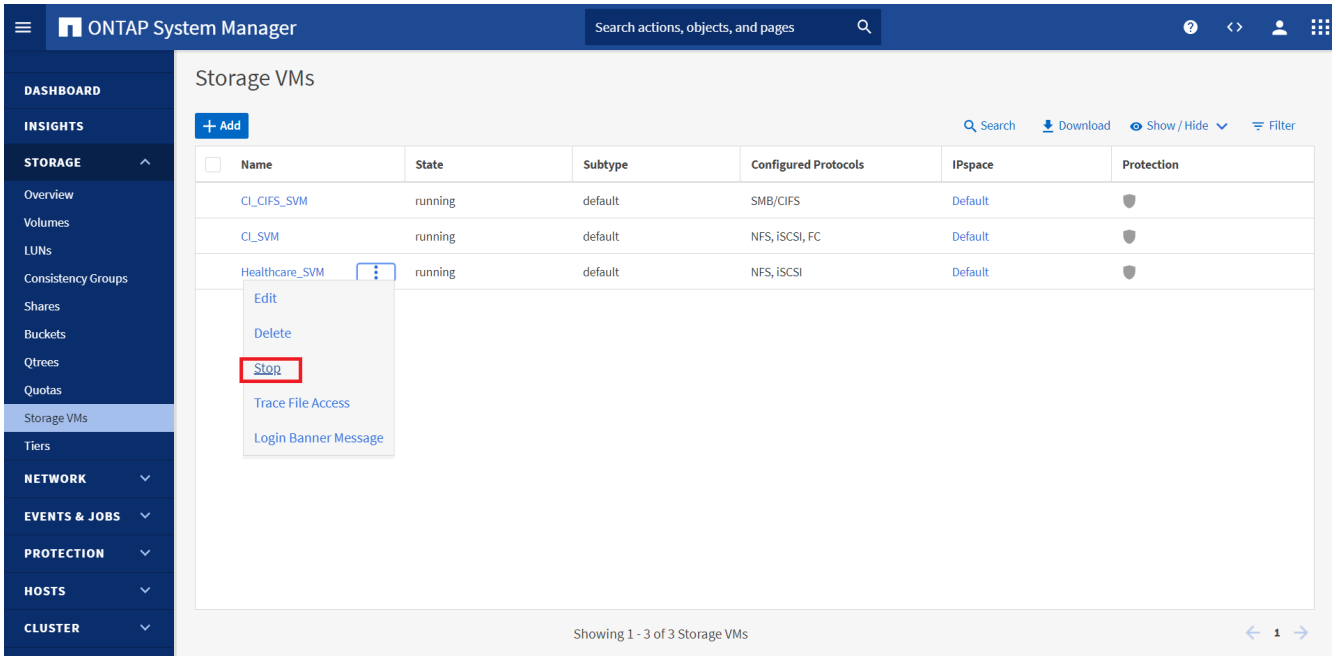
Disaster recovery

La tecnologia SnapMirror viene utilizzata anche come parte dei piani di DR. Se i dati critici vengono replicati in una posizione fisica diversa, un disastro grave non deve causare lunghi periodi di indisponibilità dei dati per le applicazioni business-critical. I client possono accedere ai dati replicati in rete fino al ripristino del sito di produzione da corruzione, eliminazione accidentale, disastro naturale e così via.

In caso di failback al sito primario, SnapMirror offre un mezzo efficiente per risincronizzare il sito DR con il sito primario, trasferendo solo i dati modificati o nuovi al sito primario dal sito DR semplicemente invertendo la relazione SnapMirror. Dopo che il sito di produzione primario riprende le normali operazioni applicative, SnapMirror continua il trasferimento al sito DR senza richiedere un altro trasferimento di riferimento.

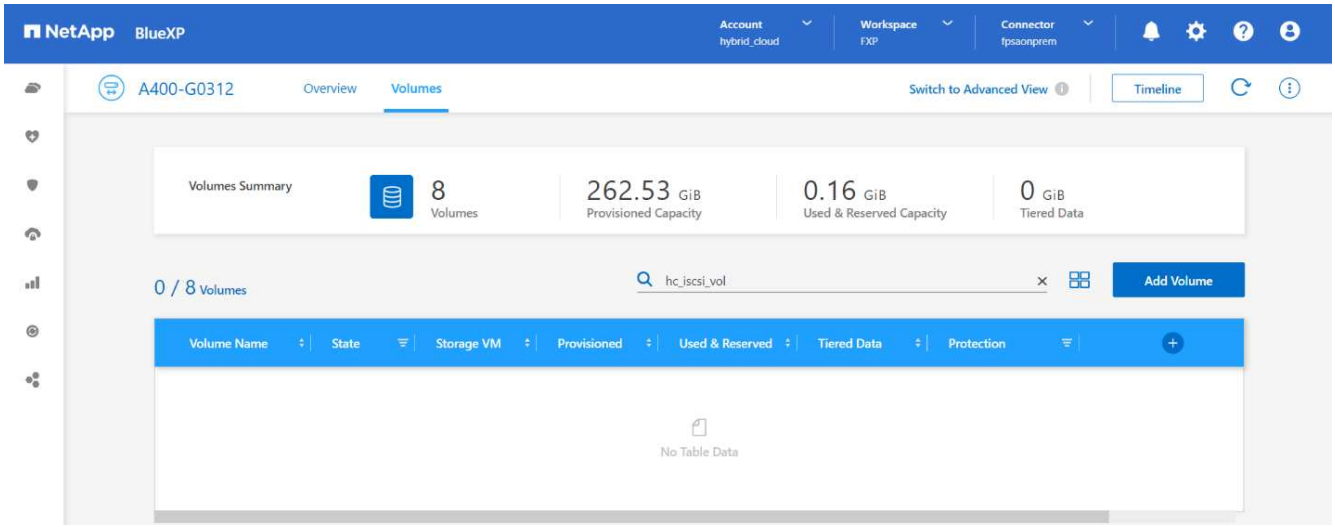
Per eseguire la convalida di uno scenario di disaster recovery corretto, attenersi alla seguente procedura:

1. Simulare un disastro sul lato di origine (produzione) arrestando la SVM che ospita il volume ONTAP on-premise (`hc_iscsi_vol`).



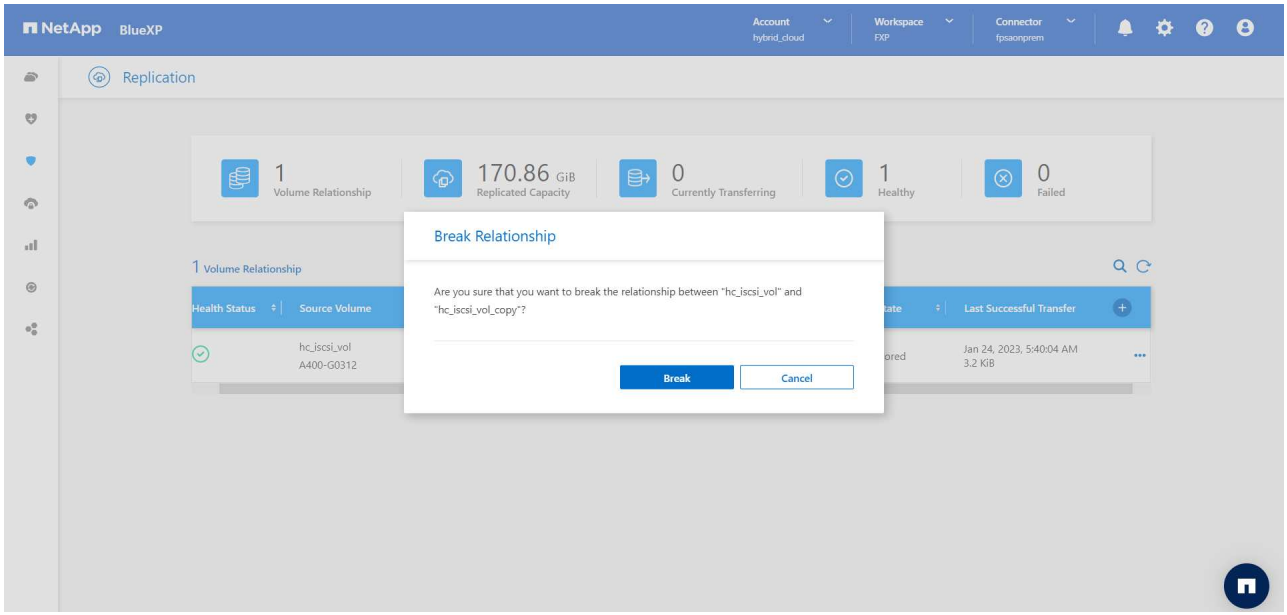
   Assicurarsi che la replica di SnapMirror sia già impostata tra ONTAP on-premise nell'istanza di FlexPod e Cloud Volumes ONTAP in AWS, in modo da poter creare snapshot delle applicazioni frequenti.

   Dopo l'arresto di SVM, il `hc_iscsi_vol` Il volume non è visibile in BlueXP.



2. Attivare DR in CVO.

   a. Interrompere la relazione di replica di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP e promuovere il volume di destinazione CVO (`hc_iscsi_vol_copy`) alla produzione.



   Una volta interrotta la relazione di SnapMirror, il tipo di volume di destinazione cambia da protezione dati (DP) a lettura/scrittura (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume             type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Attivare il volume di destinazione in Cloud Volumes ONTAP per visualizzare l'istanza EHR su un'istanza EC2 nel cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. Per accedere ai dati e al file system sull'istanza EHR nel cloud, individuare prima lo storage ONTAP e verificare lo stato del multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. Quindi attivare il gruppo di volumi.

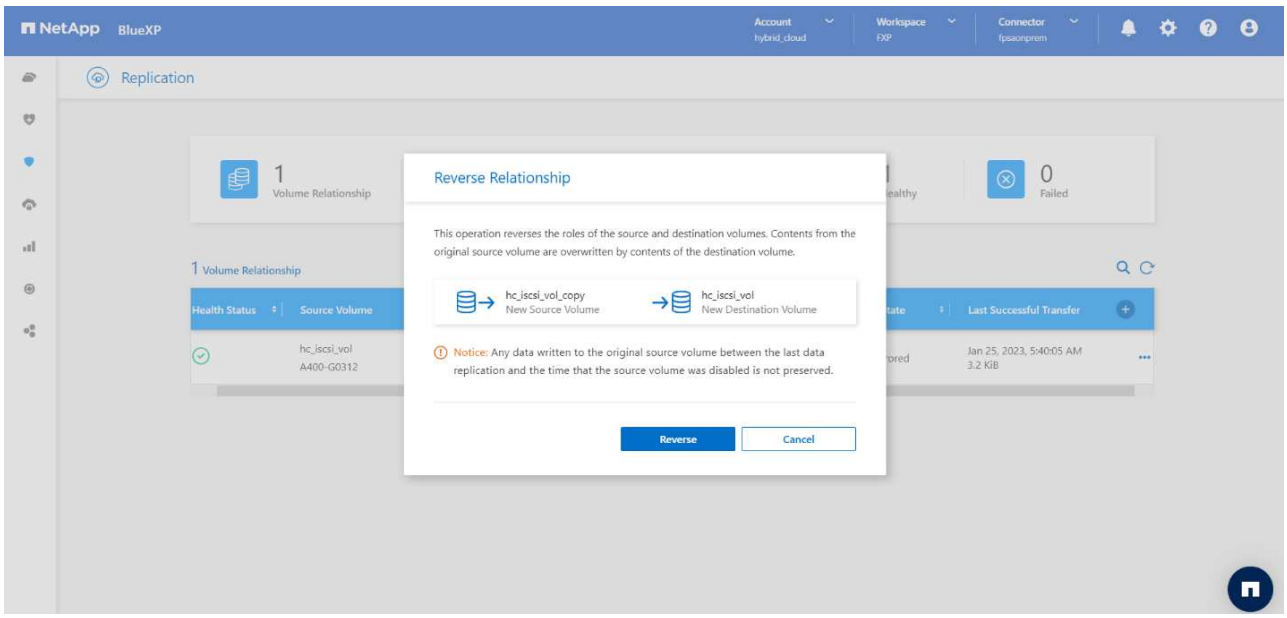
```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

e. Infine, montare il file system e visualizzare le informazioni sul file system.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                  1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

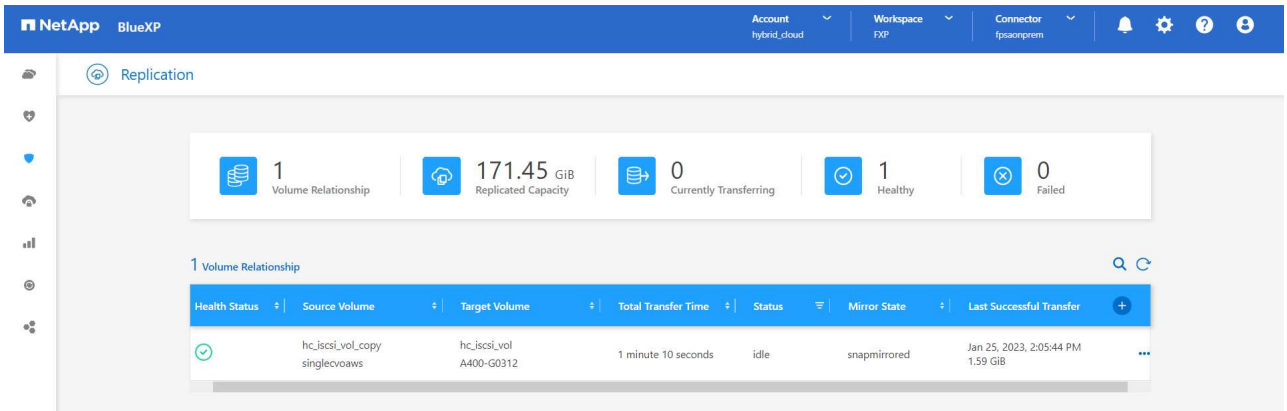
Questo output mostra che gli utenti possono accedere ai dati replicati attraverso la rete fino al ripristino del sito di produzione da un disastro.

f. Invertire la relazione di SnapMirror. Questa operazione inverte i ruoli dei volumi di origine e di destinazione.



Quando viene eseguita questa operazione, i contenuti del volume di origine originale vengono sovrascritti dai contenuti del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline.

Ora il volume CVO (`hc_iscsi_vol_copy`) diventa il volume di origine e il volume on-premise (`hc_iscsi_vol`) diventa il volume di destinazione.



Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.

a. Per verificare l'accesso in scrittura al volume CVO, creare un nuovo file sull'istanza EHR nel cloud.

```
cd /file1/
sudo touch newfile
```

Quando il sito di produzione non è attivo, i client possono comunque accedere ai dati ed eseguire operazioni di scrittura nel volume Cloud Volumes ONTAP, che ora è il volume di origine.

In caso di failback al sito primario, SnapMirror offre un mezzo efficiente per risincronizzare il sito DR con il sito primario, trasferendo solo i dati modificati o nuovi al sito primario dal sito DR semplicemente invertendo la relazione SnapMirror. Dopo che il sito di produzione primario riprende le normali operazioni applicative, SnapMirror continua il trasferimento al sito DR senza richiedere un altro trasferimento di riferimento.

In questa sezione viene illustrata la corretta risoluzione di uno scenario di disaster recovery quando il sito di produzione viene colpito da un disastro. I dati possono ora essere consumati in modo sicuro dalle applicazioni che possono ora servire i client mentre il sito di origine passa attraverso il ripristino.

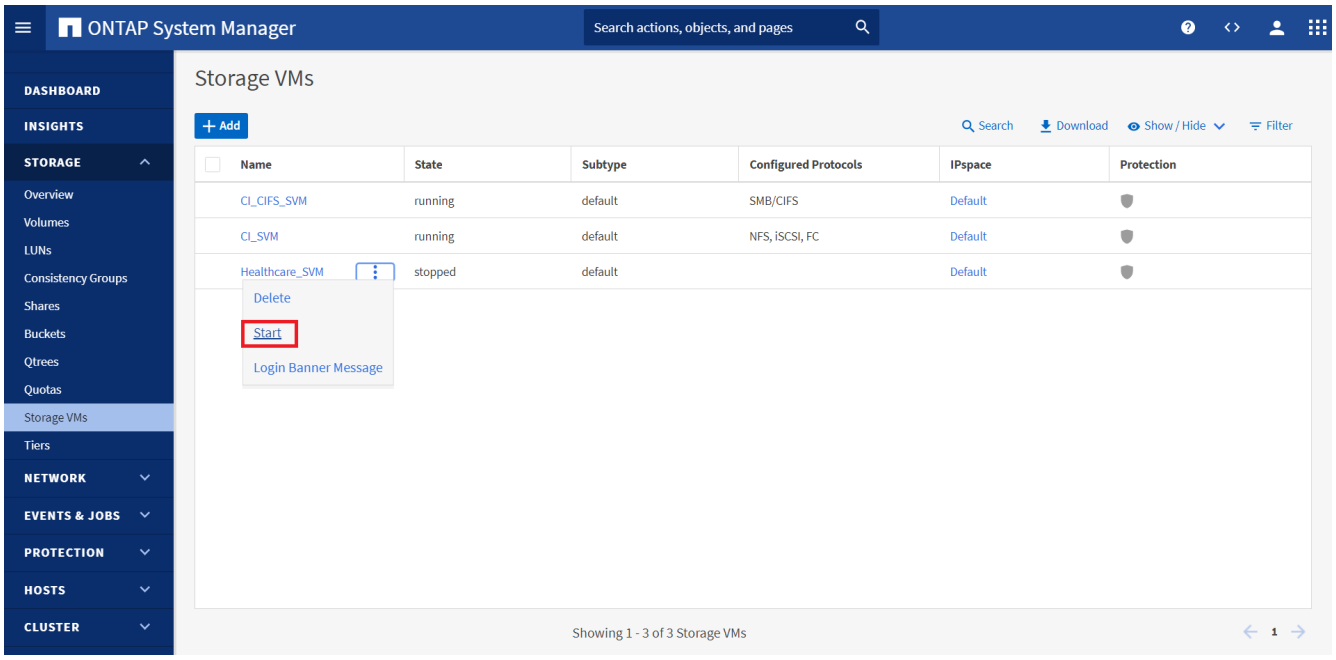
Verifica dei dati sul sito di produzione

Una volta ripristinato il sito di produzione, è necessario assicurarsi che la configurazione originale sia ripristinata e che i client siano in grado di accedere ai dati dal sito di origine.

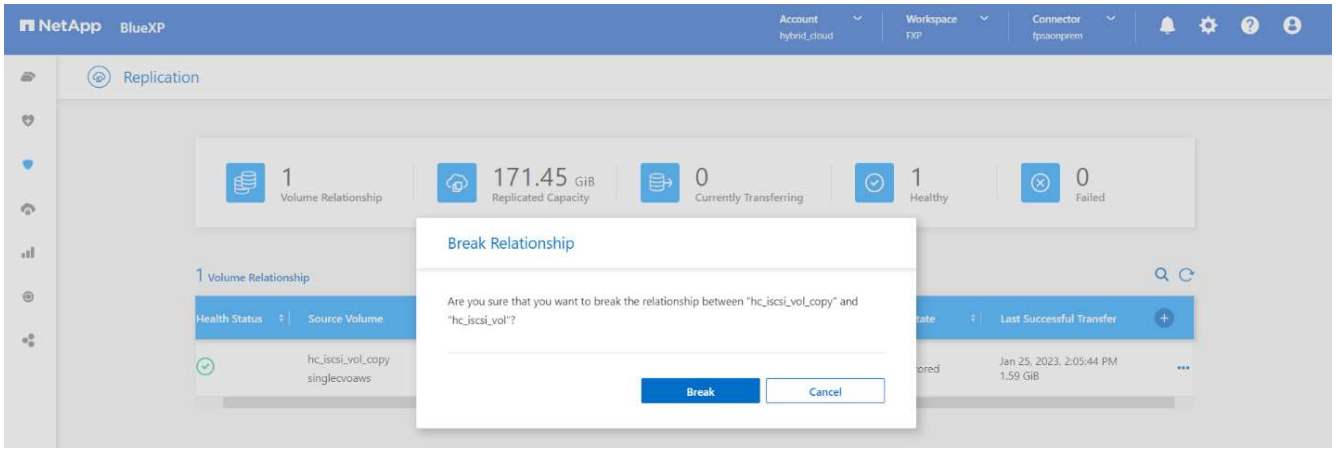
In questa sezione, parleremo di come attivare il sito di origine, ripristinare la relazione di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP e infine eseguire un controllo dell'integrità dei dati sul lato di origine

Per la verifica dei dati sul sito di produzione è possibile utilizzare la seguente procedura:

1. Assicurarsi che il sito di origine sia attivo. A tale scopo, avviare la SVM che ospita il volume ONTAP on-premise (`hc_iscsi_vol`).



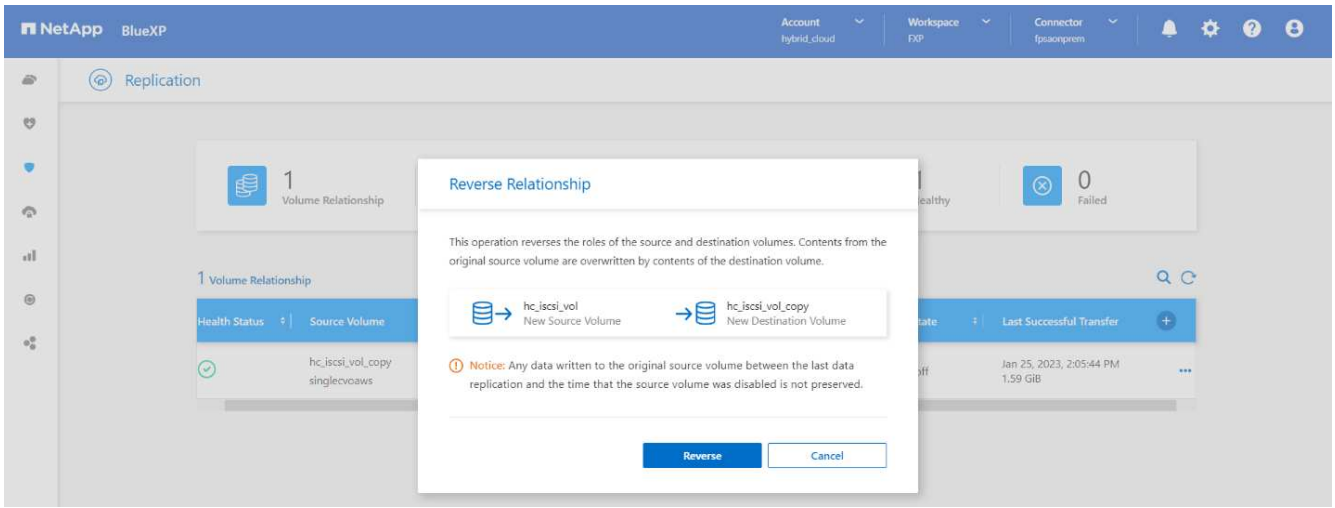
2. Interrompere la relazione di replica di SnapMirror tra Cloud Volumes ONTAP e ONTAP on-premise e promuovere il volume on-premise (`hc_iscsi_vol`) torna alla produzione.



Una volta interrotta la relazione di SnapMirror, il tipo di volume on-premise cambia da protezione dati (DP) a lettura/scrittura (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. Invertire la relazione di SnapMirror. Ora, il volume on-premise ONTAP (`hc_iscsi_vol`) Diventa il volume di origine e il volume Cloud Volumes ONTAP (`hc_iscsi_vol_copy`) diventa il volume di destinazione.



Seguendo questa procedura, la configurazione originale è stata ripristinata correttamente.

4. Riavviare l'istanza EHR on-premise. Montare il file system e verificare che `newfile` Esiste anche qui quello che hai creato sull'istanza EHR nel cloud quando la produzione era inattiva.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

Possiamo dedurre che la replica dei dati dall'origine alla destinazione è stata completata correttamente e che l'integrità dei dati è stata mantenuta. Questa operazione completa la verifica dei dati sul sito di produzione.

"Prossimo: Conclusione."

Conclusione

"Precedente: Convalida della soluzione."

La creazione di un cloud ibrido è un obiettivo per la maggior parte delle organizzazioni sanitarie di fornire la disponibilità dei dati in qualsiasi momento. In questa soluzione, abbiamo implementato una soluzione di cloud ibrido FlexPod con Cloud Volumes ONTAP, utilizzando la tecnologia di replica SnapMirror di NetApp per convalidare alcuni casi di utilizzo per il backup e il ripristino di applicazioni e carichi di lavoro nel settore sanitario.

FlexPod, un'infrastruttura convergente rigorosamente testata e prevalidata dalla partnership strategica di Cisco e NetApp, è progettata per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio offre elevati livelli di comfort EHR e, in ultima analisi, il miglior tempo di risposta per gli utenti del sistema EHR.

Con NetApp, puoi eseguire la produzione EHR, il disaster recovery, il backup o il tiering nel cloud proprio come faresti con le funzionalità di storage NetApp in un data center on-premise. Con NetApp Cloud Volumes ONTAP, NetApp offre le funzionalità di livello Enterprise e le performance necessarie per eseguire in modo efficace i servizi EHR nel cloud. Le opzioni cloud di NetApp offrono Block-over-iSCSI e file-over-NFS o SMB.

Questa soluzione soddisfa le esigenze delle organizzazioni sanitarie e consente loro di fare un passo verso la loro trasformazione digitale. Può anche aiutarli a gestire le applicazioni e i carichi di lavoro in modo efficiente.

"Avanti: Dove trovare ulteriori informazioni."

Dove trovare ulteriori informazioni

"Precedente: Conclusione."

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

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- Avvio rapido di Cloud Volumes ONTAP in AWS

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- Replica di SnapMirror

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928: Best practice NetApp per Epic

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693: Guida all'implementazione di FlexPod Datacenter per Epic EHR

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod per Epic

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- Tool di matrice di interoperabilità NetApp

  "http://support.netapp.com/matrix/"

- Cisco UCS hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guida alla compatibilità VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Marzo 2023	Versione iniziale

Cloud ibrido FlexPod per piattaforma cloud Google con NetApp Cloud Volumes ONTAP e Cisco Intersight

TR-4939: Cloud ibrido FlexPod per piattaforma cloud Google con NetApp Cloud Volumes ONTAP e Cisco Intersight

Ruchika Lahoti, NetApp

Introduzione

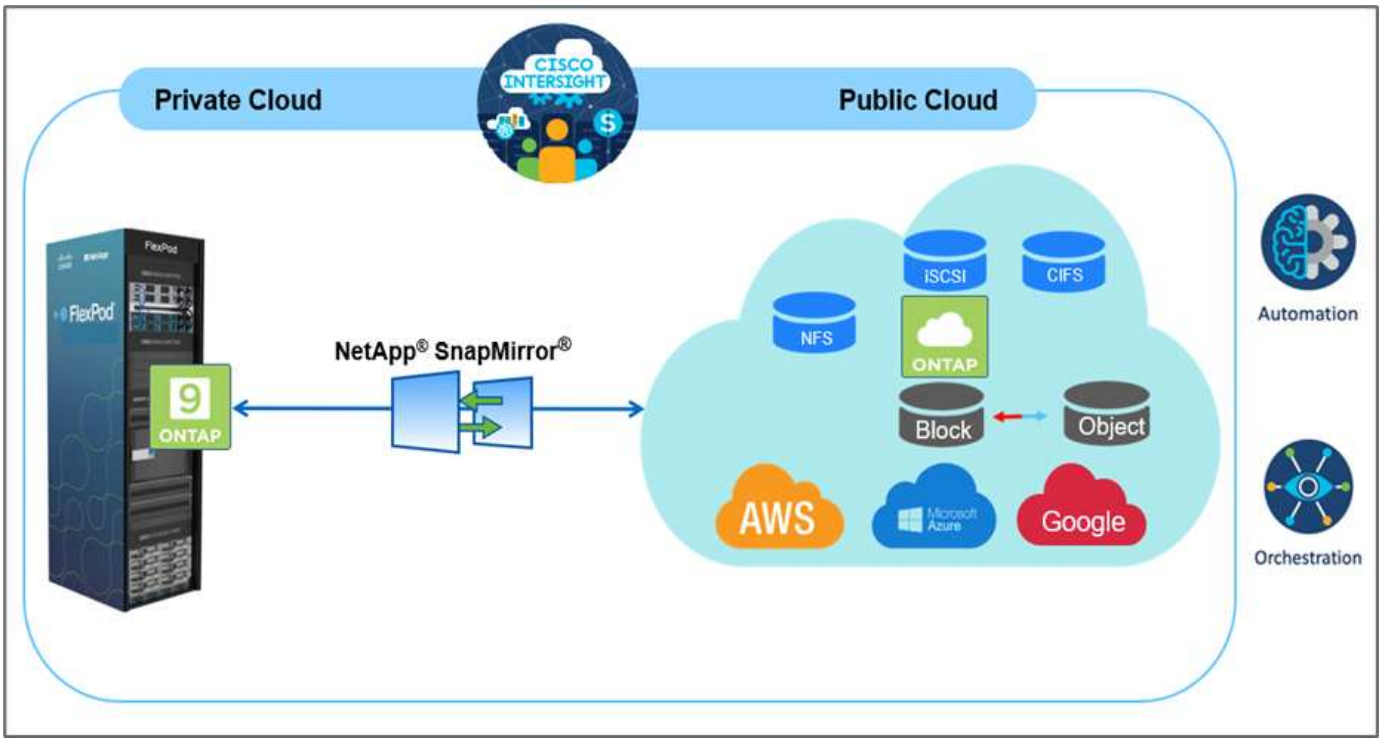
La protezione dei dati con il disaster recovery (DR) è un obiettivo critico per la business continuity. Il DR consente alle organizzazioni di eseguire il failover delle proprie operazioni di business in una posizione secondaria e di eseguire in seguito il ripristino e il failback sul sito primario in modo efficiente e affidabile. Diversi problemi, come disastri naturali, guasti di rete, vulnerabilità software ed errori umani, rendono lo sviluppo di una strategia di disaster recovery una priorità ASSOLUTA PER L'IT.

Per il DR, tutti i carichi di lavoro eseguiti sul sito primario devono essere riprodotti fedelmente sul sito DR. Un'organizzazione deve inoltre disporre di una copia aggiornata di tutti i dati aziendali, inclusi database, file service, storage NFS e iSCSI e così via. Poiché i dati nell'ambiente di produzione vengono costantemente aggiornati, le modifiche devono essere trasferite regolarmente al sito di DR.

L'implementazione di ambienti di disaster recovery è una sfida per la maggior parte delle organizzazioni a causa dei requisiti di indipendenza dell'infrastruttura e del sito. Il numero di risorse necessarie e i costi di configurazione, test e manutenzione di un data center secondario possono essere molto elevati, in genere avvicinandosi al costo dell'intero ambiente di produzione. È difficile mantenere un impatto minimo sui dati con una protezione adeguata, sincronizzando continuamente i dati e stabilendo un failover e un failback perfetti. Dopo aver creato il sito di DR, la sfida diventa replicare i dati dall'ambiente di produzione e mantenerli sincronizzati in futuro.

Questo report tecnico riunisce la soluzione di infrastruttura convergente FlexPod, NetApp Cloud Volumes ONTAP su Google Cloud e Cisco Intersight per formare un data center di cloud ibrido per il DR. In questa soluzione discuteremo della progettazione e dell'esecuzione di un workflow ONTAP on-premise utilizzando Cisco Intersight Cloud Orchestrator. Discutiamo inoltre dell'implementazione di NetApp Cloud Volumes ONTAP e dell'orchestrazione e dell'automazione della replica dei dati e del DR tra FlexPod e Cloud Volumes ONTAP utilizzando il servizio di interoperabilità Cisco per HashiCorp Terraform.

La figura seguente fornisce una panoramica della soluzione.



Questa soluzione offre diversi vantaggi, tra cui:

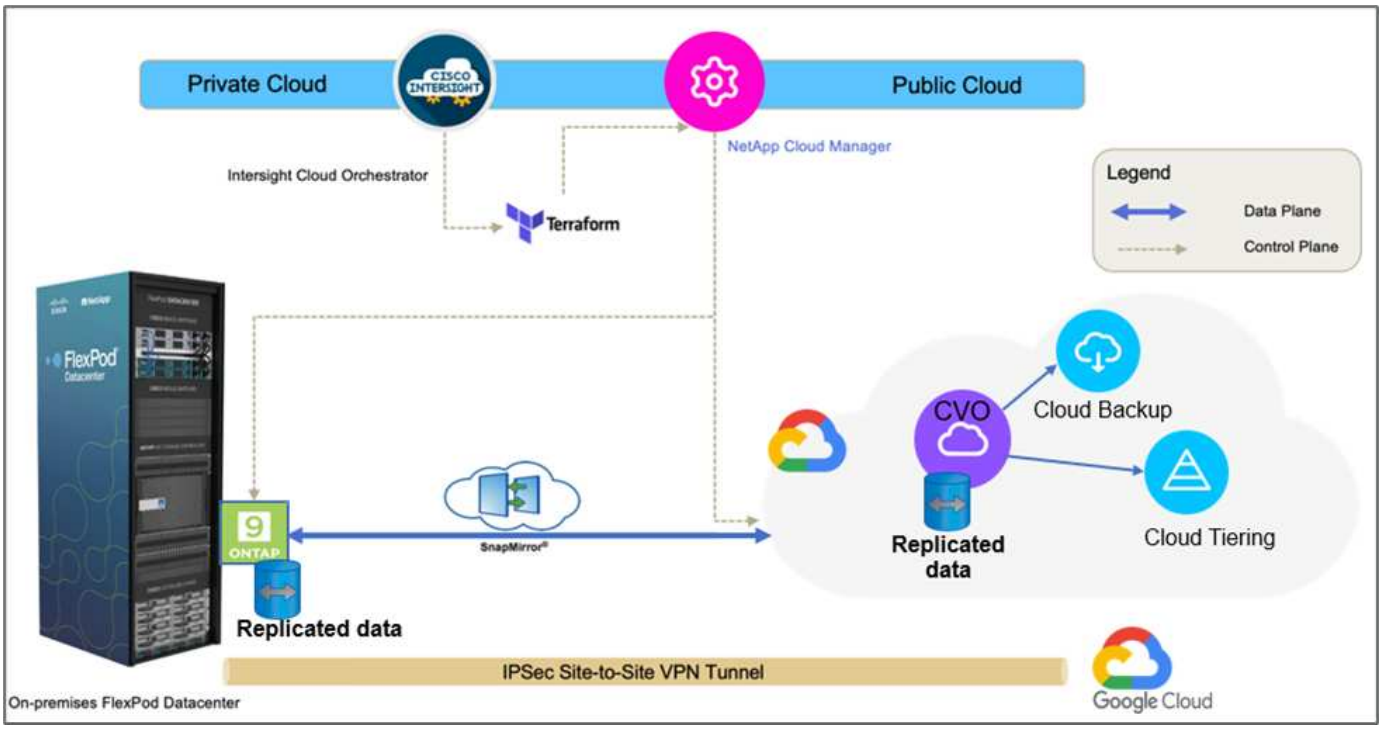
- **Orchestrazione e automazione.** Cisco Intersight semplifica le operazioni quotidiane dell'infrastruttura di cloud ibrido FlexPod fornendo framework di orchestrazione coerenti forniti tramite automazione.
- **Protezione personalizzata.** Cloud Volumes ONTAP offre replica dei dati a livello di blocco da ONTAP al cloud che mantiene aggiornata la destinazione attraverso aggiornamenti incrementali. Gli utenti possono specificare una pianificazione di sincronizzazione ogni 5 minuti o ogni ora, ad esempio, in base alle modifiche apportate all'origine che vengono trasferite.
- **Failover e failback perfetti.** in caso di disastro, gli amministratori dello storage possono eseguire rapidamente il failover sui volumi cloud. Quando il sito primario viene ripristinato, i nuovi dati creati nell'ambiente DR vengono sincronizzati di nuovo con i volumi di origine, ripristinando la replica dei dati secondari.
- **Efficienza:** lo spazio di storage e i costi per la copia del cloud secondario sono ottimizzati attraverso l'utilizzo di compressione dei dati, thin provisioning e deduplica. I dati vengono trasferiti a livello di blocco in forma compressa e deduplicata, migliorando la velocità di trasferimento. Inoltre, i dati vengono automaticamente suddivisi in livelli per lo storage a oggetti a basso costo e riportati allo storage dalle performance elevate solo quando si accede, ad esempio in uno scenario di DR. In questo modo si riducono significativamente i costi di storage in corso.
- **Aumento della produttività IT.** l'utilizzo di Intersight come singola piattaforma sicura e di livello Enterprise per la gestione del ciclo di vita dell'infrastruttura e delle applicazioni semplifica la gestione della configurazione e l'automazione delle attività manuali su larga scala per la soluzione.

Pubblico

I destinatari di questo documento includono, a titolo esemplificativo ma non esaustivo, tecnici di vendita, consulenti sul campo, servizi professionali, responsabili IT, Ingegneri partner, ingegneri dell'affidabilità del sito, architetti cloud, ingegneri cloud e clienti che vogliono sfruttare un'infrastruttura costruita per offrire efficienza IT e favorire l'innovazione IT.

Topologia della soluzione

In questa sezione viene descritta la topologia logica della soluzione. La figura seguente rappresenta la topologia della soluzione dell'ambiente FlexPod on-premise, NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud, Cisco Intersight e NetApp Cloud Manager.



I piani di controllo e i piani di dati sono chiaramente indicati tra gli endpoint. Il data plane utilizza una connessione VPN sicura da sito a sito per connettere l'istanza di ONTAP in esecuzione su FlexPod All Flash FAS all'istanza di NetApp Cloud Volumes ONTAP su Google Cloud.

La replica dei dati dei carichi di lavoro da FlexPod a NetApp Cloud Volumes ONTAP viene gestita da NetApp SnapMirror e il processo complessivo viene orchestrato utilizzando Cisco Intersight Cloud Orchestrator sia per gli ambienti on-premise che per gli ambienti cloud. Cisco Intersight Cloud Orchestrator utilizza i provider di risorse Terraform per NetApp Cloud Manager per eseguire operazioni relative all'implementazione di NetApp Cloud Volumes ONTAP e stabilire relazioni di replica dei dati.

> Questa soluzione supporta anche il backup opzionale e il tiering dei dati cold che risiedono nell'istanza di NetApp Cloud Volumes ONTAP su Google Cloud Storage.

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp ONTAP, networking Cisco Nexus, storage networking Cisco MDS e Cisco Unified Computing System (Cisco UCS). Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare

più configurazioni.

Cisco Intersight

Cisco Intersight è una piattaforma SaaS che offre automazione, osservabilità e ottimizzazione intelligenti per infrastrutture e applicazioni tradizionali e native del cloud. La piattaforma aiuta a promuovere il cambiamento con i team IT e offre un modello operativo progettato per il cloud ibrido. Cisco Intersight offre i seguenti vantaggi:

- **Delivery più rapida.** offerta come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può concentrarsi sull'accelerazione dell'erogazione per la linea di business.
- **Operazioni semplificate.** semplifica le operazioni utilizzando un unico tool sicuro fornito da SaaS con inventario, autenticazione e API comuni per lavorare nell'intero stack e in tutte le ubicazioni, eliminando i silos tra i team. Dalla gestione on-premise di server fisici e hypervisor a macchine virtuali, K8s, serverless, automazione, ottimizzazione e controllo dei costi su cloud pubblici e on-premise.
- **Ottimizzazione continua.** Ottimizza continuamente il tuo ambiente utilizzando l'intelligence fornita da Cisco Intersight su ogni livello e Cisco TAC. Questa intelligenza viene convertita in azioni consigliate e automatizzabili, in modo da poter adattare in tempo reale ad ogni cambiamento: Dallo spostamento dei carichi di lavoro al monitoraggio dello stato di salute dei server fisici ai consigli per la riduzione dei costi sui cloud pubblici con cui lavorate.

Cisco Intersight offre due modalità di gestione: UCSM Managed Mode (UMM) e Intersight Managed Mode (IMM). È possibile selezionare UMM o IMM nativi per i sistemi Cisco UCS collegati al fabric durante la configurazione iniziale delle interconnessioni fabric. In questa soluzione viene utilizzato IMM nativo.

Licenze Cisco Intersight

Cisco Intersight utilizza una licenza basata su abbonamento con più livelli.

I livelli di licenza Cisco Intersight sono i seguenti:

- **Cisco Intersight Essentials.** include tutte le funzionalità di base e le seguenti funzionalità:
  - Cisco UCS Central
  - Diritto a Cisco IMC Supervisor
  - Configurazione basata su policy con profili server
  - Gestione del firmware
  - Valutazione della compatibilità con l'elenco di compatibilità hardware (HCL)
- **Cisco Intersight Advantage.** include le funzionalità e le funzionalità del Tier Essentials oltre alle seguenti funzionalità:
  - Widget, inventario, capacità, funzionalità di utilizzo e correlazione dell'inventario tra domini tra calcolo fisico, rete, storage, virtualizzazione VMware e cloud pubblico AWS.
  - Servizio Cisco Security Advisory in cui i clienti possono ricevere importanti avvisi di sicurezza e avvisi sul campo relativi ai dispositivi endpoint interessati.
- **Cisco Intersight Premier.** oltre alle funzionalità offerte dal livello Advantage, Cisco Intersight Premier offre quanto segue:
  - Intersight Cloud Orchestrator (ICO) per Cisco e terze parti per calcolo, rete, storage, sistemi integrati, virtualizzazione, piattaforme container e cloud pubblico
  - Diritto di iscrizione completo per Cisco UCS Director senza costi aggiuntivi.

Ulteriori informazioni sulle licenze Intersight e sulle funzionalità supportate in ciascuna licenza sono disponibili "qui".

> In questa soluzione, utilizziamo Intersight Cloud Orchestrator e Intersight Service per HashiCorp Terraform. Queste funzionalità sono disponibili per gli utenti con licenza Intersight Premier, pertanto questo livello di licenza deve essere attivato.

Integrazione del cloud terraform con ICO

È possibile utilizzare Cisco Intersight Cloud Orchestrator (ICO) per creare ed eseguire flussi di lavoro che chiamano le API di Terraform Cloud (TFC). L'attività Invoke Web API Request supporta Terraform Cloud come destinazione e può essere configurata con le API di Terraform Cloud utilizzando i metodi HTTP. Pertanto, il flusso di lavoro può avere una combinazione di attività che richiama più API di Terraform Cloud utilizzando attività API generiche e altre operazioni. È necessaria una licenza Premier per utilizzare la funzione ICO.

Cisco Intersight Assist

Cisco Intersight Assist consente di aggiungere dispositivi endpoint a Cisco Intersight. Un data center potrebbe avere più dispositivi che non si connettono direttamente a Cisco Intersight. Qualsiasi dispositivo supportato da Cisco Intersight ma non connesso direttamente ad esso richiede un meccanismo di connessione. Cisco Intersight Assist offre questo meccanismo di connessione e consente di aggiungere dispositivi a Cisco Intersight.

Cisco Intersight Assist è disponibile all'interno di Cisco Intersight Virtual Appliance, che viene distribuita come macchina virtuale implementabile contenuta in un formato di file OVA (Open Virtual Appliance). È possibile installare l'appliance su un server ESXi. Per ulteriori informazioni, consultare "Cisco Intersight Virtual Appliance Getting Started Guide".

Dopo aver richiesto Intersight Assist a Intersight, puoi richiedere i dispositivi endpoint utilizzando l'opzione Claim Through Intersight Assist. Per ulteriori informazioni, vedere "Per iniziare".

NetApp Cloud Volumes ONTAP

- Utilizzo della deduplica dei dati integrata, della compressione dei dati, del thin provisioning e della clonazione per ridurre al minimo i costi dello storage.
- Affidabilità aziendale e operazioni continue in caso di guasti nel tuo ambiente cloud.
- Cloud Volumes ONTAP utilizza NetApp SnapMirror, la tecnologia di replica leader del settore, per replicare i dati on-premise nel cloud, in modo che sia facile disporre di copie secondarie per diversi casi di utilizzo.
- Cloud Volumes ONTAP si integra anche con Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.
- Passaggio tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.
- Coerenza delle copie Snapshot con NetApp SnapCenter.
- Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.
- L'integrazione con Cloud Data Sense ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

Cloud Central

Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi ti consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il

backup dei dati SaaS e migrare e controllare in modo efficace i dati su più cloud. Per ulteriori informazioni, vedere "Cloud Central".

Cloud Manager

Cloud Manager è una piattaforma di gestione di livello Enterprise basata su SaaS che consente agli esperti IT e agli architetti del cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud di NetApp. Fornisce un sistema centralizzato per la visualizzazione e la gestione dello storage on-premise e cloud per supportare più provider e account di cloud ibrido. Per ulteriori informazioni, vedere "Cloud Manager".

Connettore

Connector consente a Cloud Manager di gestire risorse e processi all'interno di un ambiente di cloud pubblico. Un'istanza di connettore è necessaria per utilizzare molte funzionalità fornite da Cloud Manager e può essere implementata nel cloud o nella rete on-premise. Il connettore è supportato nelle seguenti posizioni:

- AWS
- Microsoft Azure
- Google Cloud
- On-premise

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager consente di monitorare i cluster di storage ONTAP da un'unica interfaccia intuitiva, riprogettata, che offre intelligence basata su conoscenze della community e analytics ai. Fornisce informazioni complete su operazioni, performance e proattive sull'ambiente di storage e sulle macchine virtuali in esecuzione. Quando si verifica un problema con l'infrastruttura di storage, Unified Manager può notificare i dettagli del problema per identificare la causa principale. La dashboard della macchina virtuale offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter analizzare l'intero percorso di i/o dall'host vSphere fino alla rete e infine allo storage.

Alcuni eventi forniscono anche azioni correttive che è possibile intraprendere per risolvere il problema. È possibile configurare avvisi personalizzati per gli eventi in modo che, quando si verificano problemi, venga inviata una notifica tramite e-mail e trap SNMP. Active IQ Unified Manager consente di pianificare i requisiti di storage degli utenti prevedendo le tendenze di capacità e utilizzo per agire in modo proattivo prima che si verifichino problemi, evitando decisioni reattive a breve termine che possono portare a ulteriori problemi a lungo termine.

VMware vSphere

VMware vSphere è una piattaforma di virtualizzazione per la gestione olistica di grandi insiemi di infrastrutture (risorse tra cui CPU, storage e networking) come ambiente operativo perfetto, versatile e dinamico. A differenza dei sistemi operativi tradizionali che gestiscono un singolo computer, VMware vSphere aggrega l'infrastruttura di un intero data center per creare un singolo power house con risorse che possono essere allocate in modo rapido e dinamico a qualsiasi applicazione in necessità.

Per ulteriori informazioni su VMware vSphere, seguire "questo link".

VMware vSphere vCenter

VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da una singola console e aggrega il monitoraggio delle performance di cluster, host e macchine virtuali. VMware vCenter

Server offre agli amministratori una panoramica approfondita dello stato e della configurazione di cluster di calcolo, host, macchine virtuali, storage, sistema operativo guest, e altri componenti critici di un'infrastruttura virtuale. VMware vCenter gestisce l'insieme completo di funzionalità disponibili in un ambiente VMware vSphere.

Versioni hardware e software

Questa soluzione di cloud ibrido può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware, come definito nello strumento matrice di interoperabilità NetApp e nell'elenco di compatibilità hardware Cisco UCS.

La soluzione FlexPod utilizzata come piattaforma di riferimento nel nostro ambiente on-premise è stata implementata in base alle linee guida e alle specifiche descritte "qui".

La rete all'interno di questo ambiente è basata su ACI. Per ulteriori informazioni, vedere "qui".

- Per ulteriori informazioni, consultare i seguenti collegamenti:
- "Tool di matrice di interoperabilità NetApp"
- "Guida alla compatibilità VMware"
- "Cisco UCS hardware and Software Interoperability Tool"

La seguente tabella mostra le revisioni hardware e software di FlexPod.

Componente	Prodotto	Versione
Calcolo	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnects 6454	4.2(2a)
Rete	Cisco Nexus 9332C (colonna vertebrale)	14.2(7)
	Cisco Nexus 9336C-FX2 (Leaf)	14.2(7)
	Cisco ACI	4.2(7)
Storage	NetApp AFF A220	9.11.1
	Strumenti NetApp ONTAP per VMware vSphere	9.10
	NetApp NFS Plugin per VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Software	VSphere ESXi	7.0 (U3)
	Appliance VMware vCenter	7.0.3
	Appliance virtuale Cisco Intersight Assist	1.0.11-306

L'esecuzione delle configurazioni Terraform avviene sull'account Terraform Cloud for Business. La configurazione del terraform utilizza il provider Terraform per NetApp Cloud Manager.

La seguente tabella elenca i vendor, i prodotti e le versioni.

Componente	Prodotto	Versione
HashiCorp	Terraform	1.2.7

La seguente tabella mostra le versioni di Cloud Manager e Cloud Volumes ONTAP.

Componente	Prodotto	Versione
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"Pagina successiva: Installazione e configurazione - implementazione di FlexPod."

Installazione e configurazione

Implementare FlexPod

"Precedente: Componenti della soluzione."

Per informazioni dettagliate sulla progettazione e l'implementazione di FlexPod, inclusa la configurazione dei vari elementi di progettazione e le Best practice associate, vedere "Cisco Validated Design per FlexPod".

FlexPod può essere implementato sia in modalità gestita UCS che in modalità gestita Cisco Intersight. Se si sta implementando FlexPod in modalità gestita UCS, è possibile trovare la versione più recente di Cisco Validated Design "qui".

Cisco Unified Compute System (Cisco UCS) X-Series è un nuovissimo sistema di calcolo modulare, configurato e gestito dal cloud. È progettato per soddisfare le esigenze delle applicazioni moderne e per migliorare l'efficienza operativa, l'agilità e la scalabilità attraverso un design modulare adattabile, pronto al futuro. È possibile trovare le indicazioni di progettazione relative all'integrazione della piattaforma UCS X-Series gestita da Cisco Intersight nell'infrastruttura FlexPod "qui".

È possibile trovare FlexPod con implementazione Cisco ACI "qui".

"Pagina successiva: Configurazione di Cisco Intersight."

Configurazione di Cisco Intersight

"Precedente: Implementare FlexPod."

Per configurare Cisco Intersight e Intersight Assist, consultare il documento Cisco Validated Designs for FlexPod Found "qui".

"Pagina successiva: Integrazione del cloud terraform con prerequisito ICO."

Integrazione del cloud terraform con prerequisito ICO

"Precedente: Configurazione di Cisco Intersight."

Procedura 1: Connettere Cisco Intersight e Terraform Cloud

1. Richiedi o crea un target cloud Terraform fornendo i dettagli dell'account Terraform Cloud pertinente.
2. Creare un target di Terraform Cloud Agent per i cloud privati in modo che i clienti possano installare l'agente nel data center e abilitare la comunicazione con Terraform Cloud.

   Per ulteriori informazioni, seguire "questo link".

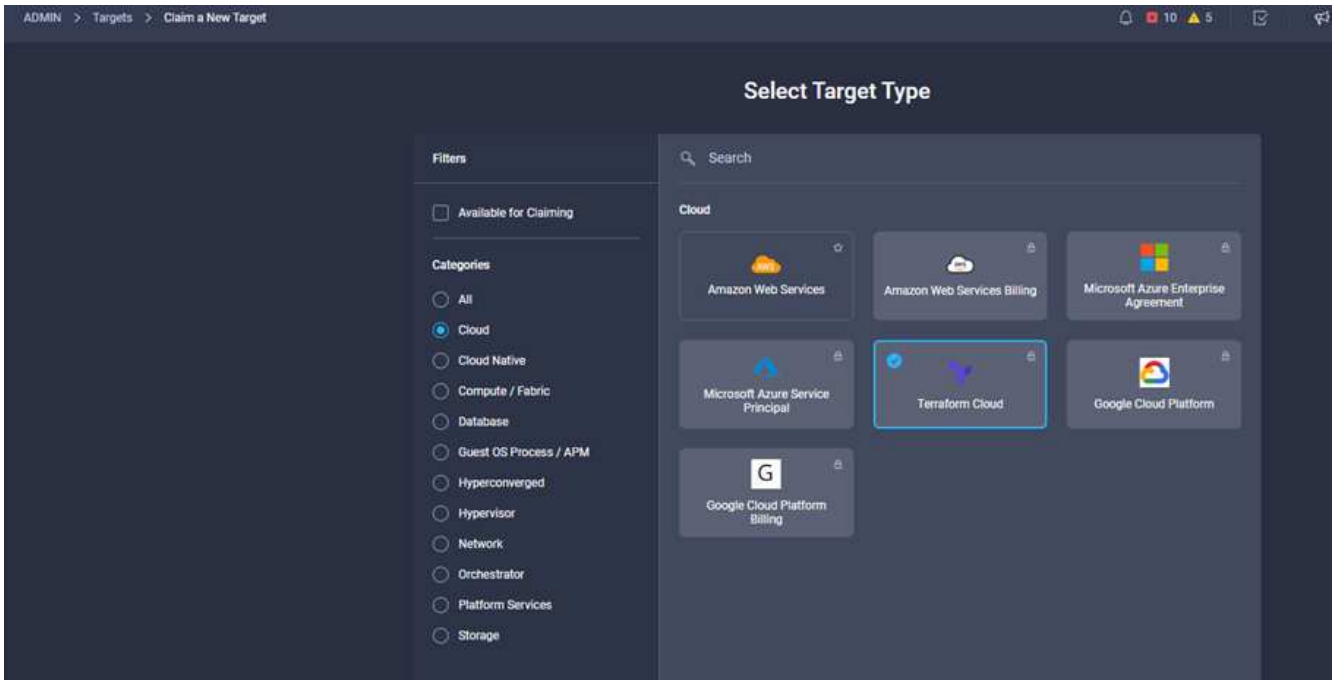
Procedura 2: Generazione del token utente

Come parte dell'aggiunta di una destinazione per Terraform Cloud, devi fornire il nome utente e il token API dalla pagina delle impostazioni di Terraform Cloud.

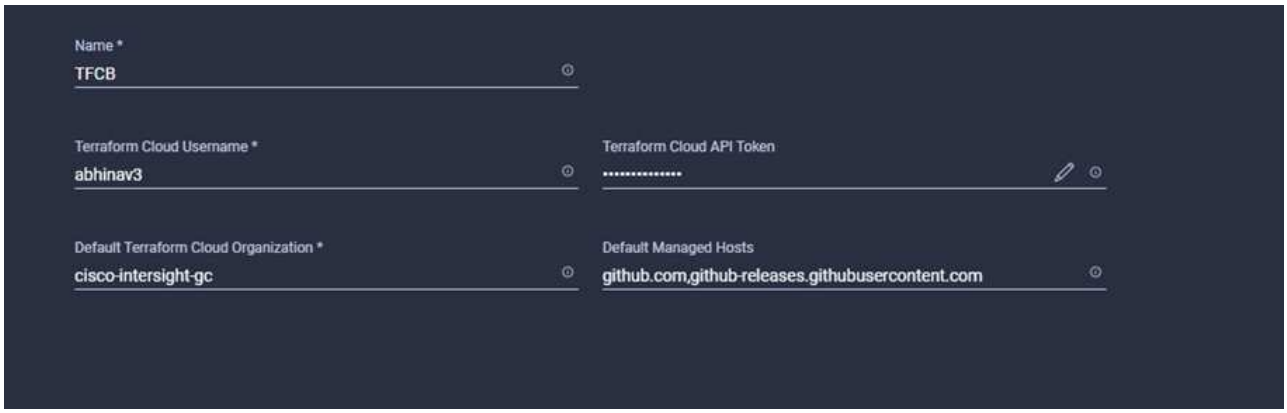
1. Accedi a Terraform Cloud e vai a **User Tokens**: "https://app.terraform.io/app/settings/tokens".
2. Fare clic su **Crea un nuovo token API**.
3. Assegnare un nome da ricordare e salvare il token in un luogo sicuro.

Procedura 3: Richiesta di rimborso del target cloud Terraform

1. Accedere a Intersight con i privilegi di account Administrator, Device Administrator o Device Technician.
2. Accedere a **ADMIN > Target > Richiedi un nuovo target**.
3. In **Categorie**, fare clic su **Cloud**.
4. Fare clic su **Terraform Cloud** e fare clic su **Start**.



5. Immettere un nome per la destinazione, il nome utente per Terraform Cloud, il token API e un'organizzazione predefinita in Terraform Cloud, come mostrato nell'immagine seguente.
6. Nel campo **Default Managed Hosts**, assicurarsi di aggiungere i seguenti collegamenti insieme ad altri host gestiti:
   - github.com
   - github-releases.githubusercontent.com



Se tutto viene inserito correttamente, il target di Terraform Cloud verrà visualizzato nella sezione **Intersight targets**.

Procedura 4: Aggiunta di agenti Terraform Cloud

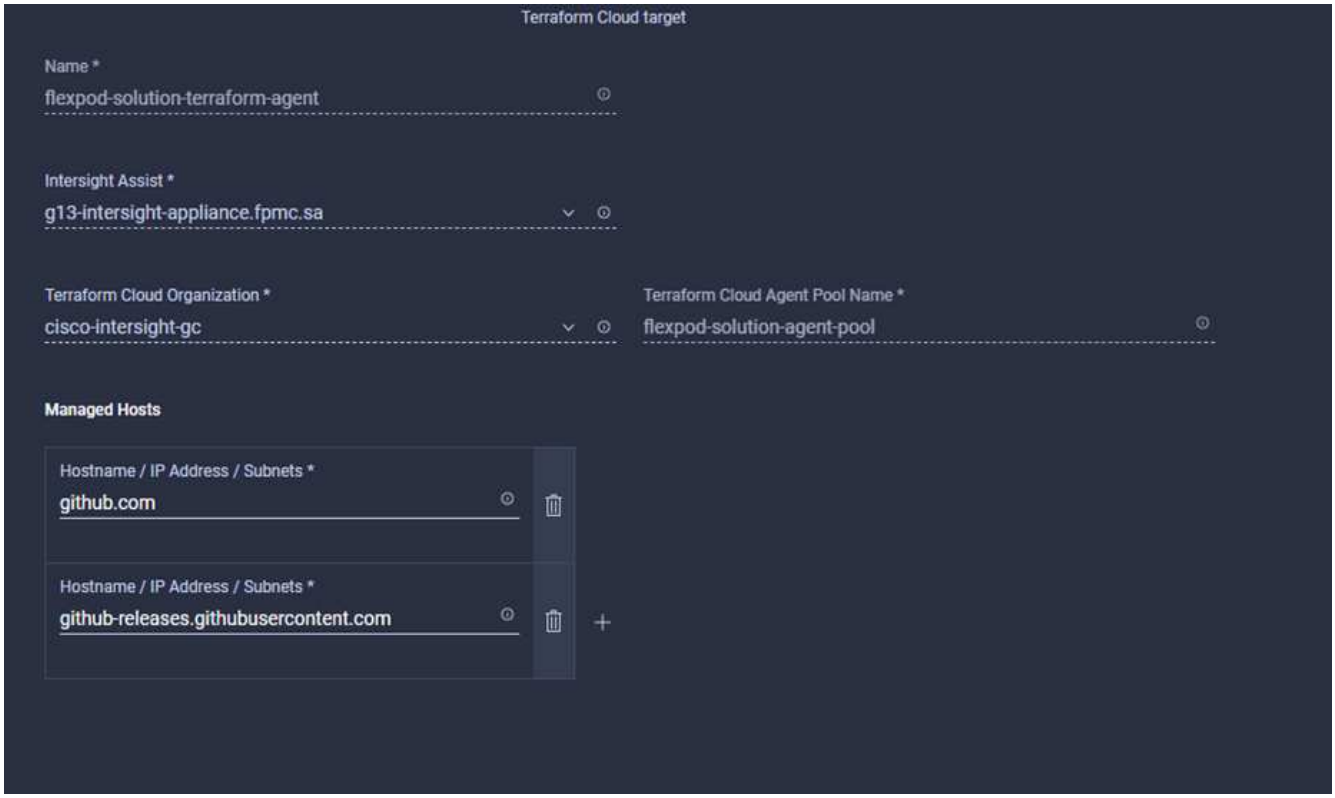
Prerequisiti:

- Destinazione di Terraform Cloud.
- Ha richiesto Intersight Assist in Intersight prima di implementare Terraform Cloud Agent.

> È possibile richiedere solo cinque agenti per ciascun Assist.

> Dopo aver creato la connessione a Terraform, è necessario eseguire lo spin up di un Terraform Agent per eseguire il codice Terraform.

1. Fare clic su **Claim Terraform Cloud Agent** dall'elenco a discesa della destinazione di Terraform Cloud.
2. Inserire i dettagli dell'agente Terraform Cloud. La seguente schermata mostra i dettagli di configurazione per l'agente Terraform.



È possibile aggiornare qualsiasi proprietà di Terraform Agent. Se la destinazione si trova nello stato **non connesso** e non si trova mai nello stato **connesso**, non è stato generato alcun token per l'agente Terraform.

Una volta completata la convalida dell'agente e generato un token, non è possibile riconfigurare l'organizzazione e/o il pool di agenti. La corretta implementazione di un agente Terraform è indicata dallo stato **connesso**.

Dopo aver attivato e richiesto l'integrazione di Terraform Cloud, puoi implementare uno o più agenti di Terraform Cloud in Cisco Intersight Assist. L'agente Terraform Cloud viene modellato come target figlio dell'obiettivo di Terraform Cloud. Quando si richiede l'obiettivo dell'agente, viene visualizzato un messaggio che indica che la richiesta di rimborso è in corso.

Dopo alcuni secondi, la destinazione viene spostata nello stato **connesso** e la piattaforma Intersight instrada i pacchetti HTTPS dall'agente al gateway Terraform Cloud.

Il tuo Agente Terraform deve essere correttamente richiesto e deve essere visualizzato sotto obiettivi come **connesso**.

"Avanti: Configurare il provider di servizi cloud pubblico."

Configurare il provider di servizi di cloud pubblico

"Precedente: Integrazione del cloud terraform con prerequisito ICO."

Procedura 1: Accesso a NetApp Cloud Manager

Per accedere a NetApp Cloud Manager e ad altri servizi cloud, devi iscriverti a. "NetApp Cloud Central".

Per configurare le aree di lavoro e gli utenti nell'account Cloud Central, fare clic su "qui".

Procedura 2: Implementare il connettore

Per implementare Connector in Google Cloud, consulta questa sezione "collegamento".

"Successivo: Implementazione automatica dello storage NetApp per il cloud ibrido."

Implementazione automatica dello storage NetApp per il cloud ibrido

"Precedente: Configurare il provider di servizi di cloud pubblico."

Google Cloud

È necessario innanzitutto abilitare le API e creare un account di servizio che fornisca a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP che si trovano nello stesso progetto del connettore o in progetti diversi.

Prima di implementare un connettore in un progetto Google Cloud, assicurarsi che il connettore non sia in esecuzione in sede o in un altro provider cloud.

Prima di implementare un connettore direttamente da Cloud Manager, è necessario disporre di due set di autorizzazioni:

- È necessario implementare Connector utilizzando un account Google che disponga delle autorizzazioni per avviare l'istanza di Connector VM da Cloud Manager.
- Durante l'implementazione di Connector, viene richiesto di selezionare l'istanza della macchina virtuale. Cloud Manager ottiene le autorizzazioni dall'account del servizio per creare e gestire i sistemi Cloud Volumes ONTAP per conto dell'utente. Le autorizzazioni vengono fornite allegando un ruolo personalizzato all'account del servizio.è necessario impostare due file YAML che includono le autorizzazioni richieste per l'utente e l'account del servizio. Scopri come utilizzare "I file YAML per impostare le autorizzazioni" qui.

Vedere "questo video dettagliato" per tutti i prerequisiti richiesti.

Architettura e modalità di implementazione di Cloud Volumes ONTAP

Cloud Volumes ONTAP è disponibile in Google Cloud come sistema a nodo singolo e come coppia di nodi ad alta disponibilità (ha). In base ai requisiti, possiamo scegliere la modalità di implementazione di Cloud Volumes ONTAP. L'aggiornamento di un sistema a nodo singolo a una coppia ha non è supportato. Se si desidera passare da un sistema a nodo singolo a una coppia ha, è necessario implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

Cloud Volumes ONTAP altamente disponibile in Google Cloud

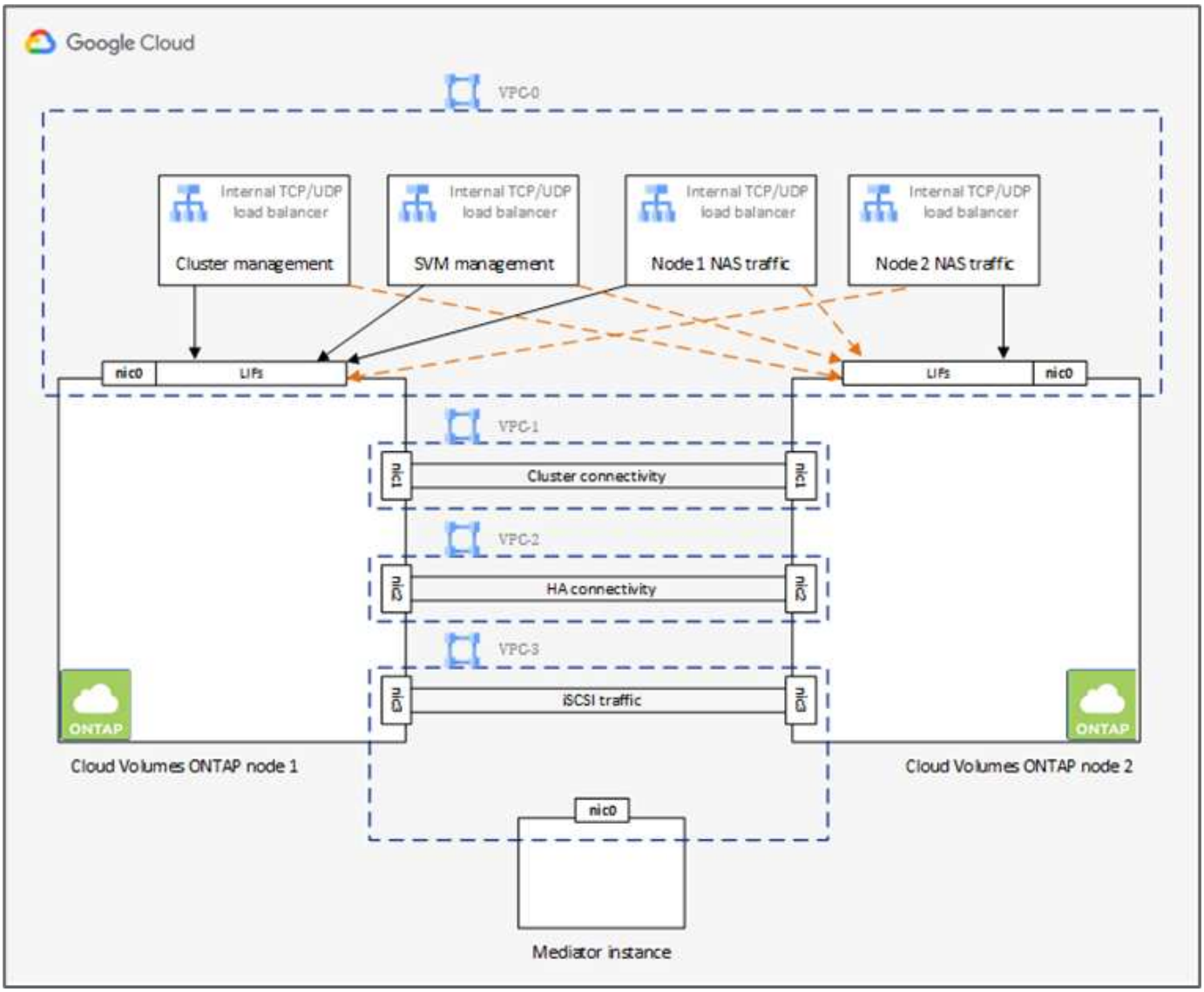
Google Cloud supporta l'implementazione di risorse in più aree geografiche e in più zone all'interno di una regione. L'implementazione ha è costituita da due nodi ONTAP che utilizzano potenti tipi di computer standard n1 o n2 disponibili in Google Cloud. I dati vengono replicati in modo sincrono tra i due nodi Cloud Volumes ONTAP per garantire la disponibilità in caso di guasto. L'implementazione HA di Cloud Volumes ONTAP richiede quattro VPC e una subnet privata in ciascun VPC. Le subnet dei quattro VPC devono essere dotate di intervalli CIDR non sovrapposti.

I quattro VPC vengono utilizzati per i seguenti scopi:

- VPC 0 consente la comunicazione in entrata ai nodi dati e Cloud Volumes ONTAP.

- VPC 1 offre connettività cluster tra nodi Cloud Volumes ONTAP.
- VPC 2 consente la replica RAM non volatile (NVRAM) tra i nodi.
- VPC 3 viene utilizzato per la connettività all'istanza del mediatore ha e per il traffico di replica del disco per le ricostruzioni dei nodi.

La seguente immagine mostra un Cloud Volumes ONTAP altamente disponibile in Goggle Cloud.



Per ulteriori informazioni, vedere "questo link".

Per i requisiti di rete per Cloud Volumes ONTAP in Google Cloud, consulta "questo link".

Per ulteriori informazioni sul tiering dei dati, vedere "questo link".

Impostare i prerequisiti dell'ambiente

La creazione automatica di cluster Cloud Volumes ONTAP, la configurazione di SnapMirror tra un volume on-premise e un volume cloud, la creazione di un volume cloud e così via vengono eseguite utilizzando la configurazione Terraform. Queste configurazioni Terraform sono ospitate su un account Terraform Cloud for Business. Utilizzando Intersight Cloud Orchestrator, puoi orchestrare attività come la creazione di un'area di lavoro in un account Terraform Cloud per Business, aggiungere tutte le variabili richieste all'area di lavoro,

eseguire un piano Terraform e così via.

Per queste attività di automazione e orchestrazione, sono necessari alcuni requisiti e dati, come descritto nelle sezioni seguenti.

Repository di GitHub

Devi disporre di un account GitHub per ospitare il tuo codice Terraform. Intersight Orchestrator crea un nuovo spazio di lavoro nell'account Terraform Cloud for Business. Questa area di lavoro è configurata con un flusso di lavoro di controllo della versione. A tale scopo, è necessario mantenere la configurazione Terraform in un repository GitHub e fornirla come input durante la creazione dello spazio di lavoro.

"Questo link GitHub" Fornisce la configurazione Terraform con diverse risorse. Puoi forare questo repository e fare una copia nel tuo account GitHub.

In questo repository, `provider.tf` Ha la definizione per il provider Terraform richiesto. Viene utilizzato il provider di terraform per NetApp Cloud Manager.

`variables.tf` contiene tutte le dichiarazioni variabili. Il valore di queste variabili viene immesso come input del workflow di Intersight Cloud Orchestrator. In questo modo è possibile passare i valori a un'area di lavoro ed eseguire la configurazione del Terraform.

`resources.tf` Definisce le varie risorse necessarie per aggiungere un ONTAP on-premise all'ambiente di lavoro, creare un cluster Cloud Volumes ONTAP a nodo singolo su Google Cloud, stabilire una relazione SnapMirror tra on-premise e Cloud Volumes ONTAP, creare un volume cloud su Cloud Volumes ONTAP e così via.

In questo repository:

- `provider.tf` Ha NetApp Cloud Manager come definizione per il Terraform provider richiesto.
- `variables.tf` Contiene le dichiarazioni variabili utilizzate come input per il flusso di lavoro di Intersight Cloud Orchestrator. In questo modo è possibile passare i valori all'area di lavoro ed eseguire la configurazione Terraform.
- `resources.tf` Definisce varie risorse per aggiungere un ONTAP on-premise all'ambiente di lavoro, creare un cluster Cloud Volumes ONTAP a nodo singolo su Google Cloud, stabilire una relazione SnapMirror tra on-premise e Cloud Volumes ONTAP, creare un volume cloud su Cloud Volumes ONTAP e così via.

È possibile aggiungere un ulteriore blocco di risorse per creare più volumi su Cloud Volumes ONTAP o utilizzare il conteggio o. `for_each` Costrutti di terraform.

Per connettere spazi di lavoro, moduli e set di policy Terraform a repository contenenti configurazioni Terraform, Terraform Cloud deve accedere al tuo repo GitHub.

Se si aggiunge un client, l'ID token OAuth del client viene utilizzato come input del flusso di lavoro di Intersight Cloud Orchestrator.

1. Accedi al tuo account Terraform Cloud per Business. Selezionare **Impostazioni > Provider**.
2. Fare clic su **Aggiungi un provider VCS**.
3. Selezionare la versione.
4. Seguire la procedura sotto **Configura provider**.
5. Il client aggiunto viene visualizzato in **VCS Providers**. Prendere nota dell'ID token OAuth.

Token di refresh per le operazioni API di NetApp Cloud Manager

Oltre all'interfaccia del browser Web, Cloud Manager dispone di un'API REST che fornisce agli sviluppatori software l'accesso diretto alla funzionalità Cloud Manager attraverso l'interfaccia SaaS. Il servizio Cloud Manager è costituito da diversi componenti distinti che formano collettivamente una piattaforma di sviluppo estensibile. Il token refresh consente di generare token di accesso che si aggiungono all'intestazione Authorization per ogni chiamata API.

Senza chiamare direttamente un'API, il provider netapp-cloudmanager utilizza un token di refresh e traduce le risorse Terraform in corrispondenti chiamate API. Devi generare un token di refresh per le operazioni API di NetApp Cloud Manager da "NetApp Cloud Central".

Per creare risorse su Cloud Manager, ad esempio la creazione di un cluster Cloud Volumes ONTAP, la configurazione di SnapMirror e così via, è necessario disporre dell'ID client di Cloud Manager Connector.

1. Accedi a Cloud Manager: "https://cloudmanager.netapp.com/".
2. Fare clic su **Connector** (connettore).
3. Fare clic su **Gestisci connettori**.
4. Fare clic sui puntini di sospensione e copiare l'ID del connettore.

Sviluppare il workflow di Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator è disponibile in Cisco Intersight se:

- È stata installata la licenza Intersight Premier.
- Sei un amministratore dell'account, un amministratore dello storage, un amministratore della virtualizzazione o un amministratore del server e hai almeno un server assegnato.

Progettazione workflow

Workflow Designer consente di creare nuovi flussi di lavoro (oltre a attività e tipi di dati) e modificare i flussi di lavoro esistenti per gestire le destinazioni in Cisco Intersight.

Per avviare Workflow Designer, accedere a **Orchestration > Workflow**. Una dashboard visualizza i seguenti dettagli nelle schede **My workflow**, **Sample workflow** e **All workflow**:

- Stato di convalida
- Ultimo stato di esecuzione
- Flussi di lavoro principali in base al numero di esecuzioni
- Categorie principali di flussi di lavoro
- Numero di flussi di lavoro definiti dal sistema
- Flussi di lavoro principali in base alle destinazioni

Utilizzando la dashboard, è possibile creare, modificare, clonare o eliminare una scheda. Per creare una scheda di visualizzazione personalizzata, fare clic su **+**, specificare un nome, quindi selezionare i parametri necessari da visualizzare nelle colonne, nelle colonne dei tag e nei widget. È possibile rinominare una scheda se non presenta l'icona **Lock**.

Sotto la dashboard è presente un elenco tabulare di flussi di lavoro che visualizza le seguenti informazioni:

- Nome visualizzato

- Descrizione
- Definito dal sistema
- Versione predefinita
- Esecuzioni
- Ultimo stato di esecuzione
- Stato di convalida
- Ultimo aggiornamento
- Organizzazione

La colonna Actions (azioni) consente di eseguire le seguenti azioni:

- **Esegui.** esegue il flusso di lavoro.
- **History.** Visualizza la cronologia di esecuzione del workflow.
- **Gestisci versioni.** Crea e gestisci le versioni per i flussi di lavoro.
- **Delete.** Elimina un flusso di lavoro.
- **Riprova.** Riprovare un flusso di lavoro non riuscito.

Workflow

Creare un flusso di lavoro composto dai seguenti passaggi:

- **Definizione di un flusso di lavoro.** specificare il nome visualizzato, la descrizione e altri attributi importanti.
- **Definire gli input e gli output del workflow.** specificare quali parametri di input sono obbligatori per l'esecuzione del workflow e gli output generati al momento dell'esecuzione
- **Aggiungi attività di workflow.** Aggiungi una o più attività di workflow in Workflow Designer che sono necessarie al workflow per svolgere la sua funzione.
- *Convalidare il flusso di lavoro. *Convalidare un workflow per garantire che non ci siano errori nella connessione degli input e output delle attività.

Creazione di flussi di lavoro per lo storage FlexPod on-premise

Per configurare un flusso di lavoro per lo storage FlexPod on-premise, vedere "questo link".

"Segue: Workflow di DR."

Workflow di DR

"Precedente: Implementazione automatica dello storage NetApp per il cloud ibrido."

La sequenza delle fasi è la seguente:

1. Definire il flusso di lavoro.
    - Creare un nome breve e intuitivo per il flusso di lavoro, ad esempio Disaster Recovery Workflow.
2. Definire l'input del flusso di lavoro. Gli input che prendiamo per questo flusso di lavoro includono quanto segue:

- Opzioni del volume (nome del volume, percorso di montaggio)
- Capacità del volume
- Data center associato al nuovo datastore
- Cluster su cui è ospitato il datastore
- Nome del nuovo datastore da creare in vCenter
- Tipo e versione del nuovo datastore
- Nome dell'organizzazione Terraform
- Spazio di lavoro terraform
- Descrizione dell'area di lavoro Terraform
- Variabili (sensibili e non sensibili) richieste per eseguire la configurazione Terraform
- Motivo dell'avvio del piano

3. Aggiungere le attività del flusso di lavoro.

   Le attività correlate alle operazioni in FlexPod includono quanto segue:

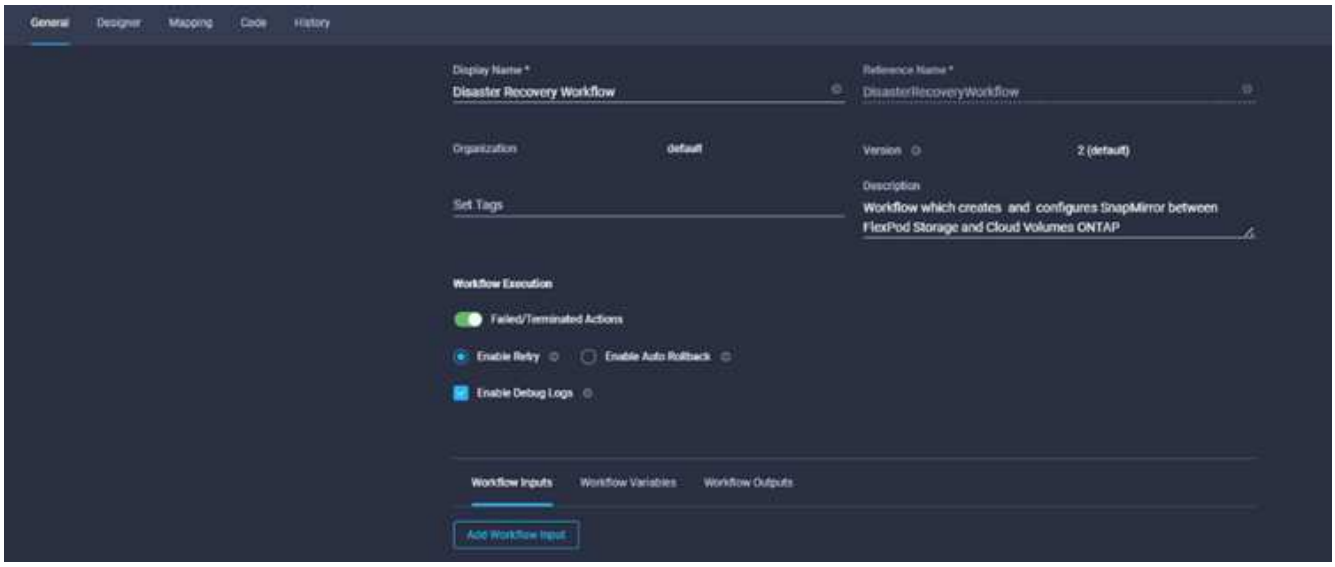
   - Creare un volume in FlexPod.
   - Aggiungere il criterio di esportazione dello storage al volume creato.
   - Mappare il volume appena creato su un datastore in VMware vCenter.

     Le attività relative alla creazione del cluster Cloud Volumes ONTAP:

   - Aggiungi spazio di lavoro Terraform
   - Aggiungere variabili terraform
   - Aggiungere variabili sensibili al terraform
   - Avvia un nuovo piano Terraform
   - Confermare l'esecuzione di Terraform
4. Validare il workflow.

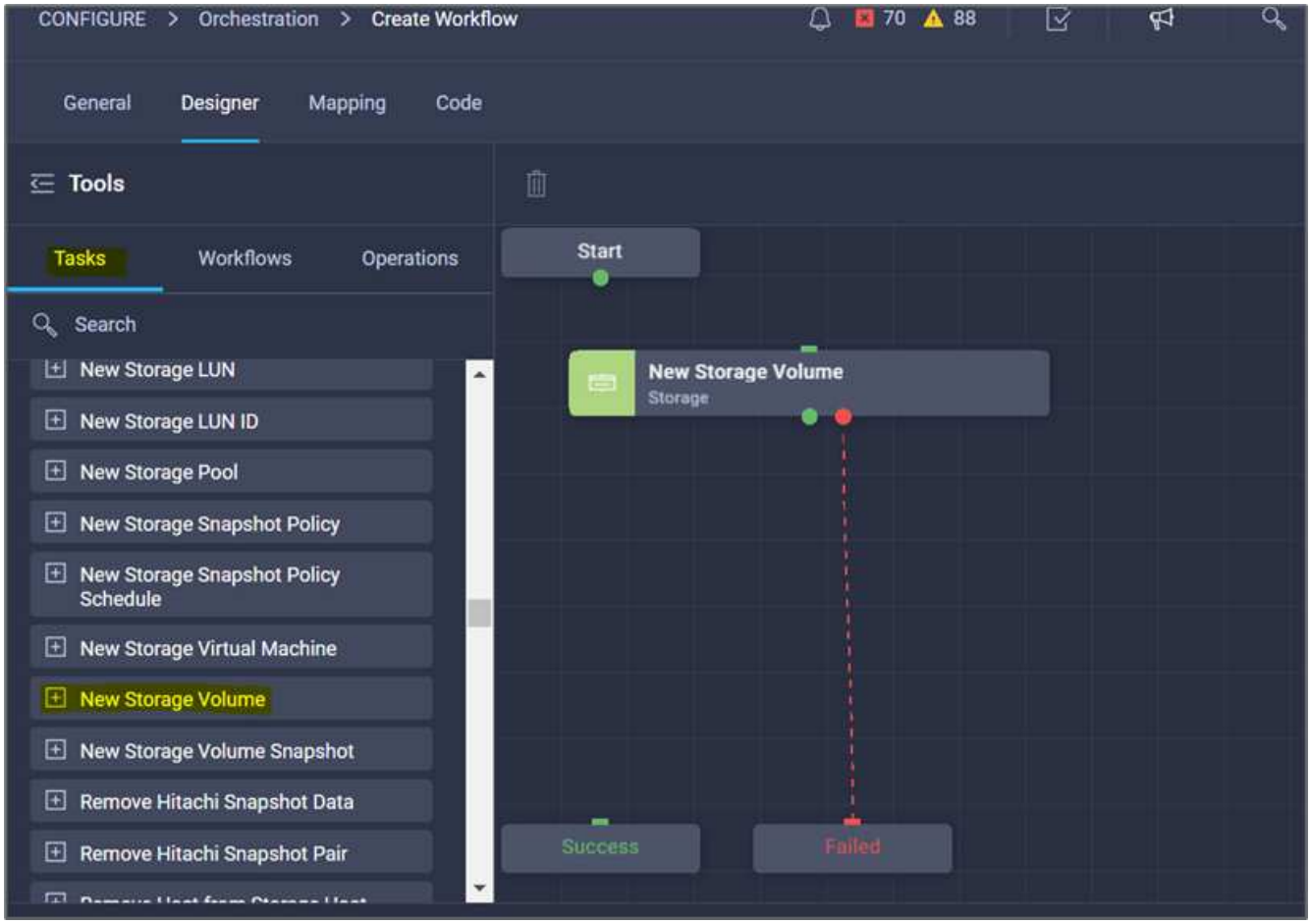
Procedura 1: Creazione del flusso di lavoro

1. Fare clic su **Orchestration** (orchestrazione) nel riquadro di navigazione a sinistra e fare clic su **Create Workflow** (Crea flusso di lavoro).
2. Nella scheda **Generale**:
   a. Fornire il nome visualizzato (flusso di lavoro di disaster recovery).
   b. Selezionare l'organizzazione, impostare i tag e fornire una descrizione.
3. Fare clic su Salva.

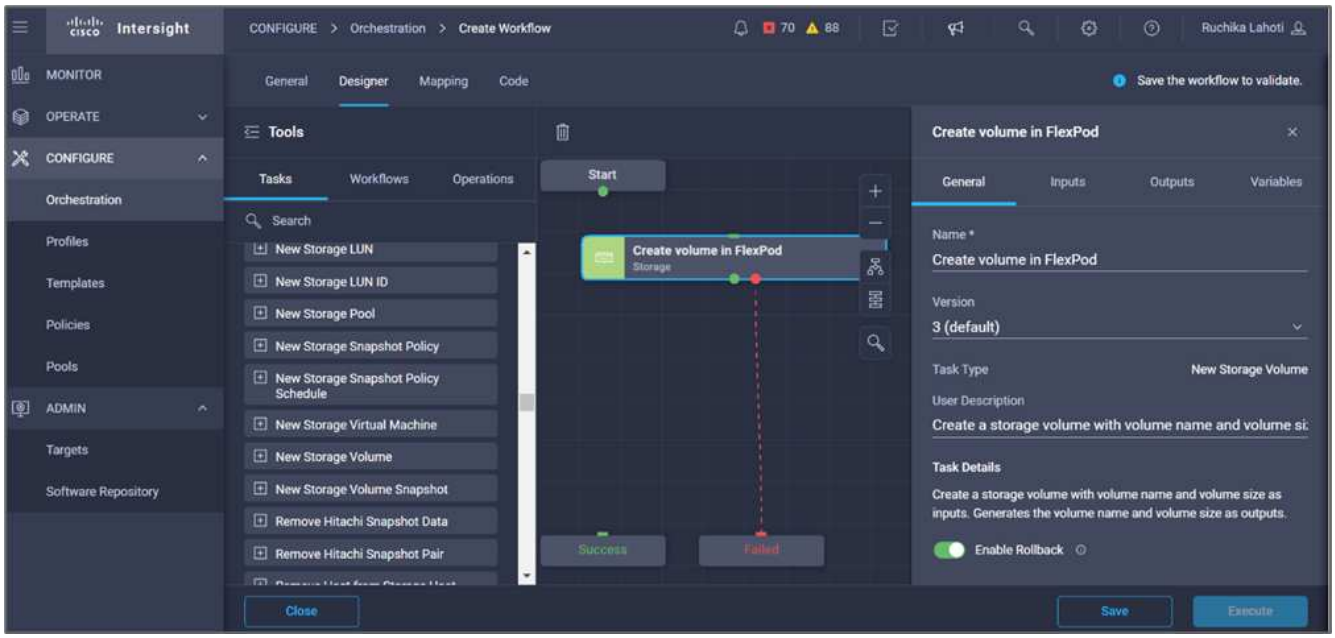


Procedura 2. Creare un nuovo volume in FlexPod

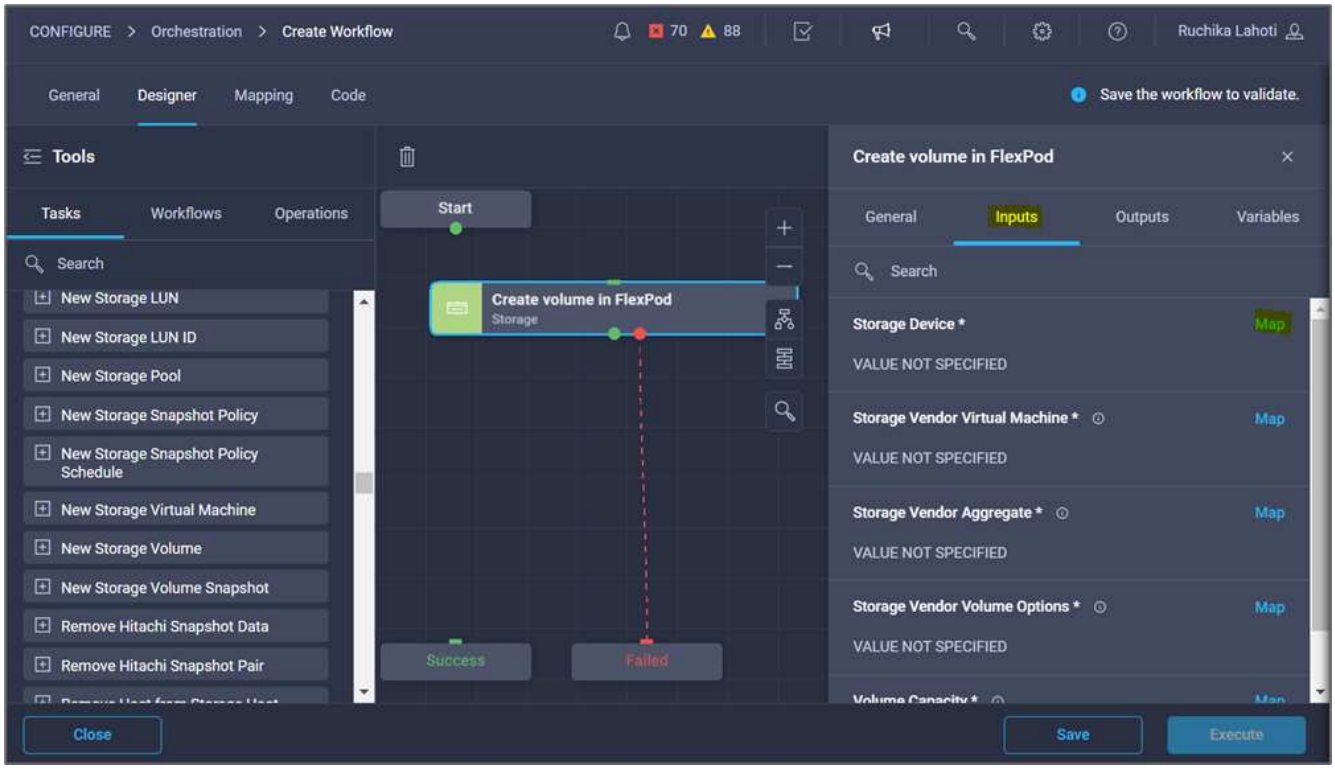
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Storage > New Storage Volume** (Storage > nuovo volume di storage) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Fare clic su **New Storage Volume** (nuovo volume di storage).



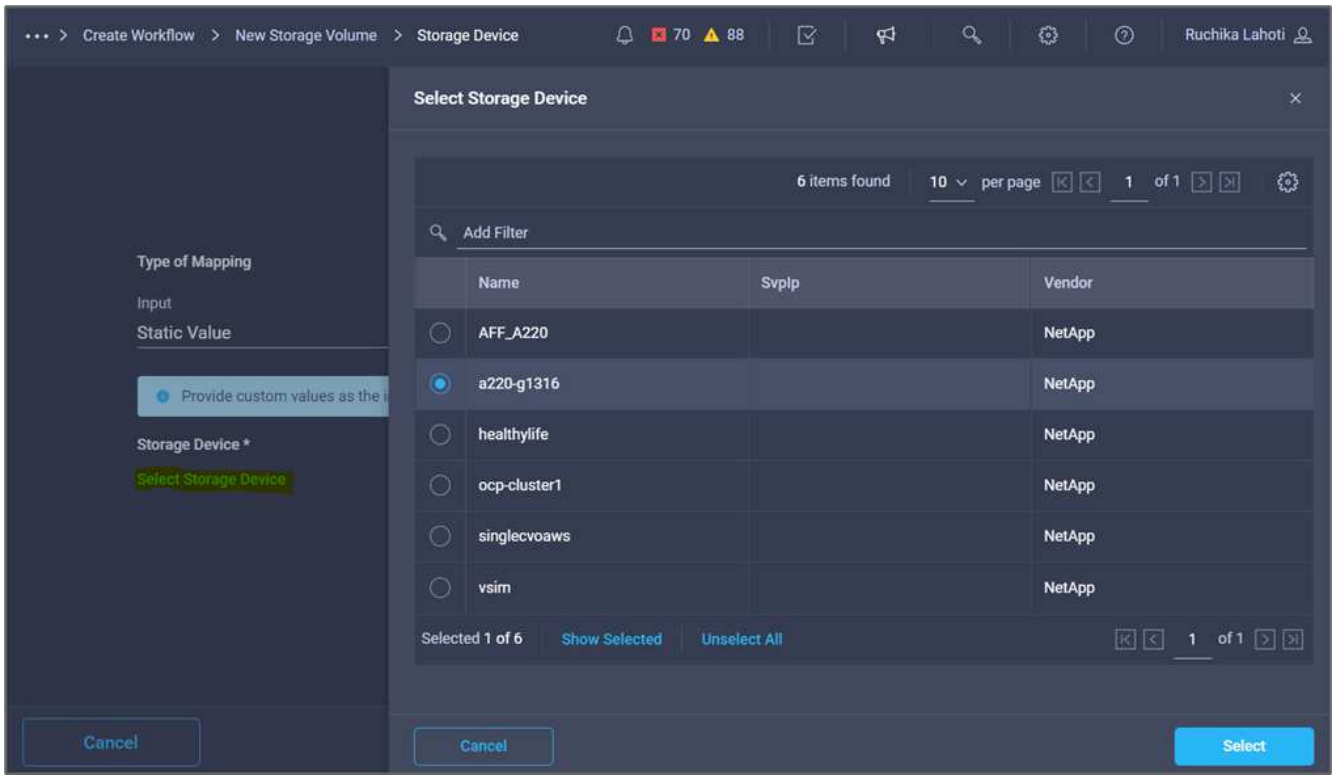
4. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Crea volume in FlexPod**.



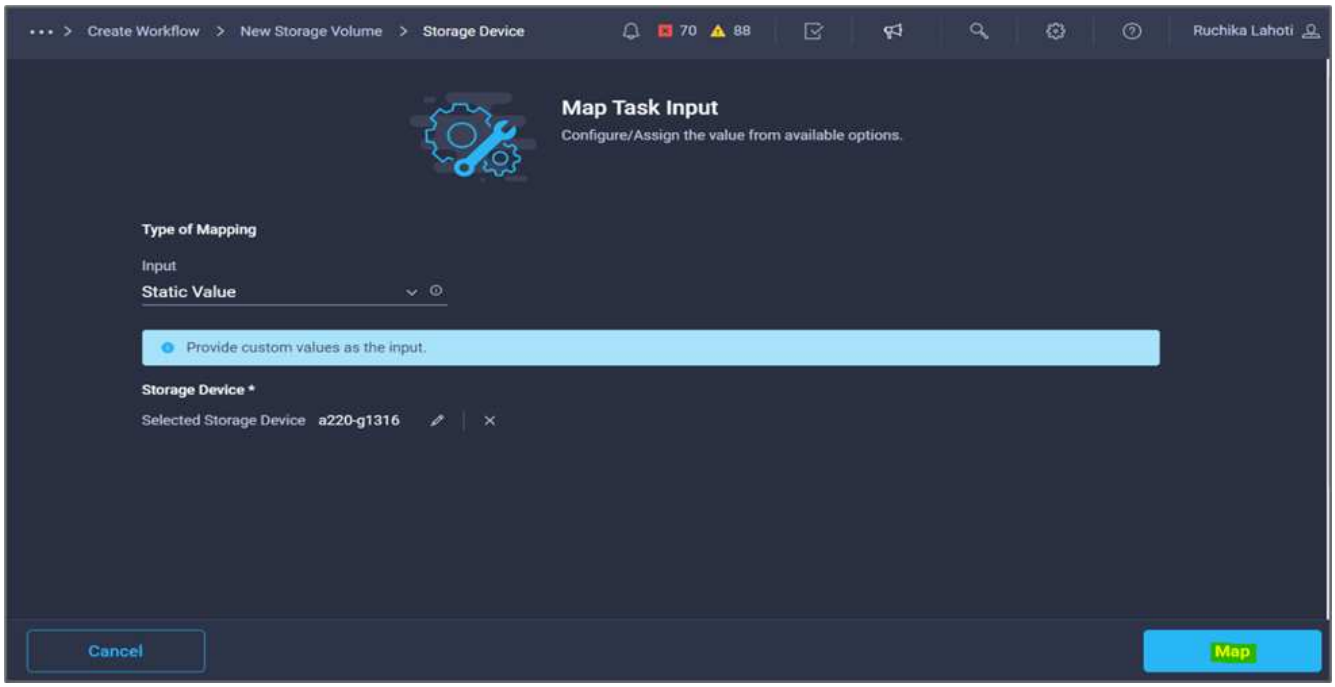
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Storage Device**.



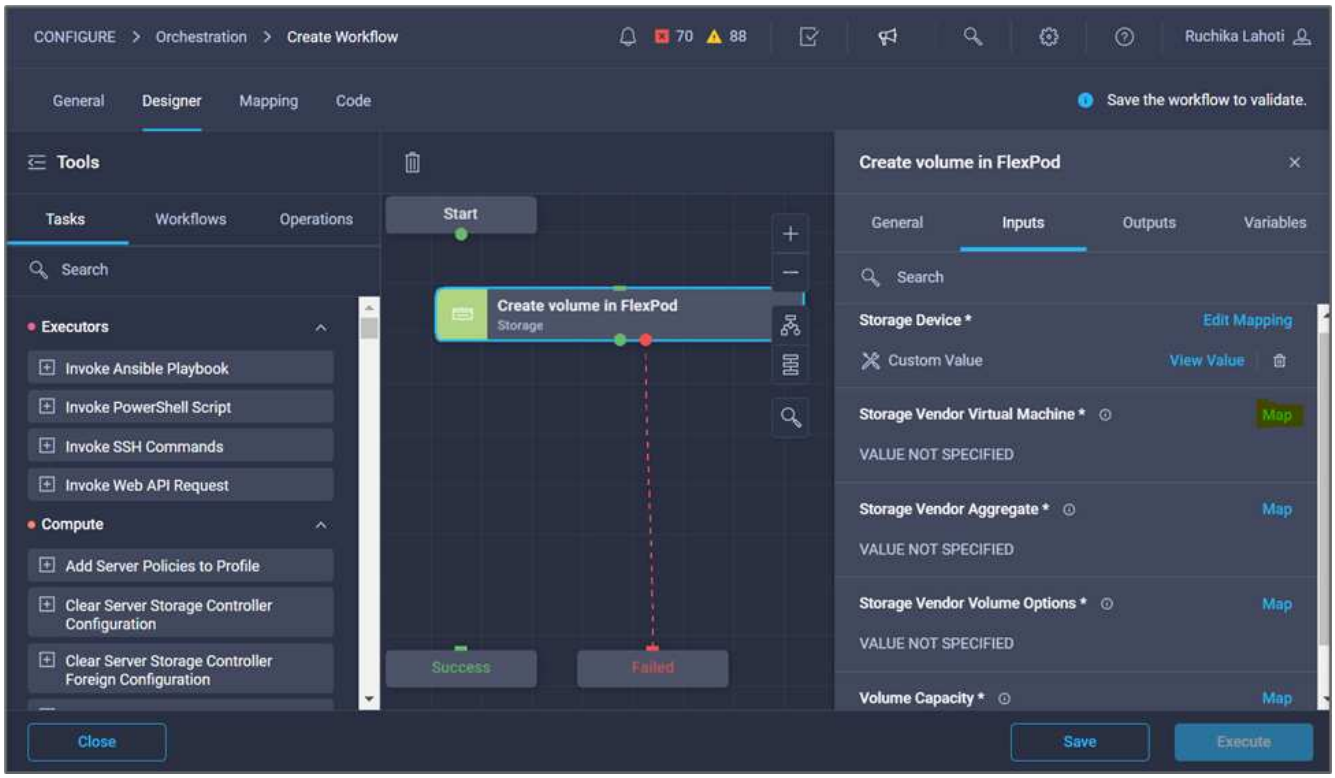
7. Scegliere **valore statico** e fare clic su **Seleziona dispositivo di storage**.
8. Fare clic sulla destinazione di storage aggiunta e fare clic su **Select** (Seleziona).



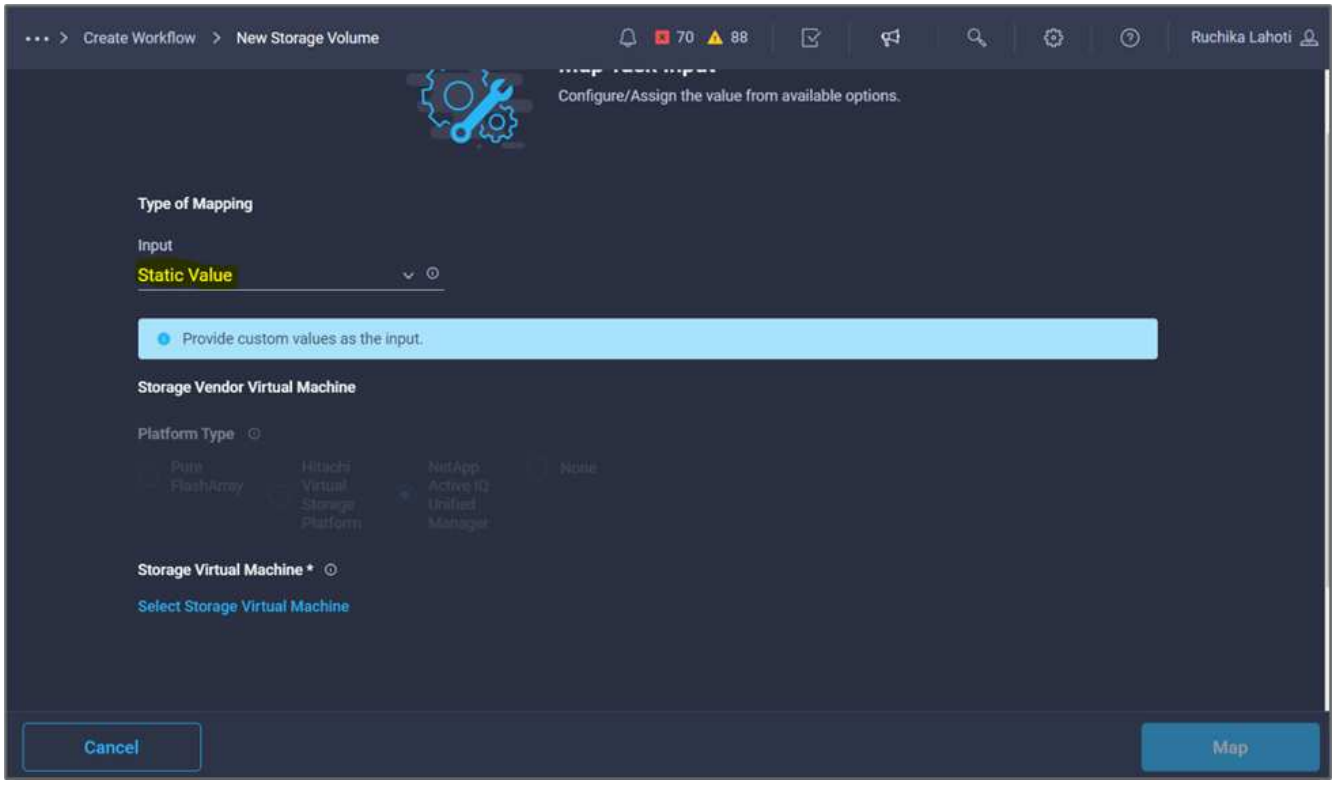
9. Fare clic su **Map** (Mappa).



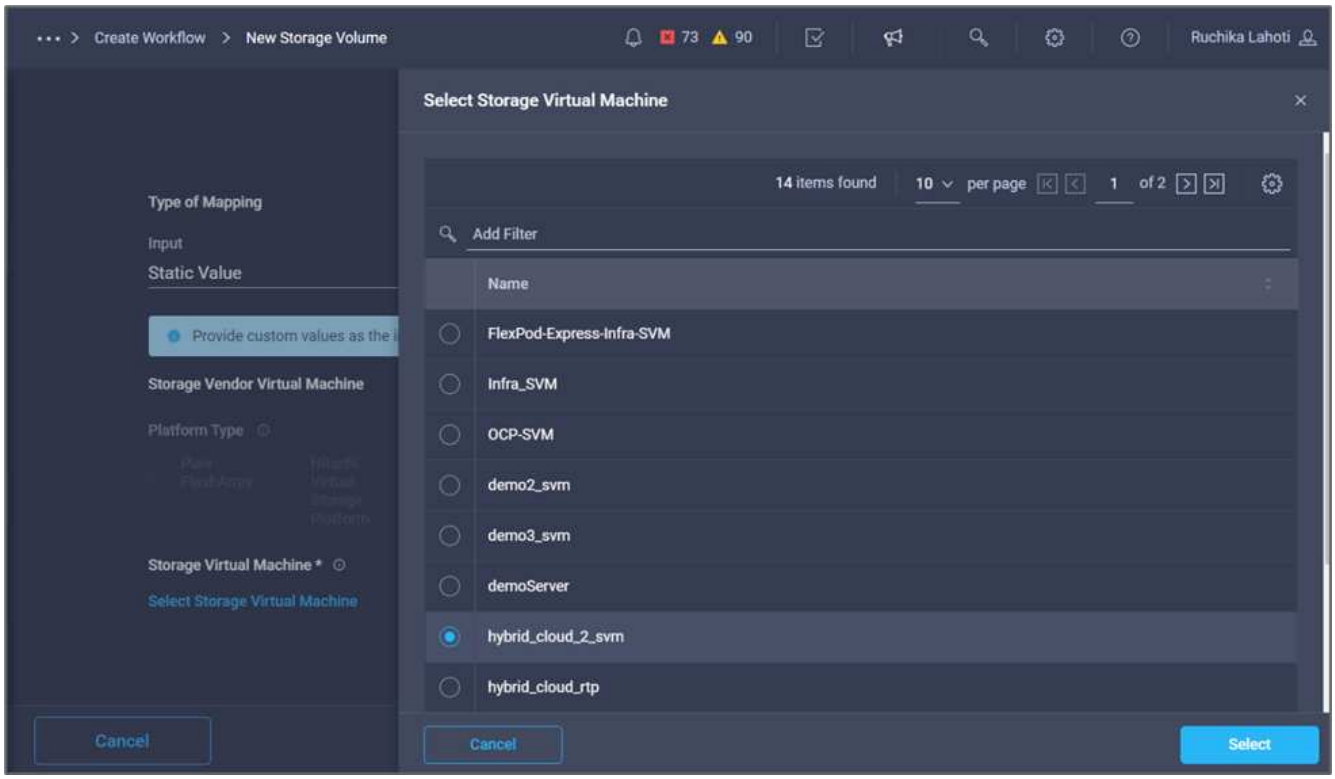
10. Fare clic su **Map** nel campo **Storage Vendor Virtual Machine**.



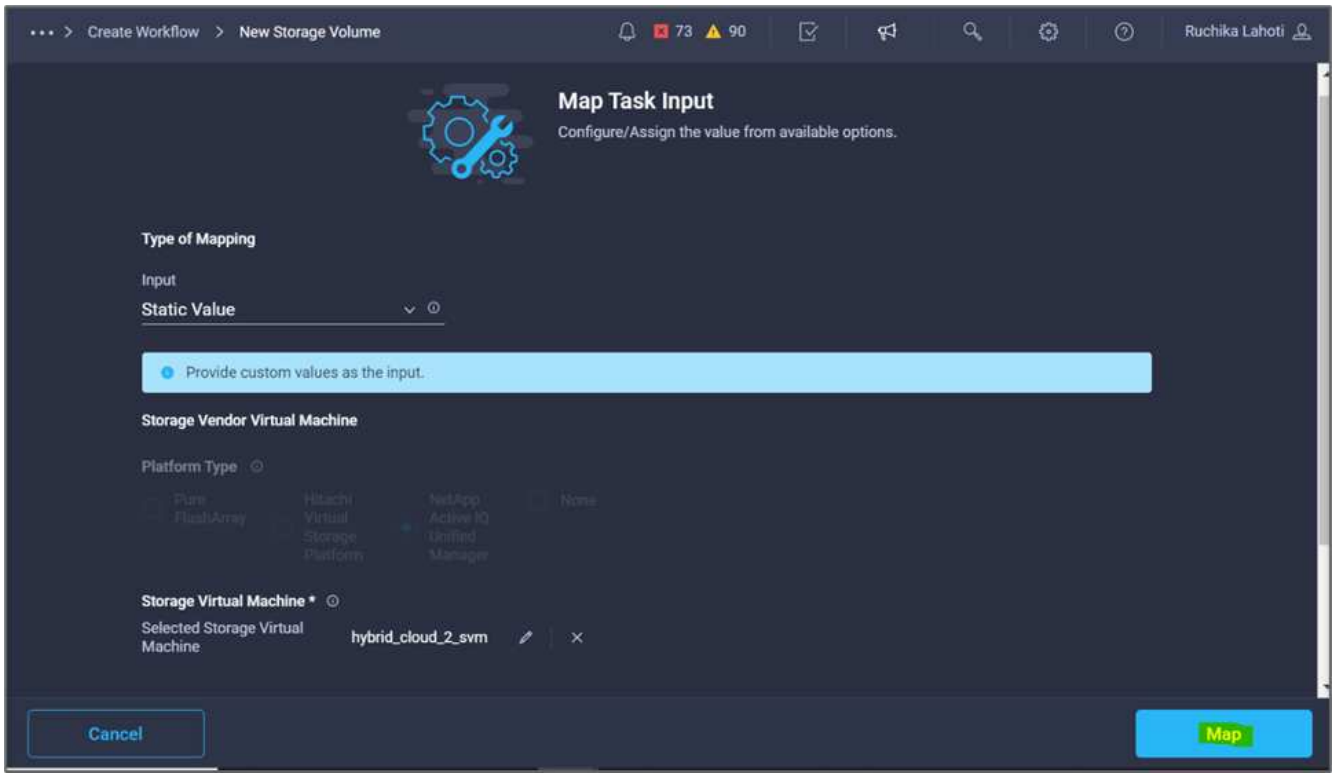
11. Scegliere **valore statico** e fare clic su **Seleziona Storage Virtual Machine**.



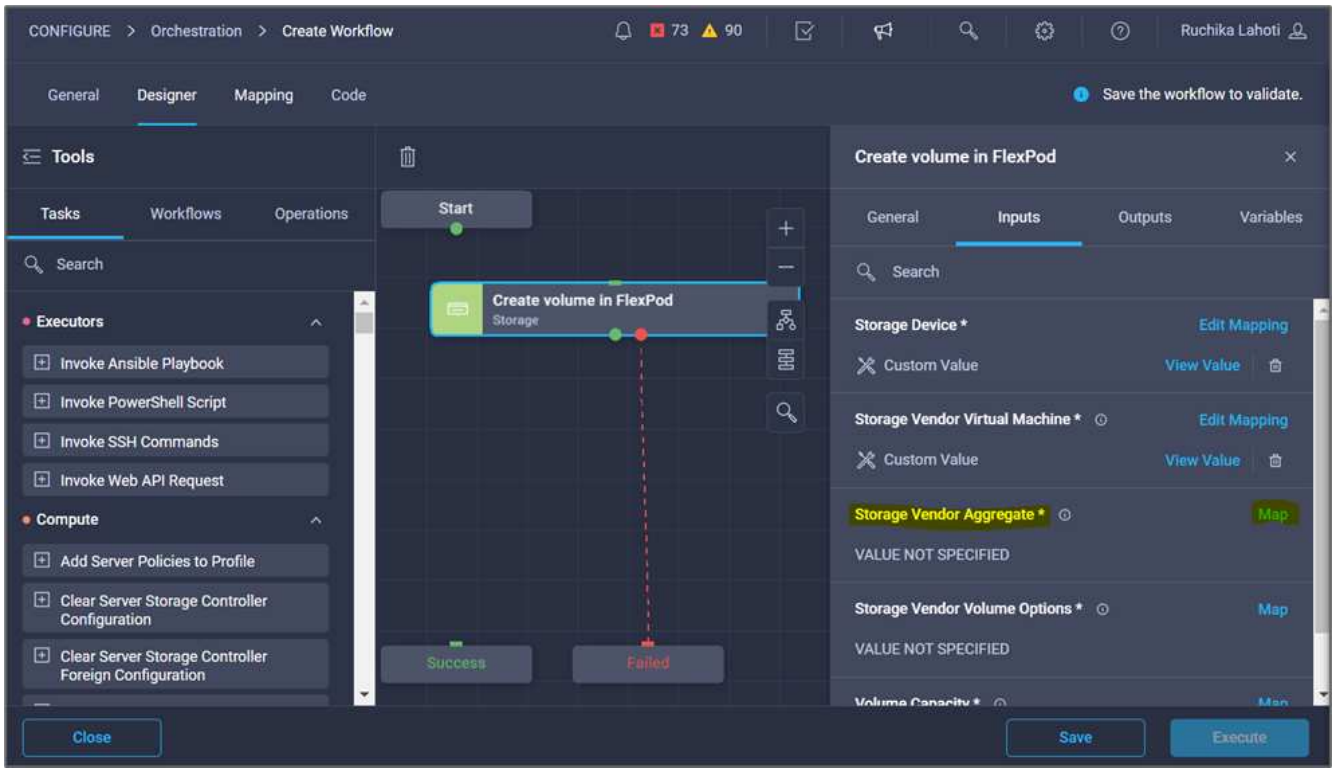
12. Selezionare la macchina virtuale di storage in cui creare il volume e fare clic su **Select** (Seleziona).



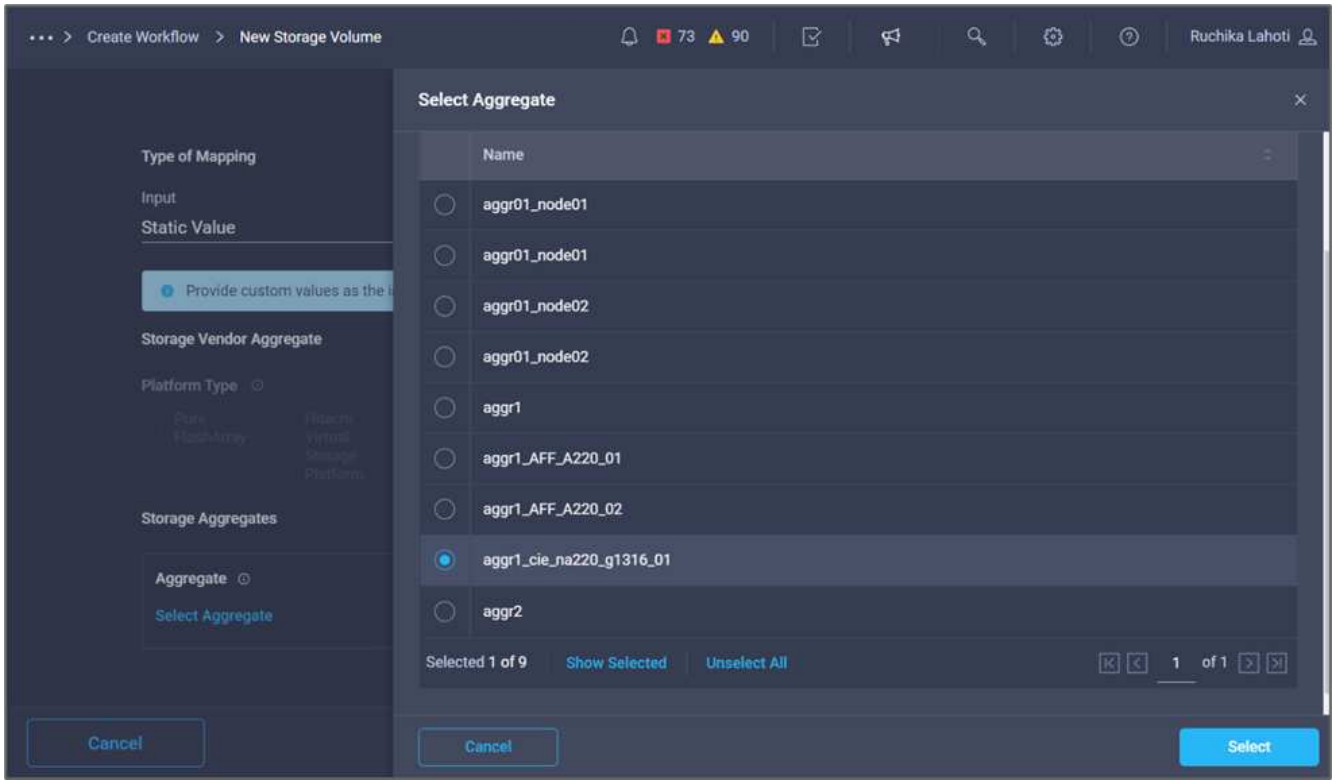
13. Fare clic su **Map** (Mappa).



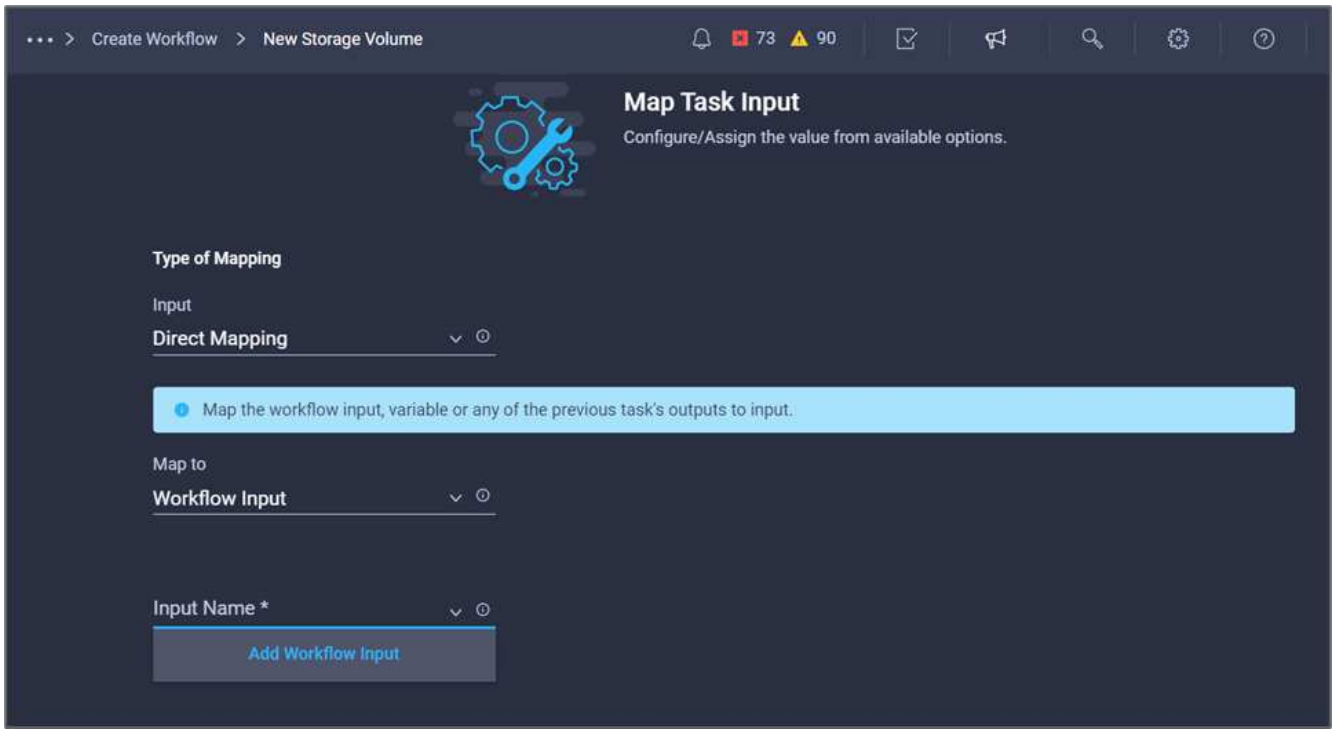
14. Fare clic su **Map** nel campo **Storage Vendor aggregate**.



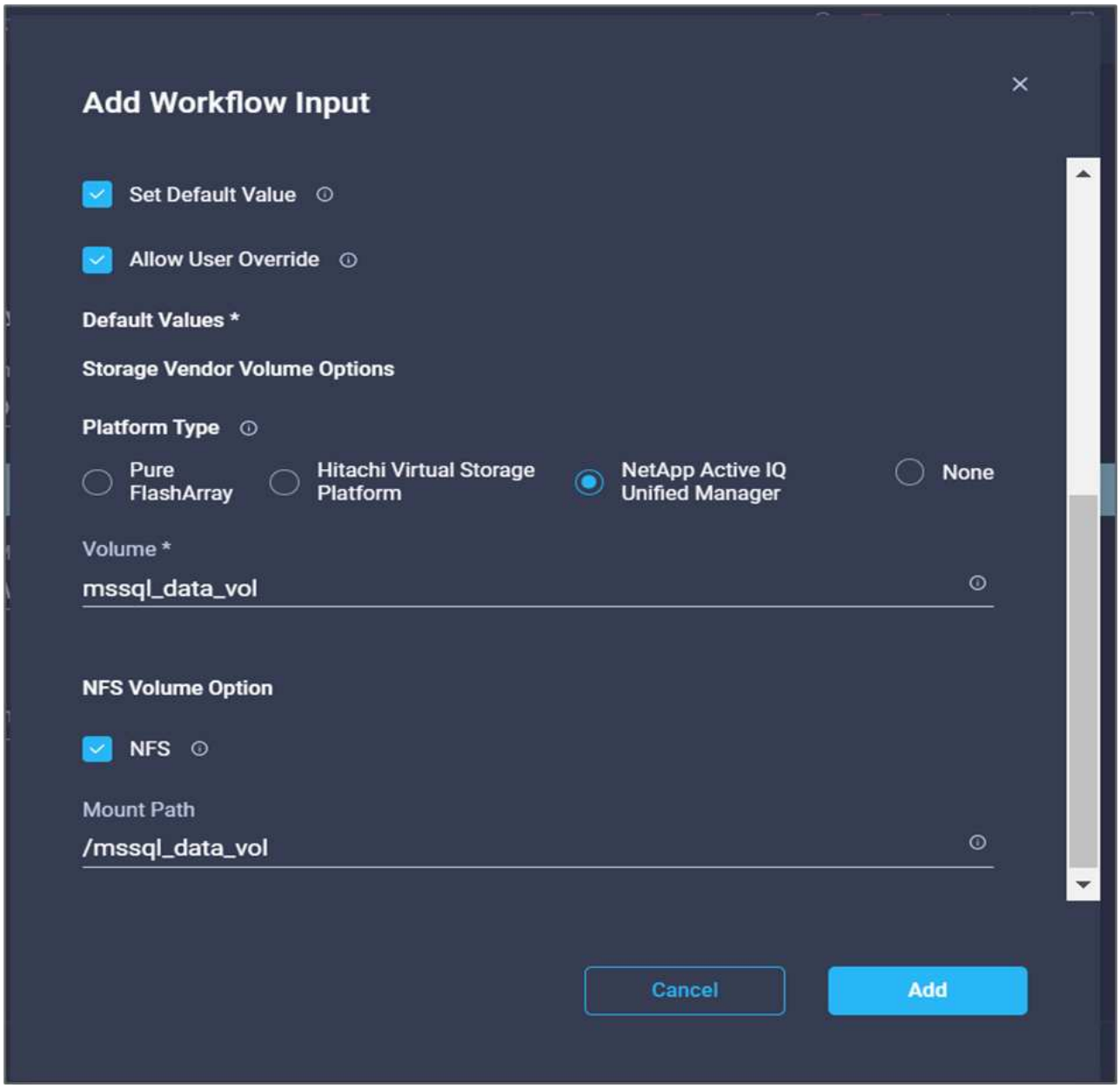
15. Scegliere **valore statico** e fare clic su **Seleziona aggregato di storage**. Scegliere l'aggregato e fare clic su **Select** (Seleziona).



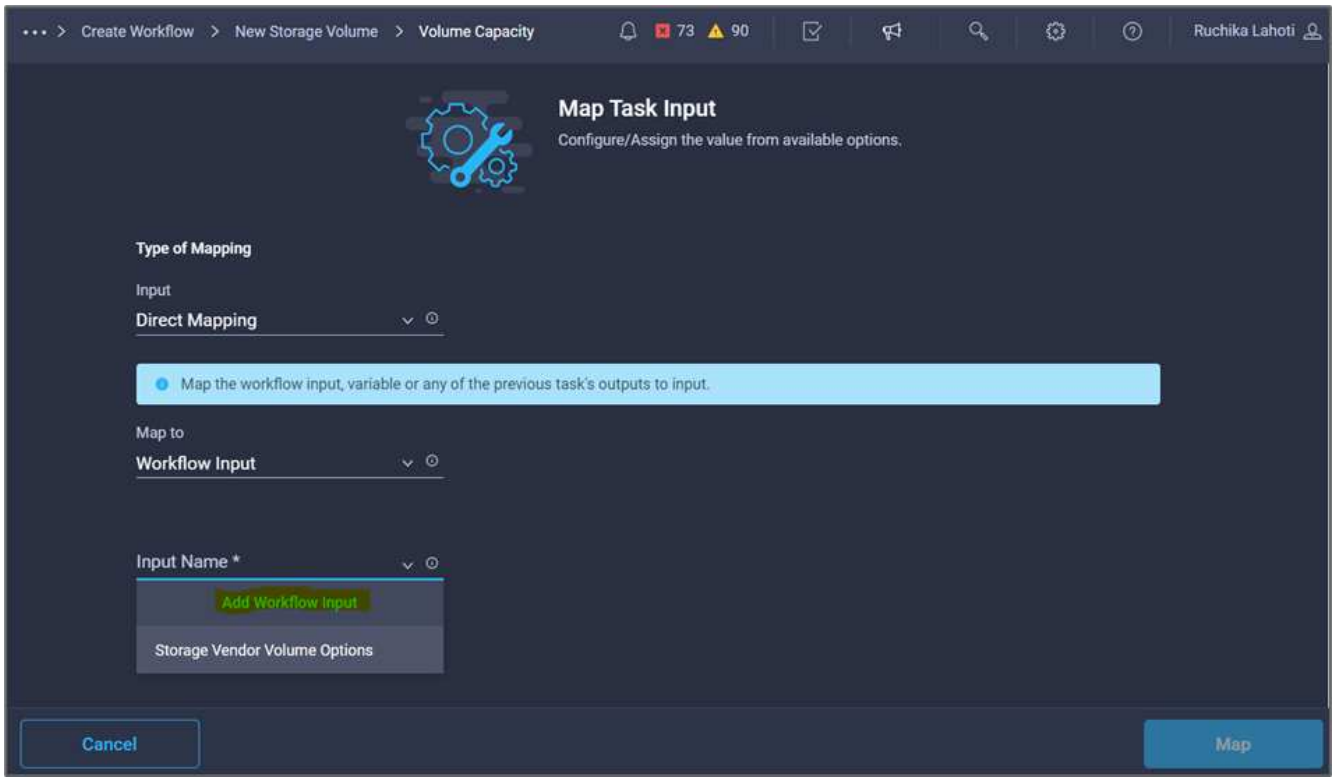
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Storage Vendor Volume Options**.
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.



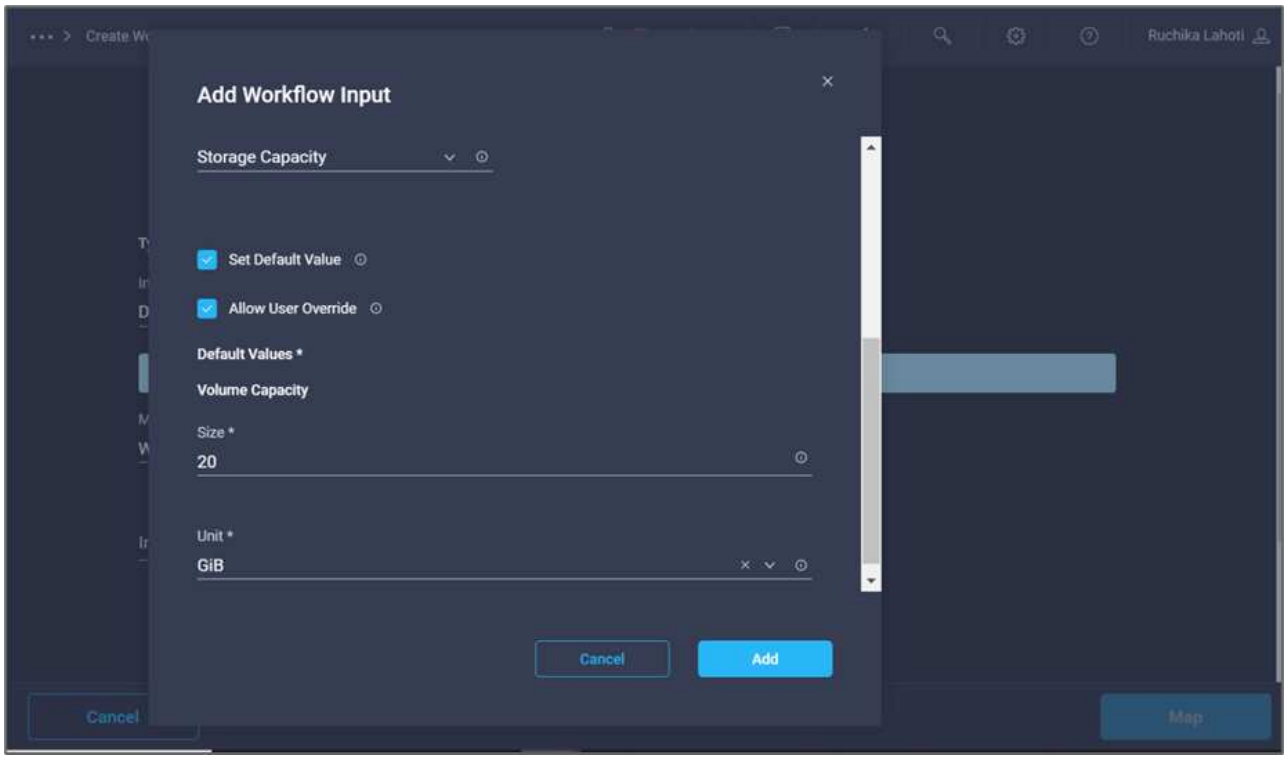
19. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi che l'opzione **Storage Vendor Volume Options** sia selezionata per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fare clic su **obbligatorio**.
    e. Impostare **tipo di piattaforma** su **NetApp Active IQ Unified Manager**.
    f. Fornire un valore predefinito per il volume creato in **Volume**.
    g. Fare clic su **NFS**. Se NFS è impostato, viene creato un volume NFS. Se questo valore è impostato su false, viene creato un volume SAN.
    h. Fornire un percorso di montaggio e fare clic su **Aggiungi**.



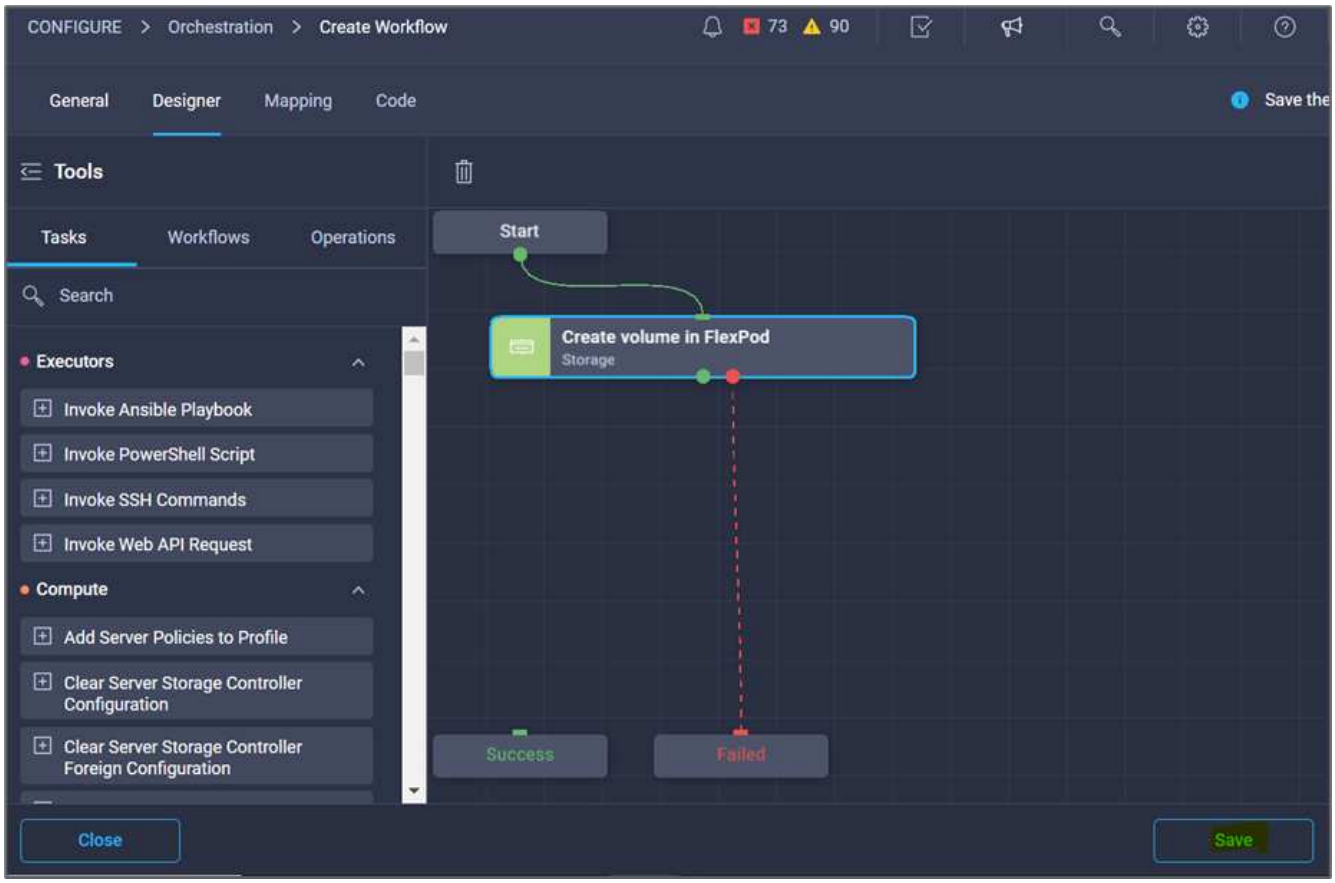
20. Fare clic su **Map** (Mappa).
21. Fare clic su **MAP** nel campo **Volume Capacity**.
22. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
23. Fare clic su **Input Name** e **Create Workflow Input**.



24. Nella procedura guidata Aggiungi input:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Per **Type**, selezionare **Storage Capacity**.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Fornire un valore predefinito per le dimensioni del volume e l'unità.
    f. Fare clic su **Aggiungi**.



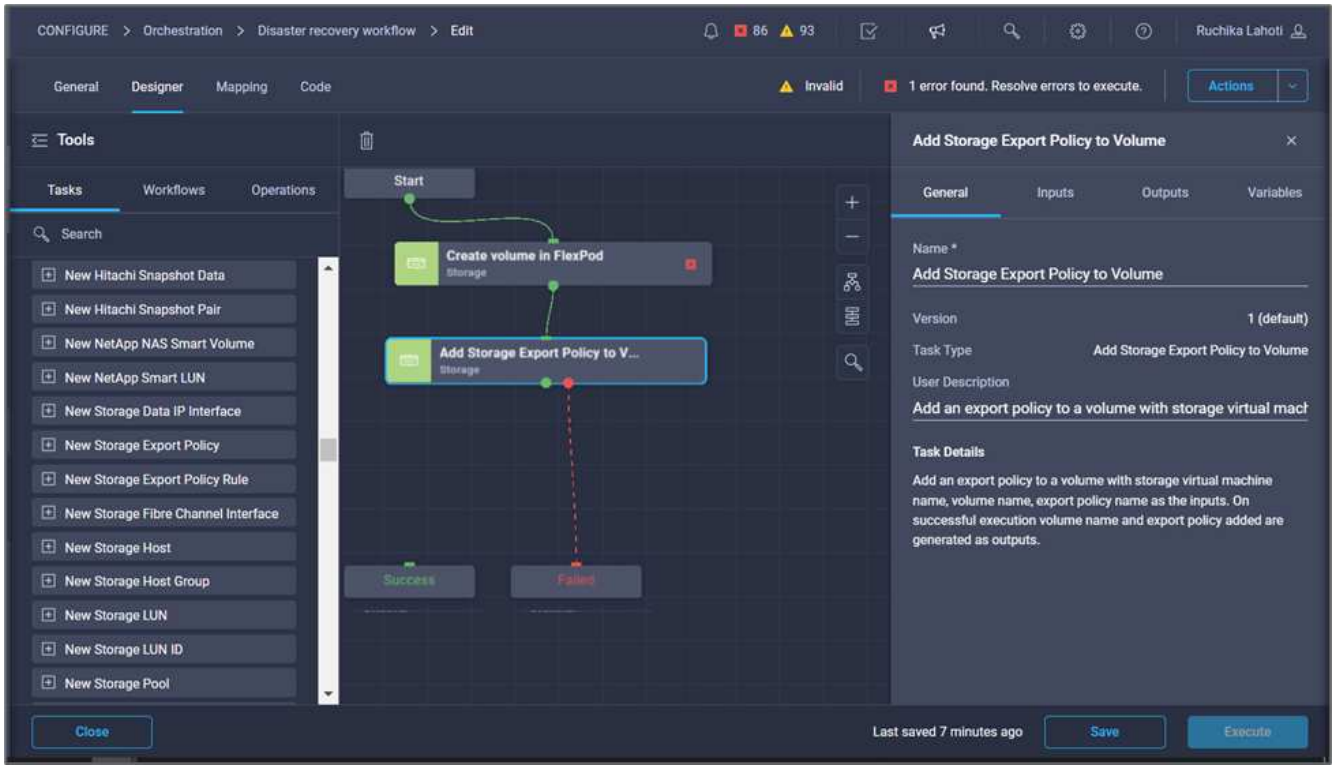
25. Fare clic su **Map** (Mappa).
26. Con Connector, creare una connessione tra le attività **Avvio** e **Crea volume in FlexPod**, quindi fare clic su **Salva**.



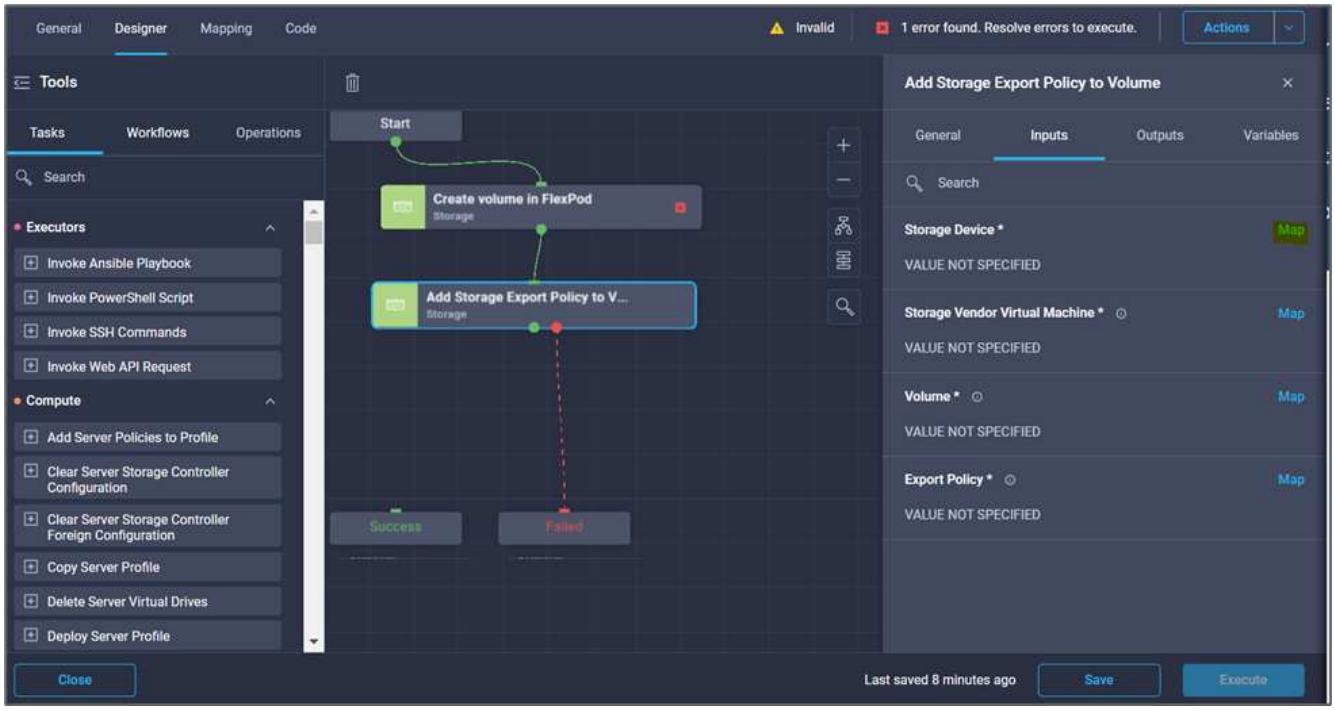
Ignorare l'errore per ora. Questo errore viene visualizzato perché non è presente alcuna connessione tra le attività **Crea volume in FlexPod** e **operazione riuscita**, necessaria per specificare la transizione corretta.

Procedura 3: Aggiunta della policy di esportazione dello storage

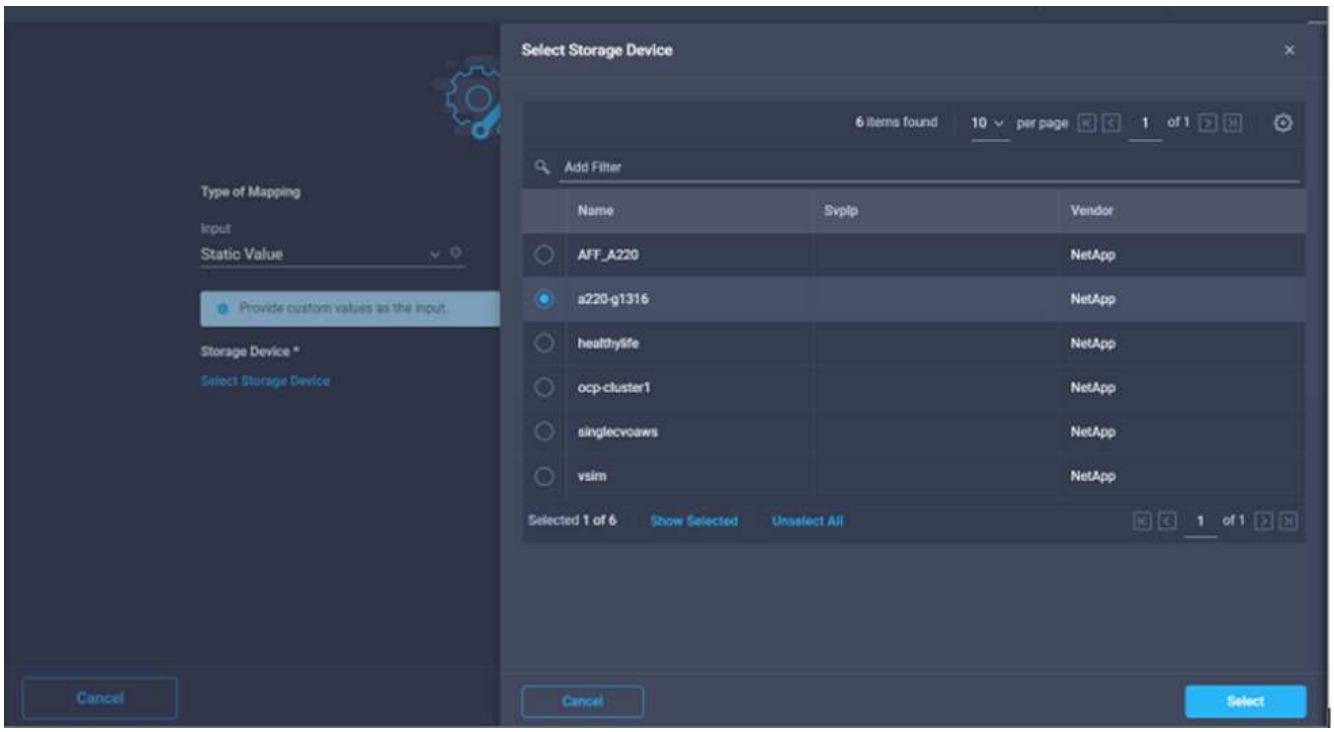
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Storage > Add Storage Export Policy to Volume** (archiviazione > Aggiungi policy di esportazione dello storage al volume) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Fare clic su **Add Storage Export Policy to Volume** (Aggiungi policy di esportazione storage al volume). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è Add Storage Export Policy (Aggiungi policy di esportazione dello storage).
4. Utilizzare Connector per stabilire una connessione tra le attività **Crea volume in FlexPod** e **Aggiungi policy di esportazione dello storage**. Fare clic su **Save** (Salva).



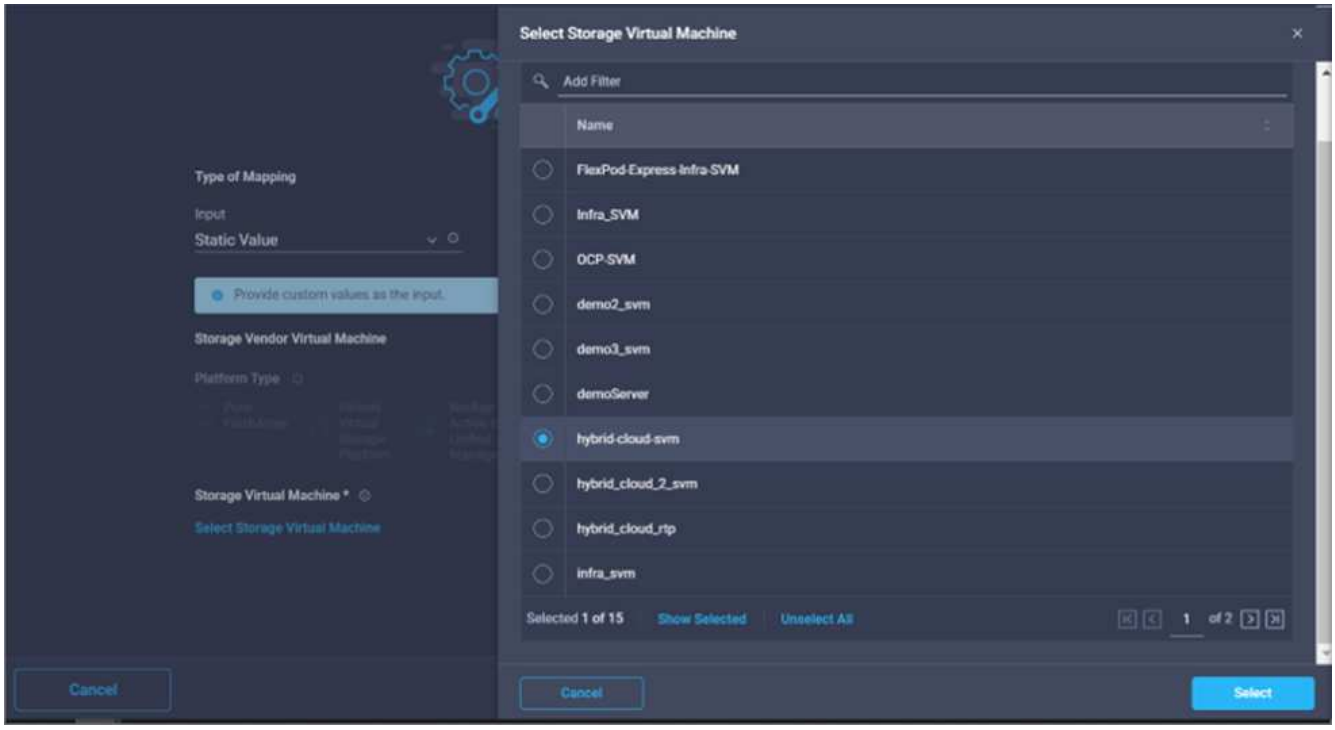
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Storage Device**.



7. Scegliere **valore statico** e fare clic su **Seleziona dispositivo di storage**. Selezionare la stessa destinazione di storage aggiunta durante la creazione dell'attività precedente di creazione di un nuovo volume di storage.
8. Fare clic su **Map** (Mappa).

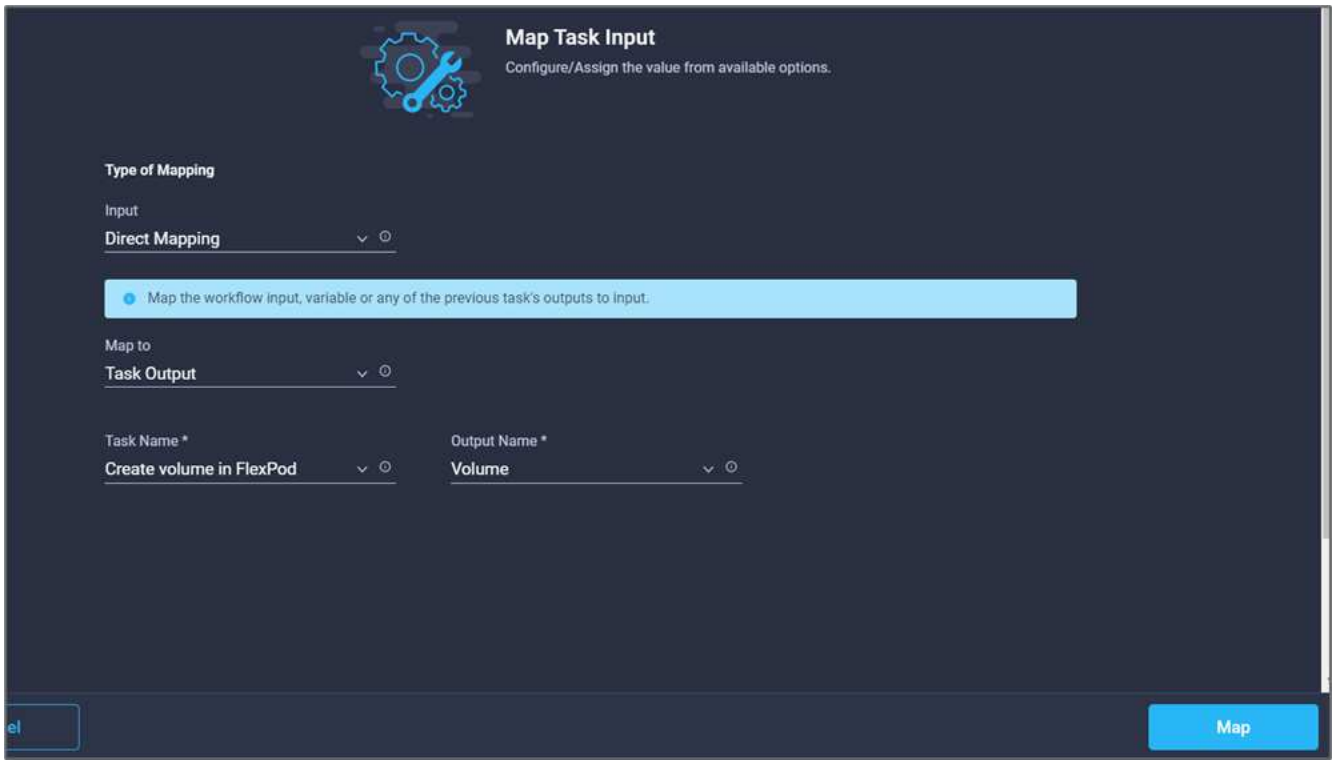


9. Fare clic su **Map** nel campo **Storage Vendor Virtual Machine**.
10. Scegliere **valore statico** e fare clic su **Seleziona Storage Virtual Machine**. Selezionare la stessa macchina virtuale di storage aggiunta durante la creazione dell'attività precedente di creazione di un nuovo volume di storage.

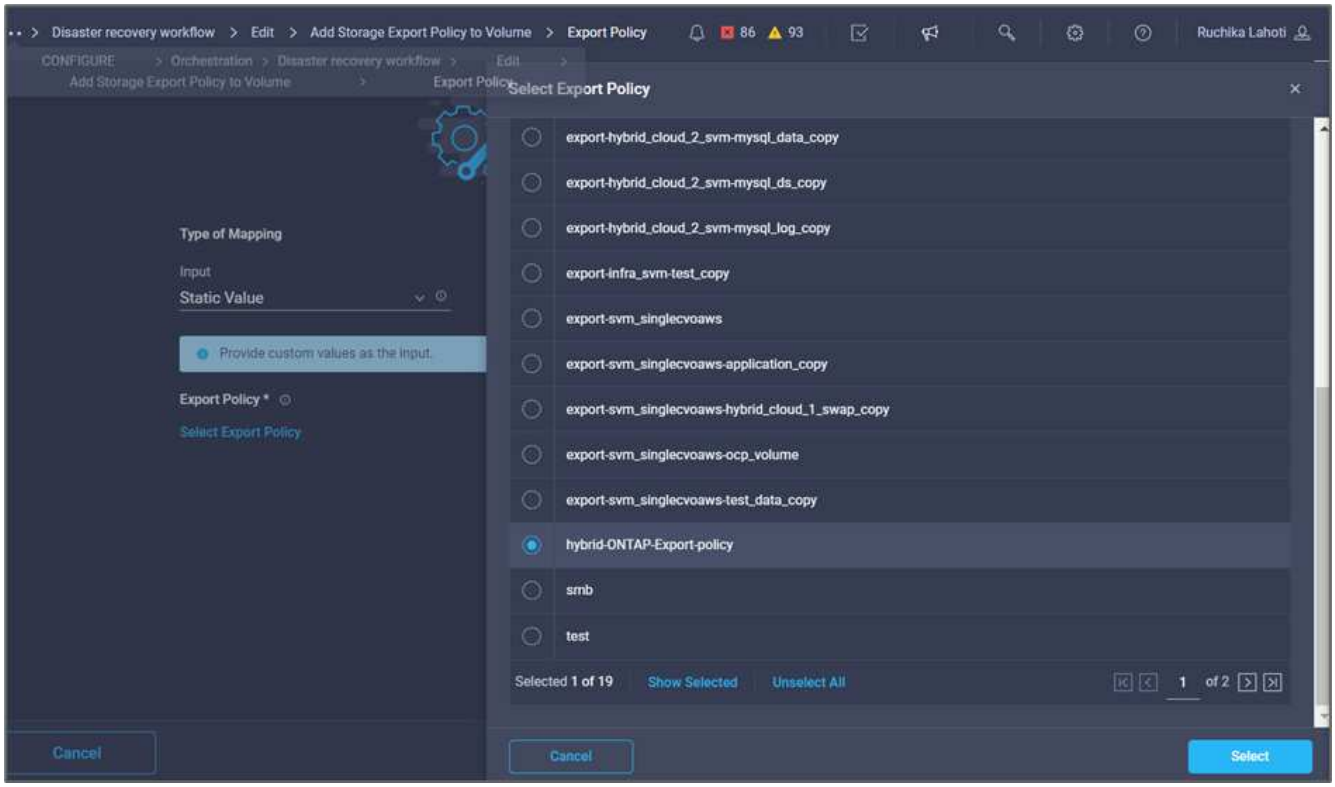


11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Volume**.
13. Fare clic su **Nome attività**, quindi su **Crea volume in FlexPod**. Fare clic su **Output Name** (Nome output), quindi su **Volume**.

> In Cisco Intersight Cloud Orchestrator, è possibile fornire l'output di un'attività precedente come input per una nuova attività. In questo esempio, i dettagli di **Volume** sono stati forniti dall'attività **Crea volume in FlexPod** come input per l'attività **Aggiungi policy di esportazione dello storage**.



14. Fare clic su **Map** (Mappa).
15. Fare clic su **Map** nel campo **Export Policy**.
16. Scegliere **valore statico** e fare clic su **Seleziona policy di esportazione**. Selezionare la policy di esportazione creata.

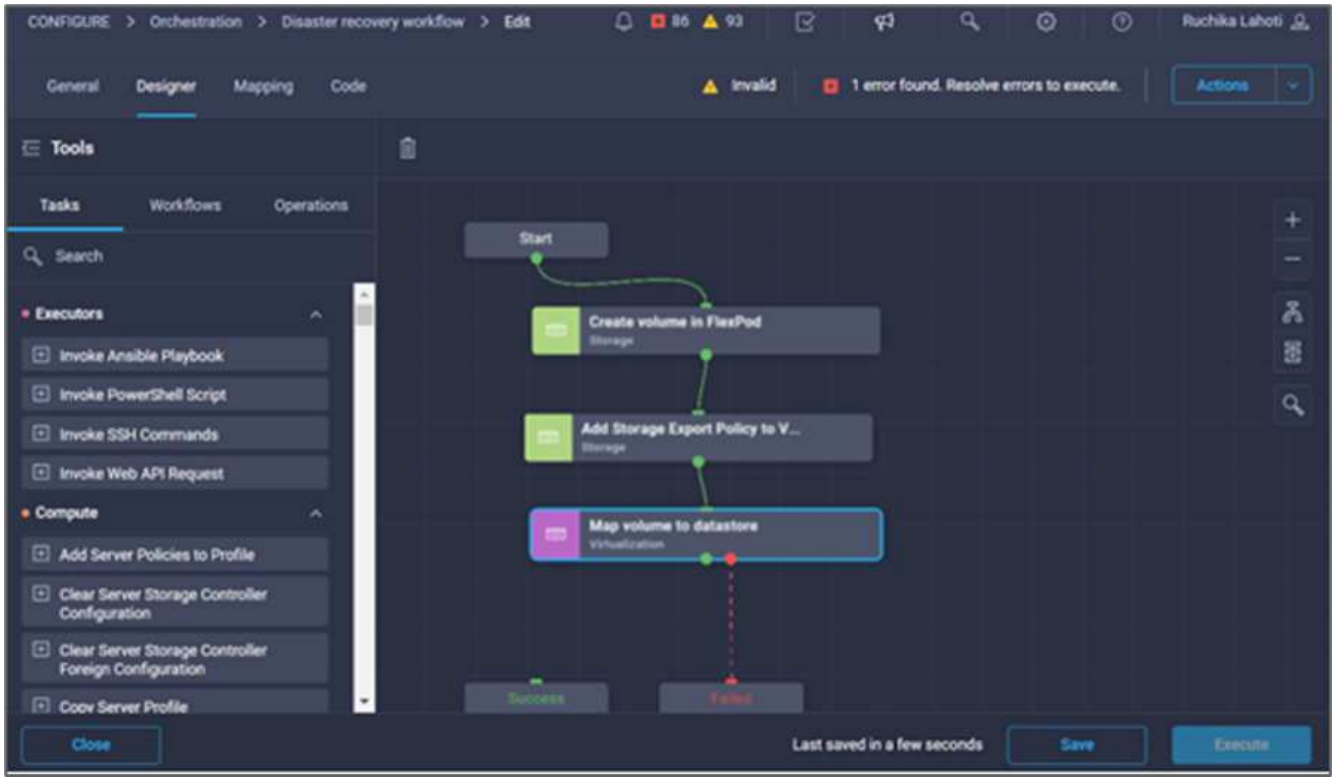


17. Fare clic su **Map** (Mappa), quindi su **Save** (Salva).

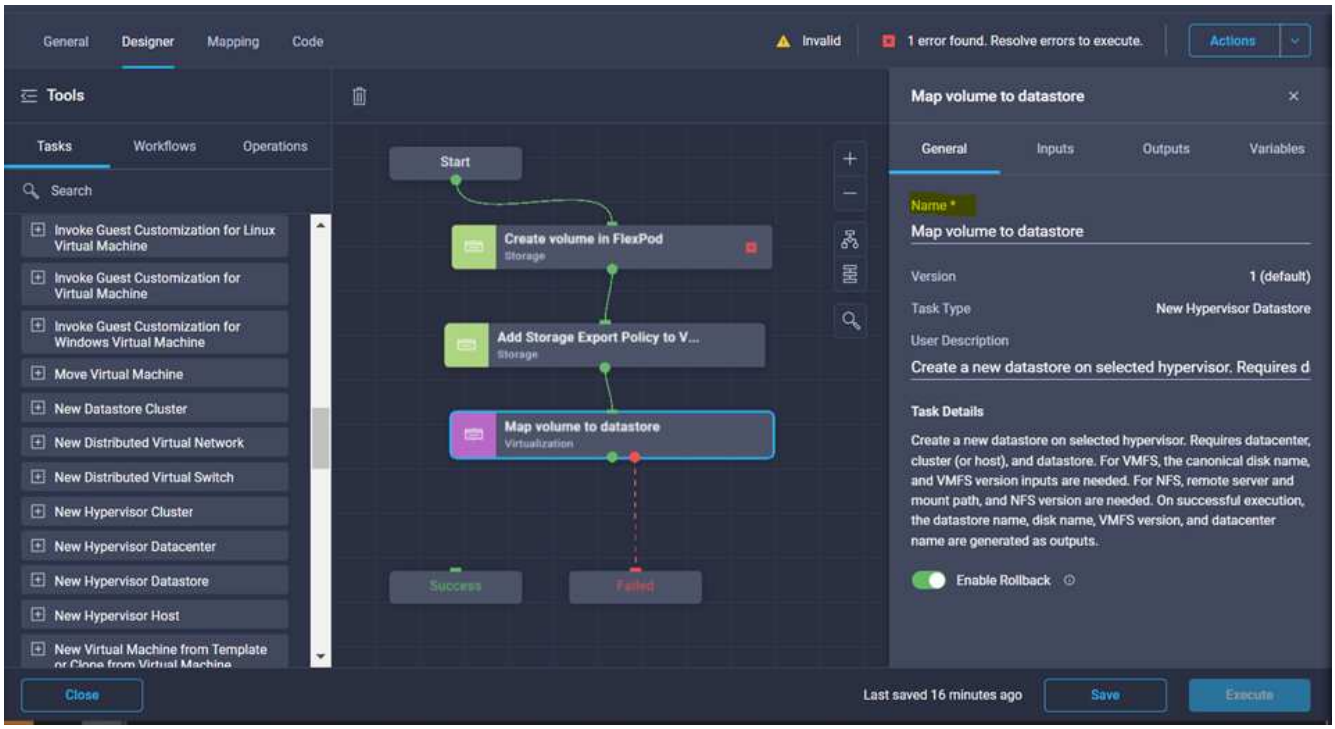
In questo modo, viene completata l'aggiunta di un criterio di esportazione al volume. Quindi, creare un nuovo datastore mappando il volume creato.

Procedura 4: Mappare il volume FlexPod all'archivio dati

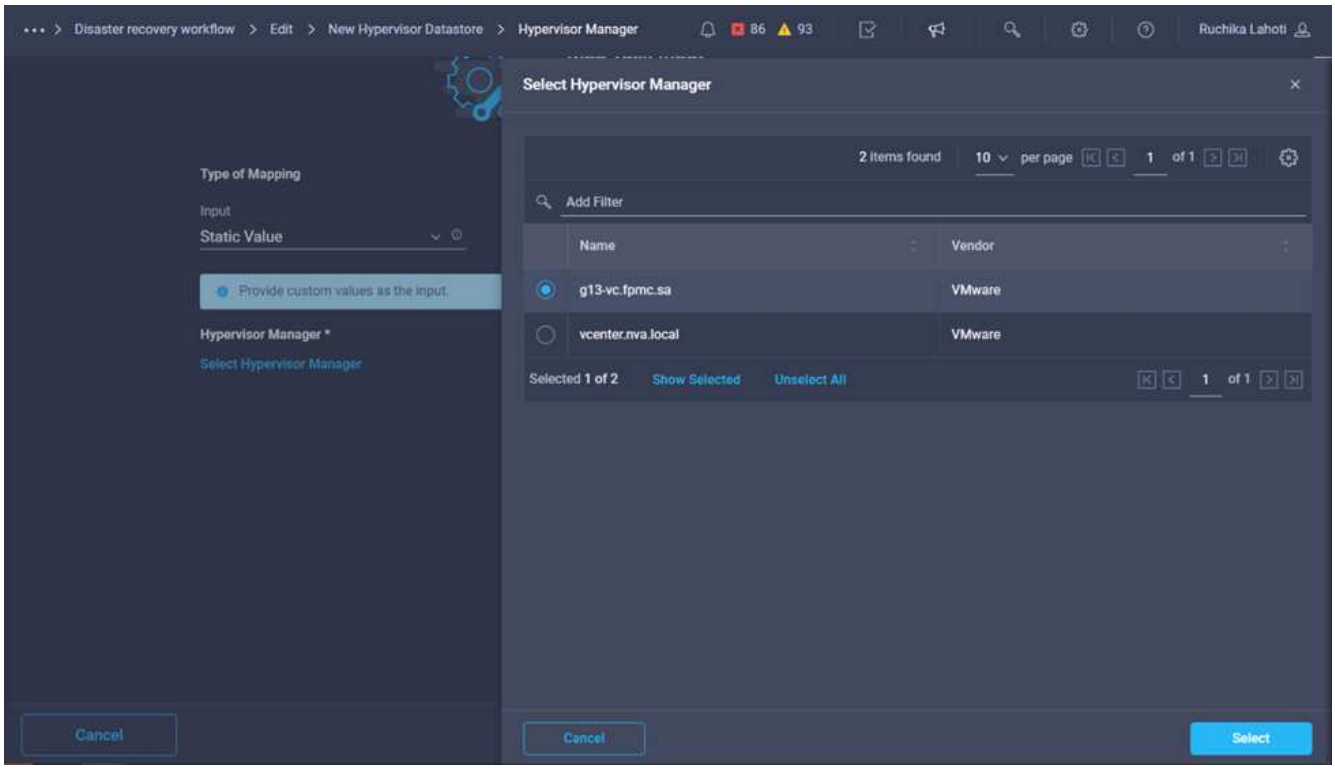
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Virtualization > New Hypervisor Datastore** (virtualizzazione > nuovo archivio dati hypervisor) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per stabilire una connessione tra le attività **Add Storage Export Policy** (Aggiungi policy di esportazione dello storage) e **New Hypervisor Datastore** (nuovo archivio dati hypervisor). Fare clic su **Save** (Salva).



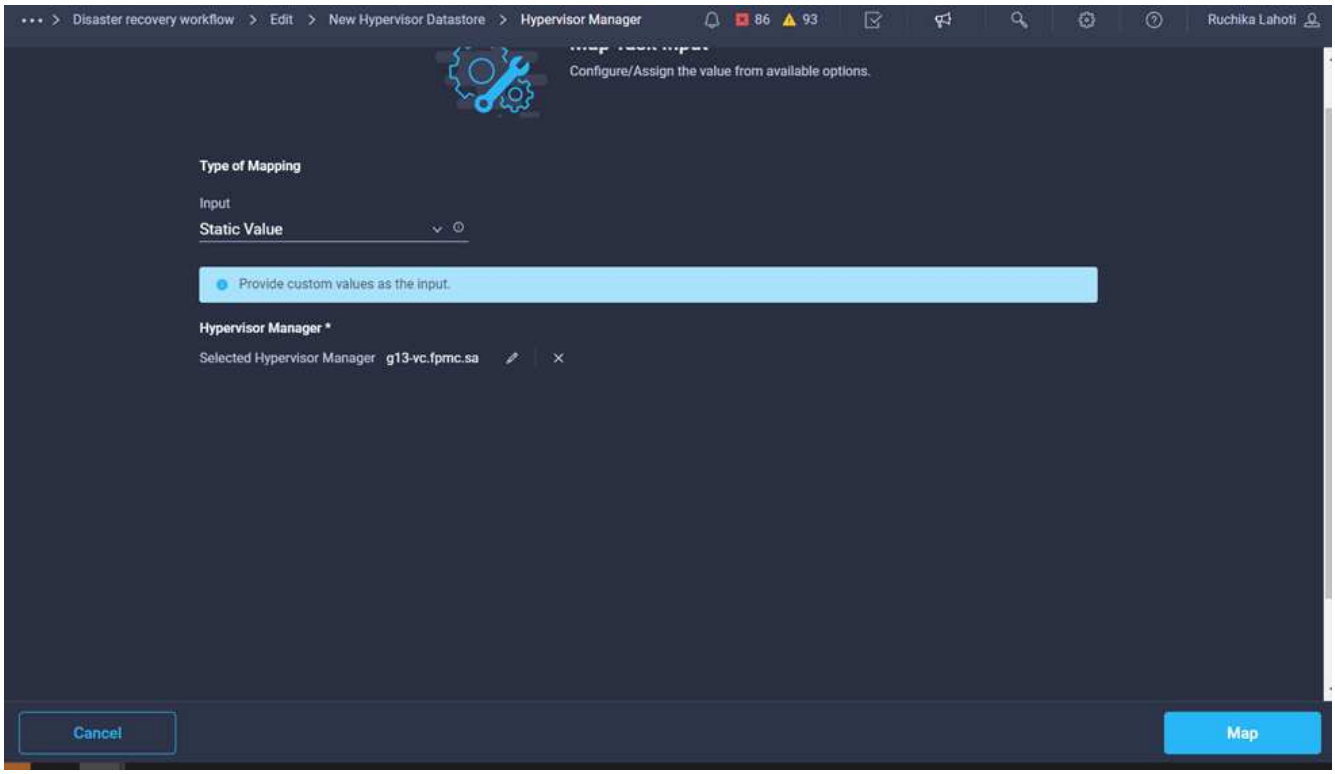
4. Fare clic su **New Hypervisor Datastore** (nuovo archivio dati hypervisor). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Mapp volume to Datastore**.



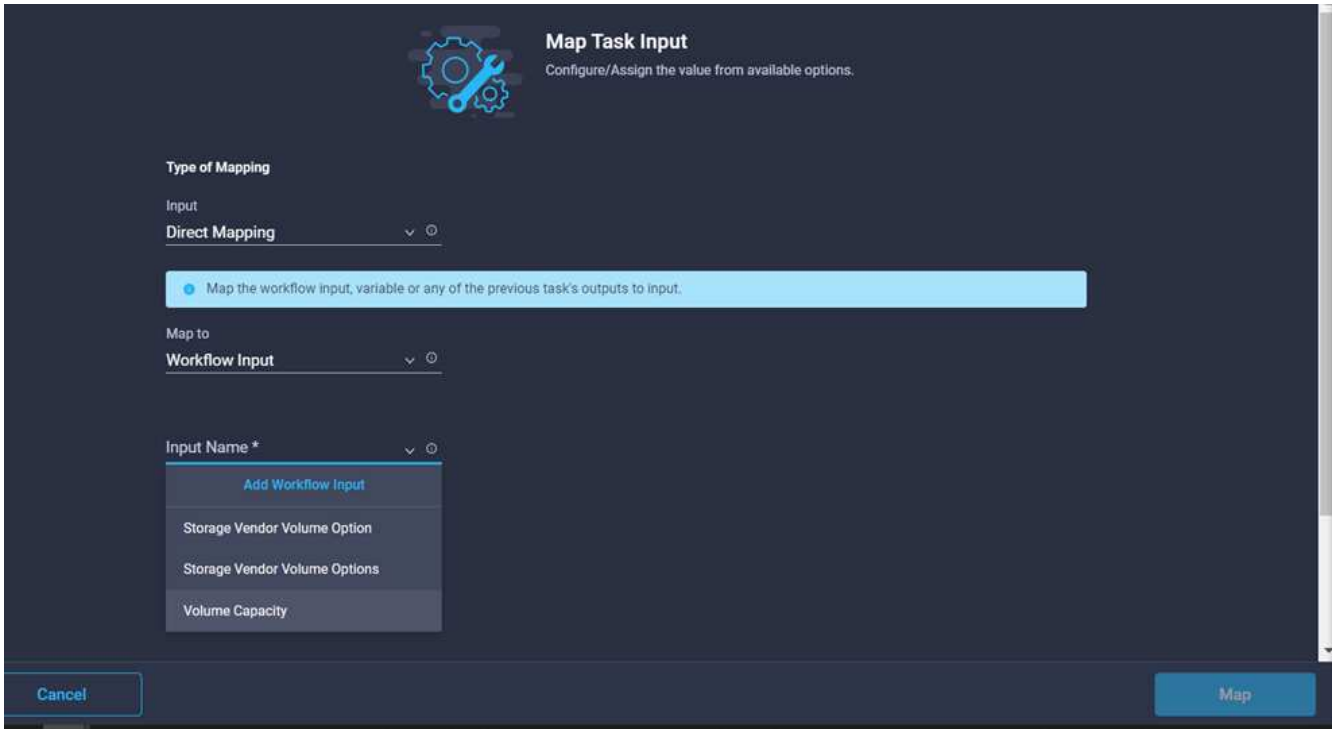
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Hypervisor Manager**.
7. Scegliere **Static Value** (valore statico) e fare clic su **Select Hypervisor Manager** (Seleziona gestore hypervisor). Fare clic sulla destinazione di VMware vCenter.



8. Fare clic su **Map** (Mappa).

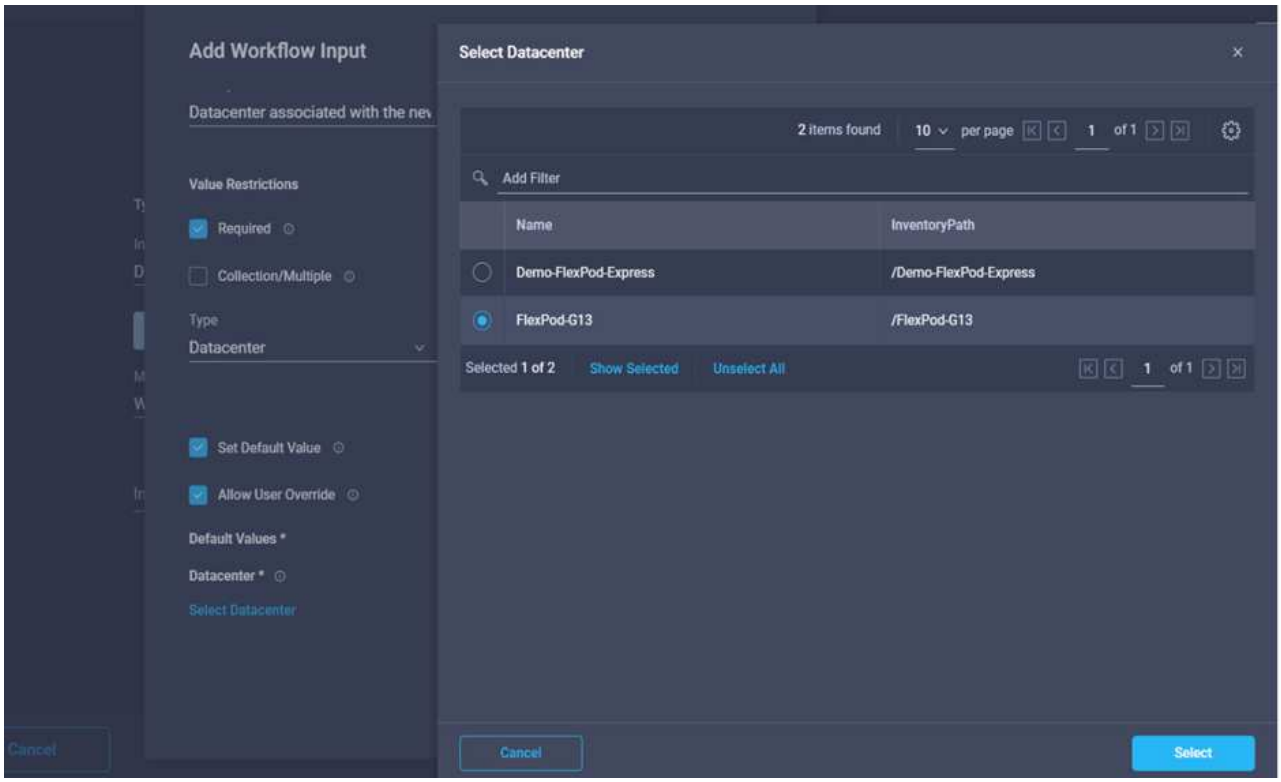


9. Fare clic su **Map** nel campo **Data center**. Si tratta del data center associato al nuovo datastore.
10. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
11. Fare clic su **Input Name**, quindi su **Create Workflow Input**.



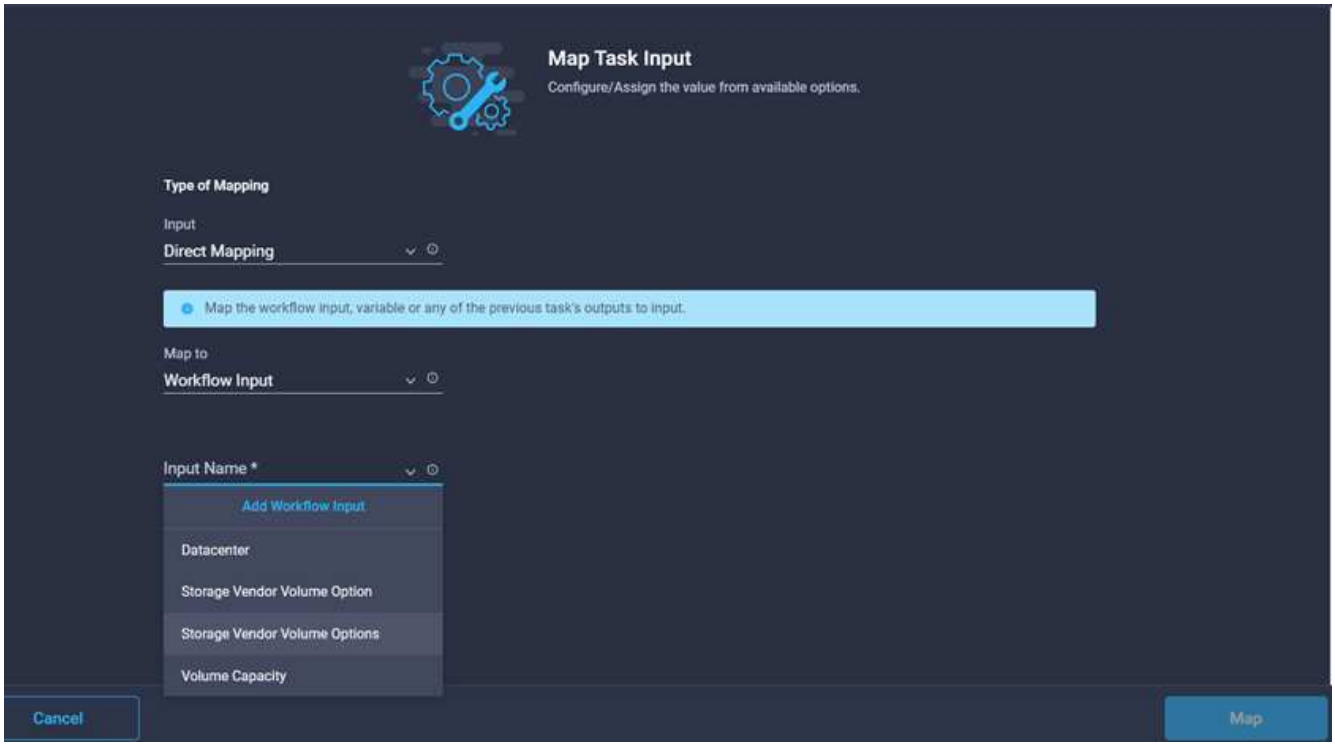
12. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Selezionare **Datacenter** come tipo.

c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
d. Fare clic su **Seleziona data center**.
e. Fare clic sul data center associato al nuovo datastore, quindi fare clic su **Select** (Seleziona).

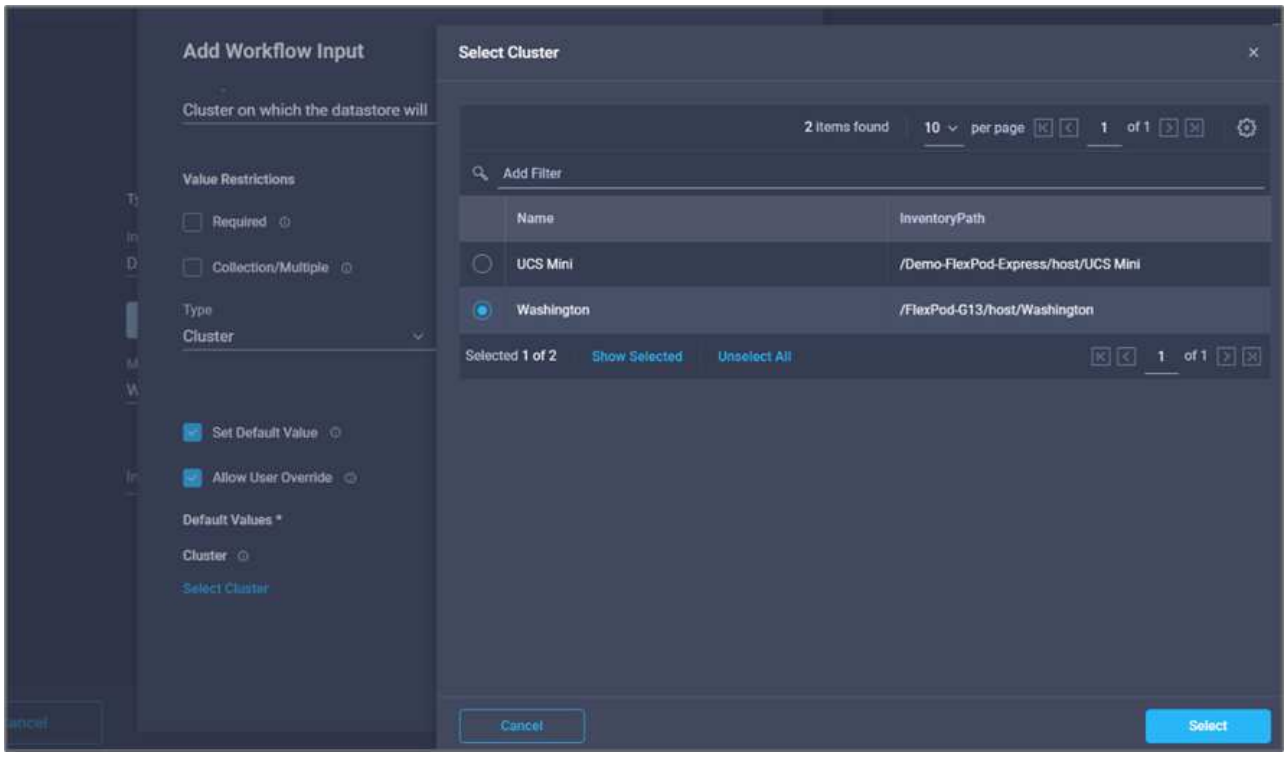


- Fare clic su **Aggiungi**.

13. Fare clic su **Map** (Mappa).
14. Fare clic su **Map** nel campo **Cluster**.
15. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.

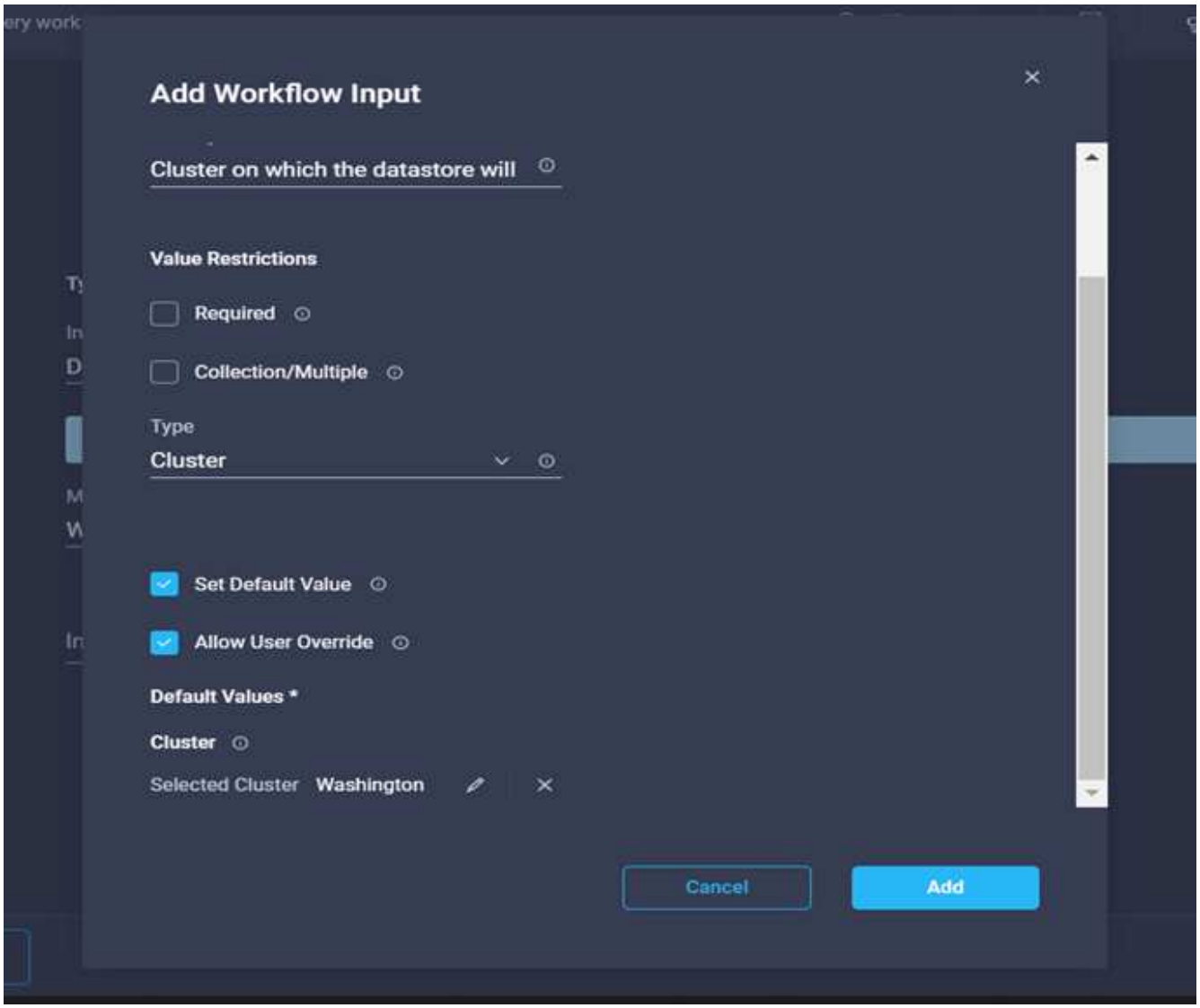


16. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Selezionare Cluster come tipo.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Fare clic su **Select Cluster** (Seleziona cluster).
    f. Fare clic sul cluster associato al nuovo datastore.
    g. Fare clic su **Seleziona**.

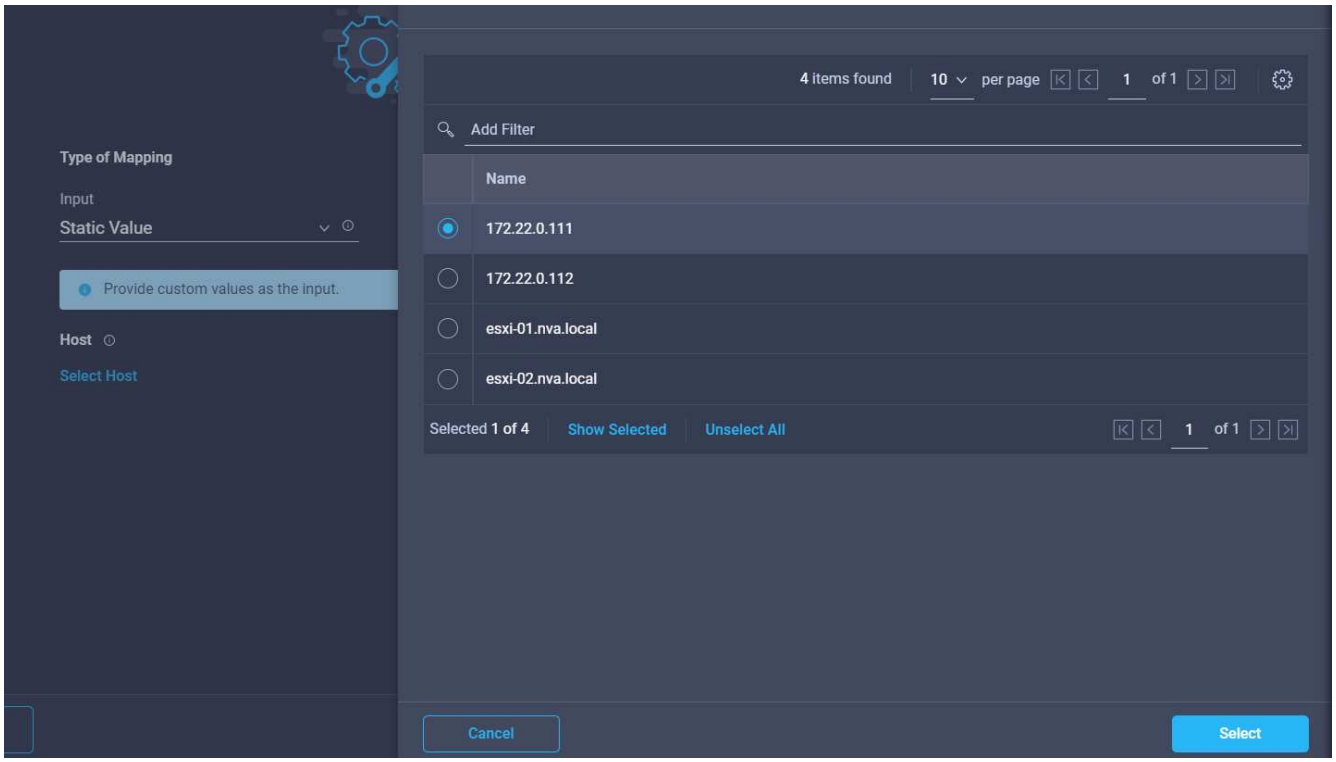


h. Fare clic su **Aggiungi**.

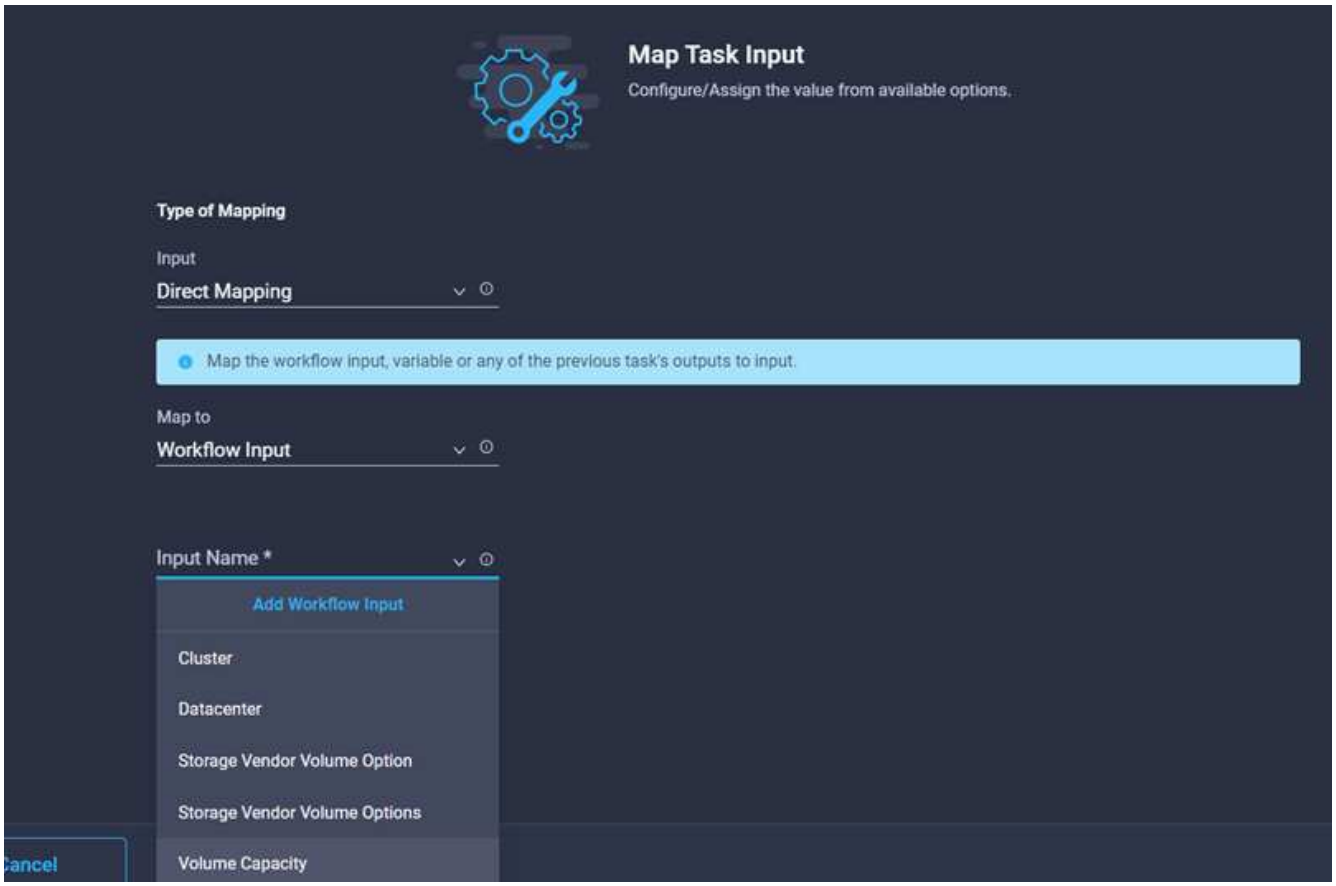
17. Fare clic su **Map** (Mappa).
18. Fare clic su **Map** nel campo **host**.



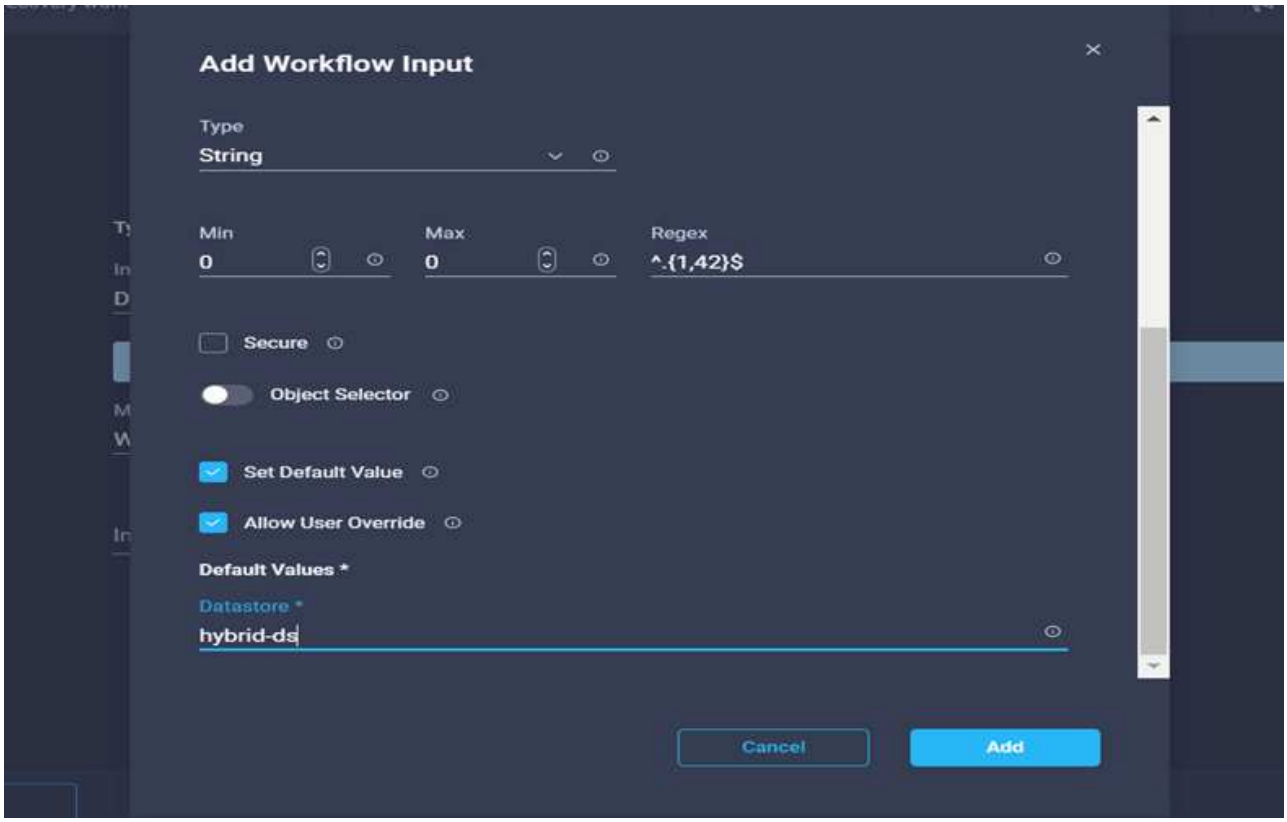
19. Scegliere **Static Value** (valore statico) e fare clic sull'host su cui verrà ospitato il datastore. Se viene specificato un cluster, l'host viene ignorato.



20. Fare clic su **Select and Map** (Seleziona e mappa).
21. Fare clic su **Map** nel campo **Datastore**.
22. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
23. Fare clic su **Input Name** e **Create Workflow Input**.

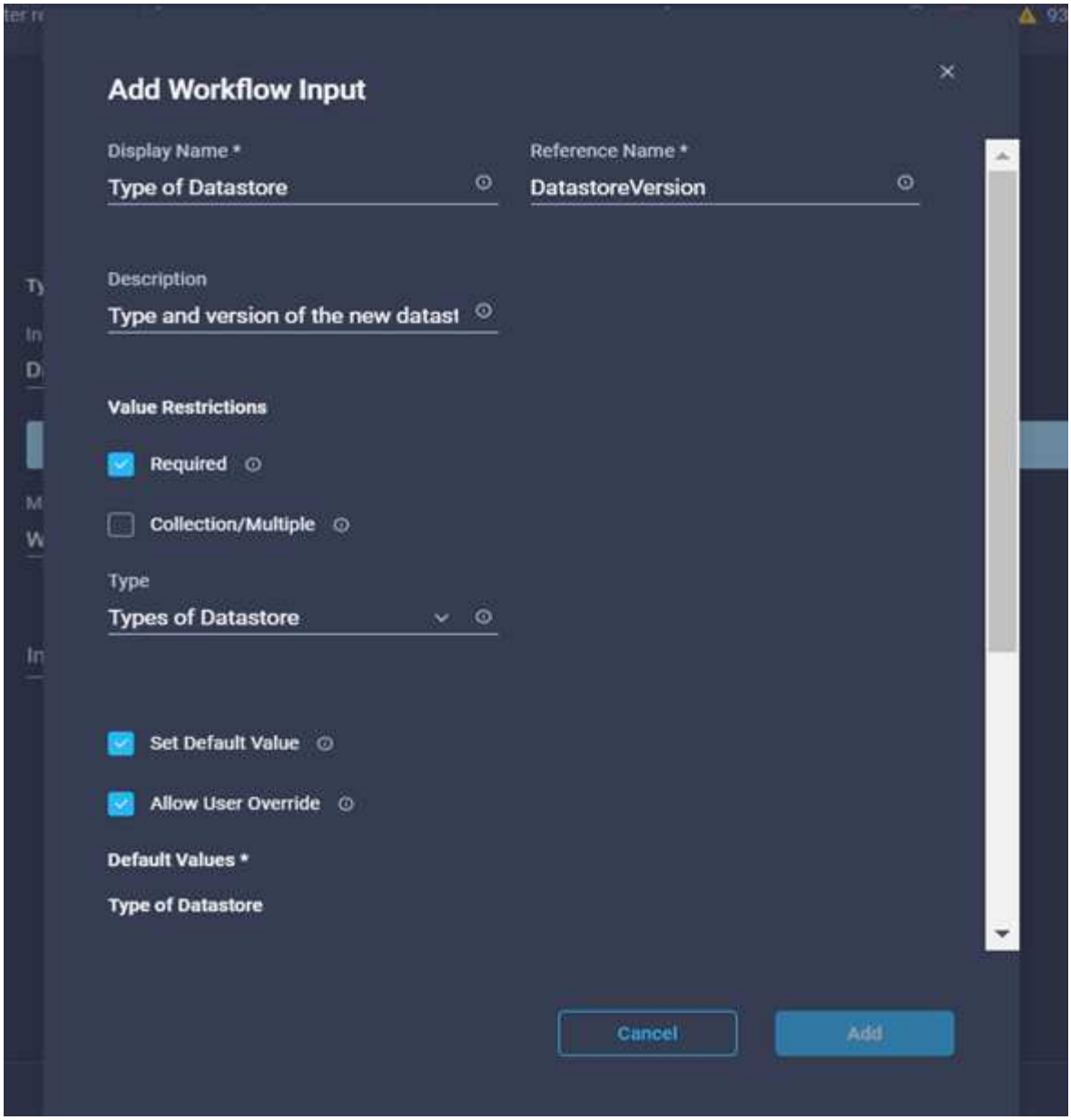


24. Nella procedura guidata Aggiungi input:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fornire un valore predefinito per l'archivio dati e fare clic su **Add** (Aggiungi).



25. Fare clic su **Map** (Mappa).
26. Fare clic su **Map** nel campo di immissione **Type of Datastore**.
27. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
28. Fare clic su **Input Name** e **Create Workflow Input**.

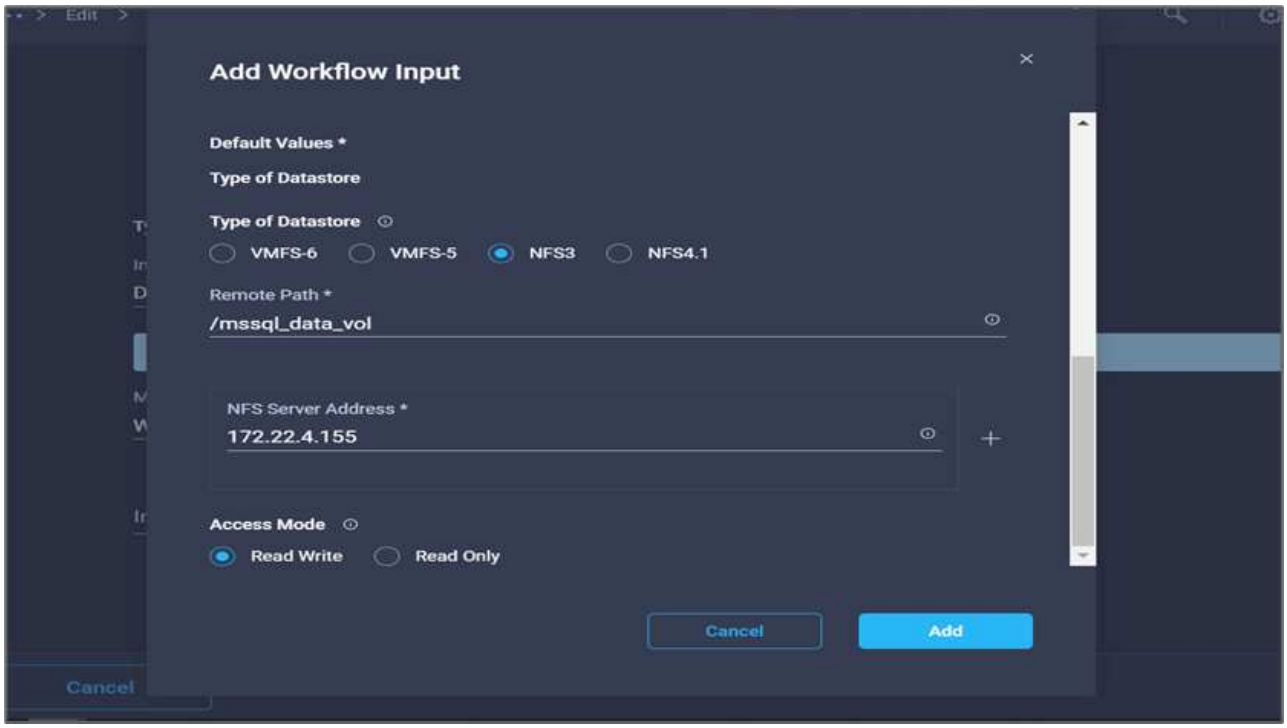
29. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo) e fare clic su **obbligatorio**.
    b. Assicurarsi di selezionare il tipo **tipi di datastore** e fare clic su **Imposta valore predefinito e Ignora**.



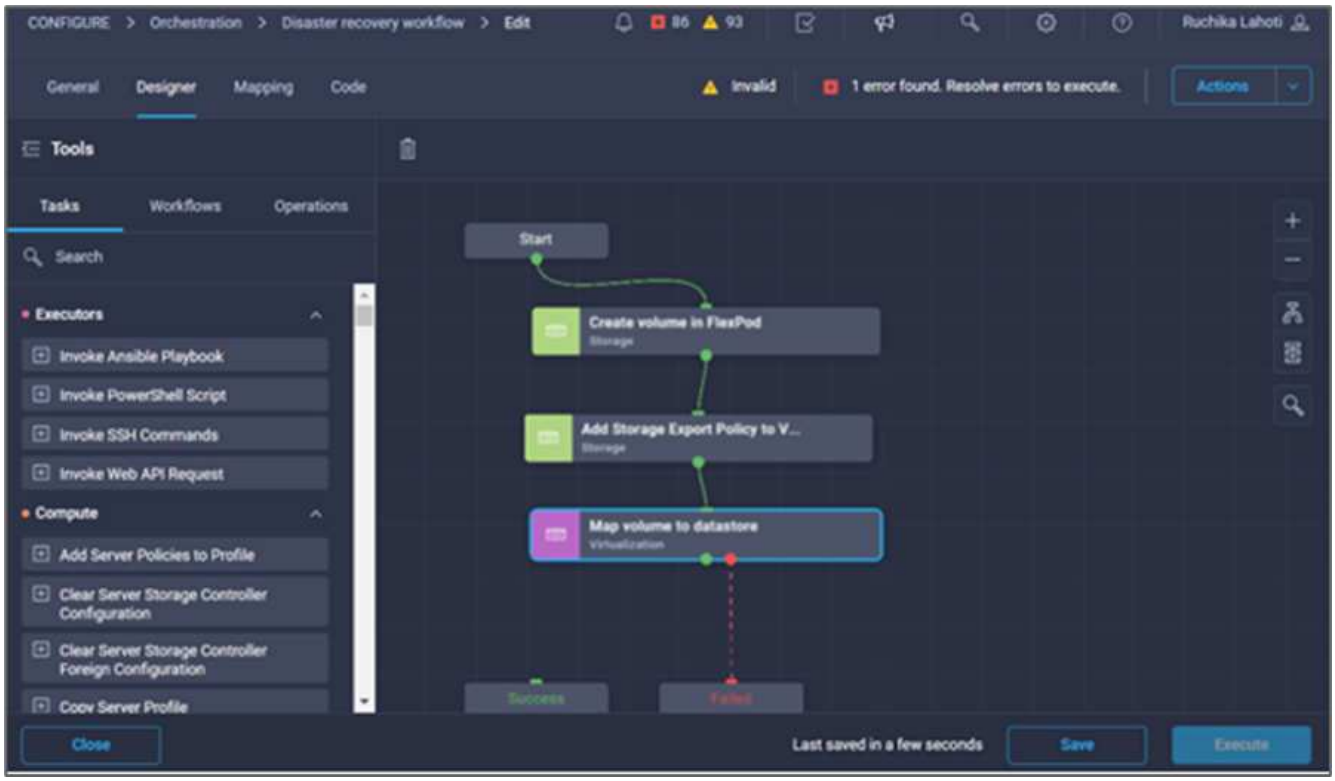
c. Fornire il percorso remoto. Questo è il percorso remoto del punto di montaggio NFS.

d. Fornire i nomi host o gli indirizzi IP del server NFS remoto in NFS Server Address (Indirizzo server NFS).

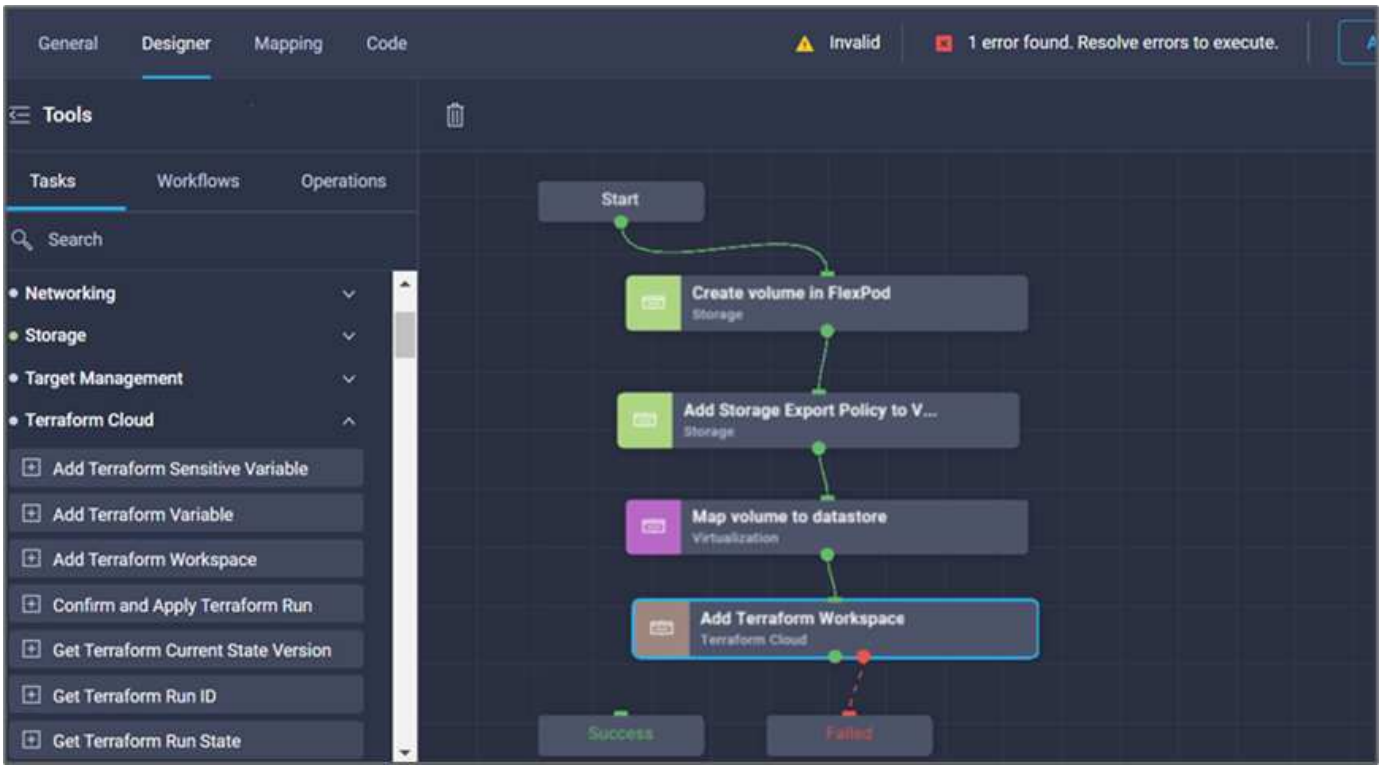
e. Fare clic su **Access Mode** (modalità di accesso). La modalità Access è per il server NFS. Fare clic su Read-only (sola lettura) se i volumi vengono esportati in sola lettura. Fare clic su **Aggiungi**.



30. Fare clic su **Map** (Mappa).
31. Fare clic su **Save** (Salva).

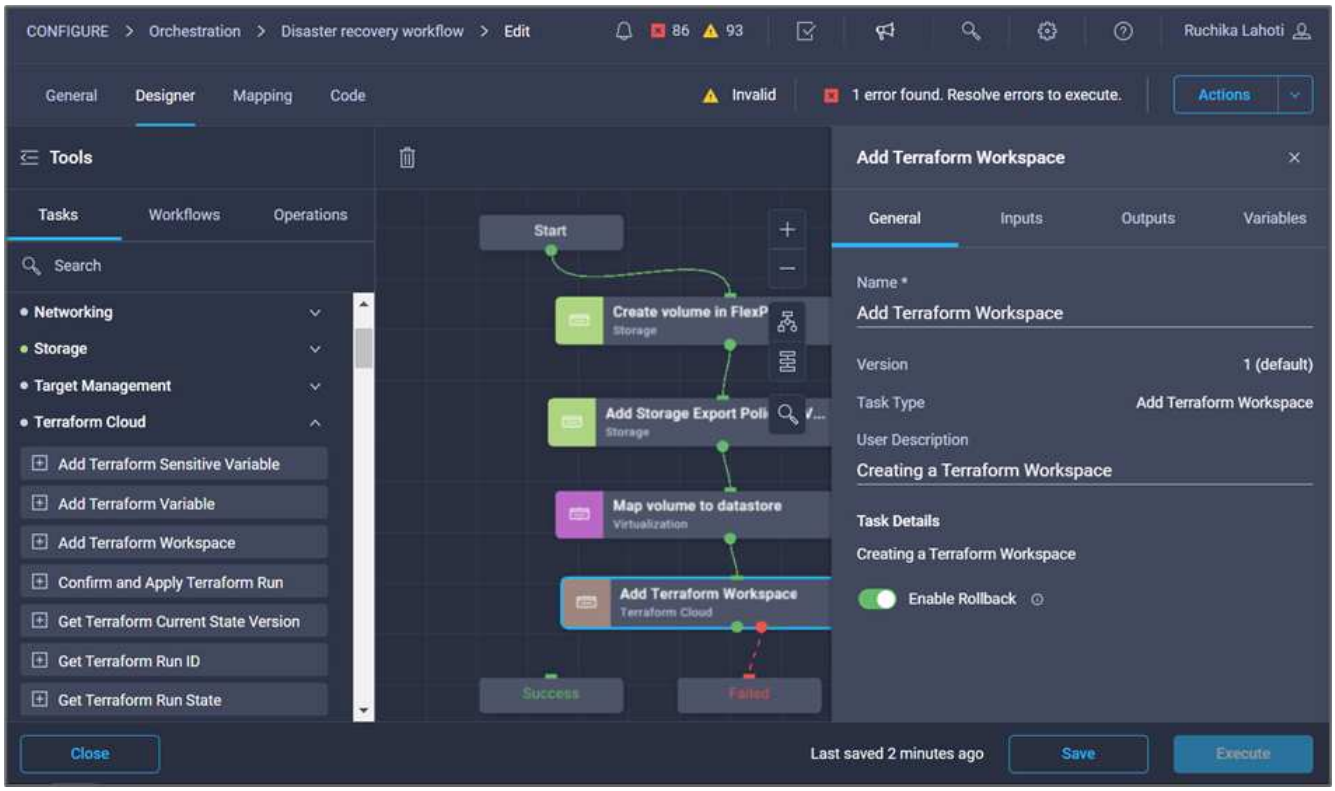


In questo modo viene completata l'attività di creazione dell'archivio dati. Tutte le attività eseguite nel data center FlexPod on-premise sono state completate.

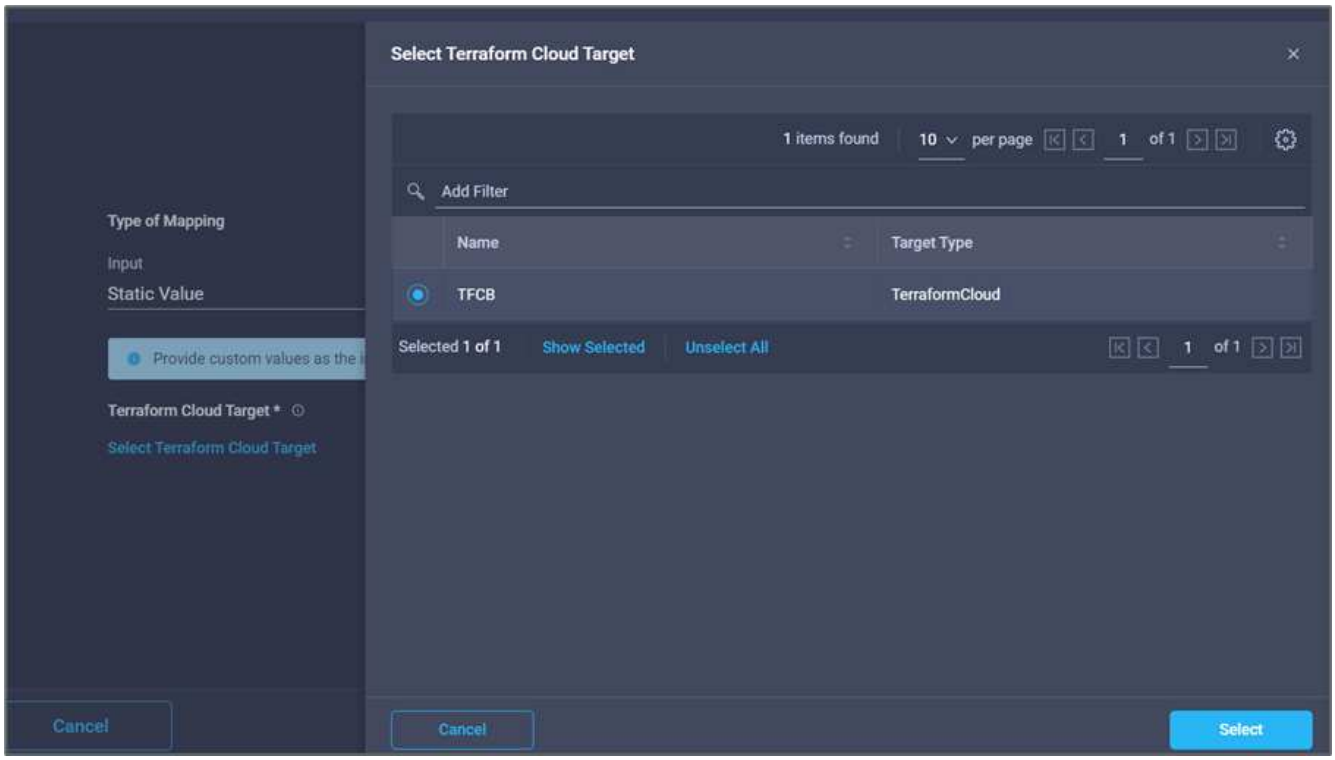


Procedura 5: Aggiungere una nuova area di lavoro Terraform

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Add Terraform Workspace** dalla sezione Tools (Strumenti) dell'area Design (progettazione).
3. Utilizzare Connector per connettere le attività **Map volume to Datastore** e **Add Terraform Workspace** e fare clic su **Save**.
4. Fare clic su **Aggiungi area di lavoro Terraform**. Nell'area Task Properties (Proprietà attività), fare clic sulla scheda **General** (Generale). In alternativa, è possibile modificare il nome e la descrizione dell'attività.

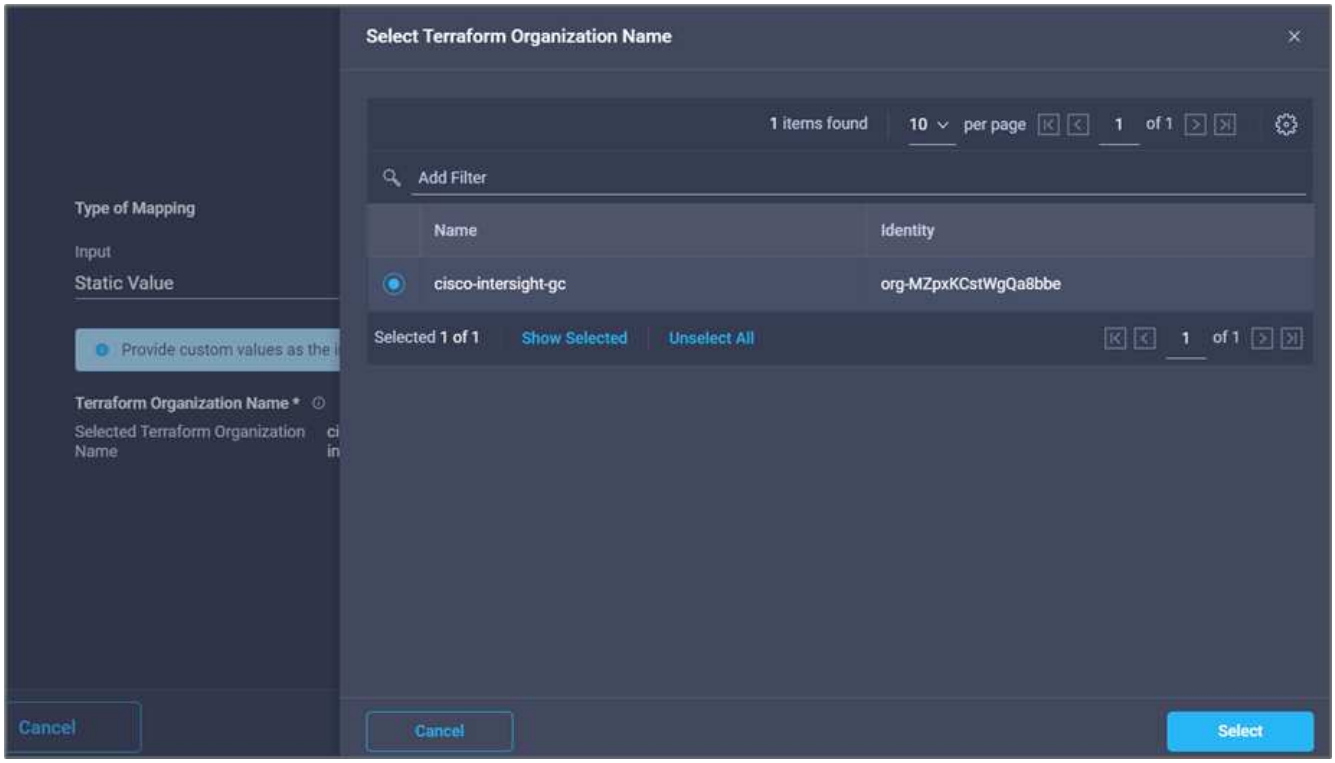


5. Nell'area Task Properties (Proprietà operazione), fare clic su **Input**.
6. Fare clic su **Map** nel campo di immissione **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto come spiegato in "Configurare Cisco Intersight Service per HashiCorp Terraform".".

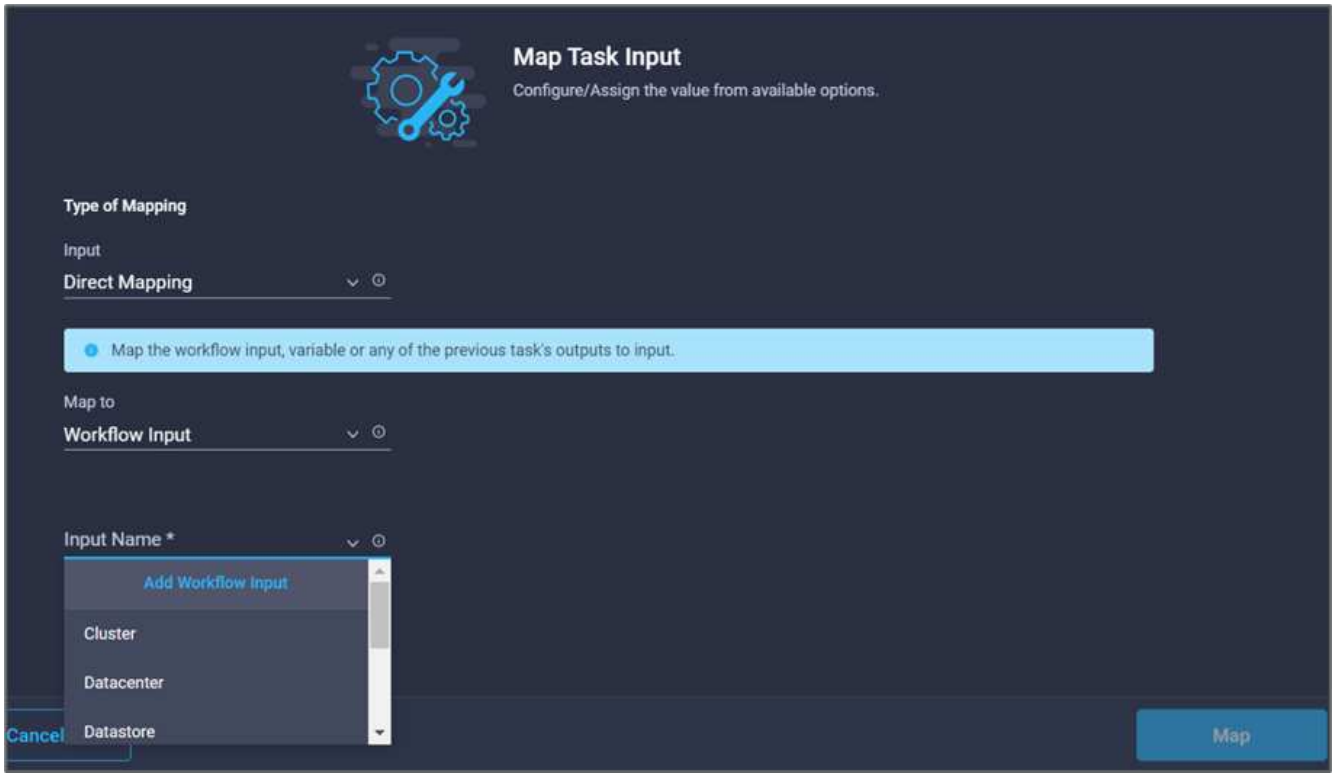


8. Fare clic su **Map** (Mappa).

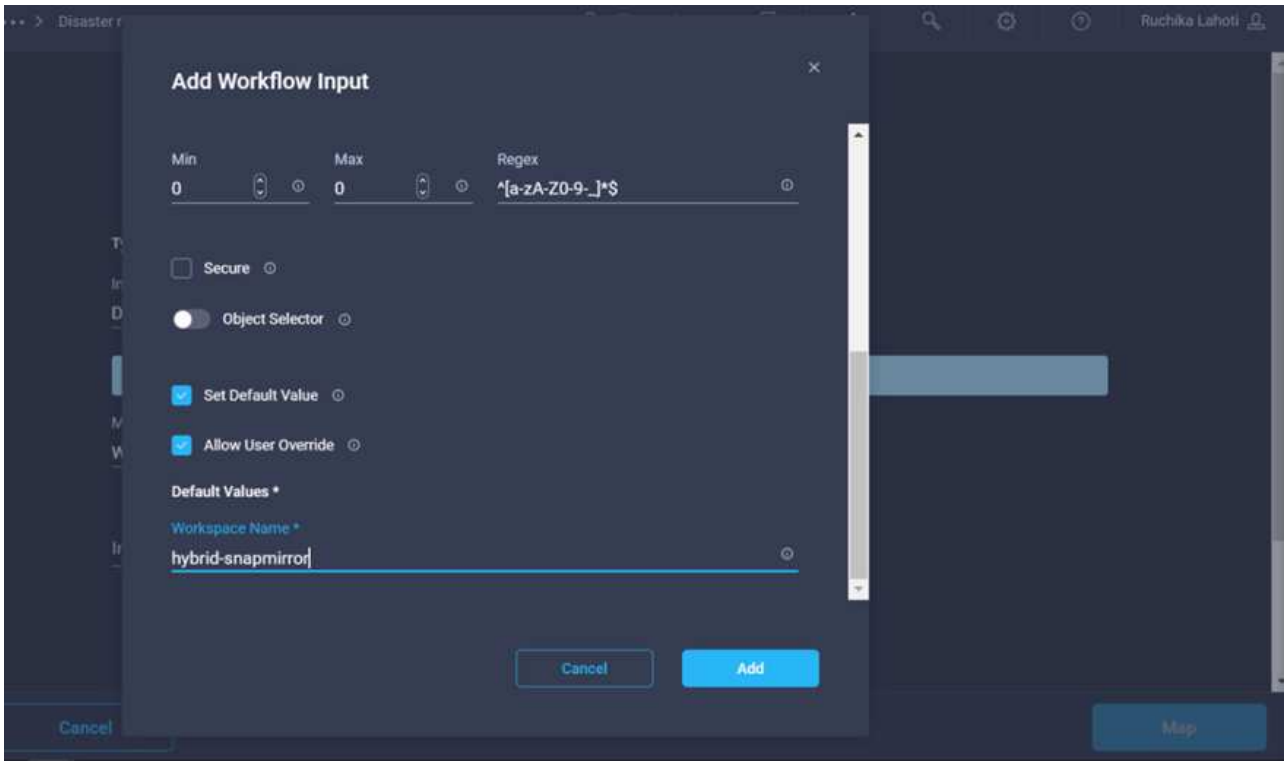
9. Fare clic su **Map** nel campo di immissione **Terraform Organization Name**.
10. Scegliere **Static Value** (valore statico), quindi fare clic su **Select Terraform Organization** (Seleziona organizzazione terraform). Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.



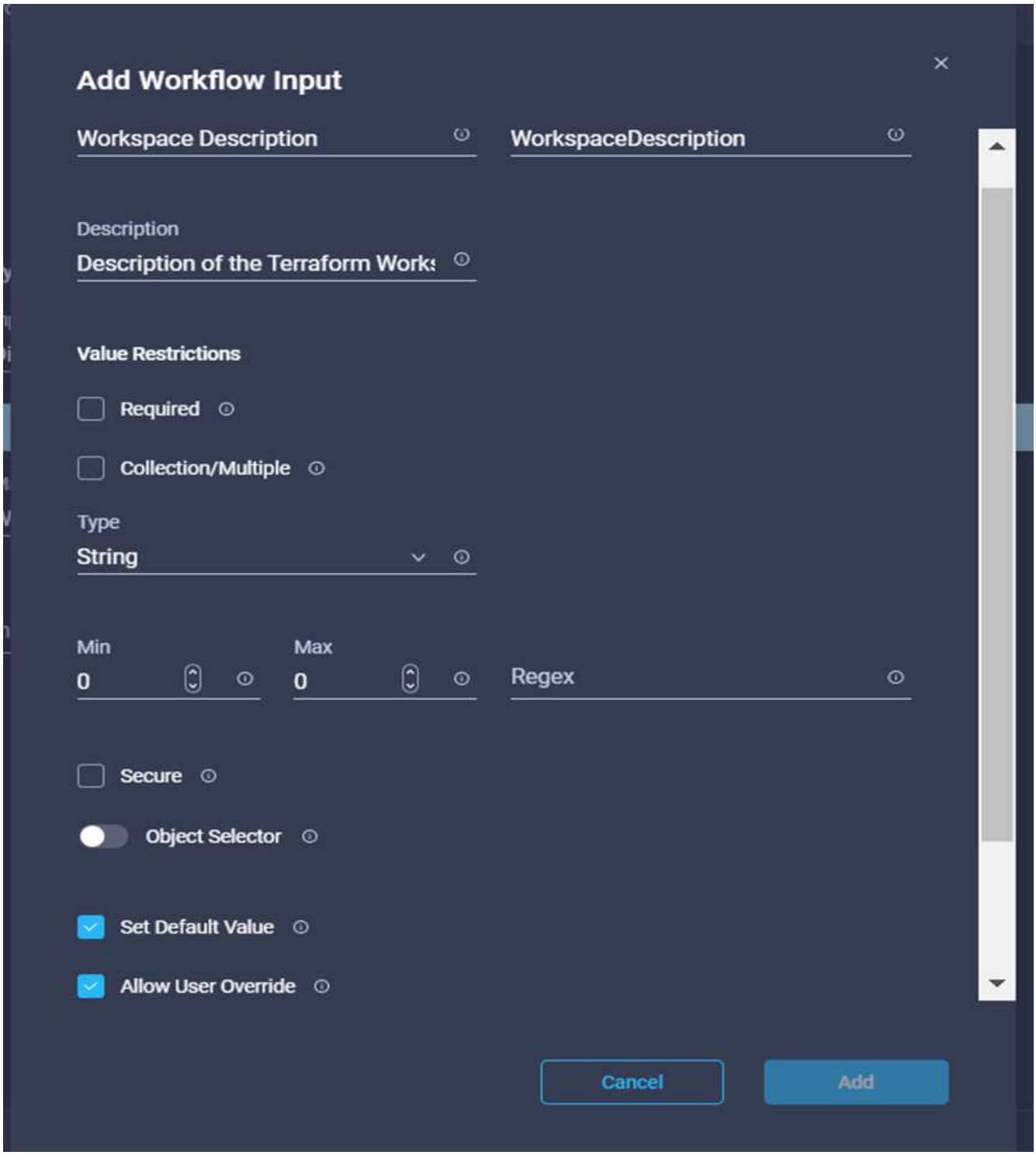
11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**. Questo è il nuovo spazio di lavoro nell'account Terraform Cloud for Business.
13. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
14. Fare clic su **Input Name** e **Create Workflow Input**.



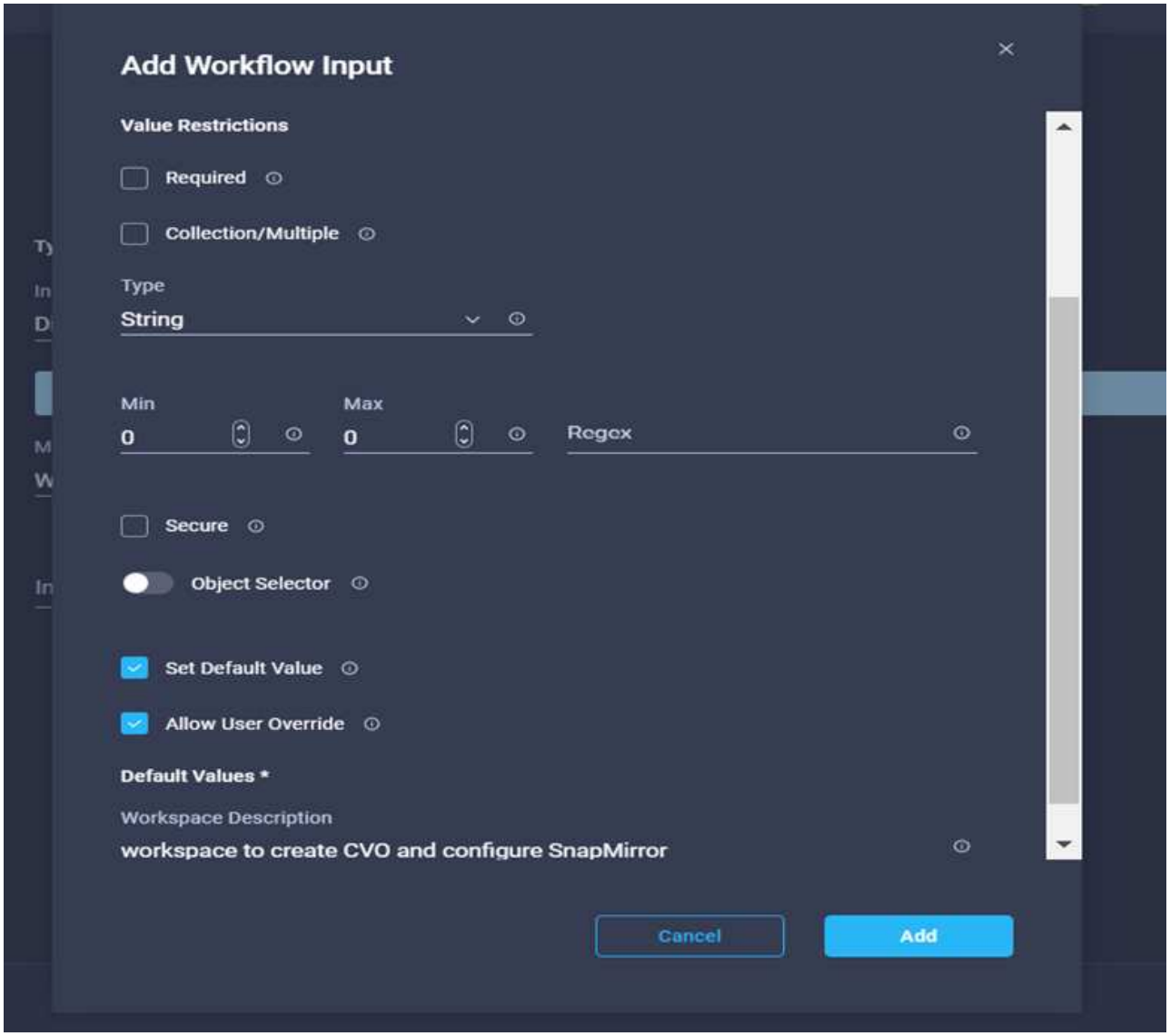
15. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Assicurarsi di selezionare **String** per **Type**.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Specificare un nome predefinito per l'area di lavoro.
    f. Fare clic su **Aggiungi**.



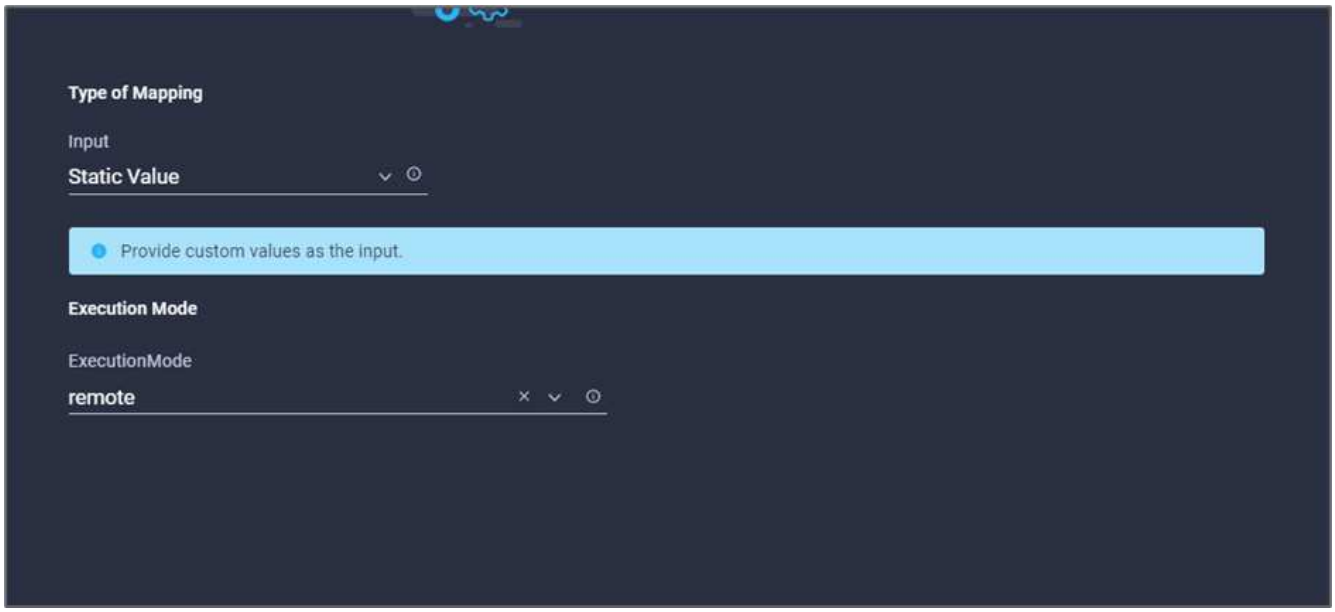
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** (Mappa) nel campo **Workspace Description** (Descrizione area di lavoro).
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.



20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fornire una descrizione dell'area di lavoro e fare clic su **Aggiungi**.



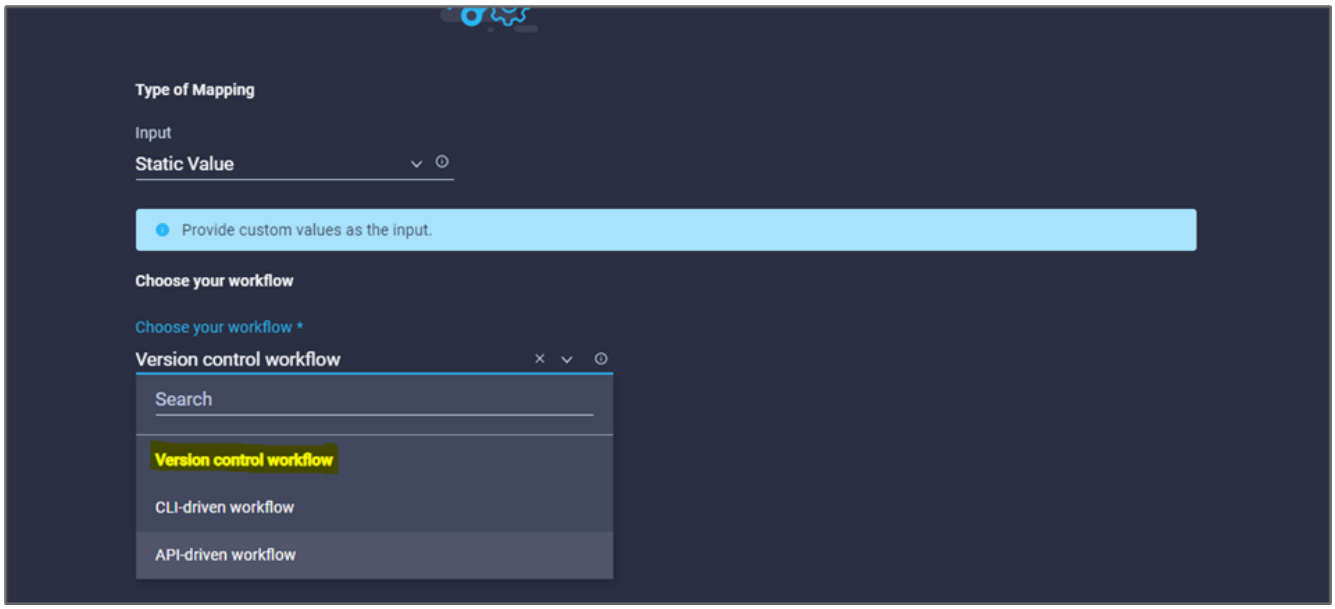
21. Fare clic su **Map** (Mappa).
22. Fare clic su **Map** nel campo **Execution Mode**.
23. Scegliere **valore statico**, fare clic su **modalità di esecuzione**, quindi fare clic su **remoto**.



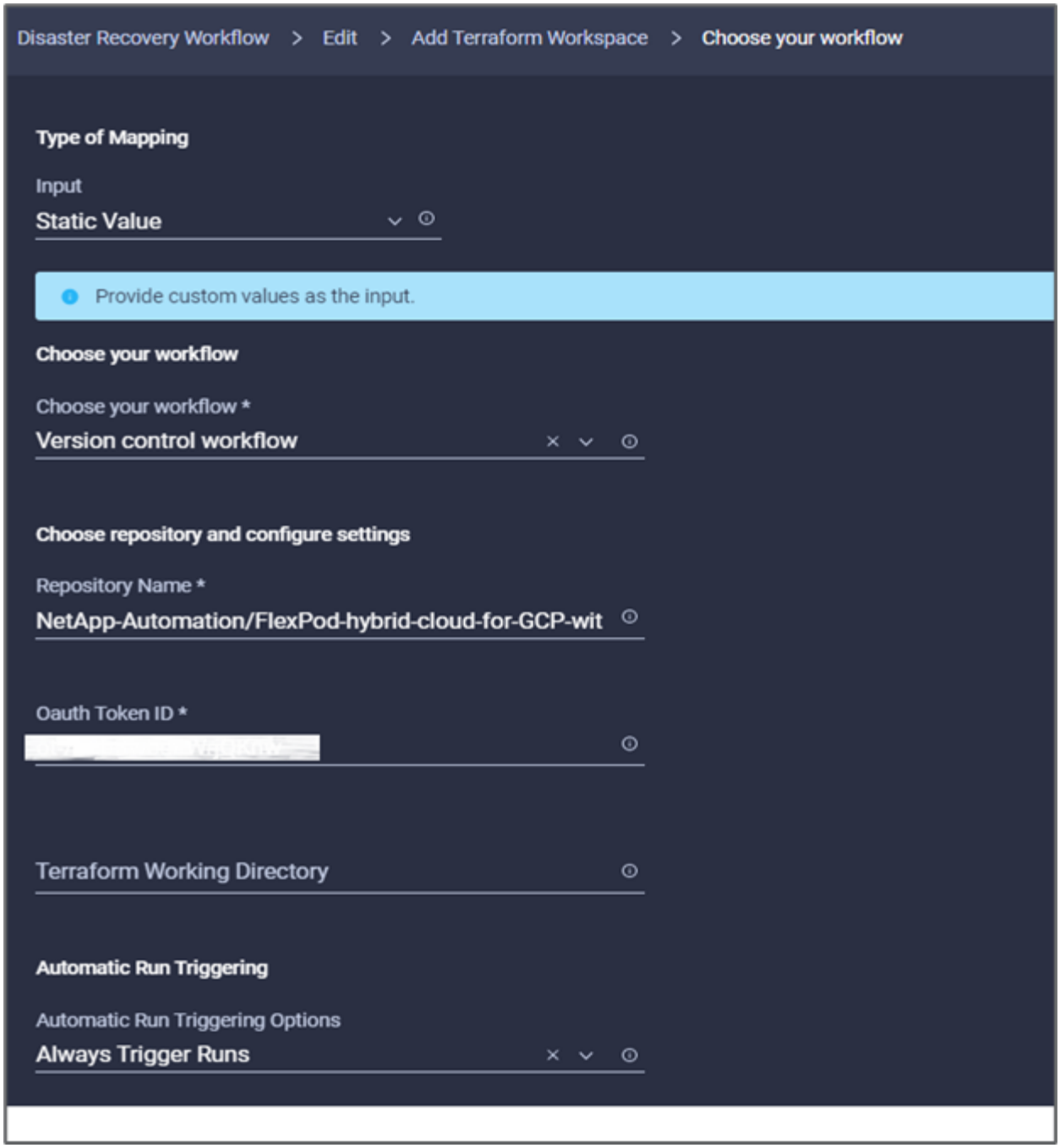
24. Fare clic su **Map** (Mappa).
25. Fare clic su **Map** nel campo **Apply Method** (Applica metodo).
26. Scegliere **valore statico** e fare clic su **Applica metodo**. Fare clic su **Manual Apply** (Applica manuale).

27. Fare clic su **Map** (Mappa).
28. Fare clic su **Map** (Mappa) nel campo **User Interface** (interfaccia utente).
29. Scegliere **Static Value** (valore statico) e fare clic su **User Interface** (interfaccia utente). Fare clic su **Console UI**.

30. Fare clic su **Map** (Mappa).
31. Fare clic su **Map** nel campo di immissione e selezionare il flusso di lavoro.
32. Selezionare **valore statico** e fare clic su **Scegli il flusso di lavoro**. Fare clic su **Version Control Workflow**.



33. Fornire i seguenti dettagli sul repository GitHub:
    a. In **Repository Name** (Nome repository), immettere il nome del repository descritto nella sezione ""Configurazione dei prerequisiti dell'ambiente"".
    b. Fornire l'ID token OAuth come descritto in dettaglio nella sezione ""Configurazione dei prerequisiti dell'ambiente"".
    c. Selezionare l'opzione **Automatic Run Triggering**.



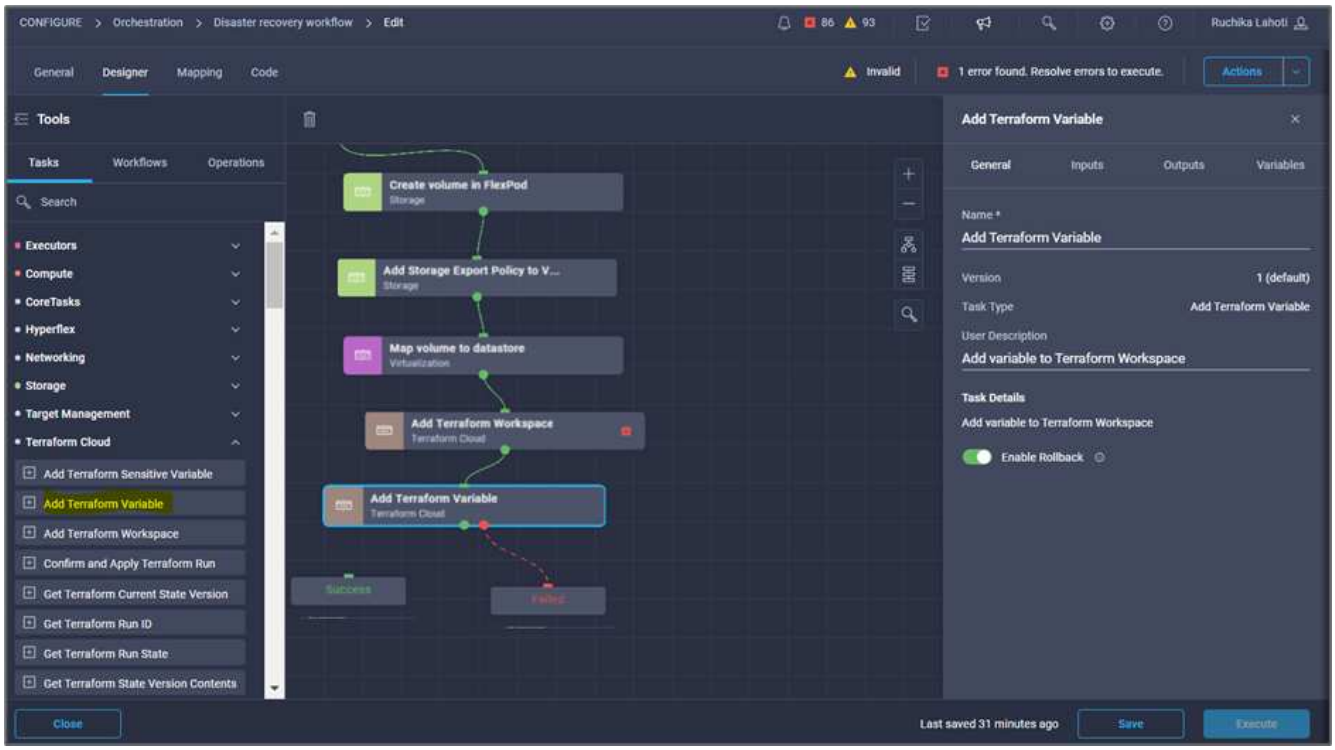
34. Fare clic su **Map** (Mappa).
35. Fare clic su **Save** (Salva).

In questo modo viene completata l'attività di creazione di uno spazio di lavoro in un account Terraform Cloud for Business.

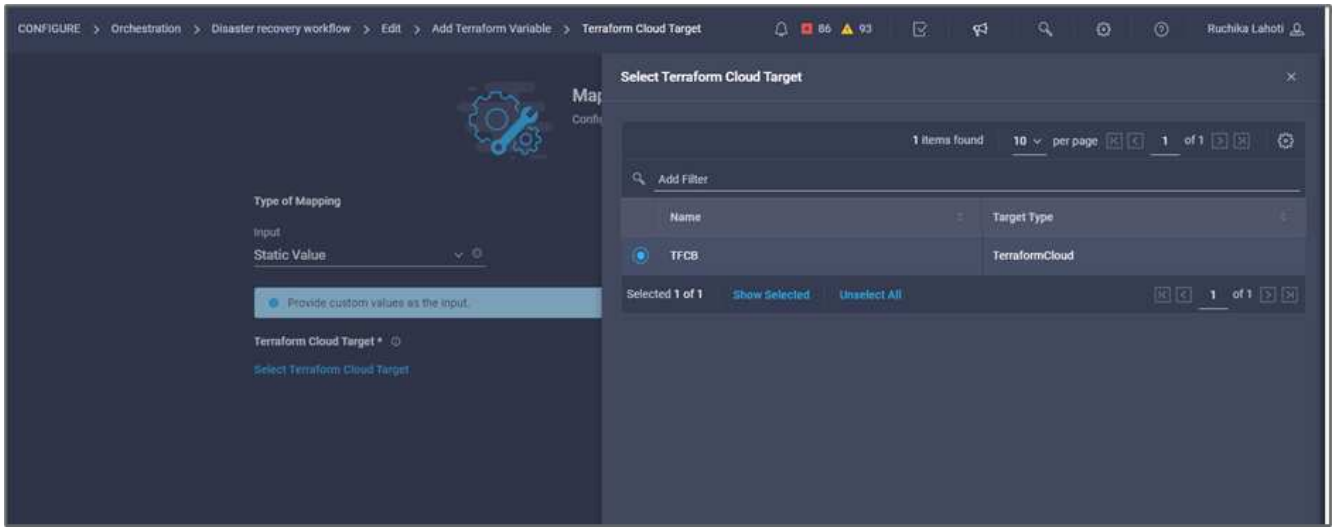
Procedura 6: Aggiunta di variabili non sensibili all'area di lavoro

1. Accedere alla scheda **Designer** e fare clic sulla sezione **flussi di lavoro da Strumenti**.
2. Trascinare il flusso di lavoro **Terraform > Add Terraform Variables** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le attività **Add Terraform Workspace** e **Add Terraform Variables**. Fare clic su **Save** (Salva).

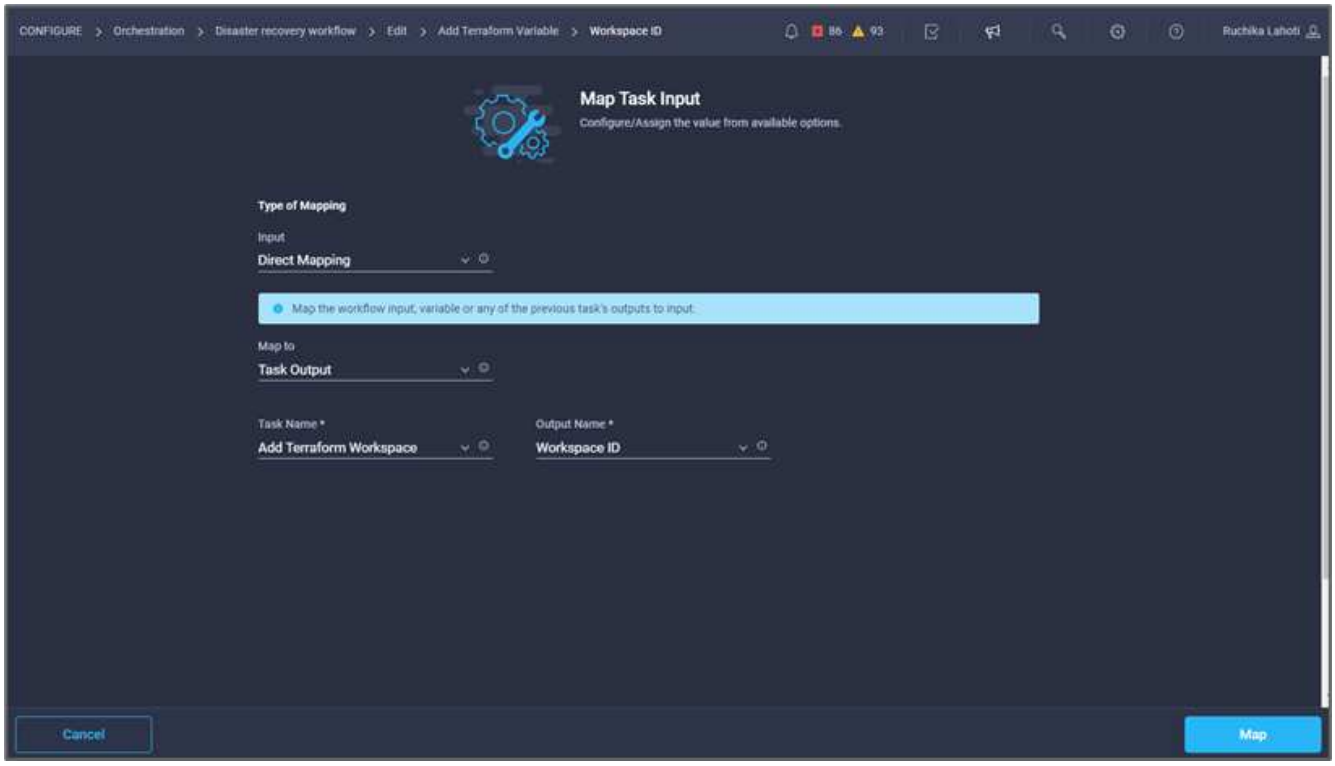
4. Fare clic su **Aggiungi variabili terraform**. Nell'area **Workflow Properties** (Proprietà flusso di lavoro), fare clic sulla scheda **General** (Generale). In alternativa, è possibile modificare il nome e la descrizione dell'attività.



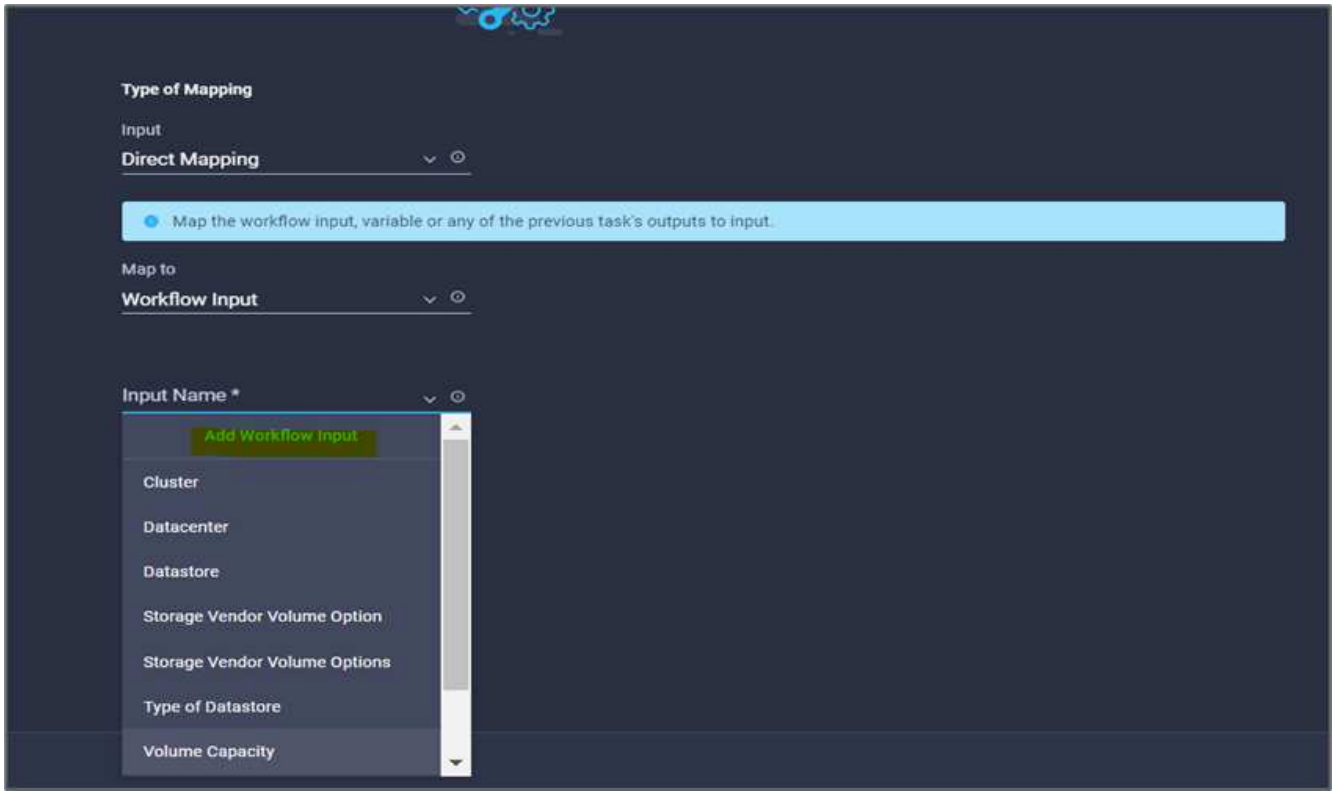
5. Nell'area **Workflow Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto come spiegato in "Configurare Cisco Intersight Service per HashiCorp Terraform".".



8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo *Terraform Organization Name *.
10. Scegliere **valore statico** e fare clic su **Seleziona organizzazione terraform**. Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.

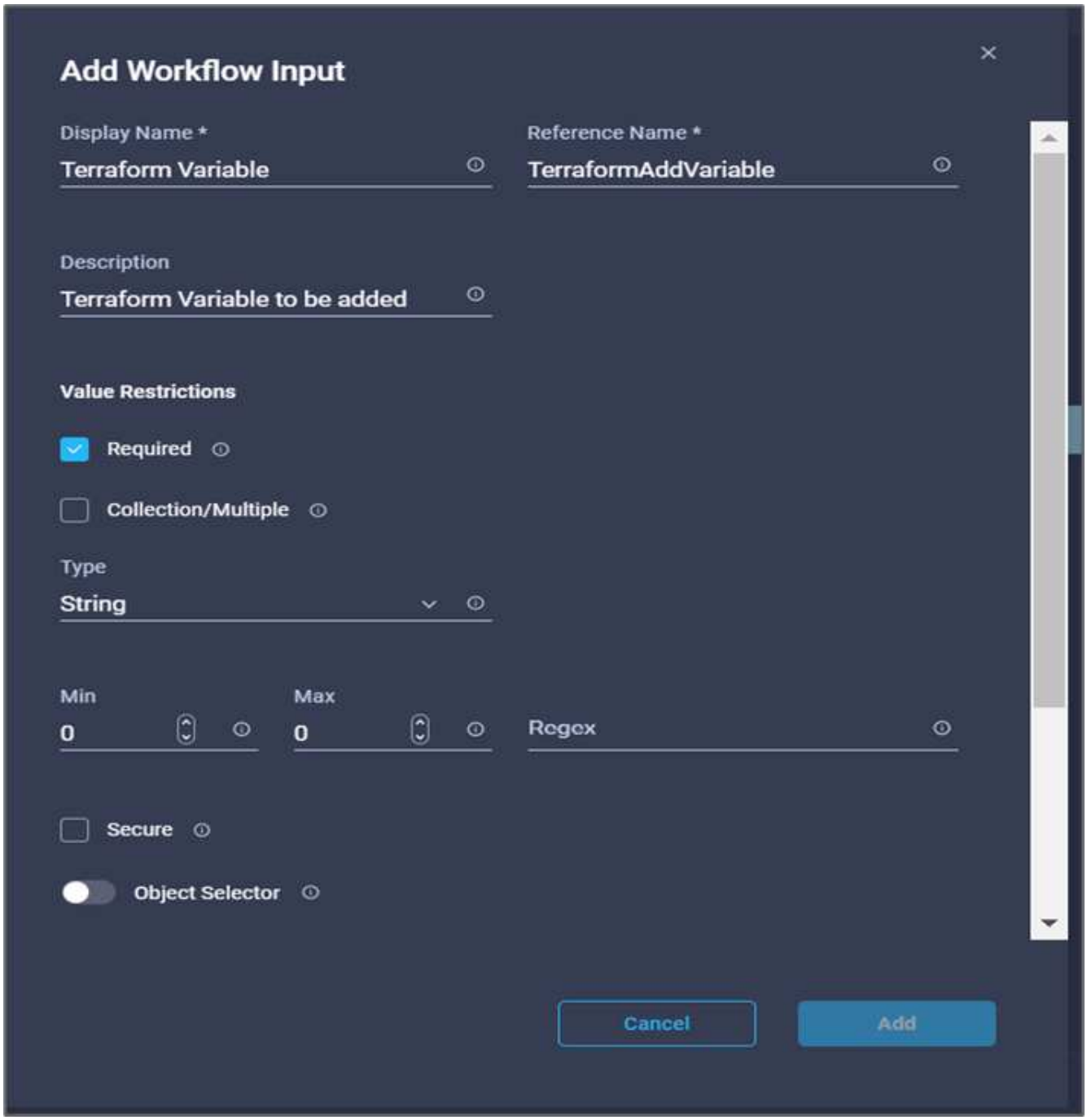


11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**.
13. Scegliere **Direct Mapping** e fare clic su **Task Output**.
14. Fare clic su **Nome attività** e fare clic su **Aggiungi area di lavoro terraform**.



15. Fare clic su **Output Name** (Nome output) e su **Workspace Name** (Nome area di lavoro).

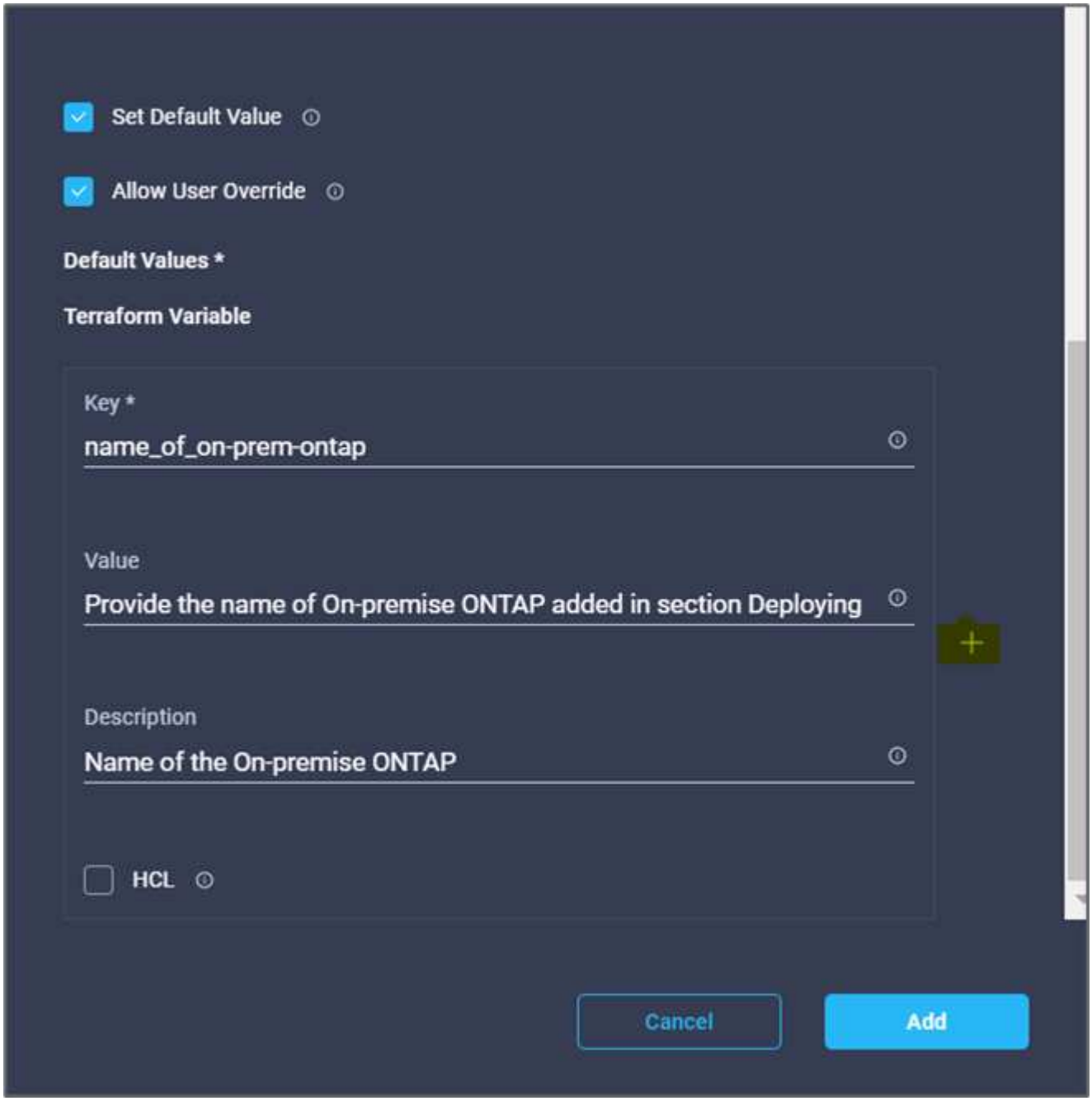
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Add Variables Options**.
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.



20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (opzionale).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fare clic su **Variable Type** (tipo di variabile), quindi su **non-sensitive Variables** (variabili non

sensibili).

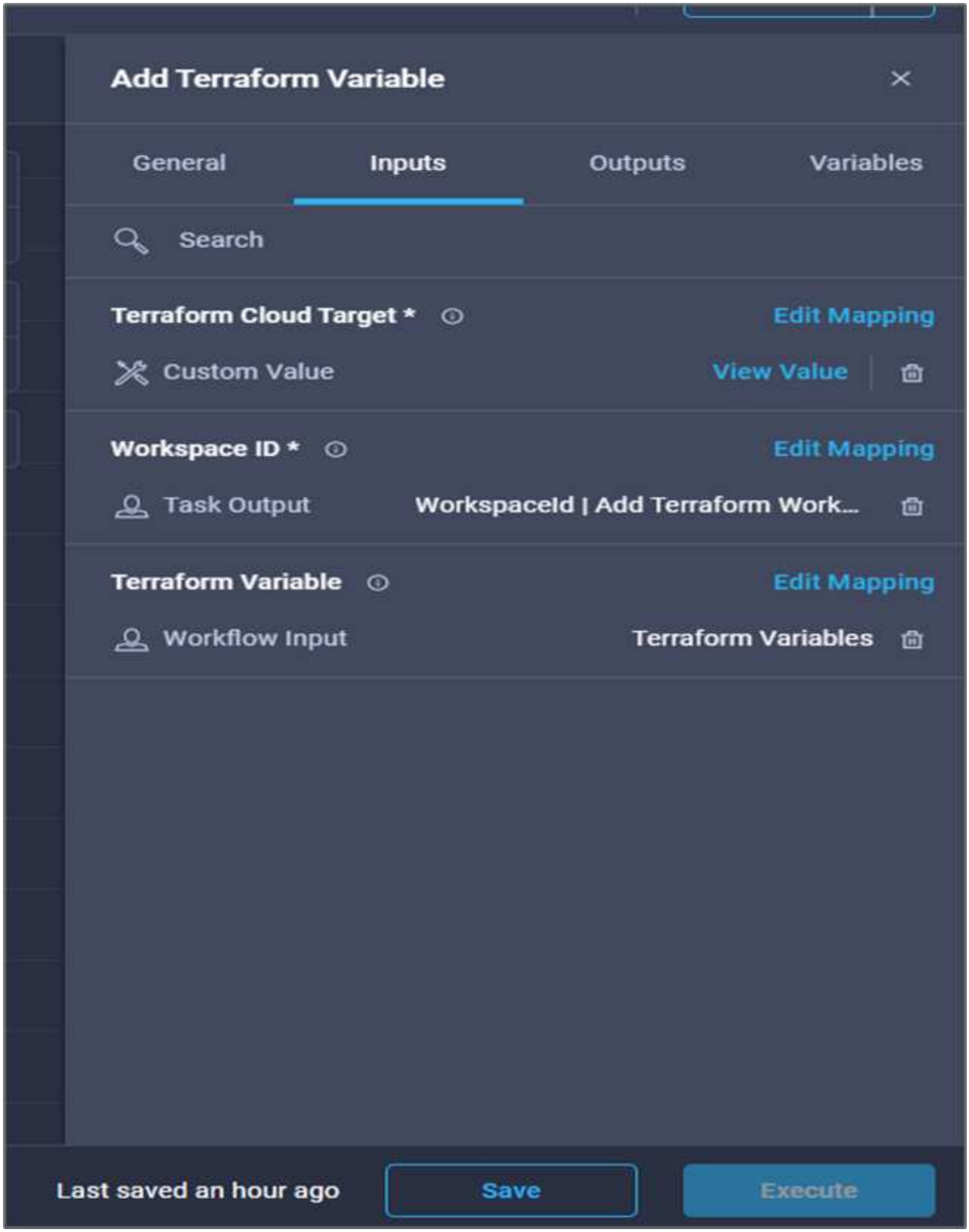
21. Nella sezione **Add Terraform Variables**, fornire le seguenti informazioni:
    - **Chiave.** `name_of_on-prem-ontap`
    - **Value.** indica il nome di on-premise ONTAP.
    - **Descrizione.** Nome del ONTAP on-premise.
22. Fare clic su **+** per aggiungere ulteriori variabili.



23. Aggiungere tutte le variabili Terraform come mostrato nella tabella seguente. È inoltre possibile specificare un valore predefinito.

Nome della variabile terraform	Descrizione
name_of_on-premise-ontap	Nome del FlexPod (on-premise ONTAP)
ip_cluster_ontap on-premise	L'indirizzo IP dell'interfaccia di gestione del cluster di storage
nome_utente_ontap_on-premise	Nome utente amministratore per il cluster di storage
Zona	Regione GCP in cui verrà creato l'ambiente di lavoro
subnet_id	id subnet GCP in cui verrà creato l'ambiente di lavoro
id_vpc	L'ID VPC in cui verrà creato l'ambiente di lavoro
nome_pacchetto_capacità	Il tipo di licenza da utilizzare
volume_origine	Il nome del volume di origine
source_storage_vm_name	Il nome della SVM di origine
destination_volume	Nome del volume su Cloud Volumes ONTAP
schedule_of_replication	L'impostazione predefinita è 1 ora
name_of_volume_to_create_on_cvo	Nome del volume cloud
id_area di lavoro	L'id_area di lavoro in cui verrà creato l'ambiente di lavoro
ID_progetto	l'id_progetto in cui verrà creato l'ambiente di lavoro
name_of_cvo_cluster	Il nome dell'ambiente di lavoro Cloud Volumes ONTAP
account_servizio_gcp	account_servizio_gcp dell'ambiente di lavoro Cloud Volumes ONTAP

24. Fare clic su **Map** (Mappa), quindi su **Save** (Salva).



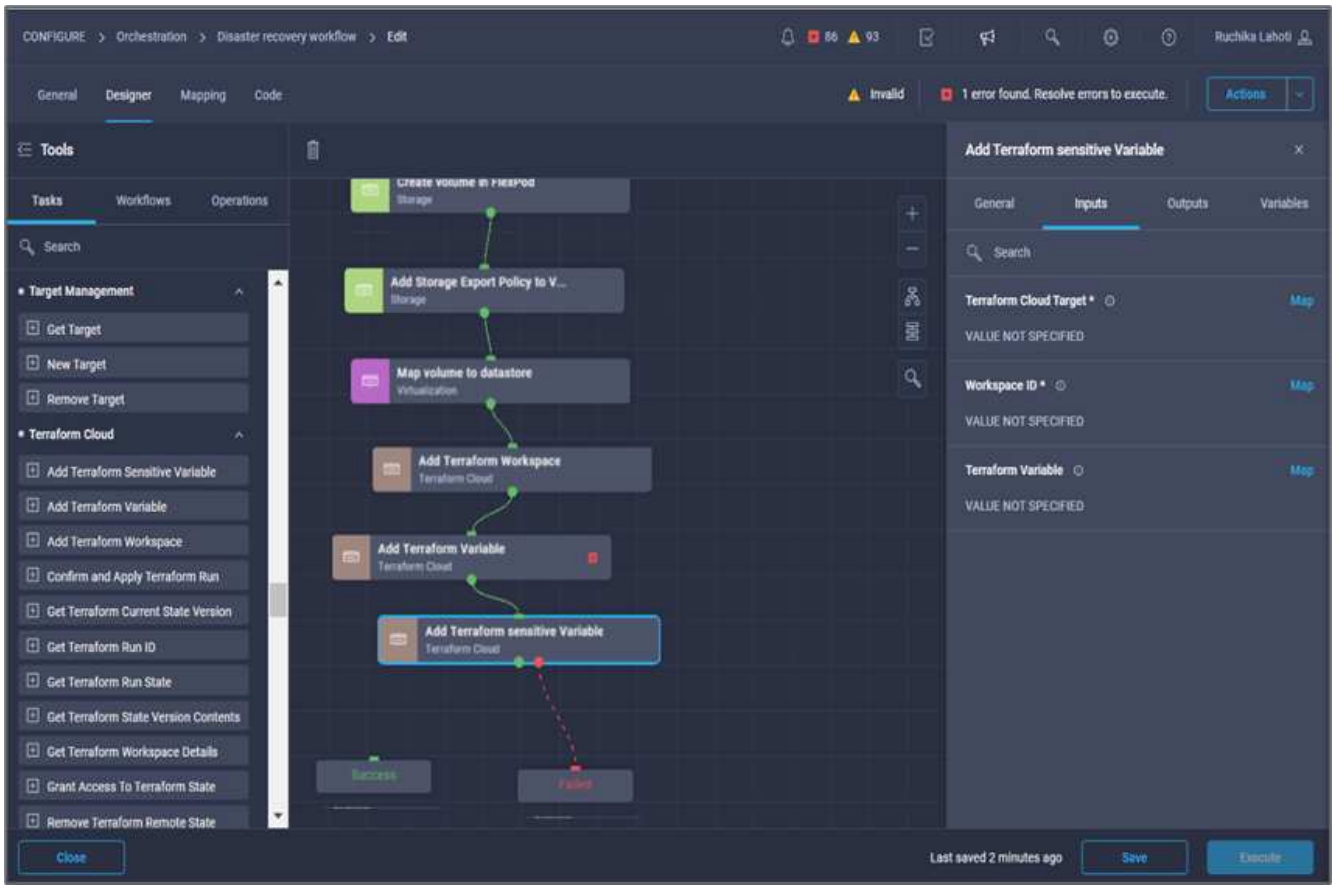
In questo modo viene completata l'attività di aggiunta delle variabili Terraform richieste all'area di lavoro. Quindi, aggiungere le variabili Terraform sensibili richieste all'area di lavoro. È inoltre possibile combinare entrambi in un'unica attività.

Procedura 7: Aggiunta di variabili sensibili a un'area di lavoro

1. Accedere alla scheda **Designer** e fare clic su **workflow** nella sezione **Strumenti**.
2. Trascinare il flusso di lavoro **Terraform > Add Terraform Variables** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le due attività **Add Terraform Workspace**. Fare clic su **Save** (Salva).

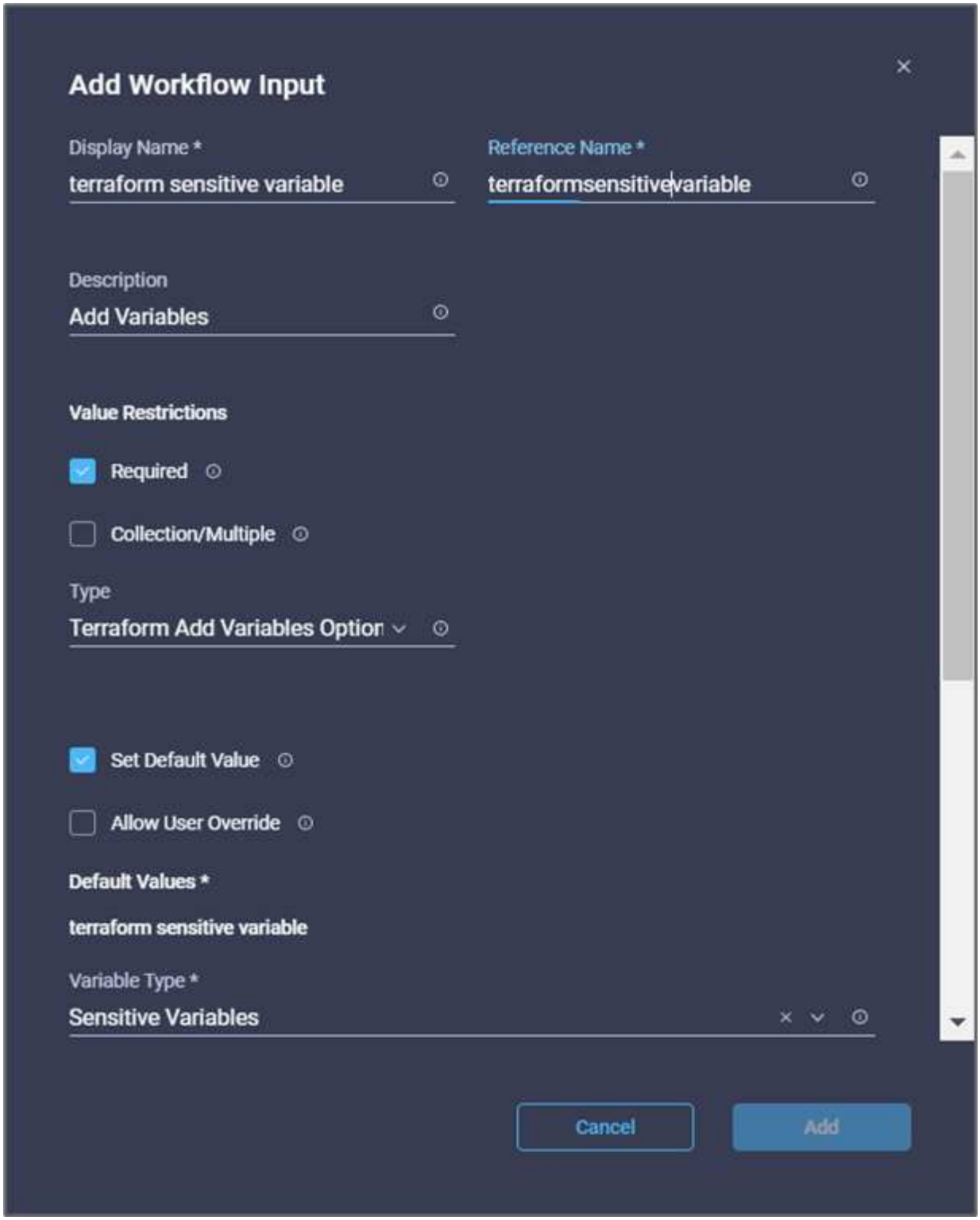
> Viene visualizzato un avviso che indica che le due attività hanno lo stesso nome. Ignorare l'errore per ora perché si modifica il nome dell'attività nel passaggio successivo.

4. Fare clic su **Aggiungi variabili terraform**. Nell'area **Workflow Properties** (Proprietà flusso di lavoro), fare clic sulla scheda **General** (Generale). Modificare il nome in **Aggiungi variabili sensibili al terraform**.



5. Nell'area **Workflow Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Seleziona l'account Terraform Cloud for Business che è stato aggiunto nella sezione "Configurare Cisco Intersight Service per HashiCorp Terraform"."
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Terraform Organization Name**.
10. Scegliere **valore statico** e fare clic su **Seleziona organizzazione terraform**. Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.
11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**.

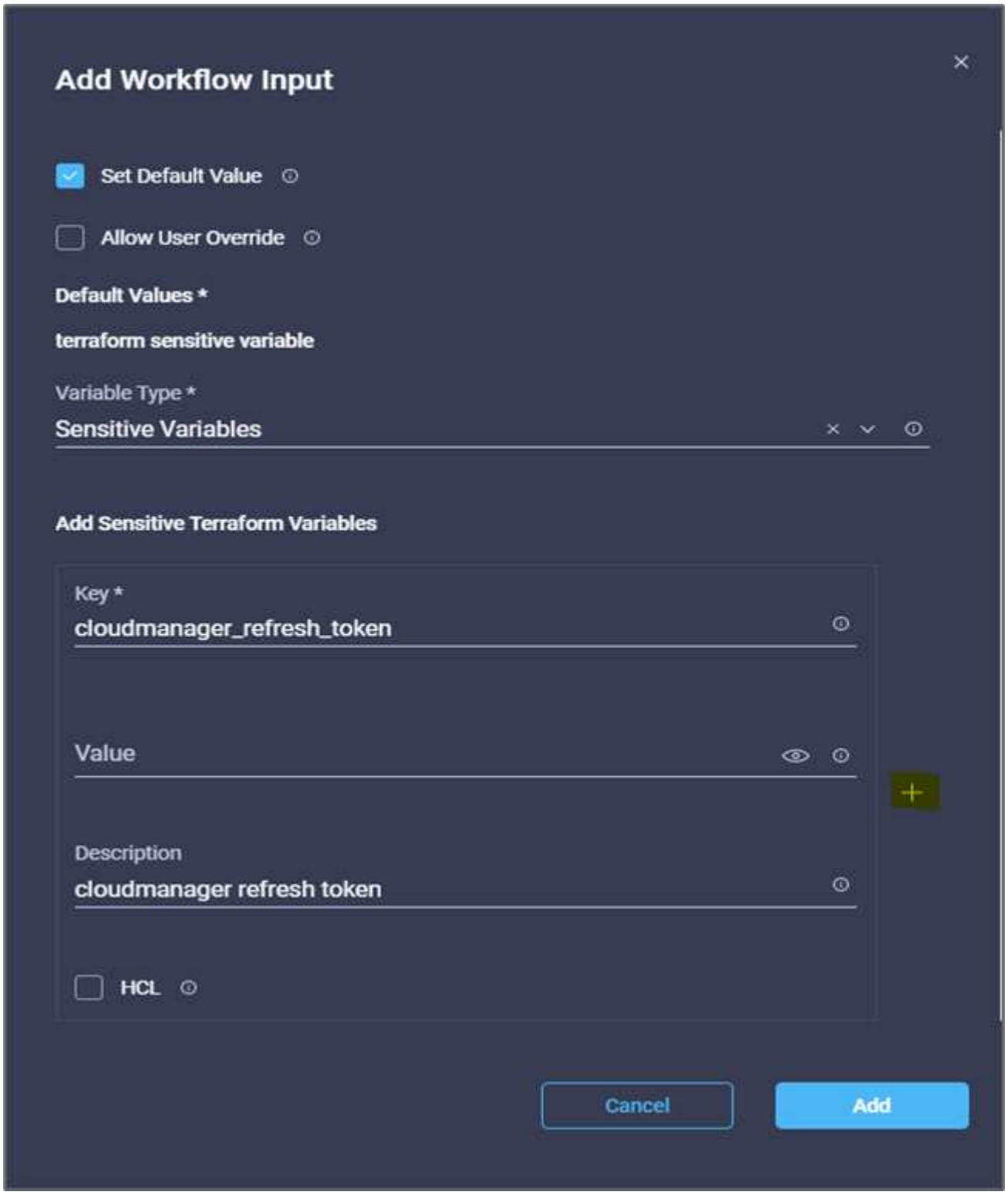
13. Scegliere **Direct Mapping** e fare clic su **Task Output**.
14. Fare clic su **Nome attività**, quindi su **Aggiungi area di lavoro terraform**.
15. Fare clic su **Output Name** (Nome output) e selezionare l'output **Workspace Name** (Nome area di lavoro).
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Add Variables Options**.
18. Scegliere **Direct Mapping**, quindi fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.
20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **Terraform Add Variables Options** per il tipo.
    c. Fare clic su **Set Default Value** (Imposta valore predefinito).
    d. Fare clic su **Variable Type** (tipo variabile), quindi su **Sensitive Variables** (variabili sensibili).
    e. Fare clic su **Aggiungi**.



21. Nella sezione **Add Terraform Variables**, fornire le seguenti informazioni:

    - **Chiave.** `cloudmanager_refresh_token`.
    - **Valore.** inserire il token di refresh per le operazioni API di NetApp Cloud Manager.
    - **Descrizione.** Aggiorna token.

Per ulteriori informazioni su come ottenere un token di refresh per le operazioni API di NetApp Cloud Manager, consulta la sezione ""Configurazione dei prerequisiti dell'ambiente"."



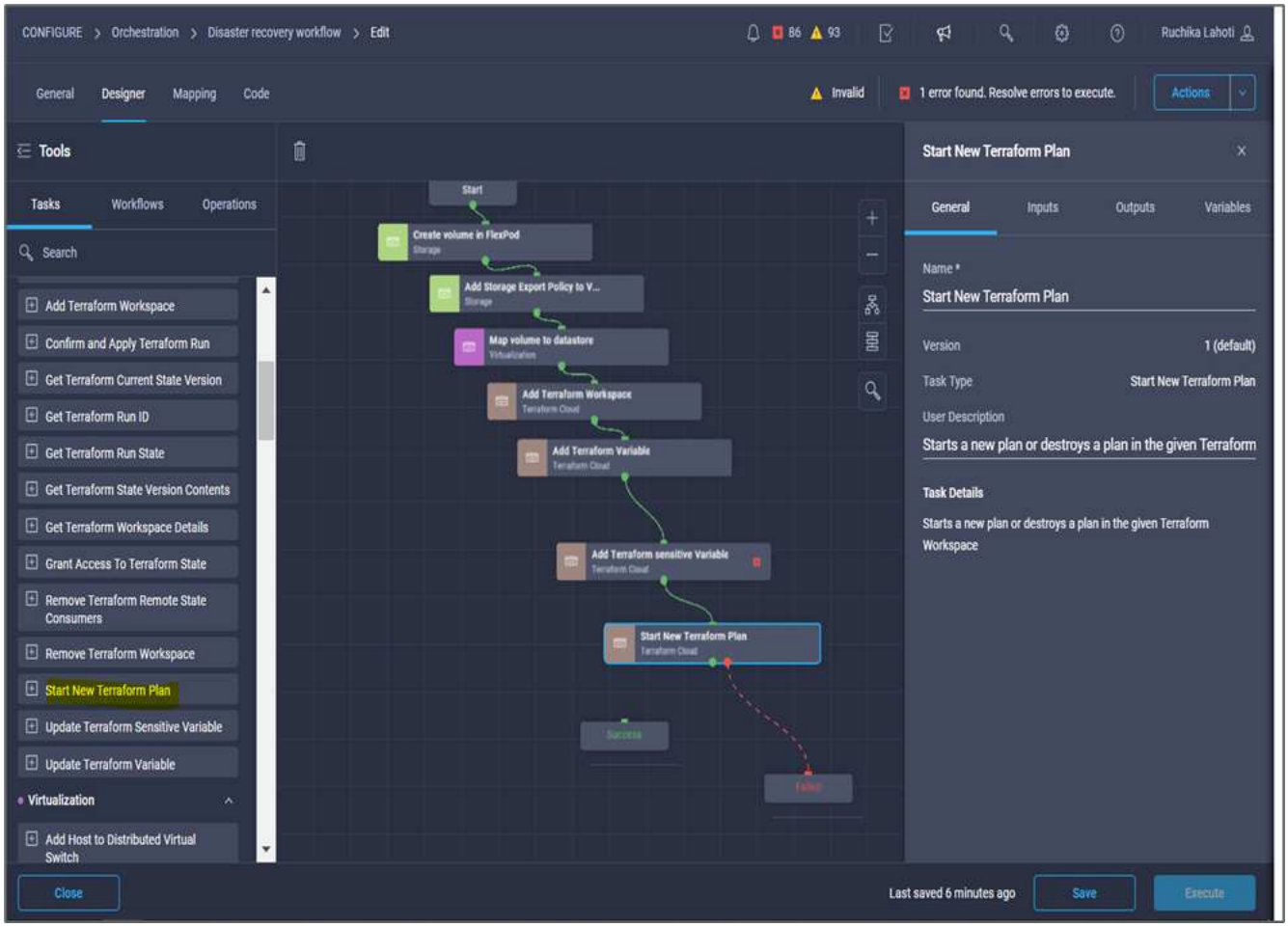
22. Aggiungere tutte le variabili sensibili al terraform come mostrato nella tabella seguente. È inoltre possibile specificare un valore predefinito.

Nome variabile sensibile al terraform	Descrizione
cloud_manager_refresh_token	Aggiorna token. Ottenerlo da:
id_connettore	L'ID client di Cloud Manager Connector. Ottenerlo da
cvo_admin_password	La password admin per Cloud Volumes ONTAP
on-premise-ontap_user_password	Password di amministratore per il cluster di storage

23. Fare clic su **Map** (Mappa) per completare l'operazione di aggiunta delle variabili sensibili al Terraform richieste all'area di lavoro. Quindi, avviare un nuovo piano Terraform nell'area di lavoro configurata.

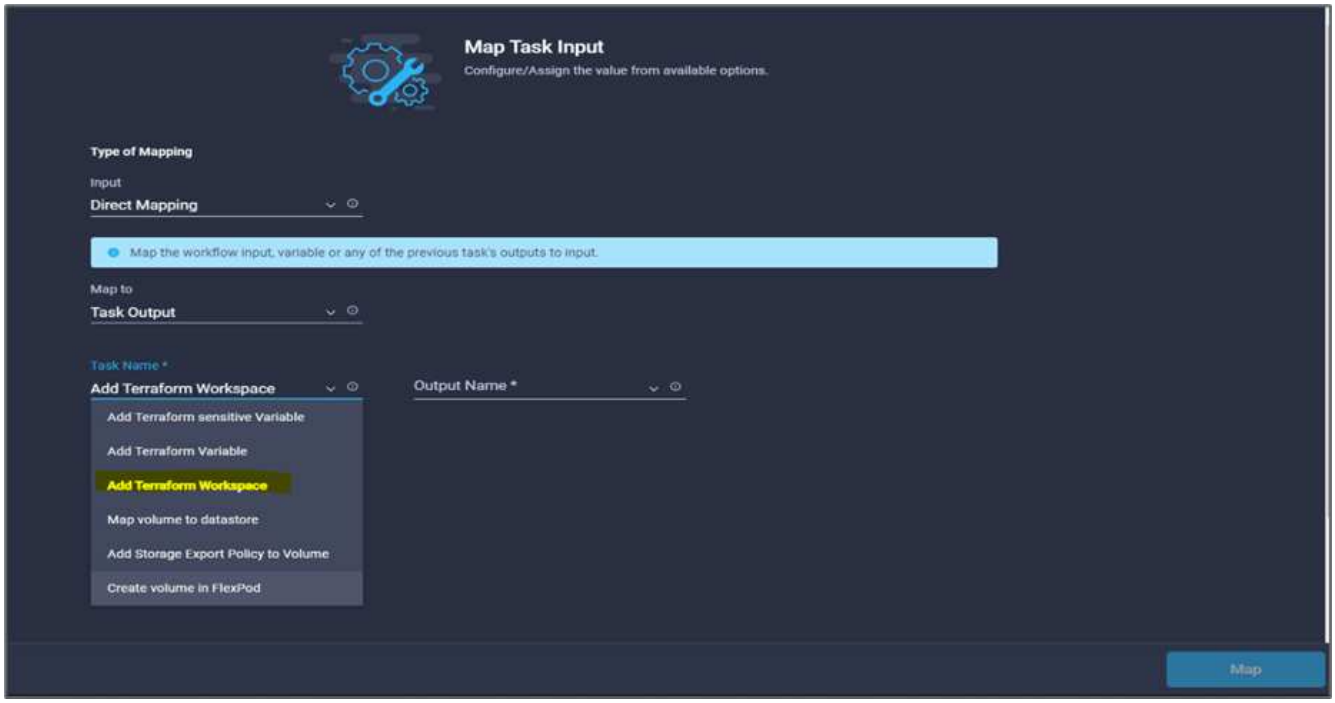
Procedura 8: Avviare un nuovo piano Terraform

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Start New Terraform Plan** (Avvia nuovo piano di terraform) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per connettersi tra le attività **Aggiungi variabili sensibili al terraform** e **Avvia nuove attività del piano di terraform**. Fare clic su **Save** (Salva).
4. Fare clic su **Start New Terraform Plan** (Avvia nuovo piano terraform). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività.

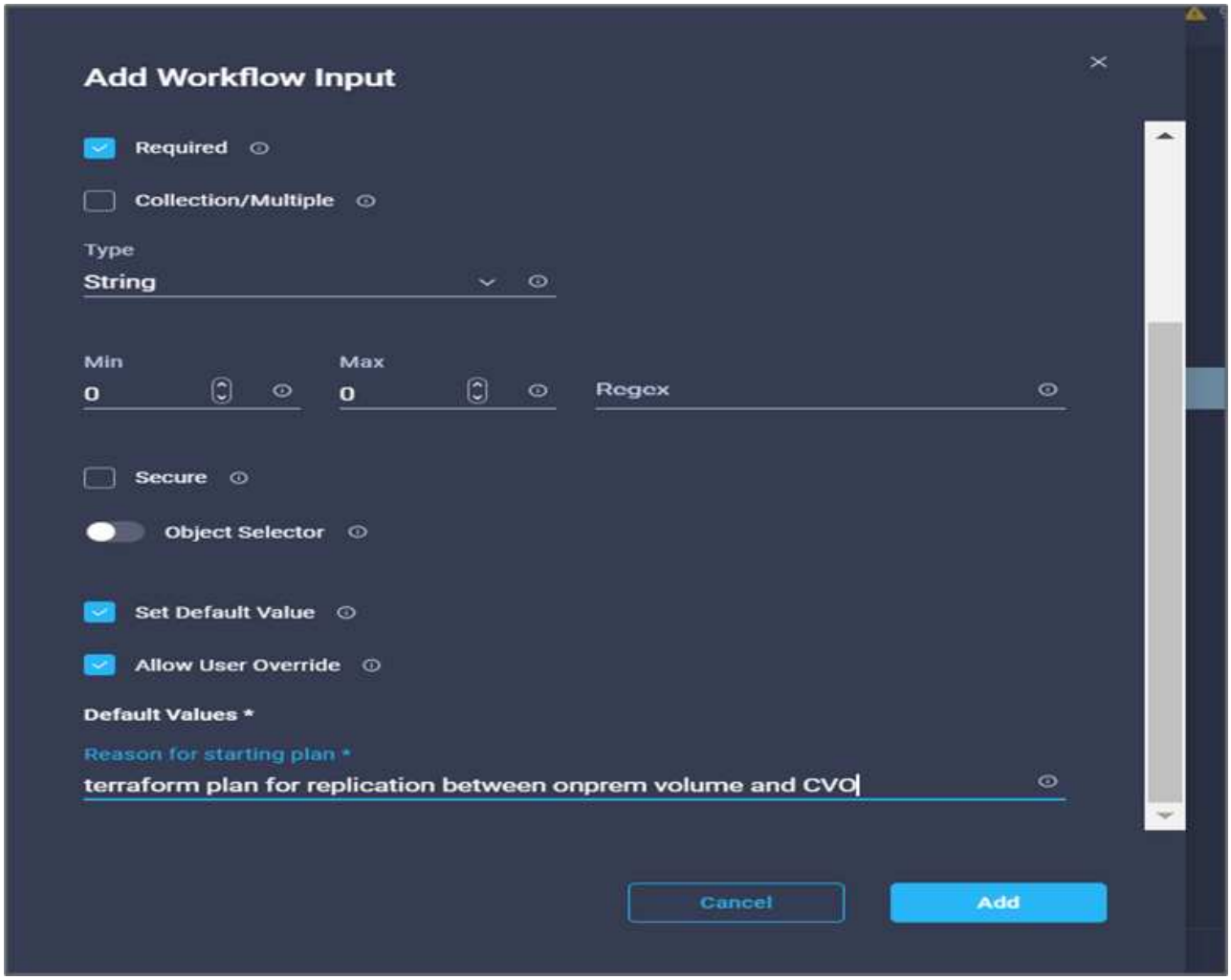


5. Nell'area **Task Properties**, fare clic su **Input**.

6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto nella sezione "Configurazione di Cisco Intersight Service per HashiCorp Terraform".
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Workspace ID**.
10. Scegliere **Direct Mapping** e fare clic su **Task Output**.
11. Fare clic su **Nome attività**, quindi su **Aggiungi area di lavoro terraform**.



12. Fare clic su **Output Name**, **Workspace ID**, quindi su **Map**.
13. Fare clic su **Map** nel campo **Reason for Starting plan** (motivo del piano di avvio).
14. Scegliere **Direct Mapping**, quindi fare clic su **Workflow Input**.
15. Fare clic su **Input Name**, quindi su **Create Workflow Input**.
16. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Inserire un valore predefinito per **motivo dell'avvio del piano** e fare clic su **Aggiungi**.



17. Fare clic su **Map** (Mappa).
18. Fare clic su **Map** (Mappa) nel campo **Plan Operation** (operazione piano).
19. Scegliere **valore statico** e fare clic su **operazione piano**. Fare clic su **nuovo piano**.

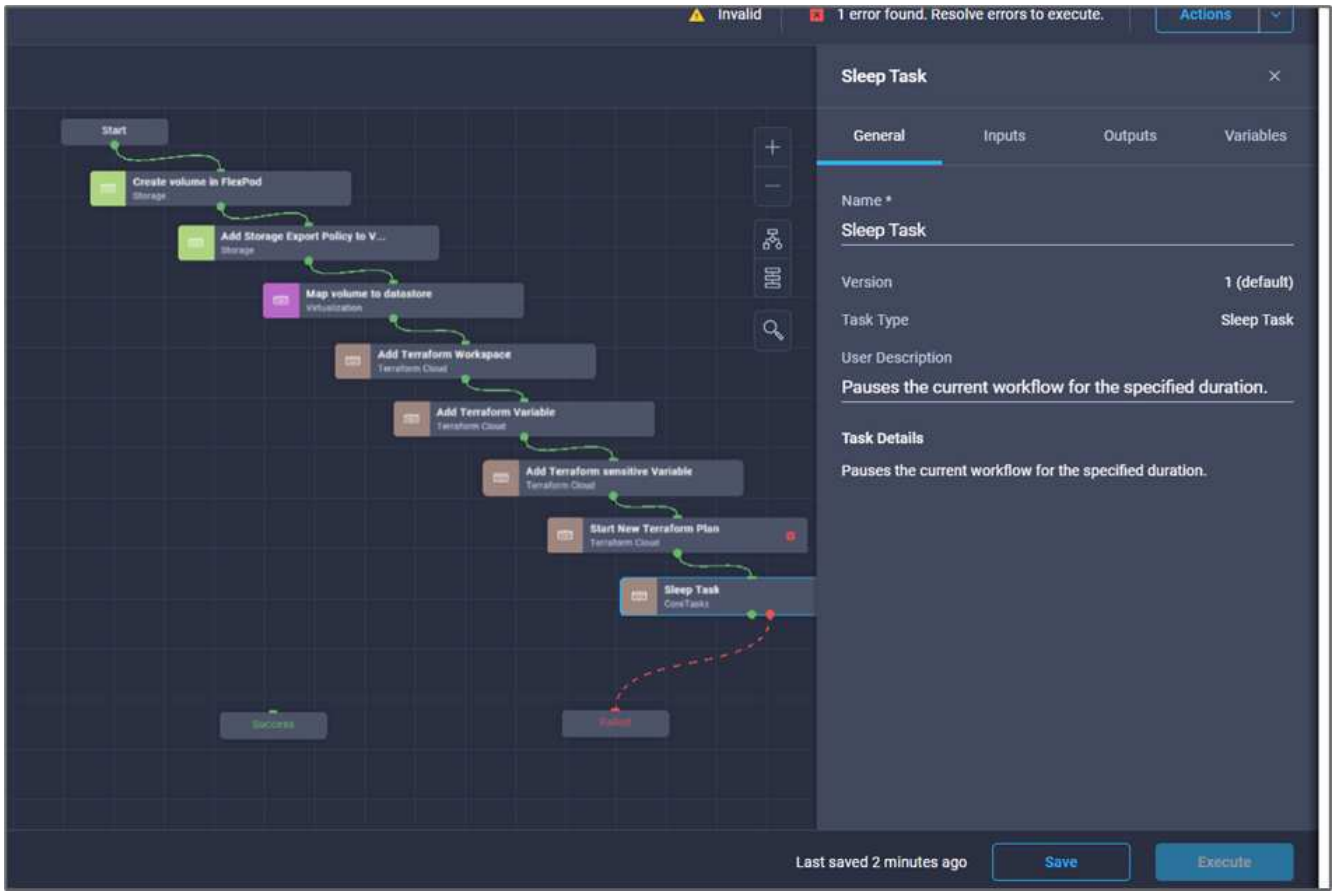
20. Fare clic su **Map** (Mappa).
21. Fare clic su **Save** (Salva).

In questo modo, viene completata l'attività di aggiunta di un piano Terraform in un account Terraform Cloud for Business. Quindi, creare un'attività di sospensione per alcuni secondi.

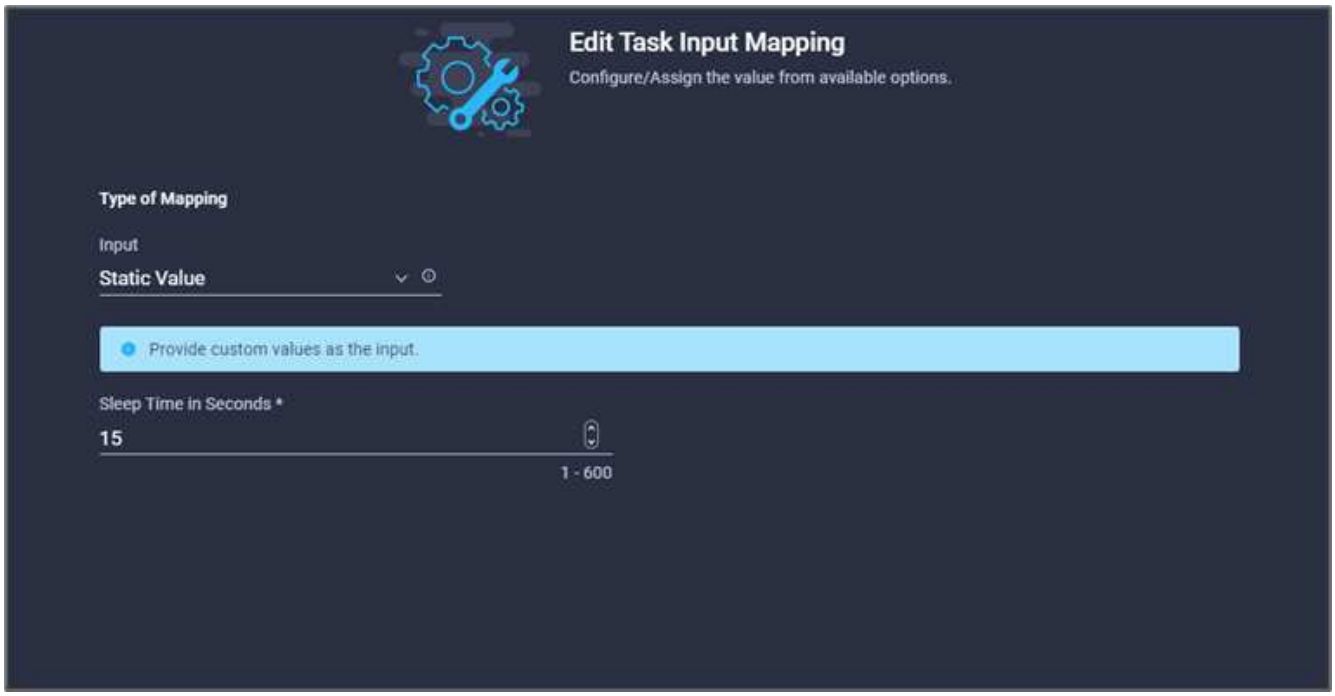
Procedura 9: Attività di sospensione per la sincronizzazione

Terraform Apply richiede RunID, che viene generato come parte dell'attività Terraform Plan. Attendere alcuni secondi tra il piano Terraform e le azioni Terraform Apply evita i problemi di tempistica.

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare **Core Tasks > Sleep Task** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le attività **Avvia nuovo piano terraform** e **sospensione attività**. Fare clic su **Save** (Salva).



4. Fare clic su **attività sospensione**. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Synchronize**.
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Sleep Time in seconds**.
7. Scegliere **valore statico** e inserire **15** in per il valore **tempo di pausa in secondi**.

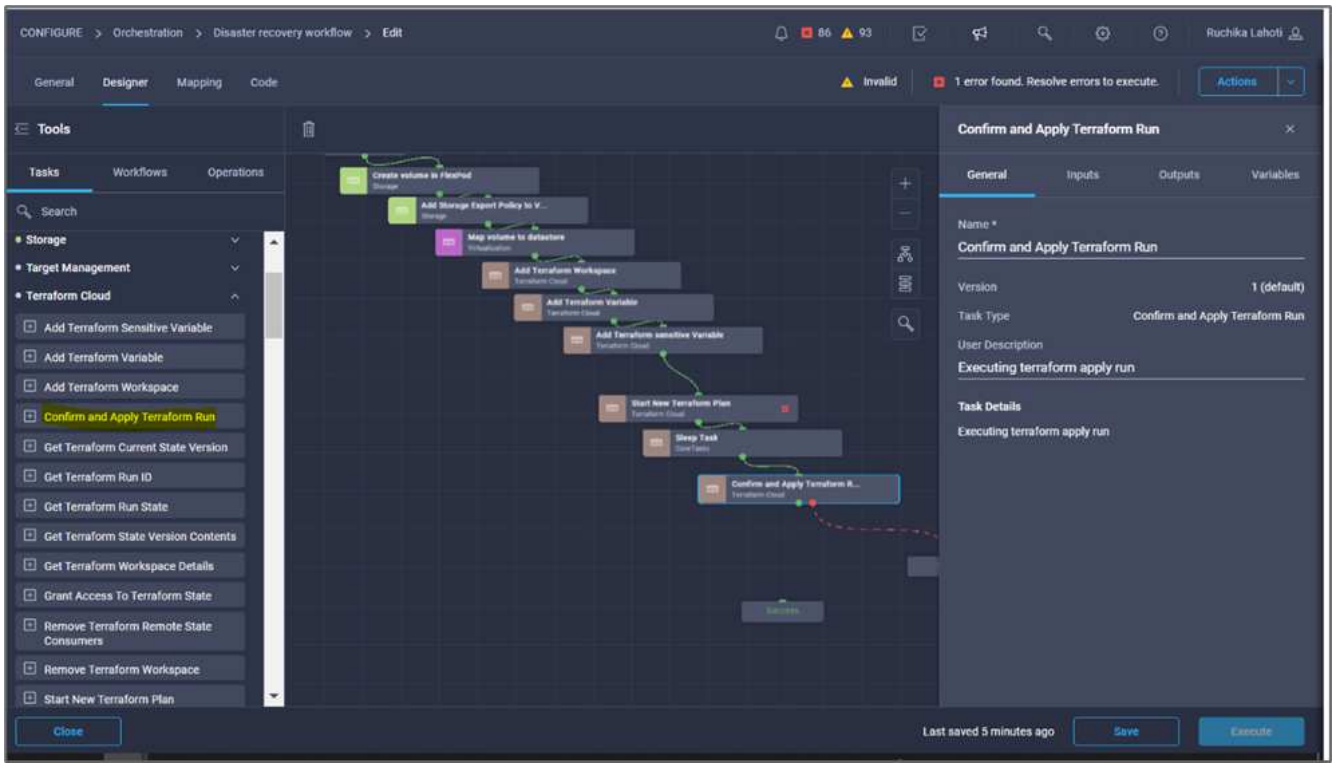


8. Fare clic su **Map** (Mappa).
9. Fare clic su **Save** (Salva).

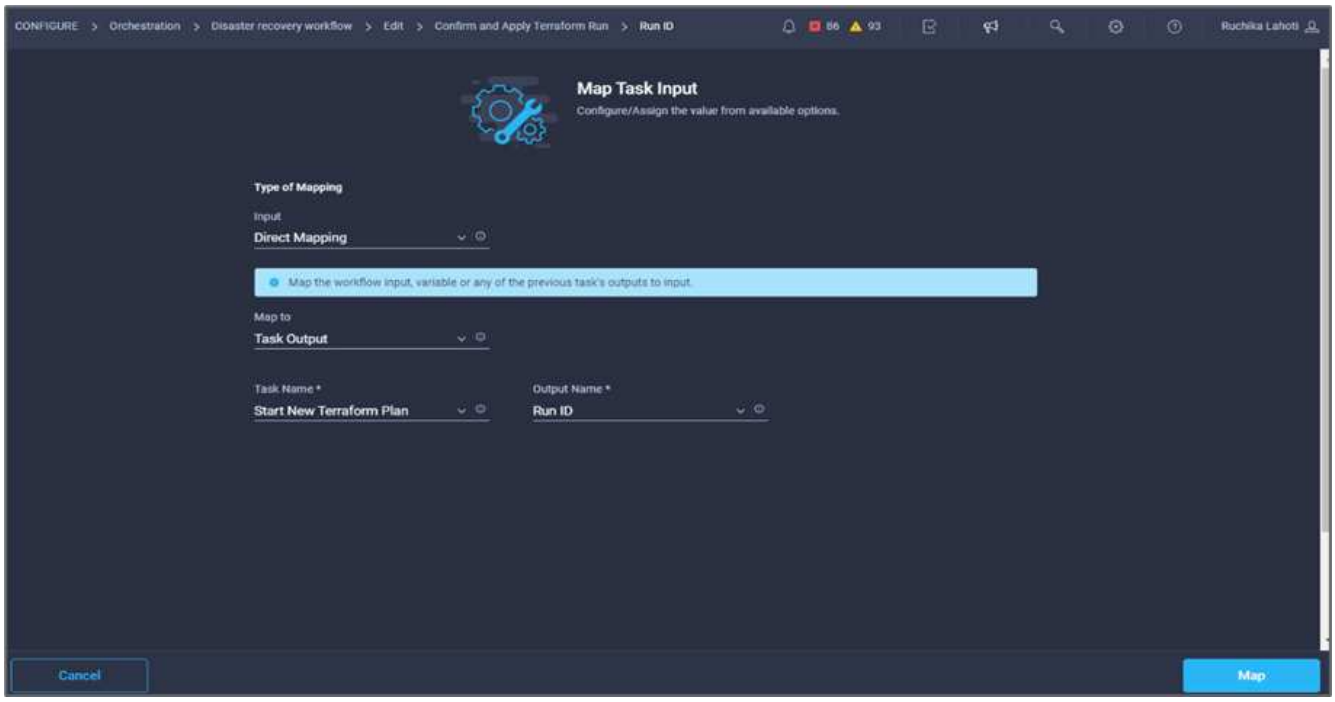
L'attività di sospensione viene completata. Quindi, creare l'ultima attività di questo flusso di lavoro, confermando e applicando Terraform Run.

Procedura 10: Confermare e applicare Terraform Run

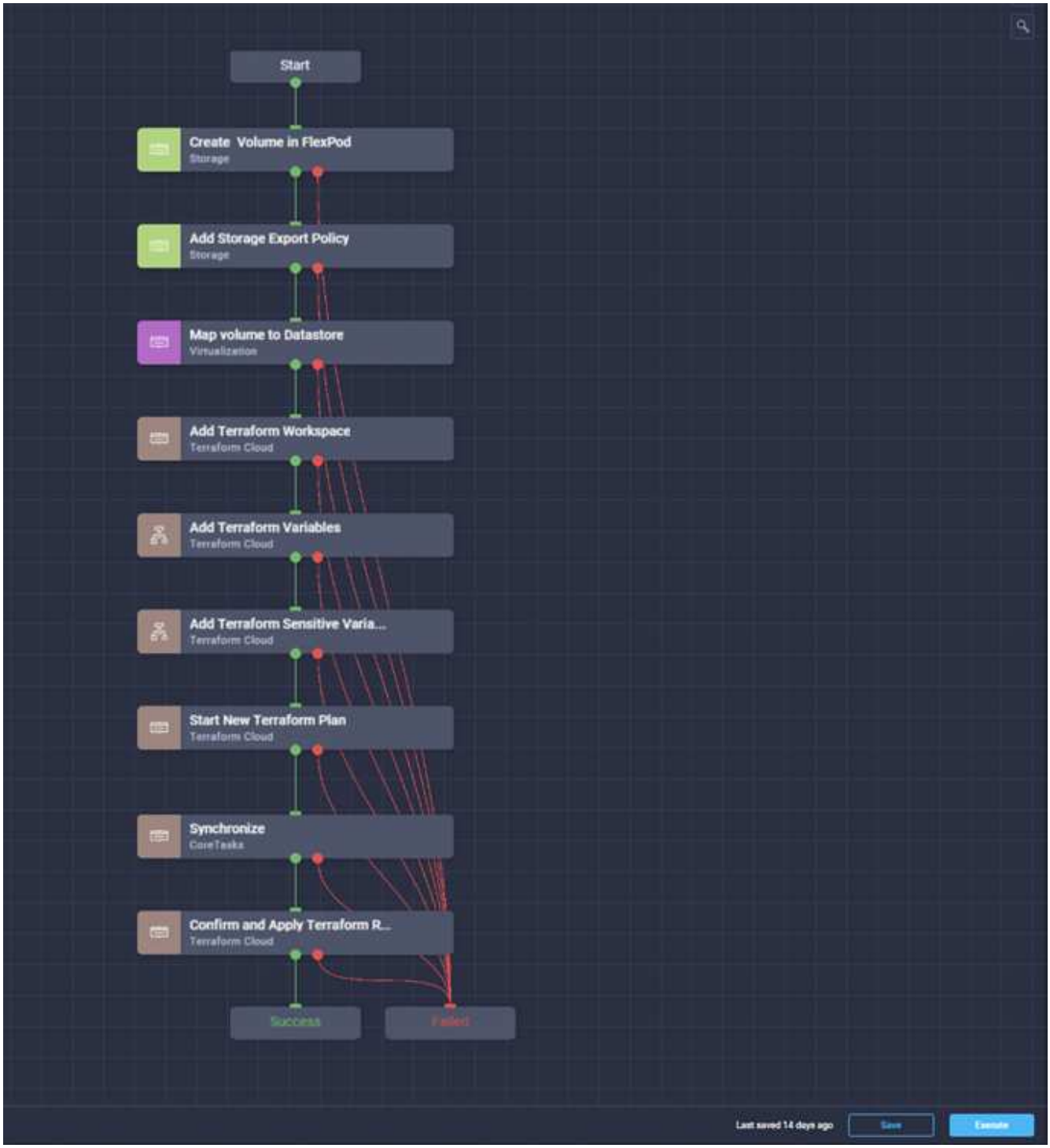
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Confirm and Apply Terraform Run** (Conferma e applica esecuzione terraform) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per collegare le attività **Synchronize** e **Confirm and Apply Terraform Run**. Fare clic su **Save** (Salva).
4. Fare clic su **Conferma** e **Applica esecuzione terraform**. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività.



5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Seleziona l'account Terraform Cloud for Business aggiunto in "Configurare Cisco Intersight Service per HashiCorp Terraform"."
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Run ID** (ID analisi).
10. Scegliere **Direct Mapping** e fare clic su **Task Output**.
11. Fare clic su **Nome attività** e fare clic su **Avvia nuovo piano di terraform**.
12. Fare clic su **Output Name** (Nome output), quindi su **Run ID** (ID esecuzione).



13. Fare clic su **Map** (Mappa).
14. Fare clic su **Save** (Salva).
15. Fare clic su **Auto Align Workflow** (allineamento automatico flusso di lavoro) per allineare tutte le attività. Fare clic su **Save** (Salva).



Questa operazione completa l'attività Confirm and Apply Terraform Run (Conferma e applica esecuzione terraform). Utilizzare Connector per connettersi tra le attività **Confirm and Apply Terraform Run** e le attività **Success** e **Failed**.

Procedura 11: Importazione di un flusso di lavoro creato da Cisco

Cisco Intersight Cloud Orchestrator consente di esportare i flussi di lavoro da un account Cisco Intersight al sistema e di importarli in un altro account. È stato creato un file JSON esportando il workflow creato che può essere importato nel tuo account.

In è disponibile un file JSON per il componente del flusso di lavoro "Repository di GitHub".

"Pagina successiva: Esecuzione del terraform dal controller."

Esecuzione del terraform dal controller

"Precedente: Workflow DR."

Possiamo eseguire il piano Terraform utilizzando un controller. Puoi saltare questa sezione se hai già eseguito il tuo piano Terraform utilizzando un workflow ICO.

Prerequisiti

La configurazione della soluzione inizia con una workstation di gestione che ha accesso a Internet e con un'installazione funzionante di Terraform.

È possibile trovare una guida per l'installazione di Terraform "qui".

Clonare GitHub repo

La prima fase del processo consiste nella clonazione del repo GitHub in una nuova cartella vuota della workstation di gestione. Per clonare il repository GitHub, attenersi alla seguente procedura:

1. Dalla workstation di gestione, creare una nuova cartella per il progetto. Creare una nuova cartella all'interno di questa cartella denominata `/root/snapmirror-cvo` E Clone il repo GitHub in esso.
2. Aprire un'interfaccia a riga di comando o console sulla workstation di gestione e modificare le directory nella nuova cartella appena creata.
3. Clonare l'insieme GitHub utilizzando il seguente comando:

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Modificare le directory nella nuova cartella denominata `snapmirror-cvo`.

Esecuzione terraform

- **Init.** Inizializza l'ambiente Terraform (locale). Di solito viene eseguita una sola volta per sessione.
- **Plan.** Confronta lo stato del terraform con lo stato as-in nel cloud e crea e visualizza un piano di esecuzione. Ciò non modifica la distribuzione (sola lettura).
- **Apply.** applicare il piano dalla fase del piano. In questo modo è possibile modificare l'implementazione (lettura e scrittura).
- **Destroy.** tutte le risorse gestite da questo specifico ambiente terraform.

  Per ulteriori informazioni, vedere "qui".

"Successivo: Convalida della soluzione."

Convalida della soluzione

"Precedente: Esecuzione del terraform dal controller."

In questa sezione, rivisitiamo la soluzione con un workflow di replica dei dati di esempio e effettuiamo alcune misurazioni per verificare l'integrità della replica dei dati dall'istanza di NetApp ONTAP in esecuzione in FlexPod a NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud.

Abbiamo utilizzato Cisco Intersight workflow orchestrator in questa soluzione e continueremo a utilizzarla per il nostro caso d'utilizzo.

In particolare, la serie limitata di flussi di lavoro Cisco Intersight utilizzata in questa soluzione non rappresenta la serie completa di flussi di lavoro di cui Cisco Intersight è dotato. È possibile creare flussi di lavoro personalizzati in base ai requisiti specifici e attivarli da Cisco Intersight.

Per eseguire la convalida di uno scenario di disaster recovery di successo, spostare i dati da un volume in ONTAP che fa parte di FlexPod a Cloud Volumes ONTAP utilizzando SnapMirror. Quindi, puoi tentare di accedere ai dati dall'istanza di calcolo del cloud di Google seguita da un controllo dell'integrità dei dati.

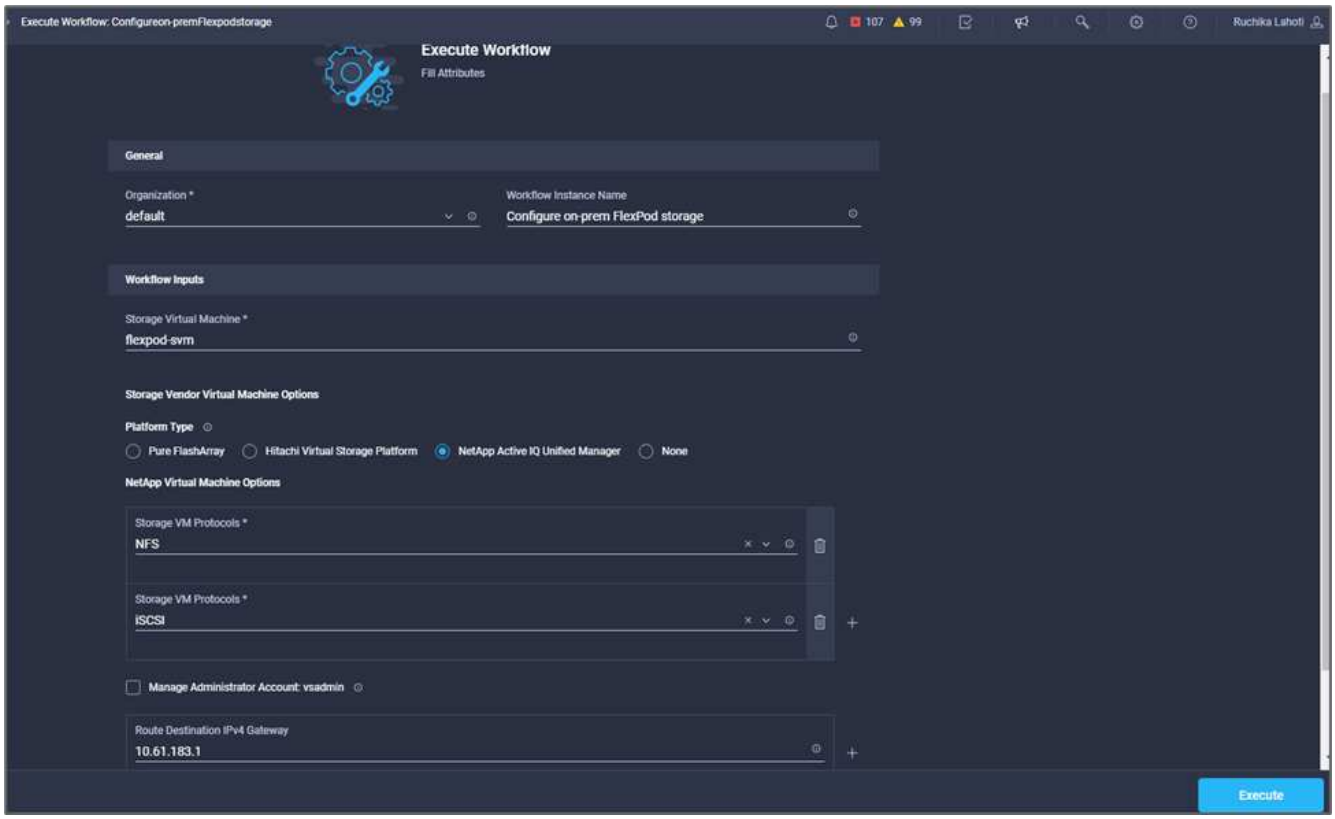
Per verificare i criteri di successo di questa soluzione, vengono utilizzati i seguenti passaggi di alto livello:

1. Generare un checksum SHA256 nel set di dati di esempio presente in un volume ONTAP in FlexPod.
2. Impostare una relazione di SnapMirror tra ONTAP in FlexPod e Cloud Volumes ONTAP.
3. Replicare il set di dati di esempio da FlexPod a Cloud Volumes ONTAP.
4. Interrompere la relazione di SnapMirror e promuovere il volume in Cloud Volumes ONTAP alla produzione.
5. Mappare il volume Cloud Volumes ONTAP con il dataset in un'istanza di calcolo in Google Cloud.
6. Generare un checksum SHA256 nel set di dati di esempio in Cloud Volumes ONTAP.
7. Confrontare il checksum sull'origine e sulla destinazione; presumibilmente, i checksum su entrambi i lati corrispondono.

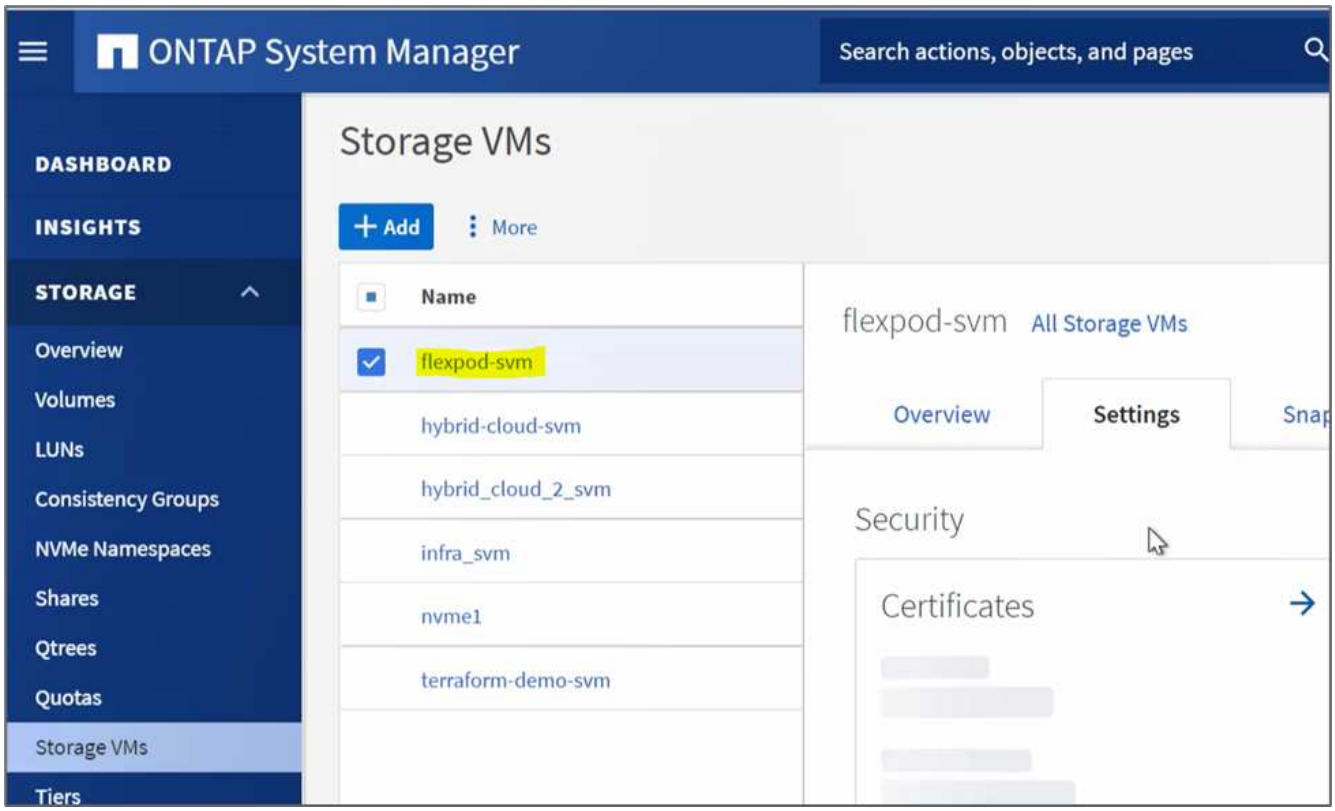
Per eseguire il flusso di lavoro on-premise, attenersi alla seguente procedura:

1. Crea un workflow in Intersight per FlexPod on-premise.

2. Fornire gli input richiesti ed eseguire il workflow.

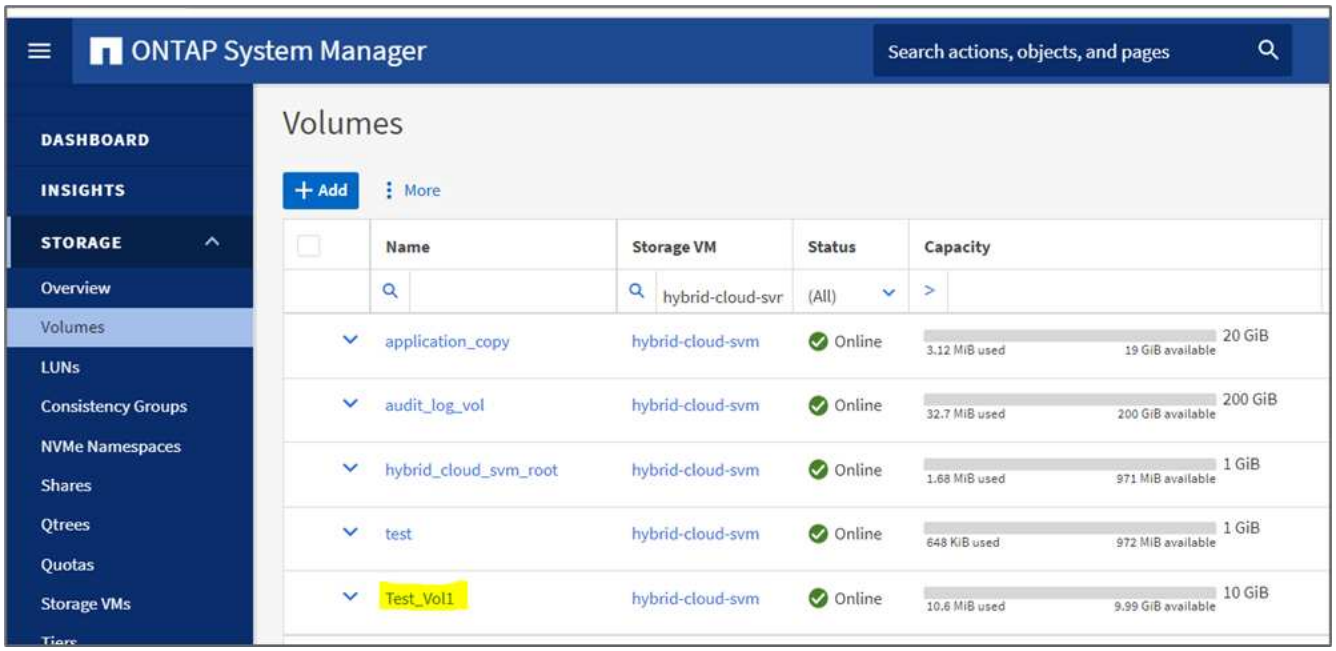


3. Verificare la SVM appena creata in System Manager.



4. Creare ed eseguire un altro flusso di lavoro di disaster recovery per creare un volume in FlexPod on-premise e stabilire una relazione SnapMirror tra questo volume in FlexPod e Cloud Volumes ONTAP.

5. Verificare il volume appena creato in ONTAP System Manager.

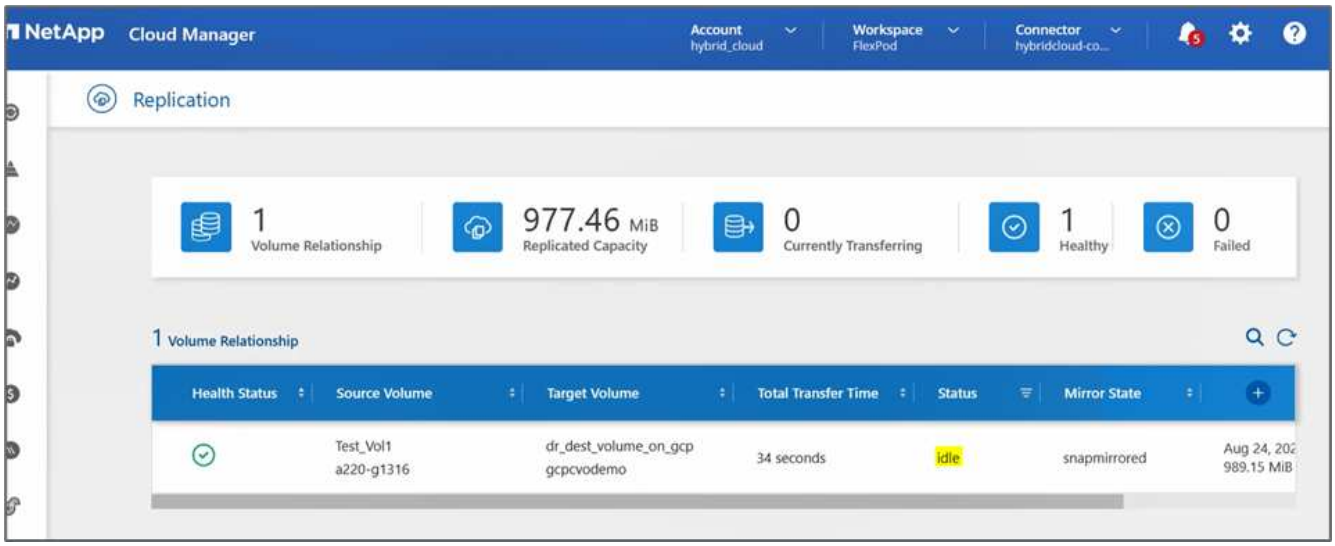


6. Montare lo stesso volume NFS su una macchina virtuale on-premise, quindi copiare il set di dati di esempio ed eseguire il checksum.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                 Size  Used Avail Use% Mounted on
udev                       1.9G     0  1.9G   0% /dev
tmpfs                      394M  1.1M  393M   1% /run
/dev/sda2                   16G   11G  4.2G  72% /
tmpfs                      2.0G     0  2.0G   0% /dev/shm
tmpfs                      5.0M     0  5.0M   0% /run/lock
tmpfs                      2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                  55M   55M     0 100% /snap/core18/1705
/dev/loop2                  69M   69M     0 100% /snap/lxd/14804
/dev/loop0                  28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1     10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

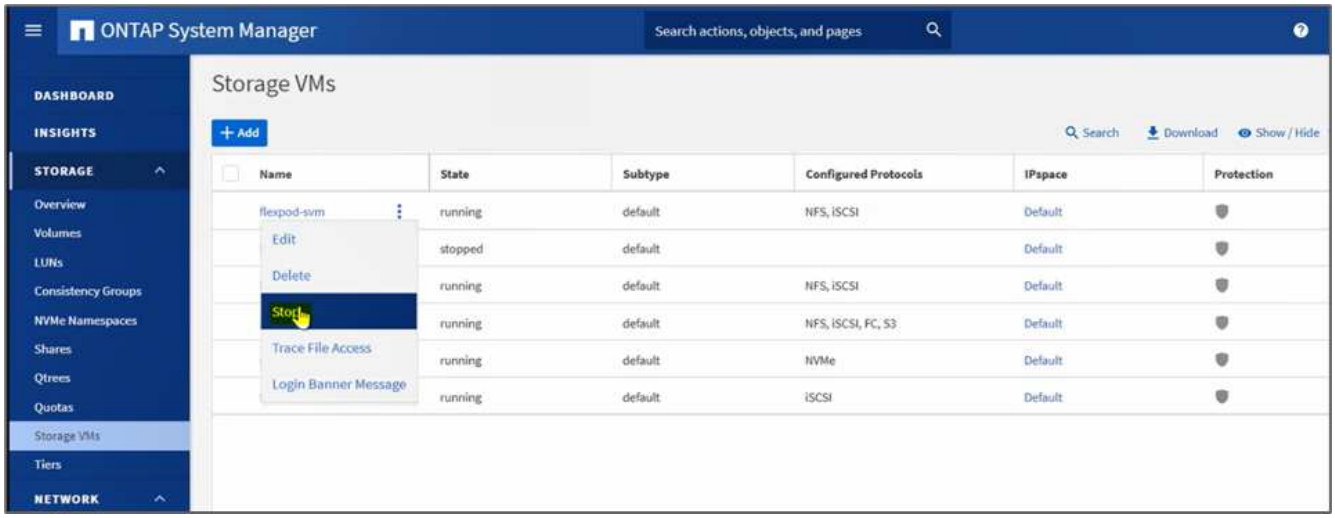
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Controllare lo stato della replica in Cloud Manager. Il trasferimento dei dati può richiedere alcuni minuti in base alle dimensioni dei dati. Al termine, lo stato di SnapMirror sarà **Idle**.

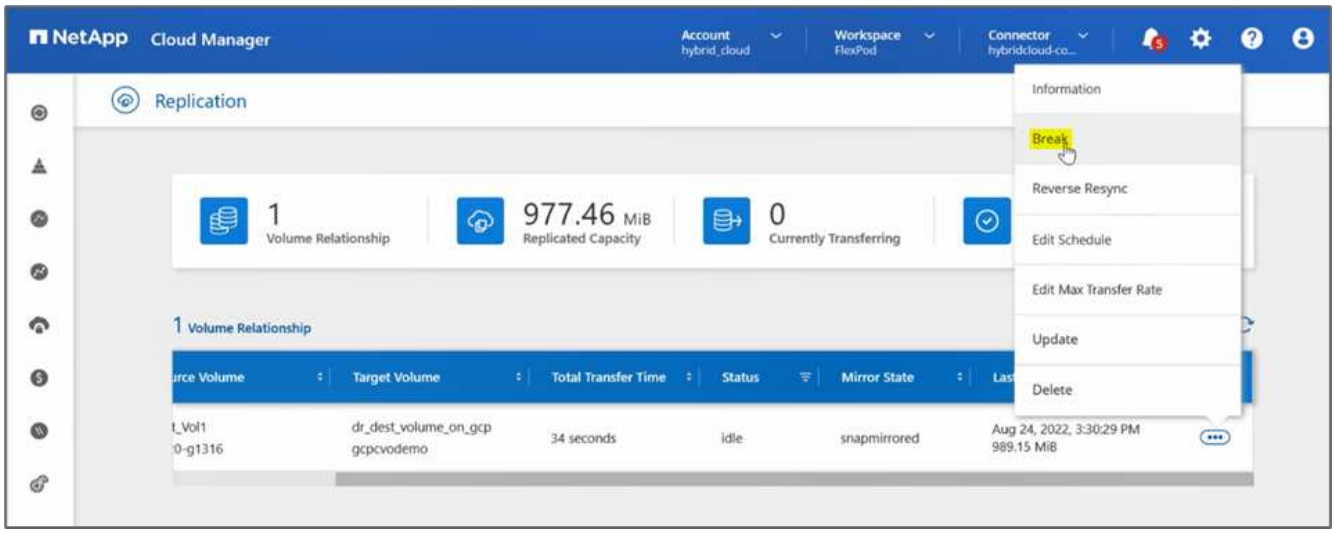


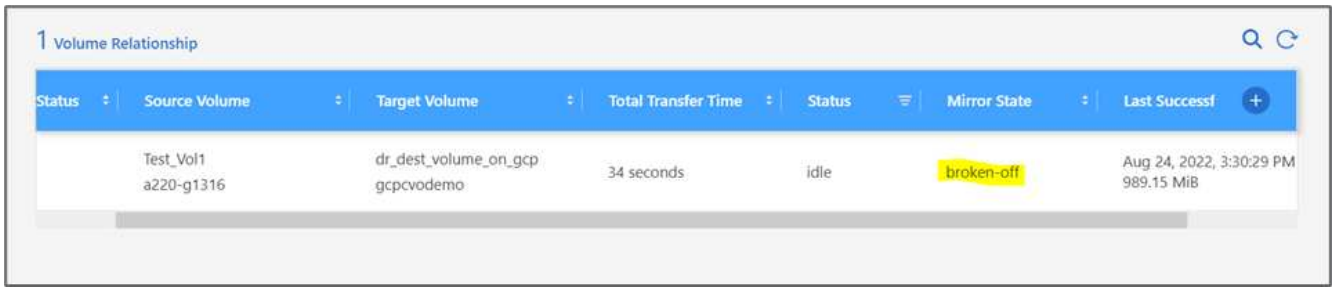
8. Una volta completato il trasferimento dei dati, simulare un disastro sul lato di origine arrestando la SVM che ospita `Test_vol1` volume.

   Dopo l'arresto di SVM, il `Test_vol1` Il volume non è visibile in Cloud Manager.

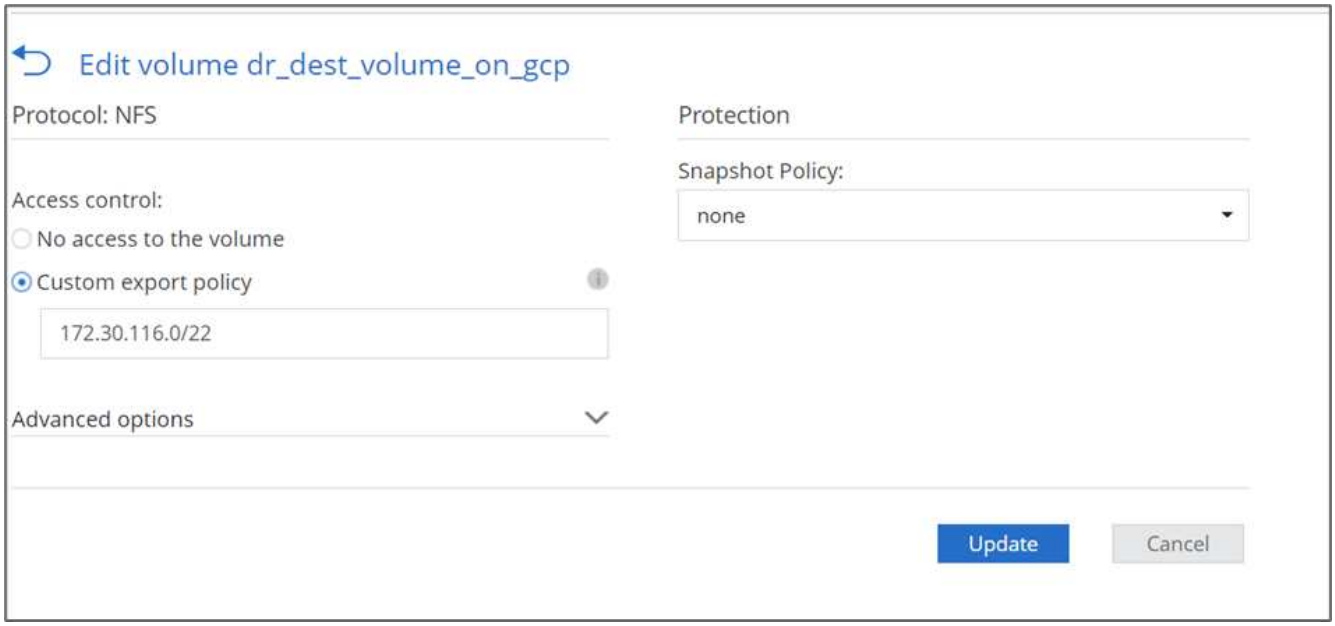


9. Interrompere la relazione di replica e promuovere il volume di destinazione Cloud Volumes ONTAP in produzione.

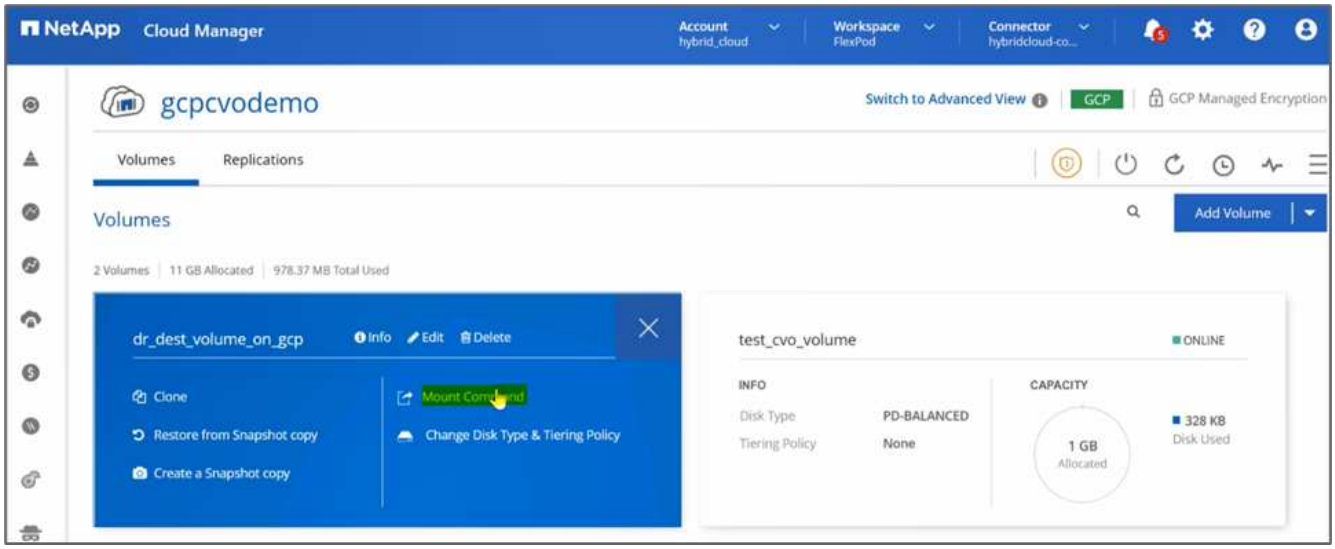




10. Modificare il volume e abilitare l'accesso client associandolo a un criterio di esportazione.



11. Ottenere il comando mount pronto all'uso per il volume.



12. Montare il volume su un'istanza di calcolo, verificare che i dati siano presenti nel volume di destinazione e generare il checksum SHA256 di `sample_dataset_2GB` file.

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Confrontare i valori del checksum sia in corrispondenza dell'origine (FlexPod) che in corrispondenza della destinazione (Cloud Volumes ONTAP).
14. I checksum corrispondono all'origine e alla destinazione.

È possibile confermare che la replica dei dati dall'origine alla destinazione sia stata completata correttamente e che l'integrità dei dati sia stata mantenuta. Questi dati possono ora essere consumati in modo sicuro dalle applicazioni per servire i client mentre il sito di origine passa attraverso il ripristino.

"Prossimo: Conclusione."

Conclusione

"Precedente: Convalida della soluzione."

In questa soluzione, il servizio dati cloud NetApp, Cloud Volumes ONTAP e l'infrastruttura del data center FlexPod sono stati utilizzati per creare una soluzione di DR con un cloud pubblico basato su Cisco Intersight Cloud Orchestrator. La soluzione FlexPod si è evoluta costantemente per consentire ai clienti di modernizzare le proprie applicazioni e i processi di business delivery. Con questa soluzione, è possibile creare un piano BCDR con il cloud pubblico come punto di accesso per un piano di disaster recovery transitorio o a tempo pieno, mantenendo al contempo bassi i costi della soluzione di disaster recovery.

La replica dei dati tra FlexPod on-premise e NetApp Cloud Volumes ONTAP è stata gestita dalla comprovata tecnologia SnapMirror, ma è anche possibile selezionare altri strumenti di trasferimento e sincronizzazione dei dati NetApp come Cloud Sync per i requisiti di mobilità dei dati. Sicurezza dei dati in volo grazie alle tecnologie di crittografia integrate basate su TLS/AES.

Sia che si disponga di un piano di DR temporaneo per un'applicazione o di un piano di DR a tempo pieno per un'azienda, il portfolio di prodotti utilizzati in questa soluzione può soddisfare entrambi i requisiti su larga scala. Basato su Cisco Intersight Workflow Orchestrator, lo stesso può essere automatizzato con flussi di lavoro predefiniti che non solo eliminano la necessità di ricostruire i processi, ma accelerano anche l'implementazione di un piano BCDR.

La soluzione consente la gestione on-premise di FlexPod e la replica dei dati in un cloud ibrido in modo molto semplice e conveniente con l'automazione e l'orchestrazione fornite da Cisco Intersight Cloud Orchestrator.

Dove trovare ulteriori informazioni

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

GitHub

- Tutte le configurazioni terraform utilizzate

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- File JSON per l'importazione dei flussi di lavoro

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centro assistenza Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentazione di Cisco Intersight Cloud Orchestrator:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service per documentazione HashiCorp Terraform

"https://intersight.com/help/saas/features/terraform_cloud/admin"

- Scheda informativa su Cisco Intersight

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Scheda informativa di Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Scheda informativa di Cisco Intersight Service per HashiCorp Terraform

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

  "FlexPod Datacenter con Cisco UCS 4.2(1) in modalità gestita UCS, VMware vSphere 7.0 U2 e guida alla progettazione di NetApp ONTAP 9.9"

- Data center FlexPod con Cisco UCS serie X.

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

Interoperabilità

- Tool di matrice di interoperabilità NetApp

  "http://support.netapp.com/matrix/"

- Cisco UCS hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guida alla compatibilità VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Documenti di riferimento NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Calcolatore del TCO di Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Cloud Assessment Tool

  https://cloud.netapp.com/assessments

- Cloud ibrido NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentazione API di Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Risoluzione dei problemi

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Cloud terraformo

  "https://www.terraform.io/cloud"

- Documentazione terraform

  "https://www.terraform.io/docs/"

- Registro di NetApp Cloud Manager

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- Alta disponibilità ONTAP per GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- Requisito GCP

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Cloud ibrido FlexPod con NetApp Astra e Cisco Intersight per Red Hat OpenShift

TR-4936: Cloud ibrido FlexPod con NetApp Astra e Cisco Intersight per Red Hat OpenShift

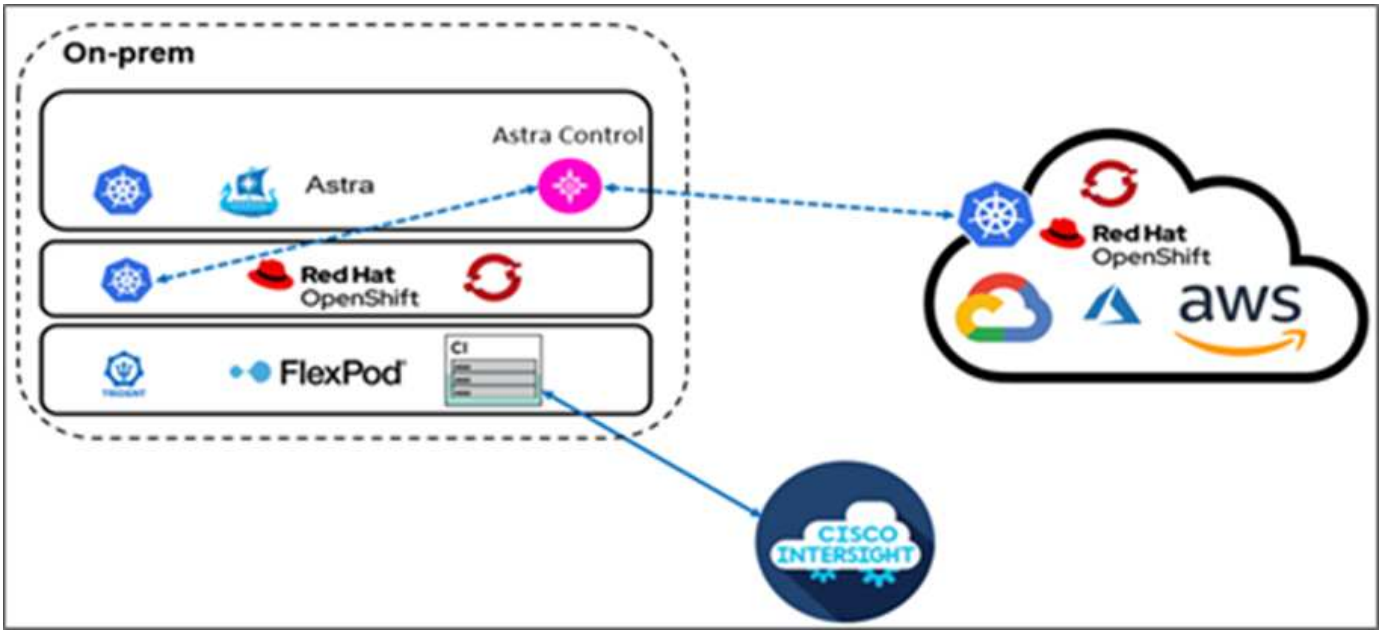
Abhinav Singh

Introduzione

Mentre container e Kubernetes diventano la scelta de facto per lo sviluppo, l'implementazione, l'esecuzione, la gestione e la scalabilità delle applicazioni containerizzate, le aziende eseguono sempre più applicazioni business-critical su di esse. Le applicazioni business-critical dipendono in larga misura dallo stato. Un'applicazione stateful dispone di informazioni sullo stato, sui dati e sulla configurazione associate e dipende dalle transazioni dei dati precedenti per eseguire la propria logica di business. Le applicazioni business-critical eseguite su Kubernetes continuano ad avere requisiti di disponibilità e business continuity come le applicazioni tradizionali. Un'interruzione del servizio può compromettere seriamente la perdita di ricavi, produttività e reputazione dell'azienda. Pertanto, è molto importante proteggere, ripristinare e spostare rapidamente e facilmente i workload Kubernetes all'interno e tra cluster, data center on-premise e ambienti cloud ibridi. Le aziende hanno riscontrato i vantaggi derivanti dal passaggio del business a un modello di cloud ibrido e la modernizzazione delle applicazioni a un fattore di forma nativo del cloud è un fattore di importanza fondamentale.

Questo report tecnico riunisce il centro di controllo Astra di NetApp con la piattaforma container OpenShift di Red Hat su una soluzione di infrastruttura convergente FlexPod e si estende ai servizi web Amazon (AWS) per formare un data center di cloud ibrido. Sulla base della familiarità con "FlexPod e Red Hat OpenShift", Questo documento illustra NetApp Astra Control Center, a partire dall'installazione, dalla configurazione, dai flussi di lavoro per la protezione delle applicazioni e dalla migrazione delle applicazioni tra on-premise e cloud. Vengono inoltre illustrati i vantaggi delle funzionalità di gestione dei dati application-aware (come backup e recovery, business continuity) quando si utilizza NetApp Astra Control Center per le applicazioni containerizzate eseguite su Red Hat OpenShift.

La figura seguente illustra la panoramica della soluzione.



Pubblico

Il pubblico di riferimento di questo documento comprende Chief Technology Officer (CTO), sviluppatori di applicazioni, architetti di soluzioni cloud, tecnici dell'affidabilità del sito (SRE), ingegneri DevOps, ITOps e team di servizi professionali che si occupano della progettazione, dell'hosting e della gestione delle applicazioni containerizzate.

NetApp Astra Control – casi di utilizzo chiave

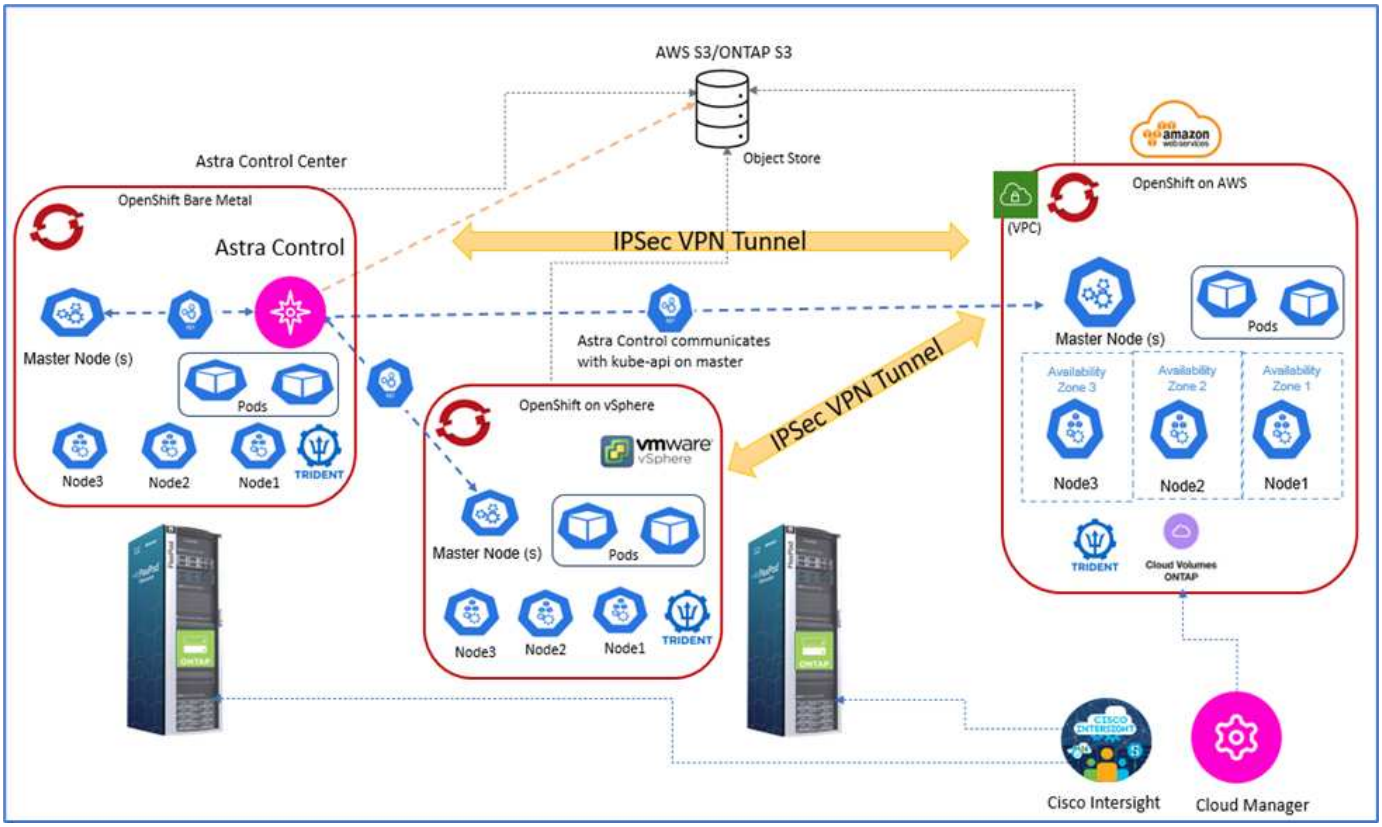
NetApp Astra Control mira a semplificare la protezione delle applicazioni per i clienti che si occupano di microservizi nativi del cloud:

- **Rappresentazione applicativa point-in-time (PIT) con snapshot.** con Astra Control è possibile creare snapshot end-to-end delle applicazioni containerizzate che includono i dettagli di configurazione dell'applicazione in esecuzione su Kubernetes e lo storage persistente associato. In caso di incidente, è possibile ripristinare le applicazioni a uno stato sicuramente funzionante facendo clic sul pulsante.
- **Backup completo dell'applicazione.** con Astra Control è possibile eseguire un backup completo dell'applicazione in base a una pianificazione predefinita che può essere utilizzata per ripristinare l'applicazione sullo stesso cluster K8s o su un cluster K8s diverso on-demand in modo automatizzato.
- **Portabilità dell'applicazione e migrazione con cloni.** con Astra Control è possibile clonare un'intera applicazione insieme ai relativi dati da un cluster Kubernetes a un altro o all'interno dello stesso cluster K8s. Questa funzionalità consente inoltre di eseguire il porting o la migrazione di un'applicazione tra cluster K8s, indipendentemente da dove si trovano i cluster (è sufficiente eliminare l'istanza dell'applicazione di origine dopo la clonazione).
- **Personalizza la coerenza delle applicazioni.** con Astra Control puoi assumere il controllo della definizione degli stati di quiesce delle applicazioni sfruttando gli hook di esecuzione. Rilasciare i ganci di esecuzione 'pre' e 'post' nei flussi di lavoro di snapshot e backup, le applicazioni verranno interrotti a modo proprio prima di eseguire un'istantanea o un backup.
- **Automatizzare il disaster recovery (DR) a livello applicativo.** con Astra Control è possibile configurare un piano di disaster recovery per la business continuity (BCDR) per le applicazioni containerizzate. NetApp SnapMirror viene utilizzato nel back-end e l'implementazione completa del flusso di lavoro DR viene automatizzata.

Topologia della soluzione

In questa sezione viene descritta la topologia logica della soluzione.

La seguente illustrazione rappresenta la topologia della soluzione che comprende l'ambiente on-premise di FlexPod con cluster di piattaforme container OpenShift e un cluster di piattaforme container OpenShift autogestiti su AWS con NetApp Cloud Volumes ONTAP, Cisco Intersight e la piattaforma SaaS di NetApp Cloud Manager.



Il primo cluster della piattaforma container OpenShift è un'installazione bare-metal su FlexPod, il secondo cluster della piattaforma container OpenShift è implementato su VMware vSphere in esecuzione su FlexPod e il terzo cluster della piattaforma container OpenShift è implementato come "cluster privato" In un cloud privato virtuale (VPC) esistente su AWS come infrastruttura autogestiva.

In questa soluzione, FlexPod è connesso ad AWS attraverso una VPN sito-sito, tuttavia i clienti possono anche utilizzare le implementazioni di connessione diretta per estendersi a un cloud ibrido. Cisco Intersight viene utilizzato per gestire i componenti dell'infrastruttura FlexPod.

In questa soluzione, Astra Control Center gestisce l'applicazione containerizzata ospitata sul cluster della piattaforma container OpenShift in esecuzione su FlexPod e AWS. Astra Control Center è installato sull'istanza bare-metal di OpenShift in esecuzione su FlexPod. Astra Control comunica con kube-api sul nodo master e controlla continuamente il cluster Kubernetes per eventuali modifiche. Tutte le nuove applicazioni aggiunte al cluster K8s vengono automaticamente rilevate e rese disponibili per la gestione.

Le rappresentazioni PIT delle applicazioni containerizzate possono essere acquisite come snapshot utilizzando Astra Control Center. Le snapshot delle applicazioni possono essere attivate tramite una policy di protezione pianificata o on-demand. Per le applicazioni supportate da Astra, lo snapshot è coerente con il crash. Uno snapshot applicativo costituisce uno snapshot dei dati dell'applicazione nei volumi persistenti e dei metadati dell'applicazione delle varie risorse Kubernetes associate a tale applicazione.

È possibile creare una copia di backup completa di un'applicazione utilizzando Astra Control utilizzando una pianificazione di backup predefinita o on-demand. Viene utilizzato uno storage a oggetti per memorizzare il backup dei dati dell'applicazione. NetApp ONTAP S3, NetApp StorageGRID e qualsiasi implementazione generica S3 possono essere utilizzati come archivio di oggetti.

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp ONTAP, networking Cisco Nexus, storage networking Cisco MDS, Cisco Unified Computing System (Cisco UCS). Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare più configurazioni.

Controllo Astra

Astra Control offre servizi di protezione dei dati application-aware per applicazioni native del cloud ospitate sia in cloud pubblici che on-premise. Astra Control offre funzionalità di protezione dei dati, disaster recovery e migrazione per le applicazioni containerizzate in esecuzione su Kubernetes.

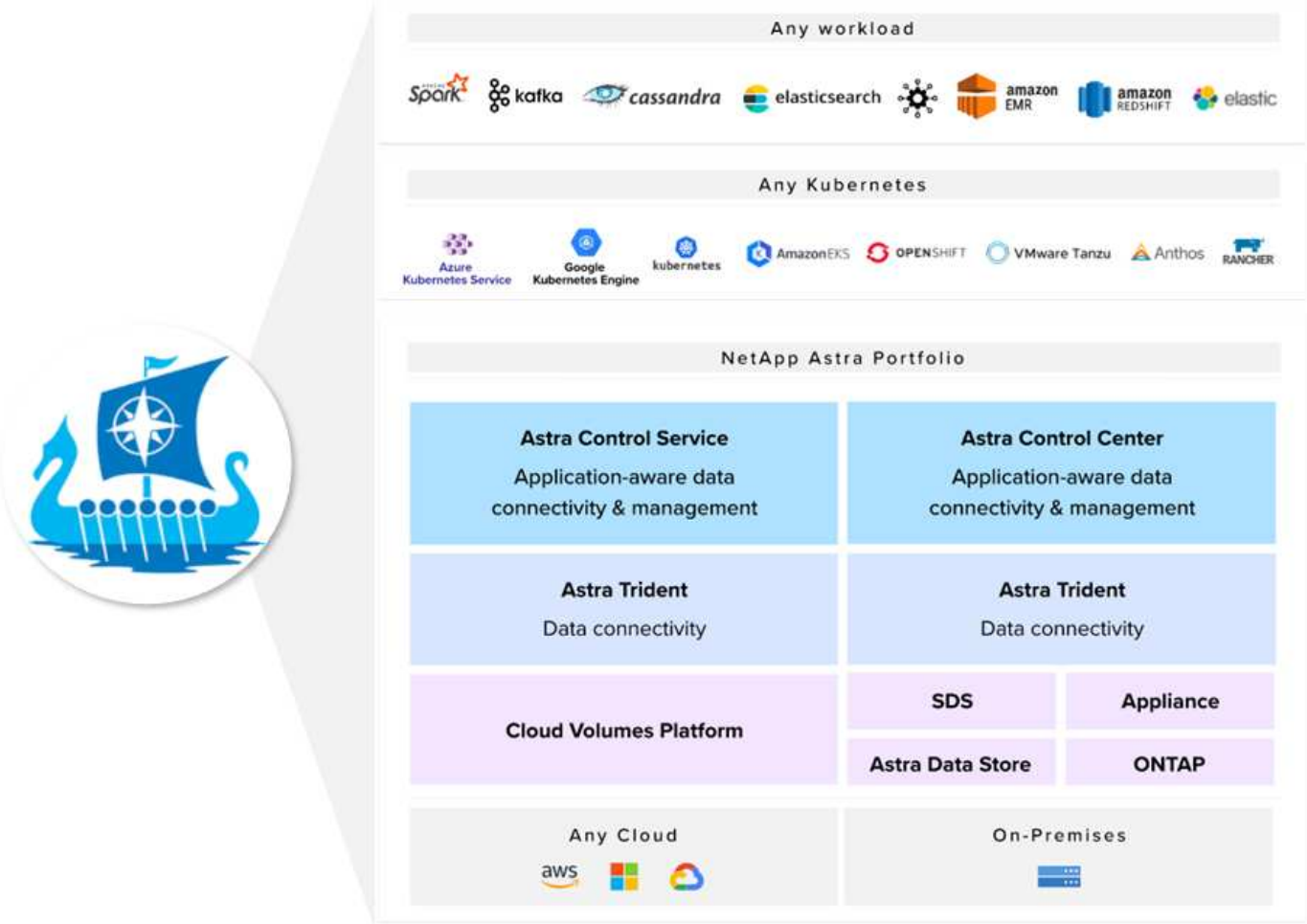
Caratteristiche

Astra Control offre funzionalità critiche per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes:

- Gestire automaticamente lo storage persistente
- Creazione di snapshot e backup on-demand coerenti con l'applicazione
- Operazioni automatizzate di backup e snapshot basate su policy
- Migrare le applicazioni e i dati associati da un cluster Kubernetes a un altro in una configurazione di cloud ibrido
- Clonare un'applicazione nello stesso cluster K8s o in un altro cluster K8s
- Visualizzare lo stato di protezione dell'applicazione
- Fornisce un'interfaccia utente grafica e un elenco completo di API REST per implementare tutti i flussi di lavoro di protezione da strumenti interni esistenti.

Astra Control offre un singolo pannello di visualizzazione per le applicazioni containerizzate che include informazioni sulle risorse associate create sul cluster Kubernetes. Puoi visualizzare tutti i tuoi cluster, tutte le tue applicazioni, in tutti i cloud o in tutti i data center utilizzando un unico portale. È possibile utilizzare le API di controllo Astra in tutti gli ambienti (cloud pubblici o on-premise) per implementare i flussi di lavoro di gestione dei dati.

L'immagine seguente mostra le funzionalità di Astra Control.



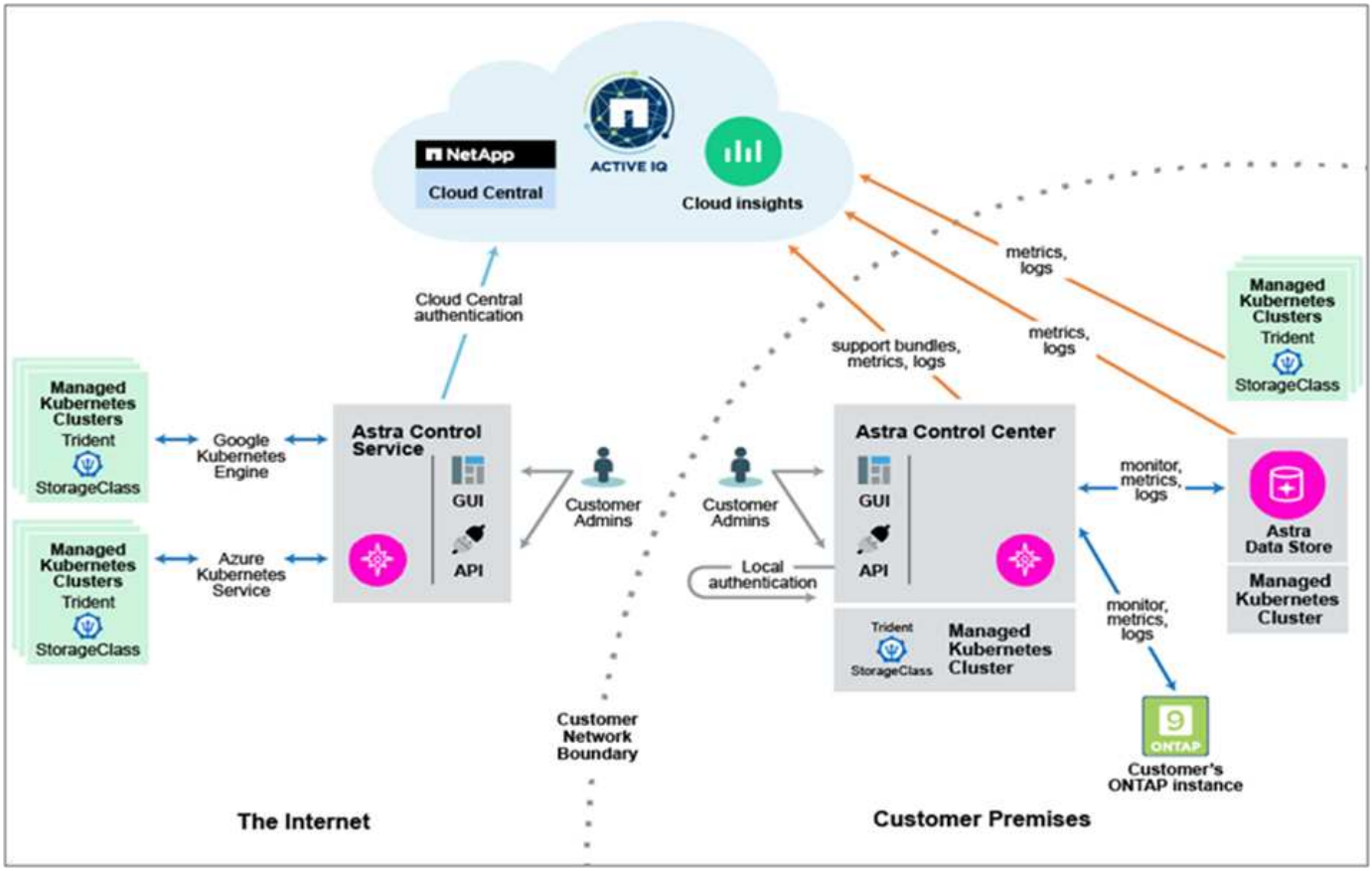
Modelli di consumo Astra Control

Astra Control è disponibile in due modelli di consumo:

- **Astra Control Service.** un servizio completamente gestito ospitato da NetApp che fornisce la gestione dei dati application-aware dei cluster Kubernetes in Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS).
- **Astra Control Center.** Software autogestito che fornisce la gestione dei dati applicativa dei cluster Kubernetes in esecuzione nel tuo ambiente di cloud ibrido e on-premise.

Questo report tecnico sfrutta Astra Control Center per la gestione delle applicazioni native del cloud eseguite su Kubernetes.

L'immagine seguente mostra l'architettura di Astra Control.



Astra Trident

Astra Trident è uno storage orchestrator open-source completamente supportato per container e distribuzioni Kubernetes. È stato progettato fin dall'inizio per soddisfare le esigenze di persistenza delle applicazioni containerizzate utilizzando interfacce standard di settore, come "CSI (Container Storage Interface)". Con Astra Trident, i microservizi e le applicazioni containerizzate possono sfruttare i servizi storage di livello Enterprise forniti dal portfolio di sistemi storage NetApp.

Astra Trident viene implementato sui cluster Kubernetes come pod e fornisce servizi di orchestrazione dello storage dinamico per i carichi di lavoro Kubernetes. Consente alle applicazioni containerizzate di consumare storage persistente in modo rapido e semplice dall'ampio portfolio NetApp, che include NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, Cloud, E Amazon FSX per NetApp ONTAP), il software NetApp Element (NetApp SolidFire), il servizio Azure NetApp Files, il servizio volumi cloud su Google Cloud e il servizio volumi cloud su AWS. In un ambiente FlexPod, Astra Trident viene utilizzato per eseguire il provisioning e la gestione dinamica dei volumi persistenti per i container supportati dai volumi e LUN FlexVol NetApp ospitati su una piattaforma di storage ONTAP, come i sistemi NetApp AFF e FAS e Cloud Volumes ONTAP. Trident svolge anche un ruolo chiave nell'implementazione degli schemi di protezione delle applicazioni forniti da Astra Control. Per ulteriori informazioni su Astra Trident, vedere "Documentazione di Astra Trident."

Back-end dello storage

Per utilizzare Astra Trident, è necessario il backend dello storage supportato. Un backend Trident definisce la relazione tra Trident e un sistema storage. Spiega a Trident come comunicare con quel sistema storage e come Trident dovrebbe eseguire il provisioning dei volumi da esso. Trident offrirà automaticamente pool di storage da backend che insieme soddisfano i requisiti definiti da una classe di storage.

- Backend di storage ONTAP AFF e FAS. In qualità di piattaforma hardware e software per lo storage,

ONTAP offre servizi di storage di base, supporto per più protocolli di accesso allo storage e funzionalità di gestione dello storage, come copie Snapshot e mirroring NetApp.

- Back-end dello storage Cloud Volumes ONTAP
- "Archivio dati Astra" back-end dello storage

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è un'offerta di storage software-defined che offre gestione avanzata dei dati per carichi di lavoro di file e blocchi. Con Cloud Volumes ONTAP, puoi ottimizzare i costi di cloud storage e aumentare le performance applicative, migliorando al contempo protezione dei dati, sicurezza e conformità.

I vantaggi principali includono:

- Sfrutta la deduplica dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi dello storage.
- Garantisci l'affidabilità aziendale e le operazioni continue in caso di guasti nel tuo ambiente cloud.
- Cloud Volumes ONTAP sfrutta SnapMirror, la tecnologia di replica leader del settore di NetApp, per replicare i dati on-premise nel cloud, in modo da poter disporre facilmente di copie secondarie per diversi casi di utilizzo.
- Cloud Volumes ONTAP si integra anche con Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.
- Passa tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.
- Garantire la coerenza delle copie Snapshot con NetApp SnapCenter.
- Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.
- L'integrazione con Cloud Data Sense ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

Cloud Central

Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il backup dei dati e migrare e controllare in modo efficace i dati su più cloud. Per ulteriori informazioni, vedere "Cloud Central."

Cloud Manager

Cloud Manager è una piattaforma di gestione di livello Enterprise basata su SaaS che consente agli esperti IT e agli architetti del cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud di NetApp. Fornisce un sistema centralizzato per la visualizzazione e la gestione dello storage on-premise e cloud, supportando account e provider di cloud ibridi e multipli. Per ulteriori informazioni, vedere "Cloud Manager".

Connettore

Connector è un'istanza che consente a Cloud Manager di gestire risorse e processi all'interno dell'ambiente di cloud pubblico. È necessario un connettore per utilizzare molte funzionalità offerte da Cloud Manager. Un connettore può essere implementato nel cloud o nella rete on-premise.

Il connettore è supportato nelle seguenti posizioni:

- AWS
- Microsoft Azure
- Google Cloud
- On-premise

Per ulteriori informazioni su Connector, vedere "questo link."

NetApp Cloud Insights

Cloud Insights, uno strumento di monitoraggio dell'infrastruttura cloud di NetApp, consente di monitorare le performance e l'utilizzo dei cluster Kubernetes gestiti dal centro di controllo Astra. Cloud Insights mette in relazione l'utilizzo dello storage con i carichi di lavoro. Quando si attiva la connessione Cloud Insights in Astra Control Center, le informazioni di telemetria vengono visualizzate nelle pagine dell'interfaccia utente di Astra Control Center.

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager consente di monitorare i cluster di storage ONTAP da un'unica interfaccia intuitiva e ridisegnata che offre intelligence basata su saggezza della community e analisi ai. Fornisce informazioni complete su operazioni, performance e attività proattive nell'ambiente di storage e nelle macchine virtuali (VM) in esecuzione sull'ambiente IT. Quando si verifica un problema con l'infrastruttura di storage, Unified Manager può notificare i dettagli del problema per identificare la causa principale. Il dashboard delle macchine virtuali offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter analizzare l'intero percorso di i/o dall'host VMware vSphere fino alla rete e infine allo storage. Alcuni eventi forniscono anche azioni correttive che possono essere intraprese per risolvere il problema. È possibile configurare avvisi personalizzati per gli eventi in modo che, quando si verificano problemi, venga inviata una notifica tramite e-mail e trap SNMP. Active IQ Unified Manager consente di pianificare i requisiti di storage degli utenti prevedendo le tendenze di capacità e utilizzo per agire in modo proattivo prima che si verifichino problemi, evitando decisioni reattive a breve termine che possono portare a ulteriori problemi a lungo termine.

Cisco Intersight

Cisco Intersight è una piattaforma SaaS che offre automazione, osservabilità e ottimizzazione intelligenti per infrastrutture e applicazioni tradizionali e native del cloud. La piattaforma aiuta a promuovere il cambiamento con i team IT e offre un modello operativo progettato per il cloud ibrido.

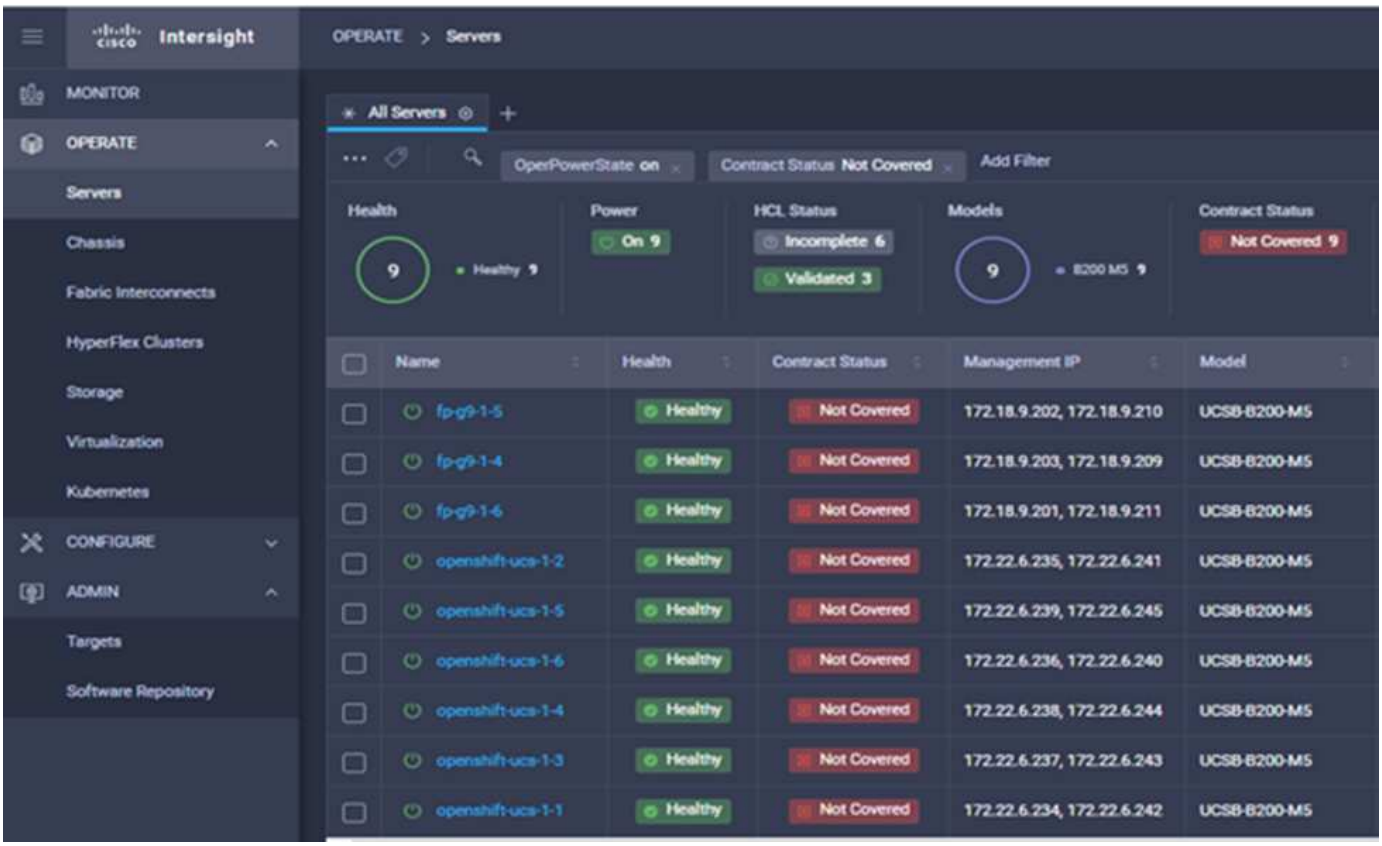
Cisco Intersight offre i seguenti vantaggi:

- **Delivery più rapida.** offerta come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può semplicemente concentrarsi sull'accelerazione della consegna per la linea di business.
- **Operazioni semplificate.** semplifica le operazioni utilizzando un unico tool sicuro fornito da SaaS con inventario, autenticazione e API comuni per lavorare in stack completi e in tutte le ubicazioni, eliminando i silos tra i team. Dalla gestione on-premise di server fisici e hypervisor a macchine virtuali, K8s, serverless, automazione, ottimizzazione e controllo dei costi su cloud pubblici e on-premise.
- **Ottimizzazione continua.** Ottimizza continuamente il tuo ambiente utilizzando l'intelligence fornita da Cisco Intersight su ogni livello e Cisco TAC. Questa intelligenza viene convertita in azioni consigliate e automatizzabili, in modo da poter adattare in tempo reale ad ogni cambiamento: Dallo spostamento dei carichi di lavoro al monitoraggio dello stato di salute dei server fisici al dimensionamento automatico dei cluster K8s, ai consigli per la riduzione dei costi sui cloud pubblici con cui lavorate.

Cisco Intersight offre due modalità di gestione: UCSM Managed Mode (UMM) e Intersight Managed Mode

(IMM). È possibile selezionare L'UMM o IMM nativo per i sistemi Cisco UCS collegati al fabric durante la configurazione iniziale delle interconnessioni fabric. In questa soluzione viene utilizzato UMM nativo.

La seguente immagine mostra la dashboard di Cisco Intersight.

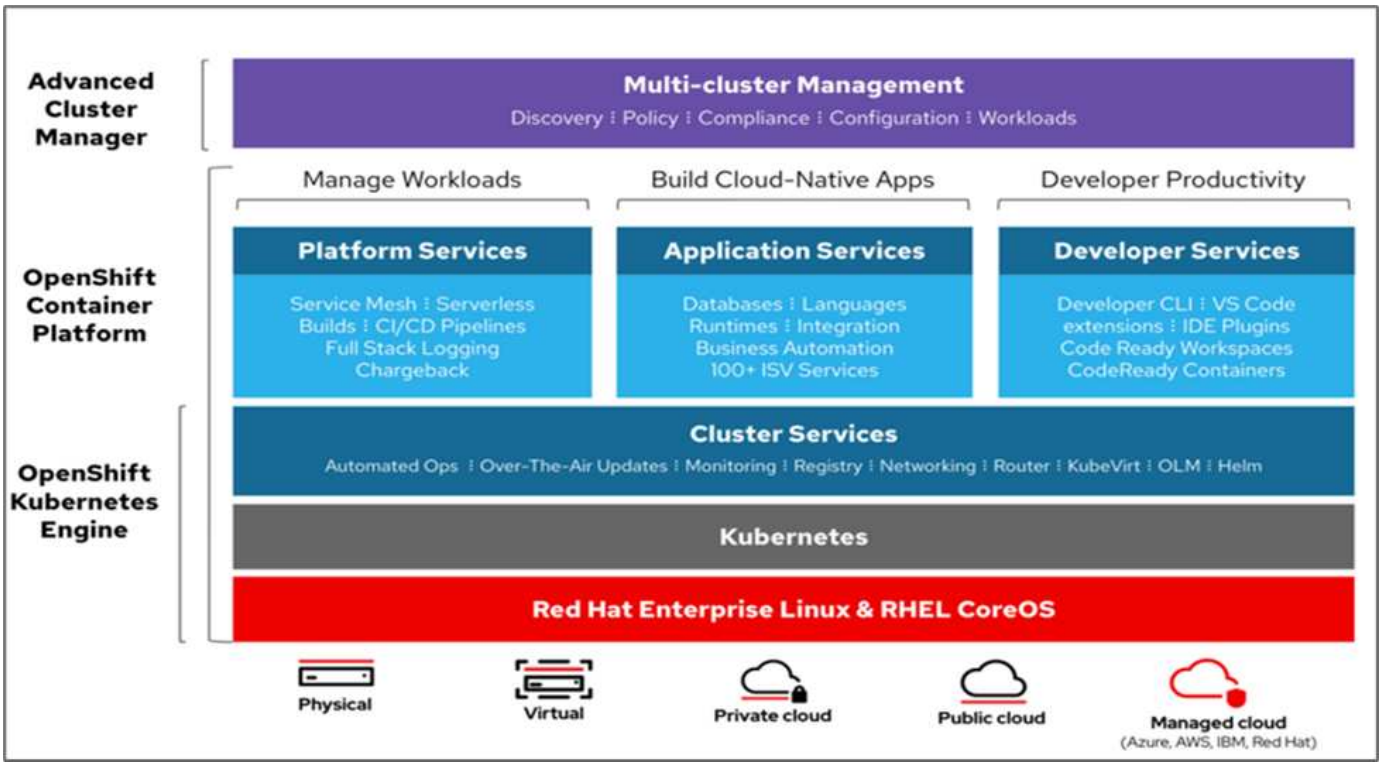


Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform è una piattaforma applicativa container che riunisce CRI-o e Kubernetes e fornisce un'API e un'interfaccia web per gestire questi servizi. CRI-o è un'implementazione della Kubernetes Container Runtime Interface (CRI) per consentire l'utilizzo di runtime compatibili con Open Container Initiative (OCI). Si tratta di un'alternativa leggera all'utilizzo di Docker come runtime per Kubernetes.

OpenShift Container Platform consente ai clienti di creare e gestire container. I container sono processi standalone che vengono eseguiti all'interno del proprio ambiente, indipendentemente dal sistema operativo e dall'infrastruttura sottostante. OpenShift Container Platform aiuta a sviluppare, implementare e gestire applicazioni basate su container. Offre una piattaforma self-service per creare, modificare e implementare applicazioni on-demand, consentendo cicli di sviluppo e rilascio più rapidi. OpenShift Container Platform dispone di un'architettura basata su microservizi di unità più piccole e separate che funzionano insieme. Viene eseguito su un cluster Kubernetes, con i dati sugli oggetti memorizzati in etcd, un archivio chiavi-valore in cluster affidabile.

L'immagine seguente è una panoramica della piattaforma container Red Hat OpenShift.



Infrastruttura Kubernetes

All'interno di OpenShift Container Platform, Kubernetes gestisce le applicazioni containerizzate su un set di host runtime CRI-o e fornisce meccanismi per l'implementazione, la manutenzione e la scalabilità delle applicazioni. Il servizio CRI-o crea pacchetti, crea istanze ed esegue applicazioni containerizzate.

Un cluster Kubernetes è costituito da uno o più master e da un insieme di nodi di lavoro. Questa progettazione della soluzione include funzionalità ad alta disponibilità (ha) sull'hardware e sullo stack software. Un cluster Kubernetes è progettato per essere eseguito in modalità ha con tre nodi master e un minimo di due nodi di lavoro per garantire che il cluster non abbia un singolo punto di errore.

So Red Hat Core

OpenShift Container Platform utilizza Red Hat Enterprise Linux CoreOS (RHCOS), un sistema operativo orientato ai container che combina alcune delle migliori funzionalità dei sistemi operativi CoreOS e Red Hat Atomic host. RHCOS è progettato appositamente per l'esecuzione di applicazioni containerizzate da OpenShift Container Platform e lavora con nuovi tool per fornire installazione rapida, gestione basata sull'operatore e aggiornamenti semplificati.

RHCOS include le seguenti funzionalità:

- Ignition, che OpenShift Container Platform utilizza come prima configurazione del sistema di boot per l'avvio iniziale e la configurazione delle macchine.
- CRI-o, un'implementazione nativa del runtime di container di Kubernetes che si integra a stretto contatto con il sistema operativo per offrire un'esperienza Kubernetes efficiente e ottimizzata. CRI-o offre funzionalità per l'esecuzione, l'arresto e il riavvio dei container. Sostituisce completamente Docker Container Engine, utilizzato in OpenShift Container Platform 3.
- Kubernetes, il principale agente di nodo di Kubernetes, è responsabile del lancio e del monitoraggio dei container.

VMware vSphere 7.0

VMware vSphere è una piattaforma di virtualizzazione per la gestione olistica di grandi insiemi di infrastrutture (risorse tra cui CPU, storage e networking) come ambiente operativo perfetto, versatile e dinamico. A differenza dei sistemi operativi tradizionali che gestiscono un singolo computer, VMware vSphere aggrega l'infrastruttura di un intero data center per creare un singolo power house con risorse che possono essere allocate in modo rapido e dinamico a qualsiasi applicazione in necessità.

Per ulteriori informazioni, vedere "VMware vSphere".

VMware vSphere vCenter

VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da una singola console e aggrega il monitoraggio delle performance di cluster, host e macchine virtuali. VMware vCenter Server offre agli amministratori una panoramica approfondita dello stato e della configurazione di cluster di calcolo, host, macchine virtuali, storage, sistema operativo guest, e altri componenti critici di un'infrastruttura virtuale. VMware vCenter gestisce l'insieme completo di funzionalità disponibili in un ambiente VMware vSphere.

Revisioni hardware e software

Questa soluzione può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware, come definito nella "Tool di matrice di interoperabilità NetApp" e. "Elenco di compatibilità hardware Cisco UCS." Il cluster OpenShift viene installato su FlexPod in maniera bare metal e su VMware vSphere.

Solo una singola istanza di Astra Control Center è necessaria per gestire più cluster OpenShift (k8s), mentre Trident CSI è installato su ciascun cluster OpenShift. Astra Control Center può essere installato su uno qualsiasi di questi cluster OpenShift. In questa soluzione, Astra Control Center viene installato sul cluster bare-metal OpenShift.

La seguente tabella elenca le revisioni hardware e software di FlexPod per OpenShift.

Componente	Prodotto	Versione
Calcolo	Cisco UCS Fabric Interconnects 6454	4.1(3c)
	Server Cisco UCS B200 M5	4.1(3c)
Rete	Sistema operativo Cisco Nexus 9336C-FX2 NX	9.3(8)
Storage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9.11
Software	Driver Ethernet Nenico VMware ESXi	1.0.35.0
	VSphere ESXi	7.0 (U2)
	Appliance VMware vCenter	7.0 U2b

Componente	Prodotto	Versione
	Appliance virtuale Cisco Intersight Assist	1.0.9-342
	Piattaforma container OpenShift	4.9
	Nodo master della piattaforma container OpenShift	RHCOS 4.9
	Nodo di lavoro della piattaforma container OpenShift	RHCOS 4.9

La seguente tabella elenca le versioni software di OpenShift su AWS.

Componente	Prodotto	Versione
Calcolo	Tipo istanza master: m5.xlarge	n/a.
	Tipo di istanza di lavoro: m5.Large	n/a.
Rete	Virtual Private Cloud Transit Gateway	n/a.
Storage	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Software	Piattaforma container OpenShift	4.9
	Nodo master della piattaforma container OpenShift	RHCOS 4.9
	Nodo di lavoro della piattaforma container OpenShift	RHCOS 4.9

"Avanti: Installazione bare-metal di FlexPod per la piattaforma container OpenShift 4."

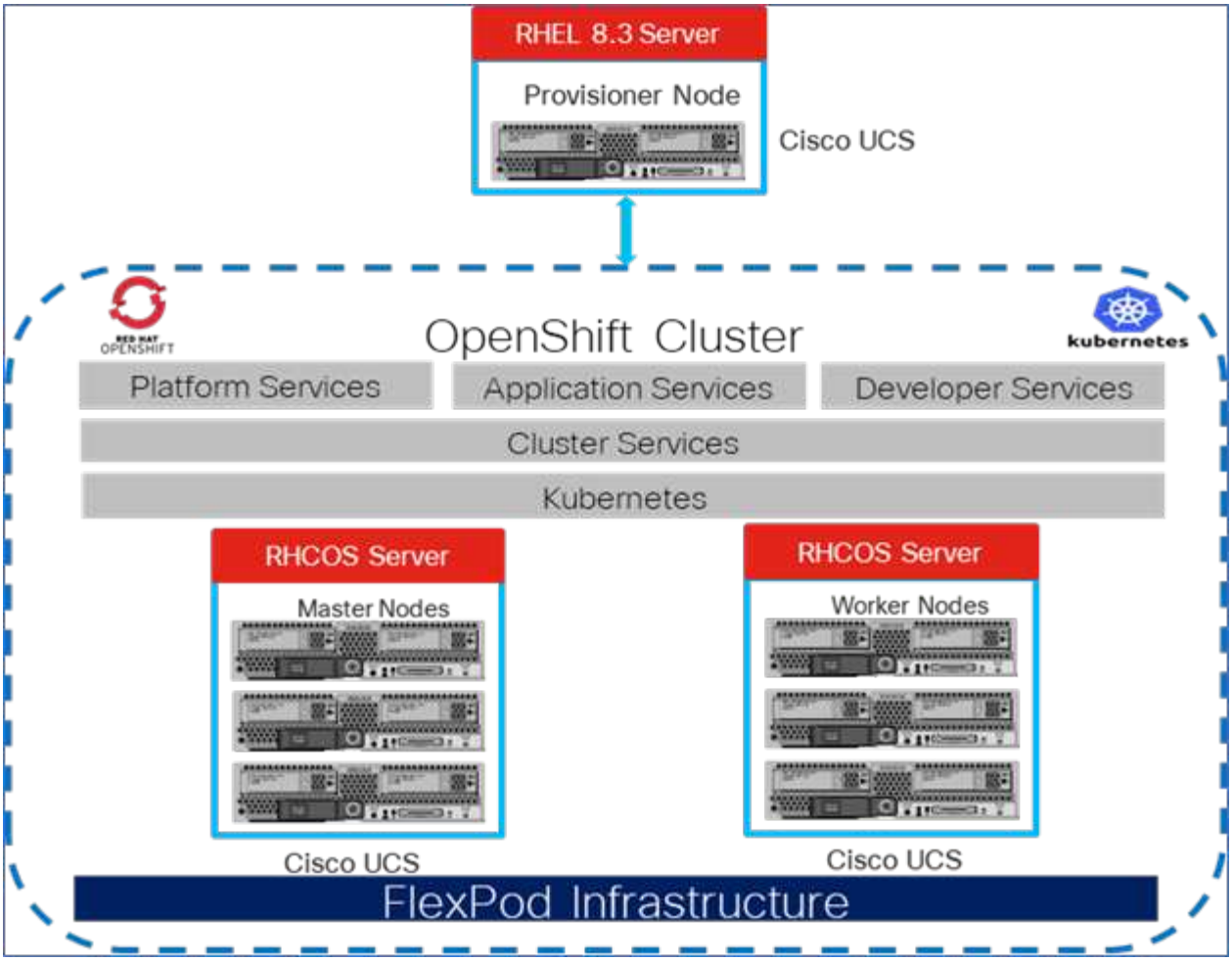
Installazione e configurazione

Installazione bare-metal di FlexPod per piattaforma container OpenShift 4

"Precedente: Componenti della soluzione."

Per informazioni sulla progettazione bare-metal di FlexPod per la piattaforma container OpenShift 4, sui dettagli di implementazione e sull'installazione e configurazione di NetApp Astra Trident, vedere "FlexPod con OpenShift Guida alla progettazione e all'implementazione validate di Cisco (CVD)". Questo CVD copre l'implementazione di FlexPod e della piattaforma container OpenShift utilizzando Ansible. Il CVD fornisce inoltre informazioni dettagliate sulla preparazione dei nodi di lavoro, sull'installazione di Astra Trident, sul backend dello storage e sulle configurazioni di classe storage, che sono i pochi prerequisiti per l'implementazione e la configurazione di Astra Control Center.

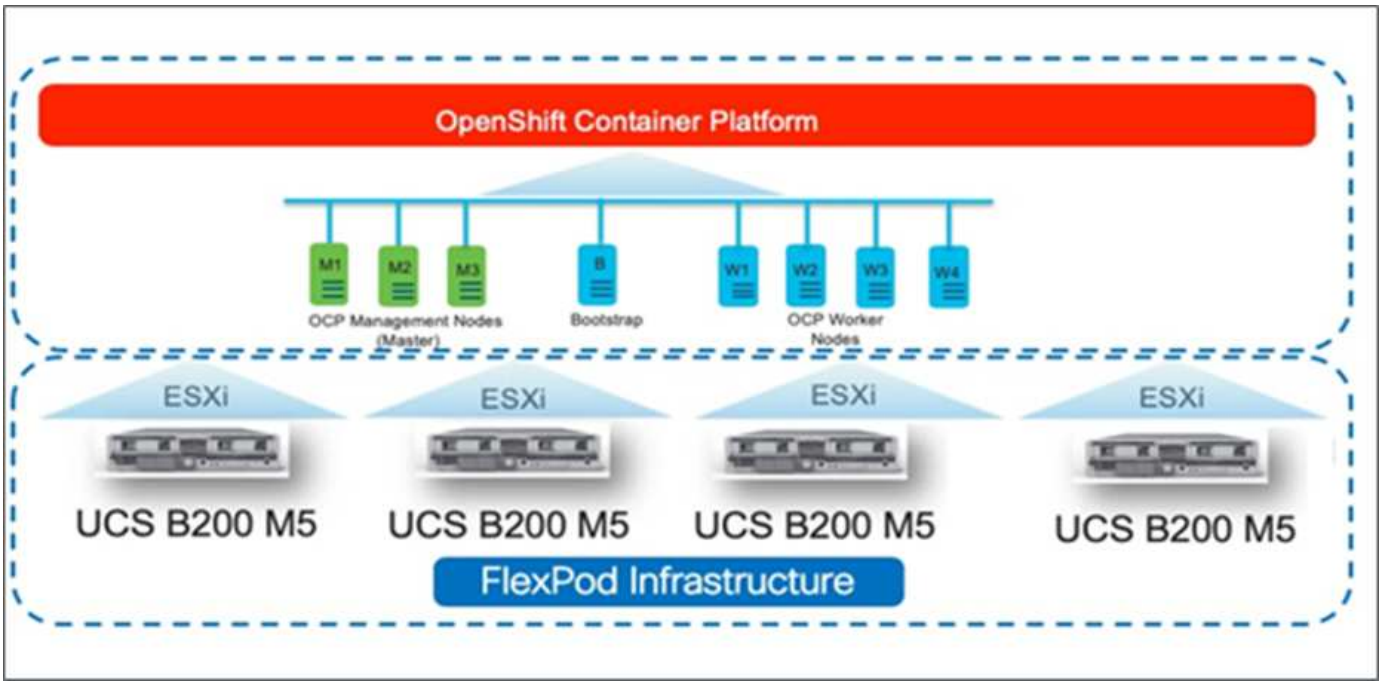
La figura seguente illustra la piattaforma container OpenShift 4 Bare Metal su FlexPod.



Installazione di FlexPod per piattaforma container OpenShift 4 su VMware

Per ulteriori informazioni sull'implementazione di Red Hat OpenShift Container Platform 4 su FlexPod con VMware vSphere, vedere "Data center FlexPod per piattaforma container OpenShift 4".

La figura seguente illustra FlexPod per piattaforma container OpenShift 4 su vSphere.

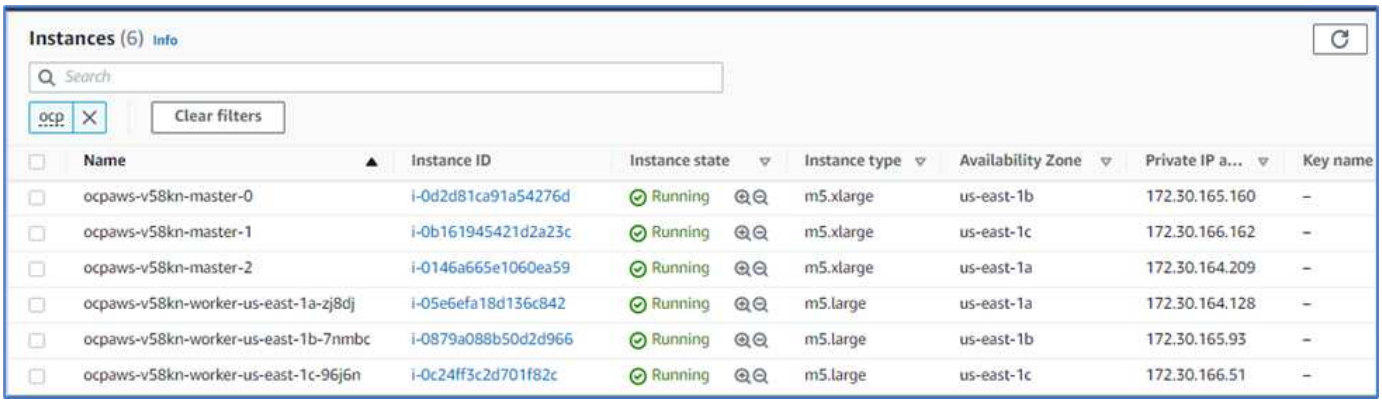


"Avanti: Red Hat OpenShift su AWS."

Red Hat OpenShift su AWS

"Precedente: Installazione bare-metal di FlexPod per piattaforma container OpenShift 4."

Un cluster OpenShift Container Platform 4 separato e autogestito viene implementato su AWS come sito di DR. I nodi master e worker si estendono in tre zone di disponibilità per garantire l'alta disponibilità.



Instances (6) Info

Search

ocp | Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                              STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal    Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal    Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal     Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal    Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal     Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift viene implementato come "cluster privato" In un VPC esistente su AWS. Un cluster OpenShift Container Platform privato non espone endpoint esterni ed è accessibile solo da una rete interna e non è visibile su Internet. Un NetApp Cloud Volumes ONTAP a nodo singolo viene implementato utilizzando NetApp Cloud Manager, che fornisce un backend di storage ad Astra Trident.

Per ulteriori informazioni sull'installazione di OpenShift su AWS, vedere "Documentazione di OpenShift".

"Pagina successiva: NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Precedente: Red Hat OpenShift su AWS."

L'istanza di NetApp Cloud Volumes ONTAP viene implementata su AWS e funge da storage back-end per Astra Trident. Prima di aggiungere un ambiente di lavoro Cloud Volumes ONTAP, è necessario implementare un connettore. Cloud Manager ti chiede se provi a creare il tuo primo ambiente di lavoro Cloud Volumes ONTAP senza un connettore. Per implementare un connettore in AWS, vedere "Creare un connettore".

Per implementare Cloud Volumes ONTAP su AWS, vedere "Quick Start per AWS".

Una volta implementato Cloud Volumes ONTAP, è possibile installare Astra Trident e configurare il backend dello storage e la classe Snapshot sul cluster della piattaforma container OpenShift.

"Avanti: Installazione di Astra Control Center su OpenShift Container Platform."

Installazione di Astra Control Center su OpenShift Container Platform

"Precedente: NetApp Cloud Volumes ONTAP."

È possibile installare Astra Control Center sul cluster OpenShift in esecuzione su FlexPod o su AWS con un backend di storage Cloud Volumes ONTAP. In questa soluzione, Astra Control Center viene implementato sul cluster bare-metal OpenShift.

Astra Control Center può essere installato utilizzando il processo standard descritto "qui" Oppure da Red Hat OpenShift OperatorHub. Astra Control Operator è un operatore certificato Red Hat. In questa soluzione, Astra Control Center viene installato utilizzando Red Hat OperatorHub.

Requisiti ambientali

- Astra Control Center supporta più distribuzioni Kubernetes; per Red Hat OpenShift, le versioni supportate

includono Red Hat OpenShift Container Platform 4.8 o 4.9.

- Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse applicative dell'ambiente e dell'utente finale:

Componenti	Requisito
Capacità di back-end dello storage	Almeno 500 GB disponibili
Nodi di lavoro	Almeno 3 nodi di lavoro, con 4 core CPU e 12 GB di RAM ciascuno
Indirizzo FQDN (Fully Qualified Domain Name)	Un indirizzo FQDN per Astra Control Center
Astra Trident	Astra Trident 21.04 o versione successiva installata e configurata
Controller di ingresso o bilanciamento del carico	Configurare il controller di ingresso per esporre Astra Control Center con un URL o un bilanciamento del carico per fornire l'indirizzo IP che verrà risolto nell'FQDN

- È necessario disporre di un registro di immagini privato esistente in cui trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui vengono caricate le immagini.

> Alcune immagini vengono estratte durante l'esecuzione di determinati flussi di lavoro e i container vengono creati e distrutti quando necessario.

- Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Centro di controllo Astra supporta i seguenti driver ONTAP forniti da Astra Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-economy

> Supponiamo che i cluster OpenShift implementati abbiano Astra Trident installato e configurato con un backend ONTAP e sia definita anche una classe di storage predefinita.

- Per la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per modificare il criterio di esportazione ONTAP in modo da consentire queste operazioni, eseguire i seguenti comandi:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

> Per aggiungere un secondo ambiente operativo OpenShift come risorsa di calcolo gestita, assicurarsi che la funzione Astra Trident Volume snapshot sia attivata. Per abilitare e testare le snapshot dei volumi con Astra Trident, consulta la pagina ufficiale "Istruzioni di Astra Trident".

- R "VolumeSnapClass" Deve essere configurato su tutti i cluster Kubernetes da cui vengono gestite le applicazioni. Questo potrebbe includere anche il cluster K8s su cui è installato Astra Control Center. Astra Control Center è in grado di gestire le applicazioni sul cluster K8s su cui è in esecuzione.

Requisiti di gestione delle applicazioni

- **Licensing.** per gestire le applicazioni utilizzando Astra Control Center, è necessaria una licenza Astra Control Center.
- **Namespaces.** Uno spazio dei nomi è l'entità più grande che può essere gestita come applicazione da Astra Control Center. È possibile scegliere di filtrare i componenti in base alle etichette dell'applicazione e alle etichette personalizzate in uno spazio dei nomi esistente e gestire un sottoinsieme di risorse come applicazione.
- **StorageClass.** se si installa un'applicazione con un StorageClass esplicitamente impostato ed è necessario clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la StorageClass originariamente specificata. La clonazione di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass ha esito negativo.
- **Kubernetes resources.** le applicazioni che utilizzano risorse Kubernetes non acquisite da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati applicativi. Astra Control può acquisire le seguenti risorse Kubernetes:

Risorse Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	CustomResource	Lavoro di cassa
DemonSet	HorizontalPodAutoscaler	Ingresso
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
NetworkPolicy	ReplicaSet	Ruolo
RoleBinding	Percorso	Segreto
ValidatingWebhook		

Installare Astra Control Center utilizzando OpenShift OperatorHub

La seguente procedura consente di installare Astra Control Center utilizzando Red Hat OperatorHub. In questa soluzione, Astra Control Center viene installato su un cluster OpenShift bare-metal in esecuzione su FlexPod.

1. Scarica il bundle Astra Control Center (`astra-control-center-[version].tar.gz`) da "Sito di supporto NetApp".
2. Scaricare il file .zip per i certificati e le chiavi di Astra Control Center da "Sito di supporto NetApp".
3. Verificare la firma del bundle.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Estrarre le immagini Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Passare alla directory Astra.

```
cd astra-control-center-[version]
```

6. Aggiungere le immagini al registro locale.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilizzare lo script appropriato per caricare le immagini, etichettarle e inserirle nel registro locale.

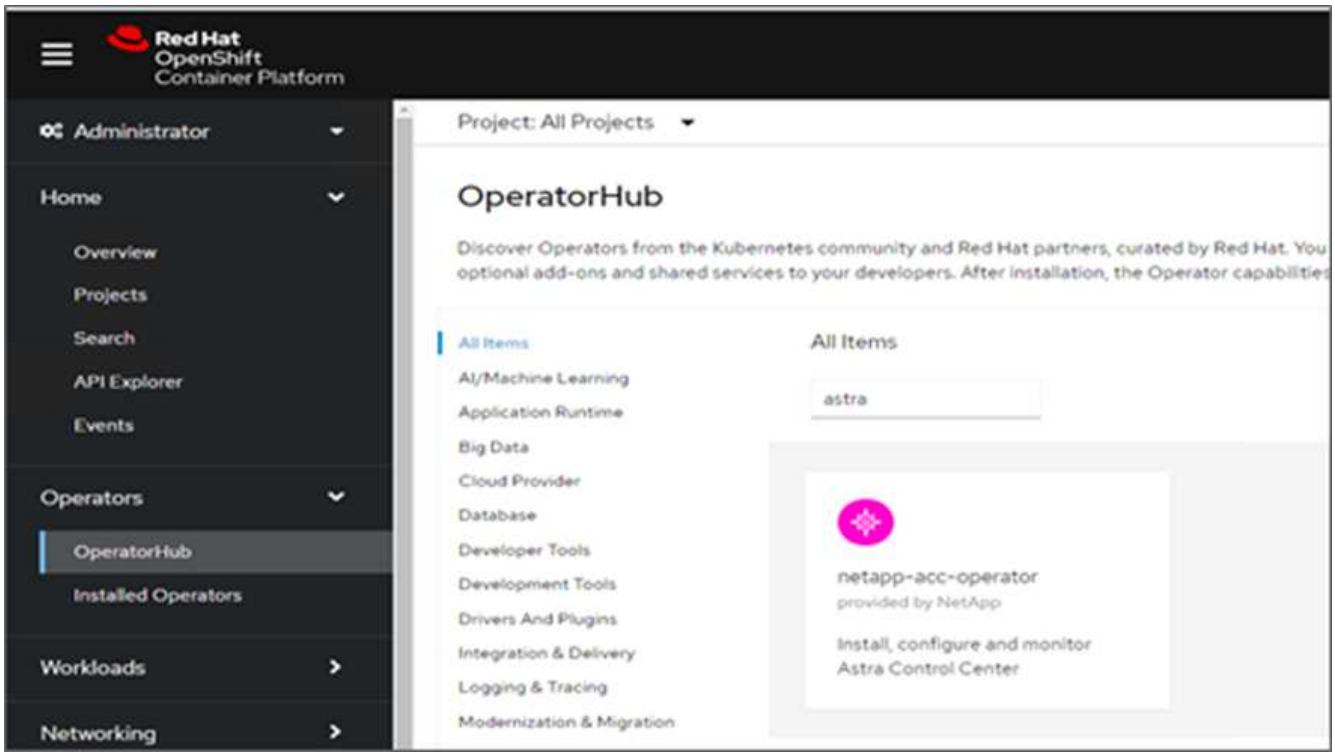
   Per Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Per Podman:

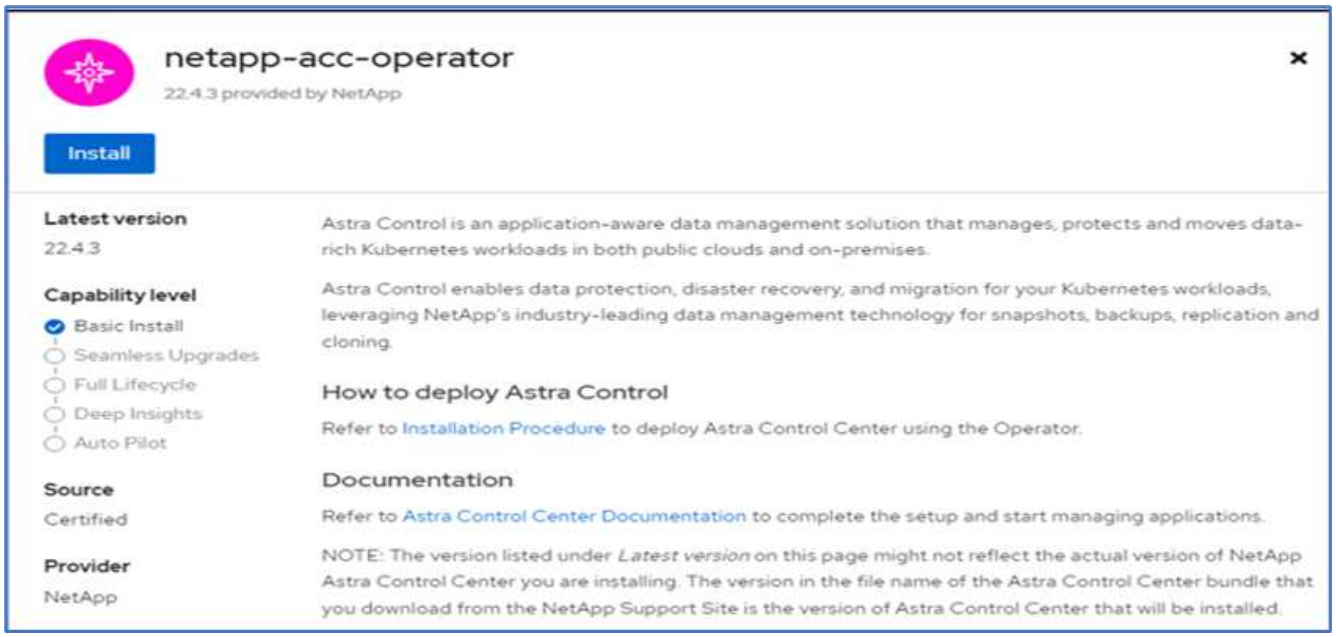
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Accedere alla console web del cluster OpenShift bare-metal. Dal menu laterale, selezionare Operator (operatori) > OperatorHub. Invio `astra` per visualizzare l'elenco di `netapp-acc-operator`.

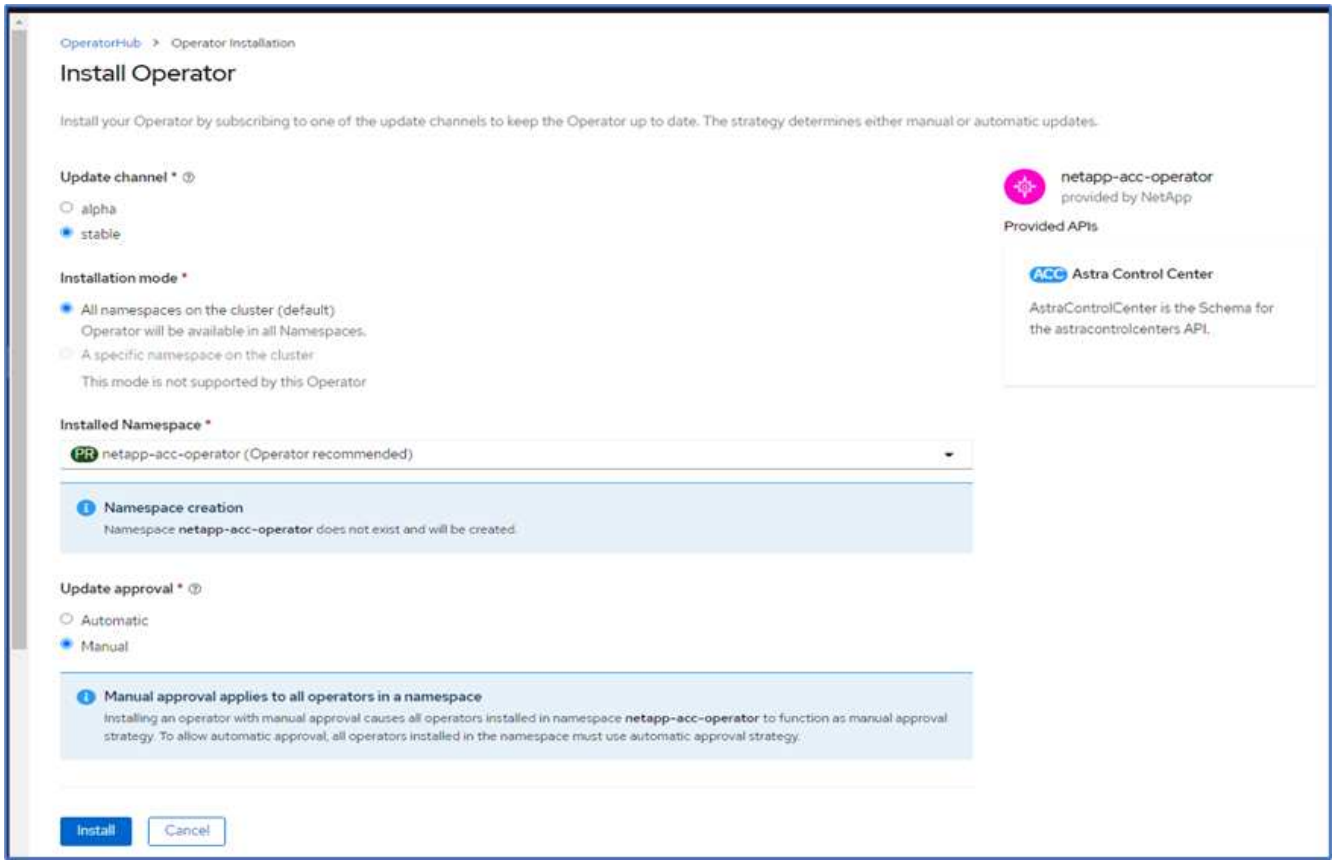


> `netapp-acc-operator` È un operatore Red Hat OpenShift certificato ed è elencato nel catalogo OperatorHub.

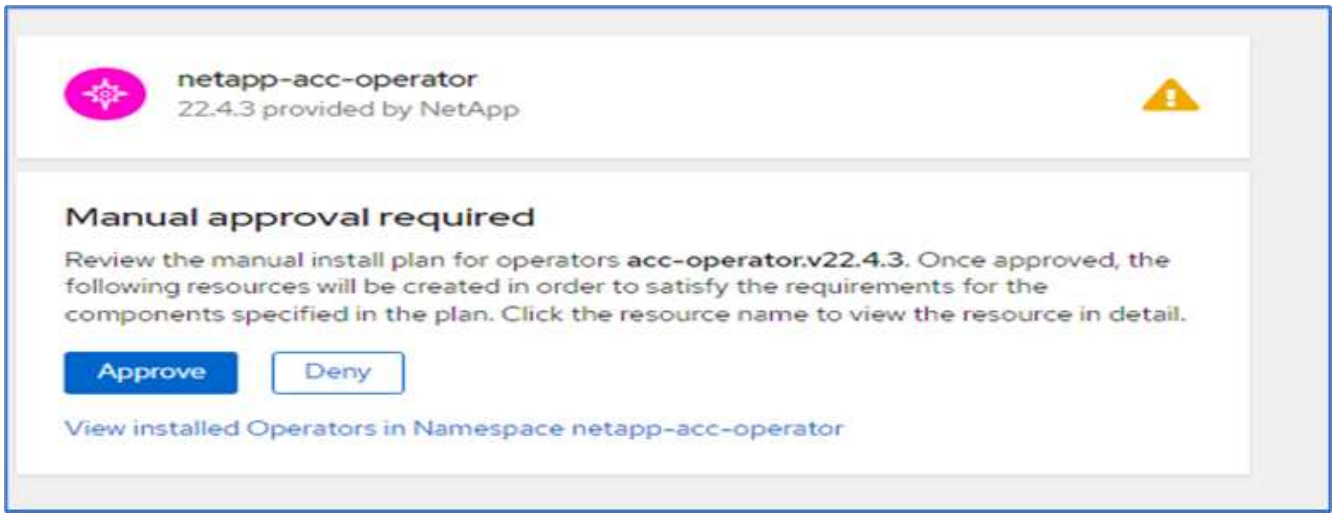
9. Selezionare `netapp-acc-operator` E fare clic su Installa.



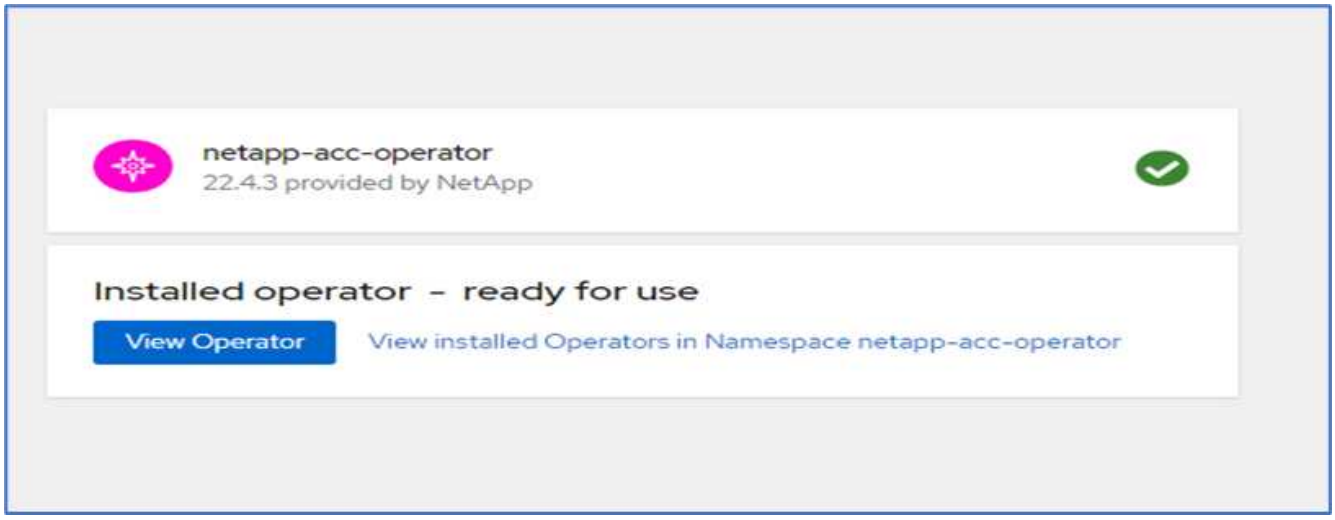
10. Selezionare le opzioni appropriate e fare clic su Install (Installa).



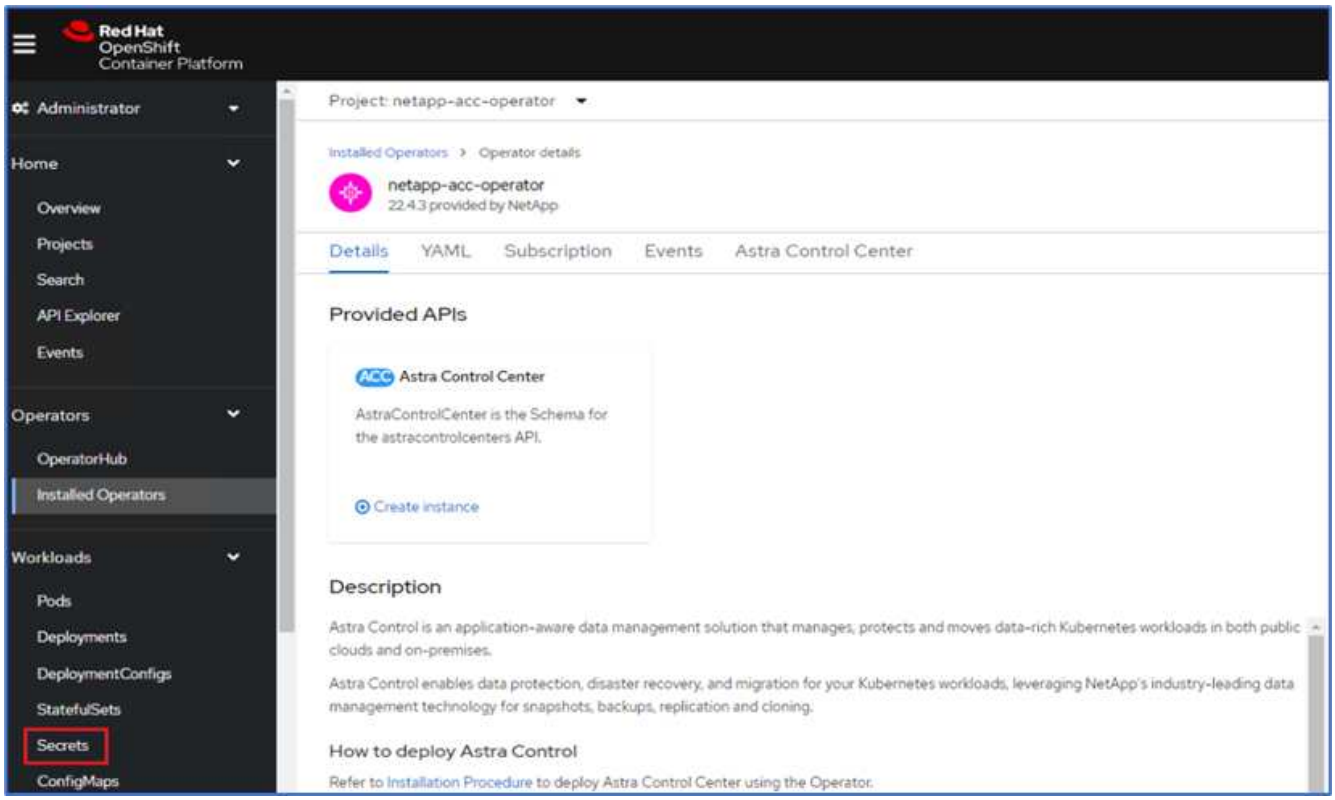
11. Approvare l'installazione e attendere l'installazione dell'operatore.



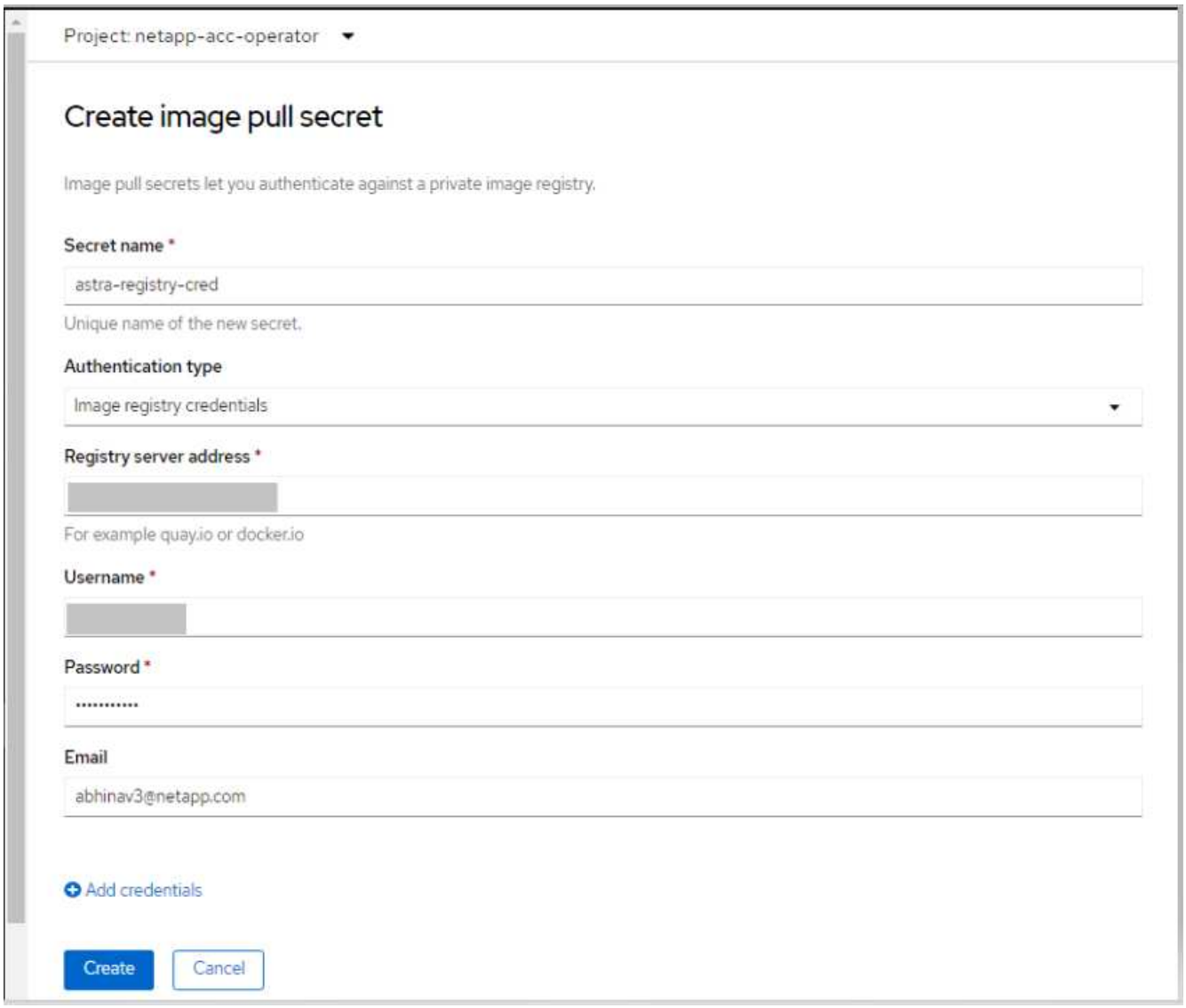
12. A questo punto, l'operatore viene installato correttamente e pronto per l'uso. Fare clic su View Operator (Visualizza operatore) per avviare l'installazione di Astra Control Center.



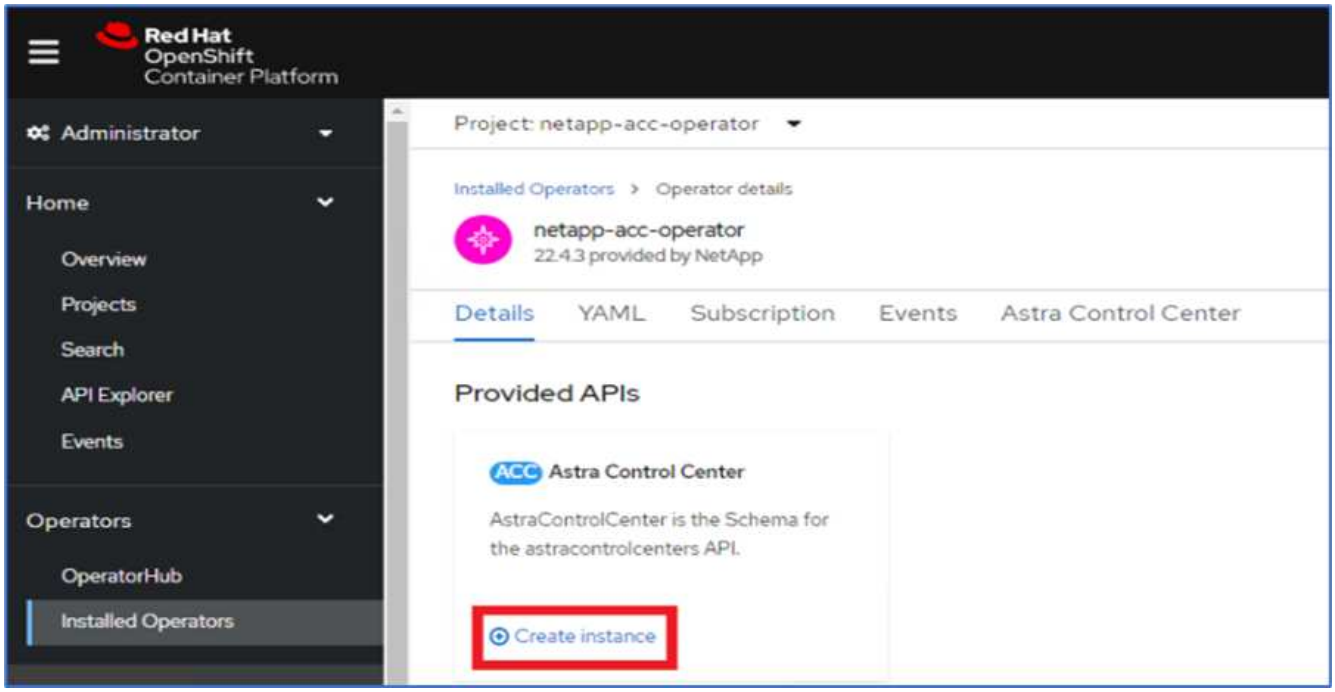
13. Prima di installare Astra Control Center, creare il segreto pull per scaricare le immagini Astra dal registro Docker precedentemente inserito.



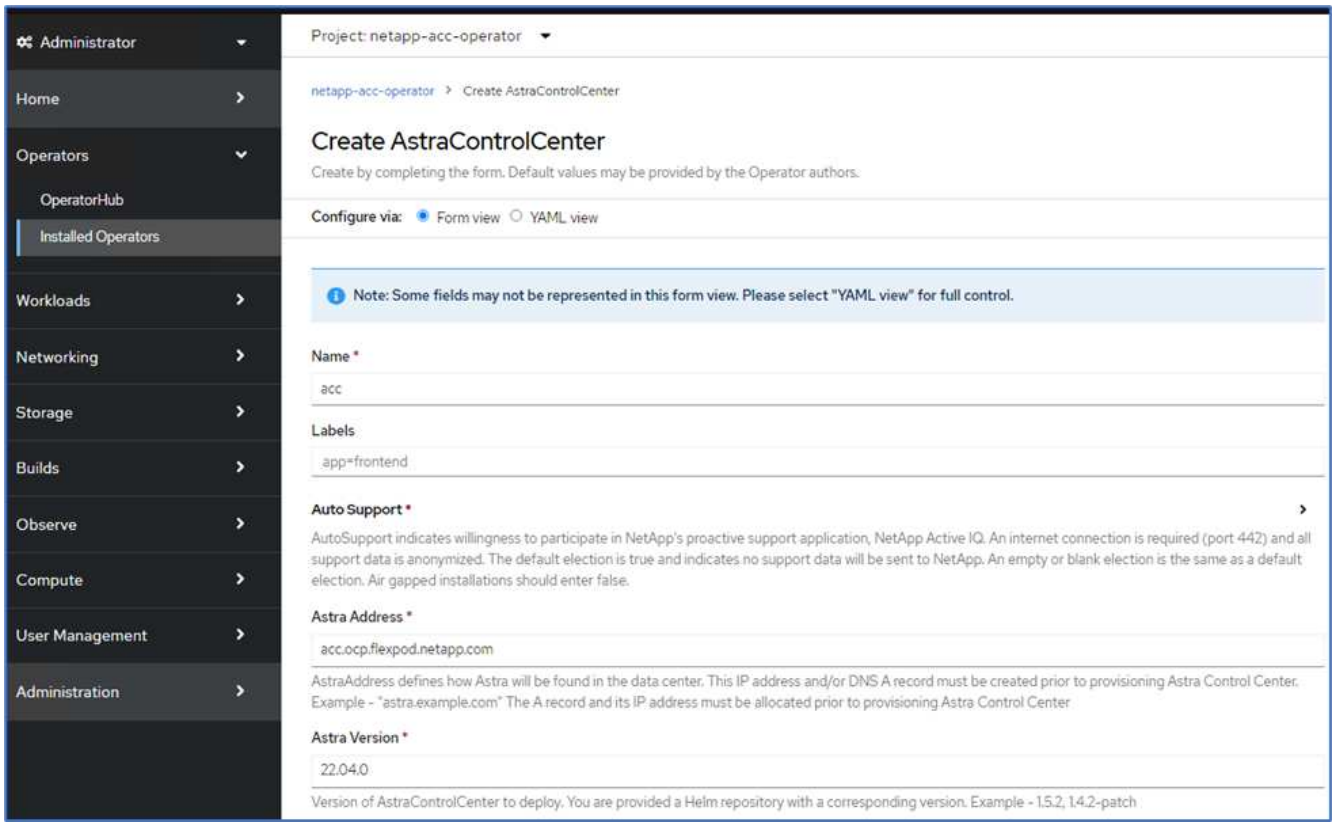
14. Per estrarre le immagini di Astra Control Center dal tuo repo privato Docker, crea un segreto in `netapp-acc-operator` namespace. Questo nome segreto viene fornito nel manifesto YAML di Astra Control Center in un passaggio successivo.



15. Dal menu laterale, selezionare Operator > Installed Operators (operatori > operatori installati) e fare clic su Create Instance (Crea istanza) nella sezione delle API fornite.



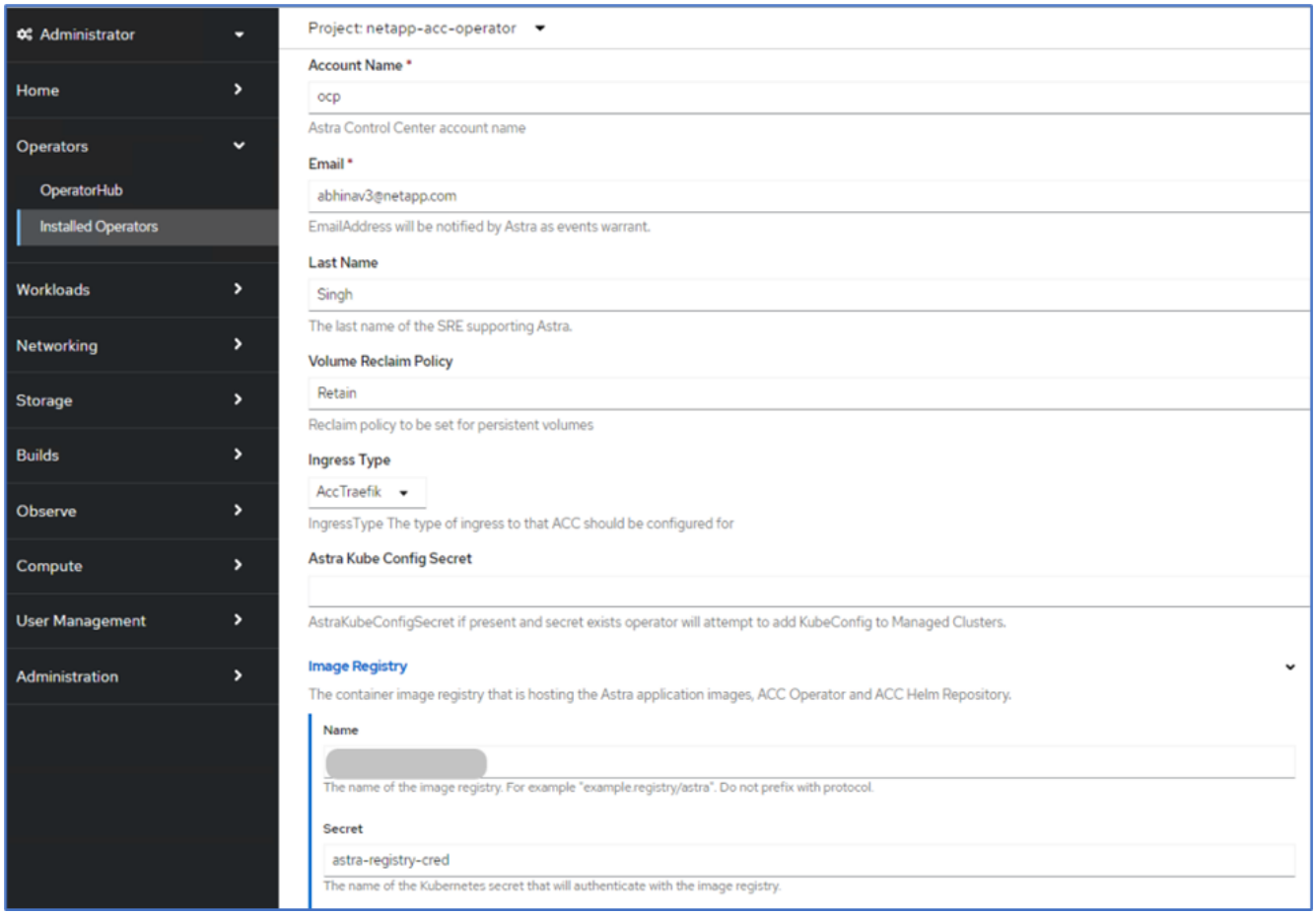
16. Completare il modulo Create AstraControlCenter. Fornire il nome, l'indirizzo Astra e la versione di Astra.



> In Astra Address (Indirizzo Astra), fornire l'indirizzo FQDN per Astra Control Center. Questo indirizzo viene utilizzato per accedere alla console Web di Astra Control Center. Il nome FQDN deve anche essere impostato su una rete IP raggiungibile e deve essere configurato nel DNS.

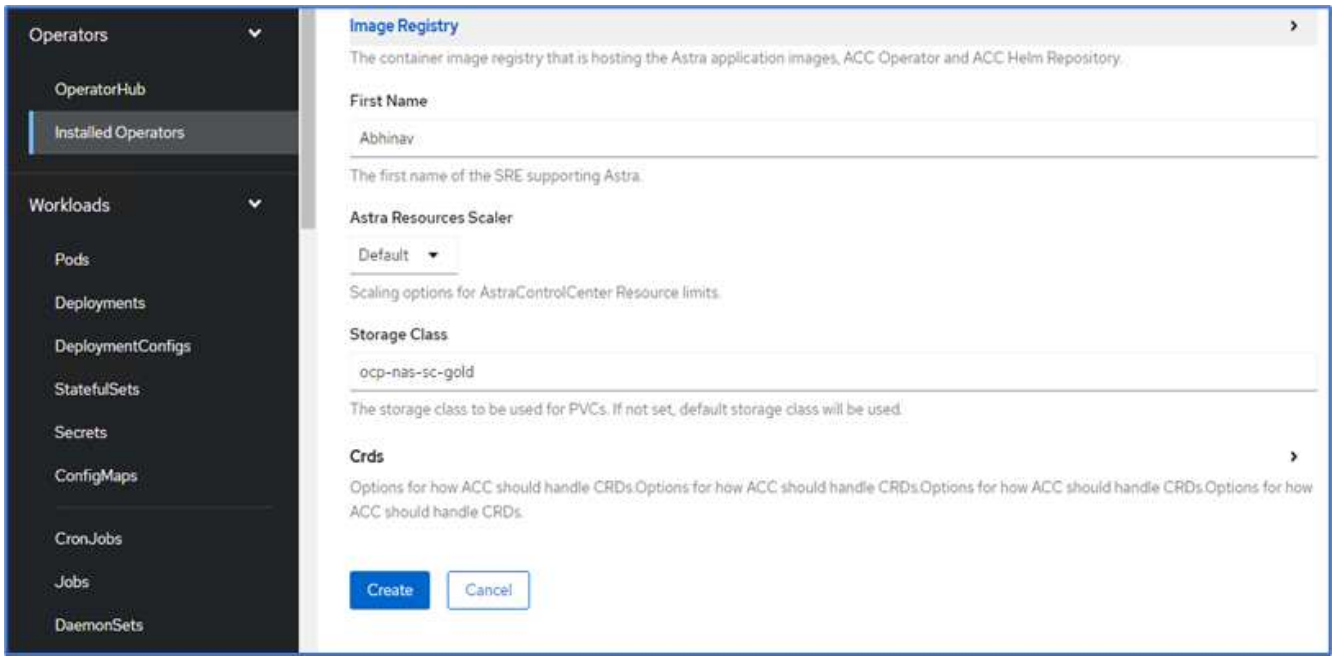
17. Immettere un nome account, un indirizzo e-mail, il cognome dell'amministratore e mantenere la policy di

recupero del volume predefinita. Se si utilizza un bilanciamento del carico, impostare il tipo di ingresso su `AccTraefik`. In caso contrario, selezionare Generico per `Ingress.Controller`. In Image Registry (Registro immagini), immettere il percorso e il segreto del Registro di sistema dell'immagine contenitore.

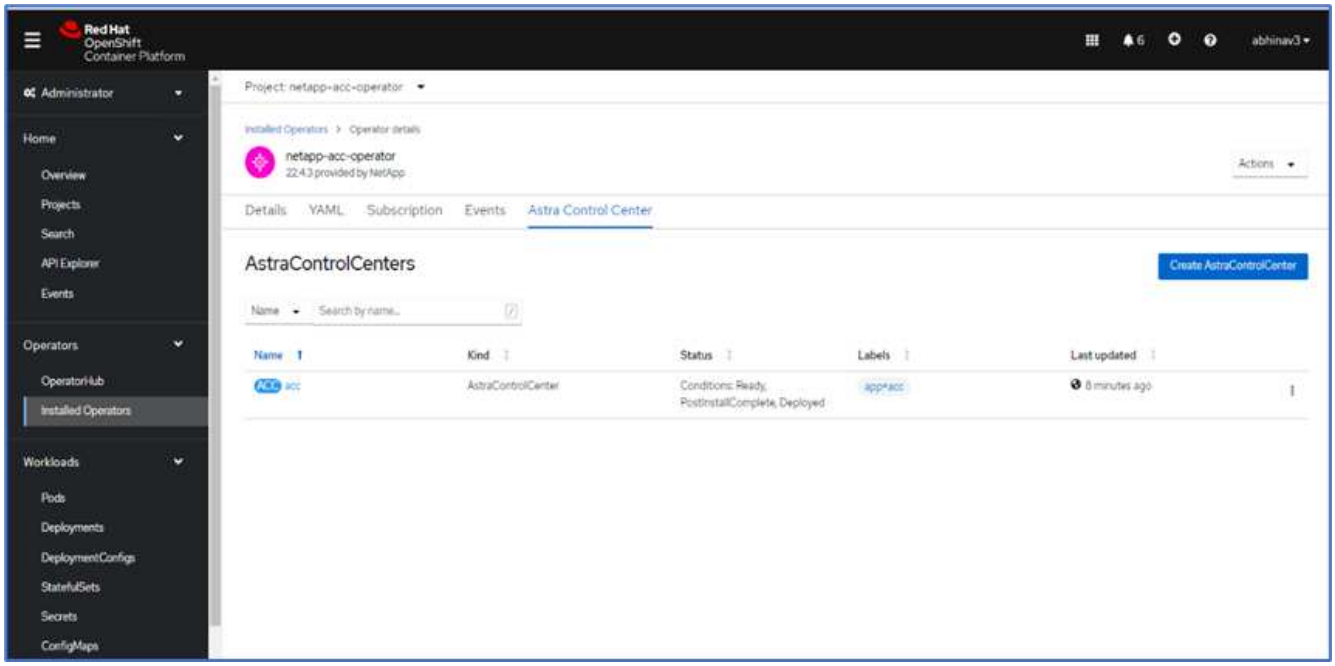


> In questa soluzione viene utilizzato il bilanciamento del carico Metallb. Pertanto, il tipo di ingresso è AccTraefik. Questo espone il gateway traefik di Astra Control Center come un servizio Kubernetes di tipo LoadBalancer.

18. Inserire il nome admin, configurare la scalabilità delle risorse e fornire la classe di storage. Fare clic su Crea.



Lo stato dell'istanza di Astra Control Center deve passare da Deploying (implementazione) a Ready (Pronto).



19. Verificare che tutti i componenti del sistema siano stati installati correttamente e che tutti i pod siano in esecuzione.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                                READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                      1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn    2/2     Running   0
```

```
13m
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
```

```
3m35s
graphql-server-698d6f4bf-kftwc                      1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                           1/1     Running   0
6m27s
influxdb2-0                                         1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                            1/1     Running   0
3m21s
license-594bbdc-rghdg                               1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                           1/1     Running   0
3m17s
loki-0                                              1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                     1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk                2/2     Running   0
3m47s
nats-0                                              1/1     Running   0
10m
nats-1                                              1/1     Running   0
9m43s
nats-2                                              1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                           1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                           1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                            1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                           1/1     Running   0
6m35s
polaris-consul-consul-server-0                      1/1     Running   0
9m22s
polaris-consul-consul-server-1                      1/1     Running   0
9m22s
polaris-consul-consul-server-2                      1/1     Running   0
9m22s
polaris-mongodb-0                                   2/2     Running   0
9m22s
polaris-mongodb-1                                   2/2     Running   0
8m58s
polaris-mongodb-2                                   2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                         1/1     Running   0
```

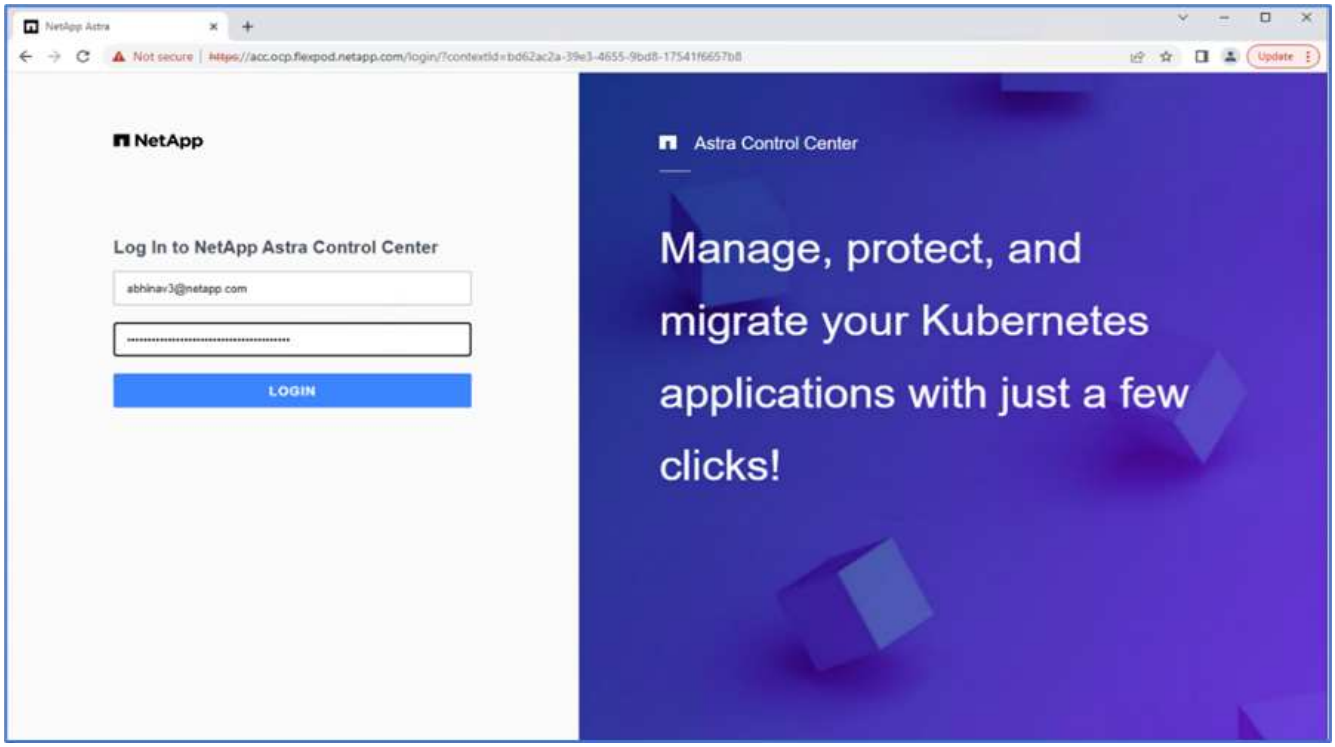
```
3m18s
polaris-vault-0                                     1/1     Running   0
9m18s
polaris-vault-1                                     1/1     Running   0
9m18s
polaris-vault-2                                     1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                     1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j            1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                    1/1     Running   0
5m25s
telegraf-ds-4zqgz                                   1/1     Running   0
3m36s
telegraf-ds-cp9x4                                   1/1     Running   0
3m36s
telegraf-ds-h4n59                                   1/1     Running   0
3m36s
telegraf-ds-jnp2q                                   1/1     Running   0
3m36s
telegraf-ds-pdz5j                                   1/1     Running   0
3m36s
telegraf-ds-znqtp                                   1/1     Running   0
3m36s
telegraf-rs-rt64j                                   1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                  1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                             1/1     Running   0
6m37s
traefik-6548496576-5v2g6                            1/1     Running   0
98s
traefik-6548496576-g82pq                            1/1     Running   0
3m8s
traefik-6548496576-psn49                            1/1     Running   0
38s
traefik-6548496576-qrkfd                            1/1     Running   0
2m53s
traefik-6548496576-srs6r                            1/1     Running   0
98s
trident-svc-679856c67-78kbt                         1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                   1/1     Running   0
7m37s
```

Ogni pod deve avere lo stato di esecuzione. L'implementazione dei pod di sistema potrebbe richiedere alcuni minuti.

20. Quando tutti i pod sono in esecuzione, eseguire il seguente comando per recuperare la password monouso. Nella versione YAML dell'output, selezionare `status.deploymentState` per il valore implementato, quindi copiare `status.uuid` valore. La password è `ACC-` Seguito dal valore UUID. (ACC-[UUID]).

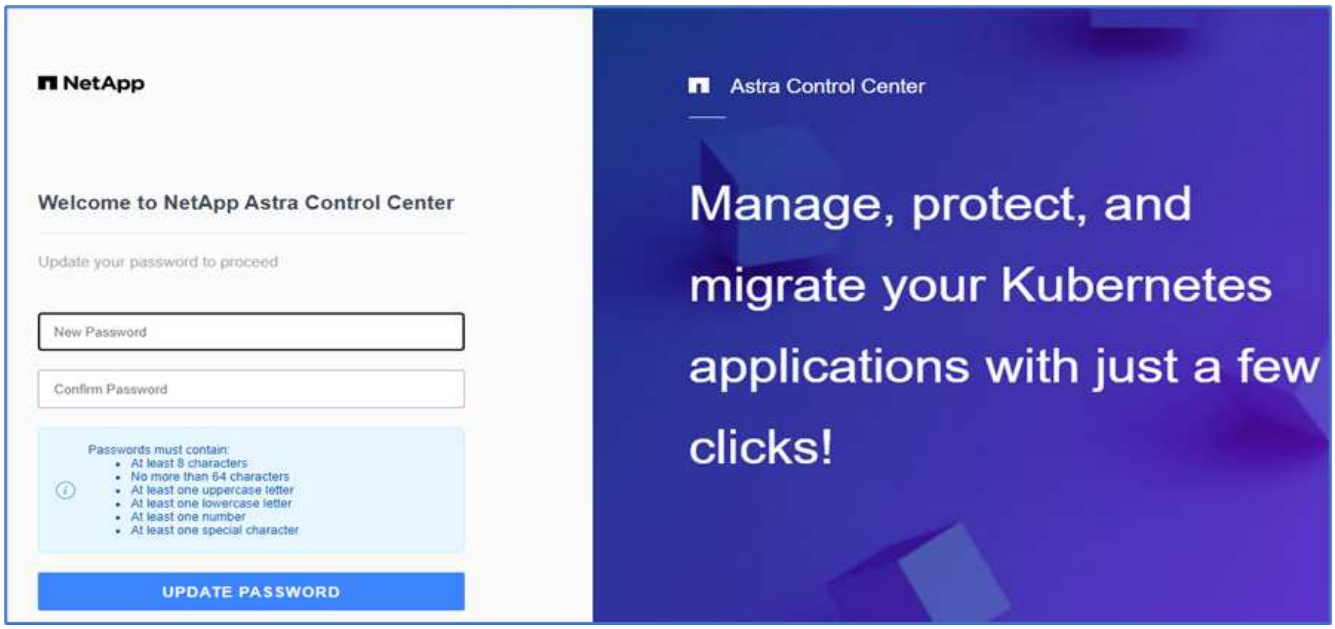
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. In un browser, accedere all'URL utilizzando l'FQDN fornito.
22. Effettuare l'accesso utilizzando il nome utente predefinito, ovvero l'indirizzo e-mail fornito durante l'installazione e la password monouso ACC-[UUID].



Se si immette una password errata per tre volte, l'account amministratore viene bloccato per 15 minuti.

23. Modificare la password e procedere.

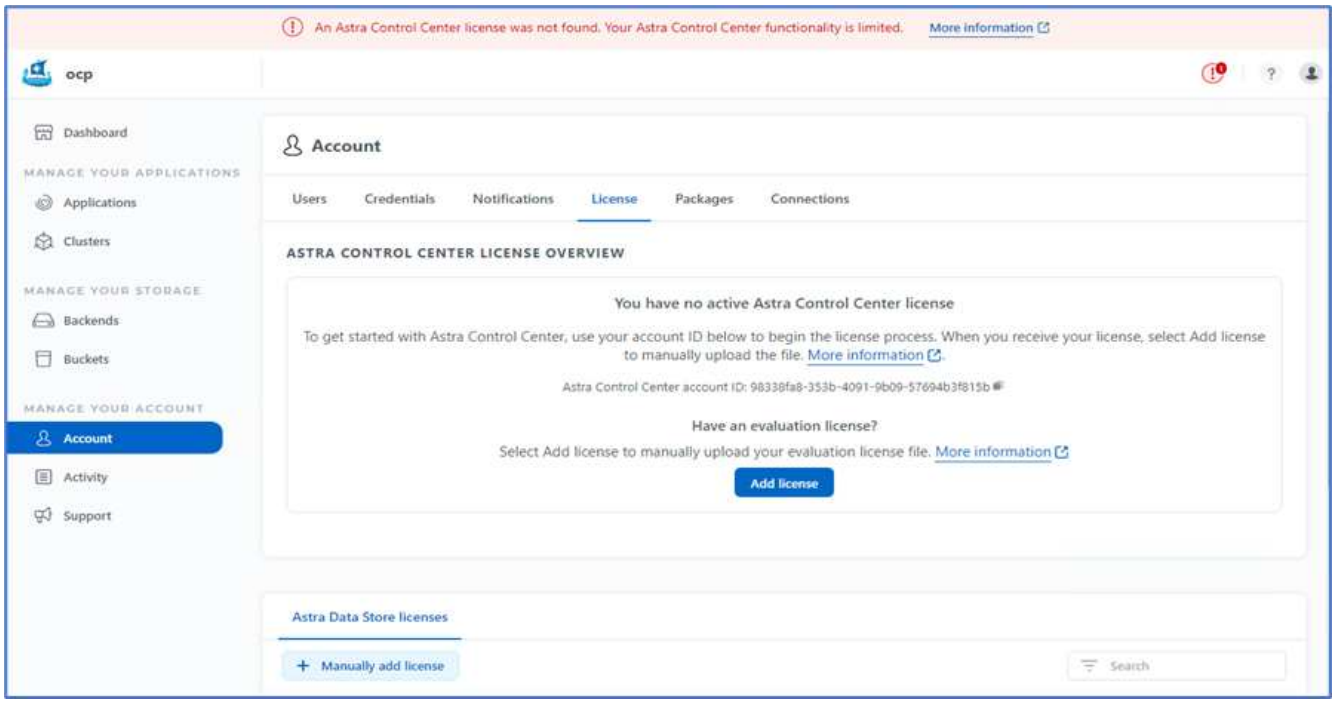


Per ulteriori informazioni sull'installazione di Astra Control Center, consultare "Panoramica dell'installazione di Astra Control Center" pagina.

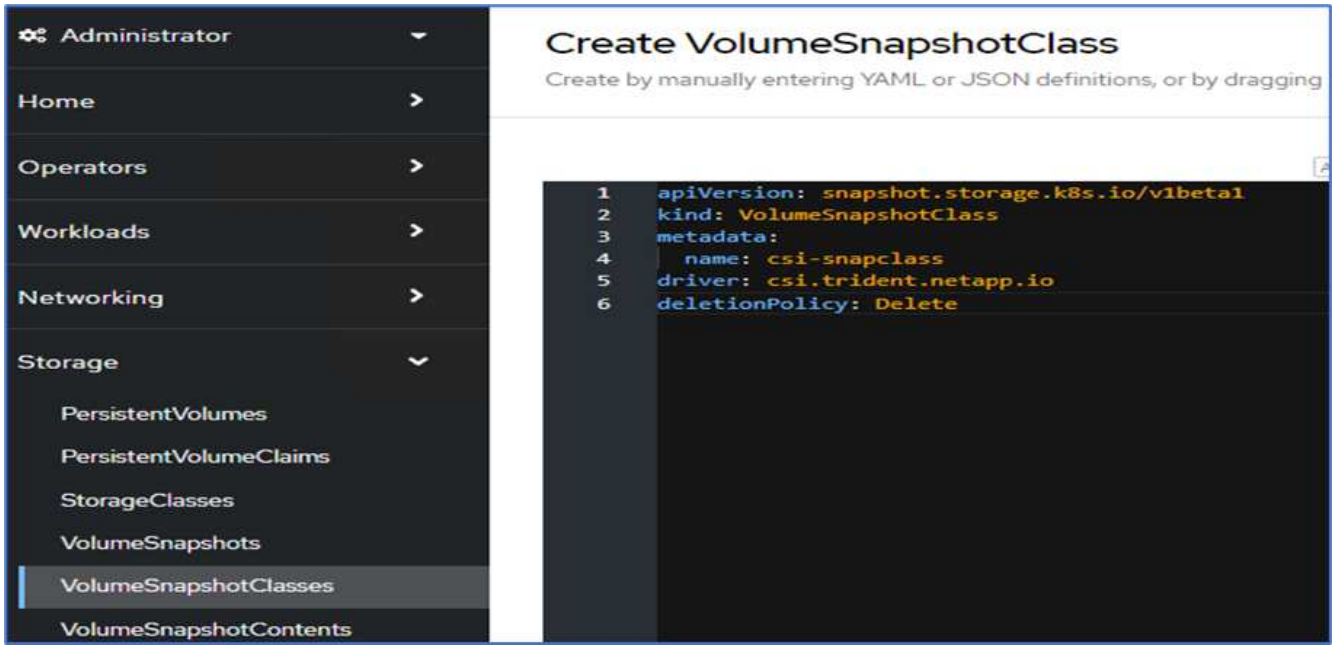
Configurare Astra Control Center

Dopo aver installato Astra Control Center, accedere all'interfaccia utente, caricare la licenza, aggiungere cluster, gestire lo storage e aggiungere bucket.

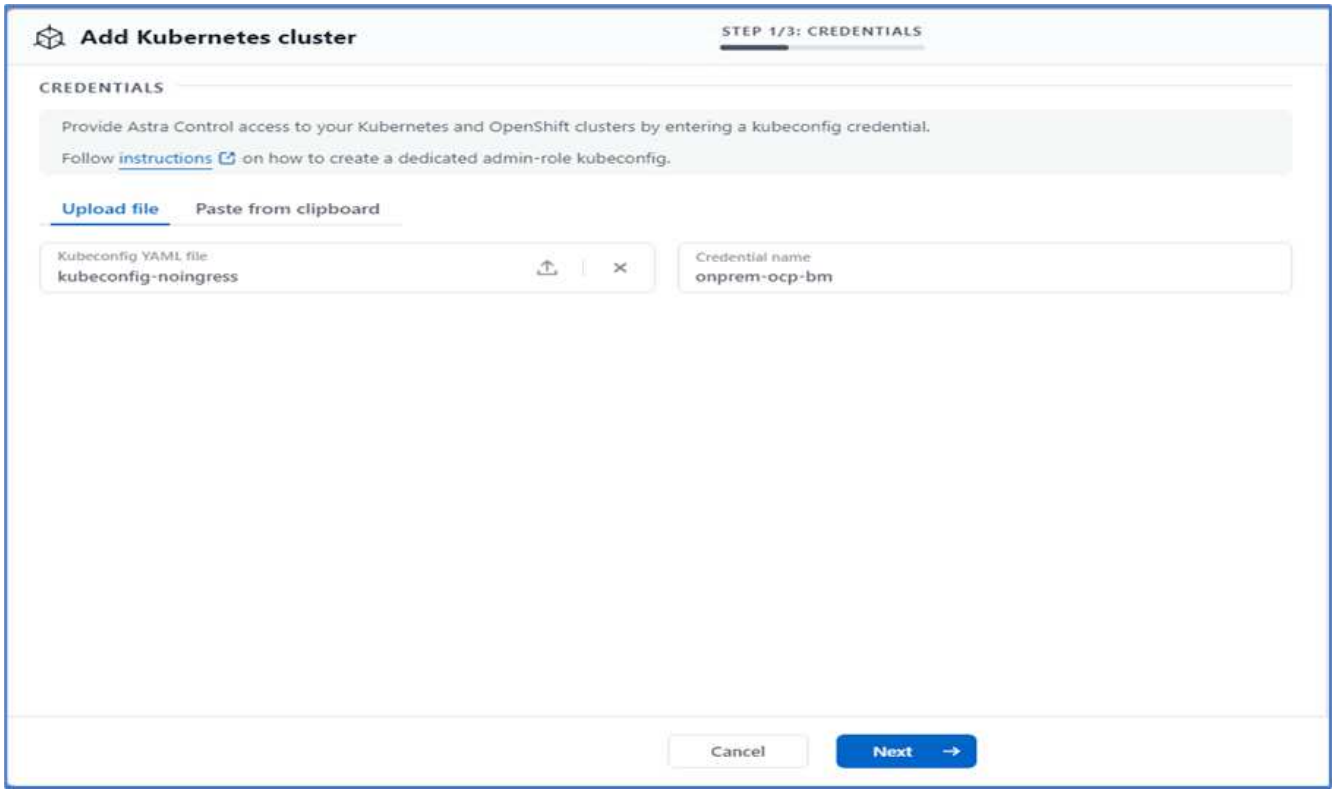
1. Nella home page, sotto account, andare alla scheda License (licenza) e selezionare Add License (Aggiungi licenza) per caricare la licenza Astra.



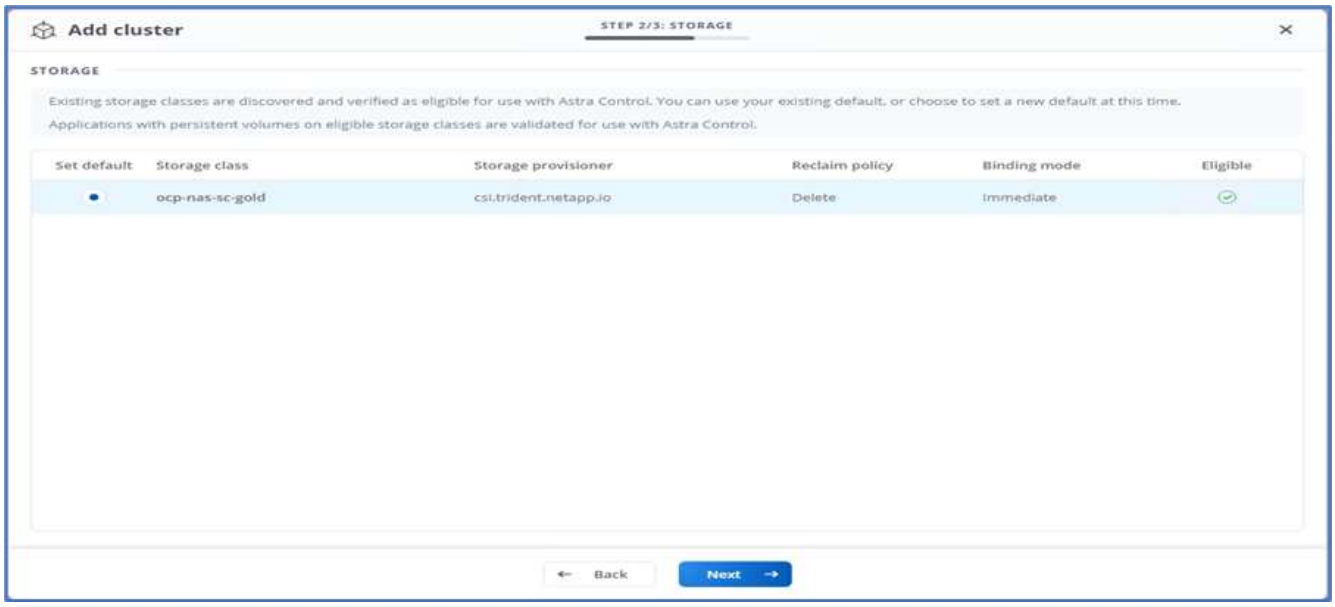
2. Prima di aggiungere il cluster OpenShift, creare una classe di snapshot Astra Trident Volume dalla console Web OpenShift. La classe Volume snapshot viene configurata con `csi.trident.netapp.io` driver.



3. Per aggiungere il cluster Kubernetes, accedere a Clusters nella home page e fare clic su Add Kubernetes Cluster (Aggiungi cluster Kubernetes). Quindi caricare `kubeconfig` per il cluster e fornire un nome di credenziale. Fare clic su Avanti.



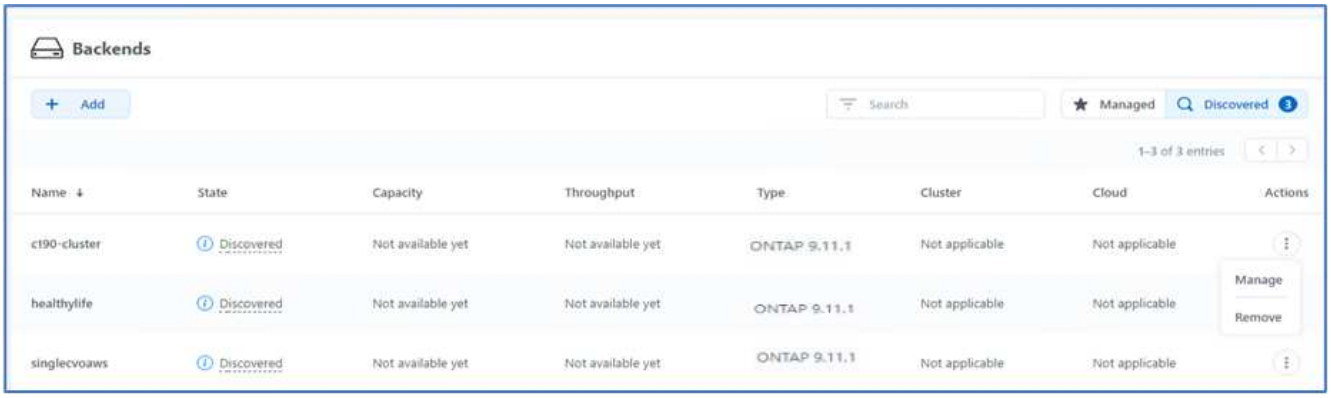
4. Le classi di storage esistenti vengono rilevate automaticamente. Selezionare la classe di storage predefinita, fare clic su Next (Avanti), quindi su Add cluster (Aggiungi cluster).



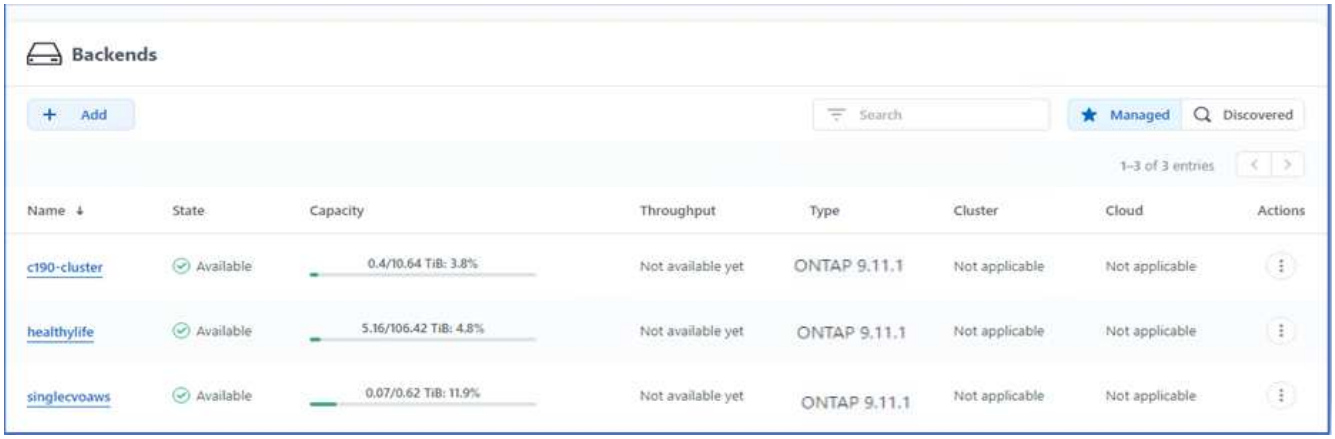
5. Il cluster viene aggiunto in pochi minuti. Per aggiungere altri cluster OpenShift Container Platform, ripetere i passaggi 1–4.

> Per aggiungere un ambiente operativo OpenShift aggiuntivo come risorsa di calcolo gestita, assicurarsi che Astra Trident "Oggetti VolumeSnapshotClass" sono definiti.

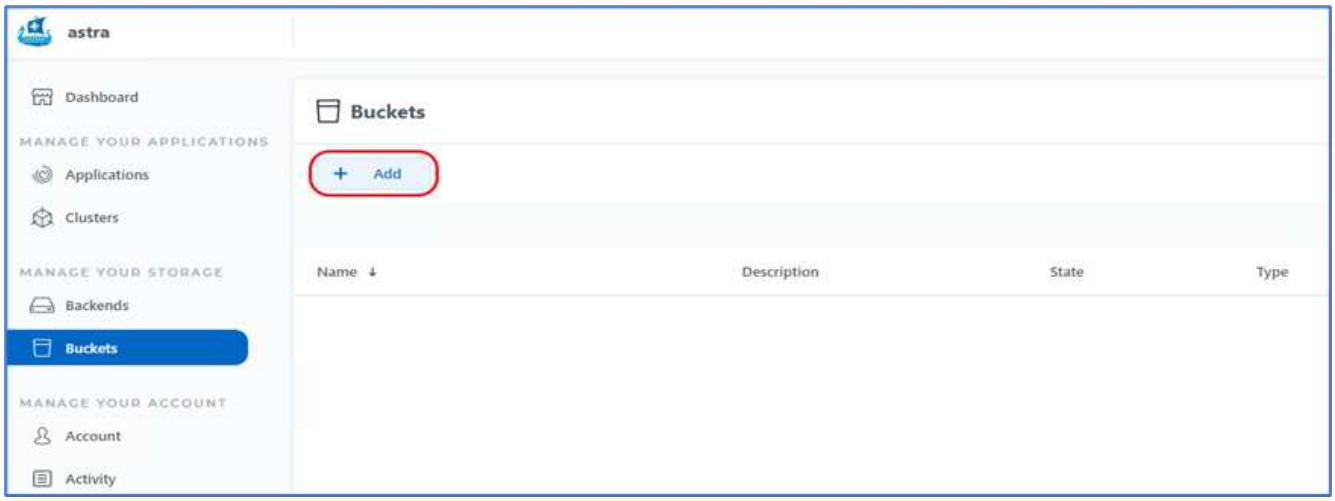
6. Per gestire lo storage, accedere a Backend, fare clic sui tre punti in azioni rispetto al backend che si desidera gestire. Fare clic su Gestisci.



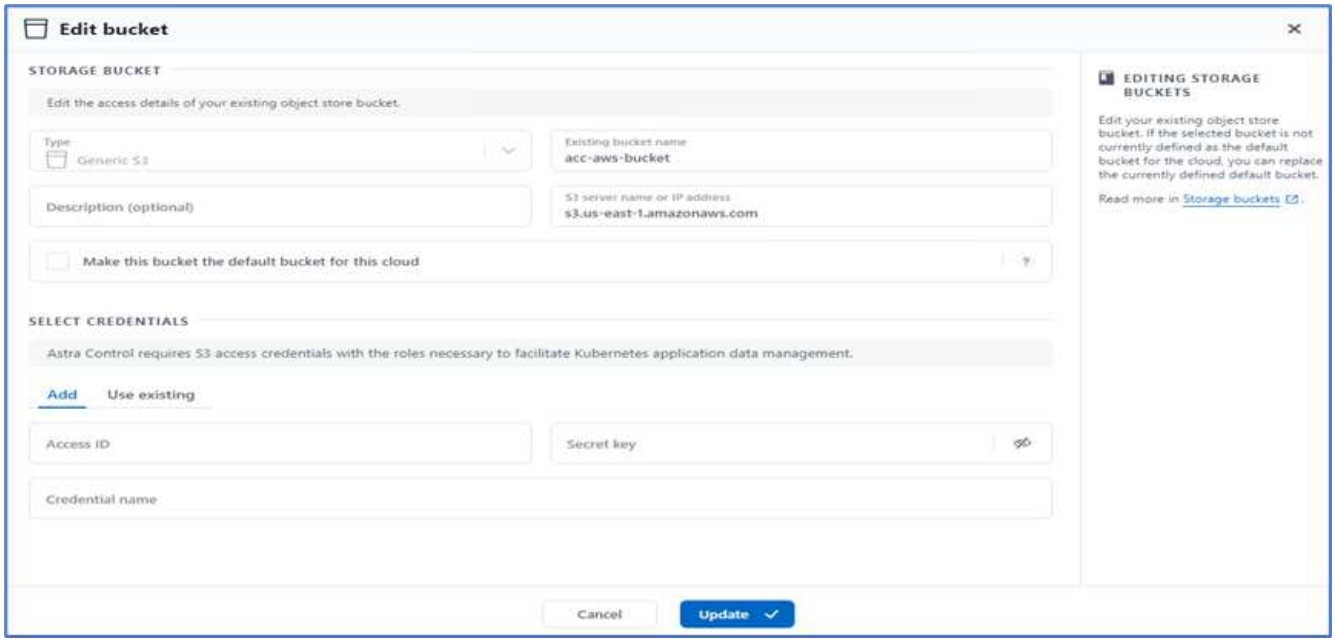
7. Fornire le credenziali ONTAP e fare clic su Avanti. Esaminare le informazioni e fare clic su Managed (gestito). I backend dovrebbero essere simili all'esempio seguente.



8. Per aggiungere un bucket ad Astra Control, selezionare Bucket e fare clic su Add (Aggiungi).

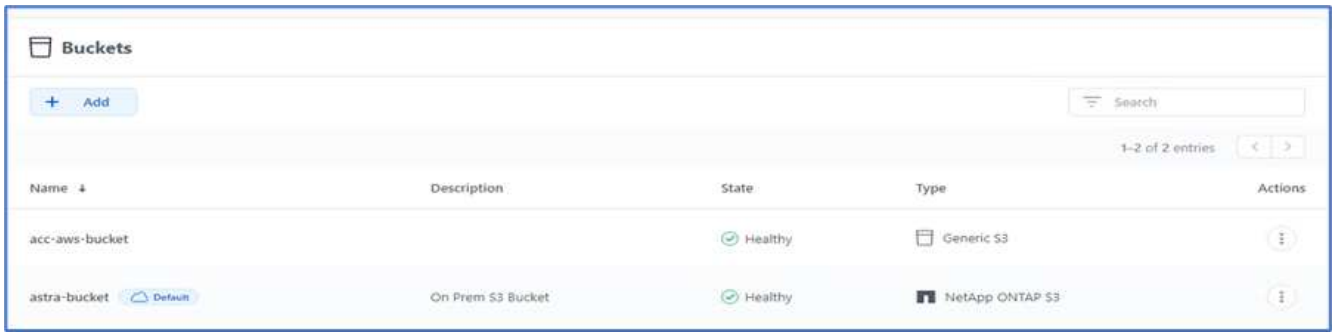


9. Selezionare il tipo di bucket e fornire il nome del bucket, il nome del server S3 o l'indirizzo IP e la credenziale S3. Fare clic su Aggiorna.



In questa soluzione vengono utilizzati entrambi i bucket AWS S3 e ONTAP S3. È anche possibile utilizzare StorageGRID.

Lo stato del bucket deve essere integro.



Come parte della registrazione del cluster Kubernetes con Astra Control Center per la gestione dei dati applicativa, Astra Control crea automaticamente associazioni di ruoli e uno spazio dei nomi di monitoraggio NetApp per raccogliere metriche e log dai pod di applicazioni e dai nodi di lavoro. Impostare una delle classi di storage basate su ONTAP supportate come predefinita.

Dopo di lei "Aggiungere un cluster alla gestione di Astra Control", È possibile installare le applicazioni sul cluster (al di fuori di Astra Control) e quindi andare alla pagina Apps (applicazioni) in Astra Control per gestire le applicazioni e le relative risorse. Per ulteriori informazioni sulla gestione delle applicazioni con Astra, consultare "Requisiti di gestione delle applicazioni".

"Pagina successiva: Panoramica sulla convalida della soluzione."

Convalida della soluzione

Panoramica

"Precedente: Installazione di Astra Control Center su OpenShift Container Platform."

In questa sezione, rivisudiamo la soluzione con alcuni casi di utilizzo:

- Ripristino di un'applicazione stateful da un backup remoto a un altro cluster OpenShift in esecuzione nel cloud.
- Ripristino di un'applicazione stateful nello stesso namespace nel cluster OpenShift.
- Mobilità applicativa mediante cloning da un sistema FlexPod (piattaforma container OpenShift Bare Metal) a un altro sistema FlexPod (piattaforma container OpenShift su VMware).

In particolare, in questa soluzione vengono validati solo pochi casi di utilizzo. Questa convalida non rappresenta in alcun modo l'intera funzionalità di Astra Control Center.

"Successivo: Ripristino delle applicazioni con backup remoti."

Recovery dell'applicazione con backup remoti

"Precedente: Panoramica sulla convalida della soluzione."

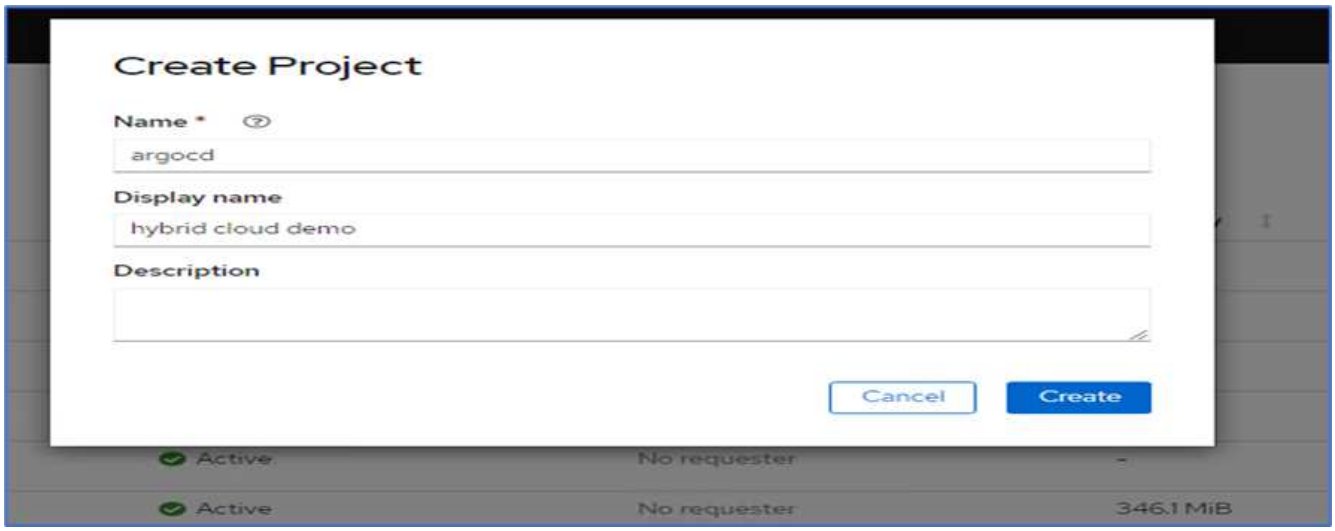
Con Astra, puoi eseguire un backup completo coerente con l'applicazione che può

essere utilizzato per ripristinare l'applicazione con i suoi dati in un cluster Kubernetes diverso in esecuzione in un data center on-premise o in un cloud pubblico.

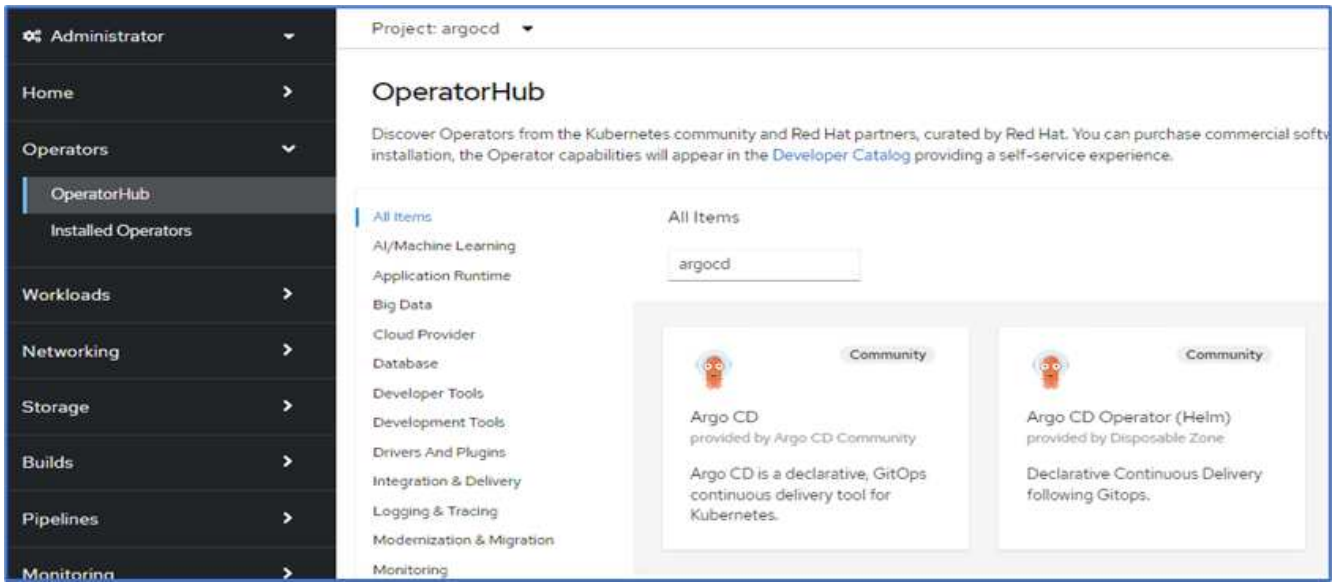
Per convalidare un ripristino dell'applicazione di successo, simulare un errore on-premise di un'applicazione in esecuzione sul sistema FlexPod e ripristinare l'applicazione su un cluster K8s in esecuzione nel cloud utilizzando un backup remoto.

L'applicazione di esempio è un'applicazione di listino prezzi che utilizza MySQL per il database. Per automatizzare l'implementazione, abbiamo utilizzato "CD Argo" tool. Argo CD è uno strumento dichiarativo, GitOps, per la consegna continua di Kubernetes.

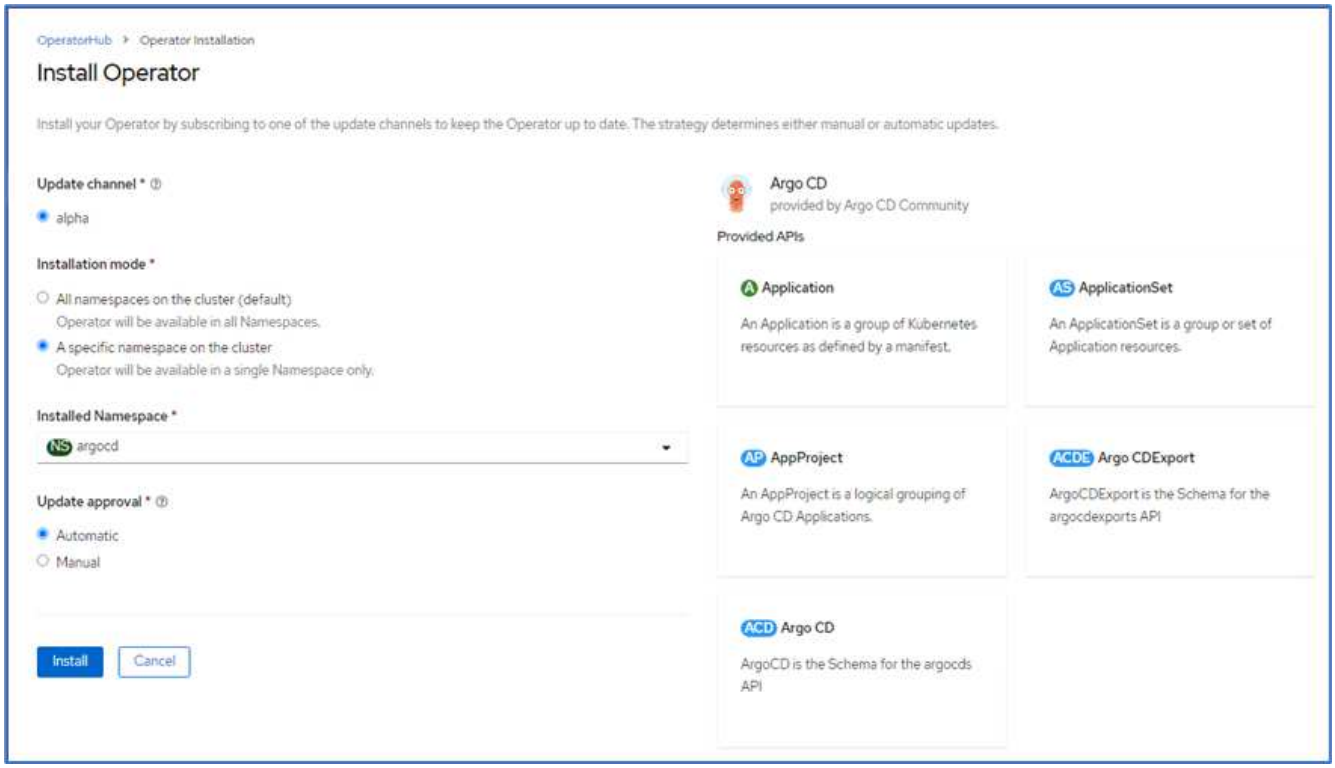
1. Accedi al cluster OpenShift on-premise e crea un nuovo progetto con il nome `argocd`.



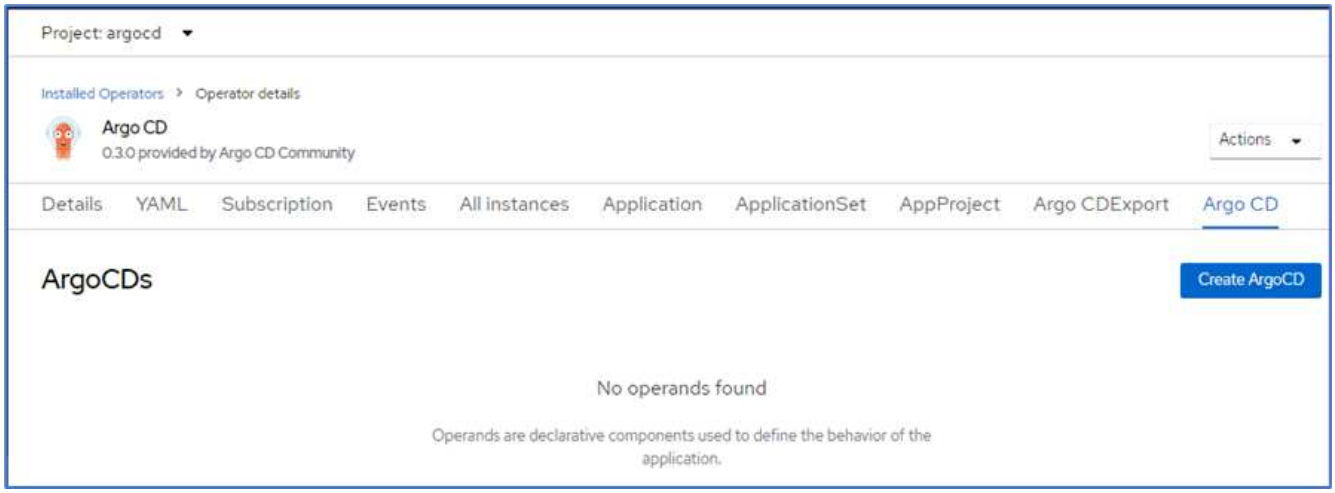
2. In OperatorHub, cercare `argocd` E selezionare Argo CD operator.



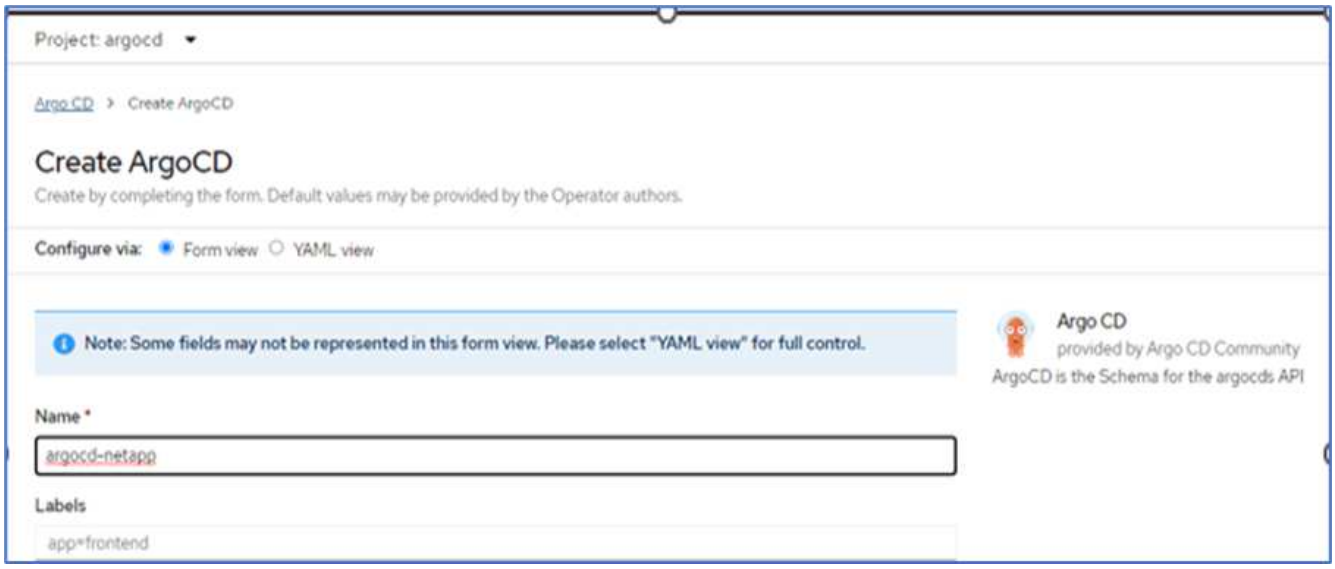
3. Installare l'operatore in `argocd` namespace.



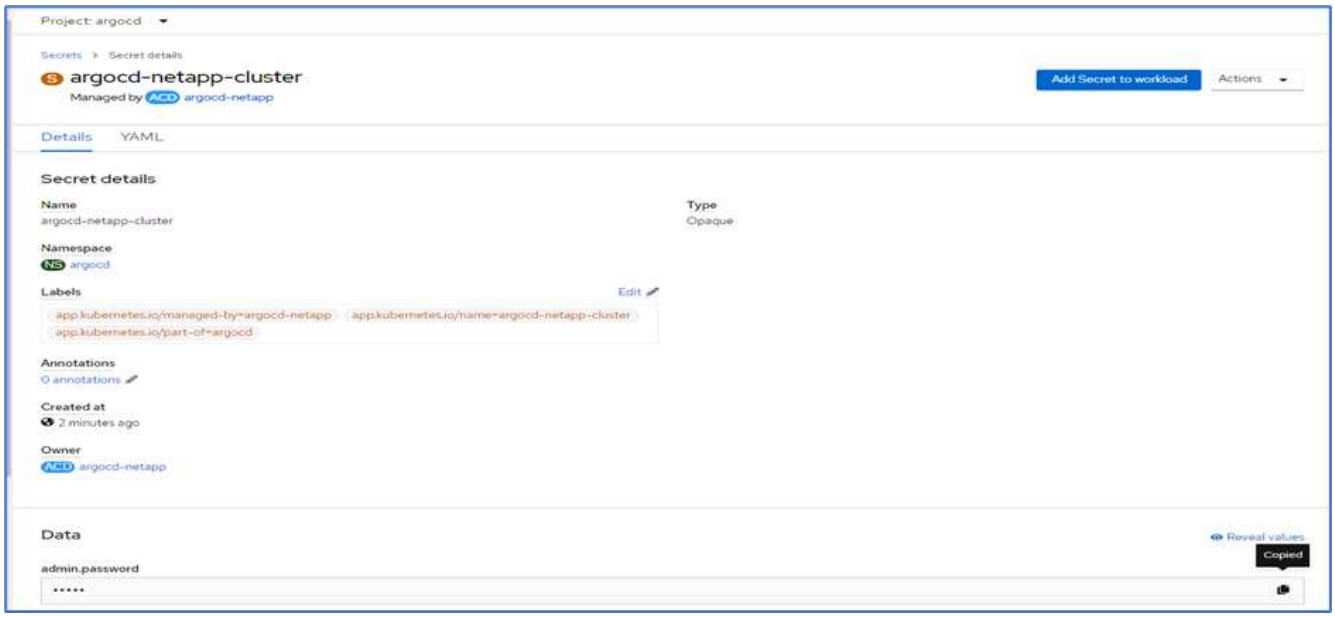
4. Accedere all'operatore e fare clic su Create ArgoCD (Crea ArgoCD).



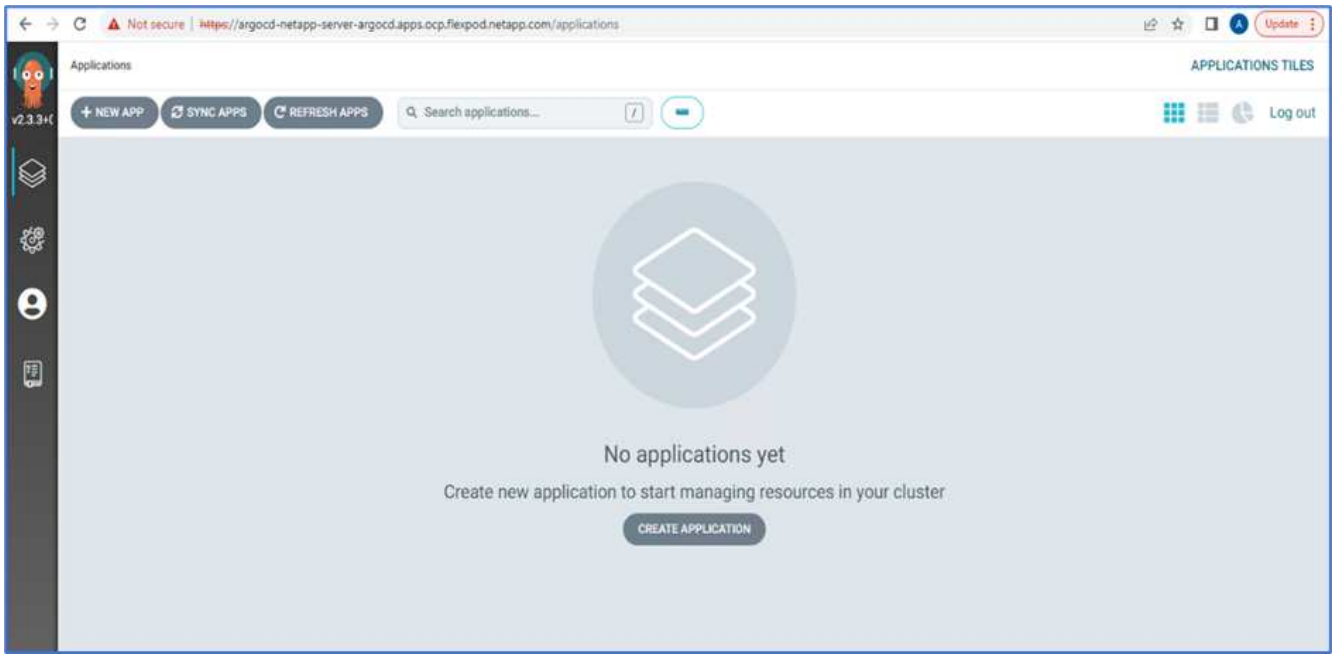
5. Per distribuire l'istanza del CD Argo in `argocd` Assegnare un nome e fare clic su Create (Crea).



6. Per accedere a Argo CD, l'utente predefinito è admin e la password si trova in un file segreto con il nome `argocd-netapp-cluster`.



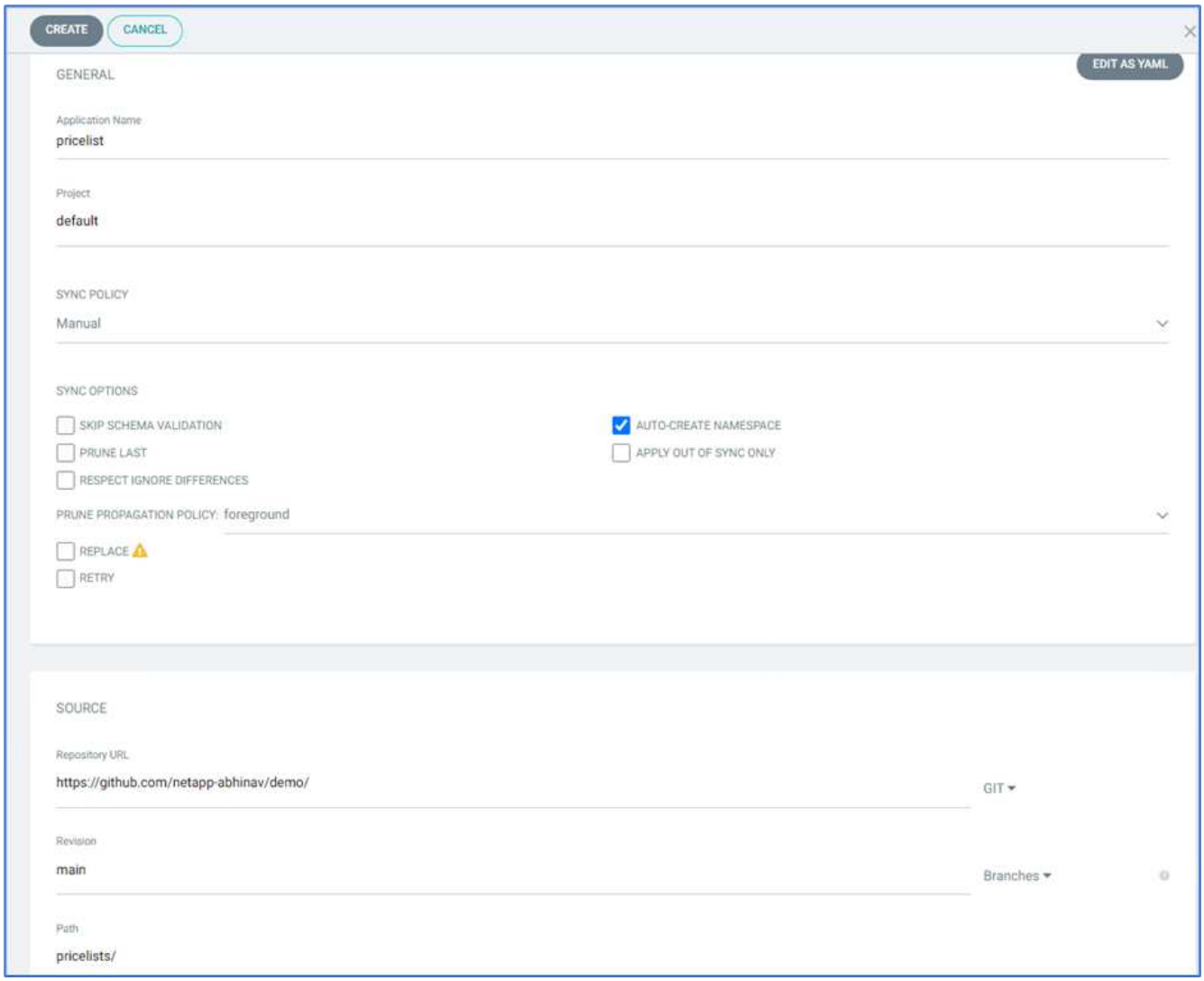
7. Dal menu laterale, selezionare routes > Location (percorsi > Località) e fare clic sull'URL del `argocd` percorsi. Immettere il nome utente e la password.



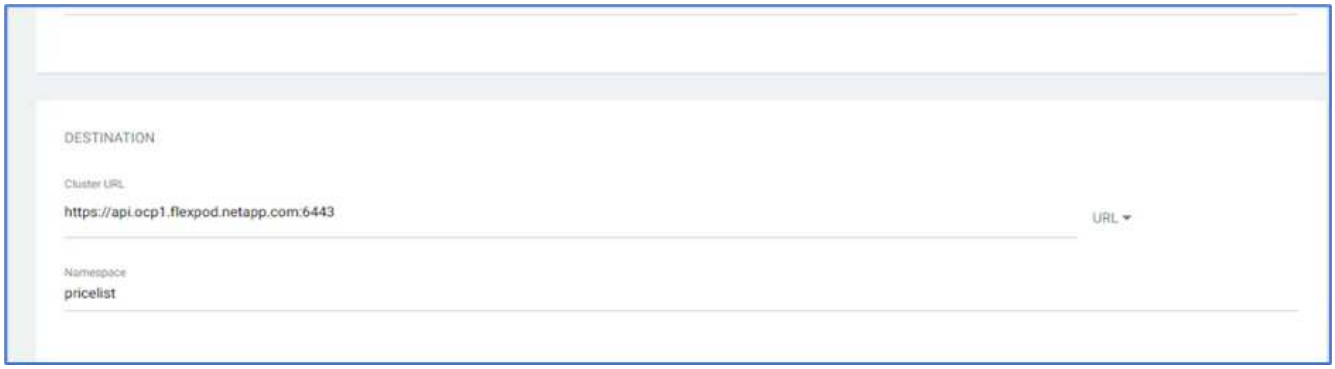
8. Aggiungere il cluster OpenShift on-premise al CD Argo attraverso la CLI.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

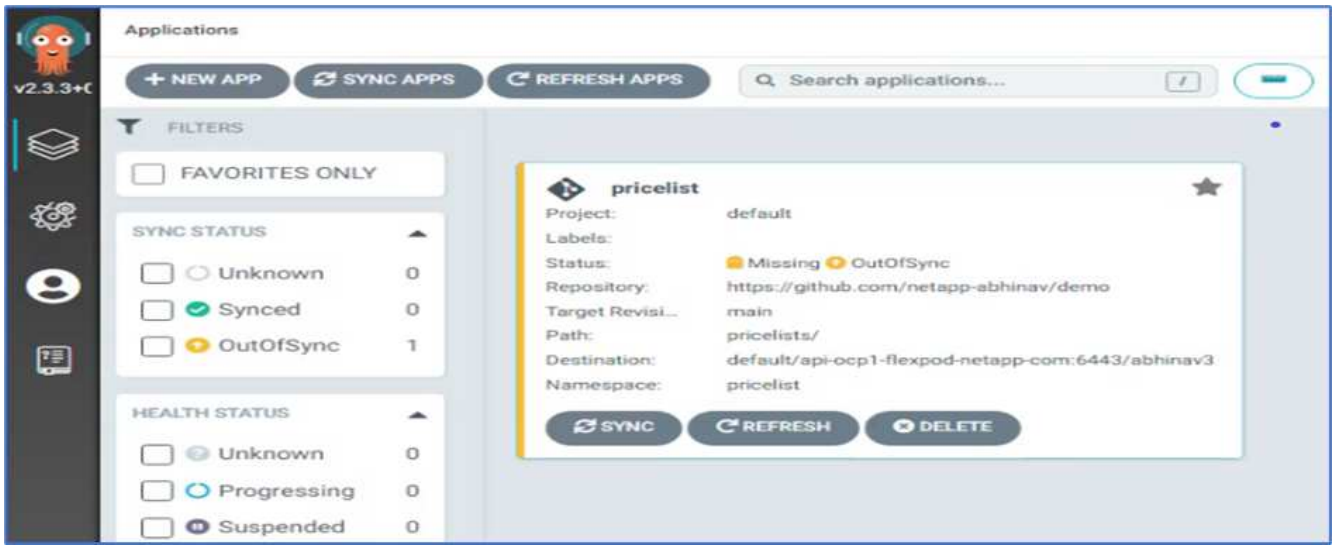
9. Nell’interfaccia utente di ArgoCD, fare clic SU NEW APP (NUOVA APPLICAZIONE) e immettere i dettagli relativi al nome dell’applicazione e al repository di codice.



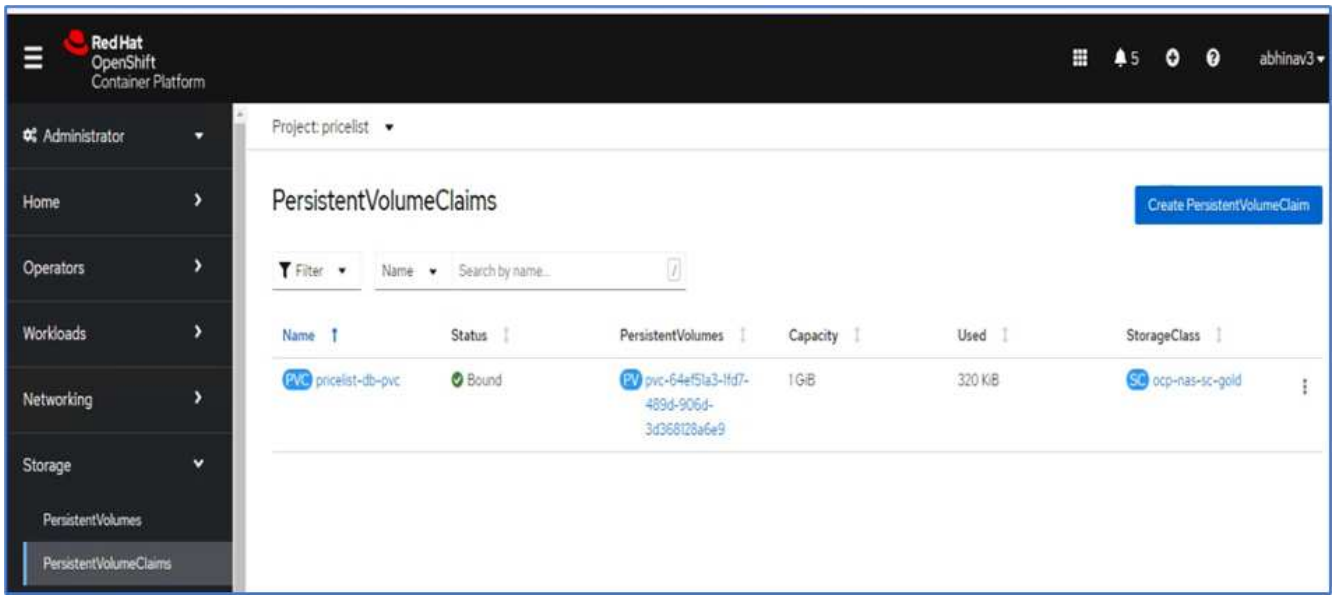
10. Inserire il cluster OpenShift in cui l’applicazione verrà implementata insieme allo spazio dei nomi.



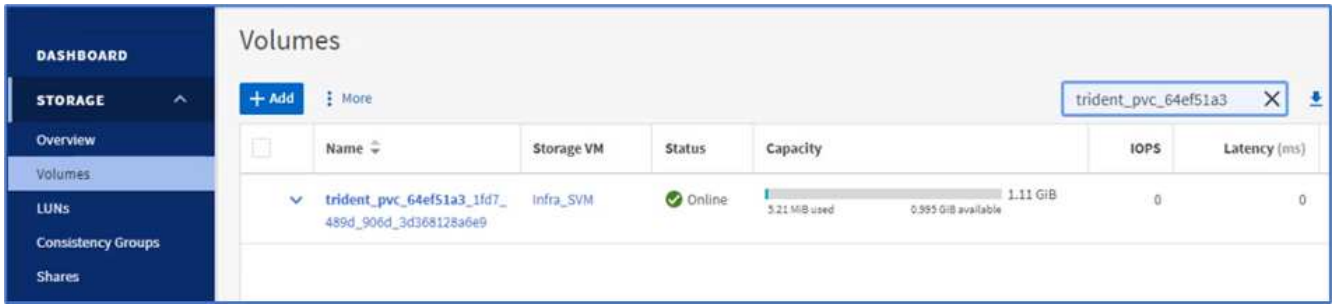
11. Per implementare l’applicazione sul cluster OpenShift on-premise, fare clic su SYNC.



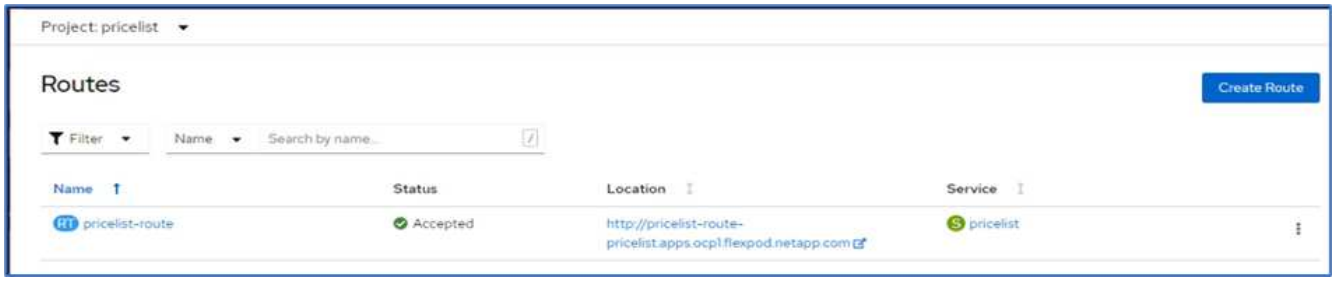
12. Nella console di OpenShift Container Platform, accedere a Preventivo progetto e, in Storage, verificare il nome e le dimensioni del PVC.



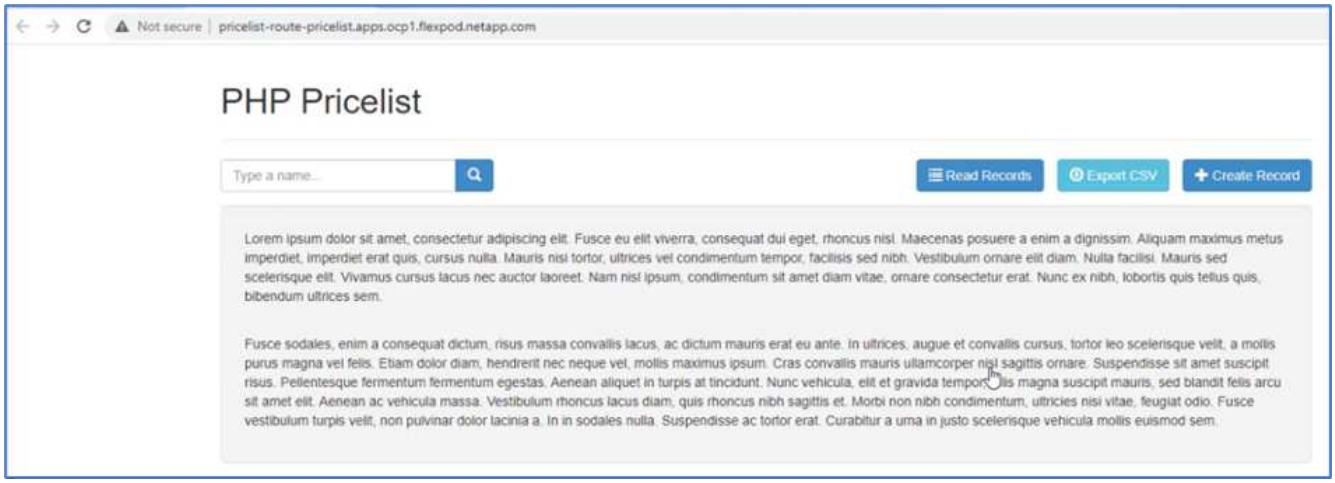
13. Accedere a System Manager e verificare il PVC.



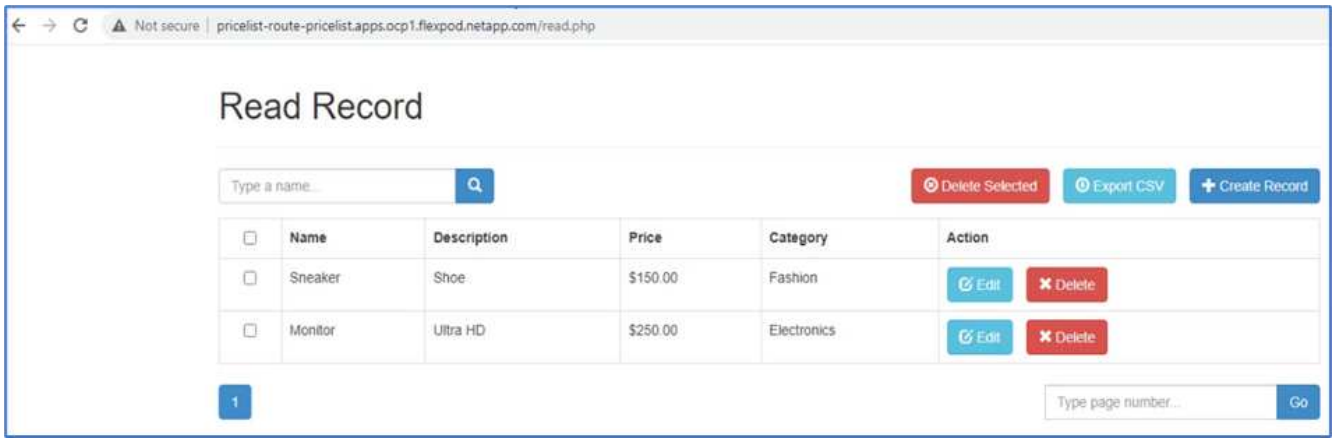
14. Una volta eseguiti i pod, selezionare rete > percorsi dal menu laterale, quindi fare clic sull'URL in posizione.



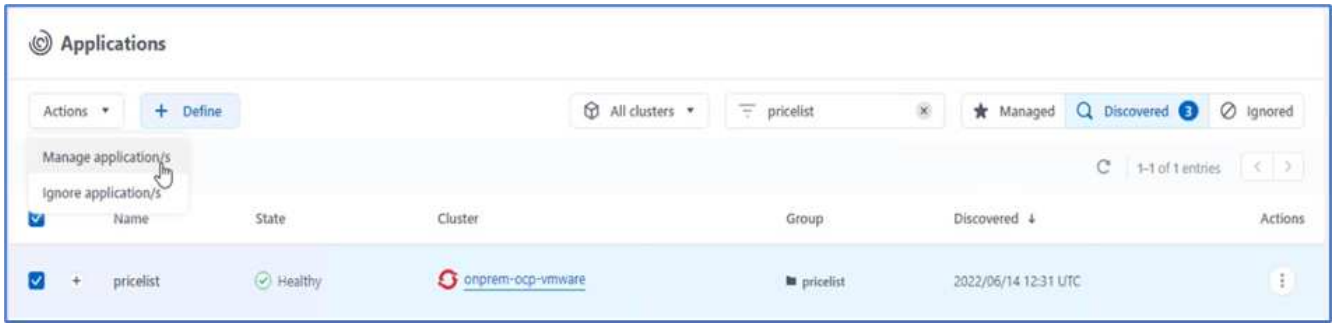
15. Viene visualizzata la pagina iniziale dell'applicazione Pricelist.



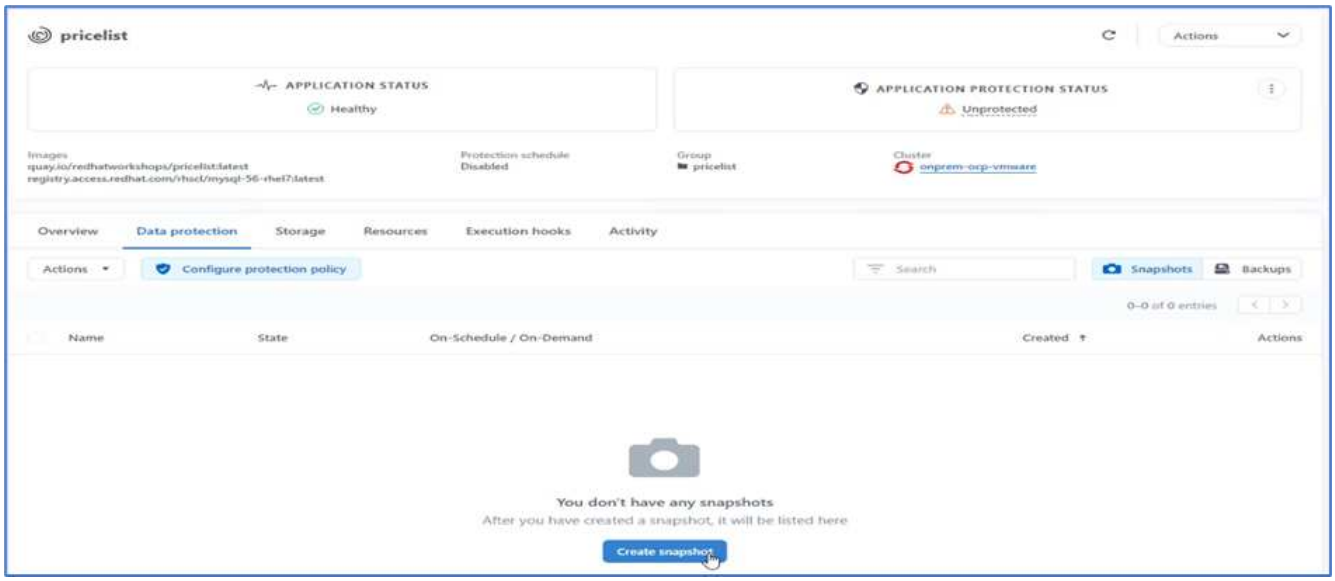
16. Creare alcuni record nella pagina Web.



17. L'applicazione viene scoperta in Astra Control Center. Per gestire l'applicazione, accedere ad applicazioni > rilevate, selezionare l'applicazione Listino prezzi e fare clic su Gestisci applicazioni in azioni.

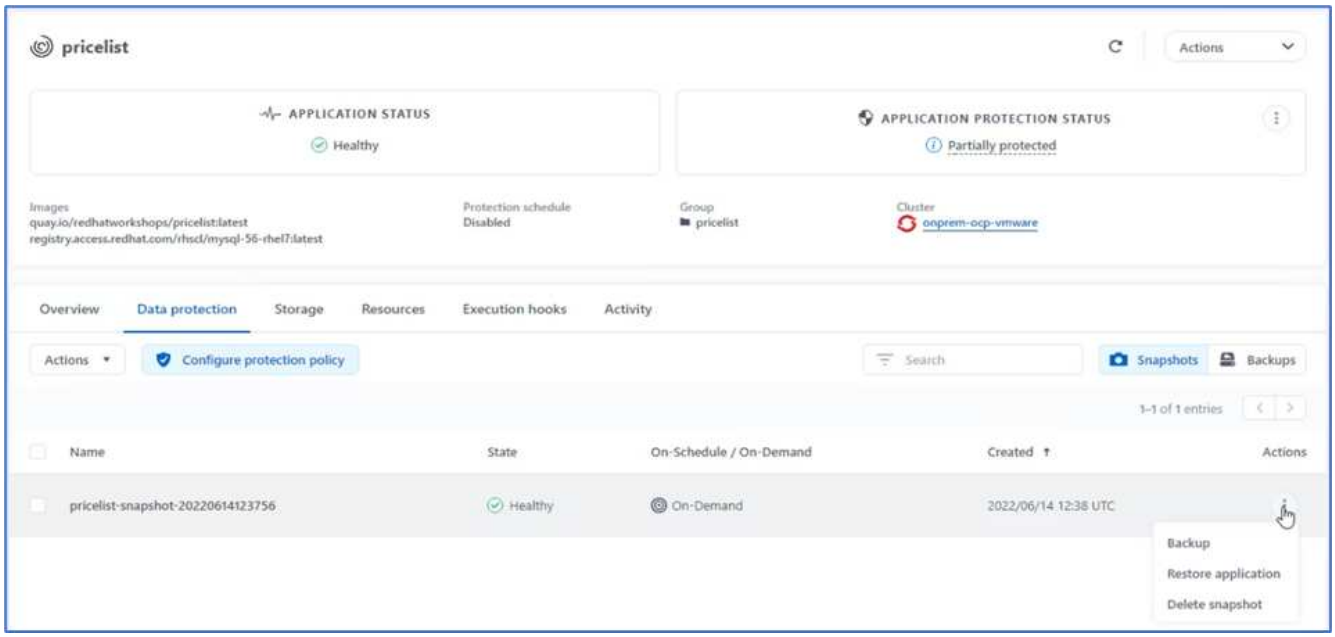


18. Fare clic sull'applicazione Listino prezzi e selezionare Data Protection (protezione dati). A questo punto, non dovrebbero esserci snapshot o backup. Fare clic su Create Snapshot (Crea istantanea) per creare un'istantanea on-demand.

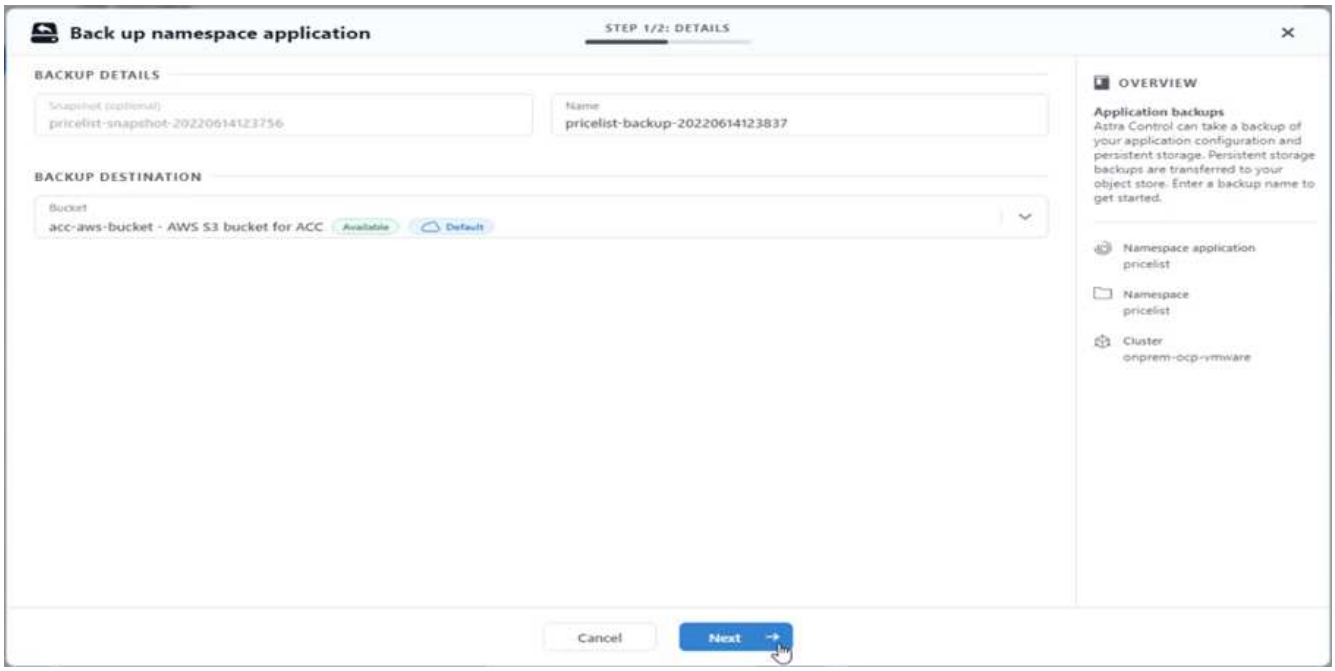


NetApp Astra Control Center supporta backup e snapshot on-demand e pianificati.

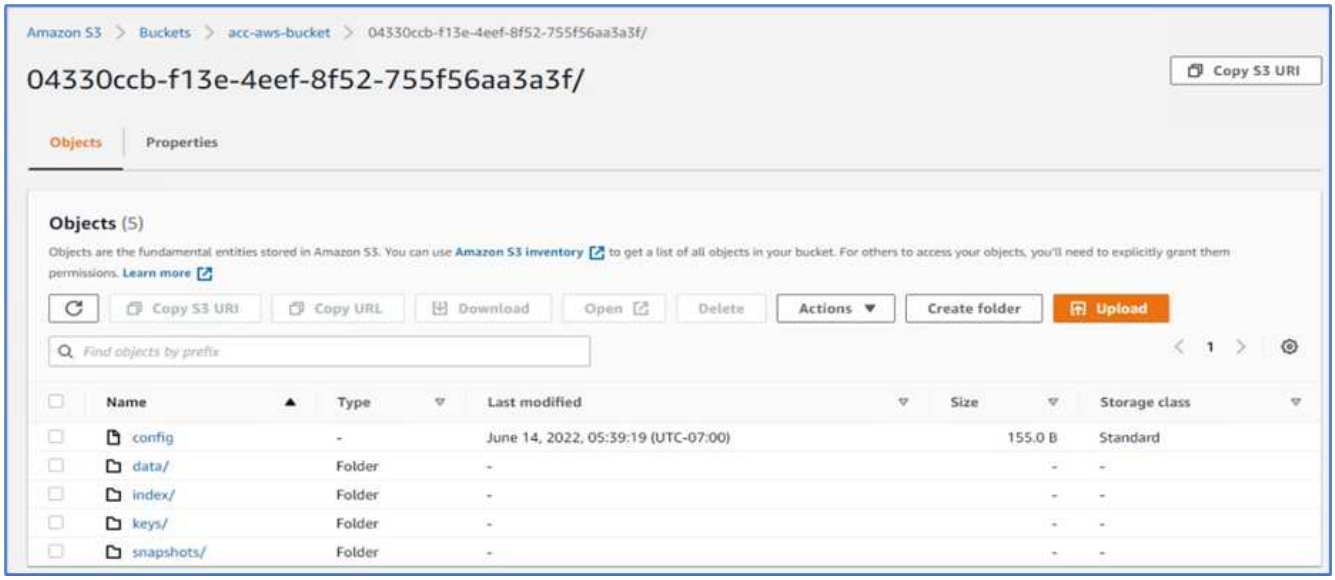
19. Una volta creata la snapshot e lo stato è integro, creare un backup remoto utilizzando tale snapshot. Questo backup viene memorizzato nel bucket S3.



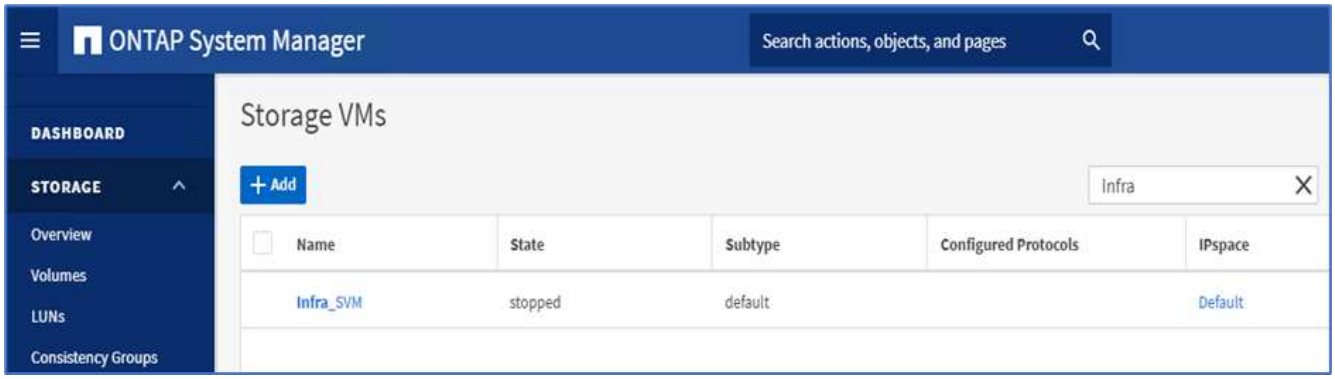
20. Selezionare il bucket AWS S3 e avviare l'operazione di backup.



21. L'operazione di backup deve creare una cartella con più oggetti nel bucket AWS S3.



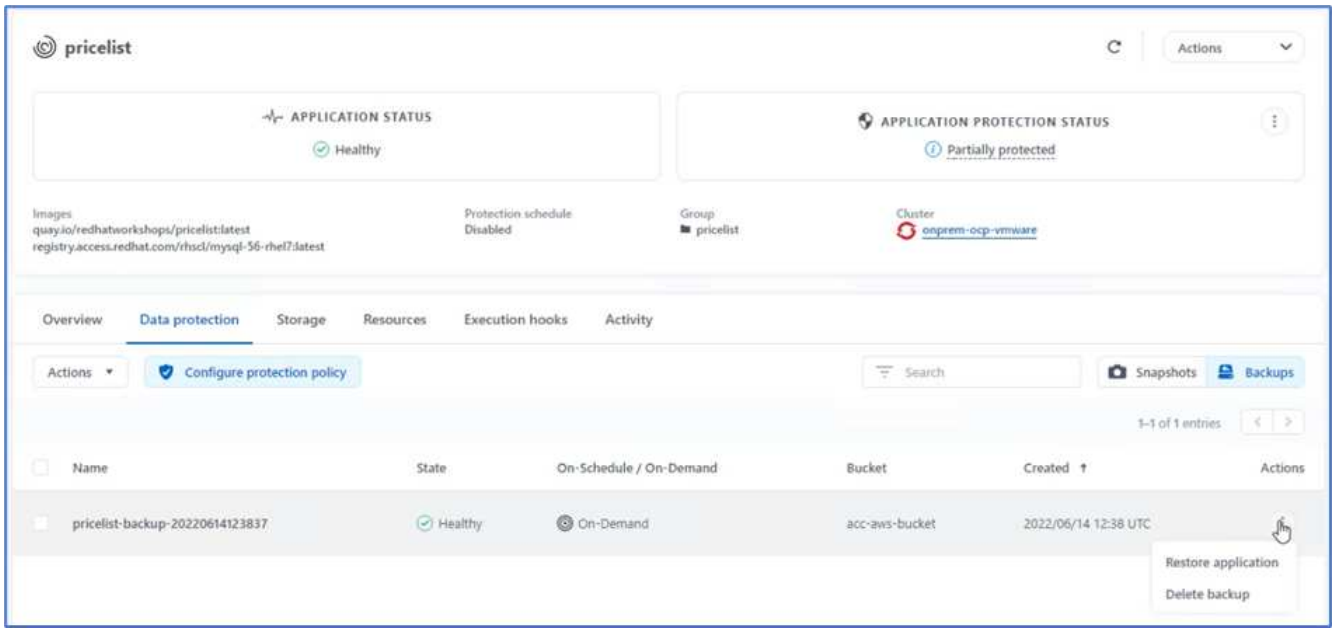
22. Una volta completato il backup remoto, simulare un disastro on-premise arrestando la storage virtual machine (SVM) che ospita il volume di backup per il PV.



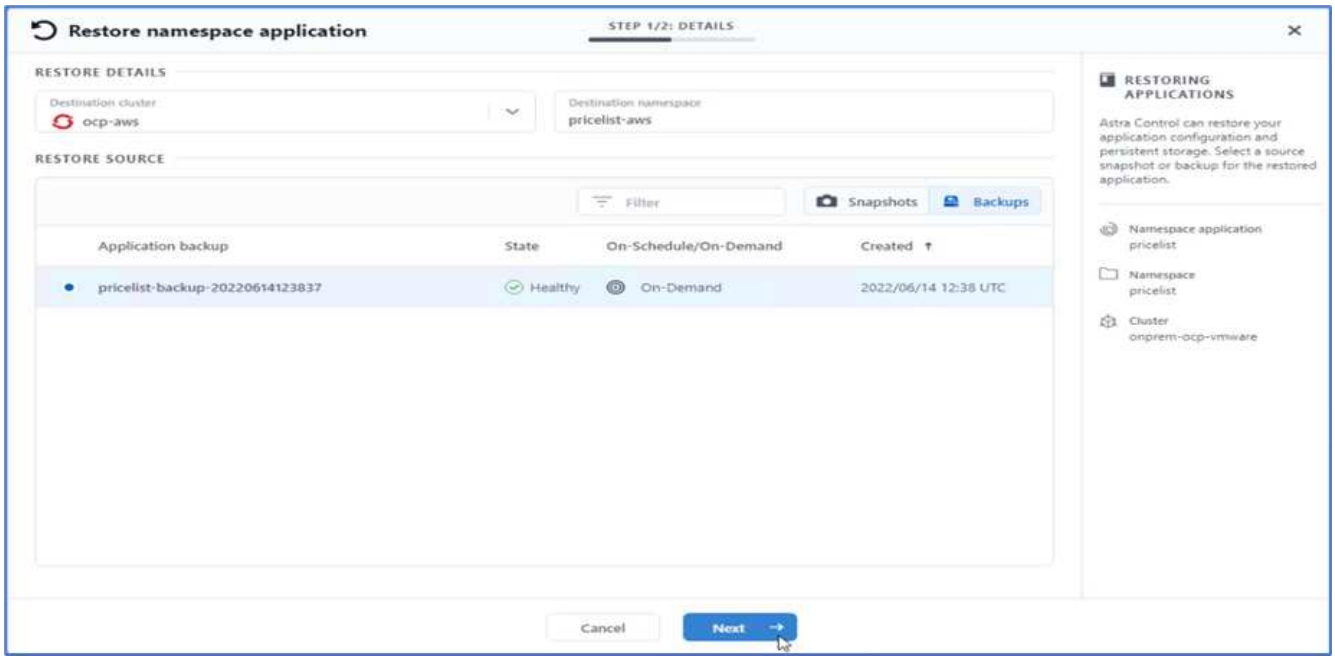
23. Aggiornare la pagina Web per confermare l'interruzione. La pagina web non è disponibile.

Come previsto, il sito Web non è disponibile, quindi ripristiniamo rapidamente l'applicazione dal backup remoto utilizzando Astra al cluster OpenShift in esecuzione in AWS.

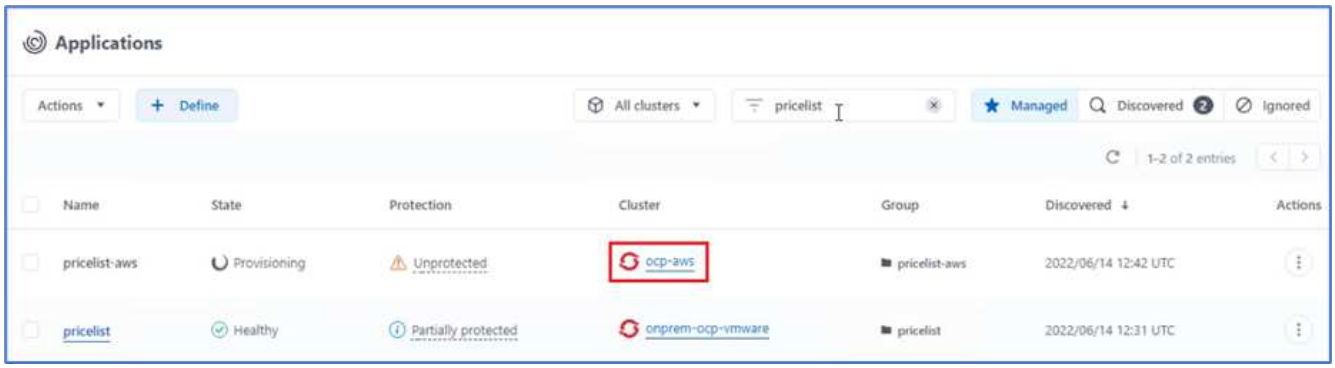
24. In Astra Control Center, fare clic sull'applicazione Pricelist e selezionare Data Protection > Backups (protezione dati > Backup). Selezionare il backup e fare clic su Restore Application (Ripristina applicazione) sotto Action (azione).



25. Selezionare `ocp-aws` come cluster di destinazione e assegnare un nome allo spazio dei nomi. Fare clic sul backup on-demand, su Next (Avanti), quindi su Restore (Ripristina).

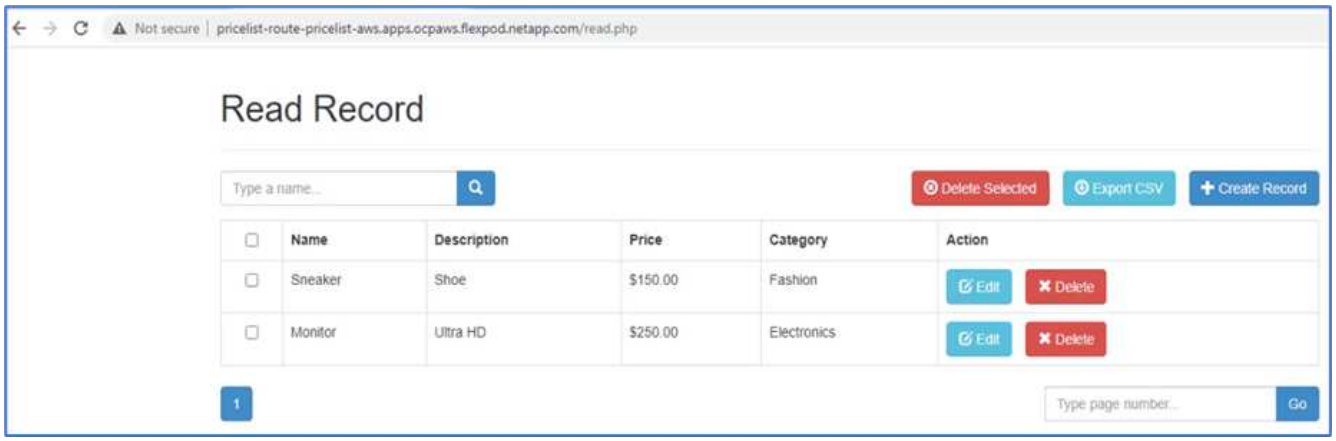


26. Una nuova applicazione con il nome `pricelist-app` Viene eseguito il provisioning sul cluster OpenShift in esecuzione in AWS.



27. Verificare lo stesso nella console Web di OpenShift.

28. Dopo tutti i pod sotto `pricelist-aws` Il progetto è in esecuzione, accedere a routes e fare clic sull'URL per avviare la pagina Web.



Questo processo convalida che l'applicazione Pricelist è stata ripristinata correttamente e che l'integrità dei dati è stata mantenuta sul cluster OpenShift che funziona perfettamente su AWS con l'aiuto di Astra Control Center.

Protezione dei dati con copie Snapshot e mobilità applicativa per DevTest

Questo caso d'utilizzo è costituito da due parti, come descritto nelle sezioni seguenti.

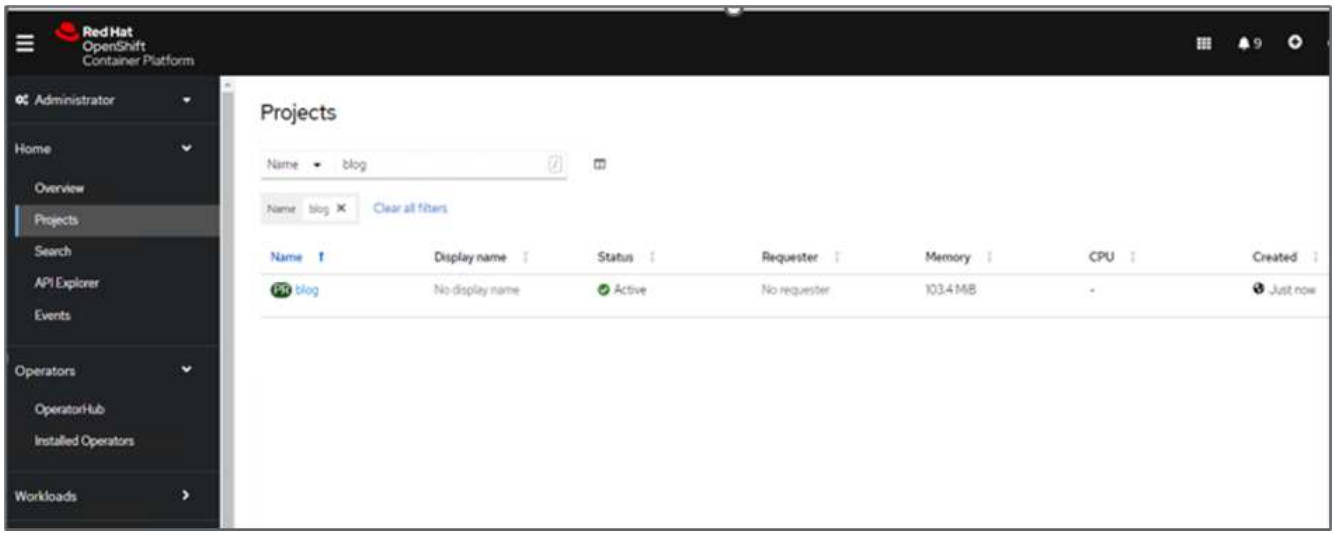
Parte 1

Con Astra Control Center, puoi creare snapshot application-aware per la protezione dei dati locali. In caso di eliminazione o danneggiamento accidentale dei dati, è possibile ripristinare le applicazioni e i dati associati a uno stato sicuramente funzionante utilizzando uno snapshot precedentemente registrato.

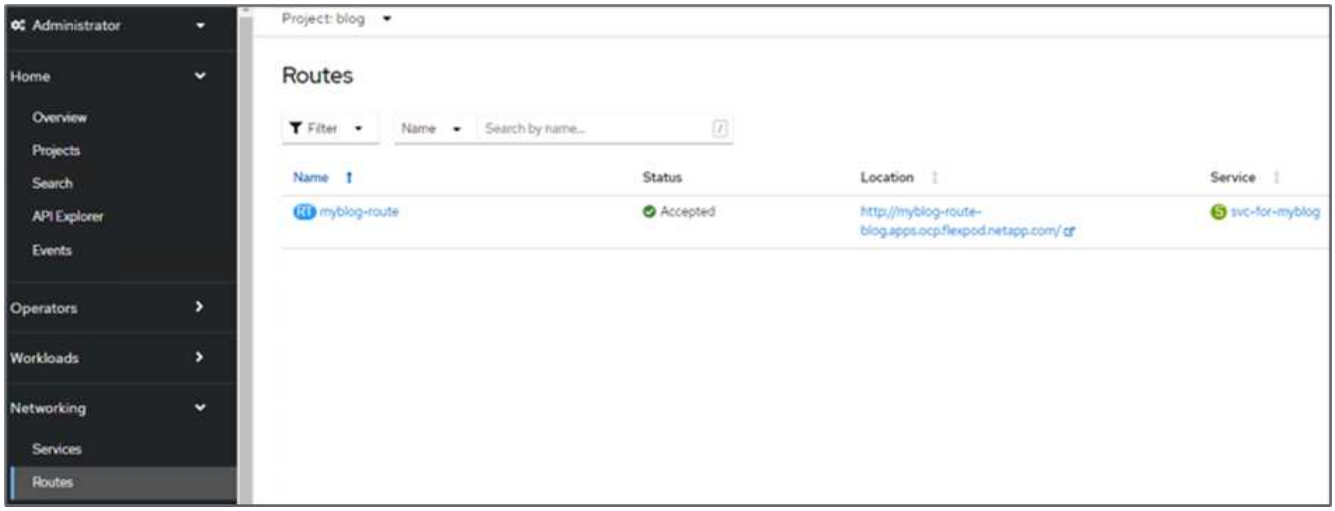
In questo scenario, un team di sviluppo e test (DevTest) implementa un'applicazione stateful di esempio (sito blog) che è un'applicazione blog Ghost, aggiunge alcuni contenuti e aggiorna l'applicazione alla versione più recente disponibile. L'applicazione Ghost utilizza SQLite per il database. Prima di aggiornare l'applicazione, viene eseguita una snapshot (on-demand) utilizzando Astra Control Center per la protezione dei dati. I passaggi dettagliati sono i seguenti:

1. Implementa l'app blogging di esempio e sincronizzala da ArgoCD.

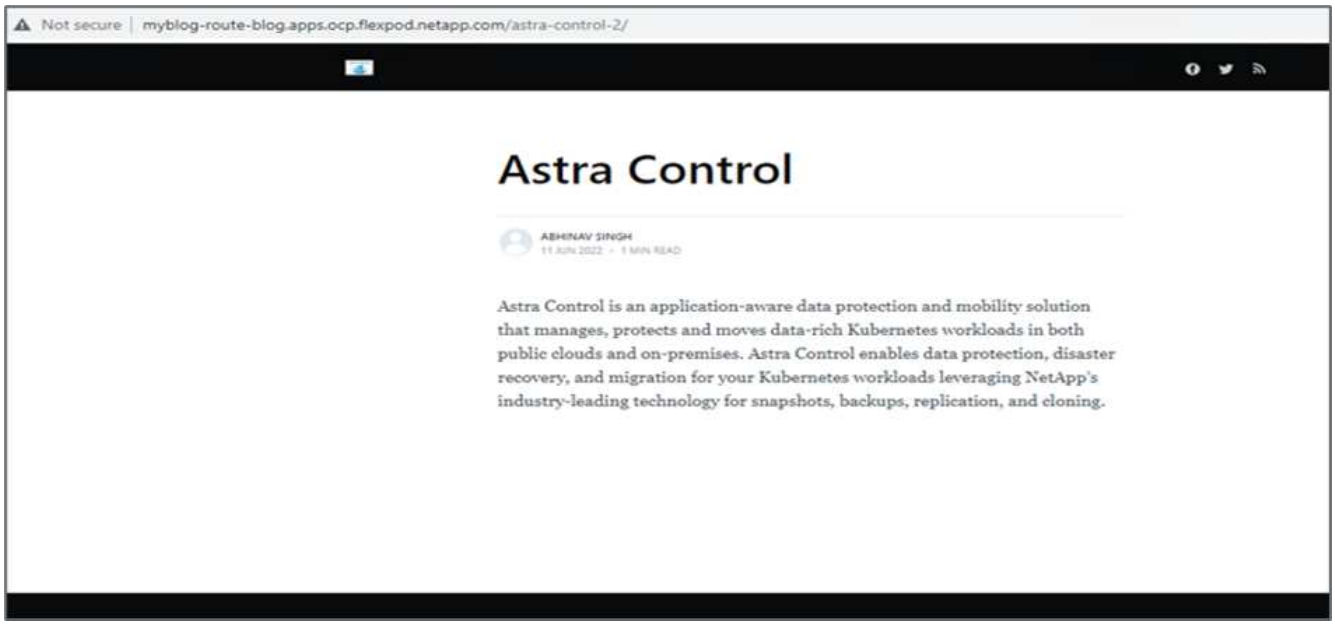
2. Accedere al primo cluster OpenShift, selezionare Project (progetto) e inserire Blog nella barra di ricerca.



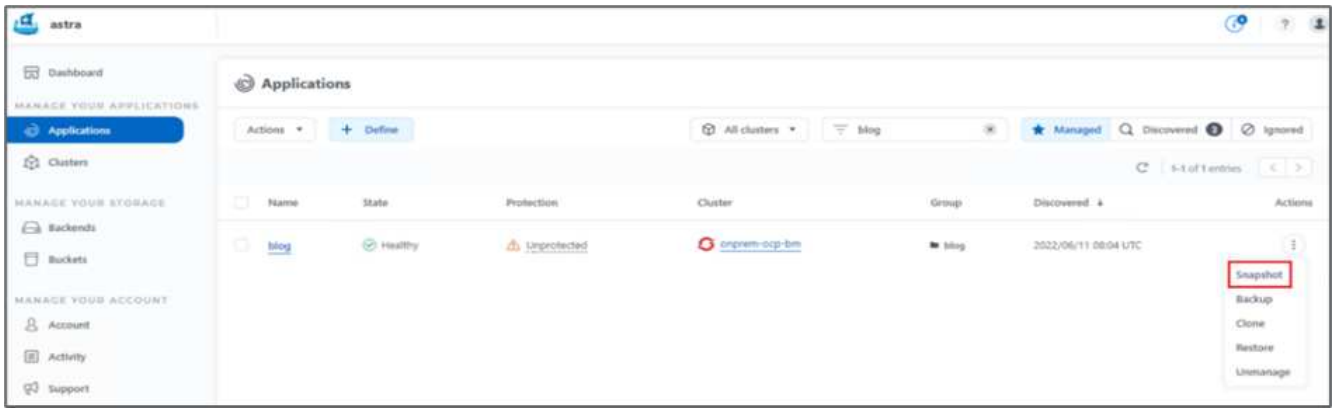
3. Dal menu laterale, selezionare rete > percorsi e fare clic sull'URL.



4. Viene visualizzata la home page del blog. Aggiungi alcuni contenuti al sito del blog e pubblicali.



5. Accedere a Astra Control Center. Gestire l'applicazione dalla scheda rilevato, quindi eseguire una copia Snapshot.

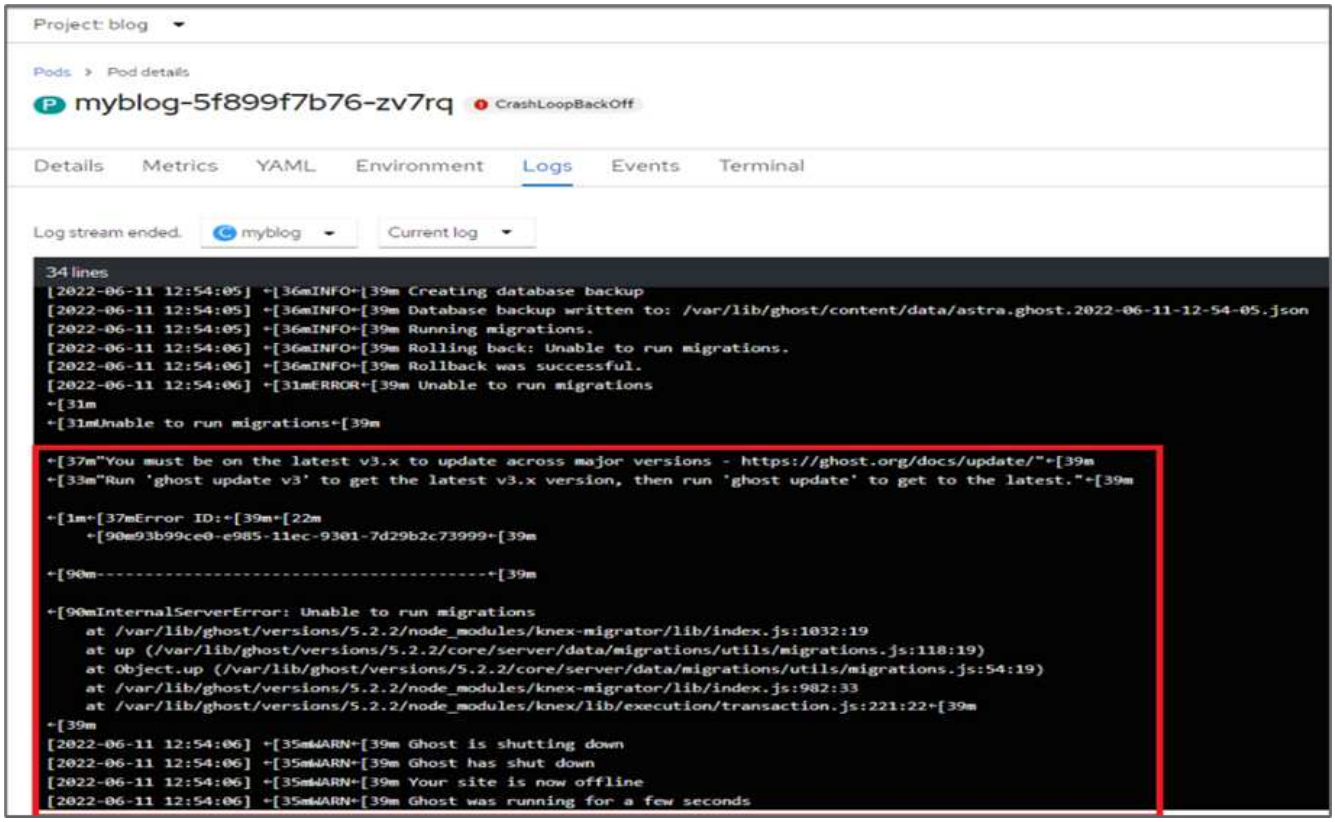


Puoi anche proteggere le tue applicazioni creando snapshot, backup o entrambi in base a una pianificazione definita. Per ulteriori informazioni, vedere "Proteggi le app con snapshot e backup".

6. Una volta creata correttamente l'istantanea on-Demand, aggiorna l'applicazione alla versione più recente. La versione corrente dell'immagine è `ghost: 3.6-alpine` e la versione di destinazione è `ghost:latest`. Per aggiornare l'applicazione, apportare le modifiche direttamente al repository Git e sincronizzarle con il CD Argo.

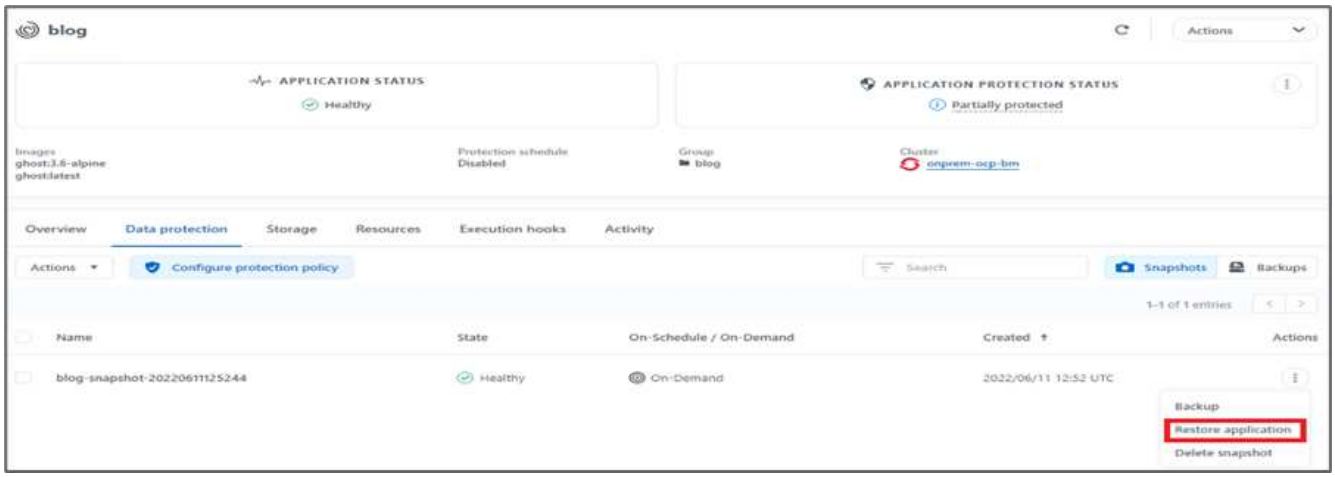
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. L'aggiornamento diretto alla versione più recente non è supportato a causa della disattivazione del sito del blog e del danneggiamento dell'intera applicazione.

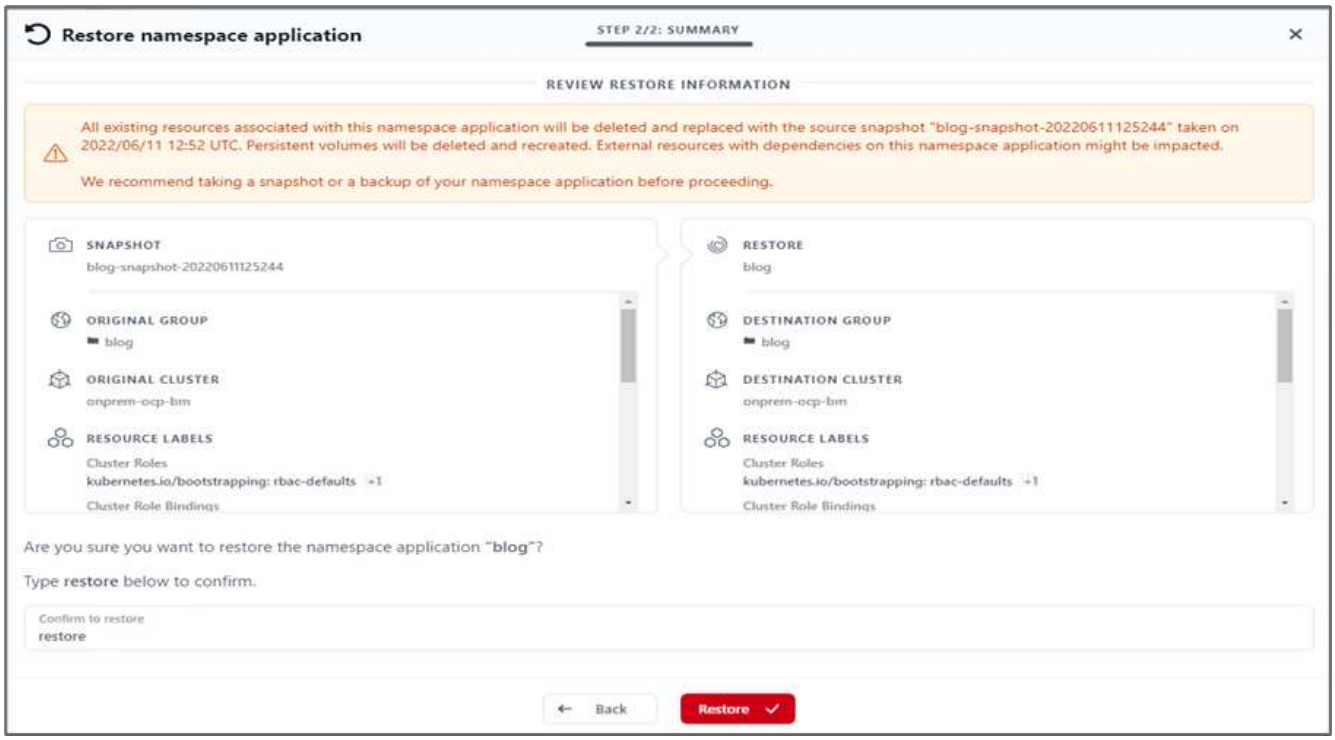


8. Per confermare la non disponibilità del sito del blog, aggiornare l'URL.

9. Ripristinare l'applicazione dallo snapshot.

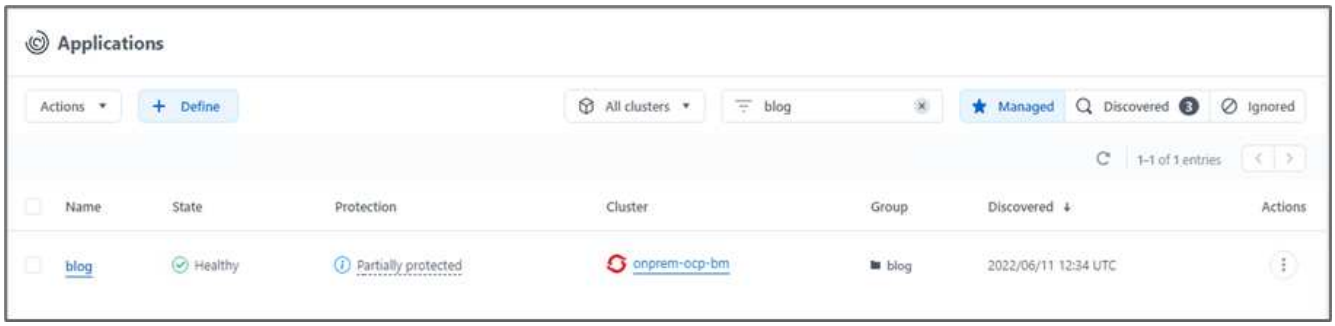


10. L'applicazione viene ripristinata sullo stesso cluster OpenShift.

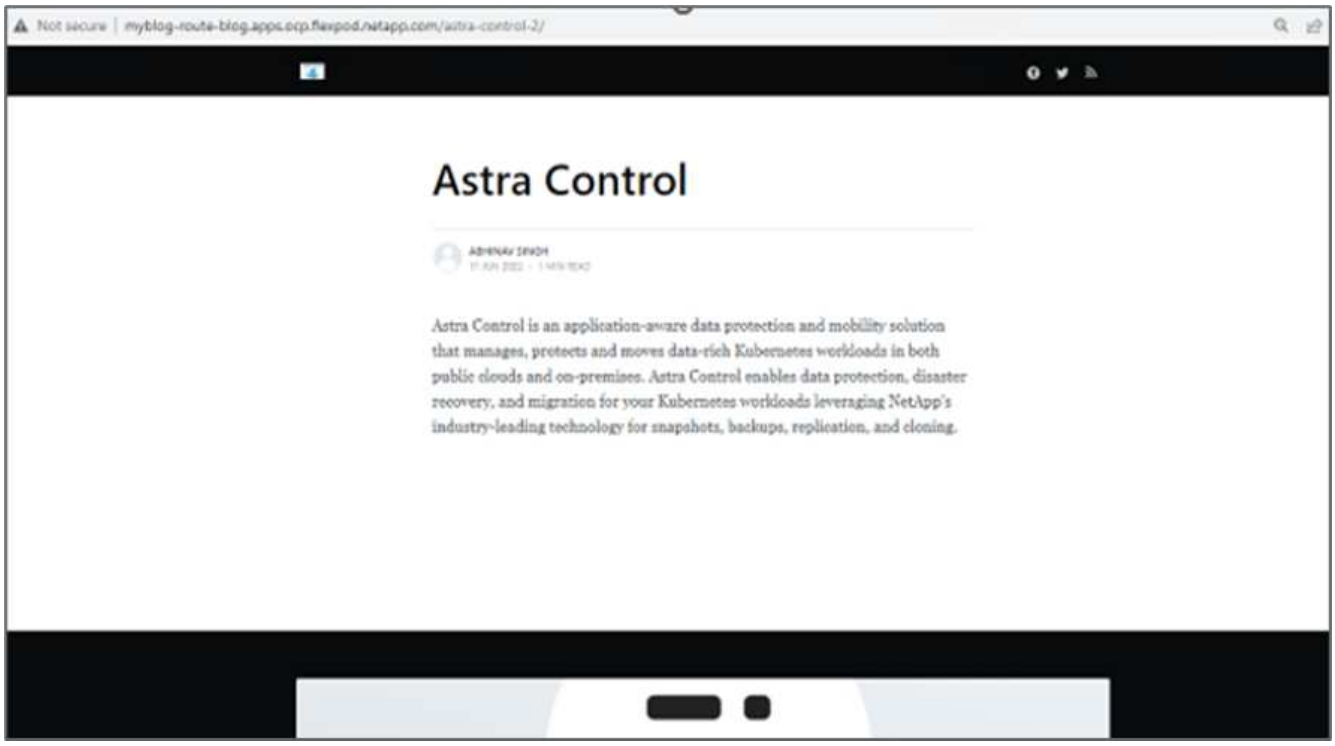


11. Il processo di ripristino dell'applicazione viene avviato immediatamente.

12. In pochi minuti, l'applicazione viene ripristinata correttamente dallo snapshot disponibile.



13. Per verificare se la pagina Web è disponibile, aggiornare l'URL.

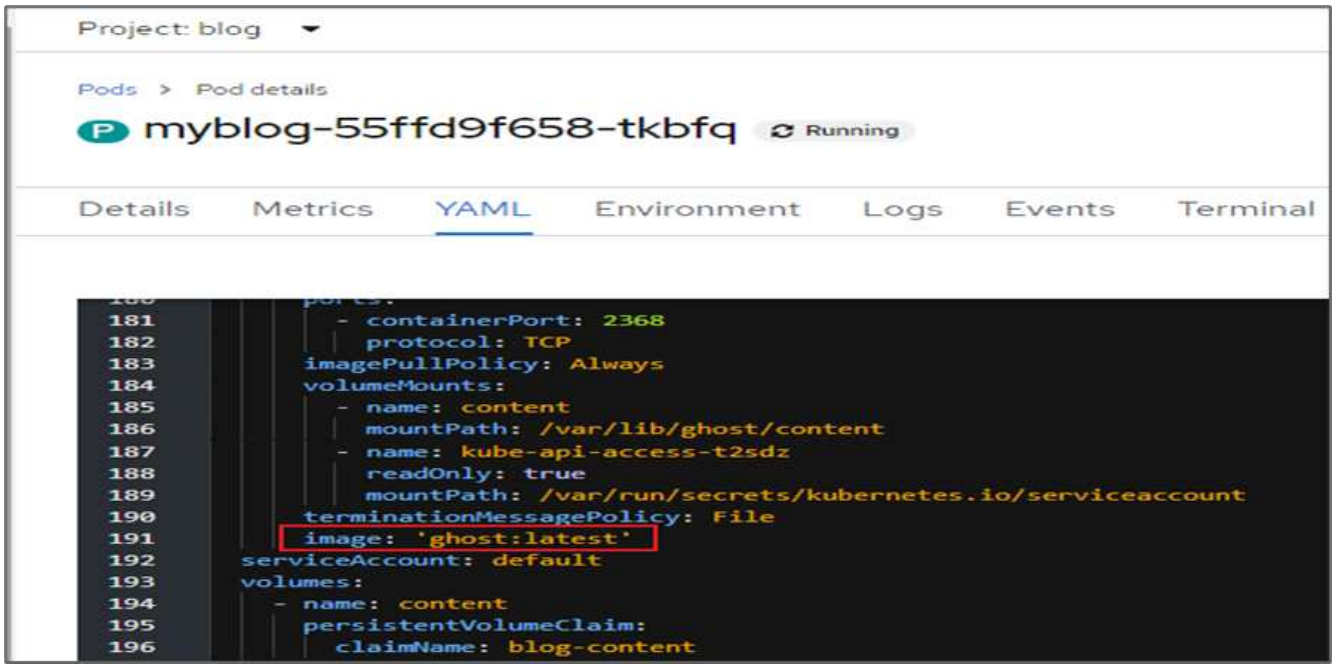


Con l'aiuto di Astra Control Center, un team DevTest può ripristinare con successo un'applicazione del sito del blog e i dati associati utilizzando lo snapshot.

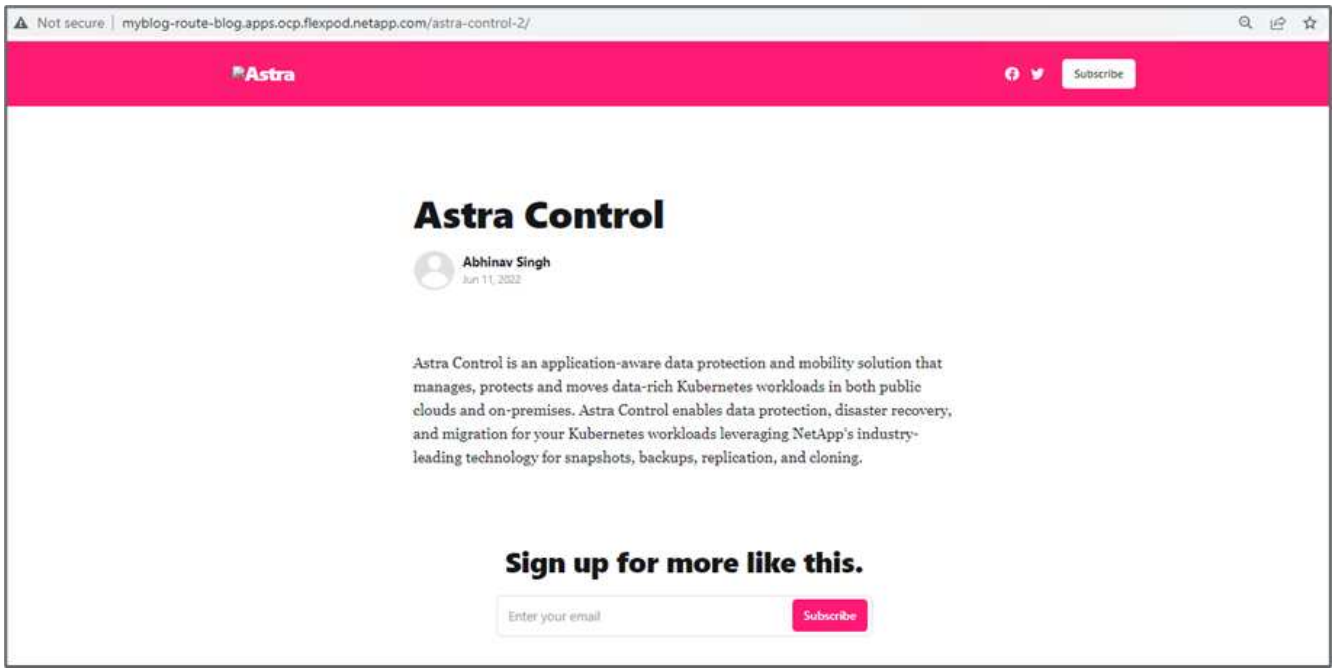
Parte 2

Con Astra Control Center, puoi spostare un'intera applicazione insieme ai suoi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trovano i cluster (on-premise o nel cloud).

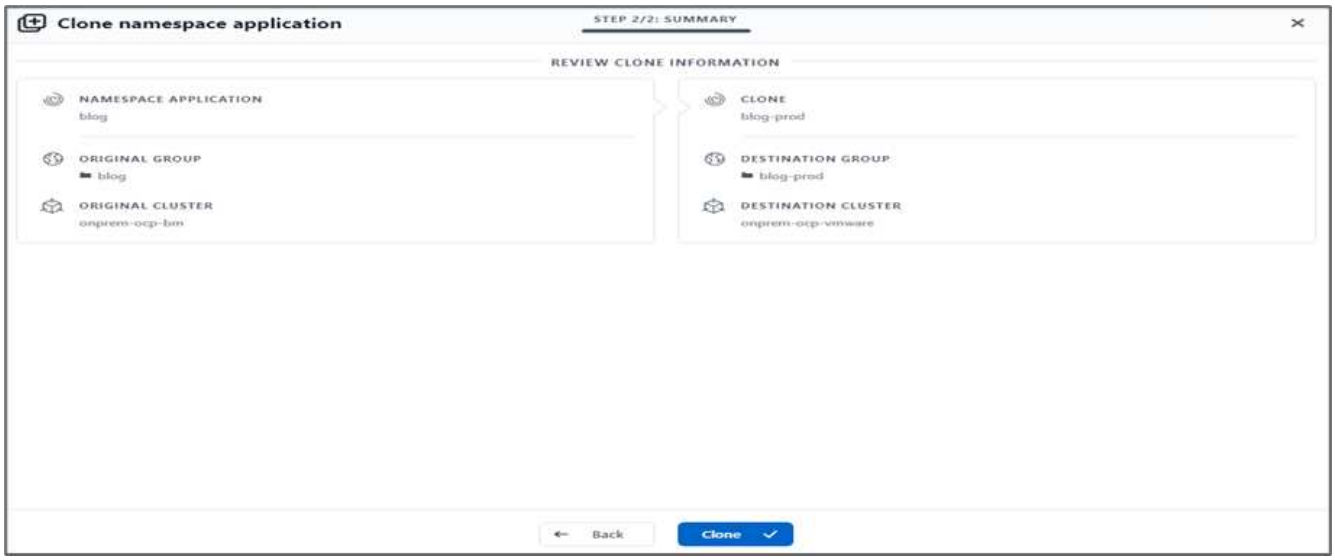
1. Il team DevTest aggiorna inizialmente l'applicazione alla versione supportata (`ghost-4.6-alpine`) prima di eseguire l'aggiornamento alla versione finale (`ghost-latest`) per preparare la produzione it. Quindi, postano un aggiornamento dell'applicazione clonata nel cluster OpenShift di produzione in esecuzione su un sistema FlexPod diverso.
2. A questo punto, l'applicazione viene aggiornata alla versione più recente e pronta per essere clonata nel cluster di produzione.



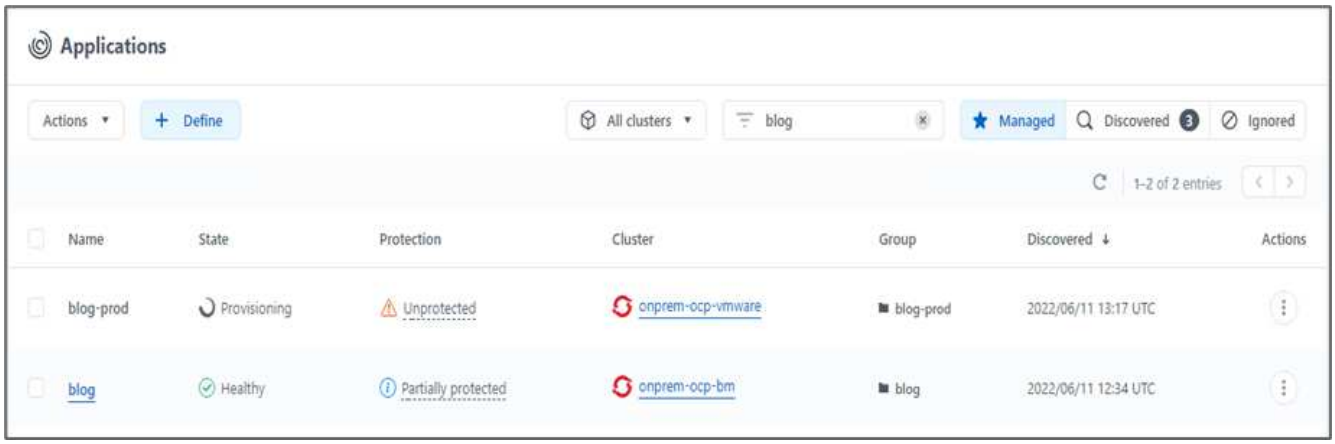
3. Per verificare il nuovo tema, aggiornare il sito del blog.



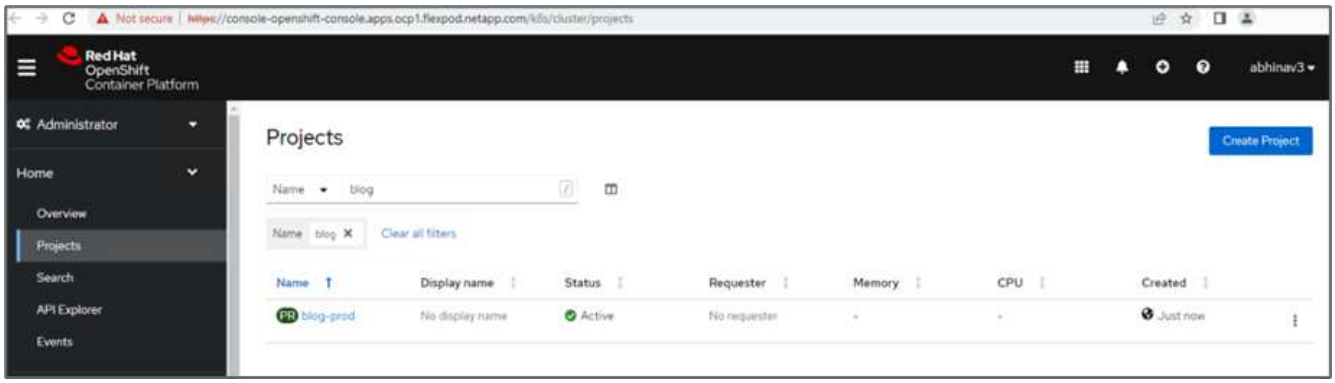
4. Da Astra Control Center, clonare l'applicazione sull'altro cluster OpenShift in produzione in esecuzione su VMware vSphere.



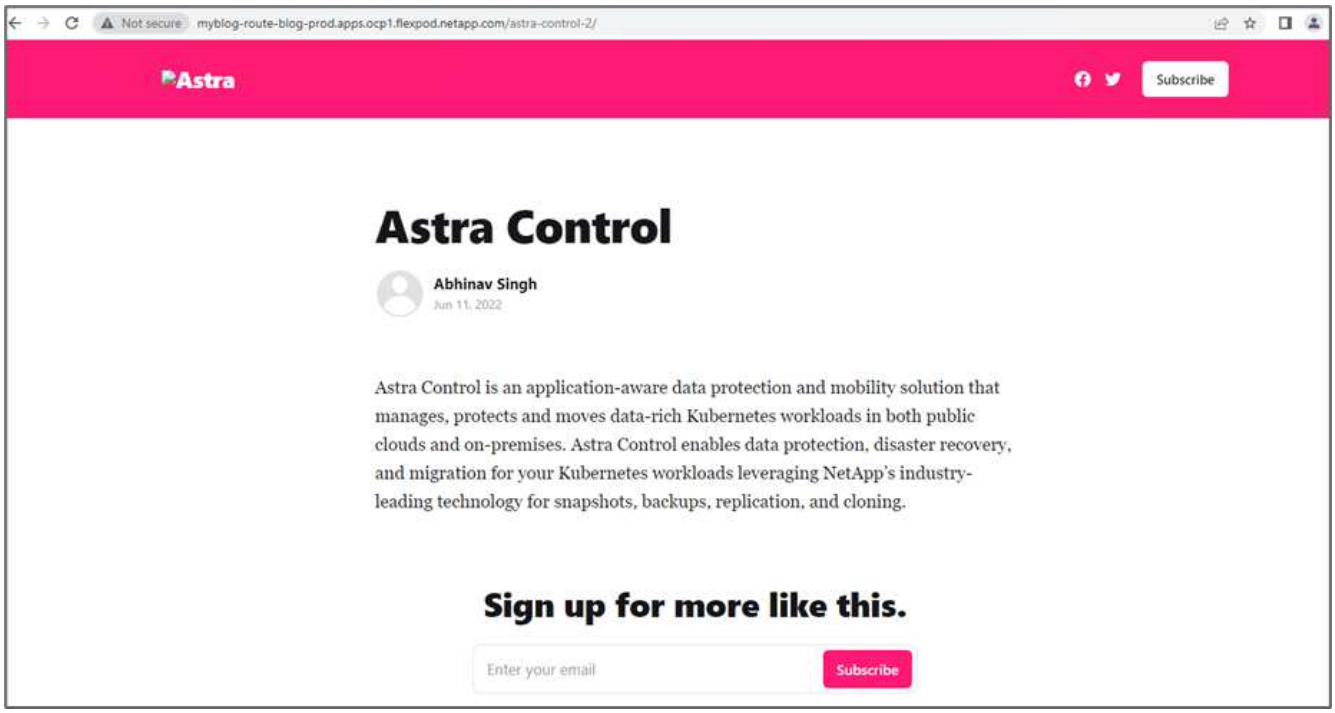
Nel cluster OpenShift di produzione viene ora eseguito il provisioning di un nuovo clone dell'applicazione.



5. Accedi al cluster OpenShift di produzione e cerca il blog del progetto.



6. Dal menu laterale, selezionare rete > percorsi e fare clic sull'URL in posizione. Viene visualizzata la stessa home page con il contenuto.



Si conclude così la convalida della soluzione Astra Control Center. È ora possibile clonare un'intera applicazione e i relativi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trova il cluster Kubernetes.

"Prossimo: Conclusione."

Conclusione

"Precedente: Ripristino dell'applicazione con backup remoti."

In questa soluzione, abbiamo implementato un piano di protezione per le applicazioni containerizzate eseguite su FlexPod e AWS utilizzando il portfolio NetApp Astra. Il centro di controllo Astra e Astra Trident di NetApp, insieme a Cloud Volumes ONTAP, Red Hat OpenShift e all'infrastruttura FlexPod, hanno costituito i componenti principali di questa soluzione.

Abbiamo dimostrato la protezione delle applicazioni acquisendo snapshot e abbiamo eseguito backup completi per ripristinare le applicazioni in diversi cluster K8s in esecuzione in ambienti cloud e on-premise.

Abbiamo anche dimostrato la clonazione delle applicazioni nei cluster K8s, consentendo così ai clienti di migrare le proprie applicazioni nei cluster K8s scelti nelle posizioni desiderate.

FlexPod si è evoluta costantemente in modo che i suoi clienti possano modernizzare le loro applicazioni e i processi di delivery aziendale. Con questa soluzione, i clienti FlexPod possono costruire con sicurezza il proprio piano BCDR per le applicazioni native del cloud con il cloud pubblico come luogo per un piano di DR transitorio o a tempo pieno, mantenendo al contempo bassi i costi della soluzione.

Astra Control consente di spostare un'intera applicazione insieme ai relativi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trovano i cluster. Può anche aiutarti ad accelerare l'implementazione, le operazioni e la protezione per le tue applicazioni native del cloud.

Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, consultare "documentazione online".

Dove trovare ulteriori informazioni

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

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Implementazione di FlexPod con infrastruttura come codice per VMware utilizzando Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Implementazione di FlexPod con infrastruttura come codice per Red Hat OpenShift Bare Metal con Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Cisco UCS hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Scheda informativa su Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentazione NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Tool di matrice di interoperabilità NetApp

  "http://support.netapp.com/matrix/"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Luglio 2022	Release per ACC 22.04.0.

NetApp Cloud Insights per FlexPod

TR-4868: NetApp Cloud Insights per FlexPod

Alan Cowles, NetApp

In collaborazione con:

La soluzione descritta in questo report tecnico è la configurazione del servizio NetApp Cloud Insights per il monitoraggio del sistema di storage NetApp AFF A800 con NetApp ONTAP, implementato come parte di una soluzione per data center FlexPod.

Valore per il cliente

La soluzione qui descritta offre valore ai clienti interessati a una soluzione di monitoraggio completa per i propri ambienti di cloud ibrido, in cui ONTAP viene implementato come sistema di storage primario. Sono inclusi gli ambienti FlexPod che utilizzano i sistemi storage NetApp AFF e FAS.

Casi di utilizzo

Questa soluzione si applica ai seguenti casi di utilizzo:

- Organizzazioni che desiderano monitorare varie risorse e utilizzo nel proprio sistema di storage ONTAP implementato come parte di una soluzione FlexPod.
- Organizzazioni che desiderano risolvere i problemi e ridurre i tempi di risoluzione degli incidenti che si verificano nella propria soluzione FlexPod con i sistemi AFF o FAS.
- Organizzazioni interessate a proiezioni di ottimizzazione dei costi, tra cui dashboard personalizzati per fornire informazioni dettagliate sulle risorse sprecate e dove è possibile realizzare risparmi sui costi nel proprio ambiente FlexPod, incluso ONTAP.

Pubblico di riferimento

Il pubblico di riferimento per la soluzione comprende i seguenti gruppi:

- Dirigenti IT e responsabili dell'ottimizzazione dei costi e della business continuity.
- Architetti di soluzioni interessati alla progettazione e alla gestione di data center o cloud ibrido.
- Tecnici del supporto tecnico responsabili della risoluzione dei problemi e della risoluzione degli incidenti.

È possibile configurare Cloud Insights in modo da fornire diversi tipi di dati utili che possono essere utilizzati per la pianificazione, la risoluzione dei problemi, la manutenzione e la garanzia di business continuity. Monitorando la soluzione di data center FlexPod con Cloud Insights e presentando i dati aggregati in dashboard personalizzate facilmente digeribili; non solo è possibile prevedere quando le risorse di un'implementazione devono essere scalate per soddisfare le esigenze, ma anche identificare applicazioni o volumi di storage specifici che causano problemi all'interno del sistema. In questo modo si garantisce che l'infrastruttura monitorata sia prevedibile e funzioni in base alle aspettative, consentendo a un'organizzazione di rispettare SLA definiti e di scalare l'infrastruttura in base alle necessità, eliminando sprechi e costi aggiuntivi.

Architettura

In questa sezione, esaminano l'architettura di un'infrastruttura convergente per data center FlexPod, incluso un sistema NetApp AFF A800 monitorato da Cloud Insights.

Tecnologia della soluzione

Una soluzione per data center FlexPod è costituita dai seguenti componenti minimi per fornire un ambiente di infrastruttura convergente altamente disponibile, facilmente scalabile, validato e supportato.

- Due nodi storage NetApp ONTAP (una coppia ha)
- Due switch di rete per data center Cisco Nexus
- Due switch Cisco MDS Fabric (opzionali per implementazioni FC)
- Due interconnessioni fabric Cisco UCS
- Uno chassis blade Cisco UCS con due server blade Cisco UCS serie B.

Oppure

- Due server Cisco UCS C-Series per il montaggio in rack

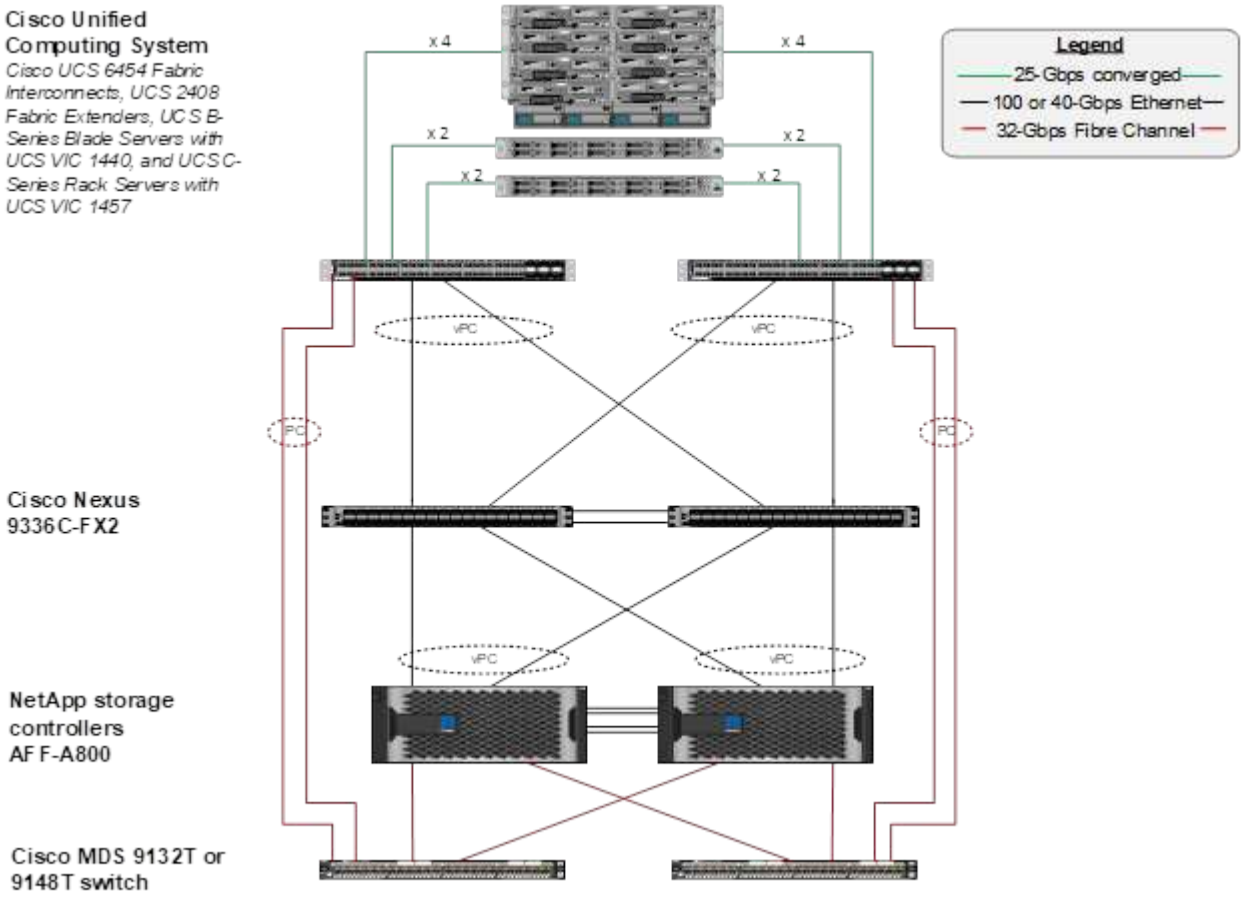
Per consentire a Cloud Insights di raccogliere i dati, un'organizzazione deve implementare un'unità di acquisizione come macchina virtuale o fisica all'interno del proprio ambiente FlexPod Datacenter o in una posizione in cui può contattare i componenti da cui sta raccogliendo i dati. È possibile installare il software Acquisition Unit su un sistema che esegue diversi sistemi operativi Windows o Linux supportati. La seguente tabella elenca i componenti della soluzione per questo software.

Sistema operativo	Versione
Microsoft Windows	10
Server Microsoft Windows	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6

Sistema operativo	Versione
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Diagramma dell'architettura

La figura seguente mostra l'architettura della soluzione.



Requisiti hardware

La seguente tabella elenca i componenti hardware necessari per implementare la soluzione. I componenti hardware utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Hardware	Quantità
Cisco Nexus 9336C-FX2	2
Cisco UCS 6454 Fabric Interconnect	2
Chassis blade Cisco UCS 5108	1
Cisco UCS 2408 Fabric Extender	2
Blade Cisco UCS B200 M5	2

Hardware	Quantità
NetApp AFF A800	2

Requisiti software

La seguente tabella elenca i componenti software necessari per implementare la soluzione. I componenti software utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Software	Versione
Firmware Cisco Nexus	9.3(5)
Versione Cisco UCS	4.1(2a)
Versione di NetApp ONTAP	9.7
Versione di NetApp Cloud Insights	Settembre 2020, Basic
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3

Utilizza i dettagli del caso

Questa soluzione si applica ai seguenti casi di utilizzo:

- Analisi dell'ambiente con i dati forniti al consulente digitale NetApp Active IQ per la valutazione dei rischi del sistema storage e consigli per l'ottimizzazione dello storage.
- Risoluzione dei problemi nel sistema storage ONTAP implementato in una soluzione FlexPod Datacenter esaminando le statistiche di sistema in tempo reale.
- Creazione di dashboard personalizzate per monitorare facilmente punti di interesse specifici per i sistemi storage ONTAP implementati in un'infrastruttura convergente del data center FlexPod.

Considerazioni di progettazione

La soluzione per data center FlexPod è un'infrastruttura convergente progettata da Cisco e NetApp per fornire un ambiente di data center dinamico, altamente disponibile e scalabile per l'esecuzione di carichi di lavoro aziendali. Le risorse di calcolo e di rete della soluzione sono fornite dai prodotti Cisco UCS e Nexus, mentre le risorse di storage sono fornite dal sistema di storage ONTAP. La progettazione della soluzione viene migliorata regolarmente, quando sono disponibili modelli hardware aggiornati o versioni software e firmware. Questi dettagli, insieme alle Best practice per la progettazione e l'implementazione della soluzione, vengono acquisiti nei documenti Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) e pubblicati regolarmente.

È disponibile il più recente documento CVD che descrive la progettazione della soluzione per data center FlexPod "qui".

Implementare Cloud Insights per FlexPod

Per implementare la soluzione, è necessario completare le seguenti attività:

1. Iscriviti al servizio Cloud Insights
2. Creare una macchina virtuale VMware (VM) da configurare come unità di acquisizione
3. Installare l'host Red Hat Enterprise Linux (RHEL)
4. Creare un'istanza dell'unità di acquisizione nel portale Cloud Insights e installare il software
5. Aggiungi il sistema storage monitorato dal data center FlexPod a Cloud Insights.

Iscriviti al servizio NetApp Cloud Insights

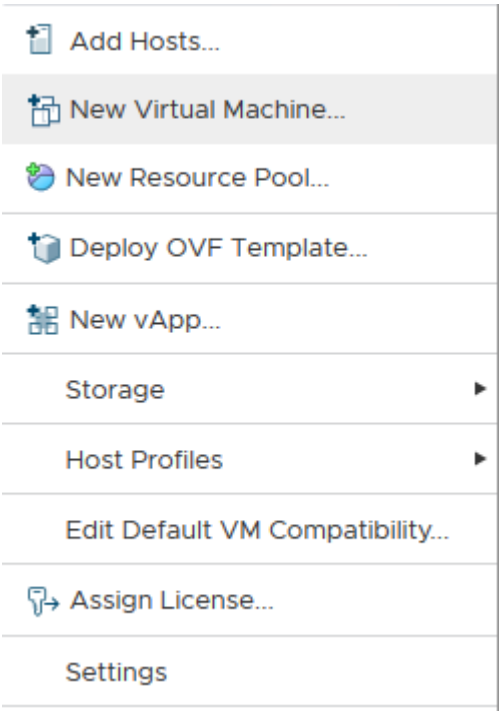
Per iscriversi al servizio NetApp Cloud Insights, attenersi alla seguente procedura:

1. Passare a. "https://cloud.netapp.com/cloud-insights"
2. Fare clic sul pulsante al centro dello schermo per avviare la prova gratuita di 14 giorni oppure sul collegamento nell'angolo in alto a destra per registrarsi o accedere a un account NetApp Cloud Central esistente.

Creare una macchina virtuale VMware da configurare come unità di acquisizione

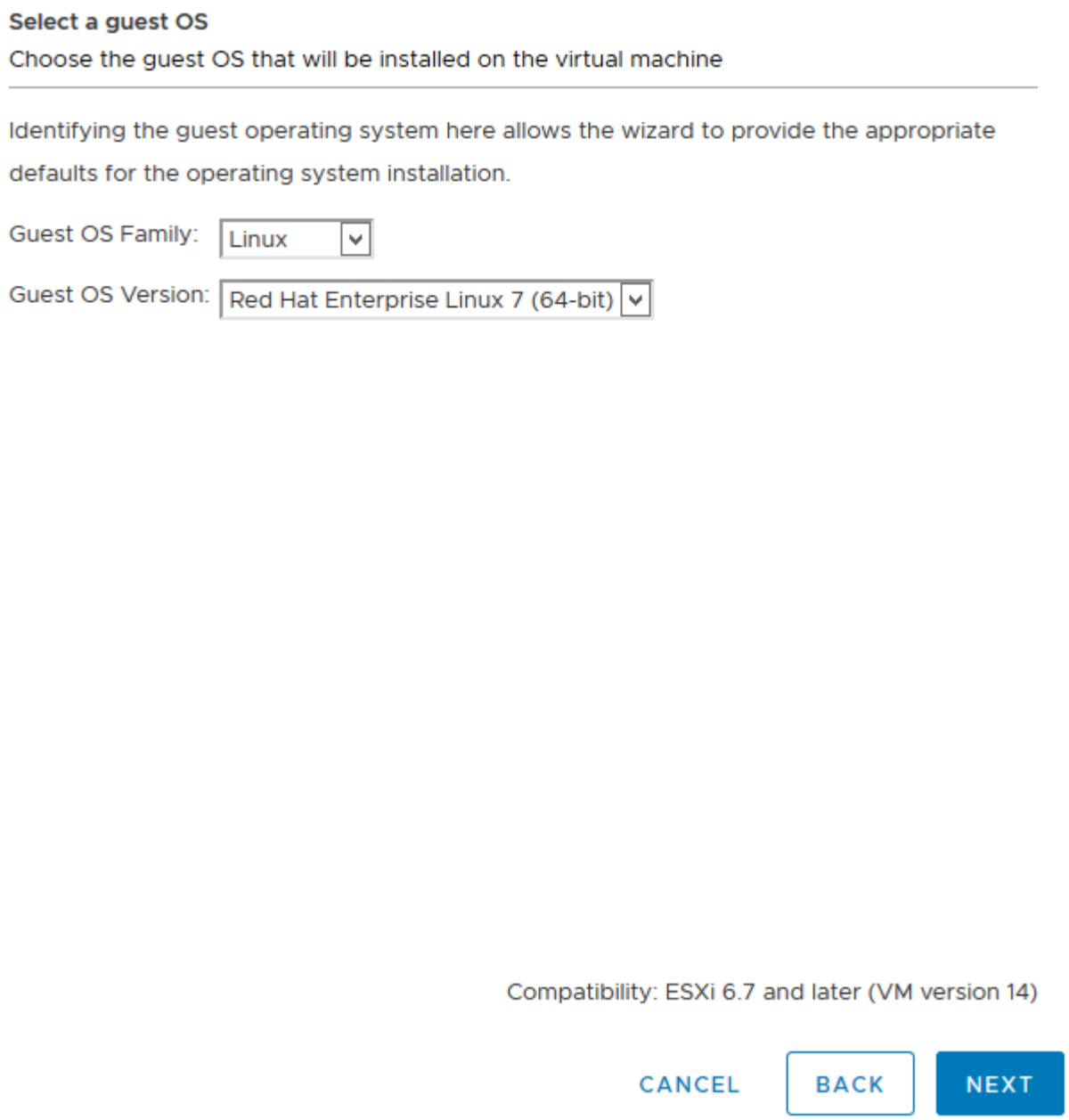
Per creare una macchina virtuale VMware da configurare come unità di acquisizione, attenersi alla seguente procedura:

1. Avviare un browser Web, accedere a VMware vSphere e selezionare il cluster che si desidera ospitare.
2. Fare clic con il pulsante destro del mouse sul cluster e selezionare Create A Virtual Machine (Crea una macchina virtuale) dal menu.



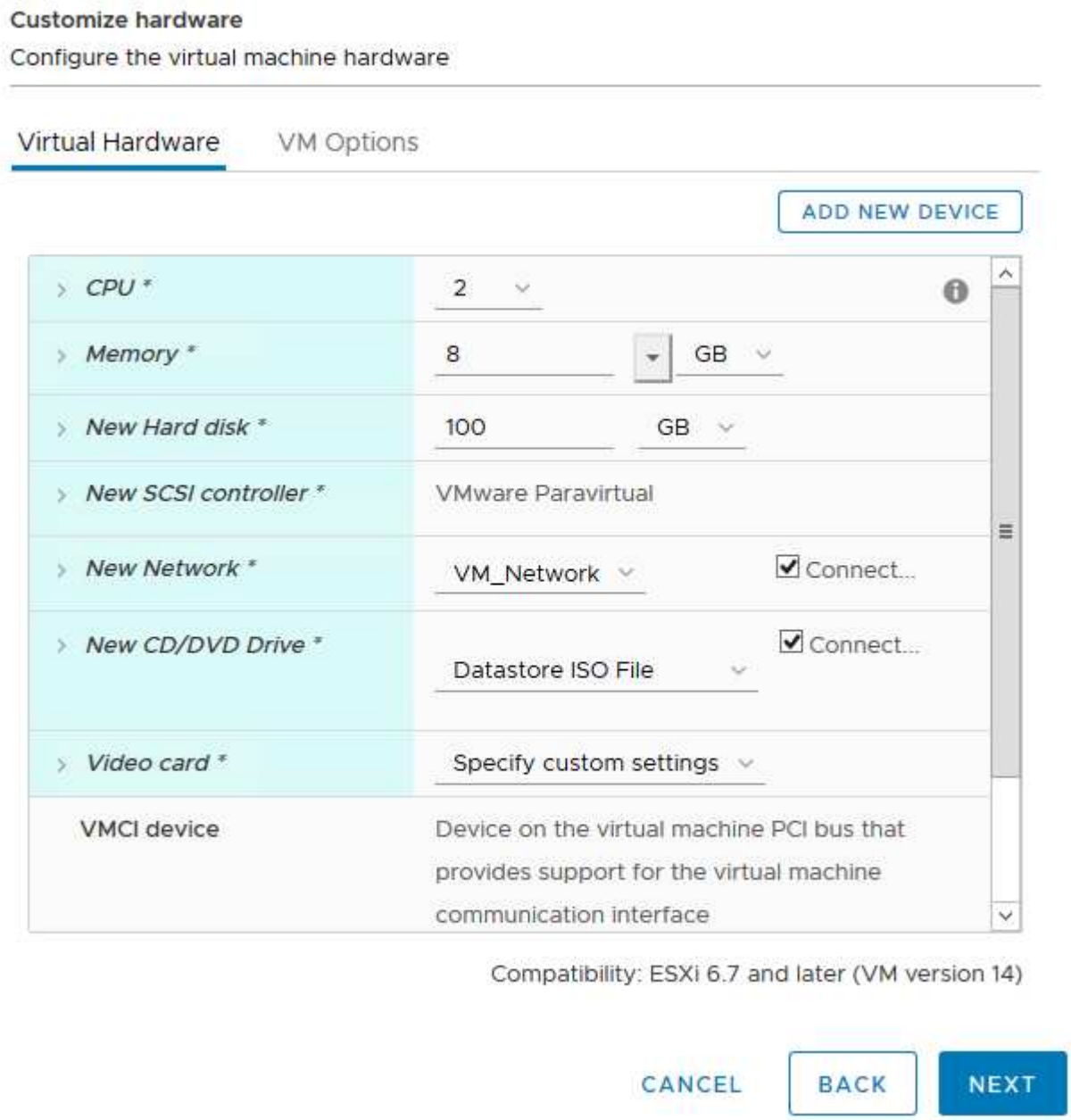
3. Nella procedura guidata Nuova macchina virtuale, fare clic su Avanti.

4. Specificare il nome della macchina virtuale e selezionare il data center in cui si desidera installarla, quindi fare clic su Next (Avanti).
5. Nella pagina seguente, selezionare il cluster, i nodi o il gruppo di risorse in cui si desidera installare la macchina virtuale, quindi fare clic su Avanti.
6. Selezionare il datastore condiviso che ospita le macchine virtuali e fare clic su Next (Avanti).
7. Verificare che la modalità di compatibilità per la macchina virtuale sia impostata su `ESXi 6.7 or later` E fare clic su Next (Avanti).
8. Selezionare la famiglia di sistemi operativi guest Linux, versione del sistema operativo guest: Red Hat Enterprise Linux 7 (64 bit).



9. La pagina successiva consente di personalizzare le risorse hardware sulla macchina virtuale. L'unità di acquisizione Cloud Insights richiede le seguenti risorse. Una volta selezionate le risorse, fare clic su Next (Avanti):

a. Due CPU
b. 8 GB di RAM
c. 100 GB di spazio su disco rigido
d. Una rete in grado di raggiungere le risorse nel data center FlexPod e nel server Cloud Insights tramite una connessione SSL sulla porta 443.
e. Immagine ISO della distribuzione Linux scelta (Red Hat Enterprise Linux) da cui eseguire l'avvio.

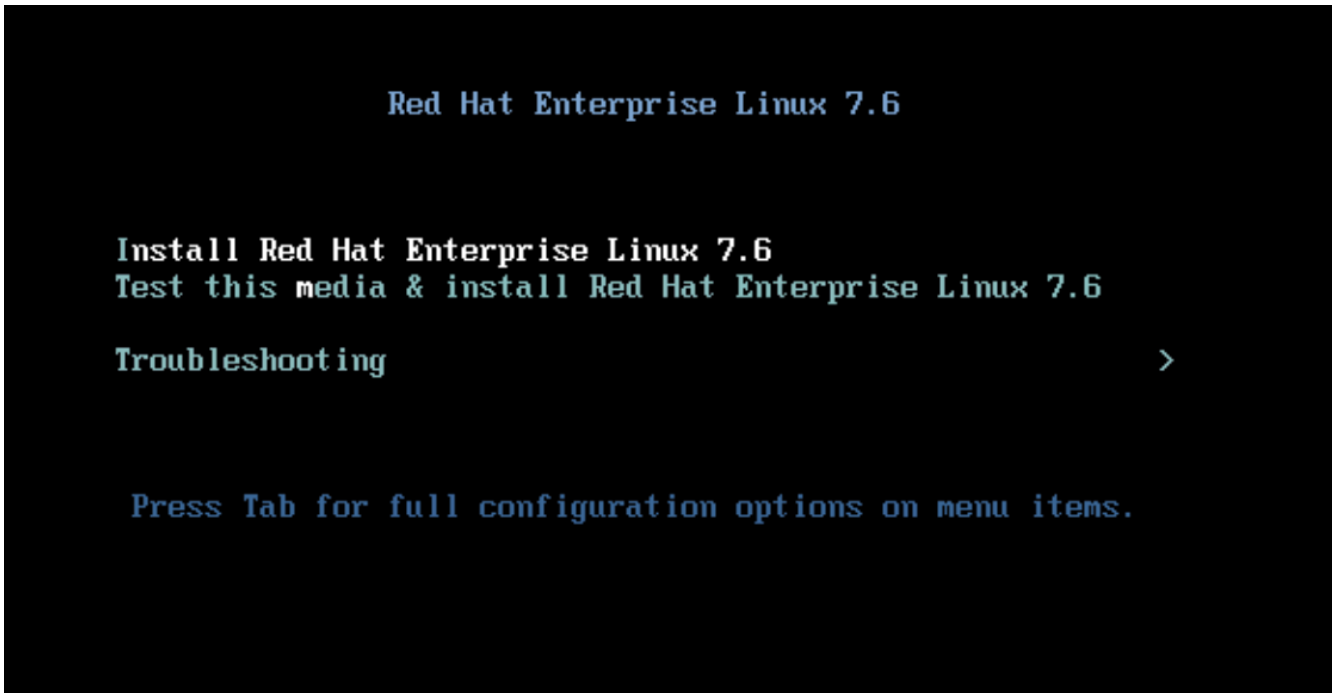


10. Per creare la macchina virtuale, nella pagina Ready to complete (Pronto per il completamento), rivedere le impostazioni e fare clic su Finish (fine).

Installare Red Hat Enterprise Linux

Per installare Red Hat Enterprise Linux, attenersi alla seguente procedura:

1. Accendere la macchina virtuale, fare clic sulla finestra per avviare la console virtuale, quindi selezionare l'opzione Installa Red Hat Enterprise Linux 7.6.

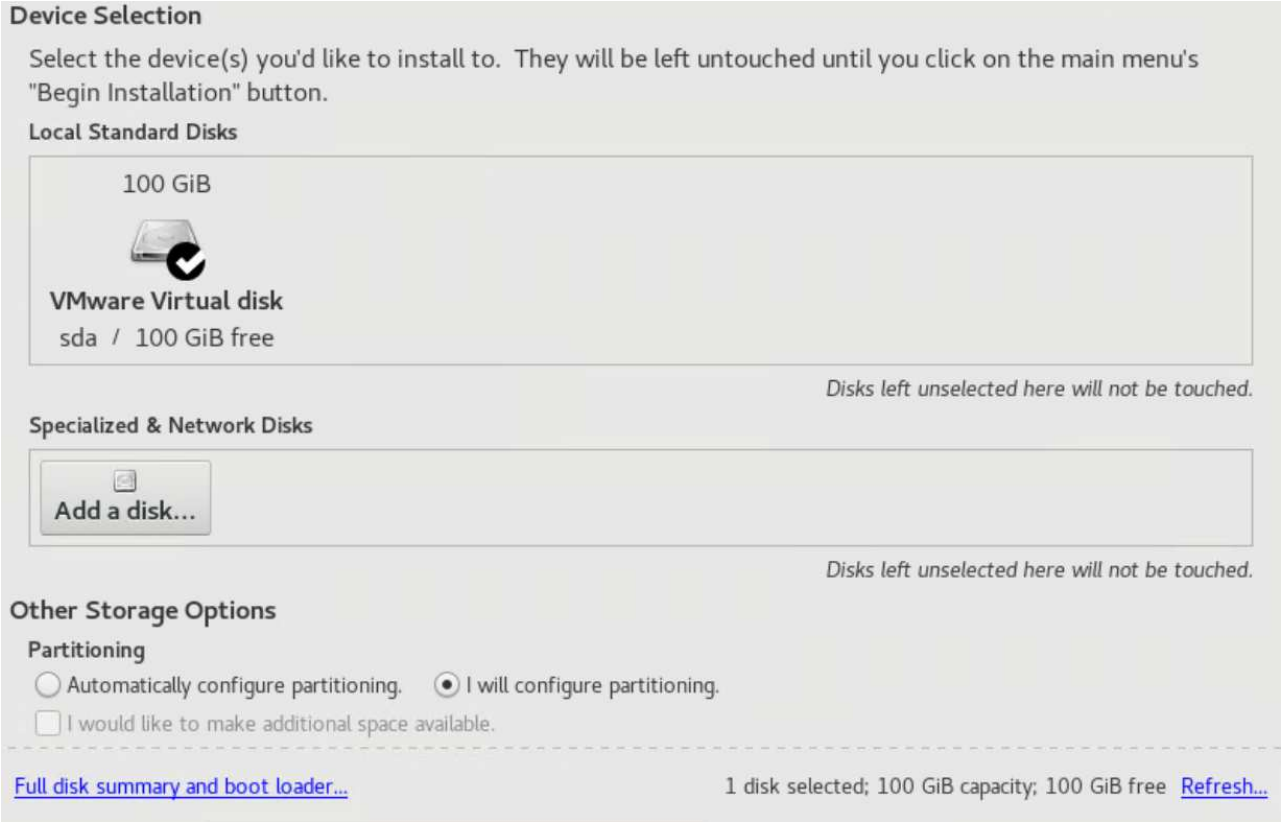


2. Selezionare la lingua desiderata e fare clic su continua.

   La pagina successiva è Riepilogo dell'installazione. Le impostazioni predefinite dovrebbero essere accettabili per la maggior parte di queste opzioni.

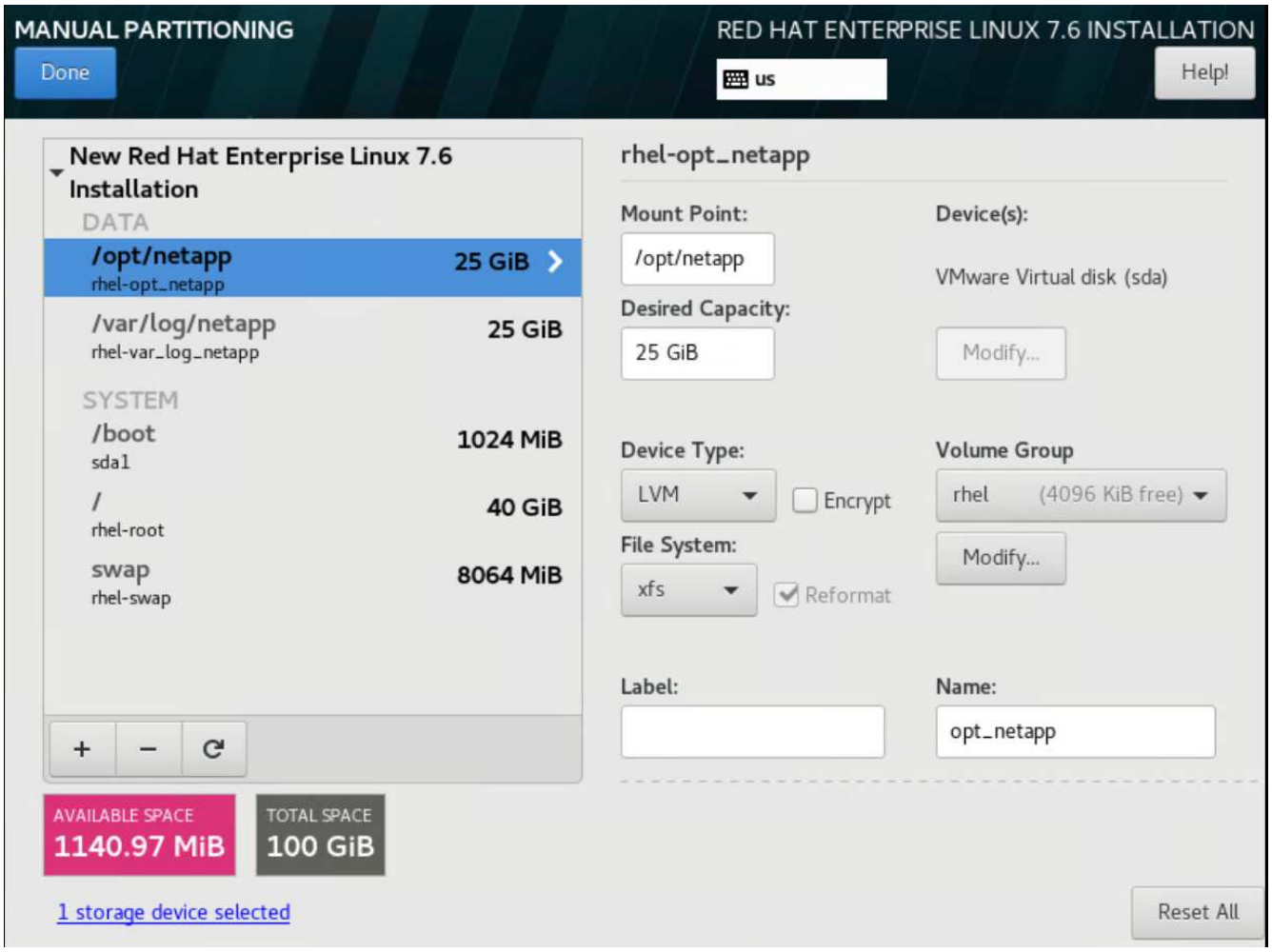
3. È necessario personalizzare il layout dello storage eseguendo le seguenti opzioni:

   a. Per personalizzare la partizione per il server, fare clic su destinazione installazione.
   b. Verificare che il disco virtuale VMware di 100GiB sia selezionato con un segno di spunta nero e selezionare il pulsante di opzione i Will Configure Partitioning (i Will Configure Partitioning).



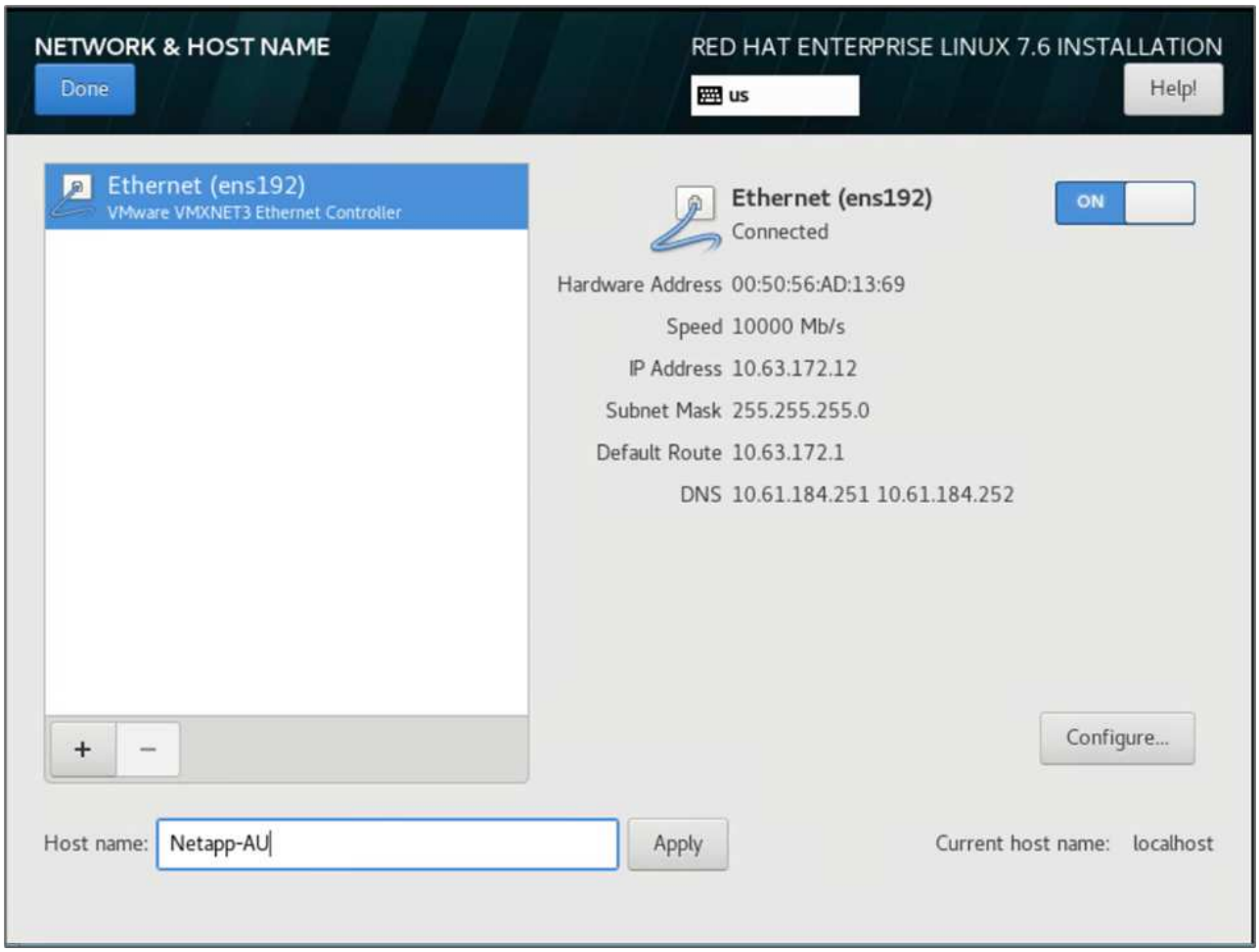
c. Fare clic su fine.

   Viene visualizzato un nuovo menu che consente di personalizzare la tabella delle partizioni. Dedicare 25 GB ciascuno a. `/opt/netapp` e. `/var/log/netapp`. È possibile allocare automaticamente il resto dello storage nel sistema.



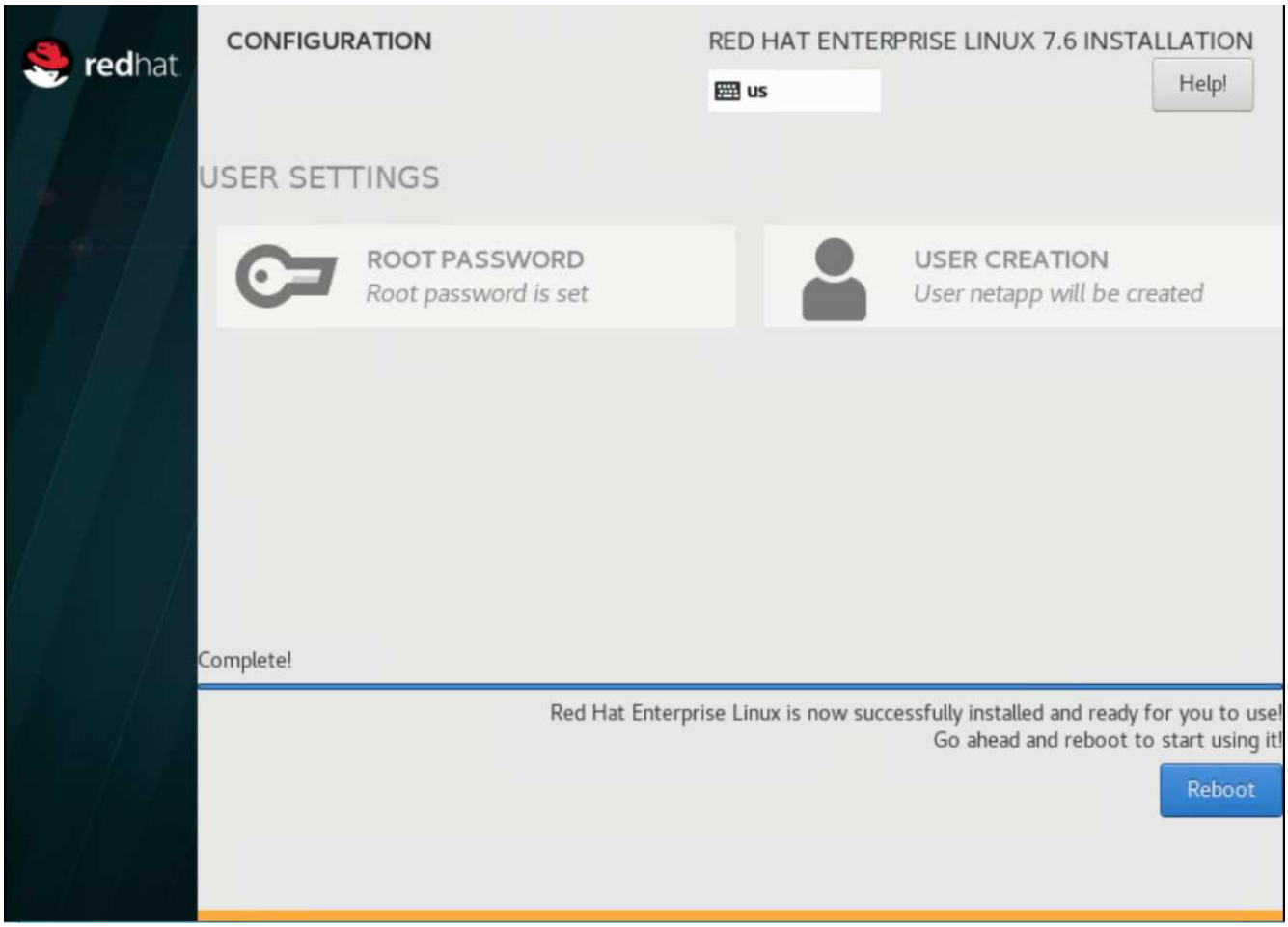
a. Per tornare al Riepilogo dell'installazione, fare clic su fine.

4. Fare clic su Network and host Name (rete e nome host)
   a. Immettere un nome host per il server.
   b. Accendere la scheda di rete facendo clic sul pulsante a scorrimento. Se il protocollo DHCP (Dynamic host Configuration Protocol) è configurato sulla rete, si riceverà un indirizzo IP. In caso contrario, fare clic su Configure (Configura) e assegnare manualmente un indirizzo.



c. . Fare clic su Done (fine) per tornare al Riepilogo dell'installazione.

5. Nella pagina Installation Summary (Riepilogo dell'installazione), fare clic su Begin Installation
6. Nella pagina Installation Progress (avanzamento installazione), è possibile impostare la password root o creare un account utente locale. Al termine dell'installazione, fare clic su Reboot (Riavvia) per riavviare il server.



7. Una volta riavviato il sistema, accedere al server e registrarlo con Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

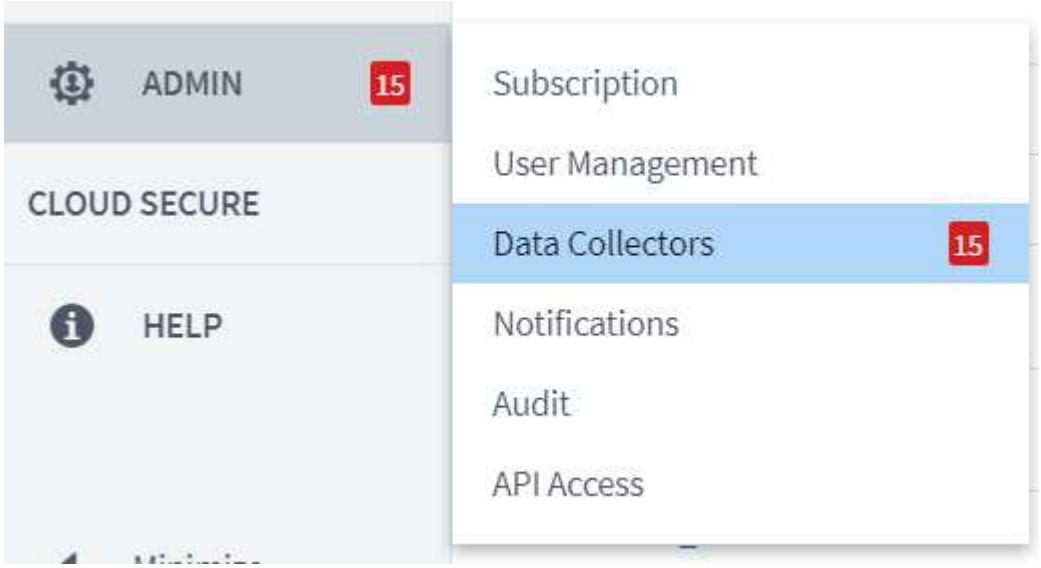
8. Allega un abbonamento disponibile per Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Creare un’istanza dell’unità di acquisizione nel portale Cloud Insights e installare il software

Per creare un’istanza dell’unità di acquisizione nel portale Cloud Insights e installare il software, attenersi alla seguente procedura:

1. Dalla home page di Cloud Insights, passare il mouse sulla voce Amministratore nel menu principale a sinistra e selezionare Data Collector dal menu.

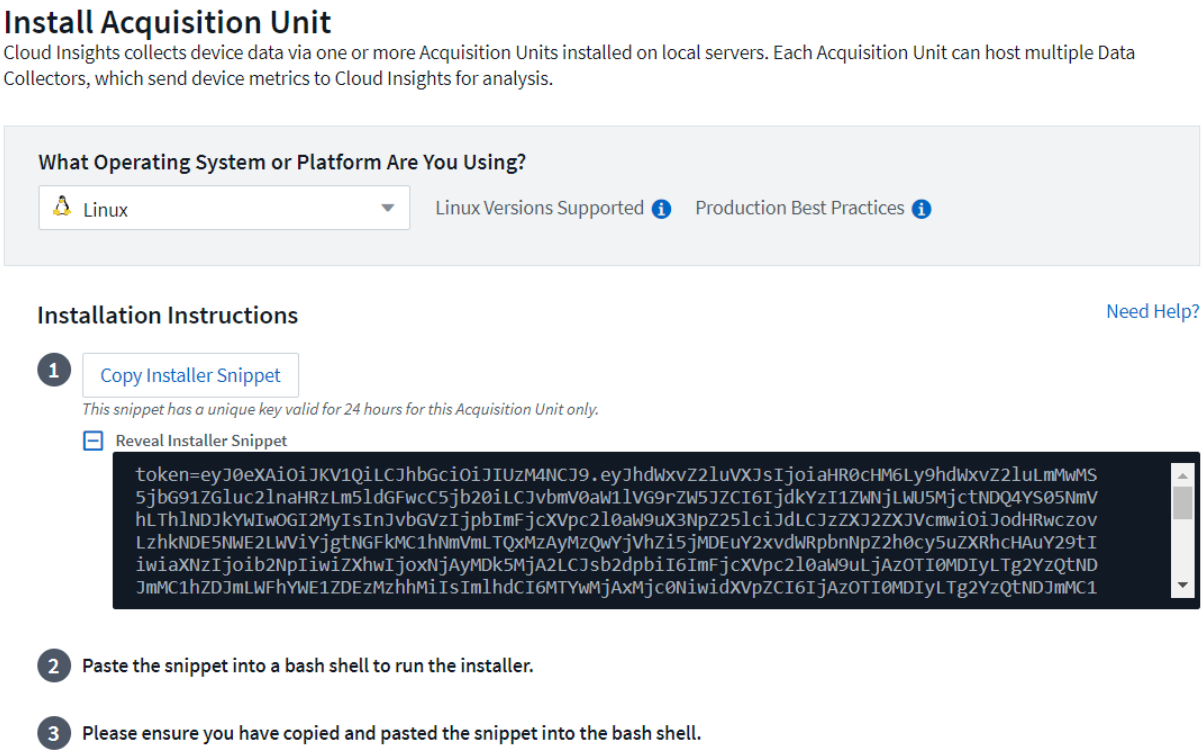


2. Nella parte superiore centrale della pagina Data Collector, fare clic sul collegamento Acquisition Units (unità di acquisizione).

3. Per creare una nuova unità di acquisizione, fare clic sul pulsante a destra.

4. Selezionare il sistema operativo che si desidera utilizzare per ospitare l'unità di acquisizione e seguire le istruzioni per copiare lo script di installazione dalla pagina Web.

   In questo esempio, si tratta di un server Linux, che fornisce un frammento e un token da incollare nella CLI sul nostro host. La pagina Web attende la connessione dell'unità di acquisizione.



5. Incollare il frammento nella CLI della macchina Red Hat Enterprise Linux che ha eseguito il provisioning e fare clic su Invio.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

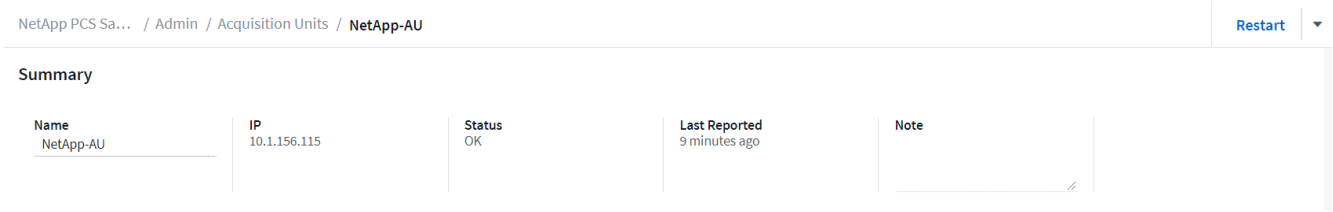
Il programma di installazione scarica un pacchetto compresso e avvia l'installazione. Una volta completata l'installazione, viene visualizzato un messaggio che indica che l'unità di acquisizione è stata registrata con NetApp Cloud Insights.

```
Welcome to CloudInsights (R) ..
Acquisition Unit

NetApp (R)
Installation: /opt/netapp/cloudinsights
Logs:         /opt/netapp/cloudinsights/logs -> /var/log/netapp/cloudinsights

To control the CloudInsights service:
  sudo cloudinsights-service.sh --help
To uninstall:
  sudo cloudinsights-uninstall.sh --help

1/8 Acquisition Unit Starting
2/8 Connecting to Cloud Insights
3/8 Sending Certificate-Signing Request..
4/8 Logging in to Cloud Insights
5/8 Updating Security Settings..
6/8 Downloading Data Collection Modules
7/8 Registering to Cloud Insights
8/8 Acquisition Unit Ready

Acquisition Unit has been installed successfully.
[root@Netapp-AU ~]#
```

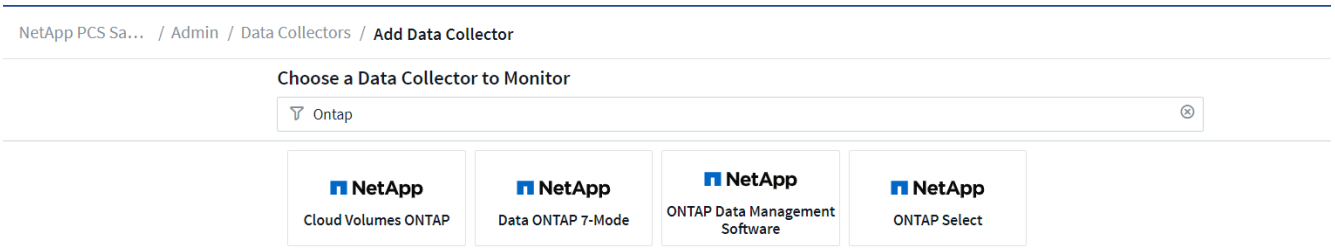
Aggiungi il sistema storage monitorato dal data center FlexPod a Cloud Insights

Per aggiungere il sistema di storage ONTAP da un'implementazione FlexPod, attenersi alla seguente procedura:

1. Tornare alla pagina unità di acquisizione sul portale Cloud Insights e individuare l'unità appena registrata elencata. Per visualizzare un riepilogo del reparto, fare clic sull'unità.

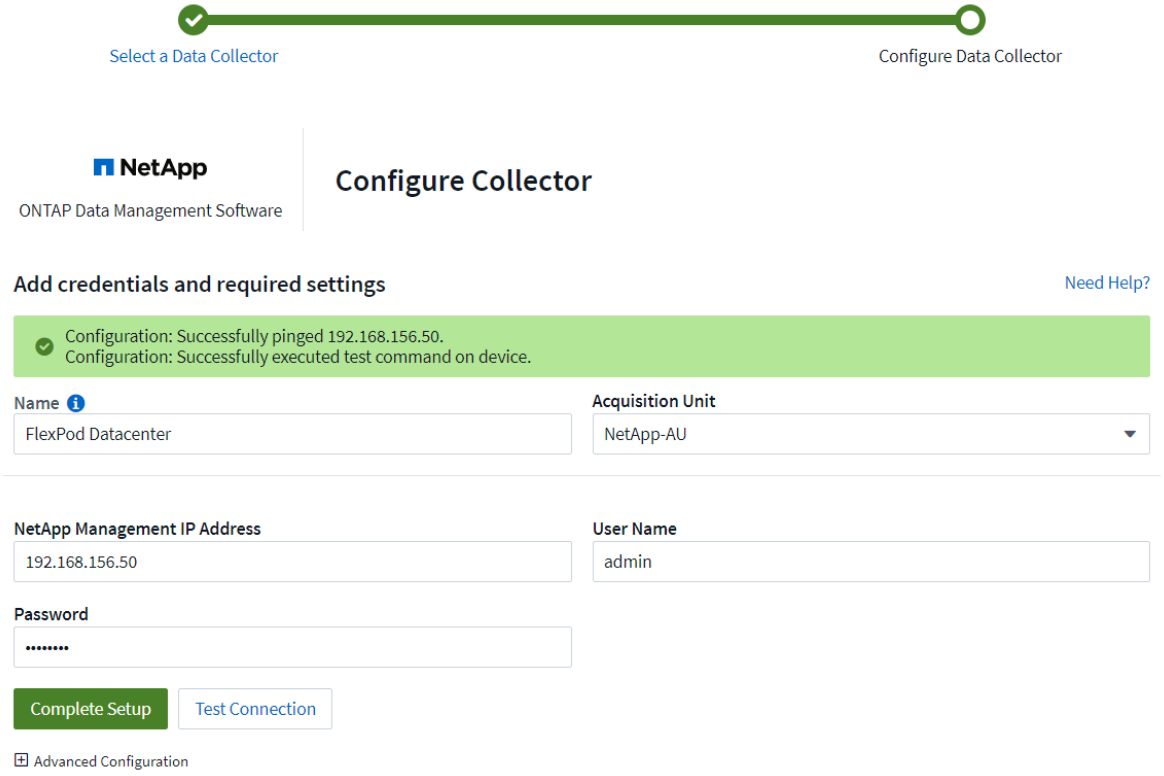


2. Per avviare una procedura guidata per aggiungere il sistema di storage, nella pagina Summary (Riepilogo), fare clic sul pulsante per creare un data collector. La prima pagina visualizza tutti i sistemi da cui è possibile raccogliere i dati. Utilizzare la barra di ricerca per cercare ONTAP.



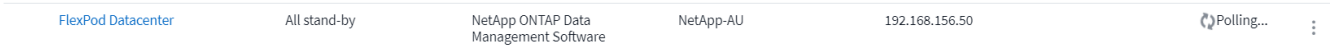
3. Selezionare il software di gestione dei dati ONTAP.

   Viene visualizzata una pagina che consente di assegnare un nome all'implementazione e selezionare l'unità di acquisizione da utilizzare. È possibile fornire le informazioni di connettività e le credenziali per il sistema ONTAP e verificare la connessione per confermare.



4. Fare clic su complete Setup (completa installazione)

   Il portale torna alla pagina Data Collector e il Data Collector inizia il primo polling per raccogliere i dati dal sistema di storage ONTAP nel data center FlexPod.



Casi di utilizzo

Con la configurazione e la configurazione di Cloud Insights per il monitoraggio della

soluzione FlexPod Datacenter, possiamo esplorare alcune delle attività che è possibile eseguire sulla dashboard per valutare e monitorare il tuo ambiente. In questa sezione, vengono evidenziati cinque casi di utilizzo principali per Cloud Insights:

- Integrazione di Active IQ
- Analisi delle dashboard in tempo reale
- Creazione di dashboard personalizzati
- Risoluzione avanzata dei problemi
- Ottimizzazione dello storage

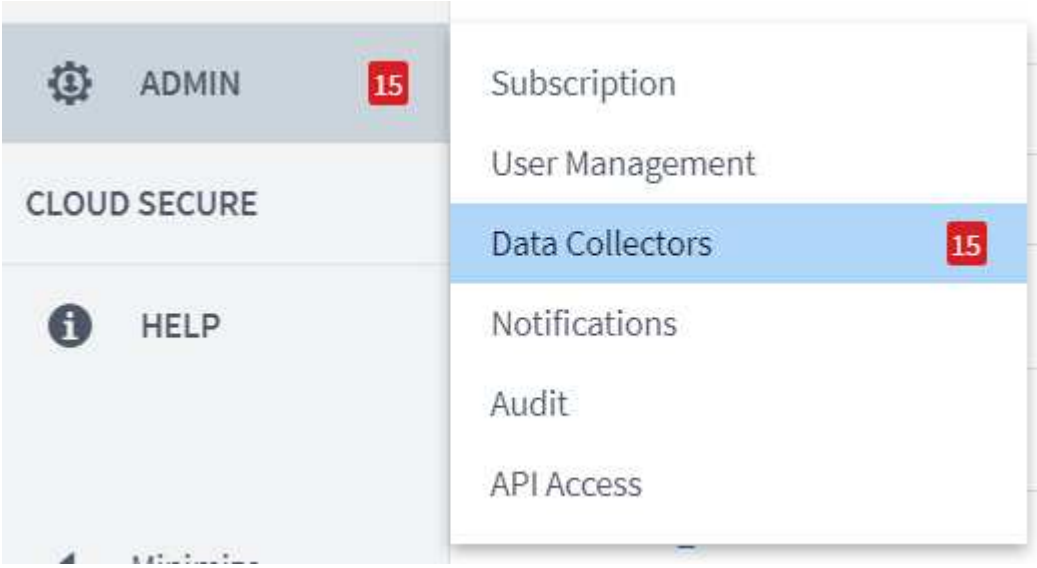
Integrazione di Active IQ

Cloud Insights è completamente integrato nella piattaforma di monitoraggio dello storage Active IQ. Un sistema ONTAP, implementato come parte di una soluzione FlexPod Datacenter, viene configurato automaticamente per inviare informazioni a NetApp attraverso la funzione AutoSupport, integrata in ciascun sistema. Questi report vengono generati in base a una pianificazione o in modo dinamico ogni volta che viene rilevato un guasto nel sistema. I dati comunicati tramite AutoSupport vengono aggregati e visualizzati in dashboard facilmente accessibili nel menu Active IQ di Cloud Insights.

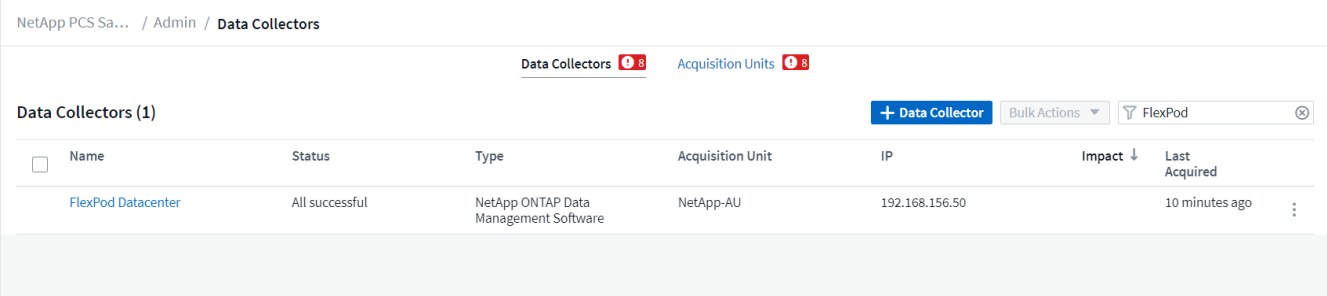
Accedere alle informazioni Active IQ dalla dashboard di Cloud Insights

Per accedere alle informazioni Active IQ dalla dashboard di Cloud Insights, attenersi alla seguente procedura:

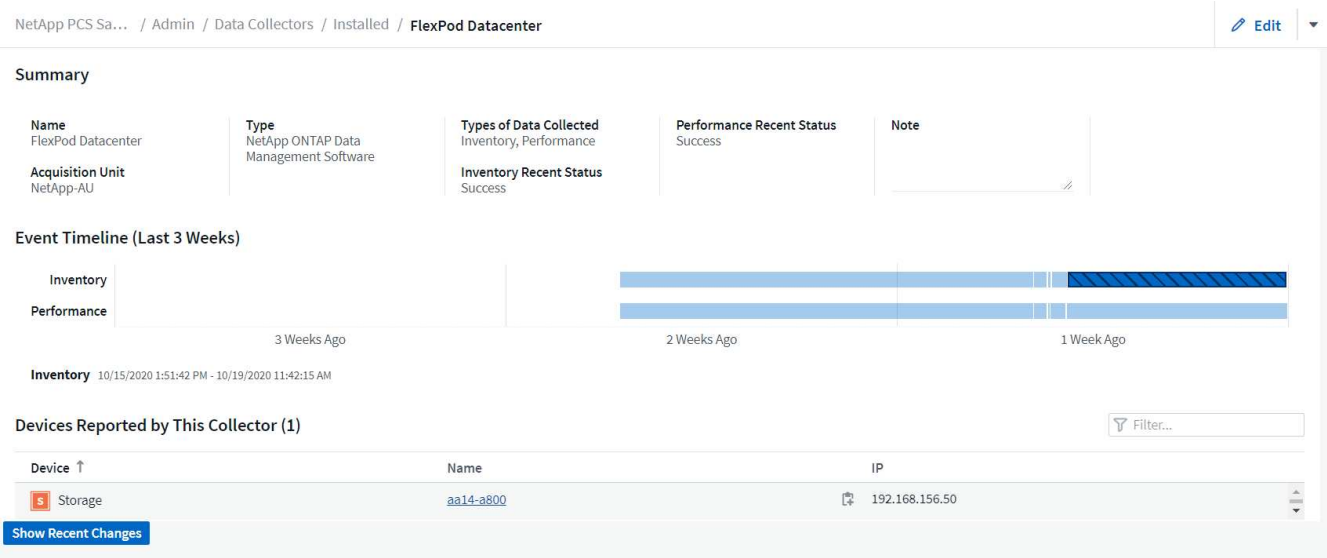
1. Fare clic sull'opzione Data Collector (raccolta dati) nel menu Admin (Amministrazione) a sinistra.



2. Filtro per il Data Collector specifico nel tuo ambiente. In questo esempio, filtriamo in base al termine FlexPod.

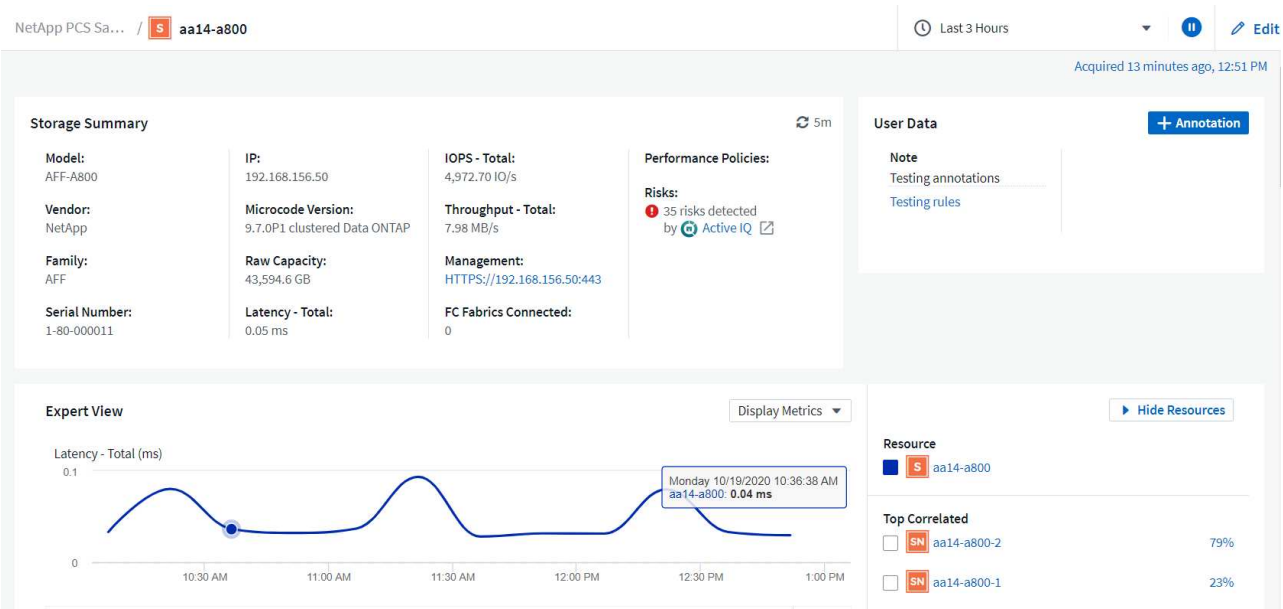


3. Fare clic su Data Collector per visualizzare un riepilogo dell'ambiente e dei dispositivi monitorati da tale collector.

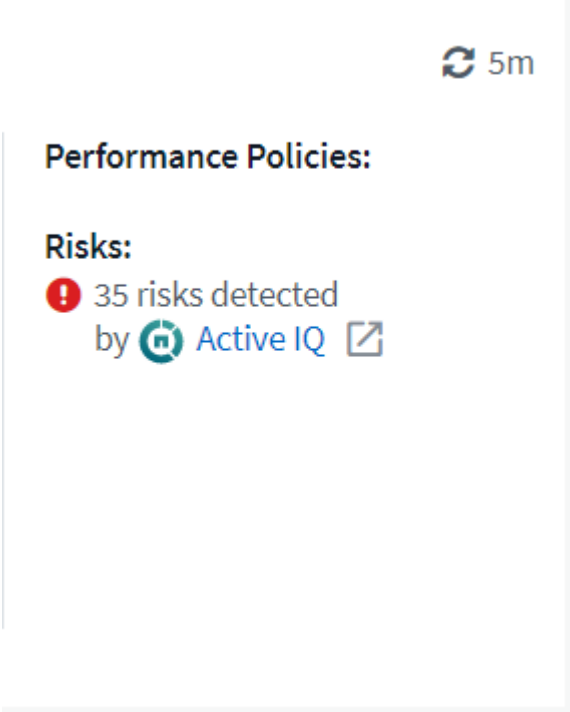


Nell'elenco dei dispositivi in basso, fare clic sul nome del sistema di storage ONTAP monitorato. Viene visualizzata una dashboard contenente le informazioni raccolte sul sistema, inclusi i seguenti dettagli:

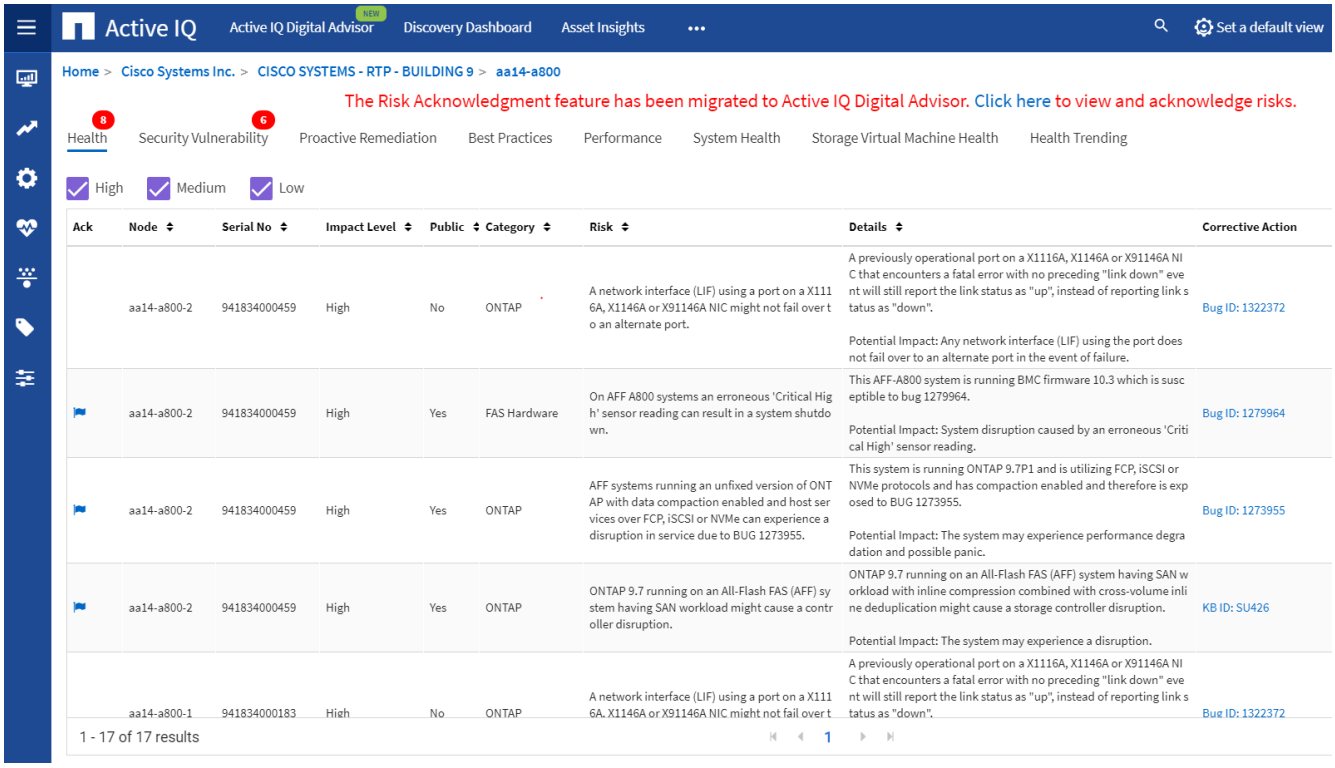
- Modello
- Famiglia
- Versione di ONTAP
- Capacità raw
- IOPS medi
- Latenza media
- Throughput medio



Inoltre, in questa pagina, nella sezione Criteri di performance, è disponibile un link a NetApp Active IQ.



4. Per aprire una nuova scheda del browser e accedere alla pagina di riduzione dei rischi, che mostra quali nodi sono interessati, quanto critici sono i rischi e quali sono le azioni appropriate da intraprendere per correggere i problemi identificati, fare clic sul link per Active IQ.

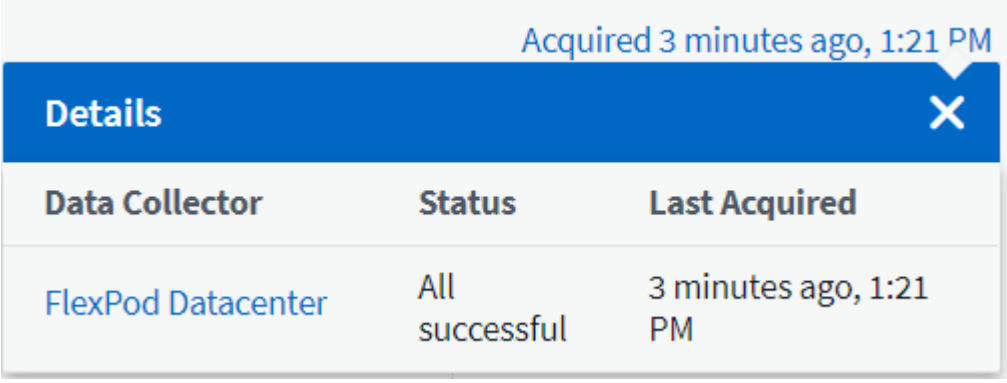


Esplora le dashboard in tempo reale

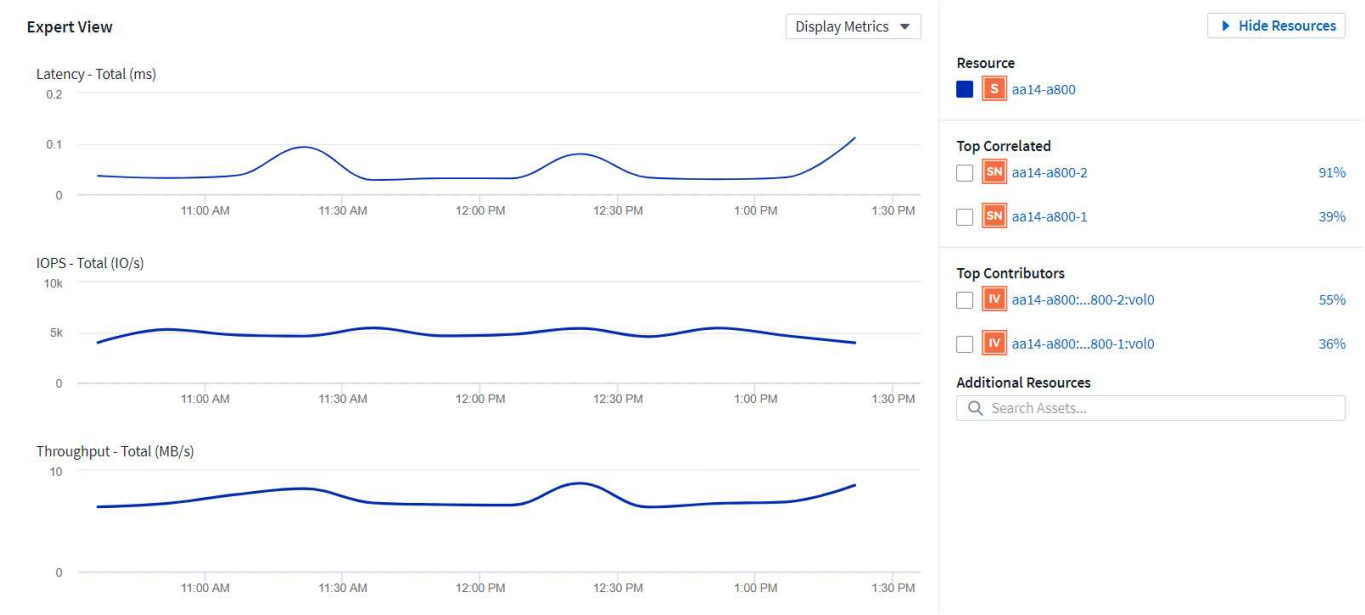
Cloud Insights può visualizzare dashboard in tempo reale delle informazioni raccolte dal sistema di storage ONTAP implementato in una soluzione FlexPod per data center. L'unità di acquisizione Cloud Insights raccoglie i dati a intervalli regolari e compila il dashboard del sistema di storage predefinito con le informazioni raccolte.

Accedi ai grafici in tempo reale dalla dashboard di Cloud Insights

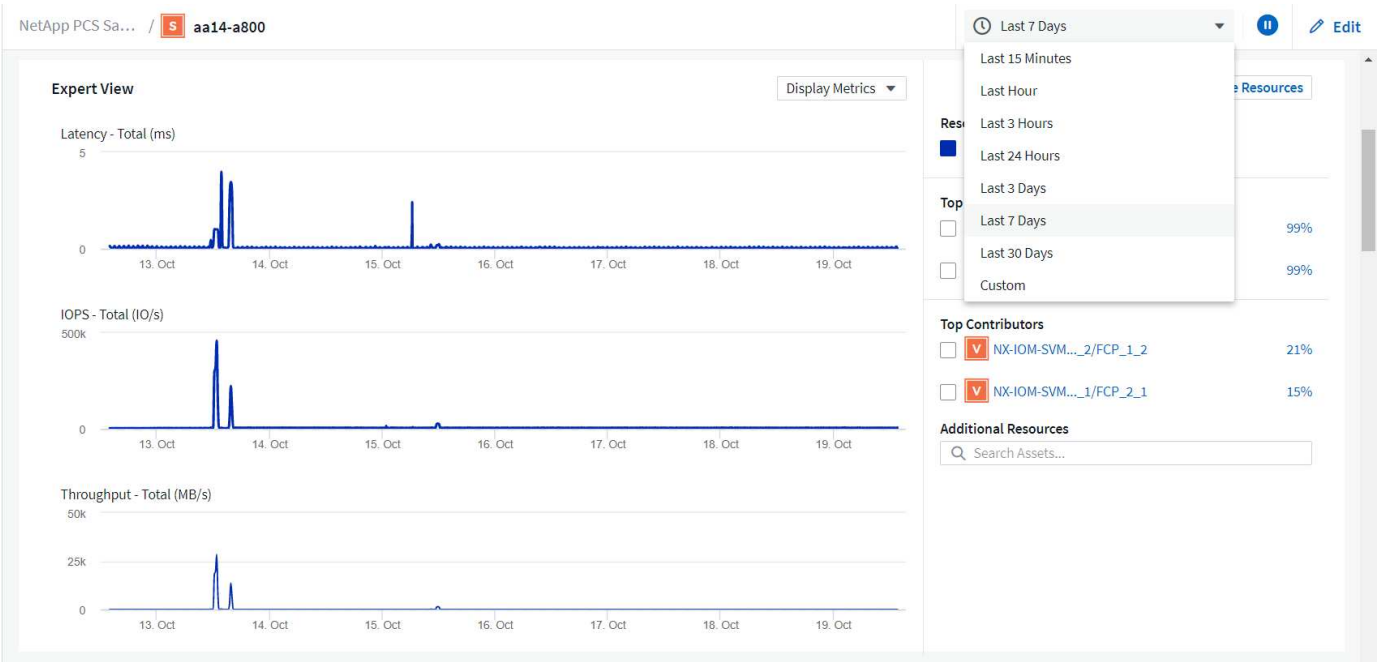
Dalla dashboard del sistema di storage, è possibile visualizzare l'ultima volta che Data Collector ha aggiornato le informazioni. Un esempio è illustrato nella figura seguente.



Per impostazione predefinita, la dashboard del sistema di storage visualizza diversi grafici interattivi che mostrano le metriche a livello di sistema dal sistema di storage sottoposto a polling o da ogni singolo nodo, tra cui latenza, IOPS e throughput, nella sezione visualizzazione avanzata. Esempi di questi grafici predefiniti sono illustrati nella figura seguente.



Per impostazione predefinita, i grafici mostrano le informazioni delle ultime tre ore, ma è possibile impostarle su un numero di valori diversi o su un valore personalizzato dall'elenco a discesa in alto a destra nella dashboard del sistema di storage. Questo è mostrato nella figura seguente.



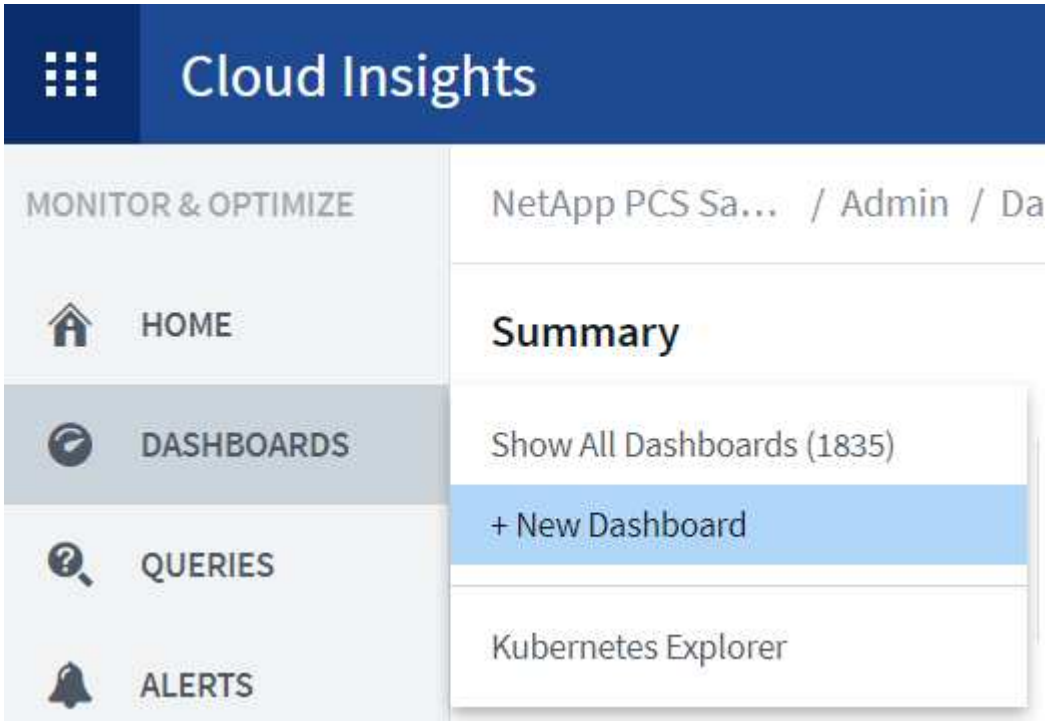
Creare dashboard personalizzati

Oltre a utilizzare i dashboard predefiniti che visualizzano informazioni a livello di sistema, è possibile utilizzare Cloud Insights per creare dashboard completamente personalizzati che consentono di concentrarsi sull'utilizzo delle risorse per volumi di storage specifici nella soluzione FlexPod Datacenter, e quindi le applicazioni implementate nell'infrastruttura convergente che dipendono da questi volumi per funzionare in modo efficace. In questo modo è possibile creare una migliore visualizzazione di applicazioni specifiche e delle risorse che consumano nell'ambiente del data center.

Creare una dashboard personalizzata per valutare le risorse di storage

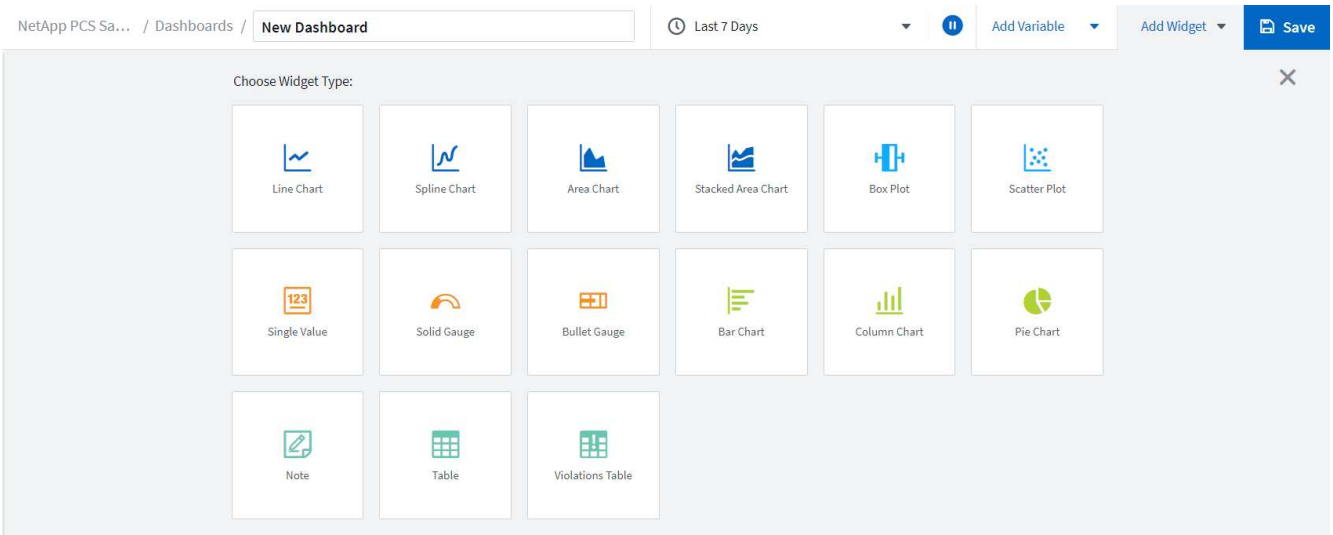
Per creare una dashboard personalizzata per la valutazione delle risorse di storage, attenersi alla seguente procedura:

1. Per creare una dashboard personalizzata, passare il mouse su dashboard nel menu principale di Cloud Insights e fare clic su + nuovo dashboard nell'elenco a discesa.



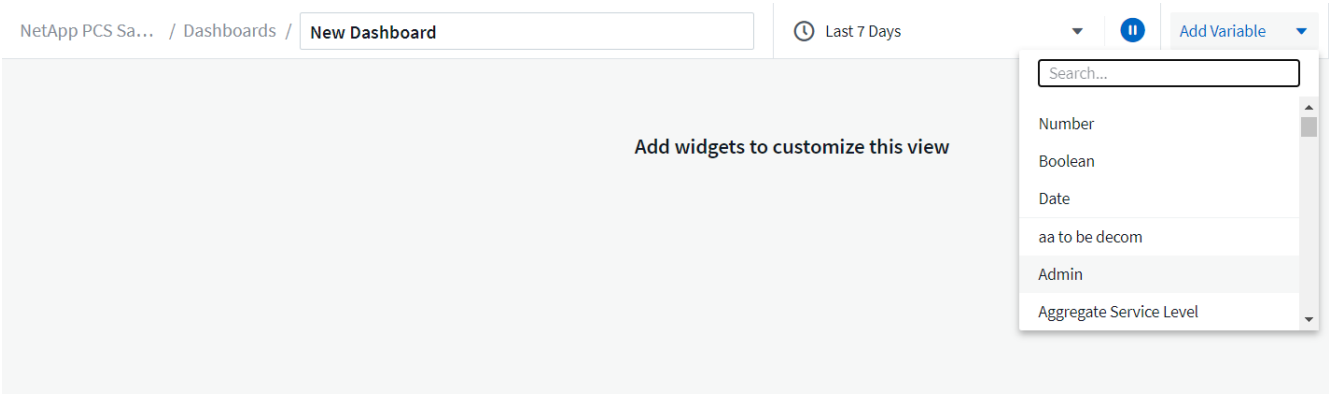
   Viene visualizzata la finestra New Dashboard (nuovo dashboard).

2. Assegnare un nome alla dashboard e selezionare il tipo di widget utilizzato per visualizzare i dati. È possibile scegliere tra diversi tipi di grafici o persino note o tipi di tabelle per visualizzare i dati raccolti.



3. Scegliere variabili personalizzate dal menu Aggiungi variabile.

   In questo modo, i dati presentati sono incentrati sulla visualizzazione di fattori più specifici o specializzati.



4. Per creare una dashboard personalizzata, selezionare il tipo di widget che si desidera utilizzare, ad esempio un grafico a torta per visualizzare l'utilizzo dello storage in base al volume:

   a. Selezionare il widget grafico a torta dall'elenco a discesa Aggiungi widget.

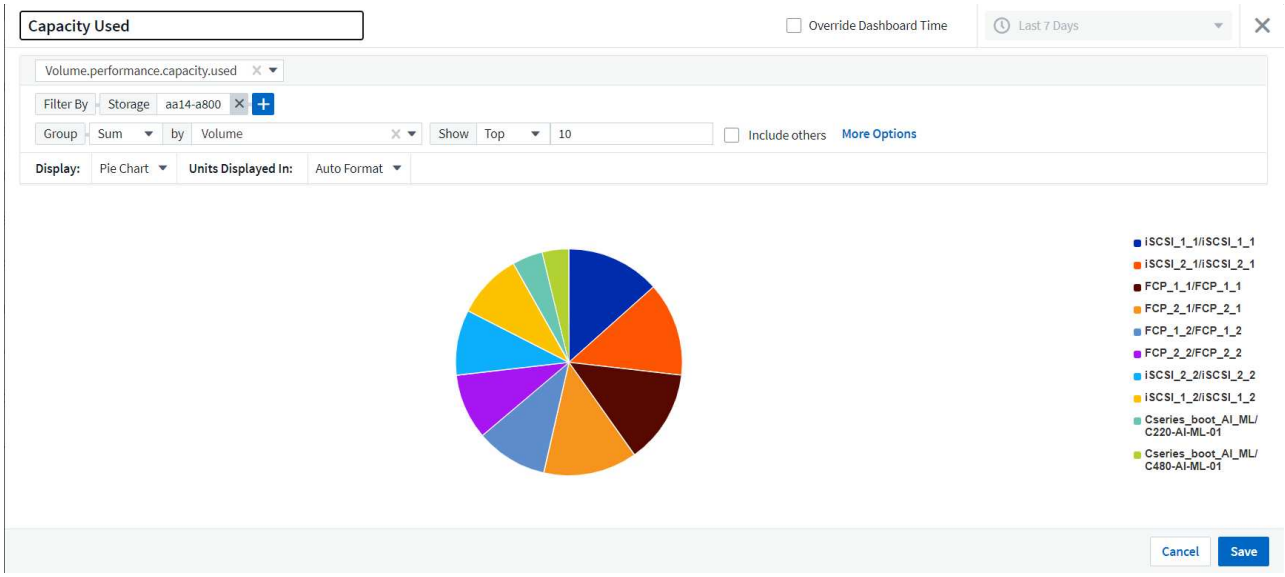
   b. Assegnare un nome al widget con un identificatore descrittivo, ad esempio `Capacity Used`.

   c. Selezionare l'oggetto che si desidera visualizzare. Ad esempio, è possibile effettuare una ricerca in base al volume dei termini chiave e selezionare `volume.performance.capacity.used`.

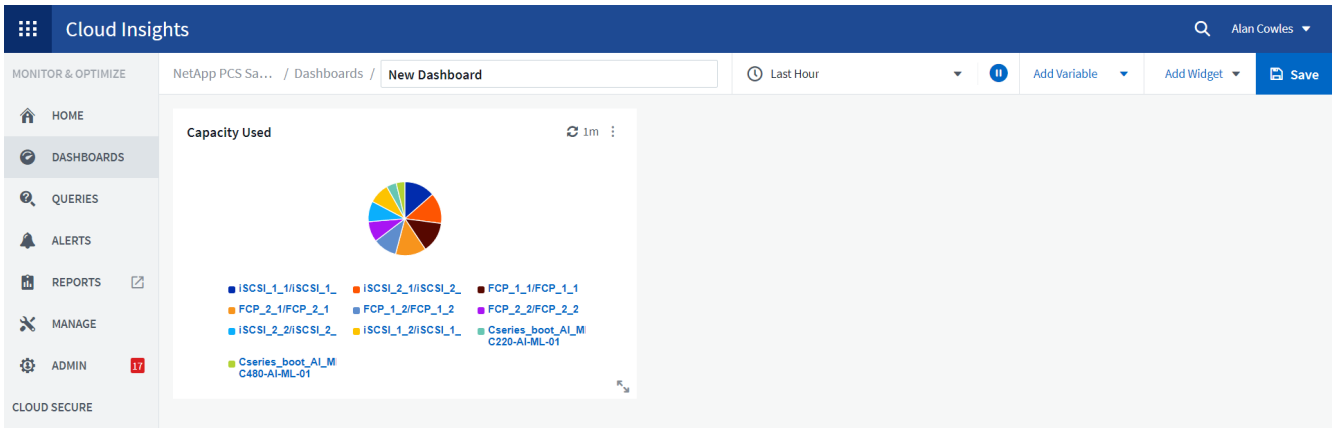
   d. Per filtrare in base ai sistemi storage, utilizzare il filtro e digitare il nome del sistema storage nella soluzione FlexPod Datacenter.

   e. Personalizzare le informazioni da visualizzare. Per impostazione predefinita, questa selezione mostra i volumi di dati ONTAP ed elenca i primi 10 volumi.

   f. Per salvare la dashboard personalizzata, fare clic sul pulsante Save (Salva).



   Dopo aver salvato il widget personalizzato, il browser torna alla pagina New Dashboard, dove viene visualizzato il widget appena creato e consente di eseguire azioni interattive, come la modifica del periodo di polling dei dati.



Risoluzione avanzata dei problemi

Cloud Insights consente di applicare metodi avanzati di troubleshooting a qualsiasi ambiente di storage in un'infrastruttura convergente FlexPod Datacenter. Utilizzando i componenti di ciascuna delle funzionalità menzionate in precedenza: Integrazione Active IQ, dashboard predefiniti con statistiche in tempo reale e dashboard personalizzati, i problemi che potrebbero insorgere vengono rilevati in anticipo e risolti rapidamente. Utilizzando l'elenco dei rischi in Active IQ, un cliente può trovare errori di configurazione segnalati che potrebbero causare problemi o scoprire bug che sono stati segnalati e versioni di codice con patch che possono rimediare. L'osservazione delle dashboard in tempo reale sulla home page di Cloud Insights può aiutare a individuare modelli di performance del sistema che potrebbero essere un indicatore precoce di un problema in aumento e contribuire a risolverlo in modo rapido. Infine, la possibilità di creare dashboard personalizzati consente ai clienti di concentrarsi sulle risorse più importanti della propria infrastruttura e di monitorarle direttamente per garantire che possano raggiungere i propri obiettivi di business continuity.

Ottimizzazione dello storage

Oltre alla risoluzione dei problemi, è possibile utilizzare i dati raccolti da Cloud Insights per ottimizzare il sistema di storage ONTAP implementato in una soluzione di infrastruttura convergente per data center FlexPod. Se un volume mostra una latenza elevata, forse perché diverse macchine virtuali con esigenze di performance elevate condividono lo stesso datastore, tali informazioni vengono visualizzate nella dashboard di Cloud Insights. Con queste informazioni, un amministratore dello storage può scegliere di migrare una o più macchine virtuali su altri volumi, migrare i volumi di storage tra Tier di aggregati o tra nodi nel sistema storage ONTAP, ottenendo un ambiente ottimizzato per le performance. Le informazioni ottenute dall'integrazione di Active IQ con Cloud Insights possono evidenziare i problemi di configurazione che portano a performance inferiori a quelle previste e fornire l'azione correttiva consigliata che, se implementata, può risolvere qualsiasi problema e garantire un sistema storage ottimizzato in modo ottimale.

Video e demo

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per valutare le risorse in un ambiente on-premise "qui".

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per monitorare l'infrastruttura e impostare soglie di allarme per l'infrastruttura "qui".

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per valutare le singole applicazioni nell'ambiente "qui".

Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione sui prodotti Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Data center FlexPod

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com"

FlexPod con FabricPool - Tiering dei dati inattivi su Amazon AWS S3

TR-4801: FlexPod con FabricPool - Tiering dei dati inattivi su Amazon AWS S3

Scott Kovacs, NetApp

I prezzi dello storage flash continuano a scendere, rendendolo disponibile per carichi di lavoro e applicazioni che non erano stati precedentemente considerati candidati per lo storage flash. Tuttavia, l'utilizzo più efficiente dell'investimento nello storage è ancora di fondamentale importanza per i responsabili IT. I reparti IT continuano a essere solleciti per offrire servizi dalle performance più elevate con un aumento minimo o nullo del budget. Per aiutare a soddisfare queste esigenze, NetApp FabricPool consente di sfruttare l'economia del cloud spostando i dati utilizzati di rado dal costoso storage flash on-premise a un Tier di storage più conveniente nel cloud pubblico. Lo spostamento nel cloud dei dati con accesso non frequente libera spazio prezioso di storage flash sui sistemi AFF o FAS per offrire maggiore capacità per i carichi di lavoro business-critical al Tier flash ad elevate performance.

Questo report tecnico analizza la funzionalità di tiering dei dati FabricPool di NetApp ONTAP nel contesto di un'architettura di infrastruttura convergente FlexPod di NetApp e Cisco. Per trarre il massimo vantaggio dai concetti discussi in questo report tecnico, è necessario conoscere l'architettura dell'infrastruttura convergente del data center FlexPod e il software di storage ONTAP. Sulla base della familiarità con FlexPod e ONTAP, discutiamo di FabricPool, del suo funzionamento e di come può essere utilizzato per ottenere un utilizzo più efficiente dello storage flash on-premise. Gran parte del contenuto di questo report viene trattato in maniera più dettagliata in "TR-4598 FabricPool Best practice" E altra documentazione sui prodotti ONTAP. Il contenuto è stato condensato per un'infrastruttura FlexPod e non copre completamente tutti i casi di utilizzo di FabricPool. Tutte le funzionalità e i concetti esaminati sono disponibili in ONTAP 9.6.

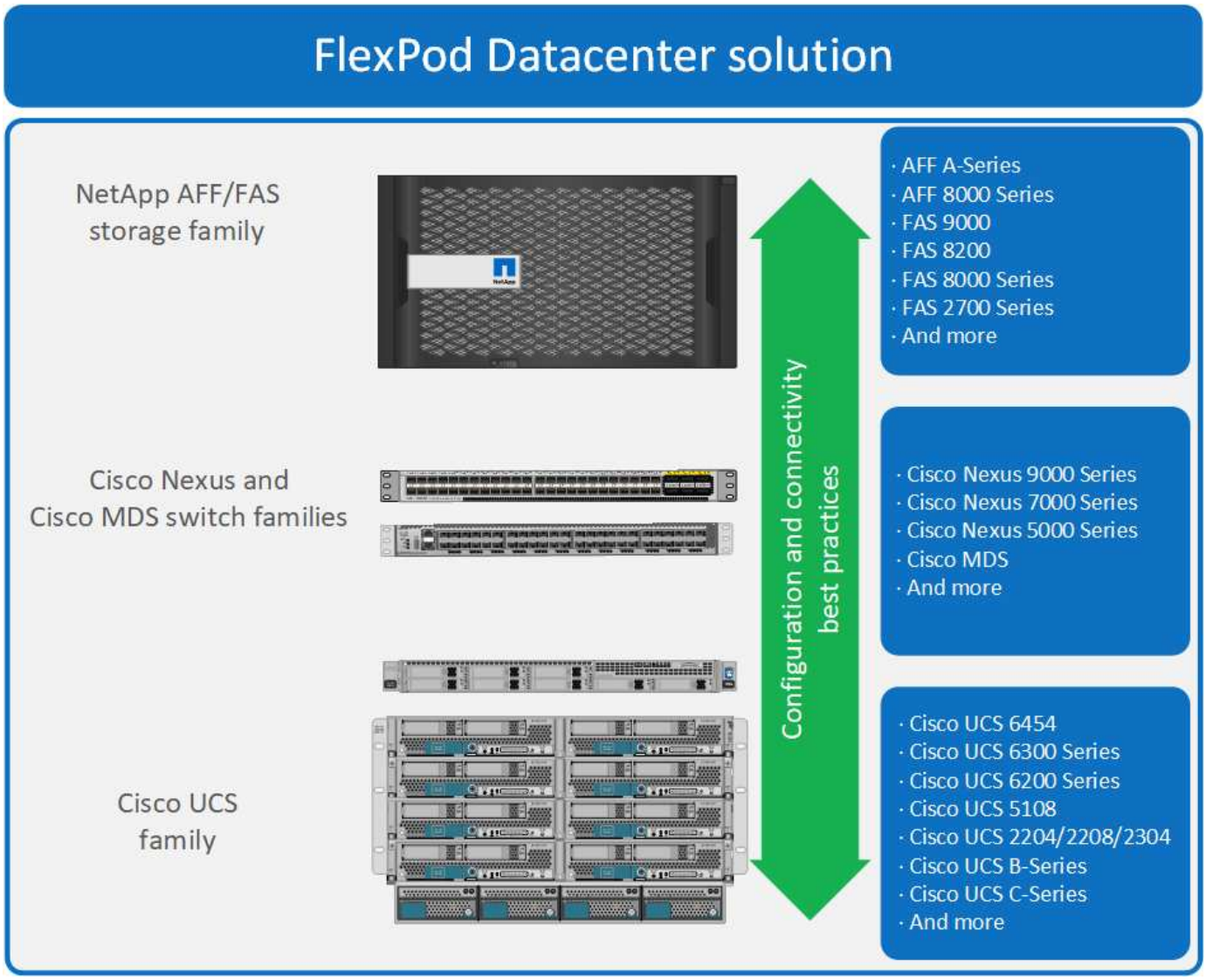
Ulteriori informazioni su FlexPod sono disponibili in "Specifiche tecniche del data center TR-4036 FlexPod".

Panoramica e architettura di FlexPod

Panoramica di FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp AFF, networking Cisco Nexus, storage networking Cisco MDS, Cisco Unified Computing System (Cisco UCS) e software VMware vSphere in un unico pacchetto. Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare più configurazioni.

Uno dei vantaggi dell'architettura FlexPod è la possibilità di personalizzare o flettere l'ambiente in base alle esigenze del cliente. Un'unità FlexPod può essere facilmente scalata in base ai requisiti e alla domanda. Un'unità può essere scalata sia in su (aggiungendo risorse a un'unità FlexPod) che in out (aggiungendo altre unità FlexPod). L'architettura di riferimento di FlexPod evidenzia la resilienza, i vantaggi in termini di costi e la facilità di implementazione di una soluzione di storage basata su Fibre Channel e IP. Un sistema storage in grado di servire più protocolli in un'unica interfaccia offre ai clienti una scelta e protegge il loro investimento perché si tratta di un'architettura wire-once. La figura seguente mostra molti dei componenti hardware di FlexPod.

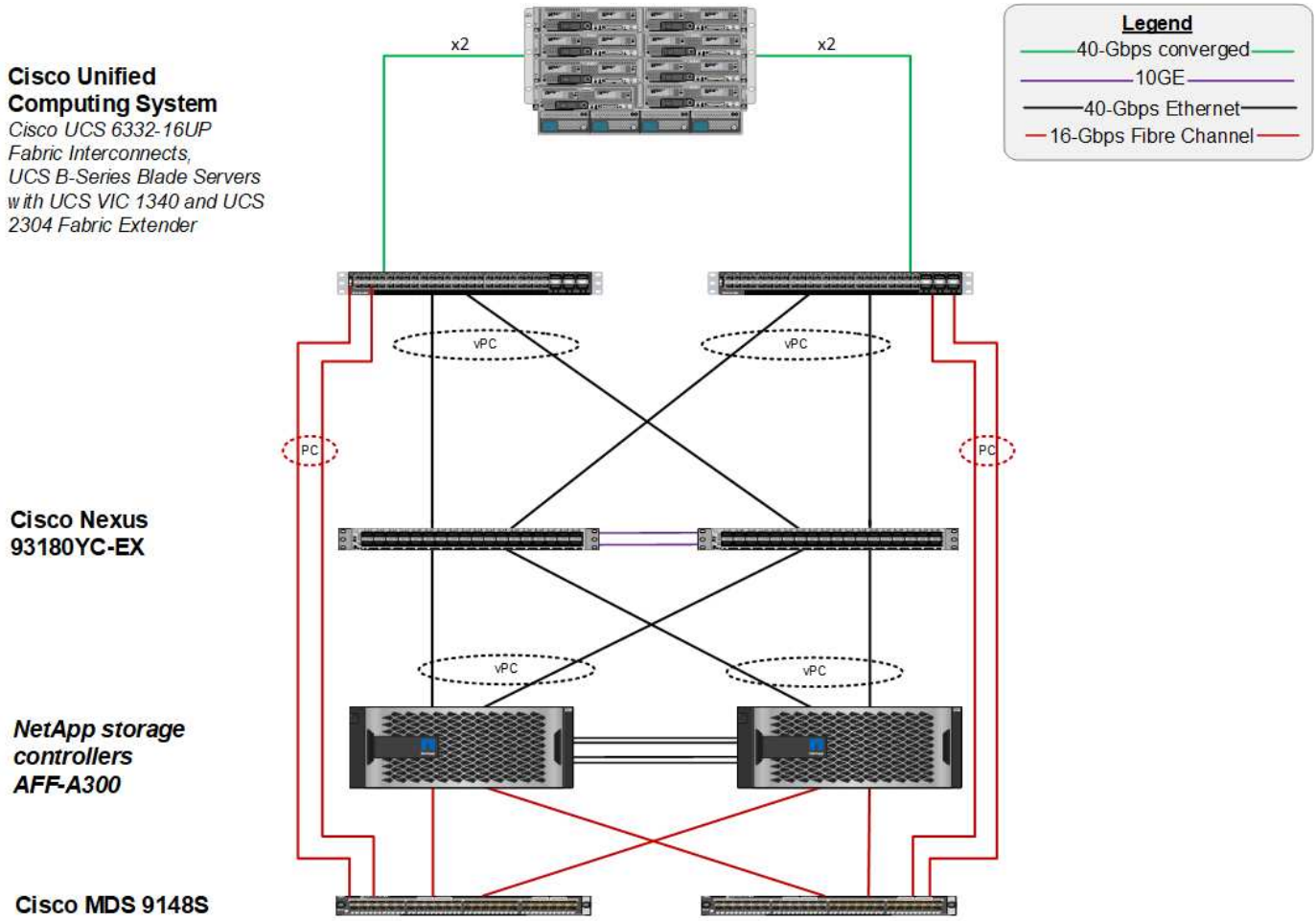


Architettura FlexPod

La figura seguente mostra i componenti di una soluzione VMware vSphere e FlexPod e le connessioni di rete necessarie per le interconnessioni fabric Cisco UCS 6454. Questo progetto ha i seguenti componenti:

- Connessioni Ethernet da 40 GB con canale di porta tra lo chassis blade Cisco UCS 5108 e le interconnessioni fabric Cisco UCS
- Connessioni Ethernet da 40 GB tra Cisco UCS Fabric Interconnect e Cisco Nexus 9000
- Connessioni Ethernet da 40 GB tra Cisco Nesxus 9000 e lo storage array NetApp AFF A300

Queste opzioni di infrastruttura sono state ampliate con l'introduzione degli switch Cisco MDS che si trovano tra l'interconnessione fabric Cisco UCS e NetApp AFF A300. Questa configurazione fornisce host con avvio FC con accesso a livello di blocco FC da 16 GB allo storage condiviso. L'architettura di riferimento rafforza la strategia wire-once, perché, con l'aggiunta di storage aggiuntivo all'architettura, non è richiesta alcuna ricablaggio dagli host all'interconnessione fabric Cisco UCS.



FabricPool

Panoramica di FabricPool

FabricPool è una soluzione di storage ibrido in ONTAP che utilizza un aggregato all-flash (SSD) come Tier di performance e un archivio di oggetti in un servizio di cloud pubblico come Tier di cloud. Questa configurazione consente lo spostamento dei dati basato su policy, a seconda che i dati siano o meno utilizzati frequentemente. FabricPool è supportato in ONTAP per aggregati AFF e all-SSD su piattaforme FAS. L'elaborazione dei dati

viene eseguita a livello di blocco, con blocchi di dati ad accesso frequente nel Tier di performance all-flash contrassegnati come blocchi a caldo e ad accesso non frequente contrassegnati come cold.

L'utilizzo di FabricPool consente di ridurre i costi dello storage senza compromettere performance, efficienza, sicurezza o protezione. FabricPool è trasparente per le applicazioni aziendali e sfrutta l'efficienza del cloud riducendo il TCO dello storage senza dover riprogettare l'infrastruttura applicativa.

FlexPod può trarre vantaggio dalle funzionalità di tiering dello storage di FabricPool per un utilizzo più efficiente dello storage flash ONTAP. Le macchine virtuali inattive (VM), i modelli di macchine virtuali utilizzati di rado e i backup delle macchine virtuali da NetApp SnapCenter per vSphere possono consumare spazio prezioso nel volume del datastore. Lo spostamento dei dati cold nel Tier cloud libera spazio e risorse per applicazioni mission-critical ad alte performance ospitate nell'infrastruttura FlexPod.

> I protocolli Fibre Channel e iSCSI in genere impiegano più tempo prima di riscontrare un timeout (da 60 a 120 secondi), ma non riprovano a stabilire una connessione nello stesso modo dei protocolli NAS. In caso di timeout di un protocollo SAN, l'applicazione deve essere riavviata. Anche una breve interruzione potrebbe essere disastrosa per le applicazioni di produzione che utilizzano i protocolli SAN perché non esiste alcun modo per garantire la connettività ai cloud pubblici. Per evitare questo problema, NetApp consiglia di utilizzare cloud privati quando si tierano i dati a cui si accede dai protocolli SAN.

In ONTAP 9.6, FabricPool si integra con tutti i principali provider di cloud pubblico: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage e Microsoft Azure Blob Storage. Questo report si concentra sullo storage Amazon AWS S3 come livello di oggetti cloud preferito.

L'aggregato composito

Un'istanza di FabricPool viene creata associando un aggregato flash ONTAP a un archivio di oggetti cloud, ad esempio un bucket AWS S3, per creare un aggregato composito. Quando i volumi vengono creati all'interno dell'aggregato composito, possono sfruttare le funzionalità di tiering di FabricPool. Quando i dati vengono scritti nel volume, ONTAP assegna una temperatura a ciascuno dei blocchi di dati. Quando il blocco viene scritto per la prima volta, viene assegnata una temperatura di caldo. Con il passare del tempo, se i dati non sono accessibili, vengono sottoposti a un processo di raffreddamento fino a quando non viene assegnato uno stato Cold. Questi blocchi di dati ad accesso non frequente vengono quindi suddivisi in tiering dall'aggregato SSD delle performance e nell'archivio di oggetti cloud.

Il periodo di tempo che intercorre tra il momento in cui un blocco viene designato come cold e il momento in cui viene spostato nello storage a oggetti cloud viene modificato dalla policy di tiering del volume in ONTAP. Un'ulteriore granularità si ottiene modificando le impostazioni di ONTAP che controllano il numero di giorni necessari per far sì che un blocco diventi freddo. I candidati per il tiering dei dati sono le snapshot dei volumi tradizionali, i backup di SnapCenter per vSphere VM e altri backup basati su Snapshot di NetApp e tutti i blocchi utilizzati di rado in un datastore vSphere, come i modelli di macchine virtuali e i dati delle macchine virtuali a cui si accede di rado.

Reporting dei dati inattivi

Il reporting dei dati inattivi (IDR) è disponibile in ONTAP per valutare la quantità di dati cold che possono essere suddivisi in più livelli da un aggregato. IDR è attivato per impostazione predefinita in ONTAP 9.6 e utilizza un criterio di raffreddamento predefinito di 31 giorni per determinare quali dati nel volume sono inattivi.

> La quantità di dati cold a più livelli dipende dai criteri di tiering impostati sul volume. Questa quantità può essere diversa dalla quantità di dati cold rilevata da IDR utilizzando il periodo di raffreddamento predefinito di 31 giorni.

Creazione di oggetti e spostamento dei dati

FabricPool lavora a livello di NetApp WAFL Block, raffreddando i blocchi, concatenandoli in oggetti storage e migrando tali oggetti a un livello cloud. Ogni oggetto FabricPool è di 4 MB ed è composto da 1,024 blocchi da 4 KB. La dimensione dell'oggetto è fissa a 4 MB in base ai consigli sulle performance dei principali cloud provider e non può essere modificata. Se i blocchi cold vengono letti e resi hot, vengono recuperati solo i blocchi richiesti nell'oggetto da 4 MB e spostati di nuovo nel Tier di performance. L'intero oggetto e l'intero file non vengono migrati di nuovo. Vengono migrati solo i blocchi necessari.

> Se ONTAP rileva un'opportunità di readhead sequenziali, richiede i blocchi dal Tier cloud prima di essere letti per migliorare le performance.

Per impostazione predefinita, i dati vengono spostati nel Tier cloud solo quando l'aggregato delle performance viene utilizzato oltre il 50%. Questa soglia può essere impostata su una percentuale inferiore per consentire lo spostamento di una minore quantità di storage dei dati sul Tier flash delle performance nel cloud. Questo potrebbe essere utile se la strategia di tiering è quella di spostare i dati cold solo quando l'aggregato si avvicina alla capacità.

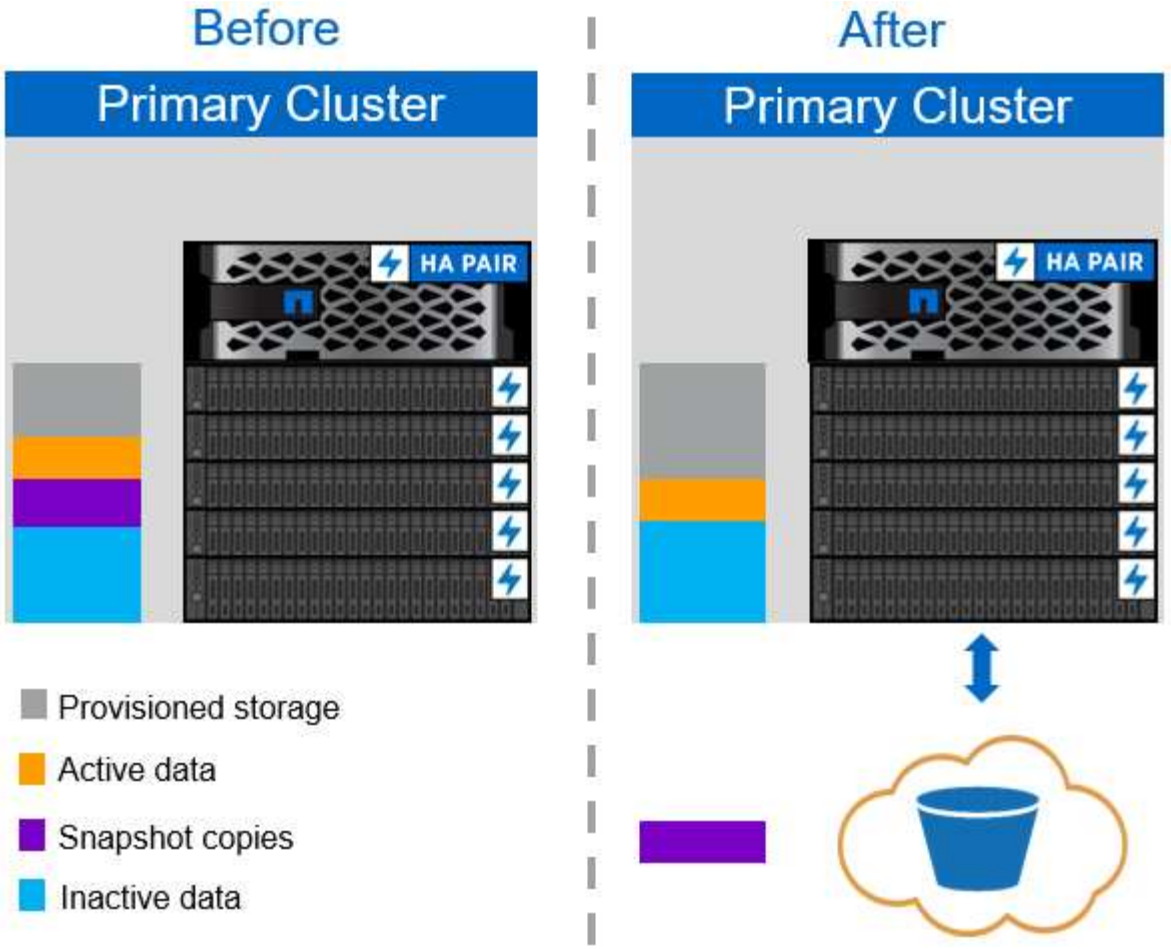
Se l'utilizzo del Tier di performance è superiore al 70% della capacità, i dati cold vengono letti direttamente dal Tier cloud senza essere riscritti nel Tier di performance. Impedendo il write-back dei dati cold su aggregati fortemente utilizzati, FabricPool preserva l'aggregato per i dati attivi.

Recuperare lo spazio del Tier di performance

Come discusso in precedenza, il caso d'utilizzo principale di FabricPool è quello di facilitare l'utilizzo più efficiente dello storage flash on-premise dalle performance elevate. I dati cold sotto forma di snapshot di volumi e backup di macchine virtuali dell'infrastruttura virtuale FlexPod possono occupare una quantità significativa di costoso storage flash. È possibile liberare lo storage Tier dalle performance preziose implementando una delle due policy di tiering: Snapshot-only o Auto.

Policy di tiering solo Snapshot

La policy di tiering Snapshot-Only, illustrata nella figura seguente, sposta i dati snapshot dei volumi cold e i backup SnapCenter per vSphere delle macchine virtuali che occupano spazio ma non condividono blocchi con il file system attivo in un archivio di oggetti cloud. La policy di tiering Snapshot-Only sposta i blocchi di dati cold nel Tier cloud. Se è necessario un ripristino, i blocchi freddi nel cloud vengono resi hot e spostati di nuovo sul Tier flash delle performance on-premise.

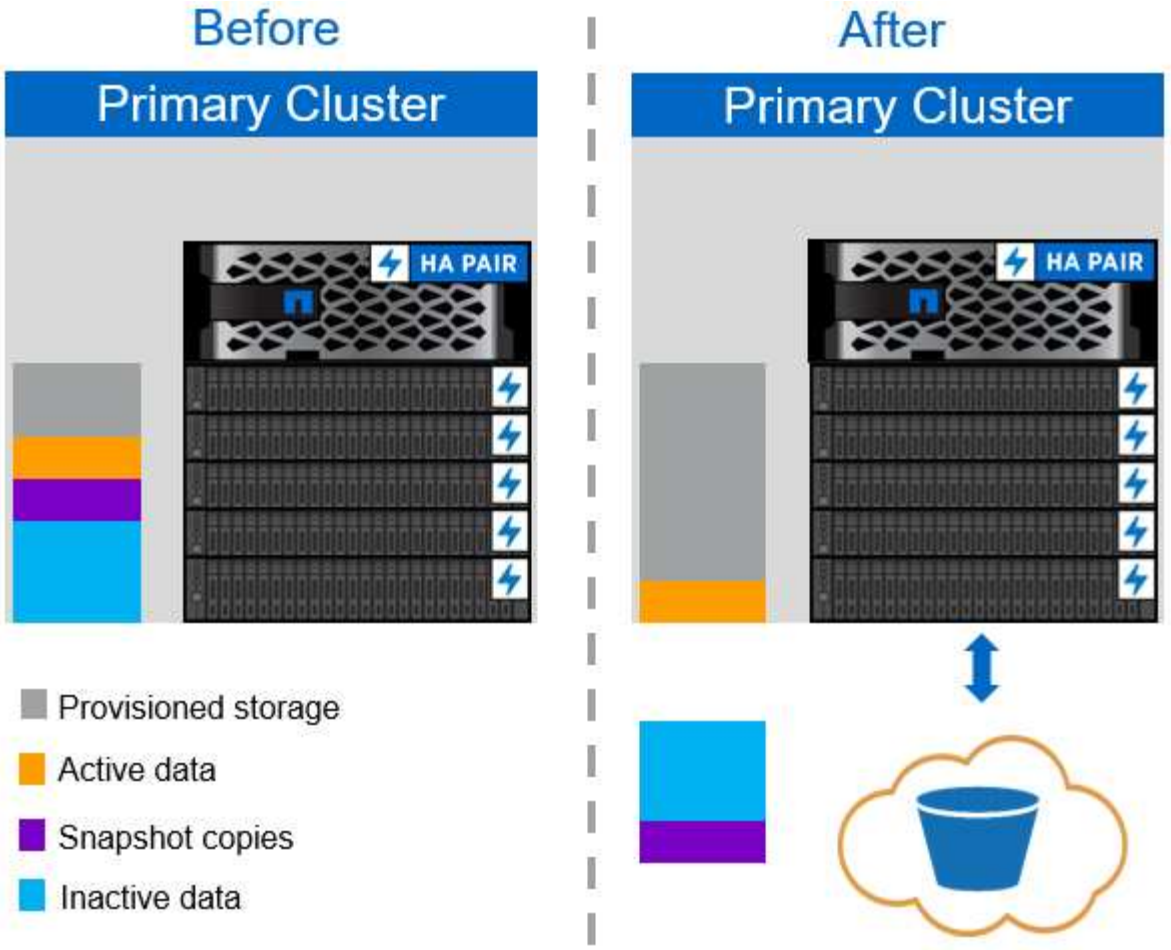


Policy di tiering automatico

La policy di tiering automatico di FabricPool, illustrata nella figura seguente, non solo sposta i blocchi di dati cold snapshot nel cloud, ma sposta anche i blocchi cold nel file system attivo. Questo può includere modelli di macchine virtuali ed eventuali dati di macchine virtuali inutilizzati nel volume dell'archivio dati. I blocchi a freddo che vengono spostati sono controllati da `tiering-minimum-cooling-days` impostazione del volume. Se un'applicazione legge casualmente i blocchi freddi nel Tier cloud, questi vengono resi hot e riportati al Tier di performance. Tuttavia, se i blocchi freddi vengono letti da un processo sequenziale come un antivirus scanner, i blocchi rimangono freddi e persistono nell'archivio di oggetti cloud; non vengono spostati di nuovo al livello di performance.

Quando si utilizza la policy di tiering automatico, i blocchi a cui si accede raramente e che vengono resi a caldo vengono ritirati dal Tier cloud alla velocità della connettività cloud. Questo può influire sulle prestazioni delle macchine virtuali se l'applicazione è sensibile alla latenza, che deve essere presa in considerazione prima di utilizzare il criterio di tiering automatico nel datastore. NetApp consiglia di posizionare le LIF Intercluster su porte con una velocità di 10 GbE per ottenere performance adeguate.

> Il profiler dell'archivio di oggetti deve essere utilizzato per verificare la latenza e il throughput nell'archivio di oggetti prima di associarlo a un aggregato FabricPool.



Policy di tiering

A differenza delle policy Auto e Snapshot-Only, la policy all tiering sposta immediatamente interi volumi di dati nel Tier cloud. Questa policy è più adatta alla protezione dei dati secondari o ai volumi di archiviazione per i quali i dati devono essere conservati per scopi storici o normativi, ma a cui si accede raramente. La policy all non è consigliata per i volumi del datastore VMware perché qualsiasi dato scritto nel datastore viene immediatamente spostato nel Tier cloud. Le successive operazioni di lettura vengono eseguite dal cloud e potrebbero potenzialmente introdurre problemi di performance per le macchine virtuali e le applicazioni che risiedono nel volume del datastore.

Sicurezza

La sicurezza è una preoccupazione centrale per il cloud e per FabricPool. Tutte le funzionalità di sicurezza native di ONTAP sono supportate nel Tier di performance e lo spostamento dei dati è protetto quando vengono trasferiti al Tier cloud. FabricPool utilizza "AES-256-GCM" algoritmo di crittografia sul tier di performance e mantiene la crittografia end-to-end nel tier cloud. I blocchi di dati spostati nell'archivio di oggetti cloud sono protetti con TLS (Transport Layer Security) v1.2 per mantenere la riservatezza e l'integrità dei dati tra i livelli di storage.

> La comunicazione con l'archivio di oggetti cloud tramite una connessione non crittografata è supportata ma non consigliata da NetApp.

Crittografia dei dati

La crittografia dei dati è fondamentale per la protezione della proprietà intellettuale, delle informazioni

commerciali e delle informazioni personali dei clienti. FabricPool supporta completamente la crittografia dei volumi NetApp (NVE) e la crittografia dello storage NetApp (NSE) per mantenere le strategie di protezione dei dati esistenti. Tutti i dati crittografati nel Tier di performance rimangono crittografati quando vengono spostati nel Tier cloud. Le chiavi di crittografia lato client sono di proprietà di ONTAP e le chiavi di crittografia dell'archivio di oggetti lato server sono di proprietà del rispettivo archivio di oggetti cloud. Tutti i dati non crittografati con NVE vengono crittografati con l'algoritmo AES-256-GCM. Non sono supportati altri tipi di crittografia AES-256.

L'utilizzo di NSE o NVE è opzionale e non è richiesto per l'utilizzo di FabricPool.

Requisiti FabricPool

FabricPool richiede ONTAP 9.2 o versione successiva e l'utilizzo di aggregati di SSD su qualsiasi piattaforma elencata in questa sezione. I requisiti FabricPool aggiuntivi dipendono dal livello cloud collegato. Per le piattaforme AFF entry-level con una capacità fissa e relativamente ridotta come NetApp AFF C190, FabricPool può essere estremamente efficace per lo spostamento dei dati inattivi nel Tier cloud.

Piattaforme

FabricPool è supportato sulle seguenti piattaforme:

- NetApp AFF
  - R800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 E AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 E FAS8040
  - FAS2750, FAS2720
  - FAS2650, FAS2620

Solo gli aggregati di SSD sulle piattaforme FAS possono utilizzare FabricPool.

- Tier cloud
  - Alibaba Cloud Object Storage Service (accesso standard e non frequente)
  - Amazon S3 (Standard, Standard-IA, One zone-IA, Intelligent-Tiering)
  - Amazon Commercial Cloud Services (C2S)
  - Google Cloud Storage (multi-regionale, regionale, nearline, coldline)
  - IBM Cloud Object Storage (Standard, Vault, Cold Vault, Flex)

- Storage Blob Microsoft Azure (caldo e freddo)

LIF di intercluster

Le coppie di cluster ad alta disponibilità (ha) che utilizzano FabricPool richiedono due interfacce logiche intercluster (LIFF) per comunicare con il livello cloud. NetApp consiglia di creare una LIF intercluster su coppie ha aggiuntive per collegare perfettamente i Tier cloud anche agli aggregati su tali nodi.

La LIF utilizzata da ONTAP per connettersi all'archivio di oggetti AWS S3 deve trovarsi su una porta a 10 Gbps.

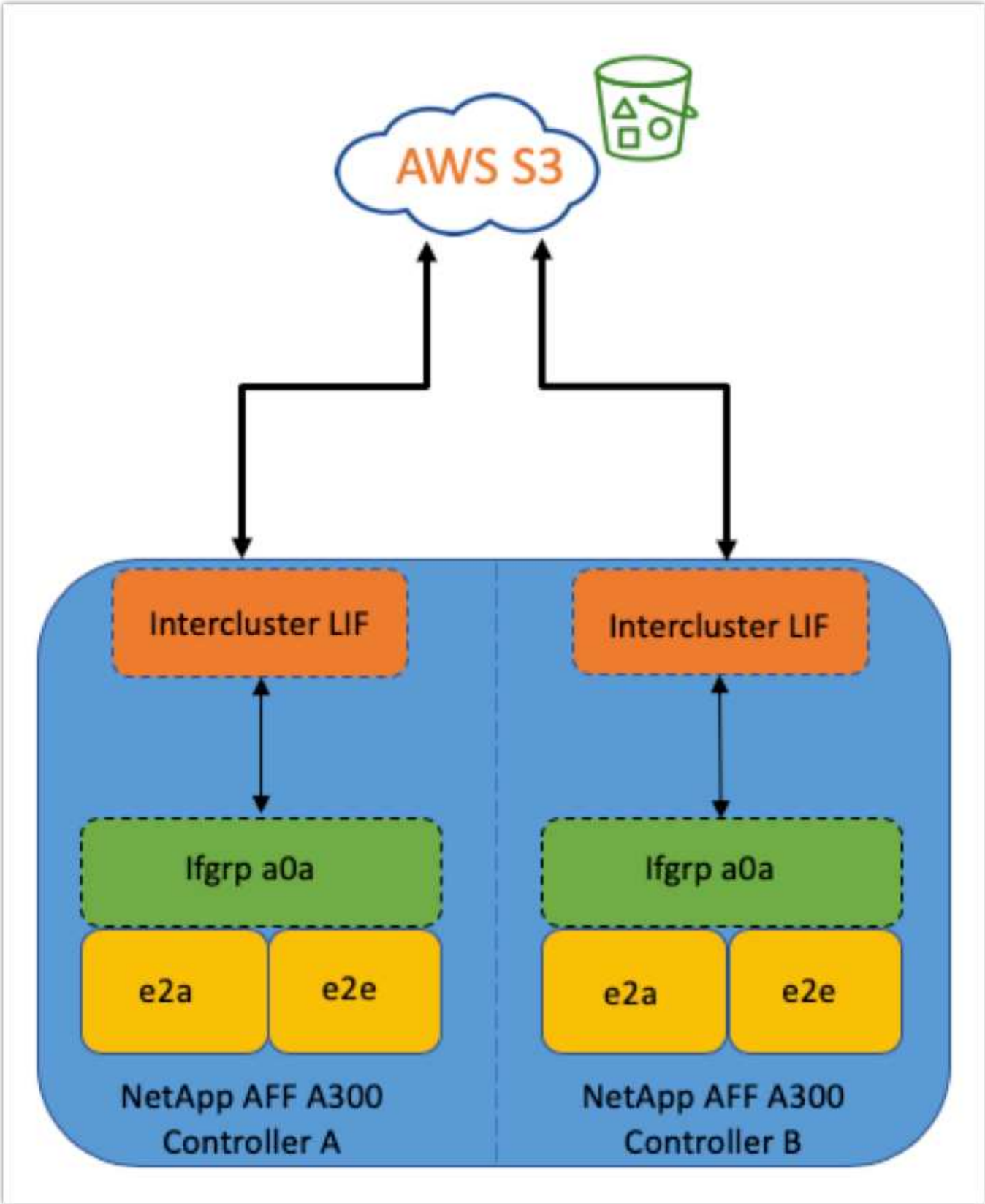
Se su un nodo con routing diverso viene utilizzato più LIF Intercluser, NetApp consiglia di inserirli in spazi IPdiversi. Durante la configurazione, FabricPool può selezionare diversi spazi IP, ma non è in grado di selezionare specifici LIF di intercluster all'interno di uno spazio IPSpace.

> La disattivazione o l'eliminazione di un LIF intercluster interrompe la comunicazione con il livello cloud.

Connettività

La latenza di lettura FabricPool è una funzione della connettività al livello cloud. Le LIF di intercluster che utilizzano porte a 10 Gbps, illustrate nella figura seguente, offrono performance adeguate. NetApp consiglia di validare la latenza e il throughput dello specifico ambiente di rete per determinare l'effetto che ha sulle performance di FabricPool.

> Quando si utilizza FabricPool in ambienti a basse performance, i requisiti minimi di performance per le applicazioni client devono continuare a essere soddisfatti e gli obiettivi dei tempi di recovery devono essere adeguati di conseguenza.



Profiler dell'archivio di oggetti

Il profiler dell'archivio di oggetti, un esempio del quale è illustrato di seguito ed è disponibile tramite l'interfaccia CLI di ONTAP, verifica la latenza e le performance di throughput degli archivi di oggetti prima che siano collegati a un aggregato FabricPool.

> Il Tier cloud deve essere aggiunto a ONTAP prima di poter essere utilizzato con il profiler dell'archivio di oggetti.

Avviare il profiler dell'archivio di oggetti dalla modalità avanzata dei privilegi in ONTAP con il seguente comando:

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Per visualizzare i risultati, eseguire il seguente comando:

```
storage aggregate object-store profiler show
```

I Tier cloud non offrono performance simili a quelle riscontrate nel Tier di performance (in genere GB al secondo). Sebbene gli aggregati FabricPool possano facilmente fornire performance simili a quelle di SATA, possono tollerare anche latenze fino a 10 secondi e un basso throughput per le soluzioni di tiering che non richiedono performance simili a quelle di SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                        min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817      69.55MB
GET     4KB        158636    0         27        1132      41        32.22MB
GET     8KB        0         0         0         0         0         0B
GET     32KB       0         0         0         0         0         0B
GET     256KB      0         0         0         0         0         0B
5 entries were displayed.
```

Volumi

Il thin provisioning dello storage è una pratica standard per l'amministratore dell'infrastruttura virtuale FlexPod. NetApp Virtual Storage Console (VSC) esegue il provisioning dei volumi di storage per gli archivi dati VMware senza alcuna garanzia di spazio (thin provisioning) e con impostazioni di efficienza dello storage ottimizzate in base alle Best practice NetApp. Se si utilizza VSC per creare datastore VMware, non è necessaria alcuna azione aggiuntiva, in quanto non è necessario assegnare alcuna garanzia di spazio al volume del datastore.

> FabricPool non può collegare un Tier cloud a un aggregato che contiene volumi utilizzando una garanzia di spazio diversa da Nessuno (ad esempio, volume).

```
volume modify -space-guarantee none
```

Impostazione di `space-guarantee none` il parametro fornisce il thin provisioning per il volume. La quantità

di spazio consumata dai volumi con questo tipo di garanzia aumenta man mano che vengono aggiunti i dati, anziché essere determinata dalla dimensione iniziale del volume. Questo approccio è essenziale per FabricPool perché il volume deve supportare i dati del Tier cloud che diventano "hot" e vengono riportati al Tier di performance.

Licensing

FabricPool richiede una licenza basata sulla capacità quando si collegano provider di storage a oggetti di terze parti (come Amazon S3) come Tier cloud per sistemi flash ibridi AFF e FAS.

Le licenze FabricPool sono disponibili in formato perpetuo o a termine (1 o 3 anni).

Il tiering al Tier cloud si interrompe quando la quantità di dati (capacità utilizzata) memorizzati nel Tier cloud raggiunge la capacità concessa in licenza. I dati aggiuntivi, incluse le copie SnapMirror sui volumi che utilizzano la policy di tiering completo, non possono essere suddivisi in più livelli fino a quando la capacità della licenza non viene aumentata. Anche se il tiering si ferma, i dati sono ancora accessibili dal Tier cloud. I dati cold aggiuntivi rimangono sugli SSD fino all'aumento della capacità concessa in licenza.

Con l'acquisto di qualsiasi nuovo cluster ONTAP 9.5 o successivo, viene fornita una licenza FabricPool a termine gratuita da 10 TB di capacità, anche se potrebbero essere applicati costi di supporto aggiuntivi. Le licenze FabricPool (inclusa la capacità aggiuntiva per le licenze esistenti) possono essere acquistate con incrementi di 1 TB.

Una licenza FabricPool può essere eliminata solo da un cluster che non contiene aggregati FabricPool.

> Le licenze FabricPool sono disponibili in tutto il cluster. L'UUID dovrebbe essere disponibile al momento dell'acquisto di una licenza (`cluster identify show`). Per ulteriori informazioni sulla licenza, fare riferimento a. "Knowledge base di NetApp".

Configurazione

Revisioni del software

La seguente tabella illustra le versioni hardware e software validate.

Layer	Dispositivo	Immagine	Commenti
Storage	NetApp AFF A300	ONTAP 9.6P2	
Calcolo	Server blade Cisco UCS B200 M5 con Cisco UCS VIC 1340	Versione 4.0(4b)	
Rete	Interconnessione fabric Cisco Nexus 6332-16UP	Versione 4.0(4b)	
	Switch Cisco Nexus 93180YC-EX in modalità standalone NX-OS	Versione 7.0(3)I7(6)	
Rete di storage	Cisco MDS 9148S	Versione 8.3(2)	

Layer	Dispositivo	Immagine	Commenti
Hypervisor		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		VMware vCenter Server	VCenter server 6.7.0.30000 build 13639309
Cloud provider		Amazon AWS S3	Bucket S3 standard con opzioni predefinite

I requisiti di base per FabricPool sono descritti nella "Requisiti FabricPool". Una volta soddisfatti tutti i requisiti di base, completare la seguente procedura per configurare FabricPool:

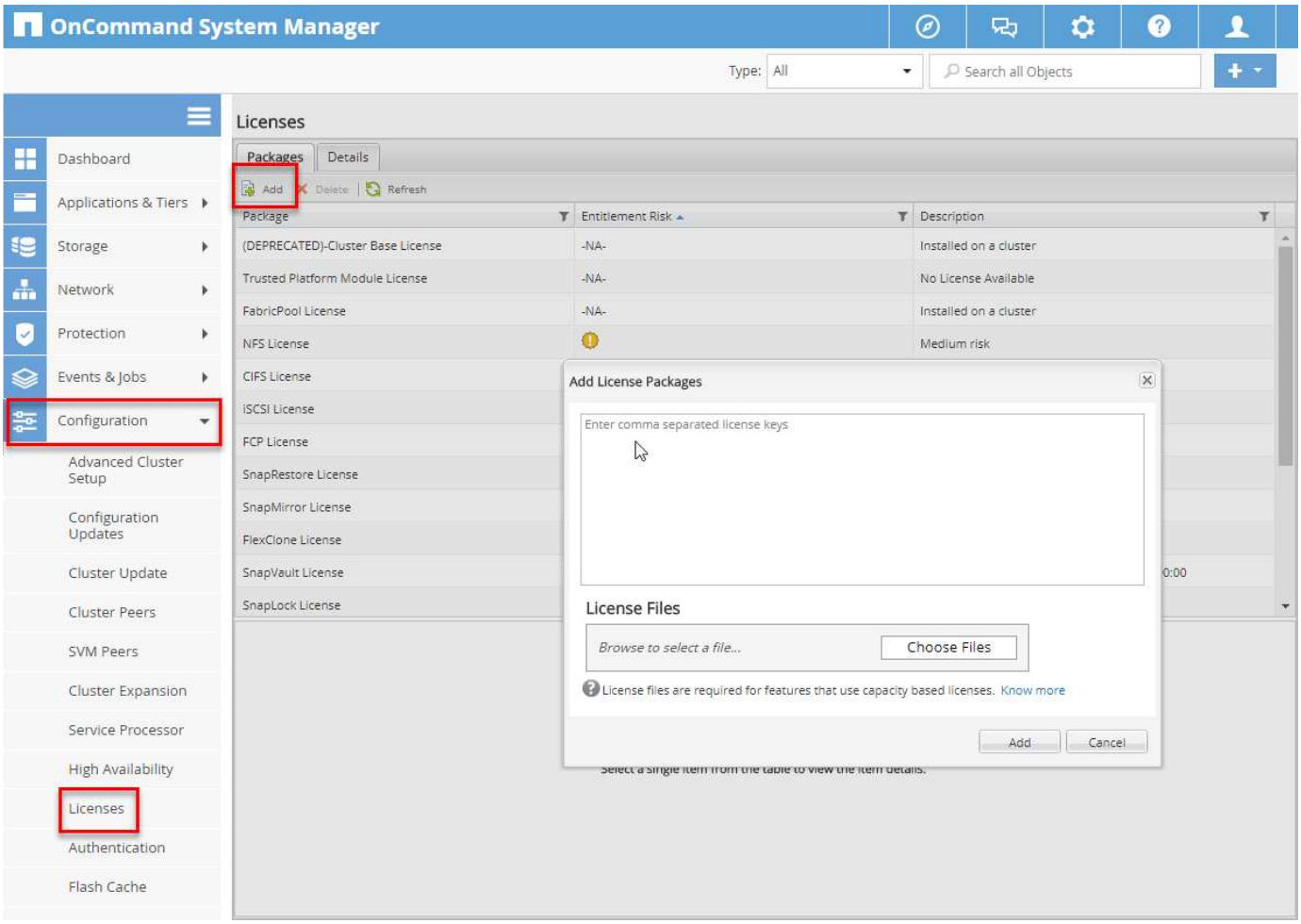
1. Installare una licenza FabricPool.
2. Creare un bucket dello store di oggetti AWS S3.
3. Aggiungi un Tier cloud a ONTAP.
4. Collegare il Tier cloud a un aggregato.
5. Impostare il criterio di tiering del volume.

"Avanti: Installare la licenza FabricPool."

Installare la licenza FabricPool

Dopo aver acquisito un file di licenza NetApp, è possibile installarlo con Gestione di sistema di OnCommand. Per installare il file di licenza, attenersi alla seguente procedura:

1. Fare clic su configurazioni.
2. Fare clic su Cluster.
3. Fare clic su licenze.
4. Fare clic su Aggiungi.
5. Fare clic su Choose Files (Scegli file) per sfogliare e selezionare un file.
6. Fare clic su Aggiungi.



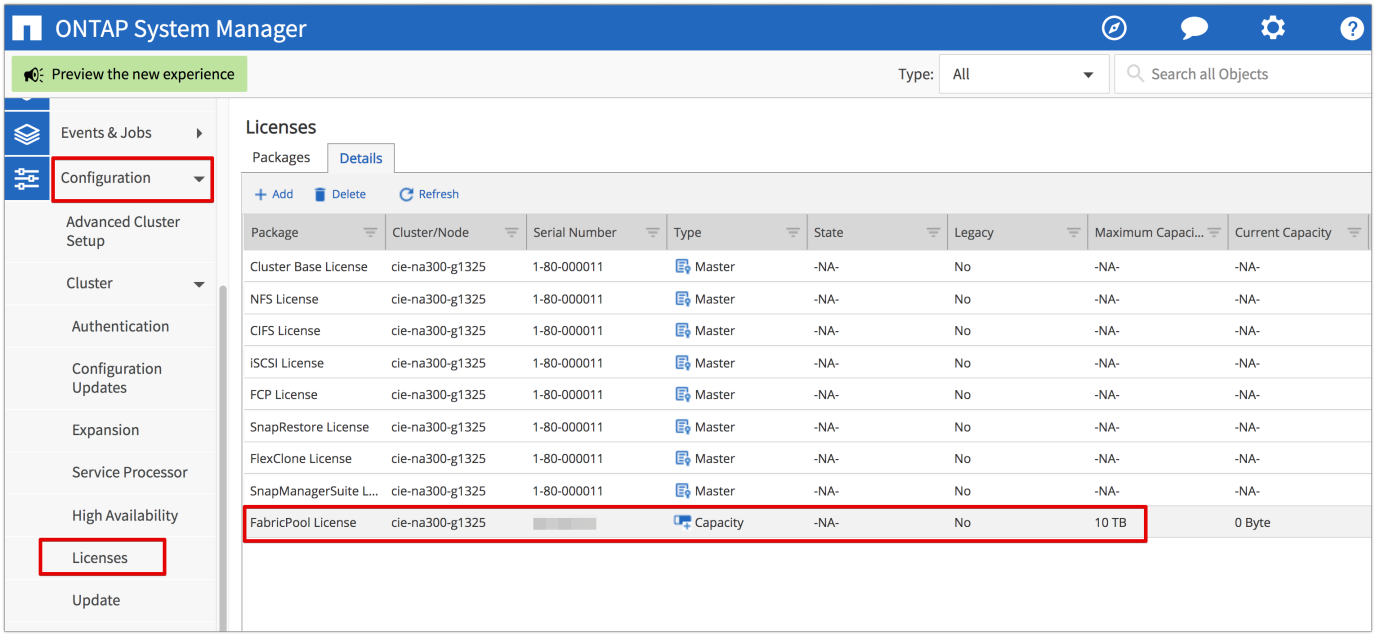
Capacità di licenza

È possibile visualizzare la capacità della licenza utilizzando l'interfaccia utente di ONTAP o Gestione di sistema di OnCommand. Per visualizzare la capacità concessa in licenza, eseguire il seguente comando nell'interfaccia utente di ONTAP:

```
system license show-status
```

In Gestore di sistema di OnCommand, attenersi alla seguente procedura:

1. Fare clic su configurazioni.
2. Fare clic su licenze.
3. Fare clic sulla scheda Dettagli.



La capacità massima e la capacità corrente sono elencate nella riga licenza FabricPool.

"Creare il bucket AWS S3."

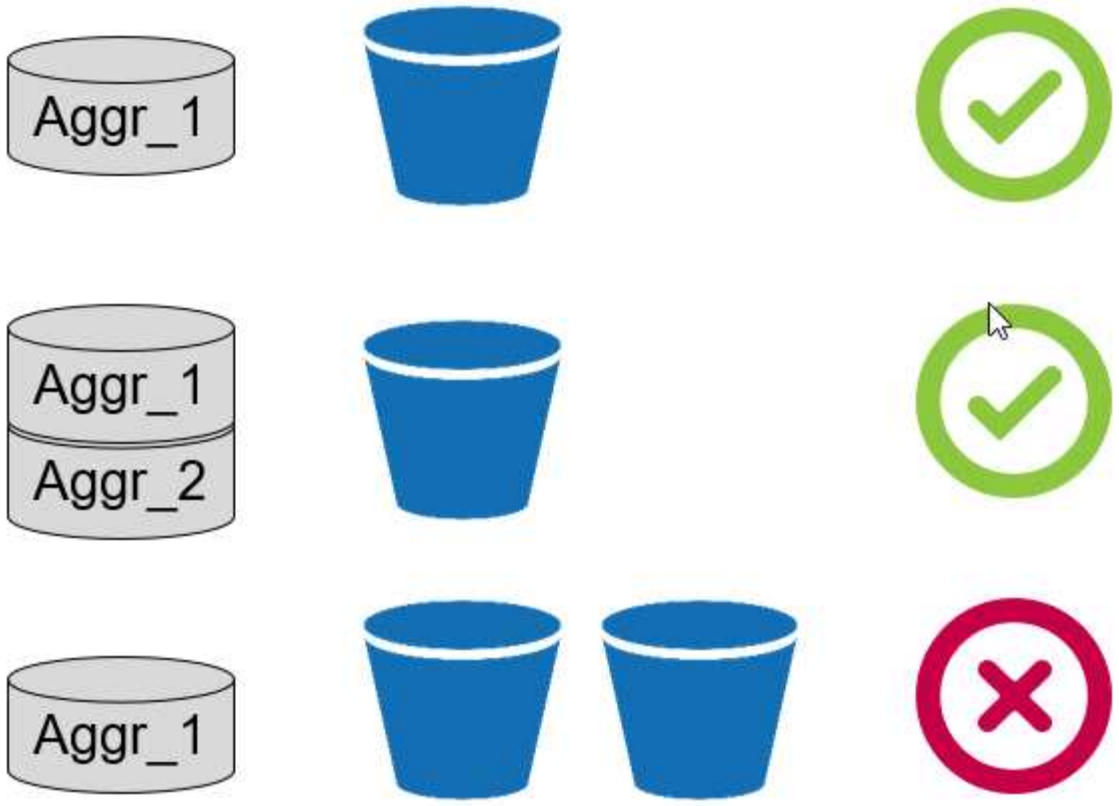
Creare il bucket AWS S3

I bucket sono contenitori di archivi di oggetti che contengono dati. È necessario fornire il nome e la posizione del bucket in cui i dati vengono memorizzati prima di poter essere aggiunti a un aggregato come Tier cloud.

> I bucket non possono essere creati utilizzando Gestione di sistema di OnCommand, Gestore unificato di OnCommand o ONTAP.

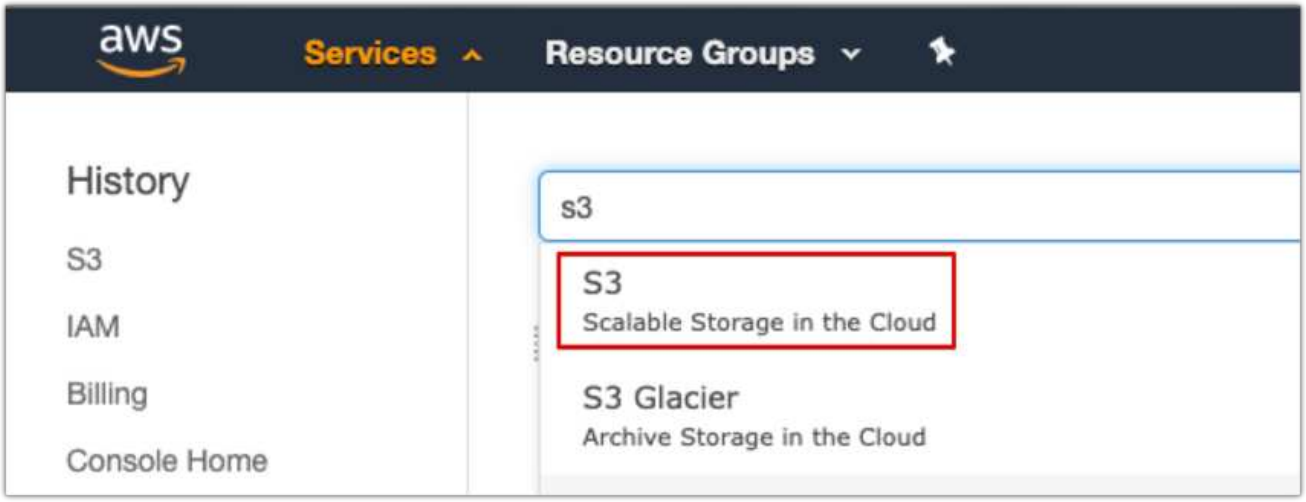
FabricPool supporta l'attacco di un bucket per aggregato, come illustrato nella figura seguente. Un singolo bucket può essere collegato a un singolo aggregato e un singolo bucket può essere collegato a più aggregati. Tuttavia, un singolo aggregato non può essere collegato a più bucket. Sebbene sia possibile collegare un singolo bucket a più aggregati in un cluster, NetApp sconsiglia di collegare un singolo bucket ad aggregati in più cluster.

Quando si pianifica un'architettura di storage, considerare come la relazione bucket-to-aggregate potrebbe influire sulle performance. Molti provider di archivi di oggetti impostano un numero massimo di IOPS supportati a livello di bucket o container. Gli ambienti che richiedono le massime performance devono utilizzare più bucket per ridurre la possibilità che le limitazioni IOPS dello storage a oggetti possano influire sulle performance di più aggregati FabricPool. Collegare un singolo bucket o container a tutti gli aggregati FabricPool in un cluster potrebbe essere più vantaggioso per gli ambienti che apprezzano la gestibilità rispetto alle performance di livello cloud.

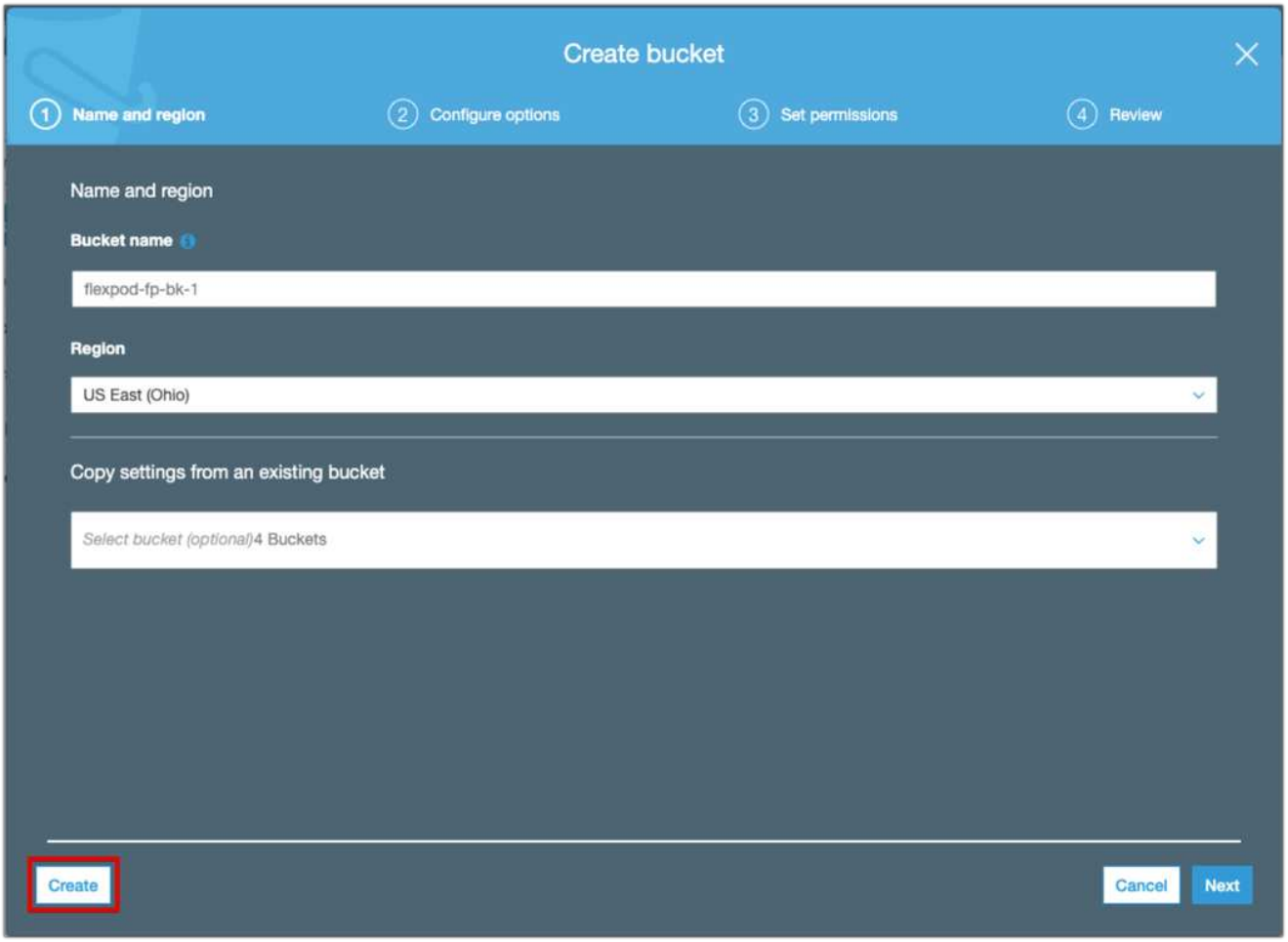


Creare un bucket S3

1. Nella console di gestione AWS dalla home page, immettere S3 nella barra di ricerca.
2. Seleziona lo storage scalabile S3 nel cloud.



3. Nella home page di S3, selezionare Create Bucket (Crea bucket).
4. Immettere un nome conforme al DNS e scegliere la regione in cui creare il bucket.



5. Fare clic su Create (Crea) per creare il bucket dell'archivio di oggetti.

"Avanti: Aggiungi un Tier cloud a ONTAP"

Aggiungi un Tier cloud a ONTAP

Prima di poter collegare un archivio di oggetti a un aggregato, è necessario aggiungerlo e identificarlo da ONTAP. Questa attività può essere completata con Gestore di sistema di OnCommand o l'interfaccia utente di ONTAP.

FabricPool supporta Amazon S3, storage cloud a oggetti IBM e archivi di oggetti storage blob Microsoft Azure come Tier cloud.

Sono necessarie le seguenti informazioni:

- Nome del server (FQDN); ad esempio, `s3.amazonaws.com`
- ID chiave di accesso
- Chiave segreta
- Nome del container (nome del bucket)

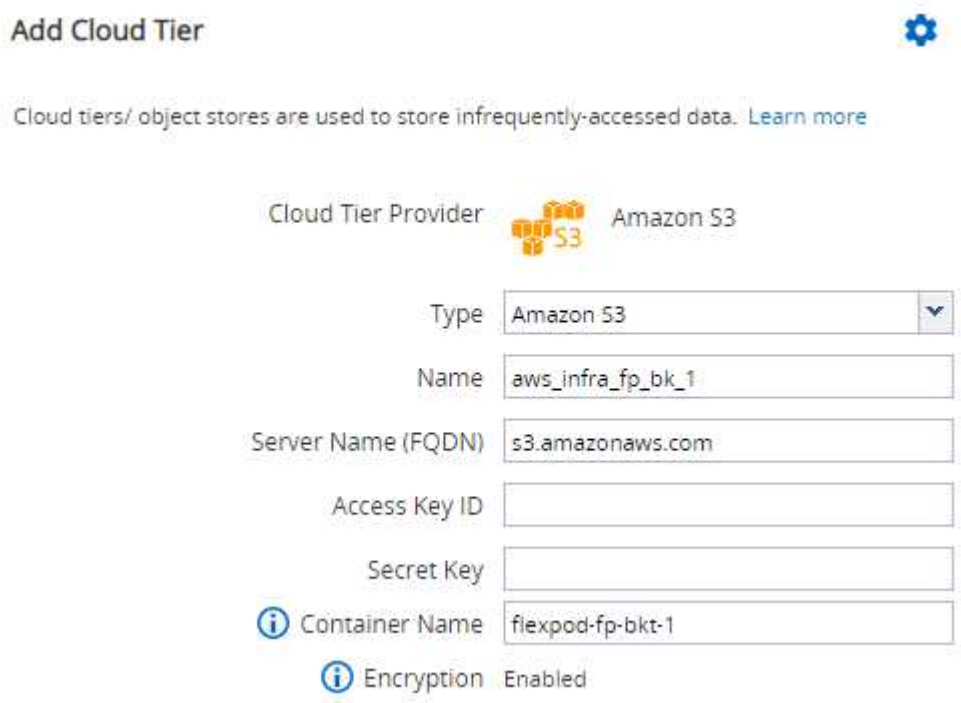
Gestore di sistema di OnCommand

Per aggiungere un livello cloud con Gestione di sistema OnCommand, attenersi alla seguente procedura:

1. Avviare Gestore di sistema di OnCommand.
2. Fare clic su Storage (archiviazione)
3. Fare clic su aggregati e dischi.
4. Fare clic su livelli cloud.
5. Selezionare un provider di archivi di oggetti.
6. Completare i campi di testo richiesti per il provider dell'archivio di oggetti.

   Nel campo Container Name (Nome contenitore), immettere il nome del bucket o del container dell'archivio di oggetti.

7. Fare clic su Save and Allega aggregati.



CLI ONTAP

Per aggiungere un livello cloud con l'interfaccia utente di ONTAP, immettere i seguenti comandi:

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Successivo: Collega un Tier cloud a un aggregato ONTAP."

Collegare un Tier cloud a un aggregato ONTAP

Una volta aggiunto e identificato da ONTAP, un archivio di oggetti deve essere collegato a un aggregato per creare un FabricPool. Questa attività può essere completata utilizzando Gestore di sistema di OnCommand o l'interfaccia utente di ONTAP.

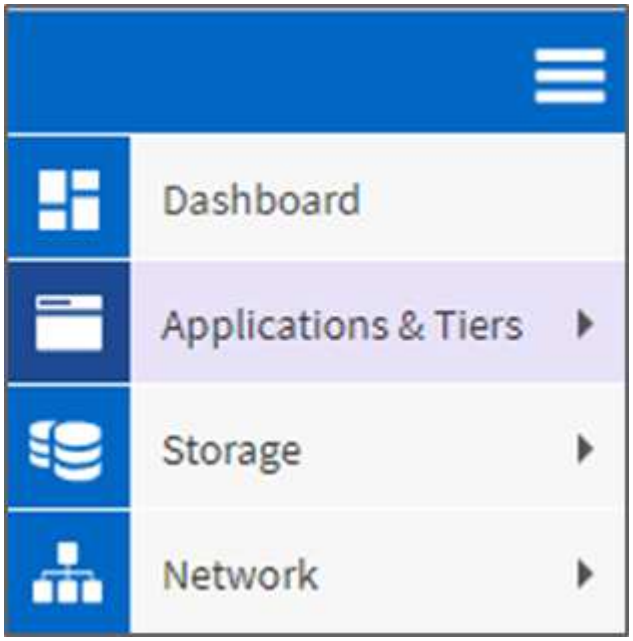
È possibile collegare più di un tipo di archivio di oggetti a un cluster, ma è possibile collegare un solo tipo di archivio di oggetti a ciascun aggregato. Ad esempio, un aggregato può utilizzare Google Cloud e un altro aggregato può utilizzare Amazon S3, ma un aggregato non può essere associato a entrambi.

> Collegare un Tier cloud a un aggregato è un'azione permanente. Un Tier cloud non può essere disconnesso da un aggregato a cui è stato collegato.

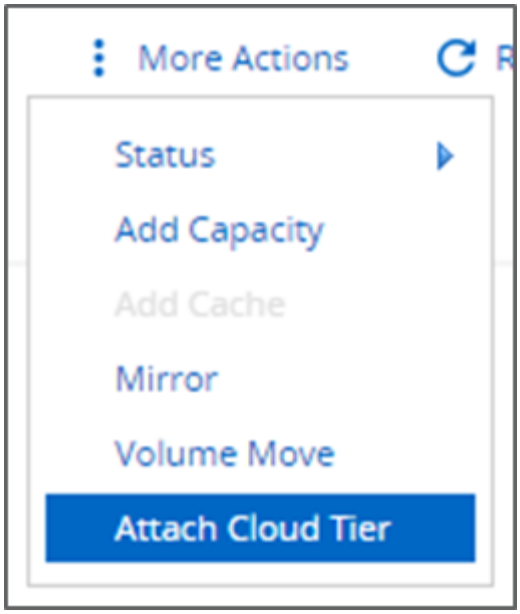
Gestore di sistema di OnCommand

Per associare un Tier cloud a un aggregato utilizzando Gestione di sistema di OnCommand, completare i seguenti passaggi:

1. Avviare Gestore di sistema di OnCommand.
2. Fare clic su applicazioni e livelli.



3. Fare clic su Storage Tier.
4. Fare clic su un aggregato.
5. Fare clic su azioni e selezionare Allega Tier cloud.



6. Seleziona un livello cloud.
7. Visualizzare e aggiornare i criteri di tiering per i volumi sull'aggregato (facoltativo). Per impostazione predefinita, il criterio di tiering del volume è impostato su Snapshot-Only (solo snapshot).
8. Fare clic su Salva.

CLI ONTAP

Per collegare un Tier cloud a un aggregato utilizzando l'interfaccia utente di ONTAP, eseguire i seguenti comandi:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Esempio:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Successivo: Impostare la policy di tiering dei volumi."

Impostare la policy di tiering dei volumi

Per impostazione predefinita, i volumi utilizzano il criterio None volume Tiering. Dopo la creazione del volume, è possibile modificare il criterio di tiering del volume utilizzando Gestione di sistema di OnCommand o l'interfaccia utente di ONTAP.

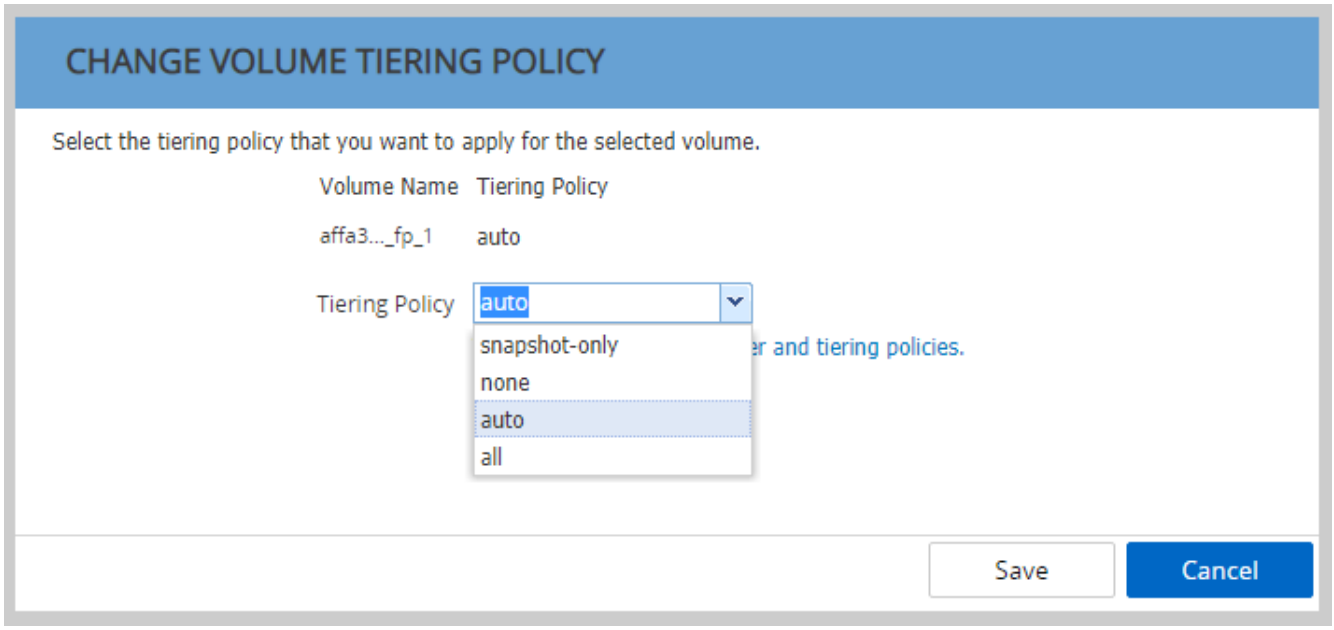
Se utilizzato con FlexPod, FabricPool offre tre criteri di tiering dei volumi, automatico, solo snapshot e Nessuno.

- **Auto**
  - Tutti i cold block nel volume vengono spostati nel Tier cloud. Supponendo che l'aggregato sia utilizzato oltre il 50%, occorrono circa 31 giorni affinché i blocchi inattivi diventino freddi. Il periodo di raffreddamento automatico può essere regolato tra 2 giorni e 63 giorni utilizzando `tiering-minimum-cooling-days` impostazione.
  - Quando i cold block in un volume con una policy di tiering impostata su Auto vengono letti in modo casuale, vengono resi hot e scritti nel Tier di performance.
  - Quando i blocchi freddi in un volume con una policy di tiering impostata su Auto vengono letti in sequenza, rimangono freddi e rimangono sul livello cloud. Non sono scritti nel Tier di performance.
- **Solo Snapshot**
  - I blocchi Cold Snapshot nel volume non condivisi con il file system attivo vengono spostati nel Tier cloud. Supponendo che l'aggregato sia utilizzato oltre il 50%, sono necessari circa 2 giorni affinché i blocchi snapshot inattivi diventino freddi. Il periodo di raffreddamento solo Snapshot può essere regolato da 2 a 63 giorni utilizzando `tiering-minimum-cooling-days` impostazione.
  - Quando i blocchi a freddo in un volume con una policy di tiering impostata su Snapshot-only vengono letti, vengono resi a caldo e scritti nel Tier di performance.
- **Nessuno (impostazione predefinita)**
  - I volumi impostati per l'utilizzo di None come policy di tiering non suddividono i dati cold nel Tier cloud.
  - L'impostazione del criterio di tiering su None impedisce il nuovo tiering.
  - I dati del volume precedentemente spostati nel Tier cloud rimangono nel Tier cloud fino a quando non diventano caldi e vengono automaticamente spostati di nuovo nel Tier di performance.

Gestore di sistema di OnCommand

Per modificare la policy di tiering di un volume utilizzando Gestione di sistema di OnCommand, attenersi alla seguente procedura:

1. Avviare Gestore di sistema di OnCommand.
2. Selezionare un volume.
3. Fare clic su altre azioni e selezionare Cambia policy di tiering.
4. Selezionare il criterio di tiering da applicare al volume.
5. Fare clic su Salva.



CLI ONTAP

Per modificare il criterio di tiering di un volume utilizzando l'interfaccia utente di ONTAP, eseguire il seguente comando:

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Successivo: Impostare i giorni minimi di raffreddamento per il tiering del volume."

Impostare i giorni minimi di raffreddamento per il tiering del volume

Il `tiering-minimum-cooling-days` L'impostazione determina il numero di giorni che devono trascorrere prima che i dati inattivi in un volume utilizzando il criterio Auto o Snapshot-Only siano considerati freddi e idonei per il tiering.

Automatico

L'impostazione predefinita `tiering-minimum-cooling-days` L'impostazione per il criterio di tiering automatico è 31 giorni.

Poiché le letture mantengono calde le temperature dei blocchi, l'aumento di questo valore potrebbe ridurre la quantità di dati che possono essere suddivisi in livelli e aumentare la quantità di dati conservati nel Tier di performance.

Se si desidera ridurre questo valore dai 31 giorni predefiniti, tenere presente che i dati non devono più essere attivi prima di essere contrassegnati come cold. Ad esempio, se si prevede che un carico di lavoro di più giorni esegua un numero significativo di scritture il giorno 7, il volume `tiering-minimum-cooling-days` l'impostazione non deve essere inferiore a 8 giorni.

> Lo storage a oggetti non è transazionale come lo storage a file o a blocchi. Apportare modifiche ai file memorizzati come oggetti nei volumi con giorni di raffreddamento minimi eccessivamente aggressivi può causare la creazione di nuovi oggetti, la frammentazione degli oggetti esistenti e l'aggiunta di inefficienze dello storage.

Solo Snapshot

L'impostazione predefinita `tiering-minimum-cooling-days` L'impostazione per la policy di tiering Snapshot-Only è di 2 giorni. Un minimo di 2 giorni offre un tempo aggiuntivo per i processi in background per fornire la massima efficienza dello storage e impedisce ai processi di protezione dei dati quotidiani di dover leggere i dati dal Tier cloud.

CLI ONTAP

Per modificare un volume `tiering-minimum-cooling-days` Impostando utilizzando l'interfaccia utente di ONTAP, eseguire il seguente comando:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

È necessario il livello di privilegio avanzato.

> La modifica della policy di tiering tra Auto e Snapshot-Only (o viceversa) ripristina il periodo di inattività dei blocchi sul Tier di performance. Ad esempio, un volume che utilizza il criterio di tiering automatico del volume con i dati sul Tier di performance inattivi per 20 giorni avrà l'inattività dei dati del Tier di performance reimpostata su 0 giorni se il criterio di tiering è impostato su Snapshot-Only.

Considerazioni sulle performance

Dimensionare il Tier di performance

Quando si prende in considerazione il dimensionamento, tenere presente che il Tier di performance deve essere in grado di svolgere le seguenti attività:

- Supporto dei dati hot
- Supporto dei dati cold fino a quando la scansione di tiering non sposta i dati nel Tier cloud
- Supporto dei dati del Tier cloud che diventano "hot" e vengono riscritti nel Tier di performance
- Supporto dei metadati WAFL associati al Tier cloud allegato

Per la maggior parte degli ambienti, un rapporto performance-capacità 1:10 sugli aggregati FabricPool è estremamente conservativo, fornendo al contempo risparmi significativi sullo storage. Ad esempio, se l'intento è quello di tierare 200 TB al livello cloud, l'aggregato del Tier di performance dovrebbe essere di almeno 20 TB.

> Le scritture dal Tier cloud al Tier performance sono disattivate se la capacità del Tier performance è superiore al 70%. In questo caso, i blocchi vengono letti direttamente dal livello cloud.

Dimensionare il Tier cloud

Quando si considera il dimensionamento, l'archivio di oggetti che agisce come Tier cloud deve essere in grado di svolgere le seguenti attività:

- Supporto delle letture dei dati cold esistenti
- Supporto delle scritture di nuovi dati cold
- Supporto dell'eliminazione e della deframmentazione degli oggetti

Costo di proprietà

Il "Calcolatore economico di FabricPool" È disponibile attraverso la società di analisi IT indipendente Evaluator Group per contribuire a proiettare i risparmi sui costi tra on-premise e cloud per lo storage dei dati cold. Il calcolatore fornisce un'interfaccia semplice per determinare il costo di archiviazione dei dati con accesso non frequente su un Tier di performance rispetto all'invio a un Tier cloud per il resto del ciclo di vita dei dati. In base a un calcolo di 5 anni, i quattro fattori chiave (capacità di origine, crescita dei dati, capacità di snapshot e percentuale di dati cold) vengono utilizzati per determinare i costi di storage nel periodo di tempo.

Conclusione

Il percorso verso il cloud varia tra le organizzazioni, tra le business unit e persino tra le business unit all'interno delle organizzazioni. Alcuni scelgono un'adozione rapida, mentre altri adottano un approccio più conservativo. FabricPool si inserisce nella strategia cloud delle organizzazioni indipendentemente dalle loro dimensioni e dalla loro velocità di adozione del cloud, dimostrando ulteriormente i vantaggi in termini di efficienza e scalabilità di un'infrastruttura FlexPod.

Dove trovare ulteriori informazioni

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

- Best practice FabricPool

  "www.netapp.com/us/media/tr-4598.pdf"

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com"

- TR-4036: Specifiche tecniche del data center FlexPod

  "https://www.netapp.com/us/media/tr-4036.pdf"

Data center FlexPod con cloud privato IBM

Sreenivasa Edula, Cisco Thanachit Wichianchai, IBM Jacky ben-Bassat, IBM Global Alliance, NetApp

IBM Cloud Private (ICP) è una piattaforma on-premise per lo sviluppo e la gestione di applicazioni containerizzate per casi di utilizzo cloud-native e application-modernization. Si tratta di un ambiente integrato basato su Kubernetes come orchestrazione di container e include un repository di immagini privato per container Docker, una console di gestione, un framework di monitoraggio, molte applicazioni open source e container IBM e molto altro ancora. Combinando ICP con FlexPod, l'infrastruttura convergente di Cisco e NetApp, è possibile semplificare l'implementazione e la gestione dell'infrastruttura. Puoi anche trarre vantaggio da una maggiore efficienza dello storage, una migliore protezione dei dati, una riduzione dei rischi e la flessibilità di scalare questo stack di infrastrutture Enterprise altamente disponibili per soddisfare nuovi requisiti di business e altre modifiche nel tempo.

"Data center FlexPod con cloud privato IBM"

Data center FlexPod per cloud ibrido con Cisco CloudCenter e storage privato NetApp - progettazione

Haseeb Niazi, Cisco David Arnette, NetApp

Cisco Validated Designs (CVD) offre sistemi e soluzioni progettati, testati e documentati per facilitare e migliorare le implementazioni dei clienti. Questi design incorporano un'ampia gamma di tecnologie e prodotti in un portfolio di soluzioni sviluppate per soddisfare le esigenze di business dei clienti e per guidarli dalla progettazione all'implementazione.

"Data center FlexPod per cloud ibrido con Cisco CloudCenter e storage privato NetApp - progettazione"

Data center FlexPod per multicloud con Cisco CloudCenter e NetApp Data Fabric

Haseeb Niazi, Cisco David Arnette, NetApp

Questo documento fornisce linee guida approfondite per la configurazione e l'implementazione per la configurazione del data center FlexPod per il cloud ibrido. I seguenti elementi di progettazione distinguono questa versione di FlexPod dai modelli precedenti:

- Integrazione di Cisco CloudCenter con FlexPod Datacenter con ACI come cloud privato
- Integrazione di Cisco CloudCenter con i cloud pubblici Amazon Web Services (AWS) e Microsoft Azure Resource Manager (MS Azure RM)
- Connettività sicura tra il data center FlexPod e i cloud pubblici per un traffico sicuro tra macchine virtuali (VM)

- Connettività sicura tra il data center FlexPod e lo storage privato NetApp (NPS) per il traffico di replica dei dati
- Possibilità di implementare istanze applicative in cloud pubblici o privati e di rendere disponibili dati applicativi aggiornati per queste istanze attraverso l'orchestrazione guidata da Cisco CloudCenter
- Impostazione, convalida ed evidenziazione degli aspetti operativi di un ambiente di sviluppo e test in questa nuova modalità di cloud ibrido.

"Data center FlexPod per multicloud con Cisco CloudCenter e NetApp Data Fabric"

Database aziendali

SAP

Introduzione a SAP su FlexPod

La piattaforma 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 controller di storage NetApp.

FlexPod è una piattaforma adatta per l'esecuzione di applicazioni SAP e le soluzioni qui fornite consentono di implementare SAP HANA in modo rapido e affidabile con un modello di integrazione dei data center su misura. FlexPod offre non solo una configurazione di base, ma anche la flessibilità di essere dimensionati e ottimizzati per adattarsi a diversi casi di utilizzo e requisiti.

Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive il data center FlexPod di Cisco e NetApp con NetApp ONTAP 9.7 su storage NetApp AFF A400 e il software unificato Cisco UCS Manager versione 4.1(1) con processori scalabili Intel Xeon di seconda generazione per SAP HANA in particolare.

FlexPod Datacenter con NetApp ONTAP 9.7 e Cisco UCS Unified Software release 4.1(1) è un'architettura di data center pre-progettata e Best-practice basata sul sistema di calcolo unificato Cisco (Cisco UCS), sulla famiglia di switch Cisco Nexus 9000, switch fabric multistrato MDS 9000, E gli storage array NetApp AFF Serie A con sistema operativo ONTAP 9.7.

"Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp ONTAP 9.7"

White paper SAP non-HANA with SQL - Design

L'attuale settore IT sta assistendo a una drastica trasformazione delle soluzioni per data center. Negli ultimi anni, si è registrato un notevole interesse per le soluzioni di data center pre-validate e progettate. L'introduzione della tecnologia di virtualizzazione nelle aree critiche ha avuto un impatto importante sui principi di progettazione e sull'architettura di queste soluzioni. Ha consentito a molte applicazioni eseguite su sistemi bare-metal di migrare verso nuove soluzioni integrate virtualizzate. FlexPod è una di queste soluzioni di data center prevalidate e progettate per soddisfare le esigenze in rapida evoluzione dei reparti IT. Cisco e NetApp hanno collaborato per offrire FlexPod, che utilizza componenti di calcolo, networking e storage di alto livello come base per una vasta gamma di carichi di lavoro aziendali, tra cui database, pianificazione delle risorse aziendali (ERP), gestione delle relazioni con i clienti (CRM) e applicazioni web.

Il consolidamento delle applicazioni IT, in particolare dei database, ha suscitato un notevole interesse negli ultimi anni. La piattaforma di database più diffusa e implementata negli ultimi anni è Microsoft SQL Server. I database di SQL Server sono spesso soggetti a una crescita incontrollata dei database, che comporta sfide IT

come server sottoutilizzati, licenze non corrette, problemi di sicurezza, problemi di gestione e costi operativi enormi. Pertanto, i database di SQL Server sono buoni candidati per il consolidamento su una piattaforma più solida, flessibile e resiliente. In questo documento viene illustrata un'architettura di riferimento di FlexPod per la distribuzione e il consolidamento dei database SQL Server.

"White paper SAP non-HANA with SQL - Design"

Soluzione FlexPod per data center per SAP con fabric di terza generazione Cisco UCS e NetApp AFF Serie A.

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive la metodologia di implementazione di Cisco e NetApp FlexPod Datacenter per SAP HANA basata su processori scalabili Intel Xeon di seconda generazione supportati da Cisco UCS Computing System (Cisco UCS).

Cisco UCS Manager (UCSM) 4.0(4) fornisce il supporto consolidato di tutti gli attuali modelli di Cisco UCS Fabric Interconnect (6200, 6300, 6324 e 6454), IOM serie 2200/2300, blade Cisco UCS B-Series e server Cisco UCS C-Series rack formFactor. FlexPod Datacenter con Cisco UCS Unified Software release 4.0(4d) e NetApp ONTAP 9.6, è un'architettura di data center pre-progettata e basata su Best practice, basata su Cisco UCS, sulla famiglia di switch Cisco Nexus 9000 e sugli storage array NetApp AFF serie A.

"Soluzione FlexPod per data center per SAP con fabric di terza generazione Cisco UCS e NetApp AFF Serie A."

Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp ONTAP 9.7 - progettazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Cisco e NetApp hanno collaborato per offrire una serie di soluzioni FlexPod che consentono piattaforme strategiche per data center. La soluzione FlexPod offre un'architettura integrata che incorpora le Best practice di progettazione di calcolo, storage e rete, riducendo al minimo i rischi PER L'IT convalidando l'architettura integrata per garantire la compatibilità tra i vari componenti. La soluzione risolve anche i problemi DELL'IT fornendo una guida documentata alla progettazione, una guida all'implementazione e un supporto che possono essere utilizzati in varie fasi (pianificazione, progettazione e implementazione) di un'implementazione.

"Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp ONTAP 9.7 - progettazione"

Soluzione FlexPod per data center per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Il presente documento descrive la soluzione FlexPod integrata Cisco ACI come approccio validato per l'implementazione di ambienti TDI (Tailored Data Center Integration) SAP HANA. Questo design validato fornisce linee guida e un framework per l'implementazione di SAP HANA con le Best practice di Cisco e NetApp.

L'architettura della soluzione consigliata si basa su Cisco Unified Computing System (Cisco UCS) utilizzando una release software unificata per supportare le piattaforme hardware Cisco UCS che includono i seguenti componenti:

- Server blade Cisco UCS B-Series e server rack Cisco UCS C-Series configurabili con l'opzione Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnect Cisco UCS serie 6400
- Switch Leaf e spine Cisco Nexus serie 9000
- Storage array NetApp All Flash

Inoltre, questo documento fornisce validazioni per Red Hat Enterprise Linux e SUSE Linux Enterprise Server per SAP HANA.

"Soluzione FlexPod per data center per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione"

Data center FlexPod per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - implementazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive l'architettura e le procedure di implementazione dell'opzione di integrazione del data center su misura SAP HANA sull'infrastruttura FlexPod, che è composta da:

- Cisco UCS Computing System (Cisco UCS) supportato dai processori scalabili Intel Xeon di seconda generazione.
- Prodotti di switching che sfruttano Cisco Application Centric Infrastructure (ACI).
- Array AFF NetApp Serie A.

Lo scopo di questo documento è quello di mostrare i passaggi di configurazione dettagliati per l'implementazione di SAP HANA

"Data center FlexPod per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - implementazione"

Soluzione FlexPod per data center per SAP con Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Il presente documento descrive la soluzione FlexPod di Cisco e NetApp, un approccio validato per l'implementazione di ambienti TDI (Tailored Data Center Integration) SAP HANA. Questo design validato fornisce linee guida e un framework per l'implementazione di SAP HANA con le Best practice di Cisco e NetApp.

FlexPod è un'infrastruttura integrata leader del settore che supporta un'ampia gamma di carichi di lavoro e casi di utilizzo aziendali. Questa soluzione consente di implementare SAP HANA in modo rapido e affidabile con un modello di modalità di integrazione del data center personalizzata.

"Soluzione FlexPod per data center per SAP con Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione"

Soluzione FlexPod Datacenter per SAP con Cisco ACI su server Cisco UCS M5 con SLES 12 SP3 e RHEL 7.4

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive l'architettura e le procedure di implementazione dell'opzione di integrazione DataCenter personalizzata SAP HANA sull'infrastruttura FlexPod composta da prodotti di calcolo e switching Cisco che sfruttano l'infrastruttura basata sull'applicazione (ACI), la soluzione di networking software-defined leader del settore (SDN), insieme agli array AFF NetApp Serie A. Lo scopo di questo documento è mostrare i principi di progettazione con le fasi di configurazione dettagliate per l'implementazione di SAP HANA.

"Soluzione FlexPod Datacenter per SAP con Cisco ACI su server Cisco UCS M5 con SLES 12 SP3 e RHEL 7.4"

Soluzione FlexPod per data center per SAP con storage basato su IP con NetApp AFF Serie A e Cisco UCS Manager 3.2

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

L'architettura di riferimento illustrata in questo documento evidenzia la resilienza, i vantaggi in termini di costi e la facilità di implementazione di una soluzione di storage basata su IP. Un sistema storage in grado di servire più protocolli in un'unica interfaccia consente di scegliere il cliente e di proteggere gli investimenti perché si tratta di un'architettura wire-once. La soluzione è progettata per ospitare carichi di lavoro SAP HANA scalabili.

"Soluzione FlexPod per data center per SAP con storage basato su IP con NetApp AFF Serie A e Cisco UCS Manager 3.2"

Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp ONTAP 9.7

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive il data center FlexPod di Cisco e NetApp con NetApp ONTAP 9.7 su storage NetApp AFF A400 e il software unificato Cisco UCS Manager versione 4.1(1) con processori scalabili Intel Xeon di seconda generazione per SAP HANA in particolare.

FlexPod Datacenter con NetApp ONTAP 9.7 e Cisco UCS Unified Software release 4.1(1) è un'architettura di data center pre-progettata e Best-practice basata sul sistema di calcolo unificato Cisco (Cisco UCS), sulla famiglia di switch Cisco Nexus 9000, switch fabric multistrato MDS 9000, E gli storage array NetApp AFF Serie A con sistema operativo ONTAP 9.7.

"Soluzione FlexPod Datacenter per SAP che utilizza SAN FibreChannel con Cisco UCS Manager 4.0 e NetApp

ONTAP 9.7"

Implementare server di applicazioni SAP su FlexPod con SQL

FlexPod è una soluzione di data center pre-validata e progettata per soddisfare le esigenze in rapida evoluzione dei reparti IT. Cisco e NetApp hanno collaborato per offrire FlexPod, che utilizza componenti di calcolo, networking e storage Best-in-class come base per una varietà di carichi di lavoro aziendali, tra cui database, pianificazione delle risorse aziendali (ERP), gestione delle relazioni con i clienti (CRM) e applicazioni web. Il consolidamento delle applicazioni IT, in particolare dei database, ha suscitato un notevole interesse negli ultimi anni. La piattaforma di database più diffusa e implementata negli ultimi anni è Microsoft SQL Server. I database di SQL Server sono spesso soggetti a una crescita incontrollata dei database, che comporta sfide IT come server sottoutilizzati, licenze non corrette, problemi di sicurezza, problemi di gestione e costi operativi enormi. Pertanto, i database di SQL Server sono buoni candidati per il consolidamento su una piattaforma più solida, flessibile e resiliente. In questo documento viene illustrata un'architettura di riferimento di FlexPod per la distribuzione e il consolidamento dei database SQL Server.

"Implementare server di applicazioni SAP su FlexPod con SQL"

Data center FlexPod per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A.

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Questo documento descrive l'architettura e le procedure di implementazione dell'opzione di integrazione del data center su misura SAP HANA sull'infrastruttura FlexPod, che è composta da:

- Cisco UCS Computing System (Cisco UCS) supportato dai processori scalabili Intel Xeon di seconda generazione.
- Prodotti di switching che sfruttano Cisco Application Centric Infrastructure (ACI).
- Array AFF NetApp Serie A.

"Data center FlexPod per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A."

Soluzione FlexPod per data center per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Il presente documento descrive la soluzione FlexPod integrata Cisco ACI come approccio validato per l'implementazione di ambienti TDI (Tailored Data Center Integration) SAP HANA. Questo design validato fornisce linee guida e un framework per l'implementazione di SAP HANA con le Best practice di Cisco e NetApp.

L'architettura della soluzione consigliata si basa su Cisco Unified Computing System (Cisco UCS) utilizzando

una release software unificata per supportare le piattaforme hardware Cisco UCS che includono i seguenti componenti:

- Server blade Cisco UCS B-Series e server rack Cisco UCS C-Series configurabili con l'opzione Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnect Cisco UCS serie 6400
- Switch Leaf e spine Cisco Nexus serie 9000
- Storage array NetApp All Flash

Inoltre, questo documento fornisce validazioni per Red Hat Enterprise Linux e SUSE Linux Enterprise Server per SAP HANA.

"Soluzione FlexPod per data center per SAP con Cisco ACI, Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione"

Soluzione FlexPod per data center per SAP con fabric di terza generazione Cisco UCS e NetApp AFF Serie A.

Shailendra Mruthunjaya, Cisco Ralf Klahr, Cisco Marco Schoen, NetApp

Questo documento descrive la metodologia di implementazione di Cisco e NetApp FlexPod Datacenter per SAP HANA basata sul sistema di calcolo Cisco UCS (Cisco UCS) supportato dai processori scalabili Intel Xeon di seconda generazione.

Cisco UCS Manager (UCSM) 4.0(4) fornisce il supporto consolidato di tutti gli attuali modelli di Cisco UCS Fabric Interconnect (6200, 6300, 6324 e 6454), IOM serie 2200/2300, blade Cisco UCS B-Series e server Cisco UCS C-Series rack formFactor. FlexPod Datacenter con Cisco UCS Unified Software release 4.0(4d) e NetApp ONTAP 9.6 è un'architettura di data center pre-progettata e basata su Best practice, basata su Cisco UCS, sulla famiglia di switch Cisco Nexus 9000 e sugli storage array NetApp AFF serie A.

"Soluzione FlexPod per data center per SAP con fabric di terza generazione Cisco UCS e NetApp AFF Serie A."

Soluzione FlexPod per data center per SAP con Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione

Pramod Ramamurthy, Cisco Marco Schoen, NetApp

Il presente documento descrive la soluzione FlexPod di Cisco e NetApp, un approccio validato per l'implementazione di ambienti TDI (Tailored Data Center Integration) SAP HANA. Questo design validato fornisce linee guida e un framework per l'implementazione di SAP HANA con le Best practice di Cisco e NetApp.

FlexPod è un'infrastruttura integrata leader del settore che supporta un'ampia gamma di carichi di lavoro e casi di utilizzo aziendali. Questa soluzione consente di implementare SAP HANA in modo rapido e affidabile con un modello di una modalità di integrazione dei data center personalizzata.

L'architettura della soluzione consigliata si basa su Cisco Unified Computing System (Cisco UCS) utilizzando una release software unificata per supportare le piattaforme hardware Cisco UCS che includono i seguenti componenti:

- Server blade Cisco UCS B-Series e server rack Cisco UCS C-Series configurabili con l'opzione Intel Optane Data Center Persistent Memory Module (DCPMM)
- Fabric Interconnect Cisco UCS serie 6300
- Switch Cisco Nexus serie 9000
- Storage array NetApp All Flash

Inoltre, questo documento fornisce validazioni per Red Hat Enterprise Linux e SUSE Linux Enterprise Server per SAP HANA.

"Soluzione FlexPod per data center per SAP con Cisco UCS Manager 4.0 e NetApp AFF Serie A - progettazione"

Oracle

Data center FlexPod con database RAC Oracle 19c su Cisco UCS e NetApp AFF con NVMe su FibreChannel

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Cisco Validated Designs (CVD) è costituito da sistemi e soluzioni progettati, testati e documentati per facilitare e migliorare le implementazioni dei clienti. Questo documento CVD descrive la soluzione Cisco e NetApp FlexPod, un approccio validato per l'implementazione di un ambiente di database Oracle RAC altamente disponibile. Cisco e NetApp hanno validato l'architettura di riferimento con diversi workload di database, come OLTP (Online Transactional Processing) e Data Warehouse nel laboratorio UCS Datacenter di Cisco. Questo documento mostra la configurazione hardware e software dei componenti coinvolti e i risultati dei vari test. Inoltre, il documento offre un framework per l'implementazione di database Oracle RAC su NVMe/FC utilizzando Cisco UCS e NetApp Storage System.

"Data center FlexPod con database RAC Oracle 19c su Cisco UCS e NetApp AFF con NVMe su FibreChannel"

Data center FlexPod con database RAC Oracle su Cisco UCS e NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

I Cisco Validated Design includono sistemi e soluzioni progettati, testati e documentati per facilitare e migliorare le implementazioni dei clienti. Questi design incorporano un'ampia gamma di tecnologie e prodotti in un portfolio di soluzioni sviluppate per soddisfare le esigenze di business dei clienti. Cisco e NetApp hanno collaborato per offrire FlexPod, che funge da base per una varietà di carichi di lavoro e consente progettazioni architetturali efficienti basate sui requisiti del cliente. Una soluzione FlexPod è un approccio validato per l'implementazione delle tecnologie Cisco e NetApp come infrastruttura cloud condivisa.

Il sistema FlexPod Datacenter con NetApp All Flash AFF è una piattaforma di infrastruttura convergente che

combina le migliori tecnologie di Cisco e NetApp in una potente piattaforma convergente per le applicazioni aziendali. Cisco e NetApp collaborano a stretto contatto con Oracle per supportare i database transazionali e sensibili ai tempi di risposta più esigenti richiesti dalle aziende di oggi.

Questo progetto validato Cisco (CVD) descrive l'architettura di riferimento di FlexPod Datacenter che utilizza Cisco UCS e NetApp All Flash AFF per l'implementazione di un ambiente di database Oracle RAC ad alta disponibilità. Questo documento mostra la configurazione hardware e software dei componenti coinvolti e i risultati di vari test. Inoltre, il presente documento offre una guida all'implementazione e alle Best practice per l'utilizzo di server di calcolo Cisco UCS, switch di interconnessione Cisco Fabric, switch Cisco MDS, switch Cisco Nexus, storage NetApp AFF e database Oracle RAC.

"Data center FlexPod con database RAC Oracle su Cisco UCS e NetApp AFF A-Series"

Data center FlexPod con RAC Oracle su Oracle Linux

Tushar Patel, Cisco Niranjan Mohapatra, Cisco John Elliott, NetApp

Cisco Unified Computing System (Cisco UCS) è una piattaforma di data center di nuova generazione che unisce calcolo, rete, accesso allo storage e virtualizzazione in un unico sistema coesivo. Cisco UCS è una piattaforma ideale per l'architettura dei carichi di lavoro di database mission-critical. La combinazione della piattaforma Cisco UCS, dello storage NetApp e dell'architettura Oracle Real Application Cluster (RAC) può accelerare la trasformazione IT consentendo implementazioni più rapide, maggiore flessibilità di scelta, efficienza e riduzione dei rischi. Questo Cisco Validated Design (CVD) evidenzia un'architettura di riferimento FlexPod flessibile, multi-tenant, dalle performance elevate e resiliente con il database RAC di Oracle 12c.

La piattaforma FlexPod, sviluppata da NetApp e Cisco, è una soluzione di infrastruttura flessibile e integrata che offre tecnologie di storage, networking e server pre-validate. È progettato per aumentare la reattività DELL'IT alle esigenze di business riducendo al contempo il costo complessivo del calcolo. Pensa al massimo uptime, al minimo rischio. I componenti FlexPod sono integrati e standardizzati per aiutarti a ottenere implementazioni puntuali, ripetibili e coerenti. È possibile pianificare con precisione l'alimentazione, lo spazio, la capacità utilizzabile, le performance e i costi di ogni implementazione FlexPod.

FlexPod adotta la tecnologia più recente e semplifica in modo efficiente i carichi di lavoro del data center che ridefiniscono il modo IN cui offre valore:

- Sfrutta le funzionalità degli array ibridi FAS di NetApp con flash pool per fornire la capacità di implementare la proporzione precisa di flash su supporti rotanti per la tua applicazione o ambiente specifico.
- Sfrutta una piattaforma pre-validata per ridurre al minimo le interruzioni del business, migliorare l'agilità IT e ridurre i tempi di implementazione da mesi a settimane.
- Ridurre del 50% i tempi di amministrazione e il TCO (Total Cost of Ownership).
- Soddisfa o supera le richieste di performance hardware in continua espansione per i carichi di lavoro del data center.

"Data center FlexPod con RAC Oracle su Oracle Linux"

Data center FlexPod con database RAC Oracle su Cisco UCS e NetApp AFF A-Series

Tushar Patel, Cisco Hardikkumar Vyas, Cisco

Il sistema FlexPod Datacenter con NetApp All Flash AFF è una piattaforma di infrastruttura convergente che combina le migliori tecnologie di Cisco e NetApp in una potente piattaforma convergente per le applicazioni aziendali. Cisco e NetApp collaborano a stretto contatto con Oracle per supportare i database transazionali e sensibili ai tempi di risposta più esigenti richiesti dalle aziende di oggi.

Questo progetto validato Cisco (CVD) descrive l'architettura di riferimento di FlexPod Datacenter che utilizza Cisco UCS e NetApp All Flash AFF per l'implementazione di un ambiente di database Oracle RAC ad alta disponibilità. Questo documento mostra la configurazione hardware e software dei componenti coinvolti e i risultati dei vari test. Inoltre, il presente documento offre una guida all'implementazione e alle Best practice per l'utilizzo di server di calcolo Cisco UCS, switch di interconnessione Cisco Fabric, switch Cisco MDS, switch Cisco Nexus, storage NetApp AFF e database Oracle RAC.

"Data center FlexPod con database RAC Oracle su Cisco UCS e NetApp AFF A-Series"

Microsoft SQL Server

Data center FlexPod per Microsoft SQL Server 2019 e VMware vSphere 6.7

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Balodia, NetApp

Questo documento descrive un'architettura di riferimento di FlexPod che utilizza i prodotti hardware e software più recenti e fornisce consigli sull'implementazione per l'hosting di database Microsoft SQL Server 2019 in ambienti virtualizzati VMware ESXi. Questa soluzione utilizza anche Cisco workload Optimization Manager (CWOM), che fornisce consigli automatizzati per un utilizzo ottimale ed efficiente delle risorse sia per i carichi di lavoro SQL che per l'infrastruttura.

La soluzione si basa su Cisco Unified Computing System (Cisco UCS) utilizzando la versione software unificata 4.1.1c per supportare le piattaforme hardware Cisco UCS, inclusi i server blade Cisco UCS serie B, le interconnessioni fabric Cisco UCS 6400, gli switch Cisco Nexus serie 9000 e gli array di storage NetApp serie AFF.

"Data center FlexPod per Microsoft SQL Server 2019 e VMware vSphere 6.7"

Data center FlexPod con Microsoft SQL Server 2016 e VMware vSphere 6.5

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco David Arnette, NetApp

In questo documento viene descritta un'architettura di riferimento di FlexPod che utilizza i prodotti hardware e software più recenti e vengono fornite raccomandazioni di configurazione per l'implementazione di database Microsoft SQL Server in un ambiente virtualizzato.

L'architettura della soluzione consigliata è basata su Cisco Unified Computing System (Cisco UCS) utilizzando

la versione software unificata per supportare le piattaforme hardware Cisco UCS, inclusi i server blade Cisco UCS B-Series, Cisco UCS 6300 Fabric Interconnect, gli switch Cisco Nexus 9000 Series e gli storage array NetApp All Flash Series. Inoltre, questa soluzione include VMware vSphere 6.5, vSphere 6.5, che offre una serie di nuove funzionalità per ottimizzare l'utilizzo dello storage e facilitare un cloud privato.

"Data center FlexPod con Microsoft SQL Server 2016 e VMware vSphere 6.5"

FlexPod Datacenter con Microsoft SQL Server 2017 su macchine virtuali Linux eseguite su VMware e Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Balodia, NetApp

In questo documento viene descritta un'architettura di riferimento FlexPod che utilizza i prodotti hardware e software più recenti e vengono fornite raccomandazioni di implementazione per l'hosting di database Microsoft SQL Server in ambienti virtualizzati VMware ESXi e Microsoft Windows Hyper-V con abilitazione del supporto Linux da parte di Microsoft per l'implementazione di SQL Server.

L'architettura della soluzione consigliata è basata su Cisco Unified Computing System (Cisco UCS) utilizzando la versione software unificata 4.0.1c per supportare le piattaforme hardware Cisco UCS, inclusi i server blade Cisco UCS serie B, le interconnessioni fabric Cisco UCS 6300, gli switch Cisco Nexus serie 9000 e gli array di storage NetApp serie AFF.

"FlexPod Datacenter con Microsoft SQL Server 2017 su macchine virtuali Linux eseguite su VMware e Hyper-V."

FlexPod Datacenter con Microsoft SQL Server 2017 su macchine virtuali Linux eseguite su VMware e Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Balodia, NetApp

In questo documento viene descritta un'architettura di riferimento FlexPod che utilizza i prodotti hardware e software più recenti e vengono fornite raccomandazioni di implementazione per l'hosting di database Microsoft SQL Server in ambienti virtualizzati VMware ESXi e Microsoft Windows Hyper-V con abilitazione del supporto Linux da parte di Microsoft per l'implementazione di SQL Server.

L'architettura della soluzione consigliata è basata su Cisco Unified Computing System (Cisco UCS) utilizzando la versione software unificata 4.0.1c per supportare le piattaforme hardware Cisco UCS, inclusi i server blade Cisco UCS serie B, le interconnessioni fabric Cisco UCS 6300, gli switch Cisco Nexus serie 9000 e gli array di storage NetApp serie AFF.

"FlexPod Datacenter con Microsoft SQL Server 2017 su macchine virtuali Linux eseguite su VMware e Hyper-V."

Settore sanitario

FlexPod per la genomica

TR-4911: Genomica FlexPod

JayaKishore Esanakula, NetApp

Ci sono pochi campi della medicina che sono più importanti della genomica per l'assistenza sanitaria e le scienze biologiche, e la genomica sta rapidamente diventando uno strumento clinico chiave per medici e infermieri. La genomica, se combinata con l'imaging medico e la patologia digitale, ci aiuta a capire in che modo i geni di un paziente potrebbero essere influenzati dai protocolli di trattamento. Il successo della genomica nel settore sanitario dipende sempre più dall'interoperabilità dei dati su larga scala. L'obiettivo finale è quello di dare un senso agli enormi volumi di dati genetici e identificare correlazioni e varianti clinicamente rilevanti che migliorano la diagnosi e rendono la medicina di precisione una realtà. La genomica ci aiuta a comprendere l'origine dei focolai di malattia, come evolvono le malattie e quali trattamenti e strategie potrebbero essere efficaci. Chiaramente, la genomica ha molti benefici che spaziano dalla prevenzione alla diagnosi e al trattamento. Le organizzazioni del settore sanitario si trovano ad affrontare diverse sfide, tra cui:

- Migliore qualità dell'assistenza
- Assistenza basata sul valore
- Esplosione dei dati
- Medicina di precisione
- Pandemie
- Dispositivi indossabili, monitoraggio remoto e assistenza
- Sicurezza informatica

Percorsi clinici e protocolli clinici standardizzati sono uno dei componenti critici della medicina moderna. Uno degli aspetti chiave della standardizzazione è l'interoperabilità tra gli operatori sanitari, non solo per le cartelle cliniche, ma anche per i dati genomici. La domanda principale è che le organizzazioni sanitarie cederanno la proprietà dei dati genomici al posto della proprietà dei pazienti dei dati personali di genomica e delle relative cartelle mediche?

L'interoperabilità dei dati dei pazienti è fondamentale per la medicina di precisione, una delle forze trainanti della recente esplosione della crescita dei dati. L'obiettivo della medicina di precisione è quello di rendere più efficaci e precise le soluzioni di manutenzione della salute, prevenzione delle malattie, diagnosi e trattamento.

Il tasso di crescita dei dati è stato esponenziale. All'inizio di febbraio 2021, i laboratori statunitensi hanno sequenziato circa 8,000 ceppi COVID-19 alla settimana. Il numero di genomi sequenziati era aumentato a 29,000 alla settimana entro aprile 2021. Ogni genoma umano completamente sequenziato ha una dimensione di circa 125 GB. Pertanto, con un tasso di 29,000 genomi sequenziati alla settimana, lo storage totale del genoma a riposo sarebbe superiore a 180 petabyte all'anno. Diversi paesi hanno impegnato risorse per l'epidemiologia genomica per migliorare la sorveglianza genomica e prepararsi alla prossima ondata di sfide sanitarie globali.

Il costo ridotto della ricerca genomica sta portando a test genetici e ricerca a un ritmo senza precedenti. I tre PS si trovano a un punto di svolta: Potenza del computer, privacy dei dati e personalizzazione della medicina. Entro il 2025 i ricercatori stimano che 100 milioni fino a 2 miliardi di genomi umani saranno sequenziati. Affinché la genomica sia efficace e una proposta preziosa, le funzionalità di genomica devono essere parte integrante dei flussi di lavoro di cura; devono essere facilmente accessibili e utilizzabili durante la visita di un paziente. Inoltre, è altrettanto importante integrare i dati medici elettronici dei pazienti con i dati genomici dei pazienti. Con l'avvento di un'infrastruttura convergente all'avanguardia come FlexPod, le organizzazioni possono introdurre le proprie funzionalità di genomica nei flussi di lavoro quotidiani di medici, infermieri e responsabili delle cliniche. Per informazioni aggiornate sulla piattaforma FlexPod, consulta questa pagina "White paper su FlexPod Datacenter con Cisco UCS serie X.".

Per un medico, il vero valore della genomica include la medicina di precisione e piani di trattamento personalizzati in base ai dati genomici di un paziente. In passato, non c'è mai stata una tale sinergia tra medici e data scientist, e la genomica sta beneficiando delle innovazioni tecnologiche del recente passato, oltre a partnership reali tra le organizzazioni sanitarie e i leader tecnologici del settore.

I centri medici accademici e le altre organizzazioni di settore sanitario e delle scienze della vita sono sulla buona strada per stabilire il centro di eccellenza (COE) nella scienza del genoma. Secondo il Dr. Charlie Gersbach, Dr Greg Crawford e il Dr. Tim e Reddy della Duke University, "sappiamo che i geni non vengono attivati o disattivati da un semplice switch binario, ma sono invece il risultato di più switch di regolazione dei geni che funzionano insieme. " Hanno anche determinato che "nessuna di queste parti del genoma funziona in isolamento. Il genoma è un web molto complicato che l'evoluzione ha intessuto" ("rif").

NetApp e Cisco si sono adoperati per implementare miglioramenti incrementali nella piattaforma FlexPod da oltre 10 anni. Tutti i commenti dei clienti vengono ascoltati, valutati e legati ai flussi di valore e ai set di funzionalità di FlexPod. È questo continuo loop di feedback, collaborazioni, miglioramenti e festeggiamenti che contraddistingue FlexPod come una piattaforma di infrastruttura convergente affidabile in tutto il mondo. È stata semplificata e progettata da zero per essere la piattaforma più affidabile, robusta, versatile e agile per le organizzazioni sanitarie.

Scopo

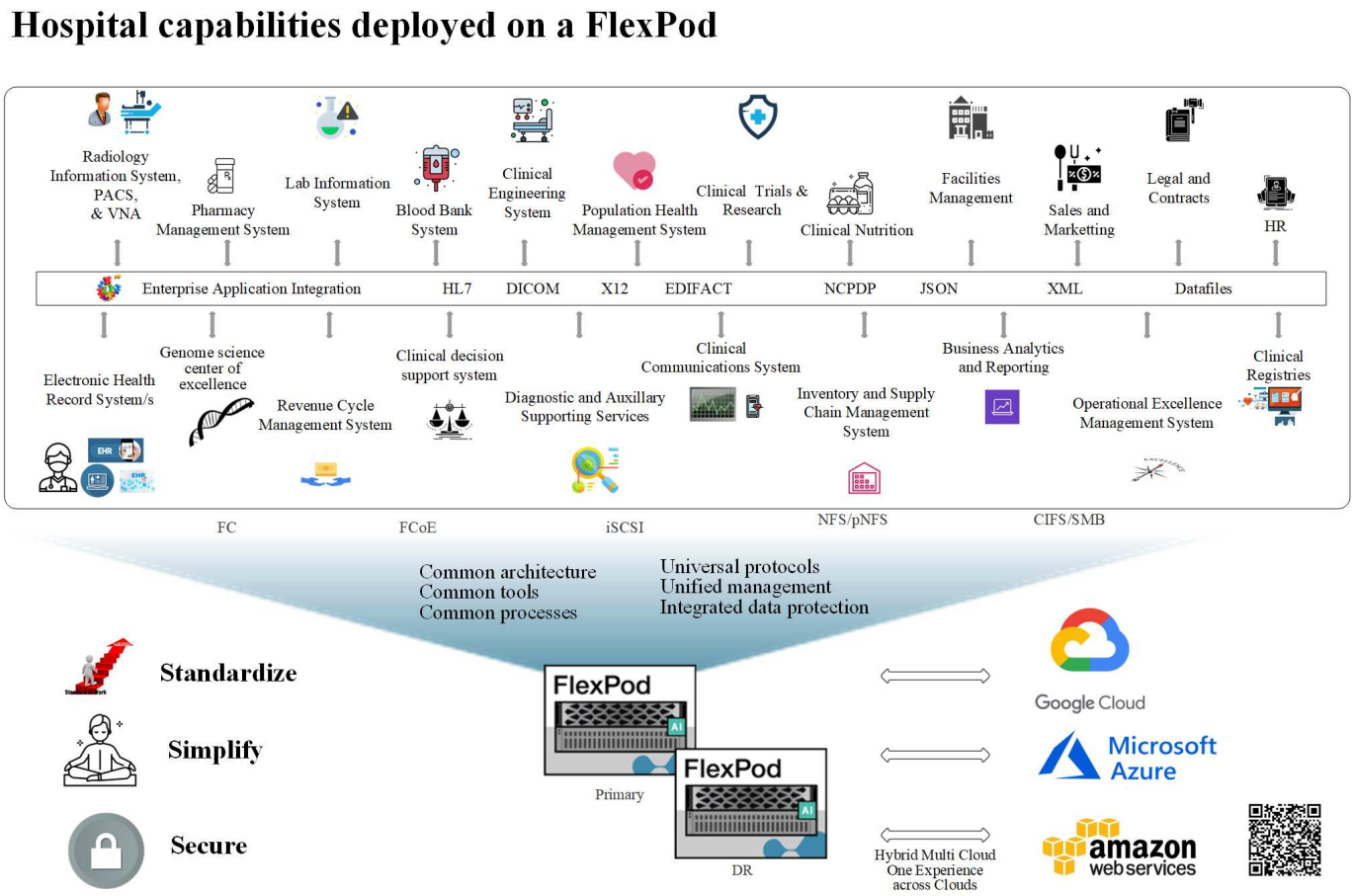
La piattaforma di infrastruttura convergente FlexPod consente a un'organizzazione sanitaria di ospitare uno o più carichi di lavoro di genomica, insieme ad altre applicazioni sanitarie cliniche e non cliniche. Questo report tecnico utilizza uno strumento di genomica open-source e standard di settore chiamato GATK durante la convalida della piattaforma FlexPod. Tuttavia, una discussione più approfondita sulla genomica o sul GATK non rientra nell'ambito di questo documento.

Pubblico

Il presente documento è destinato ai responsabili tecnici del settore sanitario, ai tecnici delle soluzioni partner Cisco e NetApp e al personale dei servizi professionali. NetApp presuppone che il lettore abbia una buona comprensione dei concetti di dimensionamento di calcolo e storage, nonché una familiarità tecnica con le minacce per il settore sanitario, la sicurezza sanitaria, i sistemi IT per il settore sanitario, Cisco UCS e i sistemi storage NetApp.

Funzionalità ospedaliere implementate su FlexPod

Un ospedale tipico dispone di un insieme diversificato di sistemi IT. La maggior parte di questi sistemi viene acquistata da un vendor, mentre pochissimi sono costruiti dal sistema ospedaliero in casa. Pertanto, il sistema ospedaliero deve gestire un ambiente di infrastruttura diversificato nei propri data center. Quando gli ospedali unificano i propri sistemi in una piattaforma di infrastruttura convergente come FlexPod, le organizzazioni possono standardizzare le operazioni del data center. Con FlexPod, le organizzazioni sanitarie possono implementare sistemi clinici e non clinici sulla stessa piattaforma, unificando in tal modo le operazioni del data center.



"Avanti: Vantaggi dell'implementazione di workload genomici su FlexPod."

Vantaggi dell'implementazione di workload genomici su FlexPod

"Precedente: Introduzione."

Questa sezione fornisce un breve elenco dei vantaggi per l'esecuzione di un carico di lavoro genomico su una piattaforma di infrastruttura convergente FlexPod. Descriviamo rapidamente le funzionalità di un ospedale. La seguente vista dell'architettura di business mostra le funzionalità di un ospedale implementate su una piattaforma di infrastruttura convergente FlexPod ibrida-pronta per il cloud.

- **Evitare i silos nell'assistenza sanitaria.** i silos nell'assistenza sanitaria sono una preoccupazione molto reale. I reparti vengono spesso inseriti in silos nel proprio set di hardware e software, non per scelta, ma organicamente per evoluzione. Ad esempio, radiologia, cardiologia, EHR, genomica, analytics, ciclo di ricavi e altri reparti finiscono con il loro set individuale di software e hardware dedicati. Le organizzazioni del settore sanitario gestiscono un numero limitato di professionisti IT per gestire le proprie risorse hardware e software. Il punto di flessione si verifica quando si prevede che questo insieme di individui gestisca un insieme molto diversificato di hardware e software. L'eterogeneità è aggravata da un insieme incongruente di processi portati all'organizzazione sanitaria dai vendor.
- **Inizia con le piccole dimensioni e fai crescere.** il kit di tool GATK è ottimizzato per l'esecuzione della CPU, che offre le migliori suite di piattaforme come FlexPod. FlexPod consente una scalabilità indipendente di rete, calcolo e storage. Inizia con le dimensioni ridotte e scala man mano che le tue capacità di genomica e l'ambiente crescono. Le organizzazioni del settore sanitario non devono investire in piattaforme specializzate per eseguire carichi di lavoro genomici. Le organizzazioni possono invece

sfruttare piattaforme versatili come FlexPod per eseguire carichi di lavoro di genomica e non genomica sulla stessa piattaforma. Ad esempio, se il reparto di pediatria desidera implementare la funzionalità di genomica, la leadership IT può eseguire il provisioning di calcolo, storage e networking su un'istanza di FlexPod esistente. Man mano che la business unit genomica cresce, le organizzazioni sanitarie possono scalare la propria piattaforma FlexPod in base alle esigenze.

- **Pannello di controllo singolo e flessibilità senza pari.** Cisco Intersight semplifica significativamente le operazioni IT attraverso il bridging delle applicazioni con l'infrastruttura, fornendo visibilità e gestione da server bare-metal e hypervisor ad applicazioni senza server, riducendo così i costi e mitigando i rischi. Questa piattaforma SaaS unificata utilizza un design Open API unificato che si integra in modo nativo con piattaforme e tool di terze parti. Inoltre, consente la gestione del tuo team operativo del data center on-site o da qualsiasi luogo utilizzando un'app mobile.

  Gli utenti possono ottenere rapidamente valore tangibile nel proprio ambiente sfruttando Intersight come piattaforma di gestione. Grazie all'automazione per molte attività manuali quotidiane, Intersight elimina gli errori e semplifica le operazioni quotidiane. Inoltre, le funzionalità di supporto avanzate di Intersight consentono agli utenti di restare al passo con i problemi e accelerare la risoluzione dei problemi. In combinazione, le organizzazioni dedicano molto meno tempo e denaro alla propria infrastruttura applicativa e più tempo allo sviluppo del business principale.

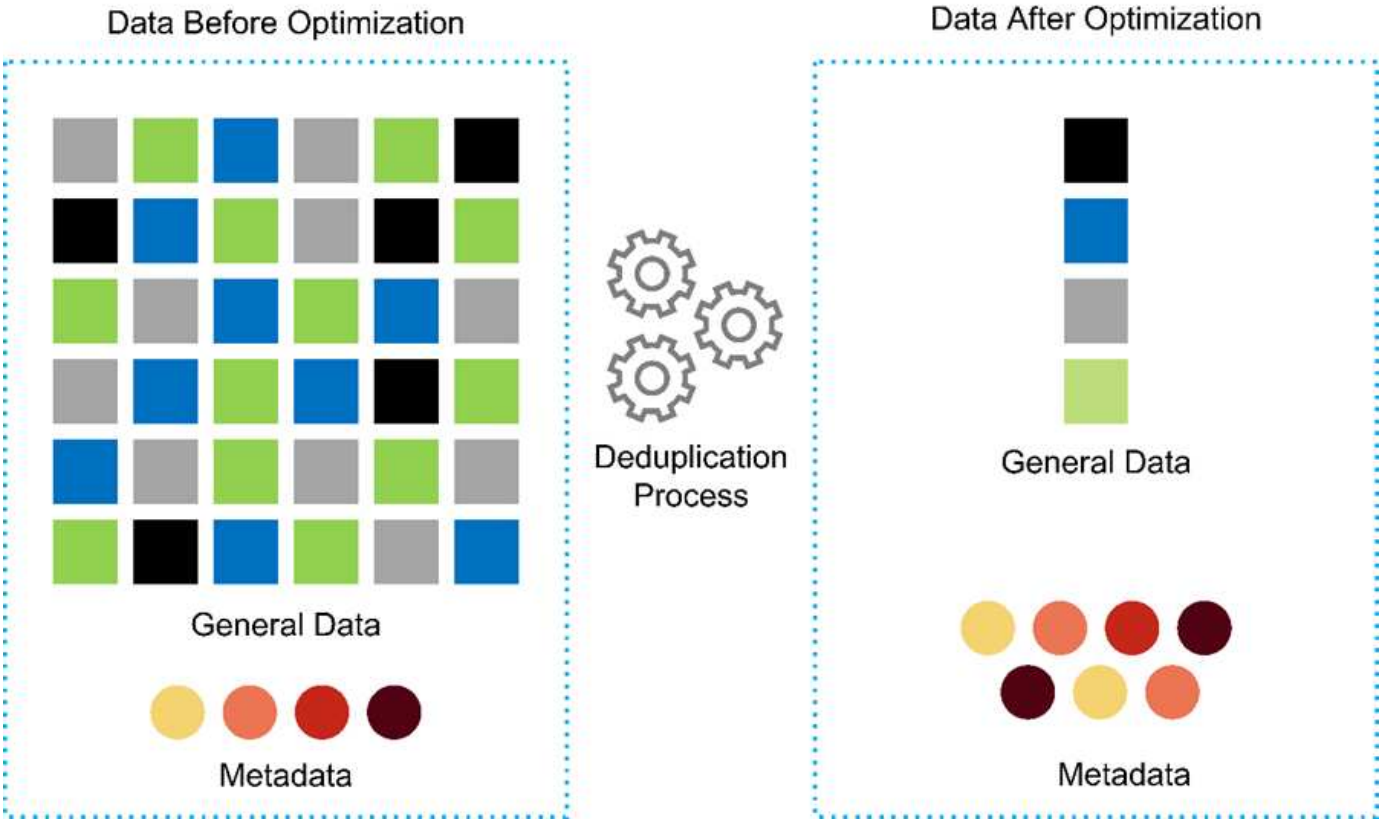
  Sfruttando la gestione di Intersight e l'architettura facilmente scalabile di FlexPod, le organizzazioni possono eseguire diversi carichi di lavoro genoma su una singola piattaforma FlexPod, aumentando l'utilizzo e riducendo il TCO (Total Cost of Ownership). FlexPod consente un dimensionamento flessibile, con scelte a partire dal nostro piccolo FlexPod Express e scalabilità in implementazioni di grandi dimensioni di FlexPod Datacenter. Grazie alle funzionalità di controllo degli accessi basate sui ruoli integrate in Cisco Intersight, le organizzazioni sanitarie possono implementare solidi meccanismi di controllo degli accessi, evitando la necessità di stack di infrastruttura separati. Più business unit all'interno dell'organizzazione sanitaria possono sfruttare la genomica come competenza chiave.

  In ultima analisi, FlexPod aiuta a semplificare le operazioni IT e a ridurre i costi operativi, consentendo agli amministratori dell'infrastruttura IT di concentrarsi su attività che aiutano i medici a innovare, anziché essere relegati per tenere le luci accese.

- **Progettazione validata e risultati garantiti.** le guide di progettazione e implementazione di FlexPod sono validate per essere ripetibili e coprono dettagli completi di configurazione e Best practice di settore che sono necessarie per implementare un FlexPod in tutta sicurezza. Le guide alla progettazione, le guide all'implementazione e le architetture validate di Cisco e NetApp aiutano la tua organizzazione sanitaria o di life science a eliminare ogni incertezza dall'implementazione di una piattaforma validata e affidabile fin dall'inizio. Con FlexPod, puoi accelerare i tempi di implementazione e ridurre costi, complessità e rischi. I design validati e le guide all'implementazione di FlexPod definiscono FlexPod come la piattaforma ideale per una vasta gamma di carichi di lavoro di genomica.
- **Innovazione e agilità.** FlexPod è una piattaforma ideale per gli EHR come Epic, Cerner, Meditech e sistemi di imaging come Agfa, GE, Philips. Per ulteriori informazioni su "EPIC Honor roll" E l'architettura della piattaforma di destinazione, vedi Epic userweb. Esecuzione di genomica su "FlexPod" consente alle organizzazioni del settore sanitario di continuare il proprio percorso di innovazione con agilità. Con FlexPod, l'implementazione del cambiamento organizzativo è naturale. Quando le organizzazioni si standardizzano su una piattaforma FlexPod, gli esperti IT del settore sanitario possono fornire tempo, impegno e risorse per innovare e quindi essere agili come richiesto dall'ecosistema.
- **Data liberated.** con la piattaforma di infrastruttura convergente FlexPod e un sistema storage NetApp ONTAP, i dati genomici possono essere resi disponibili e accessibili utilizzando un'ampia varietà di protocolli su larga scala da una singola piattaforma. FlexPod con NetApp ONTAP offre una piattaforma di cloud ibrido semplice, intuitiva e potente. Il data fabric basato su NetApp ONTAP consente di unire i dati tra siti, oltre i confini fisici e tra applicazioni diverse. Il tuo data fabric è costruito per le aziende basate sui dati in un mondo incentrato sui dati. I dati vengono creati e utilizzati in più sedi e spesso devono essere sfruttati

e condivisi con altre sedi, applicazioni e infrastrutture. Pertanto, è necessario un metodo coerente e integrato per gestirlo. FlexPod mette il tuo team IT sotto controllo e semplifica l'aumento della complessità DELL'IT.

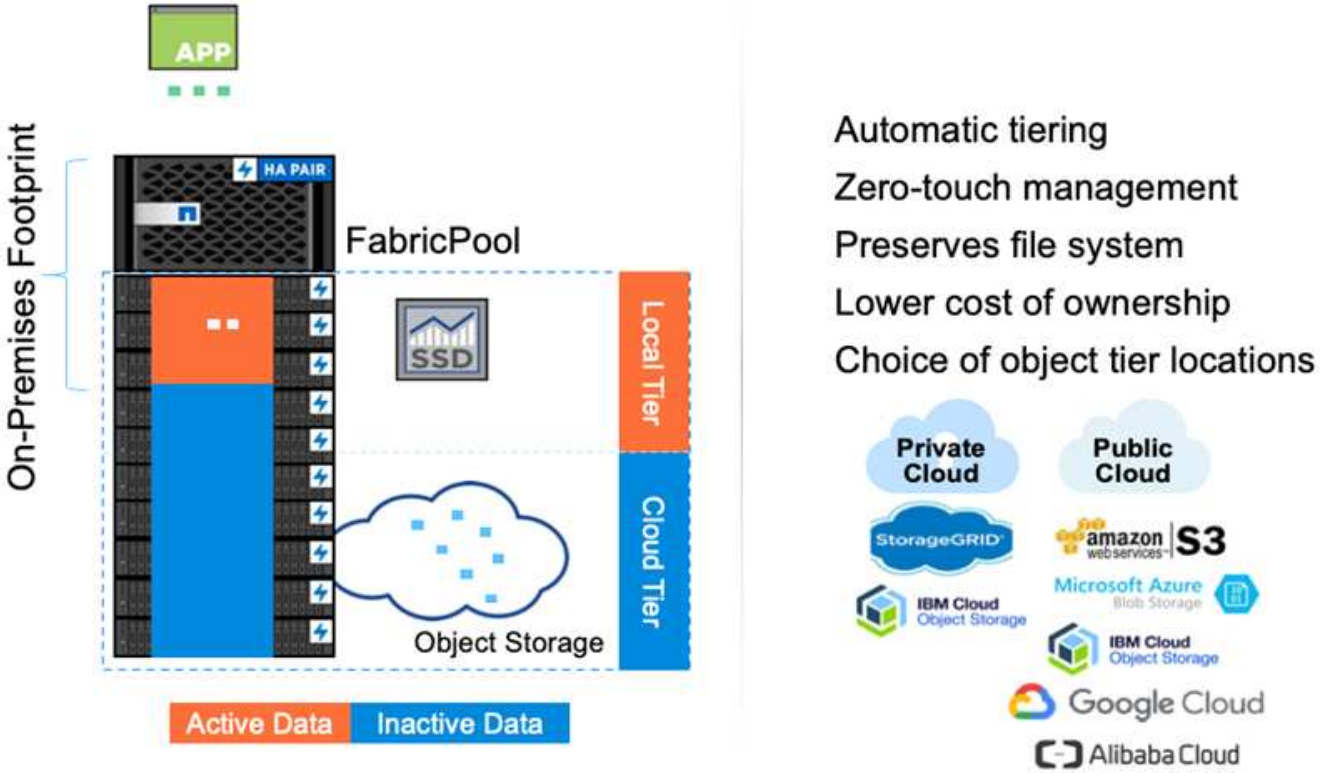
- **Multitenancy sicura.** FlexPod utilizza moduli crittografici conformi a FIPS 140-2, consentendo alle organizzazioni di implementare la sicurezza come elemento fondamentale, non come elemento secondario. FlexPod consente alle organizzazioni di implementare la multi-tenancy sicura da una singola piattaforma di infrastruttura convergente indipendentemente dalle dimensioni della piattaforma. FlexPod con multi-tenancy e QoS sicuri aiuta a separare i carichi di lavoro e a massimizzare l'utilizzo. In questo modo si evita che il capitale venga bloccato in piattaforme specializzate potenzialmente sottoutilizzate e che richiedono un set di competenze specialistiche da gestire.
- **Efficienza dello storage.** la genomica richiede che lo storage sottostante disponga di funzionalità di efficienza dello storage leader del settore. È possibile ridurre i costi dello storage con le funzionalità di efficienza dello storage NetApp come la deduplica (inline e on demand), la compressione dei dati e la compattazione dei dati ("rif"). La deduplica NetApp fornisce la deduplica a livello di blocco in un volume FlexVol. Essenzialmente, la deduplica rimuove i blocchi duplicati, memorizzando solo blocchi univoci nel volume FlexVol. La deduplica funziona con un elevato grado di granularità e opera sul file system attivo del volume FlexVol. La figura seguente mostra una panoramica del funzionamento della deduplica NetApp. La deduplica è trasparente per l'applicazione. Pertanto, può essere utilizzato per deduplicare i dati provenienti da qualsiasi applicazione che utilizzi il sistema NetApp. È possibile eseguire la deduplica del volume come processo inline e come processo in background. È possibile configurarlo in modo che venga eseguito automaticamente, pianificato o eseguito manualmente tramite CLI, Gestore di sistema NetApp ONTAP o NetApp Active IQ Unified Manager.



- **Abilitare l'interoperabilità genomica.** ONTAP FlexCache è una funzionalità di caching remoto che semplifica la distribuzione dei file, riduce la latenza della WAN e riduce i costi di larghezza di banda della WAN (. "rif"). Una delle attività chiave durante l'identificazione e l'annotazione delle varianti genomiche è la collaborazione tra i medici. La tecnologia ONTAP FlexCache aumenta il throughput dei dati anche quando i medici collaboratori si trovano in diverse aree geografiche. Data la dimensione tipica di un file *.BAM (da 1 GB a 100 GB), è fondamentale che la piattaforma sottostante possa rendere i file disponibili ai medici in

diverse aree geografiche. FlexPod con ONTAP FlexCache rende i dati genomici e le applicazioni realmente multisito, il che rende perfetta la collaborazione tra ricercatori dislocati in tutto il mondo, con bassa latenza e throughput elevato. Le organizzazioni sanitarie che eseguono applicazioni di genomica in un ambiente multisito possono scalare in orizzontale utilizzando il data fabric per bilanciare gestibilità con costi e velocità.

- **Uso intelligente della piattaforma di storage.** FlexPod con il tiering automatico ONTAP e la tecnologia Fabric Pool di NetApp semplificano la gestione dei dati. FabricPool aiuta a ridurre i costi dello storage senza compromettere performance, efficienza, sicurezza o protezione. FabricPool è trasparente per le applicazioni aziendali e sfrutta l'efficienza del cloud riducendo il TCO dello storage senza la necessità di riprogettare l'infrastruttura applicativa. FlexPod può trarre vantaggio dalle funzionalità di tiering dello storage di FabricPool per un utilizzo più efficiente dello storage flash ONTAP. Per ulteriori informazioni, vedere "FlexPod con FabricPool". Il seguente diagramma fornisce una panoramica di alto livello di FabricPool e dei suoi vantaggi.

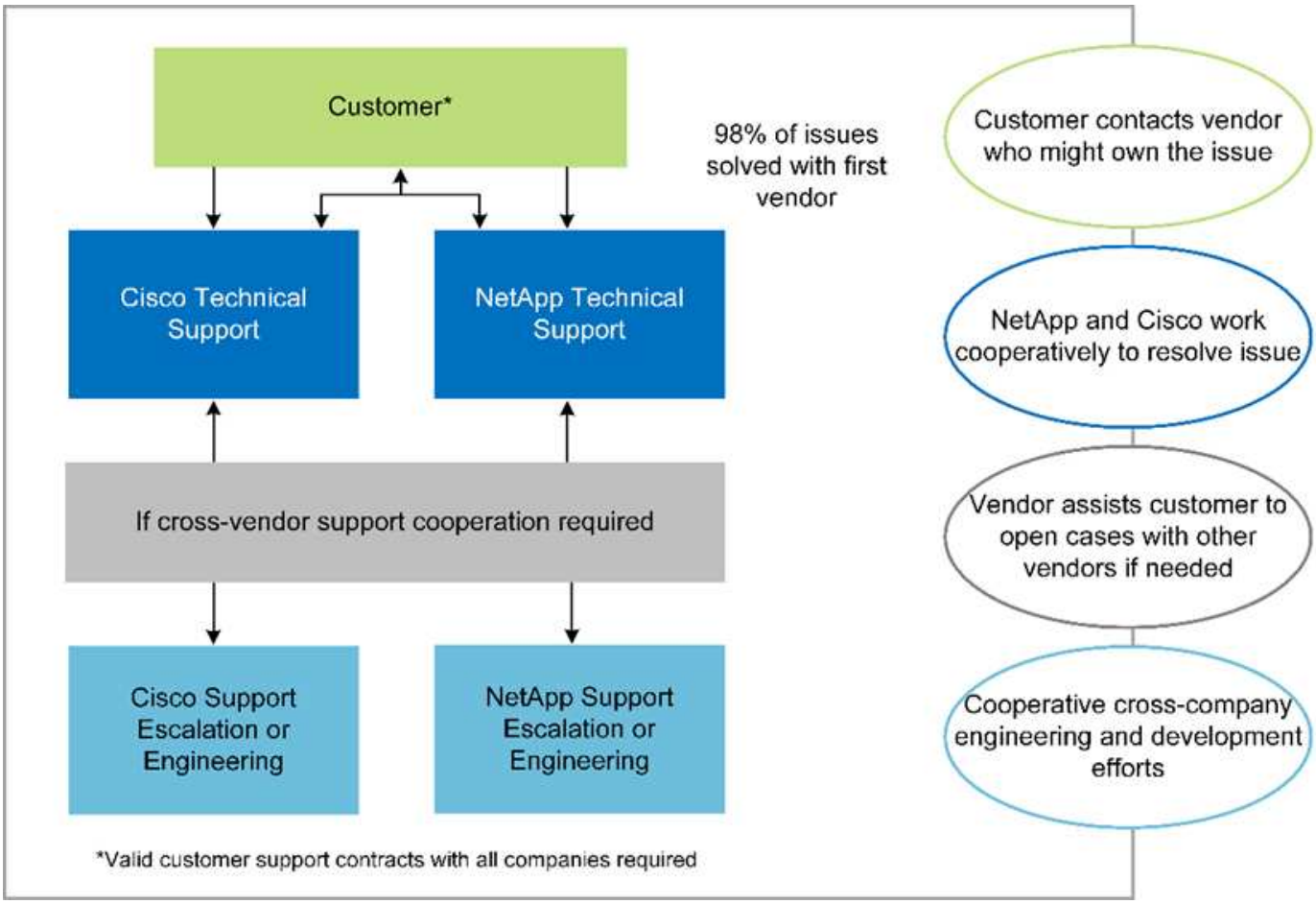


- **Analisi e annotazione delle varianti più rapide.** la piattaforma FlexPod è più veloce da implementare e da rendere operativa. La piattaforma FlexPod consente la collaborazione tra medici rendendo i dati disponibili su larga scala con bassa latenza e throughput aumentato. Una maggiore interoperabilità favorisce l'innovazione. Le organizzazioni del settore sanitario possono eseguire i workload genomici e non genomici in maniera affiancata, il che significa che le organizzazioni non hanno bisogno di piattaforme specializzate per iniziare il loro percorso di genomica.

  FlexPod ONTAP aggiunge regolarmente funzionalità all'avanguardia alla piattaforma di storage. FlexPod Datacenter è la base ottimale per l'implementazione di FC-NVMe per consentire l'accesso allo storage dalle performance elevate alle applicazioni che ne hanno bisogno. Poiché FC- NVMe si evolve per includere alta disponibilità, multipathing e supporto aggiuntivo del sistema operativo, FlexPod è la piattaforma scelta, fornendo la scalabilità e l'affidabilità necessarie per supportare queste funzionalità. ONTAP con i/o più veloce con NVMe end-to-end consente di completare più rapidamente le analisi genomiche ("rif").

I dati del genoma raw in sequenza producono file di grandi dimensioni ed è importante che questi file siano resi disponibili agli analizzatori delle varianti per ridurre il tempo totale necessario dalla raccolta dei campioni all'annotazione delle varianti. NVMe (nonvolatile memory express), se utilizzato come protocollo di accesso allo storage e di trasporto dei dati, offre livelli di throughput senza precedenti e tempi di risposta più rapidi. FlexPod implementa il protocollo NVMe durante l'accesso allo storage flash tramite il bus PCI Express (PCIe). PCIe consente l'implementazione di decine di migliaia di code di comandi, aumentando la parallelizzazione e il throughput. Un singolo protocollo, dallo storage alla memoria, consente di accedere rapidamente ai dati.

- **L'agilità per la ricerca clinica da zero.** la capacità e le performance di storage flessibili ed espandibili consentono alle organizzazioni di ricerca nel settore sanitario di ottimizzare l'ambiente in modo elastico o JIT (Just-in-Time). Disaccoppiando lo storage dall'infrastruttura di calcolo e di rete, la piattaforma FlexPod può essere scalata verso l'alto e verso l'esterno senza interruzioni. Grazie a Cisco Intersight, la piattaforma FlexPod può essere gestita con flussi di lavoro automatizzati integrati e personalizzati. I flussi di lavoro di Cisco Intersight consentono alle organizzazioni sanitarie di ridurre i tempi di gestione del ciclo di vita delle applicazioni. Quando un centro medico accademico richiede che i dati dei pazienti siano anonimi e resi disponibili al proprio centro per la ricerca informatica e/o il centro per la qualità, l'organizzazione IT può sfruttare i flussi di lavoro di Cisco Intersight FlexPod per eseguire backup dei dati sicuri, clonare e ripristinare in pochi secondi, non ore. Con NetApp Trident e Kubernetes, le organizzazioni IT possono eseguire il provisioning di nuovi data scientist e rendere disponibili i dati clinici per lo sviluppo dei modelli in pochi minuti, talvolta anche in pochi secondi.
- **Protezione dei dati genoma.** NetApp SnapLock offre un volume speciale in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non riscrivibile. I dati di produzione dell'utente che risiedono in un volume FlexVol possono essere mirrorati o archiviati in un volume SnapLock tramite la tecnologia NetApp SnapMirror o SnapVault. I file nel volume SnapLock, nel volume stesso e nel relativo aggregato di hosting non possono essere cancellati fino alla fine del periodo di conservazione. Utilizzando il software ONTAP FPolicy, le organizzazioni possono prevenire gli attacchi ransomware impedendo operazioni su file con estensioni specifiche. È possibile attivare un evento FPolicy per operazioni di file specifiche. L'evento è legato a una policy, che richiama il motore che deve utilizzare. È possibile configurare un criterio con una serie di estensioni di file che potrebbero contenere ransomware. Quando un file con un'estensione non consentita tenta di eseguire un'operazione non autorizzata, FPolicy impedisce l'esecuzione di tale operazione ("rif").
- **Supporto congiunto di FlexPod.** NetApp e Cisco hanno definito il supporto congiunto di FlexPod, un modello di supporto forte, scalabile e flessibile per soddisfare i requisiti di supporto esclusivi dell'infrastruttura convergente di FlexPod. Questo modello utilizza l'esperienza, le risorse e l'esperienza di supporto tecnico di NetApp e Cisco per offrire un processo ottimizzato per l'identificazione e la risoluzione dei problemi di supporto FlexPod, indipendentemente dalla posizione del problema. La figura seguente fornisce una panoramica del modello di supporto cooperativo FlexPod. Il cliente contatta il vendor che potrebbe essere responsabile del problema e Cisco e NetApp lavorano in collaborazione per risolverlo. Cisco e NetApp dispongono di team di sviluppo e progettazione multiazienda che lavorano insieme per risolvere i problemi. Questo modello di supporto riduce la perdita di informazioni durante la traduzione, garantisce fiducia e riduce i tempi di inattività.

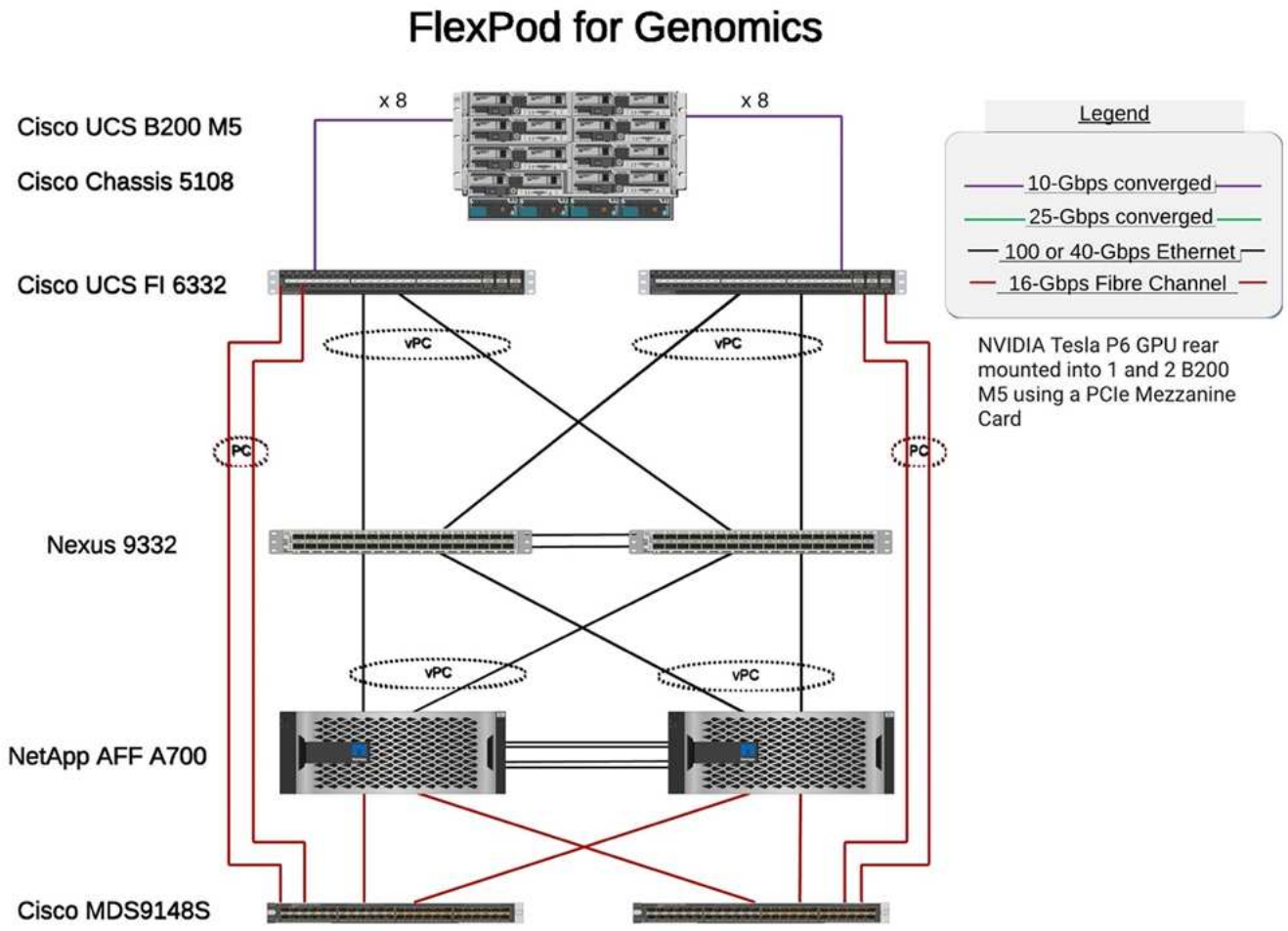


"Avanti: Componenti hardware e software dell'infrastruttura della soluzione."

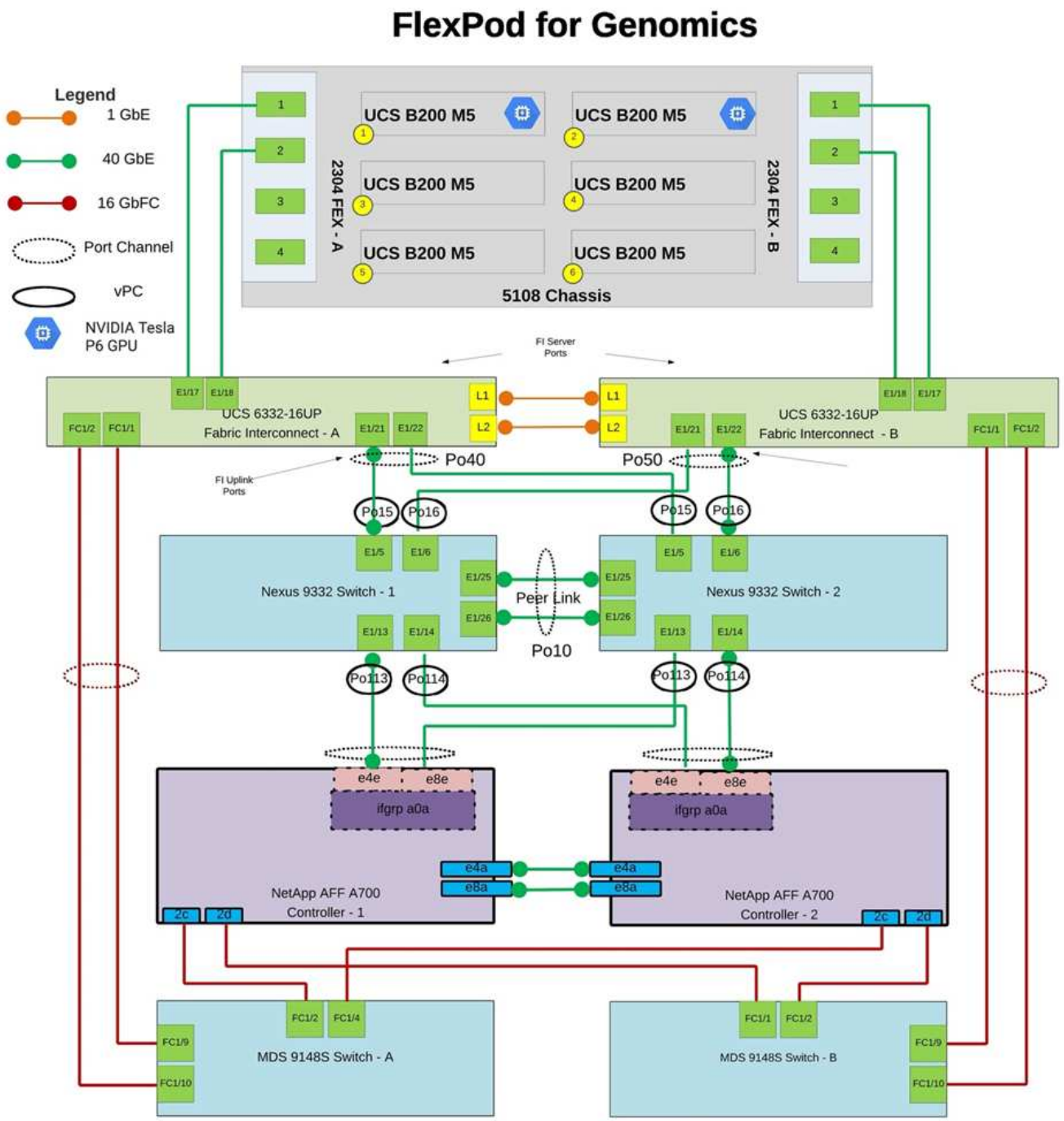
Componenti hardware e software dell'infrastruttura della soluzione

"Precedente: Vantaggi dell'implementazione di workload genomici su FlexPod."

La figura seguente mostra il sistema FlexPod utilizzato per la configurazione e la convalida di GATK. Abbiamo utilizzato "Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante il processo di configurazione.



Il seguente diagramma illustra i dettagli del cablaggio FlexPod.



La seguente tabella elenca i componenti hardware utilizzati durante il test GATK abilitando su un FlexPod. Ecco il "Tool di matrice di interoperabilità NetApp" (IMT) e. "Cisco hardware Compatibility List (HCL) (elenco compatibilità hardware Cisco)".

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1 o 2	
	Blade server Cisco UCS	6 B200 M5	Ciascuno con 2 core da 20 o più, 2,7 GHz e 128 GB di RAM

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Vedere
	2 interconnessioni fabric Cisco UCS	6332	-
Rete	Switch Cisco Nexus	2 Cisco Nexus 9332	-
Rete di storage	Rete IP per l'accesso allo storage su protocolli SMB/CIFS, NFS o iSCSI	Stessi switch di rete come sopra	-
	Accesso allo storage tramite FC	2 Cisco MDS 9148S	-
Storage	Sistema storage all-flash NetApp AFF A700	1 cluster	Cluster con due nodi
	Shelf di dischi	Uno shelf di dischi DS224C o NS224	Completamente popolato con 24 dischi
	SSD	Capacità di 24, 1,2 TB o superiore	-

Questa tabella elenca il software dell'infrastruttura.

Software	Famiglia di prodotti	Versione o release	Dettagli
Vari	Linux	RHEL 8.3	-
	Windows	Windows Server 2012 R2 (64 bit)	-
	NetApp ONTAP	ONTAP 9.8 o versione successiva	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 o versione successiva	-
	Switch Cisco Ethernet serie 3000 o 9000	Per la serie 9000, 7.0(3)I7(7) o versioni successive per la serie 3000, 9.2(4) o versioni successive	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o successiva	-
	Hypervisor	VMware vSphere ESXi 7.0	-
Storage	Sistema di gestione dell'hypervisor	VMware vCenter Server 7.0 (vCSA) o versione successiva	-
Rete	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	-

Software	Famiglia di prodotti	Versione o release	Dettagli
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	-
	Cisco UCS Manager	4.1(3c) o versione successiva	
Hypervisor	ESXi		
Gestione	Sistema di gestione dell'hypervisor VMware vCenter Server 7.0 (vCSA) o versione successiva		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	
	Cisco UCS Manager	4.1(3c) o versione successiva	

"Next: Genomica - Installazione ed esecuzione di GATK."

Genomica - Installazione ed esecuzione di GATK

"Precedente: Componenti hardware e software dell'infrastruttura della soluzione."

Secondo il National Human Genome Research Institute ("NHGRI"), "la genomica è lo studio di tutti i geni di una persona (il genoma), comprese le interazioni di questi geni tra loro e con l'ambiente di una persona. "

In base a. "NHGRI"L'acido desossiribonucleico (DNA) è il composto chimico che contiene le istruzioni necessarie per sviluppare e dirigere le attività di quasi tutti gli organismi viventi. Le molecole di DNA sono costituite da due trefoli torcenti accoppiati, spesso indicati come a doppia elica". "Il set completo di DNA di un organismo è chiamato genoma".

Il sequenziamento è il processo di determinazione dell'ordine esatto delle basi in un filamento di DNA. Uno dei tipi più comuni di sequenziamento oggi utilizzato è chiamato sequenziamento per sintesi. Questa tecnica utilizza l'emissione di segnali fluorescenti per ordinare le basi. I ricercatori possono utilizzare il sequenziamento del DNA per cercare variazioni genetiche e qualsiasi mutazione che possa svolgere un ruolo nello sviluppo o nella progressione di una malattia mentre una persona è ancora nello stadio embrionale.

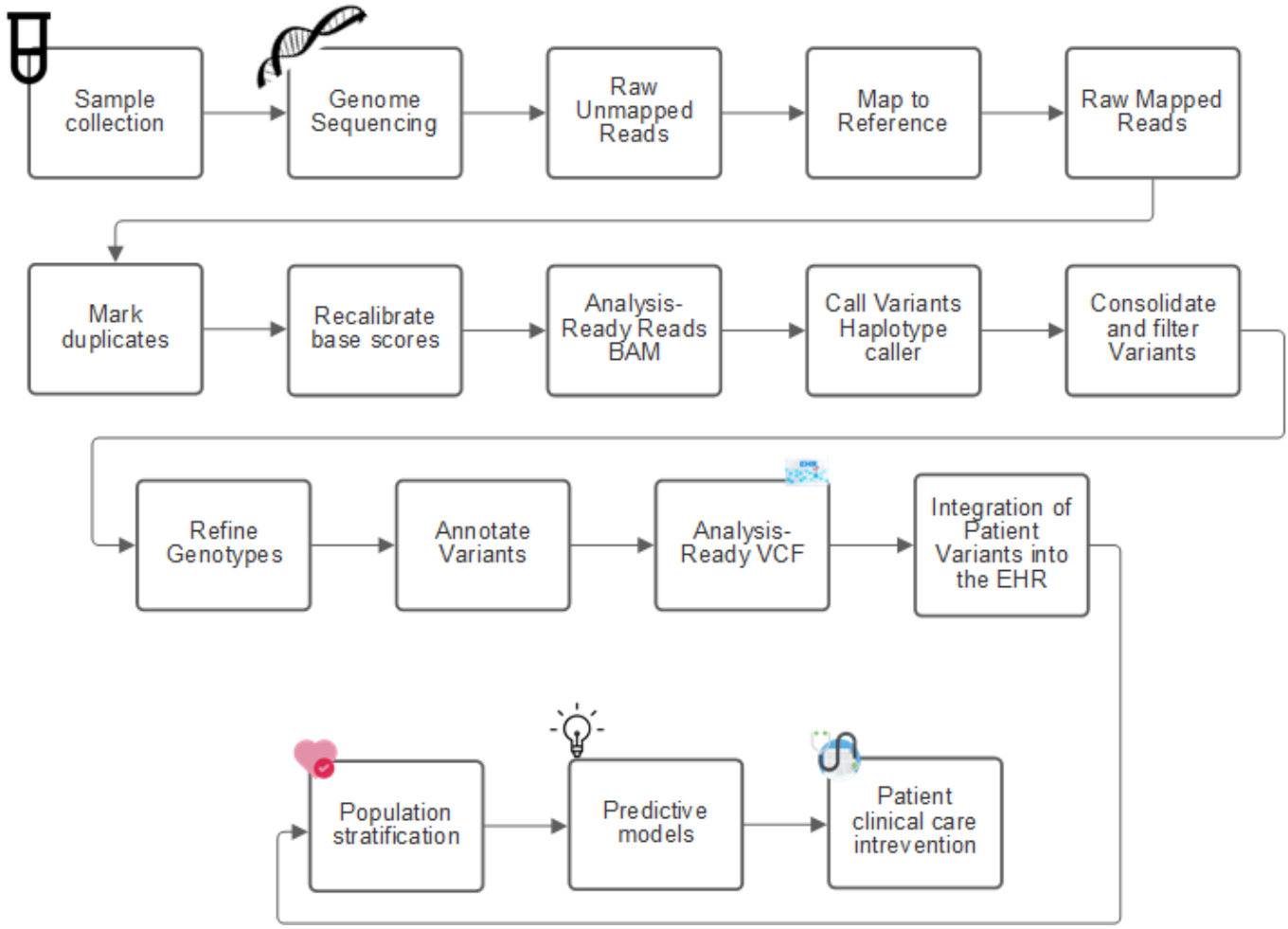
Dall'identificazione del campione alla variante, all'annotazione e alla previsione

Ad alto livello, la genomica può essere classificata nei seguenti passaggi. Questo non è un elenco completo:

1. Raccolta dei campioni.
2. "Sequenziamento del genoma" utilizzo di un sequencer per generare i dati raw.
3. Pre-elaborazione. Ad esempio, "deduplica" utilizzo di "Picard".
4. Analisi genomica.

   a. Mappatura a un genoma di riferimento.
   b. "Variante" L'identificazione e l'annotazione vengono in genere eseguite utilizzando GATK e strumenti simili.
5. Integrazione nel sistema di cartelle cliniche elettroniche (EHR).
6. "Stratificazione della popolazione" e identificazione della variazione genetica attraverso la posizione geografica e il background etnico.
7. "Modelli predittivi" utilizzando un significativo polimorfismo a singolo nucleotide.
8. "Convalida".

La figura seguente mostra il processo che va dal campionamento all'identificazione della variante, all'annotazione e alla previsione.



Il progetto Human Genome è stato completato nell'aprile 2003 e il progetto ha realizzato una simulazione di altissima qualità della sequenza di genomi umani disponibile in pubblico dominio. Questo genoma di riferimento ha dato inizio a un'esplosione nella ricerca e nello sviluppo delle capacità genomiche. Praticamente ogni disturbo umano ha una firma nei geni di quell'essere umano. Fino a poco tempo fa, i medici utilizzavano i geni per predire e determinare i difetti congeniti come l'anemia falciforme, causata da un certo schema di ereditarietà causato da un cambiamento in un singolo gene. Il tesoro dei dati messi a disposizione dal progetto sul genoma umano ha portato all'avvento dello stato attuale delle capacità genomiche.

La genomica offre una vasta gamma di vantaggi. Ecco una piccola serie di vantaggi nei settori sanitario e delle scienze biologiche:

- Migliore diagnosi presso i punti di cura
- Migliore prognosi
- Medicina di precisione
- Piani di trattamento personalizzati
- Migliore monitoraggio delle malattie
- Riduzione degli eventi avversi
- Migliore accesso alle terapie
- Miglioramento del monitoraggio delle malattie
- Partecipazione efficace agli studi clinici e migliore selezione dei pazienti per gli studi clinici basati sui genotipi.

La genomica è un "bestia a quattro teste," a causa delle esigenze di calcolo per tutto il ciclo di vita di un set di dati: acquisizione, storage, distribuzione e analisi.

GATK (Genome Analysis Toolkit)

GATK è stata sviluppata come piattaforma per la data science presso "Broad Institute". GATK è un insieme di strumenti open-source che consentono l'analisi del genoma, in particolare rilevamento, identificazione, annotazione e genotipizzazione delle varianti. Uno dei vantaggi di GATK è che il set di strumenti e/o comandi può essere concatenato per formare un workflow completo. Le principali sfide affrontate da un ampio istituto sono le seguenti:

- Comprendere le cause alla radice e i meccanismi biologici delle malattie.
- Identificare gli interventi terapeutici che agiscono alla causa fondamentale di una malattia.
- Comprendere la linea di vista dalle varianti al funzionamento in fisiologia umana.
- Creare standard e policy "framework" per la rappresentazione dei dati genoma, lo storage, l'analisi, la sicurezza e così via.
- Standardizzare e socializzare database di aggregazione dei genomi interoperabili (gnomAD).
- Monitoraggio, diagnosi e trattamento dei pazienti basati sul genoma con maggiore precisione.
- Aiuta a implementare strumenti che prevedano le malattie ben prima che appaiano i sintomi.
- Crea e potenzia una community di collaboratori interdisciplinari per affrontare i problemi più difficili e importanti della biomedicina.

Secondo il GATK e l'ampio istituto, il sequenziamento del genoma deve essere trattato come un protocollo in un laboratorio di patologia; ogni attività è ben documentata, ottimizzata, riproducibile e coerente tra campioni ed esperimenti. Di seguito viene riportata una serie di procedure consigliate dal Broad Institute. Per ulteriori informazioni, vedere "Sito web di GATK".

Configurazione di FlexPod

La convalida del carico di lavoro di genomics include una configurazione da zero di una piattaforma di infrastruttura FlexPod. La piattaforma FlexPod è altamente disponibile e può essere scalata in modo indipendente; ad esempio, la rete, lo storage e il calcolo possono essere scalati in modo indipendente. Abbiamo utilizzato la seguente guida alla progettazione convalidata da Cisco come documento di riferimento sull'architettura per configurare l'ambiente FlexPod: "Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7". Scopri i seguenti punti salienti della configurazione della piattaforma FlexPod:

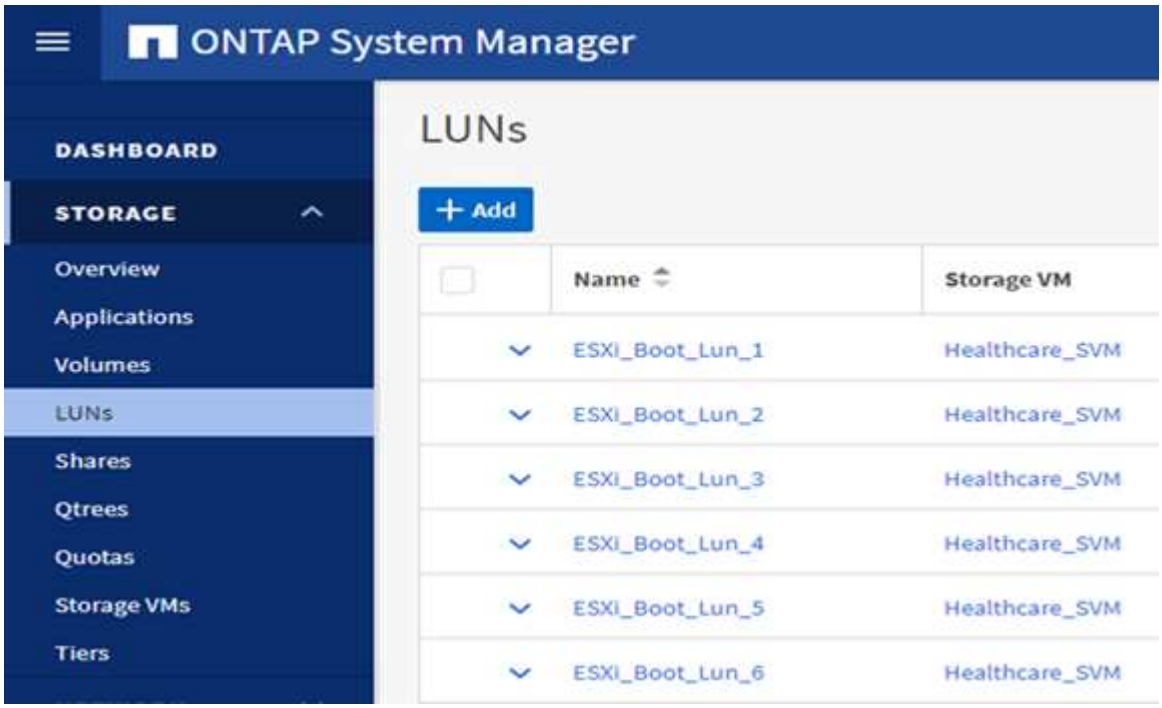
Per eseguire la configurazione del laboratorio FlexPod, attenersi alla seguente procedura:

1. La configurazione e la convalida del laboratorio FlexPod utilizza le seguenti prenotazioni IP4 e VLAN.

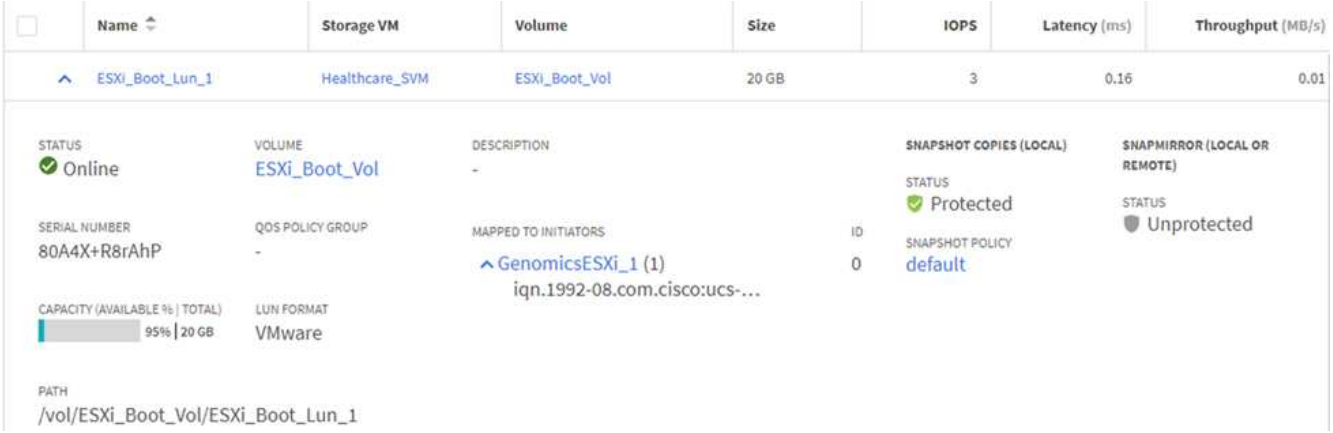
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. Configurare le LUN di avvio basate su iSCSI sulla SVM ONTAP.

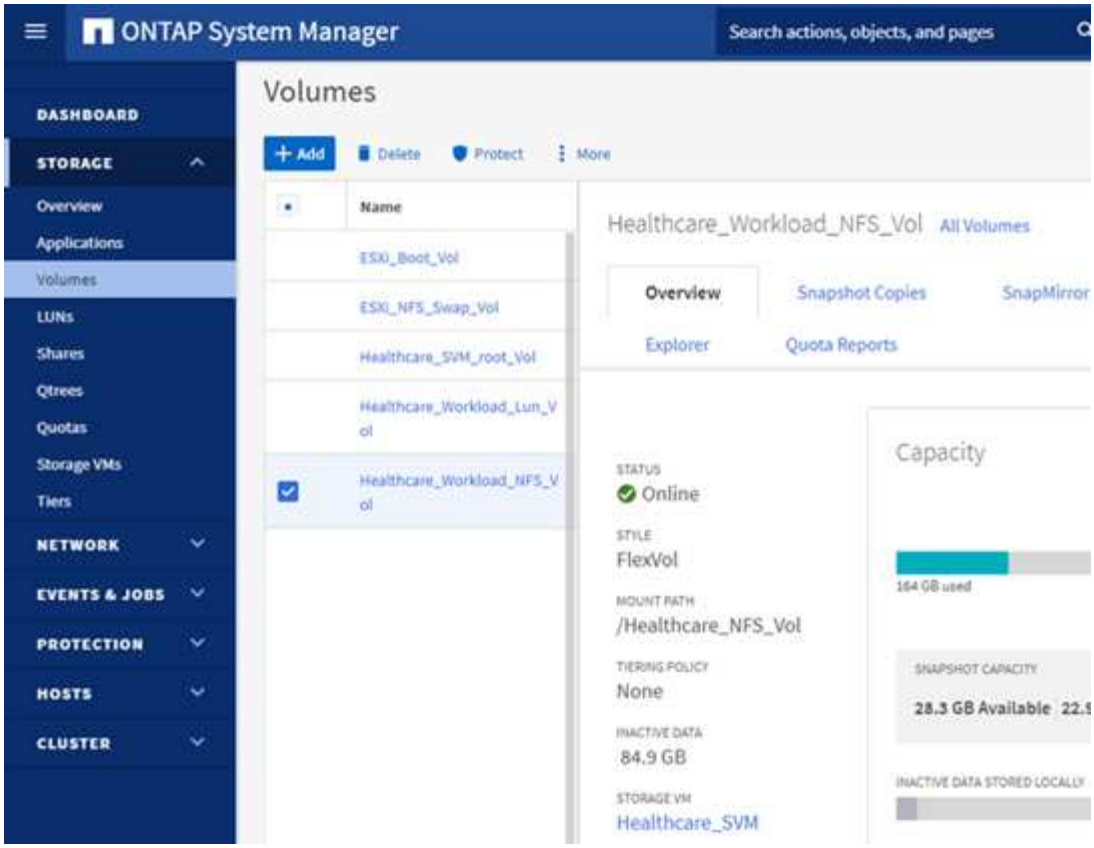


3. Mappare i LUN ai gruppi di iniziatori iSCSI.

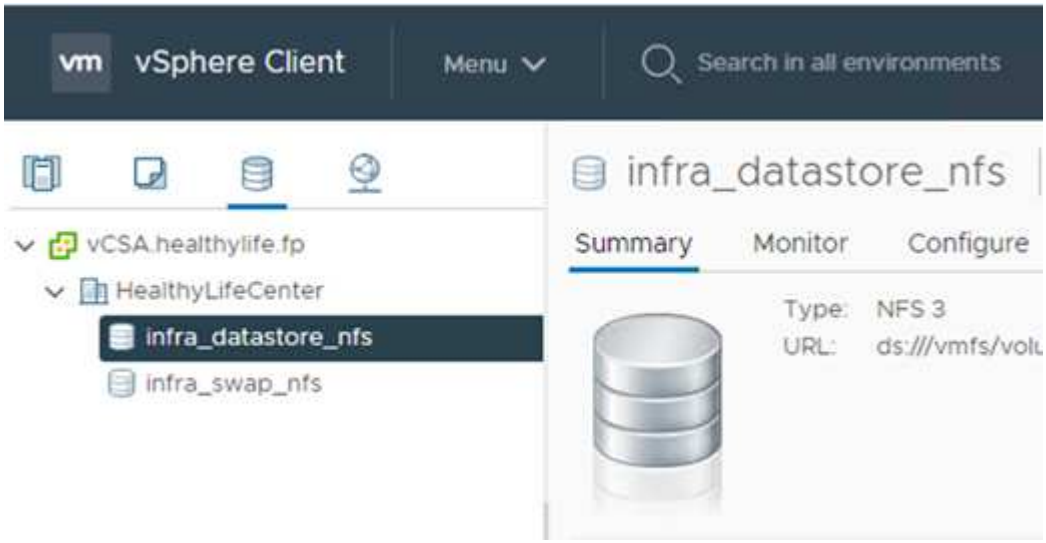


4. Installare vSphere 7.0 con l'avvio iSCSI.
5. Registrare gli host ESXi con vCenter.

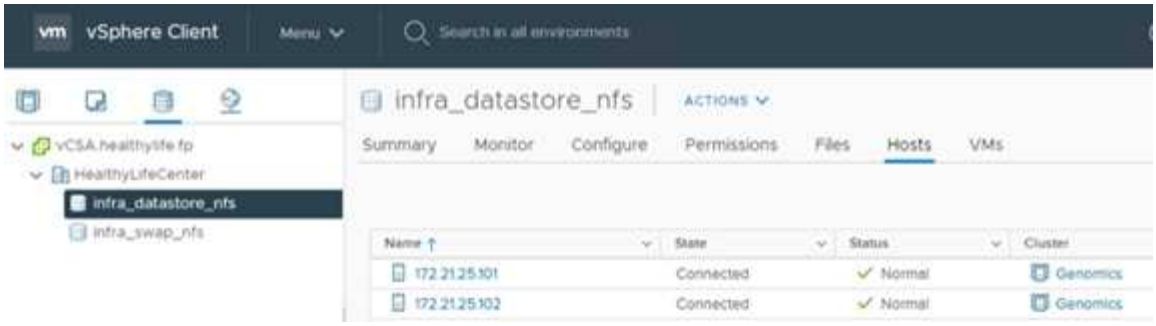
6. Eseguire il provisioning di un datastore NFS `infra_datastore_nfs` Sullo storage ONTAP.



7. Aggiungere il datastore al vCenter.



8. Utilizzando vCenter, aggiungere un datastore NFS agli host ESXi.



9. Utilizzando vCenter, creare una macchina virtuale Red Hat Enterprise Linux (RHEL) 8.3 per eseguire GATK.
10. Un datastore NFS viene presentato alla macchina virtuale e montato su `/mnt/genomics`, Utilizzato per memorizzare file eseguibili GATK, script, file BAM (Binary Alignment Map), file di riferimento, file di indice, file del dizionario e file out per la chiamata delle varianti.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb                308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

Configurazione ed esecuzione di GATK

Installare i seguenti prerequisiti su RedHat Enterprise 8.3 Linux VM:

- Java 8 o SDK 1.8 o versione successiva
- Scarica GATK 4.2.0.0 dal Broad Institute "Sito GitHub". I dati della sequenza genoma sono generalmente memorizzati sotto forma di una serie di colonne ASCII delimitate da tabulazioni. Tuttavia, ASCII occupa troppo spazio per la memorizzazione. Pertanto, un nuovo standard evoluto chiamato file BAM (**.bam). Un file BAM memorizza i dati della sequenza in un formato compresso, indicizzato e binario. Noi "scaricato" Un insieme di file BAM disponibili pubblicamente per l'esecuzione di GATK da "di dominio pubblico". Abbiamo anche scaricato file di indice (**.bai), file di dizionario (**. dict) e file di dati di riferimento (**. fasta) dello stesso dominio pubblico.

Dopo il download, il kit di strumenti GATK ha un file jar e una serie di script di supporto.

- `gatk-package-4.2.0.0-local.jar` eseguibile
- `gatk` file di script.

Abbiamo scaricato i file BAM e i corrispondenti file di indice, dizionario e genoma di riferimento per una famiglia composta da file *.bam padre, madre e figlio.

Motore Cromwell

Cromwell è un motore open-source orientato ai flussi di lavoro scientifici che consente la gestione del workflow. Il motore Cromwell può essere eseguito in due "modalità", Server mode o Run mode a singolo flusso di lavoro. Il comportamento del motore Cromwell può essere controllato tramite "File di configurazione del motore Cromwell".

- **Server mode.** attiva "Riposante" Esecuzione dei flussi di lavoro nel motore Cromwell.
- **Run mode.** la modalità Run è più adatta per l'esecuzione di singoli flussi di lavoro in Cromwell, "rif" Per una serie completa di opzioni disponibili in modalità Run.

Utilizziamo il motore Cromwell per eseguire flussi di lavoro e pipeline su larga scala. Il motore Cromwell utilizza un sistema intuitivo "linguaggio di descrizione del workflow" Linguaggio di scripting basato su (WDL). Cromwell supporta anche un secondo standard di scripting per il workflow, denominato Common workflow Language (CWL). Nel corso di questo report tecnico, abbiamo utilizzato WDL. WDL è stato originariamente sviluppato dal Broad Institute for Genome analysis Pipeline. I flussi di lavoro WDL possono essere implementati utilizzando diverse strategie, tra cui:

- **Linear Chaining.** come suggerisce il nome, l'output dell'attività n. 1 viene inviato all'attività n. 2 come input.
- **Multi-in/out.** questo è simile al concatenamento lineare in quanto ogni task può avere più output inviati come input a task successivi.
- **Scatter-Gather.** si tratta di una delle strategie di integrazione applicativa aziendale (EAI) più potenti disponibili, soprattutto se utilizzata in un'architettura basata sugli eventi. Ogni task viene eseguito in modo disaccoppiato e l'output di ogni task viene consolidato nell'output finale.

Quando si utilizza WDL per eseguire GATK in una modalità standalone, sono disponibili tre passaggi:

1. Validare la sintassi utilizzando `womtool.jar`.

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. Generare input JSON.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Eseguire il flusso di lavoro utilizzando il motore Cromwell e. `Cromwell.jar`.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

Il GATK può essere eseguito utilizzando diversi metodi; questo documento esplora tre di questi metodi.

Esecuzione di GATK utilizzando il file jar

Esaminiamo ora l'esecuzione di una singola pipeline di chiamate con il chiamante della variante haplotype.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

In questo metodo di esecuzione, utilizziamo il file jar di esecuzione locale di GATK, utilizziamo un singolo comando java per richiamare il file jar e passiamo diversi parametri al comando.

1. Questo parametro indica che stiamo richiamando `HaplotypeCaller` pipeline chiamante variante.
2. `-- input` Specifica il file BAM di input.
3. `--output` specifica il file di output della variante nel formato di chiamata della variante (*.vcf) ("rif").
4. Con `--reference` parametro, stiamo passando un genoma di riferimento.

Una volta eseguita l'operazione, i dettagli dell'output sono disponibili nella sezione "Output per l'esecuzione di GATK utilizzando il file jar."

Esecuzione di GATK utilizzando lo script ./gatk

Il kit di strumenti GATK può essere eseguito utilizzando `./gatk` script. Esaminiamo il seguente comando:

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

Passiamo diversi parametri al comando.

- Questo parametro indica che stiamo richiamando `HaplotypeCaller` pipeline chiamante variante.
- `-I` Specifica il file BAM di input.
- `-O` specifica il file di output della variante nel formato di chiamata della variante (*.vcf) ("rif").
- Con `-R` parametro, stiamo passando un genoma di riferimento.

Una volta eseguita l'operazione, i dettagli dell'output sono disponibili nella sezione

Esecuzione di GATK utilizzando il motore Cromwell

Utilizziamo il motore Cromwell per gestire l'esecuzione di GATK. Esaminiamo la riga di comando e i relativi parametri.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

In questo caso, viene richiamato il comando Java passando a. `-jar` parametro per indicare che si intende eseguire un file jar, ad esempio `Cromwell-65.jar`. Il parametro successivo è stato superato (`run`) Indica che il motore Cromwell è in esecuzione in modalità Run, mentre l'altra opzione possibile è la modalità Server. Il parametro successivo è `*.wdl` Che la modalità Run debba utilizzare per eseguire le pipeline. Il parametro successivo è l'insieme di parametri di input per i flussi di lavoro in esecuzione.

Di seguito sono elencati i contenuti di `ghplo.wdl` file simile a:

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

Ecco il file JSON corrispondente con gli input al motore Cromwell.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Tenere presente che Cromwell utilizza un database in-memory per l'esecuzione. Una volta eseguito, il log di output viene visualizzato nella sezione "Output per l'esecuzione di GATK utilizzando il motore Cromwell."

Per una serie completa di passaggi su come eseguire GATK, vedere "Documentazione GATK".

"Successivo: Output per l'esecuzione di GATK utilizzando il file jar."

Output per l'esecuzione di GATK utilizzando il file jar

"Precedente: Genomica - impostazione ed esecuzione di GATK."

L'esecuzione di GATK utilizzando il file jar ha prodotto il seguente output di esempio.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
```

```
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
```

```
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

Si noti che il file di output si trova nella posizione specificata dopo l’esecuzione.

Output per l’esecuzione di GATK utilizzando lo script ./gatk

"Precedente: Output per l’esecuzione di GATK utilizzando il file jar."

L'esecuzione di GATK utilizzando `./gatk` lo script ha prodotto il seguente output di esempio.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
```

```
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
```

```
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

Si noti che il file di output si trova nella posizione specificata dopo l'esecuzione.

"Avanti: Output per l'esecuzione di GATK utilizzando il motore Cromwell."

Output per l'esecuzione di GATK utilizzando il motore Cromwell

L'esecuzione di GATK utilizzando il motore Cromwell ha prodotto il seguente output di esempio.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
  "cromwellId" : "cromid-41b7e30",
```

```
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
helloHaplotypeCaller.haplotypeCaller
```

```
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
{
  "outputs": {
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
```

```
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
messages to process
```

```
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"Avanti: Configurazione della GPU."

Configurazione della GPU

"Precedente: Output per l'esecuzione di GATK utilizzando il motore Cromwell."

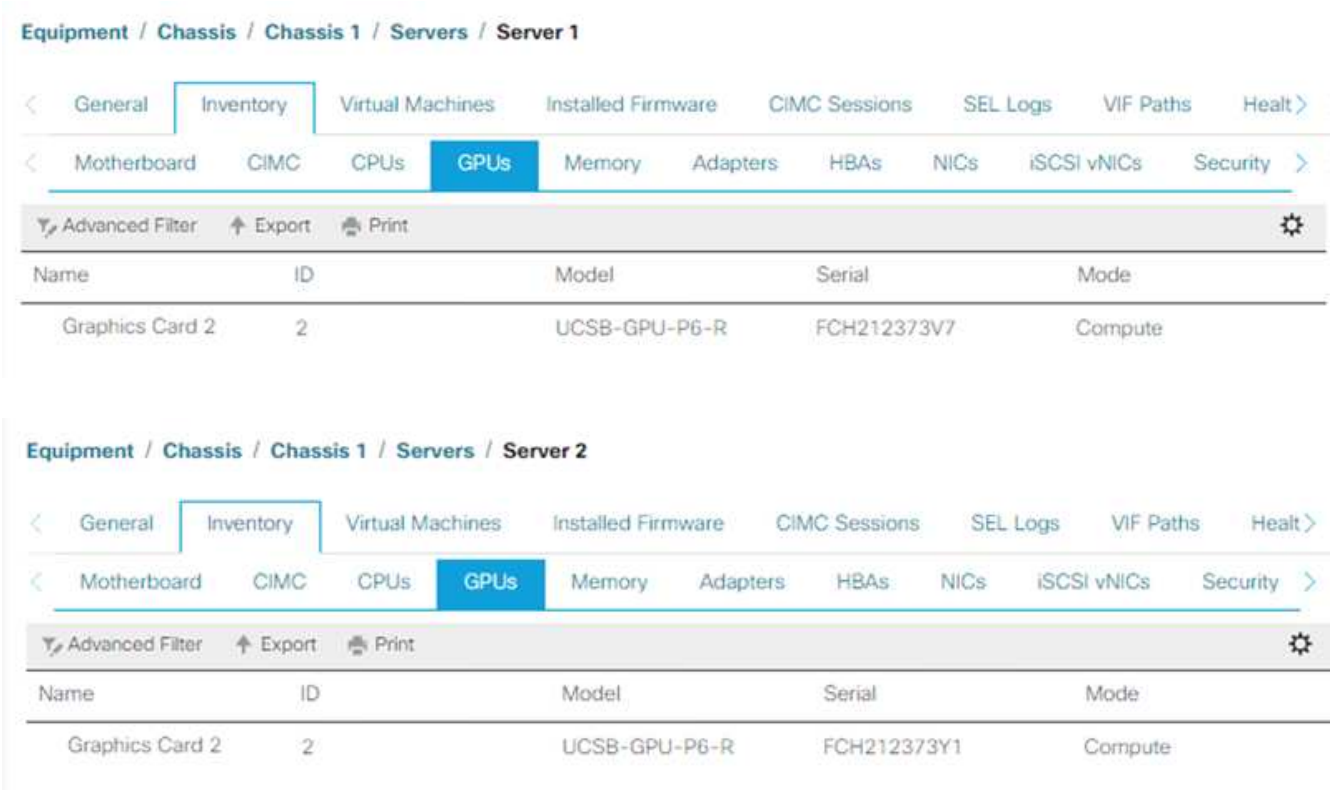
Al momento della pubblicazione, il tool GATK non supporta in modo nativo l'esecuzione on-premise basata su GPU. La seguente configurazione e guida consentono ai lettori di comprendere quanto sia semplice utilizzare FlexPod con una GPU NVIDIA Tesla P6 montata sul retro utilizzando una scheda mezzanine PCIe per GATK.

Abbiamo utilizzato il seguente progetto validato da Cisco (CVD) come architettura di riferimento e guida alle Best practice per configurare l'ambiente FlexPod in modo da poter eseguire applicazioni che utilizzano GPU.

- "Data center FlexPod per ai/ML con Cisco UCS 480 ML per l'apprendimento approfondito"

Ecco una serie di punti chiave durante questa configurazione:

1. Abbiamo utilizzato una GPU NVIDIA Tesla P6 PCIe in uno slot mezzanino nei server UCS B200 M5.



2. Per questa configurazione, ci siamo registrati sul portale partner NVIDIA e abbiamo ottenuto una licenza di

valutazione (nota anche come diritto) per poter utilizzare le GPU in modalità di calcolo.

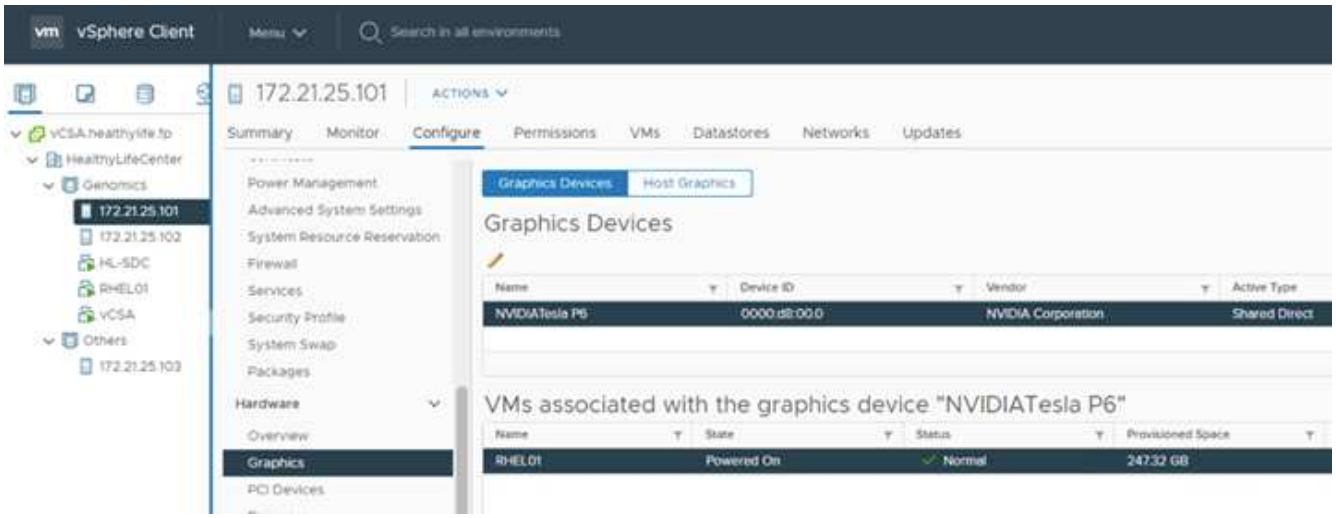
3. Il software NVIDIA vGPU richiesto è stato scaricato dal sito Web del partner NVIDIA.
4. Abbiamo scaricato i diritti `*.bin` Dal sito web del partner NVIDIA.
5. Abbiamo installato un server di licenza NVIDIA vGPU e aggiunto le autorizzazioni al server di licenza utilizzando `*.bin` File scaricato dal sito del partner NVIDIA.
6. Assicurarsi di scegliere la versione software NVIDIA vGPU corretta per l'implementazione sul portale dei partner NVIDIA. Per questa configurazione è stata utilizzata la versione del driver 460.73.02.
7. Questo comando installa "NVIDIA vGPU Manager" In ESXi.

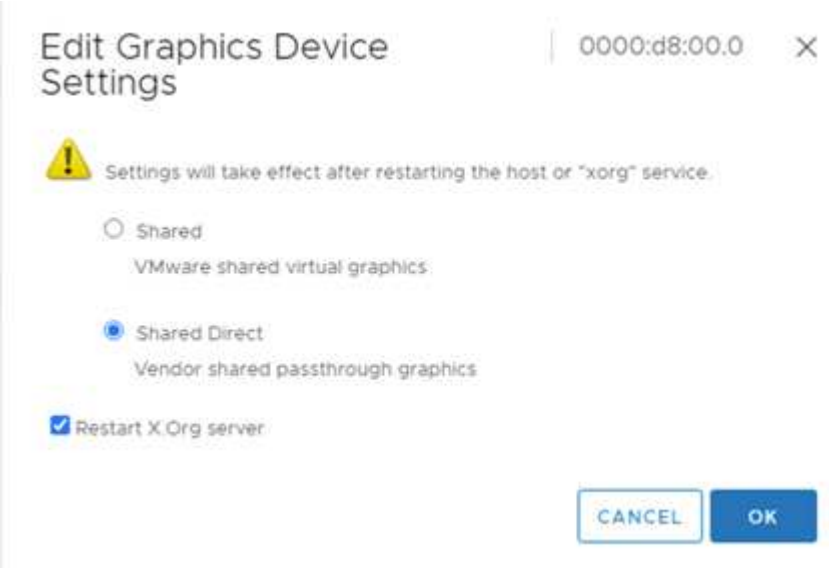
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. Dopo aver riavviato il server ESXi, eseguire il seguente comando per convalidare l'installazione e controllare lo stato delle GPU.

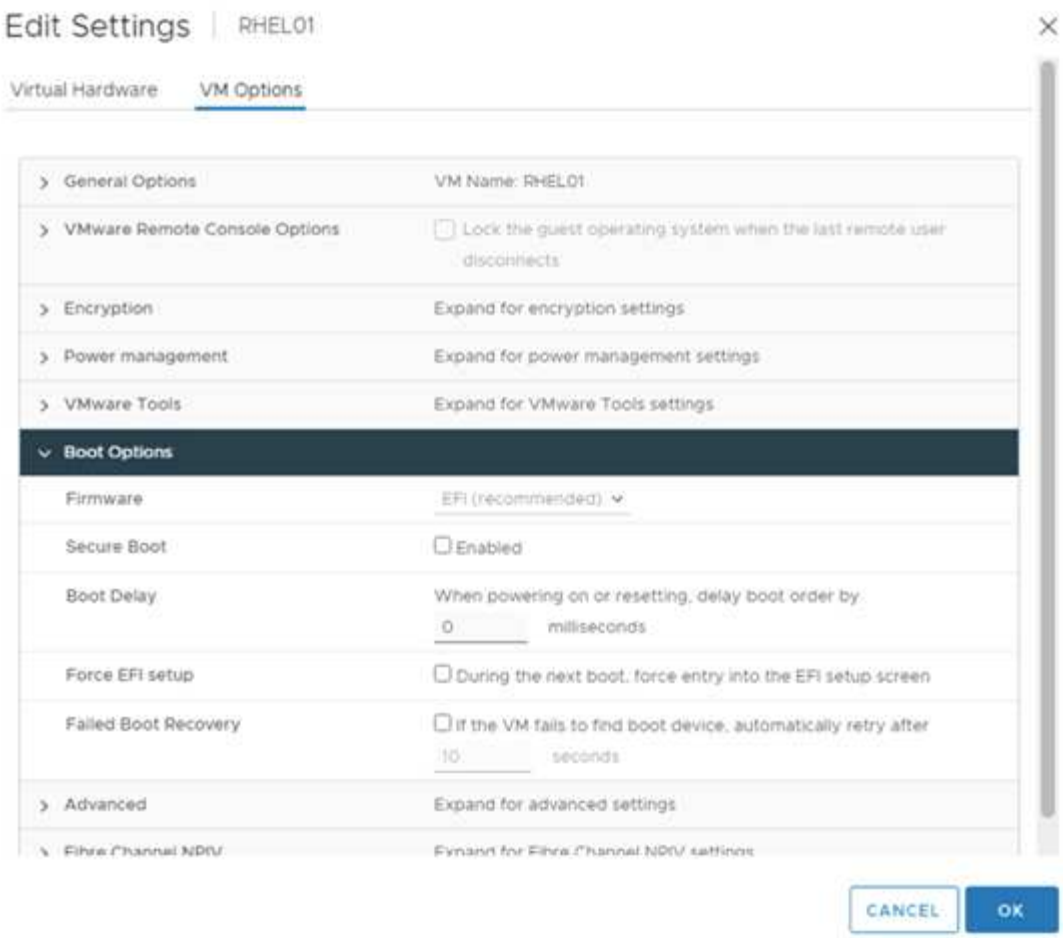
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. Utilizzando vCenter, "configurare" L'impostazione del dispositivo grafico è "Shared Direct".





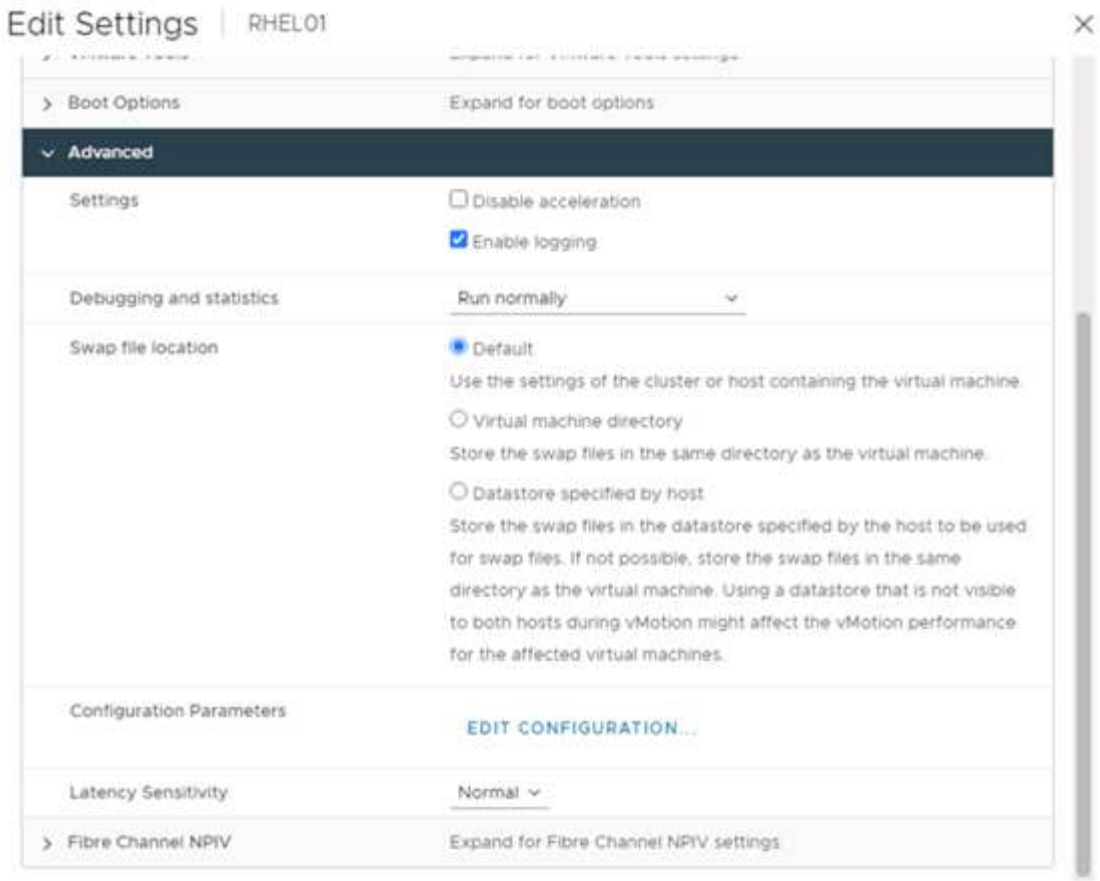
10. Assicurarsi che l'avvio sicuro sia disattivato per la macchina virtuale RedHat.
11. Assicurarsi che il firmware VM Boot Options sia impostato su EFI ("rif").

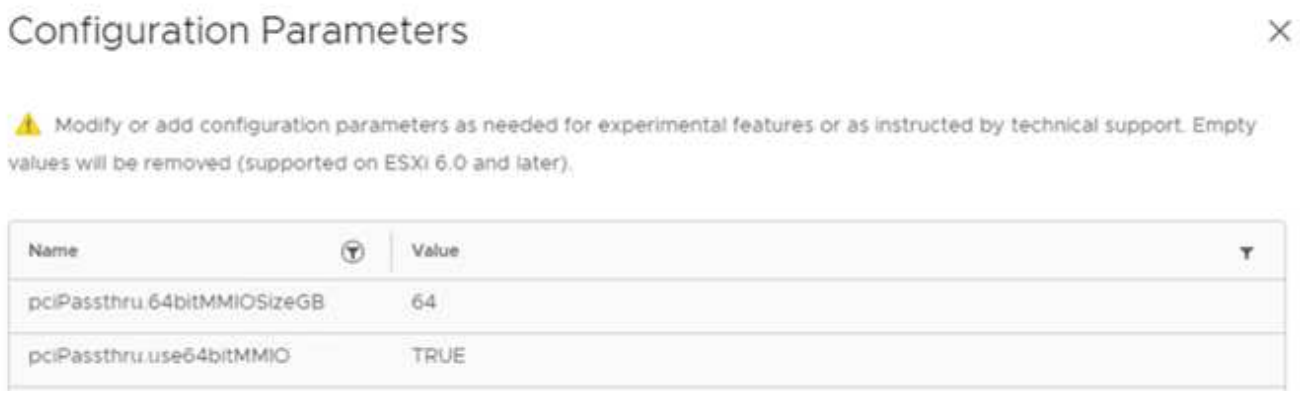


12. Assicurarsi che i SEGUENTI PARAMETRI siano aggiunti alla configurazione avanzata di modifica delle opzioni della macchina virtuale. Il valore di `pciPassthru.64bitMMIOSizeGB` Il parametro dipende dalla memoria della GPU e dal numero di GPU assegnate alla VM. Ad esempio:

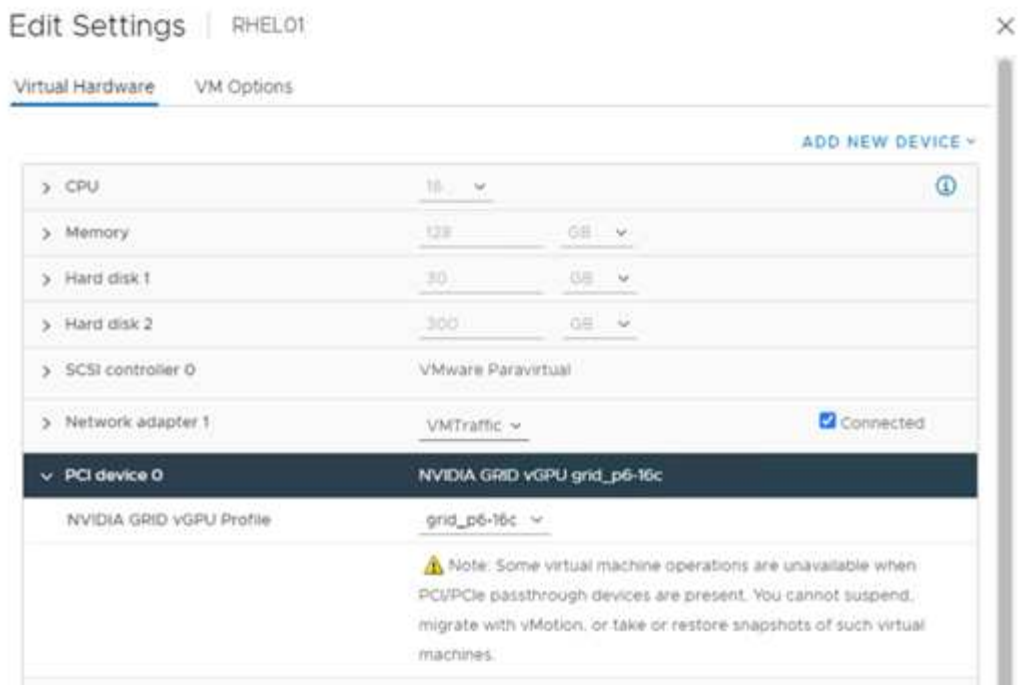
    a. Se a una macchina virtuale sono assegnate 4 GPU V100 da 32 GB, questo valore deve essere 128.

    b. Se a una macchina virtuale sono assegnate 4 GPU P6 da 16 GB, questo valore deve essere 64.





13. Quando si aggiungono vGPU come nuovo dispositivo PCI alla macchina virtuale in vCenter, assicurarsi di selezionare NVIDIA GRID vGPU come tipo di dispositivo PCI.
14. Scegliere il profilo GPU corretto che si adatta alla GPU utilizzata, alla memoria GPU e allo scopo di utilizzo: Ad esempio, grafica o calcolo.



15. Su RedHat Linux VM, i driver NVIDIA possono essere installati eseguendo il seguente comando:

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. Verificare che venga segnalato il profilo vGPU corretto eseguendo il seguente comando:

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. Dopo il riavvio, verificare che la scheda NVIDIA vGPU corretta sia riportata insieme alle versioni dei driver.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+================
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. Assicurarsi che l'IP del server di licenza sia configurato sulla macchina virtuale nel file di configurazione della griglia vGPU.
    a. Copiare il modello.

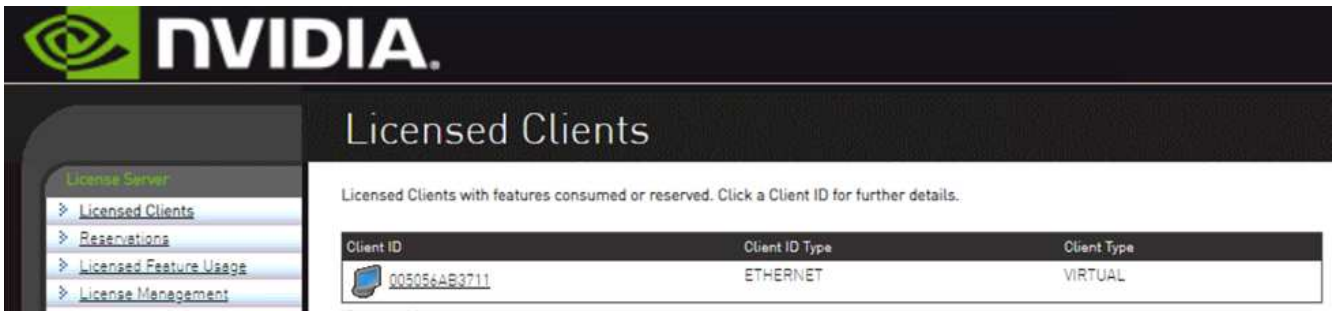
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. Modificare il file `/etc/nvidia/rid.conf`, Aggiungere l'indirizzo IP del server di licenza e impostare il tipo di funzione su 1.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. Dopo aver riavviato la macchina virtuale, nel server di licenza viene visualizzata una voce sotto Licensed Clients (Client concessi in licenza), come mostrato di seguito.



20. Per ulteriori informazioni sul download del software GATK e Cromwell, consultare la sezione Solutions Setup.

21. Dopo che GATK può utilizzare le GPU on-premise, il linguaggio di descrizione del workflow `*. wdl` ha gli attributi di runtime come mostrato di seguito.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"Prossimo: Conclusione."

Conclusione

"Precedente: Configurazione della GPU."

Molte organizzazioni sanitarie di tutto il mondo hanno standardizzato FlexPod come piattaforma comune. Con FlexPod, puoi implementare le funzionalità del settore sanitario in tutta sicurezza. FlexPod con NetApp ONTAP è dotato di serie della capacità di implementare un set di protocolli leader del settore pronto all'uso. Indipendentemente dall'origine della richiesta di eseguire genomica di un dato paziente, interoperabilità, accessibilità, disponibilità e scalabilità sono standard con una piattaforma FlexPod. Se

standardizzato su una piattaforma FlexPod, la cultura dell'innovazione diventa contagiosa.

Dove trovare ulteriori informazioni

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

- Data center FlexPod per ai/ML con Cisco UCS 480 ML per l'apprendimento approfondito

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- Centro documentazione di ONTAP 9

  "http://docs.netapp.com"

- Agile ed efficiente: Come FlexPod promuove la modernizzazione del data center

  "https://www.flexpod.com/idc-white-paper/"

- Ai nel settore sanitario

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod per il settore sanitario semplifica la tua trasformazione

  "https://flexpod.com/solutions/verticals/healthcare/"

- FlexPod di Cisco e NetApp

  "https://flexpod.com/"

- Ai e Analytics per il settore sanitario (NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- Ai nel settore sanitario le scelte di infrastruttura intelligente aumentano il successo

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- Data center FlexPod con ONTAP 9.8, connettore storage ONTAP per Cisco Intersight e modalità gestita Cisco Intersight.

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- Data center FlexPod con piattaforma OpenStack Linux aziendale Red Hat

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Novembre 2021	Release iniziale.

Guida al dimensionamento direzionale di FlexPod per MEDITECH

TR-4774: FlexPod per dimensionamento direzionale MEDITECH

Brandon Agee, John Duignan, NetApp Mike Brennan, Jon Ebmeir, Cisco

In collaborazione con:

Questo report fornisce una guida per il dimensionamento di FlexPod per un ambiente software applicativo MEDITECH EHR.

Scopo

I sistemi FlexPod possono essere implementati per ospitare i servizi di ESPANSIONE MEDITECH, 6.x, 5.x e MAGIC. I server FlexPod che ospitano il livello applicativo MEDITECH offrono una piattaforma integrata per un'infrastruttura affidabile e dalle performance elevate. La piattaforma integrata di FlexPod viene implementata rapidamente da partner di canale qualificati di FlexPod ed è supportata dai centri di assistenza tecnica Cisco e NetApp.

Il dimensionamento si basa sulle informazioni contenute nella proposta di configurazione hardware di MEDITECH e nel documento di task MEDITECH. L'obiettivo è determinare le dimensioni ottimali per i componenti dell'infrastruttura di calcolo, rete e storage.

Il "Panoramica SUL CARICO di lavoro DI MEDITECH" La sezione descrive i tipi di carichi di lavoro di calcolo e storage disponibili negli ambienti MEDITECH.

Il "Specifiche tecniche per architetture piccole, medie e grandi" La sezione descrive in dettaglio una distinta materiali di esempio per le diverse architetture di storage descritte nella sezione. Le configurazioni fornite sono solo linee guida generali. Dimensionare sempre i sistemi utilizzando i sizzer in base al carico di lavoro e ottimizzare le configurazioni di conseguenza.

Vantaggi generali della soluzione

L'esecuzione di un ambiente MEDITECH sulla base architetturale FlexPod può aiutare le organizzazioni sanitarie a migliorare la produttività e a ridurre le spese di capitale e operative. FlexPod offre un'infrastruttura convergente pre-validata, rigorosamente testata, grazie alla partnership strategica di Cisco e NetApp. È progettato e progettato specificamente per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio consente agli utenti del sistema MEDITECH EHR di ottenere tempi di risposta più rapidi.

La soluzione FlexPod di Cisco e NetApp soddisfa i requisiti di sistema MEDITECH con performance elevate,

modulare, pre-validato, convergente, virtualizzato, piattaforma efficiente, scalabile e conveniente. FlexPod Datacenter con MEDITECH offre diversi vantaggi specifici per il settore sanitario:

- **Architettura modulare**. FlexPod soddisfa le diverse esigenze dell'architettura modulare MEDITECH con sistemi FlexPod personalizzati per ogni carico di lavoro specifico. Tutti i componenti sono collegati tramite un server in cluster e un fabric di gestione dello storage e utilizzano un set di strumenti di gestione coerente.
- **Operazioni semplificate e costi ridotti**. È possibile eliminare i costi e la complessità delle piattaforme legacy sostituendole con una risorsa condivisa più efficiente e scalabile in grado di supportare i medici ovunque si trovino. Questa soluzione offre un migliore utilizzo delle risorse per un maggiore ritorno sull'investimento (ROI).
- **Implementazione più rapida dell'infrastruttura**. Il design integrato di FlexPod Datacenter con MEDITECH consente ai clienti di avere la nuova infrastruttura operativa in modo rapido e semplice per i data center on-site e remoti.
- **Architettura scale-out**. È possibile scalare SAN e NAS da terabyte a decine di petabyte senza riconfigurare le applicazioni in esecuzione.
- **Operazioni senza interruzioni**. Puoi eseguire la manutenzione dello storage, le operazioni del ciclo di vita dell'hardware e gli aggiornamenti software senza interrompere il business.
- **Multitenancy sicura**. Questo vantaggio supporta le crescenti esigenze di server virtualizzati e infrastruttura storage condivisa, consentendo la multi-tenancy sicura delle informazioni specifiche della struttura. Questo vantaggio è importante se si ospitano più istanze di database e software.
- **Ottimizzazione delle risorse in pool**. Questo vantaggio può contribuire a ridurre il numero di server fisici e controller di storage, bilanciare il carico di lavoro richiesto, aumentare l'utilizzo e migliorare contemporaneamente le performance.
- **Qualità del servizio (QoS).** FlexPod offre qualità del servizio (QoS) sull'intero stack. Le policy di storage QoS leader del settore consentono livelli di servizio differenziati in un ambiente condiviso. Queste policy consentono performance ottimali per i carichi di lavoro e aiutano a isolare e controllare le applicazioni incontrollate.
- **Efficienza dello storage**. Puoi ridurre i costi di storage con l'efficienza dello storage NetApp 7:1.
- **Agilità**. Gli strumenti di automazione, orchestrazione e gestione del workflow leader del settore offerti dai sistemi FlexPod consentono ALL'IT di rispondere in maniera molto più reattiva alle richieste di business. Queste richieste di business possono spaziare dal backup MEDITECH e provisioning di più ambienti di test e formazione alle repliche di database di analisi per iniziative di gestione dello stato di salute della popolazione.
- **Produttività**. È possibile implementare e scalare rapidamente questa soluzione per un'esperienza ottimale per l'utente finale del medico.
- **Data Fabric**. L'architettura NetApp Data Fabric consente di unire i dati tra i siti, oltre i confini fisici e tra le applicazioni. Il NetApp Data Fabric è costruito per le aziende basate sui dati in un mondo incentrato sui dati. I dati vengono creati e utilizzati in più ubicazioni e spesso condivisi con applicazioni e infrastrutture. Il data fabric consente di gestire i dati in modo coerente e integrato. Offre inoltre all'IT un maggiore controllo sui dati e semplifica la complessità DELL'IT in continua crescita.

Scopo

Questo documento tratta gli ambienti che utilizzano lo storage basato su Cisco UCS e NetApp ONTAP. Fornisce architetture di riferimento di esempio per l'hosting di MEDITECH.

Non copre:

- Guida dettagliata al dimensionamento con NetApp System Performance Modeler (SPM) o altri tool di dimensionamento NetApp.
- Dimensionamento per carichi di lavoro non in produzione.

Pubblico

Il presente documento è destinato ai Systems engineer di NetApp e dei partner e al personale dei NetApp Professional Services. NetApp presuppone che il lettore abbia una buona conoscenza dei concetti di dimensionamento di calcolo e storage, nonché una buona familiarità tecnica con i sistemi di storage Cisco UCS e NetApp.

Documenti correlati

I seguenti report tecnici e altri documenti sono pertinenti al presente report tecnico e costituiscono una serie completa di documenti necessari per il dimensionamento, la progettazione e l'implementazione di MEDITECH su infrastruttura FlexPod.

- "TR-4753: Guida all'implementazione di FlexPod Datacenter per MEDITECH"
- "TR-4190: Linee guida di dimensionamento NetApp per ambienti MEDITECH"
- "TR-4319: Linee guida per l'implementazione NetApp per ambienti MEDITECH"

> Per accedere ad alcuni di questi report, sono necessarie le credenziali di accesso per il Field Portal di NetApp.

Panoramica SUL CARICO di lavoro DI MEDITECH

In questa sezione vengono descritti i tipi di workload di calcolo e storage che si possono trovare negli ambienti MEDITECH.

CARICHI DI lavoro DI BACKUP E MEDITECH

Quando si dimensionano i sistemi storage NetApp per ambienti MEDITECH, è necessario prendere in considerazione sia il carico di lavoro di produzione MEDITECH che il carico di lavoro di backup.

Host MEDITECH
Un host MEDITECH è un server di database. Questo host è anche chiamato file server MEDITECH (per LA piattaforma EXPSE, 6.x o C/S 5.x) o UNA MACCHINA MAGICA (per la piattaforma MAGICA). Questo documento utilizza il termine host MEDITECH per fare riferimento a un file server MEDITECH e a una MACCHINA MAGICA.

Le sezioni seguenti descrivono le caratteristiche di i/o e i requisiti di performance di questi due carichi di lavoro.

Carico DI lavoro DI MEDITECH

In un ambiente MEDITECH, più server che eseguono il software MEDITECH eseguono diverse attività come un sistema integrato noto come sistema MEDITECH. Per ulteriori informazioni sul sistema MEDITECH, consultare la documentazione MEDITECH:

- Per gli ambienti MEDITECH in produzione, consultare la documentazione MEDITECH appropriata per determinare il numero di host MEDITECH e la capacità di storage da includere nel dimensionamento del sistema storage NetApp.

- Per i nuovi ambienti MEDITECH, consultare il documento relativo alla proposta di configurazione dell'hardware. Per gli ambienti MEDITECH esistenti, consultare il documento delle attività di valutazione dell'hardware. L'attività di valutazione dell'hardware è associata a un ticket MEDITECH. I clienti possono richiedere questi documenti a MEDITECH.

È possibile scalare il sistema MEDITECH per aumentare capacità e performance aggiungendo host. Ogni host richiede capacità di storage per i file di database e applicazioni. Lo storage disponibile per ciascun host MEDITECH deve supportare anche l'i/o generato dall'host. In un ambiente MEDITECH, è disponibile un LUN per ciascun host per supportare i requisiti di storage di database e applicazioni di quell'host. Il tipo di categoria MEDITECH e il tipo di piattaforma da implementare determinano le caratteristiche del carico di lavoro di ciascun host MEDITECH e, di conseguenza, dell'intero sistema.

Categorie MEDITECH

MEDITECH associa le dimensioni dell'implementazione a un numero di categoria compreso tra 1 e 6. La categoria 1 rappresenta le implementazioni MEDITECH più piccole; la categoria 6 rappresenta le più grandi. Esempi di specifiche applicative MEDITECH associate a ciascuna categoria includono metriche come:

- Numero di letti ospedalieri
- Pazienti inpazienti all'anno
- Pazienti esterni all'anno
- Visite di pronto soccorso all'anno
- Esami all'anno
- Prescrizioni al giorno in caso di degenza
- Prescrizioni ambulatoriali al giorno

Per ulteriori informazioni sulle categorie MEDITECH, consulta la scheda di riferimento della categoria MEDITECH. È possibile ottenere questa scheda da MEDITECH attraverso il cliente o attraverso il programma di installazione del sistema MEDITECH.

Piattaforme MEDITECH

MEDITECH dispone di quattro piattaforme:

- ESPANDI
- MEDITECH 6.x
- Client/Server 5.x (C/S 5.x)
- MAGIA

Per le piattaforme ESPANSE MEDITECH, 6.x e C/S 5.x, le caratteristiche di i/o di ciascun host sono definite come casuali al 100% con una dimensione della richiesta di 4,000. Per la piattaforma MAGICA MEDITECH, le caratteristiche i/o di ciascun host sono definite come casuali al 100% con una dimensione della richiesta di 8,000 o 16,000. Secondo MEDITECH, la dimensione della richiesta per una tipica implementazione DI PRODUZIONE MAGICA è 8,000 o 16,000.

Il rapporto di lettura e scrittura varia in base alla piattaforma implementata. MEDITECH stima il mix medio di lettura e scrittura e quindi li esprime come percentuali. MEDITECH stima anche il valore medio sostenuto di IOPS richiesto per ciascun host MEDITECH su una specifica piattaforma MEDITECH. La tabella seguente riassume le caratteristiche di i/o specifiche della piattaforma fornite da MEDITECH.

CATEGORIA MEDITECH	Piattaforma MEDITECH	Percentuale media di lettura casuale	Percentuale media di scrittura casuale	IOPS medi sostenuti per host MEDITECH
1	ESPANSIONI, 6.x	20	80	750
2-6	ESPANDI	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	MAGIA	90	10	400

In un sistema MEDITECH, il livello IOPS medio di ciascun host deve essere uguale ai valori IOPS definiti nella tabella precedente. Per determinare il corretto dimensionamento dello storage in base a ciascuna piattaforma, i valori IOPS specificati nella tabella precedente vengono utilizzati come parte della metodologia di dimensionamento descritta nella "Specifiche tecniche per architetture piccole, medie e grandi" sezione.

MEDITECH richiede che la latenza media di scrittura casuale rimanga al di sotto di 1 ms per ciascun host. Tuttavia, gli aumenti temporanei della latenza di scrittura fino a 2 ms durante i processi di backup e riallocazione sono considerati accettabili. MEDITECH richiede inoltre che la latenza media di lettura casuale rimanga inferiore a 7 ms per gli host di categoria 1 e inferiore a 5 ms per gli host di categoria 2. Questi requisiti di latenza si applicano a tutti gli host, indipendentemente dalla piattaforma MEDITECH utilizzata.

La tabella seguente riassume le caratteristiche di i/o da prendere in considerazione quando si dimensiona lo storage NetApp per i carichi di lavoro MEDITECH.

Parametro	CATEGORIA MEDITECH	ESPANDI	MEDITECH 6.x	C/S 5.x	MAGIA
Dimensione richiesta	1-6	4K	4K	4K	8K o 16K
Casuale/sequenziale		100% casuale	100% casuale	100% casuale	100% casuale
IOPS medi sostenuti	1	750	750	N/A.	N/A.
	2-6	750	750	600	400
Rapporto di lettura/scrittura	1-6	20% lettura, 80% scrittura	20% lettura, 80% scrittura	40% lettura, 60% scrittura	90% lettura, 10% scrittura
Latenza di scrittura		<1 ms.	<1 ms.	<1 ms.	<1 ms.
Latenza temporanea di picco in scrittura	1-6	<2 ms.	<2 ms.	<2 ms.	<2 ms.
Latenza di lettura	1	<7 ms.	<7 ms.	N/A.	N/A.
	2-6	<5 ms.	<5 ms.	<5 ms.	<5 ms.

Gli host MEDITECH delle categorie da 3 a 6 hanno le stesse caratteristiche di i/o della categoria 2. Per le categorie MEDITECH da 2 a 6, il numero di host implementati in ciascuna categoria è diverso.

Il sistema storage NetApp deve essere dimensionato per soddisfare i requisiti di performance descritti nelle sezioni precedenti. Oltre al carico di lavoro di produzione MEDITECH, il sistema storage NetApp deve essere in grado di mantenere questi obiettivi di performance MEDITECH durante le operazioni di backup, come descritto nella sezione seguente.

Descrizione del carico di lavoro di backup

Il software di backup certificato MEDITECH esegue il backup del LUN utilizzato da ciascun host MEDITECH in un sistema MEDITECH. Affinché i backup siano in uno stato coerente con l'applicazione, il software di backup interrompe il sistema MEDITECH e sospende le richieste di i/o su disco. Mentre il sistema è in stato di quiescenza, il software di backup invia un comando al sistema di storage NetApp per creare una copia Snapshot di NetApp dei volumi che contengono le LUN. Il software di backup in seguito rende più completo il sistema MEDITECH, che consente alle richieste di i/o di produzione di continuare con il database. Il software crea un volume NetApp FlexClone in base alla copia Snapshot. Questo volume viene utilizzato dall'origine del backup mentre le richieste di i/o di produzione continuano sui volumi principali che ospitano le LUN.

Il carico di lavoro generato dal software di backup deriva dalla lettura sequenziale delle LUN che risiedono nei volumi FlexClone. Il carico di lavoro è definito come un carico di lavoro di lettura sequenziale al 100% con una dimensione della richiesta di 64,000. Per il carico di lavoro di produzione MEDITECH, il criterio delle performance è quello di mantenere gli IOPS richiesti e i livelli di latenza di lettura/scrittura associati. Per il carico di lavoro di backup, tuttavia, l'attenzione viene spostata sul throughput dei dati complessivo (Mbps) generato durante l'operazione di backup. I backup DEL LUN DI MEDITECH devono essere completati in una finestra di backup di otto ore, ma NetApp consiglia di completare il backup di tutti i LUN MEDITECH in sei ore o meno. L'obiettivo di completare il backup in meno di sei ore riduce gli eventi, come un aumento non pianificato del carico di lavoro MEDITECH, le operazioni in background di NetApp ONTAP o la crescita dei dati nel tempo. Uno di questi eventi potrebbe richiedere tempi di backup aggiuntivi. Indipendentemente dalla quantità di dati applicativi memorizzati, il software di backup esegue un backup completo a livello di blocco dell'intero LUN per ogni host MEDITECH.

Calcolare il throughput di lettura sequenziale necessario per completare il backup all'interno di questa finestra in funzione degli altri fattori coinvolti:

- La durata del backup desiderata
- Il numero di LUN
- Le dimensioni di ciascun LUN di cui eseguire il backup

Ad esempio, in un ambiente MEDITECH con 50 host in cui le dimensioni del LUN di ciascun host sono pari a 200 GB, la capacità totale del LUN per il backup è pari a 10 TB.

Per eseguire il backup di 10 TB di dati in otto ore, è necessario il seguente throughput:

- = (10 x 10^6)MB (8 x 3,600) s.
- = 347,2 MBps

Tuttavia, per tenere conto degli eventi non pianificati, viene selezionata una finestra di backup conservativa di 5.5 ore per fornire spazio oltre le sei ore consigliate.

Per eseguire il backup di 10 TB di dati in otto ore, è necessario il seguente throughput:

- = (10 x 10^6)MB (5.5 x 3,600)s
- = 500 Mbps

Con una velocità di throughput di 500 Mbps, il backup può essere completato in un intervallo di tempo di 5.5

ore, comodamente entro le 8 ore di backup richieste.

La tabella seguente riassume le caratteristiche i/o del carico di lavoro di backup da utilizzare quando si dimensiona il sistema storage.

Parametro	Tutte le piattaforme
Dimensione richiesta	64.000
Casuale/sequenziale	100% sequenziale
Rapporto di lettura/scrittura	100% di lettura
Throughput medio	Dipende dal numero di host MEDITECH e dalle dimensioni di ogni LUN: Il backup deve essere completato entro 8 ore.
Durata del backup richiesta	8 ore

Cisco UCS Reference Architecture per MEDITECH

L'architettura di MEDITECH su FlexPod si basa sulla guida di MEDITECH, Cisco e NetApp e sull'esperienza dei partner nella collaborazione con clienti MEDITECH di tutte le dimensioni. L'architettura è adattabile e applica le Best practice per MEDITECH, a seconda della strategia del data center del cliente: Piccola o grande, centralizzata, distribuita o multi-tenant.

Durante l'implementazione di MEDITECH, Cisco ha progettato architetture di riferimento Cisco UCS che si allineano direttamente con le Best practice di MEDITECH. Cisco UCS offre una soluzione perfettamente integrata per performance elevate, alta disponibilità, affidabilità e scalabilità per supportare le pratiche dei medici e i sistemi ospedalieri con diverse migliaia di letti.

Specifiche tecniche per architetture piccole, medie e grandi

In questa sezione viene illustrata una distinta materiali di esempio per architetture storage di diverse dimensioni.

Distinta dei materiali per architetture di piccole, medie e grandi dimensioni.

Il design di FlexPod è un'infrastruttura flessibile che comprende diversi componenti e versioni software. Utilizzare "TR-4036: Specifiche tecniche di FlexPod" Come guida all'assemblaggio di una configurazione FlexPod valida. Le configurazioni riportate nella tabella seguente rappresentano i requisiti minimi per FlexPod e sono solo un esempio. La configurazione può essere espansa per ogni famiglia di prodotti in base alle esigenze di ambienti e casi di utilizzo diversi.

Per questo esercizio di dimensionamento piccolo corrisponde a un ambiente MEDITECH di categoria 3, medio a una categoria 5 e grande a una categoria 6.

	Piccolo	Medio	Grande
Piattaforma	Una coppia ha di sistemi storage all-flash NetApp AFF A220	Una coppia NetApp AFF A220 ha	Una coppia di sistemi storage all-flash ha NetApp AFF A300
Shelf di dischi	9 TB x 3,8 TB	13 TB x 3,8 TB	19 TB x 3,8 TB

	Piccolo	Medio	Grande
Dimensione del database MEDITECH	DA 3 TB A 12 TB	17 TB	>30 TB
IOPS MEDITECH	Meno di 22,000 IOPS	>25,000 IOPS	>32,000 IOPS
IOPS totali	22000	27000	35000
Raw	34,2 TB	49,4 TB	68,4 TB
Capacità utilizzabile	18.53TiB	27,96TiB	33.82TiB
Capacità effettiva (efficienza dello storage 2:1)	55,6TiB	83,89TiB	101,47TiB

Alcuni ambienti dei clienti potrebbero avere più carichi di lavoro di produzione MEDITECH in esecuzione simultaneamente o potrebbero avere requisiti IOPS più elevati. In questi casi, collaborate con il team degli account NetApp per dimensionare i sistemi storage in base agli IOPS e alla capacità richiesti. Dovresti essere in grado di determinare la piattaforma giusta per i carichi di lavoro. Ad esempio, esistono clienti che eseguono con successo più ambienti MEDITECH su una coppia ha di sistemi storage all-flash NetApp AFF A700.

La seguente tabella mostra il software standard richiesto per le configurazioni MEDITECH.

Software	Famiglia di prodotti	Versione o release	Dettagli
Storage	ONTAP	Disponibilità generale (GA) di ONTAP 9.4	
Rete	Cisco UCS Fabric Interconnects	Cisco UCSM 4.x	Versione corrente consigliata
	Switch Ethernet Cisco Nexus	7.0(3)I7(6)	Versione corrente consigliata
	Cisco FC: Cisco MDS 9132T	8.3(2)	Versione corrente consigliata
Hypervisor	Hypervisor	VMware vSphere ESXi 6.7	
	Macchine virtuali (VM)	Windows 2016	
Gestione	Sistema di gestione dell’hypervisor	VMware vCenter Server 6.7 U1 (VCSA)	
	NetApp Virtual Storage Console (VSC)	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4.0	
	Cisco UCS Manager	4.x	

La seguente tabella mostra un piccolo esempio di configurazione (categoria 3): Componenti dell’infrastruttura.

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1	Supporta fino a otto blade half-width o quattro blade full-width. Aggiungi chassis con l'aumento dei requisiti dei server.
	Moduli i/o chassis Cisco	2 x 2208	8 GB x 10 GB di porte uplink
	Blade server Cisco UCS	4 x B200 M5	Ciascuno con 2 x 14 core, velocità di clock di 2,6 GHz o superiore e 384 GB BIOS 3.2 (n. 3)
	Cisco UCS Virtual Interface Card	4 x UCS 1440	Driver FC fNIC VMware ESXi: 1.6.0.47 driver Ethernet ENIC VMware ESXi: 1.0.27.0 (vedere la matrice di interoperabilità: https://ucshcltool.cloudapps.cisco.com/public/)
	2 Cisco UCS Fabric Interconnects (Fi)	2 UCS 6454 Fi	Fabric interconnects di quarta generazione che supporta Ethernet 10/25/100GB e FC 32 GB
Rete	Switch Ethernet Cisco	2 x Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB, 100 GB
Rete di storage	IP Network Nexus 9k per storage BLOB		Chassis FI e UCS
	FC: CISCO MDS 9132T		Due switch Cisco 9132T
Storage	Sistema storage all-flash NetApp AFF A300	1 coppia ha	Cluster a 2 nodi per tutti i carichi di lavoro MEDITECH (file server, Image Server, SQL Server, VMware e così via)
	Shelf di dischi DS224C	1 shelf di dischi DS224C	
	Disco a stato solido (SSD)	9 x 3,8 TB	

La seguente tabella mostra un esempio di configurazione del supporto (categoria 5) – componenti dell'infrastruttura

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1	Supporta fino a otto blade half-width o quattro blade full-width. Aggiungi chassis con l'aumento dei requisiti dei server.
	Moduli i/o chassis Cisco	2 x 2208	8 GB x 10 GB di porte uplink
	Blade server Cisco UCS	6 x B200 M5	Ciascuno con 2 x 16 core, velocità di clock di 2,5 GHz/o superiore e 384 GB o più di memoria BIOS 3.2 (n. 3)
	Cisco UCS Virtual Interface Card (VIC)	6 VICS UCS 1440	Driver FC fNIC VMware ESXi: 1.6.0.47 driver Ethernet ENIC VMware ESXi: 1.0.27.0 (vedere matrice di interoperabilità:)
	2 Cisco UCS Fabric Interconnects (Fi)	2 UCS 6454 Fi	Fabric interconnects di quarta generazione che supporta Ethernet 10 GB/25 GB/100 GB e FC 32 GB
Rete	Switch Ethernet Cisco	2 x Nexus 9336c-FX2	1 GB, 10 GB, 25 GB, 40 GB, 100 GB
Rete di storage	IP Network Nexus 9k per storage BLOB		
	FC: CISCO MDS 9132T		Due switch Cisco 9132T
Storage	Sistema storage all-flash NetApp AFF A220	2 coppia ha	Cluster a 2 nodi per tutti i carichi di lavoro MEDITECH (file server, Image Server, SQL Server, VMware e così via)
	Shelf di dischi DS224C	1 shelf di dischi DS224C	
	SSD	13 x 3,8 TB	

La seguente tabella mostra un esempio di configurazione di grandi dimensioni (categoria 6): Componenti dell'infrastruttura.

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1	
	Moduli i/o chassis Cisco	2 x 2208	8 porte uplink da 10 GB
	Blade server Cisco UCS	8 x B200 M5	Ciascuno con 2 x 24 core, 2,7 GHz e 768 GB BIOS 3.2 (n. 3)
	Cisco UCS Virtual Interface Card (VIC)	8 VICS UCS 1440	Driver FC fNIC VMware ESXi: 1.6.0.47 driver Ethernet ENIC VMware ESXi: 1.0.27.0 (vedere la matrice di interoperabilità: https://ucshcltool.cloudapps.cisco.com/public/)
	2 connessioni fabric Cisco UCS (Fi)	2 UCS 6454 Fi	Fabric interconnects di quarta generazione che supporta Ethernet 10 GB/25 GB/100 GB e FC 32 GB
Rete	Switch Ethernet Cisco	2 x Nexus 9336c-FX2	2 Cisco Nexus 9332PQ1, 10 GB, 25 GB, 40 GB, 100 GB
Rete di storage	IP Network N9k per storage BLOB		
	FC: CISCO MDS 9132T		Due switch Cisco 9132T
Storage	AFF A300	1 coppia ha	Cluster a 2 nodi per tutti i carichi di lavoro MEDITECH (file server, Image Server, SQL Server, VMware e così via)
	Shelf di dischi DS224C	1 shelf di dischi DS224C	
	SSD	19 x 3,8 TB	

Queste configurazioni forniscono un punto di partenza per le indicazioni sul dimensionamento. Alcuni ambienti dei clienti potrebbero avere più carichi di lavoro di produzione MEDITECH e non MEDITECH in esecuzione simultaneamente, oppure potrebbero avere requisiti di IOP più elevati. È necessario collaborare con il team commerciale NetApp per dimensionare i sistemi storage in base agli IOPS, ai carichi di lavoro e alla capacità richiesti per determinare la piattaforma giusta per i carichi di lavoro.

Ulteriori informazioni

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

- Data center FlexPod con design validato FC Cisco.

"https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Linee guida per l'implementazione NetApp per ambienti MEDITECH.

  "https://fieldportal.netapp.com/content/248456" (Accesso NetApp richiesto)

- Linee guida di dimensionamento NetApp per ambienti MEDITECH.

  "www.netapp.com/us/media/tr-4190.pdf"

- Data center FlexPod per l'implementazione Epic EHR

  "www.netapp.com/us/media/tr-4693.pdf"

- Area di progettazione FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- FlexPod DC con storage FC (switch MDS) con NetApp AFF, vSphere 6.5U1 e Cisco UCS Manager

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco Healthcare

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

Ringraziamenti

Le seguenti persone hanno contribuito alla stesura e alla creazione di questa guida.

- Brandon Agee, Technical Marketing Engineer, NetApp
- John Duignan, Solutions Architect - Healthcare, NetApp
- Ketan Mota, Product Manager, NetApp
- Jon Ebmeier, Technical Solutions Architect, Cisco Systems, Inc
- Mike Brennan, Product Manager, Cisco Systems, Inc

Guida all'implementazione di FlexPod Datacenter per MEDITECH

TR-4753: Guida all'implementazione di FlexPod Datacenter per MEDITECH

Brandon Agee e John Duignan, NetApp Mike Brennan e Jon Ebmeier, Cisco

In collaborazione con:

Vantaggi generali della soluzione

Eseguendo un ambiente MEDITECH sulla base architetturale FlexPod, la tua organizzazione sanitaria può aspettarsi un miglioramento della produttività del personale e una riduzione delle spese di capitale e operative. FlexPod Datacenter per MEDITECH offre diversi vantaggi specifici per il settore sanitario, tra cui:

- **Operazioni semplificate e costi ridotti.** Elimina i costi e la complessità delle piattaforme legacy sostituendole con una risorsa condivisa più efficiente e scalabile in grado di supportare i medici ovunque si trovino. Questa soluzione offre un maggiore utilizzo delle risorse per un maggiore ritorno sull'investimento (ROI).
- **Implementazione più rapida dell'infrastruttura.** sia che si tratti di un data center esistente o di una postazione remota, grazie al design integrato e testato di FlexPod Datacenter, è possibile attivare e utilizzare la nuova infrastruttura in meno tempo, con meno sforzo.
- **Storage certificato.** il software per la gestione dei dati NetApp ONTAP con MEDITECH ti offre l'affidabilità superiore di un vendor di storage testato e certificato. MEDITECH non certifica altri componenti dell'infrastruttura.
- **Architettura scale-out.** scalare SAN e NAS da terabyte (TB) a decine di petabyte (PB) senza riconfigurare le applicazioni in esecuzione.
- **Operazioni senza interruzioni.** eseguire la manutenzione dello storage, le operazioni del ciclo di vita dell'hardware e gli aggiornamenti FlexPod senza interrompere il business.
- **Multi-tenancy sicura.** supporto delle maggiori esigenze di infrastruttura condivisa storage e server virtualizzati, che consente la multi-tenancy sicura di informazioni specifiche della struttura, in particolare se il sistema ospita più istanze di database e software.
- **Ottimizzazione delle risorse in pool.** aiuta a ridurre il numero di server fisici e controller di storage, bilanciare il carico di lavoro richiesto e aumentare l'utilizzo migliorando al contempo le performance.
- **Qualità del servizio (QoS).** FlexPod offre QoS sull'intero stack. Le policy di rete, calcolo e storage QoS leader del settore consentono livelli di servizio differenziati in un ambiente condiviso. Queste policy consentono performance ottimali per i carichi di lavoro e aiutano a isolare e controllare le applicazioni incontrollate.
- * Efficienza dello storage.* Riduci i costi dello storage con "Garanzia di efficienza dello storage NetApp 7:1".
- **Agilità.** grazie ai tool di automazione, orchestrazione e gestione del workflow leader del settore forniti dai sistemi FlexPod, il tuo team IT può essere molto più reattivo alle richieste di business. Queste richieste di business possono spaziare dal backup MEDITECH e provisioning di più ambienti di test e formazione alle repliche di database di analisi per iniziative di gestione dello stato di salute della popolazione.
- **Aumento della produttività.** implementazione e scalabilità rapide di questa soluzione per un'esperienza ottimale dell'utente finale del medico.
- **NetApp Data Fabric.** l'architettura NetApp Data Fabric consente di unire i dati tra siti, oltre i confini fisici e tra applicazioni diverse. Il NetApp Data Fabric è costruito per le aziende basate sui dati in un mondo incentrato sui dati. I dati vengono creati e utilizzati in più sedi e spesso è necessario sfruttarli e condividerli con altre sedi, applicazioni e infrastrutture. Hai bisogno di un modo per gestire i tuoi dati in modo coerente e integrato. Il Data Fabric offre un modo per gestire i dati che ne consente il controllo e semplifica l'aumento della complessità DELL'IT.

FlexPod

Nuovo approccio infrastrutturale per gli EHR MEDITECH

Le organizzazioni di fornitori di servizi sanitari come la tua continuano a essere sotto pressione per massimizzare i benefici derivanti da investimenti sostanziali in cartelle cliniche elettroniche (EHR) MEDITECH

leader del settore. Per le applicazioni mission-critical, quando i clienti progettano i propri data center per le soluzioni MEDITECH, spesso identificano i seguenti obiettivi per l'architettura del data center:

- Elevata disponibilità delle applicazioni MEDITECH
- Performance elevate
- Facilità di implementazione di MEDITECH nel data center
- Agilità e scalabilità per consentire la crescita con nuove release o applicazioni MEDITECH
- Convenienza
- Allineamento con la guida MEDITECH e le piattaforme di destinazione
- Gestibilità, stabilità e facilità di supporto
- Solida protezione dei dati, backup, recovery e continuità del business

Man mano che gli utenti di MEDITECH evolvono le proprie organizzazioni per diventare organizzazioni responsabili e adattarsi a modelli di rimborso più rigorosi e integrati, la sfida diventa offrire l'infrastruttura MEDITECH necessaria in un modello DI delivery IT più efficiente e agile.

Valore dell'infrastruttura convergente prevalidata

A causa di un requisito fondamentale per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità, MEDITECH è prescrittivo in merito ai requisiti hardware dei suoi clienti.

FlexPod è un'infrastruttura convergente pre-validata e rigorosamente testata dalla partnership strategica di Cisco e NetApp. È progettato e progettato specificamente per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio si traduce in conformità MEDITECH e in tempi di risposta ottimali per gli utenti del sistema MEDITECH.

La soluzione FlexPod di Cisco e NetApp soddisfa i requisiti di sistema di MEDITECH con un sistema modulare dalle performance elevate, pre-validato, convergente, virtualizzato, piattaforma efficiente, scalabile e conveniente. Offre:

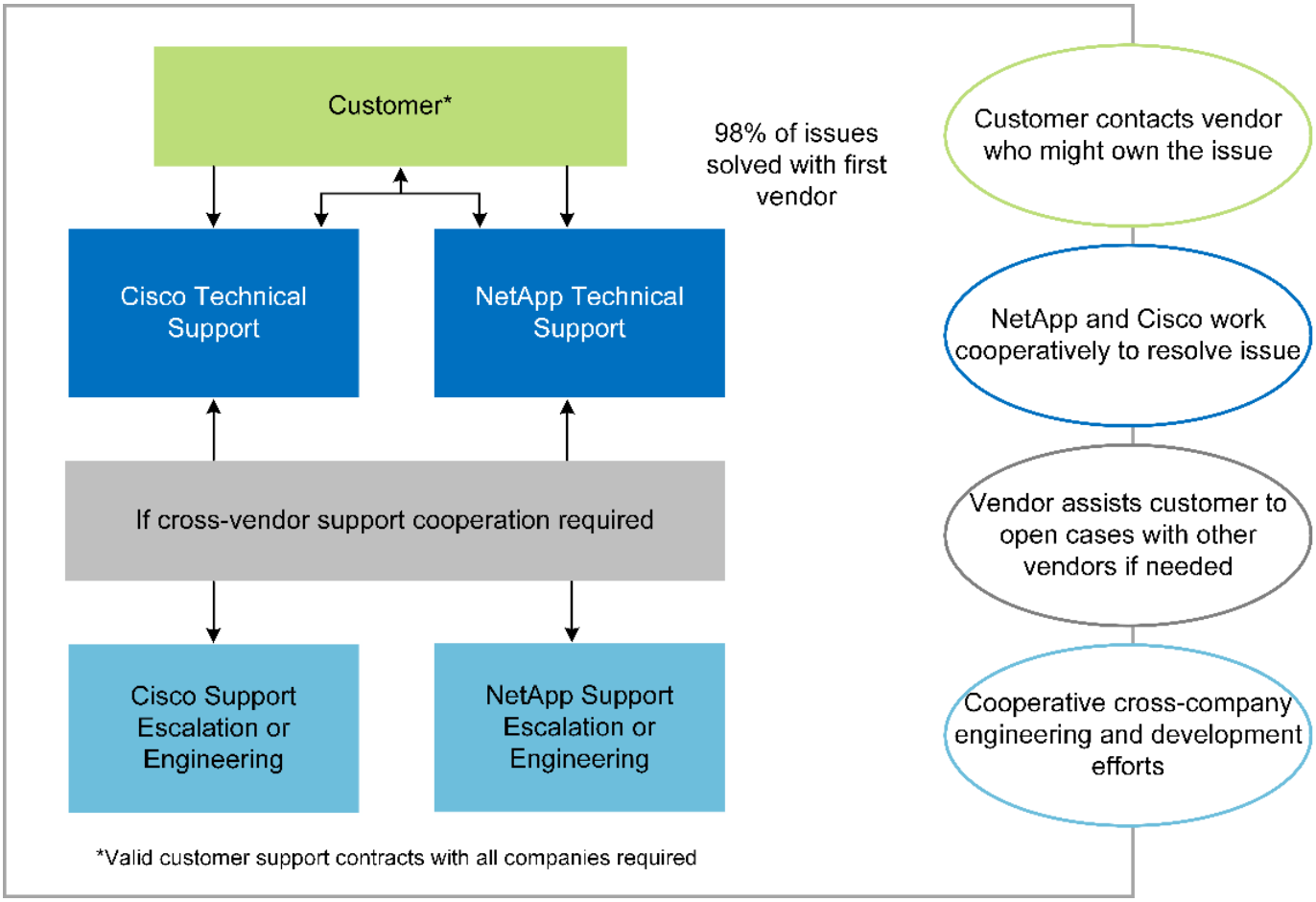
- **Architettura modulare.** FlexPod soddisfa le diverse esigenze dell'architettura modulare MEDITECH con piattaforme FlexPod appositamente configurate per ogni carico di lavoro specifico. Tutti i componenti sono collegati tramite un server in cluster, un fabric di gestione dello storage e un set di strumenti di gestione coesivi.
- **Tecnologia leader del settore a ogni livello dello stack convergente.** Cisco, NetApp, VMware e Microsoft Windows sono tutti classificati come numero 1 o 2 dagli analisti di settore nelle rispettive categorie di server, networking, storage e sistemi operativi.
- **Protezione degli investimenti con IT standardizzato e flessibile.** l'architettura di riferimento di FlexPod anticipa le nuove versioni e gli aggiornamenti dei prodotti, con rigorosi test di interoperabilità continui per adattarsi alle tecnologie future non appena diventano disponibili.
- **Implementazione collaudata in un'ampia gamma di ambienti.** FlexPod è stato installato in più organizzazioni di clienti MEDITECH, pre-testato e validato congiuntamente con i più diffusi hypervisor, sistemi operativi, applicazioni e software di infrastruttura.

Comprovata architettura FlexPod e supporto congiunto

FlexPod è una soluzione comprovata per data center, che offre un'infrastruttura flessibile e condivisa che può essere facilmente scalabile per supportare la crescita dei carichi di lavoro senza influire negativamente sulle performance. Sfruttando l'architettura FlexPod, questa soluzione offre tutti i vantaggi di FlexPod, tra cui:

- **Prestazioni per soddisfare i requisiti dei carichi di lavoro MEDITECH.** a seconda dei requisiti della proposta di configurazione hardware MEDITECH, è possibile implementare diverse piattaforme ONTAP per soddisfare i requisiti di i/o e latenza richiesti.
- **Scalabilità per adattarsi facilmente alla crescita dei dati clinici.** scalabilità dinamica di macchine virtuali (VM), server e capacità di storage on-demand, senza limiti tradizionali.
- **Efficienza migliorata.** Riduci sia il tempo di amministrazione che il TCO con un'infrastruttura virtualizzata convergente, che è più semplice da gestire e che memorizza i dati in modo più efficiente, migliorando al contempo le performance del software MEDITECH.
- **Rischi ridotti.** Riduci al minimo le interruzioni del business con una piattaforma pre-validata basata su un'architettura definita che elimina le incertezze di implementazione e consente l'ottimizzazione continua dei workload.
- **Supporto congiunto di FlexPod.** NetApp e Cisco hanno definito il supporto congiunto, un modello di supporto forte, scalabile e flessibile per soddisfare i requisiti di supporto specifici dell'infrastruttura convergente di FlexPod. Questo modello utilizza l'esperienza, le risorse e l'esperienza di supporto tecnico di NetApp e Cisco per fornire un processo semplificato per identificare e risolvere il problema di supporto FlexPod, indipendentemente dalla posizione del problema. Con il modello di supporto cooperativo FlexPod, il tuo sistema FlexPod funziona in modo efficiente e sfrutta la tecnologia più aggiornata, mentre lavori con un team esperto per aiutarti a risolvere i problemi di integrazione.

  Il supporto cooperativo FlexPod è particolarmente utile per le organizzazioni sanitarie che eseguono applicazioni business-critical come MEDITECH sull'infrastruttura convergente FlexPod. La figura seguente illustra il modello di supporto cooperativo FlexPod.



Oltre a questi vantaggi, ogni componente dello stack di data center FlexPod con la soluzione MEDITECH offre

vantaggi specifici per i flussi di lavoro MEDITECH EHR.

Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS), un sistema autointegrato e consapevole, è costituito da un singolo dominio di gestione che è interconnesso con un'infrastruttura i/o unificata. Affinché l'infrastruttura possa fornire informazioni critiche sui pazienti con la massima disponibilità, Cisco UCS per ambienti MEDITECH è stato allineato con le raccomandazioni e le Best practice dell'infrastruttura MEDITECH.

La base di MEDITECH sull'architettura Cisco UCS è la tecnologia Cisco UCS, con la gestione integrata dei sistemi, i processori Intel Xeon e la virtualizzazione dei server. Queste tecnologie integrate risolvono le sfide del data center e ti aiutano a raggiungere i tuoi obiettivi di progettazione del data center per MEDITECH. Cisco UCS unifica la gestione di LAN, SAN e sistemi in un unico collegamento semplificato per server rack, server blade e macchine virtuali. Cisco UCS è un'architettura i/o end-to-end che incorpora Cisco Unified Fabric e la tecnologia Cisco Fabric Extender (tecnologia FEX) per collegare ogni componente di Cisco UCS con un singolo fabric di rete e un singolo layer di rete.

Il sistema può essere implementato come una singola o più unità logiche che incorporano e sono scalabili su più chassis blade, server rack, rack e data center. Il sistema implementa un'architettura radicalmente semplificata che elimina i molteplici dispositivi ridondanti che popolano i tradizionali chassis per server blade e server rack. Nei sistemi tradizionali, i dispositivi ridondanti come gli adattatori Ethernet e FC e i moduli di gestione dello chassis danno luogo a livelli di complessità. Cisco UCS è costituito da una coppia ridondante di Cisco UCS Fabric Interconnects (Fi) che forniscono un singolo punto di gestione e un singolo punto di controllo per tutto il traffico i/O.

Cisco UCS utilizza profili di servizio per garantire che i server virtuali nell'infrastruttura Cisco UCS siano configurati correttamente. I profili di servizio sono composti da policy di rete, storage e calcolo create una volta dagli esperti in ogni disciplina. I profili di servizio includono informazioni critiche sull'identità del server, come indirizzi LAN e SAN, configurazioni i/o, versioni del firmware, ordine di avvio, LAN virtuale di rete (VLAN), porta fisica e policy QoS. I profili di servizio possono essere creati dinamicamente e associati a qualsiasi server fisico nel sistema in pochi minuti, anziché in ore o giorni. L'associazione dei profili di servizio con i server fisici viene eseguita come un'operazione semplice e singola e consente la migrazione delle identità tra i server dell'ambiente senza richiedere alcuna modifica della configurazione fisica. Facilita il provisioning bare-metal rapido delle sostituzioni per i server ritirati.

L'utilizzo dei profili di servizio garantisce che i server siano configurati in modo coerente in tutta l'azienda. Quando vengono utilizzati più domini di gestione Cisco UCS, Cisco UCS Central può utilizzare profili di servizio globali per sincronizzare le informazioni di configurazione e policy tra i domini. Se la manutenzione deve essere eseguita in un dominio, l'infrastruttura virtuale può essere migrata in un altro dominio. Questo approccio aiuta a garantire che anche quando un singolo dominio è offline, le applicazioni continuino a funzionare con alta disponibilità.

Per dimostrare che soddisfa i requisiti di configurazione del server, Cisco UCS è stato ampiamente testato con MEDITECH in un periodo di più anni. Cisco UCS è una piattaforma server supportata, elencata sul sito MEDITECH Product Resources System Support.

Networking Cisco

Gli switch Cisco Nexus e Cisco MDS Multilayer Director offrono connettività di livello Enterprise e consolidamento SAN. La rete di storage multiprotocollo Cisco riduce i rischi aziendali fornendo flessibilità e opzioni: FC, Fibre Connection (FICON), FC over Ethernet (FCoE), SCSI over IP (iSCSI) e FC over IP (FCIP).

Gli switch Cisco Nexus offrono una delle funzionalità di rete del data center più complete in un'unica piattaforma. Offrono performance e densità elevate per data center e core del campus. Offrono inoltre un set completo di funzionalità per l'aggregazione del data center, l'end-of-row e le implementazioni di

interconnessione del data center in una piattaforma modulare altamente resiliente.

Cisco UCS integra le risorse di calcolo con gli switch Cisco Nexus e un fabric i/o unificato che identifica e gestisce diversi tipi di traffico di rete. Questo traffico include l'i/o dello storage, il traffico desktop in streaming, la gestione e l'accesso alle applicazioni cliniche e aziendali. Otterrai:

- **Scalabilità dell'infrastruttura.** virtualizzazione, alimentazione e raffreddamento efficienti, scalabilità del cloud con automazione, alta densità e performance elevate supportano una crescita efficiente del data center.
- **Continuità operativa.** il design integra hardware, funzionalità software NX-OS e gestione per supportare ambienti senza downtime.
- **QoS di rete e computer.** Cisco offre classe di servizio (COS) e QoS basati su policy per reti, storage e fabric di calcolo per performance ottimali delle applicazioni mission-critical.
- **Flessibilità di trasporto.** adotta in modo incrementale nuove tecnologie di rete con una soluzione conveniente.

Insieme, Cisco UCS con switch Cisco Nexus e Cisco MDS Multilayer director offre una soluzione di calcolo, networking e connettività SAN ottimale per MEDITECH.

NetApp ONTAP

Lo storage NetApp che esegue il software ONTAP riduce i costi complessivi dello storage e offre i tempi di risposta in lettura e scrittura a bassa latenza e gli IOPS necessari per i carichi di lavoro MEDITECH. ONTAP supporta configurazioni di storage all-flash e ibride per creare una piattaforma di storage ottimale che soddisfi i requisiti MEDITECH. I sistemi con accelerazione flash di NetApp hanno ricevuto la convalida e la certificazione MEDITECH, offrendo ai clienti MEDITECH le performance e la reattività fondamentali per le operazioni MEDITECH sensibili alla latenza. Creando più domini di errore in un singolo cluster, i sistemi NetApp possono anche isolare la produzione dalla non produzione. I sistemi NetApp riducono inoltre i problemi di performance con un livello minimo garantito di performance per i carichi di lavoro con QoS ONTAP.

L'architettura scale-out del software ONTAP può adattarsi in modo flessibile a diversi carichi di lavoro i/O. Per offrire il throughput necessario e la bassa latenza di cui le applicazioni cliniche hanno bisogno, fornendo al contempo un'architettura scalabile e modulare, le configurazioni all-flash vengono generalmente utilizzate nelle architetture ONTAP. I nodi AFF di NetApp possono essere combinati nello stesso cluster scale-out con nodi di storage ibridi (HDD e flash) adatti per l'archiviazione di set di dati di grandi dimensioni con throughput elevato. Oltre a una soluzione di backup approvata da MEDITECH, puoi clonare, replicare ed eseguire il backup del tuo ambiente MEDITECH, dal costoso storage SSD (Solid-state Drive) allo storage HDD più economico su altri nodi. Questo approccio soddisfa o supera le linee guida MEDITECH per la clonazione basata SU SAN e il backup dei pool di produzione.

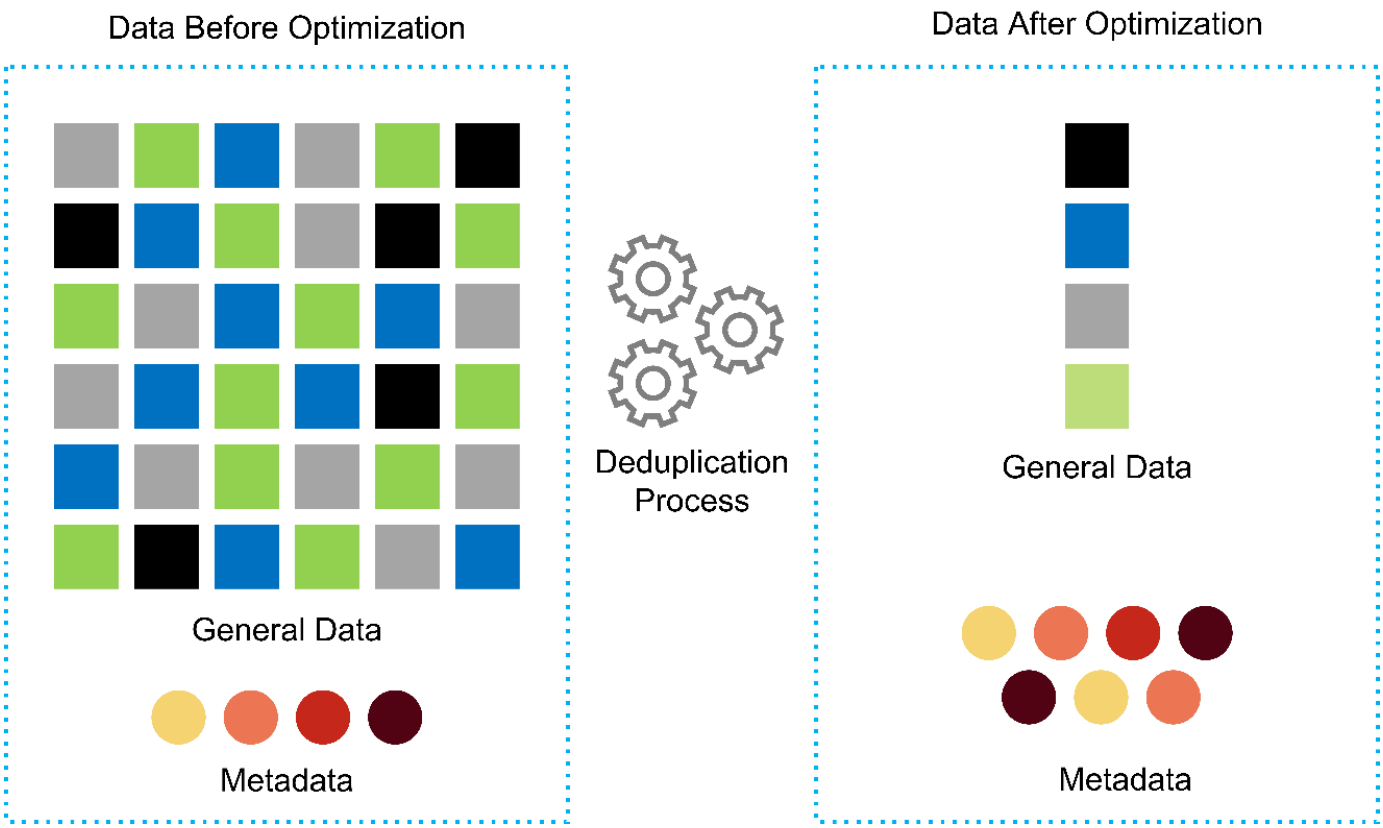
Molte delle funzionalità di ONTAP sono particolarmente utili negli ambienti MEDITECH: Semplificazione della gestione, aumento della disponibilità e dell'automazione e riduzione della quantità totale di storage necessario. Grazie a queste funzionalità, otterrai:

- **Performance eccezionali.** la soluzione NetApp AFF condivide l'architettura di storage unificata, il software ONTAP, l'interfaccia di gestione, i servizi dati avanzati e il set di funzionalità avanzate di cui dispongono le altre famiglie di prodotti NetApp FAS. Questa innovativa combinazione di supporti all-flash e ONTAP offre la bassa latenza costante e alti IOPS dello storage all-flash con la qualità leader del settore del software ONTAP.
- **Efficienza dello storage.** Riduci i requisiti di capacità totale con la deduplica, la tecnologia di replica dei dati NetApp FlexClone, la compressione inline, la compattazione inline, la replica thin, il thin provisioning, e deduplica aggregata.

La deduplica NetApp fornisce la deduplica a livello di blocco in un volume o in un componente di dati NetApp FlexVol. In sostanza, la deduplica rimuove i blocchi duplicati, memorizzando solo blocchi univoci nel volume FlexVol o nel componente dati.

La deduplica funziona con un elevato grado di granularità e opera sul file system attivo del volume FlexVol o del componente dati. È trasparente per le applicazioni, pertanto è possibile utilizzarlo per deduplicare i dati provenienti da qualsiasi applicazione che utilizzi il sistema NetApp. È possibile eseguire la deduplica del volume come processo inline (a partire da ONTAP 8.3.2). È inoltre possibile eseguirlo come processo in background che può essere configurato per essere eseguito automaticamente, pianificato o eseguito manualmente tramite CLI, Gestore di sistema NetApp ONTAP o NetApp Active IQ Unified Manager.

La seguente figura illustra il funzionamento della deduplica NetApp al massimo livello.

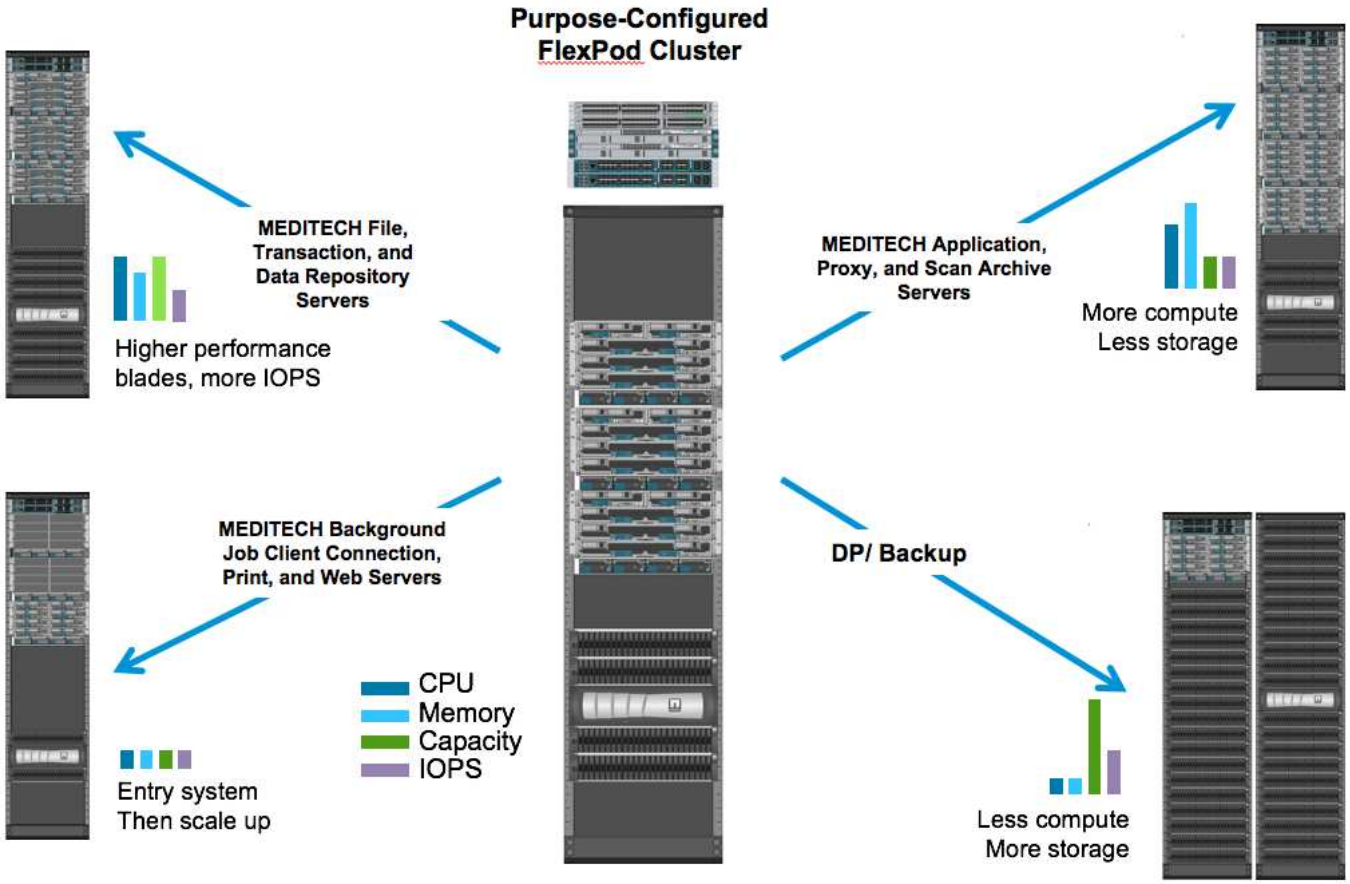


- **Cloning efficiente in termini di spazio.** la funzionalità FlexClone consente di creare cloni quasi istantaneamente per supportare il refresh dell'ambiente di backup e test. Questi cloni consumano più storage solo quando vengono apportate modifiche.
- **Le tecnologie NetApp Snapshot e SnapMirror.** ONTAP è in grado di creare copie Snapshot efficienti in termini di spazio dei LUN (Logical Unit Number) utilizzati dall'host MEDITECH. Per le implementazioni dual-site, è possibile implementare il software SnapMirror per una maggiore capacità di replica e resilienza dei dati.
- **Protezione integrata dei dati.** le funzionalità complete di protezione dei dati e disaster recovery consentono di proteggere le risorse di dati critiche e fornire il disaster recovery.
- **Operazioni senza interruzioni.** è possibile eseguire aggiornamenti e manutenzione senza interrompere la trasmissione dei dati.
- **QoS e QoS adattivi (AQoS).** la QoS dello storage consente di limitare i potenziali carichi di lavoro ingombrante. Cosa più importante, la QoS può garantire un minimo di performance per carichi di lavoro critici come la produzione MEDITECH. Limitando i conflitti, NetApp QoS può ridurre i problemi legati alle

performance. AQoS funziona con gruppi di criteri predefiniti, che è possibile applicare direttamente a un volume. Questi gruppi di policy possono scalare automaticamente un limite massimo di throughput o le dimensioni da pavimento a volume, mantenendo il rapporto tra IOPS e terabyte e gigabyte al variare delle dimensioni del volume.

- **NetApp Data Fabric.** NetApp Data Fabric semplifica e integra la gestione dei dati in ambienti cloud e on-premise per accelerare la trasformazione digitale. Offre applicazioni e servizi di gestione dei dati coerenti e integrati per la visibilità e le informazioni sui dati, l'accesso e il controllo dei dati, la protezione e la sicurezza dei dati. NetApp è integrato con Amazon Web Services (AWS), Azure, Google Cloud Platform e i cloud IBM Cloud, offrendo un'ampia scelta.

La figura seguente illustra l'architettura FlexPod per i carichi di lavoro MEDITECH.



Panoramica DI MEDITECH

Medical Information Technology, Inc., comunemente nota come MEDITECH, è una società di software con sede in Massachusetts che fornisce sistemi informativi per le organizzazioni sanitarie. MEDITECH fornisce un sistema EHR progettato per memorizzare e organizzare i dati più recenti dei pazienti e per fornire i dati al personale clinico. I dati dei pazienti includono, a titolo esemplificativo ma non esaustivo, dati demografici, anamnesi medica, farmaci, risultati dei test di laboratorio; immagini radiologiche e informazioni personali come età, altezza e peso.

Non rientra nell'ambito di questo documento la copertura dell'ampia gamma di funzioni supportate dal software MEDITECH. L'Appendice A fornisce ulteriori informazioni su questi ampi set di funzioni MEDITECH. Le applicazioni MEDITECH richiedono diverse macchine virtuali per supportare queste funzioni. Per implementare queste applicazioni, consulta le raccomandazioni di MEDITECH.

Per ogni implementazione, dal punto di vista del sistema storage, tutti i sistemi software MEDITECH richiedono

un database distribuito incentrato sul paziente. MEDITECH dispone di un proprio database proprietario, che utilizza il sistema operativo Windows.

Bridgehead e CommVault sono le due applicazioni software di backup certificate da NetApp e MEDITECH. L'ambito di questo documento non riguarda l'implementazione di queste applicazioni di backup.

L'obiettivo principale di questo documento è consentire allo stack FlexPod (server e storage) di soddisfare i requisiti di performance-driven per il database MEDITECH e i requisiti di backup nell'ambiente EHR.

Costruito ad hoc per carichi di lavoro MEDITECH specifici

MEDITECH non rivende hardware, hypervisor o sistemi operativi per server, rete o storage; tuttavia, ha requisiti specifici per ogni componente dello stack dell'infrastruttura. Pertanto, Cisco e NetApp hanno lavorato insieme per testare e abilitare FlexPod Datacenter per essere correttamente configurato, implementato e supportato in modo da soddisfare i requisiti dell'ambiente di produzione MEDITECH di clienti come te.

Categorie MEDITECH

MEDITECH associa le dimensioni dell'implementazione a un numero di categoria compreso tra 1 e 6. La categoria 1 rappresenta le implementazioni MEDITECH più piccole, mentre la categoria 6 rappresenta le implementazioni MEDITECH più grandi.

Per informazioni sulle caratteristiche di i/o e sui requisiti di performance per un host MEDITECH in ciascuna categoria, consulta NetApp "TR-4190: Linee guida di dimensionamento NetApp per ambienti MEDITECH".

Piattaforma MEDITECH

La piattaforma di espansione MEDITECH è l'ultima versione del software EHR dell'azienda. Le piattaforme MEDITECH precedenti sono Client/Server 5.x e MAGIC. Questa sezione descrive la piattaforma MEDITECH (applicabile a expse, 6.x, C/S 5.x e MAGIC), relativa all'host MEDITECH e ai relativi requisiti di storage.

Per tutte le piattaforme MEDITECH precedenti, più server eseguono il software MEDITECH, eseguendo diverse attività. La figura precedente mostra un tipico sistema MEDITECH, inclusi gli host MEDITECH che fungono da server di database applicativi e altri server MEDITECH. Esempi di altri server MEDITECH includono l'applicazione Data Repository, l'applicazione Scanning and Archiving e i background Job Client. Per l'elenco completo degli altri server MEDITECH, consultare i documenti "proposta di configurazione hardware" (per le nuove implementazioni) e "attività di valutazione hardware" (per le implementazioni esistenti). È possibile ottenere questi documenti da MEDITECH attraverso l'integratore di sistema MEDITECH o dal Technical account Manager (TAM) MEDITECH.

Host DI MEDITECH

Un host MEDITECH è un server di database. Questo host è anche chiamato file server MEDITECH (per la piattaforma expse, 6.x o C/S 5.x) o COME MACCHINA MAGICA (per la piattaforma MAGICA). Questo documento utilizza il termine host MEDITECH per fare riferimento a un file server MEDITECH o A UNA MACCHINA MAGICA.

GLI host MEDITECH possono essere server fisici o macchine virtuali in esecuzione sul sistema operativo Microsoft Windows Server. Più comunemente sul campo, gli host MEDITECH vengono implementati come macchine virtuali Windows eseguite su un server VMware ESXi. Al momento della stesura del presente documento, VMware è l'unico hypervisor supportato da MEDITECH. Un host MEDITECH memorizza il proprio programma, il dizionario e i file di dati su un'unità Microsoft Windows (ad esempio, l'unità e) sul sistema Windows.

In un ambiente virtuale, un disco Windows e risiede su un LUN collegato alla macchina virtuale tramite un

RDM (raw device mapping) in modalità di compatibilità fisica. L'utilizzo dei file VMDK (Virtual Machine Disk) come disco Windows e in questo scenario non è supportato da MEDITECH.

Caratteristica i/o del carico di lavoro host MEDITECH

La caratteristica di i/o di ciascun host MEDITECH e del sistema nel suo complesso dipende dalla piattaforma MEDITECH implementata. Tutte le piattaforme MEDITECH (expse, 6.x, C/S 5.x e MAGIC) generano carichi di lavoro casuali al 100%.

La piattaforma di espansione MEDITECH genera il carico di lavoro più impegnativo perché ha la percentuale più alta di operazioni di scrittura e IOPS complessivi per host, seguiti da 6.x, C/S 5.x e le piattaforme MAGICHE.

Per ulteriori informazioni sulle descrizioni dei carichi di lavoro MEDITECH, vedere "TR-4190: Linee guida di dimensionamento NetApp per ambienti MEDITECH".

Rete di storage

MEDITECH richiede l'utilizzo del protocollo FC per il traffico di dati tra il sistema NetApp FAS o AFF e gli host MEDITECH di tutte le categorie.

Presentazione dello storage per un host MEDITECH

Ogni host MEDITECH utilizza due dischi Windows:

- **Disco C.** questo disco memorizza il sistema operativo Windows Server e i file dell'applicazione host MEDITECH.
- **Disco E.** l'host MEDITECH memorizza il proprio programma, il dizionario e i file di dati sull'unità e del sistema operativo Windows Server. L'unità e è un LUN mappato dal sistema NetApp FAS o AFF utilizzando il protocollo FC. MEDITECH richiede l'utilizzo del protocollo FC per soddisfare i requisiti di latenza di lettura e scrittura dell'host MEDITECH.

Convenzione di naming del volume e del LUN

MEDITECH richiede l'utilizzo di una specifica convenzione di denominazione per tutte le LUN.

Prima di qualsiasi implementazione dello storage, verificare la proposta di configurazione hardware MEDITECH per confermare la convenzione di denominazione per i LUN. Il processo di backup MEDITECH si basa sulla convenzione di naming del volume e del LUN per identificare correttamente le LUN specifiche da eseguire.

Strumenti di gestione completi e funzionalità di automazione

Cisco UCS con Cisco UCS Manager

Cisco si concentra su tre elementi chiave per offrire un'infrastruttura di data center superiore: Semplificazione, sicurezza e scalabilità. Il software Cisco UCS Manager, combinato con la modularità della piattaforma, offre una piattaforma di virtualizzazione desktop semplificata, sicura e scalabile:

- **Simplified.** Cisco UCS offre un approccio completamente nuovo al computing standard di settore e fornisce il nucleo dell'infrastruttura del data center per tutti i carichi di lavoro. Cisco UCS offre numerose funzionalità e vantaggi, tra cui la riduzione del numero di server necessari e la riduzione del numero di cavi utilizzati per server. Un'altra caratteristica importante è la capacità di implementare rapidamente o di eseguire il reprovisioning dei server attraverso i profili di servizio Cisco UCS. Con un numero inferiore di server e cavi da gestire e con un provisioning ottimizzato dei workload di applicazioni e server, le

operazioni sono semplificate. È possibile eseguire il provisioning di diversi server blade e rack in pochi minuti con i profili di servizio di Cisco UCS Manager. I profili di servizio Cisco UCS eliminano i runbook di integrazione dei server ed eliminano la deriva della configurazione. Questo approccio accelera il time-to-Productivity per gli utenti finali, migliora l'agilità del business e consente l'allocazione delle risorse IT ad altre attività.

Cisco UCS Manager automatizza molte operazioni del data center comuni e soggette a errori, come la configurazione e il provisioning di server, rete e infrastruttura di accesso allo storage. Inoltre, i server blade Cisco UCS B-Series e i server rack C-Series con grandi ingombri di memoria consentono un'elevata densità dell'utente delle applicazioni, riducendo i requisiti dell'infrastruttura server.

La semplificazione consente un'implementazione dell'infrastruttura MEDITECH più rapida e di maggior successo.

- **Secure.** sebbene le macchine virtuali siano intrinsecamente più sicure rispetto ai loro predecessori fisici, introducono nuove sfide per la sicurezza. I server web e applicativi mission-critical che utilizzano un'infrastruttura comune, come i desktop virtuali, sono ora a maggior rischio per le minacce alla sicurezza. Il traffico tra macchine virtuali rappresenta ora un'importante considerazione per la sicurezza che i responsabili IT devono affrontare, soprattutto negli ambienti dinamici in cui le macchine virtuali, utilizzando VMware vMotion, si spostano nell'infrastruttura server.

  La virtualizzazione, pertanto, aumenta significativamente la necessità di una consapevolezza a livello di macchine virtuali delle policy e della sicurezza, soprattutto in considerazione della natura dinamica e fluida della mobilità delle macchine virtuali in un'infrastruttura di calcolo estesa. La facilità con cui i nuovi desktop virtuali possono proliferare aumenta l'importanza di un'infrastruttura di sicurezza e di rete consapevole della virtualizzazione. L'infrastruttura del data center Cisco (soluzioni Cisco UCS, Cisco MDS e della famiglia Cisco Nexus) per la virtualizzazione dei desktop offre una solida sicurezza per data center, rete e desktop, con una sicurezza completa dal desktop all'hypervisor. La sicurezza viene migliorata con la segmentazione dei desktop virtuali, le policy e l'amministrazione VM-aware e la sicurezza di rete nell'infrastruttura LAN e WAN.

- **Scalabile.** la crescita delle soluzioni di virtualizzazione è tutt'altro che inevitabile, quindi una soluzione deve essere in grado di scalare e scalare in modo prevedibile con questa crescita. Le soluzioni di virtualizzazione Cisco supportano un'elevata densità di macchine virtuali (VM per server) e un numero maggiore di server è in grado di scalare con performance quasi lineari. L'infrastruttura del data center Cisco offre una piattaforma flessibile per la crescita e migliora l'agilità del business. I profili di servizio di Cisco UCS Manager consentono il provisioning host on-demand e rendono semplice l'implementazione di centinaia di host quanto l'implementazione di decine di host.

  I server Cisco UCS offrono performance e scalabilità quasi lineari. Cisco UCS implementa la tecnologia brevettata Cisco Extended Memory per offrire un ampio spazio di memoria con meno socket (con una scalabilità fino a 1 TB di memoria con server a 2 e 4 socket). Utilizzando la tecnologia Unified Fabric come building block, la larghezza di banda aggregata di Cisco UCS Server può scalare fino a 80 Gbps per server, mentre Cisco UCS Fabric Interconnect a nord può produrre 2 Tbps alla velocità di linea. Questa funzionalità aiuta a prevenire i colli di bottiglia di i/o e memoria per la virtualizzazione dei desktop. Cisco UCS, con la sua architettura di rete basata su Unified Fabric ad alte performance e bassa latenza, supporta elevati volumi di traffico di desktop virtuale, incluso il traffico video e di comunicazioni ad alta risoluzione. Inoltre, ONTAP aiuta a mantenere la disponibilità dei dati e le performance ottimali durante le tempeste di avvio e accesso come parte delle soluzioni di virtualizzazione FlexPod.

  I design dell'infrastruttura per data center Cisco UCS, Cisco MDS e Cisco Nexus offrono un'eccellente piattaforma per la crescita. Ottieni una scalabilità trasparente delle risorse di server, rete e storage per supportare la virtualizzazione dei desktop, le applicazioni dei data center e il cloud computing.

VMware vCenter Server

VMware vCenter Server offre una piattaforma centralizzata per la gestione degli ambienti MEDITECH, in modo che la tua organizzazione sanitaria possa automatizzare e fornire un'infrastruttura virtuale in tutta sicurezza:

- **Implementazione semplice.** implementazione rapida e semplice di vCenter Server mediante un'appliance virtuale.
- **Controllo e visibilità centralizzati.** amministrare l'intera infrastruttura VMware vSphere da un'unica posizione.
- **Ottimizzazione proattiva.** allocare e ottimizzare le risorse per la massima efficienza.
- **Management.** utilizza potenti plug-in e tool per semplificare la gestione ed estendere il controllo.

Virtual Storage Console per VMware vSphere

Virtual Storage Console (VSC), vSphere API for Storage Awareness (VASA) Provider e VMware Storage Replication Adapter (SRA) per VMware vSphere di NetApp costituiscono una singola appliance virtuale. La suite di prodotti include SRA e VASA Provider come plug-in di vCenter Server, che fornisce una gestione del ciclo di vita end-to-end per le macchine virtuali in ambienti VMware che utilizzano sistemi storage NetApp.

L'appliance virtuale per VSC, VASA Provider e SRA si integra perfettamente con VMware vSphere Web Client e consente di utilizzare i servizi SSO. In un ambiente con più istanze di VMware vCenter Server, ogni istanza di vCenter Server che si desidera gestire deve avere la propria istanza registrata di VSC. La pagina del dashboard VSC consente di controllare rapidamente lo stato generale dei datastore e delle macchine virtuali.

Implementando l'appliance virtuale per VSC, VASA Provider e SRA, è possibile eseguire le seguenti attività:

- **Utilizzare VSC per implementare e gestire lo storage e configurare l'host ESXi.** è possibile utilizzare VSC per aggiungere credenziali, rimuovere credenziali, assegnare credenziali e impostare autorizzazioni per i controller di storage nell'ambiente VMware. Inoltre, è possibile gestire server ESXi connessi ai sistemi storage NetApp. Con un paio di clic, è possibile impostare i valori delle Best practice consigliate per timeout host, NAS e multipathing per tutti gli host. È inoltre possibile visualizzare i dettagli dello storage e raccogliere informazioni diagnostiche.
- **Utilizzare il provider VASA per creare profili di funzionalità di storage e impostare gli allarmi.** il provider VASA per ONTAP viene registrato con VSC quando si attiva l'interno del provider VASA. È possibile creare e utilizzare profili di funzionalità storage e datastore virtuali. È inoltre possibile impostare gli allarmi per avvisare l'utente quando le soglie per volumi e aggregati sono quasi piene. È possibile monitorare le performance dei VMDK e delle VM create su datastore virtuali.
- **Utilizzare SRA per il disaster recovery.** è possibile utilizzare SRA per configurare siti protetti e di ripristino nel proprio ambiente per il disaster recovery durante i guasti.

NetApp OnCommand Insight e ONTAP

NetApp OnCommand Insight integra la gestione dell'infrastruttura nella catena di erogazione dei servizi MEDITECH. Questo approccio offre alla tua organizzazione sanitaria un controllo, un'automazione e un'analisi migliori della tua infrastruttura di storage, rete e calcolo. Può ottimizzare l'infrastruttura attuale per ottenere il massimo vantaggio, semplificando al contempo il processo di determinazione di cosa e quando acquistare. Inoltre, riduce i rischi associati a complesse migrazioni tecnologiche. Poiché non richiede agenti, l'installazione è semplice e senza interruzioni. Lo storage installato e i dispositivi SAN vengono continuamente rilevati e vengono raccolte informazioni dettagliate per una visibilità completa dell'intero ambiente di storage. È possibile identificare rapidamente le risorse utilizzate in modo errato, disallineate, sottoutilizzate o orfane e recuperarle per alimentare un'espansione futura. OnCommand Insight ti aiuta a:

- **Ottimizzare le risorse esistenti.** identificare le risorse utilizzate in modo errato, sottoutilizzate o orfane

utilizzando Best practice consolidate per evitare problemi e soddisfare i livelli di servizio.

- **Prendere decisioni migliori.** i dati in tempo reale aiutano a risolvere i problemi di capacità in modo più rapido per pianificare con precisione gli acquisti futuri, evitare l'overspanning e rinviare le spese di capitale.
- **Accelera le iniziative IT.** meglio comprendere i tuoi ambienti virtuali per aiutarti a gestire i rischi, ridurre al minimo i downtime e accelerare l'implementazione del cloud.

Progettazione

L'architettura di FlexPod per MEDITECH si basa sulle indicazioni di MEDITECH, Cisco e NetApp e sull'esperienza dei partner nella collaborazione con clienti MEDITECH di tutte le dimensioni. L'architettura è adattabile e applica le Best practice per MEDITECH, a seconda della strategia del data center, delle dimensioni dell'organizzazione e del sistema centralizzato, distribuito o multitenant.

La corretta architettura dello storage può essere determinata dalla dimensione complessiva con gli IOPS totali. Le performance da sole non sono l'unico fattore e potresti decidere di utilizzare un numero maggiore di nodi in base ai requisiti aggiuntivi del cliente. Il vantaggio dell'utilizzo dello storage NetApp consiste nel fatto che è possibile scalare il cluster in modo semplice e senza interruzioni in base alle esigenze. È inoltre possibile rimuovere senza interruzioni i nodi dal cluster per riutilizzare le apparecchiature o durante gli aggiornamenti delle apparecchiature.

Ecco alcuni dei vantaggi dell'architettura di storage NetApp ONTAP:

- **Scale-up e scale-out semplici e senza interruzioni.** puoi aggiornare, aggiungere o rimuovere dischi e nodi utilizzando le operazioni senza interruzioni di ONTAP. Puoi iniziare con quattro nodi e passare a sei nodi o eseguire l'upgrade a controller più grandi senza interruzioni.
- * Efficienza dello storage.* Riduci i requisiti di capacità totale con deduplica, NetApp FlexClone, compressione inline, compaction inline, replica thin, thin provisioning e deduplica aggregata. La funzionalità FlexClone consente di creare cloni quasi istantaneamente per supportare gli aggiornamenti dell'ambiente di backup e test. Questi cloni consumano più storage solo quando vengono apportate modifiche.
- **Server shadow del database per il disaster recovery.** il server shadow del database per il disaster recovery fa parte della strategia di business continuity (utilizzato per supportare la funzionalità di sola lettura dello storage e potenzialmente configurato per essere un'istanza di lettura/scrittura dello storage). Pertanto, il posizionamento e il dimensionamento del terzo sistema storage sono in genere gli stessi del sistema storage del database in produzione.
- **Coerenza del database (richiede una certa considerazione).** se si utilizzano le copie di backup di NetApp SnapMirror in relazione alla business continuity, vedere "TR-3446: Guida alle Best practice e alla panoramica di SnapMirror Async".

Layout dello storage

Aggregati dedicati per host MEDITECH

Il primo passo per soddisfare i requisiti di performance elevate e alta disponibilità di MEDITECH è progettare correttamente il layout dello storage per l'ambiente MEDITECH per isolare il carico di lavoro di produzione dell'host MEDITECH su storage dedicato e dalle performance elevate.

È necessario eseguire il provisioning di un aggregato dedicato su ciascun controller di storage per memorizzare il programma, il dizionario e i file di dati degli host MEDITECH. Per eliminare la possibilità che altri carichi di lavoro utilizzino gli stessi dischi e influiscano sulle performance, non viene eseguito il

provisioning di altri storage da questi aggregati.

> Lo storage previsto per gli altri server MEDITECH non deve essere inserito nell'aggregato dedicato per le LUN utilizzate dagli host MEDITECH. È necessario collocare lo storage per altri server MEDITECH su un aggregato separato. I requisiti di storage per altri server MEDITECH sono disponibili nei documenti "proposta di configurazione hardware" (per le nuove implementazioni) e "attività di valutazione hardware" (per le implementazioni esistenti). È possibile ottenere questi documenti da MEDITECH attraverso l'integratore di sistema MEDITECH o dal Technical account Manager (TAM) MEDITECH. I tecnici delle soluzioni NetApp possono consultare il team NetApp MEDITECH Independent Software Vendor (ISV) per facilitare una configurazione corretta e completa del dimensionamento dello storage NetApp.

Distribuire uniformemente il carico di lavoro host MEDITECH in tutti i controller storage

I sistemi NetApp FAS e AFF vengono implementati come una o più coppie ad alta disponibilità. NetApp consiglia di distribuire uniformemente i carichi di lavoro di espansione MEDITECH e 6.x in ciascun controller di storage per applicare le risorse di calcolo, rete e caching su ciascun controller di storage.

Utilizza le seguenti linee guida per distribuire uniformemente i carichi di lavoro MEDITECH in ogni controller di storage:

- Se conosci gli IOPS per ciascun host MEDITECH, puoi distribuire uniformemente i carichi di lavoro di espansione MEDITECH e 6.x in tutti i controller di storage confermando che ciascun controller fornisce un numero simile di IOPS dagli host MEDITECH.
- Se non si conoscono gli IOPS per ciascun host MEDITECH, è comunque possibile distribuire uniformemente i carichi di lavoro di espansione MEDITECH e 6.x in tutti i controller storage. Completare questa attività confermando che la capacità degli aggregati per gli host MEDITECH è distribuita uniformemente su tutti i controller di storage. In questo modo, il numero di dischi è lo stesso in tutti gli aggregati di dati dedicati agli host MEDITECH.
- Utilizzare tipi di dischi simili e gruppi RAID identici per creare aggregati di storage di entrambi i controller per distribuire i carichi di lavoro in modo equo. Prima di creare l'aggregato di storage, contatta un NetApp Certified Integrator.

> Secondo MEDITECH, due host nel sistema MEDITECH generano IOPS superiori rispetto agli altri host. Le LUN di questi due host devono essere collocate in controller di storage separati. È necessario identificare questi due host con l'assistenza del team MEDITECH prima di implementare il sistema.

Posizionamento dello storage

Storage di database per host MEDITECH

Lo storage del database per un host MEDITECH viene presentato come un dispositivo a blocchi (ovvero un LUN) dal sistema NetApp FAS o AFF. Il LUN viene generalmente montato sul sistema operativo Windows come disco E.

Altro storage

Il sistema operativo host MEDITECH e l'applicazione di database generano normalmente una notevole quantità di IOPS sullo storage. Il provisioning dello storage per le macchine virtuali host MEDITECH e i relativi file VMDK, se necessario, viene considerato indipendente dallo storage necessario per soddisfare le soglie di performance MEDITECH.

Lo storage fornito per gli altri server MEDITECH non deve essere inserito nell'aggregato dedicato per le LUN utilizzate dagli host MEDITECH. Collocare lo storage per altri server MEDITECH su un aggregato separato.

Configurazione dello storage controller

Alta disponibilità

Per mitigare l'effetto del guasto del controller e consentire aggiornamenti senza interruzioni del sistema storage, è necessario configurare il sistema storage con controller in una coppia ad alta disponibilità in modalità ad alta disponibilità.

Con la configurazione della coppia di controller ad alta disponibilità, gli shelf di dischi devono essere collegati ai controller tramite percorsi multipli. Questa connessione aumenta la resilienza dello storage proteggendosi da un guasto a percorso singolo e migliora la coerenza delle performance in caso di failover del controller.

Performance dello storage durante il failover del controller storage

Per i sistemi storage configurati con controller in coppia ad alta disponibilità, nell'improbabile caso di guasto di un controller, il controller partner assume il controllo delle risorse di storage e dei carichi di lavoro del controller guasto. È importante consultare il cliente per determinare i requisiti di performance che devono essere soddisfatti in caso di guasto del controller e dimensionare il sistema di conseguenza.

Takeover assistito dall'hardware

NetApp consiglia di attivare la funzione di Takeover assistito dall'hardware su entrambi i controller di storage.

Il Takeover assistito dall'hardware è progettato per ridurre al minimo il tempo di failover del controller dello storage. Consente al modulo LAN remota o al modulo Service Processor di un controller di notificare al partner un guasto del controller più rapidamente di un trigger di timeout heartbeat, riducendo il tempo necessario per il failover. La funzione di Takeover assistito dall'hardware è attivata per impostazione predefinita per i controller di storage in una configurazione ad alta disponibilità.

Per ulteriori informazioni sul Takeover assistito dall'hardware, consultare "Centro documentazione di ONTAP 9".

Tipo di disco

Per supportare il requisito di bassa latenza di lettura dei carichi di lavoro MEDITECH, NetApp consiglia di utilizzare un SSD dalle performance elevate per gli aggregati su sistemi AFF dedicati agli host MEDITECH.

NetApp AFF

NetApp offre array AFF dalle performance elevate per soddisfare i carichi di lavoro MEDITECH che richiedono un throughput elevato e che dispongono di schemi di accesso casuale ai dati e requisiti di bassa latenza. Per i carichi di lavoro MEDITECH, gli array AFF offrono vantaggi in termini di performance rispetto ai sistemi basati su HDD. La combinazione di tecnologia flash e gestione dei dati aziendali offre vantaggi in tre aree principali: Performance, disponibilità ed efficienza dello storage.

Strumenti e servizi di supporto NetApp

NetApp offre un set completo di strumenti e servizi di supporto. Il tool NetApp AutoSupport deve essere abilitato e configurato sui sistemi NetApp AFF/FAS per chiamare casa in caso di guasto hardware o configurazione errata del sistema. Chiamando a casa, il team di supporto NetApp avvisa di porre rimedio a qualsiasi problema in modo tempestivo. NetApp Active IQ è un'applicazione basata sul web che si basa sulle informazioni AutoSupport dei sistemi NetApp, fornendo informazioni predittive e proattive per migliorare

disponibilità, efficienza e performance.

Implementazione e configurazione

Panoramica

Le linee guida per lo storage NetApp per l'implementazione di FlexPod fornite in questo documento riguardano:

- Ambienti che utilizzano ONTAP
- Ambienti che utilizzano server blade e rack Cisco UCS

Questo documento non tratta:

- Implementazione dettagliata dell'ambiente del data center FlexPod

  Per ulteriori informazioni, vedere "Data center FlexPod con design validato FC Cisco" (CVD).

- Una panoramica degli ambienti software MEDITECH, delle architetture di riferimento e delle Best practice di integrazione.

  Per ulteriori informazioni, vedere "TR-4300i: Guida alle Best practice per i sistemi di storage NetApp FAS e all-flash per gli ambienti MEDITECH" (Accesso NetApp richiesto).

- Requisiti quantitativi di performance e guida al dimensionamento.

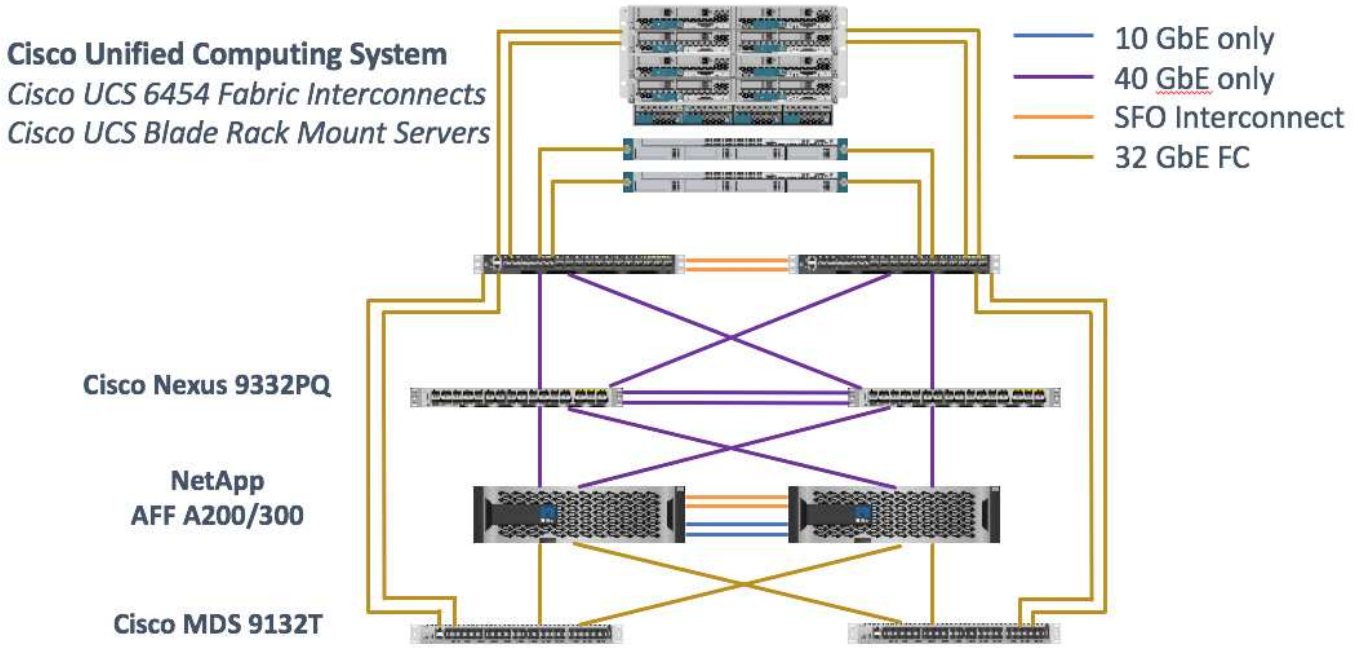
  Per ulteriori informazioni, vedere "TR-4190: Linee guida di dimensionamento NetApp per ambienti MEDITECH".

- Utilizzo delle tecnologie NetApp SnapMirror per soddisfare i requisiti di backup e disaster recovery.
- Guida generica all'implementazione dello storage NetApp.

In questa sezione viene fornita una configurazione di esempio con Best practice per l'implementazione dell'infrastruttura ed elenca i vari componenti hardware e software dell'infrastruttura e le versioni che è possibile utilizzare.

Schema di cablaggio

La figura seguente illustra il diagramma della topologia FC/40GbE da 32 GB per un'implementazione MEDITECH.



Utilizzare sempre il "Tool di matrice di interoperabilità (IMT)" per verificare che tutte le versioni del software e del firmware siano supportate. La tabella nella sezione "Moduli E componenti MEDITECH" elenca i componenti hardware e software dell'infrastruttura utilizzati nel test della soluzione.

"Pagina successiva: Configurazione dell'infrastruttura di base."

Configurazione dell'infrastruttura di base

Connettività di rete

Prima di configurare l'infrastruttura, è necessario disporre delle seguenti connessioni di rete:

- L'aggregazione di collegamenti che utilizza i canali delle porte e i canali delle porte virtuali (VPC) viene utilizzata ovunque, consentendo la progettazione di una maggiore larghezza di banda e disponibilità elevata:
  - VPC viene utilizzato tra gli switch Cisco Fi e Cisco Nexus.
  - Ogni server dispone di schede di interfaccia di rete virtuale (vNIC) con connettività ridondante all'Unified Fabric. Il failover NIC viene utilizzato tra gli IF per la ridondanza.
  - Ogni server dispone di vHBA (Virtual host Bus Adapter) con connettività ridondante all'Unified Fabric.
- Cisco UCS Fi viene configurato in modalità end-host come consigliato, fornendo il pinning dinamico delle vNIC agli switch uplink.

Connettività dello storage

Prima di configurare l'infrastruttura, è necessario disporre delle seguenti connessioni di storage:

- Gruppi di interfacce per porte di storage (ifgroup, VPC)
- Collegamento 10 GB allo switch N9K-A.
- Collegamento 10 GB allo switch N9K-B.
- Gestione in banda (bond attivo-passivo):

    - Collegamento da 1 GB allo switch di gestione N9K-A.
    - Collegamento da 1 GB allo switch di gestione N9K-B.
- Connettività end-to-end FC da 32 GB tramite switch Cisco MDS; configurazione dello zoning a singolo iniziatore
- Avvio SAN FC per ottenere il massimo livello di stateless computing; i server vengono avviati dalle LUN nel volume di boot che risiede nel cluster di storage AFF
- Tutti i carichi di lavoro MEDITECH sono ospitati su LUN FC, che sono distribuiti tra i nodi dello storage controller

Software host

È necessario installare il seguente software:

- ESXi installato sui blade Cisco UCS
- VMware vCenter installato e configurato (con tutti gli host registrati in vCenter)
- VSC installato e registrato in VMware vCenter
- Cluster NetApp configurato

"Pagina successiva: Configurazione di server blade e switch Cisco UCS."

Configurazione di server blade e switch Cisco UCS

Il software FlexPod per MEDITECH è progettato con tolleranza di errore a ogni livello. Non esiste un singolo punto di errore nel sistema. Per ottenere prestazioni ottimali, Cisco consiglia l'utilizzo di server blade hot spare.

Questo documento fornisce una guida di alto livello sulla configurazione di base di un ambiente FlexPod per il software MEDITECH. In questa sezione, vengono presentate alcune fasi di alto livello con alcuni esempi per preparare l'elemento della piattaforma di calcolo Cisco UCS della configurazione FlexPod. Un prerequisito per questa guida è che la configurazione FlexPod sia in rack, alimentata e cablata in base alle istruzioni contenute nella "Data center FlexPod con storage Fibre Channel con VMware vSphere 6.5 Update 1, NetApp AFF Serie A e Cisco UCS Manager 3.2"CVD.

Configurazione dello switch Cisco Nexus

Per la soluzione viene implementata una coppia di switch Ethernet Cisco Nexus serie 9300 con tolleranza di errore. Collegare questi switch come descritto nella "Schema di cablaggio" sezione. La configurazione di Cisco Nexus consente di ottimizzare i flussi di traffico Ethernet per l'applicazione MEDITECH.

1. Una volta completata la configurazione iniziale e la licenza, eseguire i seguenti comandi per impostare i parametri di configurazione globale su entrambi gli switch:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Creare le VLAN per la soluzione su ogni switch utilizzando la modalità di configurazione globale:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Creare l'interfaccia di distribuzione NTP (Network Time Protocol), i canali delle porte, i parametri del canale delle porte e le descrizioni delle porte per la risoluzione dei problemi come indicato in "Data center FlexPod con storage Fibre Channel con VMware vSphere 6.5 Update 1, NetApp AFF Serie A e Cisco UCS Manager 3.2"CVD.

Configurazione di Cisco MDS 9132T

Gli switch FC Cisco MDS serie 9100 offrono una connettività FC ridondante da 32 GB tra i controller NetApp AFF A200 o AFF A300 e il compute fabric Cisco UCS. Collegare i cavi come descritto in "Schema di cablaggio" sezione.

1. Dalle console di ogni switch MDS, eseguire i seguenti comandi per abilitare le funzioni richieste per la soluzione:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Configurare le singole porte, i canali delle porte e le descrizioni in base alla sezione di configurazione dello switch Cisco MDS di FlexPod in "Data center FlexPod con design validato FC Cisco".
3. Per creare le SAN virtuali (VSAN) necessarie per la soluzione, completare i seguenti passaggi in modalità

di configurazione globale:

a. Per lo switch Fabric-A MDS, eseguire i seguenti comandi:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

I numeri dei canali delle porte nelle ultime due righe del comando sono stati creati quando le singole porte, i canali delle porte e le descrizioni sono stati forniti utilizzando il documento di riferimento.

b. Per lo switch Fabric-B MDS, eseguire i seguenti comandi:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

I numeri dei canali delle porte nelle ultime due righe del comando sono stati creati quando le singole porte, i canali delle porte e le descrizioni sono stati forniti utilizzando il documento di riferimento.

4. Per ogni switch FC, creare nomi alias dei dispositivi che rendano l'identificazione di ciascun dispositivo intuitiva per le operazioni in corso, utilizzando i dettagli nel documento di riferimento.
5. Infine, creare le zone FC utilizzando i nomi alias del dispositivo creati nel passaggio 4 per ogni switch MDS come segue:

a. Per lo switch Fabric-A MDS, eseguire i seguenti comandi:

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. Per lo switch Fabric-B MDS, eseguire i seguenti comandi:

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Guida alla configurazione di Cisco UCS

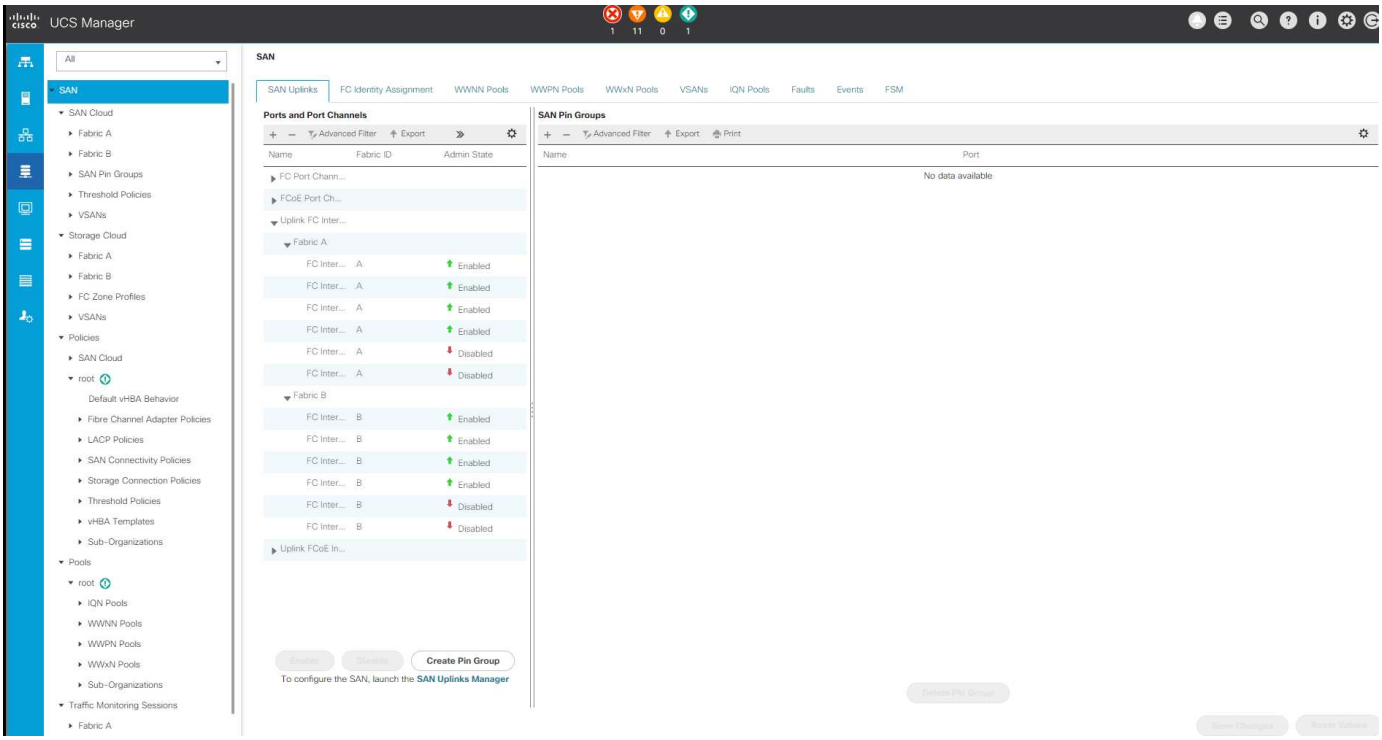
Cisco UCS consente ai clienti MEDITECH di sfruttare i propri esperti in materia di rete, storage e calcolo per creare policy e modelli che personalizzino l'ambiente in base alle proprie esigenze specifiche. Una volta creati,

questi criteri e modelli possono essere combinati in profili di servizio che offrono implementazioni coerenti, ripetibili, affidabili e rapide di server blade e rack Cisco.

Cisco UCS offre tre metodi per la gestione di un sistema Cisco UCS, denominato dominio:

- GUI di Cisco UCS Manager HTML5
- Cisco UCS CLI
- Cisco UCS Central per ambienti multidominio

La figura seguente mostra una schermata di esempio del nodo SAN in Cisco UCS Manager.



Nelle implementazioni di maggiori dimensioni, è possibile creare domini Cisco UCS indipendenti per una maggiore tolleranza agli errori a livello dei principali componenti funzionali MEDITECH.

In progetti altamente tolleranti agli errori con due o più data center, Cisco UCS Central svolge un ruolo chiave nella definizione di policy globali e profili di servizio globali per garantire la coerenza tra gli host in tutta l'azienda.

Per configurare la piattaforma di calcolo Cisco UCS, completare le seguenti procedure. Eseguire queste procedure dopo aver installato i server blade Cisco UCS B200 M5 nello chassis blade Cisco UCS 5108 AC. Inoltre, è necessario competere con i requisiti di cablaggio descritti nella "Schema di cablaggio" sezione.

1. Aggiornare il firmware di Cisco UCS Manager alla versione 3.2(2f) o successiva.
2. Configurare le impostazioni di reporting, chiamata a casa Cisco e NTP per il dominio.
3. Configurare il server e le porte di uplink su ogni fabric Interconnect.
4. Modificare la policy di rilevamento dello chassis.
5. Creare i pool di indirizzi per la gestione fuori banda, gli UUID (Universal Unique Identifier), l'indirizzo MAC, i server, il nome del nodo mondiale (WWNN) e il nome della porta mondiale (WWPN).
6. Creare i canali delle porte di uplink Ethernet e FC e le reti VSAN.

7. Creare policy per connettività SAN, controllo di rete, qualifica del pool di server, controllo dell'alimentazione, BIOS del server, e manutenzione predefinita.
8. Creare modelli vNIC e vHBA.
9. Creare policy di avvio vMedia e FC.
10. Creare modelli di profilo di servizio e profili di servizio per ciascun elemento della piattaforma MEDITECH.
11. Associare i profili di servizio ai blade server appropriati.

Per informazioni dettagliate sulla configurazione di ciascun elemento chiave dei profili di servizio Cisco UCS per FlexPod, consultare la "Data center FlexPod con storage Fibre Channel con VMware vSphere 6.5 Update 1, NetApp AFF Serie A e Cisco UCS Manager 3.2"Documento CVD.

"Pagina successiva: Best practice per la configurazione di ESXi."

Best practice per la configurazione di ESXi

Per la configurazione sul lato host di ESXi, configurare gli host VMware come si farebbe per qualsiasi carico di lavoro del database aziendale:

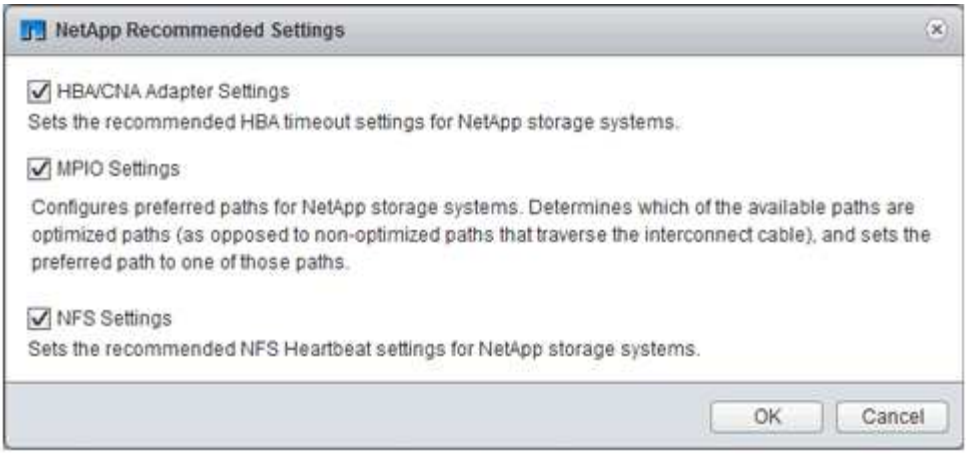
- VSC per VMware vSphere controlla e imposta le impostazioni di multipathing host ESXi e le impostazioni di timeout HBA che funzionano meglio con i sistemi storage NetApp. I valori impostati da VSC si basano su rigorosi test interni eseguiti da NetApp.
- Per ottenere performance di storage ottimali, considerare l'utilizzo di hardware di storage che supporti le API vStorage VMware - Array Integration (VAAI). Il plug-in NetApp per VAAI è una libreria software che integra le librerie di dischi virtuali VMware installate sull'host ESXi. Il pacchetto VMware VAAI consente l'offload di determinate attività dagli host fisici all'array di storage.

  È possibile eseguire attività come il thin provisioning e l'accelerazione hardware a livello di array per ridurre il carico di lavoro sugli host ESXi. La funzione di offload delle copie e di riserva dello spazio migliorano le prestazioni delle operazioni VSC. È possibile scaricare il pacchetto di installazione del plug-in e ottenere le istruzioni per l'installazione del plug-in dal sito del supporto NetApp.

  VSC imposta i timeout degli host ESXi, le impostazioni multipath, le impostazioni di timeout HBA e altri valori per ottenere performance ottimali e il failover corretto dei controller di storage NetApp. Attenersi alla seguente procedura:

  a. Dalla home page di VMware vSphere Web Client, selezionare vCenter > hosts.
  b. Fare clic con il pulsante destro del mouse su un host e selezionare Actions > NetApp VSC > Set Recommended Values (azioni > NetApp VSC > Imposta valori
  c. Nella finestra di dialogo NetApp Recommended Settings (Impostazioni consigliate NetApp), selezionare i valori più adatti al sistema.

     I valori standard consigliati sono impostati per impostazione predefinita.



a. Fare clic su OK.

"Pagina successiva: Configurazione NetApp."

Configurazione di NetApp

Lo storage NetApp implementato per gli ambienti software MEDITECH utilizza i controller di storage in una configurazione a coppia ad alta disponibilità. Lo storage deve essere presentato da entrambi i controller ai server di database MEDITECH tramite il protocollo FC. La configurazione presenta lo storage di entrambi i controller per bilanciare uniformemente il carico dell'applicazione durante il normale funzionamento.

Configurazione di ONTAP

Questa sezione descrive un esempio di procedure di implementazione e provisioning che utilizzano i relativi comandi ONTAP. L'enfasi è quella di mostrare come viene eseguito il provisioning dello storage per implementare il layout di storage consigliato da NetApp, che utilizza una coppia di controller ad alta disponibilità. Uno dei principali vantaggi di ONTAP è la possibilità di scalare in orizzontale senza disturbare le coppie ad alta disponibilità esistenti.

Licenze ONTAP

Dopo aver configurato i controller di storage, applicare le licenze per abilitare le funzionalità ONTAP consigliate da NetApp. Le licenze per i carichi di lavoro MEDITECH sono FC, CIFS e NetApp Snapshot, SnapRestore, FlexClone, E SnapMirror.

Per configurare le licenze, aprire Gestione di sistema NetApp ONTAP, accedere a Configurazione-licenze, quindi aggiungere le licenze appropriate.

In alternativa, eseguire il seguente comando per aggiungere le licenze utilizzando la CLI:

```
license add -license-code <code>
```

Configurazione di AutoSupport

Il tool NetApp AutoSupport invia a NetApp informazioni di supporto riepilogative tramite HTTPS. Per configurare AutoSupport, eseguire i seguenti comandi ONTAP:

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

Configurazione del Takeover assistita dall'hardware

Su ciascun nodo, abilitare il Takeover assistito dall'hardware per ridurre al minimo il tempo necessario per avviare un Takeover nell'improbabile caso di un guasto del controller. Per configurare il Takeover assistito dall'hardware, attenersi alla seguente procedura:

1. Eseguire il seguente comando ONTAP su xxx.

   Impostare l'opzione indirizzo partner sull'indirizzo IP della porta di gestione per `prod1-01`.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. Eseguire il seguente comando ONTAP per xxx:

   Impostare l'opzione indirizzo partner sull'indirizzo IP della porta di gestione per `cluster1-02`.

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. Eseguire il seguente comando ONTAP per abilitare il Takeover assistito dall'hardware su entrambi `prod1-01` e a. `prod1-02` Coppia di controller HA.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"Pagina successiva: Configurazione aggregata."

Configurazione dell'aggregato

NetApp RAID DP

NetApp consiglia la tecnologia NetApp RAID DP come tipo RAID per tutti gli aggregati di un sistema NetApp FAS o AFF, inclusi i normali aggregati di Flash Pool NetApp. La documentazione MEDITECH potrebbe specificare l'utilizzo di RAID 10, ma MEDITECH ha approvato l'utilizzo di RAID DP.

Dimensione del gruppo RAID e numero di gruppi RAID

La dimensione predefinita del gruppo RAID è 16. Queste dimensioni potrebbero essere o meno ottimali per gli aggregati degli host MEDITECH del sito specifico. Per il numero di dischi che NetApp consiglia di utilizzare in un gruppo RAID, vedere "NetApp TR-3838: Guida alla configurazione del sottosistema di storage".

La dimensione del gruppo RAID è importante per l'espansione dello storage, in quanto NetApp consiglia di aggiungere dischi a un aggregato con uno o più gruppi di dischi uguali alla dimensione del gruppo RAID. Il numero di gruppi RAID dipende dal numero di dischi dati e dalle dimensioni del gruppo RAID. Per determinare il numero di dischi dati necessari, utilizza lo strumento di dimensionamento di NetApp System Performance Modeler (SPM). Dopo aver determinato il numero di dischi dati, regolare le dimensioni del gruppo RAID per ridurre al minimo il numero di dischi di parità entro l'intervallo consigliato per le dimensioni del gruppo RAID per tipo di disco.

Per ulteriori informazioni su come utilizzare lo strumento di dimensionamento SPM per ambienti MEDITECH, vedere "NetApp TR-4190: Linee guida di dimensionamento NetApp per ambienti MEDITECH".

Considerazioni sull'espansione dello storage

Quando si espandono gli aggregati con più dischi, aggiungere i dischi in gruppi che sono uguali alle dimensioni del gruppo RAID aggregato. Seguendo questo approccio è possibile garantire la coerenza delle performance nell'intero aggregato.

Ad esempio, per aggiungere storage a un aggregato creato con una dimensione del gruppo RAID pari a 20, il numero di dischi che NetApp consiglia di aggiungere è uno o più gruppi da 20 dischi. Quindi, è necessario aggiungere 20, 40, 60 e così via, dischi.

Dopo aver espanso gli aggregati, è possibile migliorare le performance eseguendo attività di riallocazione sui volumi interessati o aggregando per distribuire le strisce di dati esistenti sui nuovi dischi. Questa azione è utile soprattutto se l'aggregato esistente era quasi pieno.

> È necessario pianificare la riallocazione delle pianificazioni durante le ore di non produzione, poiché si tratta di un'attività che richiede un'elevata quantità di CPU e dischi.

Per ulteriori informazioni sull'utilizzo della riallocazione dopo un'espansione dell'aggregato, vedere "NetApp TR-3929: Guida alla riallocazione delle Best practice".

Copie Snapshot a livello di aggregato

Impostare la riserva di copia Snapshot NetApp a livello aggregato su zero e disattivare la pianificazione Snapshot aggregata predefinita. Eliminare eventuali copie Snapshot a livello aggregato preesistenti, se possibile.

"Pagina successiva: Configurazione della macchina virtuale per lo storage."

Configurazione della macchina virtuale per lo storage

Questa sezione riguarda la distribuzione su ONTAP 8.3 e versioni successive.

> Una macchina virtuale per lo storage (SVM) è nota anche come Vserver nell'API ONTAP e nell'interfaccia utente di ONTAP.

SVM per LUN host MEDITECH

È necessario creare una SVM dedicata per ogni cluster di storage ONTAP per possedere e gestire gli aggregati che contengono le LUN per gli host MEDITECH.

Impostazione di codifica della lingua SVM

NetApp consiglia di impostare la codifica della lingua per tutte le SVM. Se non viene specificata alcuna impostazione di codifica della lingua al momento della creazione di SVM, viene utilizzata l'impostazione predefinita di codifica della lingua. L'impostazione predefinita per la codifica della lingua è C.UTF-8 per ONTAP. Una volta impostata la codifica della lingua, non è possibile modificare la lingua di una SVM con Infinite Volume in un secondo momento.

I volumi associati a SVM ereditano l'impostazione di codifica del linguaggio SVM, a meno che non si specifichi esplicitamente un'altra impostazione al momento della creazione dei volumi. Per consentire il funzionamento di determinate operazioni, è necessario utilizzare l'impostazione di codifica della lingua in modo coerente in tutti i volumi del sito. Ad esempio, SnapMirror richiede che la SVM di origine e di destinazione abbia la stessa impostazione di codifica della lingua.

"Pagina successiva: Configurazione del volume."

Configurazione del volume

Provisioning di volumi

I volumi MEDITECH dedicati agli host MEDITECH possono essere thick o thin provisioning.

Copie Snapshot predefinite a livello di volume

Le copie Snapshot vengono create come parte del flusso di lavoro di backup. Ogni copia Snapshot può essere utilizzata per accedere ai dati memorizzati nelle LUN MEDITECH in momenti diversi. La soluzione di backup approvata da MEDITECH crea volumi FlexClone con thin provisioning basati su queste copie Snapshot per fornire copie point-in-time delle LUN MEDITECH. L'ambiente MEDITECH è integrato con una soluzione software di backup approvata. Pertanto, NetApp consiglia di disattivare la pianificazione predefinita delle copie Snapshot su ciascuno dei volumi NetApp FlexVol che costituiscono le LUN del database di produzione MEDITECH.

Importante: i volumi FlexClone condividono lo spazio del volume dei dati padre, pertanto è fondamentale che il volume disponga di spazio sufficiente per le LUN dei dati MEDITECH e per i volumi FlexClone creati dai server di backup. I volumi FlexClone non occupano più spazio come i volumi di dati. Tuttavia, se le LUN MEDITECH vengono eliminate in tempi brevi, i volumi dei cloni potrebbero crescere.

Numero di volumi per aggregato

Per un sistema NetApp FAS che utilizza il caching con Flash Pool o Flash cache, NetApp consiglia di fornire tre o più volumi per aggregato dedicati alla memorizzazione del programma, del dizionario e dei file di dati MEDITECH.

Per i sistemi AFF, NetApp consiglia di dedicare quattro o più volumi per aggregato per memorizzare il programma MEDITECH, il dizionario e i file di dati.

Pianificazione di riallocazione a livello di volume

Il layout dei dati dello storage diventa meno ottimale nel tempo, soprattutto quando viene utilizzato da carichi di lavoro con un elevato utilizzo di scrittura, come le piattaforme MEDITECH expse, 6.x e C/S 5.x. Con il passare

del tempo, questa situazione potrebbe aumentare la latenza di lettura sequenziale, con conseguente maggiore tempo per completare il backup. Anche un layout o una frammentazione dei dati errati possono influire sulla latenza di scrittura. È possibile utilizzare la riallocazione a livello di volume per ottimizzare il layout dei dati su disco per migliorare le latenze di scrittura e l'accesso in lettura sequenziale. Il layout dello storage migliorato consente di completare il backup entro un intervallo di tempo di 8 ore.

Best practice
Come minimo, NetApp consiglia di implementare una pianificazione settimanale di riallocazione dei volumi per eseguire operazioni di riallocazione durante il downtime di manutenzione allocato o durante le ore fuori orario di punta in un sito di produzione. NetApp consiglia vivamente di eseguire l'attività di riallocazione su un volume alla volta per controller.

Per ulteriori informazioni sulla determinazione di una pianificazione di riallocazione dei volumi appropriata per lo storage del database di produzione, vedere la sezione 3.12 in "NetApp TR-3929: Guida alla riallocazione delle Best practice". Questa sezione illustra inoltre come creare una pianificazione settimanale di riallocazione per un sito occupato.

"Pagina successiva: Configurazione del LUN."

Configurazione del LUN

Il numero di host MEDITECH nell'ambiente determina il numero di LUN creati all'interno del sistema NetApp FAS o AFF. La proposta di configurazione hardware specifica le dimensioni di ogni LUN.

Provisioning del LUN

LE LUN MEDITECH dedicate agli host MEDITECH possono essere thick o thin provisioning.

Tipo di sistema operativo LUN

Per allineare correttamente i LUN creati, è necessario impostare correttamente il tipo di sistema operativo per i LUN. Le LUN disallineate comportano un overhead non necessario delle operazioni di scrittura ed è costoso correggere una LUN disallineata.

Il server host MEDITECH in genere viene eseguito nell'ambiente Windows Server virtualizzato utilizzando l'hypervisor VMware vSphere. Il server host può essere eseguito anche in ambiente Windows Server su un server bare-metal. Per determinare il valore corretto del tipo di sistema operativo da impostare, fare riferimento alla sezione "creazione LUN" di "Comandi di Clustered Data ONTAP 8.3: Guida di riferimento alla pagina".

Dimensione del LUN

Per determinare le dimensioni del LUN per ciascun host MEDITECH, consultare il documento proposta di configurazione hardware (nuova implementazione) o attività di valutazione hardware (implementazione esistente) di MEDITECH.

Presentazione del LUN

MEDITECH richiede che lo storage per programmi, dizionari e file di dati venga presentato agli host MEDITECH come LUN utilizzando il protocollo FC. Nell'ambiente virtuale VMware, i LUN vengono presentati ai

server VMware ESXi che ospitano gli host MEDITECH. Quindi, ciascun LUN presentato al server VMware ESXi viene mappato a ciascuna VM host MEDITECH utilizzando RDM in modalità di compatibilità fisica.

È necessario presentare i LUN agli host MEDITCH utilizzando le convenzioni di denominazione LUN appropriate. Ad esempio, per semplificare l'amministrazione, è necessario presentare il LUN `MTFS01E` All'host MEDITECH `mt-host-01`.

Consultare la proposta di configurazione hardware MEDITECH quando si consulta il programma di installazione del sistema di backup e MEDITECH per definire una convenzione di denominazione coerente per le LUN utilizzate dagli host MEDITECH.

Un esempio di nome LUN MEDITECH è `MTFS05E`, in cui:

- `MTFS` Indica il file server MEDITECH (per l'host MEDITECH).
- `05` indica il numero host 5.
- `E` Indica il disco di Windows E.

"Pagina successiva: Configurazione del gruppo di iniziatori."

Configurazione del gruppo iniziatore

Quando si utilizza FC come protocollo di rete dati, creare due gruppi di iniziatori (igroups) su ciascun controller di storage. Il primo igroup contiene le WWPN delle schede di interfaccia host FC sui server VMware ESXi che ospitano le macchine virtuali host MEDITECH (igroup per MEDITECH).

È necessario impostare il tipo di sistema operativo MEDITECH igroup in base alla configurazione dell'ambiente. Ad esempio:

- Utilizzare il tipo di sistema operativo igroup `Windows` Per le applicazioni installate su hardware server bare-metal in un ambiente Windows Server.
- Utilizzare il tipo di sistema operativo igroup `VMware` Per le applicazioni virtualizzate mediante l'hypervisor VMware vSphere.

> Il tipo di sistema operativo per un igroup potrebbe essere diverso dal tipo di sistema operativo per un LUN. Ad esempio, per gli host MEDITECH virtualizzati, è necessario impostare il tipo di sistema operativo igroup su `VMware`. Per le LUN utilizzate dagli host MEDITECH virtualizzati, impostare il tipo di sistema operativo su `Windows 2008 or later`. Utilizzare questa impostazione perché il sistema operativo host MEDITECH è Windows Server 2008 R2 64-bit Enterprise Edition.

Per determinare il valore corretto per il tipo di sistema operativo, vedere le sezioni "LUN iGroup Create" e "LUN Create" nel "Comandi di Clustered Data ONTAP 8.2: Guida di riferimento alla pagina".

"Successivo: Mappature LUN."

Mappature LUN

Le mappature LUN per gli host MEDITECH vengono stabilite al momento della creazione dei LUN.

Moduli E componenti MEDITECH

L'applicazione MEDITECH copre diversi moduli e componenti. La seguente tabella elenca le funzioni trattate da questi moduli. Per ulteriori informazioni sulla configurazione e l'implementazione di questi moduli, consultare la documentazione MEDITECH.

Funzione	Tipo
Connettività	• Server Web • Server applicativo live (WI – integrazione Web) • Test del server applicazioni (WI) • Server di autenticazione SAML (WI) • Server proxy SAML (WI) • Server di database
Infrastruttura	• File server • Client processi in background • Server di connessione • Server delle transazioni
Scansione e archiviazione	• Server di immagini
Repository di dati	• SQL Server
Analytics aziendali e clinici	• Server di live intelligence (BCA) • Server di intelligence di test (BCA) • Server di database (BCA)
Assistenza a casa	• Soluzione per siti remoti • Connettività • Infrastruttura • Stampa in corso • Dispositivi di campo • Scansione • Requisiti del sito in hosting • Configurazione del firewall
Supporto	• Client processi in background (CAL - licenza di accesso client)
Dispositivi dell'utente	• Tablet • Dispositivi fissi

Funzione	Tipo
Stampa in corso	• Server di stampa di rete attivo (obbligatorio; potrebbe già esistere) • Test del server di stampa di rete (obbligatorio; potrebbe già esistere)
Requisito di terze parti	• Primo database (FDB) MedKnowledge Framework v4.3

Ringraziamenti

Le seguenti persone hanno contribuito alla creazione di questa guida.

- Brandon Agee, Technical Marketing Engineer, NetApp
- Atul Balodia, Technical Marketing Engineer, NetApp
- Ketan Mota, Senior Product Manager, NetApp
- John Duignan, Solutions Architect - Healthcare, NetApp
- Jon Ebmeier, Cisco
- Mike Brennan, Cisco

Dove trovare ulteriori informazioni

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

Area di progettazione FlexPod

- "Area di progettazione FlexPod"
- "Data center FlexPod con storage FC (switch MDS) con NetApp AFF, vSphere 6.5U1 e Cisco UCS Manager"

Report tecnici NetApp

- "TR-3929: Guida alla riallocazione delle Best practice"
- "TR-3987: Plug-in di Snap Creator Framework per InterSystems Caché"
- "TR-4300i: Guida alle Best practice per i sistemi di storage NetApp FAS e all-flash per gli ambienti MEDITECH"
- "TR-4017: Best practice SAN FC"
- "TR-3446: Guida alle Best practice e alla panoramica di SnapMirror Async"

Documentazione ONTAP

- "Documentazione sui prodotti NetApp"
- "Virtual Storage Console (VSC) per la documentazione vSphere"

- "Centro documentazione di ONTAP 9":
  - "FC Express Guide per ESXi"
- "Tutta la documentazione di ONTAP 9.3":
  - "Guida all'installazione del software"
  - "Guida all'alimentazione di dischi e aggregati"
  - "GUIDA all'amministrazione SAN"
  - "Guida ALLA configurazione SAN"
  - "Guida alla configurazione FC per Windows Express"
  - "Guida all'installazione di FC SAN Optimized AFF"
  - "Guida alla configurazione ad alta disponibilità"
  - "Guida alla gestione dello storage logico"
  - "Guida al risparmio di energia per la gestione delle performance"
  - "Guida all'alimentazione per la configurazione SMB/CIFS"
  - "Riferimento SMB/CIFS"
  - "Guida all'alimentazione per la protezione dei dati"
  - "Guida al backup e ripristino su nastro Data Protection"
  - "NetApp Encryption Power Guide"
  - "Guida alla gestione di rete"
  - "Comandi: Guida di riferimento pagina manuale per ONTAP 9.3"

Guide di Cisco Nexus, MDS, Cisco UCS e Cisco UCS Manager

- "Panoramica dei server Cisco UCS"
- "Panoramica sui server blade Cisco UCS"
- "Scheda informativa su Cisco UCS B200 M5"
- "Panoramica di Cisco UCS Manager"
- "Bundle infrastruttura Cisco UCS Manager 3.2(3a)" (Richiede l'autorizzazione Cisco.com/7)
- "Switch per piattaforma Cisco Nexus 9300"
- "Switch Cisco MDS 9132T FC"

FlexPod per imaging medicale

TR-4865: FlexPod per l'imaging medicale

Jaya Kishore Esanakula e Atul Balodia, NetApp

L'imaging medicale rappresenta il 70% di tutti i dati generati dalle organizzazioni del settore sanitario. Man mano che le modalità digitali continuano a progredire e emergono nuove modalità, la quantità di dati continuerà ad aumentare. Ad esempio, la transizione dalla patologia analogica a quella digitale aumenterà drasticamente le dimensioni delle immagini a un ritmo che metterà a confronto qualsiasi strategia di gestione dei dati

attualmente in atto.

Secondo un recente, COVID-19 ha chiaramente ridefinito la trasformazione digitale "report", COVID-19 ha accelerato il commercio digitale di 5 anni. L'innovazione tecnologica guidata dai risolutori dei problemi sta cambiando radicalmente il nostro modo di procedere nella vita quotidiana. Questo cambiamento basato sulla tecnologia rivoluzionerà molti aspetti critici della nostra vita, tra cui l'assistenza sanitaria.

L'assistenza sanitaria è destinata a subire un cambiamento importante nei prossimi anni. COVID sta accelerando l'innovazione nel settore sanitario che spingerà il settore di almeno diversi anni. Il fulcro di questo cambiamento è la necessità di rendere l'assistenza sanitaria più flessibile nella gestione delle pandemie, essendo più accessibile, disponibile e accessibile, senza compromettere l'affidabilità.

Alla base di questo cambiamento nel settore sanitario c'è una piattaforma ben progettata. Una delle metriche chiave per misurare la piattaforma è la facilità con cui è possibile implementare le modifiche alla piattaforma. La velocità è la nuova scala e la protezione dei dati non può essere compromessa. Alcuni dei dati più critici al mondo vengono creati e utilizzati dai sistemi clinici che supportano i medici. NetApp ha reso disponibili i dati critici per l'assistenza ai pazienti dove i medici ne hanno bisogno, on-premise, nel cloud o in un ambiente ibrido. Gli ambienti multi-cloud ibridi sono l'attuale stato dell'arte per l'architettura IT.

Il settore sanitario, come sappiamo, si concentra su fornitori (medici, infermieri, radiologi, tecnici dei dispositivi medici e così via) e pazienti. Avvicinando pazienti e fornitori, rendendo la posizione geografica un semplice punto dati, diventa ancora più importante che la piattaforma sottostante sia disponibile quando i fornitori e i pazienti ne hanno bisogno. La piattaforma deve essere efficiente e conveniente nel lungo termine. Nel loro impegno per ridurre ulteriormente i costi di assistenza ai pazienti, "Organizzazioni responsabili dell'assistenza" (Acos) sarebbe potenziata da una piattaforma efficiente.

Quando si tratta di sistemi di informazione sanitaria utilizzati dalle organizzazioni sanitarie, la questione della costruzione rispetto all'acquisto tende ad avere una sola risposta: L'acquisto. Questo potrebbe essere per molti motivi soggettivi. Le decisioni di acquisto prese nel corso di molti anni possono creare sistemi informativi eterogenei. Ciascun sistema dispone di un insieme specifico di requisiti per la piattaforma su cui viene implementato. Il problema più significativo è l'ampio e diversificato insieme di protocolli di storage e livelli di performance richiesti dai sistemi informativi, che rendono la standardizzazione della piattaforma e l'efficienza operativa ottimale una sfida significativa. Le organizzazioni del settore sanitario non possono concentrarsi su problemi mission-critical perché la loro attenzione è concentrata su esigenze operative banali come l'ampio set di piattaforme che richiedono un insieme diversificato di competenze e quindi la conservazione delle PMI.

Le sfide possono essere classificate nelle seguenti categorie:

- Esigenze di storage eterogenee
- Silos di reparto
- Complessità operativa DELL'IT
- Connettività cloud
- Sicurezza informatica
- Intelligenza artificiale e deep learning

Con FlexPod, otterrai una singola piattaforma che supporta FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS e così via da una singola piattaforma. Persone, processi e tecnologia fanno parte del DNA su cui FlexPod è progettato e costruito. La QoS adattiva di FlexPod aiuta a abbattere i silos di reparto supportando più sistemi clinici mission-critical sulla stessa piattaforma FlexPod sottostante. FlexPod è certificata FedRAMP e FIPS 140-2. Inoltre, le organizzazioni sanitarie devono affrontare opportunità come l'intelligenza artificiale e il deep learning. FlexPod e NetApp risolvono queste sfide e rendono i dati disponibili dove sono necessari on-premise o in un ambiente multi-cloud ibrido in una piattaforma standardizzata. Per ulteriori informazioni e per una serie di storie di successo dei clienti, vedere "FlexPod settore sanitario".

I sistemi PACS e di informazione medica tipici dispongono del seguente set di funzionalità:

- Ricezione e registrazione
- Pianificazione
- Imaging
- Trascrizione
- Gestione
- Scambio di dati
- Archivio di immagini
- Visualizzazione delle immagini per l'acquisizione e la lettura delle immagini per i tecnici e visualizzazione delle immagini per i medici

Per quanto riguarda l'imaging, il settore sanitario sta cercando di risolvere le seguenti sfide cliniche:

- Adozione più ampia di "elaborazione del linguaggio naturale" Assistenti (NLP) di tecnici e medici per la lettura delle immagini. Il reparto di radiologia può beneficiare del riconoscimento vocale per la trascrizione dei referti. NLP può essere utilizzato per identificare e rendere anonimi i record di un paziente, in particolare i tag DICOM integrati nell'immagine DICOM. Le funzionalità NLP richiedono piattaforme dalle performance elevate con tempi di risposta a bassa latenza per l'elaborazione delle immagini. La qualità del servizio FlexPod non solo offre performance e offre anche proiezioni di capacità mature per la crescita futura.
- Adozione più ampia di percorsi clinici e protocolli standardizzati da parte di Acos e delle organizzazioni sanitarie della comunità. Storicamente, i percorsi clinici sono stati utilizzati come set statico di linee guida piuttosto che come workflow integrato che guida le decisioni cliniche. Con i miglioramenti nell'elaborazione di immagini e NLP, i tag DICOM nelle immagini possono essere integrati nei percorsi clinici come fatti per guidare le decisioni cliniche. Pertanto, questi processi richiedono performance elevate, bassa latenza e throughput elevato dalla piattaforma dell'infrastruttura sottostante e dai sistemi storage.
- I modelli ML che sfruttano le reti neurali convoluzionali consentono l'automazione delle funzionalità di elaborazione delle immagini in tempo reale e richiedono pertanto un'infrastruttura che sia compatibile con GPU. FlexPod offre componenti di calcolo CPU e GPU integrati nello stesso sistema e CPU e GPU possono essere scalate indipendentemente l'una dall'altra.
- Se i tag DICOM vengono utilizzati come fatti negli avvisi delle Best practice cliniche, il sistema deve eseguire più letture di artefatti DICOM con bassa latenza e throughput elevato.
- Quando si valutano le immagini, la collaborazione in tempo reale tra radiologi di diverse organizzazioni richiede un'elaborazione grafica dalle performance elevate nei dispositivi di calcolo dell'utente finale. NetApp offre soluzioni VDI leader del settore progettate e collaudate appositamente per i casi di utilizzo della grafica high-end. Ulteriori informazioni sono disponibili "qui".
- La gestione di immagini e supporti nelle organizzazioni sanitarie ACO può utilizzare una singola piattaforma, indipendentemente dal sistema di registrazione dell'immagine, utilizzando protocolli come Digital Imaging and Communications in Medicine ("DICOM") E accesso web agli oggetti persistenti DICOM ("WADO")
- Scambio di informazioni sanitarie ("HIE") include immagini incorporate nei messaggi.
- Le modalità mobili, ad esempio dispositivi portatili e wireless di scansione (ad esempio, scanner a ultrasuoni tascabili collegati a un telefono), richiedono una solida infrastruttura di rete con sicurezza, affidabilità e latenza a livello DoD all'edge, al core e nel cloud. "Un data fabric abilitato da NetApp" fornire alle organizzazioni questa funzionalità su larga scala.
- Le modalità più recenti hanno esigenze di storage esponenziali; ad esempio, CT e MRI richiedono alcune centinaia di MB per ciascuna modalità, ma le immagini di patologia digitale (inclusa l'imaging a vetrino

intero) possono avere dimensioni di pochi GB. FlexPod è progettato con "performance, affidabilità e scalabilità come caratteristiche fondamentali".

Una piattaforma di sistemi di imaging medicale ben architettata è al centro dell'innovazione. L'architettura FlexPod offre funzionalità di calcolo e storage flessibili con efficienza dello storage leader del settore.

Vantaggi generali della soluzione

Eseguendo un ambiente applicativo di imaging su una base architetturale FlexPod, la tua organizzazione sanitaria può aspettarsi un miglioramento della produttività del personale e una riduzione delle spese di capitale e operative. FlexPod offre un prodotto rigorosamente testato, prevalidato e convergente, progettato e progettato per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio offre elevati livelli di comfort e, in ultima analisi, tempi di risposta ottimali per gli utenti del sistema di imaging medicale.

Diversi componenti del sistema di imaging potrebbero richiedere lo storage dei dati nei file system SMB/CIFS, NFS, Ext4 o NTFS. Questo requisito significa che l'infrastruttura deve fornire l'accesso ai dati sui protocolli NFS, SMB/CIFS e SAN. Un singolo sistema storage NetApp può supportare i protocolli NFS, SMB/CIFS e SAN, eliminando così la necessità di una pratica legacy di sistemi storage specifici del protocollo.

L'infrastruttura FlexPod è una piattaforma modulare, convergente, virtualizzata, scalabile (scale-out e scale-up) e conveniente. Con la piattaforma FlexPod, puoi scalare in modo indipendente calcolo, rete e storage per accelerare l'implementazione delle applicazioni. Inoltre, l'architettura modulare consente operazioni senza interruzioni anche durante le attività di scale-out e upgrade del sistema.

FlexPod offre diversi vantaggi specifici per il settore dell'imaging medicale:

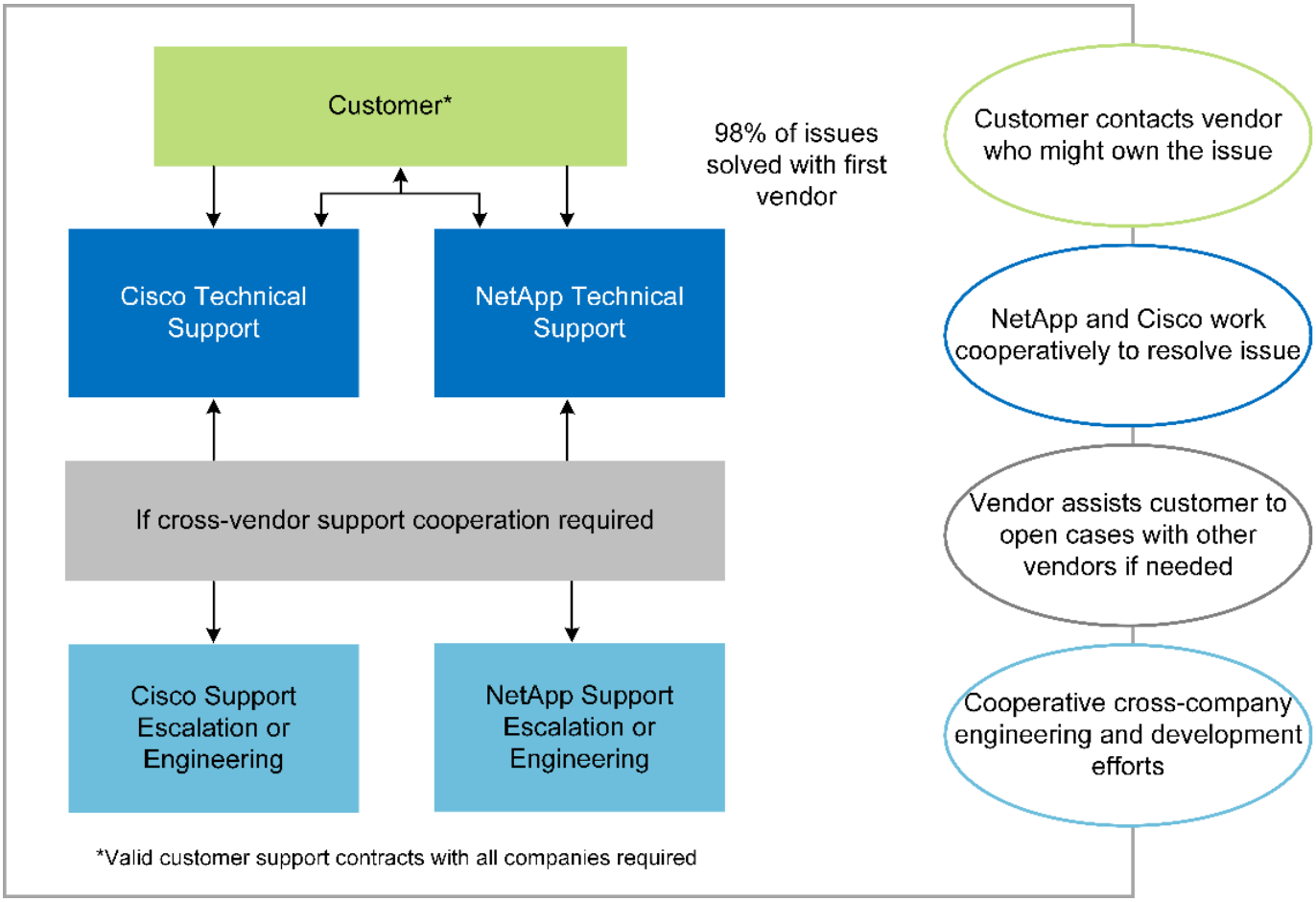
- **Prestazioni del sistema a bassa latenza.** il tempo dei radiologi è una risorsa di alto valore e l'utilizzo efficiente del tempo di un radiologo è fondamentale. L'attesa del caricamento di immagini o video può contribuire al burnout del medico e compromettere l'efficienza e la sicurezza del paziente.
- **Architettura modulare.** i componenti FlexPod sono collegati tramite un server in cluster, un fabric di gestione dello storage e un set di strumenti di gestione coesivi. Man mano che le strutture di imaging crescono anno dopo anno e il numero di studi aumenta, sarà necessario che l'infrastruttura sottostante sia scalabile di conseguenza. FlexPod è in grado di scalare calcolo, storage e rete in modo indipendente.
- **Implementazione più rapida dell'infrastruttura.** sia che si trovi in un data center esistente o in una postazione remota, il design integrato e testato di FlexPod Datacenter con imaging medicale ti consente di attivare e utilizzare la nuova infrastruttura in meno tempo, con meno sforzo.
- **Implementazione accelerata delle applicazioni.** Un'architettura prevalidata riduce i tempi di integrazione dell'implementazione e i rischi per qualsiasi carico di lavoro, mentre la tecnologia NetApp automatizza l'implementazione dell'infrastruttura. Sia che si utilizzi la soluzione per un'implementazione iniziale dell'imaging medicale, un aggiornamento dell'hardware o un'espansione, è possibile trasferire più risorse al valore di business del progetto.
- **Operazioni semplificate e costi inferiori.** è possibile eliminare i costi e la complessità delle piattaforme proprietarie legacy sostituendole con una risorsa condivisa più efficiente e scalabile in grado di soddisfare le esigenze dinamiche del carico di lavoro. Questa soluzione offre un maggiore utilizzo delle risorse dell'infrastruttura per un maggiore ritorno sull'investimento (ROI).
- **Architettura scale-out.** è possibile scalare SAN e NAS da terabyte a decine di petabyte senza riconfigurare le applicazioni in esecuzione.
- **Operazioni senza interruzioni.** è possibile eseguire manutenzione dello storage, operazioni del ciclo di vita dell'hardware e aggiornamenti software senza interrompere il business.
- **Multitenancy sicura.** questo vantaggio supporta le maggiori esigenze di infrastruttura condivisa storage e server virtualizzati, consentendo la multi-tenancy sicura di informazioni specifiche della struttura, in

particolare se si ospitano più istanze di database e software.

- **Ottimizzazione delle risorse in pool.** questo vantaggio consente di ridurre il numero di server fisici e controller di storage, bilanciare il carico di lavoro e aumentare l'utilizzo migliorando le performance.
- **Qualità del servizio (QoS).** FlexPod offre QoS sull'intero stack. Queste policy di storage QoS leader del settore consentono livelli di servizio differenziati in un ambiente condiviso. Queste policy aiutano a ottimizzare le performance per i carichi di lavoro e aiutano a isolare e controllare le applicazioni senza controllo.
- **Supporto per SLA di livello storage mediante QoS.** non è necessario implementare sistemi storage diversi per i diversi livelli di storage richiesti generalmente da un ambiente di imaging medicale. Un singolo cluster di storage con più volumi NetApp FlexVol con policy QoS specifiche per diversi livelli può servire a tale scopo. Con questo approccio, l'infrastruttura storage può essere condivisa adattando dinamicamente le mutevoli esigenze di un particolare Tier di storage. NetApp AFF può supportare diversi SLA per i Tier di storage consentendo la QoS a livello del volume FlexVol, eliminando così la necessità di sistemi storage diversi per diversi Tier di storage per l'applicazione.
- **Efficienza dello storage.** le immagini mediche sono in genere pre-compresse dall'applicazione di imaging per una compressione senza perdita di dati jpeg2k che è di circa 2.5:1. Tuttavia, si tratta di un'applicazione di imaging e specifica del vendor. In ambienti applicativi di imaging più grandi (oltre 1 PB), sono possibili risparmi del 5-10% sullo storage e puoi ridurre i costi dello storage con le funzionalità di efficienza dello storage NetApp. Collaborate con i vostri fornitori di applicazioni di imaging e con il vostro esperto NetApp per sbloccare potenziali efficienze dello storage per il vostro sistema di imaging medicale.
- **Agilità.** grazie ai tool di automazione, orchestrazione e gestione del workflow leader del settore offerti dai sistemi FlexPod, il tuo team IT può essere molto più reattivo alle richieste di business. Queste richieste di business possono spaziare dal backup dell'imaging medico al provisioning di ambienti di test e formazione aggiuntivi alle repliche dei database di analisi per iniziative di gestione dello stato di salute della popolazione.
- **Maggiore produttività.** è possibile implementare e scalare rapidamente questa soluzione per un'esperienza ottimale dell'utente finale del medico.
- **Data Fabric.** il data fabric basato su NetApp consente di unire i dati tra siti, oltre i confini fisici e tra applicazioni diverse. Il tuo data fabric basato su NetApp è costruito per le aziende basate sui dati in un mondo incentrato sui dati. I dati vengono creati e utilizzati in più sedi e spesso devono essere sfruttati e condivisi con altre sedi, applicazioni e infrastrutture. Quindi, ti serve un modo coerente e integrato per gestirlo. Questa soluzione consente di gestire i dati in modo da tenere sotto controllo il team IT e semplificare l'aumento della complessità DELL'IT.
- **FabricPool.** NetApp ONTAP FabricPool aiuta a ridurre i costi dello storage senza compromettere performance, efficienza, sicurezza o protezione. FabricPool è trasparente per le applicazioni aziendali e sfrutta l'efficienza del cloud riducendo il TCO dello storage senza la necessità di riprogettare l'infrastruttura applicativa. FlexPod può trarre vantaggio dalle funzionalità di tiering dello storage di FabricPool per un utilizzo più efficiente dello storage flash ONTAP. Per informazioni complete, vedere "FlexPod con FabricPool".
- **Sicurezza FlexPod.** la sicurezza è alla base di FlexPod. Negli ultimi anni, il ransomware è diventato una minaccia significativa e crescente. Ransomware è un malware basato sulla virologia crittografica, l'utilizzo della crittografia per la creazione di software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati. Per scoprire come FlexPod aiuta a mitigare minacce come ransomware, consulta "La soluzione per il ransomware". I componenti dell'infrastruttura FlexPod sono anche standard federali per l'elaborazione delle informazioni "(FIPS) 140-2" conforme.
- **Supporto congiunto di FlexPod.** NetApp e Cisco hanno definito il supporto congiunto di FlexPod, un modello di supporto forte, scalabile e flessibile per soddisfare i requisiti di supporto esclusivi dell'infrastruttura convergente di FlexPod. Questo modello utilizza l'esperienza, le risorse e l'esperienza di supporto tecnico di NetApp e Cisco per fornire un processo semplificato per identificare e risolvere il

problema di supporto FlexPod, indipendentemente dalla posizione del problema. Il modello di supporto cooperativo FlexPod ti aiuta a confermare che il tuo sistema FlexPod funziona in modo efficiente e sfrutta la tecnologia più aggiornata, fornendo al contempo un team esperto per risolvere i problemi di integrazione.

Il supporto congiunto di FlexPod è particolarmente utile se la tua organizzazione sanitaria esegue applicazioni business-critical. L'illustrazione riportata di seguito mostra una panoramica del modello di supporto cooperativo FlexPod.



Scopo

Questo documento fornisce una panoramica tecnica di un'infrastruttura FlexPod basata su Cisco UCS e NetApp ONTAP per l'hosting di questa soluzione di imaging medicale.

Pubblico

Il presente documento è destinato ai responsabili tecnici del settore sanitario, ai tecnici delle soluzioni partner Cisco e NetApp e al personale dei servizi professionali. NetApp presuppone che il lettore abbia una buona comprensione dei concetti di dimensionamento di calcolo e storage, nonché una buona familiarità tecnica con il sistema di imaging medicale, Cisco UCS e i sistemi storage NetApp.

Applicazione di imaging medicale

Una tipica applicazione di imaging medicale offre una suite di applicazioni che insieme costituiscono una soluzione di imaging di livello Enterprise per le piccole, medie e grandi organizzazioni sanitarie.

Il cuore della suite di prodotti è costituito dalle seguenti funzionalità cliniche:

- Repository di imaging aziendale
- Supporta le sorgenti di immagini tradizionali, ad esempio radiologia e cardiologia. Supporta anche altre aree di cura come oftalmologia, dermatologia, colonscopia e altri oggetti di imaging medico come foto e video.
- "Sistema di archiviazione e comunicazione delle immagini" (PACS), che è un mezzo computerizzato per sostituire i ruoli delle pellicole radiologiche convenzionali
- Enterprise Imaging Vendor Neutral Archive (VNA):
  - Consolidamento scalabile di documenti DICOM e non DICOM
  - Sistema di imaging medicale centralizzato
  - Supporto per la sincronizzazione dei documenti e l'integrità dei dati tra più (PACS) nell'azienda
  - Gestione del ciclo di vita dei documenti mediante un sistema esperto basato su regole che sfrutta i metadati dei documenti, come:
  - Tipo di modalità
  - Età dello studio
  - Età del paziente (corrente e al momento dell'acquisizione dell'immagine)
  - Singolo punto di integrazione all'interno e all'esterno dell'azienda (HIE):
  - Collegamento di documenti consapevole del contesto
  - Health Level Seven International (HL7), DICOM e WADO
  - Funzionalità di archiviazione indipendente dallo storage
- Integrazione con altri sistemi di informazione sanitaria che utilizzano HL7 e il collegamento contestuale:
  - Consente agli EHR di implementare collegamenti diretti alle immagini dei pazienti da cartelle dei pazienti, flussi di lavoro di imaging e così via.
  - Consente di incorporare la cronologia delle immagini di cura longitudinale di un paziente negli EHR.
- Flussi di lavoro dei tecnici di radiologia
- Visualizzatori Enterprise a impatto zero per la visualizzazione delle immagini da qualsiasi luogo su qualsiasi dispositivo compatibile
- Strumenti analitici che sfruttano i dati retrospettivi e in tempo reale:
  - Reporting sulla conformità
  - Report operativi
  - Rapporti sul controllo di qualità e sul controllo di qualità

Dimensioni dell'organizzazione sanitaria e dimensionamento della piattaforma

Le organizzazioni del settore sanitario possono essere classificate in maniera ampia utilizzando metodi basati su standard che aiutano programmi come ACO. Una di queste classificazioni utilizza il concetto di una rete integrata clinica (CIN). Un gruppo di ospedali può essere chiamato CIN se collaborano e rispettano protocolli clinici standard e percorsi comprovati per migliorare il valore dell'assistenza e ridurre i costi dei pazienti. Gli ospedali all'interno di una rete CIN dispongono di controlli e pratiche per i medici di bordo che seguono i valori fondamentali della rete CIN. Tradizionalmente, una rete di erogazione integrata (IDN) è stata limitata a ospedali e gruppi di medici. Un CIN attraversa i tradizionali confini dell'IDN e un CIN può ancora far parte di un ACO. Seguendo i principi di una CIN, le organizzazioni sanitarie possono essere classificate in piccole, medie e grandi.

Piccole organizzazioni sanitarie

Un’organizzazione sanitaria è di piccole dimensioni se include un solo ospedale con ambulatori e un reparto degente, ma non fa parte di un CIN. I medici lavorano come operatori sanitari e coordinano l’assistenza ai pazienti durante un percorso di cura. Queste piccole organizzazioni includono generalmente strutture gestite da medici. Potrebbero offrire o meno cure di emergenza e traumi come assistenza integrata per il paziente. In genere, un’organizzazione sanitaria di piccole dimensioni esegue circa 250,000 studi di imaging clinico all’anno. I centri di imaging sono considerati piccole organizzazioni sanitarie e offrono servizi di imaging. Alcuni forniscono anche servizi di dettatura radiologica ad altre organizzazioni.

Organizzazioni sanitarie di medie dimensioni

Un’organizzazione sanitaria considerata di medie dimensioni se include più sistemi ospedalieri con organizzazioni mirate, come ad esempio:

- Cliniche di cura per adulti e ospedali ricoverati per adulti
- Reparti di manodopera e consegna
- Cliniche di puericultura e ospedali ricoverati
- Un centro di trattamento del cancro
- Reparti di emergenza per adulti
- Reparti di emergenza minorenni
- Un ufficio di medicina di famiglia e di assistenza primaria
- Un centro per la cura dei traumi per adulti
- Un centro per la cura dei traumi per bambini

In un’organizzazione sanitaria di medie dimensioni, i medici seguono i principi di una CIN e operano come una singola unità. Gli ospedali dispongono di funzioni distinte di fatturazione per ospedali, medici e farmacie. Gli ospedali potrebbero essere associati a istituti di ricerca accademici ed eseguire ricerche cliniche e sperimentazioni interventistiche. Un’organizzazione sanitaria di medie dimensioni esegue fino a 500,000 studi di imaging clinico all’anno.

Grandi organizzazioni sanitarie

Un’organizzazione sanitaria è considerata di grandi dimensioni se include le caratteristiche di un’organizzazione sanitaria di medie dimensioni e offre le capacità cliniche di medie dimensioni alla comunità in diverse aree geografiche.

Un’organizzazione sanitaria di grandi dimensioni svolge in genere le seguenti funzioni:

- Dispone di una sede centrale per gestire le funzioni generali
- Partecipa a joint venture con altri ospedali
- Negozia i tassi con le organizzazioni paganti ogni anno
- Negozia le tariffe dei paganti per stato e regione
- Partecipa a programmi di utilizzo significativo (MU)
- Esegue ricerche cliniche avanzate in tutte le coorti di salute della popolazione utilizzando strumenti di gestione dello stato di salute della popolazione (PHM) basati su standard
- Esegue fino a un milione di studi di imaging clinico all’anno

Alcune grandi organizzazioni sanitarie che partecipano a una CIN dispongono anche di funzionalità di lettura

dell'imaging basate sull'ai. In genere, queste organizzazioni eseguono da uno a due milioni di studi di imaging clinico all'anno.

Prima di esaminare il modo in cui queste organizzazioni di dimensioni diverse si traducono in un sistema FlexPod di dimensioni ottimali, è necessario comprendere i vari componenti FlexPod e le diverse funzionalità di un sistema FlexPod.

FlexPod

Cisco Unified Computing System

Cisco UCS è costituito da un singolo dominio di gestione che è interconnesso con un'infrastruttura i/o unificata. Cisco UCS per ambienti di imaging medico è stato allineato con le raccomandazioni e le Best practice dell'infrastruttura del sistema di imaging medico NetApp, in modo che l'infrastruttura possa fornire informazioni critiche sui pazienti con la massima disponibilità.

La base di calcolo dell'imaging medicale aziendale è la tecnologia Cisco UCS, con la sua gestione integrata dei sistemi, i processori Intel Xeon e la virtualizzazione dei server. Queste tecnologie integrate risolvono le sfide del data center e ti consentono di raggiungere i tuoi obiettivi per la progettazione del data center con un tipico sistema di imaging medicale. Cisco UCS unifica la gestione di LAN, SAN e sistemi in un unico collegamento semplificato per server rack, blade server e macchine virtuali (VM). Cisco UCS è costituito da una coppia ridondante di interconnessioni fabric Cisco UCS che forniscono un singolo punto di gestione e un singolo punto di controllo per tutto il traffico i/O.

Cisco UCS utilizza profili di servizio in modo che i server virtuali nell'infrastruttura Cisco UCS siano configurati correttamente e in modo coerente. I profili di servizio includono informazioni critiche sull'identità del server, come indirizzi LAN e SAN, configurazioni i/o, versioni del firmware, ordine di avvio, LAN virtuale di rete (VLAN), porta fisica e policy QoS. I profili di servizio possono essere creati in modo dinamico e associati a qualsiasi server fisico nel sistema in pochi minuti anziché in ore o giorni. L'associazione dei profili di servizio con i server fisici viene eseguita come un'unica e semplice operazione che consente la migrazione delle identità tra i server dell'ambiente senza richiedere alcuna modifica della configurazione fisica. Inoltre, facilita il provisioning bare-metal rapido delle sostituzioni per i server guasti.

L'utilizzo dei profili di servizio aiuta a confermare che i server sono configurati in modo coerente in tutta l'azienda. Quando si utilizzano più domini di gestione Cisco UCS, Cisco UCS Central può utilizzare profili di servizio globali per sincronizzare le informazioni di configurazione e policy tra i domini. Se la manutenzione deve essere eseguita in un dominio, l'infrastruttura virtuale può essere migrata in un altro dominio. Con questo approccio, anche quando un singolo dominio è offline, le applicazioni continuano a funzionare con alta disponibilità.

Cisco UCS è una soluzione di prossima generazione per l'elaborazione di server blade e rack. Il sistema integra un fabric di rete unificato 40 GbE a bassa latenza, senza perdita di dati con server di classe Enterprise con architettura x86. Il sistema è una piattaforma multi-chassis integrata, scalabile, in cui tutte le risorse partecipano a un dominio di gestione unificato. Cisco UCS accelera l'erogazione di nuovi servizi in modo semplice, affidabile e sicuro attraverso il provisioning end-to-end e il supporto della migrazione per sistemi virtualizzati e non virtualizzati. Cisco UCS offre le seguenti funzionalità:

- Gestione completa
- Semplificazione radicale
- Performance elevate

Cisco UCS è costituito dai seguenti componenti:

- **Compute.** il sistema si basa su una nuova classe di sistemi di calcolo che incorpora server blade e montati

su rack basati sulla famiglia di processori scalabili Intel Xeon.

- **Network.** il sistema è integrato in un fabric di rete unificato a bassa latenza, senza perdite e 40 Gbps. Questa base di rete consolida LAN, SAN e reti di calcolo ad alte performance, che oggi sono reti separate. Il fabric unificato riduce i costi riducendo il numero di schede di rete, switch e cavi e anche diminuendo i requisiti di alimentazione e raffreddamento.
- **Virtualizzazione.** il sistema libera il pieno potenziale della virtualizzazione migliorando la scalabilità, le performance e il controllo operativo degli ambienti virtuali. Le funzionalità di sicurezza, applicazione delle policy e diagnostica di Cisco sono ora estese agli ambienti virtualizzati per supportare meglio i requisiti IT e di business in continua evoluzione.
- **Accesso allo storage.** il sistema fornisce un accesso consolidato allo storage SAN e NAS tramite il fabric unificato. È anche un sistema ideale per lo storage software-defined. Combinando i vantaggi di un singolo framework per gestire i server di calcolo e storage in un singolo pannello, è possibile implementare QoS se necessario per introdurre la limitazione di i/o nel sistema. Inoltre, gli amministratori dei server possono preassegnare le policy di accesso allo storage alle risorse di storage, semplificando la connettività e la gestione dello storage e aumentando la produttività. Oltre allo storage esterno, sia i server rack che i server blade dispongono di uno storage interno a cui è possibile accedere tramite controller RAID hardware integrati. Impostando il profilo di storage e la policy di configurazione del disco in Cisco UCS Manager, le esigenze di storage del sistema operativo host e dei dati delle applicazioni vengono soddisfatte dai gruppi RAID definiti dall'utente. Il risultato è un'elevata disponibilità e migliori performance.
- **Gestione.** il sistema integra in modo univoco tutti i componenti del sistema in modo che l'intera soluzione possa essere gestita come singola entità da Cisco UCS Manager. Per gestire tutte le operazioni e la configurazione del sistema, Cisco UCS Manager dispone di una GUI intuitiva, di una CLI e di un potente modulo di libreria di scripting per Microsoft Windows PowerShell, costruito su una solida API.

Cisco Unified Computing System unisce server e reti di livello di accesso. Questo sistema server di nuova generazione dalle performance elevate offre al tuo data center un elevato grado di agilità e scalabilità dei carichi di lavoro.

Cisco UCS Manager

Cisco UCS Manager offre una gestione integrata e unificata per tutti i componenti software e hardware di Cisco UCS. Utilizzando la tecnologia a connessione singola, UCS Manager gestisce, controlla e amministra più chassis per migliaia di macchine virtuali. Attraverso una GUI intuitiva, una CLI o un'API XML, gli amministratori utilizzano il software per gestire l'intero Cisco UCS come singola entità logica. Cisco UCS Manager risiede su una coppia di fabric Interconnect Cisco UCS 6300 Series che utilizzano una configurazione di Active-standby in cluster per una disponibilità elevata.

Cisco UCS Manager offre un'interfaccia di gestione integrata unificata che integra server, rete e storage. Cisco UCS Manager esegue il rilevamento automatico per rilevare l'inventario, gestire ed eseguire il provisioning dei componenti di sistema aggiunti o modificati. Offre un set completo di API XML per l'integrazione di terze parti ed espone 9,000 punti di integrazione. Inoltre, facilita lo sviluppo personalizzato per l'automazione, l'orchestrazione e il raggiungimento di nuovi livelli di visibilità e controllo del sistema.

I profili di servizio beneficiano sia degli ambienti virtualizzati che di quelli non virtualizzati. Aumentano la mobilità dei server non virtualizzati, ad esempio quando si spostano i carichi di lavoro da un server all'altro o quando si porta un server offline per l'assistenza o l'upgrade. È inoltre possibile utilizzare i profili insieme ai cluster di virtualizzazione per portare nuove risorse online in modo semplice, integrando la mobilità delle macchine virtuali esistenti.

Per ulteriori informazioni su Cisco UCS Manager, consultare "Pagina del prodotto Cisco UCS Manager".

Elementi di differenziazione di Cisco UCS

Cisco Unified Computing System sta rivoluzionando il modo in cui i server vengono gestiti nel data center. Scopri i seguenti elementi distintivi di Cisco UCS e Cisco UCS Manager:

- **Gestione integrata.** in Cisco UCS, i server sono gestiti dal firmware incorporato nelle interconnessioni fabric, eliminando la necessità di dispositivi fisici o virtuali esterni per gestirli.
- **Unified Fabric.** in Cisco UCS, dallo chassis per server blade o server rack alle interconnessioni fabric, viene utilizzato un singolo cavo Ethernet per LAN, SAN e traffico di gestione. Questo i/o convergente riduce il numero di cavi, SFP e adattatori necessari, riducendo le spese di capitale e operative per la soluzione complessiva.
- **AutoDiscovery.** semplicemente inserendo il server blade nello chassis o collegando i server rack alle interconnessioni fabric, il rilevamento e l'inventario delle risorse di calcolo avviene automaticamente senza alcun intervento di gestione. La combinazione di Unified Fabric e rilevamento automatico consente l'architettura wire-once di Cisco UCS, in cui è possibile estendere facilmente le funzionalità di calcolo mantenendo la connettività esterna esistente a LAN, SAN e reti di gestione.
- **Classificazione delle risorse basata su policy.** quando Cisco UCS Manager rileva una risorsa di calcolo, può essere automaticamente classificata in un determinato pool di risorse in base alle policy definite dall'utente. Questa funzionalità è utile nel cloud computing multi-tenant.
- **Gestione combinata di server blade e rack.** Cisco UCS Manager può gestire server blade B-Series e server rack C-Series nello stesso dominio Cisco UCS. Questa funzionalità, insieme al computing stateless, rende le risorse di calcolo realmente indipendenti dall'hardware.
- **Architettura di gestione basata su modelli.** l'architettura e il database di gestione di Cisco UCS Manager sono basati su modelli e basati sui dati. L'API XML aperta fornita per operare sul modello di gestione consente un'integrazione semplice e scalabile di Cisco UCS Manager con altri sistemi di gestione.
- **Criteri, pool e modelli.** l'approccio di gestione di Cisco UCS Manager si basa sulla definizione di policy, pool e modelli invece di una configurazione ordinata. Consente un approccio semplice, basato sui dati e liberamente accoppiato nella gestione delle risorse di calcolo, rete e storage.
- **Integrità referenziale allentata.** in Cisco UCS Manager, un profilo di servizio, un profilo di porta o policy possono fare riferimento ad altre policy o ad altre risorse logiche con integrità referenziale allentata. Una policy di riferimento non può esistere al momento della creazione della policy di riferimento, ma una policy di riferimento può essere eliminata anche se ad essa fanno riferimento altri criteri. Questa funzione consente a diversi esperti in materia di lavorare in modo indipendente l'uno dall'altro. Ottieni una grande flessibilità consentendo a diversi esperti di diversi domini, come rete, storage, sicurezza, server e virtualizzazione, di lavorare insieme per eseguire un'attività complessa.
- **Policy resolution.** in Cisco UCS Manager, è possibile creare una struttura ad albero di gerarchia di unità organizzative che imiti i tenant reali e le relazioni organizzative. È possibile definire diversi criteri, pool e modelli a diversi livelli della gerarchia organizzativa. Una policy che fa riferimento a un'altra policy per nome viene risolta nella gerarchia organizzativa con la corrispondenza di policy più vicina. Se nella gerarchia dell'organizzazione root non viene trovato alcun criterio con un nome specifico, viene eseguita la ricerca di un criterio speciale denominato "default". Questa procedura di risoluzione dei criteri consente di utilizzare API di gestione intuitive per l'automazione e offre una grande flessibilità ai proprietari delle diverse organizzazioni.
- **Profili di servizio e stateless computing.** Un profilo di servizio è una rappresentazione logica di un server che supporta le sue varie identità e policy. È possibile assegnare questo server logico a qualsiasi risorsa di calcolo fisica, purché soddisfi i requisiti delle risorse. Il computing stateless consente di procurarsi un server in pochi minuti, che in passato richiedevano giorni nei sistemi di gestione dei server legacy.
- **Supporto multi-tenancy integrato.** la combinazione di policy, pool, modelli, integrità referenziale allentata, risoluzione delle policy nella gerarchia organizzativa e un approccio basato sui profili di servizio

alle risorse di calcolo rende Cisco UCS Manager intrinsecamente amichevole per gli ambienti multi-tenant che vengono generalmente osservati nei cloud pubblici e privati.

- **Memoria estesa.** il server blade Cisco UCS B200 M5 di livello Enterprise estende le funzionalità del portfolio Cisco Unified Computing System in un fattore di forma blade half-width. Cisco UCS B200 M5 sfrutta la potenza delle più recenti CPU con processori scalabili Intel Xeon con un massimo di 3 TB di RAM. Questa funzionalità consente l'enorme rapporto macchina virtuale-server fisico che molte implementazioni richiedono o consentono a determinate architetture di supportare grandi operazioni di memoria, come i big data.
- **Virtualization-aware network.** la tecnologia Cisco Virtual Machine Fabric Extender (VM-FEX) rende il layer di rete di accesso consapevole della virtualizzazione host. Questa consapevolezza impedisce l'inquinamento dei domini di calcolo e di rete con la virtualizzazione quando una rete virtuale viene gestita da profili di porta definiti dal team di amministratori di rete. Inoltre, VM-FEX scarica la CPU dell'hypervisor eseguendo la commutazione nell'hardware, consentendo alla CPU dell'hypervisor di eseguire più attività correlate alla virtualizzazione. Per semplificare la gestione del cloud, la tecnologia VM-FEX è perfettamente integrata con VMware vCenter, Linux kernel-based Virtual Machine (KVM) e Microsoft Hyper-V SR-IOV.
- **QoS semplificato.** anche se FC ed Ethernet sono convergenti in Cisco UCS, il supporto integrato per QoS e Ethernet senza perdita di dati lo rende perfetto. Rappresentando tutte le classi di sistema in un unico pannello GUI, la QoS di rete è semplificata in Cisco UCS Manager.

Switch Cisco Nexus IP e MDS

Gli switch Cisco Nexus e Cisco MDS Multilayer director offrono connettività di livello Enterprise e consolidamento SAN. Le reti di storage multiprotocollo Cisco aiutano a ridurre i rischi aziendali fornendo flessibilità e opzioni: FC, Fibre Connection (FICON), FC over Ethernet (FCoE), iSCSI e FC over IP (FCIP).

Gli switch Cisco Nexus offrono una delle funzionalità di rete del data center più complete in un'unica piattaforma. Offrono performance e densità elevate sia per il data center che per il core del campus. Offrono inoltre un set completo di funzionalità per l'aggregazione del data center, l'end-of-row e le implementazioni di interconnessione del data center in una piattaforma modulare altamente resiliente.

Cisco UCS integra le risorse di calcolo con gli switch Cisco Nexus e un fabric unificato che identifica e gestisce diversi tipi di traffico di rete. Questo traffico include l'i/o dello storage, il traffico desktop in streaming, la gestione e l'accesso alle applicazioni cliniche e aziendali. Sono disponibili le seguenti funzionalità:

- **Scalabilità dell'infrastruttura.** virtualizzazione, alimentazione e raffreddamento efficienti, scalabilità cloud con automazione, alta densità e performance supportano una crescita efficiente del data center.
- **Continuità operativa.** il design integra hardware, funzionalità software Cisco NX-OS e gestione per supportare ambienti senza downtime.
- **Flessibilità di trasporto.** con questa soluzione conveniente è possibile adottare in modo incrementale nuove tecnologie di rete.

Insieme, Cisco UCS con switch Cisco Nexus e MDS Multilayer director offrono una soluzione di calcolo, networking e connettività SAN per un sistema di imaging medicale aziendale.

Storage all-flash NetApp

Lo storage NetApp che esegue il software ONTAP riduce i costi di storage complessivi offrendo al contempo tempi di risposta in lettura e scrittura a bassa latenza e IOPS elevati richiesti dai carichi di lavoro del sistema di imaging medicale. Per creare un sistema di storage ottimale che soddisfi i requisiti tipici dei sistemi di imaging medicale, ONTAP supporta configurazioni di storage all-flash e ibride. Lo storage flash NetApp offre ai clienti del sistema di imaging medicale come te i componenti chiave delle performance elevate e della reattività per supportare le operazioni del sistema di imaging medicale sensibili alla latenza. Creando più domini di errore in

un singolo cluster, la tecnologia NetApp può anche isolare gli ambienti di produzione dagli ambienti non di produzione. Inoltre, garantendo che le performance del sistema non scenda al di sotto di un determinato livello per i carichi di lavoro con QoS minimo ONTAP, NetApp riduce i problemi di performance del sistema.

L'architettura scale-out del software ONTAP può adattarsi in modo flessibile ai vari carichi di lavoro i/O. Per offrire il throughput necessario e la bassa latenza di cui le applicazioni cliniche hanno bisogno e per fornire un'architettura scalabile modulare, le configurazioni all-flash sono generalmente utilizzate nelle architetture ONTAP. I nodi AFF di NetApp possono essere combinati nello stesso cluster scale-out con nodi di storage ibridi (HDD e flash), adatti per l'archiviazione di set di dati di grandi dimensioni con throughput elevato. È possibile clonare, replicare ed eseguire il backup dell'ambiente del sistema di imaging medicale, dal costoso storage SSD allo storage HDD più economico su altri nodi. Con lo storage NetApp abilitato al cloud e un data fabric fornito da NetApp, puoi eseguire il backup su storage a oggetti on-premise o nel cloud.

Per l'imaging medicale, ONTAP è stato validato dalla maggior parte dei sistemi di imaging medicale leader del settore. Ciò significa che è stato testato per offrire performance veloci e affidabili per l'imaging medicale. Inoltre, le seguenti funzionalità semplificano la gestione, aumentano la disponibilità e l'automazione e riducono la quantità totale di storage necessaria.

- **Performance eccezionali.** la soluzione NetApp AFF condivide la stessa architettura di storage unificata, il software ONTAP, l'interfaccia di gestione, i servizi dati avanzati e il set di funzionalità avanzate delle altre famiglie di prodotti NetApp FAS. Questa innovativa combinazione di supporti all-flash e ONTAP offre una latenza costantemente bassa e IOPS elevati dello storage all-flash con il software ONTAP leader del settore.
- **Efficienza dello storage.** è possibile ridurre i requisiti di capacità totale lavorare con il proprio SME NetApp per comprendere come questo ha applicato il proprio sistema di imaging medicale specifico.
- **Cloning efficiente in termini di spazio.** con la funzionalità FlexClone, il sistema può creare cloni quasi istantaneamente per supportare il refresh dell'ambiente di backup e test. Questi cloni consumano storage aggiuntivo solo quando vengono apportate modifiche.
- **Protezione integrata dei dati.** le funzionalità complete di protezione dei dati e disaster recovery ti aiutano a proteggere le tue risorse di dati critici e a fornire il disaster recovery.
- **Operazioni senza interruzioni.** è possibile eseguire aggiornamenti e manutenzione senza interrompere la trasmissione dei dati.
- **QoS.** la QoS dello storage ti aiuta a limitare i potenziali carichi di lavoro ingombrante. Cosa ancora più importante, la qualità del servizio crea una garanzia di performance minime che garantisce che le performance del sistema non scenderanno al di sotto di un determinato livello per i carichi di lavoro critici, come ad esempio l'ambiente di produzione di un sistema di imaging medicale. Inoltre, limitando i conflitti, NetApp QoS può anche ridurre i problemi legati alle performance.
- **Data Fabric.** per accelerare la trasformazione digitale, il data fabric fornito da NetApp semplifica e integra la gestione dei dati in ambienti cloud e on-premise. Offre applicazioni e servizi di gestione dei dati coerenti e integrati per una visibilità e informazioni dei dati superiori, accesso e controllo dei dati, protezione e sicurezza dei dati. NetApp è integrato con grandi cloud pubblici, come AWS, Azure, Google Cloud e IBM Cloud, un'ampia scelta.

Virtualizzazione host: VMware vSphere

Le architetture FlexPod sono validate con VMware vSphere 6.x, la piattaforma di virtualizzazione leader del settore. VMware ESXi 6.x viene utilizzato per implementare ed eseguire le macchine virtuali. VCenter Server Appliance 6.x viene utilizzato per gestire host e macchine virtuali ESXi. Per formare un cluster VMware ESXi vengono utilizzati più host ESXi eseguiti su blade Cisco UCS B200 M5. Il cluster VMware ESXi raggruppa le risorse di calcolo, memoria e rete di tutti i nodi del cluster e fornisce una piattaforma resiliente per le macchine virtuali in esecuzione sul cluster. Le funzionalità del cluster VMware ESXi, l'alta disponibilità di vSphere e il DRS (Distributed Resource Scheduler) contribuiscono alla tolleranza del cluster vSphere per resistere agli

errori e aiutano a distribuire le risorse tra gli host VMware ESXi.

Il plug-in per lo storage NetApp e il plug-in Cisco UCS si integrano con VMware vCenter per consentire flussi di lavoro operativi per le risorse di calcolo e storage richieste.

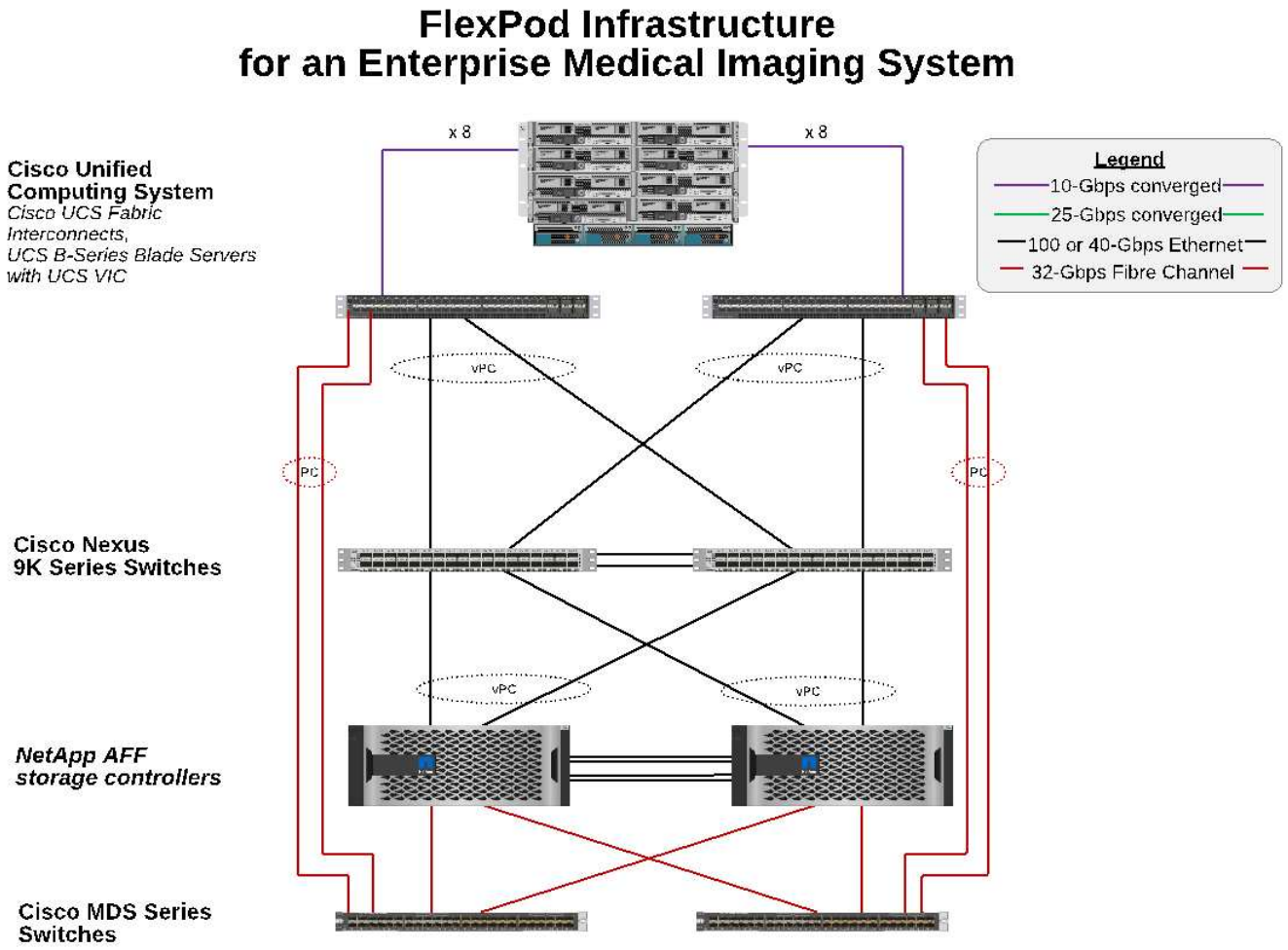
Il cluster VMware ESXi e vCenter Server offrono una piattaforma centralizzata per l'implementazione di ambienti di imaging medicale nelle macchine virtuali. La tua organizzazione sanitaria può realizzare con sicurezza tutti i vantaggi di un'infrastruttura virtuale leader del settore, come ad esempio:

- **Implementazione semplice.** implementazione rapida e semplice di vCenter Server mediante un'appliance virtuale.
- **Controllo e visibilità centralizzati.** amministrare l'intera infrastruttura vSphere da un'unica posizione.
- **Ottimizzazione proattiva.** allocare, ottimizzare e migrare le risorse per la massima efficienza.
- **Management.** utilizza potenti plug-in e tool per semplificare la gestione ed estendere il controllo.

Architettura

L'architettura FlexPod è progettata per fornire alta disponibilità in caso di guasto di un componente o di un collegamento nell'intero stack di calcolo, rete e storage. I percorsi di rete multipli per l'accesso al client e allo storage offrono il bilanciamento del carico e un utilizzo ottimale delle risorse.

La figura seguente illustra la topologia FC da 16 GB/Ethernet da 40 GbE per l'implementazione della soluzione di sistema di imaging medicale.



Architettura dello storage

Utilizzare le linee guida sull'architettura dello storage in questa sezione per configurare l'infrastruttura di storage per un sistema di imaging medicale aziendale.

Tier di storage

Un tipico ambiente di imaging medicale aziendale è costituito da diversi livelli di storage. Ogni Tier presenta requisiti specifici per le performance e il protocollo di storage. Lo storage NetApp supporta varie tecnologie RAID; ulteriori informazioni sono disponibili "qui". Ecco come i sistemi storage NetApp AFF soddisfano le esigenze dei diversi Tier di storage per il sistema di imaging:

- **Performance Storage (Tier 1).** questo Tier offre performance elevate ed elevata ridondanza per database, dischi del sistema operativo, datastore VMware Virtual Machine file System (VMFS) e così via. L'i/o a blocchi si sposta su fibra in un array di storage condiviso di SSD, come configurato in ONTAP. La latenza minima è da 1 ms a 3 ms, con un picco occasionale di 5 ms. Questo Tier di storage viene generalmente utilizzato per la cache di storage a breve termine, in genere da 6 a 12 mesi di storage delle immagini per un rapido accesso alle immagini DICOM online. Questo Tier offre performance elevate ed elevata ridondanza per cache di immagini, backup di database e così via. Gli array all-flash NetApp offrono una latenza <1 ms a una larghezza di banda sostenuta, che è molto inferiore ai tempi di servizio previsti da un tipico ambiente di imaging medicale aziendale. NetApp ONTAP supporta sia RAID-TEC (RAID a tripla parità per supportare tre guasti dei dischi) che RAID DP (RAID a doppia parità per sostenere due guasti dei dischi).

- **Storage di archiviazione (Tier 2).** questo Tier viene utilizzato per l'accesso tipico ai file ottimizzato in termini di costi, per lo storage RAID 5 o RAID 6 per volumi più grandi e per l'archiviazione a lungo termine con costi e performance inferiori. NetApp ONTAP supporta sia RAID-TEC (RAID a tripla parità per supportare tre guasti dei dischi) che RAID DP (RAID a doppia parità per sostenere due guasti dei dischi). NetApp FAS in FlexPod consente l'imaging dell'i/o dell'applicazione su NFS/SMB in un array di dischi SAS. I sistemi NetApp FAS offrono una latenza di ~10 ms con una larghezza di banda sostenuta, che è molto inferiore ai tempi di servizio previsti per lo storage di livello 2 in un ambiente di sistema di imaging medicale aziendale.

L'archiviazione basata sul cloud in un ambiente di cloud ibrido può essere utilizzata per l'archiviazione a un provider di cloud storage pubblico utilizzando S3 o protocolli simili. La tecnologia NetApp SnapMirror consente la replica dei dati di imaging da array all-flash o FAS a array di storage più lenti basati su disco o a Cloud Volumes ONTAP per AWS, Azure o Google Cloud.

NetApp SnapMirror offre funzionalità di replica dei dati leader del settore che aiutano a proteggere il tuo sistema di imaging medicale con la replica unificata dei dati. Semplifica la gestione della protezione dei dati nel data fabric con la replica multipiattaforma, dalla flash al disco al cloud:

- Trasportare i dati in modo perfetto ed efficiente tra i sistemi storage NetApp per supportare backup e disaster recovery con lo stesso volume di destinazione e lo stesso flusso di i/O.
- Failover su qualsiasi volume secondario. Ripristino da qualsiasi snapshot point-in-time sullo storage secondario.
- Proteggi i carichi di lavoro più critici con la replica sincrona senza perdita di dati disponibile (RPO=0).
- Ridurre il traffico di rete. Riduci l'impatto dello storage attraverso operazioni efficienti.
- Riduci il traffico di rete trasportando solo i blocchi di dati modificati.
- Preserva i benefici dell'efficienza dello storage sullo storage primario durante il trasporto, tra cui deduplica, compressione e compattazione.
- Maggiore efficienza inline con la compressione di rete.

Ulteriori informazioni sono disponibili "qui".

La tabella riportata di seguito elenca ciascun livello richiesto da un sistema di imaging medicale tipico per la latenza specifica e le caratteristiche di performance del throughput.

Tier di storage	Requisiti	Raccomandazione NetApp
1	Latenza di 1-5 ms throughput di 35 Mbps	AFF con latenza <1 ms AFF A300 coppia ad alta disponibilità (ha) con due shelf di dischi può gestire un throughput fino a ~1,6 Gbps
2	Archivio on-premise	FAS con una latenza fino a 30 ms.
	Archiviazione nel cloud	Replica SnapMirror su Cloud Volumes ONTAP o archiviazione di backup con il software NetApp StorageGRID

Connettività di rete storage

Fabric FC

- Il fabric FC è per l'i/o del sistema operativo host dal calcolo allo storage.
- Due fabric FC (fabric A e fabric B) sono collegati rispettivamente al fabric Cisco UCS A e al fabric UCS B.
- Su ciascun nodo controller è presente una macchina virtuale di storage (SVM) con due interfacce logiche FC (LIFF). Su ciascun nodo, un LIF è connesso al fabric A e l'altro al fabric B.
- La connettività end-to-end FC a 16 Gbps avviene tramite switch Cisco MDS. Sono configurati un singolo iniziatore, più porte di destinazione e zoning.
- L'avvio FC SAN viene utilizzato per creare un calcolo completamente stateless. I server vengono avviati dalle LUN nel volume di boot che risiede nel cluster di storage AFF.

Rete IP per l'accesso allo storage su iSCSI, NFS e SMB/CIFS

- Due LIF iSCSI si trovano nella SVM su ciascun nodo del controller. Su ciascun nodo, un LIF è connesso al fabric A e il secondo al fabric B.
- Due LIF dati NAS si trovano nella SVM su ciascun nodo controller. Su ciascun nodo, un LIF è connesso al fabric A e il secondo al fabric B.
- Gruppi di interfacce per porte di storage (Virtual Port Channel [VPC]) per collegamenti da 10 Gbps allo switch N9k-A e per collegamenti da 10 Gbps allo switch N9k-B.
- Carico di lavoro nei file system Extens4 o NTFS dalla macchina virtuale allo storage:
  - Protocollo iSCSI su IP.
- Macchine virtuali ospitate nell'archivio dati NFS:
  - L'i/o del sistema operativo VM passa su più percorsi Ethernet attraverso gli switch Nexus.

Gestione in-band (bond attivo-passivo)

- Collegamento da 1 Gbps allo switch di gestione N9k-A e collegamento da 1 Gbps allo switch di gestione N9k-B.

Backup e recovery

Il data center di FlexPod si basa su un array di storage gestito dal software di gestione dei dati NetApp ONTAP. Il software ONTAP si è evoluto in oltre 20 anni per fornire molte funzionalità di gestione dei dati per macchine virtuali, database Oracle, condivisioni di file SMB/CIFS e NFS. Fornisce inoltre tecnologie di protezione come la tecnologia Snapshot di NetApp, la tecnologia SnapMirror e la tecnologia di replica dei dati NetApp FlexClone. Il software NetApp SnapCenter dispone di un server e di un client GUI per utilizzare le funzionalità Snapshot, SnapRestore e FlexClone di ONTAP per il backup e il ripristino di macchine virtuali, file share SMB/CIFS, NFS e database Oracle.

Utilizzo del software NetApp SnapCenter "brevettato" Tecnologia Snapshot per creare istantaneamente un backup di un'intera macchina virtuale o database Oracle su un volume di storage NetApp. Rispetto a Oracle Recovery Manager (RMAN), le copie Snapshot non richiedono una copia di backup di riferimento completa, perché non vengono memorizzate come copie fisiche dei blocchi. Le copie Snapshot vengono memorizzate come puntatori ai blocchi di storage così come esistevano nel file system ONTAP WAFL al momento della creazione delle copie Snapshot. A causa di questa stretta relazione fisica, le copie Snapshot vengono mantenute sullo stesso array di storage dei dati originali. Le copie Snapshot possono essere create anche a livello di file per offrire un controllo più granulare per il backup.

La tecnologia Snapshot si basa su una tecnica di redirect-on-write. Inizialmente contiene solo puntatori di metadati e non consuma molto spazio fino alla prima modifica dei dati in un blocco di storage. Se un blocco

esistente viene bloccato da una copia Snapshot, un nuovo blocco viene scritto dal file system ONTAP WAFL come copia attiva. Questo approccio evita le doppie scritture che si verificano con la tecnica change-on-write.

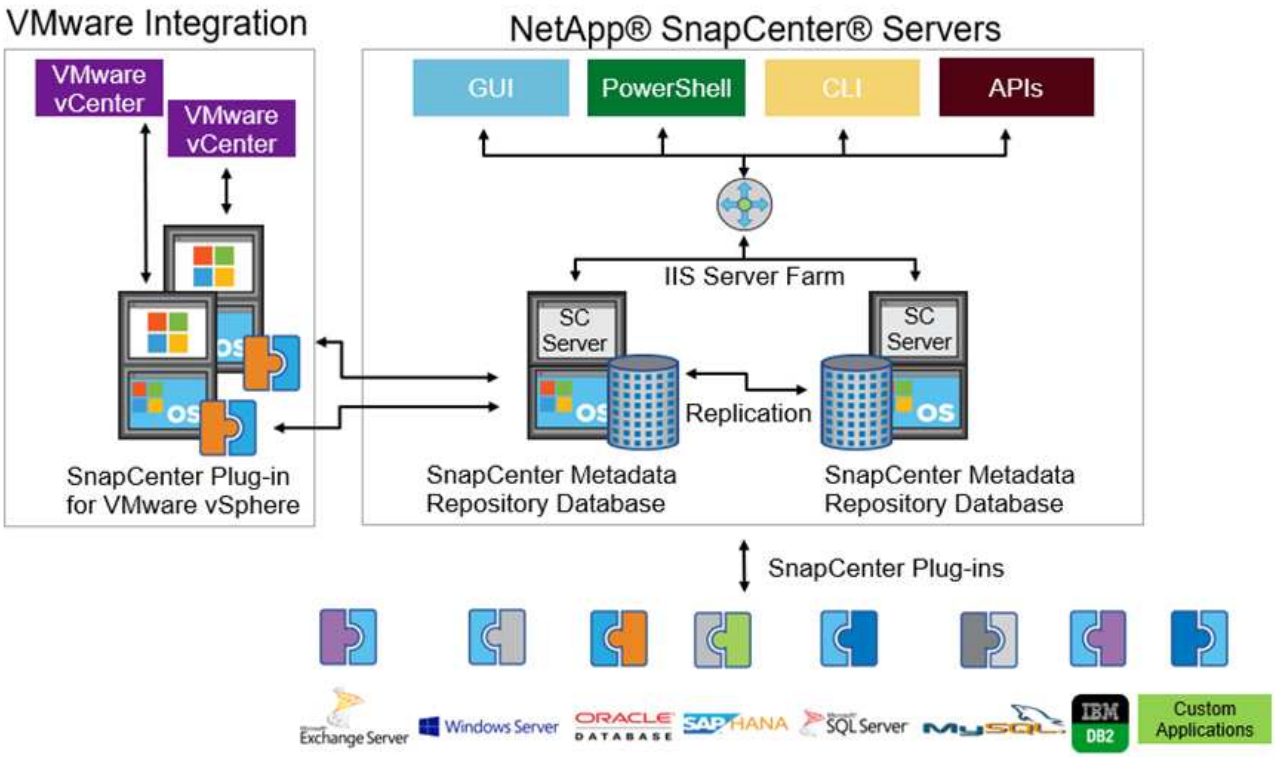
Per il backup del database Oracle, le copie Snapshot consentono risparmi di tempo incredibili. Ad esempio, il completamento di un backup che ha richiesto 26 ore utilizzando solo RMAN può richiedere meno di 2 minuti utilizzando il software SnapCenter.

Inoltre, poiché il ripristino dei dati non copia alcun blocco di dati, ma inverte i puntatori alle immagini dei blocchi Snapshot coerenti con l'applicazione al momento della creazione della copia Snapshot, una copia di backup Snapshot può essere ripristinata quasi istantaneamente. La clonazione SnapCenter crea una copia separata dei puntatori di metadati su una copia Snapshot esistente e monta la nuova copia su un host di destinazione. Questo processo è anche rapido ed efficiente in termini di storage.

La seguente tabella riassume le principali differenze tra Oracle RMAN e il software NetApp SnapCenter.

	Backup	**Ripristinare**	**Clonare**	**Backup completo necessario**	**Utilizzo dello spazio**	**Copia off-site**
RMAN	Lento	Lento	Lento	Sì	Alto	Sì
SnapCenter	Veloce	Veloce	Veloce	No	Basso	Sì

La figura seguente illustra l'architettura di SnapCenter.



Le configurazioni di NetApp MetroCluster sono utilizzate da migliaia di aziende in tutto il mondo per alta disponibilità (ha), nessuna perdita di dati e operazioni senza interruzioni sia all'interno che all'esterno del data center. MetroCluster è una funzionalità gratuita del software ONTAP che esegue il mirroring sincrono dei dati e della configurazione tra due cluster ONTAP in posizioni o domini di errore separati. MetroCluster offre storage continuamente disponibile per le applicazioni gestendo automaticamente due obiettivi: Zero recovery point

objective (RPO) mediante il mirroring sincrono dei dati scritti nel cluster. RTO (Near Zero Recovery Time Objective) tramite il mirroring della configurazione e l'automazione dell'accesso ai dati nel secondo sito MetroCluster offre semplicità con il mirroring automatico dei dati e la configurazione tra i due cluster indipendenti situati nei due siti. Poiché lo storage viene fornito all'interno di un cluster, viene automaticamente eseguito il mirroring nel secondo cluster del secondo sito. La tecnologia NetApp SyncMirror offre una copia completa di tutti i dati senza RPO. , Pertanto, i carichi di lavoro da un sito possono passare al sito opposto in qualsiasi momento e continuare a servire i dati senza perdita di dati. Ulteriori informazioni sono disponibili "qui".

Networking

Una coppia di switch Cisco Nexus fornisce percorsi ridondanti per il traffico IP dal calcolo allo storage e per i client esterni del visualizzatore di immagini del sistema di imaging medicale:

- L'aggregazione di collegamenti che utilizza i canali di porta e i VPC vengono utilizzati ovunque, consentendo la progettazione di una maggiore larghezza di banda e disponibilità elevata:
  - VPC viene utilizzato tra lo storage array NetApp e gli switch Cisco Nexus.
  - VPC viene utilizzato tra Cisco UCS Fabric Interconnect e gli switch Cisco Nexus.
  - Ogni server dispone di schede di interfaccia di rete virtuali (vNIC) con connettività ridondante all'Unified Fabric. Il failover NIC viene utilizzato tra le interconnessioni fabric per la ridondanza.
  - Ogni server dispone di vHBA (Virtual host bus adapter) con connettività ridondante all'Unified Fabric.
- Le interconnessioni fabric Cisco UCS sono configurate in modalità end-host come consigliato, fornendo il pinning dinamico delle vNIC agli switch uplink.
- Una rete di storage FC è fornita da una coppia di switch Cisco MDS.

Calcolo: Cisco Unified Computing System

Due fabric Cisco UCS attraverso diverse interconnessioni fabric forniscono due domini di errore. Ogni fabric è collegato sia agli switch di rete IP che a diversi switch di rete FC.

Profili di servizio identici per ogni blade Cisco UCS vengono creati in base alle Best practice FlexPod per eseguire VMware ESXi. Ciascun profilo di servizio deve avere i seguenti componenti:

- Due vNIC (una su ciascun fabric) per trasportare NFS, SMB/CIFS e traffico client o di gestione
- VLAN aggiuntive richieste alle vNIC per NFS, SMB/CIFS e traffico client o di gestione
- Due vNIC (una su ciascun fabric) per trasportare il traffico iSCSI
- Due HBA FC di storage (uno per fabric) per il traffico FC verso lo storage
- Boot SAN

Virtualizzazione

Il cluster host VMware ESXi esegue workload VM. Il cluster comprende istanze di ESXi in esecuzione sui server blade Cisco UCS.

Ciascun host ESXi include i seguenti componenti di rete:

- Boot SAN su FC o iSCSI
- LUN di boot su storage NetApp (in un FlexVol dedicato per il sistema operativo di boot)
- Due VMNIC (Cisco UCS vNIC) per NFS, SMB/CIFS o traffico di gestione

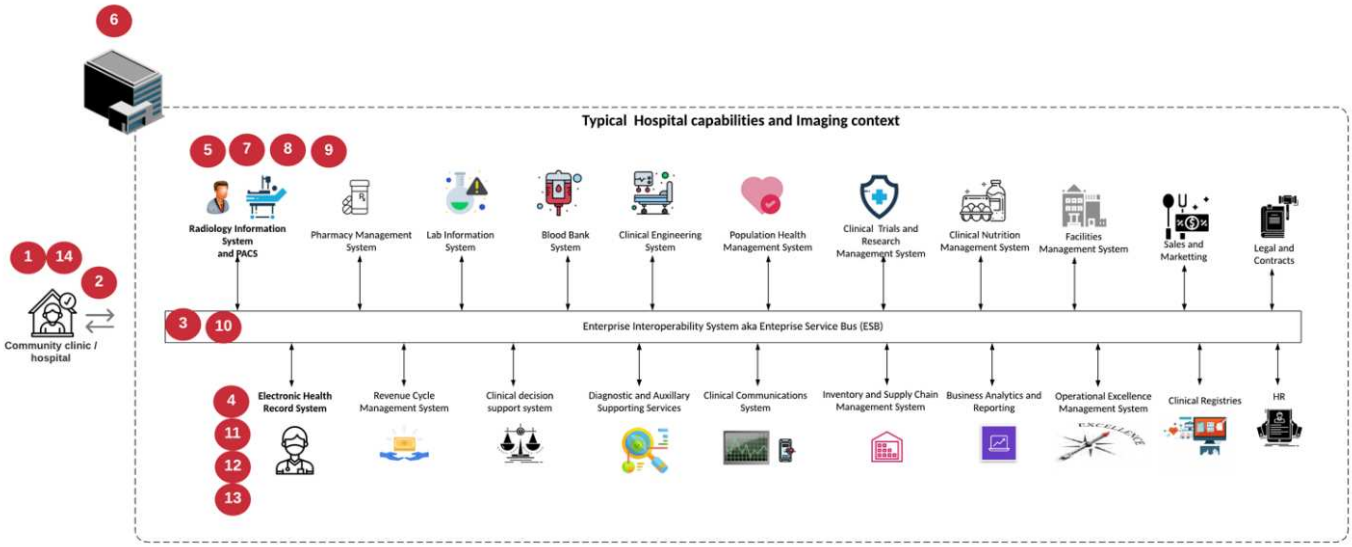
- Due HBA storage (Cisco UCS FC vHBA) per il traffico FC verso lo storage
- Switch standard o switch virtuale distribuito (in base alle necessità)
- Datastore NFS per workload VM
- Gestione, rete di traffico client e gruppi di porte di rete storage per macchine virtuali
- Adattatore di rete per la gestione, il traffico client e l'accesso allo storage (NFS, iSCSI o SMB/CIFS) per ciascuna macchina virtuale
- VMware DRS attivato
- Multipathing nativo abilitato per percorsi FC o iSCSI verso lo storage
- Snapshot VMware per VM disattivate
- NetApp SnapCenter è stato implementato per VMware per i backup delle macchine virtuali

Architettura del sistema di imaging medicale

Nelle organizzazioni sanitarie, i sistemi di imaging medicale sono applicazioni critiche e ben integrati nei flussi di lavoro clinici che iniziano dalla registrazione dei pazienti e terminano con le attività correlate alla fatturazione nel ciclo dei ricavi.

Il diagramma seguente mostra i vari sistemi coinvolti in un tipico ospedale di grandi dimensioni; questo diagramma è stato progettato per fornire un contesto architettonico a un sistema di imaging medicale prima di eseguire lo zoom sui componenti architettonici di un tipico sistema di imaging medicale. I flussi di lavoro variano notevolmente e sono specifici per ospedale e caso d'utilizzo.

La figura seguente mostra il sistema di imaging medico nel contesto di un paziente, di una clinica comunitaria e di un grande ospedale.



1. Il paziente visita la clinica della comunità con i sintomi. Durante la consultazione, il medico di comunità invia un ordine di imaging all'ospedale più grande sotto forma di messaggio di ordine HL7.
2. Il sistema EHR del medico di comunità invia il messaggio HL7 Order/ORD all'ospedale più grande.
3. Il sistema di interoperabilità aziendale (noto anche come Enterprise Service Bus [ESB]) elabora il messaggio di ordine e invia il messaggio di ordine al sistema EHR.
4. L'EHR elabora il messaggio di ordine. Se non esiste una cartella paziente, viene creata una nuova cartella paziente.

5. L'EHR invia un ordine di imaging al sistema di imaging medicale.
6. Il paziente chiama l'ospedale più grande per un appuntamento con l'imaging.
7. Il banco di ricezione e registrazione delle immagini pianifica il paziente per un appuntamento di imaging utilizzando informazioni radiologiche o sistemi simili.
8. Il paziente arriva per l'appuntamento di imaging e le immagini o il video vengono creati e inviati al PACS.
9. Il radiologo legge le immagini e le annota nel PACS utilizzando un visualizzatore di diagnostica high-end/GPU abilitato. Alcuni sistemi di imaging dispongono di funzionalità di miglioramento dell'efficienza abilitate dall'intelligenza artificiale (ai) integrate nei flussi di lavoro di imaging.
10. I risultati dell'ordine di immagini vengono inviati all'EHR sotto forma di messaggio ORU HL7 dei risultati dell'ordine tramite l'ESB.
11. L'EHR elabora i risultati dell'ordine nella cartella del paziente, inserisce un'immagine in miniatura con un collegamento contestuale all'immagine DICOM effettiva. I medici possono avviare il visualizzatore diagnostico se è necessaria un'immagine con una risoluzione superiore dall'EHR.
12. Il medico esamina l'immagine e inserisce le note del medico nella cartella clinica del paziente. Il medico potrebbe utilizzare il sistema di supporto decisionale clinico per migliorare il processo di revisione e agevolare la corretta diagnosi del paziente.
13. Il sistema EHR invia quindi i risultati dell'ordine sotto forma di messaggio relativo ai risultati dell'ordine all'ospedale della comunità. A questo punto, se l'ospedale della comunità è in grado di ricevere l'immagine completa, l'immagine viene inviata tramite WADO o DICOM.
14. Il medico di comunità completa la diagnosi e fornisce le fasi successive al paziente.

Un tipico sistema di imaging medicale utilizza un'architettura a più livelli. Il componente principale di un sistema di imaging medicale è un server applicativo per ospitare vari componenti applicativi. I server applicazioni tipici sono basati su Java runtime o su CLC n. .Net. La maggior parte delle soluzioni di imaging medicale aziendali utilizza un database Oracle Server o MS SQL Server o Sybase come database primario. Inoltre, alcuni sistemi di imaging medicale aziendali utilizzano database per l'accelerazione dei contenuti e il caching in un'area geografica. Alcuni sistemi di imaging medico aziendale utilizzano anche database NoSQL come MongoDB, Redis e così via in combinazione con server di integrazione aziendale per interfacce DICOM e/o API.

Un tipico sistema di imaging medicale consente l'accesso alle immagini per due diversi set di utenti: Utente/radiologo diagnostico o medico che ha ordinato l'imaging.

I radiologi in genere utilizzano visualizzatori di diagnostica high-end abilitati per la grafica che vengono eseguiti su workstation di elaborazione e grafica high-end fisiche o parte di un'infrastruttura di desktop virtuale. Se stai per iniziare il tuo percorso nell'infrastruttura di desktop virtuale, puoi trovare ulteriori informazioni "qui".

Quando l'uragano Katrina ha distrutto due dei principali ospedali di insegnamento della Louisiana, i leader si sono riuniti e hanno costruito un sistema di cartelle cliniche elettroniche resiliente che includeva oltre 3000 desktop virtuali in tempi record. Ulteriori informazioni sull'architettura di riferimento dei casi di utilizzo e sui bundle di riferimento FlexPod sono disponibili "qui".

I medici accedono alle immagini in due modi principali:

- **Accesso basato su web.** che viene generalmente utilizzato dai sistemi EHR per incorporare le immagini PACS come collegamenti contestuali nella cartella clinica elettronica (EMR) del paziente e collegamenti che possono essere inseriti in flussi di lavoro di imaging, workflow di procedure, flussi di lavoro delle note di avanzamento e così via. I collegamenti basati sul Web consentono inoltre di accedere alle immagini dei pazienti attraverso i portali dei pazienti. L'accesso basato su Web utilizza un modello tecnologico chiamato link contestualizzati. I collegamenti in base al contesto possono essere collegamenti statici/URI direttamente al supporto DICOM oppure collegamenti/URI generati dinamicamente utilizzando macro

personalizzate.

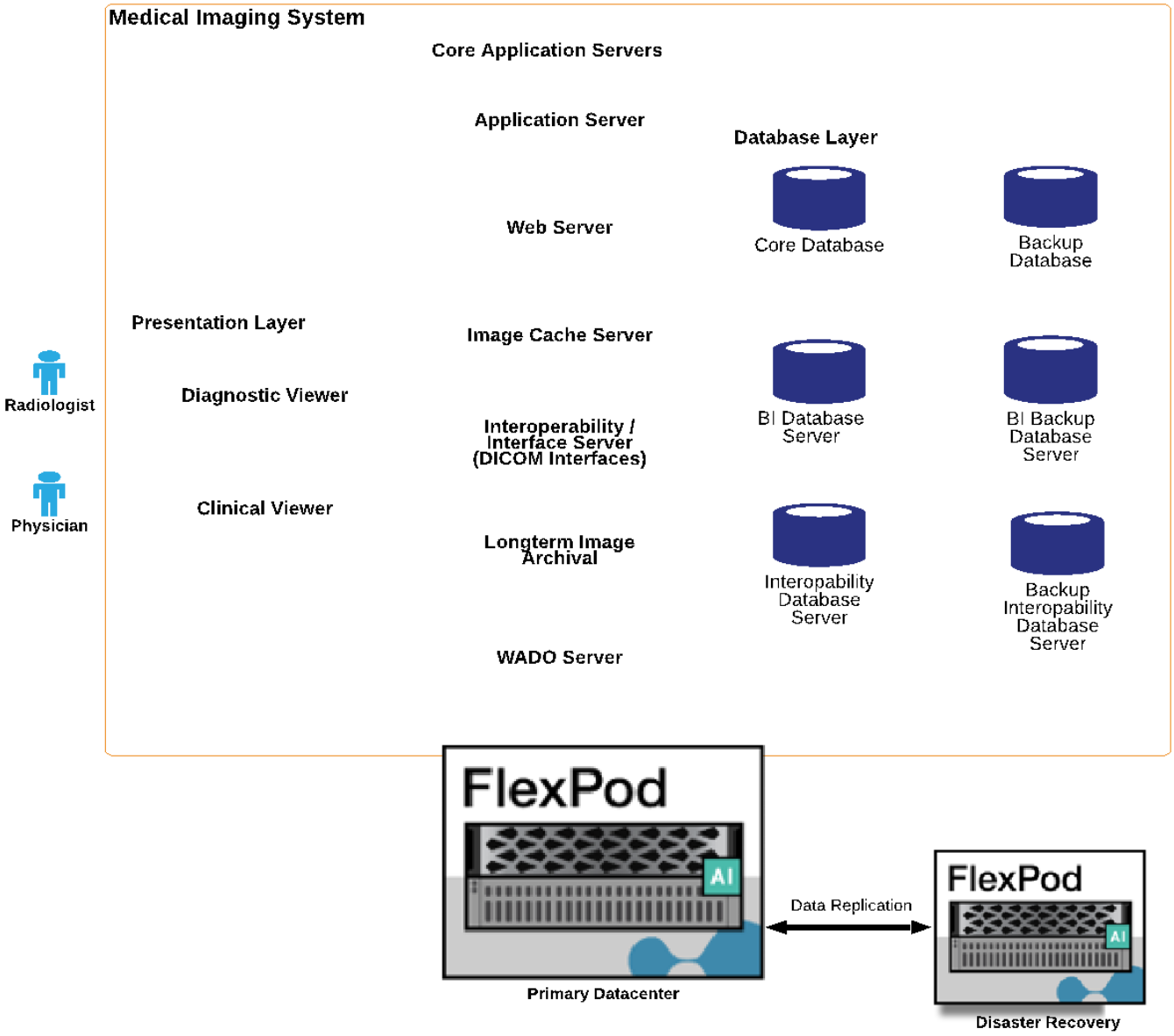
- **Thick client.** alcuni sistemi medici aziendali consentono inoltre di utilizzare un approccio basato su thick client per visualizzare le immagini. È possibile avviare un thick client dall'interno dell'EMR del paziente o come applicazione standalone.

Il sistema di imaging medico può fornire l'accesso alle immagini a una comunità di medici o a medici partecipanti alla CIN. I sistemi di imaging medicale tipici includono componenti che consentono l'interoperabilità delle immagini con altri sistemi IT sanitari all'interno e all'esterno dell'organizzazione sanitaria. I medici della community possono accedere alle immagini tramite un'applicazione basata su web o sfruttare una piattaforma di scambio di immagini per l'interoperabilità delle immagini. Le piattaforme di scambio di immagini utilizzano in genere WADO o DICOM come protocollo di scambio di immagini sottostante.

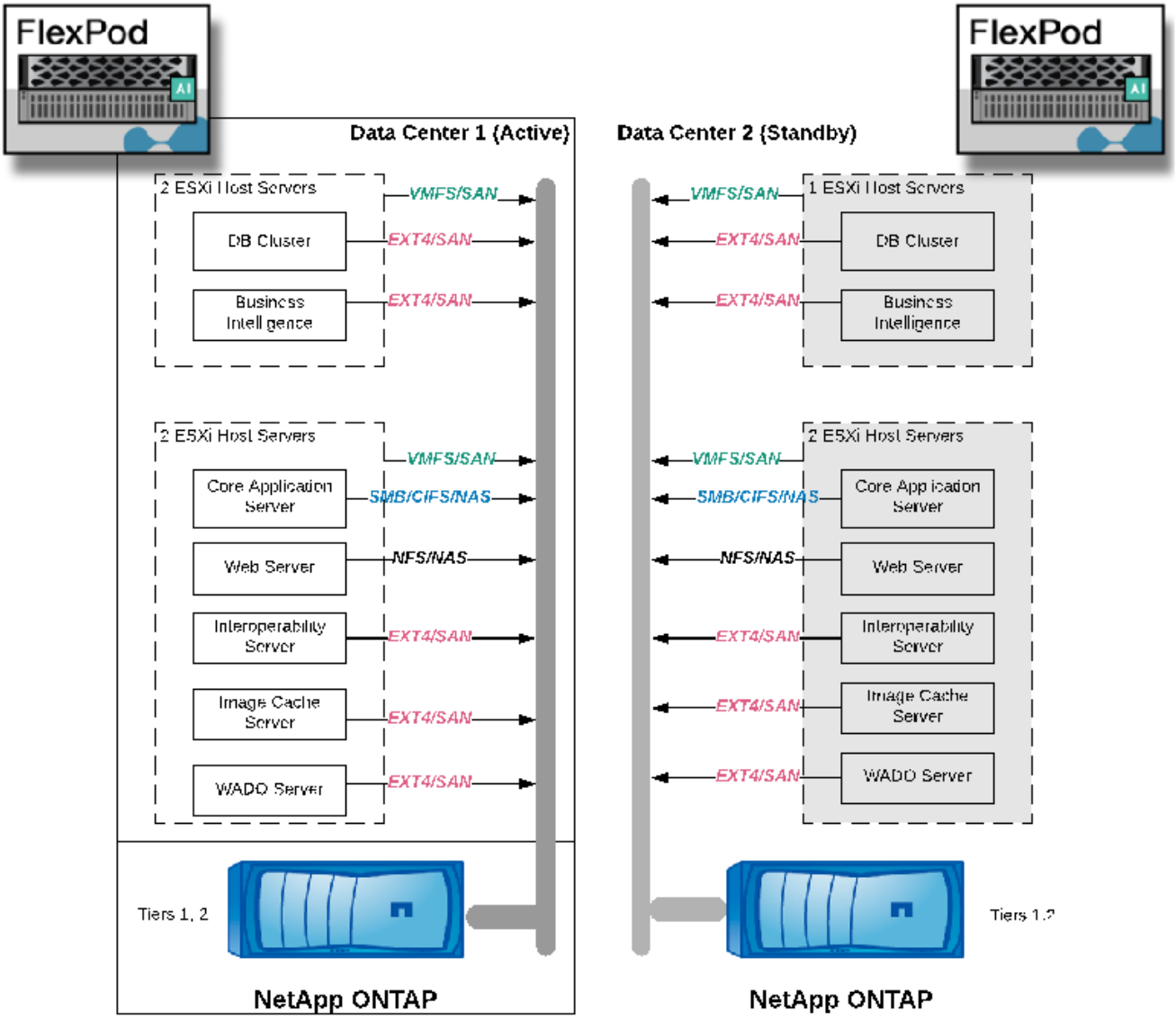
I sistemi di imaging medico possono anche supportare centri medici accademici che necessitano di sistemi PACS o di imaging per l'utilizzo in classe. Per supportare le attività accademiche, un tipico sistema di imaging medicale può avere le funzionalità di un sistema PACS con un ingombro ridotto o un ambiente di imaging solo didattico. I tipici sistemi di archiviazione indipendenti dal vendor e alcuni sistemi di imaging medicale di livello Enterprise offrono funzionalità di morphing delle etichette delle immagini DICOM per rendere anonime le immagini utilizzate a scopo didattico. Il morphing dei tag consente alle organizzazioni sanitarie di scambiare immagini DICOM tra sistemi di imaging medicali di diversi fornitori in modo indipendente dal vendor. Inoltre, il morphing dei tag consente ai sistemi di imaging medicale di implementare una funzionalità di archiviazione indipendente dal vendor a livello aziendale per le immagini mediche.

I sistemi di imaging medicale stanno iniziando a utilizzare "Funzionalità di calcolo basate su GPU" migliorare i flussi di lavoro umani pre-elaborando le immagini e migliorando così l'efficienza. I tipici sistemi di imaging medico aziendale sfruttano le funzionalità di efficienza dello storage NetApp leader del settore. I sistemi di imaging medicale aziendali utilizzano in genere RMAN per le attività di backup, ripristino e ripristino. Per ottenere performance migliori e ridurre il tempo necessario per la creazione dei backup, è disponibile la tecnologia Snapshot per le operazioni di backup e la tecnologia SnapMirror per la replica.

La figura seguente mostra i componenti logici dell'applicazione in una vista architetturale a più livelli.



La figura seguente mostra i componenti fisici dell'applicazione.



I componenti dell'applicazione logica richiedono che l'infrastruttura supporti un insieme diversificato di protocolli e file system. Il software NetApp ONTAP supporta un set leader del settore di protocolli e file system.

La tabella seguente elenca i componenti dell'applicazione, il protocollo di storage e i requisiti del file system.

Componente dell'applicazione	SAN/NAS	Tipo di file system	Tier di storage	Tipo di replica
Database prod host VMware	locale	SAN	VMFS	Tier 1
Applicazione	Database prod host VMware	REP	SAN	VMFS
Tier 1	Applicazione	Applicazione di supporto host VMware	locale	SAN

Componente dell'applicazione	SAN/NAS	Tipo di file system	Tier di storage	Tipo di replica
VMFS	Tier 1	Applicazione	Applicazione di supporto host VMware	REP
SAN	VMFS	Tier 1	Applicazione	Server database principale
SAN	Ext4	Tier 1	Applicazione	Server del database di backup
SAN	Ext4	Tier 1	Nessuno	Server della cache delle immagini
NAS	SMB/CIFS	Tier 1	Nessuno	Server di archiviazione
NAS	SMB/CIFS	Tier 2	Applicazione	Server Web
NAS	SMB/CIFS	Tier 1	Nessuno	Server WADO
SAN	NFS	Tier 1	Applicazione	Server di business intelligence
SAN	NTFS	Tier 1	Applicazione	Backup di business intelligence
SAN	NTFS	Tier 1	Applicazione	Server di interoperabilità
SAN	Ext4	Tier 1	Applicazione	Server di database per l'interoperabilità

Componenti hardware e software dell'infrastruttura della soluzione

Le seguenti tabelle elencano rispettivamente i componenti hardware e software dell'infrastruttura FlexPod per il sistema di imaging medicale.

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1 o 2	In base al numero di blade necessari per supportare il numero di studi annuali
	Blade server Cisco UCS	B200 M5	Numero di blade basato sul numero di studi all'anno, ciascuno con 2 x 20 o più core, 2,7 GHz e 128-384 GB di RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Vedere
	2 interconnessioni fabric Cisco UCS	6454 o versione successiva	–

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Rete	Switch Cisco Nexus	2 Cisco Nexus serie 3000 o 9000	–
Rete di storage	Rete IP per l'accesso allo storage su protocolli SMB/CIFS, NFS o iSCSI	Stessi switch di rete come sopra	–
	Accesso allo storage tramite FC	2 Cisco MDS 9132T	–
Storage	Sistema storage all-flash NetApp AFF A400	1 o più coppie ha	Cluster con due o più nodi
	Shelf di dischi	1 o più shelf di dischi DS224C o NS224	Completamente popolato con 24 dischi
	SSD	Capacità superiore a 24, 1,2 TB	–

Software	Famiglia di prodotti	Versione o release	Dettagli
Sistema di imaging medico aziendale			
	MS SQL o Oracle Database Server	Come suggerito dal fornitore del sistema di imaging medicale	
	Nessun DBS SQL come MongoDB Server	Come suggerito dal fornitore del sistema di imaging medicale	
	Server applicazioni	Come suggerito dal fornitore del sistema di imaging medicale	
	Integration Server (MS BizTalk, MuleSoft, Rhapsody, Tibco)	Come suggerito dal fornitore del sistema di imaging medicale	
	Macchine virtuali	Linux (64 bit)	
	Macchine virtuali	Windows Server (64 bit)	
Storage	ONTAP	ONTAP 9.7 o versione successiva	
Rete	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 o versione successiva	
	Switch Ethernet Cisco	9.2(3)I7(2) o versione successiva	
	Cisco FC: Cisco MDS 9132T	8.4(2) o versione successiva	
Hypervisor	Hypervisor	VMware vSphere ESXi 6.7 U2 o versione successiva	

Software	Famiglia di prodotti	Versione o release	Dettagli
Gestione	Sistema di gestione dell'hypervisor	VMware vCenter Server 6.7 U1 (vCSA) o versione successiva	
	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	
	SnapCenter	SnapCenter 4.3 o versione successiva	

Dimensionamento della soluzione

Dimensionamento dello storage

Questa sezione descrive il numero di studi e i requisiti dell'infrastruttura corrispondenti.

I requisiti di storage elencati nella tabella seguente presuppongono che i dati esistenti siano del valore di 1 anno più la crescita prevista per 1 anno di studio nel sistema primario (Tier 1, 2). Le esigenze di storage aggiuntive per la crescita prevista per 3 anni oltre i primi 2 anni sono elencate separatamente.

	Piccolo	Medio	Grande
Studi annuali	<250.000 studi	250.000-500.000 studi	500.000–1 milione di studi
Storage di livello 1			
IOPS (media)	1,5 K-5K	5.000–15.000	15.000-40.000
IOPS (picco)	5K	20.000	65.000
Throughput	50 Mbps	50 Mbps	100 Mbps
Capacity Data Center 1 (1 anno di dati vecchi e 1 anno di nuovo studio)	70 TB	140 TB	260 TB
Capacity data center 1 (necessità aggiuntiva di 4 anni per il nuovo studio)	25 TB	45 TB	80 TB
Capacity data center 2 (1 anno di dati vecchi e 1 anno di nuovo studio)	45 TB	110 TB	165 TB
Capacity data center 2 (necessità aggiuntiva di 4 anni per il nuovo studio)	25 TB	45 TB	80 TB
Storage di livello 2			
IOPS (media)	1.000	2K	3.000
Data center di capacità 1	320 TB	800 TB	2000 TB

Dimensionamento del calcolo

La tabella seguente elenca i requisiti di calcolo per i sistemi di imaging medicale di piccole, medie e grandi

dimensioni.

	Piccolo	Medio	Grande
Studi annuali	<250.000 studi	250.000-500.000 studi	500.000–1 milione di studi
Data center 1			
Numero di macchine virtuali	21	27	35
Numero totale di CPU virtuali (vCPU)	56	124	220
Requisito di memoria totale	225 GB	450 GB	900 GB
Specifiche dei server fisici (blade) (si supponga 1 vCPU -=1 core)	4 server con 20 core e 192 GB di RAM ciascuno	8 server con 20 core e 128 GB di RAM ciascuno	14 server con 20 core e 128 GB di RAM ciascuno
Data center 2			
Numero di macchine virtuali	15	17	22
Numero totale di vCPU	42	72	140
Requisito di memoria totale	179 GB	243 GB	513 GB
Specifiche dei server fisici (blade) (si supponga che 1 vCPU = 1 core)	3 server con 20 core e 168 GB di RAM ciascuno	6 server con 20 core e 128 GB di RAM ciascuno	8 server con 24 core e 128 GB di RAM ciascuno

Dimensionamento dell’infrastruttura Cisco UCS e networking

La tabella seguente elenca i requisiti di rete e dell’infrastruttura Cisco UCS per i sistemi di imaging medicale di piccole, medie e grandi dimensioni.

	Piccolo	Medio	Grande
Data center 1			
Numero di porte del nodo di storage	2 adattatori di rete convergenti (CNA); 2 FCS	2 CNA; 2 FCS	2 CNA; 2 FCS
Porte switch di rete IP (Cisco Nexus 9000)	switch a 48 porte	switch a 48 porte	switch a 48 porte
Switch FC (Cisco MDS)	switch a 32 porte	switch a 32 porte	switch a 48 porte
Numero di chassis Cisco UCS	1 x 5108	1 x 5108	2 x 5108
Cisco UCS Fabric Interconnect	2 x 6332	2 x 6332	2 x 6332
Data center 2			

	Piccolo	Medio	Grande
Numero di chassis Cisco UCS	1 x 5108	1 x 5108	1 x 5108
Cisco UCS Fabric Interconnect	2 x 6332	2 x 6332	2 x 6332
Numero di porte del nodo di storage	2 CNA; 2 FCS	2 CNA; 2 FCS	2 CNA; 2 FCS
Porte switch di rete IP (Cisco Nexus 9000)	switch a 48 porte	switch a 48 porte	switch a 48 porte
Switch FC (Cisco MDS)	switch a 32 porte	switch a 32 porte	switch a 48 porte

Best practice

Best practice per lo storage

Alta disponibilità

Il design del cluster di storage NetApp offre alta disponibilità a ogni livello:

- Nodi del cluster
- Connettività storage back-end
- TEC RAID in grado di sostenere tre guasti dei dischi
- RAID DP in grado di sostenere due guasti dei dischi
- Connettività fisica a due reti fisiche da ciascun nodo
- Percorsi di dati multipli per LUN e volumi di storage

Multi-tenancy sicura

Le storage virtual machine (SVM) di NetApp forniscono un array di storage virtuale per separare il dominio di sicurezza, le policy e le reti virtuali. NetApp consiglia di creare SVM separate per ogni organizzazione tenant che ospita i dati nel cluster di storage.

Best practice per lo storage NetApp

Prendere in considerazione le seguenti Best practice per lo storage NetApp:

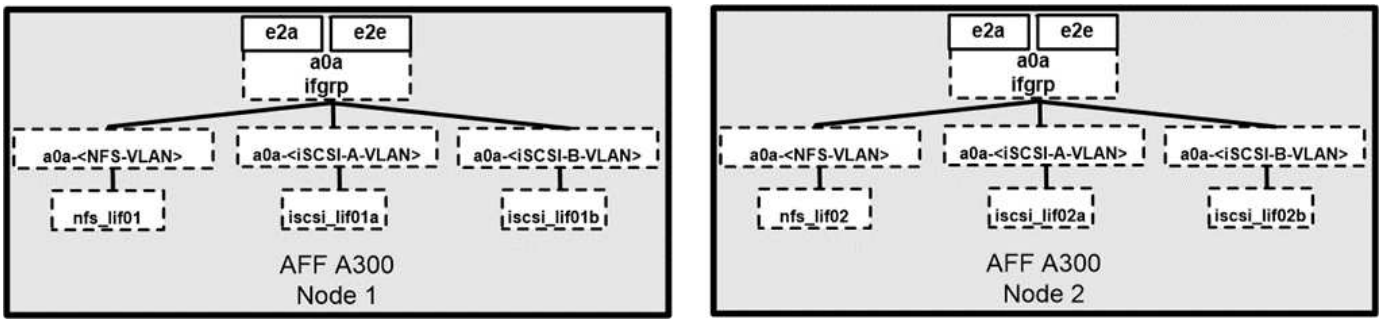
- Abilitare sempre la tecnologia NetApp AutoSupport, che invia a NetApp informazioni riepilogative sul supporto tramite HTTPS.
- Per ottenere la massima disponibilità e mobilità, assicurarsi di creare una LIF per ogni SVM su ciascun nodo del cluster NetApp ONTAP. ALUA (Asymmetric Logical Unit Access) viene utilizzato per analizzare i percorsi e identificare i percorsi attivi ottimizzati (diretti) rispetto ai percorsi attivi non ottimizzati. ALUA viene utilizzato sia per FC, FCoE e iSCSI.
- Un volume contenente solo LUN non deve essere montato internamente, né è necessario un percorso di giunzione.
- Se si utilizza il protocollo CHAP (Challenge-Handshake Authentication Protocol) in ESXi per l'autenticazione di destinazione, è necessario configurarlo anche in ONTAP. Utilizzare la CLI (`vserver iscsi security create`) O Gestore di sistema NetApp ONTAP (modificare la sicurezza dell'iniziatore

in Storage > SVM > Impostazioni SVM > protocolli > iSCSI).

Boot SAN

NetApp consiglia di implementare l'avvio SAN per i server Cisco UCS nella soluzione FlexPod Datacenter. Questa fase consente al sistema operativo di essere protetto in modo sicuro dal sistema di storage NetApp AFF, fornendo performance migliori. Il design delineato in questa soluzione utilizza l'avvio SAN iSCSI.

Nell'avvio SAN iSCSI, a ogni Cisco UCS Server vengono assegnate due vNIC iSCSI (una per ogni fabric SAN), che forniscono connettività ridondante fino allo storage. Le porte di storage di questo esempio, e2a e e2e, collegate agli switch Cisco Nexus, sono raggruppate in modo da formare una porta logica chiamata gruppo di interfacce (ifgrp) (in questo esempio, a0a). Le VLAN iSCSI vengono create sull'igroup e le LIF iSCSI vengono create sui gruppi di porte iSCSI (in questo esempio, a0a-<iSCSI-A-VLAN>). Il LUN di avvio iSCSI viene esposto ai server attraverso il LIF iSCSI utilizzando igroups. Questo approccio consente solo al server autorizzato di accedere al LUN di avvio. Per il layout di porta e LIF, vedere la figura seguente.



A differenza delle interfacce di rete NAS, le interfacce di rete SAN non sono configurate per il failover durante un guasto. Se invece un'interfaccia di rete non è disponibile, l'host sceglie un nuovo percorso ottimizzato per un'interfaccia di rete disponibile. ALUA, uno standard supportato da NetApp, fornisce informazioni sulle destinazioni SCSI, consentendo a un host di identificare il percorso migliore per lo storage.

Efficienza dello storage e thin provisioning

NetApp è leader del settore nell'innovazione dell'efficienza dello storage, ad esempio con la prima deduplica per i carichi di lavoro primari e con la compattazione dei dati inline, che migliora la compressione e memorizza file di piccole dimensioni e i/o in modo efficiente. ONTAP supporta la deduplica in linea e in background, nonché la compressione inline e in background.

Per sfruttare i vantaggi della deduplica in un ambiente a blocchi, le LUN devono essere con thin provisioning. Anche se il LUN viene ancora considerato dall'amministratore della macchina virtuale come una capacità fornita, i risparmi della deduplica vengono restituiti al volume per essere utilizzati per altre esigenze. NetApp consiglia di implementare questi LUN in volumi FlexVol con thin provisioning e capacità doppia rispetto al LUN. Quando si implementa il LUN in questo modo, il volume FlexVol funge semplicemente da quota. Lo storage utilizzato dal LUN viene riportato nel volume FlexVol e nel relativo aggregato.

Per ottenere il massimo risparmio sulla deduplica, è consigliabile pianificare la deduplica in background. Tuttavia, questi processi utilizzano le risorse di sistema quando sono in esecuzione. Pertanto, idealmente, è necessario pianificarli in tempi meno attivi (come i fine settimana) o eseguirli più frequentemente per ridurre la quantità di dati modificati da elaborare. La deduplica automatica in background sui sistemi AFF ha un effetto molto minore sulle attività in primo piano. La compressione in background (per sistemi basati su disco rigido) consuma anche le risorse, pertanto è consigliabile considerarla solo per carichi di lavoro secondari con requisiti di performance limitati.

Qualità del servizio

I sistemi che eseguono il software ONTAP possono utilizzare la funzione QoS dello storage ONTAP per limitare il throughput in megabit al secondo (Mbps) e per limitare gli IOPS per diversi oggetti di storage come file, LUN, volumi o intere SVM. La QoS adattiva viene utilizzata per impostare un piano IOPS (minimo QoS) e un soffitto (massimo QoS), che si regolano dinamicamente in base alla capacità del datastore e allo spazio utilizzato.

I limiti di throughput sono utili per controllare carichi di lavoro sconosciuti o di test prima di un'implementazione per confermare che non influiscono su altri carichi di lavoro. Questi limiti possono essere utilizzati anche per limitare un carico di lavoro ingombrante dopo che è stato identificato. Sono supportati anche i livelli minimi di servizio basati sugli IOPS per fornire performance costanti per gli oggetti SAN in ONTAP.

Con un datastore NFS, è possibile applicare una policy di QoS all'intero volume FlexVol o ai singoli file del disco macchina virtuale (VMDK) al suo interno. Con gli archivi di dati VMFS (volumi condivisi cluster [CSV] in Hyper-V) che utilizzano LUN ONTAP, è possibile applicare i criteri di QoS al volume FlexVol che contiene le LUN o alle singole LUN. Tuttavia, poiché ONTAP non è a conoscenza di VMFS, non è possibile applicare i criteri di qualità del servizio ai singoli file VMDK. Quando si utilizza VMware Virtual Volumes (VVol) con VSC 7.1 o versione successiva, è possibile impostare il QoS massimo su singole macchine virtuali utilizzando il profilo di capacità dello storage.

Per assegnare un criterio QoS a una LUN, inclusi VMFS o CSV, è possibile ottenere la SVM ONTAP (visualizzata come `Vserver`), il percorso del LUN e il numero di serie dal menu Storage Systems (sistemi storage) nella home page del VSC. Selezionare il sistema di storage (SVM), quindi Related Objects (oggetti correlati) > SAN. Utilizzare questo approccio quando si specifica la qualità del servizio utilizzando uno degli strumenti ONTAP.

È possibile impostare il limite massimo di throughput QoS su un oggetto in Mbps e in IOPS. Se si utilizzano entrambi, il primo limite raggiunto viene applicato da ONTAP. Un carico di lavoro può contenere più oggetti e una policy QoS può essere applicata a uno o più carichi di lavoro. Quando applichi una policy a più workload, questi condividono il limite totale della policy. Gli oggetti nidificati non sono supportati (ad esempio, per un file all'interno di un volume, non possono avere una propria policy). I valori minimi di QoS possono essere impostati solo in IOPS.

Layout dello storage

In questa sezione vengono fornite le Best practice per il layout di LUN, volumi e aggregati sullo storage.

LUN dello storage

Per ottenere performance, gestione e backup ottimali, NetApp consiglia le seguenti Best practice di progettazione LUN:

- Creare un LUN separato per memorizzare i dati del database e i file di log.
- Creare un LUN separato per ogni istanza per memorizzare i backup del log del database Oracle. I LUN possono far parte dello stesso volume.
- Provisioning delle LUN con thin provisioning (disattivazione dell'opzione Space Reservation) per file di database e file di log.
- Tutti i dati di imaging sono ospitati in LUN FC. Creare queste LUN in volumi FlexVol distribuiti tra gli aggregati di proprietà di diversi nodi storage controller.

Per il posizionamento delle LUN in un volume di storage, seguire le linee guida della sezione successiva.

Volumi di storage

Per ottenere performance e gestione ottimali, NetApp consiglia le seguenti Best practice per la progettazione dei volumi:

- Isolare i database con query i/o-intensive su volumi di storage separati.
- I file di dati possono essere posizionati su un singolo LUN o volume, ma si consiglia di utilizzare più volumi/LUN per un throughput più elevato.
- Il parallelismo di i/o può essere ottenuto utilizzando qualsiasi filesystem supportato quando si utilizzano più LUN.
- Posizionare i file di database e i log delle transazioni su volumi separati per aumentare la granularità del ripristino.
- Considerare l'utilizzo di attributi di volume come dimensioni automatiche, Snapshot Reserve, QoS e così via.

Aggregati

Gli aggregati sono i principali container di storage per le configurazioni di storage NetApp e contengono uno o più gruppi RAID costituiti da dischi di dati e dischi di parità.

NetApp ha eseguito vari test di caratterizzazione dei carichi di lavoro i/o utilizzando aggregati condivisi e dedicati con file di dati e file di log delle transazioni separati. I test dimostrano che un grande aggregato con più gruppi e unità RAID (HDD o SSD) ottimizza e migliora le performance dello storage ed è più facile da gestire per gli amministratori per due motivi:

- Un grande aggregato rende disponibili le capacità di i/o di tutti i dischi per tutti i file.
- Un grande aggregato consente l'utilizzo più efficiente dello spazio su disco.

Per un disaster recovery efficace, NetApp consiglia di collocare la replica asincrona su un aggregato che fa parte di un cluster di storage separato nel sito di disaster recovery e di utilizzare la tecnologia SnapMirror per replicare il contenuto.

Per ottenere performance di storage ottimali, NetApp consiglia di disporre di almeno il 10% di spazio libero in un aggregato.

La guida al layout degli aggregati di storage per i sistemi AFF A300 (con due shelf di dischi con 24 dischi) include:

- Conserva due dischi di riserva.
- Utilizzare la partizione avanzata dei dischi per creare tre partizioni su ciascun disco: Root e dati.
- Utilizzare un totale di 20 partizioni dati e due partizioni di parità per ciascun aggregato.

Best practice per il backup

NetApp SnapCenter viene utilizzato per i backup di macchine virtuali e database. NetApp consiglia le seguenti Best practice per il backup:

- Quando SnapCenter viene implementato per creare copie Snapshot per i backup, disattivare la pianificazione Snapshot per FlexVol che ospita le macchine virtuali e i dati delle applicazioni.
- Creare un FlexVol dedicato per i LUN di boot host.
- Utilizzare una policy di backup simile o singola per le macchine virtuali che hanno lo stesso scopo.

- Utilizzare una policy di backup simile o singola per tipo di carico di lavoro; ad esempio, utilizzare una policy simile per tutti i carichi di lavoro del database. Utilizza policy diverse per database, server Web, desktop virtuali degli utenti finali e così via.
- Abilitare la verifica del backup in SnapCenter.
- Configurare l'archiviazione delle copie Snapshot di backup nella soluzione di backup NetApp SnapVault.
- Configurare la conservazione dei backup sullo storage primario in base alla pianificazione dell'archiviazione.

Best practice per l'infrastruttura

Best practice per il networking

NetApp consiglia le seguenti Best practice per il networking:

- Assicurarsi che il sistema includa NIC fisiche ridondanti per il traffico di produzione e di storage.
- VLAN separate per traffico iSCSI, NFS e SMB/CIFS tra calcolo e storage.
- Assicurarsi che il sistema includa una VLAN dedicata per l'accesso client al sistema di imaging medicale.

Ulteriori Best practice per il networking sono disponibili nelle guide alla progettazione e all'implementazione dell'infrastruttura FlexPod.

Calcolo delle Best practice

NetApp consiglia le seguenti Best practice di calcolo:

- Assicurarsi che ogni vCPU specificata sia supportata da un core fisico.

Best practice per la virtualizzazione

NetApp consiglia le seguenti Best practice per la virtualizzazione:

- Utilizzare VMware vSphere 6 o versione successiva.
- Impostare il BIOS del server host ESXi e il livello del sistema operativo su Custom Controlled - High Performance (controllo personalizzato - prestazioni elevate).
- Creazione di backup durante le ore di lavoro non di punta.

Best practice per il sistema di imaging medicale

Consultare le seguenti Best practice e alcuni requisiti di un tipico sistema di imaging medicale:

- Non eseguire il commit eccessivo della memoria virtuale.
- Assicurarsi che il numero totale di vCPU corrisponda al numero di CPU fisiche.
- Se si dispone di un ambiente di grandi dimensioni, sono necessarie VLAN dedicate.
- Configurare le macchine virtuali del database con cluster ha dedicati.
- Assicurarsi che i VMDK del sistema operativo delle macchine virtuali siano ospitati in uno storage Tier 1 veloce.
- Collabora con il fornitore del sistema di imaging medicale per identificare l'approccio migliore per preparare i modelli di macchine virtuali per una rapida implementazione e manutenzione.

- Le reti di gestione, storage e produzione richiedono la segregazione LAN per il database, con VLAN isolate per VMware vMotion.
- Utilizza la tecnologia di replica basata su array di storage NetApp chiamata "SnapMirror" Invece della replica basata su vSphere.
- Utilizzare tecnologie di backup che sfruttano le API VMware; le finestre di backup devono essere al di fuori delle normali ore di produzione.

Conclusione

Eseguendo un ambiente di imaging medico su FlexPod, la tua organizzazione sanitaria può aspettarsi un miglioramento della produttività del personale e una riduzione delle spese di capitale e operative. FlexPod offre un'infrastruttura convergente pre-validata e rigorosamente testata grazie alla partnership strategica di Cisco e NetApp. È progettato e progettato specificamente per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio offre un'esperienza utente superiore e tempi di risposta ottimali per gli utenti del sistema di imaging medicale.

Diversi componenti di un sistema di imaging medicale richiedono lo storage dei dati nei file system SMB/CIFS, NFS, Ext4 e NTFS. Pertanto, l'infrastruttura deve fornire l'accesso ai dati tramite protocolli NFS, SMB/CIFS e SAN. I sistemi di storage NetApp supportano questi protocolli da un singolo array di storage.

Disponibilità elevata, efficienza dello storage, backup rapidi pianificati basati su copie Snapshot, operazioni di ripristino rapido, replica dei dati per il disaster recovery e funzionalità dell'infrastruttura di storage FlexPod offrono un sistema di storage e gestione dei dati leader del settore.

Ulteriori informazioni

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

- Guida alla progettazione di FlexPod Datacenter per ai/ML con Cisco UCS 480 ML per l'apprendimento approfondito

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- Infrastruttura per data center FlexPod con VMware vSphere 6.7 U1, Cisco UCS di quarta generazione e NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_datacenter_vmware_netappaffa.html"

- FlexPod Datacenter: Backup di database Oracle con SnapCenter - Descrizione della soluzione

  "https://www.netapp.com/us/media/sb-3999.pdf"

- Data center FlexPod con database RAC Oracle su Cisco UCS e NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- Data center FlexPod con RAC Oracle su Oracle Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod per Microsoft SQL Server

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- FlexPod di Cisco e NetApp

  "https://flexpod.com/"

- "Soluzioni NetApp per MongoDB" Solution Brief (accesso NetApp richiesto)

  "https://fieldportal.netapp.com/content/734702"

- TR-4700: Plug-in SnapCenter per database Oracle

  "https://www.netapp.com/us/media/tr-4700.pdf"

- Documentazione sui prodotti NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- FlexPod per le soluzioni di infrastruttura di desktop virtuale (VDI)

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

Infrastruttura di desktop virtuale

Data center FlexPod con applicazioni virtuali Citrix e desktop 1912 LTSR e VMware vSphere 7 per un massimo di 6000 postazioni

Jeff Nichols, Cisco Suresh Thoppay, NetApp Dre Jackson, NetApp

Questo documento fornisce l'architettura e la progettazione di un'infrastruttura di desktop virtuale per un massimo di 6000 utenti finali. La soluzione viene virtualizzata sui server blade Cisco UCS B200 M5 di quinta generazione, avviando VMware vSphere 7.01 Update 1 tramite FC SAN dall'array di storage AFF A400. I desktop virtuali sono alimentati con Citrix Provisioning Server 1912 LTSR e Citrix RDS/Citrix Virtual Apps & Desktops 1912 LTSR, con una combinazione di desktop condivisi in hosting RDS (6000), desktop virtuali Windows 10 in pool e/o non persistenti (5000), E desktop Windows 10 virtuali ospitati in maniera persistente con provisioning di Citrix Machine Creation Services (5000) per supportare la popolazione di utenti. Ove applicabile, il documento fornisce consigli sulle Best practice e linee guida per il dimensionamento per le implementazioni di questa soluzione da parte dei clienti.

"Data center FlexPod con applicazioni virtuali Citrix desktop 1912 LTSR e VMware vSphere 7 per un massimo di 6000 postazioni"

FlexPod Datacenter con VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 e NetApp ONTAP 9.6 per un massimo di 6700 postazioni

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Questo documento fornisce un'architettura di riferimento e una guida alla progettazione per un carico di lavoro desktop da 5000 postazioni a 6000 postazioni, un ambiente di calcolo per l'utente finale su FlexPod Datacenter con Cisco UCS e NetApp AFF A300 e il software di gestione dei dati NetApp ONTAP. La soluzione include sessioni RDS Windows Server 2019 basate su server VMware Horizon, desktop virtuali Microsoft Windows 10 con clone completo persistente VMware Horizon e desktop virtuali Microsoft Windows 10 con clone istantaneo e non persistente VMware Horizon su VMware vSphere 6.7U2

"FlexPod Datacenter con VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 e NetApp ONTAP 9.6 per un massimo di 6700 postazioni"

Visualizzazione grafica 3D con Citrix e NVIDIA - White paper

Questo documento descrive le prestazioni di Citrix XenDesktop su Citrix XenServer con schede NVIDIA Tesla P4, P6 e P40 su server Cisco UCS C240 M5 e B200 M5 con

SPECviewperf 13.

"Visualizzazione grafica 3D con Citrix e NVIDIA - White paper"

FlexPod Datacenter con Citrix XenDesktop/XenApp 7.15 e VMware vSphere 6.5 Update 1 per 6000 postazioni

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

Questo documento fornisce un'architettura di riferimento per la progettazione di desktop virtuali e applicazioni che utilizzano Citrix XenApp/XenDesktop 7.15 basato su Cisco UCS con uno storage NetApp All Flash FAS (AFF) A300 e la piattaforma hypervisor VMware vSphere ESXi 6.5.

Il panorama della virtualizzazione di desktop e applicazioni sta cambiando costantemente. I nuovi server blade Cisco UCS M5 dalle performance elevate e il fabric unificato Cisco UCS, combinati come parte dell'infrastruttura comprovata di FlexPod, con lo storage NetApp AFF di ultima generazione, offrono una piattaforma più compatta, potente, affidabile ed efficiente.

"FlexPod Datacenter con Citrix XenDesktop/XenApp 7.15 e VMware vSphere 6.5 Update 1 per 6000 postazioni"

FlexPod Datacenter con VMware Horizon View 7.3 e VMware vSphere 6.5 Update 1 con Cisco UCS Manager 3.2 per 5000 postazioni

Ramesh Guduru, Cisco David Arnette, NetApp

Questo documento fornisce un'architettura di riferimento, una guida alla progettazione e un'implementazione per un ambiente di calcolo per l'utente finale con un massimo di 5000 postazioni e workload misti su FlexPod Datacenter con Cisco UCS e storage NetApp All Flash FAS (AFF) A300. La soluzione include sessioni host di server desktop remoto basate su server VMware Horizon, desktop virtuali persistenti Microsoft Windows 10 VMware Horizon e desktop virtuali clonati istantanei Microsoft Windows 10 non persistenti VMware Horizon su VMware vSphere 6.5.

"FlexPod Datacenter con VMware Horizon View 7.3 e VMware vSphere 6.5 Update 1 con Cisco UCS Manager 3.2 per 5000 postazioni"

FlexPod Datacenter con VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 e NetApp ONTAP 9.6 per un massimo di 6700 postazioni

Vadim Lebedev, Cisco Suresh Thoppay, NetApp

Questo documento fornisce un'architettura di riferimento e una guida alla progettazione per un ambiente di elaborazione per l'utente finale con workload da 5000 postazioni a

6000 postazioni su FlexPod Datacenter con Cisco UCS e NetApp AFF A300 e il software per la gestione dei dati NetApp ONTAP. La soluzione include sessioni RDS Windows Server 2019 basate su server VMware Horizon, desktop virtuali persistenti e cloni completi VMware Horizon Microsoft Windows 10 e desktop virtuali VMware Horizon non persistenti e con clonazione istantanea Microsoft Windows 10 su VMware vSphere 6.7 U2.

"FlexPod Datacenter con VMware Horizon View 7.10, VMware vSphere 6.7 U2, Cisco UCS Manager 4.0 e NetApp ONTAP 9.6 per un massimo di 6700 postazioni"

Applicazioni moderne

Data center FlexPod per ai e ML combinati con Cisco UCS 480 ML per deep learning - progettazione

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Questo documento fornisce dettagli di progettazione sull'integrazione della piattaforma Cisco UCS C480 ML M5 nella soluzione FlexPod Datacenter per offrire un approccio unificato per fornire funzionalità ai e ML all'interno dell'infrastruttura convergente. Offrendo ai clienti la possibilità di gestire i server con funzionalità combinate di ai e ML con gli strumenti familiari che utilizzano per amministrare i sistemi FlexPod tradizionali, l'overhead amministrativo e il costo di implementazione della piattaforma di deep learning sono notevolmente ridotti. Il design presentato in questo CVD include anche altre piattaforme Cisco UCS come il server C220 M5 con due GPU NVIDIA T4 e il server C240 M5 dotato di due schede NVIDIA V100 32GB PCIe come opzioni aggiuntive per la gestione simultanea di carichi di lavoro ai e ML.

"Data center FlexPod per ai e ML combinati con Cisco UCS 480 ML per deep learning - progettazione"

Implementa il plug-in NetApp Trident CSI sulla piattaforma container Cisco con FlexPod

Questo documento fornisce procedure dettagliate per l'implementazione del plug-in NetApp Trident Container Storage Interface (CSI) su un cluster tenant Kubernetes della piattaforma container Cisco in una soluzione FlexPod.

"Implementa il plug-in NetApp Trident CSI sulla piattaforma container Cisco con FlexPod"

Data center FlexPod per piattaforma container OpenShift 4 - implementazione

Haseeb Niazi, Cisco Alan Cowles, NetApp

Red Hat OpenShift è una piattaforma container Kubernetes pronta per le aziende per gestire le implementazioni di cloud ibrido e multi-cloud. Red Hat OpenShift Container Platform include tutto il necessario per lo sviluppo e le implementazioni di cloud ibrido, container Enterprise e Kubernetes. Include un sistema operativo Linux di livello Enterprise, runtime container, networking, monitoraggio, registro container, soluzioni di autenticazione e autorizzazione.

La combinazione di Red Hat OpenShift con la soluzione FlexPod Datacenter può semplificare l'implementazione e la gestione dell'infrastruttura container. I clienti possono beneficiare di una maggiore efficienza, di una migliore protezione dei dati, di una riduzione dei rischi e della flessibilità necessaria per scalare questo stack di infrastrutture Enterprise altamente disponibili per soddisfare i nuovi requisiti di business. L'approccio alle soluzioni convergenti pre-validate aiuta le organizzazioni a raggiungere la velocità,

la flessibilità e la scalabilità richieste per tutte le iniziative di modernizzazione delle applicazioni e di trasformazione digitale.

"Data center FlexPod per piattaforma container OpenShift 4 - implementazione"

Data center FlexPod con Docker Enterprise Edition per la gestione dei container

Muhammad Afzal, Cisco John George, Cisco Amit Borulkar, NetApp Uday Shetty, Docker

Docker è la piattaforma di container software leader a livello mondiale per sviluppatori e operazioni IT per creare, spedire ed eseguire applicazioni distribuite ovunque. Con l'architettura dei microservizi che sta plasmando l'IT di prossima generazione, le aziende con grandi investimenti in applicazioni monolitiche stanno trovando modi per adottare Docker come strategia per modernizzare le proprie architetture applicative e mantenere l'organizzazione competitiva e conveniente. La containerizzazione offre l'agilità, il controllo e la portabilità richiesti dagli sviluppatori e dalle operazioni IT per creare e implementare le applicazioni in qualsiasi infrastruttura. La piattaforma Docker consente di comporre facilmente le applicazioni distribuite in un contenitore di applicazioni leggero che può cambiare dinamicamente e senza interruzioni. Questa funzionalità rende le applicazioni portatili in ambienti di sviluppo, test e produzione eseguiti su macchine fisiche o virtuali a livello locale, nei data center e nelle reti di diversi provider di servizi cloud.

"Data center FlexPod con Docker Enterprise Edition per la gestione dei container"

Data center FlexPod per piattaforma container OpenShift 4 - progettazione

Haseeb Niazi, Cisco Alan Cowles, NetApp

Cisco e NetApp hanno collaborato per offrire una serie di soluzioni FlexPod che consentono piattaforme strategiche per data center. La soluzione FlexPod offre un'architettura integrata che incorpora Best practice per il computing, lo storage e la progettazione di rete, riducendo al minimo i rischi PER L'IT convalidando l'architettura integrata per garantire la compatibilità tra i vari componenti. La soluzione affronta anche i punti critici DELL'IT fornendo una guida documentata alla progettazione, una guida all'implementazione e un supporto che possono essere utilizzati in varie fasi (pianificazione, progettazione e implementazione) di un'implementazione.

"Data center FlexPod per piattaforma container OpenShift 4 - progettazione"

Data center FlexPod per l'ai e L'ML combinati con Cisco UCS 480 ML per l'apprendimento approfondito - implementazione

Haseeb Niazi, Cisco Arvind Ramakrishnan, NetApp

Questo documento fornisce dettagli sull'implementazione e indicazioni sull'integrazione della piattaforma Cisco UCS C480 ML M5 nella soluzione per data center FlexPod per offrire un approccio unificato per fornire funzionalità ai e ML all'interno dell'infrastruttura convergente. Questo documento spiega anche la configurazione delle GPU NVIDIA sulle piattaforme Cisco UCS C220 e C240. Per una discussione dettagliata sulla progettazione delle piattaforme e delle tecnologie utilizzate in questa soluzione, fare riferimento a. "Data center FlexPod per l'ai e L'ML combinati con Cisco UCS 480 ML per un design di deep learning".

"Data center FlexPod per l'ai e L'ML combinati con Cisco UCS 480 ML per l'apprendimento approfondito - implementazione"

Visualizzazione grafica 3D con VMware e NVIDIA su Cisco UCS - White paper

Questo documento descrive le prestazioni dell'hypervisor VMware ESXi e della soluzione VMware Horizon con NVIDIA Tesla P4, P6 e P40 sui server rack Cisco UCS C240 M5 e sui server blade B200 M5.

"Visualizzazione grafica 3D con VMware e NVIDIA su Cisco UCS - White paper"

Visualizzazione grafica 3D con Citrix e NVIDIA - White paper

Questo documento descrive le prestazioni di Citrix XenDesktop su Citrix XenServer con schede NVIDIA Tesla P4, P6 e P40 su server Cisco UCS C240 M5 e B200 M5 con SPECviewperf 13.

"Visualizzazione grafica 3D con Citrix e NVIDIA - White paper"

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:

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."

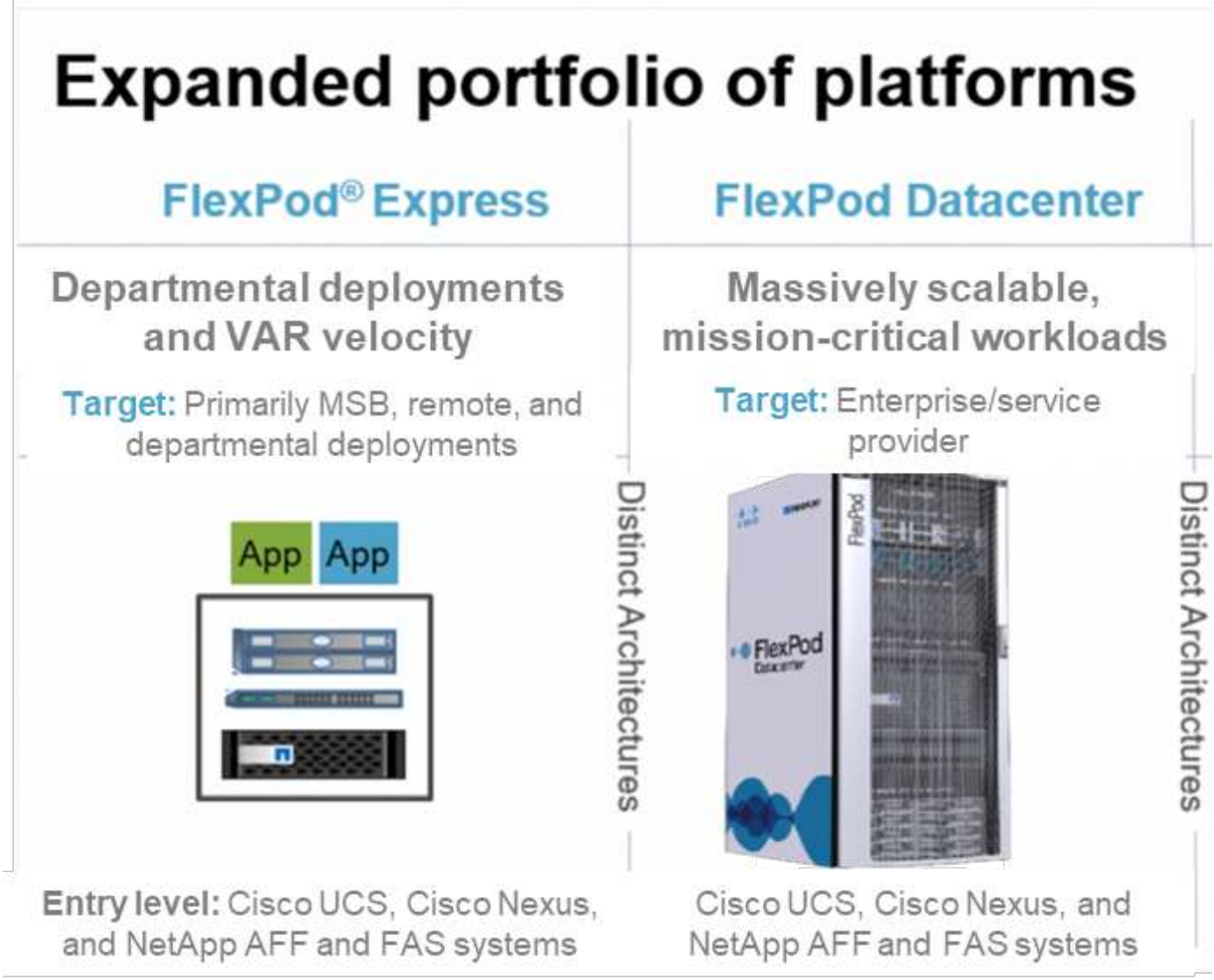
Riepilogo del programma

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.



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:

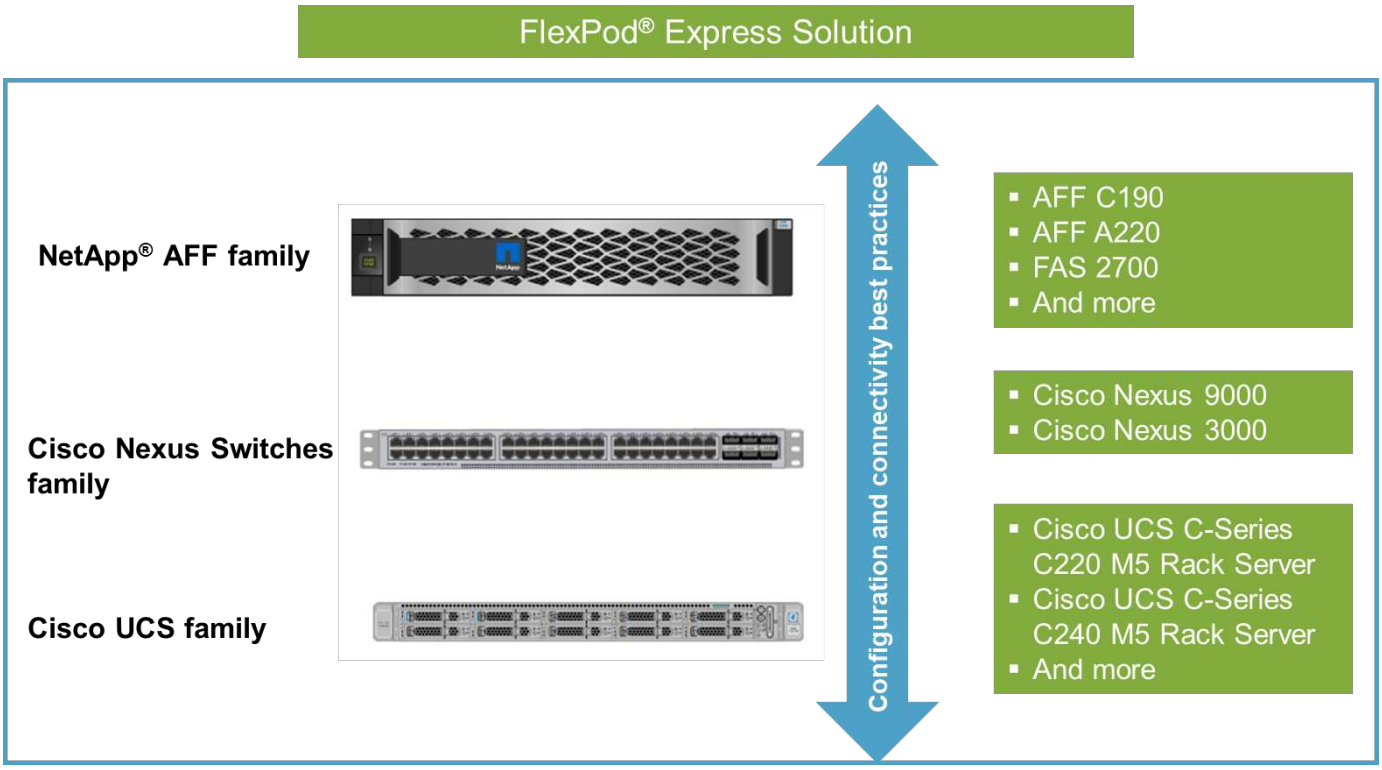
- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione
- Accelera il time-to-market questa guida illustra in dettaglio la progettazione di FlexPod con VMware vSphere.

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.

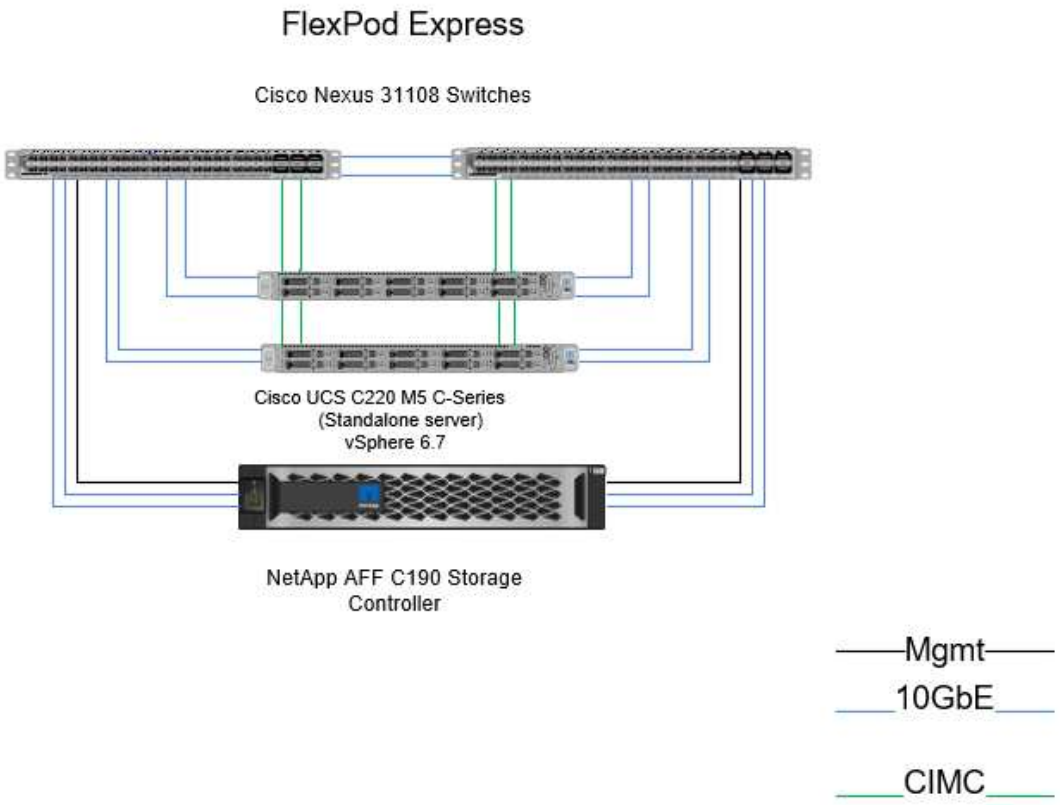


Pubblico di riferimento

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.



"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

Hardware	Quantità
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:

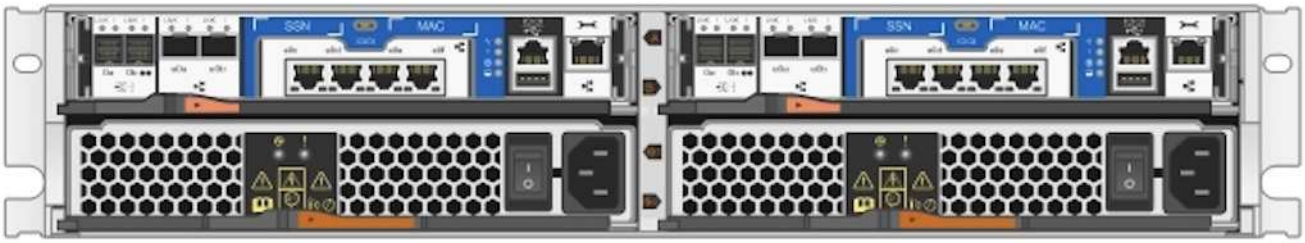
- CIFS, NFS, iSCSI e FCP
- Software di replica dei dati NetApp SnapMirror, software di backup NetApp SnapVault, software di ripristino dei dati NetApp SnapRestore, suite di prodotti software per la gestione dello storage NetApp SnapManager e software NetApp SnapCenter

- 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+.

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



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:

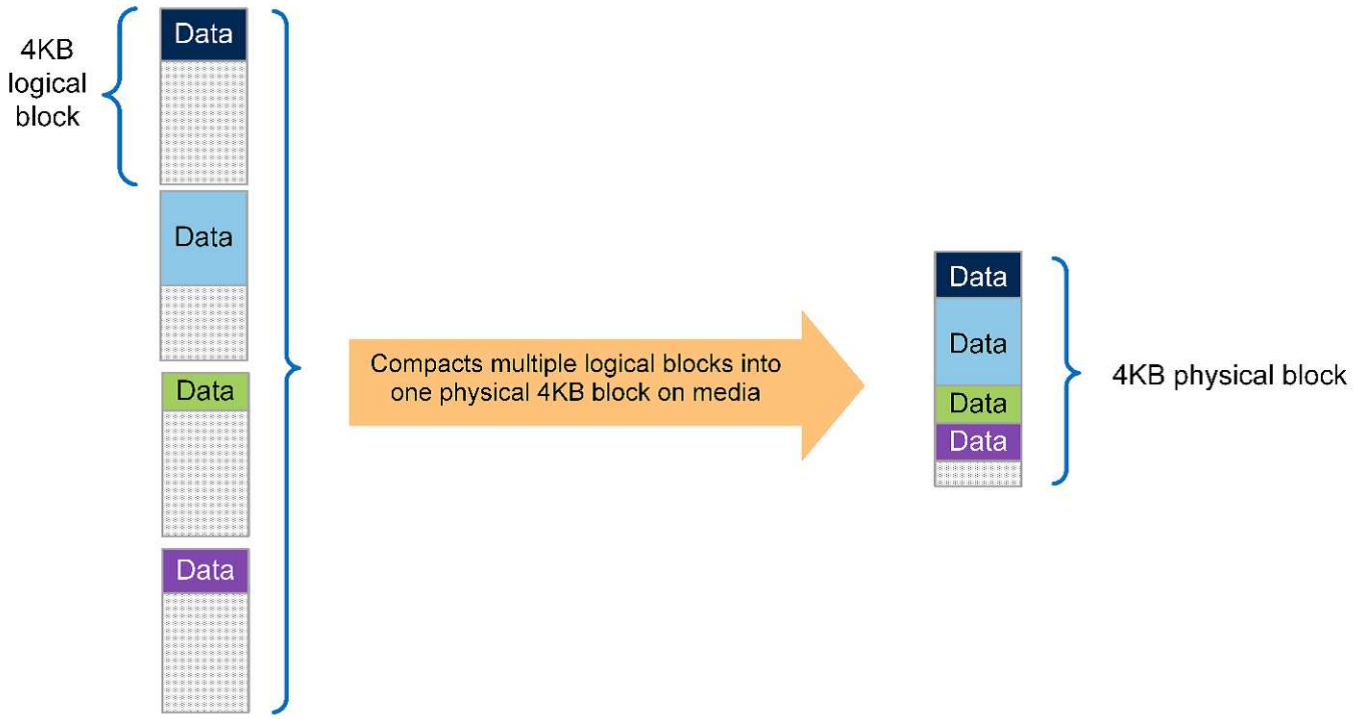
- 8x 960 GB
- 12x 960 GB
- 18x 960 GB
- 24x 960 GB

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.



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.

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

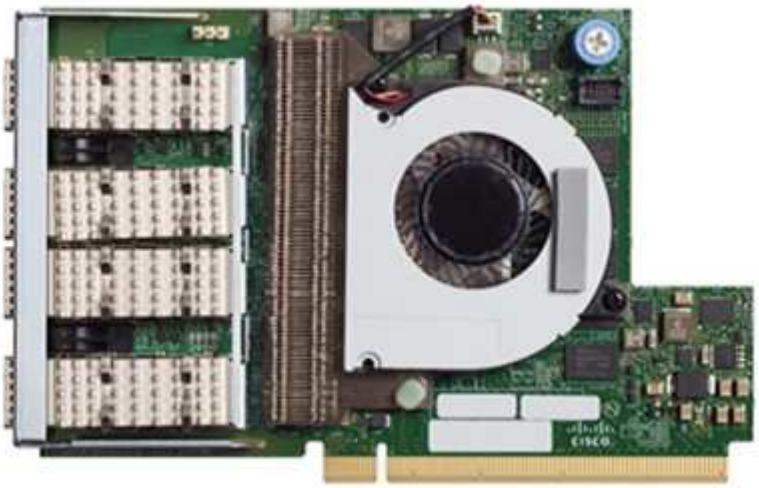
Il server rack Cisco UCS C220 M5, mostrato nella figura precedente, è tra i server per applicazioni e infrastrutture aziendali generici più versatili del settore. Si tratta di un server rack a due socket ad alta densità che offre performance ed efficienza leader di settore per un'ampia gamma di carichi 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.



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:

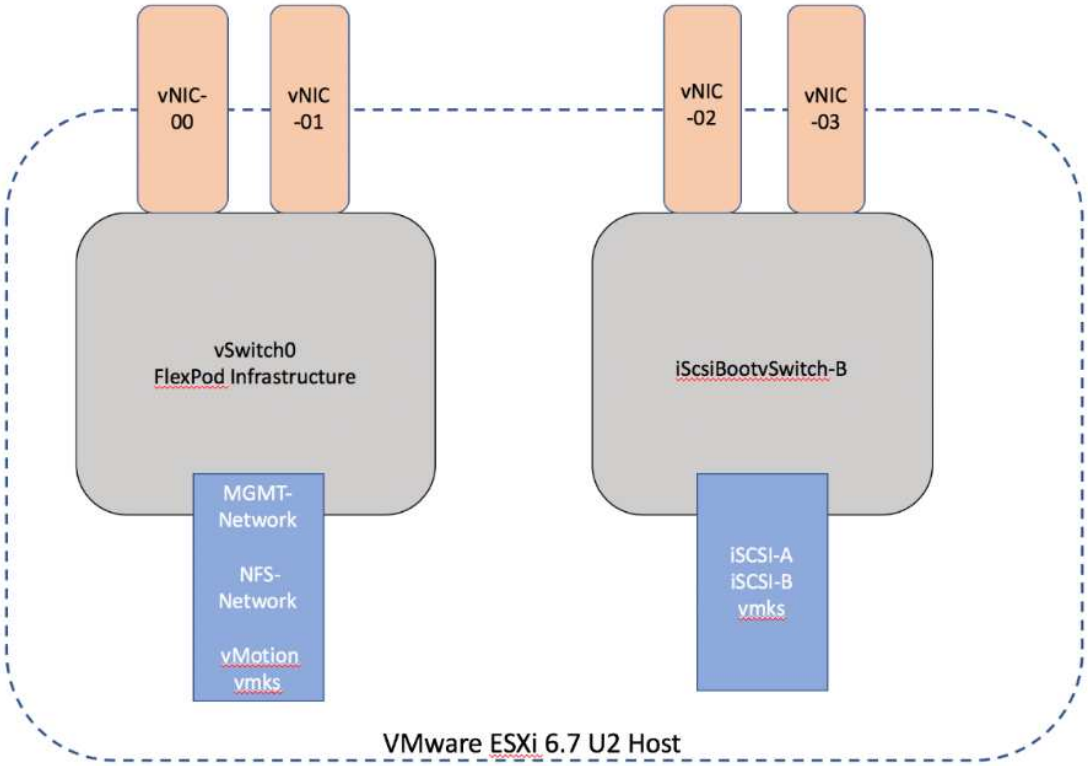
- LUN SAN iSCSI
- Scheda SD Cisco FlexFlash
- Disco locale

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.



"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"

- Pagina delle risorse di documentazione di AFF

  "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"

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.

Programma NetApp Verified Architecture

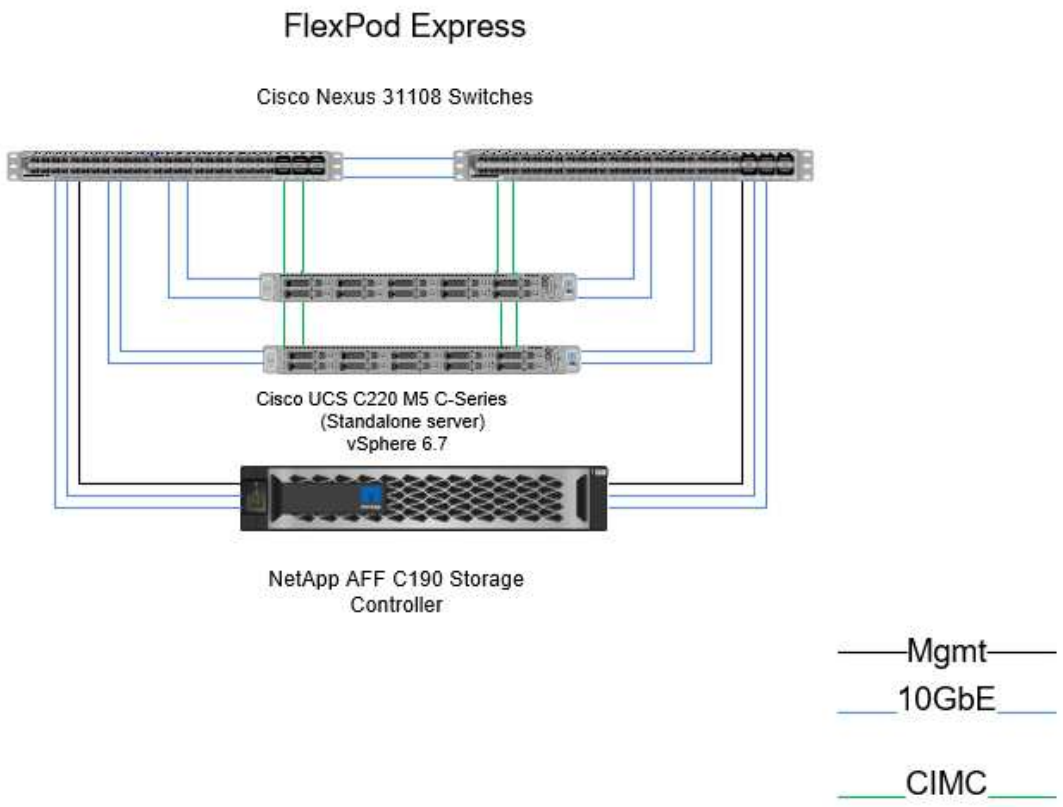
Il programma NetApp Verified Architecture offre ai clienti un'architettura verificata per le soluzioni NetApp. Un'architettura verificata di NetApp offre un'architettura della soluzione NetApp con le seguenti qualità:

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

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

Tecnologia della soluzione

Questa soluzione sfrutta le più recenti tecnologie di NetApp, Cisco e VMware. Questa soluzione include il nuovo NetApp AFF C190 con ONTAP 9.6, due switch Cisco Nexus 31108 e server rack Cisco UCS C220 M5 con VMware vSphere 6.7U2. Questa soluzione validata utilizza la tecnologia 10 GbE. Viene inoltre fornita una guida su come scalare la capacità di calcolo aggiungendo due nodi hypervisor alla volta, in modo che l'architettura FlexPod Express possa adattarsi alle esigenze di business in evoluzione di un'organizzazione.



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

Riepilogo del caso d'utilizzo

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

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

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

- Nuovo supporto del protocollo per il backup e il ripristino di un'appliance server vCenter, inclusi HTTP,

HTTPS, FTP, FTPS, SCP, NFS E SMB.

- Nuovo dal punto di vista funzionale quando si utilizza la libreria di contenuti. La sincronizzazione dei modelli VM nativi tra le librerie di contenuti è ora disponibile quando vCenter Server è configurato per la modalità link avanzata.
- Una pagina aggiornata del plug-in del client.
- Miglioramenti aggiunti in vSphere Update Manager (VUM) e nel client vSphere. È ora possibile eseguire le azioni di collegamento, verifica della conformità e correzione, il tutto da un'unica schermata.

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

Requisiti tecnologici

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

Requisiti hardware

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

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

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

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

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

Requisiti software

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

Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	4.0.4	Per server rack Cisco UCS C220 M5
Driver Cisco Nenic	1.0.0.29	Per le schede di interfaccia VIC 1457
Sistema operativo Cisco NX	7.0(3)I7(6)	Per switch Cisco Nexus 31108PC-V.
NetApp ONTAP	9.6	Per controller AFF C190

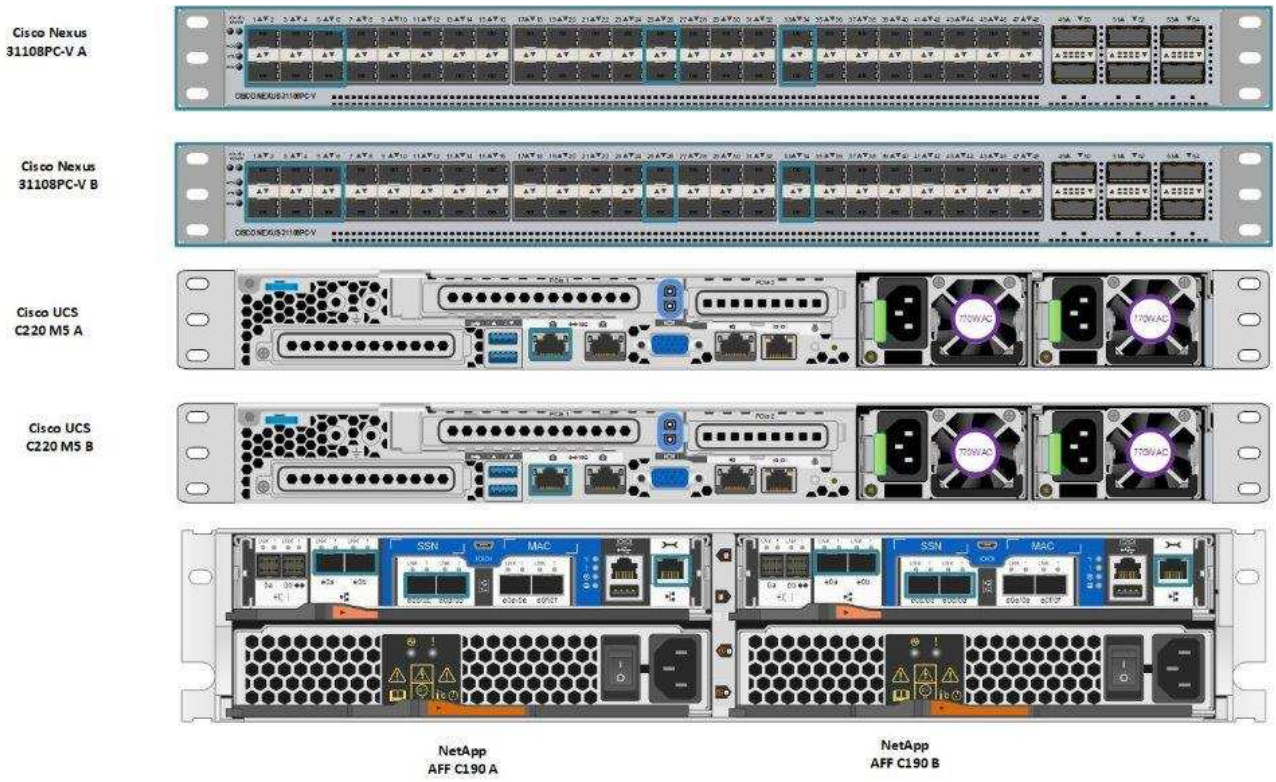
Questa tabella elenca il software necessario per tutte le implementazioni di VMware vSphere su FlexPod Express.

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

Informazioni di cablaggio FlexPod Express

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

Questa figura mostra il cablaggio di convalida di riferimento.



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

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

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

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

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

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

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

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

Procedure di implementazione

Panoramica

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

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

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

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

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

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

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

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

In questa convalida sono stati creati due vSwitch.

La seguente tabella elenca i vSwitch della soluzione.

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

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

La tabella seguente elenca le macchine virtuali VMware create.

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

Implementare Cisco Nexus 31108PC-V.

Questa sezione descrive in dettaglio la configurazione dello switch Cisco Nexus 331108PC-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? (y
es/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

Eseguire 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).

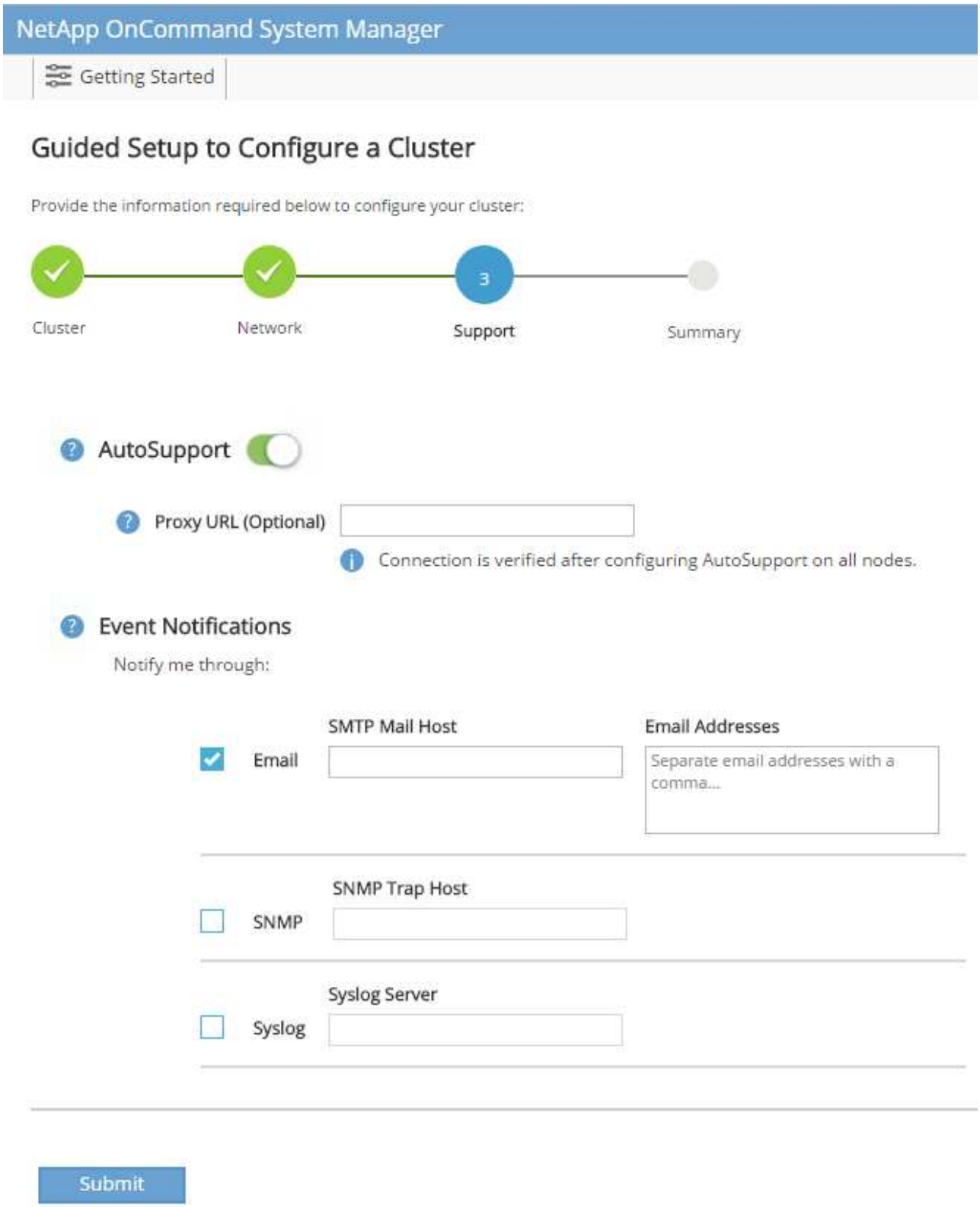
> È inoltre possibile inserire un server NTP alternativo. L'indirizzo IP `10.63.172.162` da `<<var_ntp_server_ip>>` È l'IP di gestione Nexus.

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.



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
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. 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,fcp
```

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

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

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

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

> I comandi sono preceduti da `vserver` Nella riga di comando perché le 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	[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 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 -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

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

8. Ripristinare il livello di privilegio admin e creare la configurazione per consentire 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.

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>>`

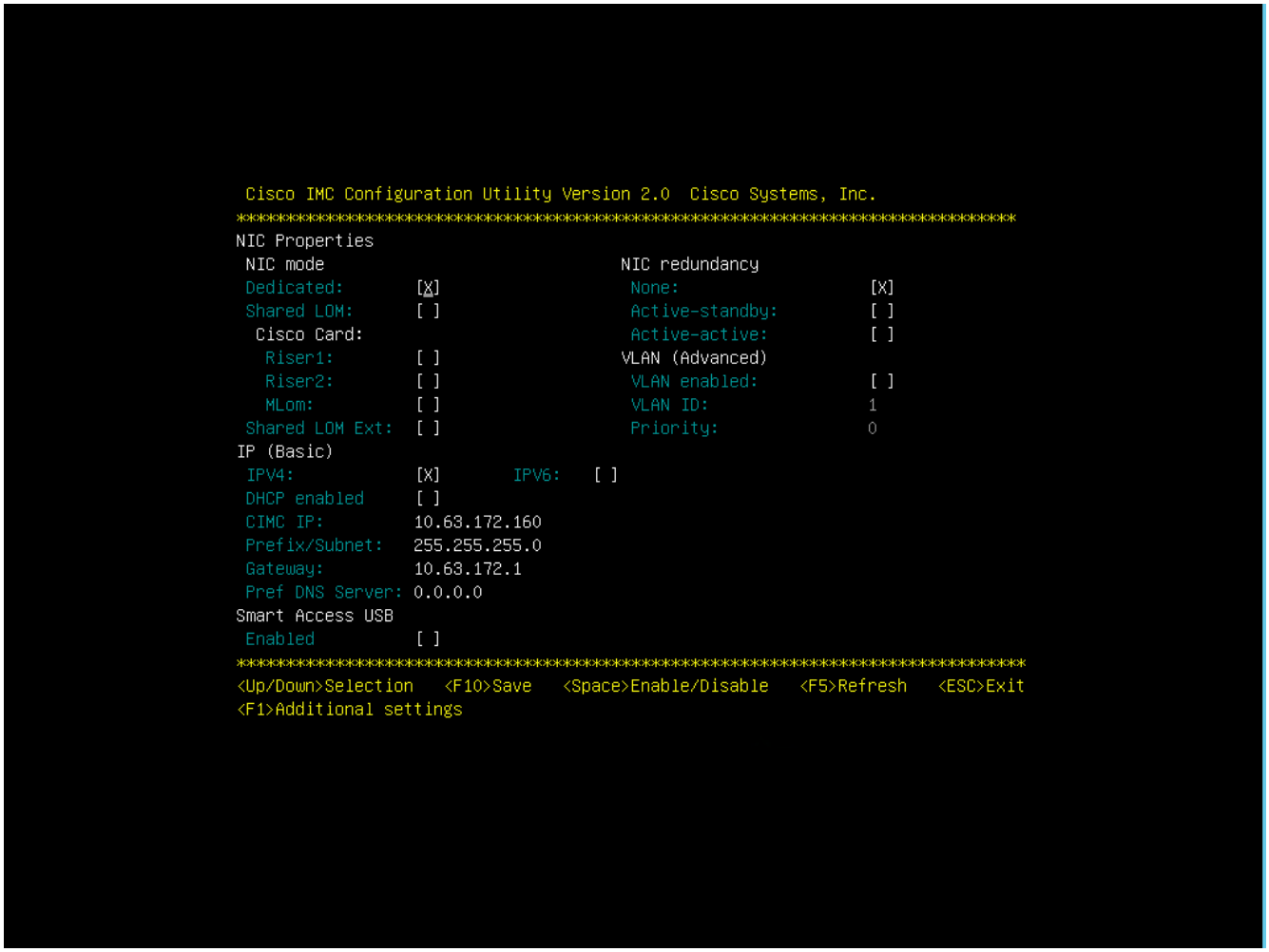
      Prefisso/sottorete: `<<cimc_netmask>>`

      Gateway: `<<cimc_gateway>>`

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

      Ridondanza della NIC

      Nessuno: `[X]`



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.

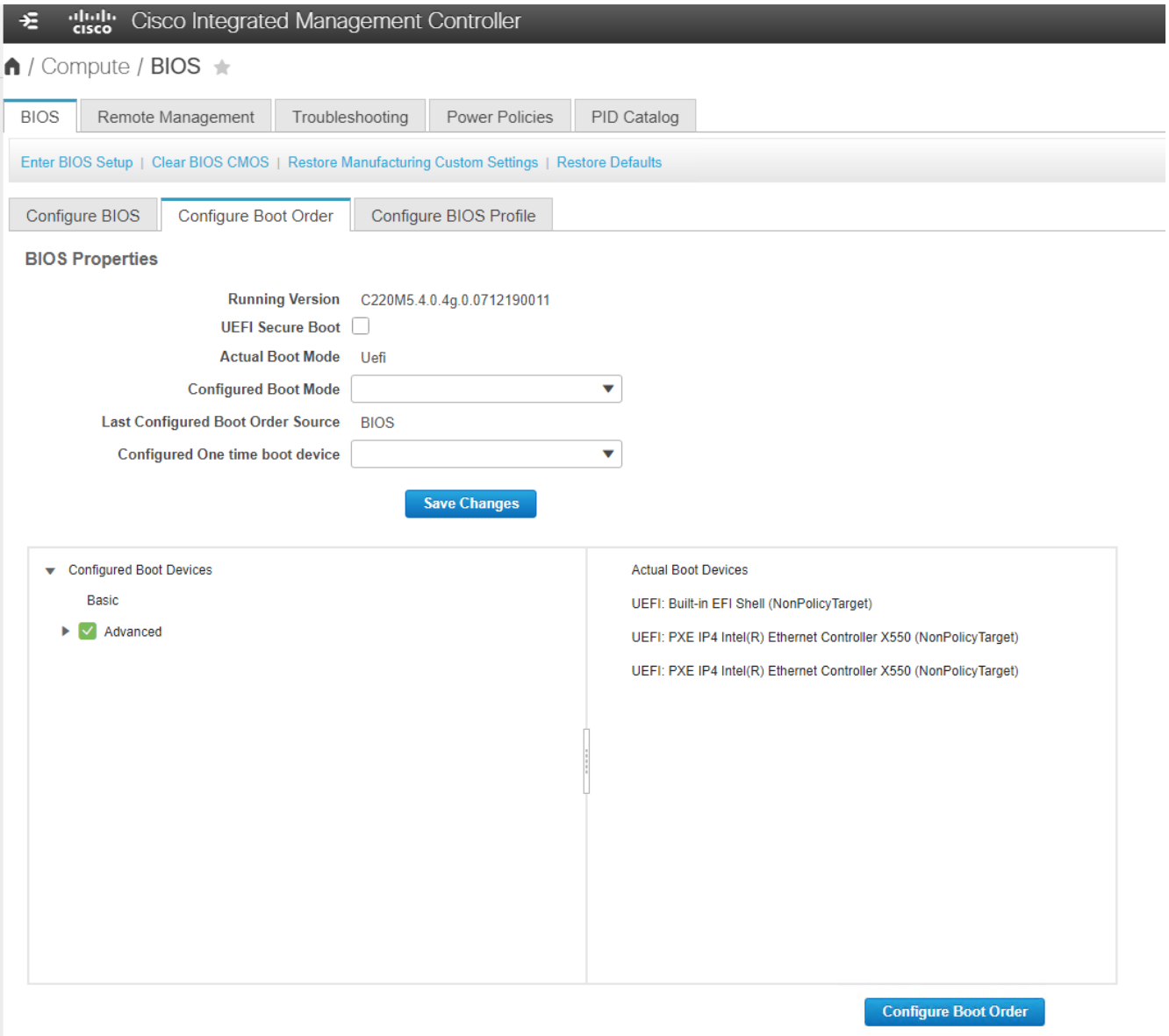
> Un font corsivo indica le variabili univoche per ogni host ESXi.

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.



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.

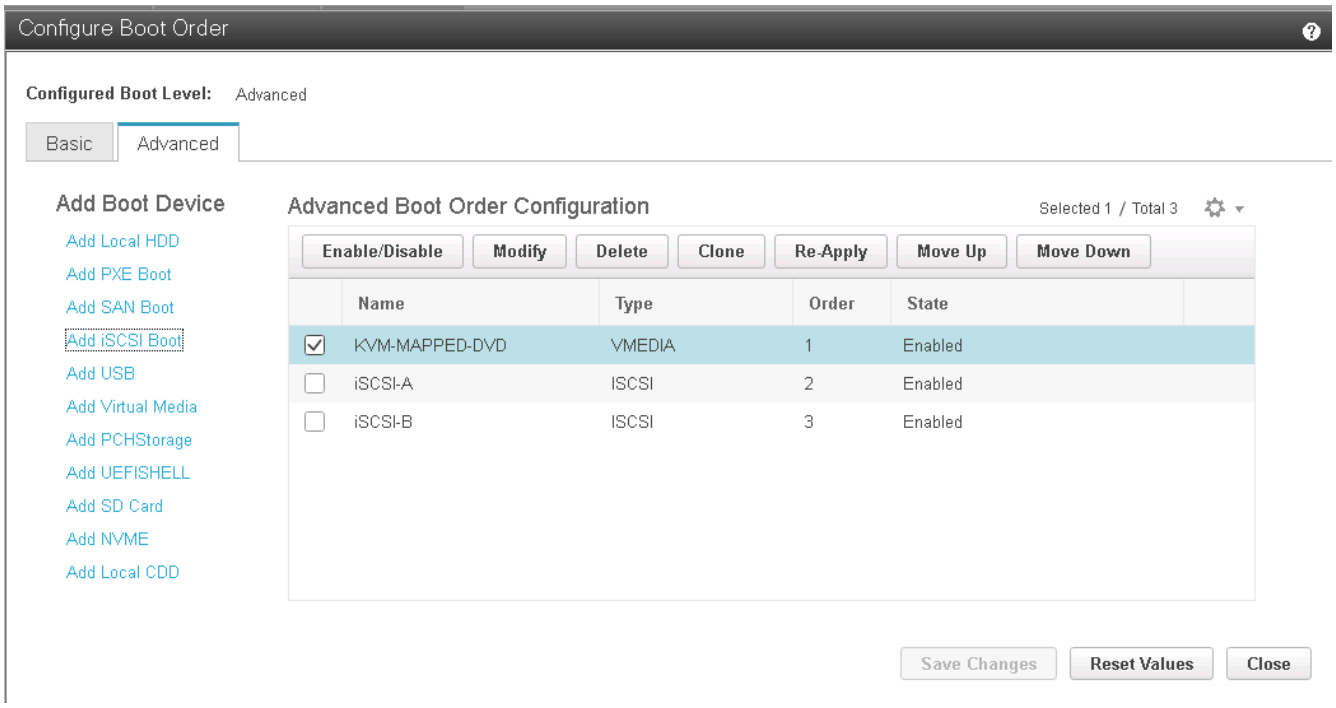
Stato: Attivato

Ordine: 3

Slot: MLOM

Porta: 3

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

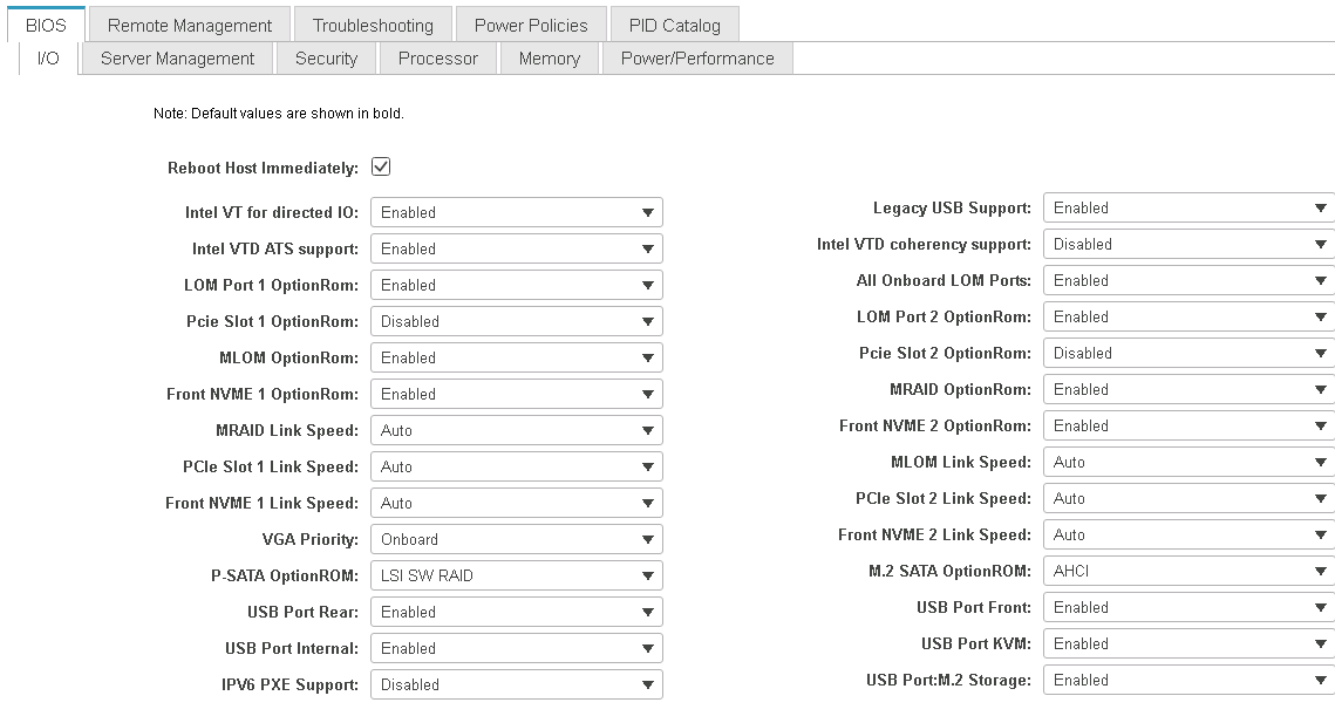


6. Riavviare il server per eseguire l'avvio con il nuovo ordine di avvio.

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).

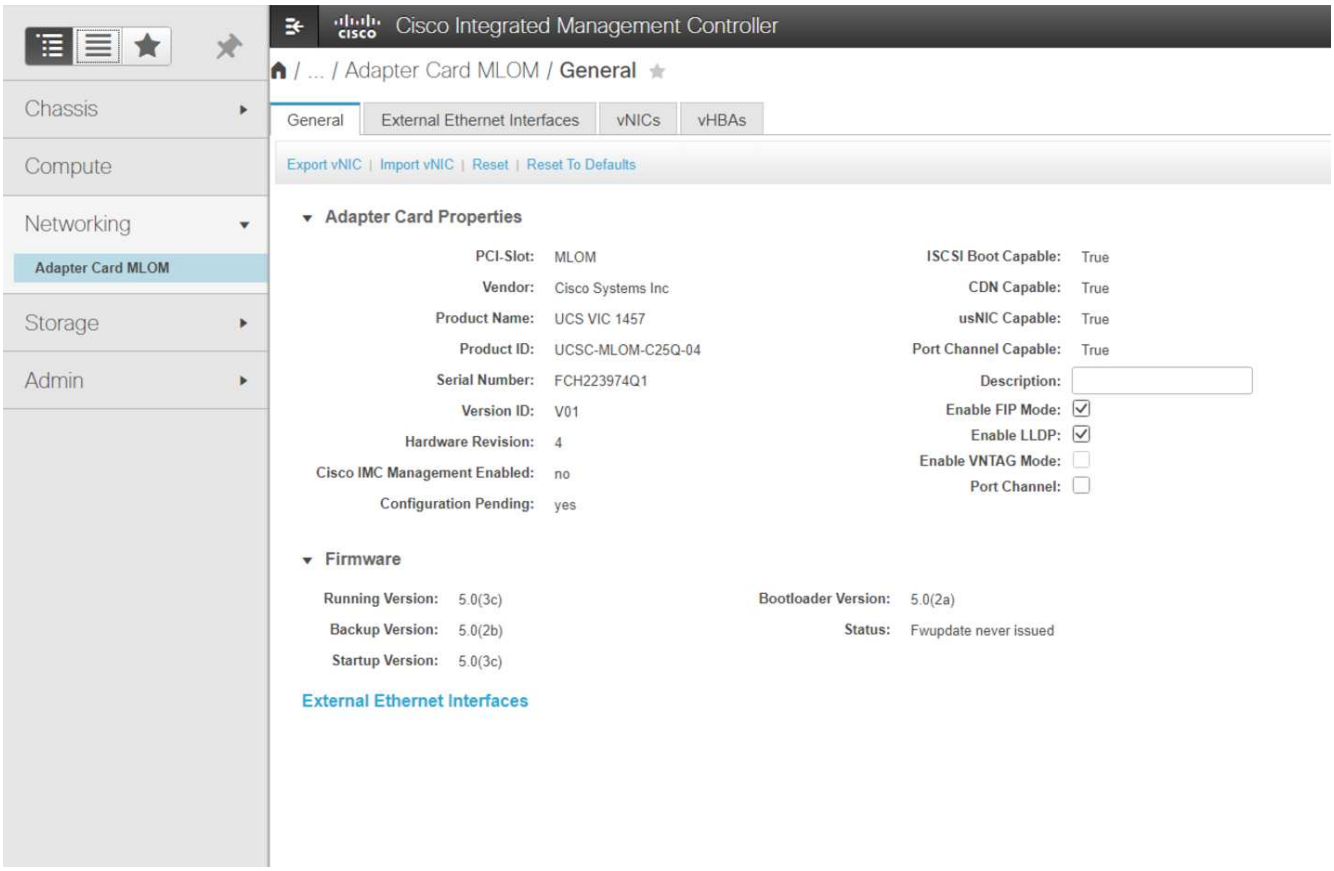


Configurare Cisco VIC1457 per l'avvio iSCSI

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:

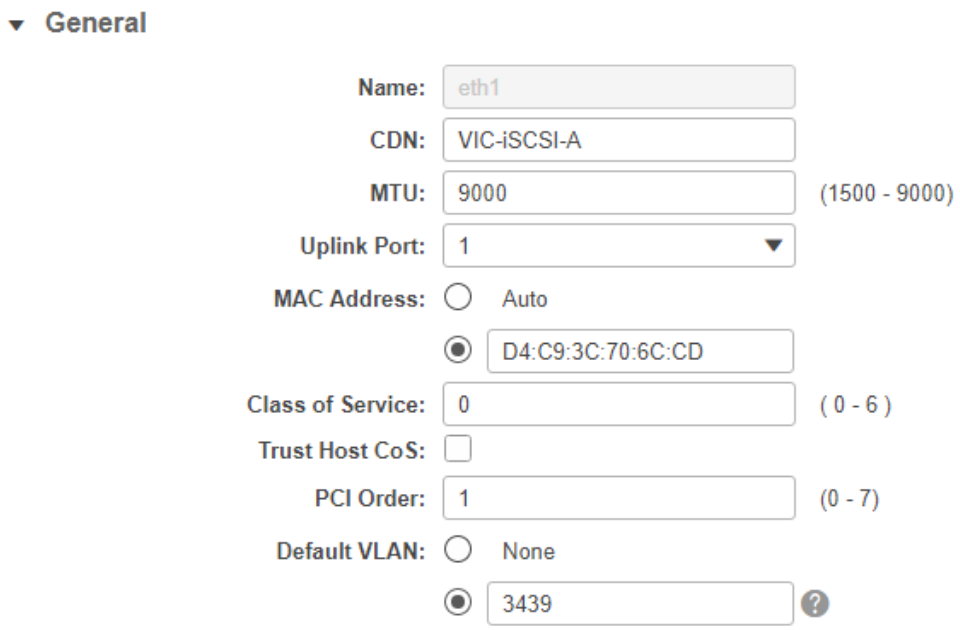
1. Nella scheda rete, fare clic su MLOM scheda adattatore.
2. Nella scheda General (Generale), deselezionare il canale della porta.
3. Salvare le modifiche e riavviare CIMC.



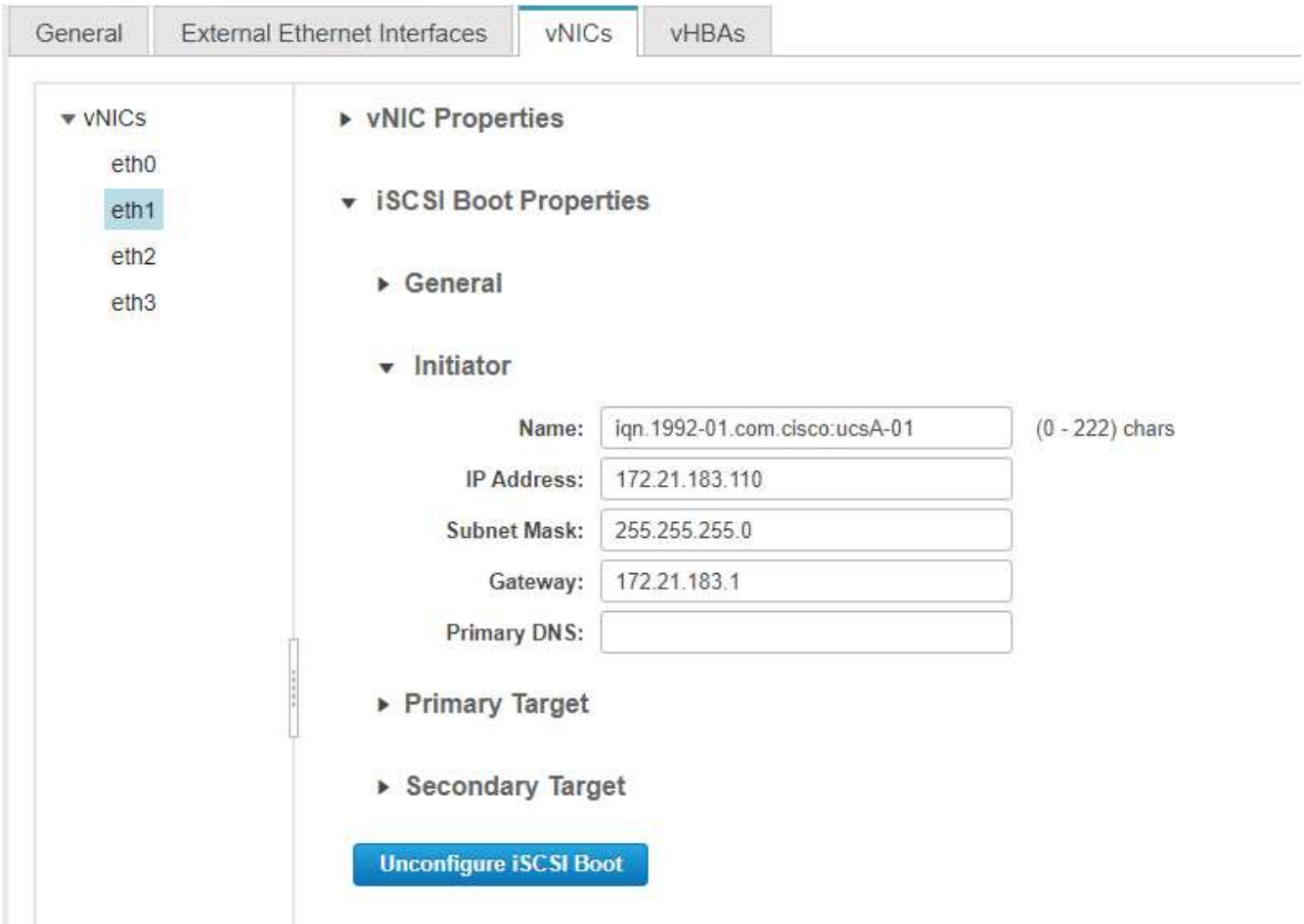
Creare vNIC iSCSI

Per creare vNIC iSCSI, attenersi alla seguente procedura:

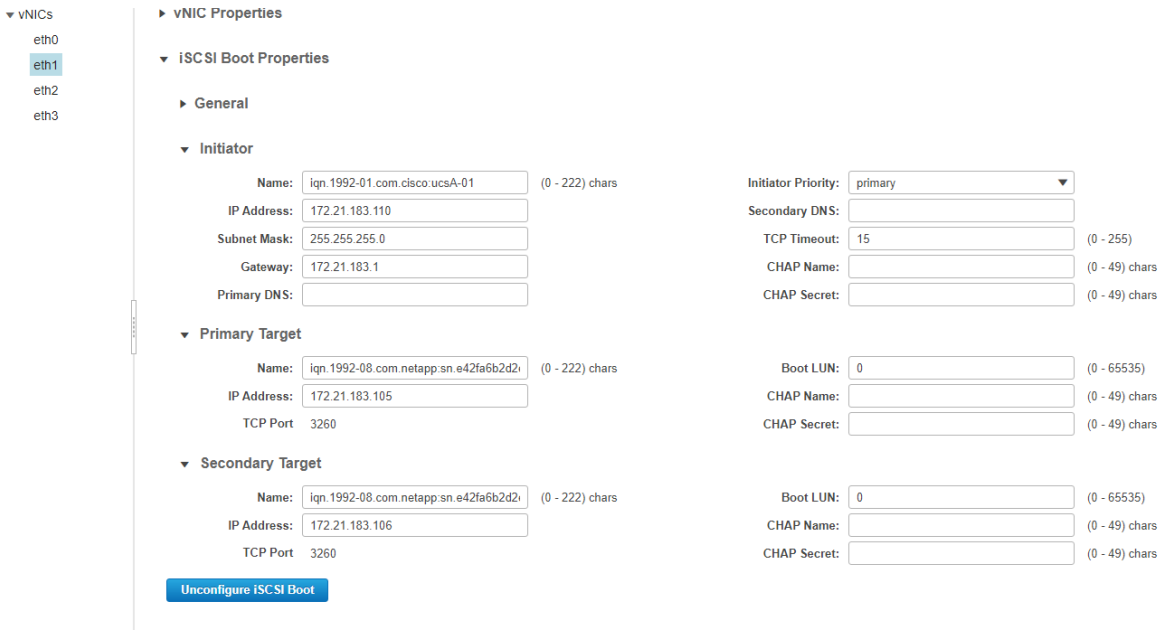
1. Nella scheda rete, fare clic su scheda adattatore MLOM.
2. Fare clic su Add vNIC (Aggiungi vNIC) per creare una vNIC.
3. Nella sezione Add vNIC (Aggiungi vNIC), immettere le seguenti impostazioni:
    - Nome: Eth1
    - Nome CDN: ISCSI-vNIC-A.
    - MTU: 9000
    - VLAN predefinita: `<<var_iscsi_vlan_a>>`
    - 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.



6. Selezionare la vNIC eth1 a sinistra.



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>>`



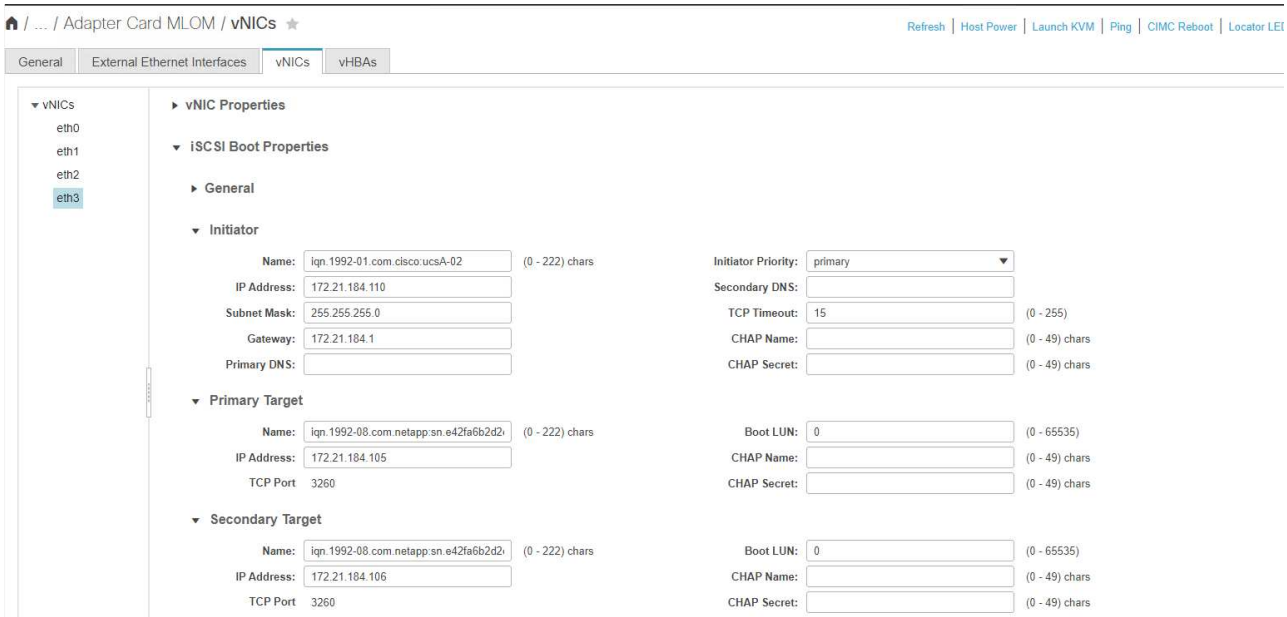
8. Inserire i dettagli principali del target:
    - Name (Nome): Numero IQN di infra-SVM
    - IP address (Indirizzo IP): Indirizzo IP di iscsi_lif01a
    - LUN di boot: 0
9. Inserire i dettagli del target secondario:
    - Name (Nome): Numero IQN di infra-SVM
    - IP address (Indirizzo IP): Indirizzo 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>>`



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.

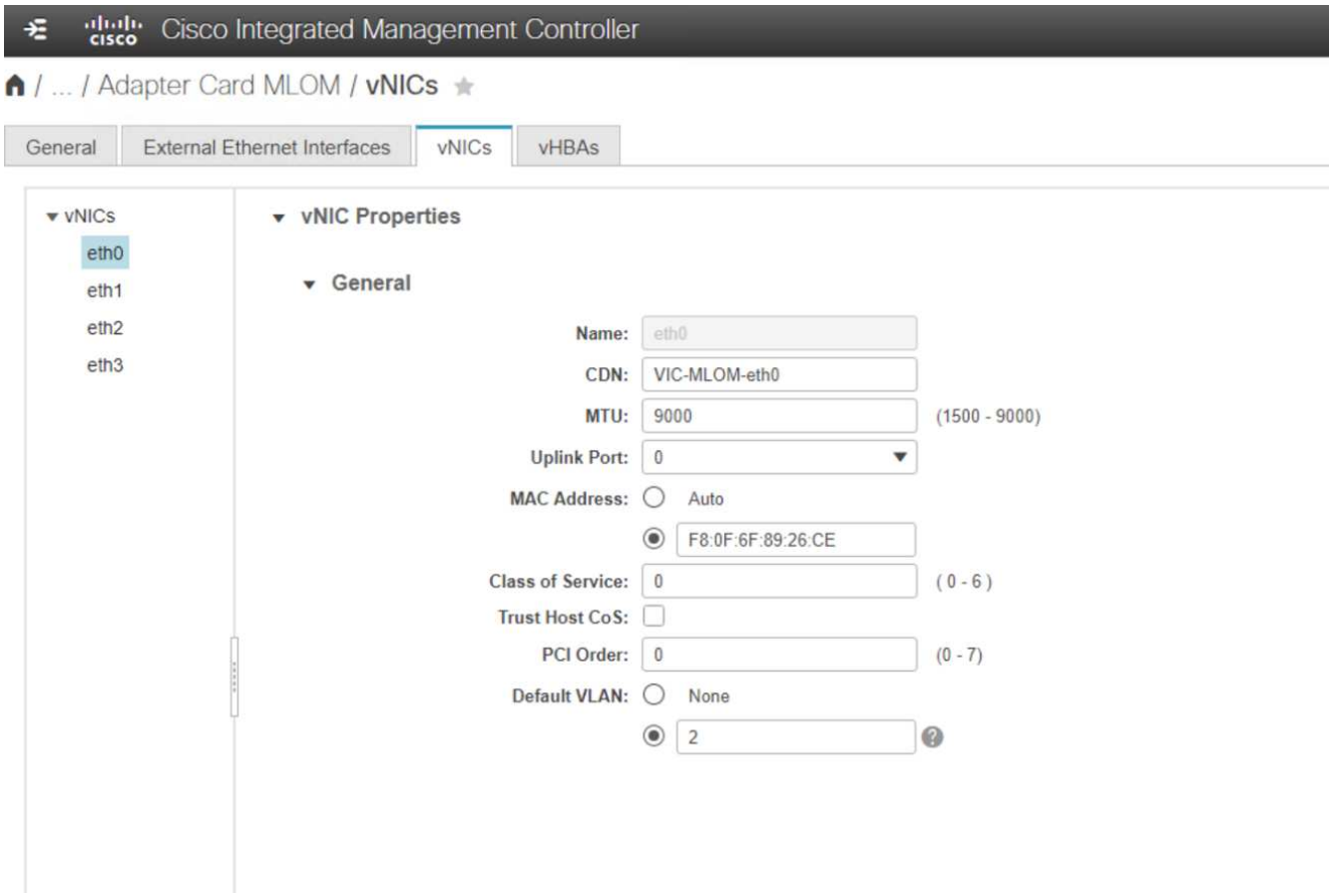
> Assicurarsi di registrare i nomi IQN per ogni vNIC. Sono necessari per un passaggio successivo.

16. Fare clic su Salva modifiche.
17. Ripetere questa procedura per configurare l'avvio iSCSI per il server Cisco UCS B.

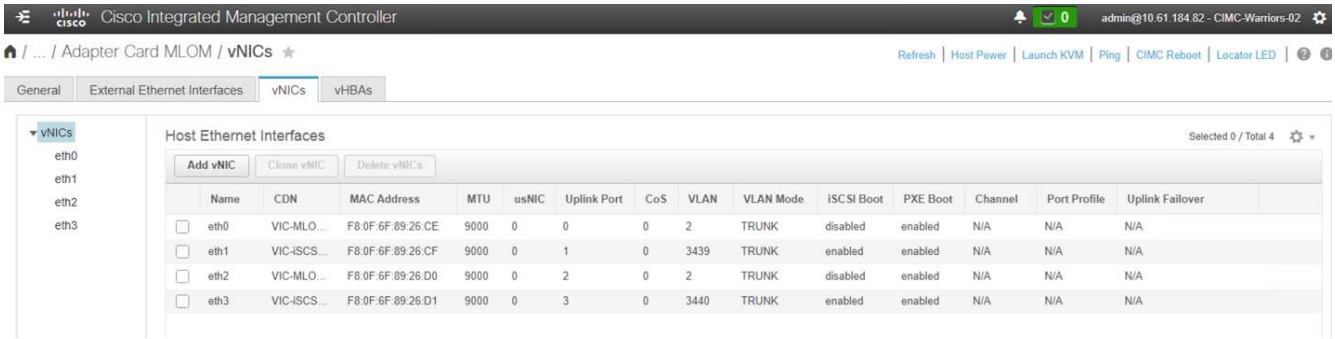
Configurare vNIC per ESXi

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.



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



Questa procedura deve essere ripetuta per ogni nodo iniziale 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.

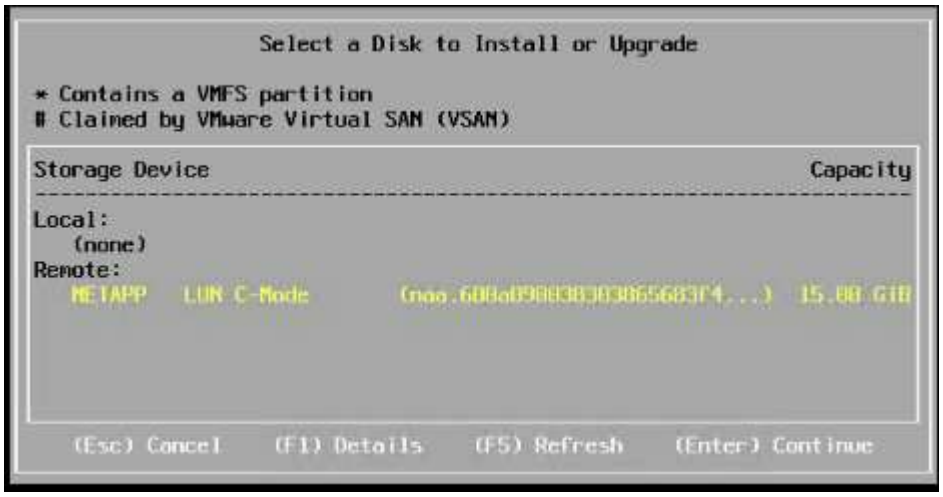
Installare VMware ESXi

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.



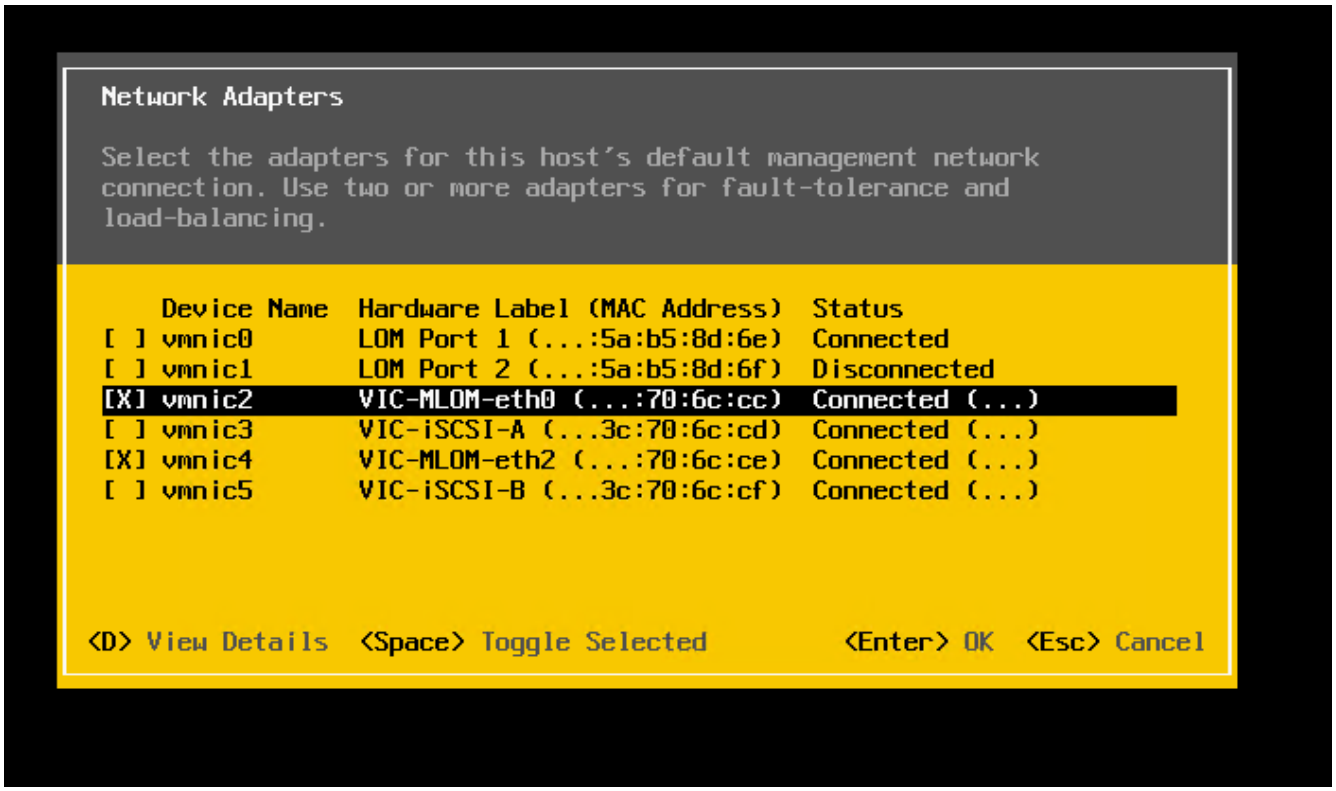
9. Selezionare il layout di tastiera appropriato e premere Invio.
10. Inserire e confermare la password root e premere Invio.
11. Il programma di installazione avvisa che le partizioni esistenti vengono rimosse nel volume. Continuare con l'installazione premendo F11. Il server si riavvia dopo l'installazione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



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 deselezionando 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. 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

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.

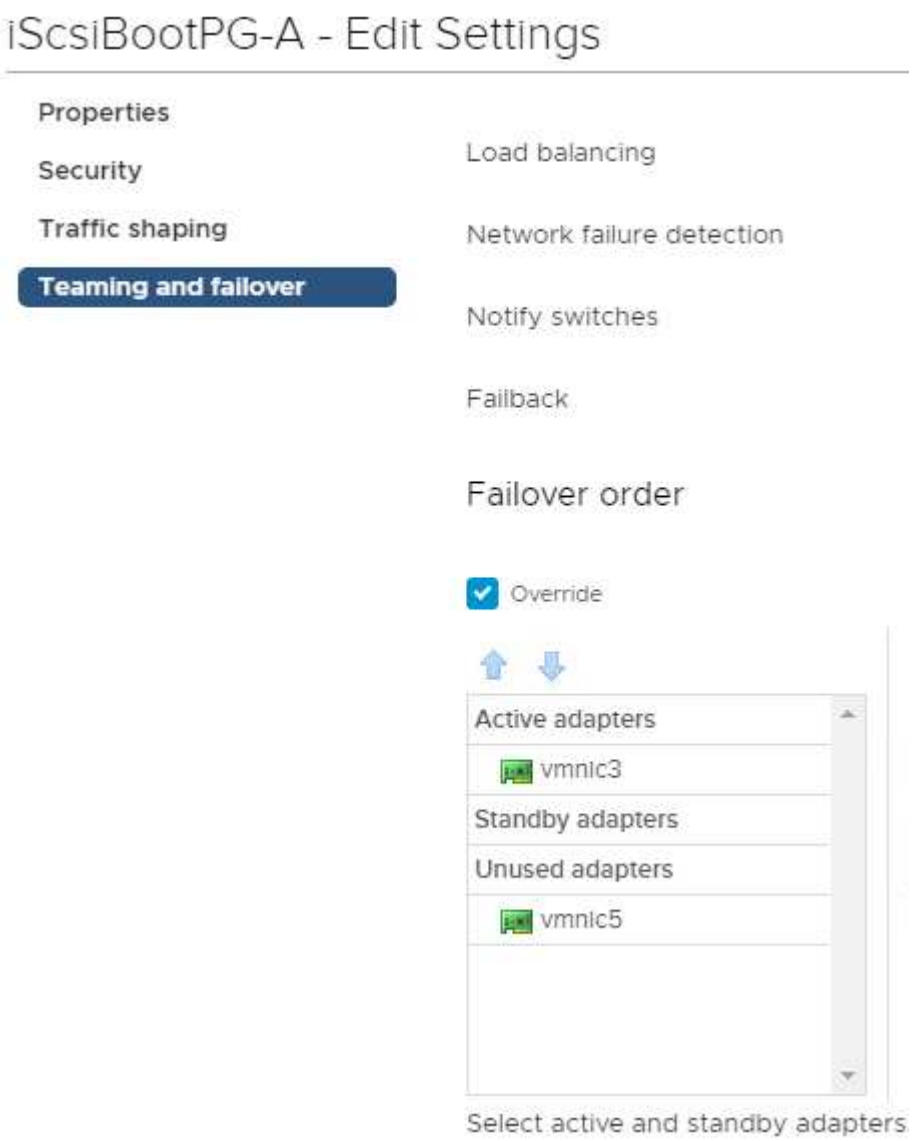
i. Fare clic su Crea.

> 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.

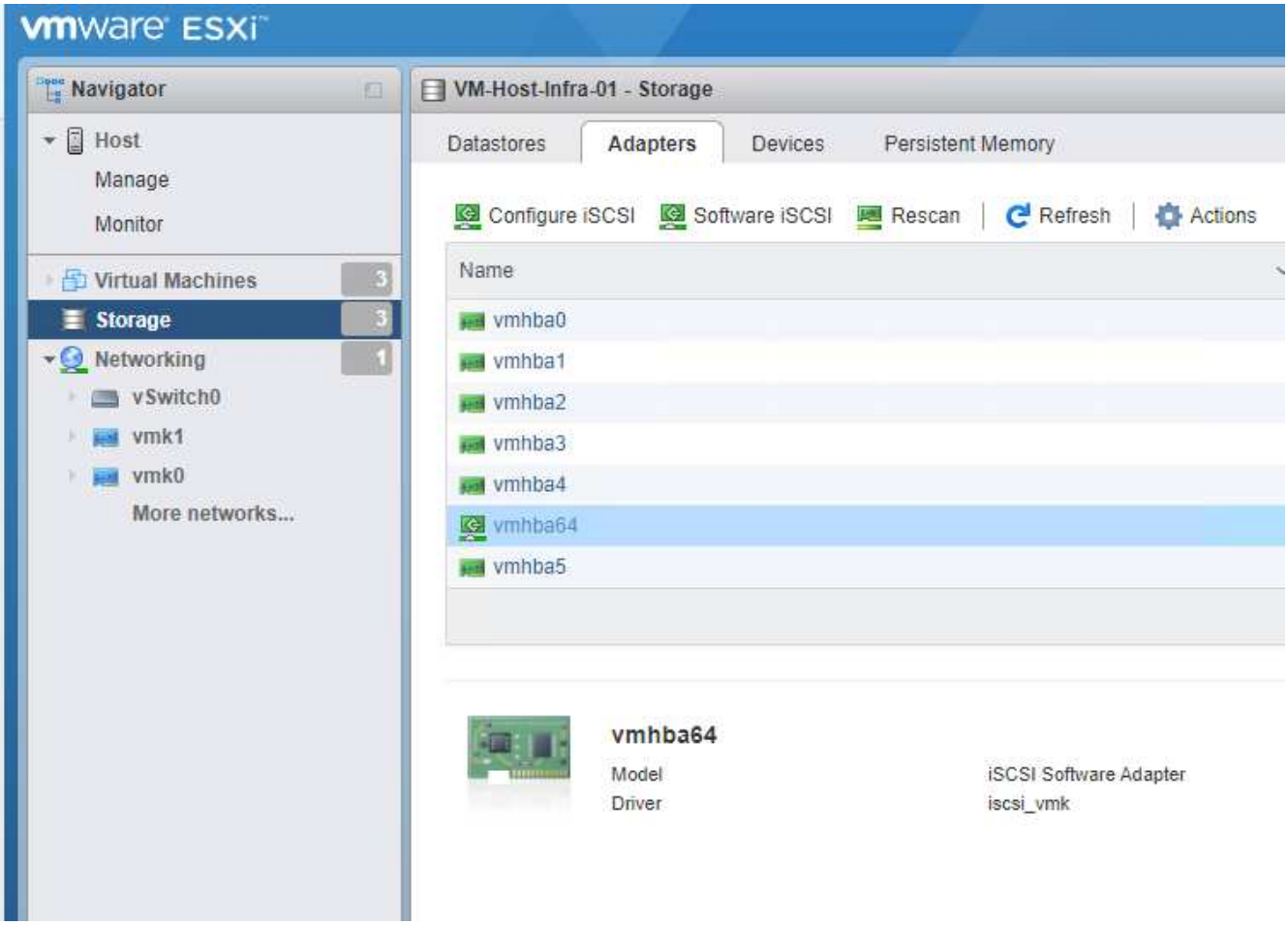
   b. Fare clic su Edit Settings (Modifica impostazioni) in iSCSIBootPG-B > Teaming and failover (Teaming e failover) > failover Order (Ordine di failover) > Vmnic5. Vmnic5 deve essere attivo e vmnic3 deve essere inutilizzato.



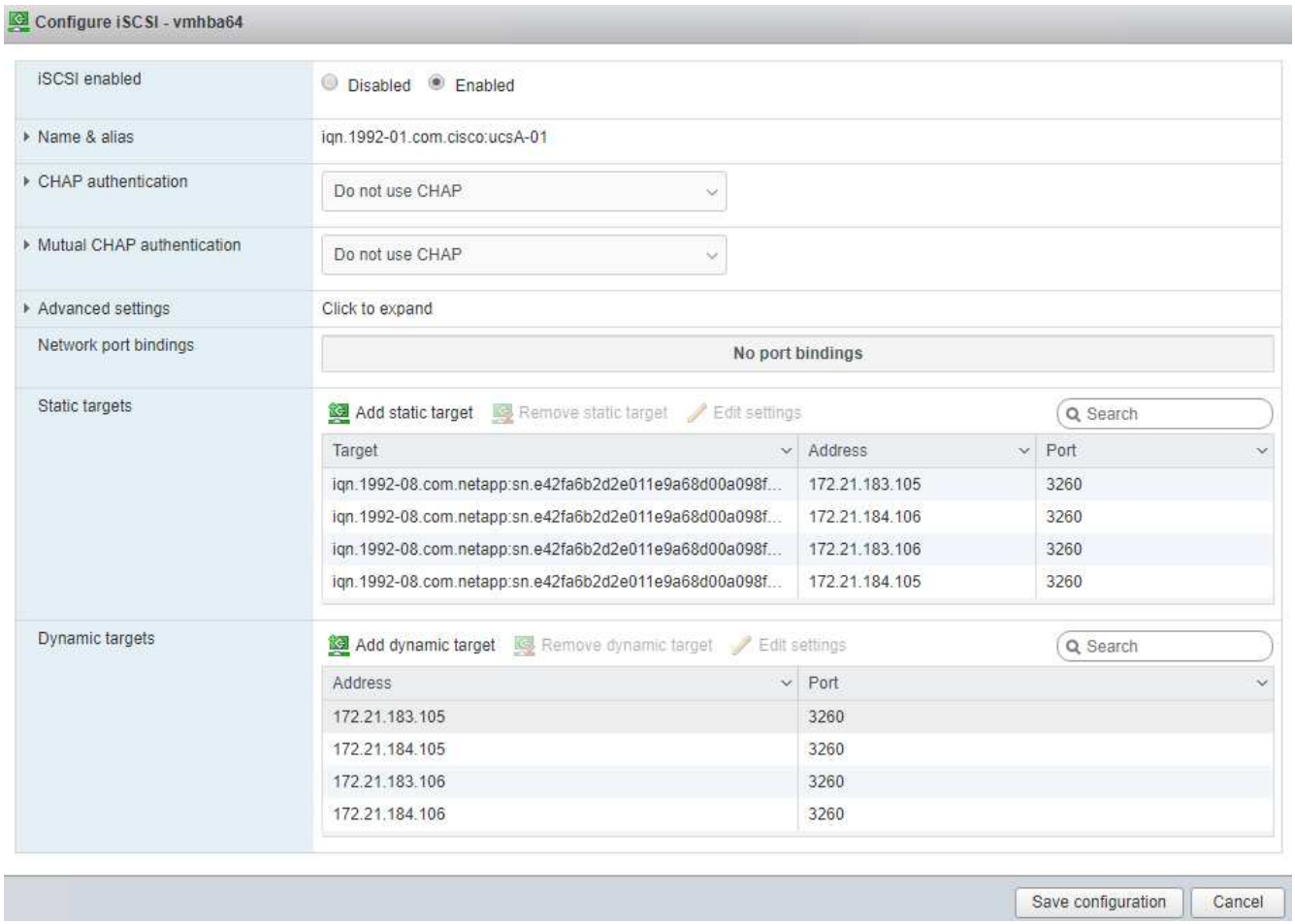
Configurare il multipathing iSCSI

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

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



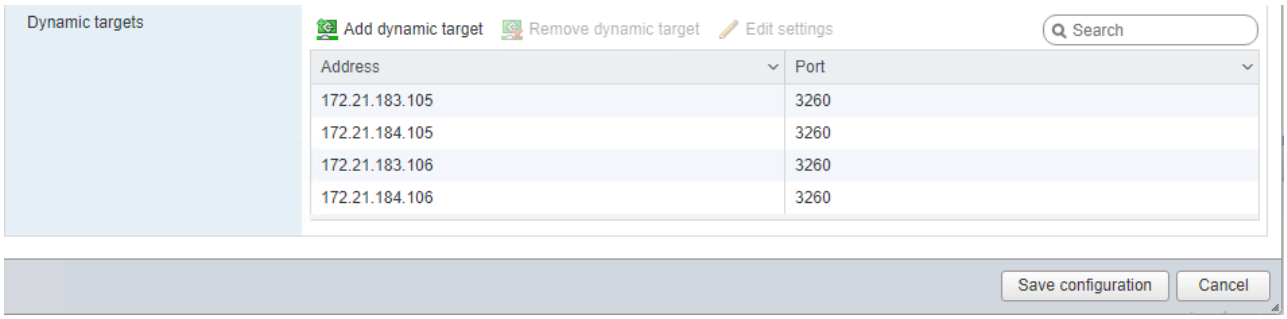
3. In Dynamic Targets (destinazioni dinamiche), fare clic su Add Dynamic Target (Aggiungi destinazione dinamica



4. Inserire l'indirizzo IP `iscsi_lif01a`.

   a. Ripetere l'operazione con gli indirizzi IP `iscsi_lif01b`, `iscsi_lif02a`, e. `iscsi_lif02b`.

   b. Fare clic su Salva configurazione.



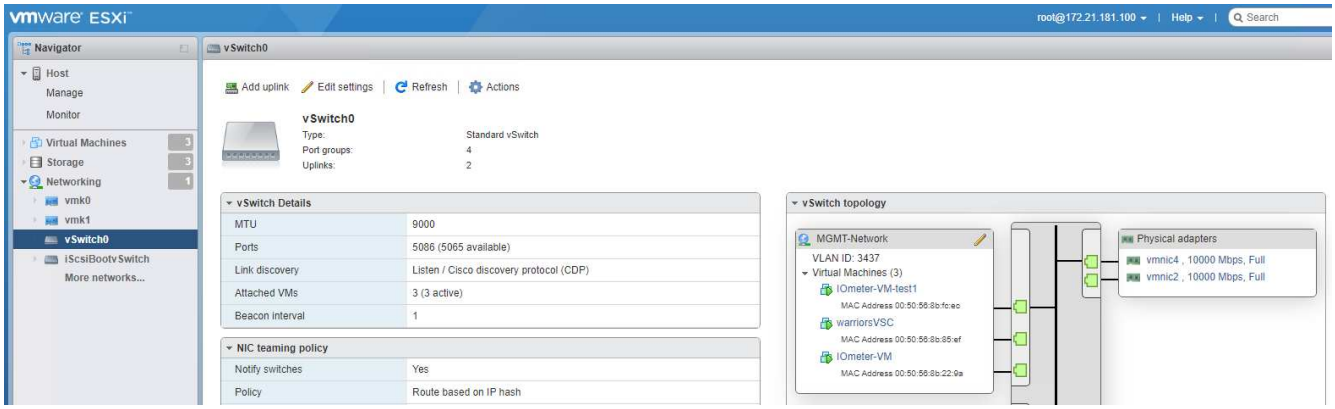
> È possibile trovare gli indirizzi IP LIF iSCSI eseguendo il comando di visualizzazione dell'interfaccia di rete sul cluster NetApp o osservando la scheda Network Interfaces (interfacce di rete) in System Manager.

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.

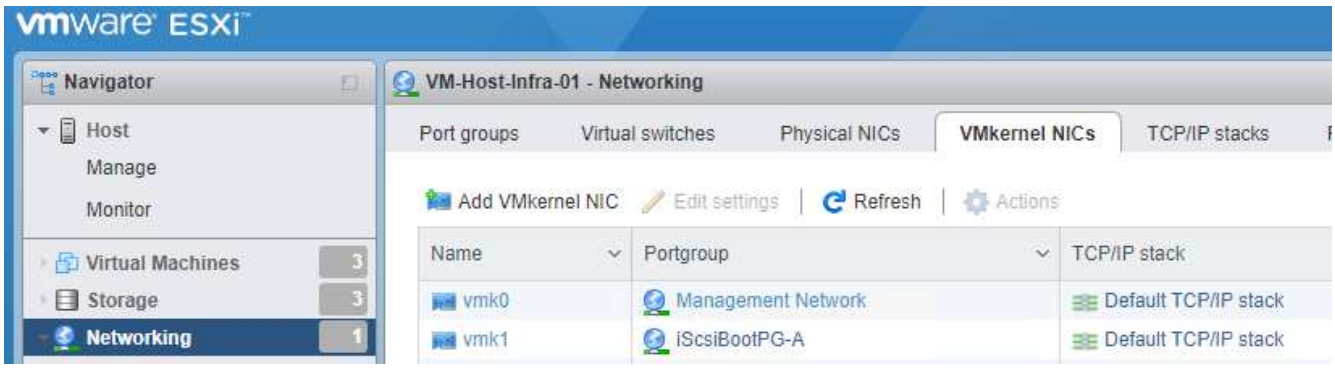
> Il metodo hash IP per il bilanciamento del carico richiede che lo switch fisico sottostante sia configurato correttamente utilizzando SRC-DST-IP EtherChannel con un canale di porta statico (mode-on). La connessione potrebbe essere intermittente a causa di possibili errori di configurazione dello switch. 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:

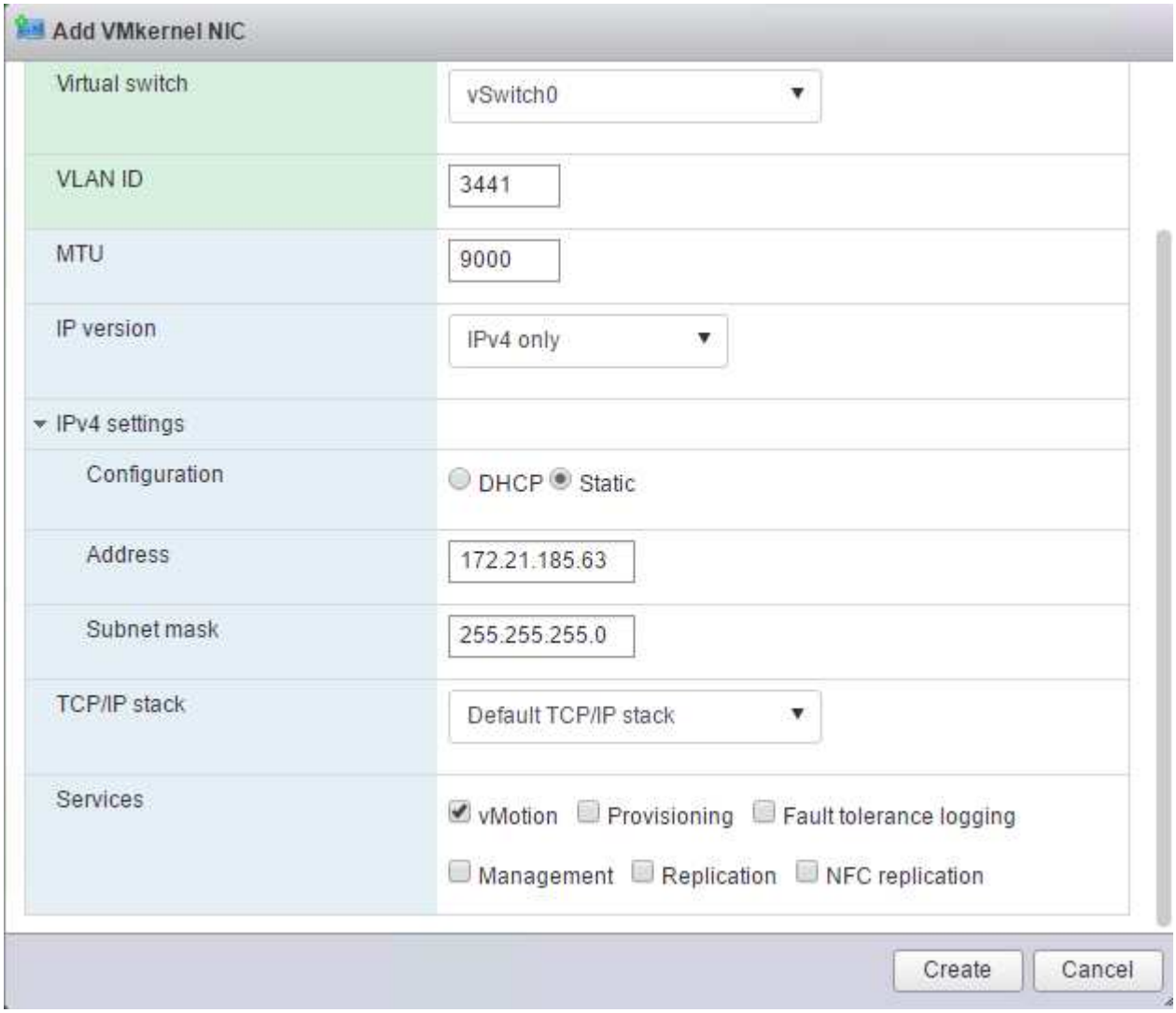
1. Nel riquadro di spostamento a sinistra, selezionare rete.
2. Fare clic con il pulsante destro del mouse sulla scheda gruppi di porte.

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.

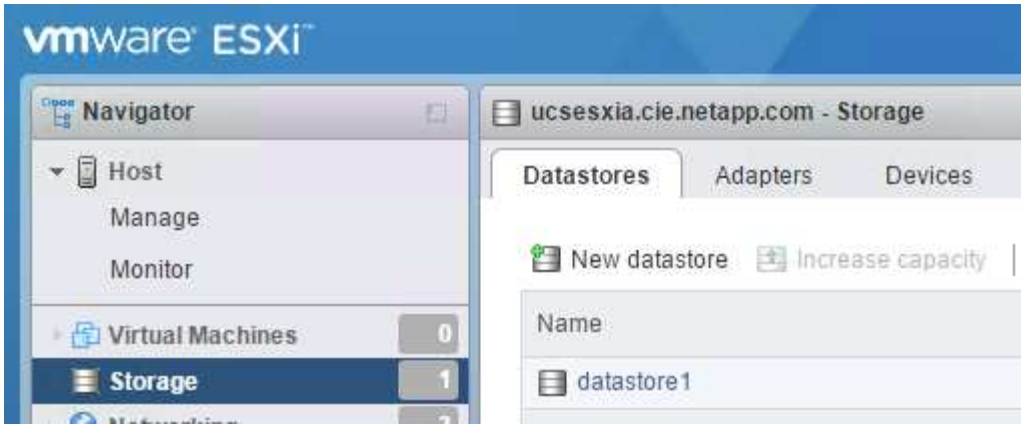


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

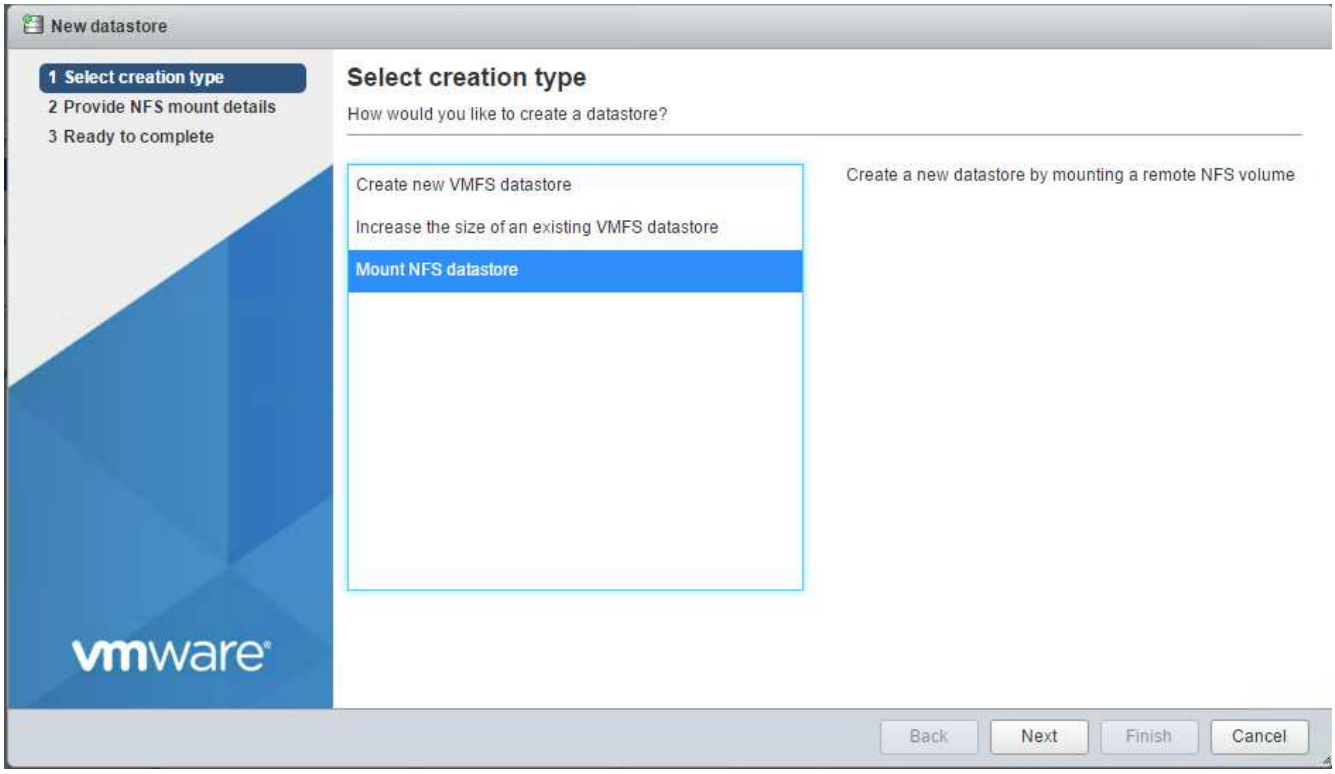
Montare i primi datastore

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).



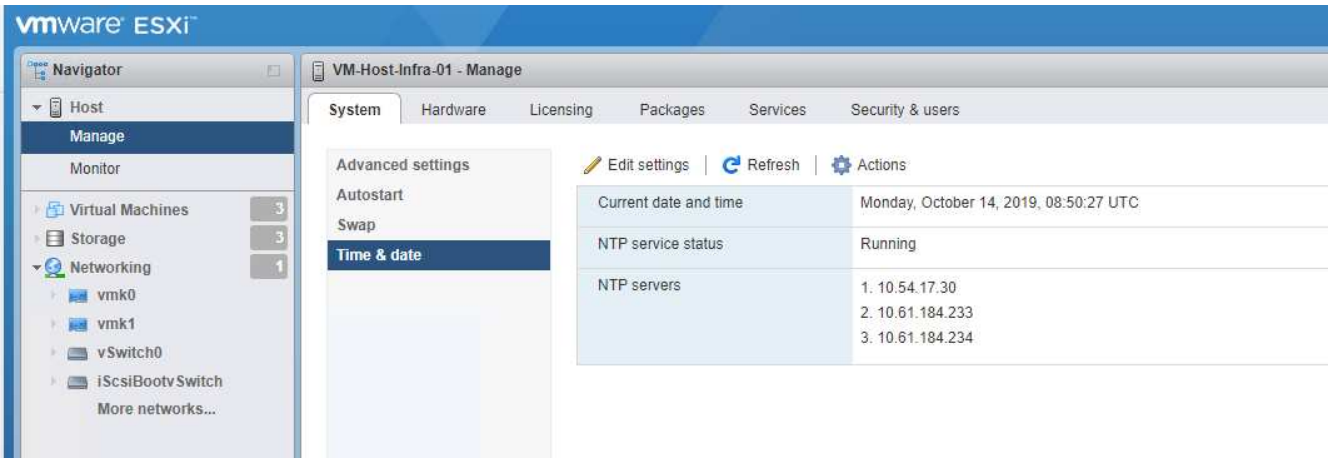
3. Inserire le seguenti informazioni nella pagina fornire dettagli sull'installazione NFS:
   - Nome: `infra_datastore`
   - Server NFS: `<<var_nodea_nfs_lif>>`
   - Condividere: `/infra_datastore`
   - Assicurarsi che sia selezionato NFS 3.
4. Fare clic su fine. È possibile visualizzare il completamento 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:

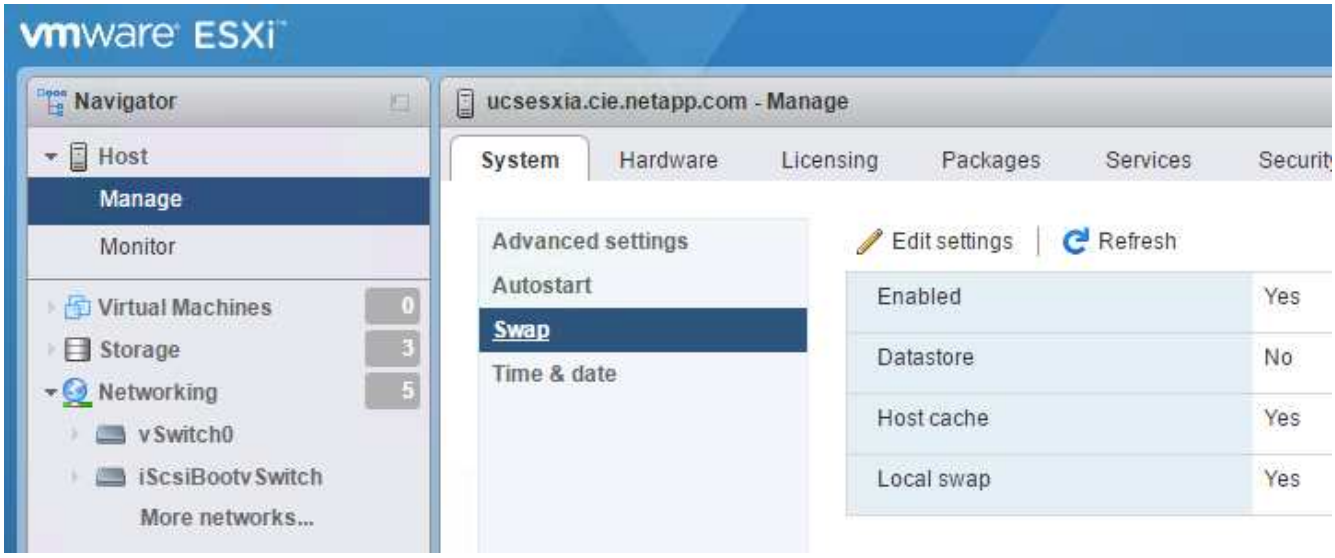
1. Fare clic su Manage (Gestisci) nel riquadro di navigazione a sinistra. Selezionare sistema nel riquadro di destra, quindi fare clic su Data e ora.
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio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

3. Fare clic su Salva.

"Procedura di installazione di VMware vCenter Server 6.7U2."

Procedura di installazione di VMware vCenter Server 6.7U2

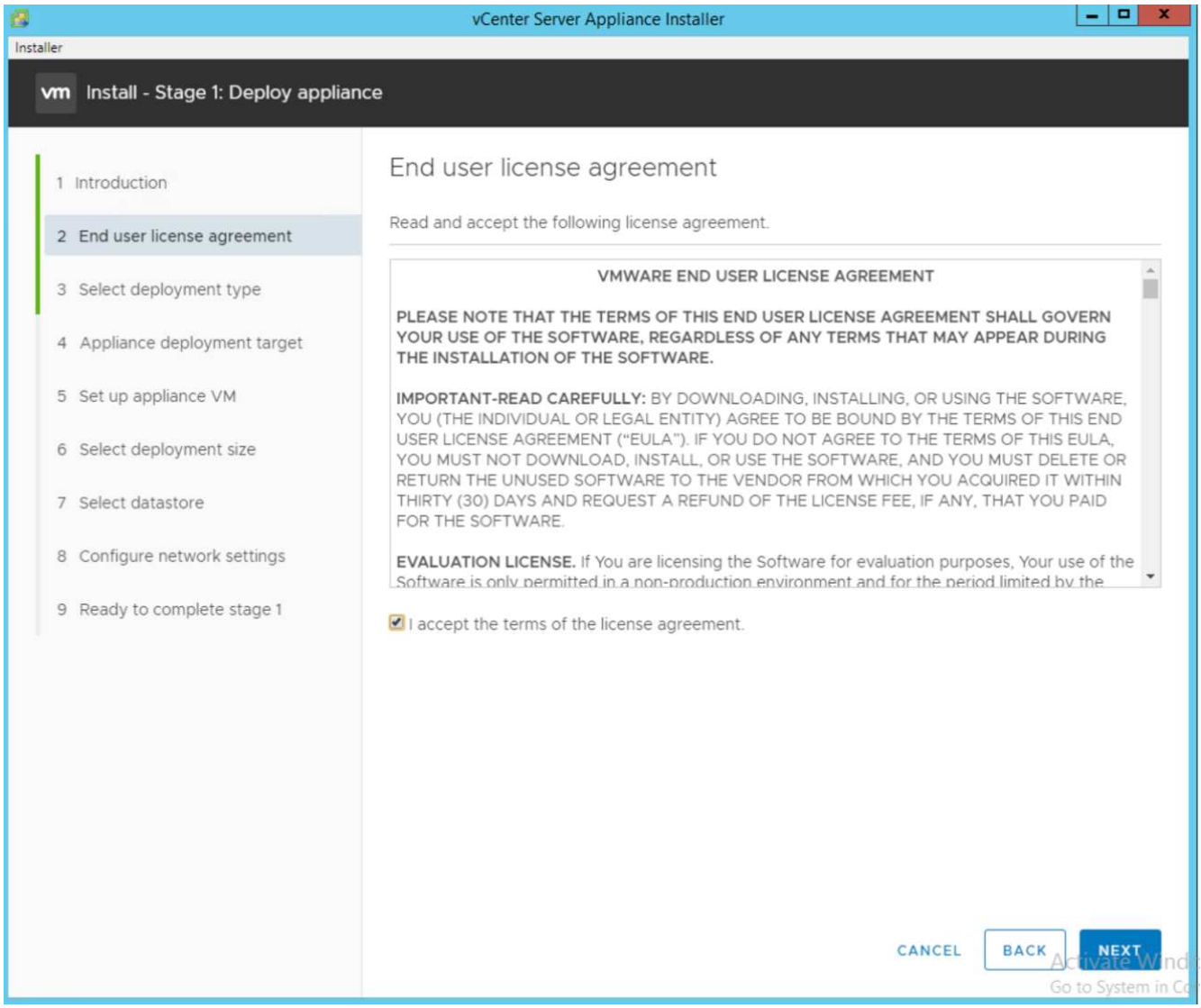
Questa sezione fornisce procedure dettagliate per l'installazione di VMware vCenter Server 6.7 in una configurazione FlexPod Express.

FlexPod utilizza l'appliance server vCenter (VCSA).

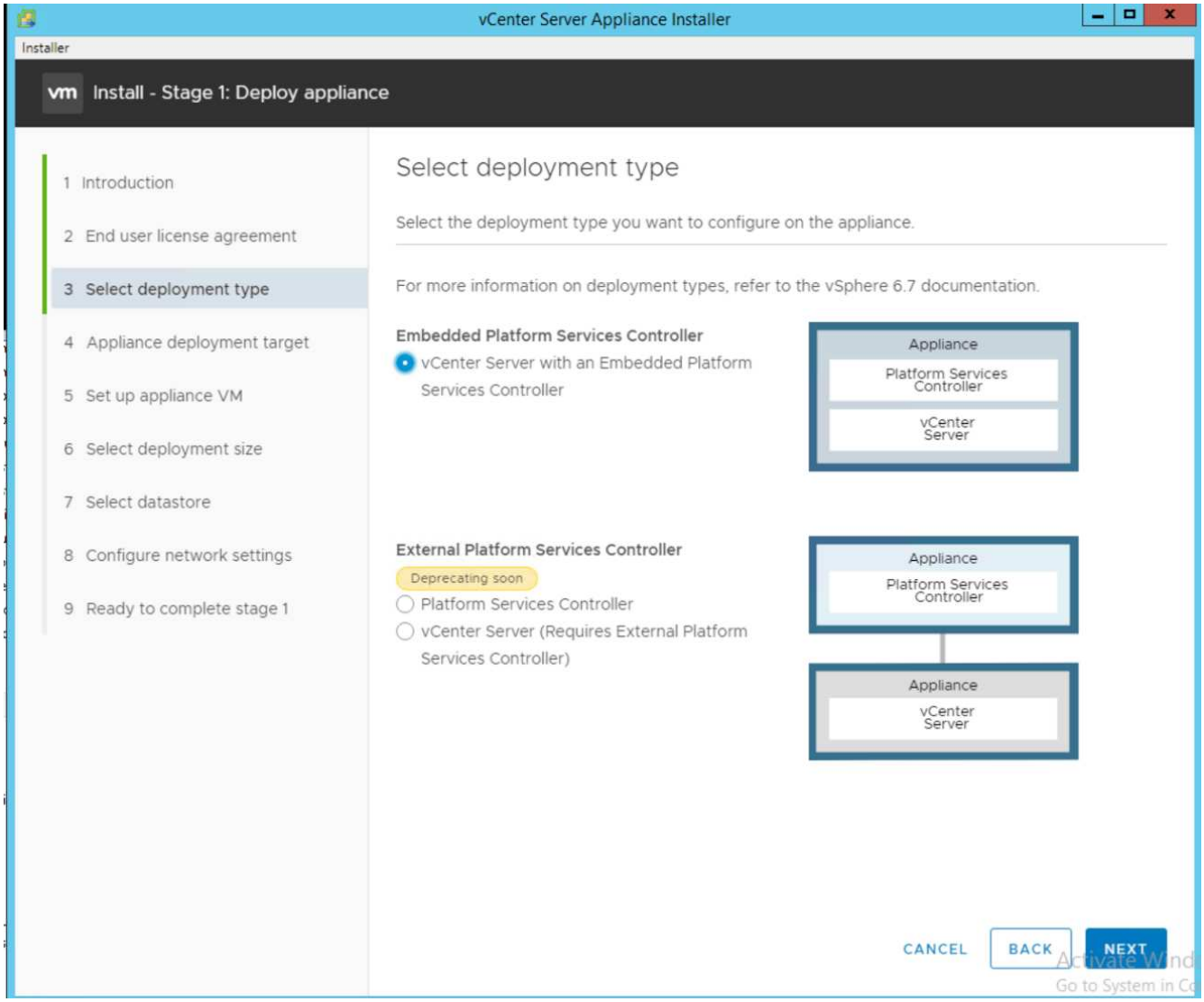
Scarica VMware vCenter Server Appliance

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.

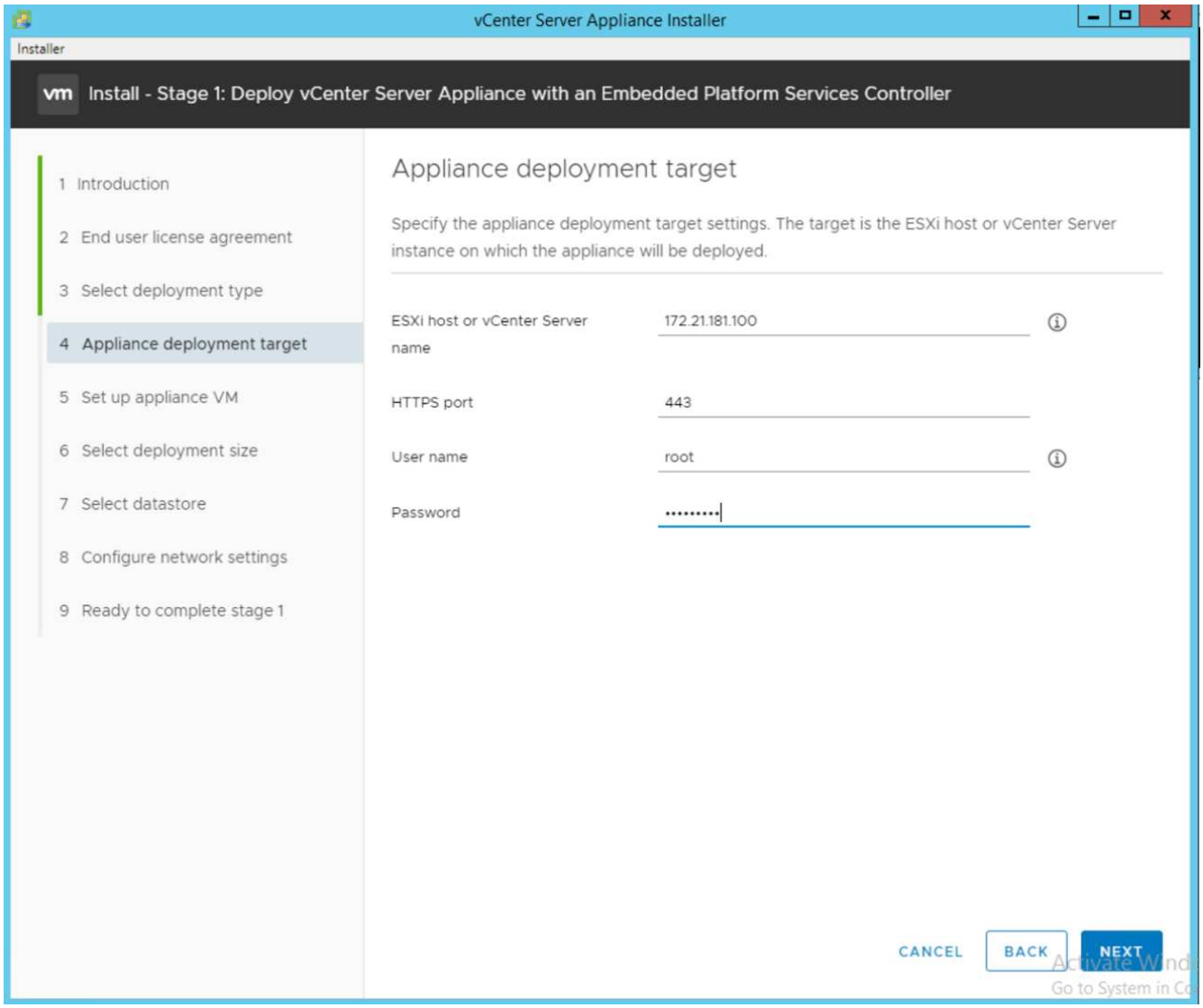


8. Selezionare Embedded Platform Services Controller come tipo di implementazione.

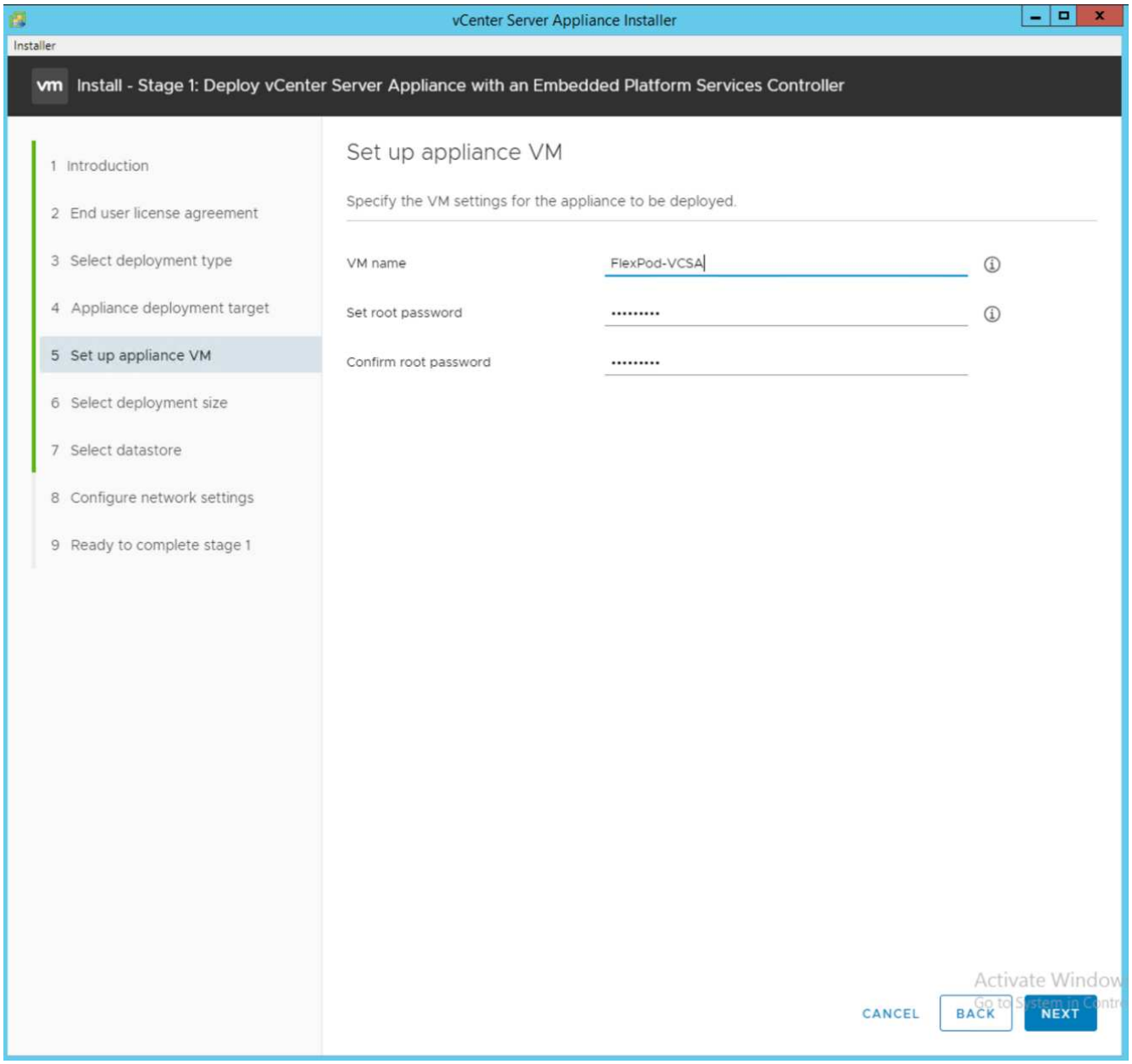


Se necessario, l'implementazione del controller dei servizi della piattaforma esterna è supportata anche come parte della soluzione FlexPod Express.

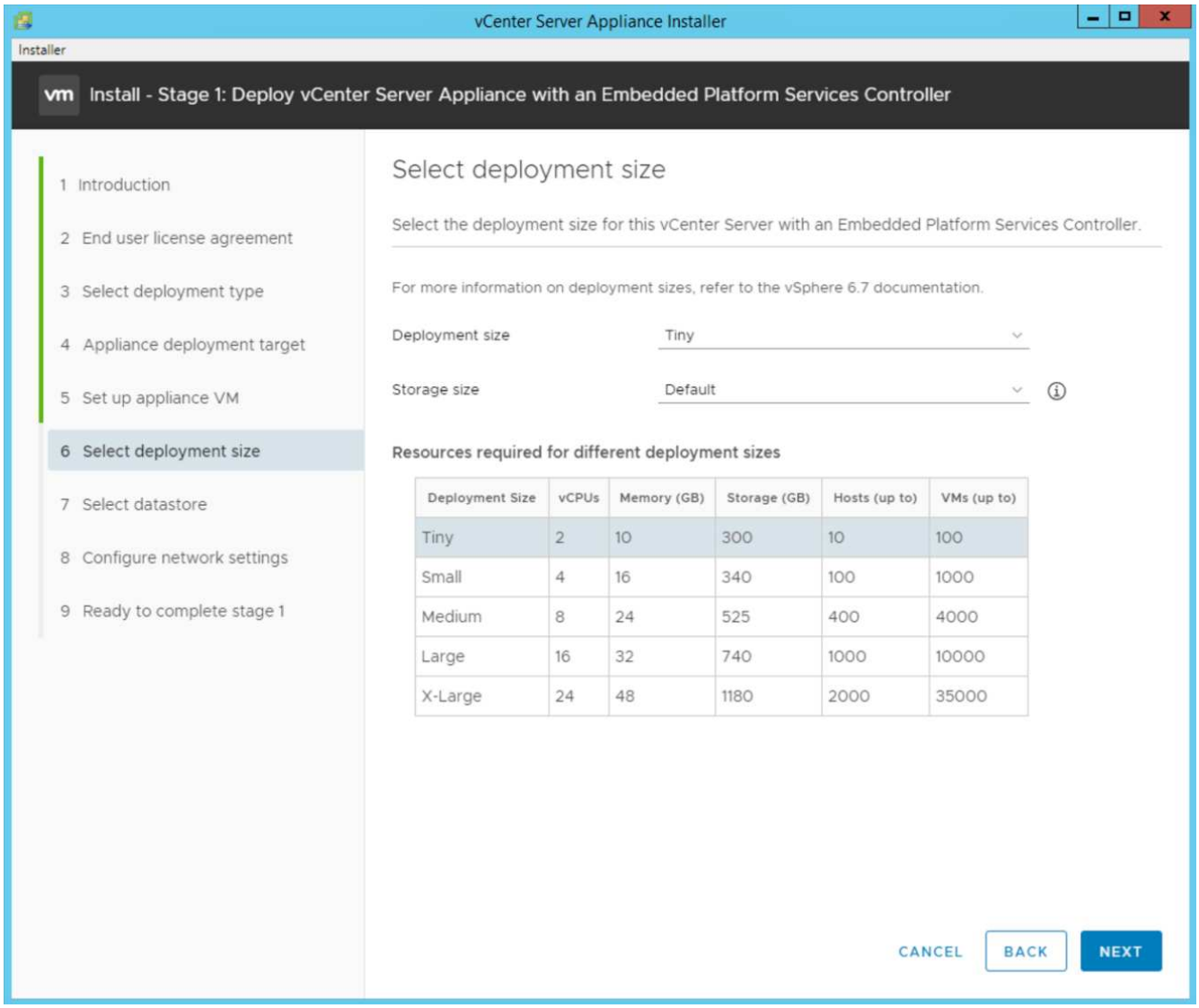
9. In Appliance Deployment Target (destinazione implementazione appliance), immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root.



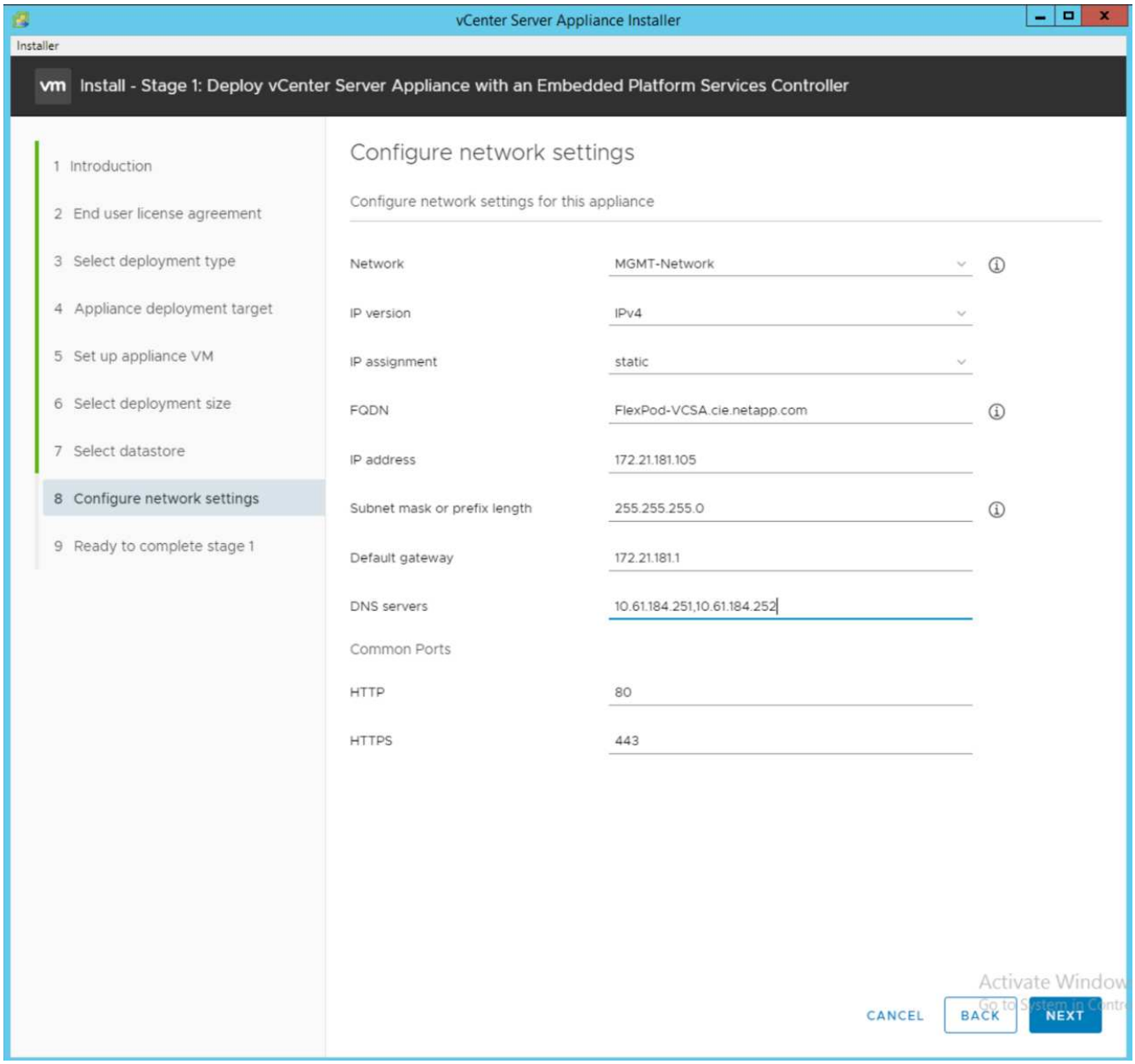
10. Impostare la macchina virtuale dell’appliance immettendo VCSA come nome della macchina virtuale e password root che si desidera utilizzare per VCSA.



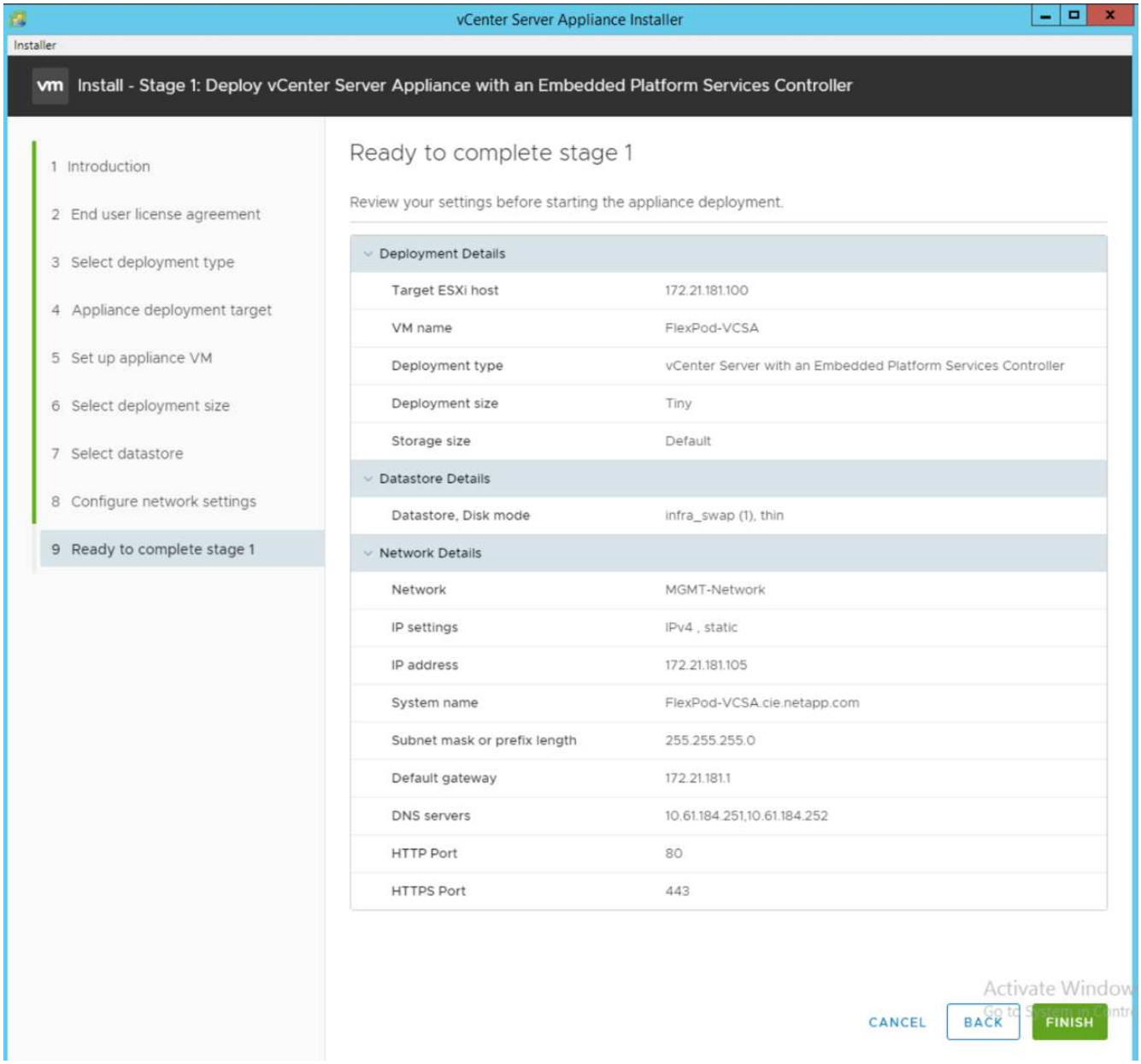
11. Selezionare la dimensione di implementazione più adatta al proprio ambiente. Fare clic su Avanti.



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.

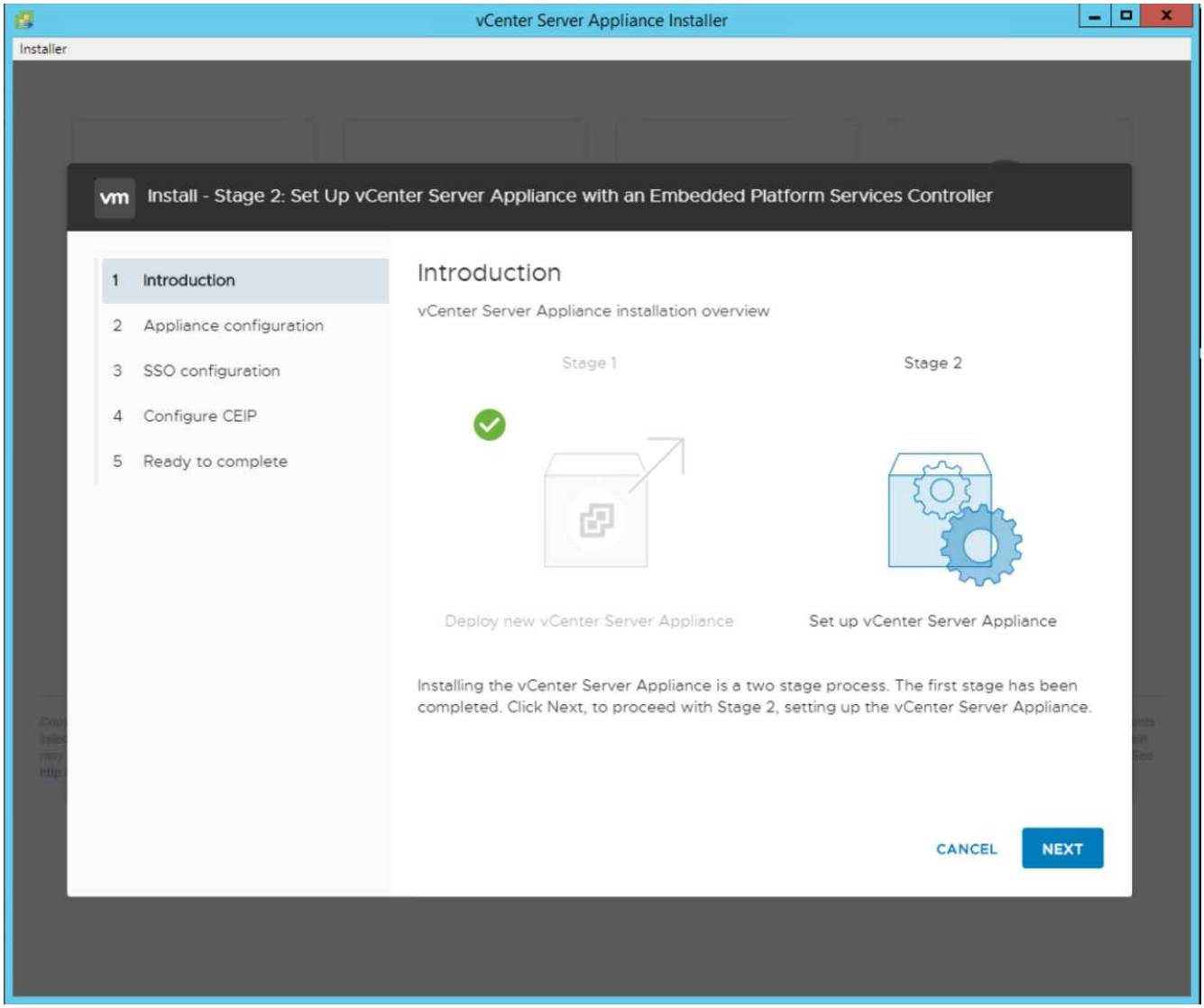


15. Rivedere le impostazioni nella fase 1 prima di avviare l’implementazione dell’appliance.

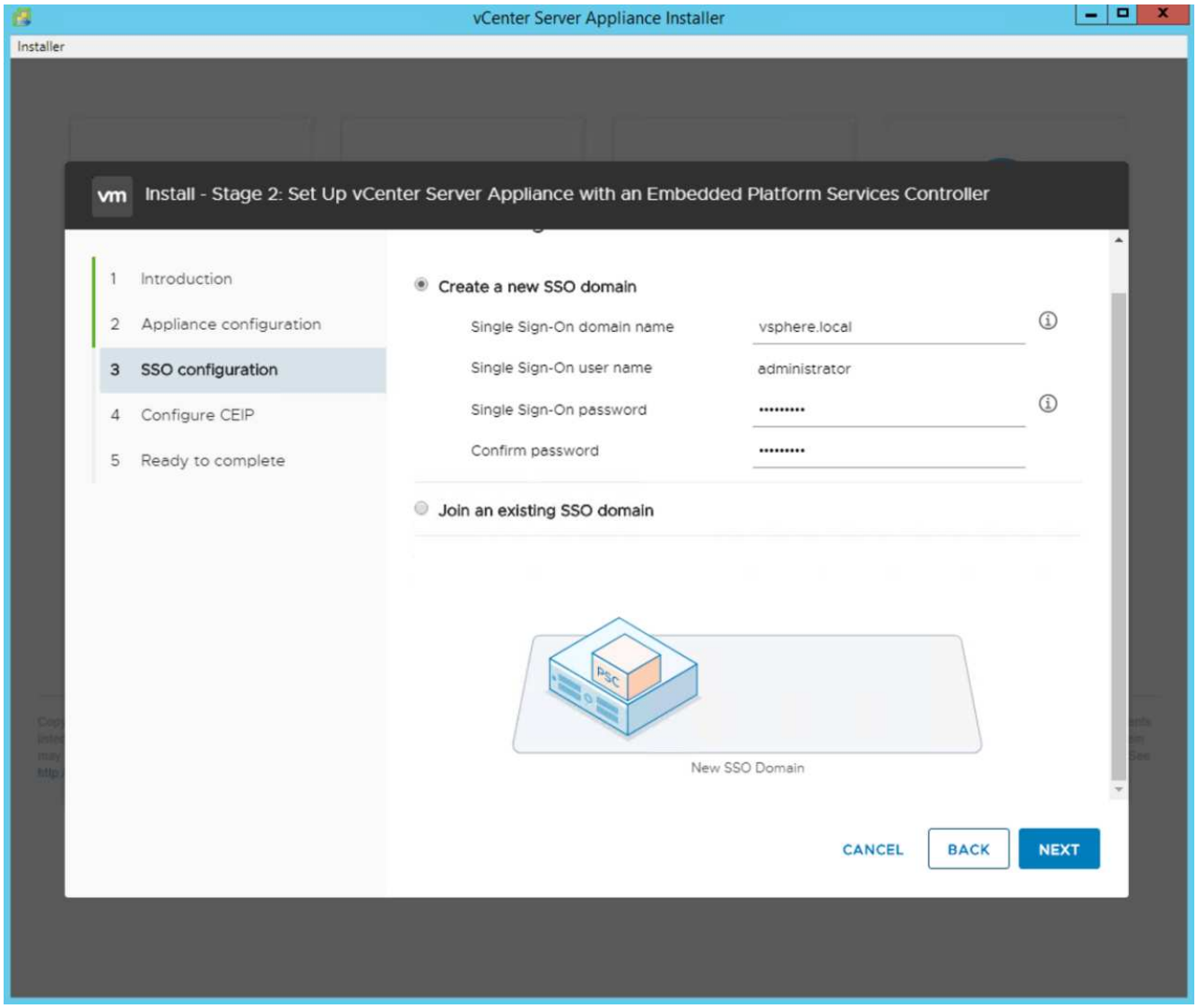


VCSA viene installato ora. Questo processo richiede alcuni minuti.

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.

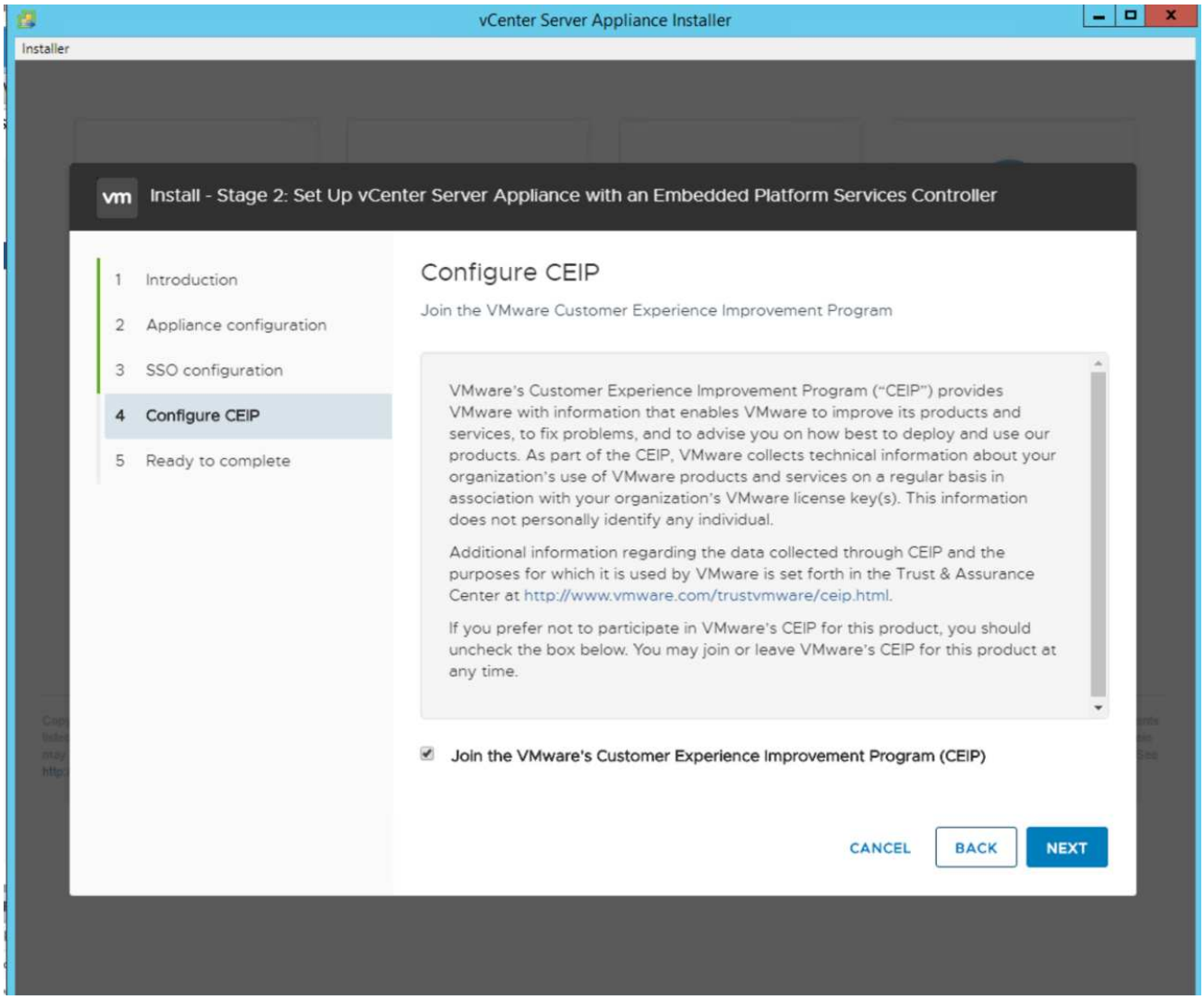


18. Invio `<<var_ntp_id>>` Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.
19. Se si intende utilizzare vCenter Server High Availability (ha), assicurarsi che l'accesso SSH sia attivato.
20. Configurare il nome di dominio SSO, la password e il nome del sito. Fare clic su Avanti.

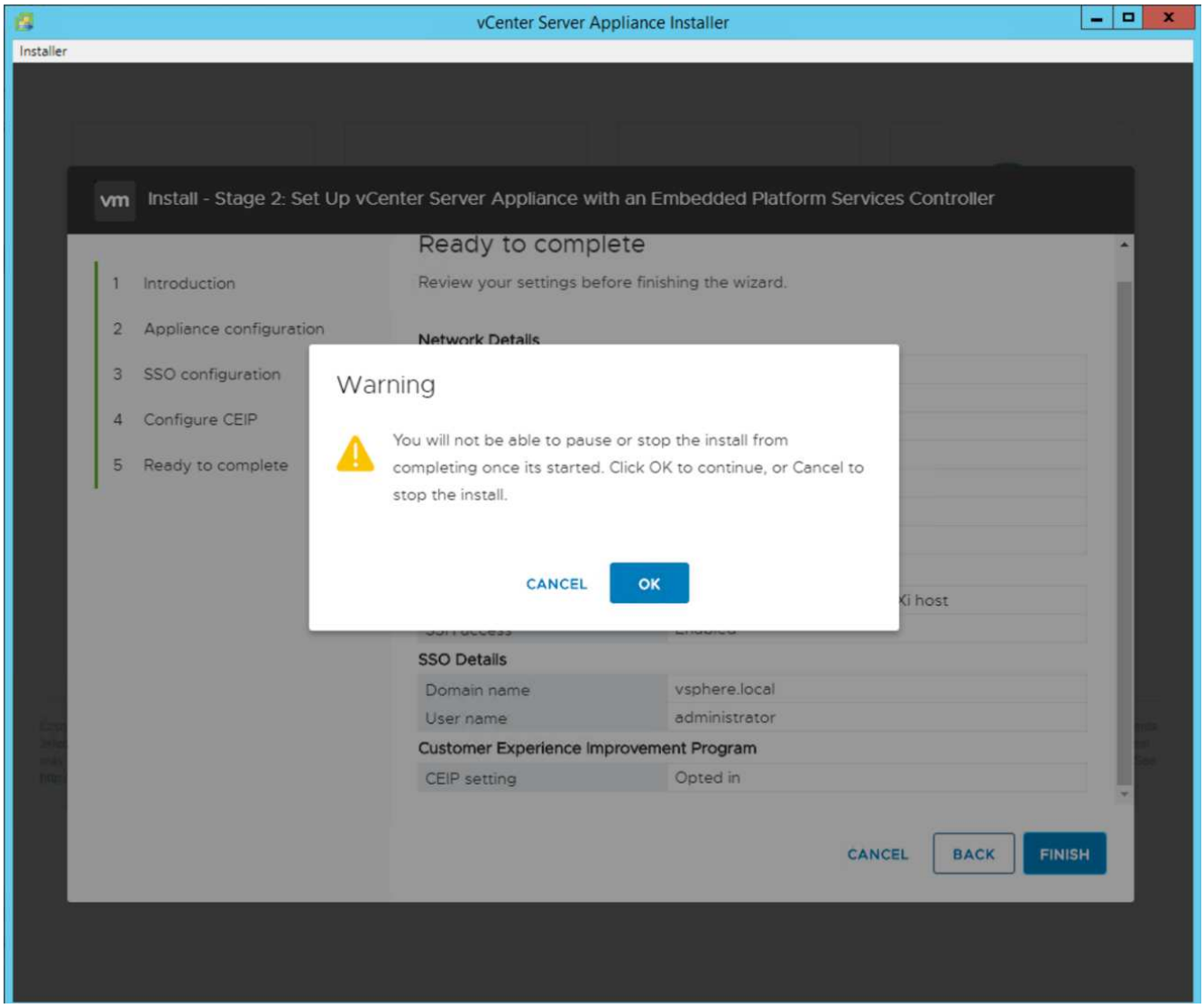


Registrare questi valori come riferimento, in particolare se si discosta da `vsphere.local` nome di dominio.

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:

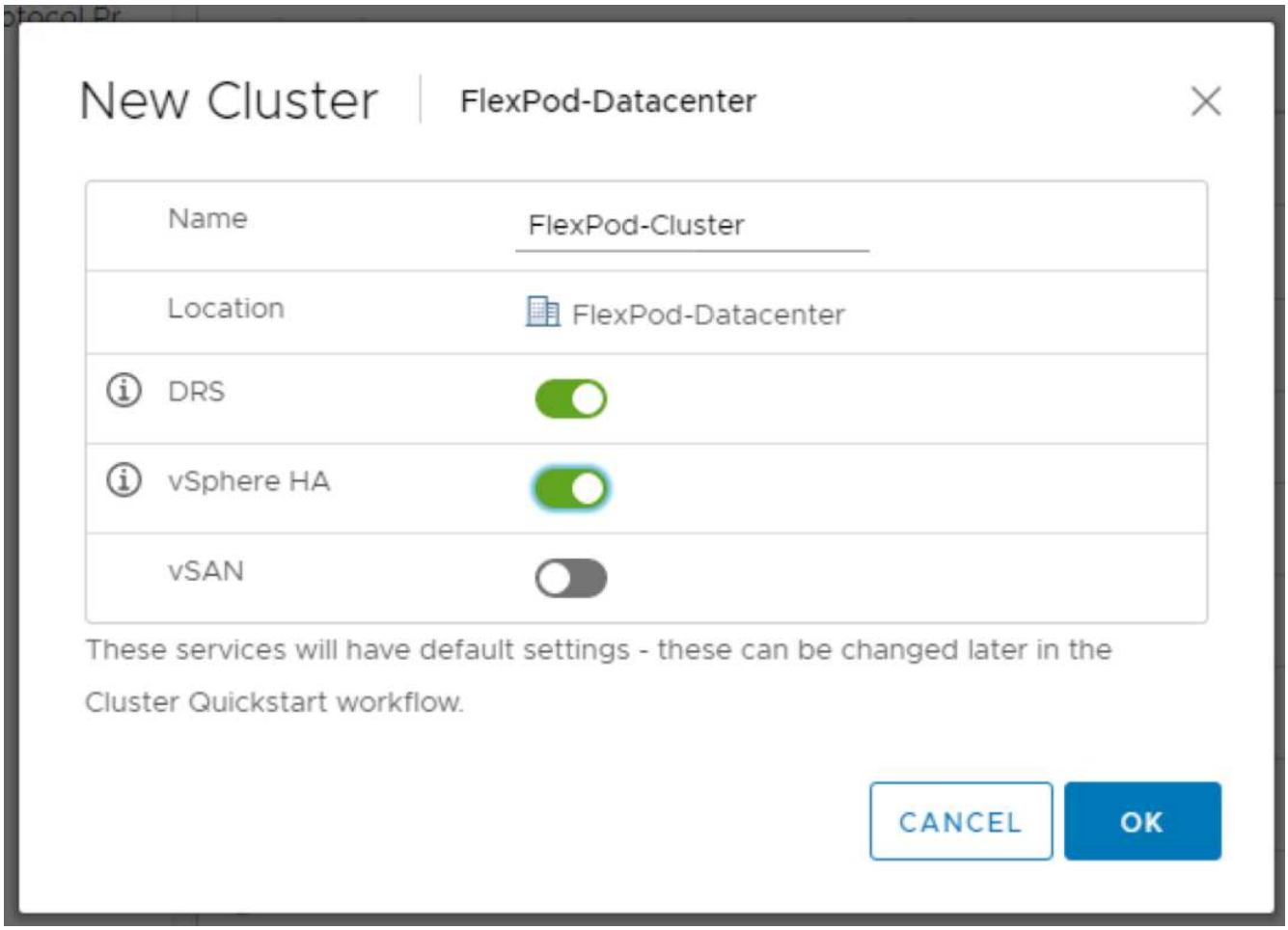
1. Selezionare `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Fare clic su Launch vSphere Client.
3. Accedere con il nome utente Administrator@vsphere.local e la password SSO immessa durante il processo di configurazione di VCSA.
4. Fare clic con il pulsante destro del mouse sul nome di vCenter 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:

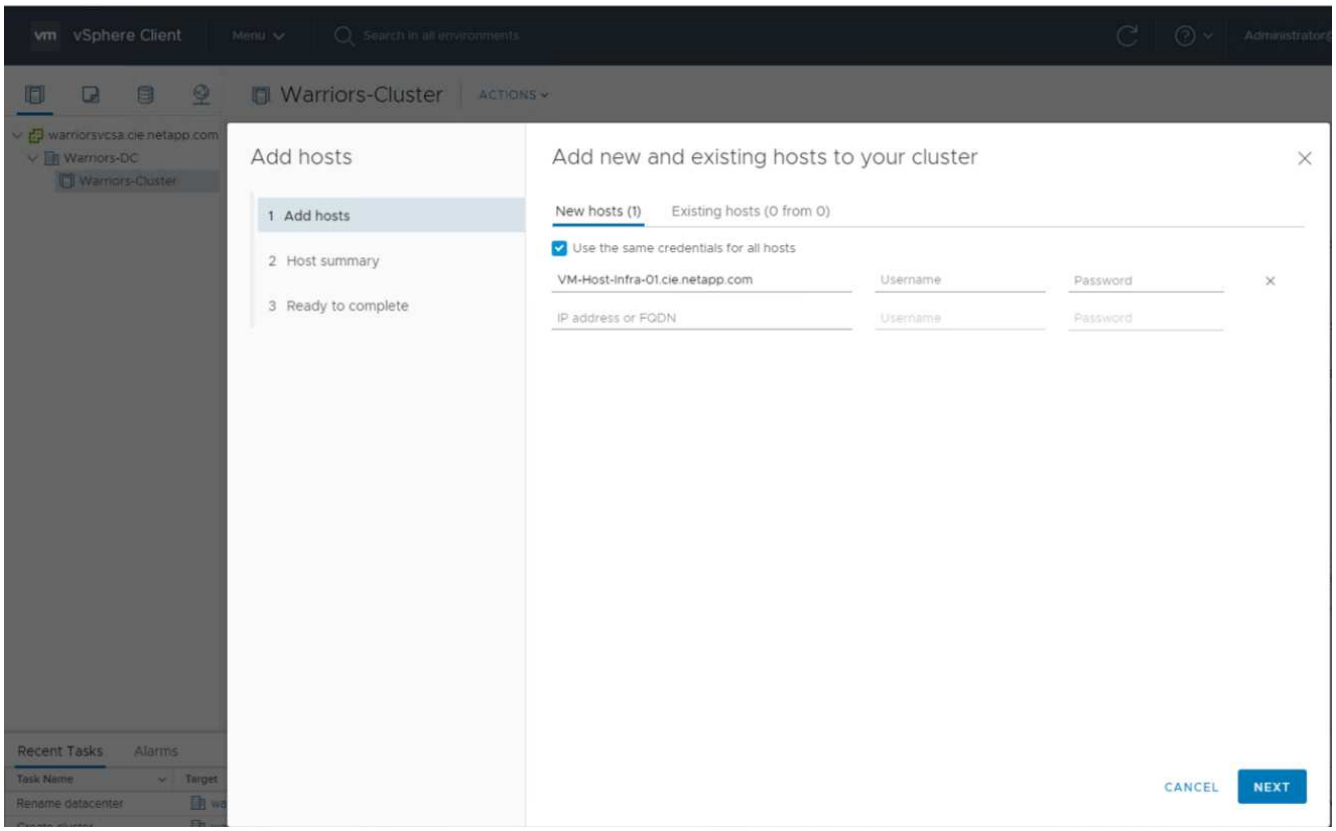
1. Fare clic con il pulsante destro del mouse sul data center appena creato e selezionare New Cluster (nuovo cluster).
2. Inserire un nome per il cluster.
3. Attivare DR e vSphere ha selezionando le caselle di controllo.
4. Fare clic su OK.



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.

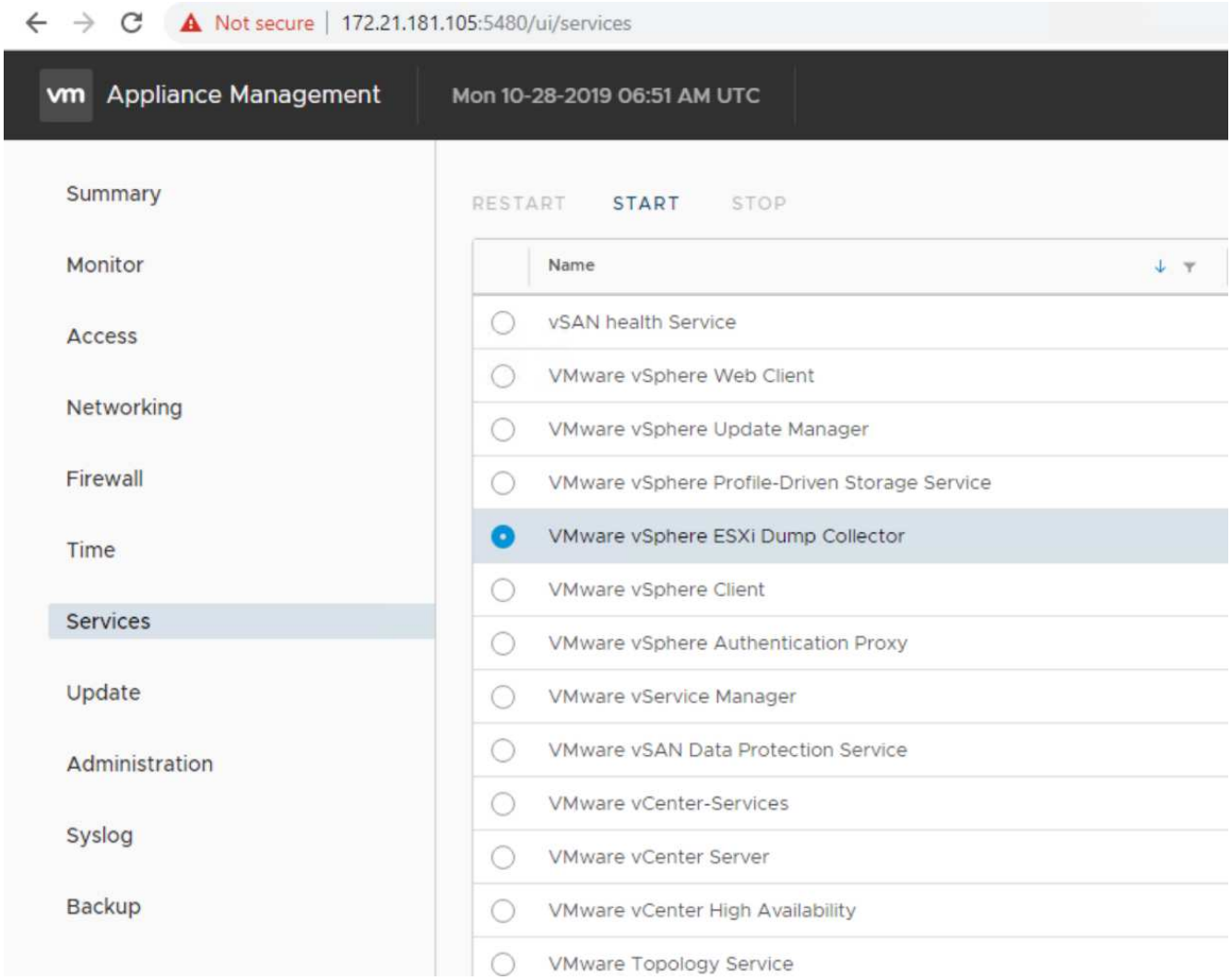
> Questo processo deve essere completato per tutti gli host aggiuntivi aggiunti alla configurazione di FlexPod Express.

Configurare il coredump sugli host ESXi

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

1. Accedere a https:// "VCenter" 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
erified 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."

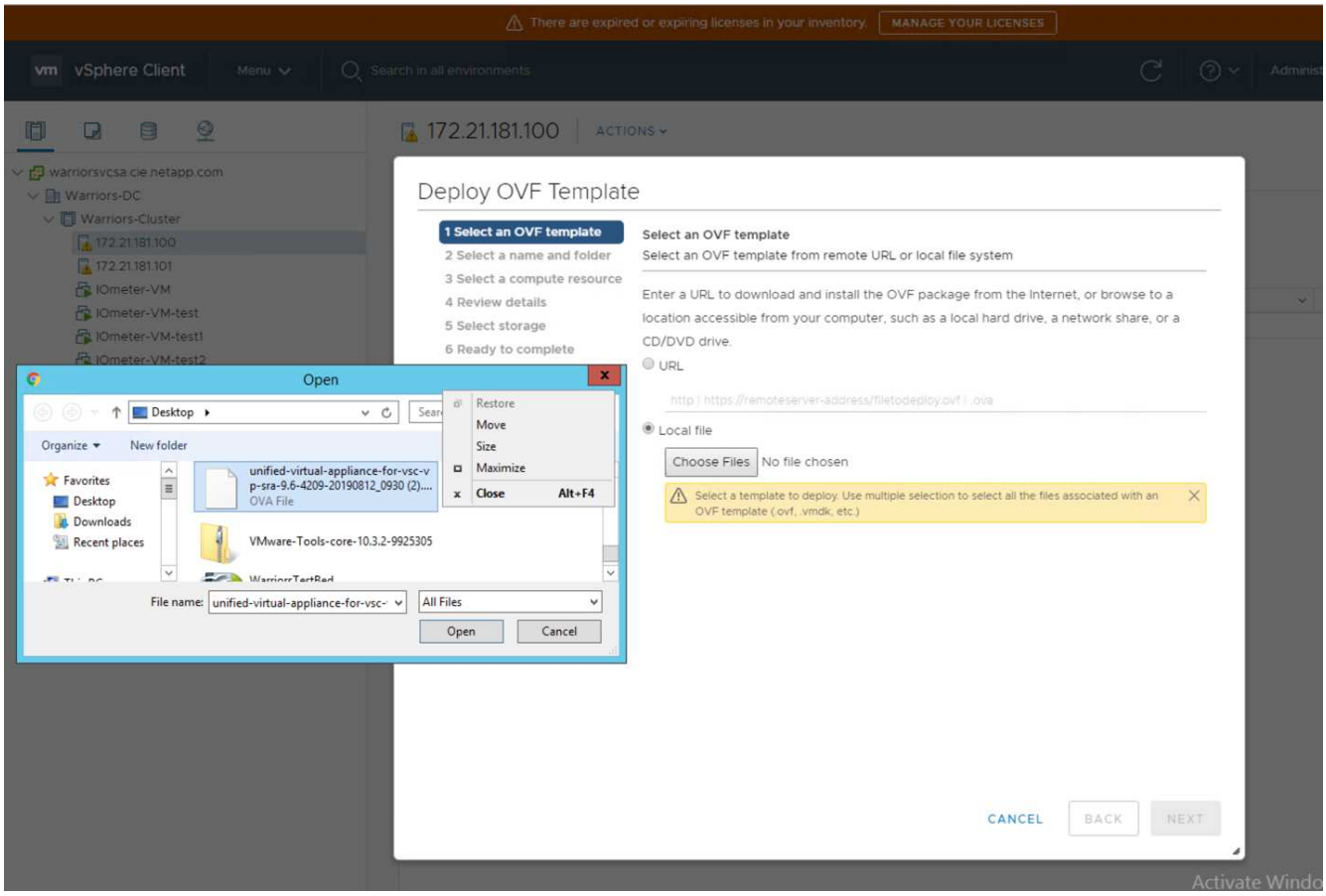
Procedure di implementazione di NetApp Virtual Storage Console 9.6

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

Installare Virtual Storage Console 9.6

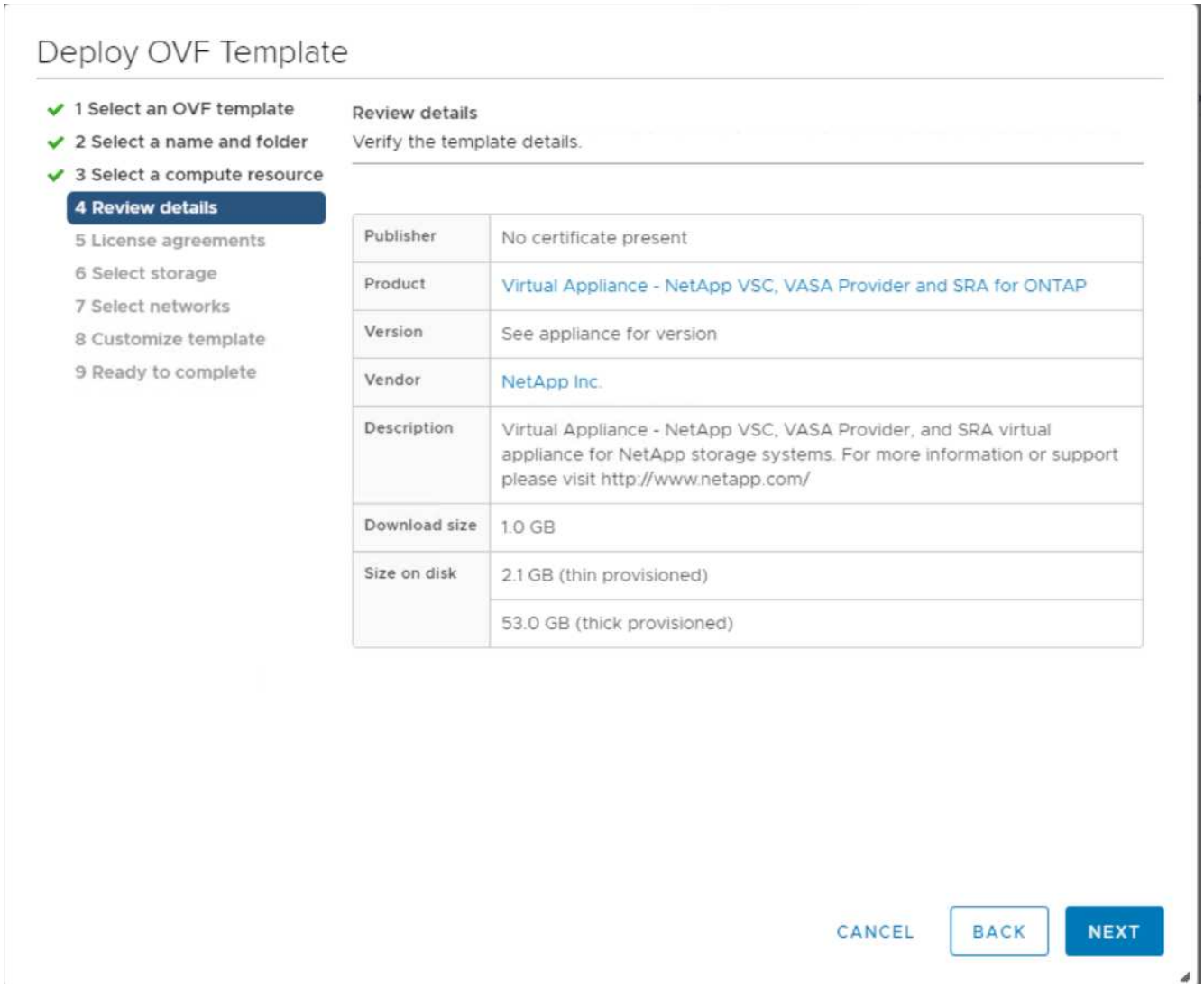
Per installare il software VSC 9.6 utilizzando un'implementazione Open Virtualization Format (OVF), attenersi alla seguente procedura:

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.

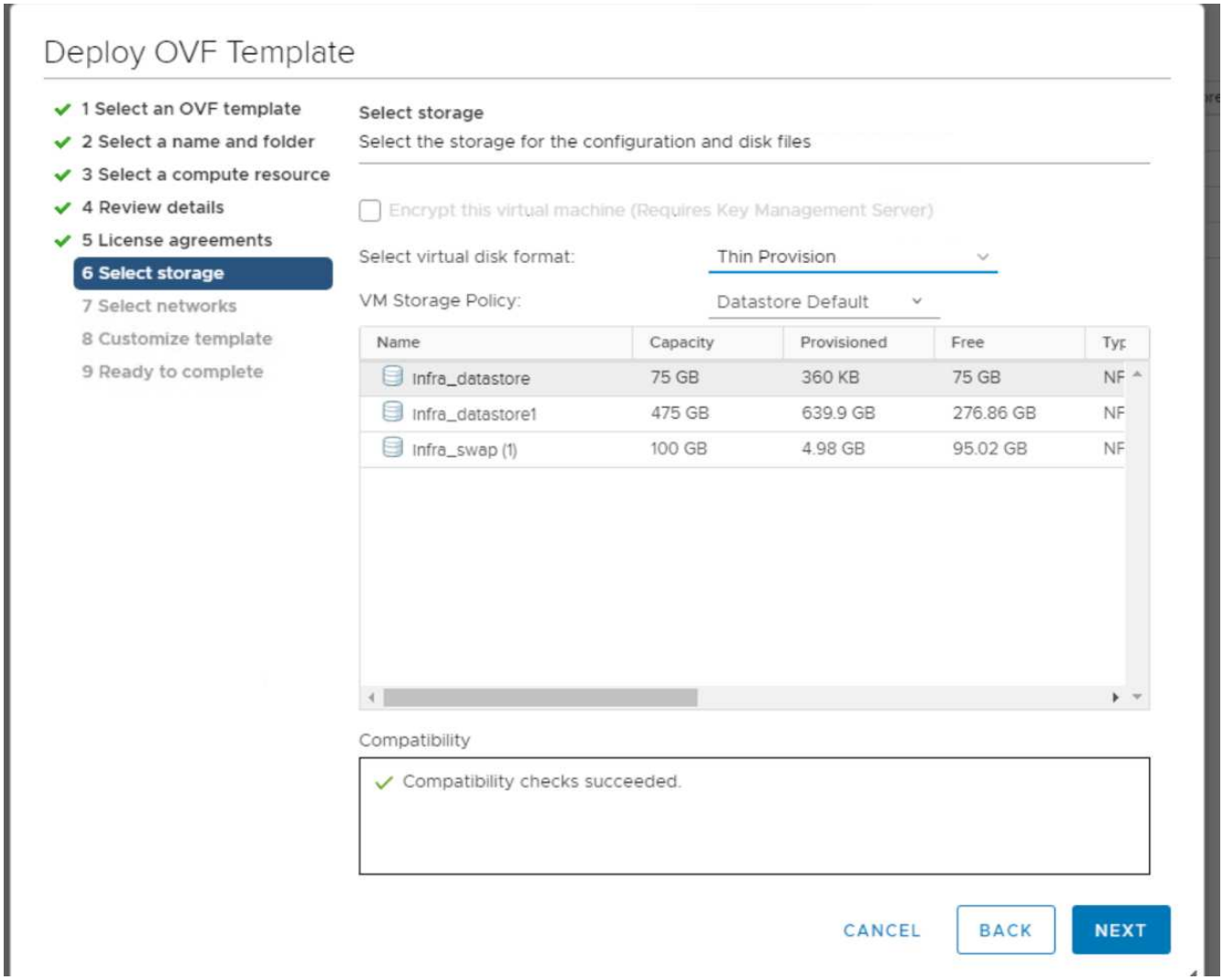


3. Inserire il nome della macchina virtuale e selezionare un data center o una cartella in cui eseguire l'implementazione. Fare clic su Avanti.

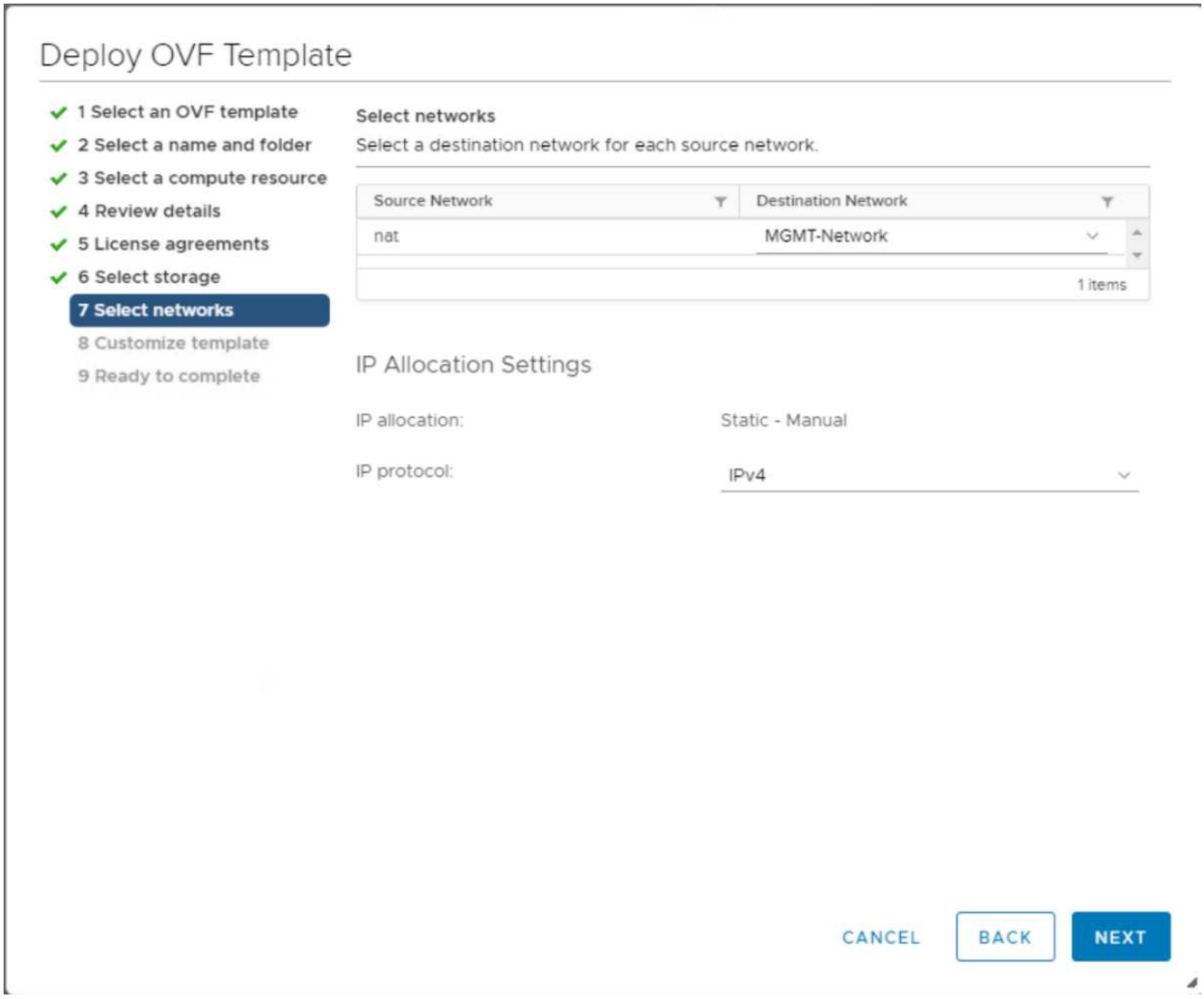
4. Selezionare il cluster ESXi FlexPod-Cluster e fare clic su Next (Avanti).
5. Esaminare i dettagli e fare clic su Next (Avanti).



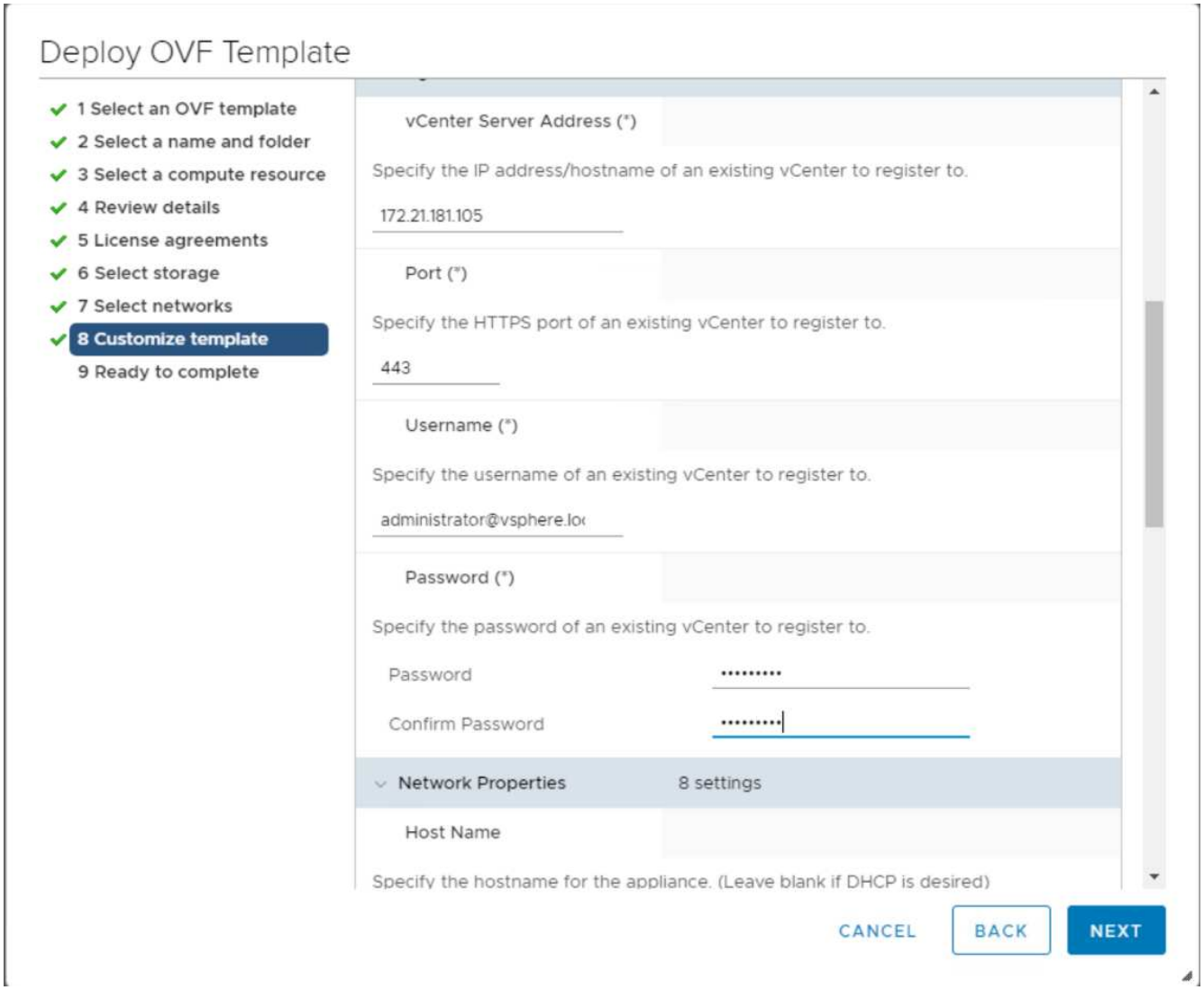
6. Fare clic su Accept (Accetta) per accettare la licenza e fare clic su Next (Avanti).
7. Selezionare il formato del disco virtuale di thin provisioning e uno degli archivi dati NFS. Fare clic su Avanti.



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



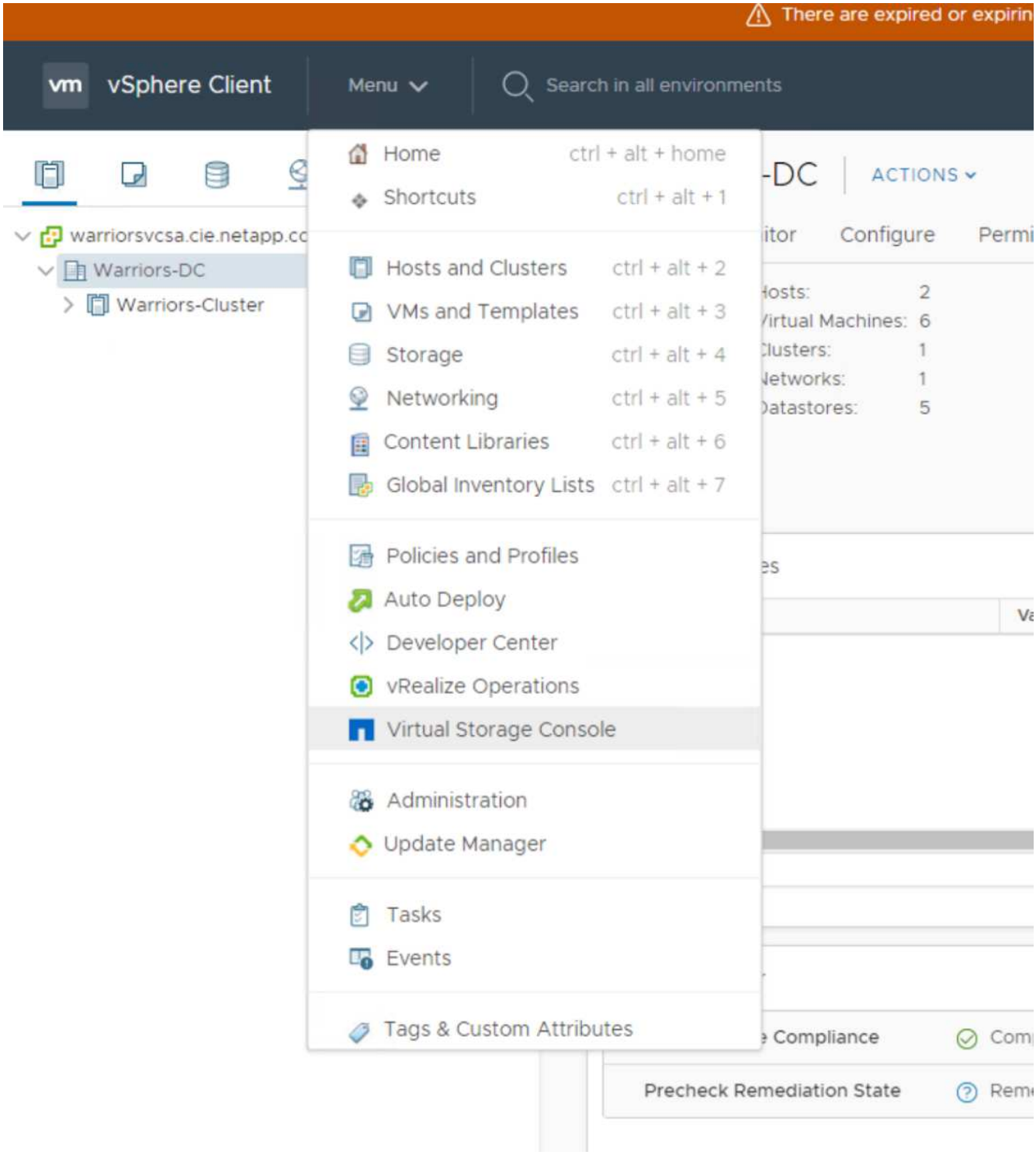
9. Da Customize Template (Personalizza modello), immettere la password dell'amministratore VSC, il nome vCenter o l'indirizzo IP e altri dettagli di configurazione, quindi fare clic su Next (Avanti).



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

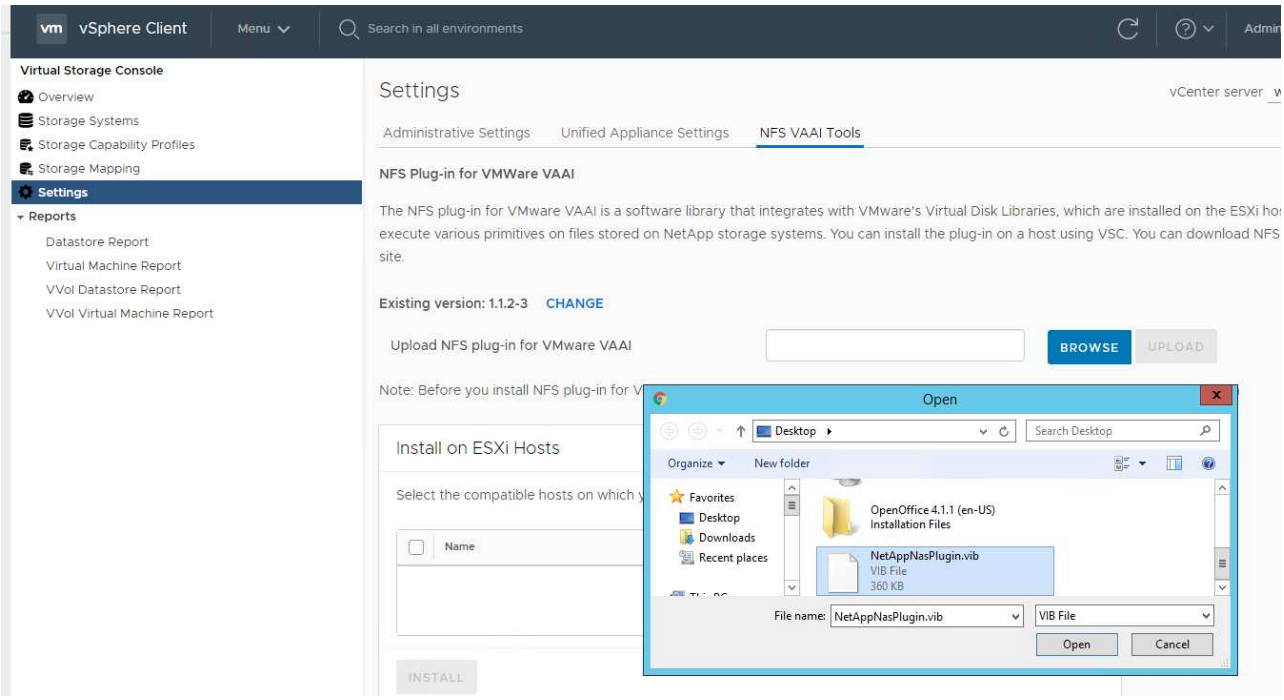
Per scaricare e installare il plug-in NetApp NFS VAAI, attenersi alla seguente procedura:

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.

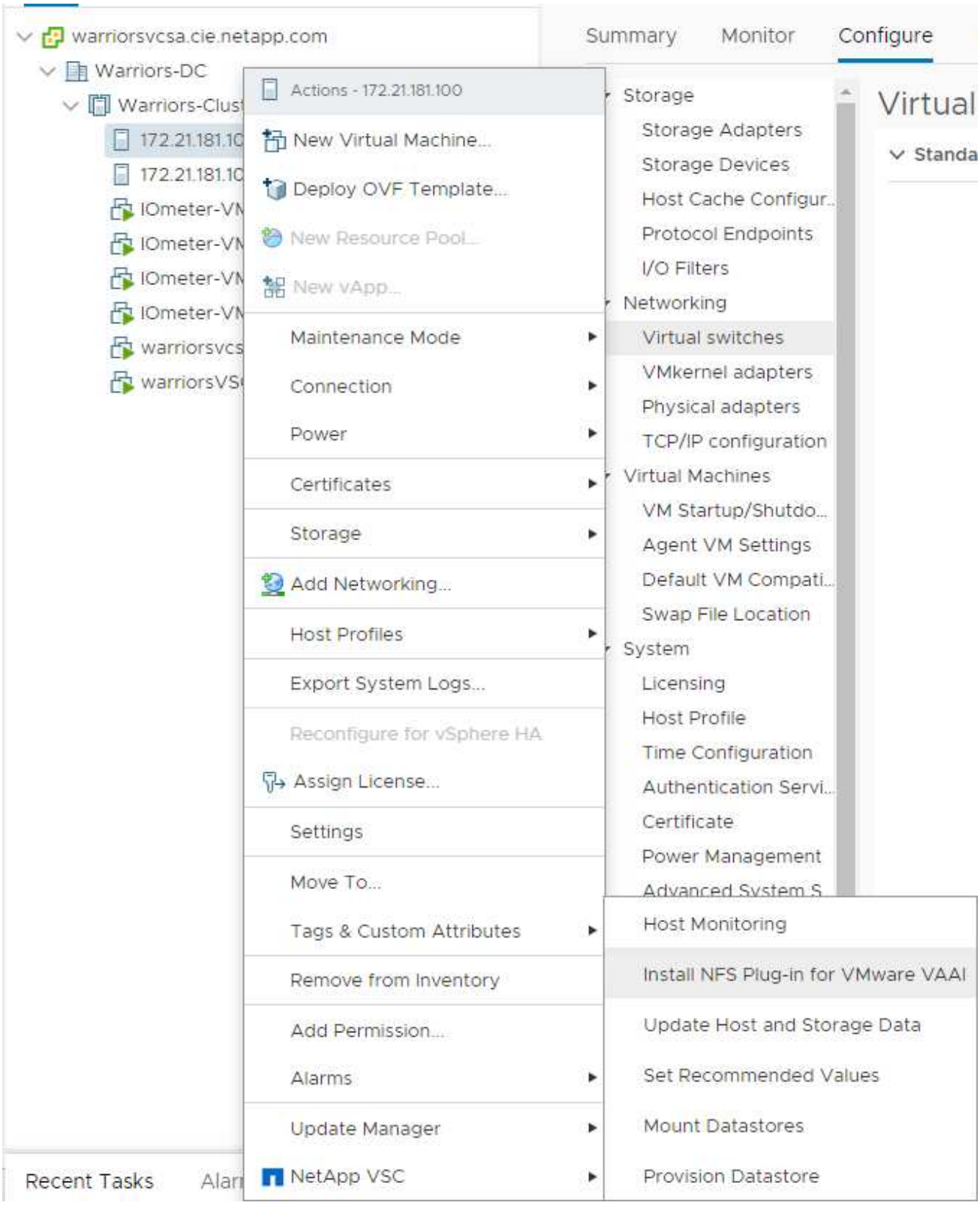
c. Dalla schermata iniziale del client Web vSphere, selezionare Virtual Storage Console.

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.

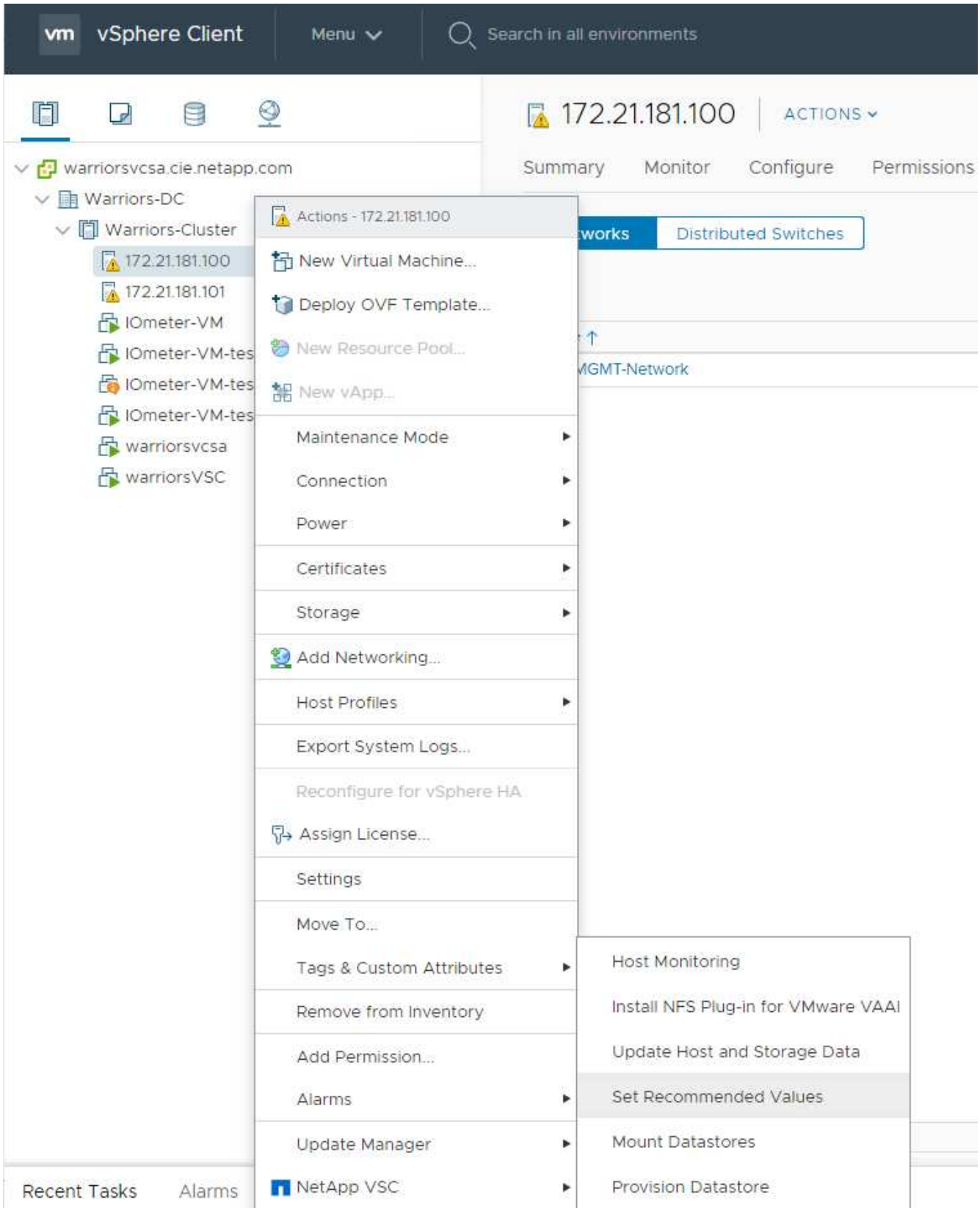
4. Selezionare l'host, quindi scegliere NetApp VSC > Install NFS Plug-in for VMware VAAI.



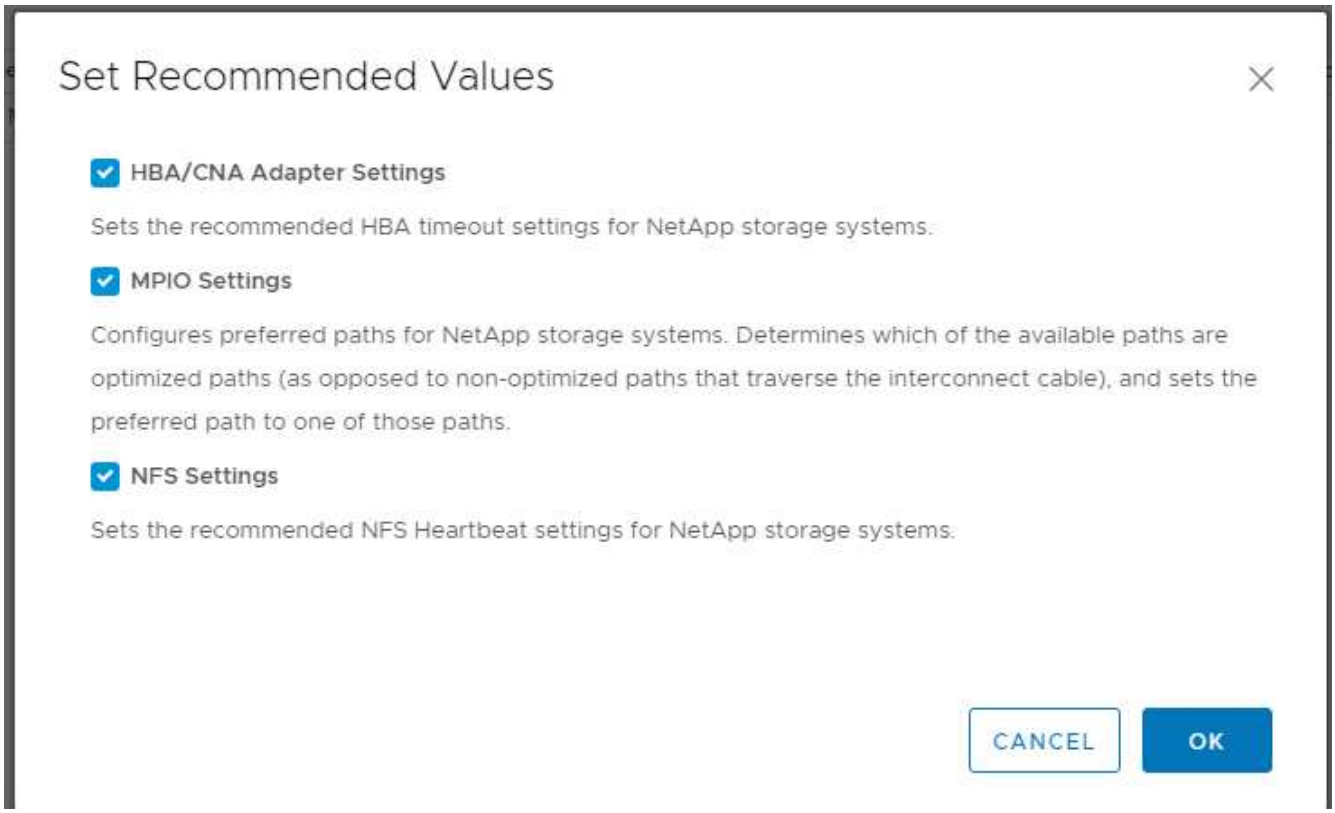
Utilizzare le impostazioni di storage ottimali per gli host ESXi

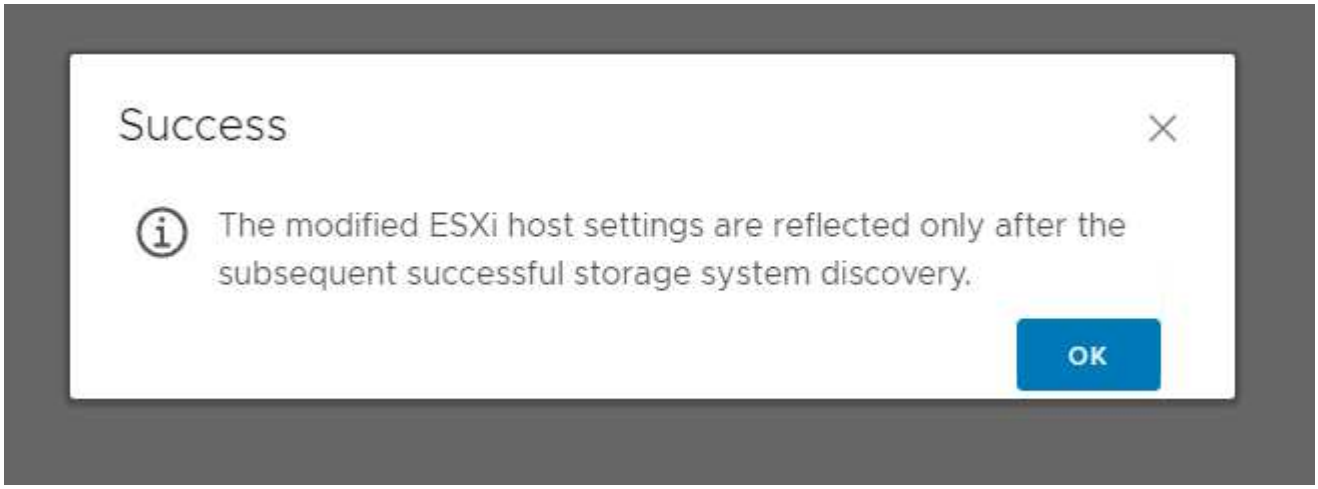
VSC consente la configurazione automatica delle impostazioni relative allo storage per tutti gli host ESXi connessi ai controller di storage NetApp. Per utilizzare queste impostazioni, attenersi alla seguente procedura:

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

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"

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."

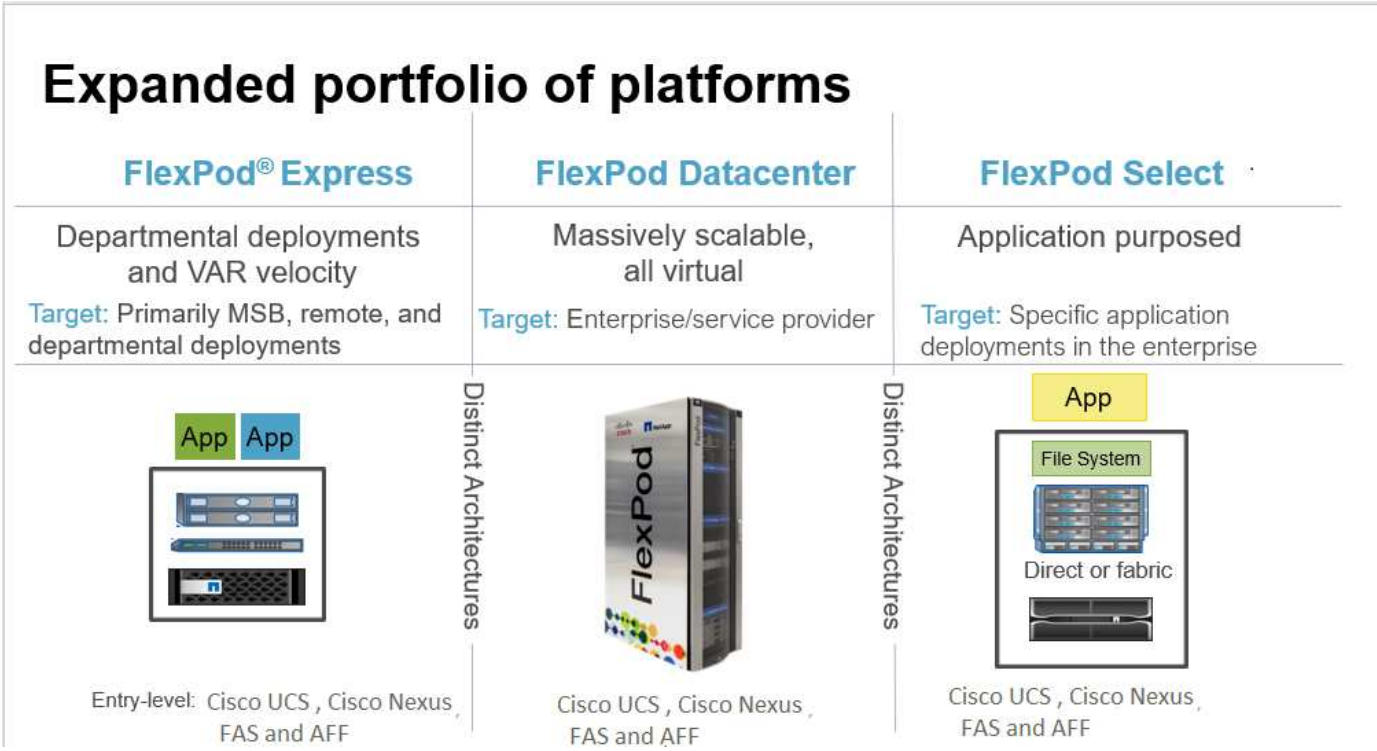
Riepilogo del programma

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.

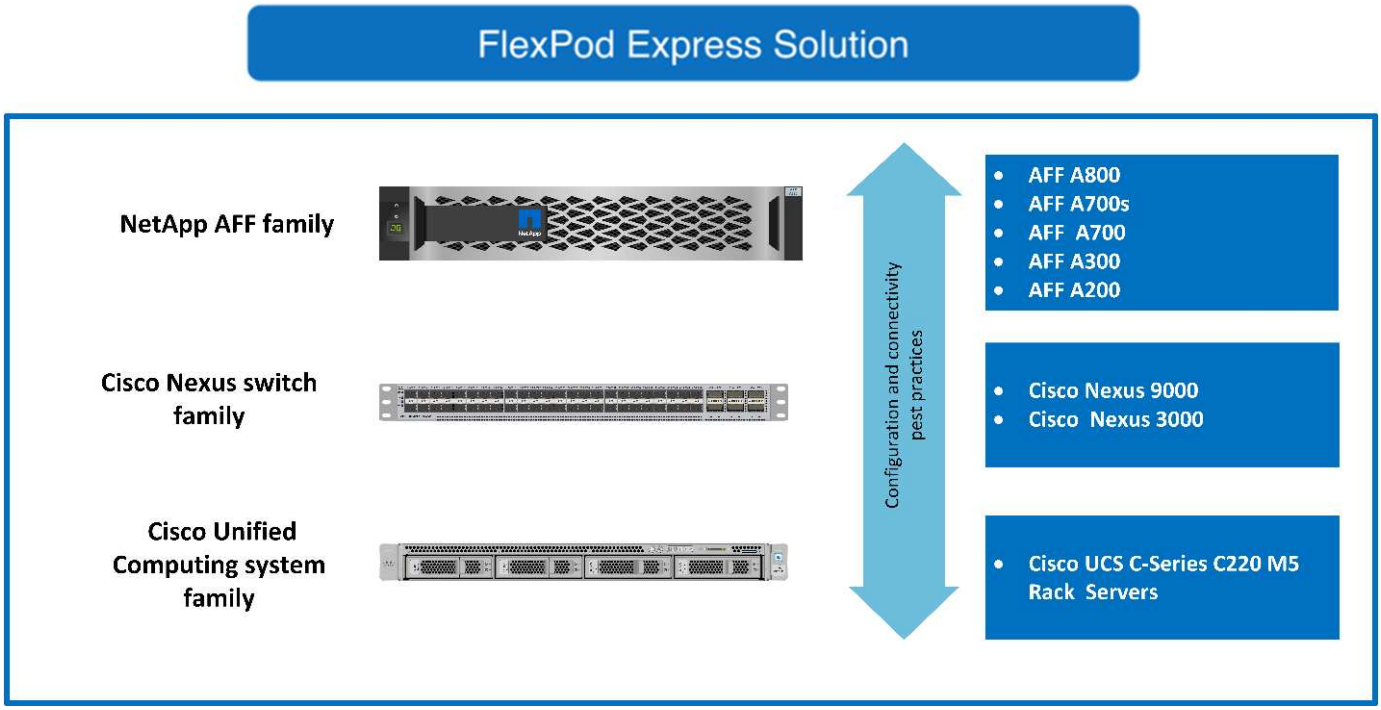
Sebbene questo documento sia validato per AFF A220, questa soluzione supporta anche FAS2700.

"Pagina successiva: Panoramica della soluzione."

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.

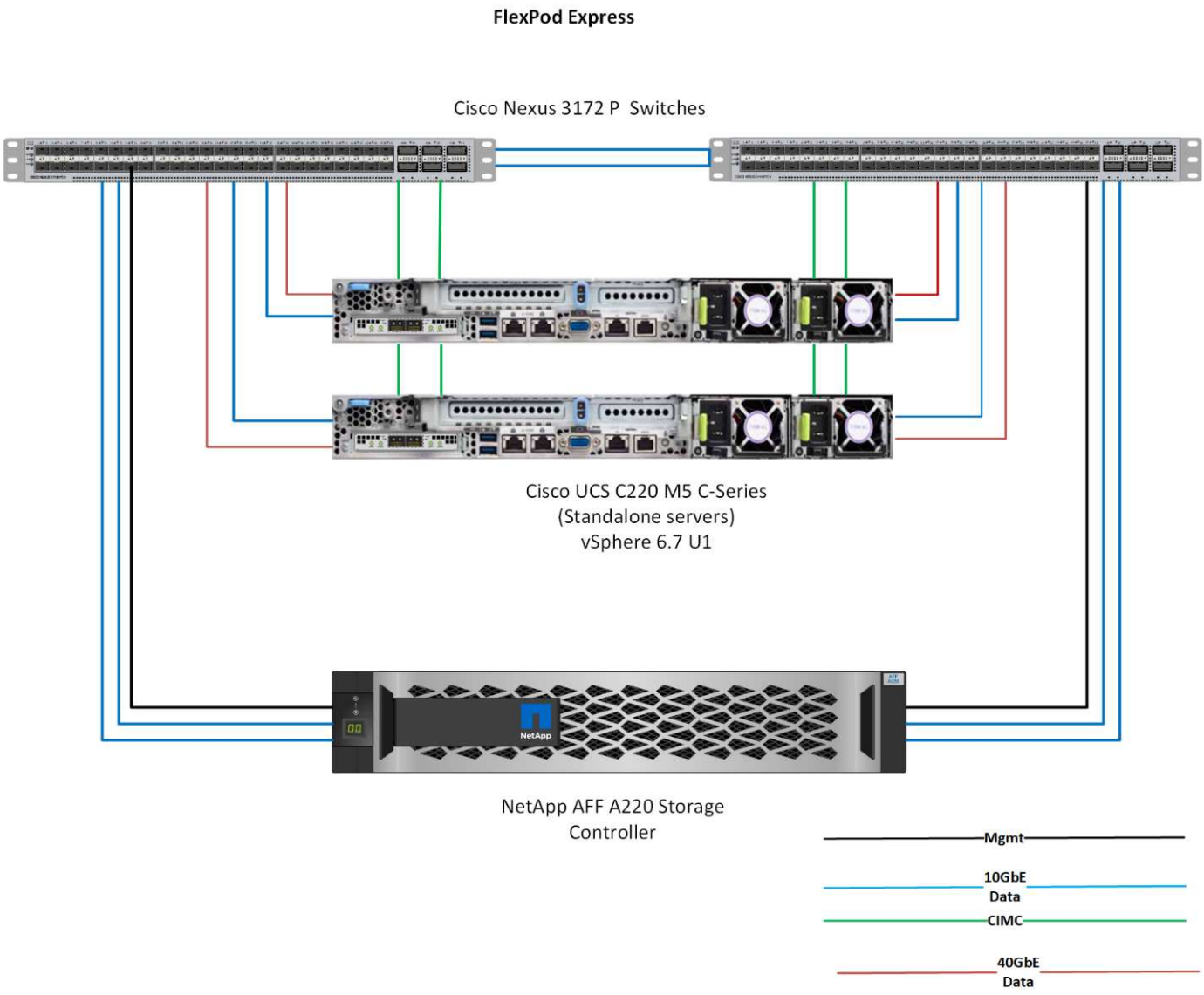


Pubblico di riferimento

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.



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.I7.5.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.

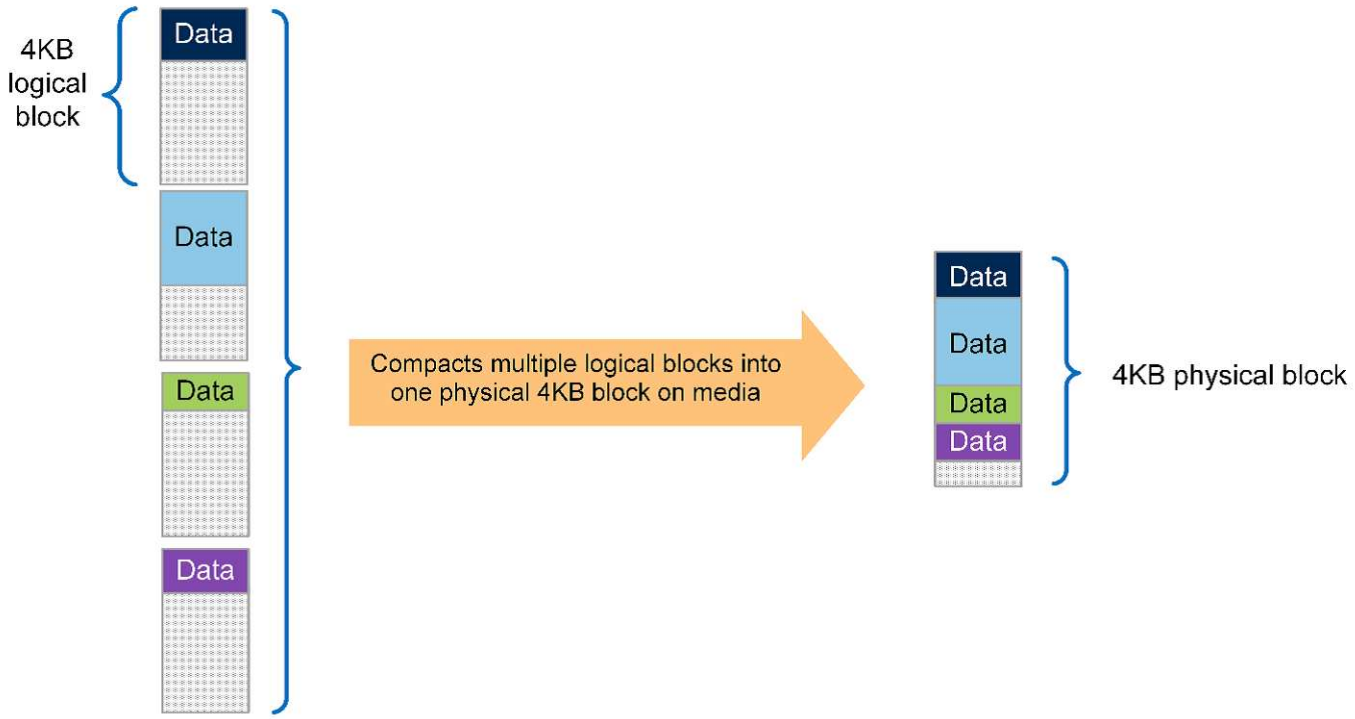
Sistema AFF A220

Per ulteriori informazioni sul sistema hardware AFF A220, consultare "Pagina principale di AFF A-Series".

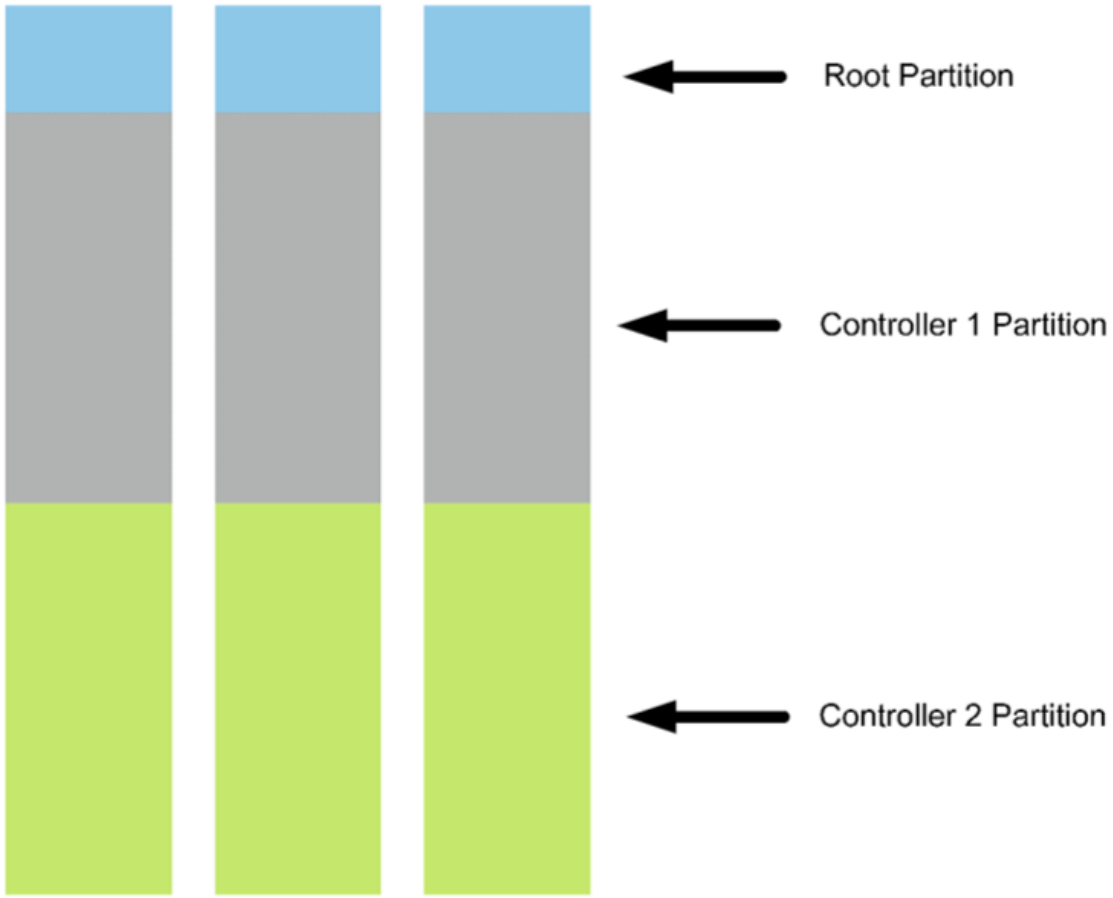
Software ONTAP 9.4

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"

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

  "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

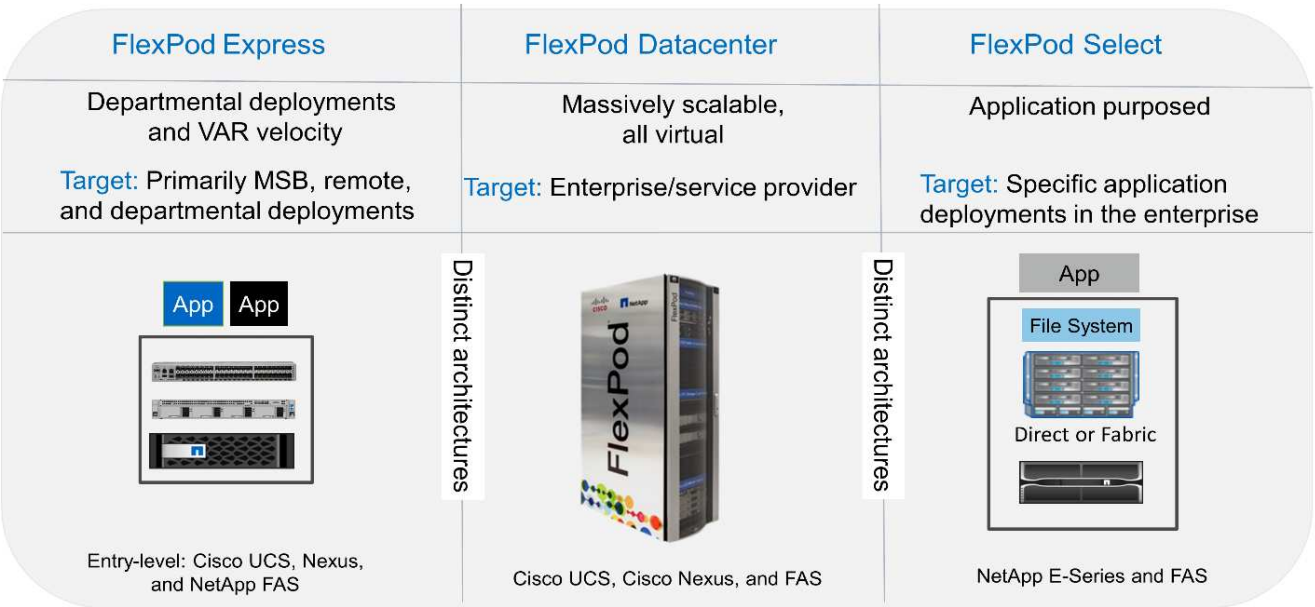
Questa soluzione FlexPod Express fa parte del programma di infrastruttura convergente FlexPod.

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:

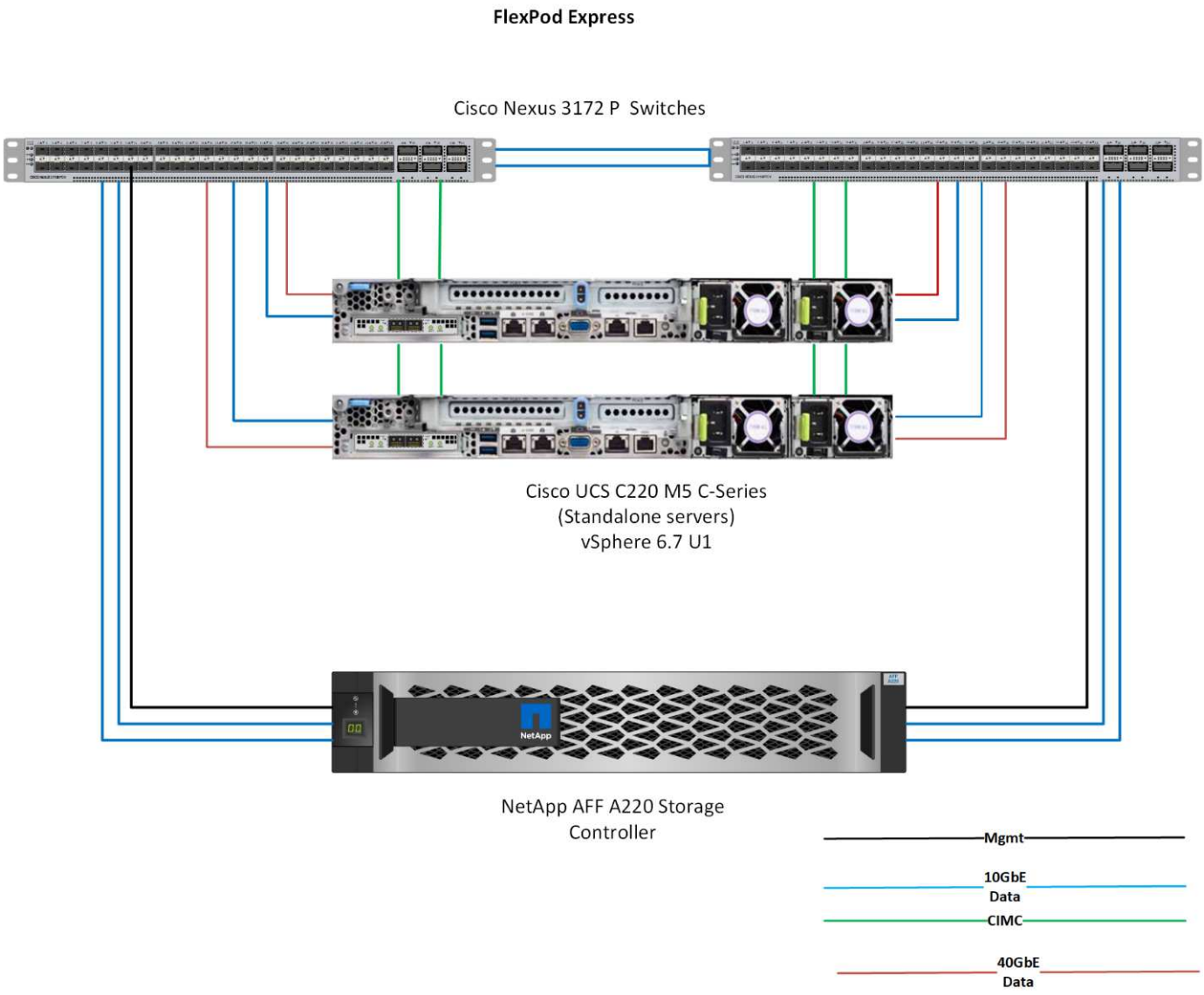
- È stato testato a fondo
- È prescrittivo in natura
- Riduce al minimo i rischi di implementazione
- Accelera il time-to-market

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.



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.

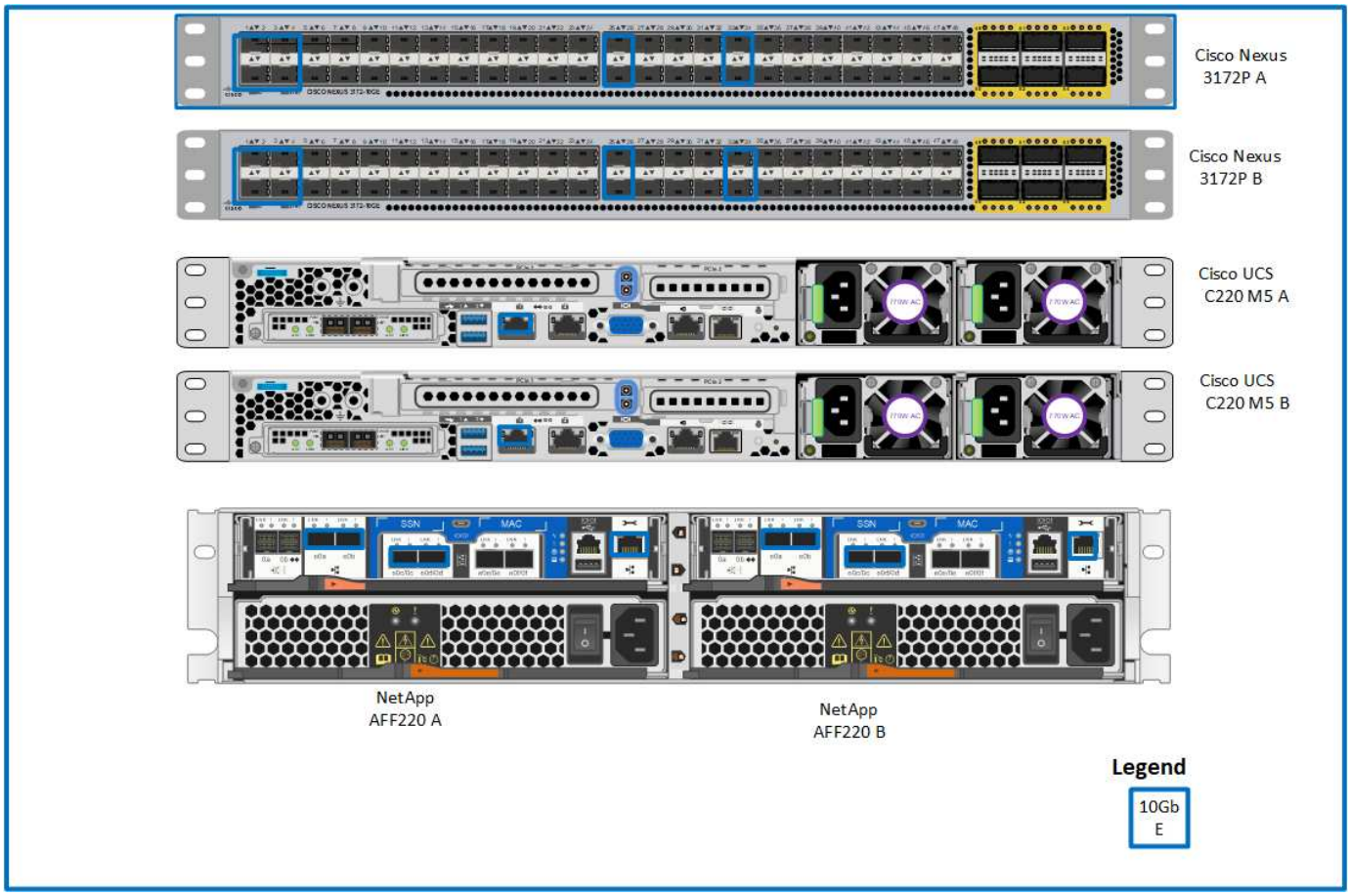
Software	Versione	Dettagli
Cisco Integrated Management Controller (CIMC)	3.1 (3g)	Per server rack Cisco UCS C220 M5
Driver Cisco Nenic	1.0.25.0	Per le schede di interfaccia VIC 1387
Sistema operativo Cisco NX	nxos.7.0.3.I7.5.bin	Per switch Cisco Nexus 3172P
NetApp ONTAP	9.4	Per controller AFF A220

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
```

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

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

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

Abilitare le funzionalità avanzate

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

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

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

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

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

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

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

Eseguire la configurazione spanning-tree globale

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

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

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

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

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

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

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

Definire le VLAN

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

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

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

Configurare le descrizioni delle porte di accesso e di gestione

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

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

Switch Cisco Nexus A

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

Switch Cisco Nexus B

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

Configurare le interfacce di gestione dello storage e del server

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

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

Switch Cisco Nexus A

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

Switch Cisco Nexus B

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

Eseguire la configurazione globale del canale della porta virtuale

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

Un VPC offre i seguenti vantaggi:

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

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

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

Switch Cisco Nexus A

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

Switch Cisco Nexus B

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

Configurare i canali delle porte di storage

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

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

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

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

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

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

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

Configurare le connessioni al server

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

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

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

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

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

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

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

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

Uplink nell'infrastruttura di rete esistente

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

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

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

Procedura di implementazione dello storage NetApp (parte 1)

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

Installazione del controller di storage NetApp serie AFF2xx

NetApp Hardware Universe

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

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

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

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

Controller di storage

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

NetApp ONTAP 9.4

Foglio di lavoro per la configurazione

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

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

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

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

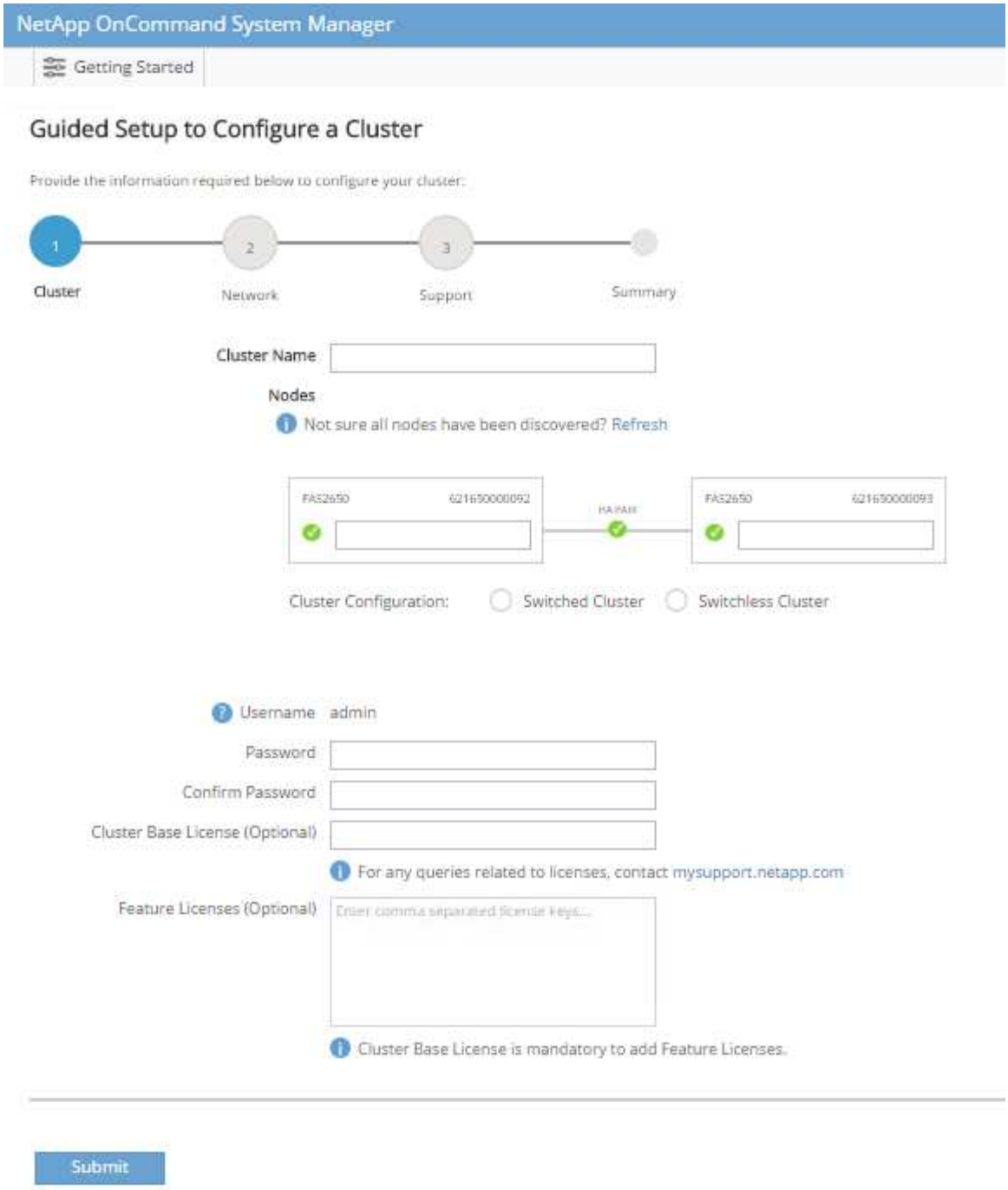
1. Seguire le istruzioni per impostare il nodo A.

```
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.



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

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

   È possibile immettere più indirizzi IP del server DNS.

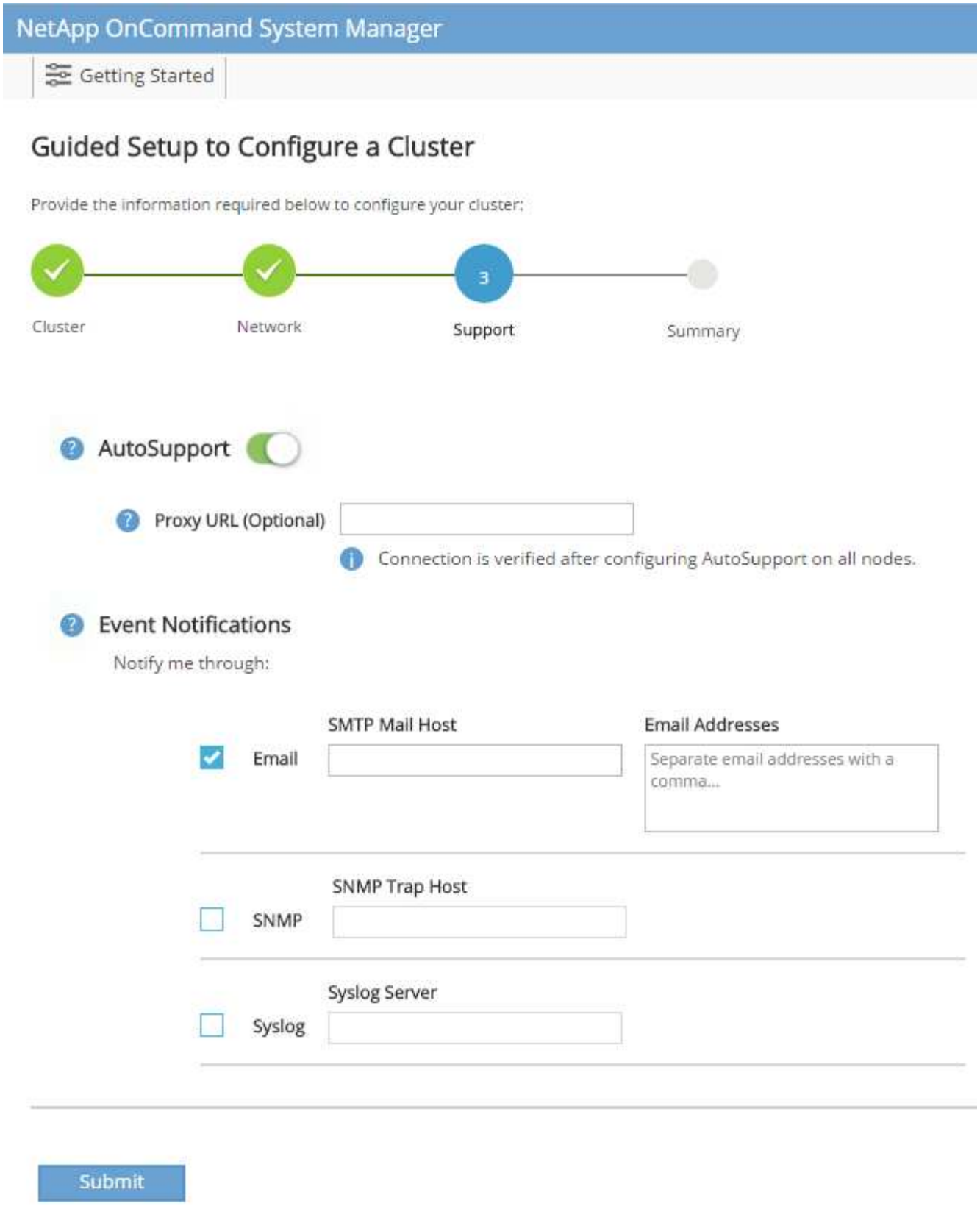
e. Invio `<<var_ntp_server_ip>>` Nel campo Primary NTP Server (Server NTP primario).

   È inoltre possibile inserire un server NTP alternativo.

8. Configurare le informazioni di supporto.

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

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



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

Continuazione della configurazione del cluster di storage

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

Azzerare tutti i dischi spare

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

```
disk zerospares
```

Impostare la personalità delle porte UTA2 a bordo scheda

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

```
AFF A220::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

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

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

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

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

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

Rinominare le interfacce logiche di gestione (LIF)

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

1. Mostra i nomi LIF di gestione correnti.

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

2. Rinominare la LIF di gestione del cluster.

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

3. Rinominare la LIF di gestione del nodo B.

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

Impostare il revert automatico sulla gestione del cluster

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

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

Configurare l'interfaccia di rete del Service Processor

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

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

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

Abilitare il failover dello storage in ONTAP

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

1. Verificare lo stato del failover dello storage.

```
storage failover show
```

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

2. Attivare il failover su uno dei due nodi.

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

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

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

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

```
cluster ha show
```

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

```
High Availability Configured: true
```

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

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

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

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

```
storage failover hwassist show
```

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

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

Creare un dominio di trasmissione MTU con frame jumbo in ONTAP

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

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

Rimuovere le porte dati dal dominio di trasmissione predefinito

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

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

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

Disattiva il controllo di flusso sulle porte UTA2

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

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

Configurare IFGRP LACP in ONTAP

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

Dal prompt del cluster, completare la seguente procedura.

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

Configurare i frame jumbo in NetApp ONTAP

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

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

Creare VLAN in ONTAP

Per creare VLAN in ONTAP, attenersi alla seguente procedura:

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

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

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

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

3. Creare porte MGMT-VLAN.

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

Creare aggregati in ONTAP

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

Per creare aggregati, eseguire i seguenti comandi:

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

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

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

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

Configurare il fuso orario in ONTAP

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

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

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

Configurare SNMP in ONTAP

Per configurare SNMP, attenersi alla seguente procedura:

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

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

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

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

Configurare SNMPv1 in ONTAP

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

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

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

Configurare SNMPv3 in ONTAP

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

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

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

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

Configurare HTTPS AutoSupport in ONTAP

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

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

Creare una macchina virtuale per lo storage

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

1. Eseguire `vserver create` comando.

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

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

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

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

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

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

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

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

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

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

Configurare NFSv3 in ONTAP

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

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

Per configurare NFS su SVM, eseguire i seguenti comandi:

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

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

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

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

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

Creare un servizio iSCSI in ONTAP

Per creare il servizio iSCSI, completare la seguente fase:

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

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

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

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

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

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

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

3. Creare le relazioni di mirroring.

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

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

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

Configurare l'accesso HTTPS in ONTAP

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

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

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

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

```
security certificate show
```

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

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

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

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

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

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

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

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

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

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

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

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

Creare un volume NetApp FlexVol in ONTAP

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

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

Attiva la deduplica in ONTAP

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

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

Creare LUN in ONTAP

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

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

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

Creazione di LIF iSCSI in ONTAP

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

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

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

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

Creare LIF NFS in ONTAP

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

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

1. Creare una LIF NFS.

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

Aggiungere l'amministratore SVM dell'infrastruttura

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

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

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

1. Eseguire il seguente comando:

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

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

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

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

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

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

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

Procedura di implementazione dei server rack Cisco UCS C-Series

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

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

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

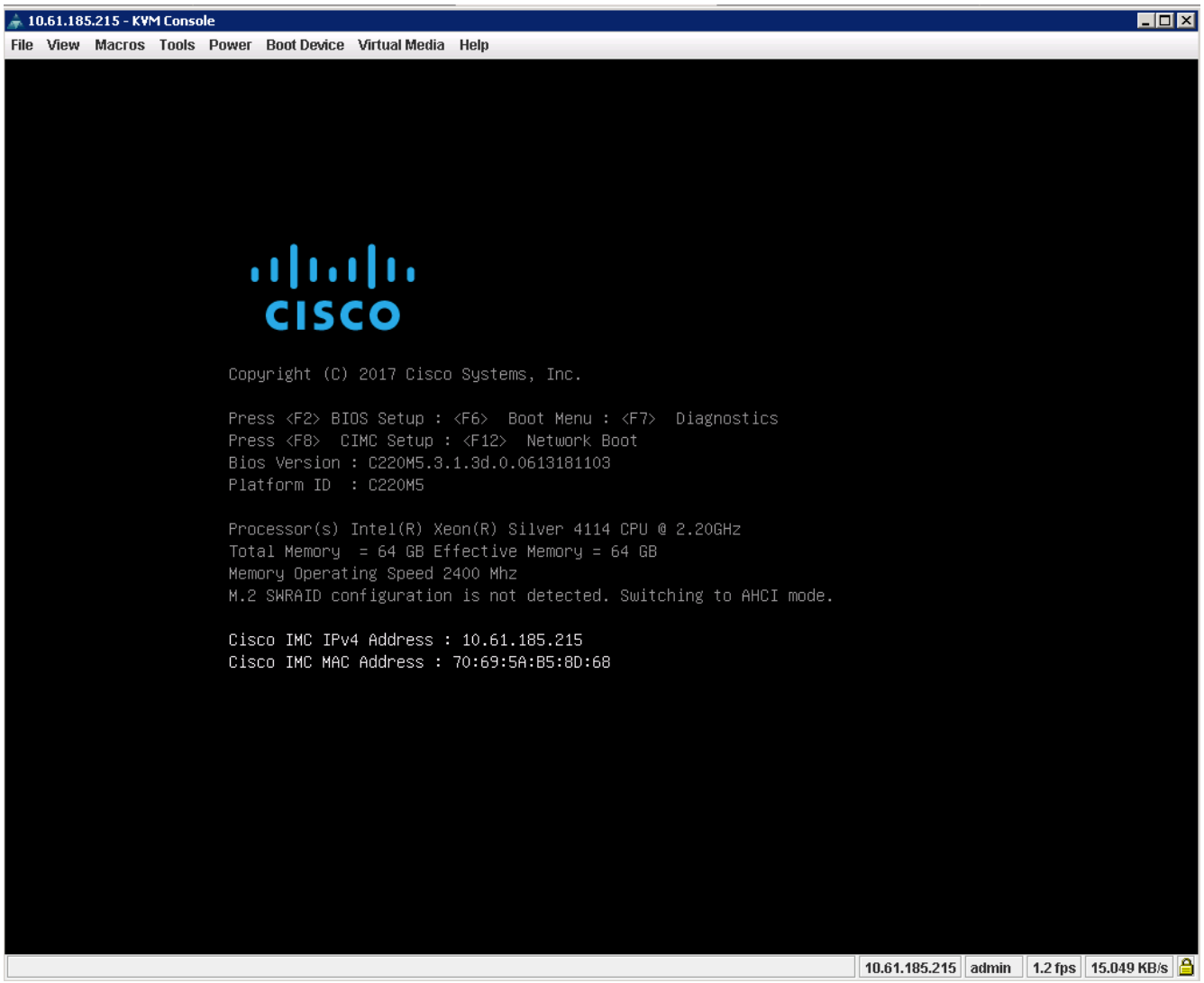
La seguente tabella elenca le informazioni necessarie per configurare CIMC per ogni server standalone Cisco UCS C-Series.

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

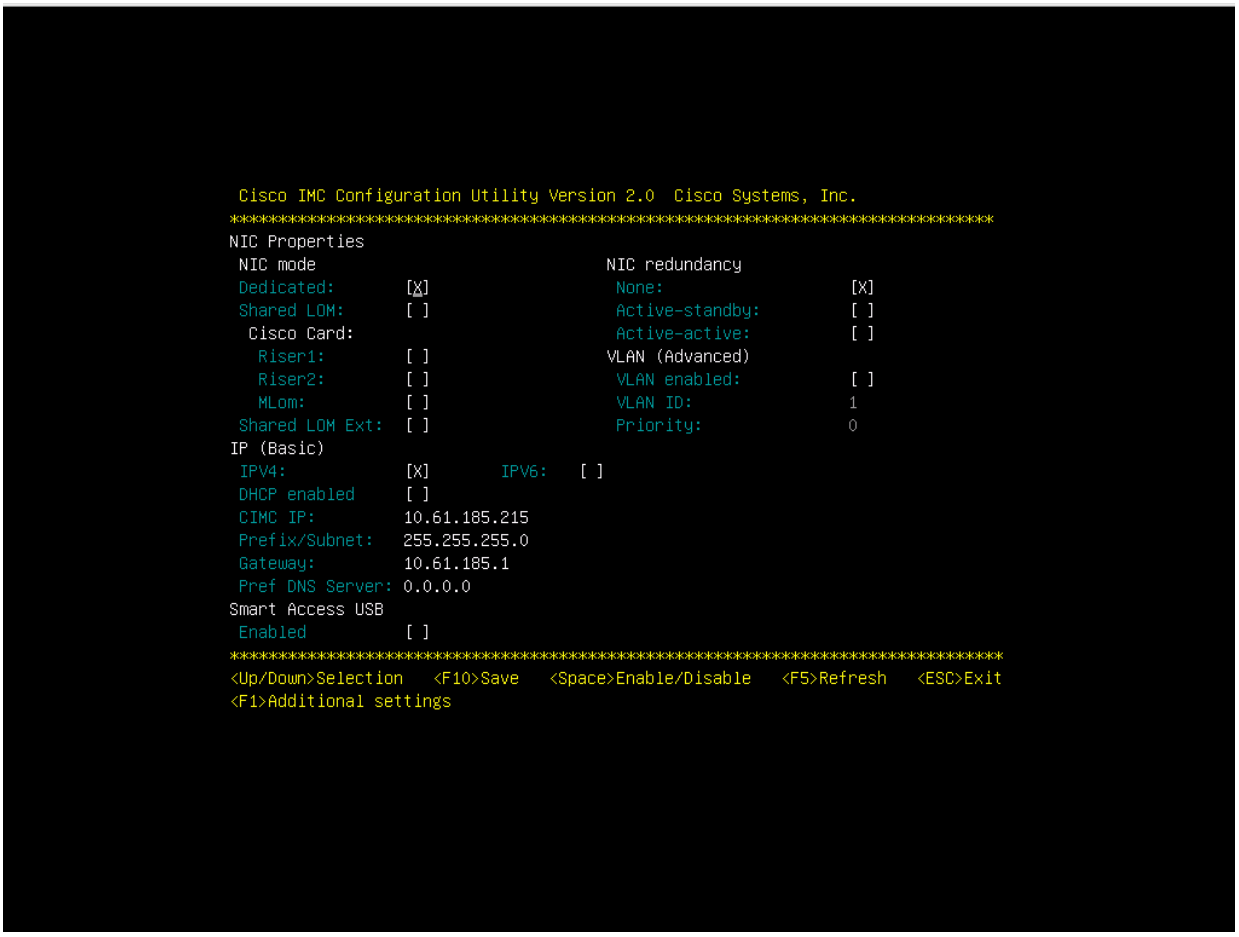
La versione di CIMC utilizzata per questa convalida è CIMC 3.1.3(g).

Tutti i server

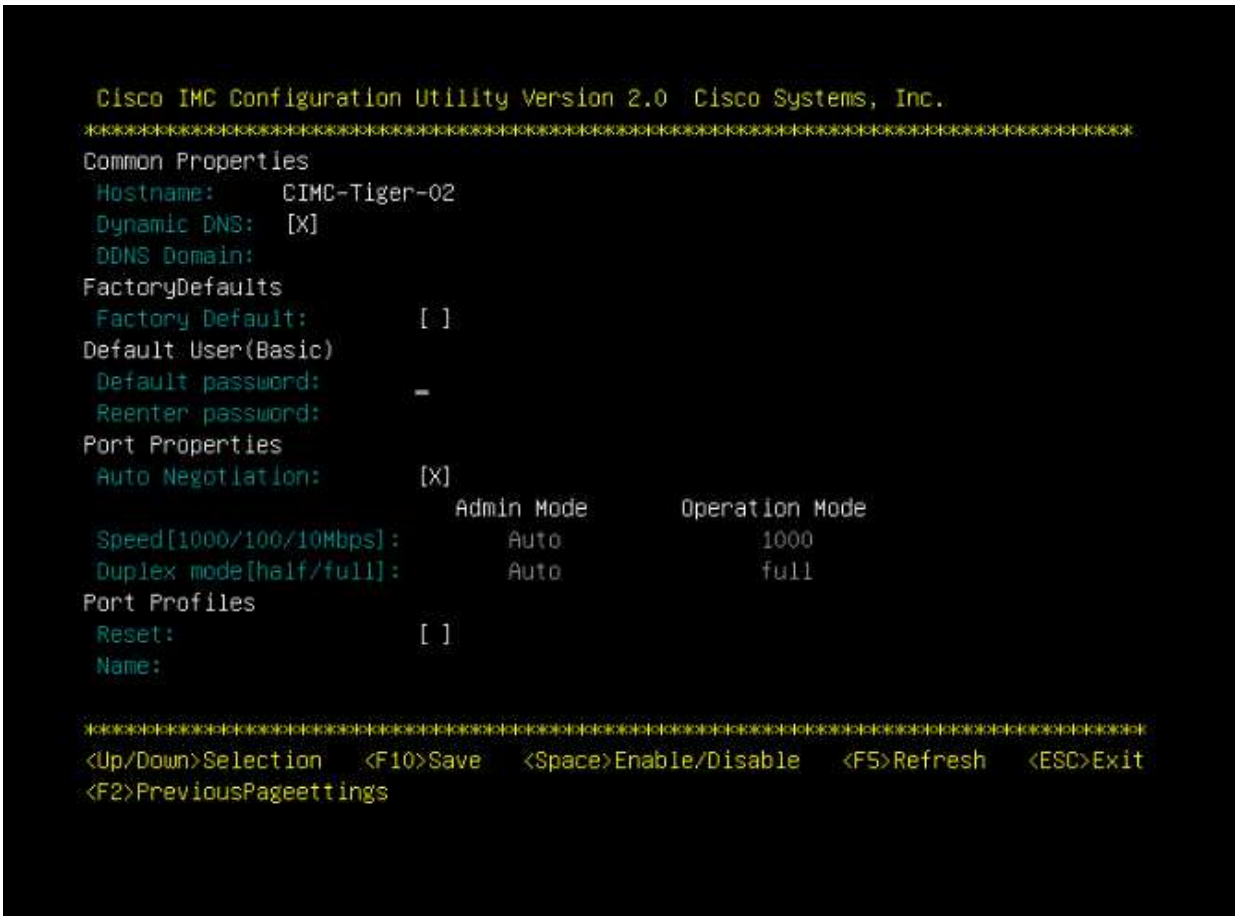
1. Collegare il dongle KVM (tastiera, video e mouse) Cisco (fornito con il server) alla porta KVM sulla parte anteriore del server. Collegare un monitor VGA e una tastiera USB alle porte dongle KVM appropriate.
2. Accendere il server e premere F8 quando richiesto per accedere alla configurazione CIMC.



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



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



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

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

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

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

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

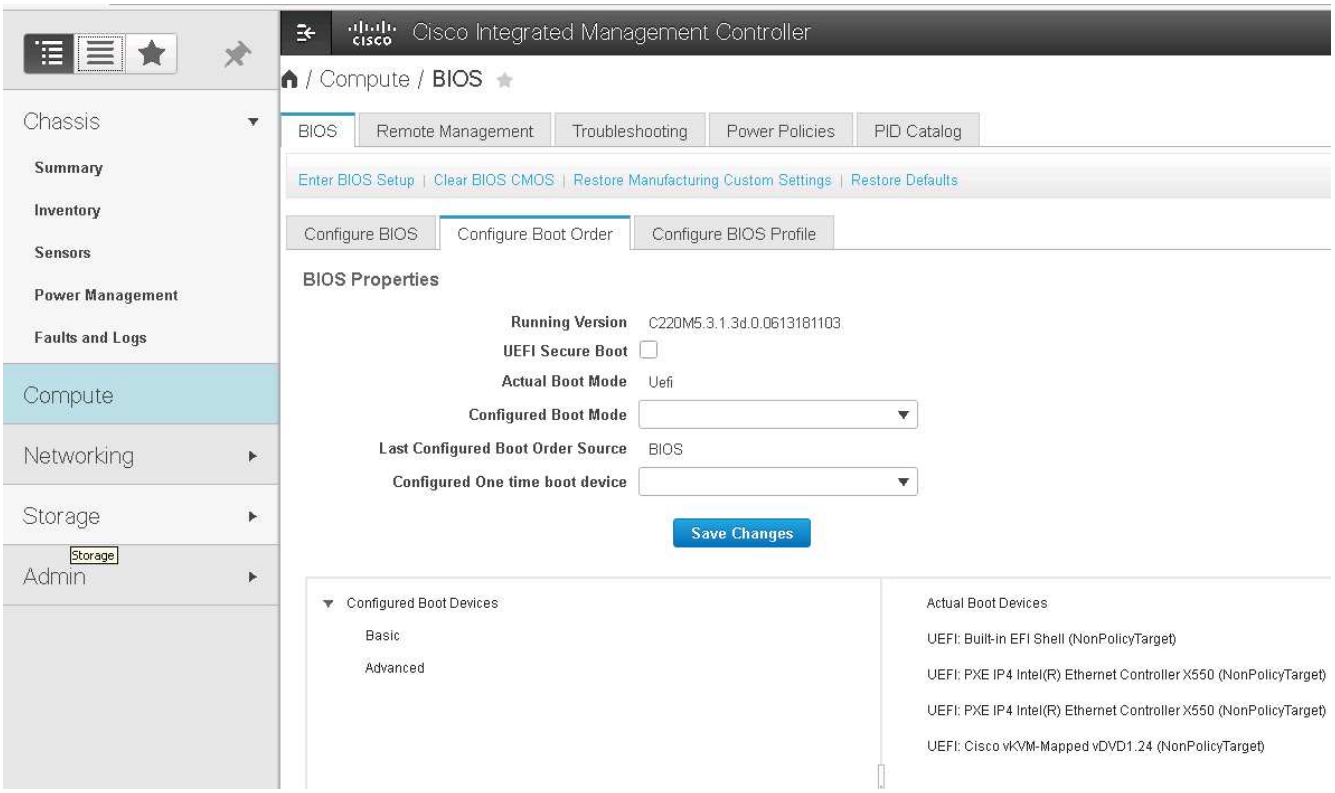
Dettaglio	Valore di dettaglio
Nome dell'iniziatore host ESXi	[var_ucs_initiator_name_A]
IP iSCSI-A host ESXi	[var_esxi_host_iscsiA_ip]
Host ESXi iSCSI-A network mask	[var_esxi_host_iscsiA_mask]
ESXi host iSCSI Un gateway predefinito	[var_esxi_host_iscsiA_gateway]
Nome B dell'iniziatore host ESXi	[var_ucs_initiator_name_B]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

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

Configurazione dell'ordine di avvio

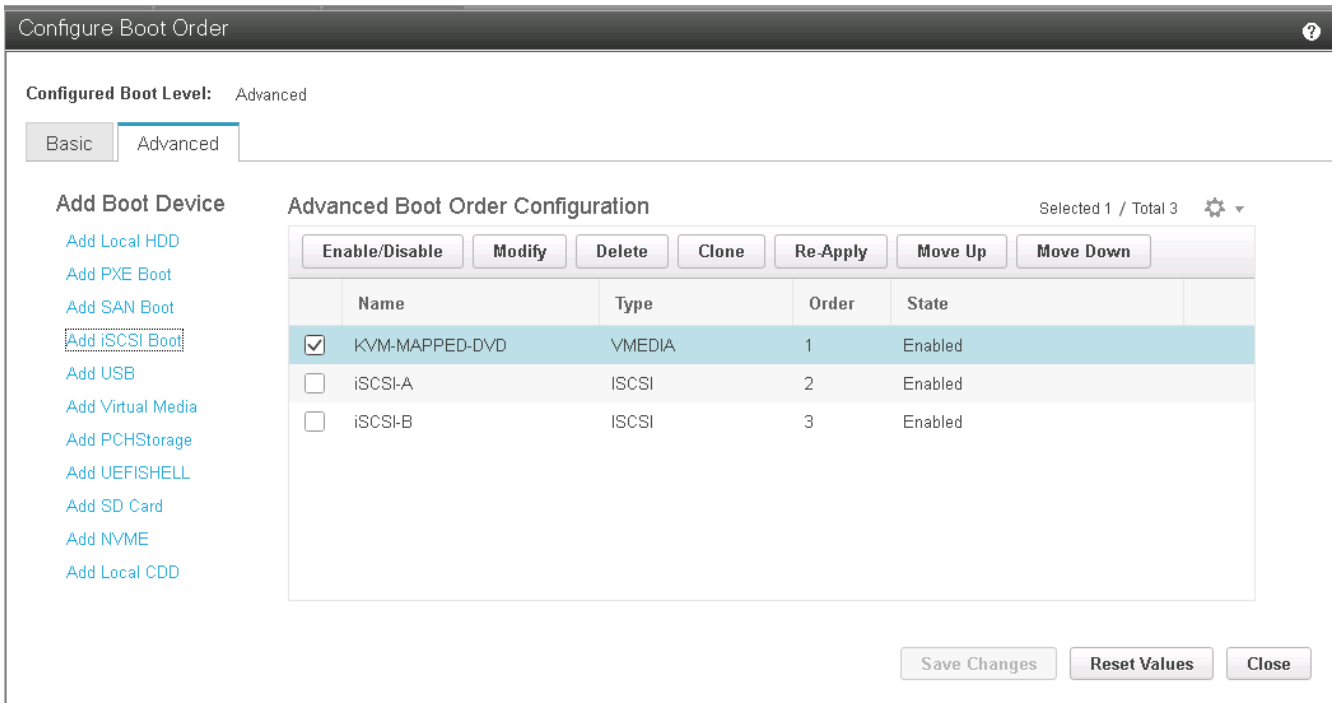
Per impostare la configurazione dell'ordine di avvio, attenersi alla seguente procedura:

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



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

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

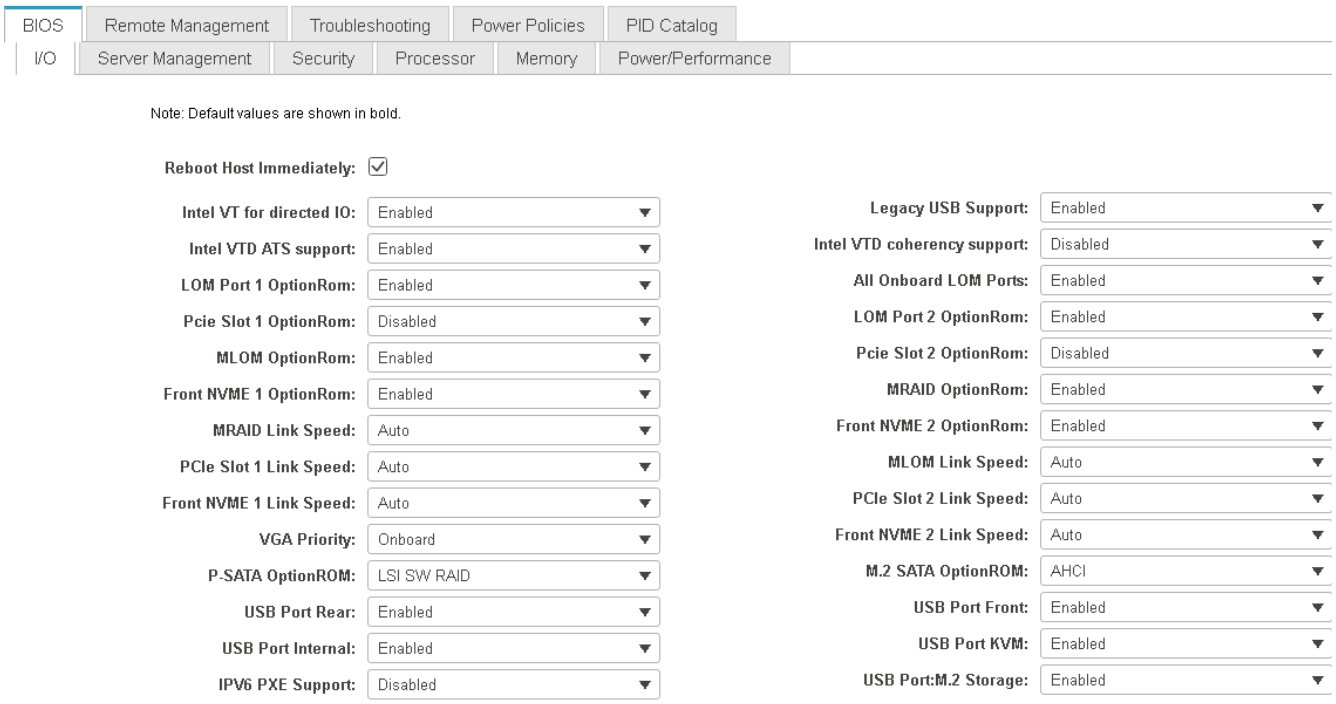


6. Riavviare il server per eseguire l'avvio con il nuovo ordine di avvio.

Disattivazione del controller RAID (se presente)

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

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



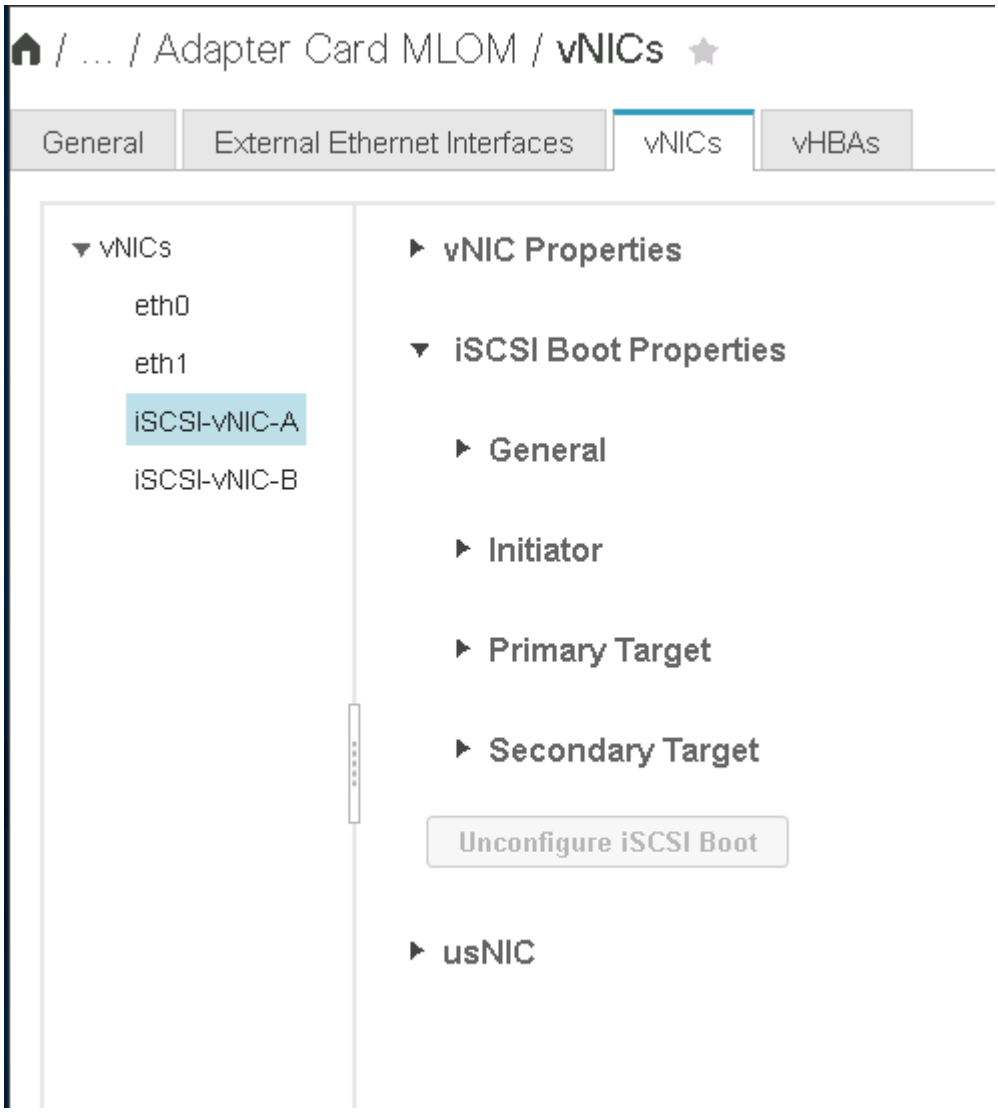
Configurare Cisco VIC1387 per l'avvio iSCSI

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

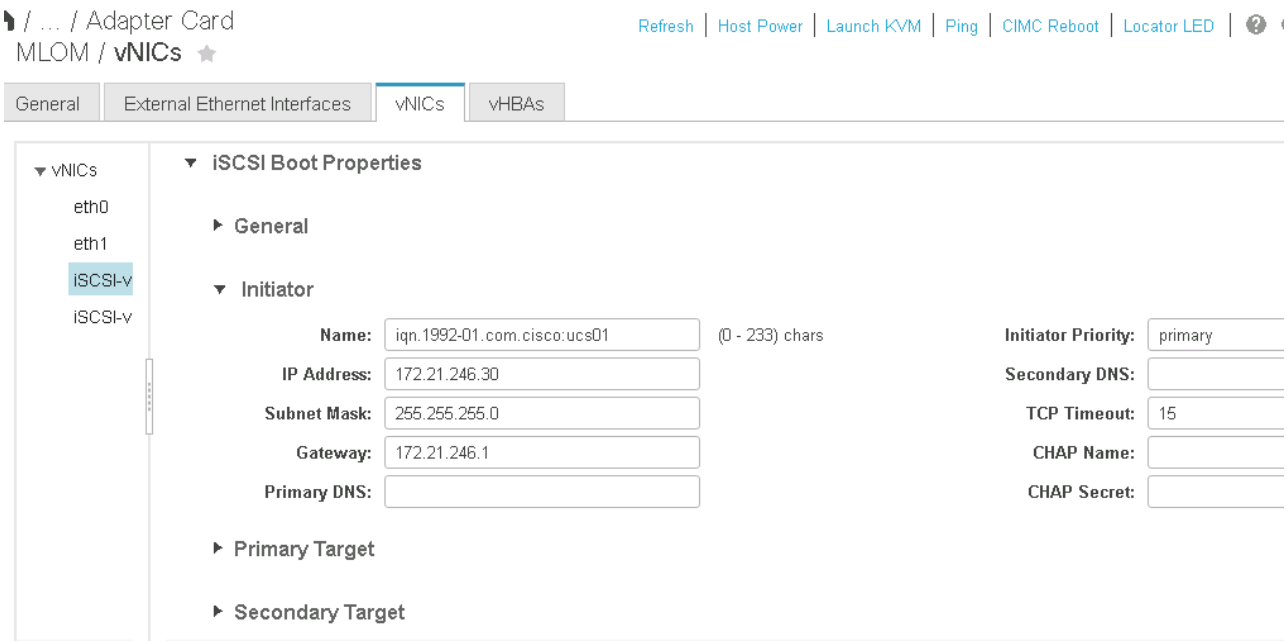
Creare vNIC iSCSI

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

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



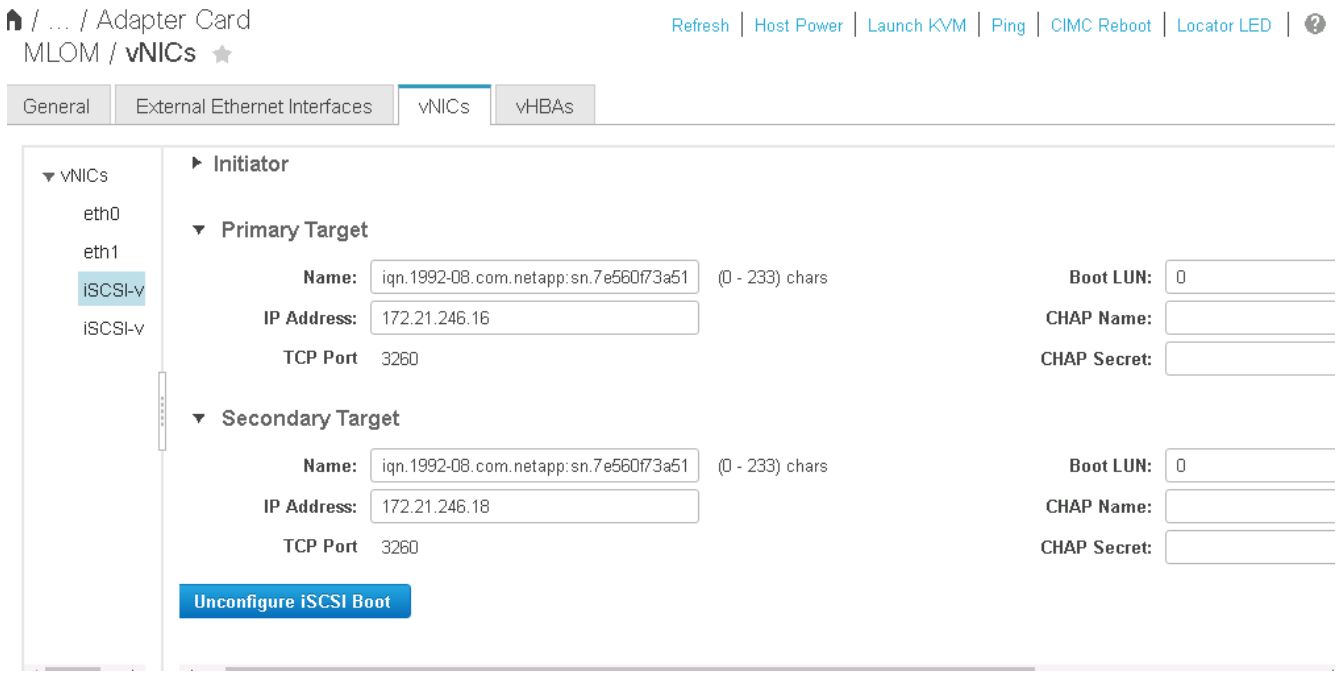
6. In iSCSI Boot Properties (Proprietà di avvio iSCSI), immettere i dettagli dell'iniziatore:
   - Nome:[var_ucsa_initiator_name_a]
   - Indirizzo IP:[var_esxi_hostA_iscsiA_ip]
   - Subnet mask:[var_esxi_hostA_iscsiA_mask]
   - Gateway:[var_esxi_hostA_iscsiA_gateway]



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

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

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



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

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

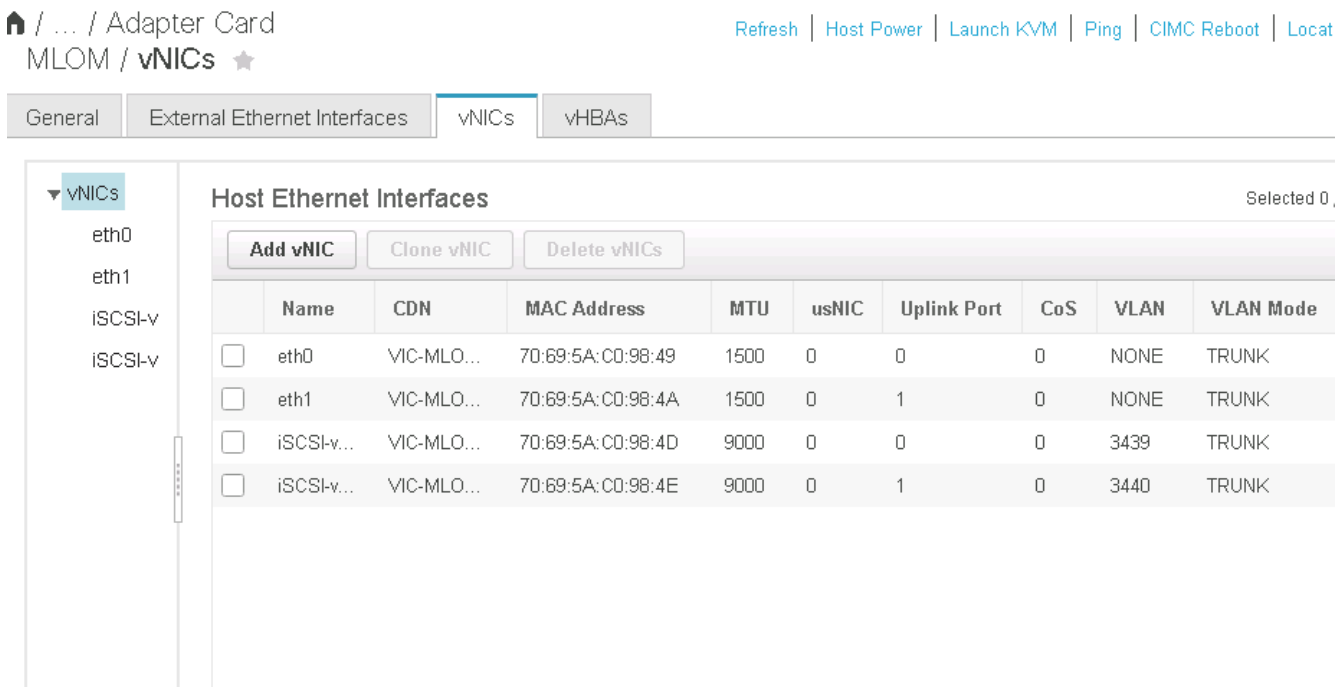
    > Assicurarsi di registrare i nomi IQN per ogni vNIC. Sono necessari per un passaggio successivo.

15. Fare clic su Configura ISCSI.

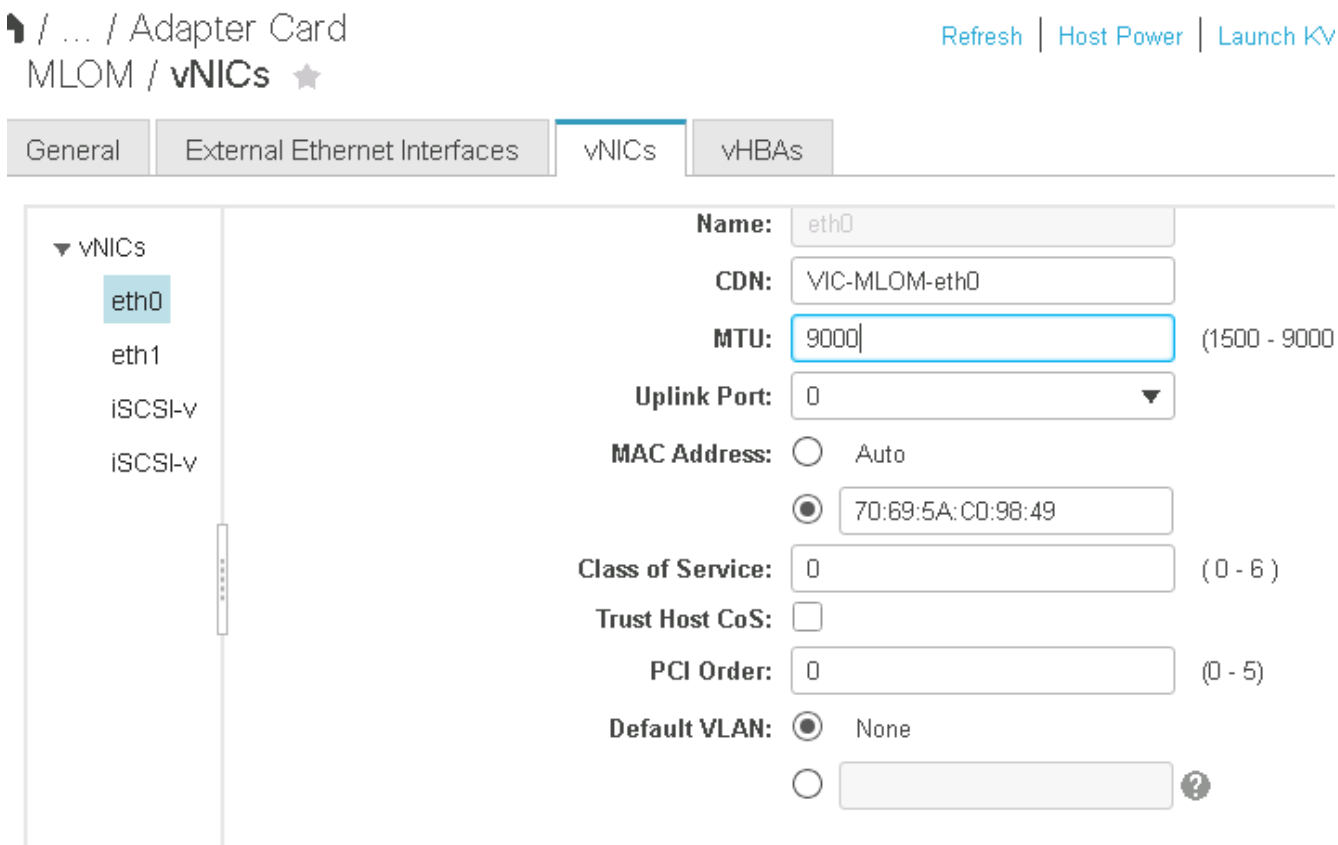
16. Ripetere questa procedura per configurare l'avvio iSCSI per il server Cisco UCS B.

Configurare vNIC per ESXi

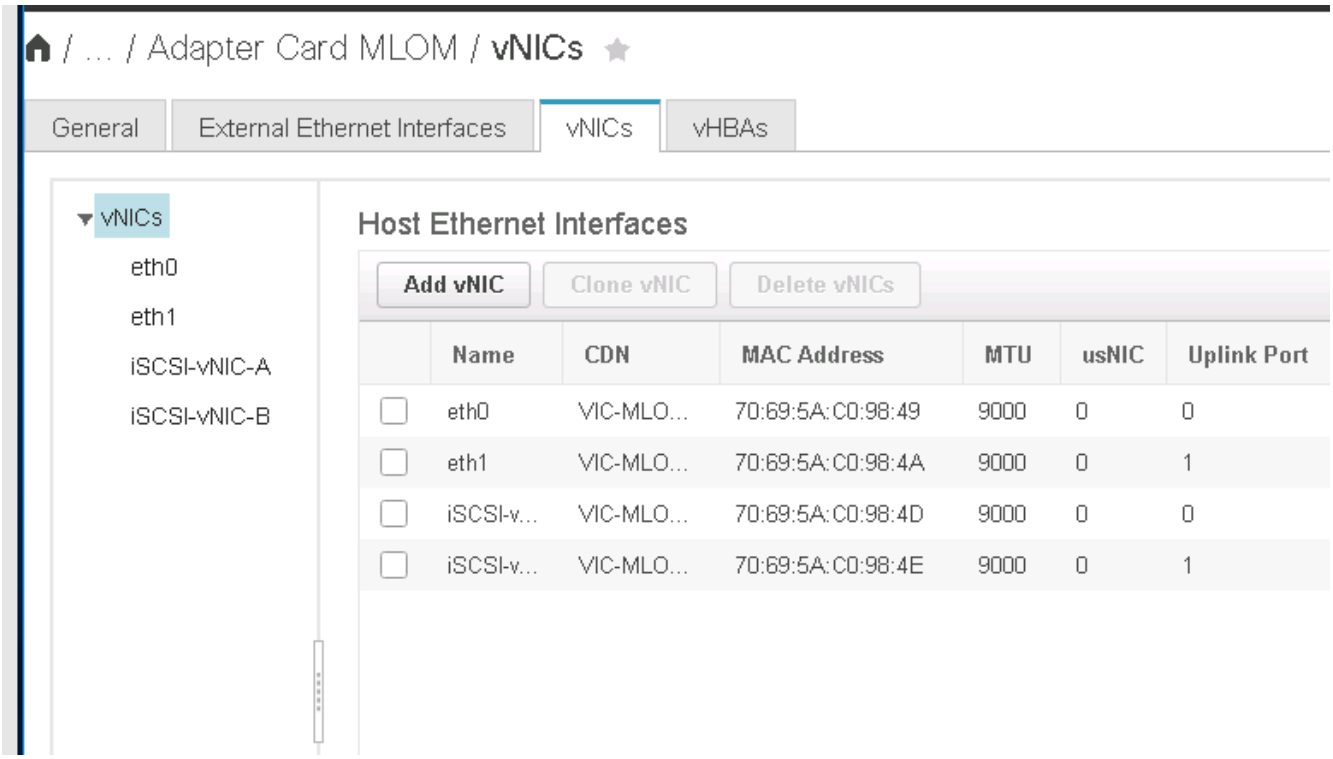
1. Dalla finestra del browser dell'interfaccia CIMC, fare clic su Inventory (inventario), quindi su Cisco VIC adapter (adattatori VIC Cisco) nel riquadro destro.
2. In schede adattatore, selezionare Cisco UCS VIC 1387, quindi selezionare le vNIC sottostanti.



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



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



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

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

Procedura di implementazione dello storage NetApp AFF (parte 2)

Configurazione dello storage di boot SAN ONTAP

Creare igroups iSCSI

Per creare igroups, completare il seguente passaggio:

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

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

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

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

Mappare le LUN di avvio a igroups

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

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

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

"Procedura di implementazione di VMware vSphere 6.7."

Procedura di implementazione di VMware vSphere 6.7

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

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

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

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

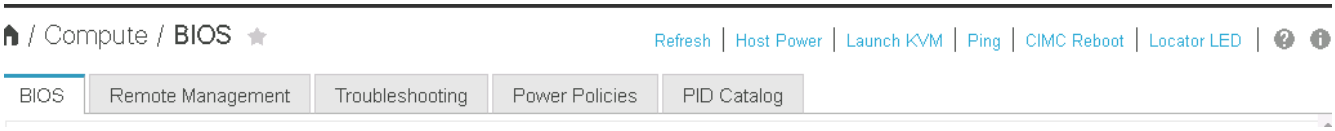
Questa procedura deve essere completata per tutti i nodi aggiuntivi aggiunti al cluster.

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

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

Tutti gli host

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



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

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

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

Installare VMware ESXi

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

Scarica L'immagine personalizzata di ESXI 6.7 Cisco

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

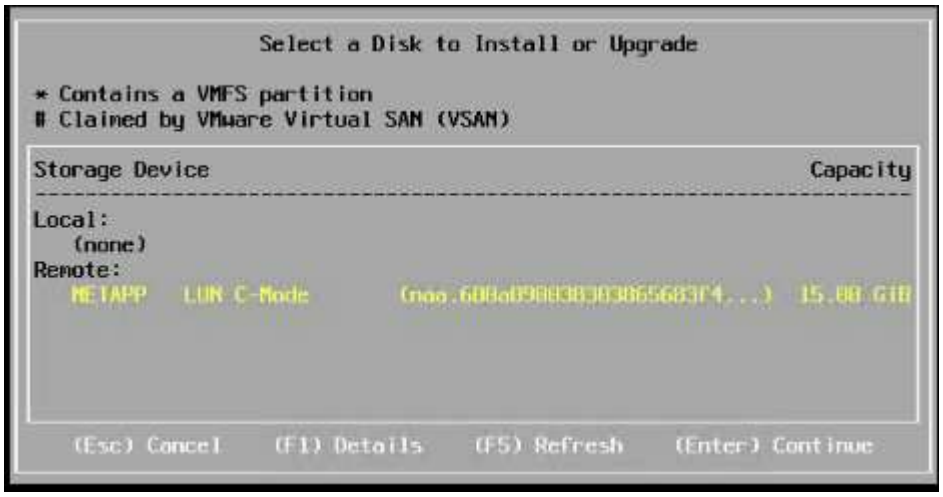
Tutti gli host

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

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

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

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



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

Configurare il networking per la gestione degli host VMware ESXi

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

Tutti gli host

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

   Selezionare le porte corrispondenti a eth0 e eth1 in CIMC.

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

Configurare l'host ESXi

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

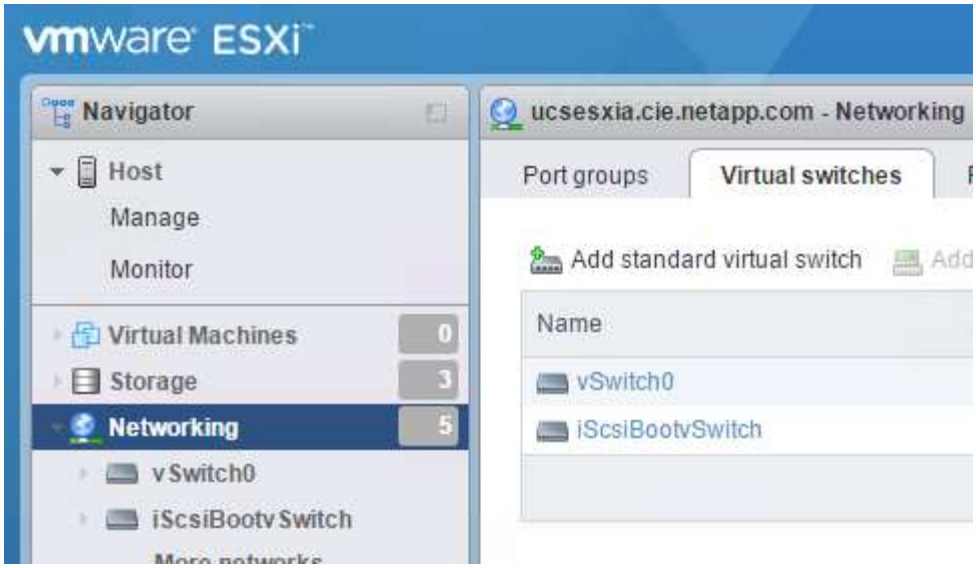
Dettaglio	Valore
Nome host ESXi	
IP di gestione host ESXi	
Maschera di gestione host ESXi	
Gateway di gestione host ESXi	
IP NFS host ESXi	
ESXi host NFS mask	
Gateway NFS host ESXi	
IP vMotion host ESXi	
Host ESXi vMotion mask	
Gateway vMotion host ESXi	
IP iSCSI-A host ESXi	
Host ESXi iSCSI-A mask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

Accedere all’host ESXi

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

Configurare l’avvio iSCSI

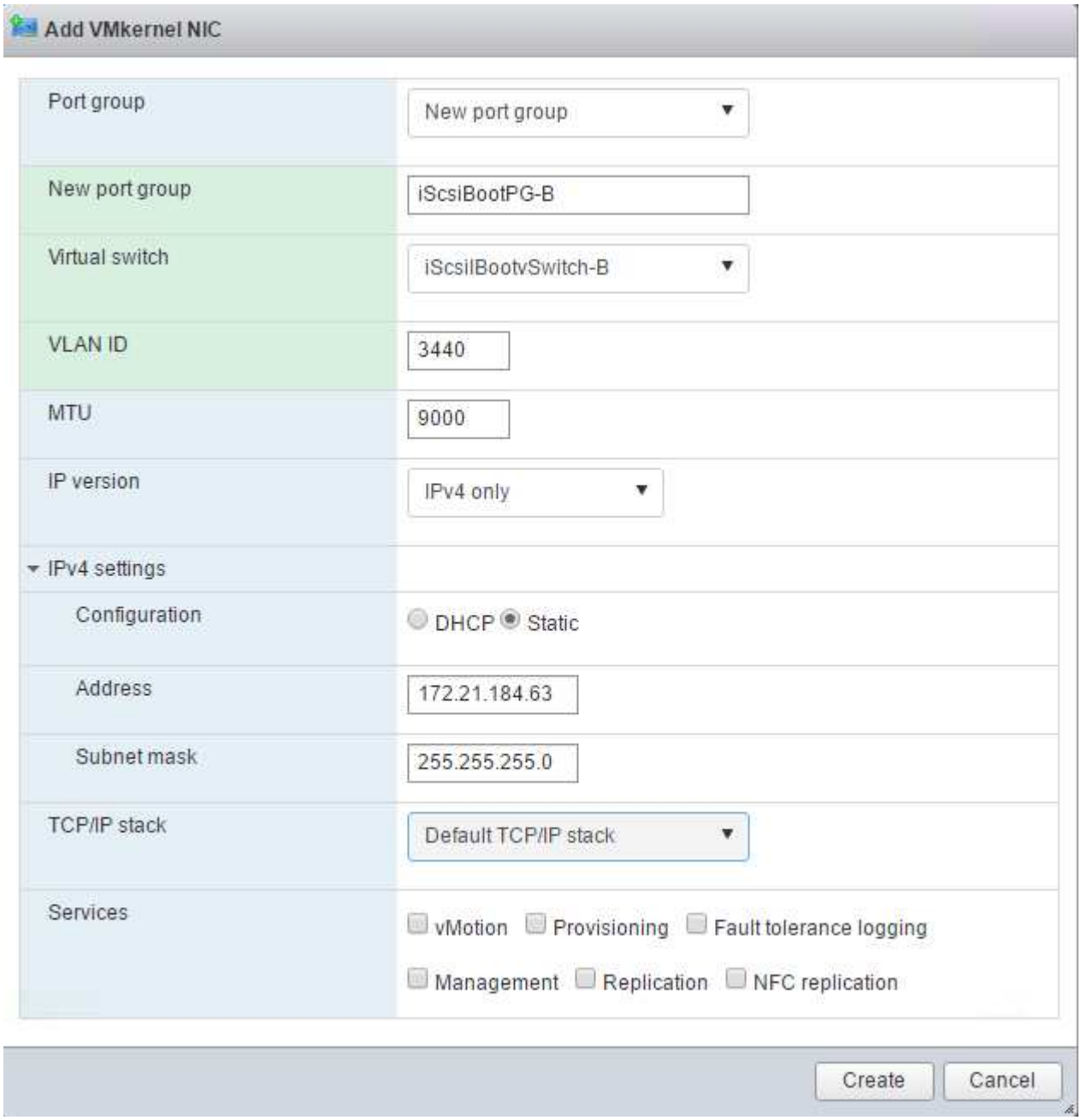
1. Selezionare Networking (rete) a sinistra.
2. A destra, selezionare la scheda Virtual Switches (interruttori virtuali).



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

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

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

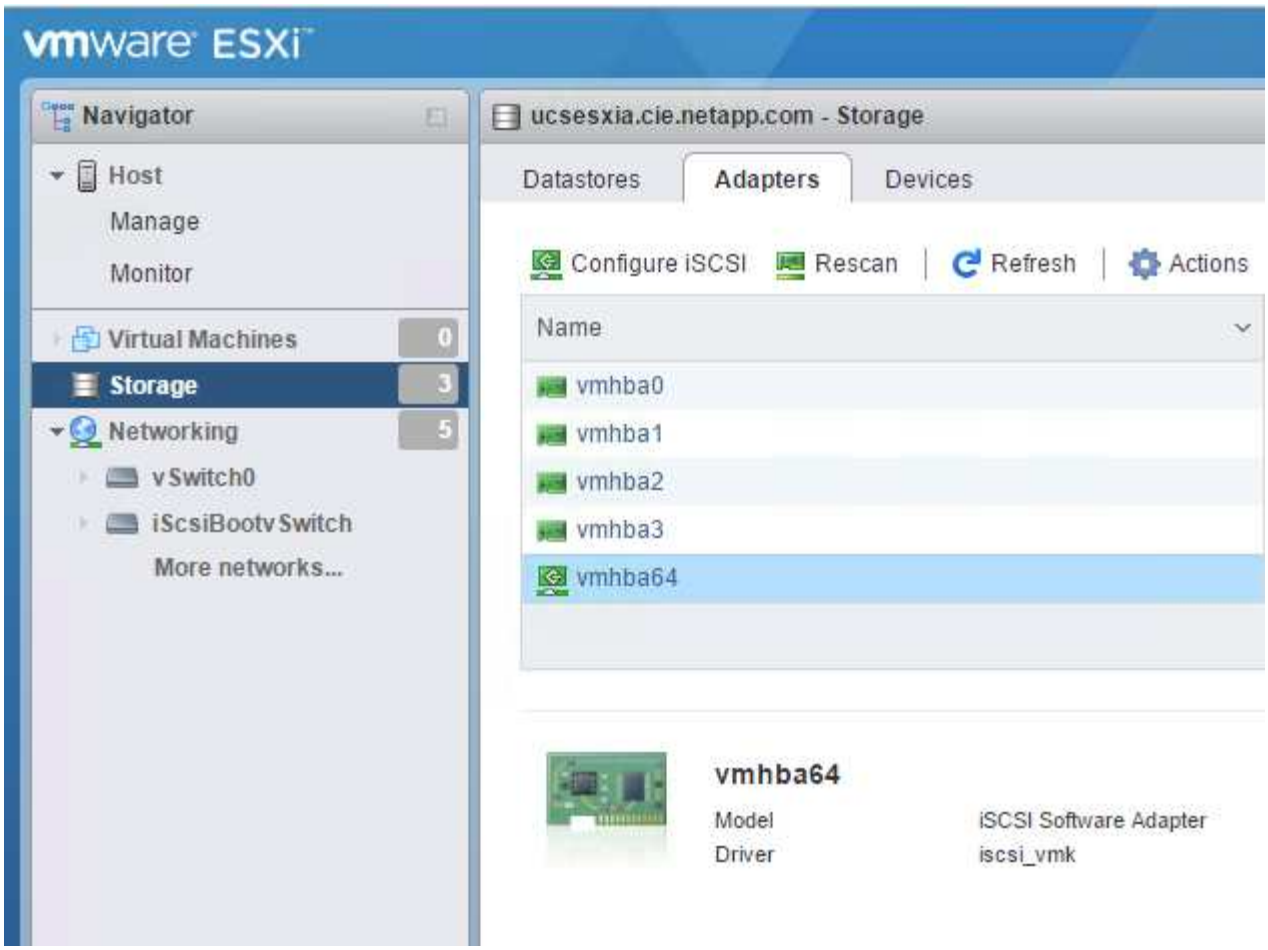


Impostare MTU su 9000 ON `iScsiBootPG- A.`

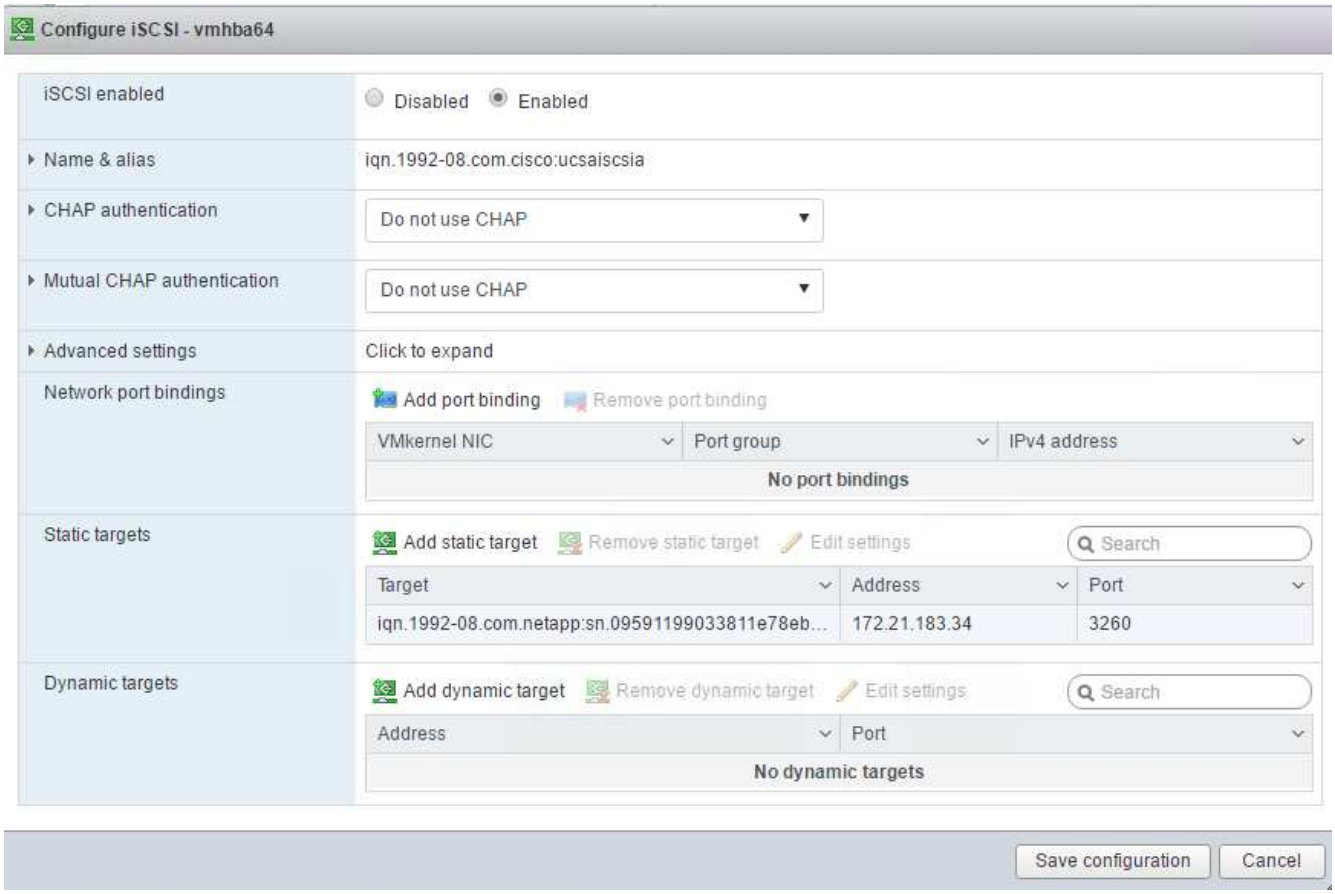
Configurare il multipathing iSCSI

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

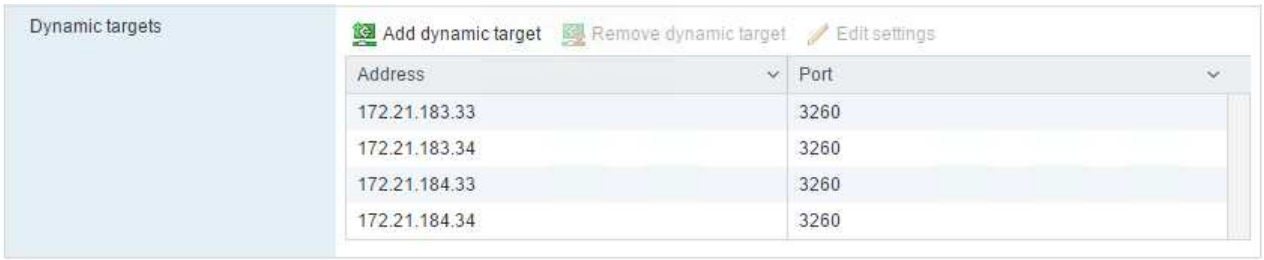
1. Selezionare Storage (archiviazione) nel riquadro di navigazione a sinistra. Fare clic su adattatori.
2. Selezionare l'adattatore software iSCSI e fare clic su Configure iSCSI (Configura iSCSI).



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



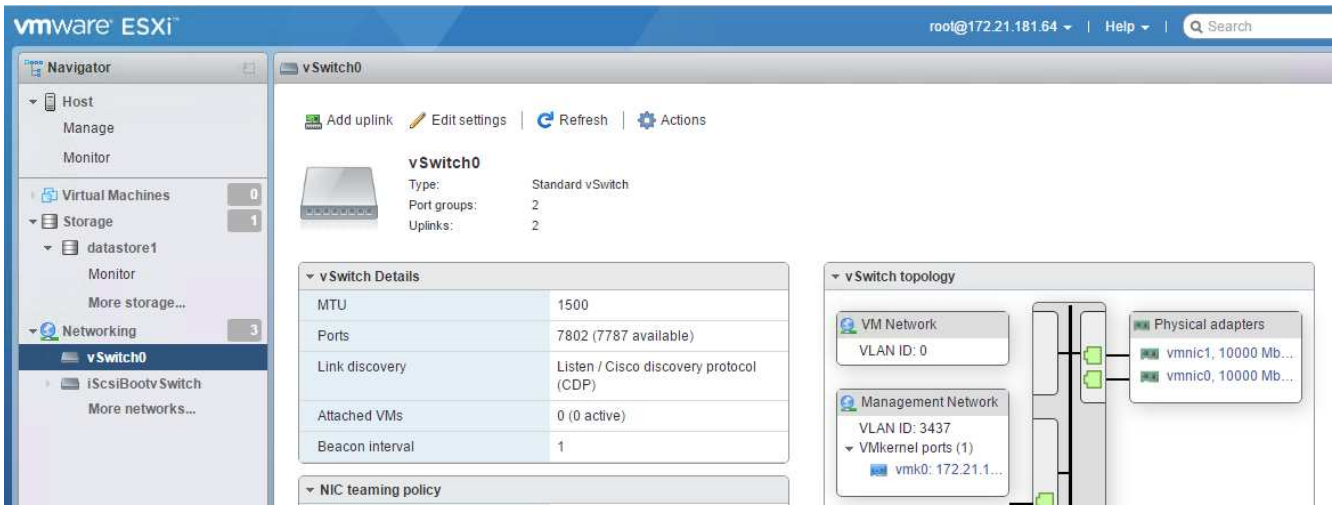
4. Inserire l'indirizzo IP `iscsi_lif01a`.
   - Ripetere l'operazione con gli indirizzi IP `iscsi_lif01b`, `iscsi_lif02a`, e. `iscsi_lif02b`.
   - Fare clic su Salva configurazione.



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

Configurare l'host ESXi

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



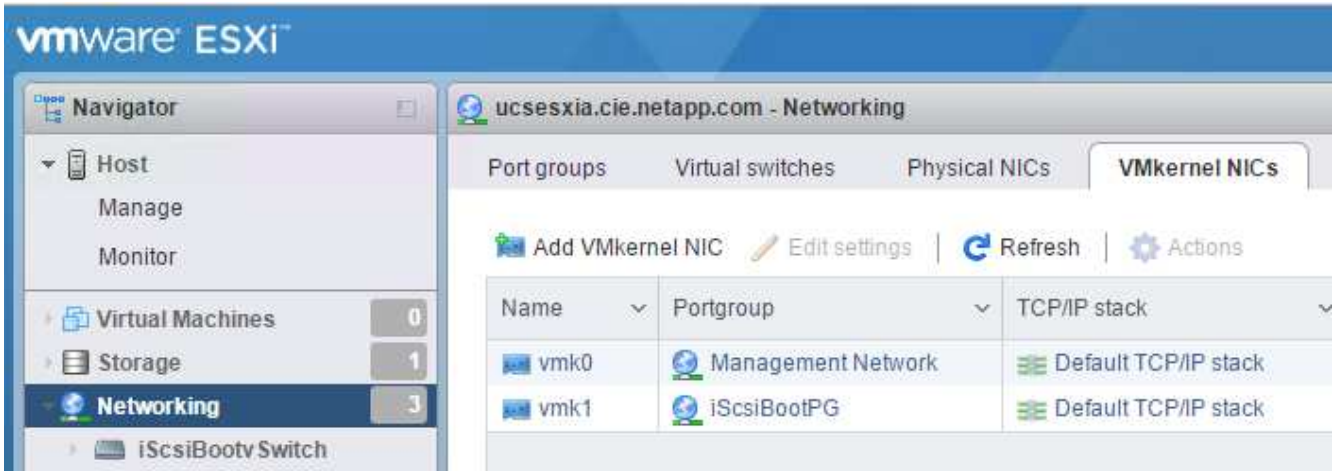
3. Selezionare Edit Settings (Modifica impostazioni).
4. Impostare la MTU su 9000.
5. Espandere NIC Teaming e verificare che vmnic0 e vmnic1 siano impostati su Active.

Configurare i gruppi di porte e le NIC VMkernel

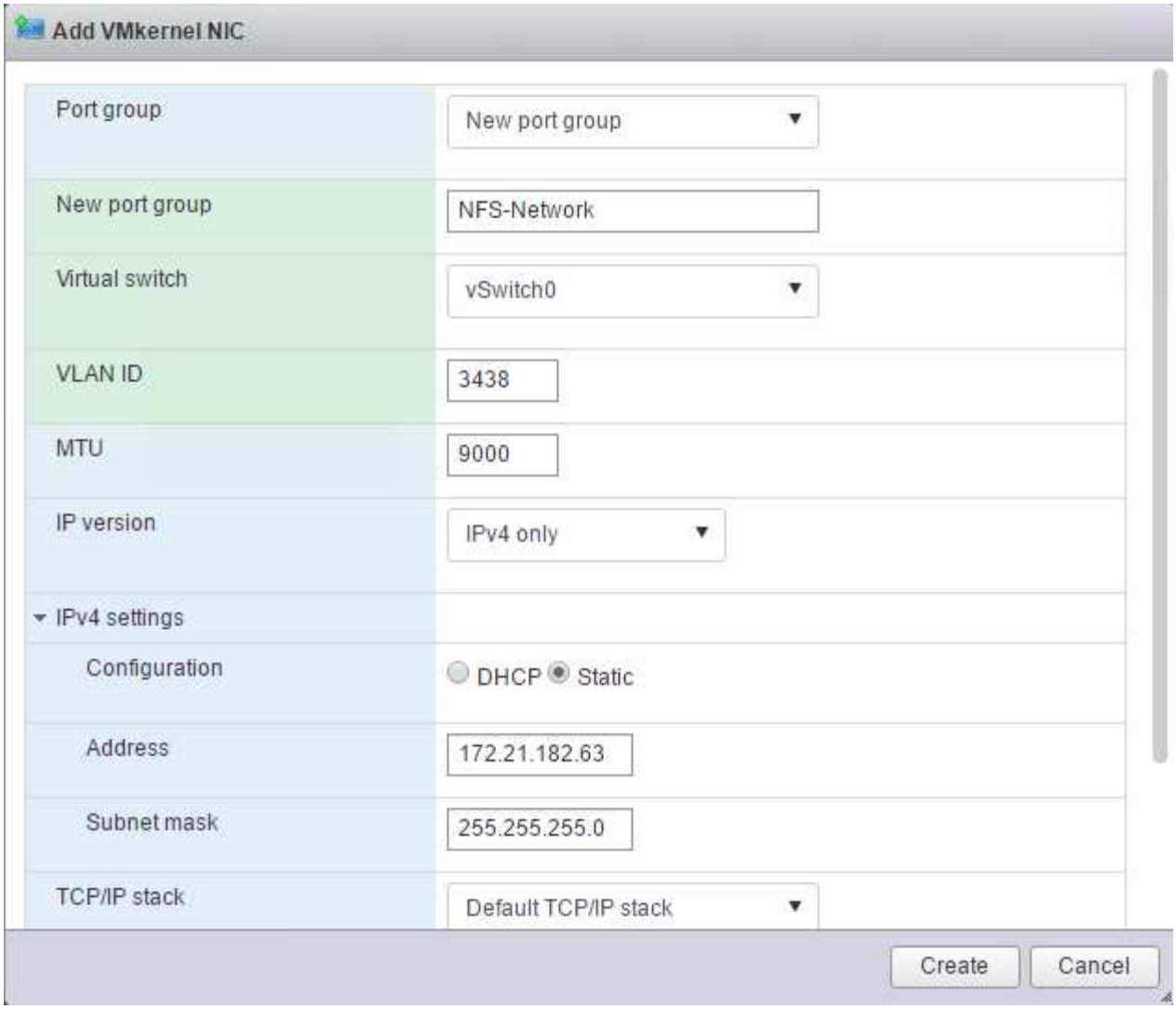
1. Nel riquadro di spostamento a sinistra, selezionare rete.
2. Fare clic con il pulsante destro del mouse sulla scheda gruppi di porte.

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

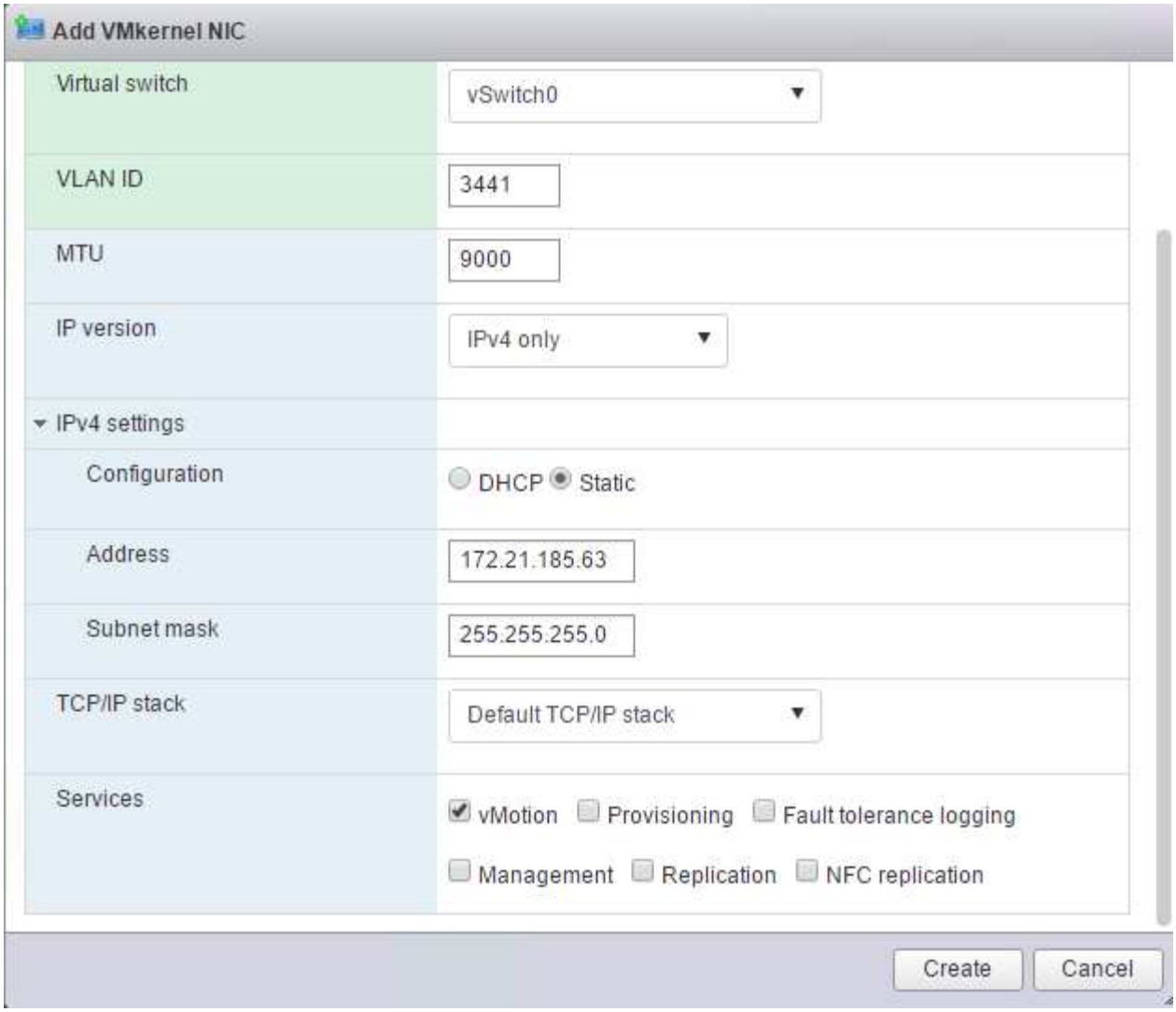
5. Fare clic sulla scheda NIC VMkernel.



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



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

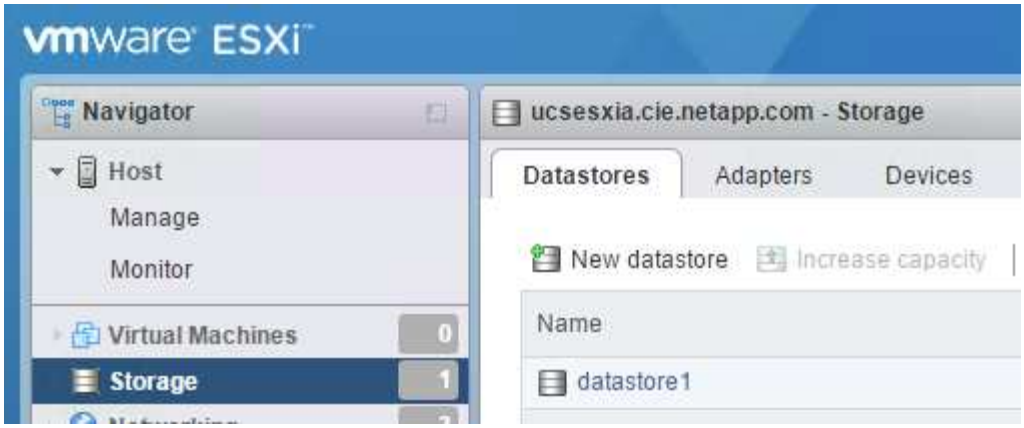


Esistono diversi modi per configurare il networking ESXi, tra cui l'utilizzo dello switch distribuito VMware vSphere, se la licenza lo consente. Le configurazioni di rete alternative sono supportate in FlexPod Express se sono richieste per soddisfare i requisiti di business.

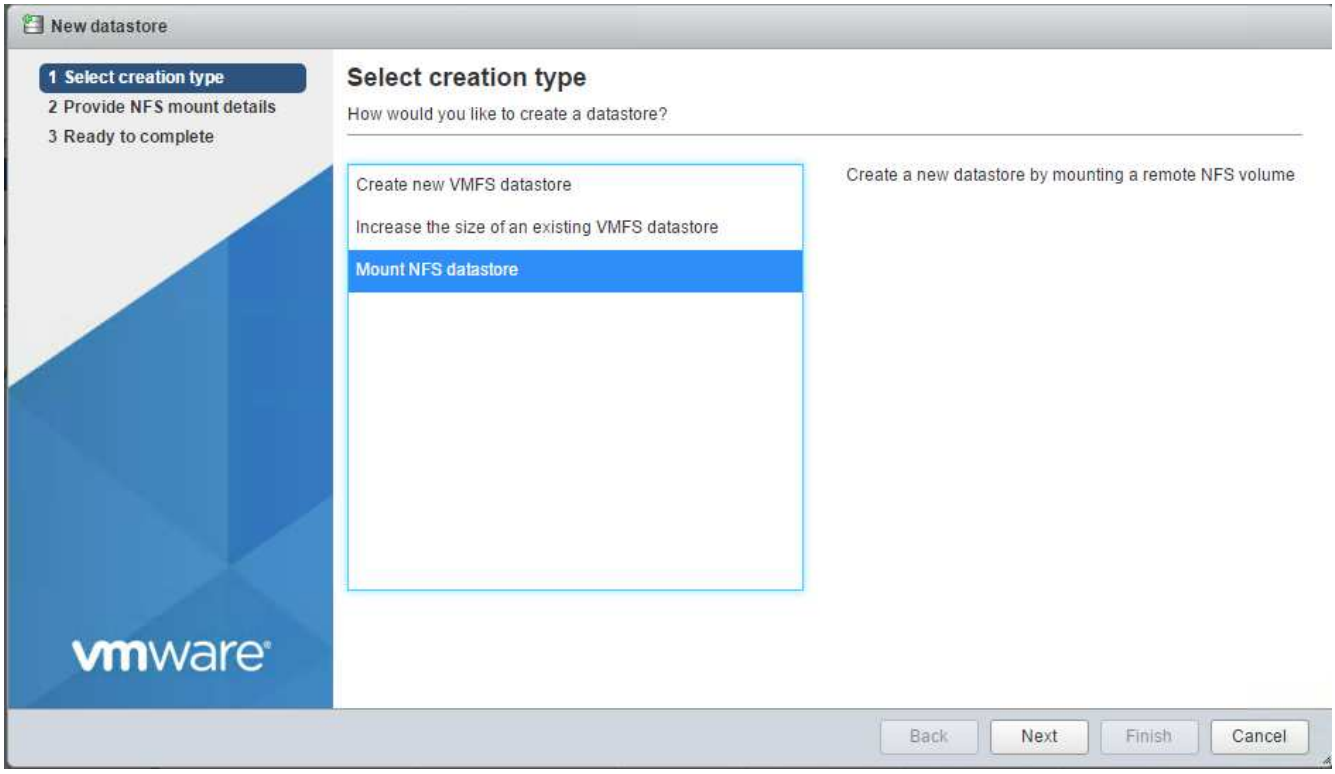
Montare i primi datastore

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

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



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



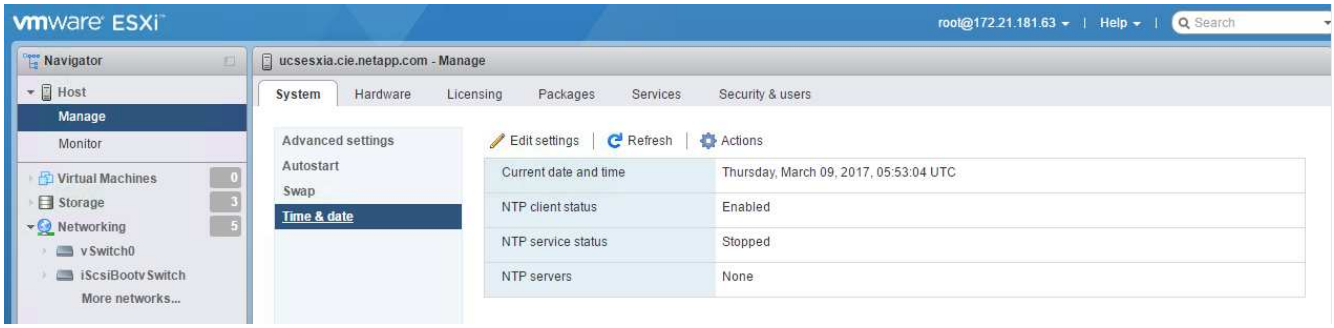
3. Quindi, inserire le seguenti informazioni nella pagina fornire i dettagli del montaggio NFS:
   - Nome: `infra_datastore_1`
   - Server NFS: `<<var_nodea_nfs_lif>>`
   - Share: /Infra_datastore_1
   - Assicurarsi che sia selezionato NFS 3.
4. Fare clic su fine. È possibile visualizzare il completamento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

- Assicurarsi che sia selezionato NFS 3.

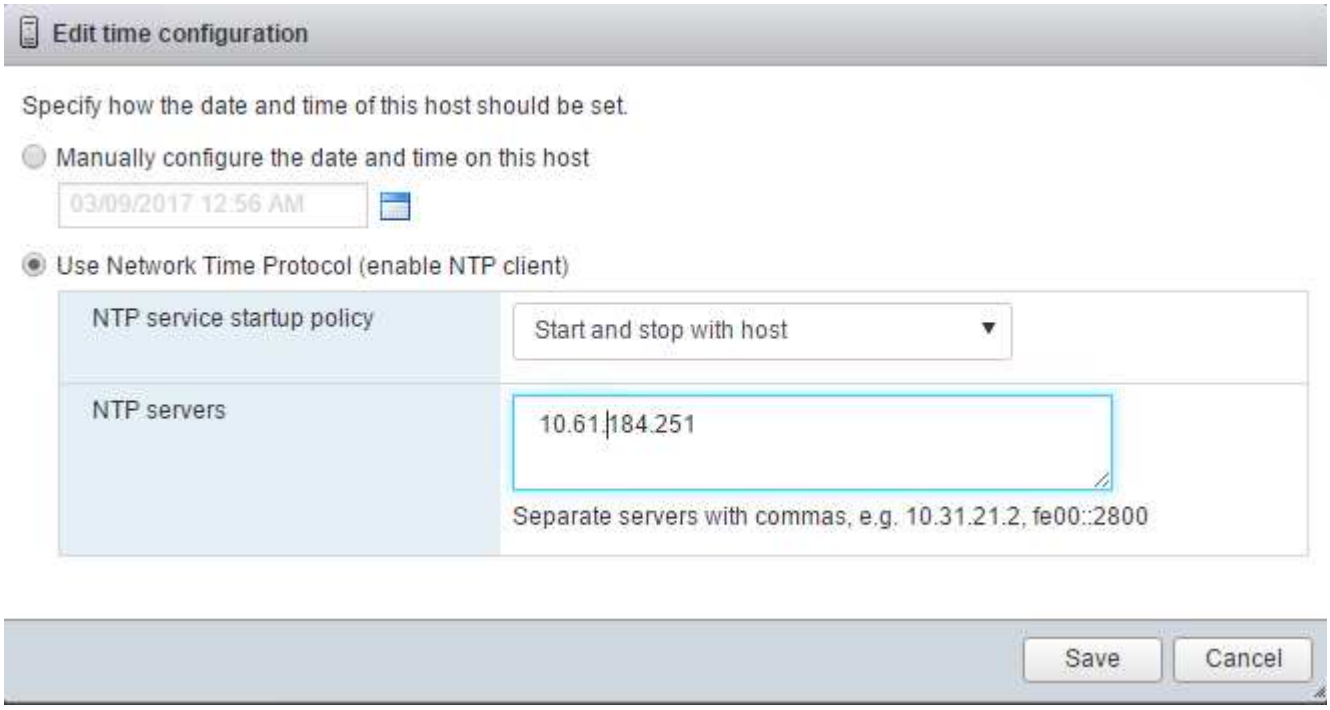
Configurare NTP

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

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



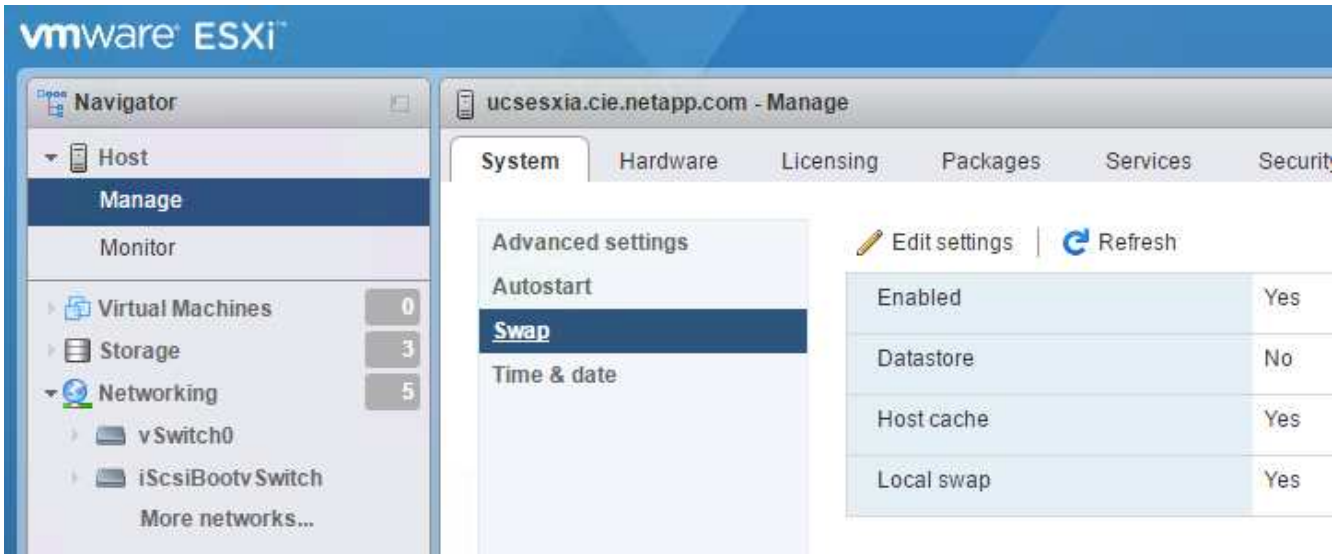
2. Selezionare Use Network Time Protocol (attiva client NTP).
3. Selezionare Start and Stop with host (Avvia e arresta con host) come criterio di avvio del servizio NTP.
4. Invio `<<var_ntp>>` Come server NTP. È possibile impostare più server NTP.
5. Fare clic su Salva.



Spostare la posizione del file di swap della macchina virtuale

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

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



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

3. Fare clic su Salva.

Installare il plug-in NetApp NFS 1.0.20 per VMware VAAI

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

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

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

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

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

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

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

Questi comandi producono il seguente output:

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

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

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

"Installazione di VMware vCenter Server 6.7"

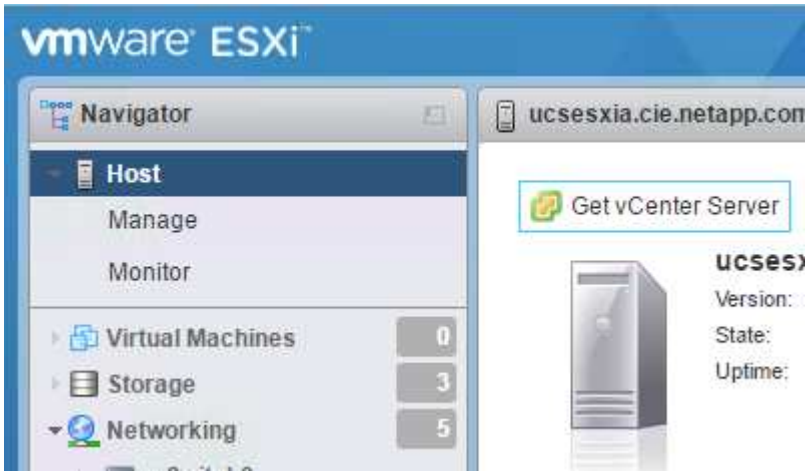
Installare VMware vCenter Server 6.7

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

> FlexPod utilizza l'appliance server vCenter (VCSA).

Scarica l'appliance server VMware vCenter

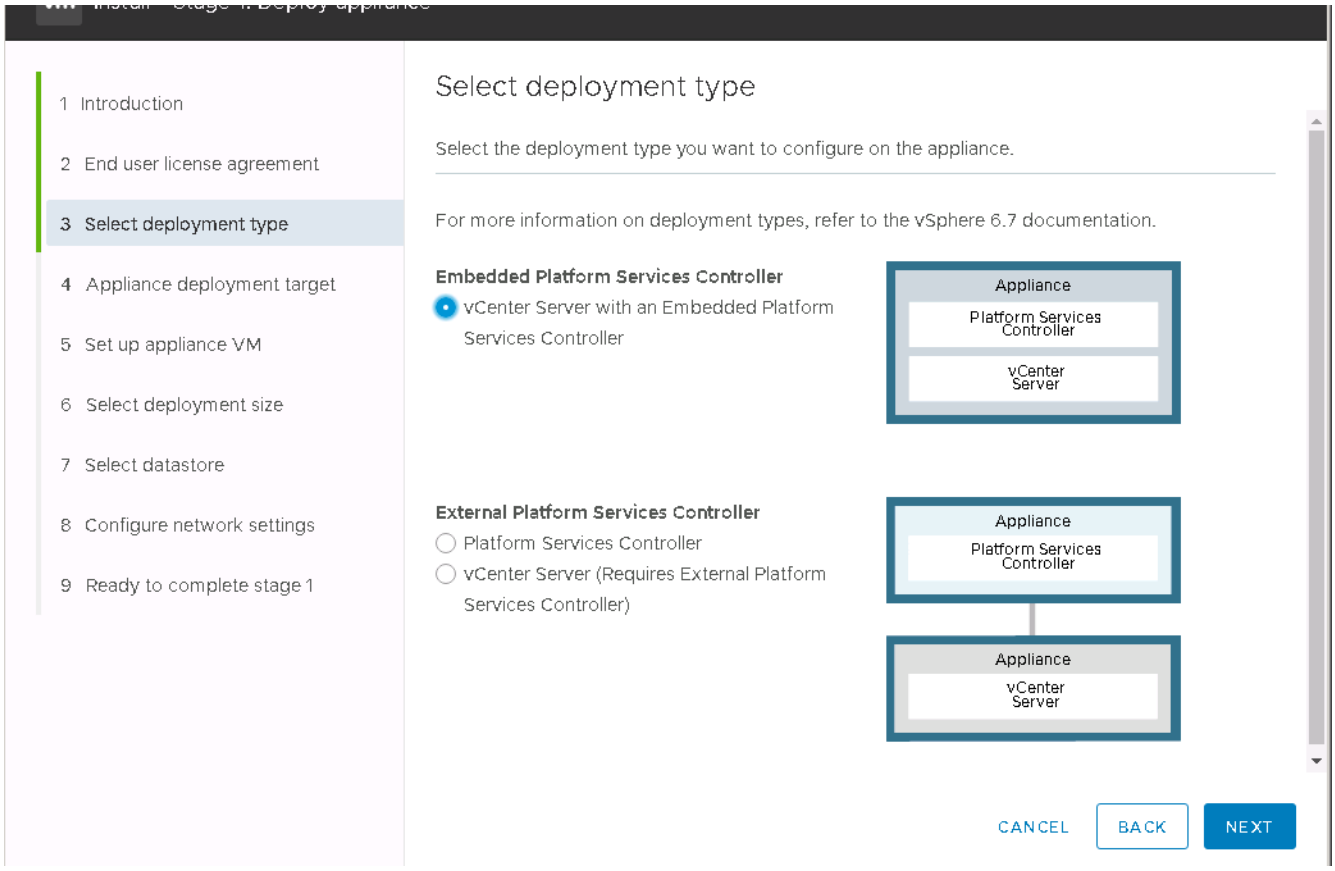
1. Scarica VCSA. Per accedere al collegamento per il download, fare clic sull'icona Get vCenter Server (Ottieni server vCenter) durante la gestione dell'host ESXi.



2. Scaricare VCSA dal sito VMware.

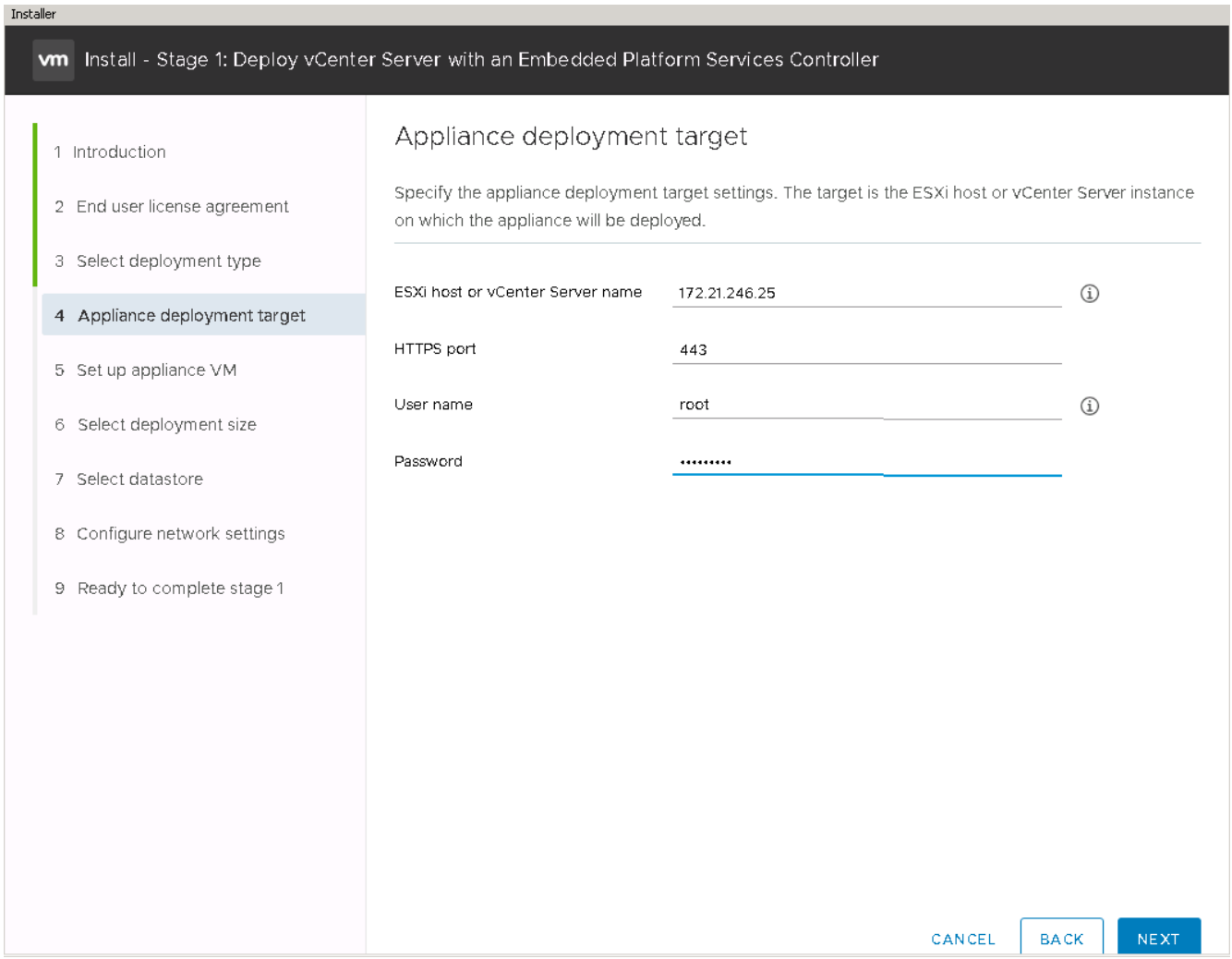
> Sebbene sia supportato l'installabile di Microsoft Windows vCenter Server, VMware consiglia VCSA per le nuove implementazioni.

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

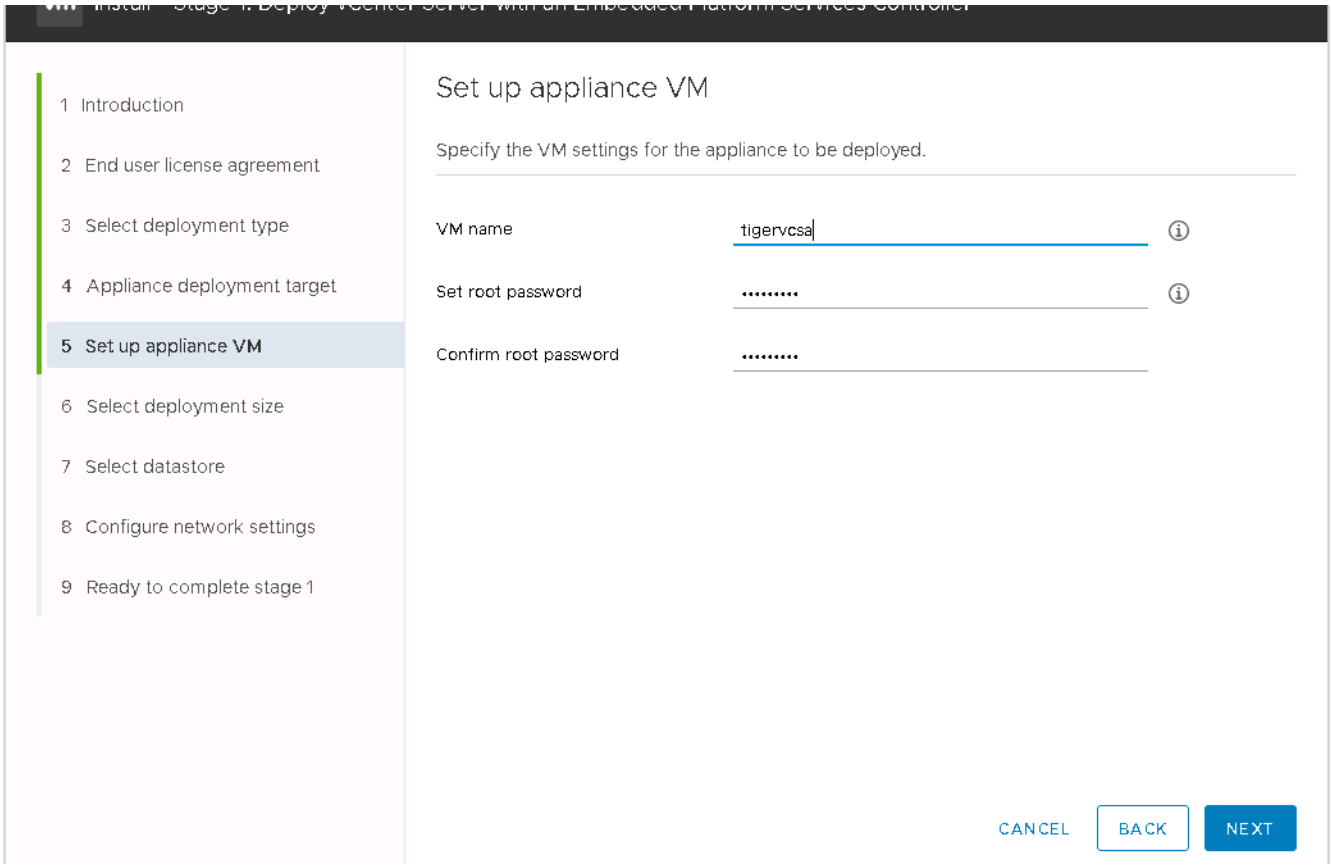


Se necessario, l'implementazione del controller dei servizi della piattaforma esterna è supportata anche come parte della soluzione FlexPod Express.

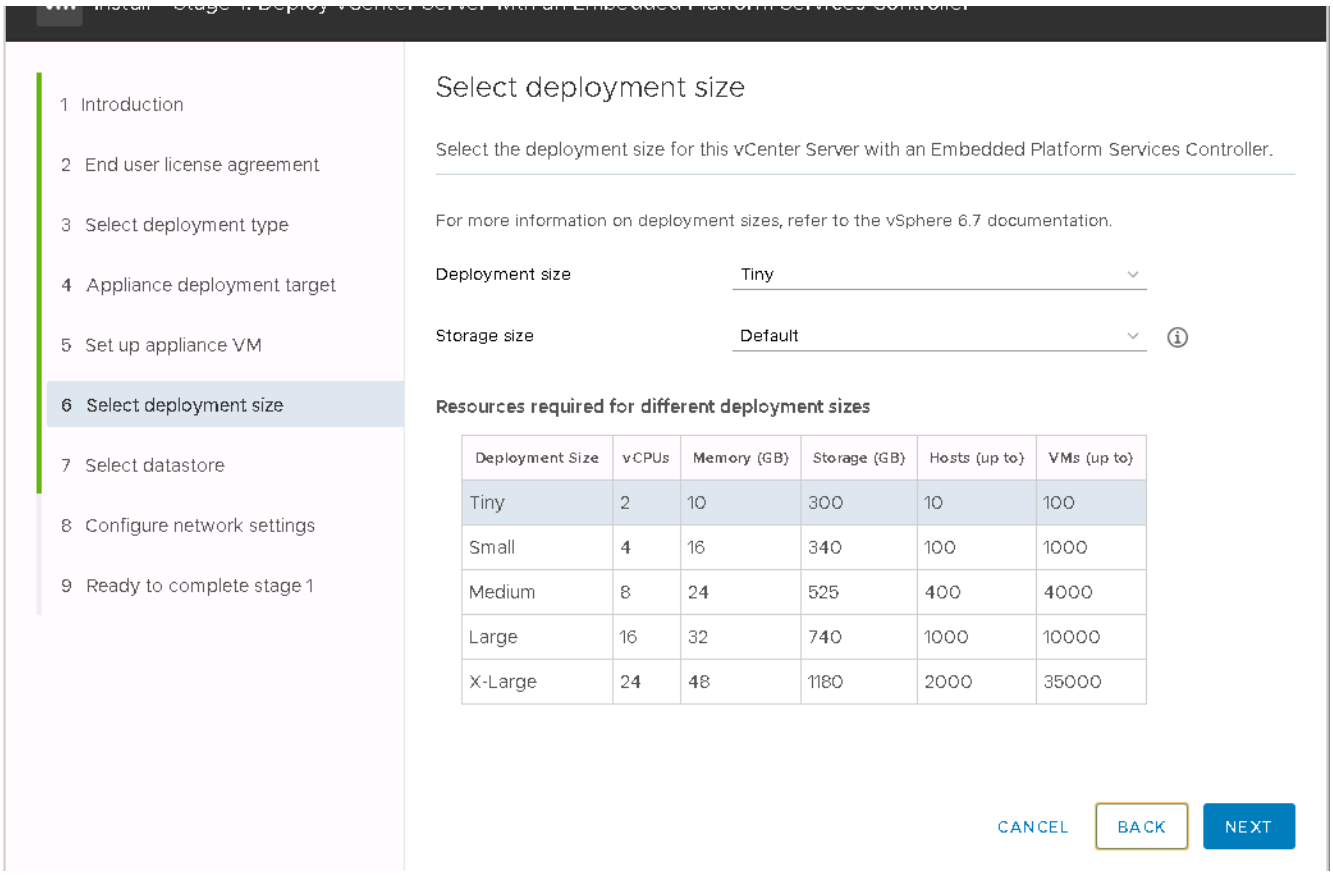
9. In Appliance Deployment Target (destinazione di implementazione dell'appliance), immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root.



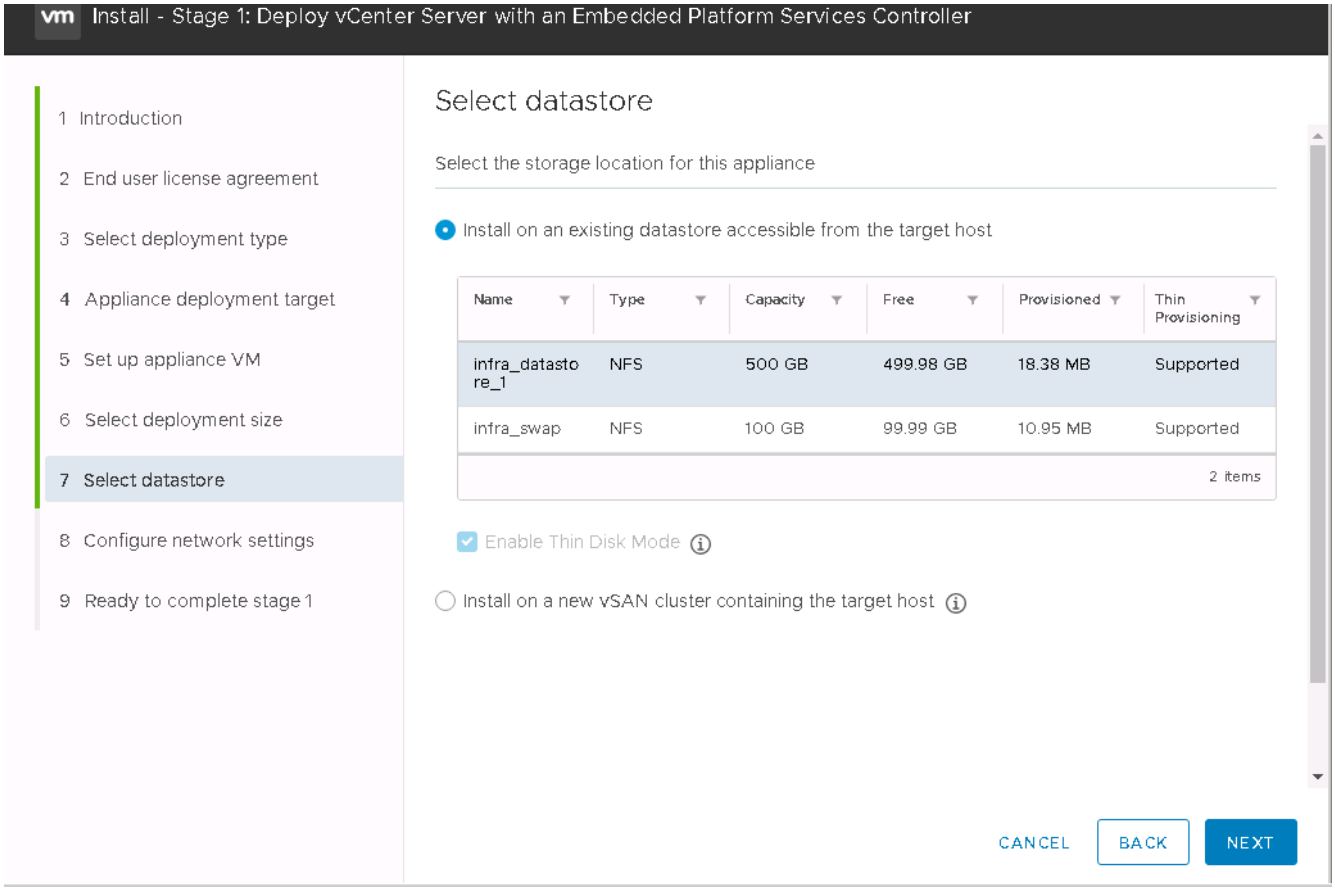
10. Impostare la VM dell'appliance immettendo `VCSA` Come nome della macchina virtuale e password root che si desidera utilizzare per VCSA.



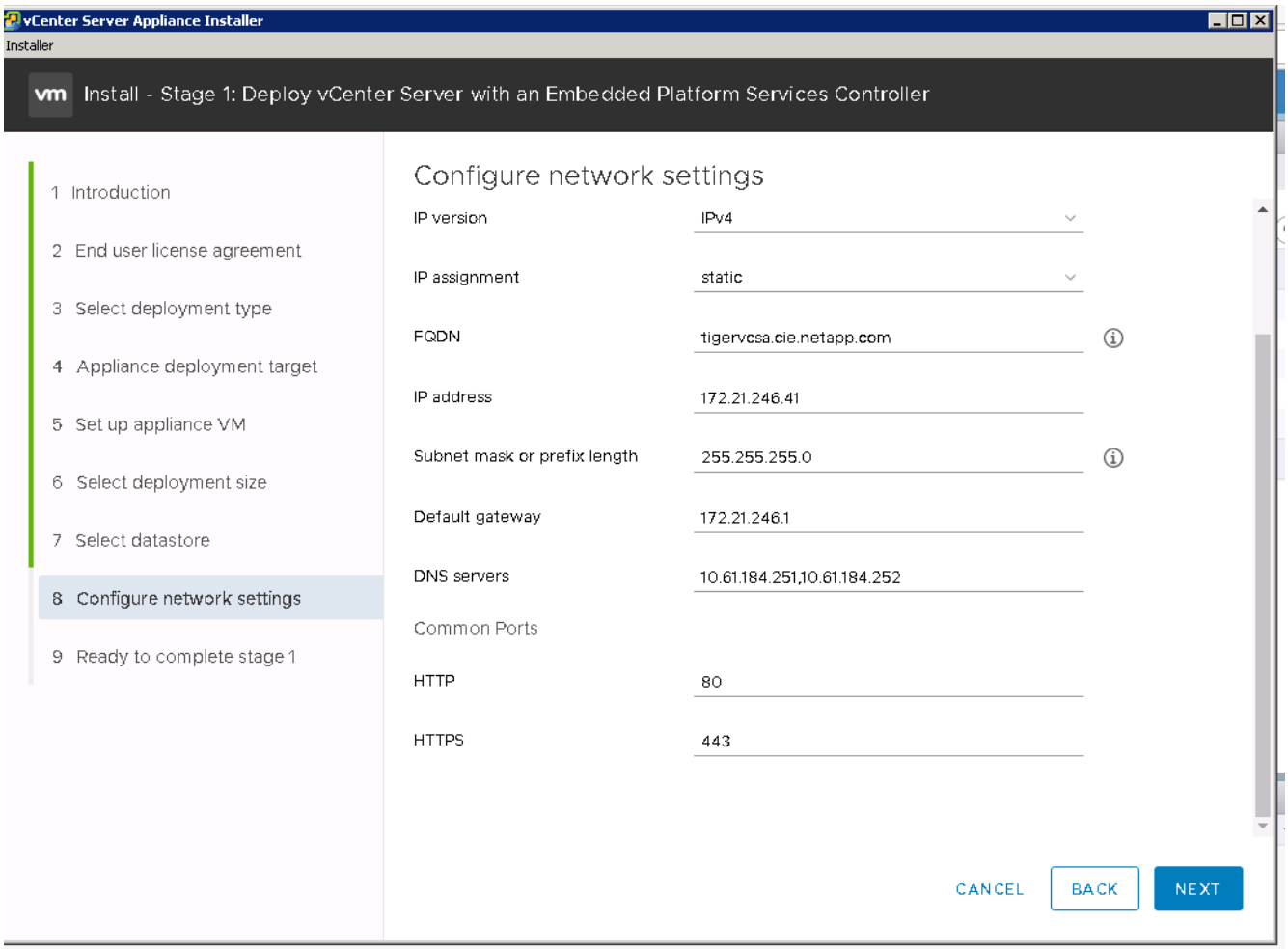
11. Selezionare la dimensione di implementazione più adatta al proprio ambiente. Fare clic su Avanti.



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

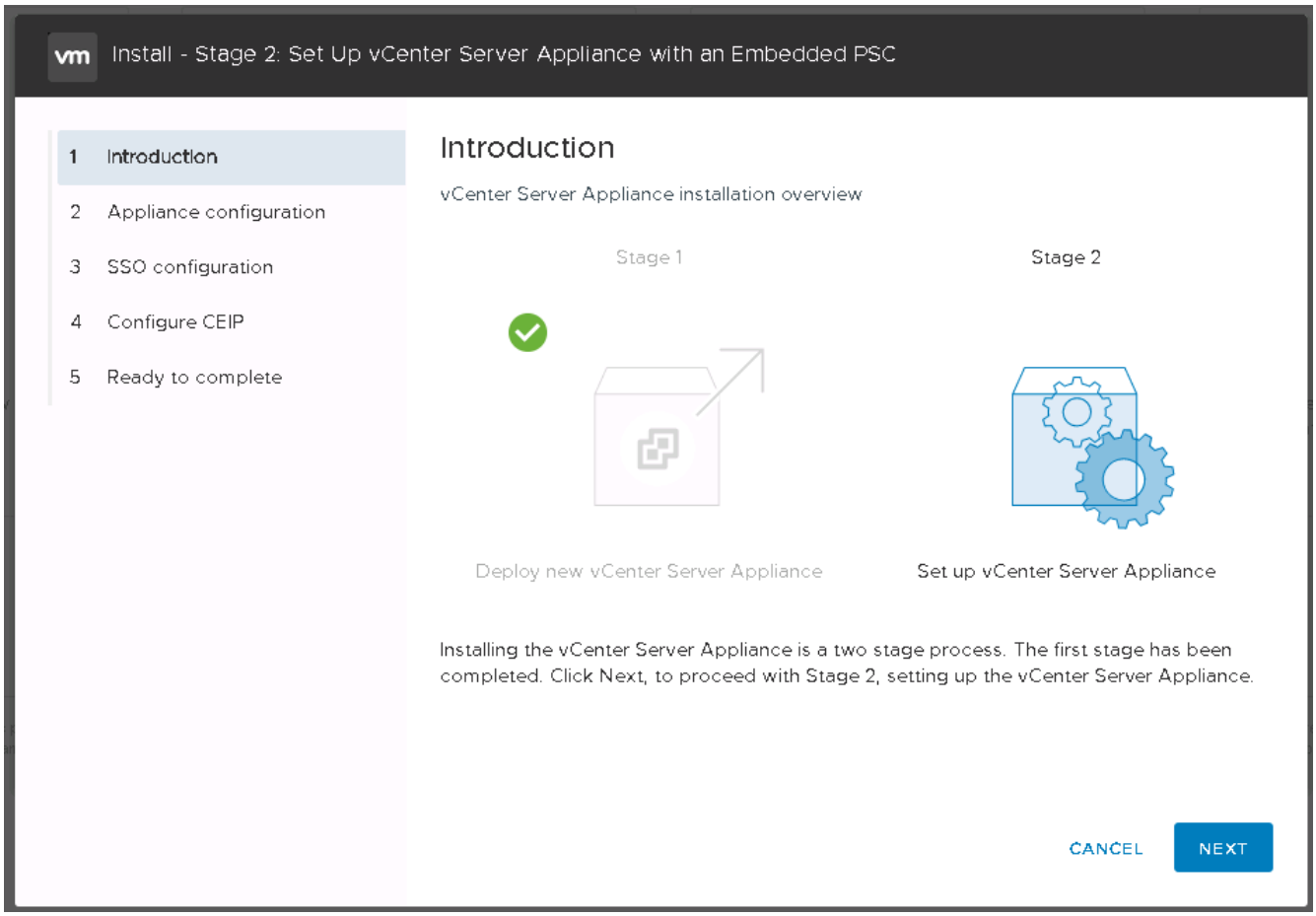


13. Inserire le seguenti informazioni nella pagina Configure network settings (Configura impostazioni di rete) e fare clic su Next (Avanti).
    a. Selezionare MGMT-Network for Network (rete MGMT per rete).
    b. Inserire l'FQDN o l'IP da utilizzare per VCSA.
    c. Inserire l'indirizzo IP da utilizzare.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



VCSA viene installato ora. Questo processo richiede alcuni minuti.

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



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

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

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

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

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

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

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

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

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

Configurare il clustering di VMware vCenter Server 6.7 e vSphere

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

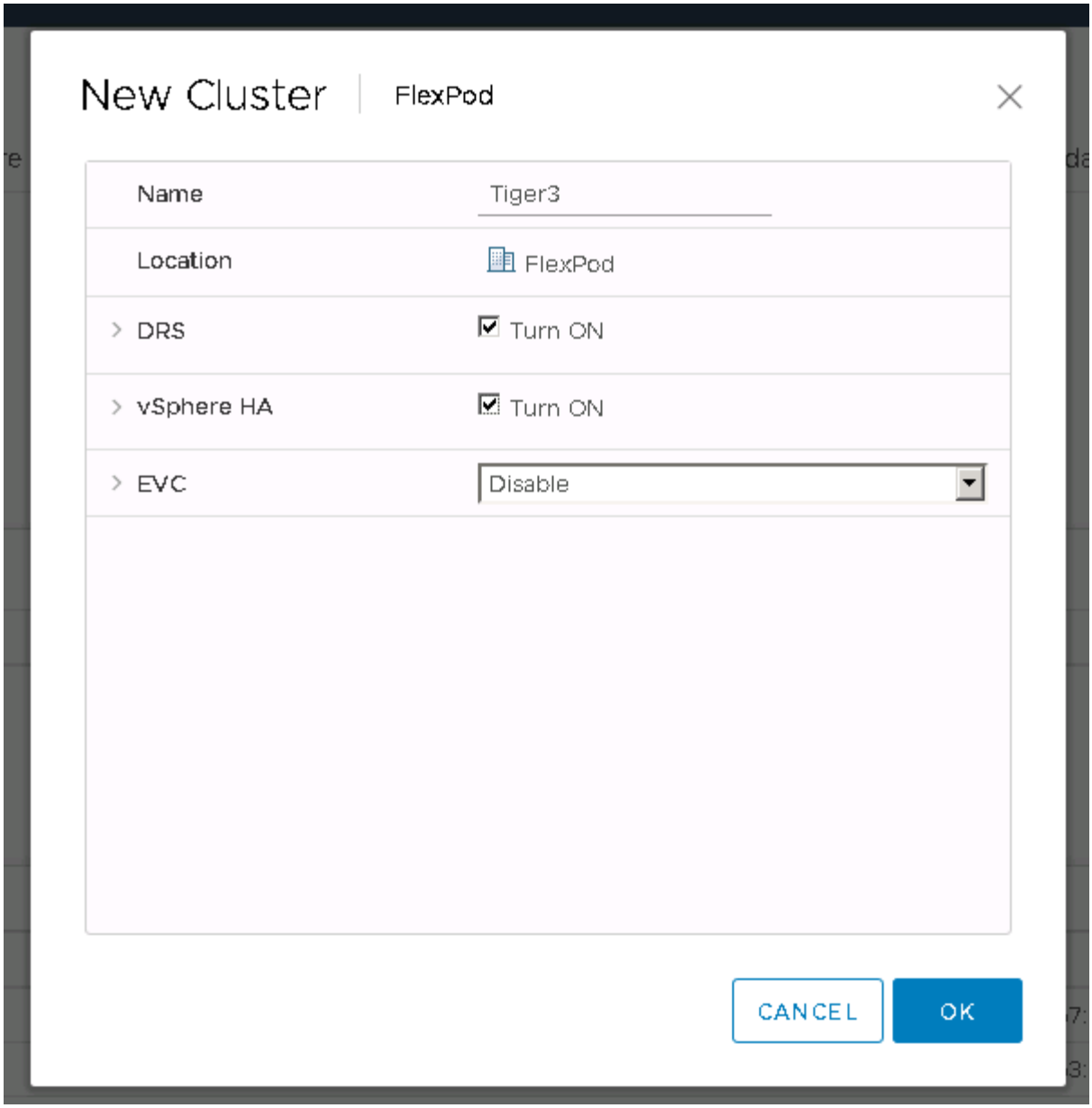
seguente procedura:

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

Creare il cluster vSphere

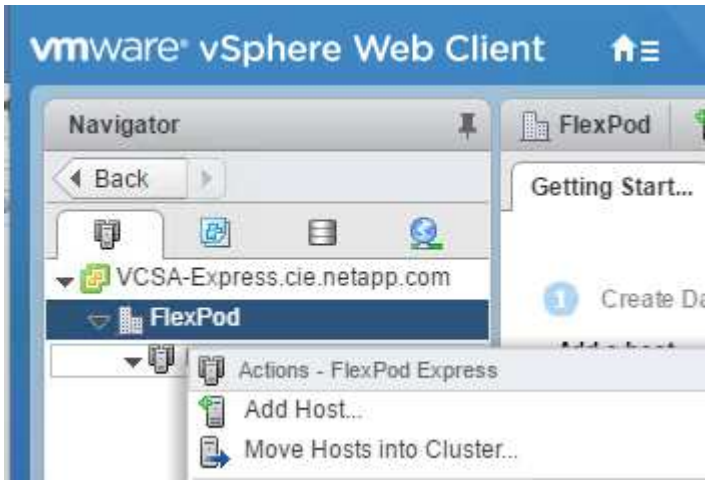
Per creare un cluster vSphere, attenersi alla seguente procedura:

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



Aggiungere host ESXi al cluster

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



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

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

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

Configurare il coredump sugli host ESXi

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

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

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

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

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"

- 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"

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

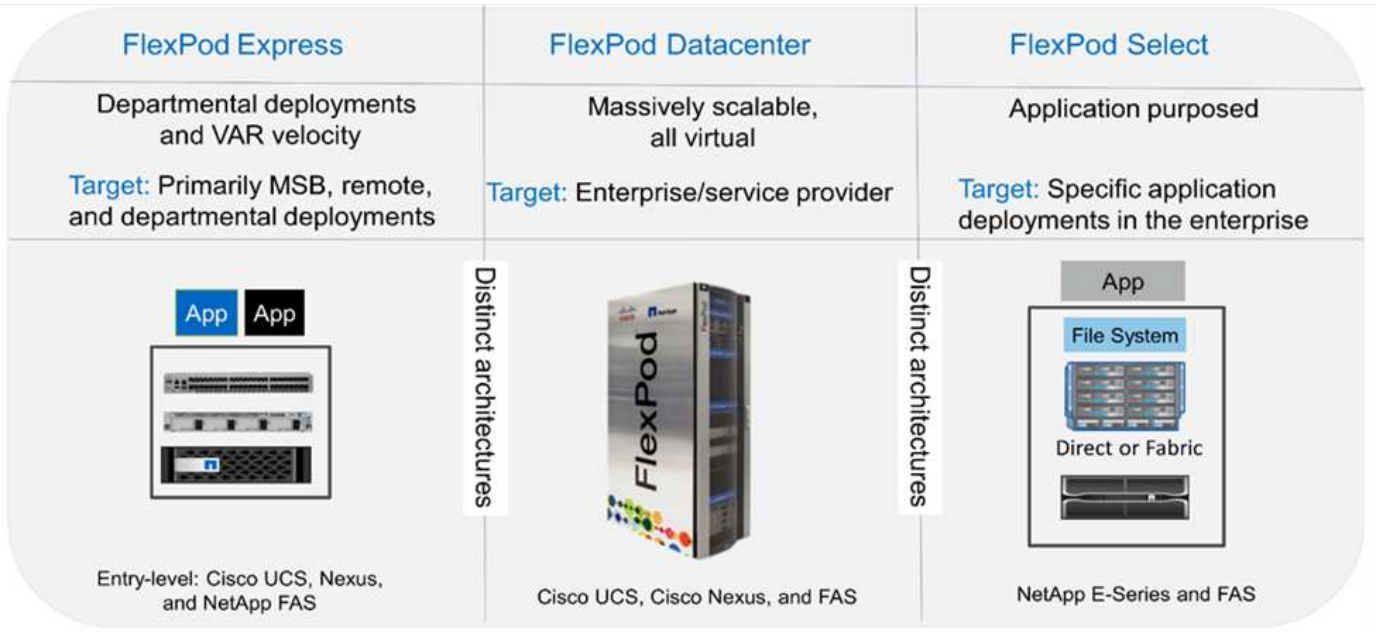
Le architetture di riferimento FlexPod vengono fornite come Cisco Validated Design (CVD) o NetApp Verified Architectures (NVA). Sono consentite deviazioni in base ai requisiti del cliente rispetto a un determinato CVD o NVA se queste variazioni non creano una configurazione non supportata.

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

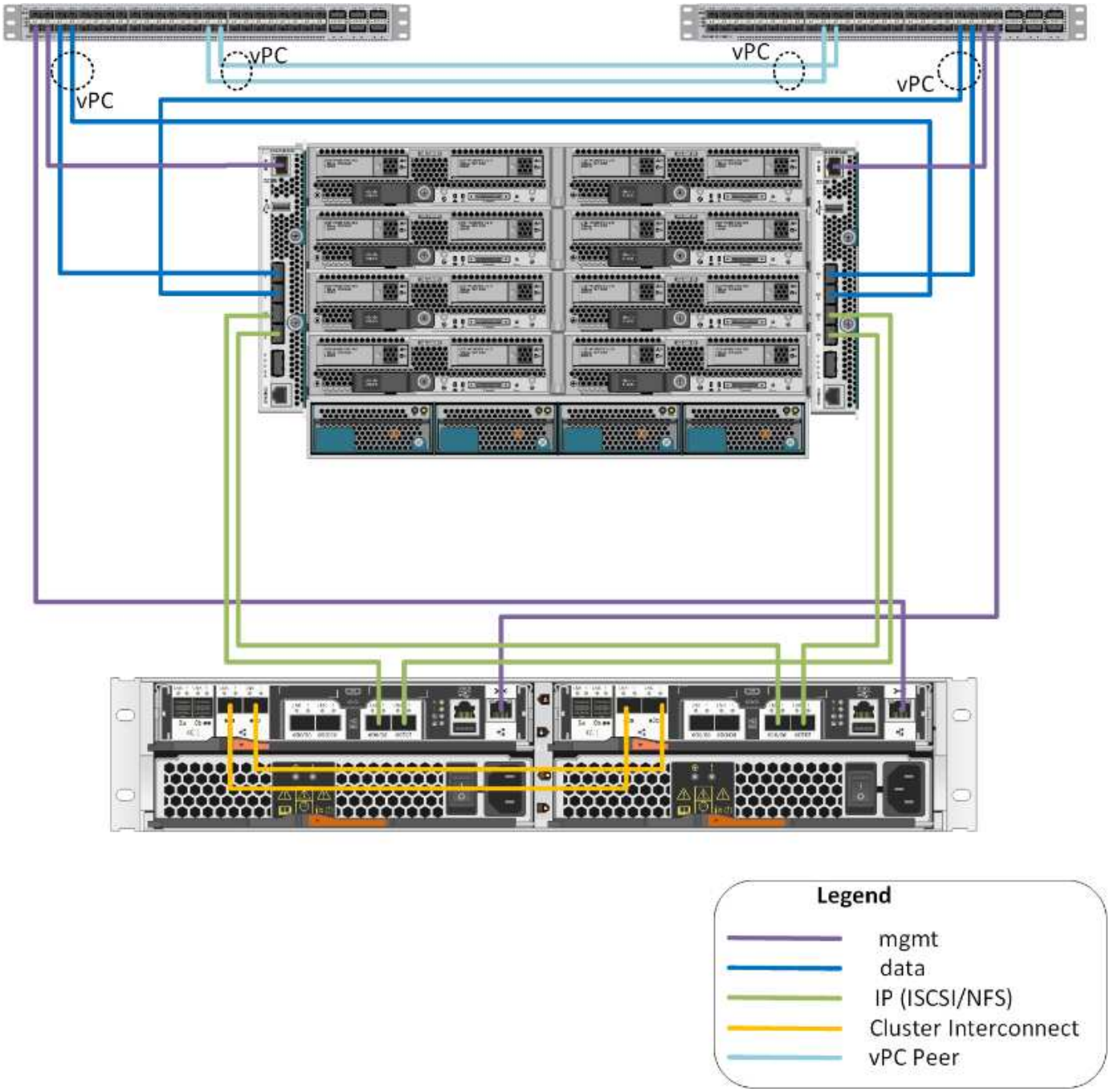
Componenti software

- 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>
```

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]: no
```

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 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
                       Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. 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
```

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 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,fcp
```

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

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

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

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

> I comandi sono preceditti 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 completamento per selezionare ed eliminare ogni certificato predefinito.

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

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

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

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

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

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

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

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

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

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

Creare un volume NetApp FlexVol in ONTAP

Per creare un volume NetApp FlexVol®, immettere il nome, 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 -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

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

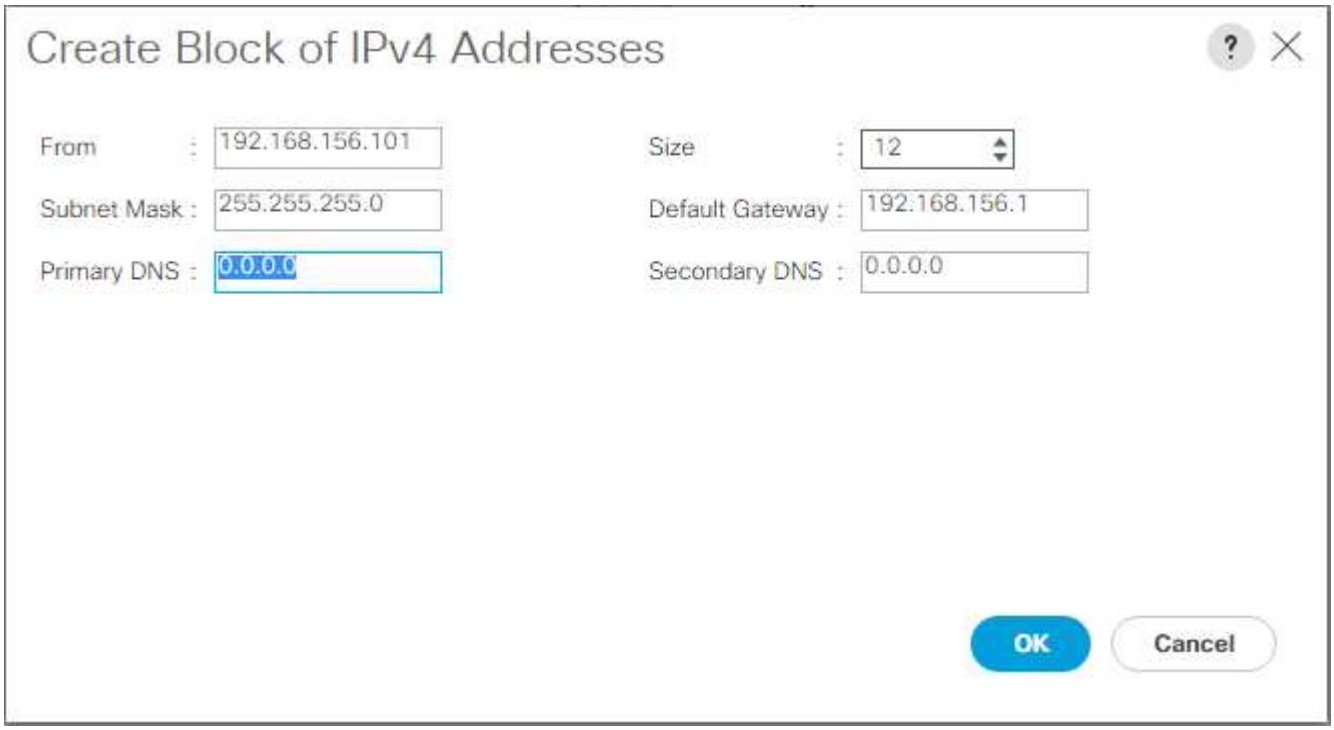
Cisco consiglia vivamente di configurare Call Home in Cisco UCS Manager. La configurazione di Call Home accelera la risoluzione dei casi di supporto. Per configurare Call Home, attenersi alla seguente procedura:

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.



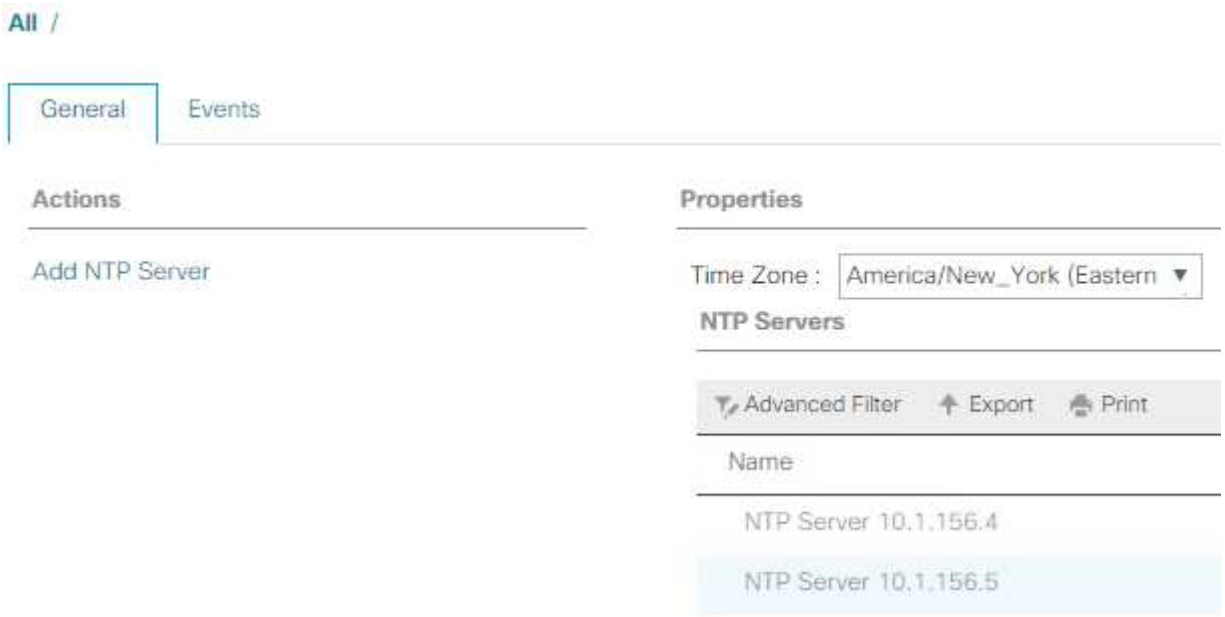
5. Fare clic su OK per creare il blocco.
6. Fare clic su OK nel messaggio di conferma.

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.

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.



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.

Equipment / Fabric Interconnects / Fabric Interconnect A (subordinate) / Fixed Module

General | Ethernet Ports | FC Ports | Faults | Events

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | 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.

Equipment / Fabric Interconnects / Fabric Interconnect B (primar... / Fixed Module / Ethernet Ports

Ethernet Ports

Advanced Filter | Export | Print | All | Unconfigured | Network | Server | FCoE Uplink | Unified Uplink | Appliance Storage | FCoE Storage | Unified Storage | 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	

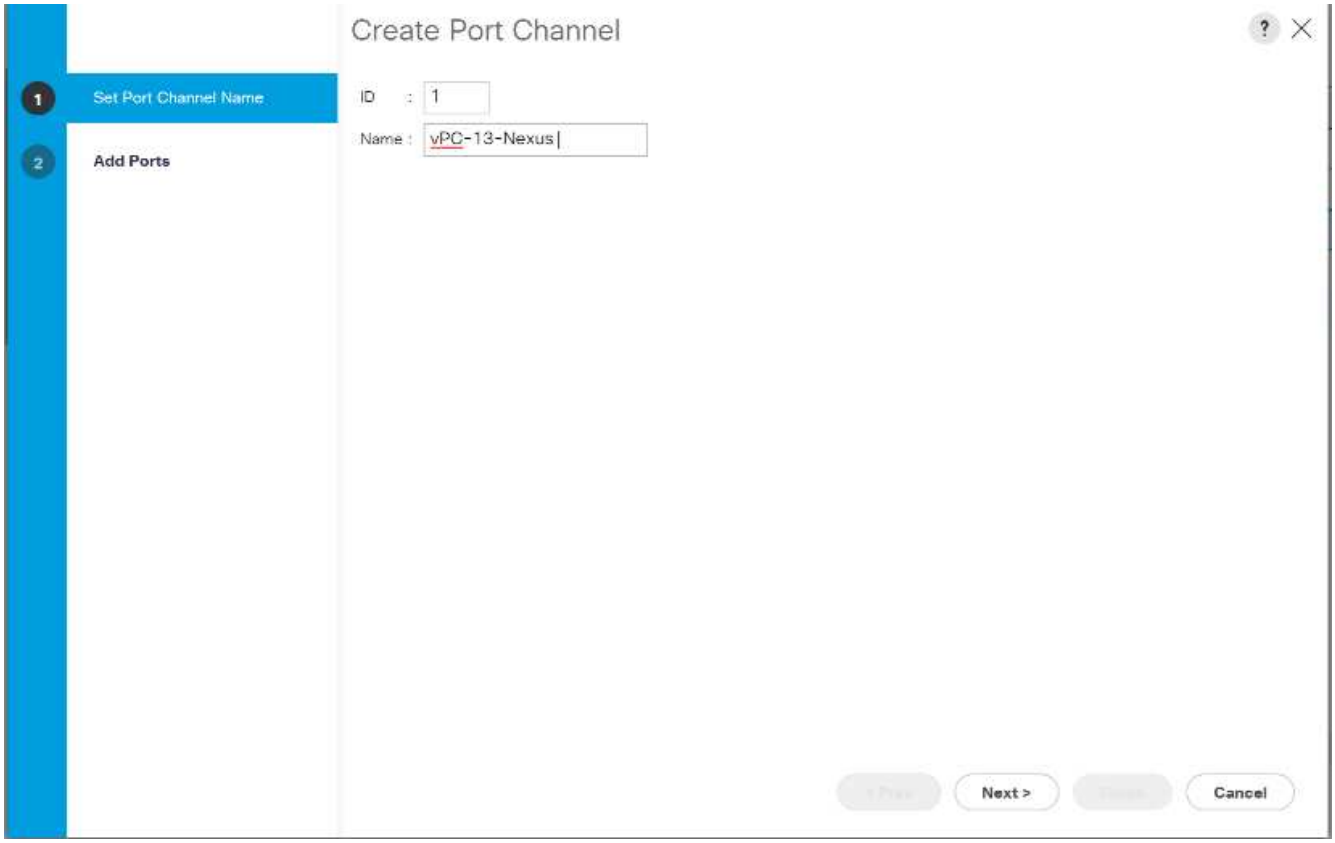
Creazione di canali di porte uplink per switch Cisco Nexus 31108

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:

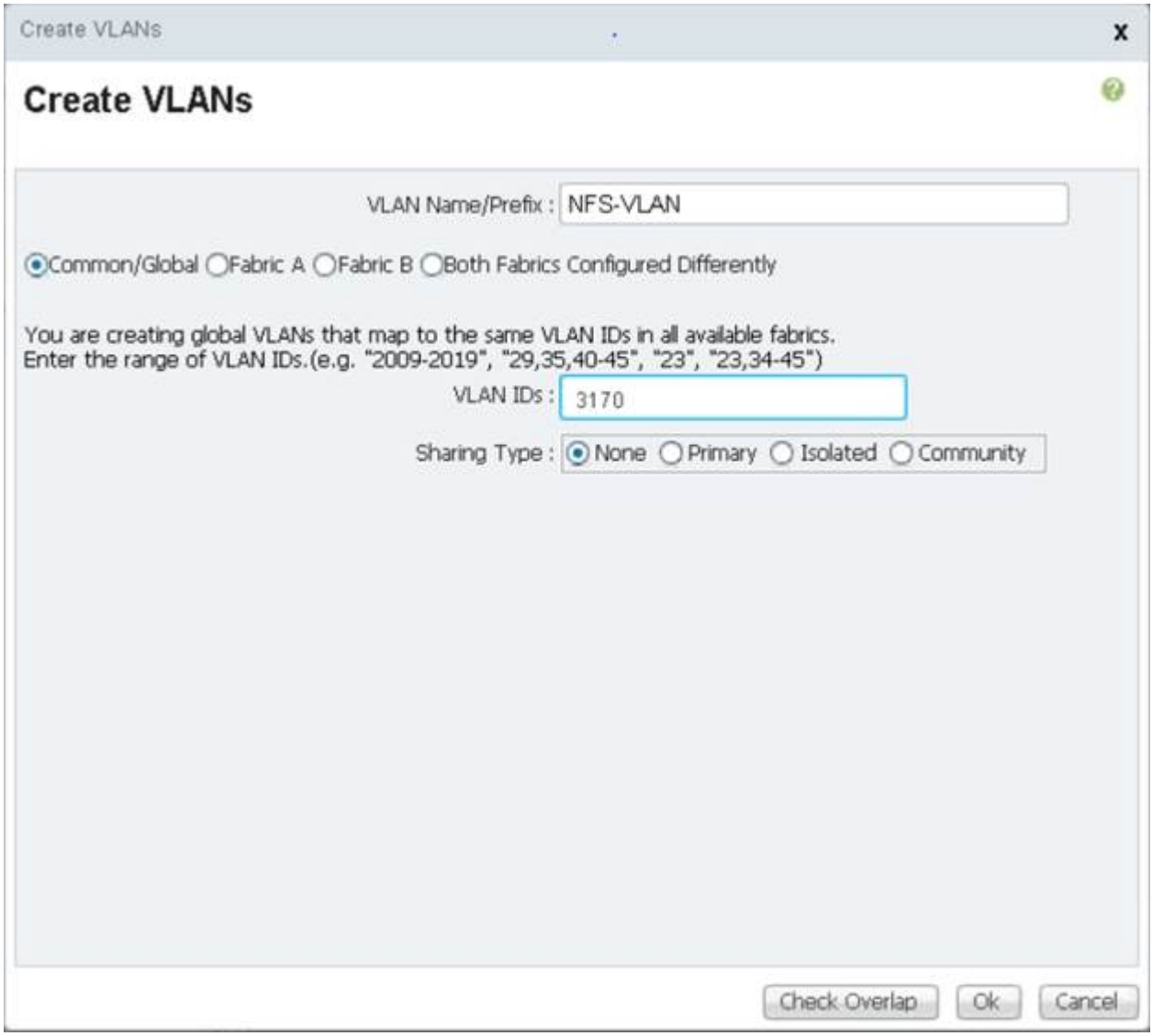
1. In Cisco UCS Manager, dal menu New (nuovo) nella barra degli strumenti nella parte superiore della finestra, selezionare Create Organization (Crea organizzazione).
2. Immettere un nome per l'organizzazione.
3. Facoltativo: Inserire una descrizione per l'organizzazione. Fare clic su OK.
4. Fare clic 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:

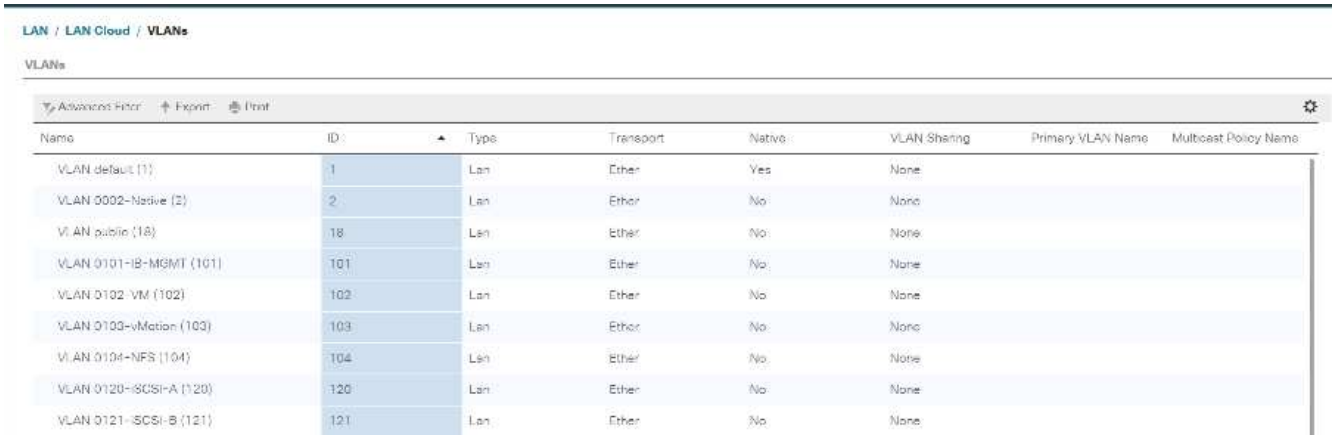
1. In Cisco UCS Manager, selezionare la scheda LAN.
2. Espandere il cloud Appliances.
3. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.
4. Selezionare Create VLAN (Crea VLAN).
5. Inserire NFS-VLAN come nome della VLAN NFS dell'infrastruttura.
6. Lasciare selezionato Common/Global (comune/globale).
7. Invio `<<var_nfs_vlan_id>>` Per l'ID VLAN.

8. Lasciare l'opzione Sharing Type (tipo di condivisione) impostata su None

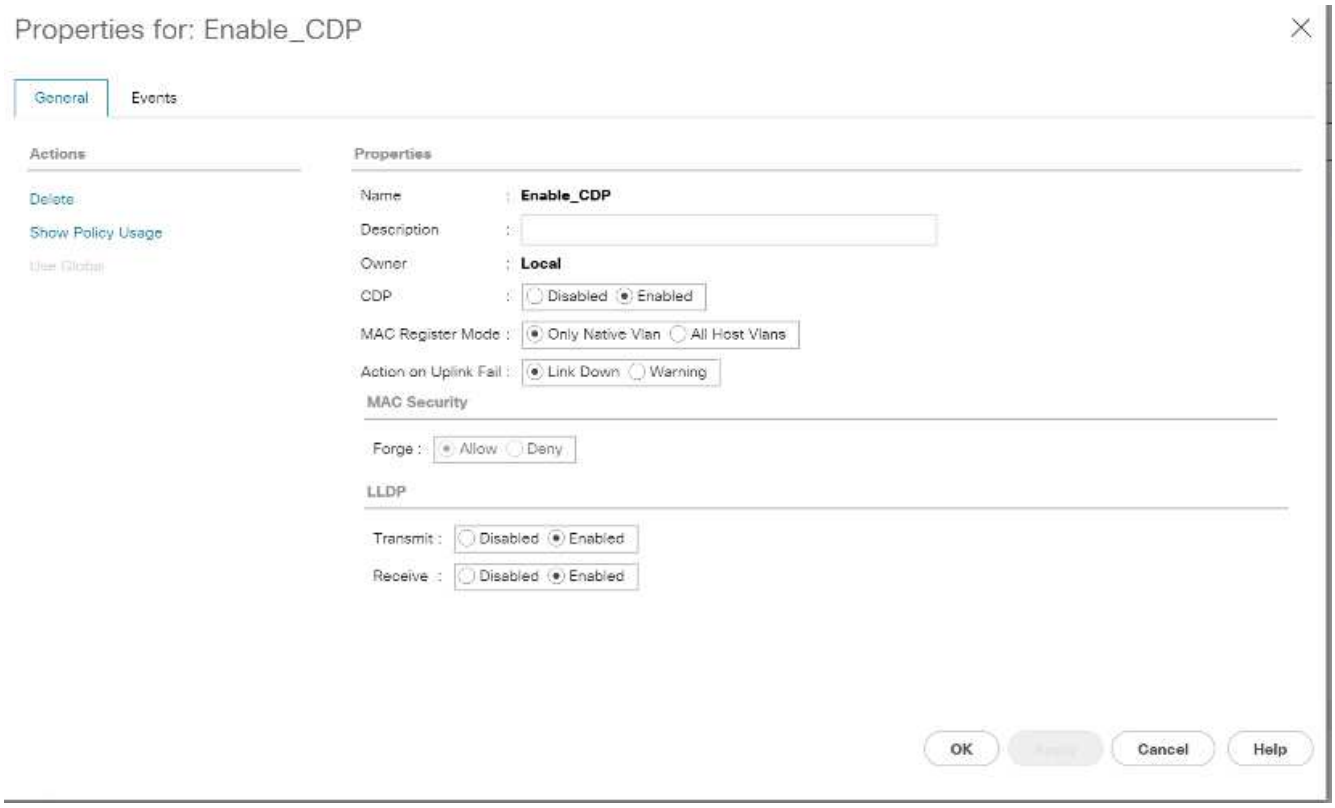


9. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.
10. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.
11. Selezionare Create VLAN (Crea VLAN).
12. Inserire iSCSI-A-VLAN come nome per il fabric iSCSI infrastruttura A VLAN.
13. Lasciare selezionato Common/Global (comune/globale).
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.

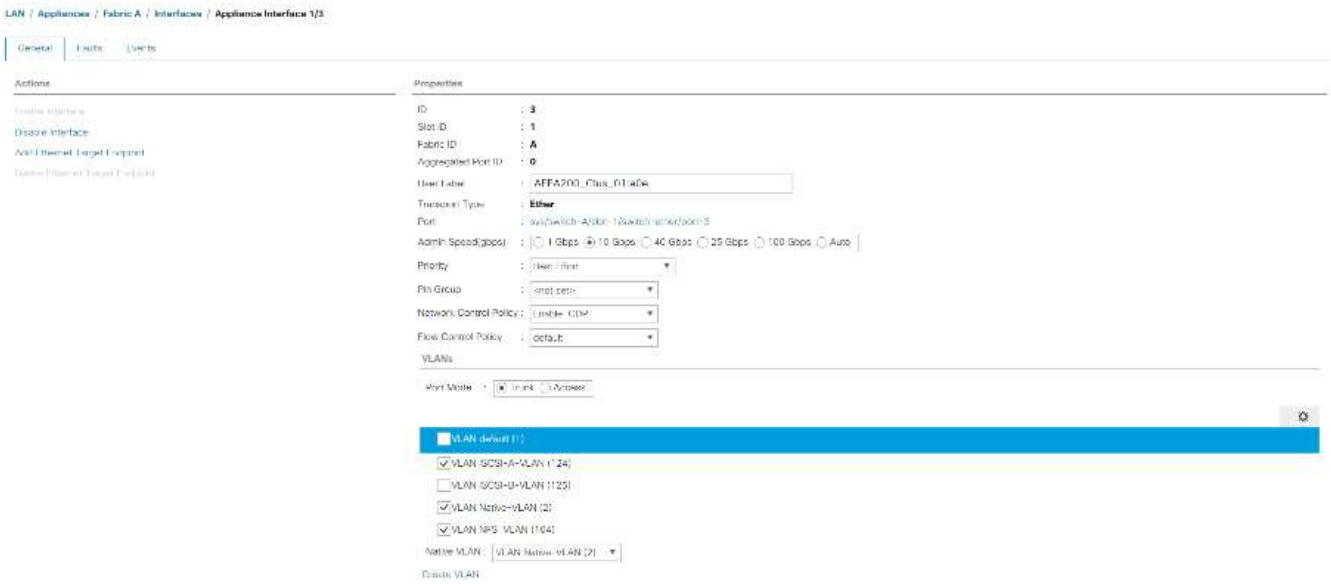
22. Fare clic con il pulsante destro del mouse su VLAN in Appliances Cloud.
23. Selezionare Create VLAN (Crea VLAN).
24. Inserire la VLAN nativa come nome della VLAN nativa.
25. Lasciare selezionato Common/Global (comune/globale).
26. Invio `<<var_native_vlan_id>>` Per l'ID VLAN.
27. Fare clic su OK, quindi nuovamente su OK per creare la VLAN.



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_LLPD` E selezionare Enabled (attivato) accanto a CDP.
31. Attivare le funzioni di trasmissione e ricezione per LLDP.



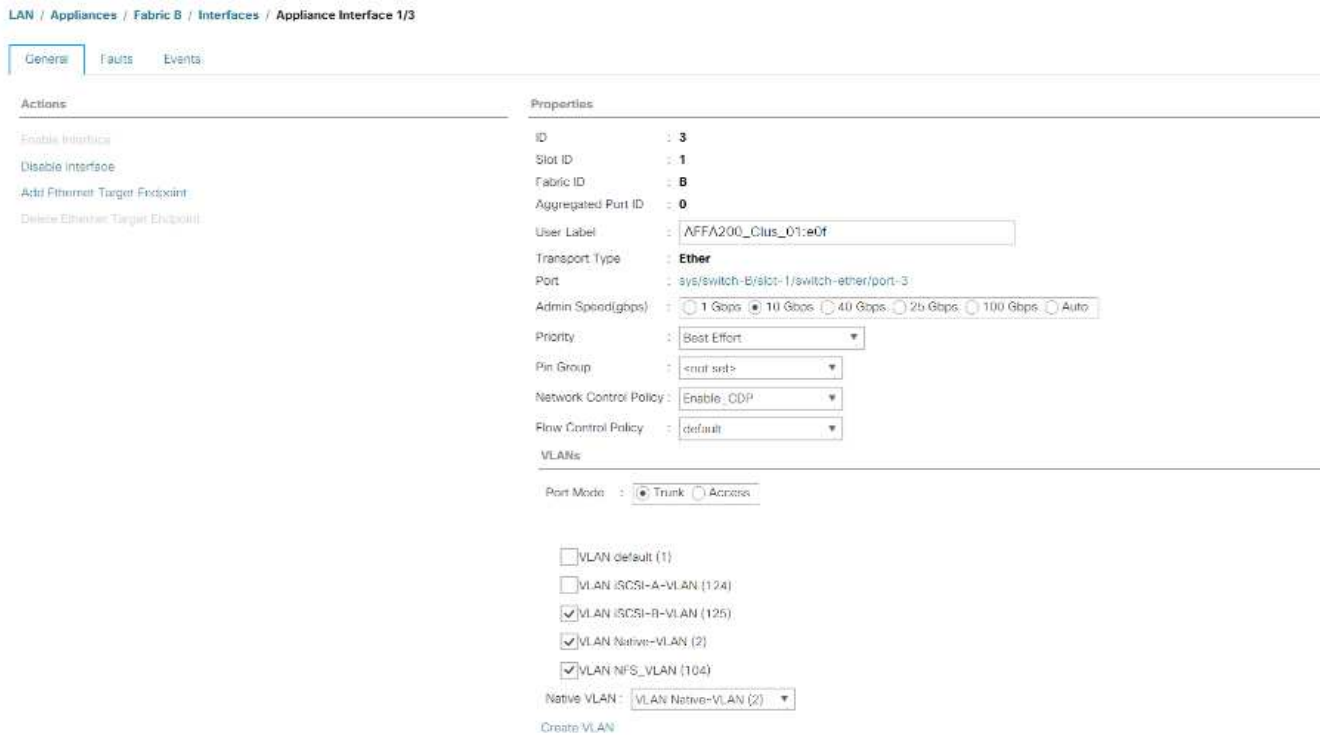
32. Fare clic su OK, quindi fare nuovamente clic su OK per creare il criterio.
33. Nel riquadro di navigazione, sotto LAN > Appliances Cloud, espandere la struttura ad albero fabric A.
34. Espandere interfacce.
35. Selezionare Appliance Interface 1/3.
36. Nel campo User Label (etichetta utente), inserire 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.



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.



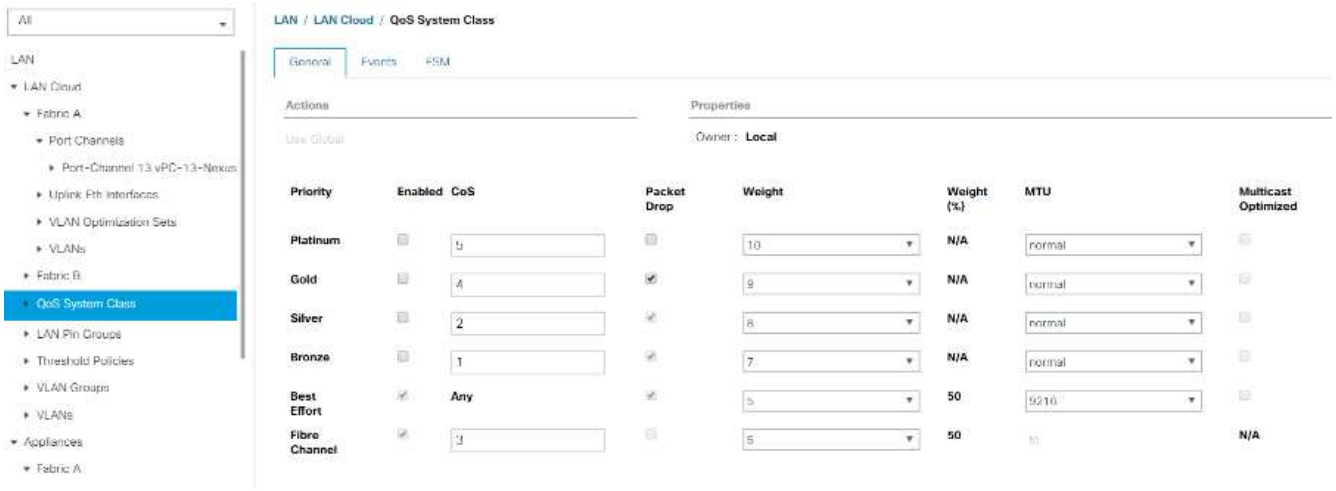
53. Fare clic su Save Changes (Salva modifiche) e OK.
54. Selezionare Appliance Interface 1/4 in Fabric B.
55. Nel campo User Label (etichetta utente), inserire le informazioni che indicano la porta dello storage controller, ad esempio `<storage_controller_02_name>:e0f`. Fare clic su Save Changes (Salva 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.



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".

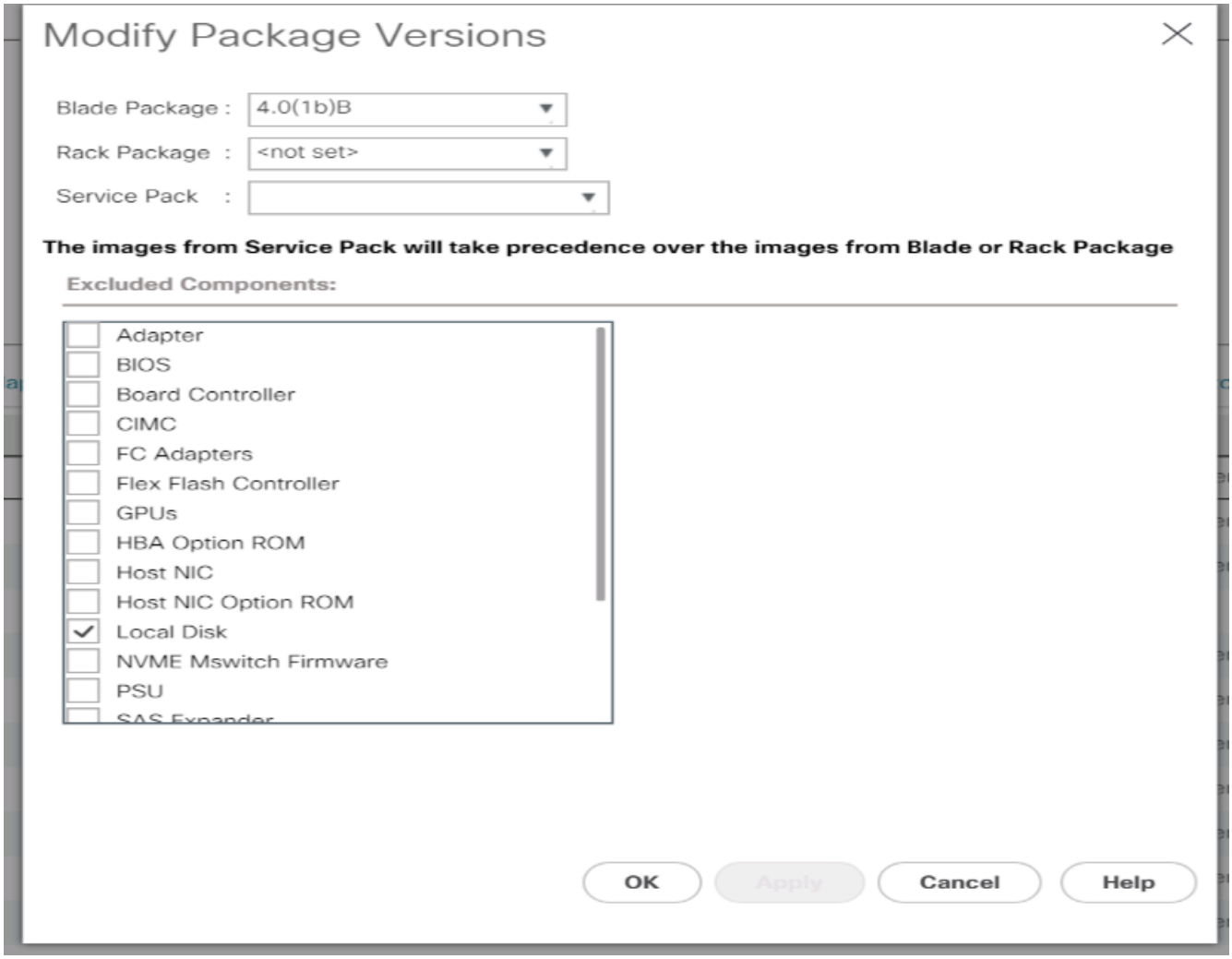
Creare un pacchetto firmware host

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.



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.

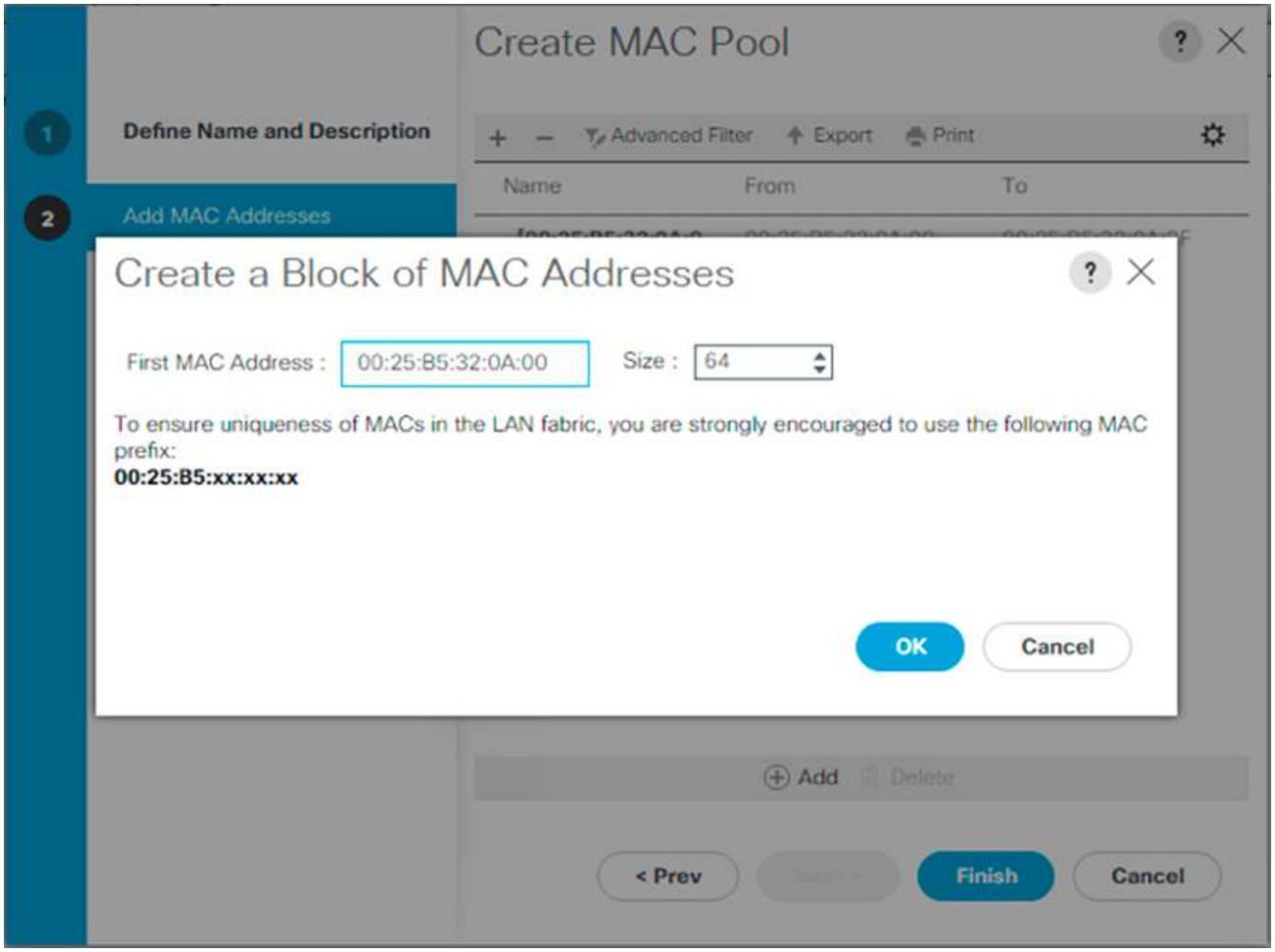
   In questa procedura vengono creati due pool di indirizzi MAC, uno per ciascun fabric di switching.

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.

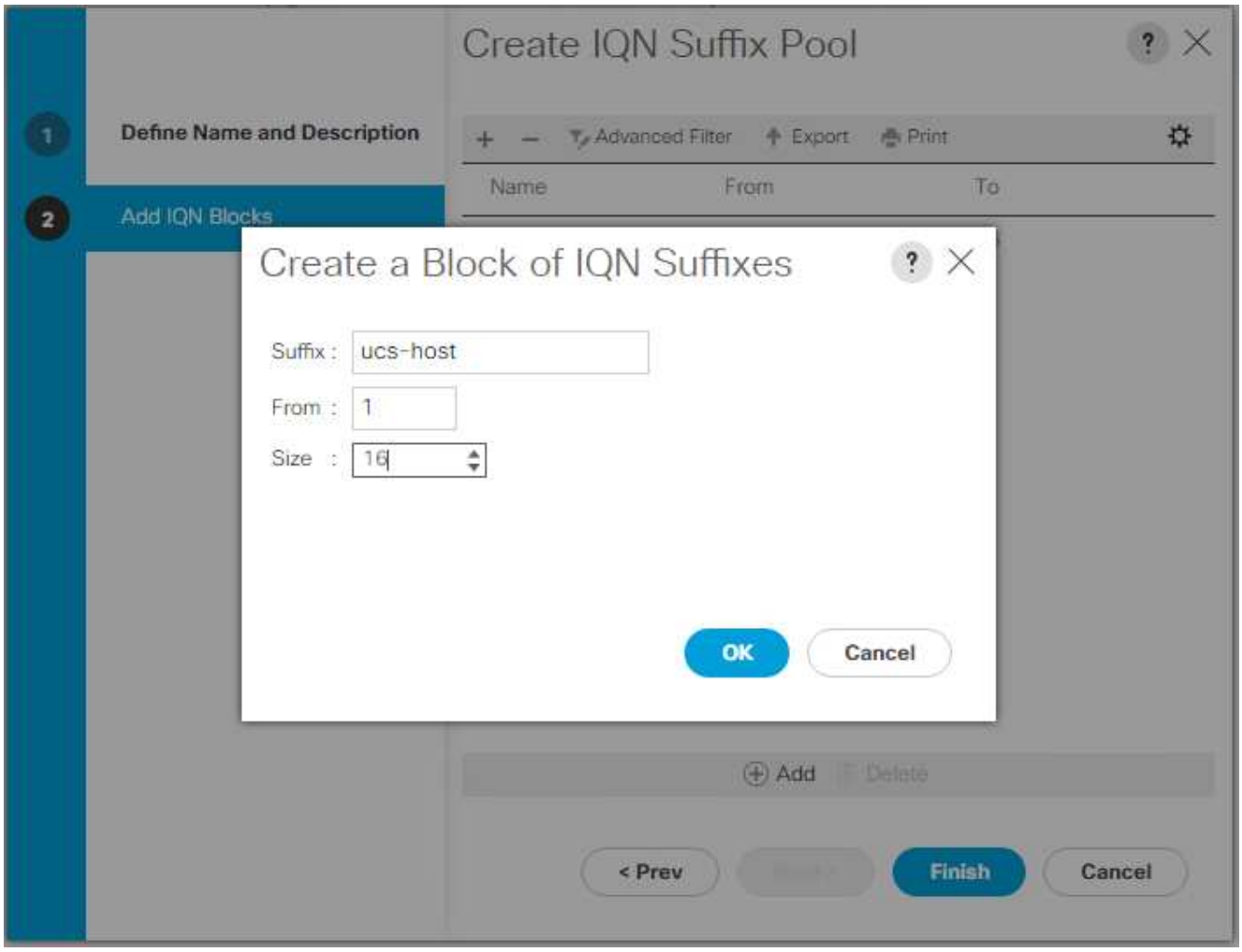
Creare un pool IQN iSCSI

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.

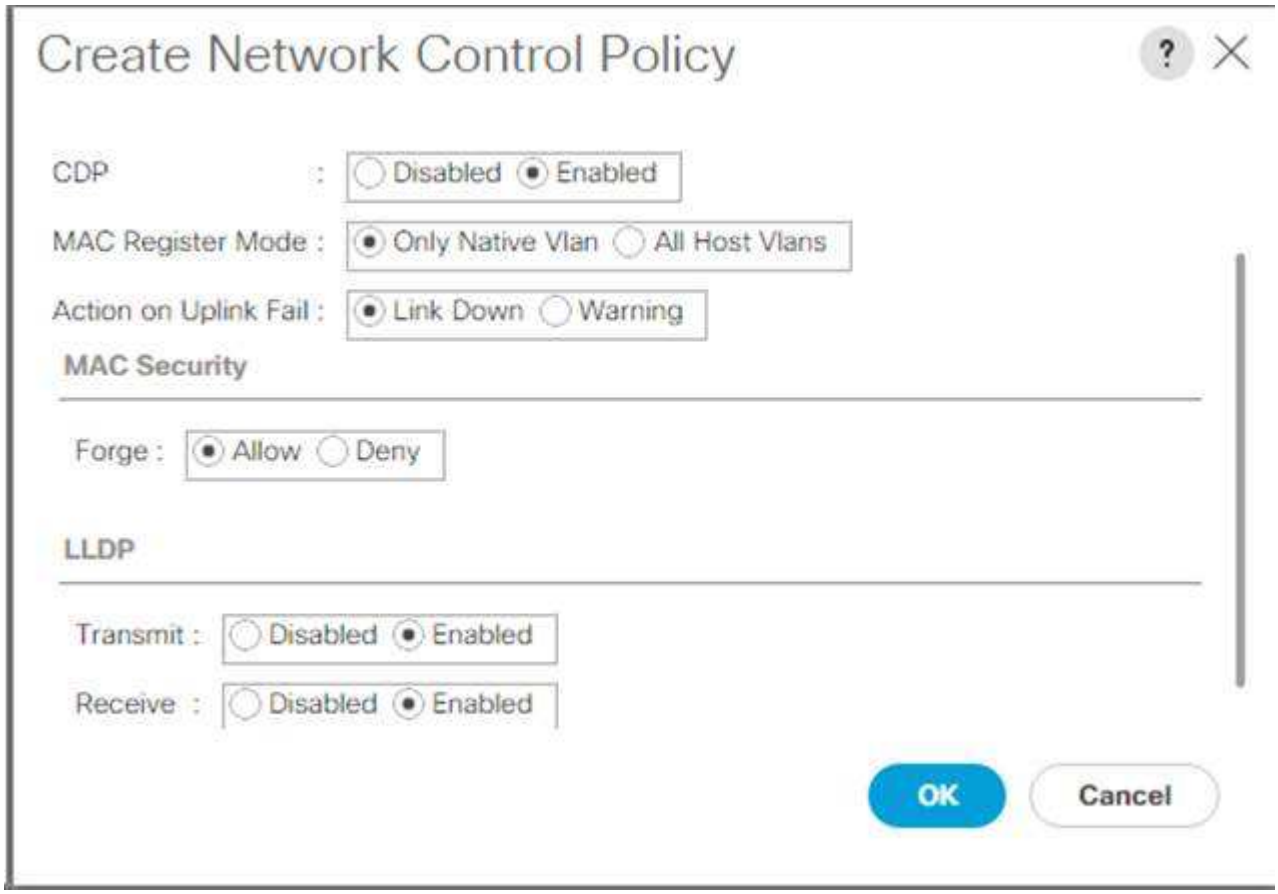
1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Pools > root.
3. Fare clic con il pulsante destro del mouse su Server Pools.

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 `s.
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:

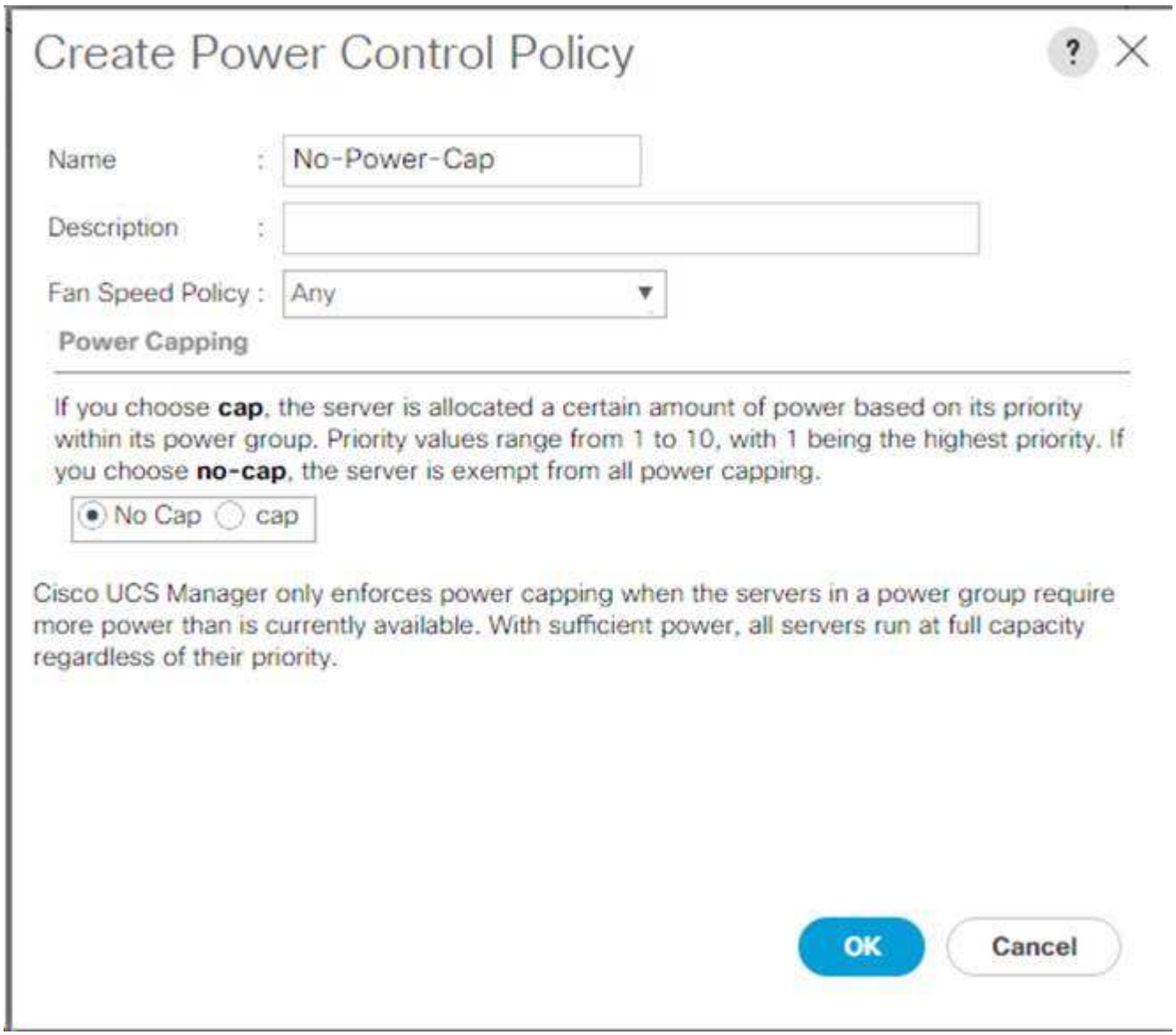
1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Criteri di controllo di rete.
4. Selezionare Crea criterio di controllo di rete.
5. Immettere il nome del criterio Enable-CDP-LLDP.
6. Per CDP, selezionare l'opzione Enabled (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.



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.

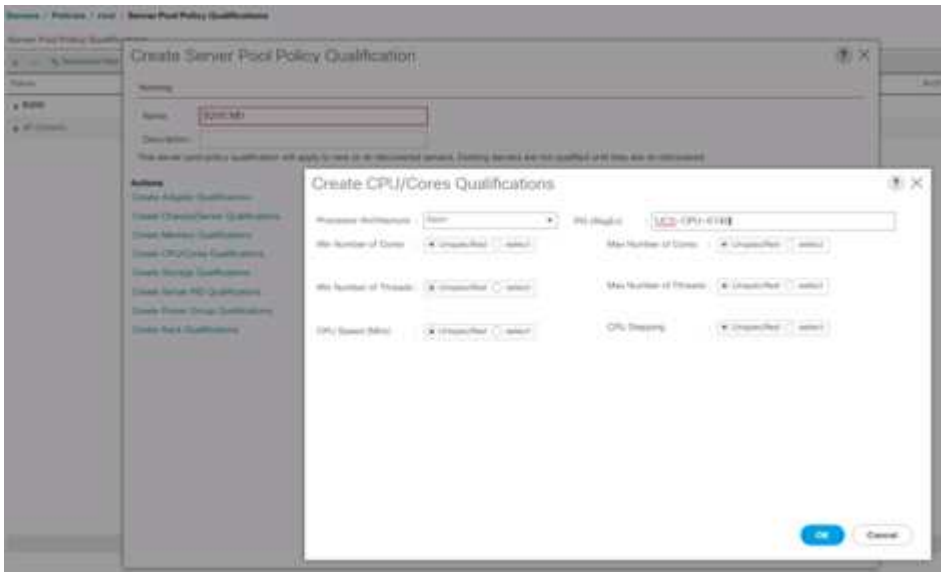


Crea policy di qualificazione del pool di server (opzionale)

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.

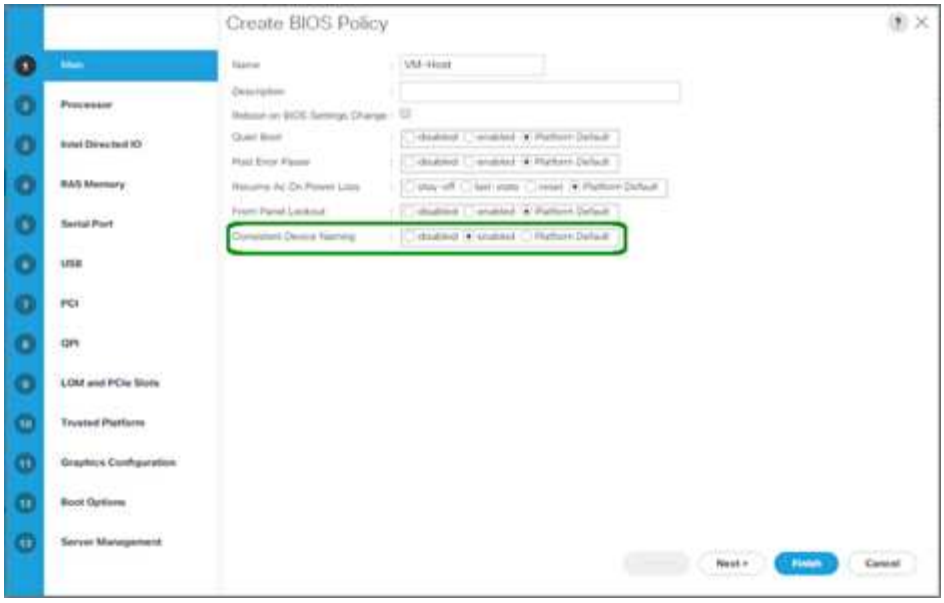
1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Selezionare Server Pool Policy Qualifications (Criteri policy pool server).
4. Selezionare Create Server Pool Policy Qualification (Crea criterio pool di server) o Add (Aggiungi).
5. Assegnare un nome 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.



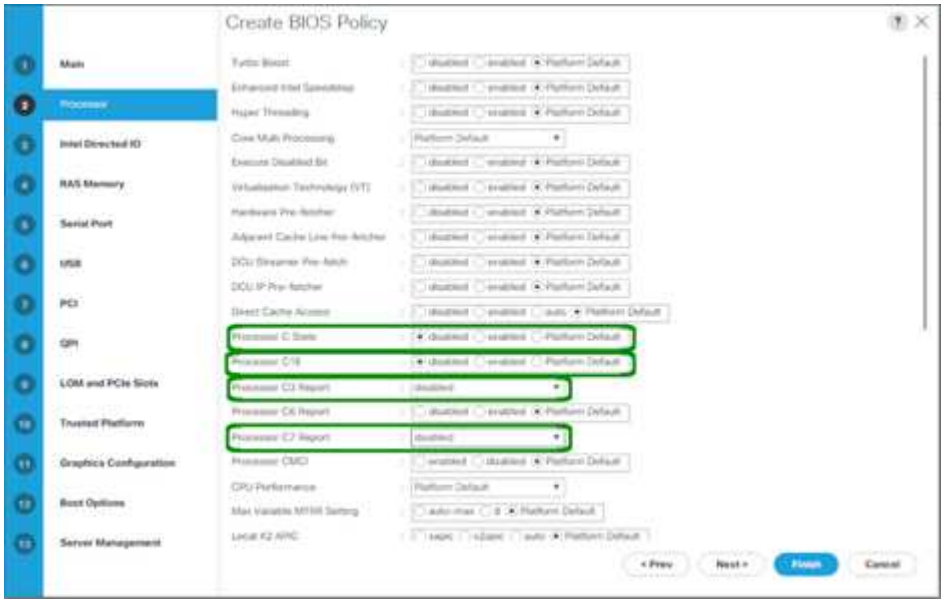
Creare una policy del BIOS del server

Per creare un criterio BIOS del server per l'ambiente Cisco UCS, attenersi alla seguente procedura:

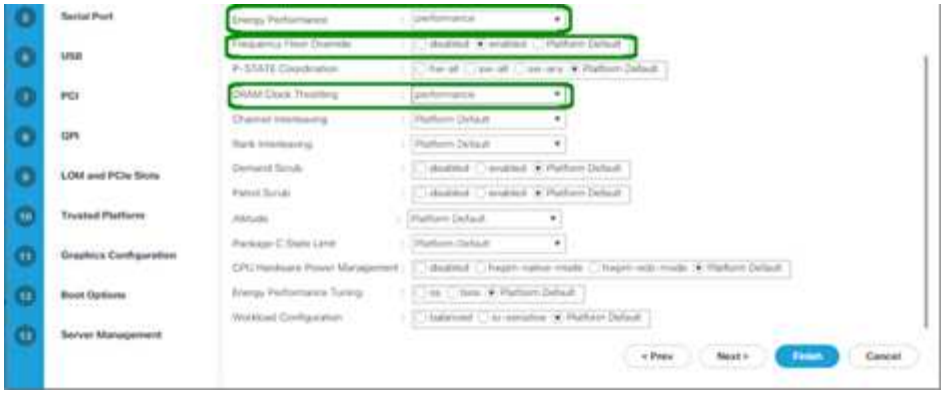
1. In Cisco UCS Manager, fare clic su Servers (Server) a sinistra.
2. Selezionare Policy > root.
3. Fare clic con il pulsante destro del mouse su Criteri del BIOS.
4. Selezionare Create BIOS Policy (Crea policy BIOS).
5. Inserire VM-host come nome del criterio del BIOS.
6. Impostare l'opzione Quiet Boot su Disabled (Disattivato).
7. Impostare l'opzione Naming periferica coerente su attivato.



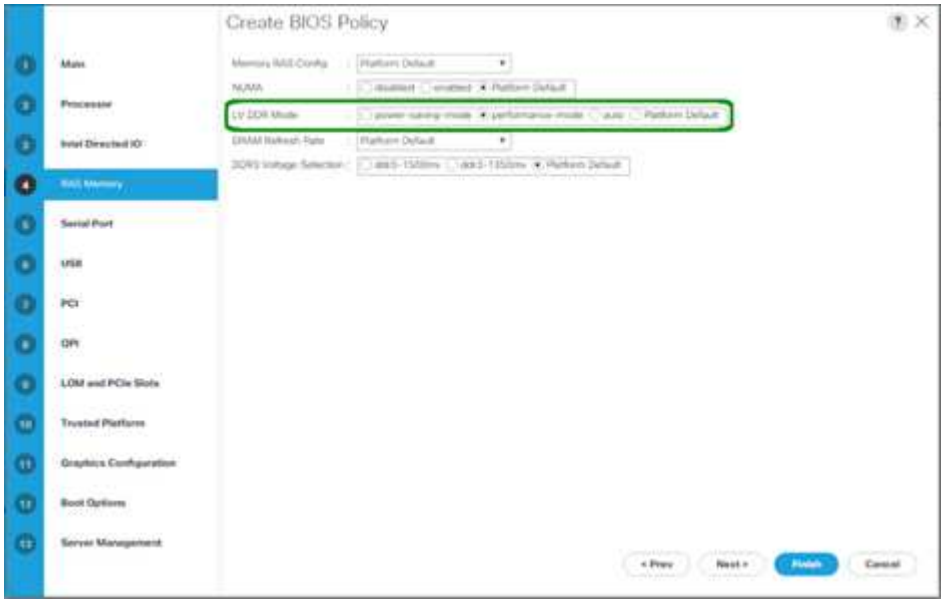
8. Selezionare la scheda Processor (processore) e impostare i seguenti parametri:
    - Stato del processore C: Disattivato
    - Processore C1E: Disattivato
    - Report del processore C3: Disattivato
    - Report processore C7: Disattivato



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)

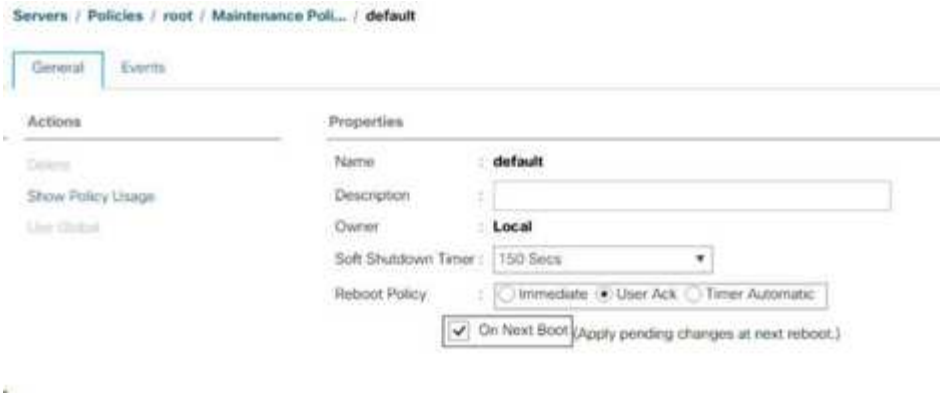


11. Fare clic su Finish (fine) per creare il criterio del BIOS.
12. Fare clic su OK.

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.



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.

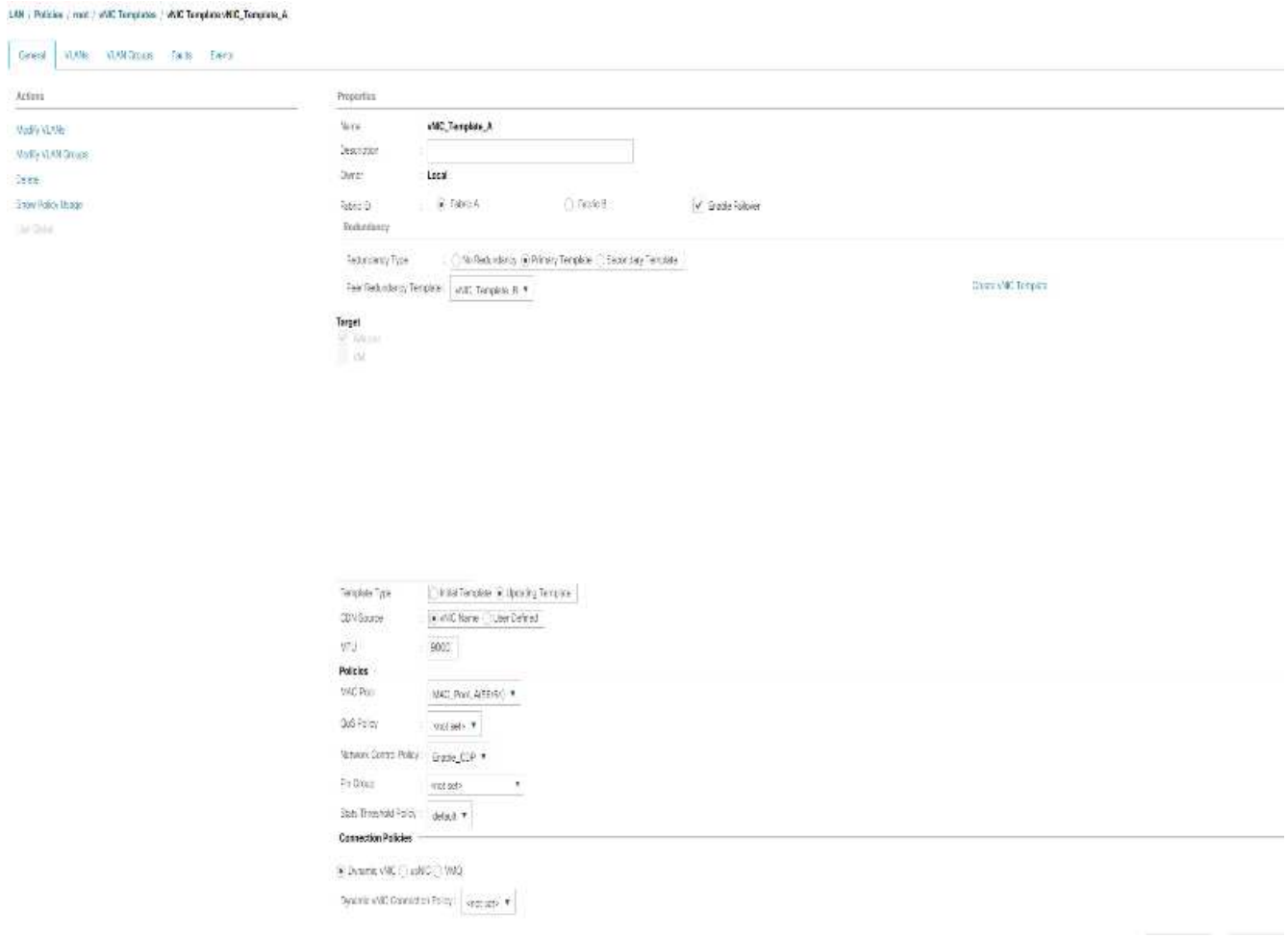
> Vengono creati in totale quattro modelli vNIC.

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.

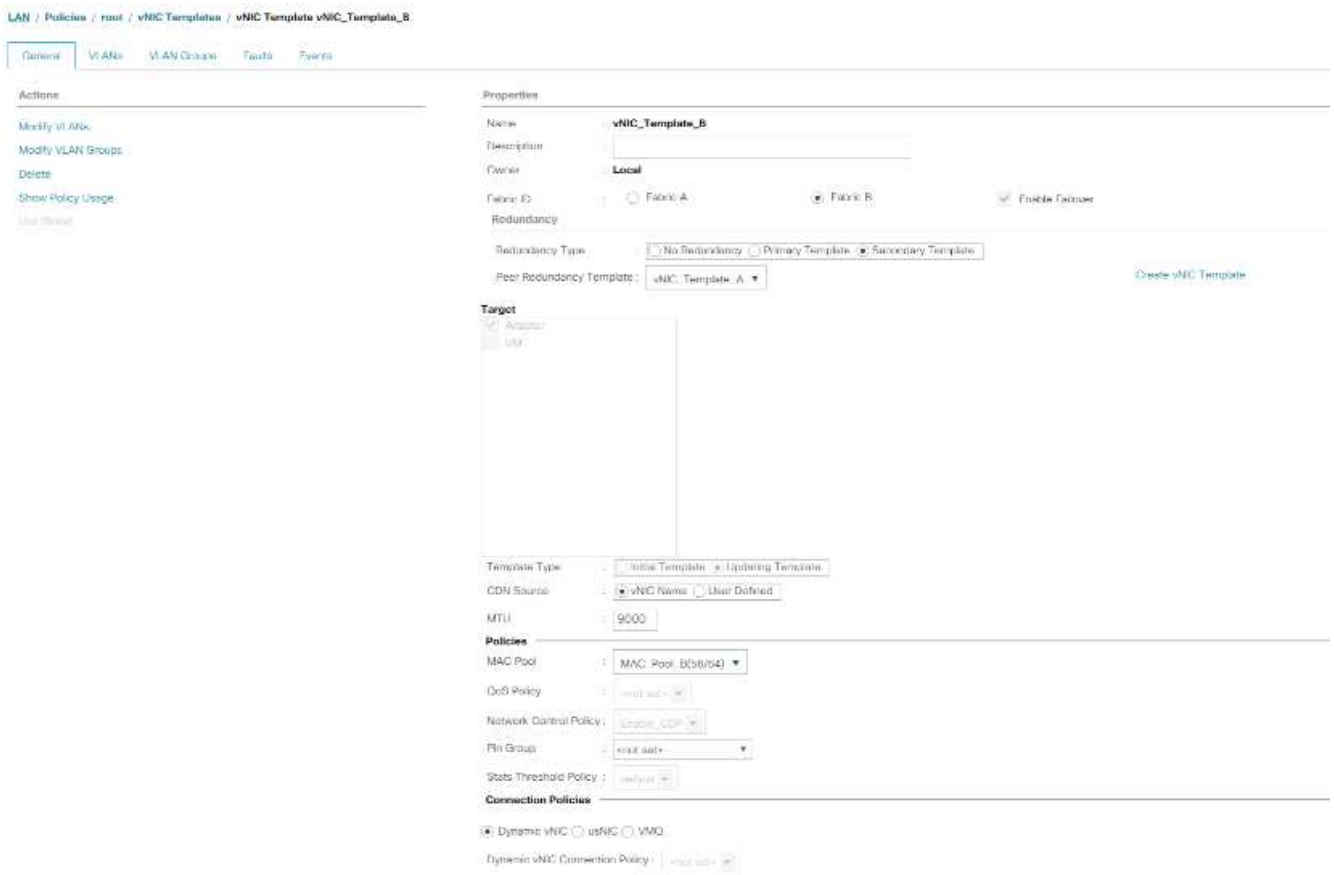


Per creare il modello di ridondanza secondario Infra-B, attenersi alla seguente procedura:

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.

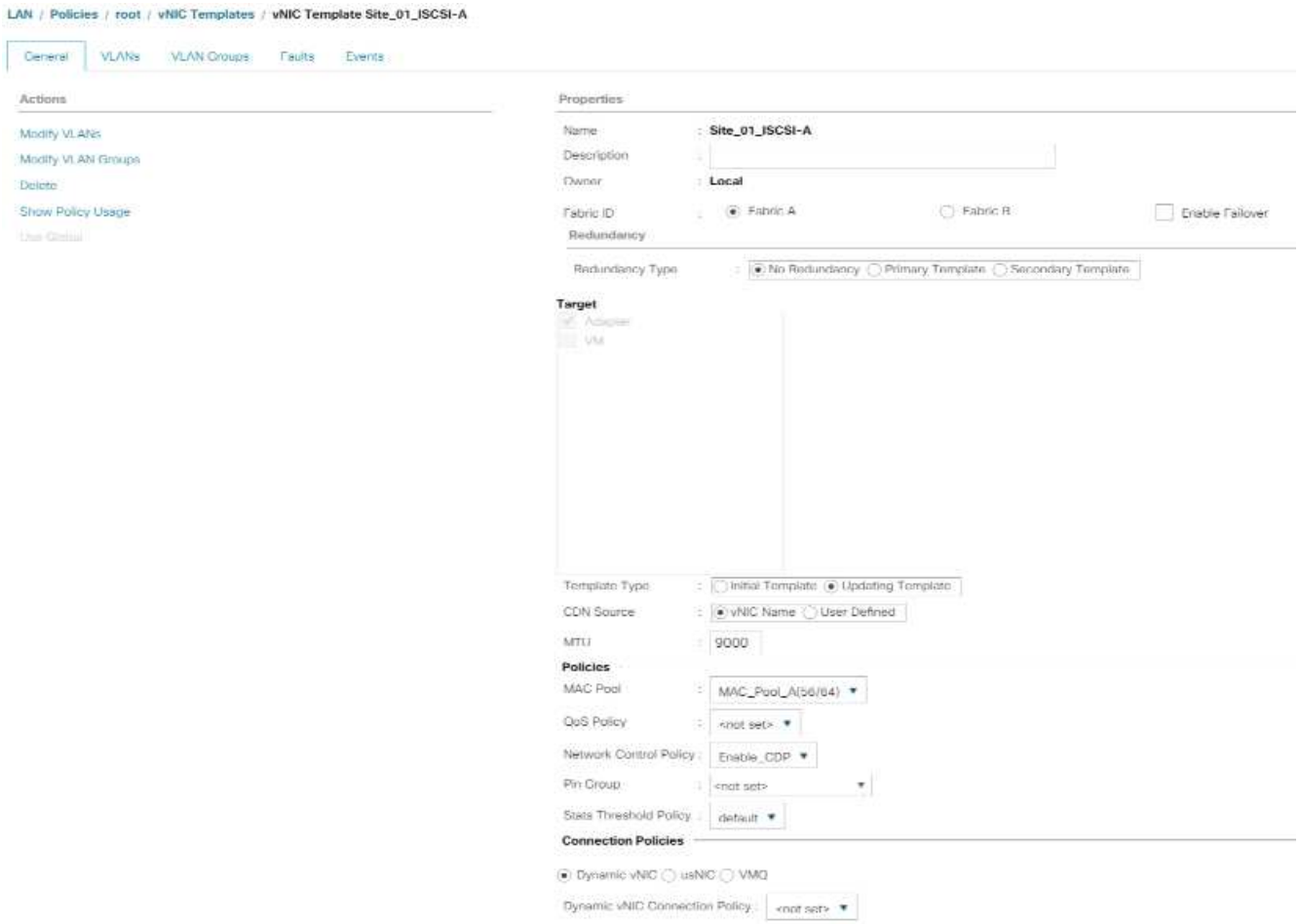


Creare vNIC iSCSI

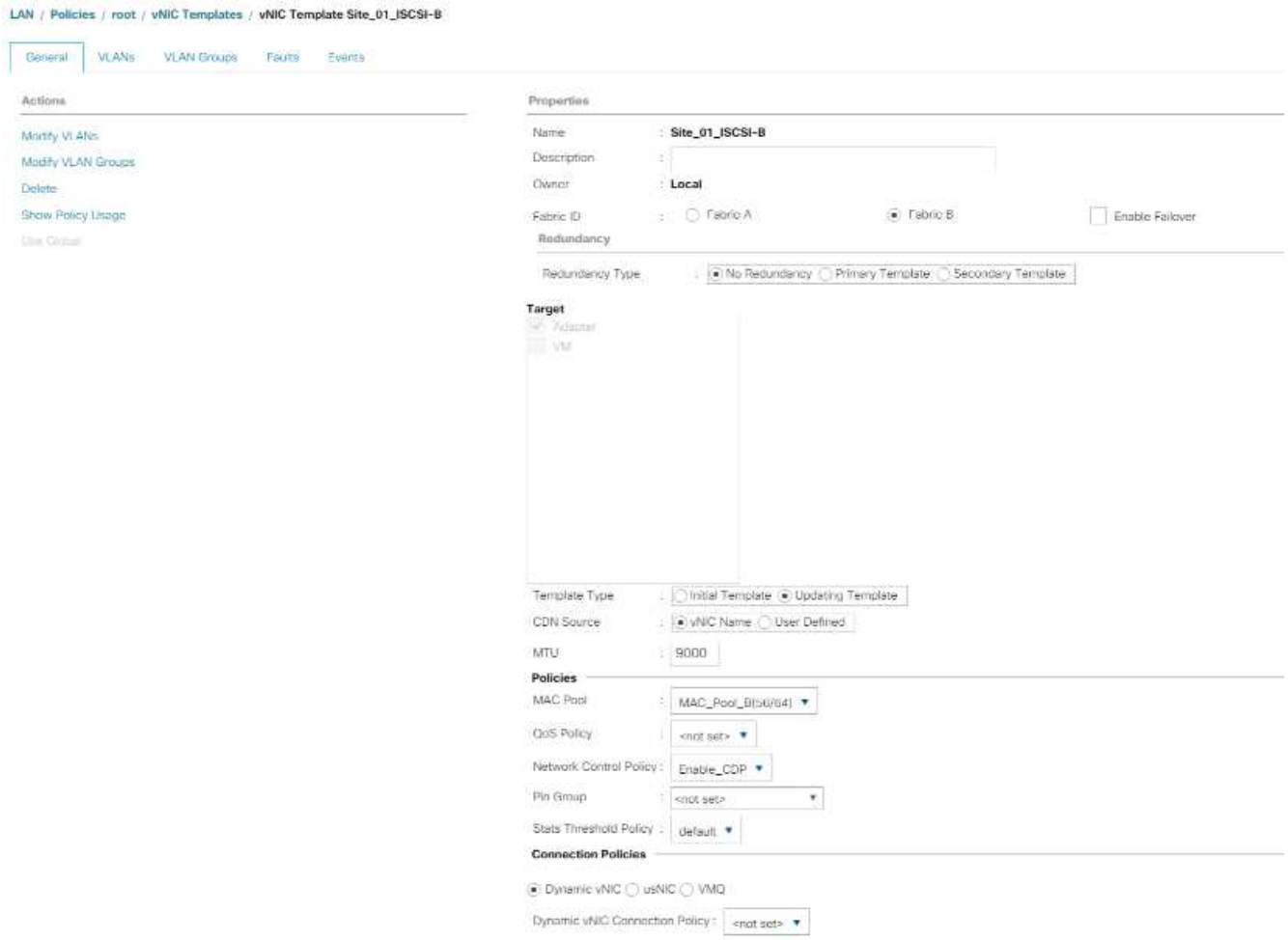
Per creare vNIC iSCSI, attenersi alla seguente procedura:

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.



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.



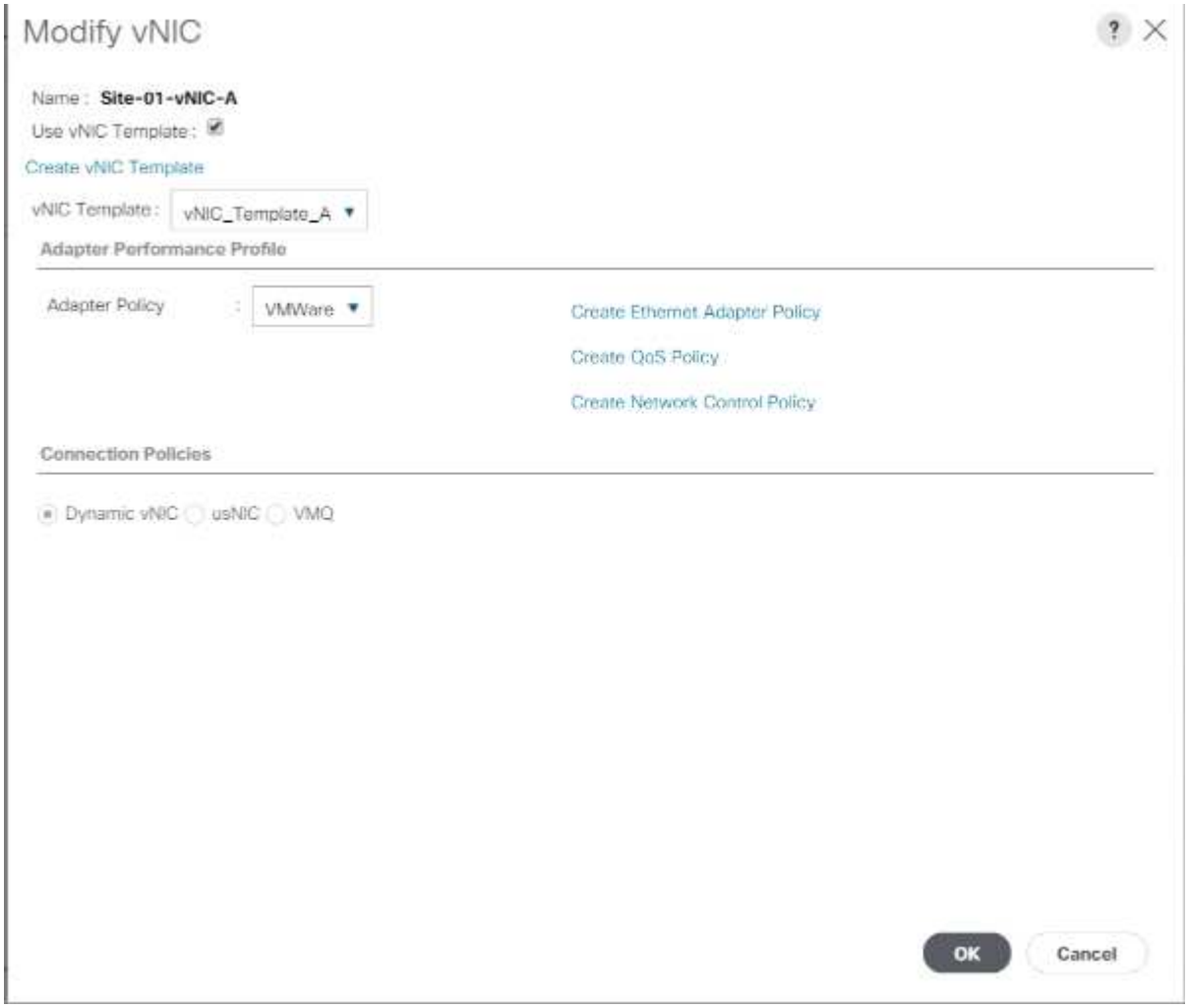
Creare una policy di connettività LAN per l'avvio iSCSI

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:

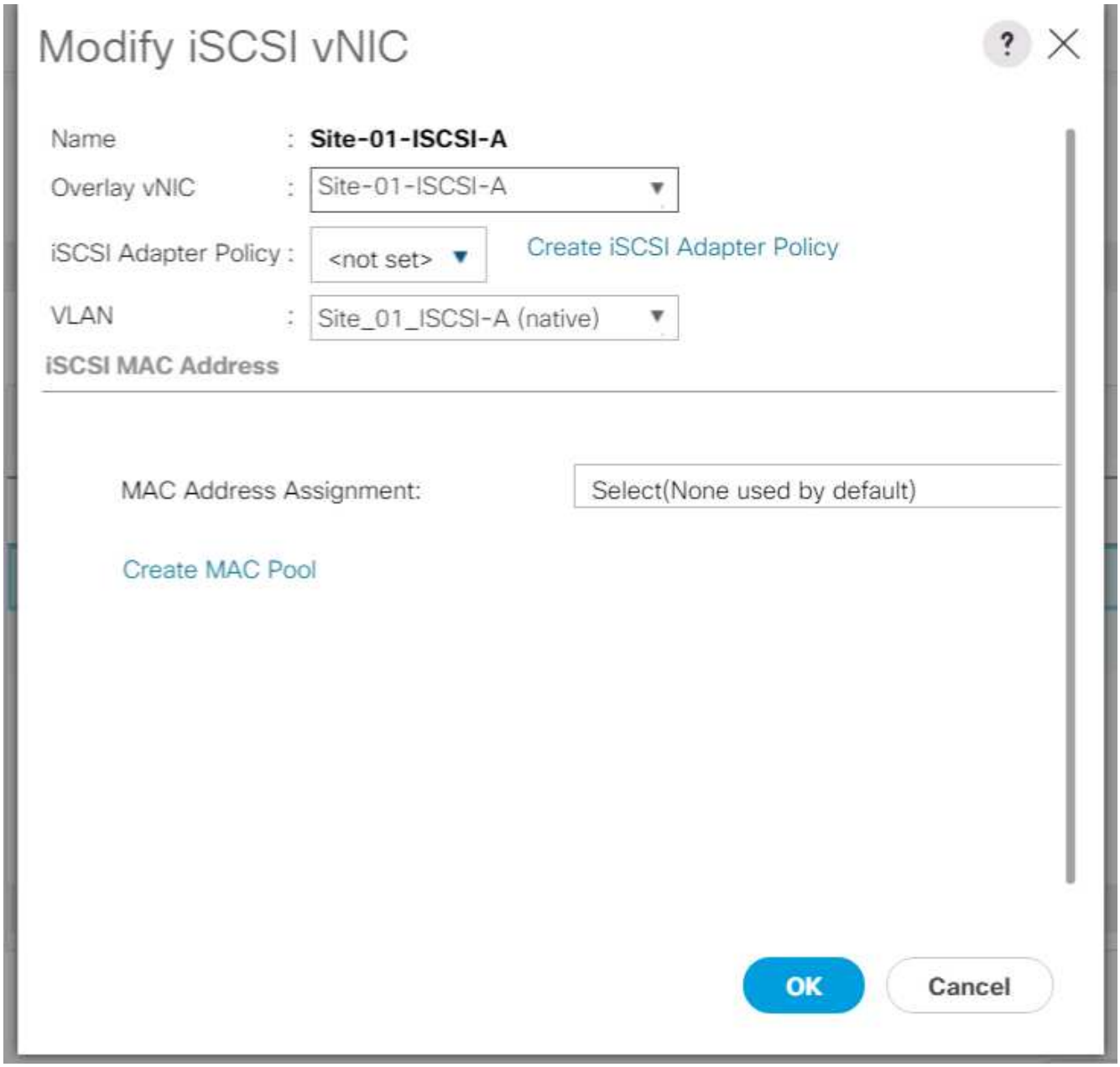
1. In Cisco UCS Manager, fare clic su LAN a sinistra.
2. Selezionare LAN > Policies > root.
3. Fare clic con il pulsante destro del mouse su Criteri di connettività LAN.
4. Selezionare Crea policy di connettività LAN.
5. Invio `Site-XX-Fabric-A` come nome del criterio.
6. Fare clic sull'opzione Add (Aggiungi) 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.

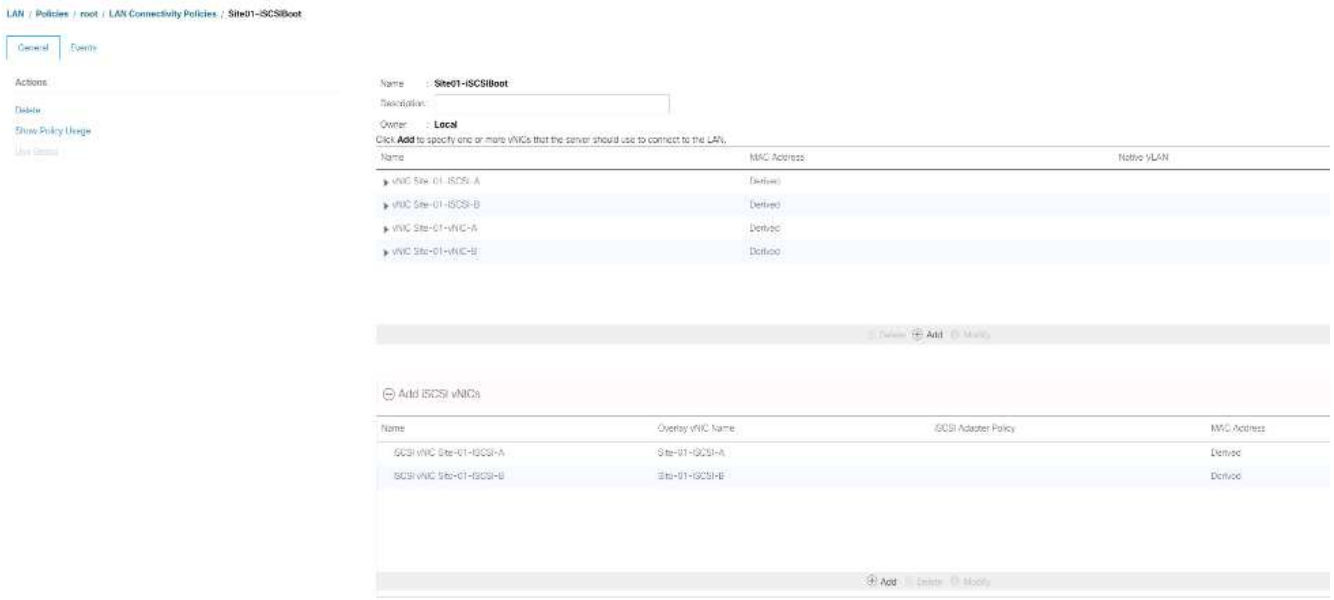


12. Fare clic sull'opzione Add (Aggiungi) superiore per aggiungere una vNIC.
13. Nella finestra di dialogo Create vNIC (Crea vNIC), immettere `Site-01-vNIC-B` Come nome della vNIC.
14. Selezionare l'opzione Use vNIC Template (Usa modello vNIC).
15. Nell'elenco vNIC Template (modello vNIC), selezionare `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.



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.

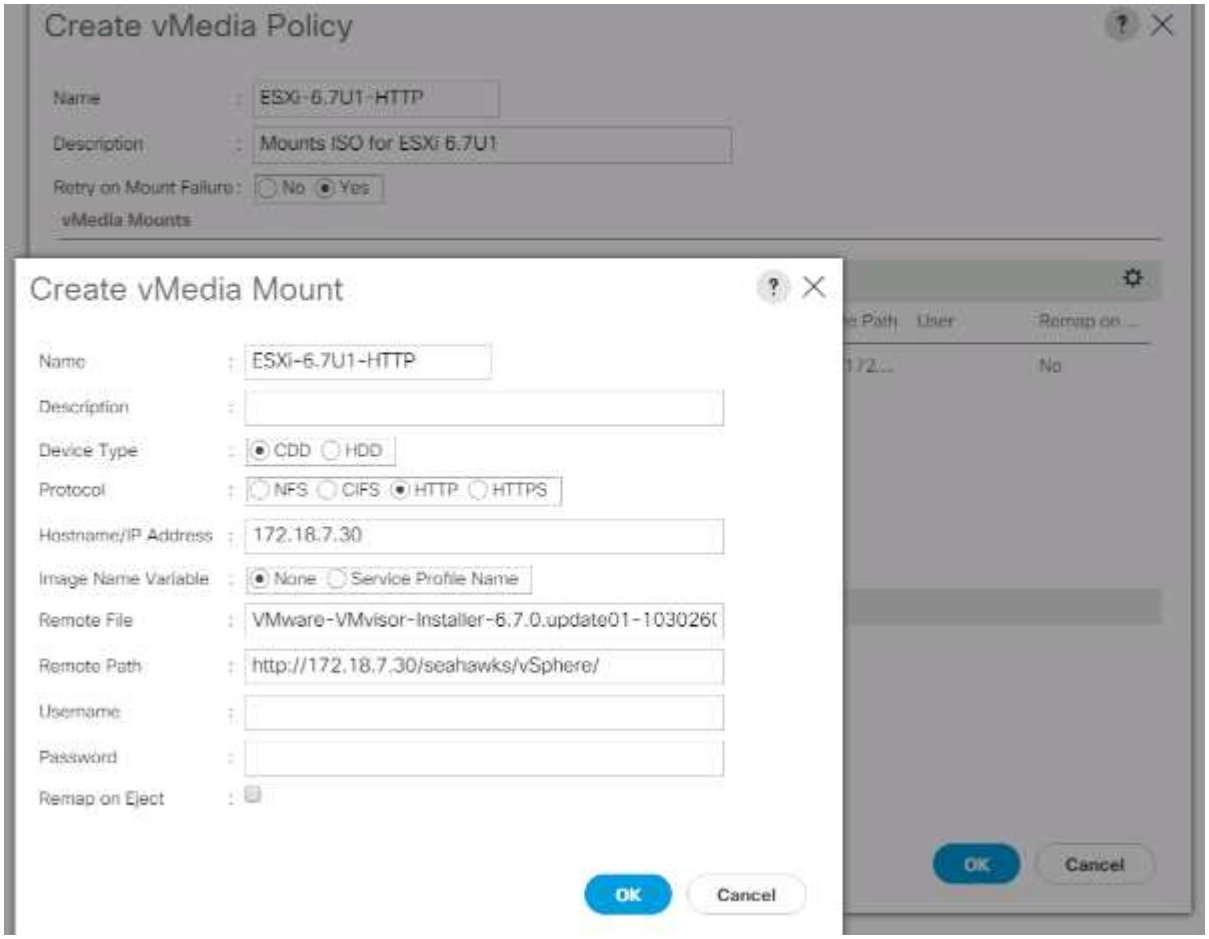
13. Invio `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso` Come nome del file remoto.

    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

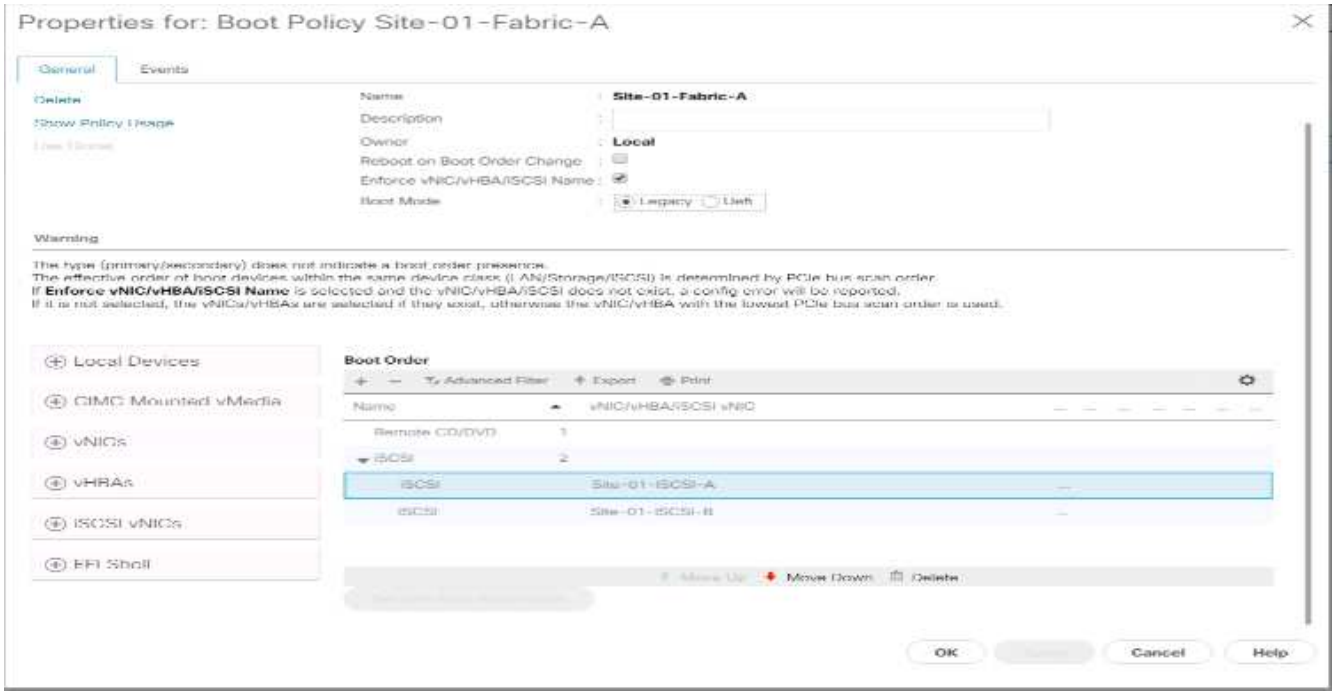
La procedura descritta in questa sezione si applica a un ambiente Cisco UCS in cui due interfacce logiche iSCSI (LIFF) si trovano sul nodo cluster 1 (`iscsi_lif01a` e. `iscsi_lif01b`) E due LIF iSCSI si trovano sul nodo cluster 2 (`iscsi_lif02a` e. `iscsi_lif02b`). Inoltre, si presuppone che I LIF A 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.



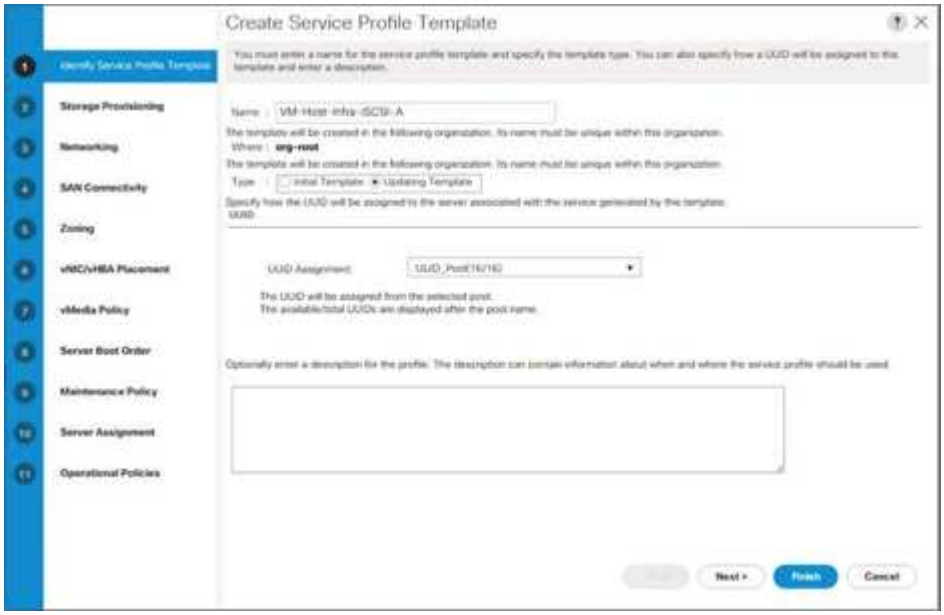
Creare un modello di profilo del servizio

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

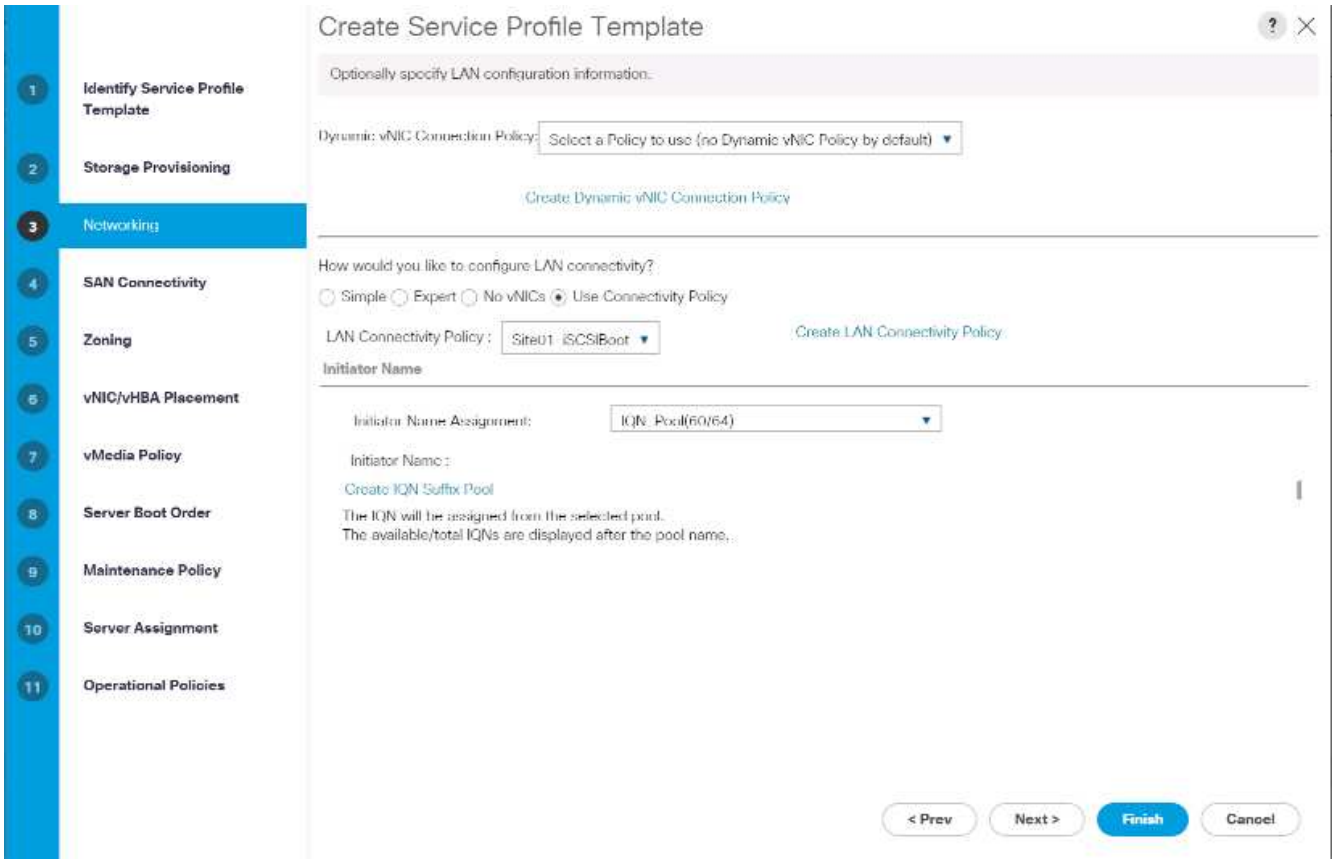
Per configurare il provisioning dello storage, attenersi alla seguente procedura:

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

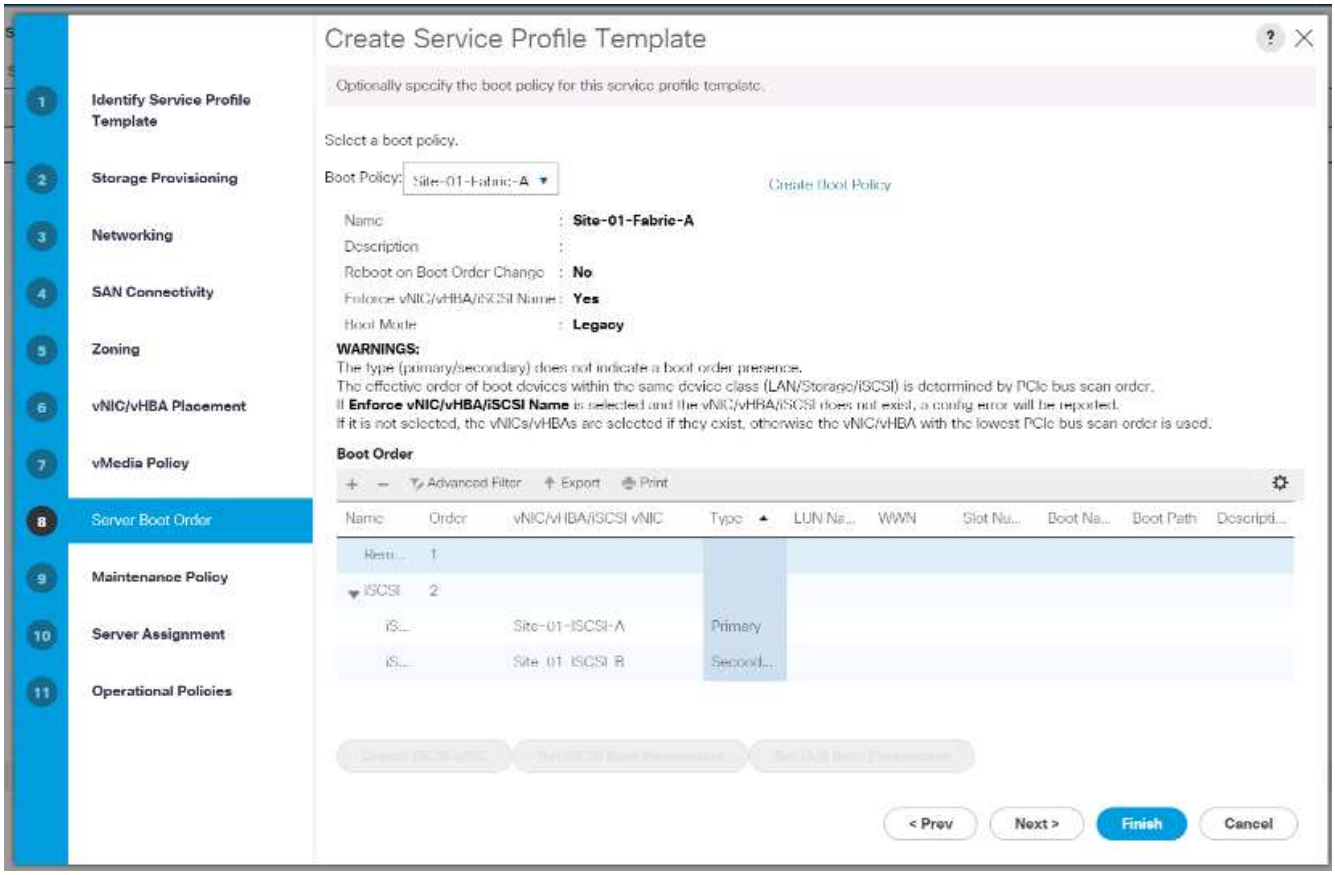
Per configurare il criterio vMedia, attenersi alla seguente procedura:

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.



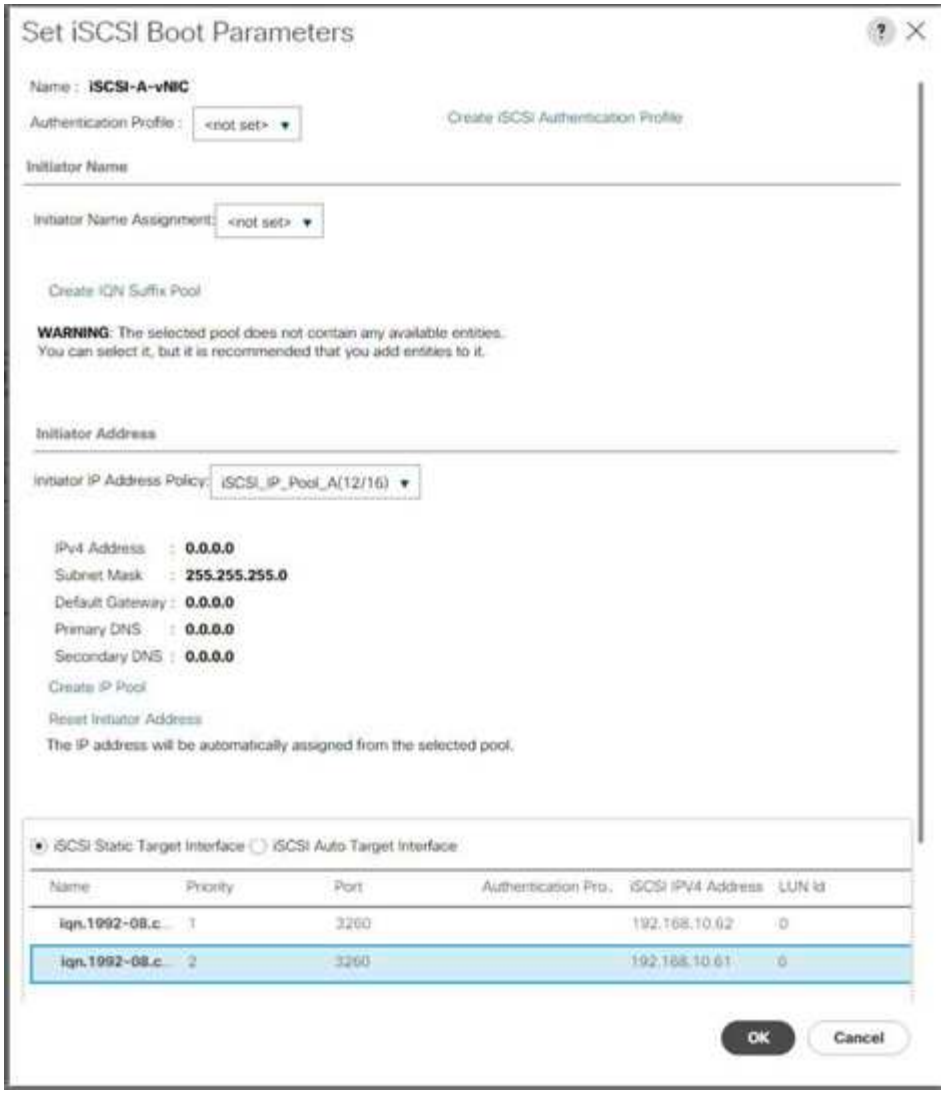
2. Nell'ordine boor, selezionare `Site-01- iSCSI-A`.
3. Fare clic su Set iSCSI Boot Parameters.
4. Nella finestra di dialogo Set iSCSI Boot Parameters (Imposta parametri di avvio iSCSI), lasciare l'opzione Authentication Profile (Profilo di autenticazione) su Not Set (non impostato) a meno che non sia 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.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                       up
```

10. Immettere l'indirizzo IP di `iscsi_lif_02a` Per il campo IPv4 Address (Indirizzo IPv4).

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).

15. Fare clic su OK per aggiungere la destinazione statica iSCSI.



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.

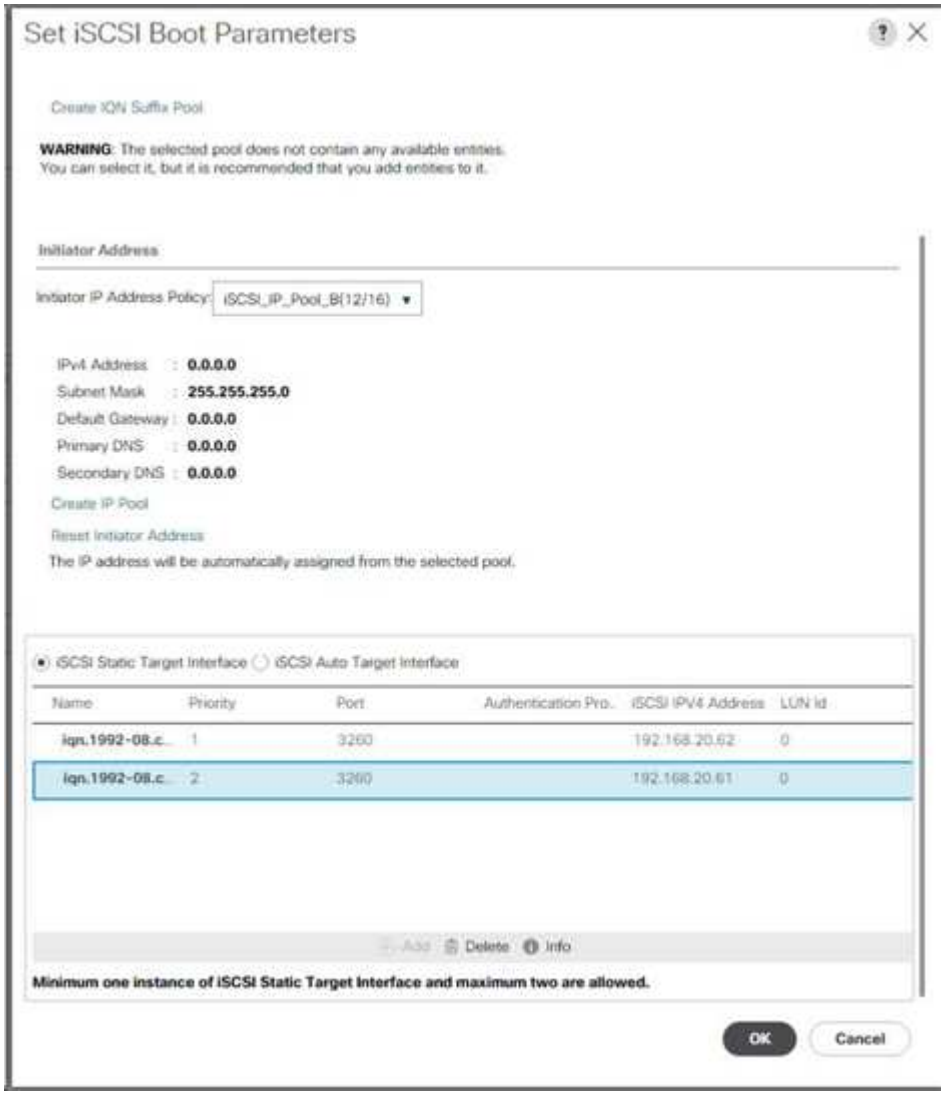
16. In Boot Order (Ordine di avvio), selezionare iSCSI-B-vNIC.
17. Fare clic su Set iSCSI Boot Parameters.
18. Nella finestra di dialogo Set iSCSI Boot Parameters (Imposta parametri di avvio iSCSI), lasciare l'opzione Authentication Profile (Profilo di autenticazione) come Not Set (non impostato), a 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
           Target                          Target                      Status
Vserver    Name                            Alias                       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).

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).

29. Fare clic su OK per aggiungere la destinazione statica iSCSI.

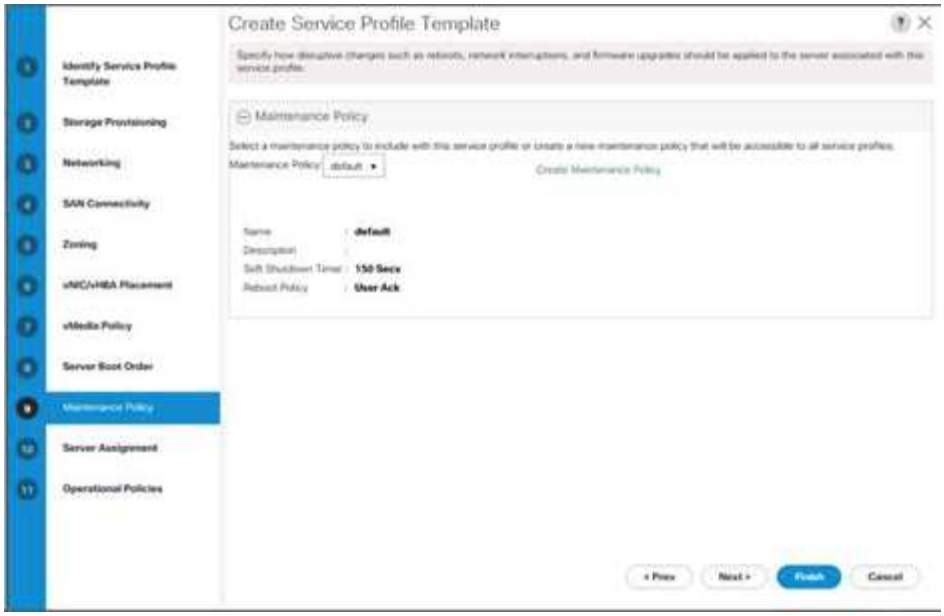


30. Fare clic su Avanti.

Configurare la policy di manutenzione

Per configurare la policy di manutenzione, attenersi alla seguente procedura:

1. Impostare la policy di manutenzione su default.

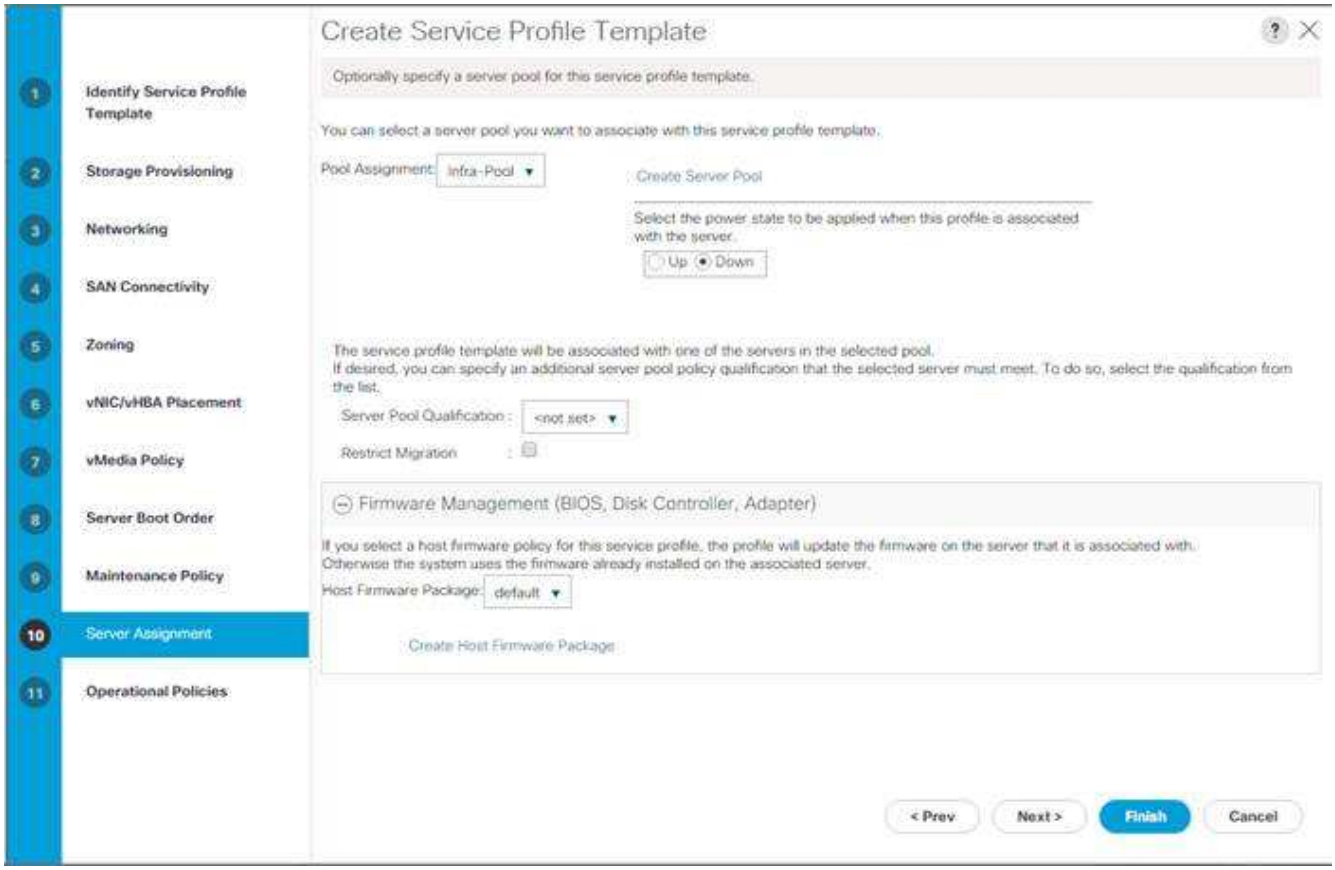


2. Fare clic su Avanti.

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.

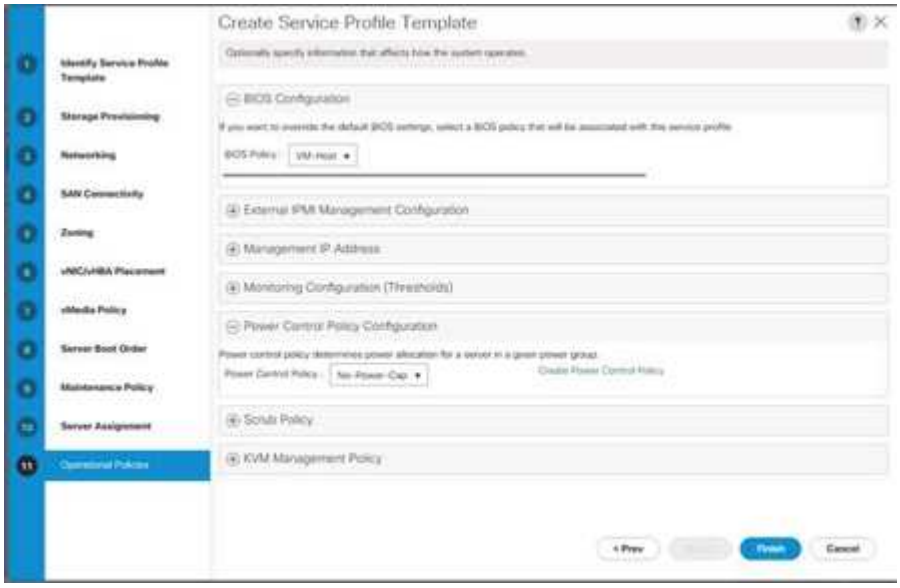


4. Fare clic su Avanti.

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

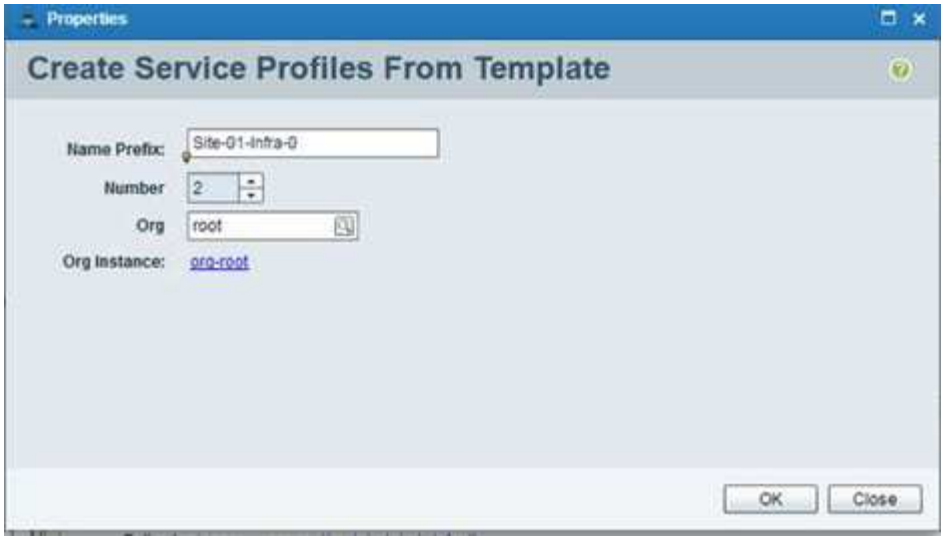
Per creare un modello di profilo del servizio con vMedia attivato, attenersi alla seguente procedura:

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.

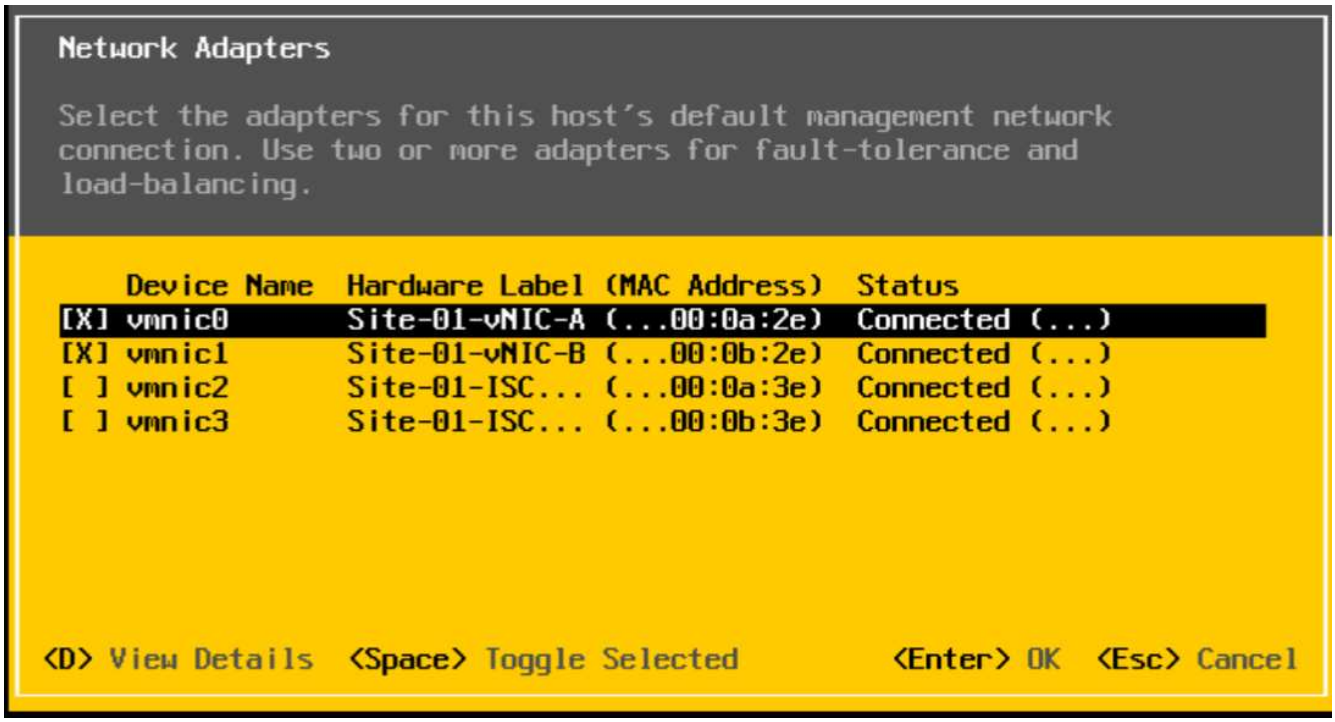
Configurare la rete di gestione per gli host ESXi

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.



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 (Sfoglia).
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.

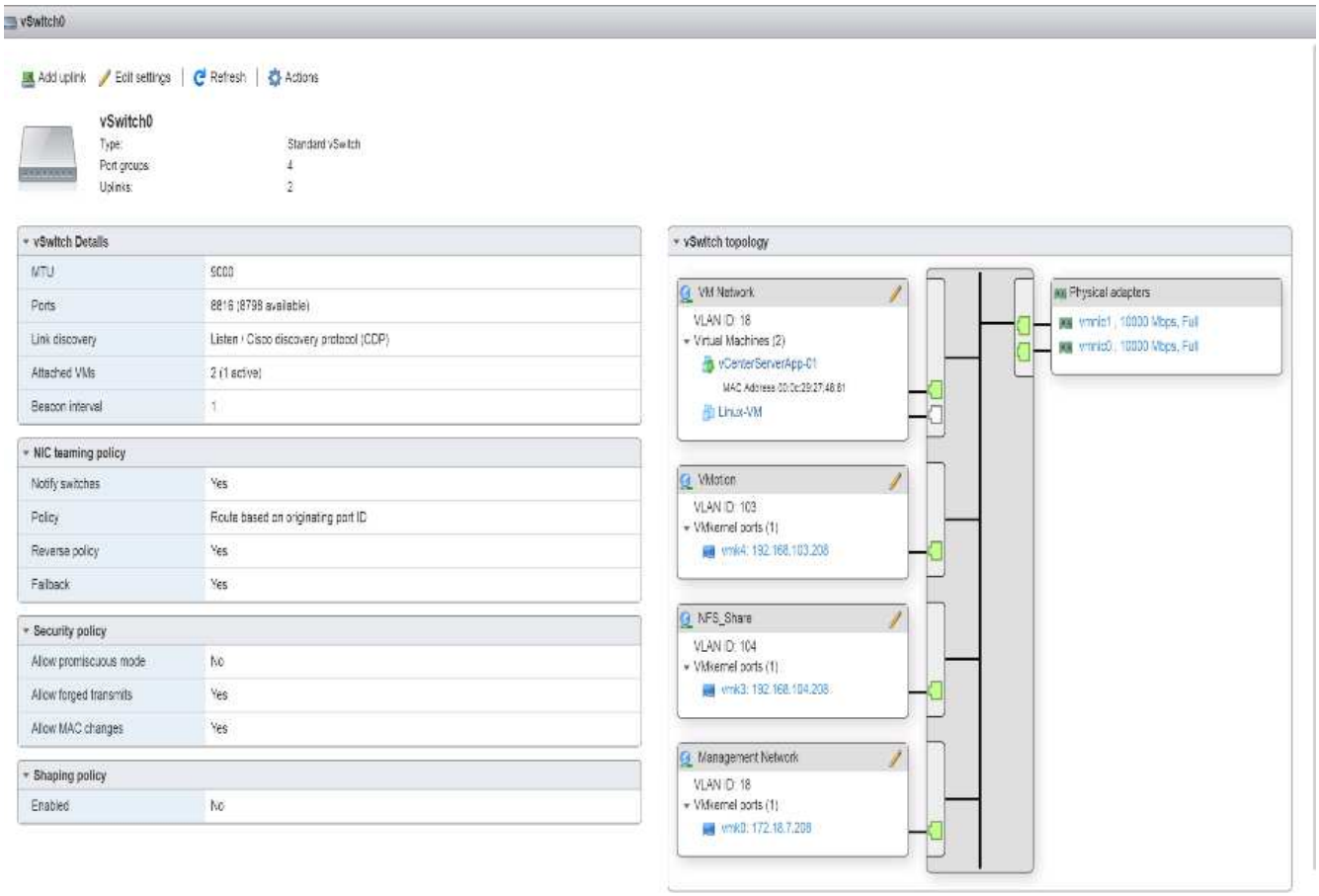
2. Nel riquadro centrale, selezionare la scheda Virtual switches (interruttori virtuali).
3. Selezionare vSwitch0.
4. Selezionare Modifica impostazioni.
5. Impostare la MTU su 9000.
6. Espandere il raggruppamento NIC.
7. Nella sezione Ordine di failover, selezionare vmnic1 e fare clic su Contrassegna 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.

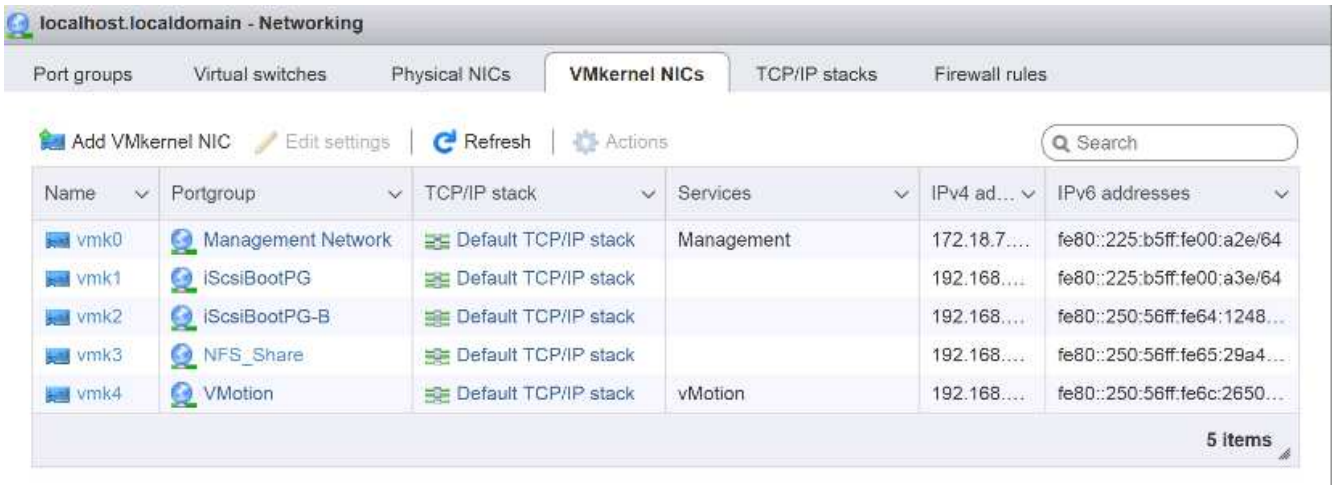
21. Fare clic su Salva.
22. Selezionare la scheda Virtual switches (interruttori virtuali).
23. Selezionare Add standard virtual switch (Aggiungi switch virtuale standard).
24. Specificare un nome di `iScsciBootvSwitch-B` Per il nome vSwitch.
25. Impostare MTU su 9000.
26. Selezionare vmnic3 dal menu 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:



62. Selezionare la scheda NIC VMkernel per confermare gli adattatori virtuali configurati. Gli adattatori elencati devono essere simili al seguente esempio:



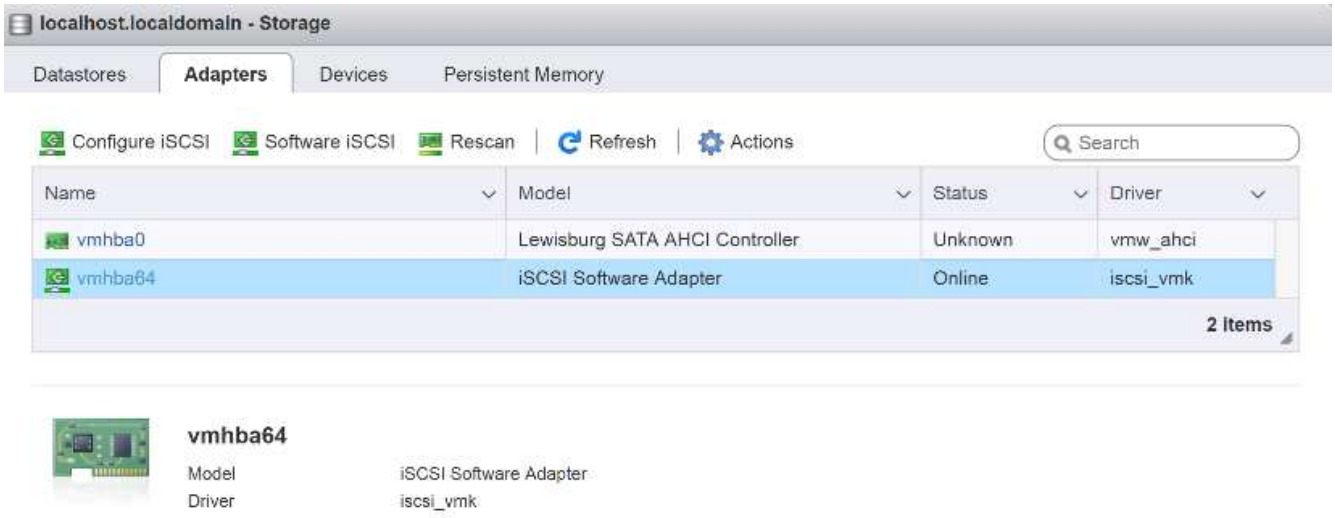
Configurare il multipathing iSCSI

ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

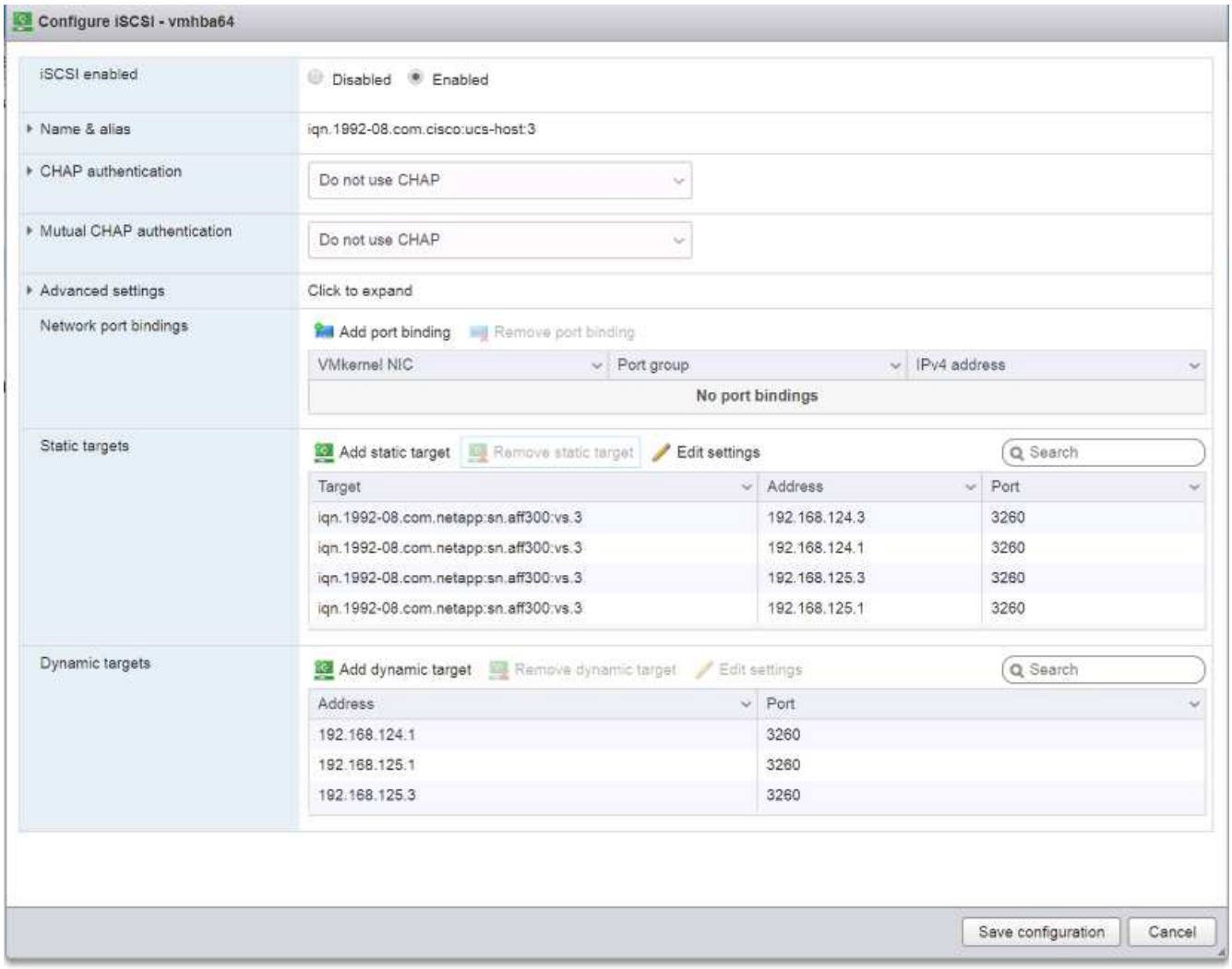
Per configurare il multipathing iSCSI sull'host ESXi VM-host-Infra-01 e VM-host-Infra-02, attenersi alla seguente procedura:

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.



Per ottenere tutti i `iscsi_lif` Indirizzi IP, accedere all'interfaccia di gestione del cluster di storage NetApp ed eseguire `network interface show` comando.

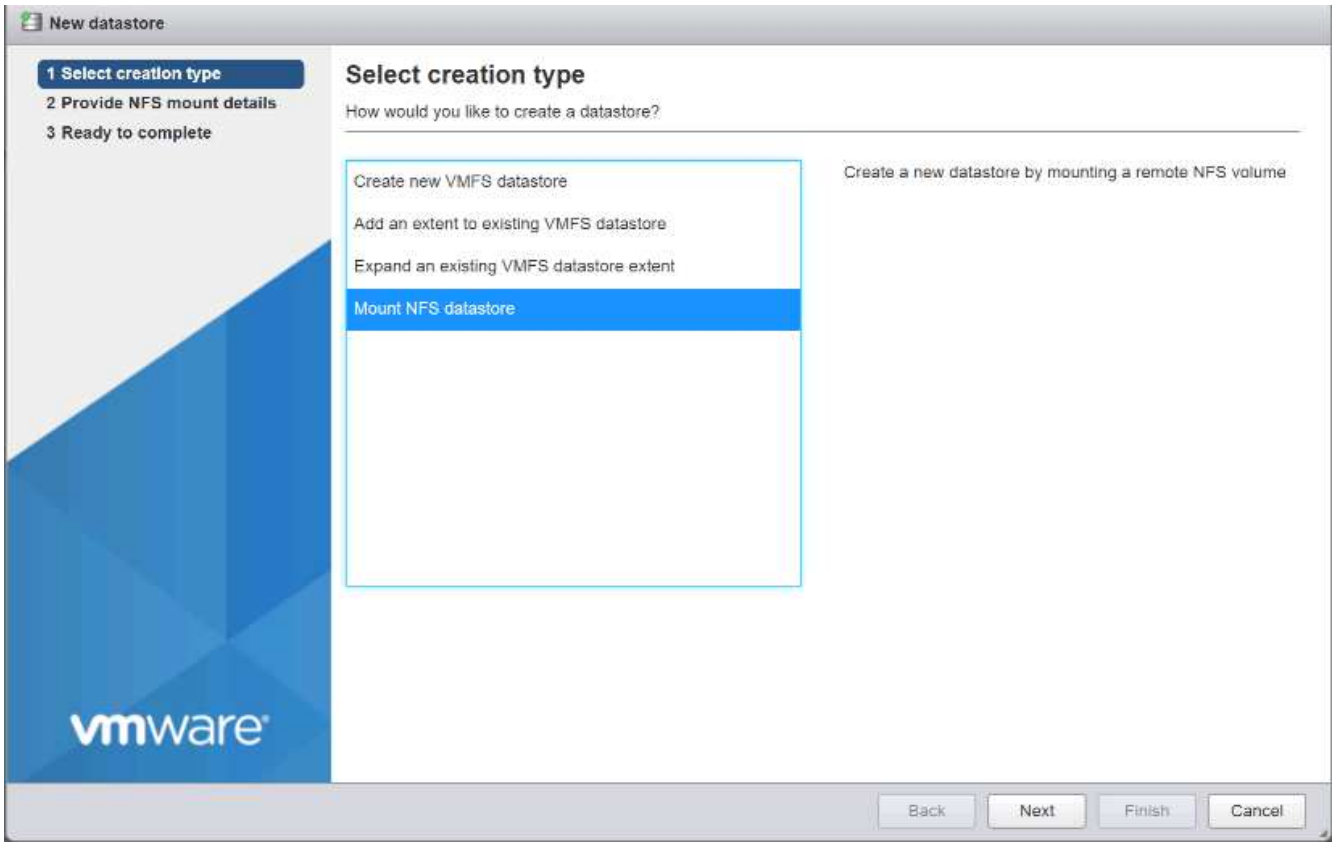
> L'host esegue automaticamente una nuova scansione dell'adattatore di storage e le destinazioni vengono aggiunte a destinazioni statiche.

Montare gli archivi dati richiesti

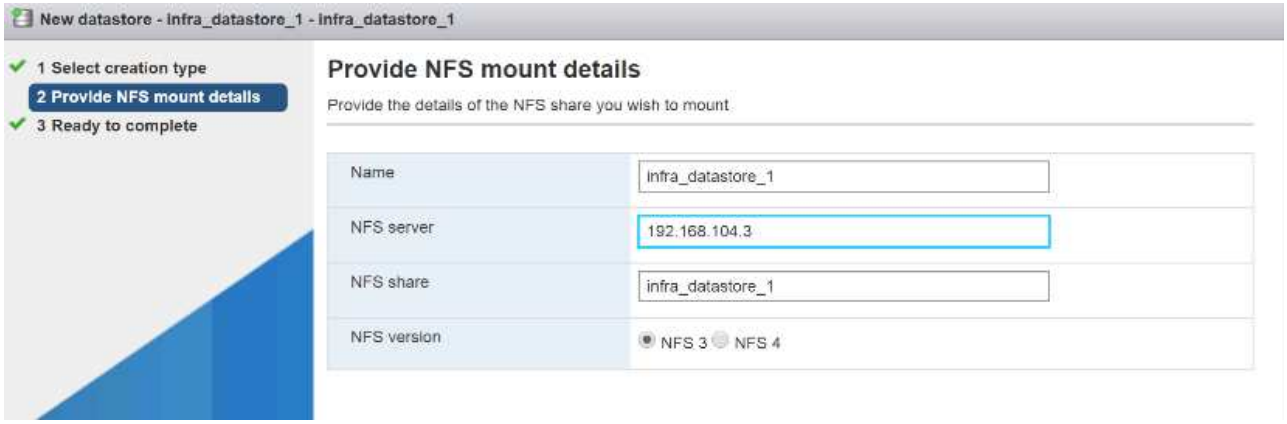
ESXi ospita VM-host-Infra-01 e VM-host-Infra-02

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).

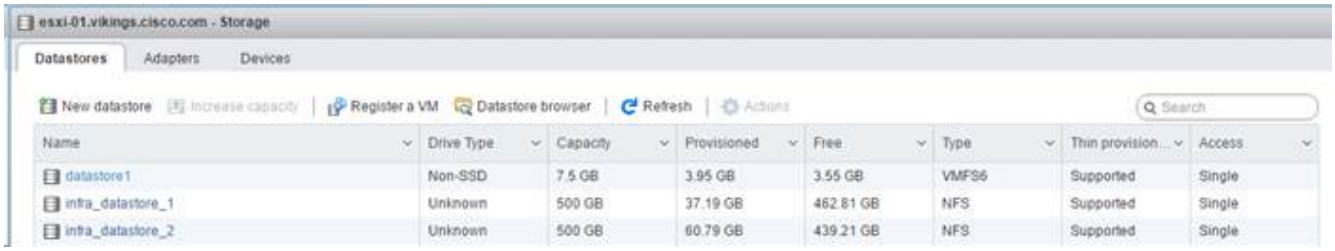


5. Nella pagina fornire dettagli sul montaggio NFS, completare la seguente procedura:
   a. Invio `infra_datastore_1` per il nome del datastore.
   b. Inserire l'indirizzo IP di `nfs_lif01_a` LIF per il server NFS.
   c. Invio `/infra_datastore_1` Per la condivisione NFS.
   d. Lasciare la versione di 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.



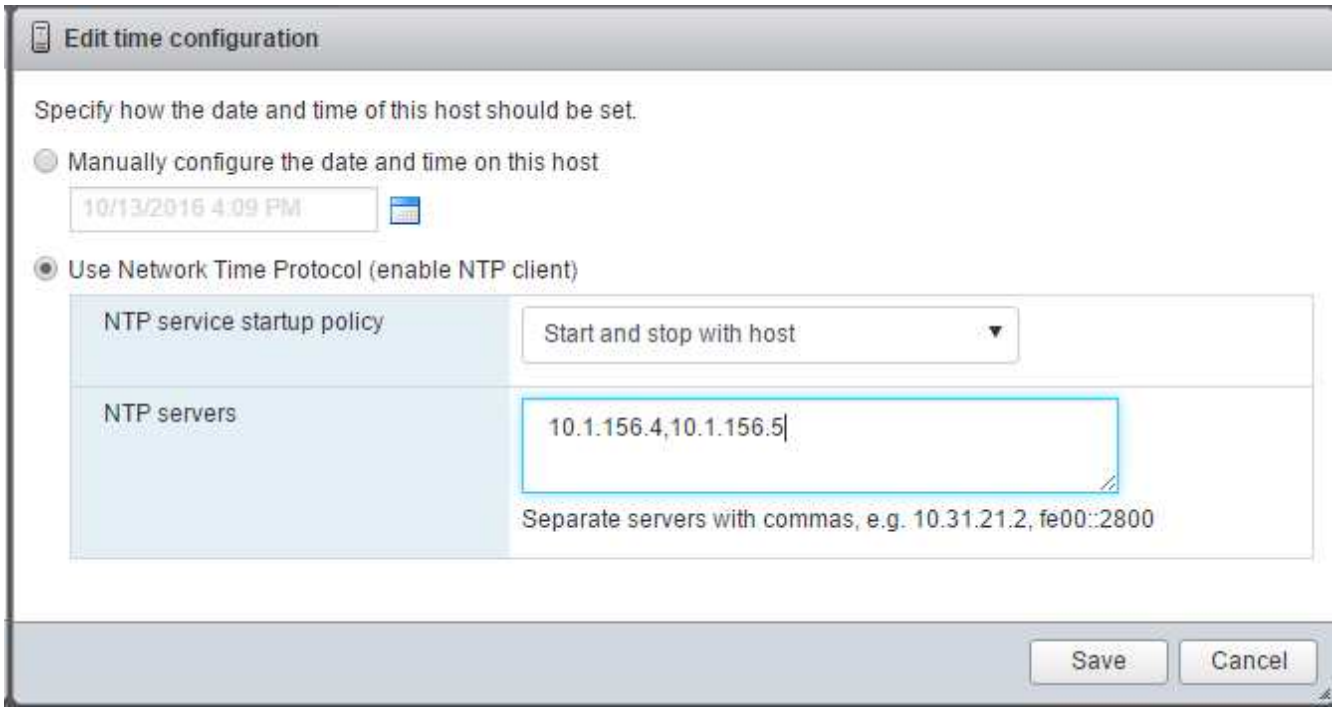
11. Montare entrambi i datastore su entrambi gli host ESXi.

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.



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

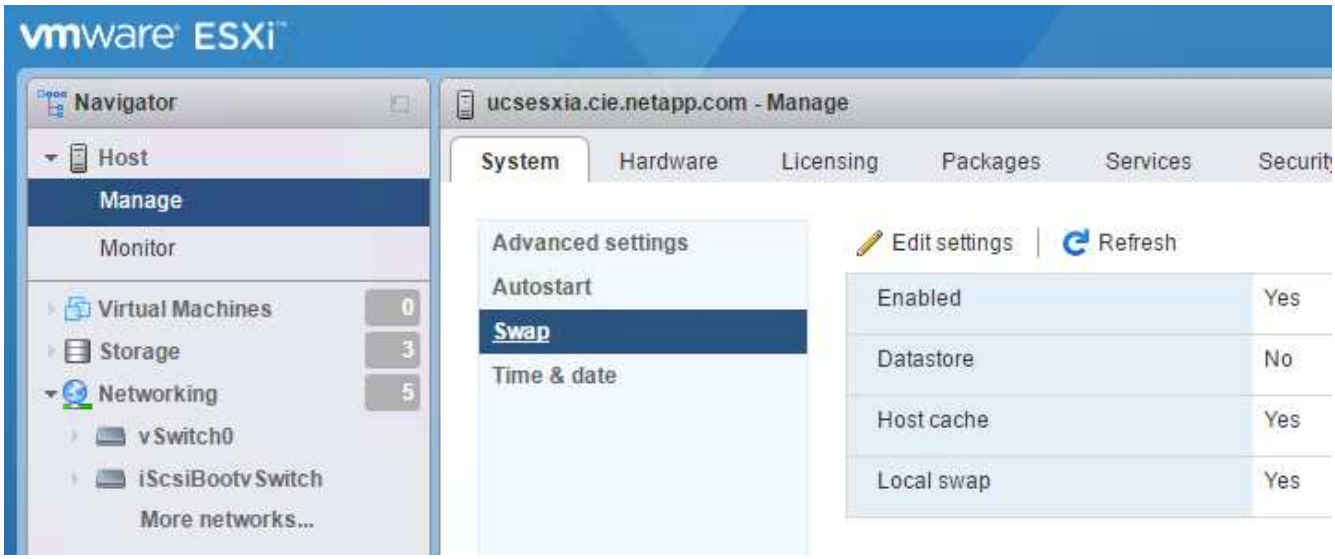
> L'ora del server NTP potrebbe variare leggermente rispetto all'ora dell'host.

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

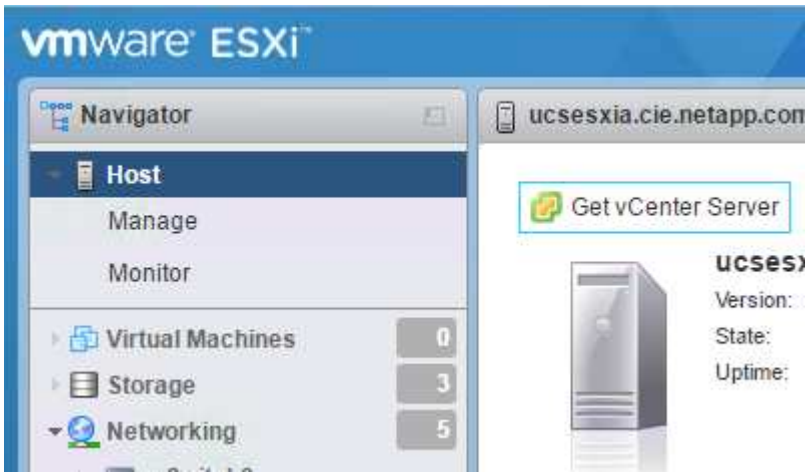
Questa sezione fornisce procedure dettagliate per l'installazione di VMware vCenter Server 6.7 in una configurazione FlexPod Express.

> FlexPod utilizza l'appliance server vCenter (VCSA).

Installare l'appliance server VMware vCenter

Per installare VCSA, attenersi alla seguente procedura:

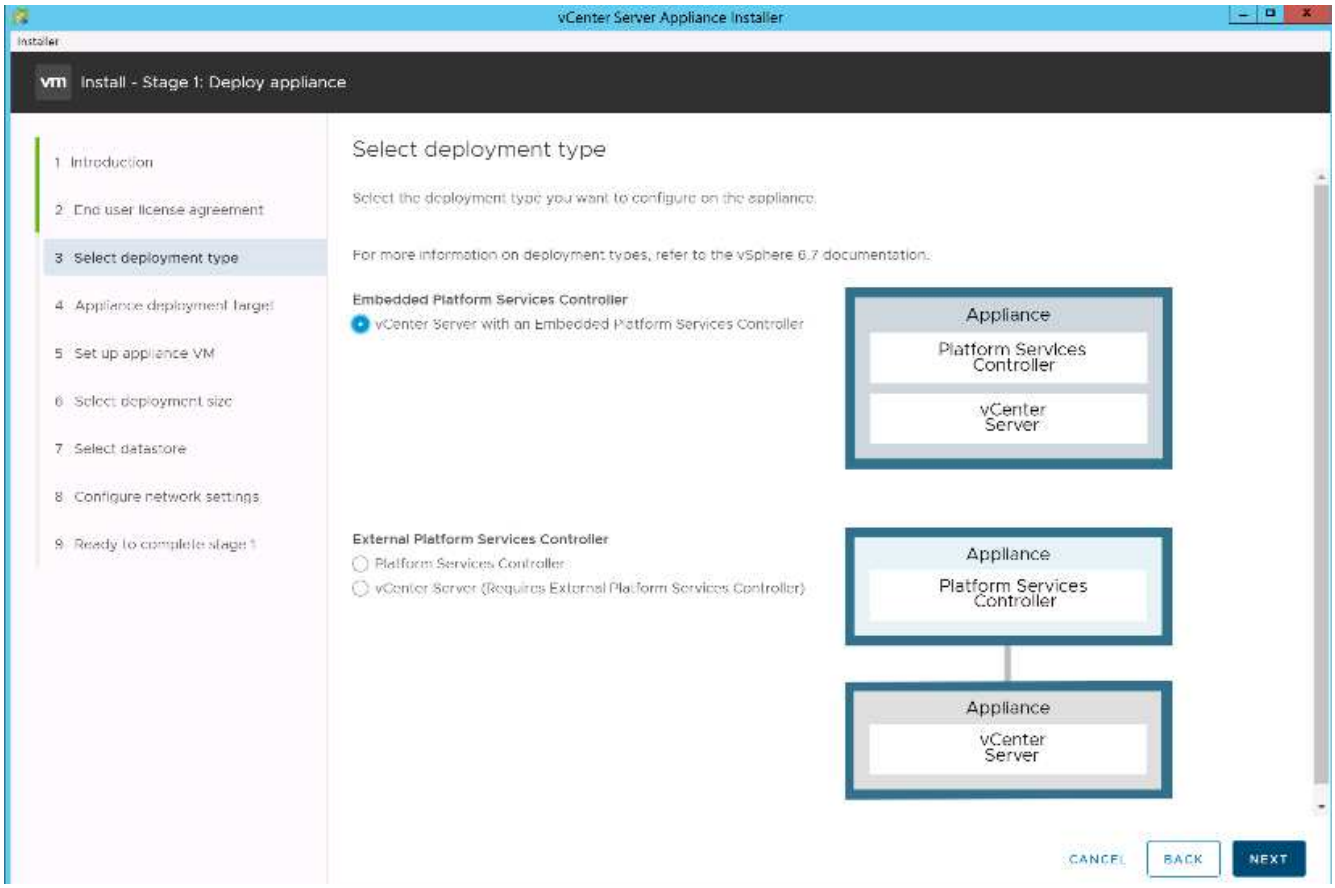
1. Scarica VCSA. Per accedere al collegamento per il download, fare clic sull'icona Get vCenter Server (Ottieni server vCenter) durante la gestione dell'host ESXi.



2. Scaricare VCSA dal sito VMware.

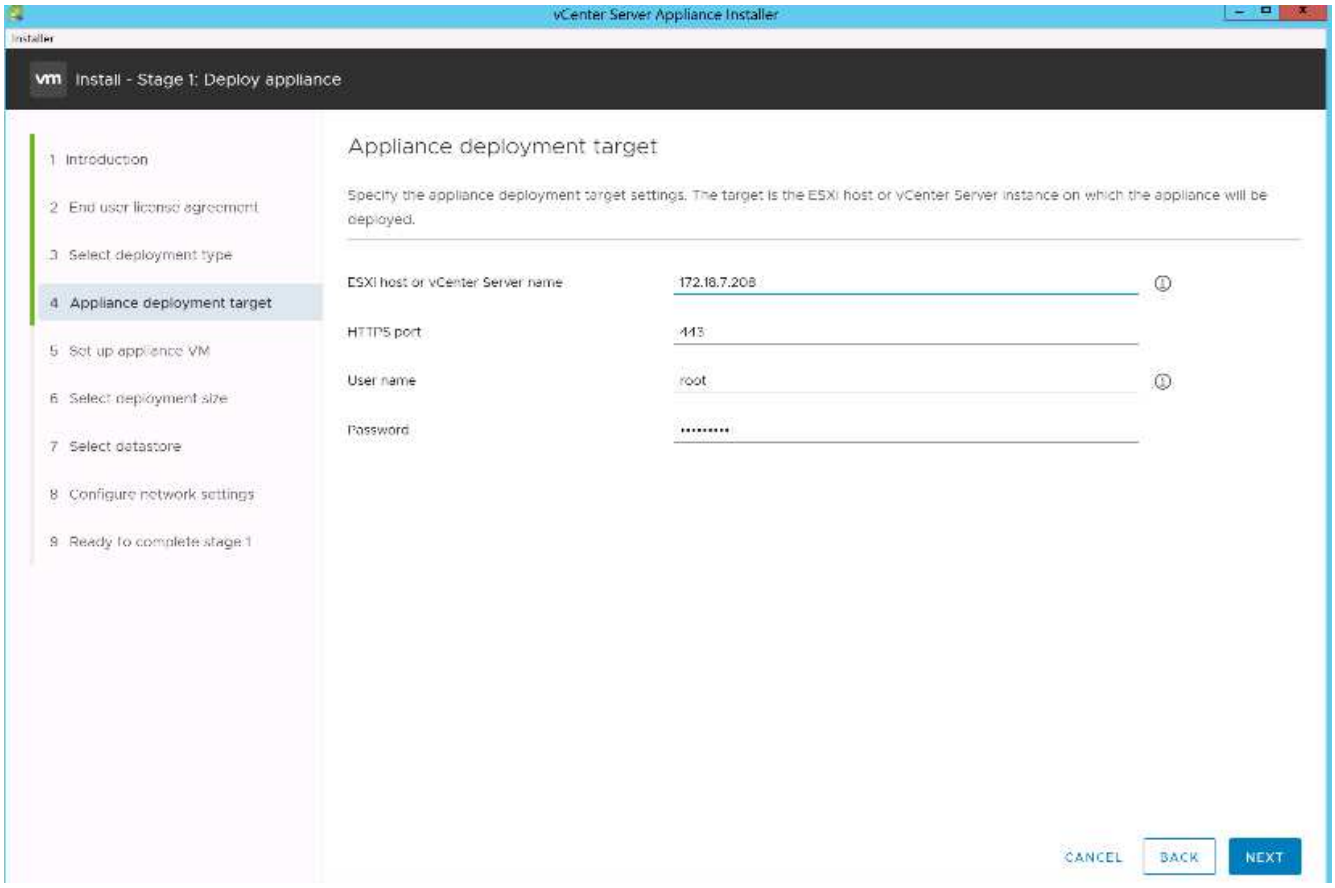
> Sebbene sia supportato l'installabile di Microsoft Windows vCenter Server, VMware consiglia VCSA per le nuove implementazioni.

3. Montare l'immagine ISO.
4. Passare a. `vcsa-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.

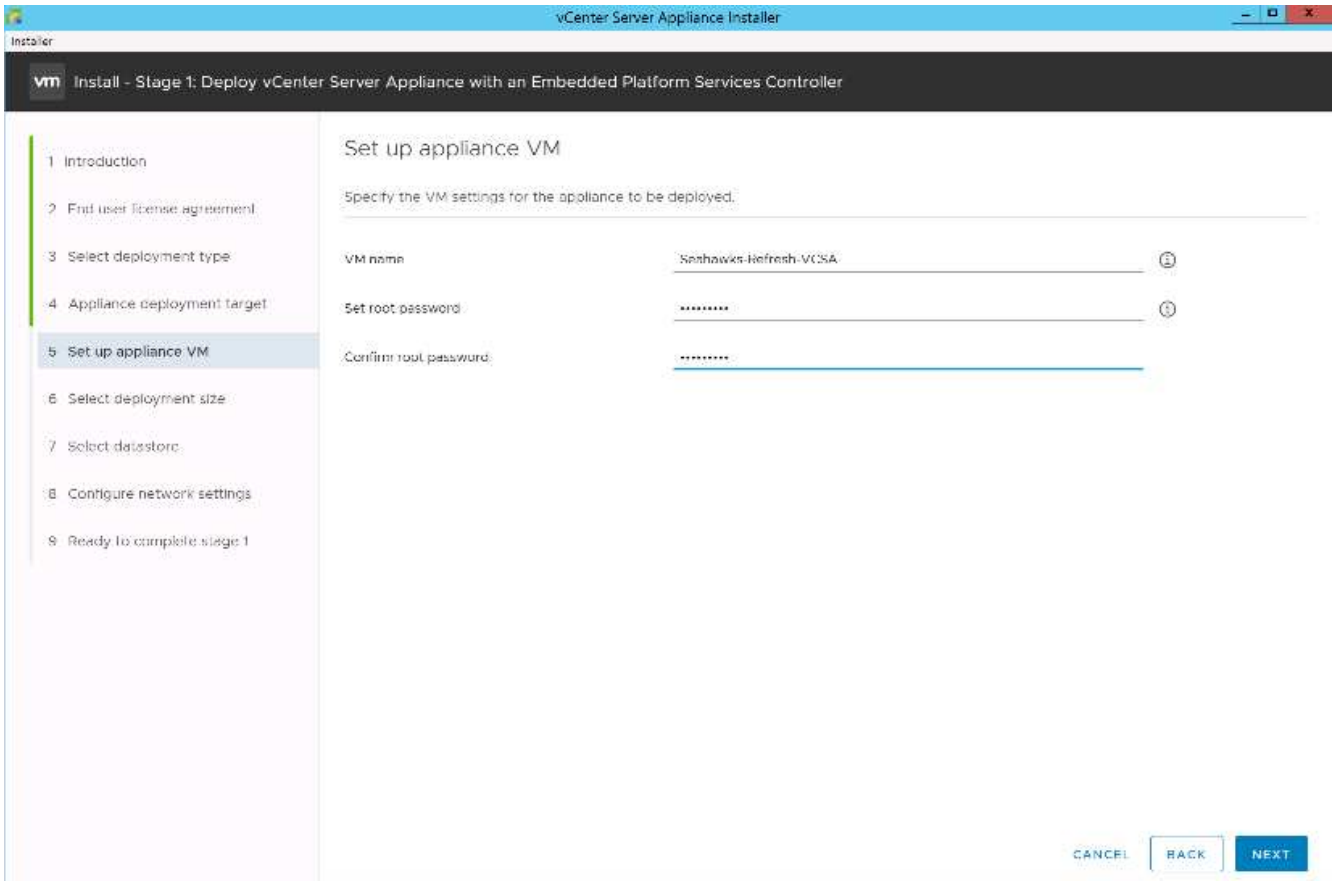


Se necessario, l'implementazione del controller dei servizi della piattaforma esterna è supportata anche come parte della soluzione FlexPod Express.

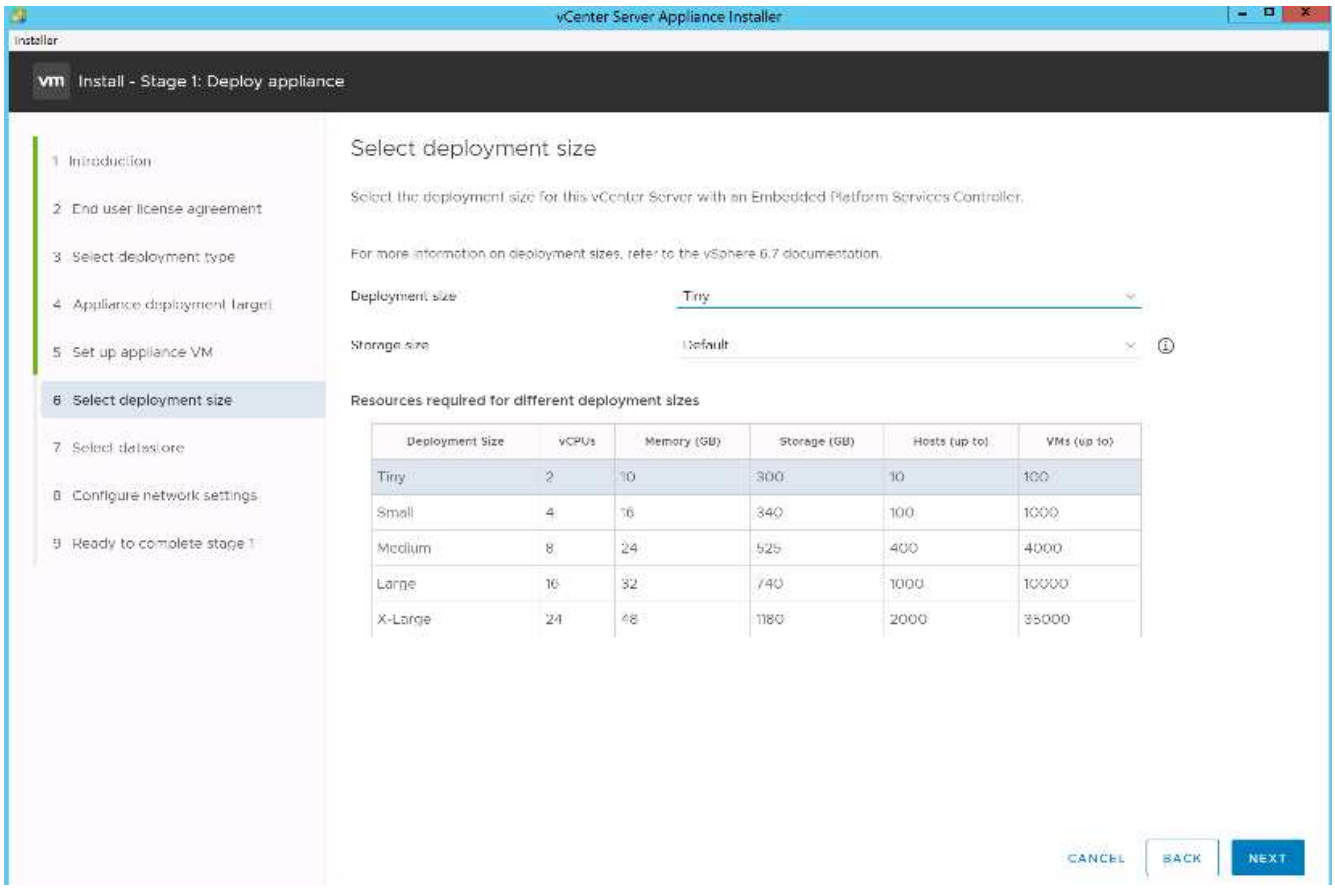
9. Nella pagina Appliance Deployment Target, immettere l'indirizzo IP di un host ESXi implementato, il nome utente root e la password root. Fare clic su Avanti.



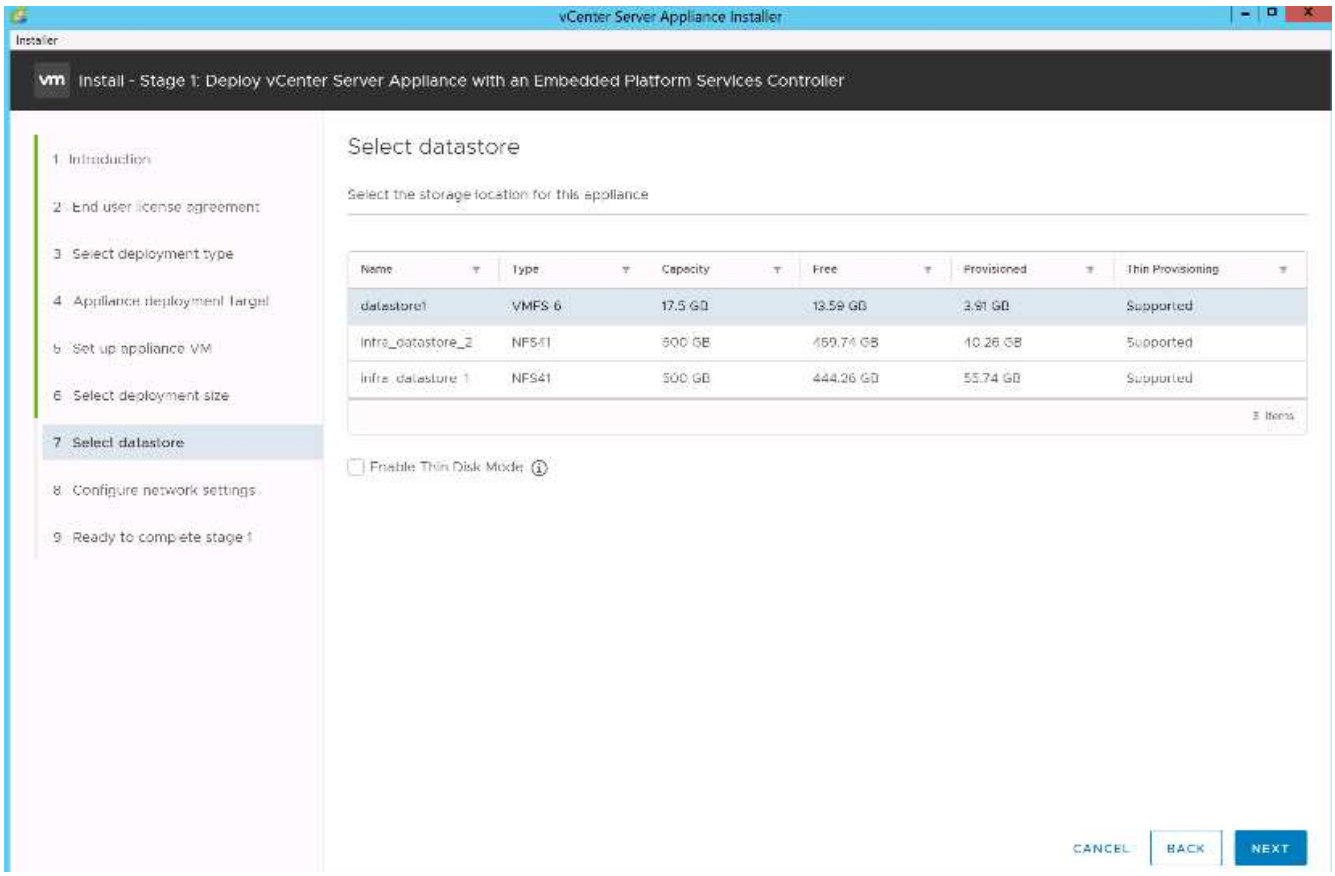
10. Impostare la macchina virtuale dell’appliance immettendo VCSA come nome della macchina virtuale e password root che si desidera utilizzare per VCSA. Fare clic su Avanti.



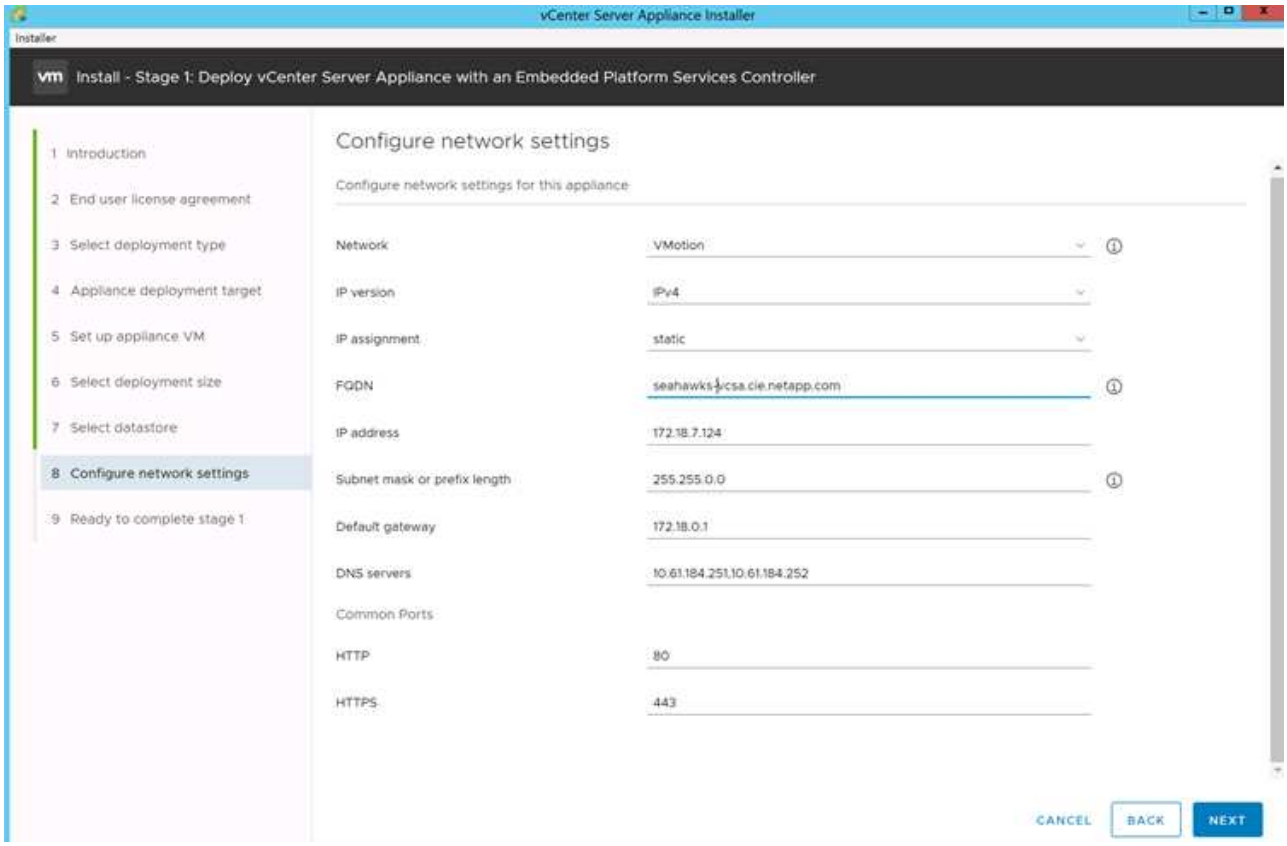
11. Selezionare la dimensione di implementazione più adatta al proprio ambiente. Fare clic su Avanti.



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



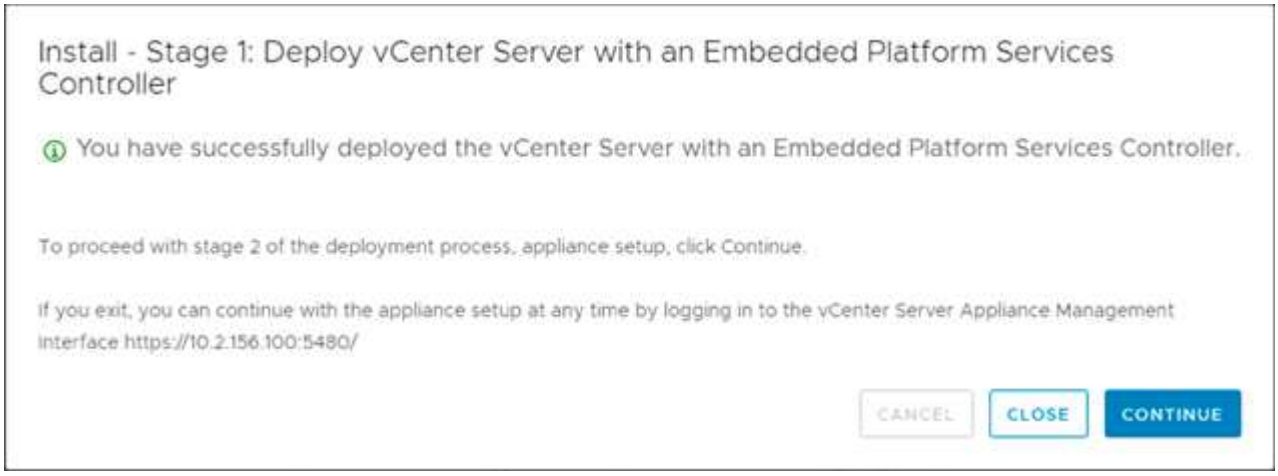
13. Inserire le seguenti informazioni nella pagina Configure Network Settings (Configura impostazioni di rete) e fare clic su Next (Avanti).
    a. Selezionare MGMT-Network come rete.
    b. Inserire l'FQDN o l'IP da utilizzare per VCSA.
    c. Inserire l'indirizzo IP da utilizzare.
    d. Inserire la subnet mask da utilizzare.
    e. Inserire il gateway predefinito.
    f. Inserire il server DNS.



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

    VCSA viene installato ora. Questo processo richiede alcuni minuti.

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



16. Nella pagina Introduzione alla fase 2, fare clic su Avanti.
17. Invio `<<var_ntp_id>>` Per l'indirizzo del server NTP. È possibile immettere più indirizzi IP NTP.

    Se si intende utilizzare 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

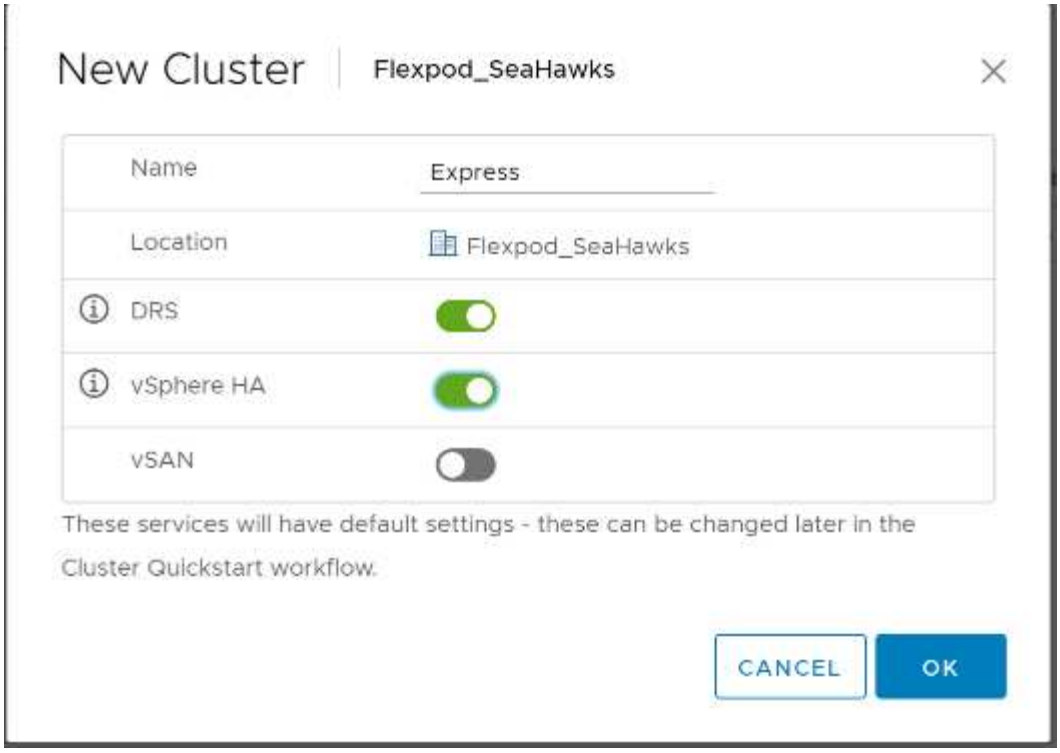
Per configurare VMware vCenter Server 6.7 e il clustering vSphere, attenersi alla seguente procedura:

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:

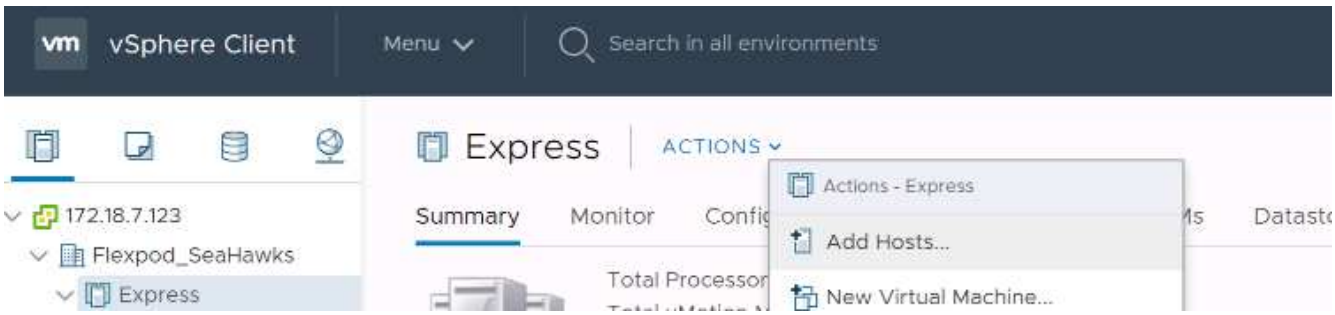
1. Fare clic con il pulsante destro del mouse sul data center appena creato e selezionare New Cluster (nuovo cluster).
2. Inserire un nome per il cluster.
3. Selezionare e attivare le opzioni DRS e vSphere ha.
4. Fare clic su OK.



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"

- Centro di documentazione per sistemi AFF e FAS

  "http://docs.netapp.com/platstor/index.jsp"

- Centro documentazione di ONTAP 9

  "http://docs.netapp.com/ontap-9/index.jsp"

- Documentazione sui prodotti NetApp

  "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"

FlexPod e sicurezza

FlexPod, la soluzione per il ransomware

TR-4802: FlexPod, la soluzione per il ransomware

Arvind Ramakrishnan, NetApp

In collaborazione con: 

Per comprendere il ransomware, è necessario prima comprendere alcuni punti chiave sulla crittografia. I metodi crittografici consentono la crittografia dei dati con una chiave segreta condivisa (crittografia a chiave simmetrica) o con una coppia di chiavi (crittografia a chiave asimmetrica). Una di queste chiavi è una chiave pubblica ampiamente disponibile e l'altra è una chiave privata non divulgata.

Ransomware è un tipo di malware basato sulla crittografia, ovvero l'utilizzo della crittografia per la creazione di software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati della vittima.

Come funziona il ransomware?

I seguenti passaggi descrivono come ransomware utilizza la crittografia per crittografare i dati della vittima senza alcun scopo per la decifratura o il ripristino da parte della vittima:

1. L'utente malintenzionato genera una coppia di chiavi come nella crittografia a chiave asimmetrica. La chiave pubblica generata viene inserita nel malware e il malware viene quindi rilasciato.
2. Una volta che il malware è entrato nel computer o nel sistema della vittima, genera una chiave simmetrica casuale utilizzando un generatore di numeri pseudocasuali (PRNG) o qualsiasi altro algoritmo di generazione di numeri casuali.
3. Il malware utilizza questa chiave simmetrica per crittografare i dati della vittima. Infine, crittografa la chiave simmetrica utilizzando la chiave pubblica dell'utente malintenzionato incorporata nel malware. L'output di questo passo è un testo cifrato asimmetrico della chiave simmetrica crittografata e il testo cifrato simmetrico dei dati della vittima.
4. Il malware azzera (cancella) i dati della vittima e la chiave simmetrica utilizzata per crittografare i dati, senza lasciare spazio per il ripristino.
5. La vittima ora mostra il testo cifrato asimmetrico della chiave simmetrica e un valore di riscatto che deve essere pagato per ottenere la chiave simmetrica utilizzata per crittografare i dati.
6. La vittima paga il riscatto e condivide il testo cifrato asimmetrico con l'autore dell'attacco. L'utente malintenzionato decrittografa il testo crittografato con la propria chiave privata, che determina la chiave simmetrica.
7. L'utente malintenzionato condivide questa chiave simmetrica con la vittima, che può essere utilizzata per decrittare tutti i dati e quindi per ripristinarli dall'attacco.

Sfide

Individui e organizzazioni devono affrontare le seguenti sfide quando vengono attaccati dal ransomware:

- La sfida più importante è che richiede un costo immediato sulla produttività dell'organizzazione o dell'individuo. Ci vuole tempo per tornare a uno stato di normalità, perché tutti i file importanti devono essere riconquistati e i sistemi devono essere protetti.
- Potrebbe portare a una violazione dei dati che contiene informazioni riservate e riservate che appartengono a clienti o clienti e che porta a una situazione di crisi che un'organizzazione vorrebbe chiaramente evitare.
- Esiste un'ottima probabilità che i dati entrino nelle mani sbagliate o vengano cancellati completamente, il che porta a un punto di non ritorno che potrebbe essere disastroso per le organizzazioni e gli individui.
- Dopo aver pagato il riscatto, non vi è alcuna garanzia che l'utente malintenzionato fornisca la chiave per ripristinare i dati.
- Non vi è alcuna garanzia che l'utente malintenzionato si asterrà dalla trasmissione dei dati sensibili nonostante il pagamento del riscatto.
- Nelle grandi imprese, identificare la lacuna che ha portato a un attacco ransomware è un compito noioso e la protezione di tutti i sistemi richiede un notevole impegno.

Chi è a rischio?

Chiunque può essere attaccato da ransomware, inclusi individui e grandi organizzazioni. Le organizzazioni che non implementano procedure e misure di sicurezza ben definite sono ancora più vulnerabili a tali attacchi. L'effetto dell'attacco su un'organizzazione di grandi dimensioni può essere più grande di quanto un individuo potrebbe sopportare.

Ransomware rappresenta circa il 28% di tutti gli attacchi di malware. In altre parole, più di un malware su quattro è un attacco ransomware. Il ransomware può diffondersi automaticamente e indiscriminatamente attraverso Internet e, in caso di mancanza di sicurezza, può entrare nei sistemi della vittima e continuare a diffondersi ad altri sistemi connessi. Gli autori degli attacchi tendono a rivolgersi a persone o organizzazioni che eseguono una grande quantità di file sharing, dispongono di molti dati sensibili e critici o mantengono una protezione inadeguata contro gli attacchi.

Gli autori degli attacchi tendono a concentrarsi sui seguenti potenziali obiettivi:

- Università e comunità studentesche
- Uffici governativi e agenzie
- Ospedali
- Banche

Questo non è un elenco completo di obiettivi. Non puoi considerarti al sicuro dagli attacchi se ti trovi al di fuori di una di queste categorie.

In che modo il ransomware entra in un sistema o si diffonde?

Esistono diversi modi in cui il ransomware può entrare in un sistema o diffondersi in altri sistemi. Nel mondo odierno, quasi tutti i sistemi sono connessi tra loro tramite Internet, LAN, WAN e così via. La quantità di dati che vengono generati e scambiati tra questi sistemi è solo in aumento.

Alcuni dei modi più comuni con cui il ransomware può diffondersi includono metodi che utilizziamo quotidianamente per condividere o accedere ai dati:

- E-mail
- Reti P2P
- Download di file
- Social network
- Dispositivi mobili
- Connessione a reti pubbliche non sicure
- Accesso agli URL Web

Conseguenze della perdita di dati

Le conseguenze o gli effetti della perdita di dati possono arrivare più ampiamente di quanto le organizzazioni potrebbero prevedere. Gli effetti possono variare a seconda della durata del downtime o del periodo di tempo durante il quale un'organizzazione non ha accesso ai propri dati. Quanto più dura l'attacco, tanto maggiore sarà l'effetto sui ricavi, sul marchio e sulla reputazione dell'organizzazione. Un'organizzazione può anche affrontare problemi legali e un drastico calo della produttività.

Poiché questi problemi continuano a persistere nel tempo, iniziano ad ingrandirsi e potrebbero finire per cambiare la cultura di un'organizzazione, a seconda di come risponde all'attacco. Nel mondo di oggi, le informazioni si diffondono rapidamente e le notizie negative su un'organizzazione potrebbero causare danni permanenti alla sua reputazione. Un'organizzazione potrebbe affrontare enormi sanzioni per la perdita di dati, che potrebbe portare alla chiusura di un'azienda.

Effetti finanziari

Secondo un recente "Report McAfee", I costi globali sostenuti a causa della criminalità informatica sono pari a circa 600 miliardi di dollari, pari a circa il 0.8% del PIL globale. Quando questo importo viene confrontato con la crescente economia mondiale di Internet di 4.2 trilioni di dollari, equivale a una tassa del 14% sulla crescita.

Ransomware prende una quota significativa di questo costo finanziario. Nel 2018, i costi sostenuti per gli attacchi ransomware sono stati di circa 8 miliardi di dollari—, un importo previsto per raggiungere i 11.5 miliardi di dollari nel 2019.

Qual è la soluzione?

Il ripristino da un attacco ransomware con downtime minimo è possibile solo implementando un piano di disaster recovery proattivo. Avere la capacità di recuperare da un attacco è un bene, ma prevenire un attacco è l'ideale.

Sebbene vi siano diversi fronti che è necessario rivedere e correggere per prevenire un attacco, il componente principale che consente di prevenire o ripristinare da un attacco è il data center.

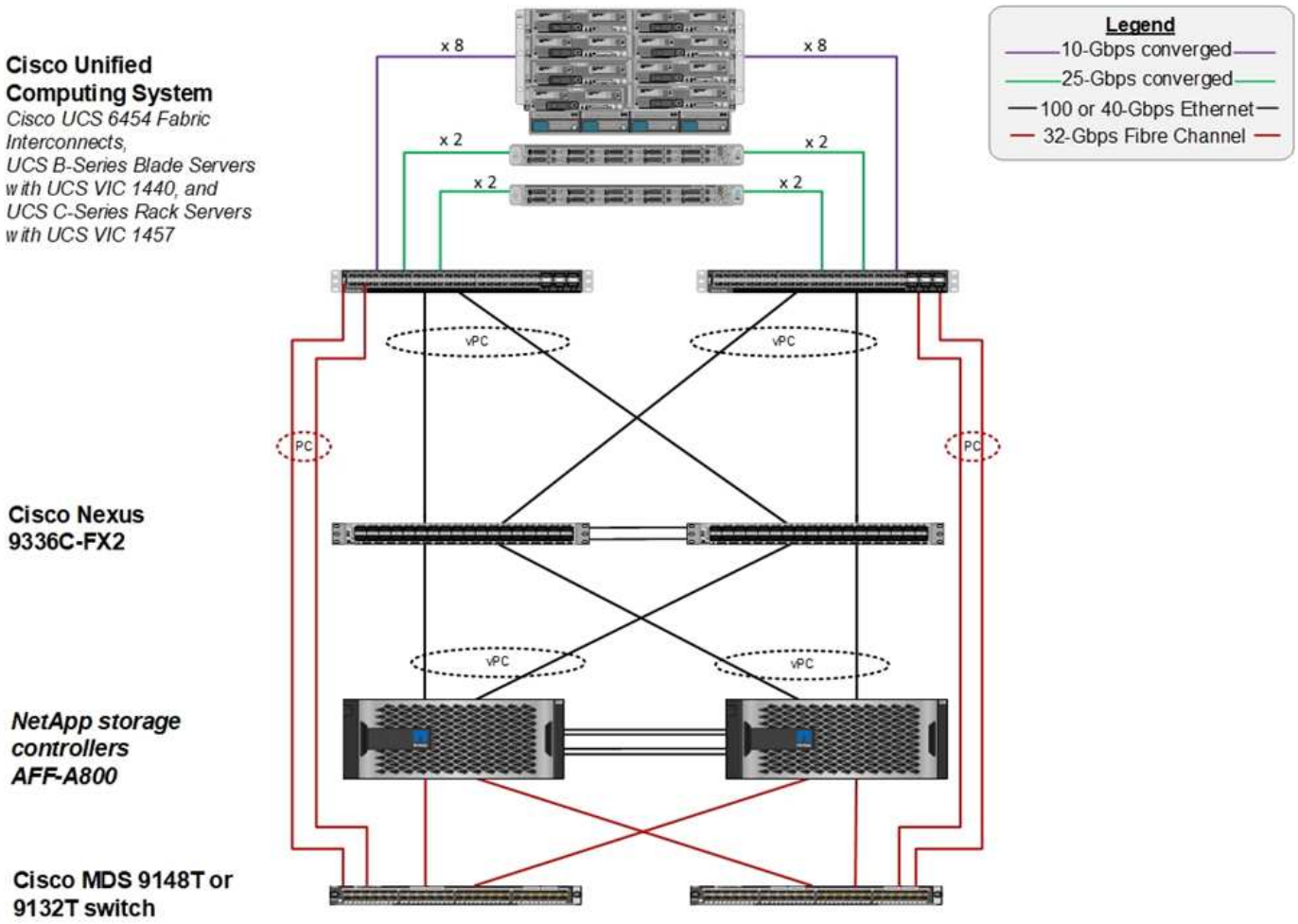
Il design del data center e le funzionalità che offre per proteggere gli end-point di rete, calcolo e storage svolgono un ruolo fondamentale nella creazione di un ambiente sicuro per le operazioni quotidiane. Questo documento mostra in che modo le funzionalità di un'infrastruttura di cloud ibrido FlexPod possono contribuire al rapido ripristino dei dati in caso di attacco e possono anche contribuire a prevenire del tutto gli attacchi.

Panoramica di FlexPod

FlexPod è un'architettura pre-progettata, integrata e validata che combina i server Cisco Unified Computing System (Cisco UCS), la famiglia di switch Cisco Nexus, gli switch Cisco MDS Fabric e gli storage array NetApp in un'unica architettura flessibile. Le

soluzioni FlexPod sono progettate per l'alta disponibilità senza singoli punti di errore, mantenendo al contempo convenienza e flessibilità di progettazione per supportare un'ampia varietà di carichi di lavoro. Un design FlexPod può supportare diversi hypervisor e server bare metal e può anche essere dimensionato e ottimizzato in base ai requisiti dei carichi di lavoro del cliente.

La figura seguente illustra l'architettura FlexPod e evidenzia chiaramente l'alta disponibilità in tutti i livelli dello stack. I componenti dell'infrastruttura di storage, rete e calcolo sono configurati in modo che le operazioni possano eseguire il failover istantaneo al partner sopravvissuto in caso di guasto di uno dei componenti.



Un vantaggio importante per un sistema FlexPod è la sua pre-progettazione, integrazione e validazione per diversi carichi di lavoro. Vengono pubblicate guide dettagliate di progettazione e implementazione per ogni convalida della soluzione. Questi documenti includono le Best practice da adottare per consentire ai carichi di lavoro di essere eseguiti senza problemi su FlexPod. Queste soluzioni sono costruite con i migliori prodotti di calcolo, rete e storage e una serie di funzionalità che si concentrano sulla sicurezza e la protezione avanzata dell'intera infrastruttura.

"L'X-Force Threat Intelligence Index di IBM" afferma: "Errore umano responsabile di due terzi dei record compromessi, compreso un salto storico del 424% nell'infrastruttura cloud non configurata correttamente".

Con un sistema FlexPod, è possibile evitare di configurare in modo errato l'infrastruttura utilizzando l'automazione attraverso i playbook Ansible che eseguono una configurazione end-to-end dell'infrastruttura in base alle Best practice descritte in Cisco Validated Designs (CVD) e NetApp Verified Architectures (NVA).

Misure di protezione ransomware

In questa sezione vengono descritte le funzionalità principali del software di gestione dei dati NetApp ONTAP e gli strumenti per Cisco UCS e Cisco Nexus che è possibile utilizzare per proteggere e ripristinare in modo efficace dagli attacchi ransomware.

Storage: NetApp ONTAP

Il software ONTAP offre molte funzionalità utili per la protezione dei dati, la maggior parte delle quali è gratuita per i clienti che dispongono di un sistema ONTAP. È possibile utilizzare le seguenti funzionalità in qualsiasi momento per proteggere i dati dagli attacchi:

- **Tecnologia NetApp Snapshot.** Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato di un file system in un momento specifico. Queste copie aiutano a proteggere i dati senza alcun effetto sulle prestazioni del sistema e, allo stesso tempo, non occupano molto spazio di storage. NetApp consiglia di creare una pianificazione per la creazione di copie Snapshot. È inoltre necessario mantenere un lungo periodo di conservazione, in quanto alcuni malware possono andare in stato di inattività e quindi riattivarsi settimane o mesi dopo un'infezione. In caso di attacco, è possibile eseguire il rollback del volume utilizzando una copia Snapshot acquisita prima dell'infezione.
- **La tecnologia NetApp SnapRestore.** il software di ripristino dei dati SnapRestore è estremamente utile per eseguire il ripristino dalla corruzione dei dati o per ripristinare solo il contenuto del file. SnapRestore non ripristina gli attributi di un volume, ma è molto più veloce di quanto un amministratore possa ottenere copiando i file dalla copia Snapshot al file system attivo. La velocità con cui è possibile recuperare i dati è utile quando molti file devono essere ripristinati il più rapidamente possibile. In caso di attacco, questo processo di recovery altamente efficiente consente di ripristinare rapidamente il business online.
- **Tecnologia NetApp SnapCenter.** il software SnapCenter utilizza le funzioni di backup e replica basate su storage NetApp per fornire una protezione dei dati coerente con l'applicazione. Questo software si integra con le applicazioni aziendali e fornisce flussi di lavoro specifici per applicazioni e database per soddisfare le esigenze degli amministratori di applicazioni, database e infrastrutture virtuali. SnapCenter offre una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system. La sua capacità di fornire una protezione dei dati coerente con l'applicazione è fondamentale durante il ripristino dei dati, perché semplifica il ripristino delle applicazioni a uno stato coerente più rapidamente.
- **Tecnologia NetApp SnapLock.** SnapLock offre un volume speciale in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non riscrivibile. I dati di produzione dell'utente che risiedono in un volume FlexVol possono essere mirrorati o archiviati in un volume SnapLock, rispettivamente tramite NetApp SnapMirror o la tecnologia SnapVault. I file nel volume SnapLock, nel volume stesso e nel relativo aggregato di hosting non possono essere cancellati fino alla fine del periodo di conservazione.
- **Tecnologia NetApp FPolicy.** Usa il software FPolicy per prevenire gli attacchi impedendo operazioni su file con estensioni specifiche. È possibile attivare un evento FPolicy per operazioni di file specifiche. L'evento è legato a una policy, che richiama il motore che deve utilizzare. È possibile configurare un criterio con una serie di estensioni di file che potrebbero contenere ransomware. Quando un file con un'estensione non consentita tenta di eseguire un'operazione non autorizzata, FPolicy impedisce l'esecuzione di tale operazione.

Rete: Cisco Nexus

Il software Cisco NX OS supporta la funzione NetFlow che consente un rilevamento avanzato delle anomalie e della sicurezza della rete. NetFlow acquisisce i metadati di ogni conversazione sulla rete, le parti coinvolte nella comunicazione, il protocollo utilizzato e la durata della transazione. Una volta aggregate e analizzate le informazioni, possono fornire informazioni dettagliate sul comportamento normale.

I dati raccolti consentono inoltre l'identificazione di modelli di attività dubbi, come la diffusione di malware nella rete, che altrimenti potrebbero passare inosservati.

NetFlow utilizza i flussi per fornire statistiche per il monitoraggio della rete. Un flusso è un flusso unidirezionale di pacchetti che arriva su un'interfaccia di origine (o VLAN) e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. Si crea un flusso utilizzando un record di flusso per definire le chiavi univoche per il flusso. È possibile esportare i dati raccolti da NetFlow per i flussi utilizzando un'esportazione di flusso in un NetFlow Collector remoto, ad esempio Cisco Stealthwatch. Stealthwatch utilizza queste informazioni per il monitoraggio continuo della rete e fornisce analisi forensi in tempo reale per il rilevamento delle minacce e la risposta agli incidenti in caso di scoppio di ransomware.

Calcolo: Cisco UCS

Cisco UCS è l'endpoint di calcolo in un'architettura FlexPod. È possibile utilizzare diversi prodotti Cisco per proteggere questo livello dello stack a livello di sistema operativo.

È possibile implementare i seguenti prodotti chiave a livello di elaborazione o applicazione:

- **Cisco Advanced malware Protection (AMP) per endpoint.** supportata sui sistemi operativi Microsoft Windows e Linux, questa soluzione integra funzionalità di prevenzione, rilevamento e risposta. Questo software di sicurezza previene le violazioni, blocca il malware nel punto di ingresso e monitora e analizza continuamente le attività di file e processi per rilevare, contenere e rimediare rapidamente alle minacce che possono eludere le difese front-line.

  Il componente di protezione delle attività dannose (MAP) di AMP monitora continuamente tutte le attività degli endpoint e fornisce il rilevamento in fase di esecuzione e il blocco del comportamento anomalo di un programma in esecuzione sull'endpoint. Ad esempio, quando il comportamento degli endpoint indica ransomware, i processi in errore vengono terminati, impedendo la crittografia degli endpoint e arrestando l'attacco.

- **Cisco Advanced malware Protection for Email Security.** le email sono diventate il mezzo principale per diffondere malware e per eseguire cyber-attacchi. In media, circa 100 miliardi di e-mail vengono scambiate in un solo giorno, il che fornisce agli autori degli attacchi un eccellente vettore di penetrazione nei sistemi degli utenti. Pertanto, è assolutamente essenziale difendersi da questa linea di attacco.

  AMP analizza le e-mail per individuare minacce come exploit zero-day e malware furtivo nascosto in allegati dannosi. Utilizza inoltre l'intelligence URL leader del settore per combattere i collegamenti dannosi. Offre agli utenti una protezione avanzata contro il phishing, il ransomware e altri attacchi sofisticati.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco firepower NGIPS può essere implementato come appliance fisica nel data center o come appliance virtuale su VMware (NGIPSv per VMware). Questo sistema di prevenzione delle intrusioni altamente efficace offre performance affidabili e un basso costo totale di proprietà. La protezione dalle minacce può essere estesa con licenze di abbonamento opzionali per fornire AMP, visibilità e controllo delle applicazioni e funzionalità di filtraggio degli URL. I NGIPS virtualizzati ispezionano il traffico tra macchine virtuali (VM) e semplificano l'implementazione e la gestione delle soluzioni NGIPS in siti con risorse limitate, aumentando la protezione per risorse fisiche e virtuali.

Proteggere e ripristinare i dati su FlexPod

Questa sezione descrive come è possibile ripristinare i dati di un utente finale in caso di attacco e come è possibile prevenire gli attacchi utilizzando un sistema FlexPod.

Panoramica testbed

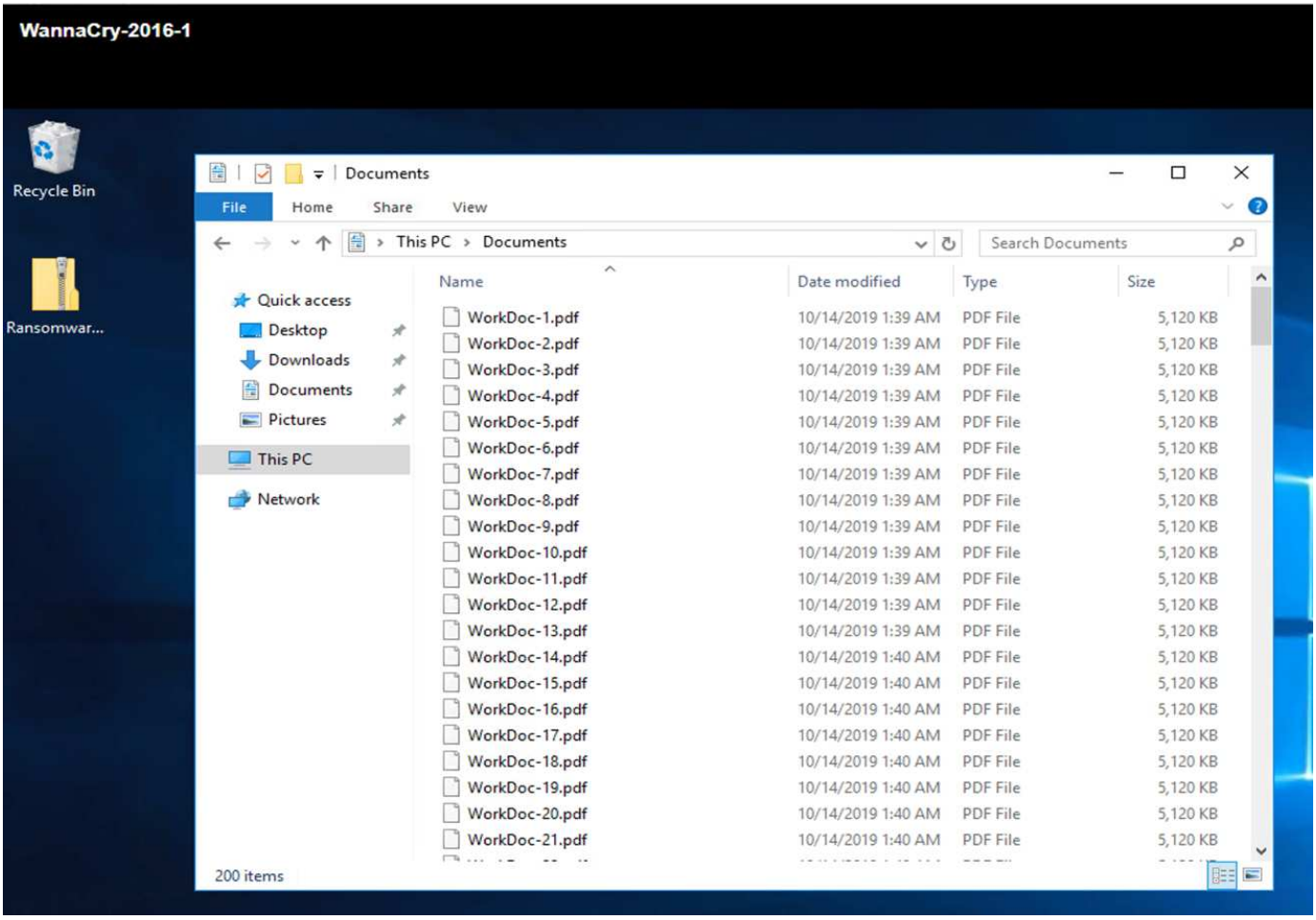
Per mostrare il rilevamento, la correzione e la prevenzione di FlexPod, è stato creato un testbed basato sulle linee guida specificate nell'ultima piattaforma CVD disponibile al momento della stesura del presente documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS 4a generazione e NetApp AFF A-Series CVD".

Una macchina virtuale Windows 2016, che forniva una condivisione CIFS dal software NetApp ONTAP, è stata implementata nell'infrastruttura VMware vSphere. Quindi, NetApp FPolicy è stato configurato sulla condivisione CIFS per impedire l'esecuzione di file con determinati tipi di estensione. Il software NetApp SnapCenter è stato implementato anche per gestire le copie Snapshot delle macchine virtuali nell'infrastruttura per fornire copie Snapshot coerenti con l'applicazione.

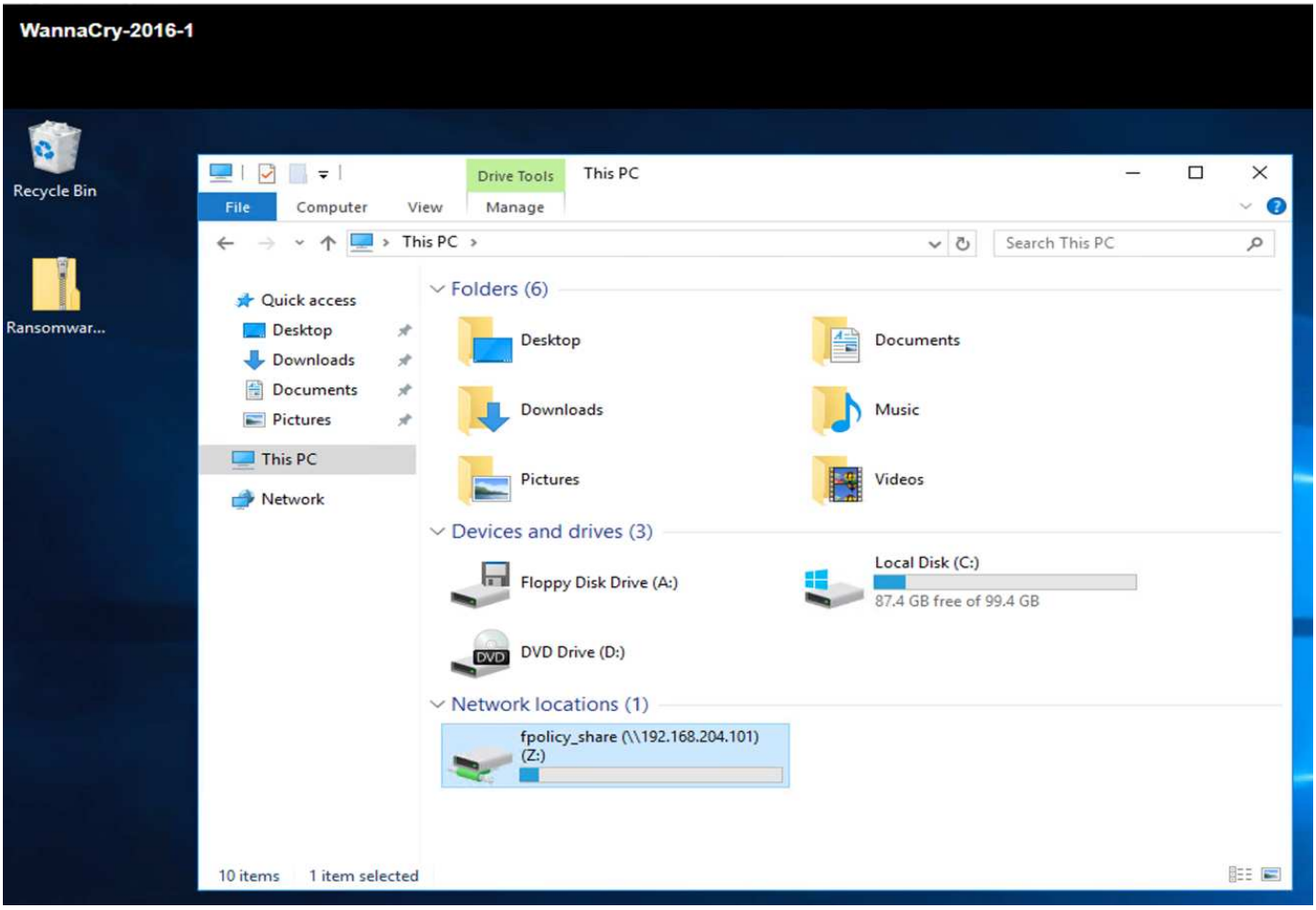
Stato della macchina virtuale e dei relativi file prima di un attacco

Questa sezione mostra lo stato dei file prima di un attacco alla macchina virtuale e la condivisione CIFS ad essa mappata.

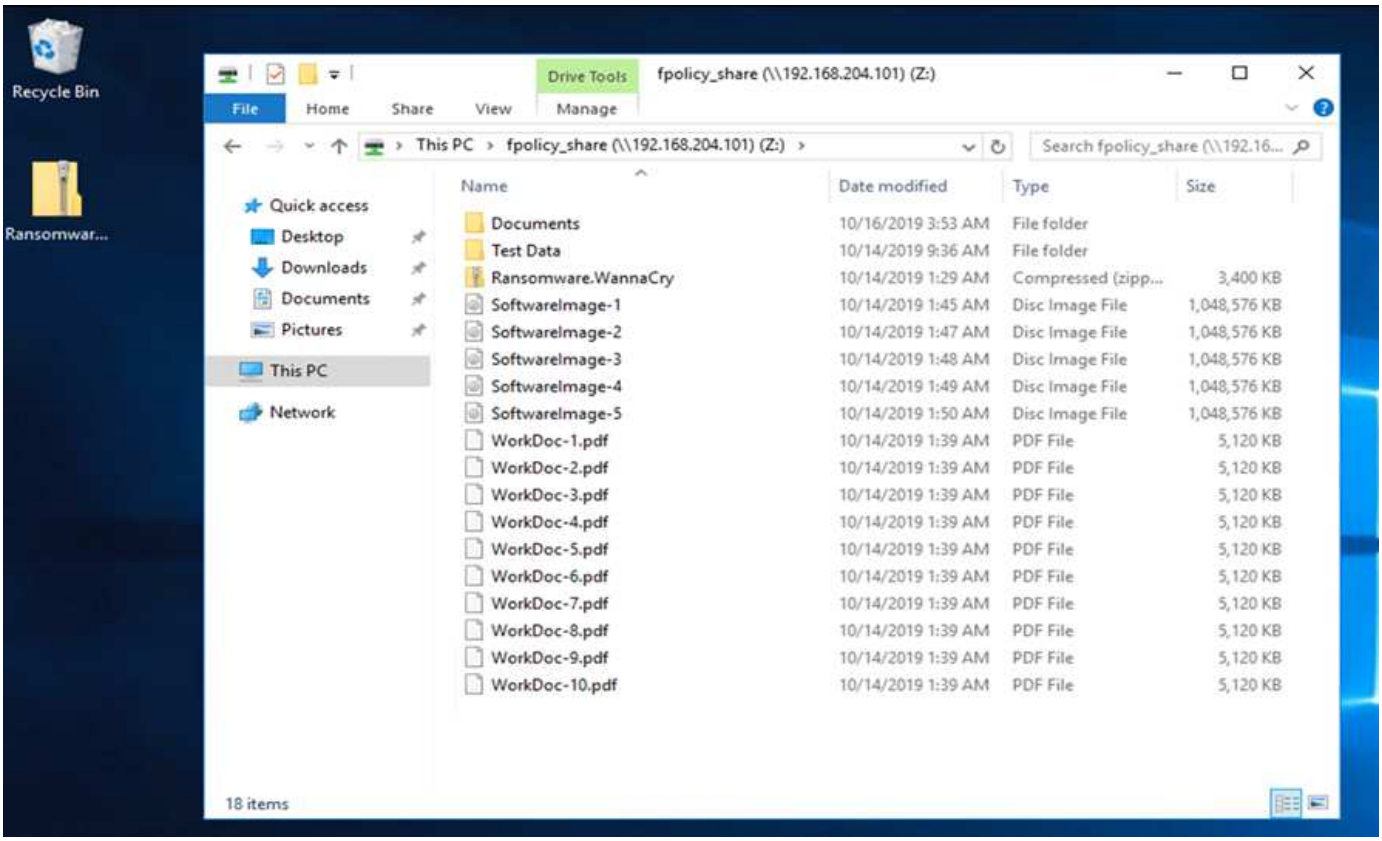
La cartella documenti della macchina virtuale aveva un set di file PDF che non sono stati ancora crittografati dal malware WannaCry.



La seguente schermata mostra la condivisione CIFS mappata alla macchina virtuale.



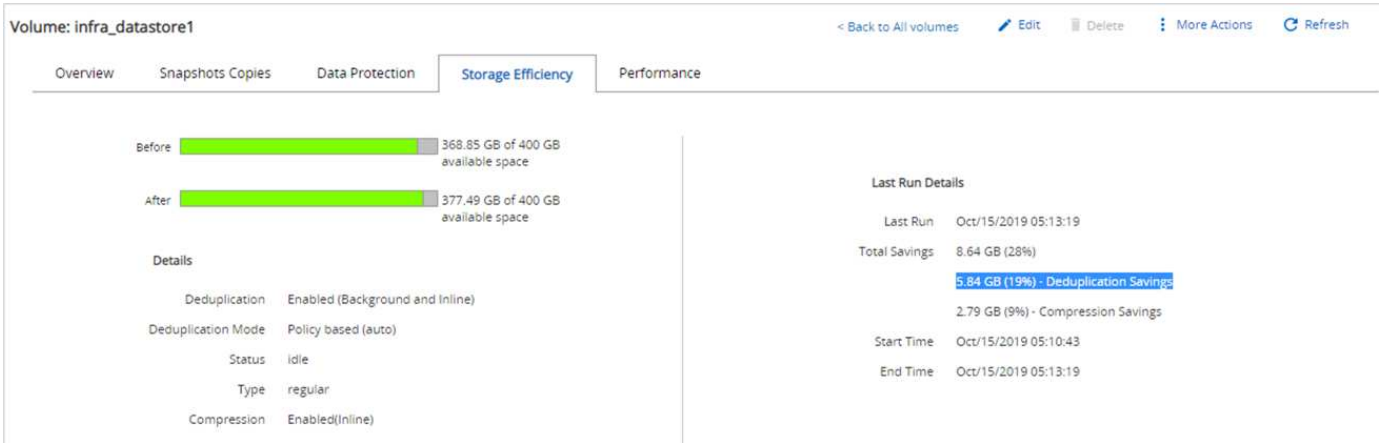
La seguente schermata mostra i file sulla condivisione CIFS `fpolicy_share` Che non sono ancora stati crittografati dal malware WannaCry.



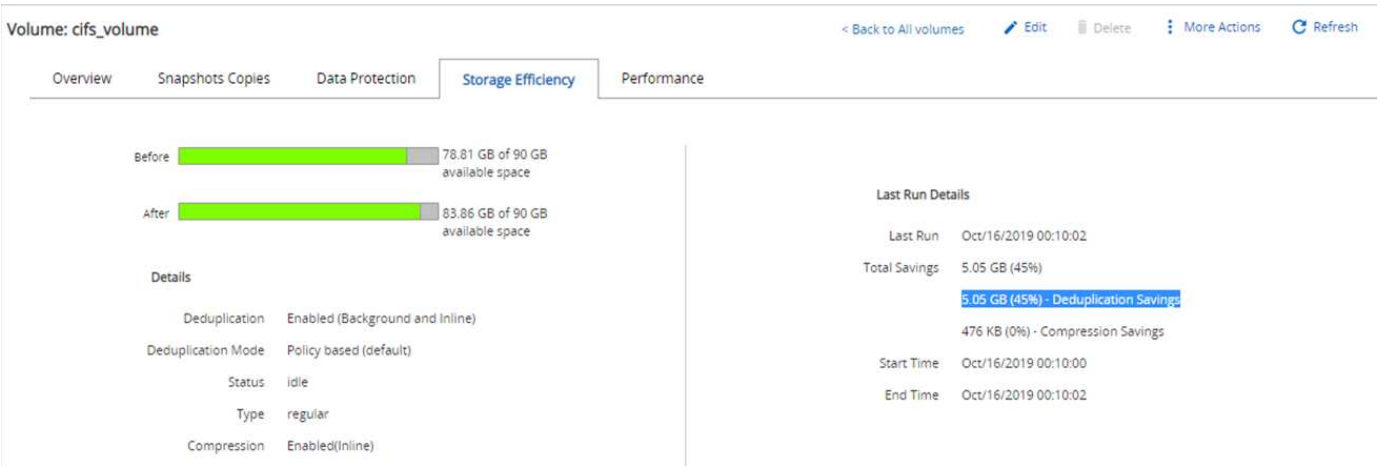
Deduplica e informazioni Snapshot prima di un attacco

I dettagli sull'efficienza dello storage e le dimensioni della copia Snapshot prima di un attacco vengono indicati e utilizzati come riferimento durante la fase di rilevamento.

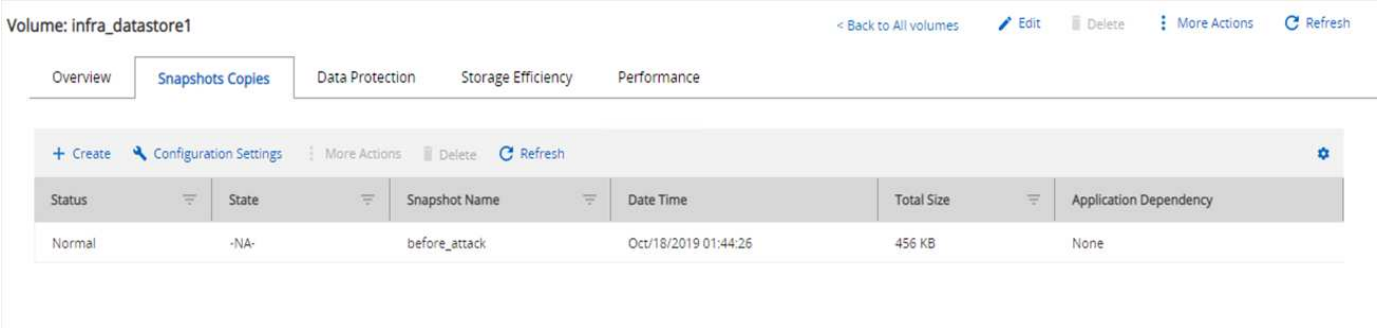
Grazie alla deduplica sul volume che ospita la macchina virtuale, sono stati ottenuti risparmi dello storage del 19%.



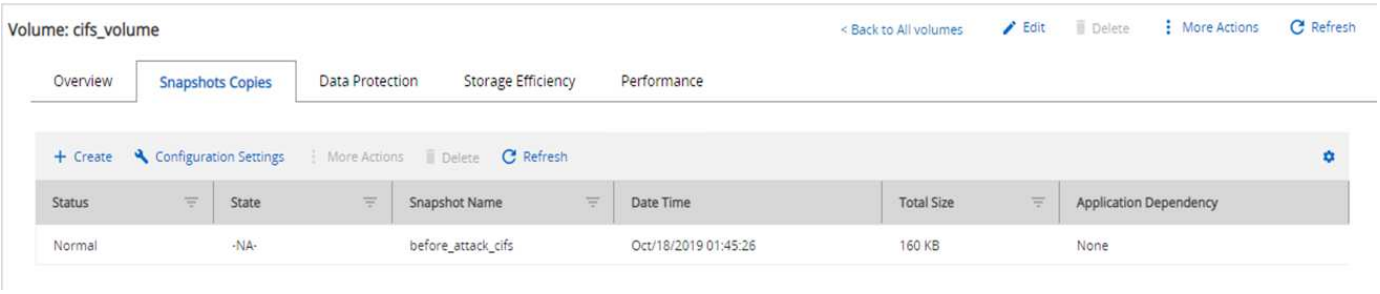
Con la deduplica sulla condivisione CIFS sono stati ottenuti risparmi dello storage del 45% `fpolicy_share`.



È stata rilevata una dimensione della copia Snapshot di 456 KB per il volume che ospita la macchina virtuale.



Per la condivisione CIFS è stata osservata una dimensione della copia Snapshot di 160 KB `fpolicy_share`.



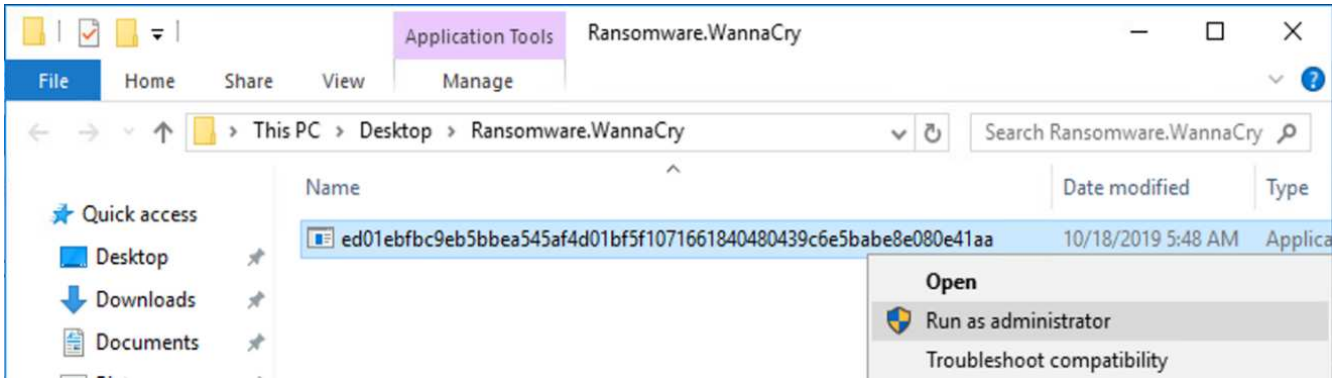
Infezione WannaCry su VM e condivisione CIFS

In questa sezione viene illustrato come il malware WannaCry è stato introdotto nell'ambiente FlexPod e le successive modifiche apportate al sistema.

I seguenti passaggi dimostrano come il malware binario WannaCry è stato introdotto nella macchina virtuale:

1. Il malware protetto è stato estratto.

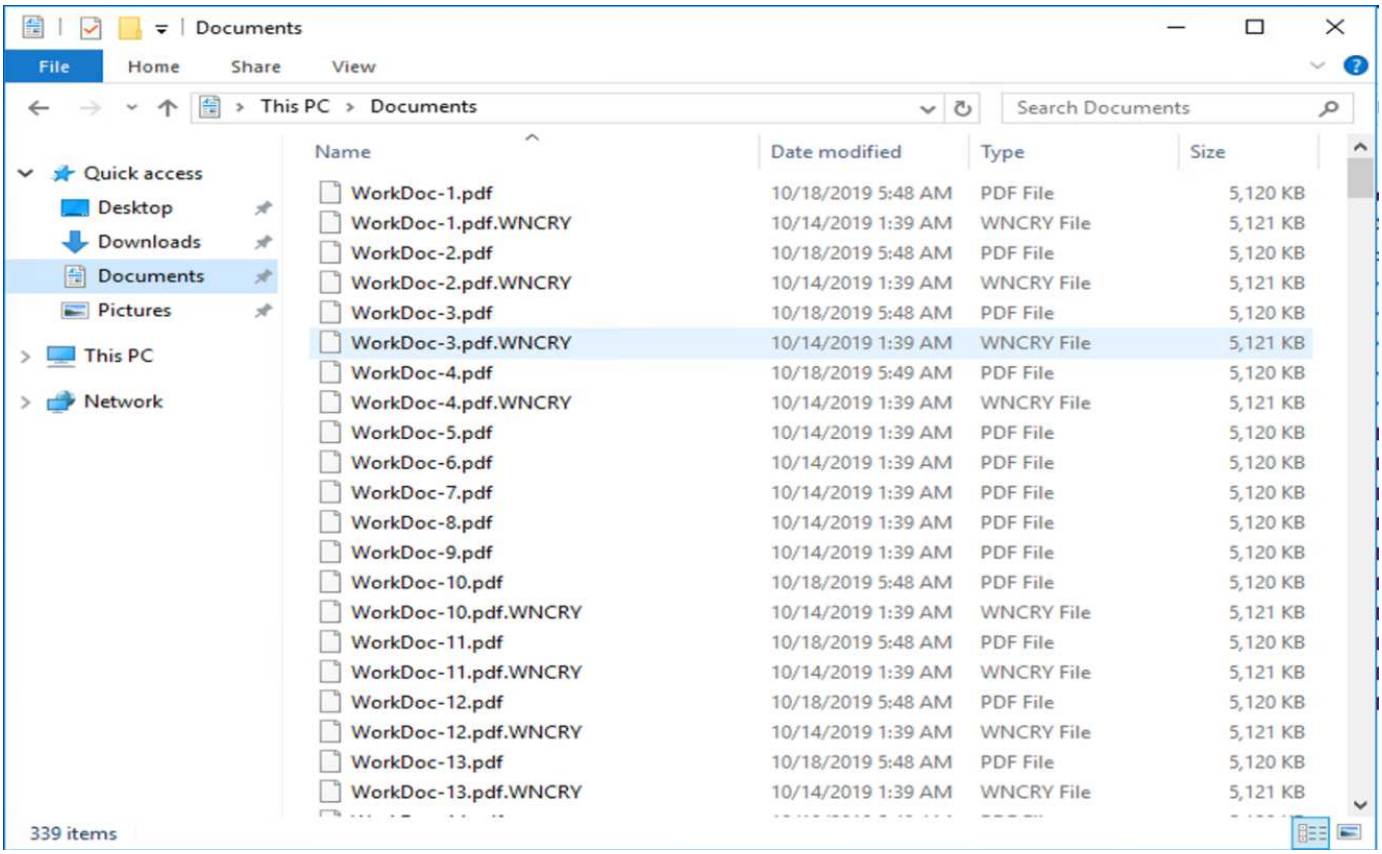
2. Il binario è stato eseguito.



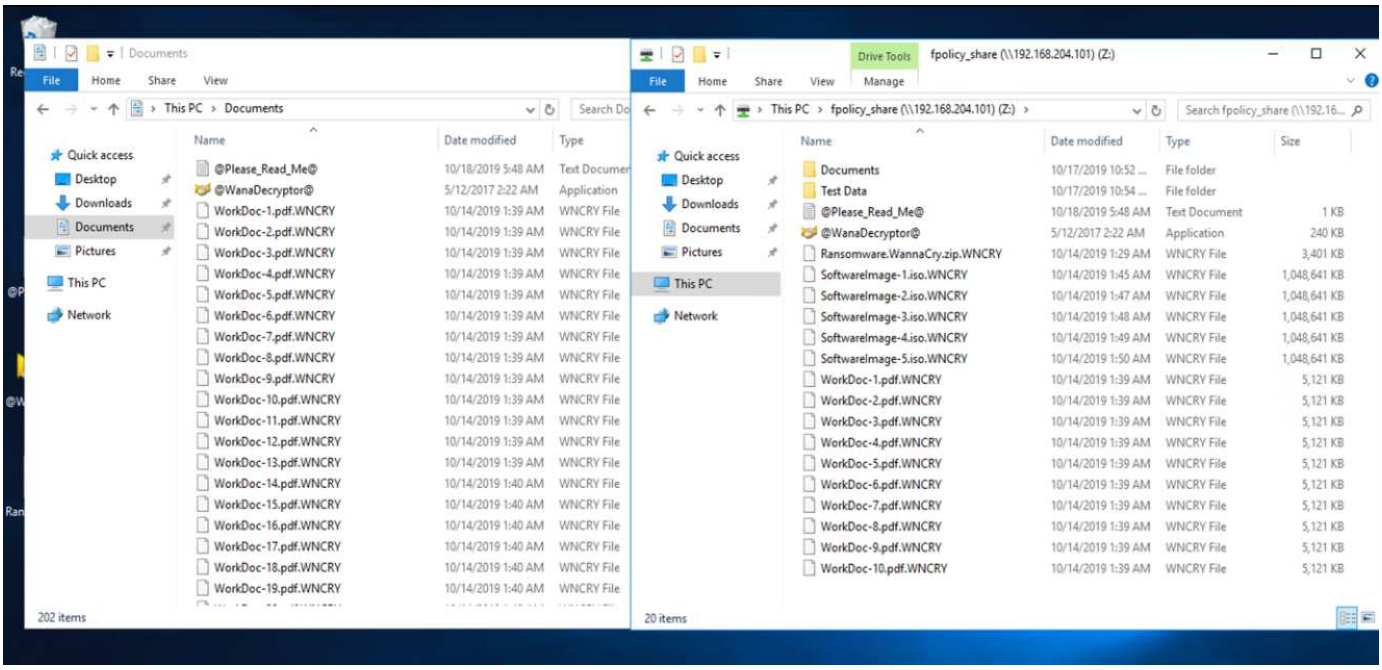
Caso 1: WannaCry crittografa il file system all'interno della VM e della condivisione CIFS mappata

Il file system locale e la condivisione CIFS mappata sono stati crittografati dal malware WannaCry.

Il malware inizia a crittografare i file con estensioni WNCRY.



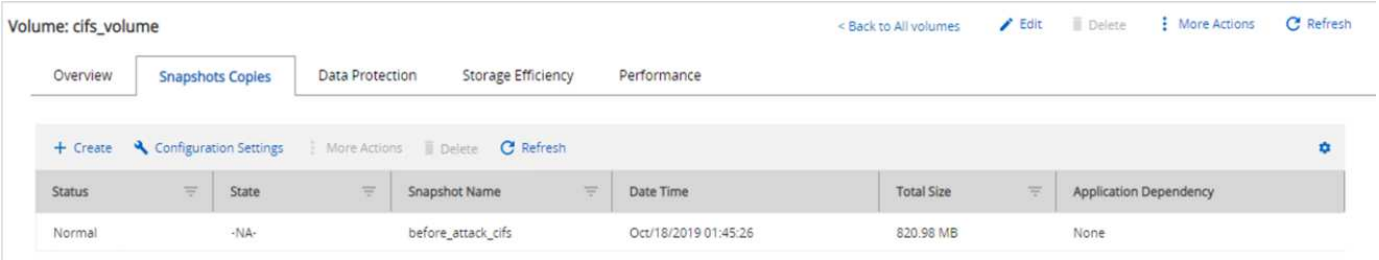
Il malware crittografa tutti i file nella VM locale e nella condivisione mappata.



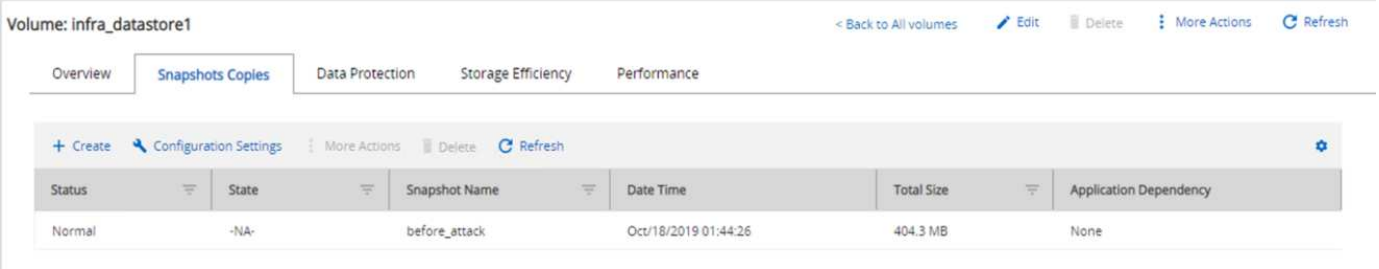
Rilevamento

Dal momento in cui il malware ha iniziato a crittografare i file, ha generato un aumento esponenziale delle dimensioni delle copie Snapshot e una diminuzione esponenziale della percentuale di efficienza dello storage.

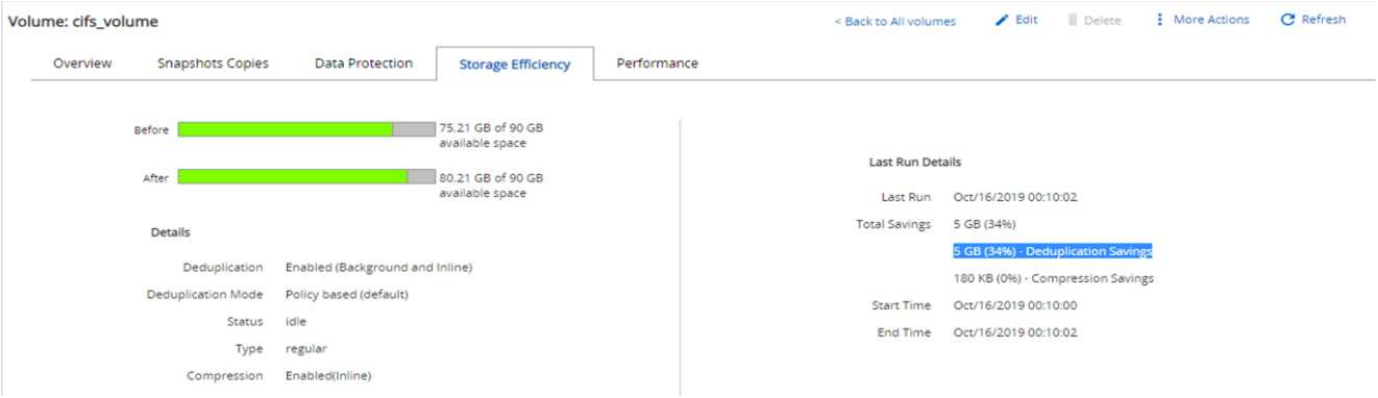
Durante l'attacco, è stato rilevato un notevole aumento delle dimensioni di Snapshot fino a 820,98 MB per il volume che ospita la condivisione CIFS.



È stato rilevato un aumento delle dimensioni della copia Snapshot fino a 404,3 MB per il volume che ospita la macchina virtuale.



L'efficienza dello storage per il volume che ospita la condivisione CIFS è scesa al 34%.



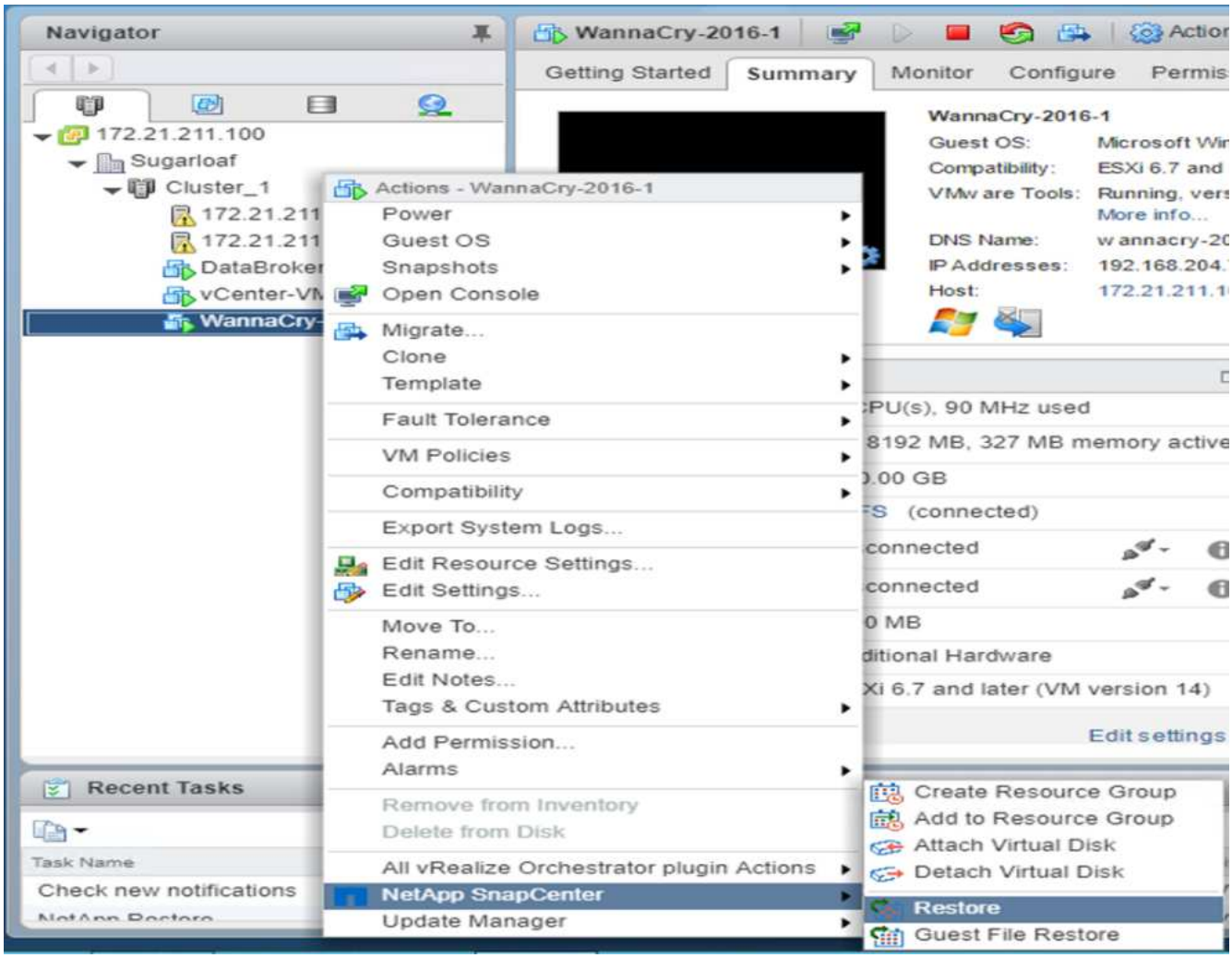
Risoluzione dei problemi

Ripristinare la VM e la condivisione CIFS mappata utilizzando una copia Snapshot pulita creata prima dell'attacco.

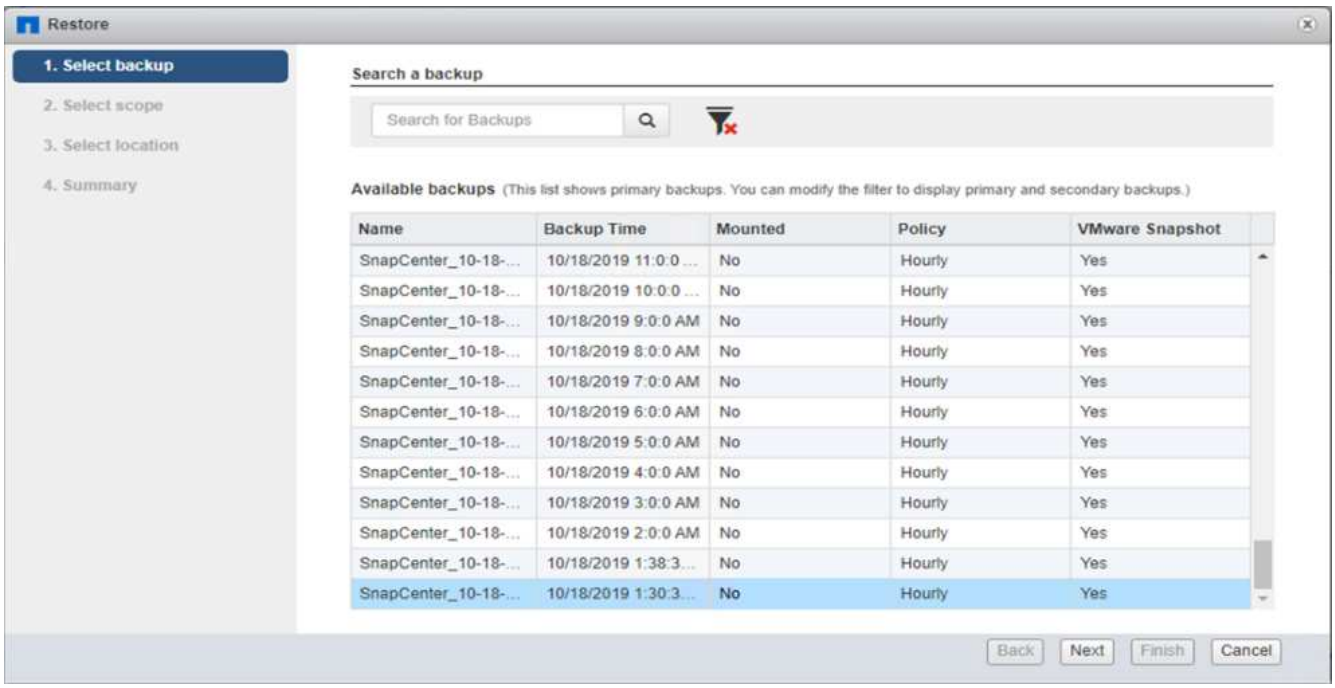
Ripristinare la macchina virtuale

Per ripristinare la macchina virtuale, attenersi alla seguente procedura:

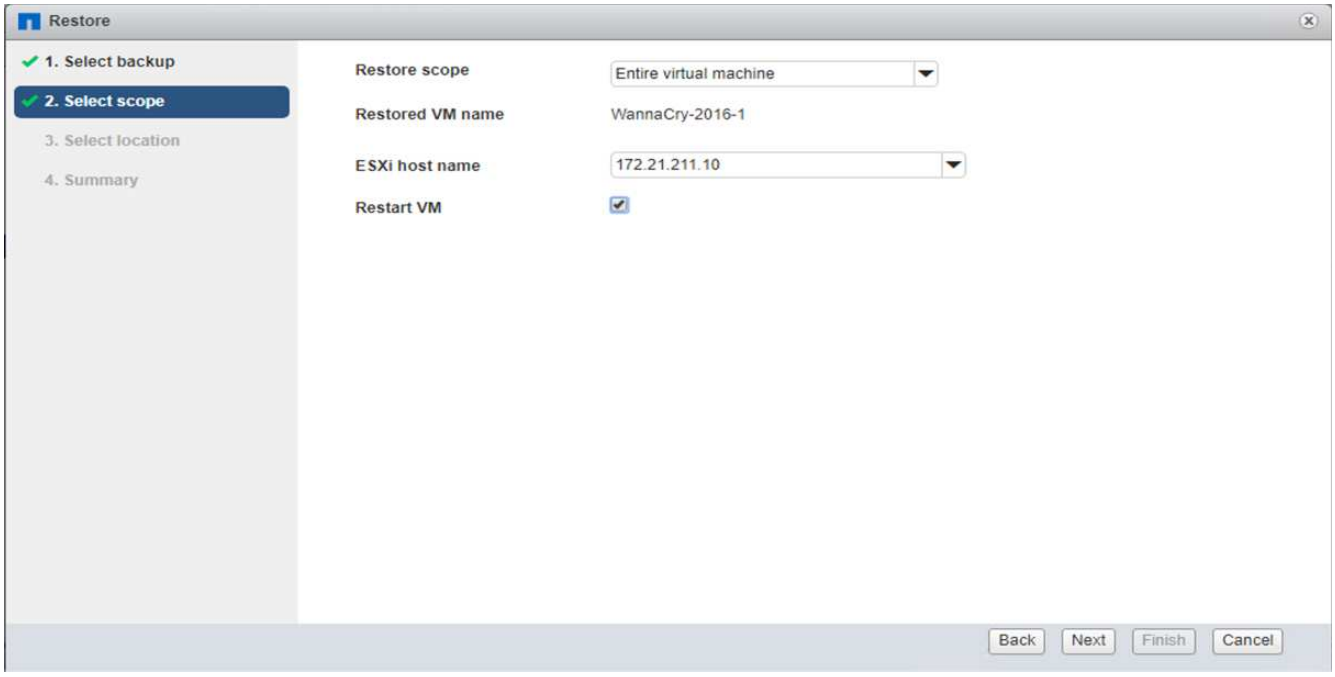
1. Utilizzare la copia Snapshot creata con SnapCenter per ripristinare la macchina virtuale.



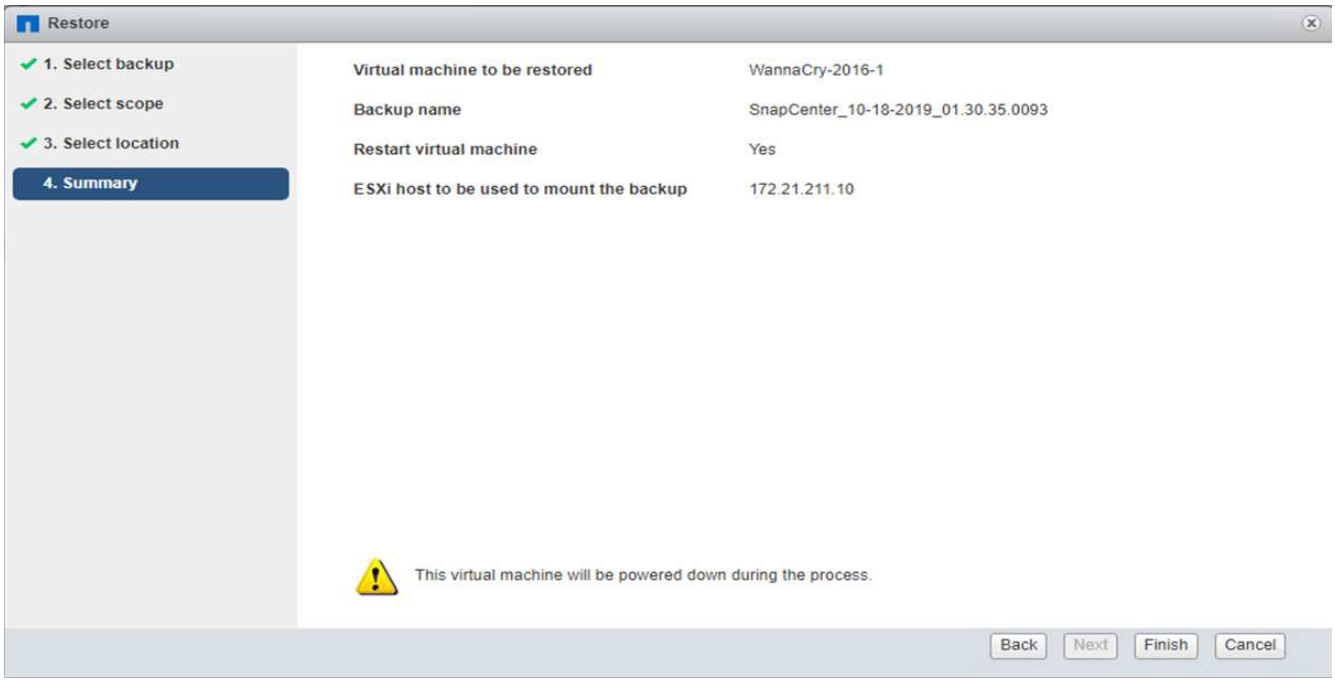
2. Selezionare la copia Snapshot coerente VMware desiderata per il ripristino.



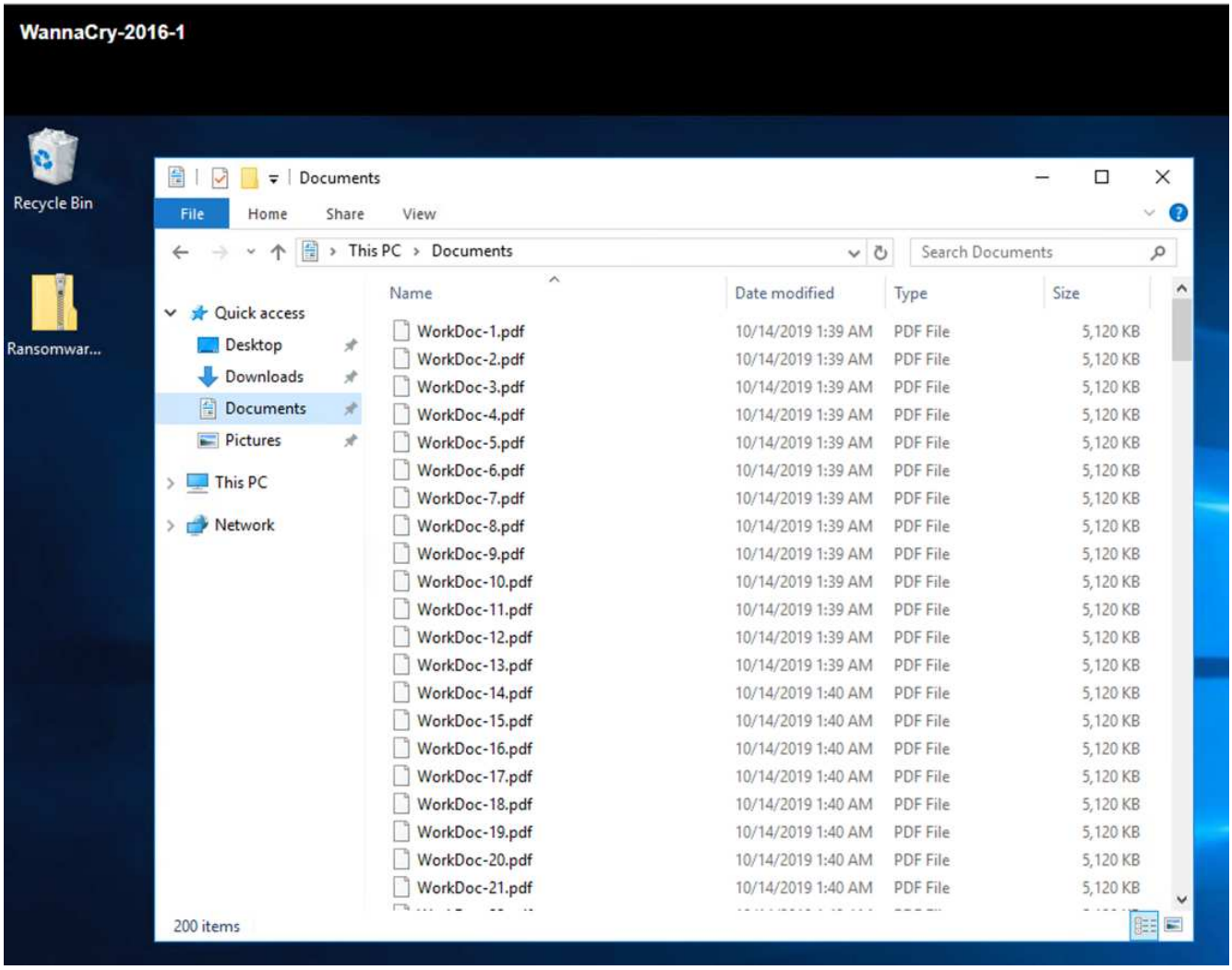
3. L'intera macchina virtuale viene ripristinata e riavviata.



4. Fare clic su Finish (fine) per avviare il processo di ripristino.



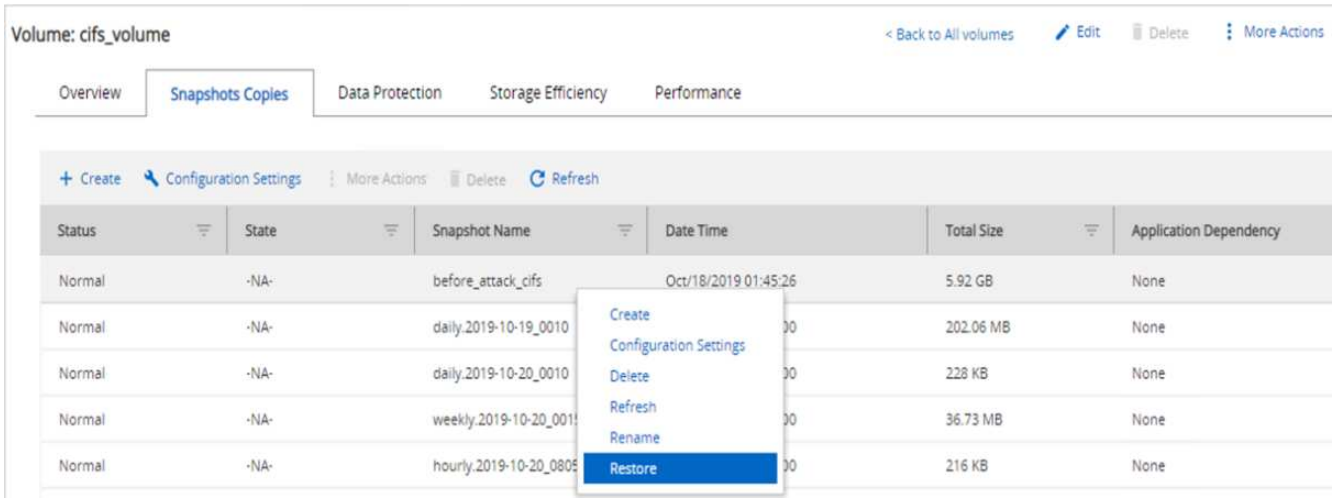
5. La macchina virtuale e i relativi file vengono ripristinati.



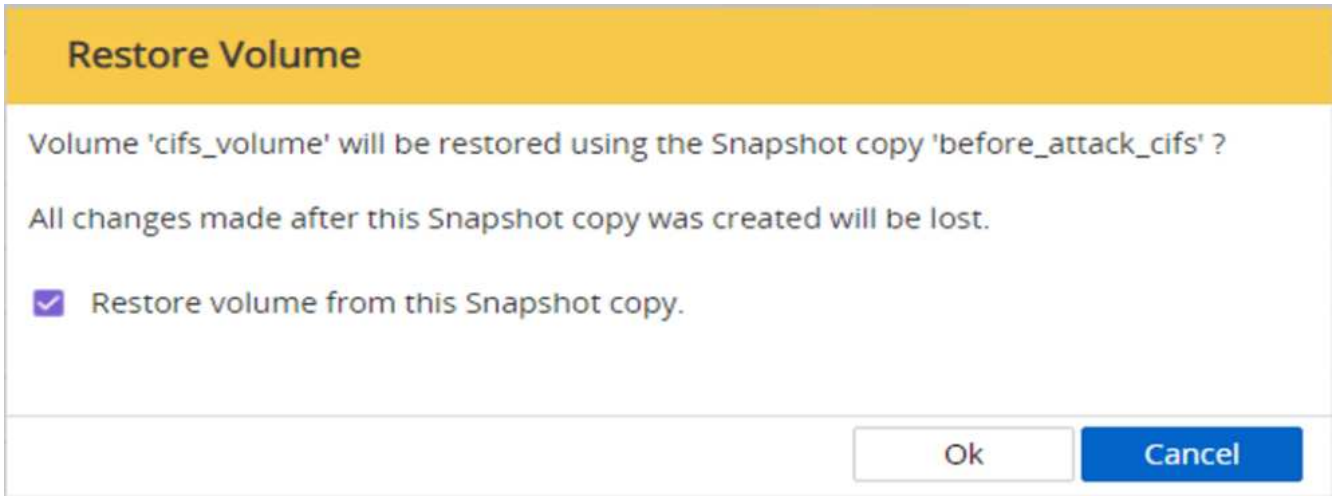
Ripristina condivisione CIFS

Per ripristinare la condivisione CIFS, attenersi alla seguente procedura:

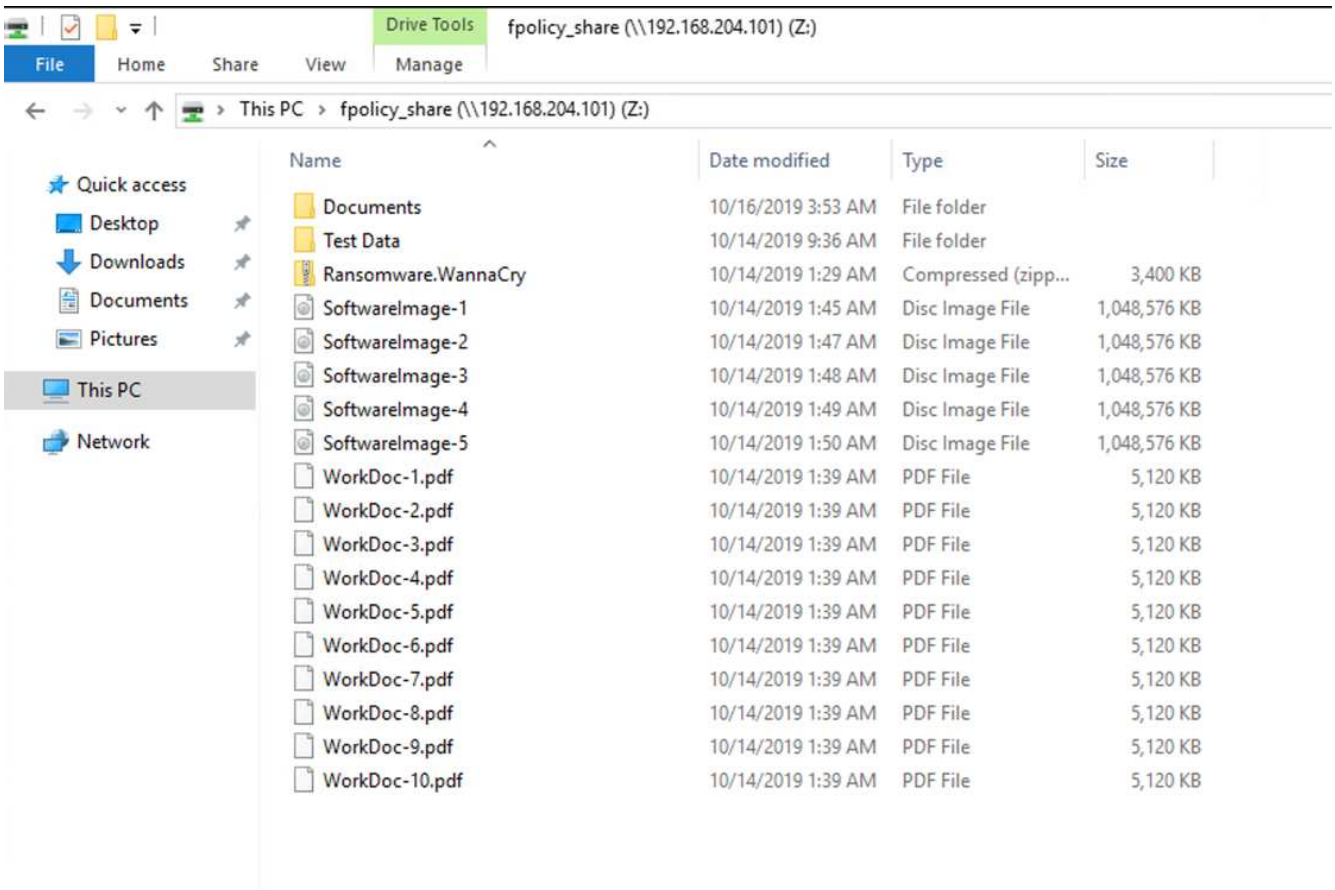
1. Utilizzare la copia Snapshot del volume preso prima dell'attacco per ripristinare la condivisione.



2. Fare clic su OK per avviare l'operazione di ripristino.



3. Visualizzare la condivisione CIFS dopo il ripristino.



Caso 2: WannaCry crittografa il file system all'interno della macchina virtuale e tenta di crittografare la condivisione CIFS mappata protetta tramite FPolicy

Prevenzione

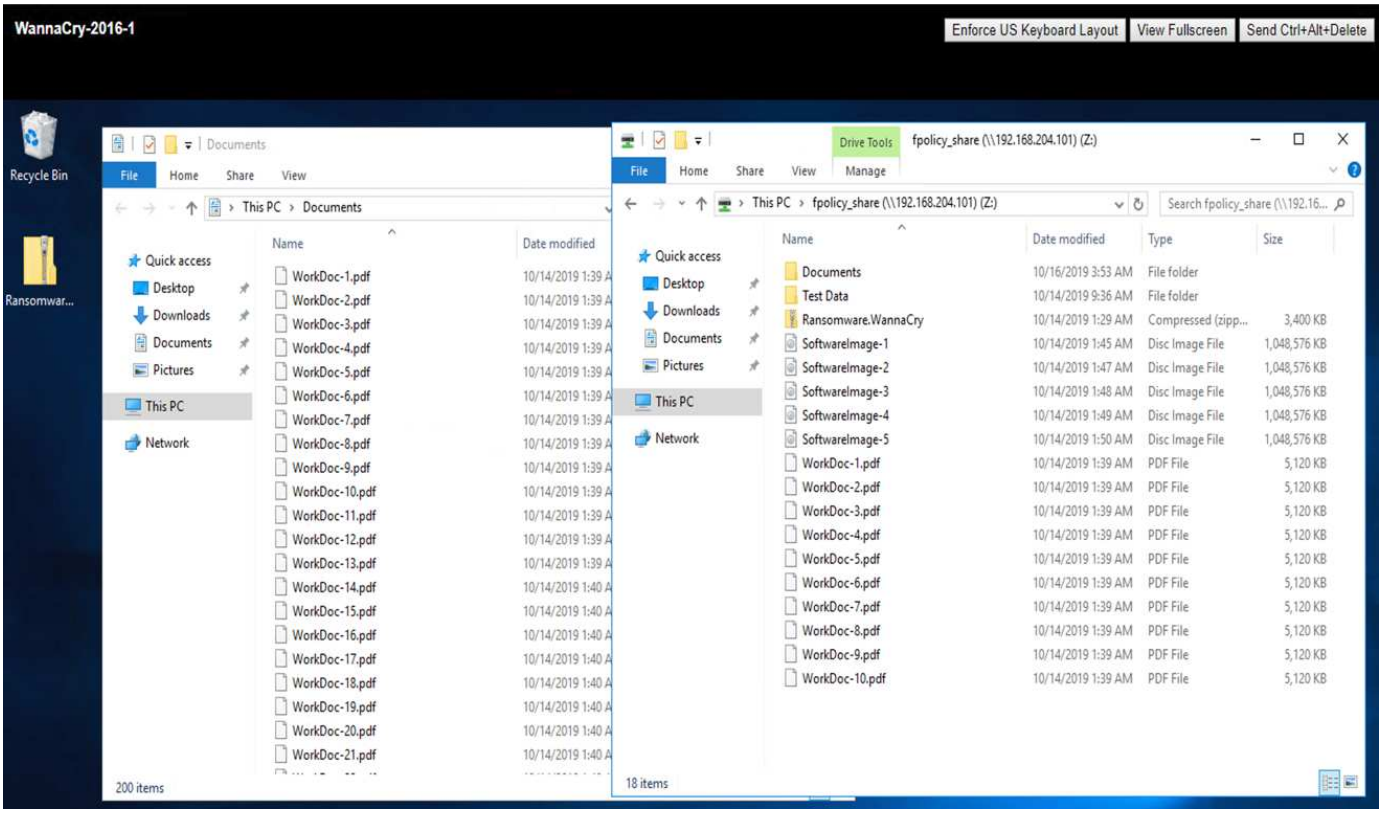
Configura FPolicy

Per configurare FPolicy sulla condivisione CIFS, eseguire i seguenti comandi sul cluster ONTAP:

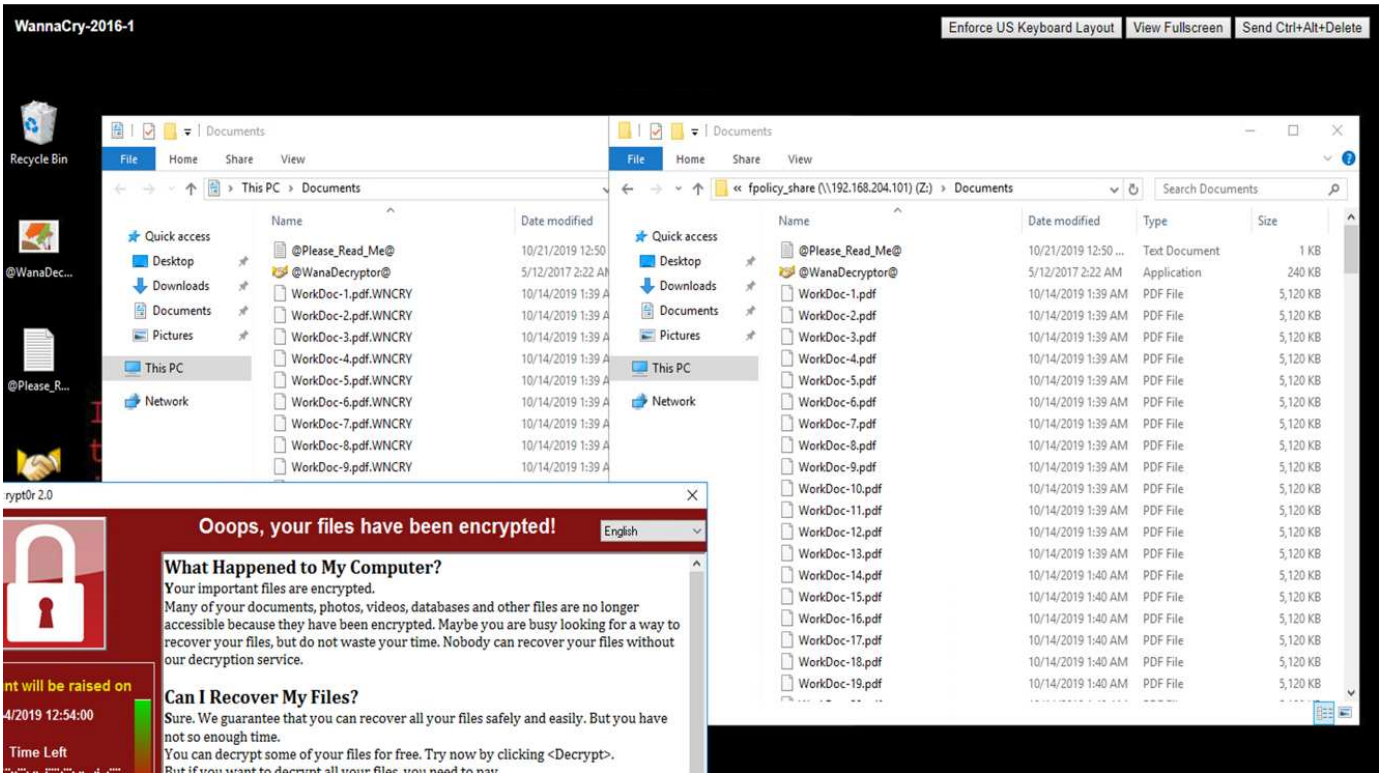
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Con questo criterio, ai file con estensioni WNCRY, Locky e ad4c non è consentito eseguire le operazioni di creazione, ridenominazione, scrittura o apertura dei file.

Visualizzare lo stato dei file prima dell'attacco: Sono non crittografati e in un sistema pulito.



I file sulla macchina virtuale sono crittografati. Il malware WannaCry tenta di crittografare i file nella condivisione CIFS, ma FPolicy impedisce che influiscano sui file.



Continua le operazioni di business senza pagare il riscatto

Le funzionalità di NetApp descritte in questo documento consentono di ripristinare i dati entro pochi minuti dopo un attacco e prevenire gli attacchi, in modo da poter continuare le operazioni di business senza ostacoli.

È possibile impostare un programma di copia Snapshot per soddisfare l'obiettivo RPO (Recovery Point Objective) desiderato. Le operazioni di ripristino basate su copia Snapshot sono molto rapide, pertanto è possibile raggiungere un obiettivo RTO (Recovery Time Objective) molto basso.

Soprattutto, non è necessario pagare alcun riscatto a seguito di un attacco e si può tornare rapidamente alle operazioni regolari.

Conclusione

Ransomware è un prodotto di crimine organizzato e gli autori degli attacchi non operano con l'etica. Possono astenersi dal fornire la chiave per la decifratura anche dopo aver ricevuto il riscatto. La vittima non solo perde i propri dati, ma anche una notevole quantità di denaro e si trova ad affrontare le conseguenze associate alla perdita dei dati di produzione.

Secondo a. "Articolo di Forbes", solo il 19% delle vittime del ransomware ottiene i propri dati dopo aver pagato il riscatto. Pertanto, gli autori consigliano di non pagare un riscatto in caso di attacco, in quanto ciò rafforza la fiducia dell'utente malintenzionato nel proprio modello di business.

Le operazioni di backup e ripristino dei dati svolgono una parte importante del ripristino ransomware. Pertanto, devono essere inclusi come parte integrante della pianificazione aziendale. L'implementazione di queste operazioni deve essere preventivata in modo da non compromettere le funzionalità di recovery in caso di attacco.

La chiave è scegliere il partner tecnologico corretto in questo percorso e FlexPod fornisce la maggior parte delle funzionalità necessarie in modo nativo senza costi aggiuntivi in un sistema FAS all-flash.

Ringraziamenti

L'autore desidera ringraziare le seguenti persone per il loro supporto nella creazione di questo documento:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Ulteriori informazioni

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

- Software NetApp Snapshot

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- Gestione del backup di SnapCenter

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- Conformità dei dati SnapLock

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- Documentazione sui prodotti NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced malware Protection (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

Soluzione FlexPod conforme alla sicurezza FIPS 140-2 per il settore sanitario

TR-4892: Soluzione FlexPod conforme alla sicurezza FIPS 140-2 per il settore sanitario

JayaKishore Esanakula, NetApp John McAbel, Cisco

La Health Information Technology for Economic and Clinical Health Act (HITECH) richiede una crittografia certificata FIPS (Federal Information Processing Standard) 140-2 di ePHI (Electronic Protected Health Information). Le applicazioni e il software HIT

(Health Information Technology) devono essere conformi a FIPS 140-2 per ottenere la certificazione Promoving Interoperability Program (in precedenza significativo programma di incentivi per l'utilizzo). I fornitori e gli ospedali idonei devono utilizzare un HIT conforme a FIPS 140-2 (livello 1) per ricevere gli incentivi Medicare e Medicaid e per evitare le sanzioni per il rimborso da parte del Center for Medicare and Medicaid (CMS). Gli algoritmi di crittografia certificati FIPS 140-2 si qualificano come protezioni tecniche richieste in base a. "Regola di sicurezza" Del Health Information Portability and Accountability Act (HIPAA).

FIPS 140-2 è un standard governativo che definisce i requisiti di sicurezza per i moduli crittografici in hardware, software e firmware che proteggono le informazioni sensibili. La conformità allo standard è richiesta per l'utilizzo da parte degli Stati Uniti enti governativi, e spesso viene utilizzato anche in settori regolamentati come i servizi finanziari e l'assistenza sanitaria. Questo report tecnico aiuta il lettore a comprendere lo standard di sicurezza FIPS 140-2 ad alto livello. Inoltre, aiuta il pubblico a comprendere le varie minacce affrontate dalle organizzazioni sanitarie. Infine, il report tecnico aiuta a capire come un sistema FlexPod conforme a FIPS 140-2 può contribuire a proteggere le risorse sanitarie quando viene implementato su un'infrastruttura convergente FlexPod.

Scopo

Questo documento è una panoramica tecnica di un'infrastruttura FlexPod basata su Cisco Unified Computing System (Cisco UCS), Cisco Nexus, Cisco MDS e NetApp ONTAP per ospitare una o più applicazioni IT per il settore sanitario o soluzioni che richiedono la conformità alla sicurezza FIPS 140-2.

Pubblico

Il presente documento è destinato ai responsabili tecnici del settore sanitario, ai tecnici delle soluzioni partner Cisco e NetApp e al personale dei servizi professionali. NetApp presuppone che il lettore abbia una buona comprensione dei concetti di dimensionamento di calcolo e storage, nonché una familiarità tecnica con le minacce per il settore sanitario, la sicurezza sanitaria, i sistemi IT per il settore sanitario, Cisco UCS e i sistemi storage NetApp.

"Avanti: Minacce alla cybersicurezza nel settore sanitario."

Minacce alla cybersicurezza nel settore sanitario

"Precedente: Introduzione."

Ogni problema presenta una nuova opportunità: Un esempio di tale opportunità è rappresentato dalla pandemia di COVID. Secondo a. "report" Dal programma Cybersecurity del Department of Health and Human Services (HHS), la risposta COVID ha portato a un aumento del numero di attacchi ransomware. Ci sono stati 6,000 nuovi domini internet registrati solo nella terza settimana di marzo 2020. Oltre il 50% dei domini ospitava malware. Gli attacchi ransomware sono stati responsabili di quasi il 50% di tutte le violazioni dei dati sanitari nel 2020 che hanno colpito più di 630 organizzazioni sanitarie e circa 29 milioni di cartelle cliniche. Diciannove leakers/siti hanno raddoppiato l'estorsione. Con il 24.5%, il settore sanitario ha registrato il maggior numero di violazioni dei dati nel 2020.

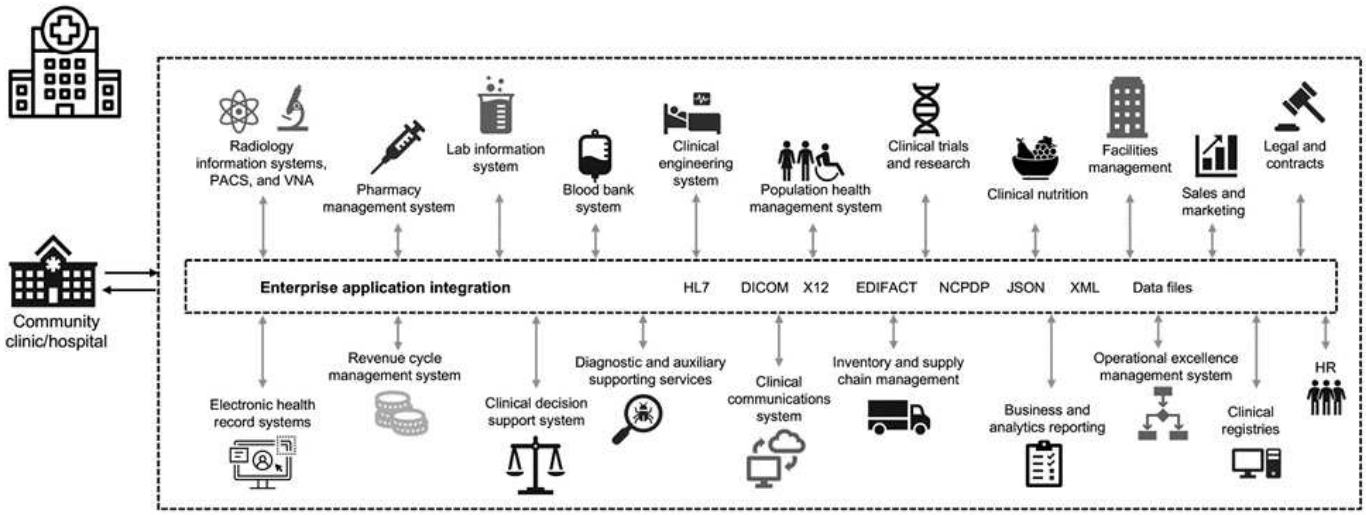
Gli agenti dannosi hanno tentato di violare la sicurezza e la privacy delle informazioni sanitarie protette (PHI)

vendendo le informazioni o minacciando di distruggerle o di esporle. Spesso vengono effettuati tentativi mirati e di trasmissione di massa per ottenere un accesso non autorizzato a ePHI. Circa il 75% delle cartelle cliniche dei pazienti esposte nella seconda metà del 2020 era dovuto a dipendenti aziendali compromessi.

Il seguente elenco di organizzazioni sanitarie è stato preso di mira dagli agenti dannosi:

- Sistemi ospedalieri
- Laboratori di life science
- Laboratori di ricerca
- Strutture di riabilitazione
- Ospedali e cliniche della comunità

La diversità delle applicazioni che costituiscono un'organizzazione sanitaria è innegabile e sempre più complessa. Gli uffici per la sicurezza delle informazioni devono fornire una governance per la vasta gamma di sistemi E risorse IT. La figura seguente illustra le funzionalità cliniche di un sistema ospedaliero tipico.



I dati dei pazienti sono al centro dell'immagine. La perdita dei dati dei pazienti e lo stigma associato a condizioni mediche sensibili sono molto reali. Altri problemi sensibili includono il rischio di esclusione sociale, ricatti, profiling, vulnerabilità al marketing mirato, sfruttamento e potenziale responsabilità finanziaria nei confronti dei pagatori in merito alle informazioni mediche al di là dei privilegi del pagatore.

Le minacce per l'assistenza sanitaria sono di natura multidimensionale e di impatto. I governi di tutto il mondo hanno adottato varie disposizioni per garantire ePHI. Gli effetti negativi e la natura in evoluzione delle minacce per l'assistenza sanitaria rendono difficile per le organizzazioni sanitarie difendere tutte le minacce.

Di seguito viene riportato un elenco delle minacce più comuni identificate nel settore sanitario:

- Attacchi ransomware
- Perdita o furto di apparecchiature o dati con informazioni sensibili
- Attacchi di phishing
- Attacchi contro i dispositivi medici collegati che possono compromettere la sicurezza del paziente
- Attacchi di phishing via e-mail
- Perdita o furto di apparecchiature o dati
- Compromissione del protocollo del desktop remoto

- Vulnerabilità del software

Le organizzazioni del settore sanitario operano in un ambiente legale e normativo complicato quanto i loro ecosistemi digitali. Questo ambiente include, a titolo esemplificativo e non esaustivo, i seguenti elementi:

- Office of the National Coordinator (for Healthcare Technology) Standard di interoperabilità con Electronic Health Information Technology con certificazione ONC
- Medicare Access e il Children's Health Insurance Program ReAuthorization Act (MACRA)/uso significativo
- Obblighi multipli ai sensi della Food and Drug Administration (FDA)
- I processi di accreditamento della Joint Commission
- Requisiti HIPAA
- Requisiti HITECH
- Standard minimi di rischio accettabili per i pagatori
- Norme di sicurezza e privacy statali
- Requisiti del Federal Information Security Modernization Act come incorporati nei contratti federali e nelle borse di ricerca attraverso agenzie come gli istituti nazionali di salute
- Payment Card Industry Data Security Standard (PCI-DSS)
- Requisiti relativi all'abuso di sostanze e all'amministrazione dei servizi di salute mentale (SAMHSA)
- Il Gramm-Leach-Bliley Act per l'elaborazione finanziaria
- La legge di Stark in relazione alla fornitura di servizi alle organizzazioni affiliate
- Family Educational Rights and Privacy Act (FERPA) per le istituzioni che partecipano all'istruzione superiore
- Genetic Information Nondiscrimination Act (GINA)
- Il nuovo regolamento generale sulla protezione dei dati (GDPR) nell'Unione europea

Gli standard dell'architettura di sicurezza sono in rapida evoluzione per impedire agli attori malintenzionati di influire sui sistemi informativi sanitari. Uno di questi standard è FIPS 140-2, definito dal National Institute of Standards and Technology (NIST). La pubblicazione FIPS 140-2 descrive in dettaglio gli Stati Uniti requisiti governativi per un modulo crittografico. I requisiti di sicurezza coprono le aree correlate a una progettazione sicura e all'implementazione di un modulo crittografico e possono essere applicati a HIT. I confini crittografici ben definiti consentono una gestione più semplice della sicurezza, mantenendo al contempo aggiornati i moduli crittografici. Questi limiti aiutano a prevenire i deboli moduli di crittografia che possono essere facilmente sfruttati da utenti malintenzionati. Inoltre, possono contribuire a prevenire gli errori umani durante la gestione dei moduli crittografici standard.

NIST insieme a Communications Security Establishment (CSE) hanno definito il programma di convalida del modulo crittografico (CMVP) per certificare i moduli crittografici per i livelli di convalida FIPS 140-2. Utilizzando un modulo certificato FIPS 140-2, le organizzazioni federali devono proteggere i dati sensibili o preziosi mentre sono a riposo e in movimento. A causa del suo successo nella protezione di informazioni sensibili o preziose, molti sistemi sanitari hanno scelto di crittografare ePHI utilizzando i moduli crittografici FIPS 140-2 oltre il livello minimo di sicurezza richiesto dalla legge.

Sfruttare e implementare le funzionalità FIPS 140-2 di FlexPod richiede solo ore (non giorni). La conformità FIPS è a portata di mano per la maggior parte delle organizzazioni sanitarie, indipendentemente dalle dimensioni. Con confini crittografici chiaramente definiti e semplici fasi di implementazione ben documentate, un'architettura FlexPod conforme a FIPS 140-2 può creare una solida base di sicurezza per l'infrastruttura e consentire semplici miglioramenti per aumentare ulteriormente la protezione per le minacce alla sicurezza.

"Pagina successiva: Panoramica di FIPS 140-2."

Panoramica di FIPS 140-2

"Precedente: Minacce alla cybersicurezza nel settore sanitario."

"FIPS 140-2" specifica i requisiti di sicurezza per un modulo crittografico utilizzato all'interno di un sistema di sicurezza che protegge le informazioni sensibili nei sistemi informatici e di telecomunicazione. Un modulo crittografico deve essere un insieme di hardware, software, firmware o una combinazione. FIPS si applica agli algoritmi di crittografia, alla generazione delle chiavi e ai gestori delle chiavi contenuti all'interno di un confine crittografico. È importante comprendere che FIPS 140-2 si applica specificamente al modulo crittografico, non al prodotto, all'architettura, ai dati o all'ecosistema. Il modulo crittografico, definito nei termini chiave più avanti in questo documento, è il componente specifico (hardware, software e/o firmware) che implementa le funzioni di sicurezza approvate. Inoltre, FIPS 140-2 specifica quattro livelli. Gli algoritmi crittografici approvati sono comuni a tutti i livelli. Gli elementi e i requisiti chiave di ciascun livello di sicurezza includono:

- **Livello di sicurezza 1**
  - Specifica i requisiti di sicurezza di base per un modulo crittografico (è richiesto almeno un algoritmo approvato o una funzione di sicurezza).
  - Per il livello 1 non sono necessari meccanismi di sicurezza fisici specifici oltre i requisiti di base per i componenti di livello di produzione.
- **Livello di sicurezza 2**
  - Migliora i meccanismi di sicurezza fisica aggiungendo il requisito per l'evidenza di manomissione utilizzando soluzioni antimanomissione come rivestimenti o sigilli, blocchi su coperture rimovibili o porte dei moduli crittografici.
  - Richiede, come minimo, il RBAC (role-based access control) in cui il modulo crittografico autentica l'autorizzazione di un operatore o amministratore ad assumere un ruolo specifico ed eseguire un set corrispondente di funzioni.
- **Livello di sicurezza 3**
  - Si basa sui requisiti di antimanomissione del livello 2 e tenta di impedire un ulteriore accesso ai parametri di sicurezza critici (CSP) all'interno del modulo crittografico.
  - I meccanismi di sicurezza fisici richiesti al livello 3 hanno un'elevata probabilità di rilevare e rispondere a tentativi di accesso fisico o a qualsiasi utilizzo o modifica del modulo crittografico. Ad esempio, enclosure potenti, rilevamento delle manomissioni e circuiti di risposta che azzerano tutti i CSP non crittografati quando viene aperto un coperchio rimovibile sul modulo crittografico.
  - Richiede meccanismi di autenticazione basati sull'identità per migliorare la sicurezza dei meccanismi RBAC specificati nel livello 2. Un modulo crittografico autentica l'identità di un operatore e verifica che l'operatore sia autorizzato a utilizzare un ruolo ed eseguire le funzioni del ruolo.
- **Livello di sicurezza 4**
  - Il massimo livello di sicurezza in FIPS 140-2.
  - Il livello più utile per le operazioni in ambienti fisicamente non protetti.
  - A questo livello, i meccanismi di sicurezza fisica sono progettati per fornire una protezione completa intorno al modulo crittografico con la responsabilità di rilevare e rispondere a qualsiasi tentativo non

autorizzato di accesso fisico.

- La penetrazione o l'esposizione del modulo crittografico deve avere un'elevata probabilità di rilevamento e determinare l'azzeramento immediato di tutti i CSP non sicuri o non crittografati.

"Avanti: Piano di controllo rispetto al piano dati."

Piano di controllo rispetto al piano dati

"Precedente: Panoramica di FIPS 140-2."

Quando si implementa una strategia FIPS 140-2, è importante comprendere cosa viene protetto. Questo può essere facilmente suddiviso in due aree: Piano di controllo e piano dati. Un piano di controllo si riferisce agli aspetti che influiscono sul controllo e sul funzionamento dei componenti all'interno del sistema FlexPod: Ad esempio, l'accesso amministrativo ai controller di storage NetApp, agli switch Cisco Nexus e ai server Cisco UCS. La protezione a questo livello viene fornita limitando i protocolli e i crittografia che gli amministratori possono utilizzare per connettersi ai dispositivi e apportare modifiche. Un piano di dati si riferisce alle informazioni effettive, come il PHI, all'interno del sistema FlexPod. Questo è protetto crittografando i dati a riposo e di nuovo per FIPS, garantendo che i moduli crittografici in uso soddisfino gli standard.

"Avanti: Calcolo Cisco UCS e FIPS 140-2 di FlexPod."

Cisco UCS Compute e FIPS 140-2 di FlexPod

"Precedente: Piano di controllo rispetto al piano dati."

Un'architettura FlexPod può essere progettata con un server Cisco UCS conforme a FIPS 140-2. In conformità con il brevetto U. S. NIST, il server Cisco UCS può funzionare in modalità di conformità FIPS 140-2 livello 1. Per un elenco completo dei componenti Cisco conformi a FIPS, vedere "Pagina FIPS 140 di Cisco". Cisco UCS Manager è validato FIPS 140-2.

Cisco UCS e Fabric Interconnect

Cisco UCS Manager viene implementato ed eseguito da Cisco Fabric Interconnects (IF).

Per ulteriori informazioni su Cisco UCS e su come attivare FIPS, consultare "Documentazione di Cisco UCS Manager".

Per attivare la modalità FIPS sull'interconnessione fabric Cisco su ciascun fabric A e B, eseguire i seguenti comandi:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

> Per sostituire un Fi in un cluster su Cisco UCS Manager versione 3.2(3) con un Fi su una release precedente a Cisco UCS Manager versione 3.2(3), disattivare la modalità FIPS (disattivare `fips-mode`) Sul Fi esistente prima di aggiungere il Fi sostitutivo al cluster. Una volta creato il cluster, durante l'avvio di Cisco UCS Manager, la modalità FIPS viene attivata automaticamente.

Cisco offre i seguenti prodotti chiave che possono essere implementati a livello di elaborazione o applicazione:

- **Cisco Advanced malware Protection (AMP) per endpoint.** supportata sui sistemi operativi Microsoft Windows e Linux, questa soluzione integra funzionalità di prevenzione, rilevamento e risposta. Questo software di sicurezza previene le violazioni, blocca il malware nel punto di ingresso e monitora e analizza continuamente le attività di file e processi per rilevare, contenere e rimediare rapidamente alle minacce che possono eludere le difese front-line. Il componente di protezione delle attività dannose (MAP) di AMP monitora continuamente tutte le attività degli endpoint e fornisce il rilevamento in fase di esecuzione e il blocco del comportamento anomalo di un programma in esecuzione sull'endpoint. Ad esempio, quando il comportamento degli endpoint indica ransomware, i processi in errore vengono terminati, impedendo la crittografia degli endpoint e arrestando l'attacco.
- **AMP per la sicurezza della posta elettronica.** le e-mail sono diventate il mezzo principale per diffondere malware e per eseguire cyberattacchi. In media, circa 100 miliardi di e-mail vengono scambiate in un solo giorno, il che fornisce agli autori degli attacchi un eccellente vettore di penetrazione nei sistemi degli utenti. Pertanto, è assolutamente essenziale difendersi da questa linea di attacco. AMP analizza le e-mail per individuare minacce come exploit zero-day e malware furtivo nascosto in allegati dannosi. Utilizza inoltre l'intelligence URL leader del settore per combattere i collegamenti dannosi. Offre agli utenti una protezione avanzata contro il phishing, il ransomware e altri attacchi sofisticati.
- **Next- Generation Intrusion Prevention System (NGIPS).** Cisco firepower NGIPS può essere implementato come appliance fisica nel data center o come appliance virtuale su VMware (NGIPSv per VMware). Questo sistema di prevenzione delle intrusioni altamente efficace offre performance affidabili e un basso costo totale di proprietà. La protezione dalle minacce può essere estesa con licenze di abbonamento opzionali per fornire AMP, visibilità e controllo delle applicazioni e funzionalità di filtraggio degli URL. I NGIPS virtualizzati ispezionano il traffico tra macchine virtuali (VM) e semplificano l'implementazione e la gestione delle soluzioni NGIPS in siti con risorse limitate, aumentando la protezione per risorse fisiche e virtuali.

"Avanti: Rete Cisco FlexPod e FIPS 140-2."

Rete Cisco FlexPod e FIPS 140-2

"Precedente: Calcolo Cisco UCS FlexPod e FIPS 140-2."

Cisco MDS

Piattaforma Cisco MDS serie 9000 con software 8.4.x IS "Conforme a FIPS 140-2". Cisco MDS implementa moduli crittografici e i seguenti servizi per SNMPv3 e SSH.

- Creazione di una sessione a supporto di ciascun servizio
- Tutti gli algoritmi crittografici sottostanti che supportano le funzioni di derivazione delle chiavi di ciascun servizio
- Hashing per ogni servizio
- Crittografia simmetrica per ciascun servizio

Prima di attivare la modalità FIPS, completare le seguenti attività sullo switch MDS:

1. Impostare le password su una lunghezza minima di otto caratteri.
2. Disattiva Telnet. Gli utenti devono effettuare l'accesso solo tramite SSH.
3. Disattiva l'autenticazione remota tramite RADIUS/TACACS+. È possibile autenticare solo gli utenti locali dello switch.
4. Disattivare SNMP v1 e v2. Tutti gli account utente esistenti sullo switch configurati per SNMPv3 devono essere configurati solo con SHA per l'autenticazione e AES/3DES per la privacy.
5. Disattiva VRRP.
6. Eliminare tutti i criteri IKE che dispongono di MD5 per l'autenticazione o DES per la crittografia. Modificare i criteri in modo che utilizzino SHA per l'autenticazione e 3DES/AES per la crittografia.
7. Eliminare tutte le coppie di chiavi RSA1 di SSH Server.

Per attivare la modalità FIPS e visualizzare lo stato FIPS sullo switch MDS, attenersi alla seguente procedura:

1. Mostra lo stato FIPS.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Impostare la chiave SSH a 2048 bit.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Attivare la modalità FIPS.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Mostra lo stato FIPS.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Salvare la configurazione nella configurazione in esecuzione.

```
MDSSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Riavviare lo switch MDS

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Mostra lo stato FIPS.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Per ulteriori informazioni, vedere "Attivazione della modalità FIPS".

Cisco Nexus

Gli switch Cisco Nexus serie 9000 (versione 9.3) sono "Conforme a FIPS 140-2". Cisco Nexus implementa moduli crittografici e i seguenti servizi per SNMPv3 e SSH.

- Creazione di una sessione a supporto di ciascun servizio
- Tutti gli algoritmi crittografici sottostanti che supportano le funzioni di derivazione delle chiavi di ciascun servizio

- Hashing per ogni servizio
- Crittografia simmetrica per ciascun servizio

Prima di attivare la modalità FIPS, completare le seguenti attività sullo switch Cisco Nexus:

1. Disattiva Telnet. Gli utenti devono effettuare l'accesso solo con Secure Shell (SSH).
2. Disattivare SNMPv1 e v2. Tutti gli account utente esistenti sul dispositivo configurati per SNMPv3 devono essere configurati solo con SHA per l'autenticazione e AES/3DES per la privacy.
3. Eliminare tutte le coppie di chiavi RSA1 del server SSH.
4. Abilitare il controllo dell'integrità del messaggio (MIC) HMAC-SHA1 da utilizzare durante la negoziazione del protocollo SAP (Security Association Protocol) Cisco TrustSec. A tale scopo, immettere l'algoritmo hash sap `HMAC-SHA-1` dal `cts-manual` oppure `cts-dot1x` modalità.

Per attivare la modalità FIPS sullo switch Nexus, attenersi alla seguente procedura:

1. Impostare una chiave SSH a 2048 bit.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Impostare la chiave SSH a 2048 bit.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Attivare la modalità FIPS.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Riavviare lo switch Nexus.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Mostra lo stato FIPS.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Inoltre, il software Cisco NX OS supporta la funzione NetFlow che consente un rilevamento avanzato delle anomalie di rete e della sicurezza. NetFlow acquisisce i metadati di ogni conversazione sulla rete, le parti coinvolte nella comunicazione, il protocollo utilizzato e la durata della transazione. Una volta aggregate e analizzate le informazioni, possono fornire informazioni dettagliate sul comportamento normale. I dati raccolti consentono inoltre l'identificazione di modelli di attività dubbi, come la diffusione di malware nella rete, che altrimenti potrebbero passare inosservati. NetFlow utilizza i flussi per fornire statistiche per il monitoraggio della rete. Un flusso è un flusso unidirezionale di pacchetti che arriva su un'interfaccia di origine (o VLAN) e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. Si crea un flusso utilizzando un record di flusso per definire le chiavi univoche per il flusso. È possibile esportare i dati raccolti da NetFlow per i flussi utilizzando un'esportazione di flusso in un NetFlow Collector remoto, ad esempio Cisco Stealthwatch. Stealthwatch utilizza queste informazioni per il monitoraggio continuo della rete e fornisce analisi forensi in tempo reale per il rilevamento delle minacce e la risposta agli incidenti in caso di scoppio di ransomware.

"Pagina successiva: Storage NetApp ONTAP e FIPS 140-2 di FlexPod."

Storage NetApp ONTAP e FIPS 140-2 di FlexPod

"Precedente: Rete Cisco FlexPod e FIPS 140-2."

NetApp offre una vasta gamma di hardware, software e servizi, che possono includere vari componenti dei moduli crittografici validati in base allo standard. Pertanto, NetApp utilizza una serie di approcci per la conformità FIPS 140-2 per il piano di controllo e il piano dati:

- NetApp include moduli crittografici che hanno ottenuto la convalida di livello 1 per la crittografia dei dati in transito e dei dati a riposo.
- NetApp acquisisce moduli hardware e software che sono stati convalidati FIPS 140-2 dai fornitori di tali componenti. Ad esempio, la soluzione NetApp Storage Encryption sfrutta dischi convalidati FIPS livello 2.
- I prodotti NetApp possono utilizzare un modulo validato in modo conforme allo standard anche se il prodotto o la funzionalità non rientra nei limiti della convalida. Ad esempio, NetApp Volume Encryption (NVE) è conforme a FIPS 140-2. Anche se non convalidato separatamente, sfrutta il modulo crittografico NetApp, validato al livello 1. Per conoscere le specifiche di conformità per la versione di ONTAP in uso, contatta il tuo SME FlexPod.

I moduli NetApp Cryptographic sono validati FIPS 140-2 livello 1

- NetApp Cryptographic Security Module (NCSM) è validato FIPS 140-2 livello 1.

I dischi con crittografia automatica NetApp sono convalidati FIPS 140-2 livello 2

NetApp acquista dischi con crittografia automatica (SED) che sono stati convalidati FIPS 140-2 dall'OEM (Original Equipment Manufacturer); i clienti che cercano questi dischi devono specificarli al momento dell'ordine. I dischi sono validati al livello 2. I seguenti prodotti NetApp possono sfruttare i SED validati:

- Sistemi storage AFF A-Series e FAS
- Sistemi storage e-Series ed EF-Series

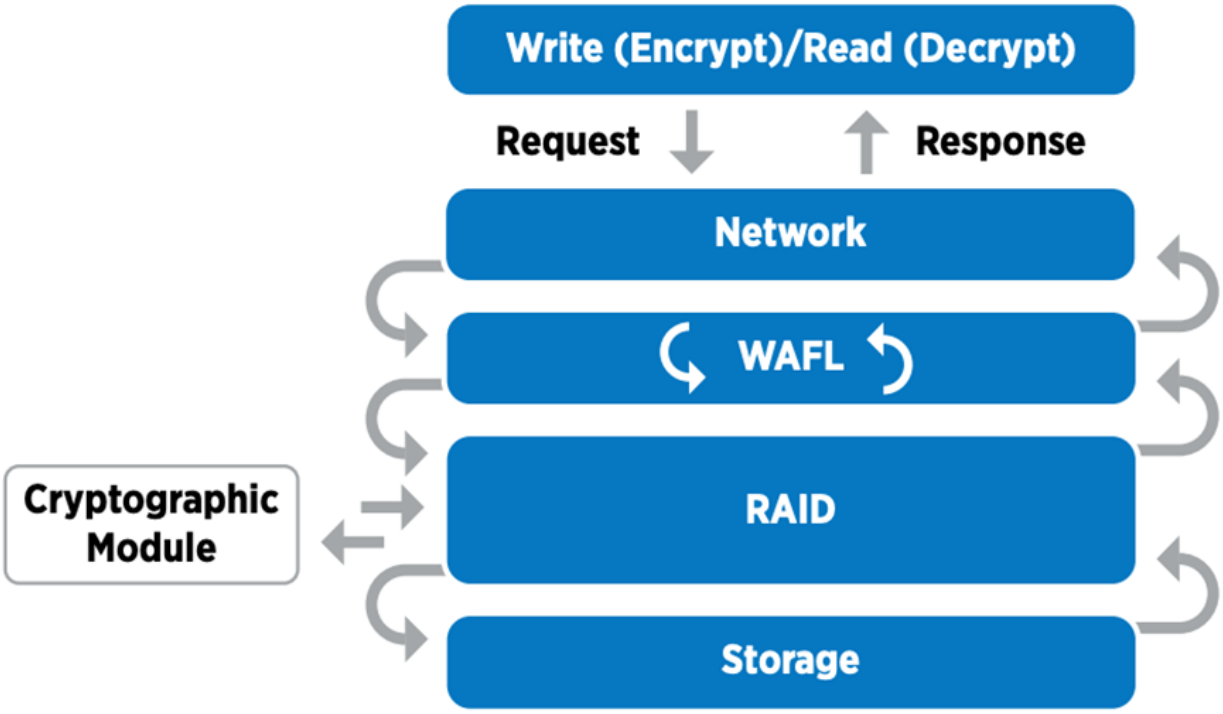
NetApp aggregate Encryption e NetApp Volume Encryption

Le tecnologie NVE e NetApp aggregate Encryption (NAE) consentono la crittografia dei dati rispettivamente a livello di volume e aggregato, rendendo la soluzione indipendente dal disco fisico.

NVE è una soluzione di crittografia dei dati a riposo basata su software disponibile a partire da ONTAP 9.1 ed è conforme a FIPS 140-2 a partire da ONTAP 9.2. NVE consente a ONTAP di crittografare i dati per ogni volume per la granularità. NAE, disponibile con ONTAP 9.6, è un'espansione di NVE; consente a ONTAP di crittografare i dati per ogni volume e i volumi possono condividere le chiavi nell'aggregato. Sia NVE che NAE utilizzano la crittografia AES a 256 bit. I dati possono anche essere memorizzati su disco senza SED. NVE e NAE consentono di utilizzare le funzionalità di efficienza dello storage anche quando la crittografia è attivata. La crittografia solo a livello di applicazione consente di ridurre tutti i vantaggi dell'efficienza dello storage. Con NVE e NAE, l'efficienza dello storage viene mantenuta perché i dati provengono dalla rete attraverso NetApp WAFL al livello RAID, che determina se i dati devono essere crittografati. Per una maggiore efficienza dello storage, è possibile utilizzare la deduplica aggregata con NAE. I volumi NVE e NAE possono coesistere sullo stesso aggregato NAE. Gli aggregati NAE non supportano volumi non crittografati.

Ecco come funziona il processo: Quando i dati vengono crittografati, vengono inviati al modulo crittografico convalidato FIPS 140-2 livello 1. Il modulo crittografico crittografa i dati e li invia di nuovo al livello RAID. I dati crittografati vengono quindi inviati al disco. Pertanto, con la combinazione di NVE e NAE, i dati sono già crittografati durante il percorso verso il disco. Le letture seguono il percorso inverso. In altre parole, i dati

lasciano il disco crittografato, vengono inviati a RAID, vengono decifrati dal modulo crittografico e quindi inviati al resto dello stack, come mostrato nella figura seguente.



NVE utilizza un modulo di crittografia software validato FIPS 140-2 livello 1.

Per ulteriori informazioni su NVE, vedere "Scheda informativa di NVE".

NVE protegge i dati nel cloud. Cloud Volumes ONTAP e Azure NetApp Files sono in grado di fornire la crittografia dei dati conforme a FIPS 140-2 a riposo.

A partire da ONTAP 9.7, gli aggregati e i volumi appena creati vengono crittografati per impostazione predefinita quando si dispone della licenza NVE e della gestione delle chiavi integrata o esterna. A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. I volumi creati nell'aggregato vengono crittografati per impostazione predefinita. È possibile ignorare l'impostazione predefinita quando si crittografa il volume.

Comandi ONTAP NAE CLI

Prima di eseguire i seguenti comandi CLI, assicurarsi che il cluster disponga della licenza NVE richiesta.

Per creare un aggregato e crittografarlo, eseguire il seguente comando (quando viene eseguito su un'interfaccia CLI del cluster ONTAP 9.6 e versioni successive):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Per convertire un aggregato non NAE in un aggregato NAE An, eseguire il seguente comando (se eseguito su

una CLI cluster ONTAP 9.6 e versioni successive):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Per convertire un aggregato NAE in un aggregato non NAE, eseguire il seguente comando (quando viene eseguito su una CLI cluster ONTAP 9.6 e versioni successive):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

Comandi CLI NVE di ONTAP

A partire da ONTAP 9.6, è possibile utilizzare la crittografia a livello di aggregato per assegnare le chiavi all'aggregato contenente per i volumi da crittografare. I volumi creati nell'aggregato vengono crittografati per impostazione predefinita.

Per creare un volume su un aggregato abilitato NAE, eseguire il seguente comando (se eseguito su una CLI cluster ONTAP 9.6 e versioni successive):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Per abilitare la crittografia di un volume esistente "inplace" senza uno spostamento del volume, eseguire il seguente comando (se eseguito su un'interfaccia CLI del cluster ONTAP 9.6 e versioni successive):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

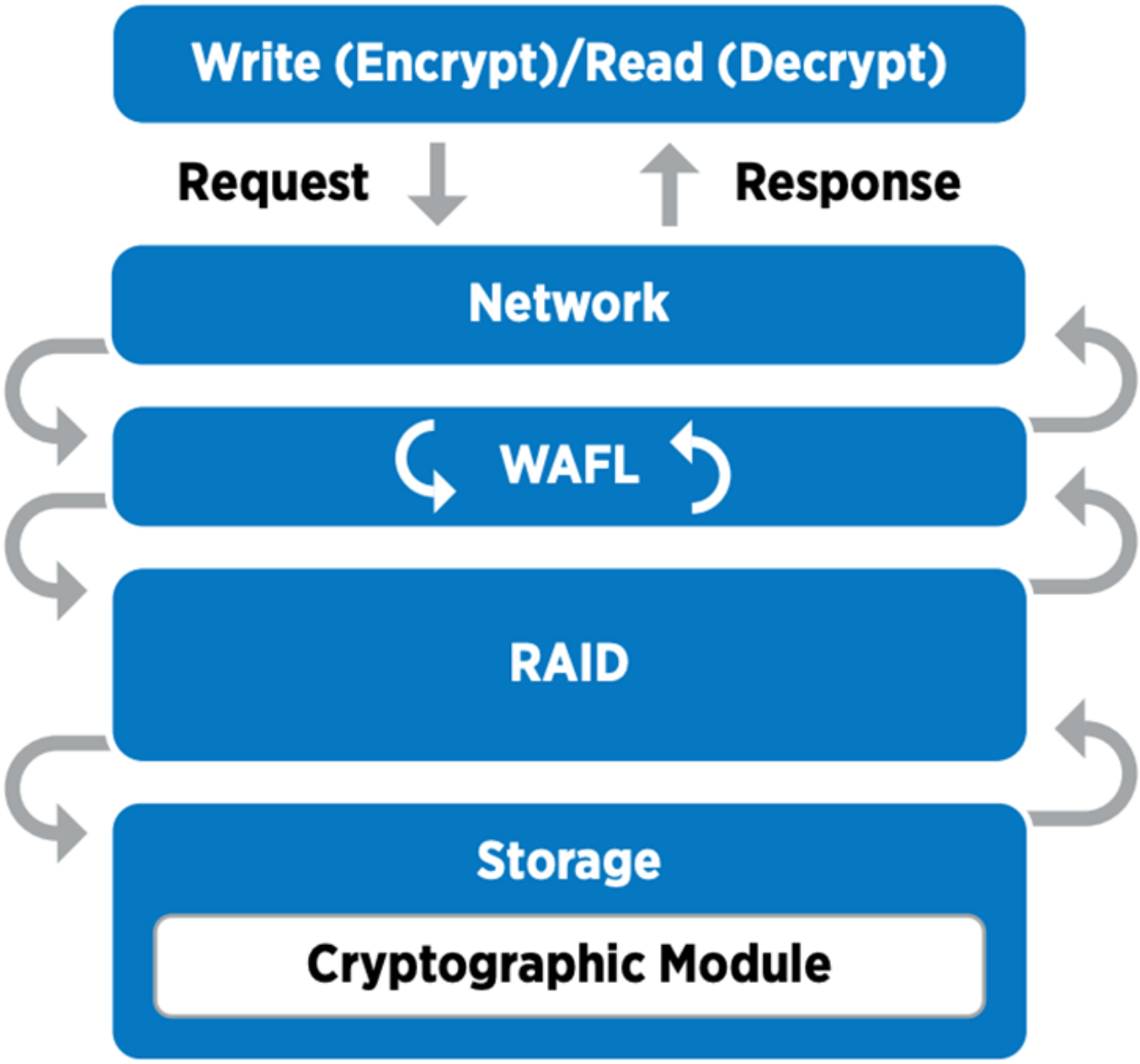
Per verificare che i volumi siano abilitati per la crittografia, eseguire il seguente comando CLI:

```
fp-health::> volume show -is-encrypted true
```

NSE

NSE utilizza i SED per eseguire la crittografia dei dati attraverso un meccanismo con accelerazione hardware.

NSE è configurato per utilizzare dischi con crittografia automatica FIPS 140-2 livello 2 per facilitare la conformità e il ritorno delle parti di ricambio, consentendo la protezione dei dati inattivi tramite crittografia trasparente dei dischi AES a 256 bit. I dischi eseguono tutte le operazioni di crittografia dei dati internamente, come illustrato nella figura seguente, inclusa la generazione della chiave di crittografia. Per impedire l'accesso non autorizzato ai dati, il sistema di storage deve autenticarsi con il disco utilizzando una chiave di autenticazione stabilita al primo utilizzo del disco.



NSE utilizza la crittografia hardware su ogni disco, convalidata FIPS 140-2 livello 2.

Per ulteriori informazioni su NSE, consultare "Scheda tecnica NSE".

Gestione delle chiavi

Lo standard FIPS 140-2 si applica al modulo crittografico come definito dal confine, come mostrato nella figura seguente.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

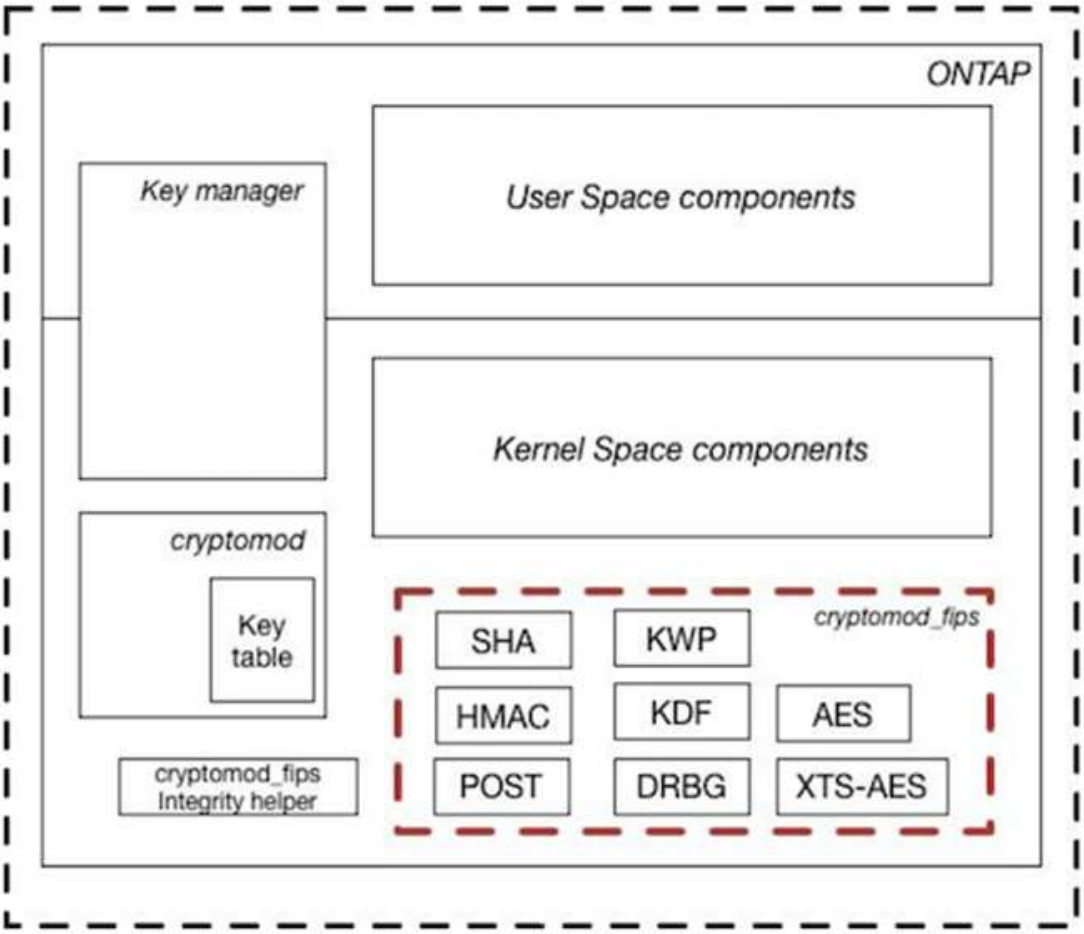


Figure 1 - Block Diagram

Key Manager tiene traccia di tutte le chiavi di crittografia utilizzate da ONTAP. I SED NSE utilizzano il gestore delle chiavi per impostare le chiavi di autenticazione per i SED NSE. Quando si utilizza il gestore delle chiavi, la soluzione combinata NVE e NAE è composta da un modulo di crittografia software, chiavi di crittografia e un gestore delle chiavi. Per ciascun volume, NVE utilizza una chiave di crittografia dati XTS-AES 256 univoca, archiviata dal gestore delle chiavi. La chiave utilizzata per un volume di dati è univoca per il volume di dati in quel cluster e viene generata quando viene creato il volume crittografato. Allo stesso modo, un volume NAE utilizza chiavi di crittografia dati XTS-AES 256 univoche per aggregato, memorizzate anche dal gestore delle chiavi. Le chiavi NAE vengono generate quando viene creato l'aggregato crittografato. ONTAP non genera in anticipo le chiavi, le riutilizza o le visualizza in testo normale, ma vengono memorizzate e protette dal gestore delle chiavi.

Supporto per gestore chiavi esterno

A partire da ONTAP 9.3, i key manager esterni sono supportati sia nelle soluzioni NVE che NSE. Lo standard FIPS 140-2 si applica al modulo crittografico utilizzato nell'implementazione del vendor specifico. Nella maggior parte dei casi, i clienti FlexPod e ONTAP utilizzano una delle seguenti soluzioni validate (in base al "Matrice di interoperabilità NetApp") responsabili chiave:

- Gemalto o SafeNet ALL'INDIRIZZO
- Vormetric (Thales)
- IBM SKLM
- Utimaco (in precedenza Microfous, HPE)

Il backup delle chiavi di autenticazione NSE e NVMe SED viene eseguito su un gestore di chiavi esterno utilizzando LO standard di settore OASIS Key Management Interoperability Protocol (KMIP). Solo il sistema di storage, il disco e il gestore delle chiavi hanno accesso alla chiave e l'unità non può essere sbloccata se viene spostata all'esterno del dominio di sicurezza, impedendo così la perdita di dati. Il gestore delle chiavi esterno memorizza anche le chiavi di crittografia del volume NVE e le chiavi di crittografia aggregate NAE. Se il controller e i dischi vengono spostati e non hanno più accesso al gestore delle chiavi esterno, i volumi NVE e NAE non saranno accessibili e non potranno essere decifrati.

Il seguente comando di esempio aggiunge due server di gestione delle chiavi all'elenco di server utilizzati dal gestore delle chiavi esterno per la macchina virtuale dello store (SVM) `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Quando un data center FlexPod viene utilizzato in uno scenario di multi-tenancy, ONTAP consente agli utenti di fornire una separazione di tenancy per motivi di sicurezza a livello di SVM.

Per verificare l'elenco dei key manager esterni, eseguire il seguente comando CLI:

```
fp-health::> security key-manager external show
```

Combinazione della crittografia per la doppia crittografia (difesa a più livelli)

Se è necessario separare l'accesso ai dati e assicurarsi che i dati siano sempre protetti, i SED NSE possono essere combinati con la crittografia a livello di rete o fabric. I SED NSE agiscono come un backstop se un amministratore dimentica di configurare o configurare in modo errato la crittografia di livello superiore. Per due diversi livelli di crittografia, è possibile combinare i SED NSE con NVE e NAE.

Modalità FIPS del piano di controllo a livello di cluster NetApp ONTAP

Il software per la gestione dei dati NetApp ONTAP dispone di una configurazione in modalità FIPS che crea un'istanza di un livello di sicurezza aggiunto per il cliente. Questa modalità FIPS si applica solo al piano di controllo. Quando la modalità FIPS è attivata, in conformità con gli elementi chiave di FIPS 140-2, Transport Layer Security v1 (TLSv1) e SSLv3 sono disattivati e solo TLS v1.1 e TLS v1.2 rimangono attivati.

> Il pannello di controllo a livello di cluster ONTAP in modalità FIPS è conforme a FIPS 140-2 livello 1. La modalità FIPS a livello di cluster utilizza un modulo crittografico basato su software fornito da NCSM.

La modalità di conformità FIPS 140-2 per il piano di controllo a livello di cluster protegge tutte le interfacce di controllo di ONTAP. Per impostazione predefinita, la modalità solo FIPS 140-2 è disattivata; tuttavia, è possibile abilitarla impostando `is- fips-enabled` parametro a. `true` per `security config modify` comando.

Per attivare la modalità FIPS sul cluster ONTAP, eseguire il seguente comando:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Quando la modalità SSL FIPS è attivata, la comunicazione SSL da ONTAP al client esterno o ai componenti server esterni a ONTAP utilizzerà la crittografia conforme a FIPS per SSL.

Per visualizzare lo stato FIPS dell'intero cluster, eseguire i seguenti comandi:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Avanti: Vantaggi della soluzione dell'infrastruttura convergente FlexPod."

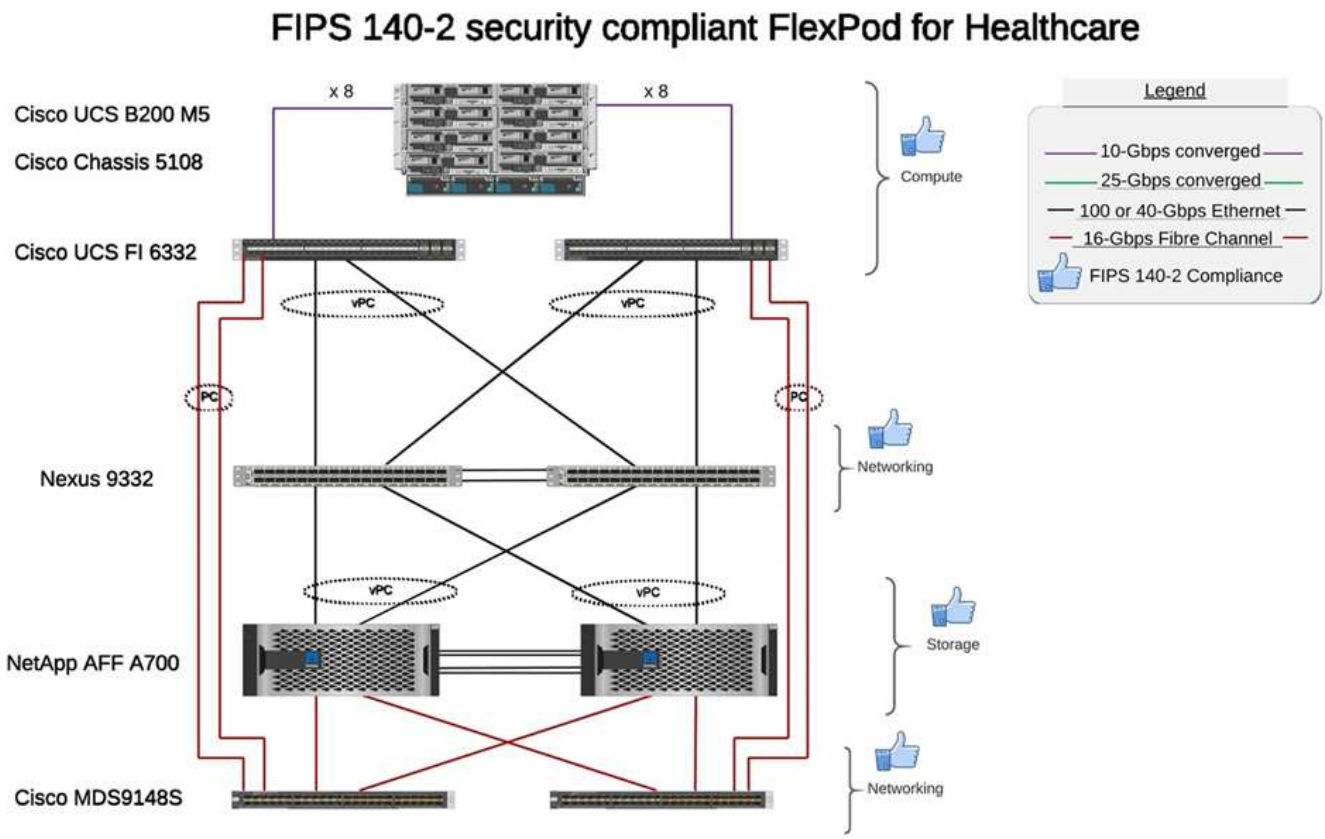
Vantaggi della soluzione dell'infrastruttura convergente FlexPod

"Precedente: Storage NetApp ONTAP FlexPod e FIPS 140-2."

Le organizzazioni del settore sanitario dispongono di diversi sistemi mission-critical. Due dei sistemi più critici sono i sistemi di cartelle cliniche elettroniche (EHR) e i sistemi di imaging medicale. Per dimostrare la configurazione FIPS su un sistema FlexPod, abbiamo utilizzato un EHR open-source e un sistema di archiviazione e comunicazione delle immagini open-source (PACS) per la configurazione del laboratorio e la convalida del carico di lavoro sul sistema FlexPod. Per un elenco completo delle funzionalità EHR, dei componenti dell'applicazione logica EHR e dei vantaggi dei sistemi EHR implementati su un sistema FlexPod, vedere "TR-4881: FlexPod per i sistemi di cartella clinica elettronica". Per un elenco completo delle funzionalità di un sistema di imaging medicale, dei componenti applicativi logici e dei vantaggi offerti dai sistemi di imaging medicale implementati su FlexPod, vedere "TR-4865: FlexPod per l'imaging medicale".

Durante la configurazione FIPS e la convalida del carico di lavoro, abbiamo esercitato caratteristiche di carico di lavoro che erano rappresentative di una tipica organizzazione sanitaria. Ad esempio, abbiamo utilizzato un sistema EHR open-source per includere scenari di modifica e accesso ai dati dei pazienti realistici. Inoltre, abbiamo esercitato carichi di lavoro di imaging medico che includevano imaging digitale e oggetti di comunicazione in medicina (DICOM) in un `*. dcm` formato del file. Gli oggetti DICOM con metadati sono stati memorizzati sia nel file che nello storage a blocchi. Inoltre, abbiamo implementato funzionalità di multipathing all'interno di un server RedHat Enterprise Linux (RHEL) virtualizzato. Abbiamo memorizzato oggetti DICOM su NFS, montato LUN utilizzando iSCSI e montato LUN utilizzando FC. Durante la configurazione e la convalida FIPS, abbiamo osservato che l'infrastruttura convergente FlexPod ha superato le nostre aspettative e ha ottenuto risultati senza problemi.

La figura seguente mostra il sistema FlexPod utilizzato per la configurazione e la convalida FIPS. Abbiamo sfruttato "Data center FlexPod con VMware vSphere 7.0 e NetApp ONTAP 9.7 Cisco Validated Design (CVD)" durante il processo di configurazione.



Componenti hardware e software dell'infrastruttura della soluzione

Le due figure seguenti elencano i componenti hardware e software rispettivamente utilizzati durante il test FIPS di abilitazione su un FlexPod. I consigli riportati in queste tabelle sono esempi; è necessario collaborare con il proprio SME NetApp per assicurarsi che i componenti siano adatti alla propria organizzazione. Inoltre, assicurarsi che i componenti e le versioni siano supportati in "Tool di matrice di interoperabilità NetApp" (IMT) e. "Cisco hardware Compatibility List (HCL) (elenco compatibilità hardware Cisco)".

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Calcolo	Chassis Cisco UCS 5108	1 o 2	
	Blade server Cisco UCS	3 B200 M5	Ciascuno con 2 core da 20 o più, 2,7 GHz e 128 GB di RAM
	Cisco UCS Virtual Interface Card (VIC)	Cisco UCS 1440	Vedere
	2 interconnessioni fabric Cisco UCS	6332	-
Rete	Switch Cisco Nexus	2 Cisco Nexus 9332	-
Rete di storage	Rete IP per l'accesso allo storage su protocolli SMB/CIFS, NFS o iSCSI	Stessi switch di rete come sopra	-
	Accesso allo storage tramite FC	2 Cisco MDS 9148S	-

Layer	Famiglia di prodotti	Quantità e modello	Dettagli
Storage	Sistema storage all-flash NetApp AFF A700	1 cluster	Cluster con due nodi
	Shelf di dischi	Uno shelf di dischi DS224C o NS224	Completamente popolato con 24 dischi
	SSD	Capacità superiore a 24, 1,2 TB	-

Software	Famiglia di prodotti	Versione o release	Dettagli
Vari	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bit)	-
	NetApp ONTAP	ONTAP 9.7 o versione successiva	-
	Cisco UCS Fabric Interconnect	Cisco UCS Manager 4.1 o versione successiva	-
	Switch Cisco Ethernet serie 3000 o 9000	Per la serie 9000, 7.0(3)I7(7) o versioni successive per la serie 3000, 9.2(4) o versioni successive	-
	Cisco FC: Cisco MDS 9132T	8.4(1a) o successiva	-
	Hypervisor	VMware vSphere ESXi 6.7 U2 o versione successiva	-
Storage	Sistema di gestione dell'hypervisor	VMware vCenter Server 6.7 U3 (vCSA) o versione successiva	-
Rete	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	-
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	-
	Cisco UCS Manager	4.1(1c) o versione successiva	
Hypervisor	ESXi		
Gestione	Sistema di gestione dell'hypervisor VMware vCenter Server 6.7 U3 (vCSA) o versione successiva		
	NetApp Virtual Storage Console (VSC)	VSC 9.7 o versione successiva	

Software	Famiglia di prodotti	Versione o release	Dettagli
	NetApp SnapCenter	SnapCenter 4.3 o versione successiva	
	Cisco UCS Manager	4.1(1c) o versione successiva	

"Avanti: Ulteriori considerazioni sulla sicurezza di FlexPod."

Ulteriori considerazioni sulla sicurezza di FlexPod

"Precedente: Vantaggi della soluzione dell'infrastruttura convergente FlexPod."

L'infrastruttura FlexPod è una piattaforma modulare, convergente, facoltativamente virtualizzata, scalabile (scale-out e scale-up) e conveniente. Con la piattaforma FlexPod, puoi scalare in modo indipendente calcolo, rete e storage per accelerare l'implementazione delle applicazioni. Inoltre, l'architettura modulare consente operazioni senza interruzioni anche durante le attività di scale-out e upgrade del sistema.

I diversi componenti di un sistema HIT richiedono l'archiviazione dei dati nei file system SMB/CIFS, NFS, Ext4 e NTFS. Questo requisito significa che l'infrastruttura deve fornire l'accesso ai dati sui protocolli NFS, CIFS e SAN. Un singolo sistema storage NetApp è in grado di supportare tutti questi protocolli, eliminando la necessità di una pratica legacy di sistemi storage specifici del protocollo. Inoltre, un singolo sistema storage NetApp può supportare carichi di lavoro HIT multipli come EHR, PACS o VNA, genomica, VDI e altro ancora, con livelli di performance garantiti e configurabili.

Se implementato in un sistema FlexPod, HIT offre diversi vantaggi specifici per il settore sanitario. Il seguente elenco contiene una descrizione di alto livello di questi vantaggi:

- **Sicurezza FlexPod**. La sicurezza è alla base di un sistema FlexPod. Negli ultimi anni, il ransomware è diventato una minaccia. Ransomware è un tipo di malware basato sulla crittografia, l'utilizzo della crittografia per creare software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati. Per scoprire come la soluzione FlexPod aiuta a mitigare minacce come ransomware, consulta "TR-4802: La soluzione per il ransomware". Lo sono anche i componenti dell'infrastruttura FlexPod "Conforme a FIPS 140-2".
- * Cisco Intersight.* Cisco Intersight è una piattaforma innovativa, basata sul cloud e di gestione come servizio che offre un singolo pannello di controllo per la gestione e l'orchestrazione di FlexPod full-stack. La piattaforma Intersight utilizza moduli crittografici conformi alla sicurezza FIPS 140-2. L'architettura di gestione out-of-band della piattaforma lo rende fuori ambito per alcuni standard o audit come HIPAA. Nessuna informazione personale identificabile sulla salute sulla rete viene mai inviata al portale Intersight.
- **Tecnologia NetApp FPolicy.** NetApp FPolicy (un'evoluzione della policy del file dei nomi) è un framework di notifica di accesso ai file per il monitoraggio e la gestione dell'accesso ai file tramite i protocolli NFS o SMB/CIFS. Questa tecnologia fa parte del software per la gestione dei dati ONTAP da oltre un decennio ed è utile per rilevare ransomware. Questo motore Zero Trust offre misure di sicurezza aggiuntive oltre alle autorizzazioni negli elenchi di controllo degli accessi (ACL). FPolicy prevede due modalità operative: Nativa ed esterna:
    - La modalità nativa offre sia la blacklist che la whitelisting delle estensioni di file.
    - La modalità esterna ha le stesse funzionalità della modalità nativa, ma si integra anche con un server FPolicy che viene eseguito esternamente al sistema ONTAP e con un sistema SIEM (Security Information and Event Management). Per ulteriori informazioni su come combattere il ransomware,

consultare "Combattere il ransomware: Terza parte – ONTAP FPolicy, un altro potente strumento nativo (alias gratuito)" blog.

- **Dati inattivi**. ONTAP 9 e versioni successive dispongono di tre soluzioni di crittografia dei dati a riposo conformi a FIPS 140-2:
  - NSE è una soluzione hardware che utilizza dischi con crittografia automatica.
  - NVE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con una chiave univoca per ciascun volume.
  - NAE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con chiavi univoche per ciascun aggregato.

> A partire da ONTAP 9.7, NAE e NVE sono attivati per impostazione predefinita se è attivo il pacchetto di licenza NVE di NetApp con il nome VE.

- **Dati in volo**. A partire da ONTAP 9.8, IPSec (Internet Protocol Security) fornisce il supporto della crittografia end-to-end per tutto il traffico IP tra un client e una SVM ONTAP. La crittografia dei dati IPSec per tutto il traffico IP include i protocolli NFS, iSCSI e SMB/CIFS. IPSec fornisce l'unica opzione di crittografia in volo per il traffico iSCSI.
- **Crittografia dei dati end-to-end su un data fabric ibrido multicloud**. I clienti che utilizzano tecnologie di crittografia dei dati a riposo come NSE o NVE e la crittografia del peering dei cluster (CPE) per il traffico di replica dei dati possono ora utilizzare la crittografia end-to-end tra client e storage nel data fabric multicloud ibrido eseguendo l'aggiornamento a ONTAP 9.8 o versione successiva e utilizzando IPSec. A partire da ONTAP 9, è possibile attivare la modalità di conformità FIPS 140-2 per le interfacce del piano di controllo a livello di cluster. Per impostazione predefinita, la modalità solo FIPS 140-2 è disattivata. A partire da ONTAP 9.6, CPE fornisce il supporto della crittografia TLS 1.2 AES-256 GCM per le funzionalità di replica dei dati ONTAP, come NetApp SnapMirror, NetApp SnapVault e le tecnologie NetApp FlexCache. La crittografia viene impostata tramite una chiave precondivisa (PSK) tra due peer del cluster.
- **Multitenancy sicura**. Supporta le crescenti esigenze di infrastruttura condivisa di storage e server virtualizzati, consentendo la multi-tenancy sicura di informazioni specifiche della struttura, in particolare quando si ospitano più istanze di database e software.

"Prossimo: Conclusione."

Conclusione

"Precedente: Ulteriori considerazioni sulla sicurezza di FlexPod."

Eseguendo la tua applicazione per il settore sanitario su una piattaforma FlexPod, la tua organizzazione sanitaria è meglio protetta da una piattaforma abilitata per FIPS 140-2. FlexPod offre una protezione multilivello per ogni singolo componente: Calcolo, rete e storage. Le funzionalità di protezione dei dati di FlexPod proteggono i dati a riposo o in volo e mantengono i backup sicuri e pronti quando necessario.

Evita gli errori umani sfruttando i design pre-validati di FlexPod che sono infrastrutture convergenti rigorosamente testate dalla partnership strategica di Cisco e NetApp. Un sistema FlexPod progettato e progettato per offrire performance di sistema prevedibili e a bassa latenza e alta disponibilità con un impatto minimo, anche quando FIPS 140-2 è abilitato nei livelli di calcolo, networking e storage. Questo approccio offre un'esperienza utente superiore e tempi di risposta ottimali per gli utenti del sistema HIT.

"Pagina successiva: Riconoscimenti, cronologia delle versioni e informazioni aggiuntive."

Riconoscimenti, cronologia delle versioni e dove trovare ulteriori informazioni

"Precedente: Conclusione."

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

- Guida alla configurazione della sicurezza NX-OS della famiglia Cisco MDS 9000

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- NetApp e la pubblicazione FIPS (Federal Information Processing Standard) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- Guida al rafforzamento di NetApp ONTAP 9

  https://www.netapp.com/us/media/tr-4569.pdf

- NetApp Encryption Power Guide

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Scheda informativa su NVE e NAE

  https://www.netapp.com/us/media/ds-3899.pdf

- Scheda informativa NSE

  https://www.netapp.com/us/media/ds-3213-en.pdf

- Centro documentazione di ONTAP 9

  http://docs.netapp.com

- NetApp e la pubblicazione FIPS (Federal Information Processing Standard) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Conformità Cisco e FIPS 140-2

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- NetApp Cryptographic Security Module

https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Procedure di cybersecuryper le organizzazioni sanitarie di medie e grandi dimensioni

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Cisco e il programma CMVP (Cryptographic Module Validation Program)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- NetApp Storage Encryption, NVMe Self-Encrypting Drive, NetApp Volume Encryption e NetApp aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- NetApp Volume Encryption e NetApp aggregate Encryption

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Crittografia dello storage NetApp

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod per sistemi di cartella clinica elettronica

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Data Now: Miglioramento delle performance negli ambienti Epic EHR con la tecnologia flash connessa al cloud

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Data center FlexPod per l'infrastruttura EHR Epic

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Guida all'implementazione di FlexPod Datacenter per Epic EHR

  https://www.netapp.com/media/10658-tr-4693.pdf

- Infrastruttura del data center FlexPod per il software MEDITECH

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- Lo standard FlexPod si estende al software MEDITECH

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- Guida al dimensionamento direzionale di FlexPod per MEDITECH

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod per imaging medicale

https://www.netapp.com/media/19793-tr-4865.pdf

- Ai nel settore sanitario

  https://www.netapp.com/us/media/na-369.pdf

- FlexPod per il settore sanitario semplifica la tua trasformazione

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod di Cisco e NetApp

  https://flexpod.com/

Ringraziamenti

- Abhinav Singh, Technical Marketing Engineer, NetApp
- Brian o'Mahony, Solution Architect Healthcare (Epic), NetApp
- Brian Pruitt, Pursuit Business Development Manager, NetApp
- Arvind Ramakrishnan, Senior Solutions Architect, NetApp
- Michael Hommer, FlexPod Global Field CTO, NetApp

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Aprile 2021	Release iniziale

Cisco Intersight con lo storage NetApp ONTAP

Cisco Intersight con NetApp Storage Quick Start Guide

In collaborazione con:

Introduzione

NetApp e Cisco hanno collaborato per fornire Cisco Intersight, una vista a singolo pannello dell'ecosistema FlexPod. Questa integrazione semplificata crea una piattaforma di gestione unificata per tutti i componenti dell'infrastruttura FlexPod e della soluzione FlexPod. Cisco Intersight consente di monitorare lo storage NetApp, il calcolo Cisco e l'inventario VMware. Consente inoltre di orchestrare o automatizzare i flussi di lavoro per eseguire le attività di storage e virtualizzazione in tandem.

Informazioni correlate

Per ulteriori informazioni, consulta i seguenti documenti e siti Web:

"TR 4883: Data center FlexPod con ONTAP 9.8, connettore storage ONTAP per Cisco Intersight e modalità gestita Cisco Intersight"

"Centro di assistenza Cisco Intersight"

"Panoramica introduttiva di Cisco Intersight"

"Guida all'installazione e all'aggiornamento di Intersight Appliance"

Novità

Questa sezione elenca le nuove funzionalità e funzionalità disponibili per Cisco Intersight con lo storage NetApp ONTAP.

Gennaio 2024

- Orchestrazione dello storage di NetApp tramite workflow di riferimento ora disponibili per il download in GitHub attraverso il "Repository del flusso di lavoro Intersight FlexPod". Per ulteriori informazioni sui nuovi flussi di lavoro di riferimento in GitHub, vedere "Caso d'utilizzo 2: Orchestrazione dello storage NetApp con flussi di lavoro di riferimento".

Novembre 2023

- È stata aggiunta la pagina NVMe Namespaces nella sezione Inventory dell'interfaccia utente.

Agosto 2023

È necessario un aggiornamento a NetApp Active IQ Unified Manager 9.13GA per garantire compatibilità e funzionalità complete con la versione più recente.

- È stata migliorata l'attività Nuova LUN smart NetApp per indicare chiaramente la disponibilità di opzioni di selezione per la creazione di un nuovo gruppo iniziatore o la selezione di un gruppo iniziatore esistente. Quando gli utenti ora selezionano la casella per creare un nuovo gruppo iniziatore, il parametro per la scelta di un gruppo iniziatore esistente non è più disponibile. Se gli utenti deselezionano la casella per creare un nuovo gruppo iniziatore, il parametro gruppo iniziatore esistente diventa disponibile.
- Miglioramento delle attività Nuova mappa LUN NetApp e Rimozione mappa LUN NetApp. La nuova relazione tra il LUN e il gruppo iniziatore è ora aggiornata. L'inventario dell'interfaccia utente viene aggiornato immediatamente per il LUN e il gruppo iniziatore all'esecuzione dell'attività.
- La pagina Controlla ora carica correttamente la prima volta che gli utenti accedono e non richiede più un aggiornamento.

Luglio 2023

> È necessario un aggiornamento a NetApp Active IQ Unified Manager 9.13GA per garantire compatibilità e funzionalità complete con la versione più recente.

- Nomi aggiornati per le attività di storage NetApp. Per un elenco completo delle attività rinominate, vedere caso d'utilizzo 3 flussi di lavoro personalizzati utilizzando un modulo senza designer.
- L'indirizzo IP dell'interfaccia NFS è stato aggiunto come output del task nuovo volume smart NAS NetApp.
- Un controllo che il trasporto ASUP sia HTTPS è stato aggiunto alla scheda Verifiche.
- Il tipo di Tier corretto per tutti i Tier viene ora visualizzato correttamente nell'interfaccia utente dei Tier.
- Tutte le licenze conformi vengono ora visualizzate correttamente nella pagina Licenses (licenze).
- Nella pagina delle condivisioni viene ora visualizzato un valore preciso per le condivisioni CIFS senza o senza home directory.
- L'ordinamento e il filtraggio sono ora abilitati per la colonna mappata nella pagina LUN.
- L'ordinamento e il filtraggio hanno attivato la colonna Authentication Enabled (autenticazione abilitata) nella pagina NTP Servers (Server NTP).
- Aggiunti nuovi controlli e le seguenti categorie corrispondenti alla scheda Verifiche.
  - Sicurezza
  - Anti-ransomware
  - Disponibilità
  - Altro
- Nella vista Dettagli inventario, viene ora utilizzato il report invece della capacità fisica utilizzata.

Giugno 2023

> È necessario un aggiornamento a NetApp Active IQ Unified Manager 9.13RC1 per garantire compatibilità e funzionalità complete con la versione più recente.

- Nomi aggiornati per le attività di storage NetApp. Vedere "USA i flussi di lavoro personalizzati del caso 3 utilizzando un modulo senza designer" per l'elenco completo delle attività rinominate.

Aprile 2023

- Aggiunte le schede Criteri di protezione (SnapMirror) e Criteri Snapshot nella pagina Criteri all'interno della sezione inventario dell'interfaccia utente.

- Aggiunta della pagina Client NFS nella sezione Inventory dell'interfaccia utente.
- Aggiunta della colonna Protected (protetto) nella pagina Storage VMS nella sezione Inventory (inventario) dell'interfaccia utente.
- Modificato il modo in cui le informazioni sulla riduzione dei dati vengono riportate e visualizzate.
- Aggiunte le schede Local Tier (livello locale) e Cloud Tier (livello cloud) nella pagina Tier (livelli) nella sezione Inventory (inventario) dell'interfaccia utente.
- La colonna Node (nodo) viene visualizzata dopo la colonna Name (Nome) nella pagina Ports (Porte) nella sezione Inventory (inventario) dell'interfaccia utente.

Gennaio 2023

> È necessario un aggiornamento a NetApp Active IQ Unified Manager 9.12 GA per garantire compatibilità e funzionalità complete con la versione più recente. Per un elenco dei problemi noti relativi a questa versione, vedere Problemi noti.

- I controlli di interoperabilità di Intersight possono ora distinguere tra le modalità firmware UCSM e IMM durante i controlli di compatibilità.
- Le relazioni di protezione non verranno visualizzate in Intersight per ONTAP 9.7. Questo problema è stato risolto in ONTAP 9.8RC1.

Agosto 2022

> È necessario un aggiornamento a NetApp Active IQ Unified Manager 9.11 GA per garantire compatibilità e funzionalità complete con la versione più recente. Per un elenco dei problemi noti relativi a questa versione, vedere Problemi noti.

- Aggiornato il calcolo della capacità disponibile del cluster in modo che corrisponda a System Manager
- Aggiornata la pagina Generale del cluster per nascondere il riepilogo delle metriche delle performance fino a quando i dati delle performance non vengono compilati
- Risolto il problema dell'interfaccia utente della pagina Generale del cluster che causava occasionalmente il blocco della pagina
- Aggiunte condivisioni CIFS, servizi CIFS, Qtree e policy SnapMirror SVM all'inventario back-end.
- Aggiunte condivisioni e Qtree al menu di navigazione dell'interfaccia utente nella sezione inventario logico
- Aggiunte condivisioni come scheda da una Storage VM selezionata
- Sono state aggiunte informazioni sul servizio CIFS nella scheda Storage VM General (Generale Storage VM) se Storage VM è abilitato CIFS
- È stata aggiunta una pagina di controllo del cluster che consente agli utenti di convalidare la configurazione dei sistemi storage NetApp in base alle Best practice

Luglio 2022

- Videografica migliorata per il rapporto di riduzione dei dati del cluster ora disponibile nel Capacity Widget
- Aggiunta della scheda FC Interfaces (interfacce FC) alla pagina Network Interfaces (interfacce di rete)
- La creazione di un nuovo volume utilizzando l'attività generica "nuovo volume di storage" ora imposta la garanzia dello spazio su nessuno e la percentuale di riserva di snapshot su 0%

- Il campo Commento sotto l'attività Edit Snapshot Policy (Modifica policy snapshot) è ora facoltativo e non più obbligatorio
- Miglioramento dell'inventario dell'interfaccia utente e della coerenza di orchestrazione
- Le informazioni sulla capacità di Intersight in Cluster Capacity sono ora coerenti con System Manager
- Aggiunta la casella di controllo sotto l'attività New Storage Virtual Machine per visualizzare tutti i parametri durante la creazione di una nuova interfaccia di gestione per migliorare l'usabilità
- Spostamento dei protocolli sotto Client Match, ora coerente con System Manager
- Pagina generale delle policy di esportazione che ora visualizza i protocolli di accesso
- rimozione igroup ora registrata in modo condizionale
- Aggiunta dei parametri "failover Policy" e "autorevert" per NAS in New Storage NAS Data Interface e New Storage iSCSI Data Interface
- Il rollback per l'attività New Storage NAS Smart Volume ora rimuove la policy di esportazione se non sono collegati altri volumi
- Miglioramenti apportati per le attività Smart Volume e Smart LUN

Aprile 2022

> Per garantire compatibilità e funzionalità complete con le versioni future, si consiglia di aggiornare NetApp Active IQ Unified Manager alla versione 9.10P1.

- Aggiunta della pagina Broadcast Domain to Ethernet Port Detail
- Modificato il termine "aggregato" in "Tier" per l'aggregato e SVM all'interno dell'interfaccia utente
- Modifica del termine "Cluster Status" in "Array Status" (Stato array)
- Il filtro MTU ora funziona per i caratteri <,>,=,⇐,>=
- Aggiunta della pagina dell'interfaccia di rete all'inventario del cluster
- Aggiunta di AutoSupport all'inventario del cluster
- Aggiunto `cdpd.enable` opzione al nodo
- Aggiunto un oggetto per CDP neighbor
- Aggiunta delle attività di storage per il workflow NetApp all'interno di Cisco Intersight. Vedere "USA i flussi di lavoro personalizzati del caso 3 utilizzando un modulo senza designer" Per un elenco completo delle attività di storage NetApp.

Gennaio 2022

- Aggiunta di allarmi di interoperabilità basati su eventi per NetApp Active IQ Unified Manager 9.10 o versioni successive.

> Per garantire compatibilità e funzionalità complete con le versioni future, si consiglia di aggiornare NetApp Active IQ Unified Manager alla versione 9.10.

- Impostare esplicitamente ciascun protocollo abilitato (vero o falso) per Storage Virtual Machine
- Stato ClusterHealthStatus mappato ok-with-suppressed su OK
- Colonna Health rinominata nella colonna Cluster Status (Stato cluster) nella pagina Cluster list (elenco cluster)

- Visualizzazione dell'array di storage "Unreachable" (irraggiungibile) se il cluster non è attivo o altrimenti irraggiungibile
- Colonna Health rinominata in colonna Array Status (Stato array) nella pagina Cluster General (Generale cluster)
- SVM dispone ora di una scheda "Volumes" (volumi) che mostra tutti i volumi per SVM
- Il volume ha una sezione di capacità di snapshot
- Le licenze ora vengono visualizzate correttamente

Ottobre 2021

- Elenco aggiornato delle attività di storage NetApp disponibili in Cisco Intersight. Vedere "USA i flussi di lavoro personalizzati del caso 3 utilizzando un modulo senza designer" Per un elenco completo delle attività di storage NetApp.
- Aggiunta della colonna Health nella pagina Cluster list (elenco cluster).
- Ulteriori dettagli sono ora disponibili nella pagina Generale per un cluster selezionato.
- La tabella Server NTP è ora accessibile dal riquadro di navigazione.
- È stata aggiunta una nuova scheda Sensors contenente la pagina General (Generale) della Storage Virtual Machine.
- Il riepilogo dei gruppi di aggregazione di collegamenti e VLAN è ora disponibile nella pagina Port General (Generale porta).
- Aggiunta della colonna capacità totale dei dati nella tabella capacità totale del volume.
- Le colonne latenza, IOPS e throughput sono state aggiunte nelle tabelle Average Volume Statistics, Average LUN Statistics, Average aggregate Statistics, Average Storage VM Statistics e Average Node Statistics

> Le suddette metriche delle performance sono disponibili solo per gli storage array monitorati tramite NetApp Active IQ Unified Manager 9.9 o superiore.

Problemi noti

- Se si utilizza una versione di AIQUM 9.11 o precedente, si verificherà una discrepanza tra i valori visualizzati nella pagina Storage List (elenco di storage) e il grafico a barre della capacità nella pagina Storage General (Generale archiviazione). Per risolvere questo problema, eseguire l'aggiornamento a AIQUM 9.12 o superiore per garantire la precisione dei valori di capacità visualizzati.
- Se si utilizza AIQUM 9.11 o una versione precedente, qualsiasi verifica eseguita dalla scheda "interoperabilità" nella pagina "sistemi integrati" non consente di distinguere accuratamente i componenti Cisco di IMM e UCSM. Per risolvere questo problema, eseguire l'aggiornamento a AIQUM 9.12 per assicurarsi che tutti i componenti siano identificati correttamente.
- Per garantire che i dati di inventario dello storage Intersight non vengano influenzati durante il processo di raccolta dei dati, tutti i cluster ONTAP non supportati (ad esempio, versioni inferiori a ONTAP 9.7P1) devono essere rimossi da Active IQ Unified Manager (AIQM).
- Tutti i target richiesti richiedono una versione AIQUM minima di 9.11 per il completamento corretto delle query di interoperabilità del sistema integrato FlexPod.
- La pagina Storage Inventory Checks (controlli dell'inventario dello storage) non viene compilata se il cluster ONTAP viene aggiunto ad AIQUM utilizzando un FQDN. Gli utenti devono aggiungere cluster ONTAP ad AIQUM utilizzando un indirizzo IP.

Requisiti

Verifica di soddisfare i requisiti di hardware, software e licenze per l'integrazione dello storage NetApp ONTAP con Cisco Intersight.

Requisiti hardware e software

Questi sono i componenti hardware e software minimi necessari per implementare la soluzione. I componenti utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Componente	Dettagli dei requisiti
NetApp ONTAP	ONTAP 9.7P1 e versioni successive
NetApp Active IQ Unified Manager	È richiesta l'ultima versione di NetApp Active IQ Unified Manager (attualmente 9.14RC1)
Storage array NetApp	Tutti gli storage array ONTAP ASA, AFF e FAS supportati per ONTAP 9.7P1 e versioni successive
Hypervisor per la virtualizzazione	VSphere 7,0 e versioni successive

Fare riferimento a. "Sistemi supportati da Cisco Intersight" Per i requisiti minimi di Cisco UCS Compute Components e della versione di UCSM.

Requisiti di licenza di Cisco Intersight

Cisco Intersight offre servizi come Servizio dell'infrastruttura e Servizio orchestratore cloud per gestire, automatizzare e ottimizzare lo storage fisico (storage NetApp). Puoi utilizzare questi servizi per gestire il server Cisco UCS e il sistema Cisco HyperFlex. Il servizio Infrastructure Service e Cloud Orchestrator utilizzano un modello di licenza basato su abbonamento con diversi Tier. Puoi scegliere il Tier di volume Cisco UCS Server richiesto per il termine di iscrizione selezionato.

Modello di licenza

Il modello di licenza di Cisco Intersight Infrastructure Services è stato semplificato e ora offre i seguenti due livelli:

- **Cisco Intersight Infrastructure Services Essentials** - il livello di licenza Essentials offre la gestione dei server, tra cui funzionalità di monitoraggio dello stato globale, inventario, supporto proattivo tramite l'integrazione Cisco TAC, autenticazione a più fattori e accesso a SDK e API.
- **Cisco Intersight Infrastructure Services Advantage** - il livello di licenza Advantage offre una gestione avanzata dei server con visibilità estesa, integrazione dell'ecosistema, automazione di hardware e software Cisco e di terze parti, oltre a fornire soluzioni multi-dominio.

Per ulteriori informazioni sulle funzionalità coperte da diversi livelli di licenza, visitare il sito Web all'indirizzo "Licenza dei servizi di infrastruttura".

Prima di iniziare

Per monitorare e orchestrare lo storage NetApp da Cisco Intersight, è necessario che NetApp Active IQ Unified Manager e Cisco Intersight Assist Virtual Appliance siano installati nell'ambiente vCenter.

Installare o aggiornare NetApp Active IQ Unified Manager

Installare o aggiornare a Active IQ Unified Manager (è necessaria l'ultima versione, attualmente 9.14RC1) se non è stato fatto. Per istruzioni, consultare "Documentazione NetApp Active IQ Unified Manager".

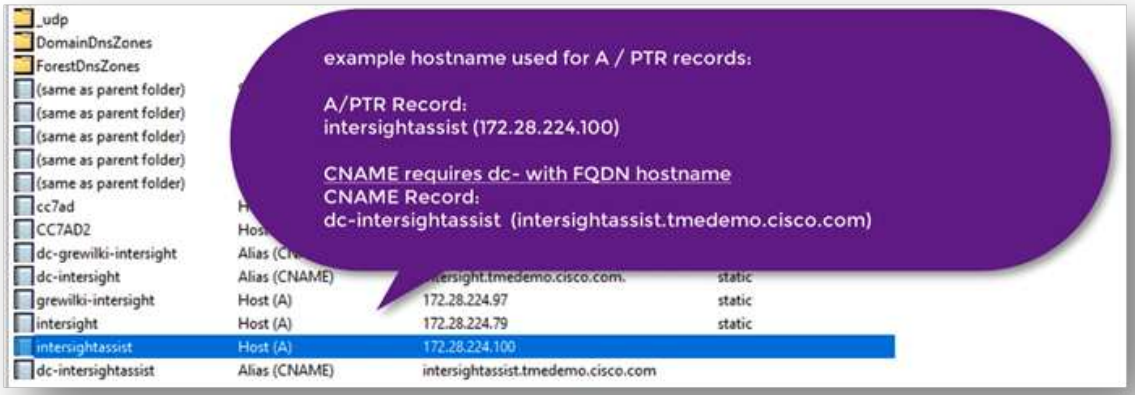
Installare l'appliance virtuale Cisco Intersight Assist

Assicurarsi di rispettare le "Requisiti di licenza, sistema e rete di Cisco Intersight Virtual Appliance".

Fasi

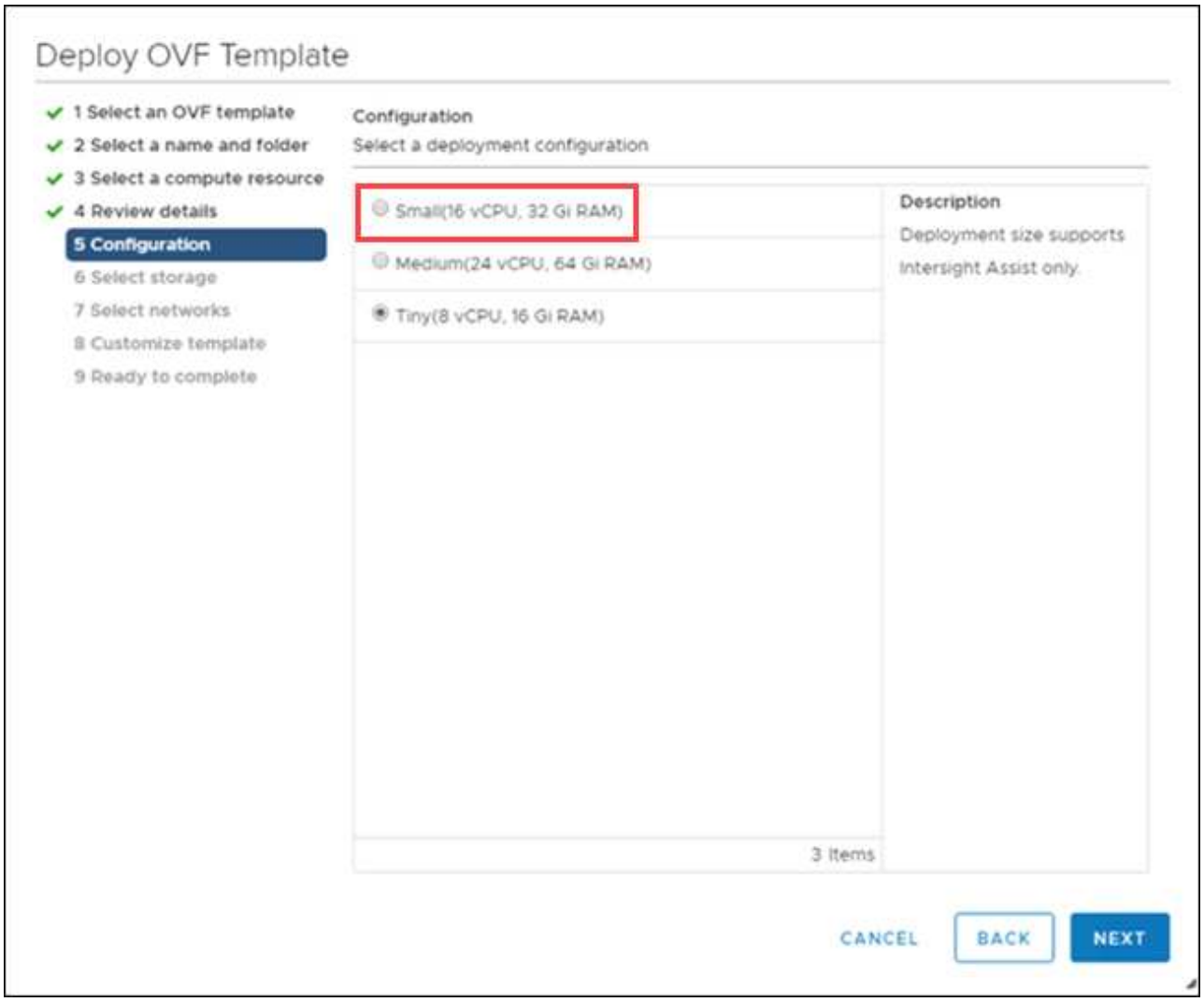
1. Creare un account Cisco Intersight. Visitare il sito "https://intersight.com/" Per creare il tuo account Intersight. Per creare un account Cisco Intersight, è necessario disporre di un ID Cisco valido.
2. Scarica Intersight Virtual Appliance all'indirizzo "software.cisco.com". Per ulteriori informazioni, consultare "Guida all'installazione e all'aggiornamento di Intersight Appliance".
3. Implementare OVA. DNS e NTP sono necessari per implementare OVA.

   a. Configurare DNS con Record a/PTR e CNAME Alias prima di implementare OVA. Vedere l'esempio riportato di seguito.

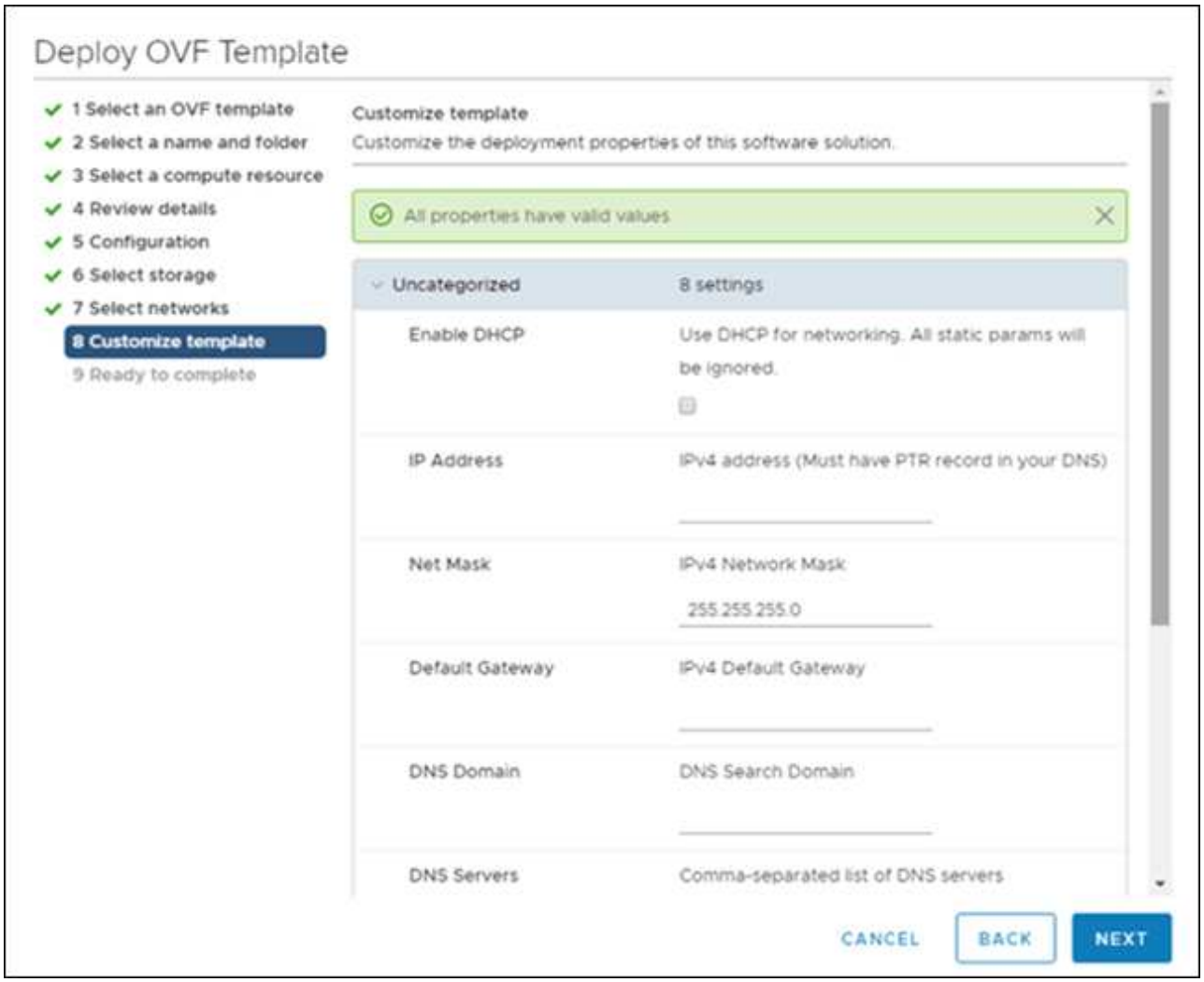


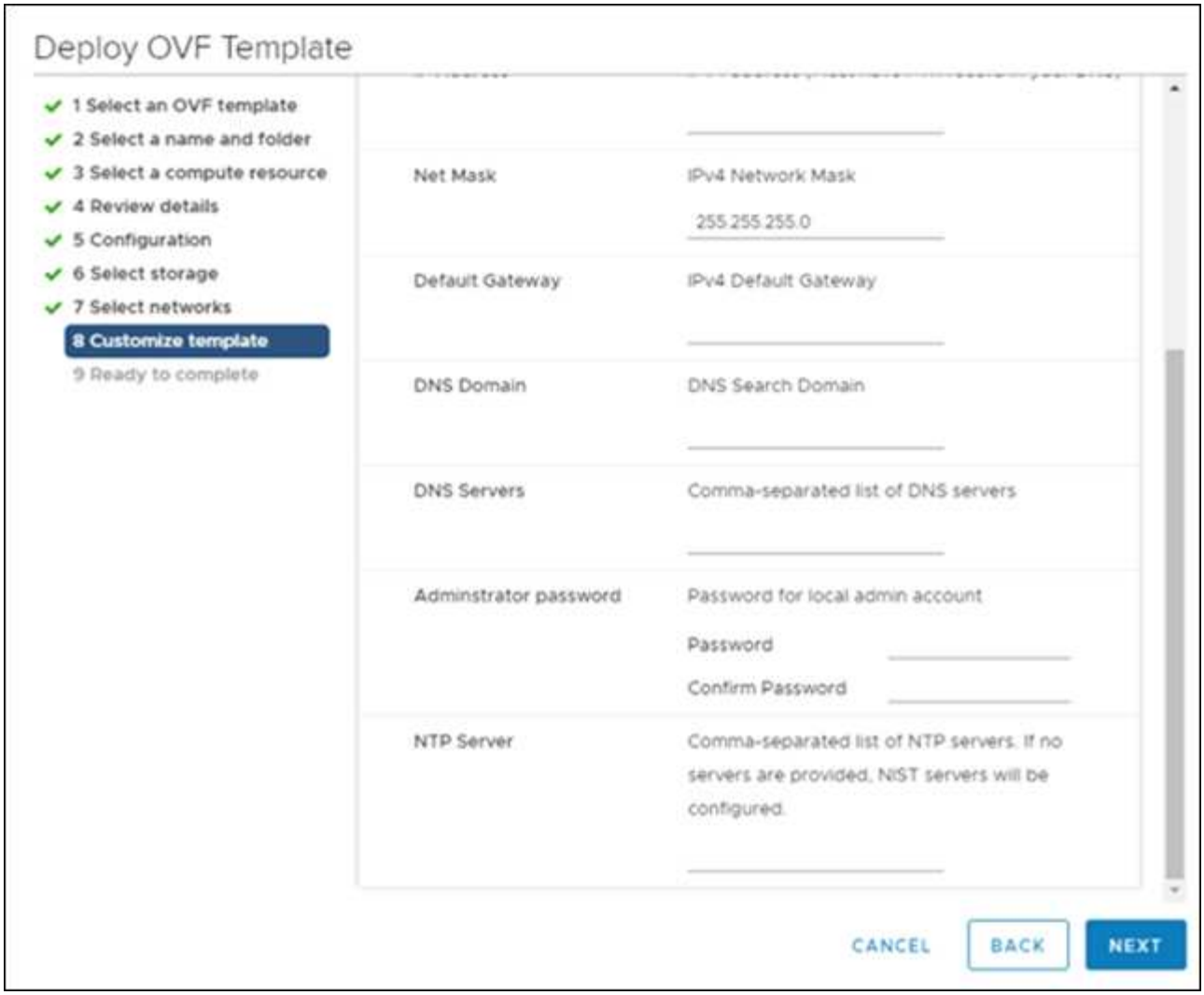
   b. Scegliere le dimensioni di configurazione appropriate (piccola, piccola o media) in base ai requisiti di implementazione OVA per Intersight Virtual Appliance.

      SUGGERIMENTO: per un cluster ONTAP a due nodi con un elevato numero di oggetti storage, NetApp consiglia di utilizzare l'opzione Small (16 vCPU, 32 Gi RAM).



c. Nella pagina **Personalizza modello**, personalizzare le proprietà di distribuzione del modello OVF. La password dell'amministratore viene utilizzata per gli utenti locali: admin(`webUI/cli/ssh`).


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Configuration
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Uncategorized
8 settings
Enable DHCP
Use DHCP for networking. All static params will be ignored.
IP Address
IPv4 address (Must have PTR record in your DNS)
Net Mask
IPv4 Network Mask
255.255.255.0
Default Gateway
IPv4 Default Gateway
DNS Domain
DNS Search Domain
DNS Servers
Comma-separated list of DNS servers
CANCEL
BACK
NEXT



a. Fare clic su **Avanti**.

4. Post-implementazione dell'appliance Intersight Assist.

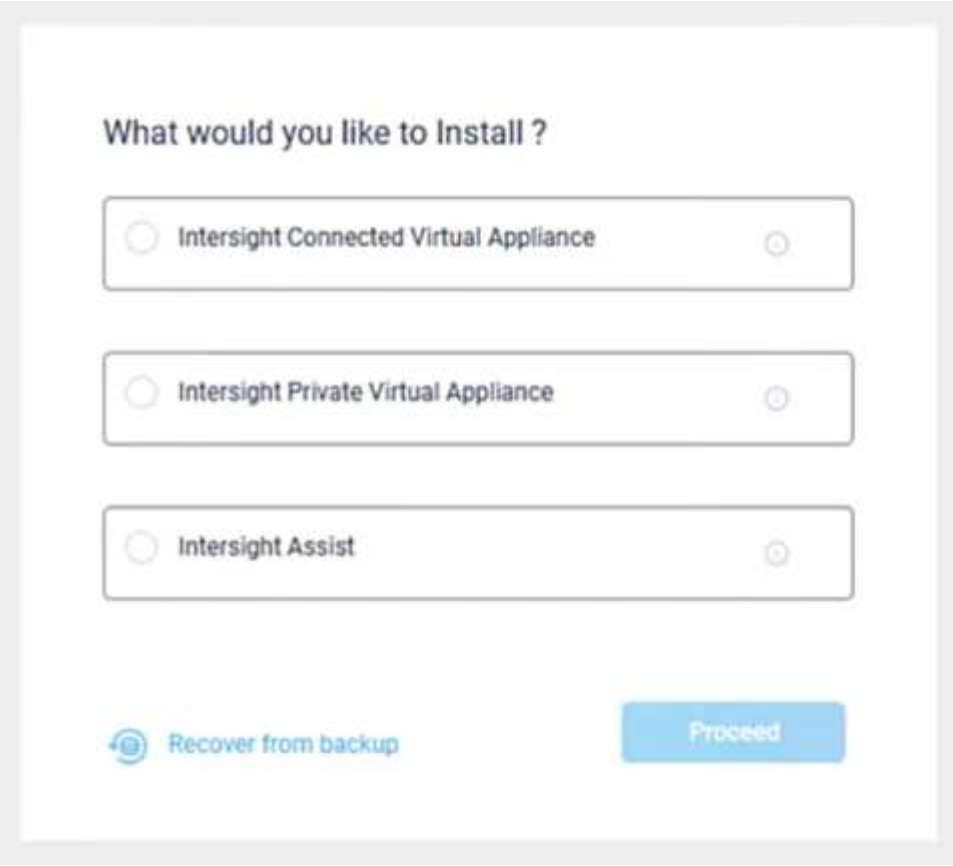
   a. Selezionare https://FQDN-of-your-appliance per completare la configurazione post-installazione dell'appliance.

      Il processo di installazione viene avviato automaticamente. L'installazione può richiedere fino a un'ora a seconda della larghezza di banda fino a Intersight.com. Dopo l'accensione della macchina virtuale, il sito sicuro può richiedere anche alcuni secondi.

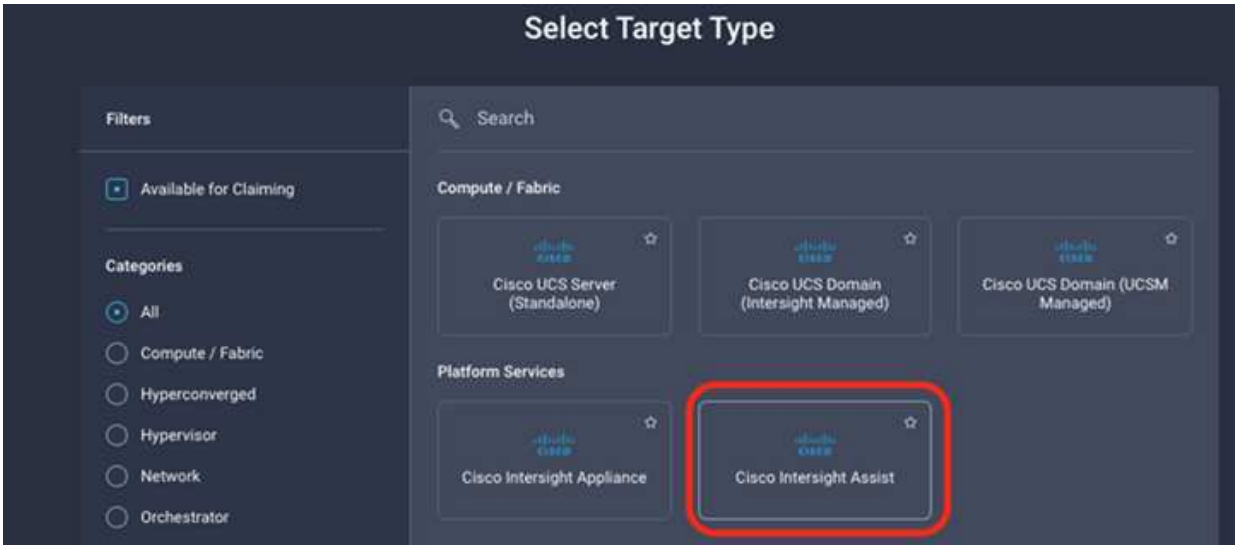
   b. Durante il processo di post-implementazione, selezionare la seguente opzione:

      - **Intersight Assist.** questa implementazione consente al modello SaaS di connettersi a Cisco Intersight.

> Quando si seleziona Intersight Assist, prendere nota dell'ID del dispositivo e del codice della richiesta di rimborso prima di continuare.



a. Fare clic su **Procedi**.
b. Selezionare **Intersight Assist** e completare la seguente procedura:
   i. Accedere all'account SaaS Intersight all'indirizzo "https://intersight.com".
   ii. Fare clic su **targets**, **Cisco Intersight Assist**, quindi su **Start**.
   iii. Richiedi l'appliance **Cisco Intersight Assist** copiando e incollando l'ID del dispositivo e il codice di richiesta dalla tua appliance virtuale Intersight Assist appena implementata.



   iv. Tornare all'appliance **Cisco Intersight Assist** e fare clic su **continua.** potrebbe essere necessario aggiornare il browser.

Viene avviato il processo di download e installazione. I file binari vengono trasferiti da Intersight Cloud all'appliance on-premise. Il tempo di completamento varia in base alla larghezza di banda di Intersight Cloud.

Configurare il server proxy AIQ UM per il servizio IMT

Se si utilizza un server proxy con AIQ UM per Cisco Intersight con lo storage NetApp ONTAP, è necessario configurare la configurazione tramite l'interfaccia a riga di comando (CLI) per utilizzare il servizio IMT (Interoperability Matrix Tool). Il servizio IMT è disponibile nella scheda **interoperabilità** della pagina **sistemi integrati**. Per configurare le impostazioni del server proxy AIQ UM, è necessario utilizzare la shell di diagnosi della macchina virtuale Active IQ Unified Manager.

> Per informazioni su come accedere alla shell AIQ UM Diag, vedere "Come accedere alla shell di DIAG della macchina virtuale Active IQ Unified Manager (OVA)"

Fasi

1. Accedere al terminale AIQ UM ed eseguire il seguente comando per accedere a um.

```
um cli login -u <um maintenance user name>
```

Esempio

```
um cli login -u admin
```

2. Impostare `imt_proxy_host` e. `imt_proxy_port` eseguendo i seguenti comandi.

> Il proxy IMT è una configurazione separata dalle configurazioni proxy ASUP (AutoSupport).

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

Esempio

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

> Le configurazioni del server proxy IMT non supportano l'autenticazione.

3. Visualizzare i dettagli del proxy IMT per verificare `proxy_host` e. `proxy_port` tramite il seguente comando.

```
um option list |grep imt
```

Obiettivi delle richieste di rimborso

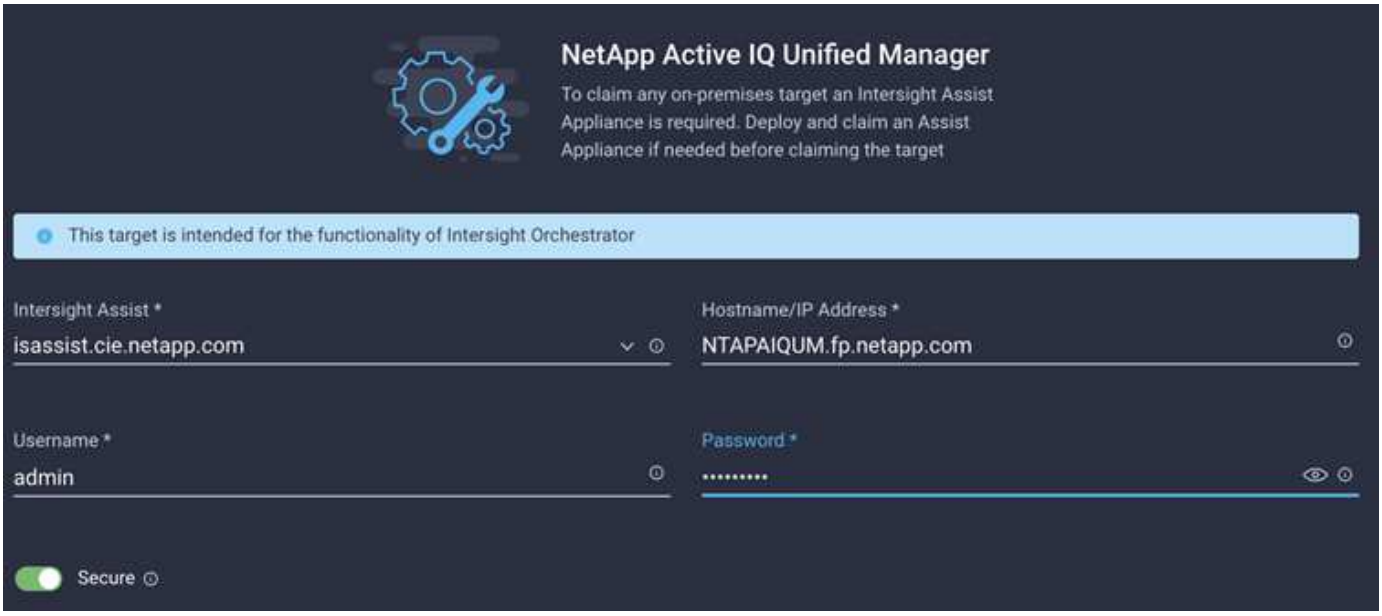
Una volta installato Cisco Intersight Assist, puoi richiedere i tuoi dispositivi di storage e virtualizzazione NetApp. Torna alla pagina **obiettivi dell'intervista** e Aggiungi i tuoi obiettivi vCenter e NetApp Active IQ Unified Manager. Per ulteriori informazioni sul processo di richiesta di rimborso, guarda il video "Richiedi un target tramite Cisco Intersight Assist."

> Assicurarsi che il gateway API di NetApp Active IQ Unified Manager (AIQ UM) sia attivato.

Da NetApp IQ Unified Manager, accedere a **Impostazioni > generali > Impostazioni delle funzioni**.

L'esempio seguente mostra il target NetApp AIQ UM richiesto da Cisco Intersight.

> Quando si rivendica la destinazione NetApp AIQ UM, tutti i cluster gestiti da Active IQ Unified Manager vengono aggiunti automaticamente a Intersight.

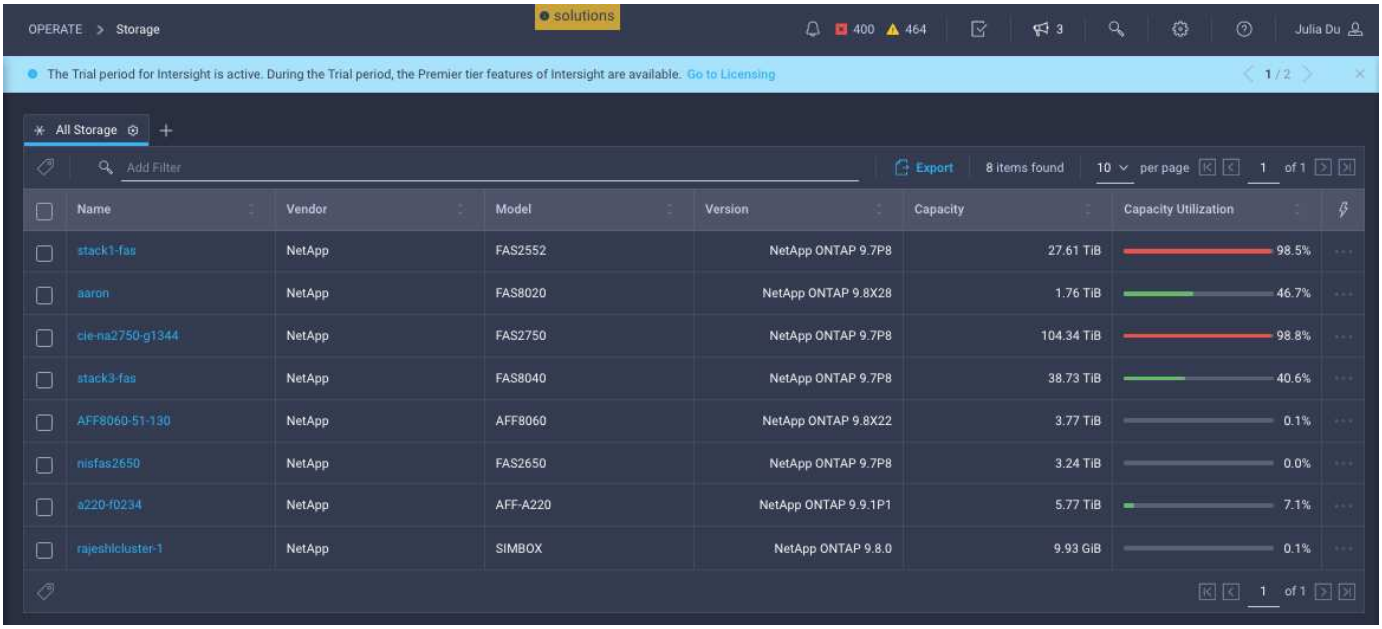


Monitorare lo storage NetApp da Cisco Intersight

Una volta rivendicati i target, i widget di storage NetApp, l'inventario dello storage e le schede di virtualizzazione diventano disponibili se si dispone di una licenza Advantage Tier. Le schede di orchestrazione sono disponibili se si dispone di una licenza Tier Premier.

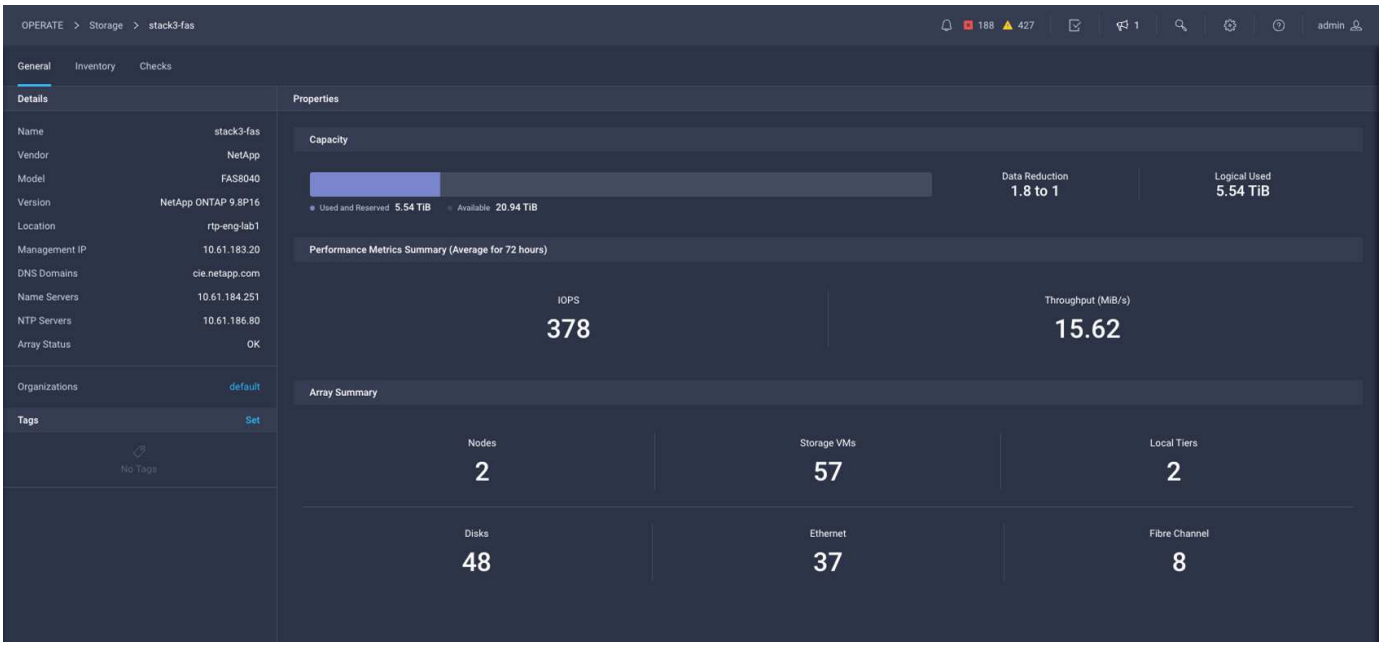
Panoramica dell'inventario dello storage

La seguente schermata visualizza la schermata **Operate > Storage** (funzionamento > archiviazione).



La seguente schermata mostra la panoramica del cluster di storage.

Le seguenti informazioni di riepilogo delle metriche di performance verranno visualizzate solo se lo storage array viene monitorato tramite NetApp Active IQ Unified Manager 9.9 o versione successiva.



Widget per lo storage

Per visualizzare i widget di storage, selezionare **Monitoring > Dashboards > View NetApp storage widgets** (monitoraggio > Dashboard > Visualizza widget di storage NetApp).

- La seguente schermata mostra il widget Storage Version Summary (Riepilogo versione storage).

- Questa schermata mostra il widget Top 5 Storage Array by Capacity Utilization.

Top 5 Storage Arrays by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	Warriors_Controller	NetApp	13.83 TiB	89.4%
2	stack3-fas	NetApp	8.95 TiB	66.2%
3	aaron	NetApp	4.71 TiB	44.1%
4	aff-a400	NetApp	40.62 TiB	0.2%

- Questa schermata mostra il widget Top 5 Storage Volumes by Capacity Utilization.

Top 5 Storage Volumes by Capacity Utilization

#	Name	Vendor	Capacity	Utilization
1	test_1_vol	NetApp	10.31 GiB	98.6%
2	test_lun_vol	NetApp	10.31 GiB	97.9%
3	vmware_server_1	NetApp	50.00 GiB	95.0%
4	vmware_server_2	NetApp	50.00 GiB	82.3%
5	VM_Datastore_vol	NetApp	150.00 GiB	67.0%

Casi di utilizzo

Questi sono alcuni esempi di casi di utilizzo per il monitoraggio e l'orchestrazione dello storage NetApp da Cisco Intersight.

Caso d'utilizzo 1: Monitoraggio dell'inventario e dei widget dello storage NetApp

Quando l'ambiente di storage NetApp è disponibile in Cisco Intersight, è possibile monitorare in dettaglio gli oggetti di storage NetApp dall'inventario dello storage e ottenere una panoramica dai widget di storage.

1. Implementazione di Intersight Assist OVA (task OnPrem in vCenter Environment).
2. Aggiungere i dispositivi NetApp AIQ UM in Intersight Assist.
3. Vai a **Storage** e naviga attraverso l'inventario dello storage NetApp.
4. Aggiungi **Widgets** per lo storage NetApp al tuo **Monitor Dashboard**.

   Ecco un "collegamento" Al video che mostra le funzionalità di monitoraggio dello storage NetApp ONTAP di Cisco Intersight.

Caso d'utilizzo 2: Orchestrazione dello storage NetApp con workflow di riferimento

Quando lo storage NetApp e gli ambienti vCenter sono disponibili in Cisco Intersight, puoi utilizzare i workflow di riferimento end-to-end disponibili in GitHub attraverso il "Repository del flusso di lavoro Intersight FlexPod".

I workflow di riferimento includono task di storage e virtualizzazione. Il file README per l'archivio fornisce i prerequisiti necessari per l'esecuzione dei flussi di lavoro, i collegamenti a risorse utili (inclusa la documentazione su come importare un flusso di lavoro) e i collegamenti alla documentazione per ogni flusso di lavoro di riferimento.

Ogni flusso di lavoro ha una cartella nell'archivio contenente due file:

- Il file JSON da scaricare e importare in Intersight,
- Un file di documentazione che fornisce una visualizzazione delle attività nel flusso di lavoro, input del flusso di lavoro e un esempio di esecuzione del flusso di lavoro.

Per importare e utilizzare un flusso di lavoro di riferimento, effettuare le seguenti operazioni:

1. Implementazione di Intersight Assist OVA (task OnPrem in vCenter Environment).
2. Aggiungere i dispositivi NetApp AIQ UM in Intersight Assist.
3. Aggiungere il target vCenter a Intersight tramite Intersight Assist.
4. Scarica il file JSON per un workflow di riferimento dal repository FlexPod-Intersight-Workflow.
5. Importare il flusso di lavoro in Intersight, quindi eseguire il flusso di lavoro.

Segue un elenco dei workflow disponibili nel repository FlexPod-Intersight-Workflow di GitHub:

- Aggiungere gli iniziatori al gruppo di iniziatori NetApp
- Nuova policy di esportazione per il volume NetApp
- Nuovo datastore NAS che utilizza il volume smart di NetApp
- Nuova interfaccia dati NetApp FC

- Nuovo gruppo iniziatore NetApp
- Nuova interfaccia dati iSCSI NetApp
- Nuova interfaccia dati NAS NetApp
- Nuova macchina virtuale per lo storage NetApp
- Nuovo datastore VMFS che utilizza NetApp Smart LUN
- Rimuovere gli iniziatori dal gruppo iniziatore NetApp
- Rimuovere il datastore NAS utilizzando il volume smart di NetApp
- Rimuovi policy di esportazione NetApp
- Rimuovere il gruppo iniziatore NetApp
- Rimuovere l'archivio dati VMFS utilizzando NetApp Smart LUN
- Aggiornare il datastore NAS utilizzando il volume smart di NetApp
- Aggiornare il datastore VMFS utilizzando NetApp Smart LUN

Caso d'utilizzo 3: Flussi di lavoro personalizzati utilizzando un modulo senza designer

Quando gli ambienti NetApp Storage e vCenter sono disponibili in Cisco Intersight, è possibile creare flussi di lavoro personalizzati utilizzando le attività di storage e virtualizzazione di NetApp.

1. Implementazione di Intersight Assist OVA (task OnPrem in ambiente vCenter)
2. Aggiungere i dispositivi NetApp AIQ UM in Intersight Assist.
3. Aggiungere il target vCenter a Intersight tramite Intersight Assist.
4. Accedere alla scheda **orchestrazione** in Intersight.
5. Selezionare **Crea flusso di lavoro**.
6. Aggiungi attività di storage e virtualizzazione ai tuoi flussi di lavoro.

   Di seguito sono riportate le attività di storage NetApp disponibili da Cisco Intersight:

   - Aggiungi ACL alla condivisione CIFS di NetApp
   - Aggiungi corrispondenza client alla regola dei criteri di esportazione NetApp
   - Aggiungi policy di esportazione al volume NetApp
   - Aggiungere gli iniziatori al gruppo di iniziatori NetApp
   - Aggiungi regola al criterio di esportazione NetApp
   - Aggiungi pianificazione alla policy di snapshot NetApp
   - Confermare lo stato della licenza NetApp
   - Confermare lo stato del protocollo FCP della macchina virtuale di storage NetApp
   - Modifica gli aggregati NetApp per la macchina virtuale di storage
   - Modifica policy NetApp asincrona SnapMirror
   - Modifica autorizzazione ACL condivisione CIFS NetApp
   - Modifica regola policy di esportazione NetApp
   - Modifica policy snapshot NetApp

- Modifica la pianificazione delle policy di Snapshot di NetApp
- Modifica lo stile di sicurezza del volume NetApp
- Modifica policy snapshot volume NetApp
- Abilitare i servizi CIFS di NetApp
- Espandere LUN NetApp
- Nuova policy SnapMirror asincrona di NetApp
- Nuovo server CIFS NetApp
- Nuova condivisione CIFS NetApp
- Trova mappa LUN del gruppo iniziatore NetApp
- Trova LUN NetApp per ID
- Trova volume NetApp per ID
- Nuova policy di esportazione NetApp
- Nuova interfaccia dati NetApp FC
- Nuovo gruppo iniziatore NetApp
- Nuova interfaccia dati iSCSI NetApp
- Nuovi mirrori di condivisione del carico NetApp per il volume root SVM
- Nuovo LUN NetApp
- Nuova mappa del LUN NetApp
- Nuova interfaccia dati NAS NetApp
- Nuovo volume smart NAS NetApp
- Nuova LUN smart NetApp
- Nuova relazione SnapMirror di NetApp per il volume
- Nuova policy Snapshot di NetApp
- Nuova macchina virtuale per lo storage NetApp
- Nuovo volume NetApp
- Nuova istantanea del volume NetApp
- Registrare il DNS per la macchina virtuale dello storage NetApp
- Rimuovere l’ACL dalla condivisione CIFS di NetApp
- Rimuovi corrispondenza client dalla regola dei criteri di esportazione NetApp
- Rimuovi policy di esportazione dal volume NetApp
- Rimuovere l’iniziatore dal gruppo di iniziatori NetApp
- Rimuovere il server CIFS NetApp
- Rimuovere la condivisione CIFS di NetApp
- Rimuovi policy di esportazione NetApp
- Rimuovere l’interfaccia dati FC NetApp
- Rimuovere il gruppo iniziatore NetApp
- Rimuovere l’interfaccia IP NetApp

- Rimuovere i mirrori di condivisione del carico di NetApp per il volume root SVM
- Rimuovere il LUN NetApp
- Rimuovere la mappa del LUN NetApp
- Rimuovere il volume smart NAS NetApp
- Rimuovere il LUN intelligente NetApp
- Rimuovere la relazione SnapMirror di NetApp per il volume
- Rimuovere il criterio SnapMirror di NetApp
- Rimuovere la policy Snapshot di NetApp
- Rimuovere la macchina virtuale dello storage NetApp
- Rimuovere il volume NetApp
- Rimuovere l'istantanea del volume NetApp
- Rimuovi regola dal criterio di esportazione NetApp
- Rimuovi pianificazione dalla policy istantanea di NetApp
- Rinominare l'istantanea del volume NetApp
- Aggiornare i mirrori di condivisione del carico di NetApp per il volume root SVM
- Aggiornare la capacità del volume NetApp

Per ulteriori informazioni sulla personalizzazione dei flussi di lavoro con le attività di storage e virtualizzazione NetApp, guarda il video "Orchestrazione dello storage NetApp ONTAP in Cisco Intersight".

Infrastruttura

NVMe end-to-end per FlexPod con Cisco UCSM, VMware vSphere 7.0 e NetApp ONTAP 9

TR-4914: NVMe end-to-end per FlexPod con Cisco UCSM, VMware vSphere 7.0 e NetApp ONTAP 9

Chris Schmitt e Kamini Singh, NetApp

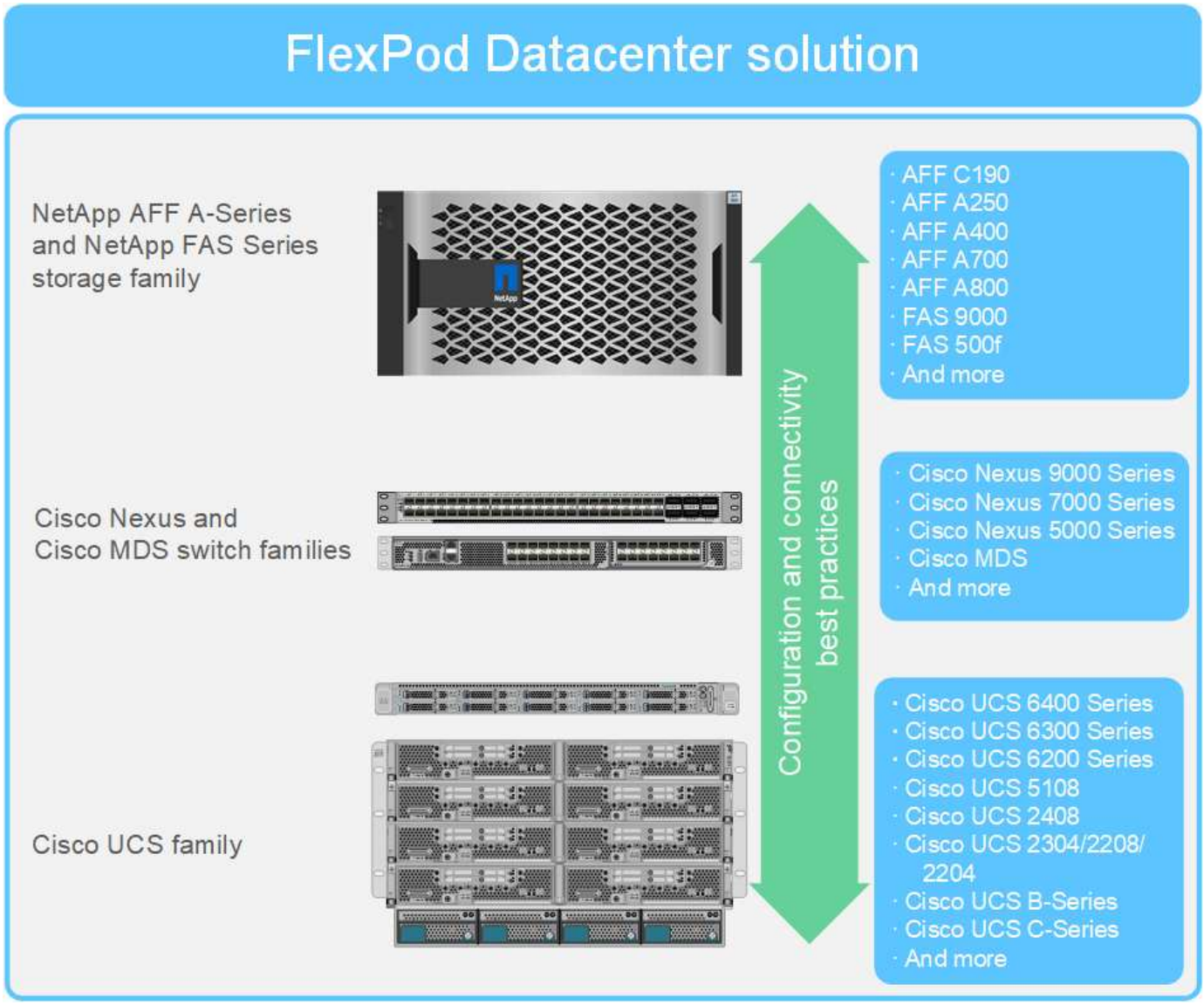
In collaborazione con:

Lo standard di storage dei dati NVMe, una tecnologia emergente, sta trasformando l’accesso e il trasporto allo storage dei dati aziendali offrendo una larghezza di banda molto elevata e un accesso allo storage a latenza molto bassa per le tecnologie di memoria attuali e future. NVMe sostituisce il set di comandi SCSI con il set di comandi NVMe.

NVMe è stato progettato per funzionare con unità flash non volatili, CPU multicore e gigabyte di memoria. Sfrutta inoltre i significativi progressi compiuti in ambito informatico dagli anni '70, consentendo set di comandi semplificati che analizzano e manipolano i dati in modo più efficiente. Un’architettura NVMe end-to-end consente inoltre agli amministratori dei data center di ripensare alla misura in cui possono spingere i propri ambienti virtualizzati e containerizzati e alla quantità di scalabilità supportata dai database orientati alle transazioni.

FlexPod è un’architettura di data center basata su Best practice che include Cisco Unified Computing System (Cisco UCS), switch Cisco Nexus, switch Cisco MDS e sistemi NetApp AFF. Questi componenti sono collegati e configurati in base alle Best practice di Cisco e NetApp per fornire una piattaforma eccellente per l’esecuzione di una vasta gamma di carichi di lavoro aziendali in tutta sicurezza. FlexPod è in grado di scalare per ottenere performance e capacità superiori (aggiungendo risorse di calcolo, rete o storage singolarmente in base alle esigenze) oppure può scalare verso l’esterno per ambienti che richiedono implementazioni multiple e coerenti (come l’implementazione di stack FlexPod aggiuntivi).

La figura seguente illustra le famiglie di componenti FlexPod.



FlexPod è la piattaforma ideale per l'introduzione di FC-NVMe. Può essere supportato con l'aggiunta di Cisco UCS VIC 1400 Series e Port Expander nei server Cisco UCS B200 M5 o M6 esistenti o nei server rack Cisco UCS C-Series M5 o M6 e con aggiornamenti software semplici e senza interruzioni al sistema Cisco UCS, agli switch Cisco MDS 32Gbps, E gli storage array NetApp AFF. Una volta implementati l'hardware e il software supportati, la configurazione di FC-NVMe è simile a quella di FCP.

NetApp ONTAP 9.5 e versioni successive offrono una soluzione FC-NVMe completa. Un aggiornamento software ONTAP senza interruzioni per gli array AFF A300, AFF A400, AFF A700, AFF A700 e AFF A800 consente a questi dispositivi di supportare uno stack di storage NVMe end-to-end. Pertanto, i server con host bus adapter (HBA) di sesta generazione e supporto dei driver NVMe possono comunicare con questi array utilizzando NVMe nativo.

Obiettivo

Questa soluzione fornisce un riepilogo di alto livello delle performance FC-NVMe con VMware vSphere 7 su FlexPod. La soluzione è stata verificata per il passaggio del traffico FC-NVMe e le metrici delle performance sono state acquisite per FC-NVMe con blocchi di dati di varie dimensioni.

Vantaggi della soluzione

NVMe end-to-end per FlexPod offre un valore eccezionale ai clienti con i seguenti vantaggi:

- NVMe si affida a PCIe, un protocollo hardware ad alta velocità e larghezza di banda molto più veloce rispetto agli standard più vecchi come SCSI, SAS e SATA. Connettività a elevata larghezza di banda e latenza ultra bassa tra Cisco UCS Server e lo storage array NetApp per la maggior parte delle applicazioni più esigenti.
- Una soluzione FC-NVMe è senza perdite e può gestire i requisiti di scalabilità delle applicazioni di prossima generazione. Queste nuove tecnologie includono intelligenza artificiale (ai), machine learning (ML), deep learning (DL), analytics in tempo reale e altre applicazioni mission-critical.
- Riduce il costo DELL'IT utilizzando in modo efficiente tutte le risorse all'interno dello stack.
- Riduce drasticamente i tempi di risposta e incrementa le performance applicative, che corrispondono a IOPS e throughput migliorati con latenza ridotta. La soluzione offre ~60% di performance in più e riduce la latenza di ~50% per i carichi di lavoro esistenti.
- FC-NVMe è un protocollo ottimizzato con eccellenti funzionalità di accodamento, in particolare in situazioni con più operazioni i/o al secondo (IOPS, cioè più transazioni) e attività parallele.
- Offre aggiornamenti software senza interruzioni per i componenti FlexPod come Cisco UCS, Cisco MDS e gli storage array NetApp AFF. Non richiede alcuna modifica alle applicazioni.

"Avanti: Approccio al test."

Approccio ai test

"Precedente: Introduzione."

In questa sezione viene fornito un riepilogo generale del test di convalida FC-NVMe su FlexPod. Include sia l'ambiente di test/configurazione che il piano di test adottato per eseguire il test del carico di lavoro in relazione a FC-NVMe per FlexPod con VMware vSphere 7.

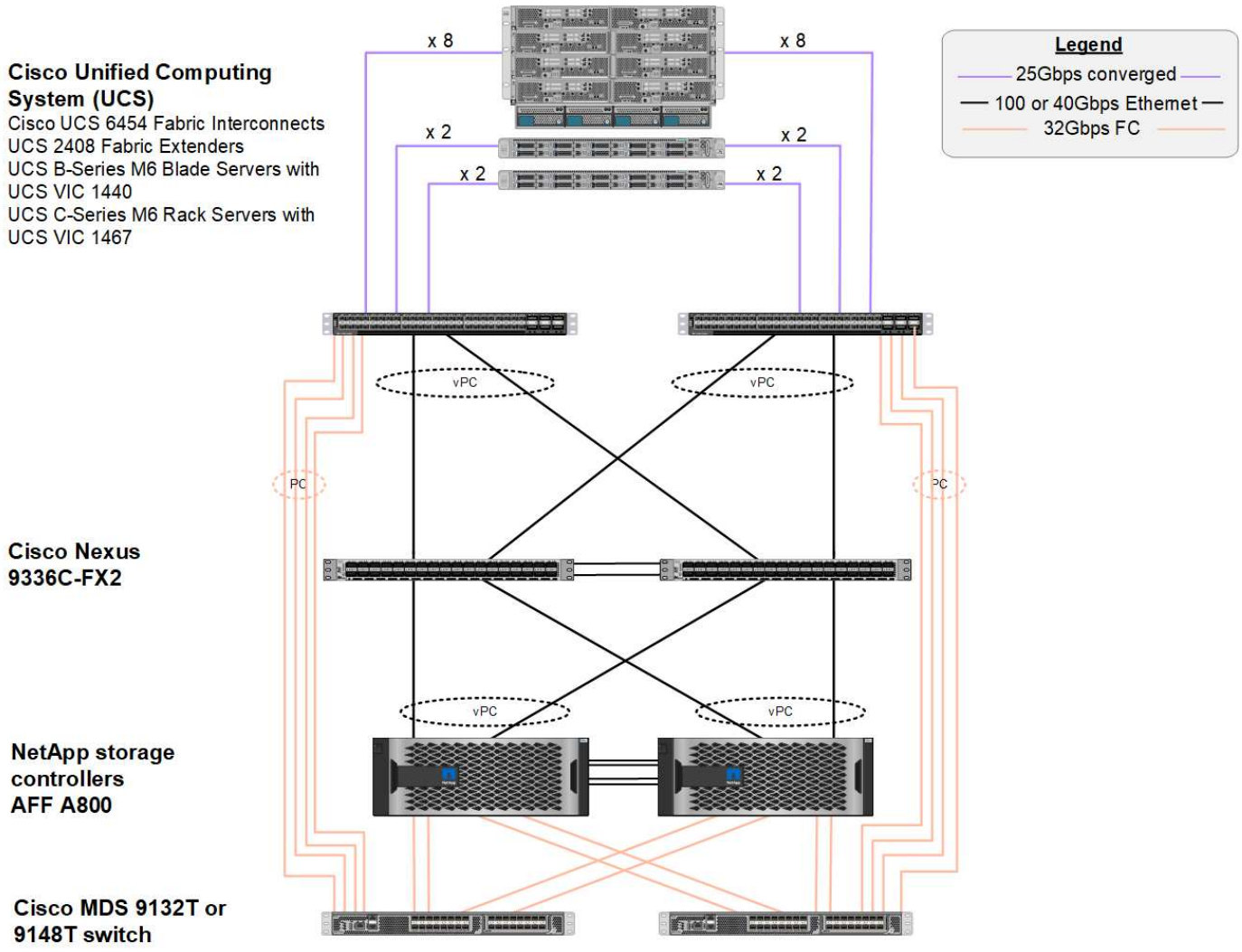
Ambiente di test

Gli switch Cisco Nexus serie 9000 supportano due modalità operative:

- NX-OS standalone, con software Cisco NX-OS
- Modalità fabric ACI, utilizzando la piattaforma Cisco Application Centric Infrastructure (Cisco ACI)

In modalità standalone, lo switch funziona come un tipico switch Cisco Nexus, con maggiore densità di porte, bassa latenza e connettività 40 GbE e 100 GbE.

FlexPod con NX-OS è progettato per essere completamente ridondante nei livelli di calcolo, rete e storage. Non esiste un singolo punto di errore dal punto di vista di un dispositivo o di un percorso di traffico. La figura seguente mostra il collegamento dei vari elementi dell'ultima progettazione FlexPod utilizzata per la convalida di FC-NVMe.



Dal punto di vista della SAN FC, questo design utilizza le ultime interconnessioni fabric Cisco UCS 6454 di quarta generazione e la piattaforma Cisco UCS VICS 1400 con espansione delle porte nei server. I server blade Cisco UCS B200 M6 nello chassis Cisco UCS utilizzano Cisco UCS VIC 1440 con Port Expander collegato a Cisco UCS 2408 Fabric Extender IOM e ogni adattatore bus host virtuale Fibre Channel over Ethernet (FCoE) (vHBA) ha una velocità di 40 Gbps. I server rack Cisco UCS C220 M5 gestiti da Cisco UCS utilizzano Cisco UCS VIC 1457 con due interfacce da 25 Gbps per ogni Fabric Interconnect. Ogni vHBA C220 M5 FCoE ha una velocità di 50 Gbps.

Le interconnessioni fabric si connettono attraverso canali di porta SAN a 32 Gbps agli switch FC Cisco MDS 9148T o 9132T di ultima generazione. La connettività tra gli switch Cisco MDS e il cluster di storage NetApp AFF A800 è anche FC a 32 Gbps. Questa configurazione supporta 32 Gbps FC, per Fibre Channel Protocol (FCP) e storage FC-NVMe tra il cluster di storage e Cisco UCS. Per questa convalida, vengono utilizzate quattro connessioni FC a ciascun controller di storage. Su ciascun controller di storage, le quattro porte FC vengono utilizzate per i protocolli FCP e FC-NVMe.

La connettività tra gli switch Cisco Nexus e il cluster di storage NetApp AFF A800 di ultima generazione è anche di 100 Gbps con canali di porta sui controller di storage e VPC sugli switch. I controller di storage NetApp AFF A800 sono dotati di dischi NVMe sul bus PCIe (Peripheral Connect Interface Express) ad alta velocità.

L'implementazione di FlexPod utilizzata in questa convalida si basa su "Data center FlexPod con Cisco UCS 4.2(1) in modalità gestita UCS, VMware vSphere 7.0U2 e NetApp ONTAP 9.9".

Hardware e software validati

La seguente tabella elenca le versioni hardware e software utilizzate durante il processo di convalida della soluzione. Si noti che Cisco e NetApp dispongono di matrici di interoperabilità che devono essere indicate per determinare il supporto per qualsiasi implementazione specifica di FlexPod. Per ulteriori informazioni, consultare le seguenti risorse:

- "Tool di matrice di interoperabilità NetApp"
- "Cisco UCS hardware and Software Interoperability Tool"

Layer	Dispositivo	Immagine	Commenti
Calcolo	• Due Cisco UCS 6454 Fabric Interconnect • Uno chassis blade Cisco UCS 5108 con due moduli i/o Cisco UCS 2408 • Quattro blade Cisco UCS B200 M6, ciascuno con un adattatore Cisco UCS VIC 1440 e una scheda di espansione porta	Versione 4.2(1f)	Include Cisco UCS Manager, Cisco UCS VIC 1440 e il port expander
CPU	Due CPU Intel Xeon Gold da 6330 a 2.0 GHz, con 42 MB di cache Layer 3 e 28 core per CPU	–	–
Memoria	1024 GB (16 DIMM da 64 GB con funzionamento a 3200MHz)	–	–
Rete	Due switch Cisco Nexus 9336C-FX2 in modalità standalone NX-OS	Versione 9.3(8)	–
Rete di storage	Due switch FC a 32 porte Cisco MDS 9132T da 32 Gbps	Versione 8.4(2c)	Supporta gli analytics FC-NVMe SAN
Storage	Due storage controller NetApp AFF A800 con 24x SSD NVMe da 1,8 TB	NetApp ONTAP 9.9.1P1	–
Software	Cisco UCS Manager	Versione 4.2(1f)	–
	VMware vSphere	7.0U2	–
	VMware ESXi	7.0.2	–
	Driver NIC Fibre Channel nativo VMware ESXi (NFNIC)	5.0.0.12	Supporta FC-NVMe su VMware

Layer	Dispositivo	Immagine	Commenti
	Driver NIC Ethernet nativo VMware ESXi (NENIC)	1.0.35.0	–
Tool di test	FIO	3.19	–

Piano di test

Abbiamo sviluppato un piano di test delle performance per validare NVMe su FlexPod utilizzando un carico di lavoro sintetico. Questo carico di lavoro ci ha consentito di eseguire letture e scritture casuali di 8 KB, nonché letture e scritture di 64 KB. Abbiamo utilizzato gli host VMware ESXi per eseguire i test case con lo storage AFF A800.

Abbiamo utilizzato FIO, uno strumento di i/o sintetico open-source che può essere utilizzato per la misurazione delle performance, per generare il nostro carico di lavoro sintetico.

Per completare i test delle performance, abbiamo condotto diverse fasi di configurazione su storage e server. Di seguito sono riportati i passaggi dettagliati per l'implementazione:

1. Per quanto riguarda lo storage, abbiamo creato quattro macchine virtuali per lo storage (SVM, in precedenza noti come Vserver), otto volumi per SVM e uno spazio dei nomi per volume. Abbiamo creato volumi da 1 TB e spazi dei nomi da 960 GB. Abbiamo creato quattro LIF per SVM e un sottosistema per SVM. Le LIF SVM erano distribuite uniformemente tra le otto porte FC disponibili sul cluster.
2. Sul lato server, abbiamo creato una singola macchina virtuale (VM) su ciascuno dei nostri host ESXi, per un totale di quattro macchine virtuali. Abbiamo installato FIO sui nostri server per eseguire i carichi di lavoro sintetici.
3. Dopo aver configurato lo storage e le macchine virtuali, siamo stati in grado di connettersi agli spazi dei nomi dello storage dagli host ESXi. Questo ci ha consentito di creare datastore in base al nostro namespace e quindi di creare Virtual Machine Disk (VMDK) in base a tali datastore.

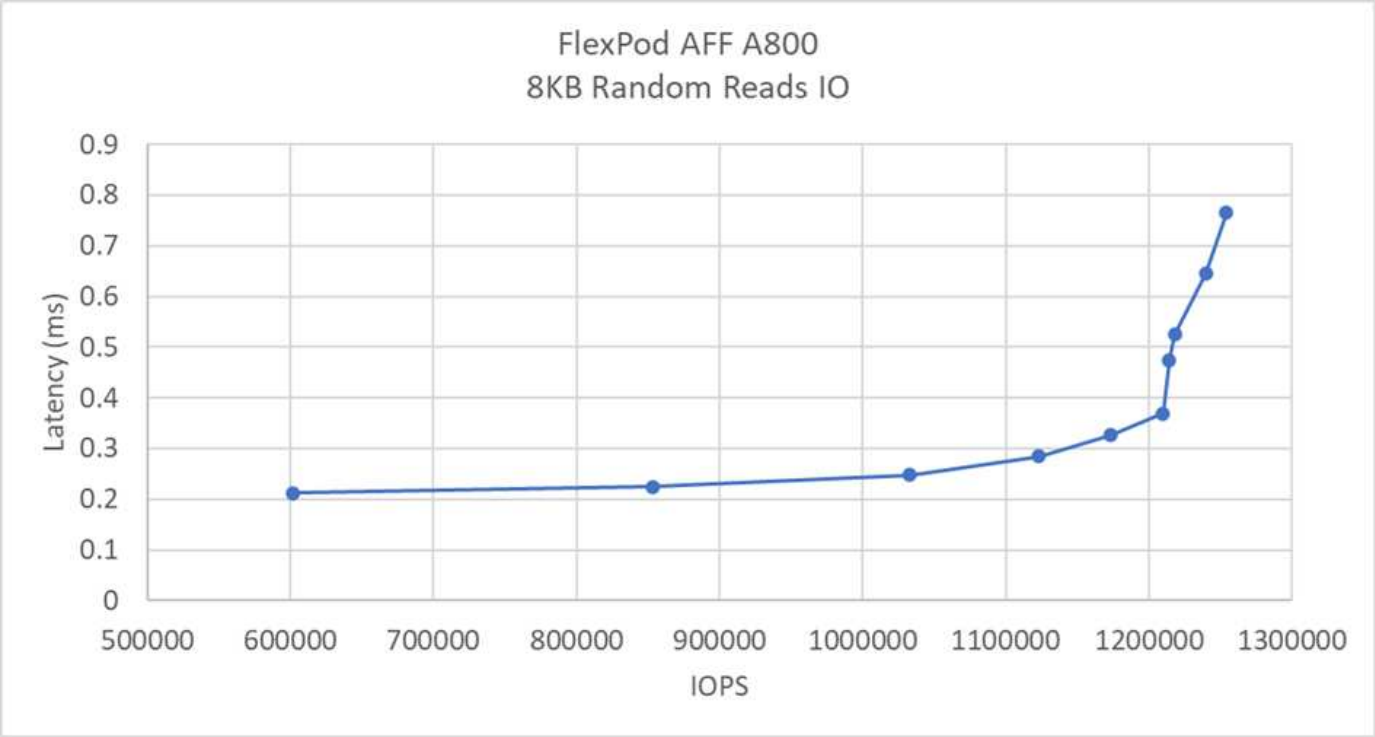
"Segue: Risultati del test."

Risultati del test

"Precedente: Approccio al test."

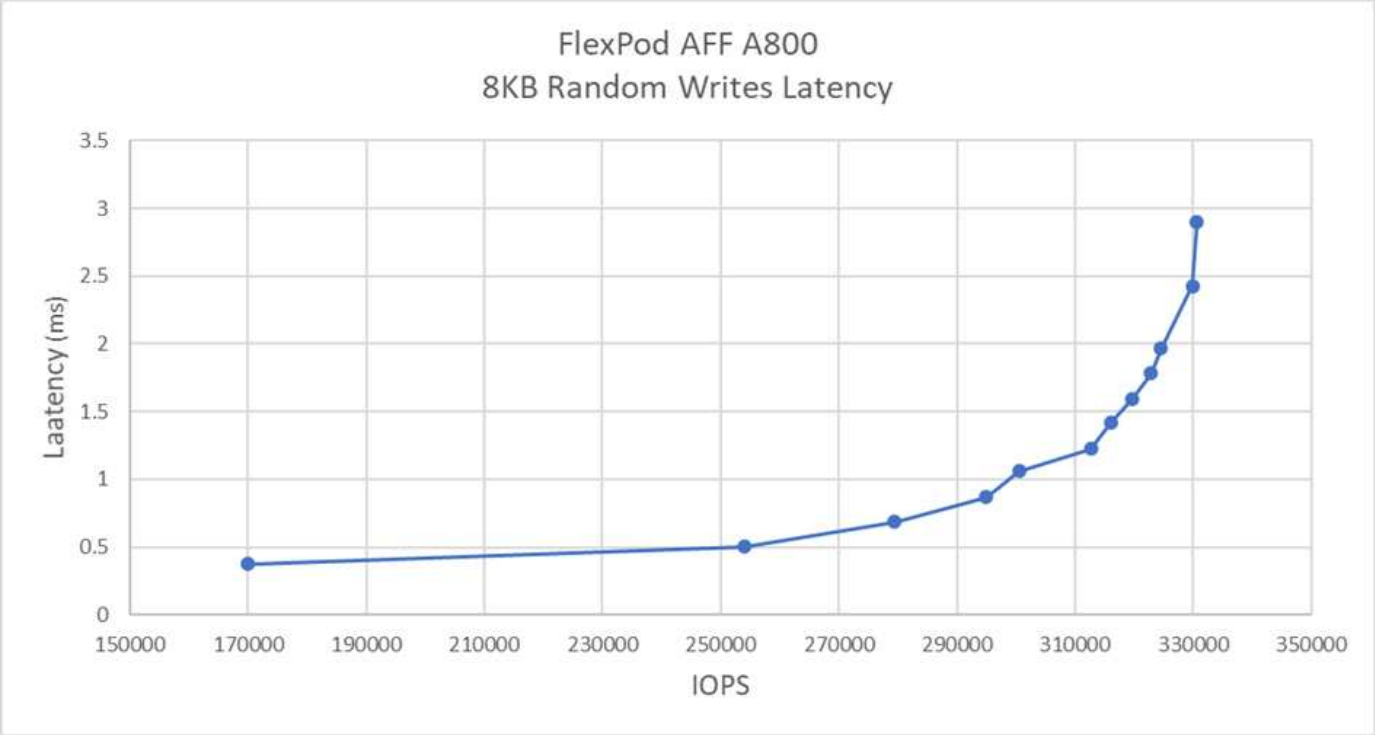
I test consistevano nell'esecuzione dei carichi di lavoro FIO per misurare le performance FC-NVMe in termini di IOPS e latenza.

Il seguente grafico illustra i risultati ottenuti durante l'esecuzione di un carico di lavoro di lettura casuale del 100% con dimensioni di blocchi di 8 KB.



Durante i test, abbiamo riscontrato che il sistema ha raggiunto oltre 1,2 milioni di IOPS mantenendo una latenza sul lato server inferiore a 0,35 ms.

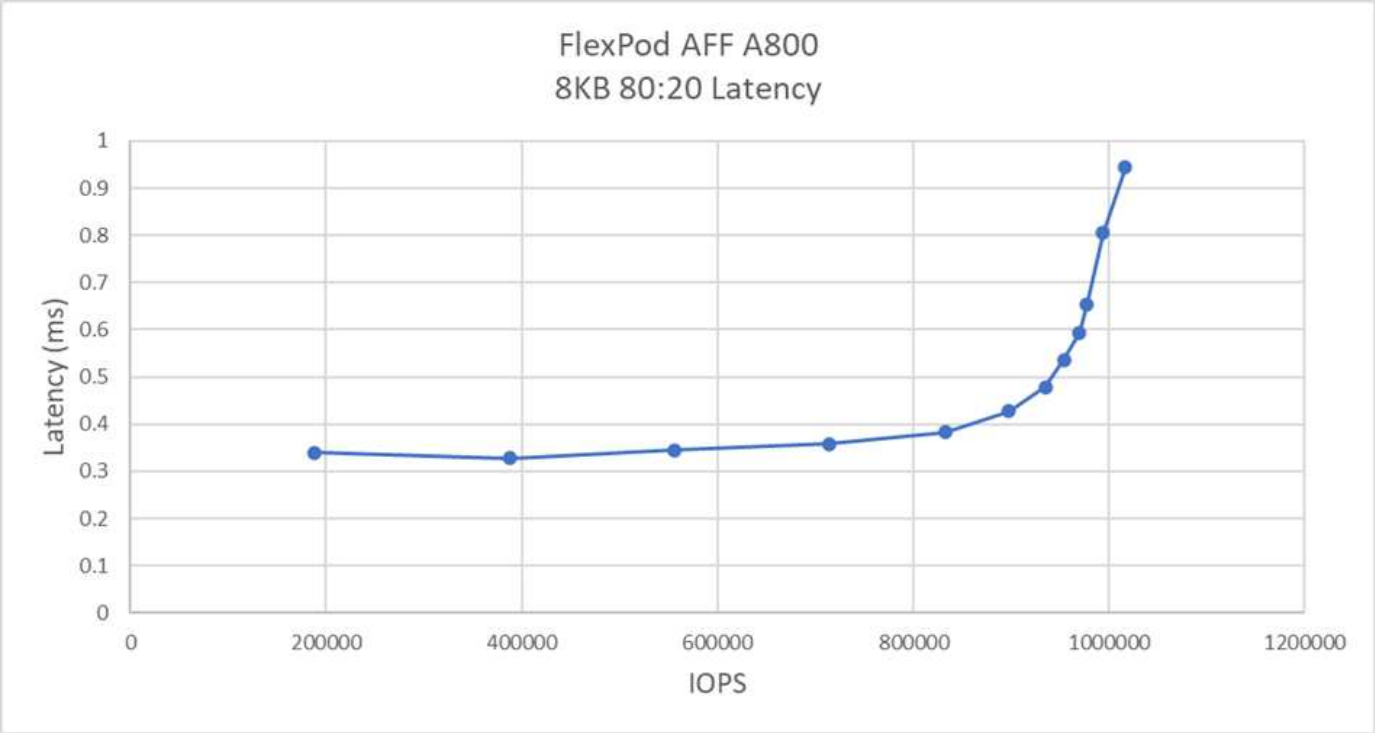
Il seguente grafico illustra i risultati ottenuti durante l'esecuzione di un carico di lavoro di scrittura casuale del 100% utilizzando blocchi di dimensioni da 8 KB.



Durante i test, abbiamo riscontrato che il sistema ha raggiunto quasi 300.000 IOPS mantenendo una latenza sul lato server inferiore a 1 ms.

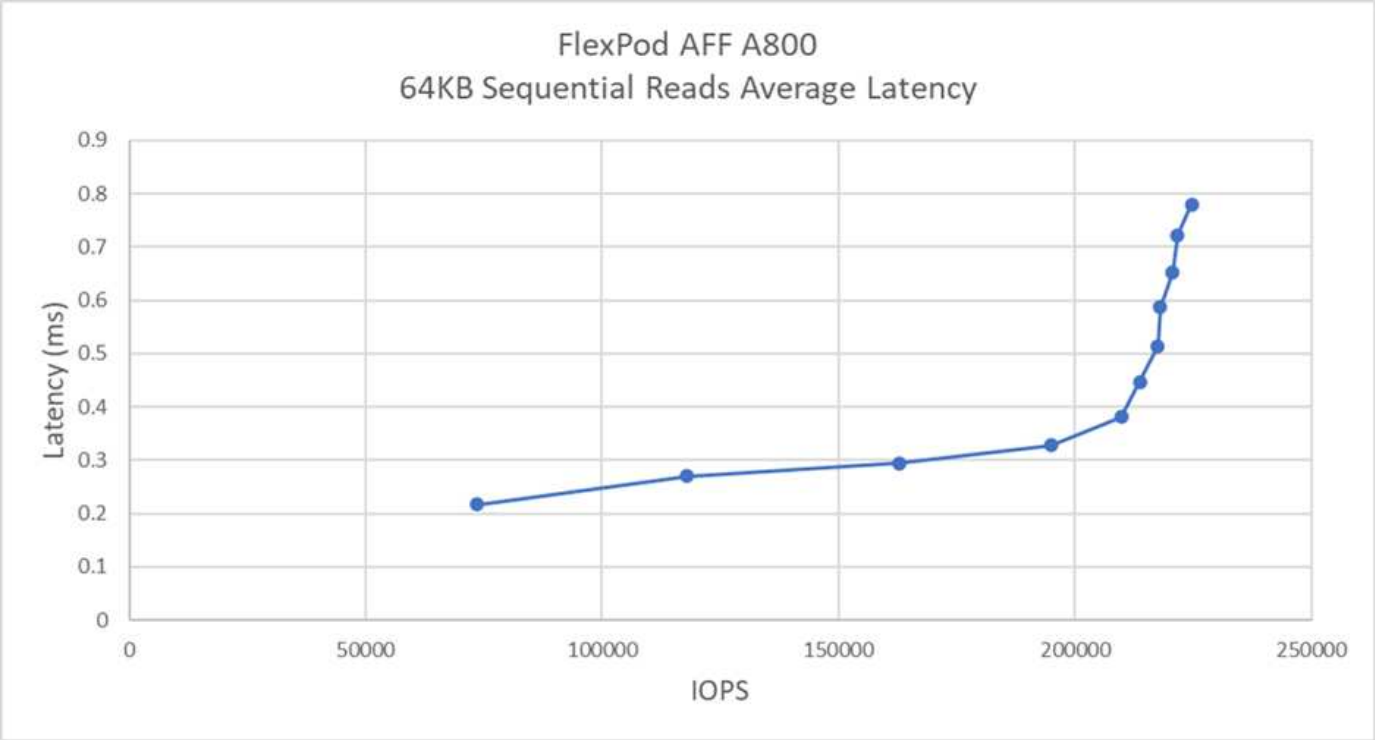
Per le dimensioni dei blocchi di 8 KB con il 80% di letture casuali e il 20% di scritture, abbiamo osservato i

seguenti risultati:



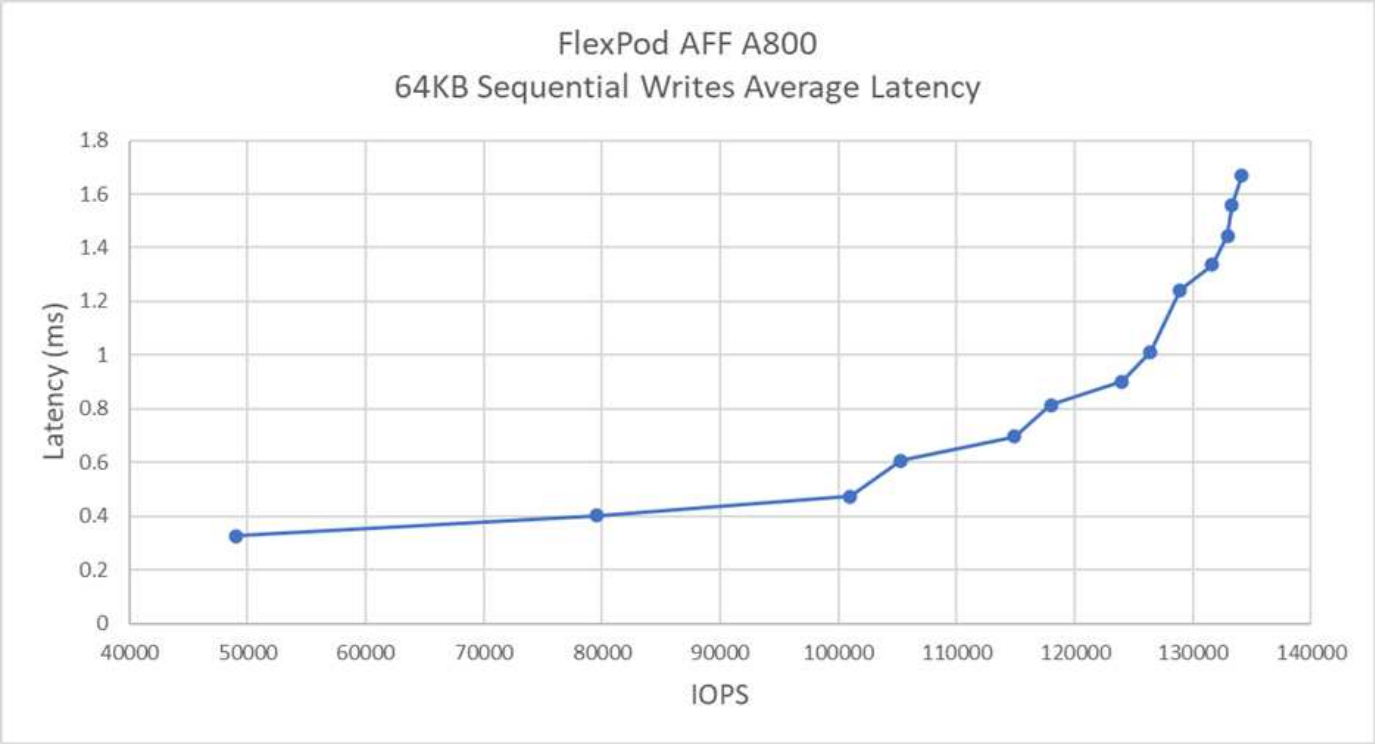
Durante i test, abbiamo riscontrato che il sistema ha raggiunto oltre 1 milione di IOPS mantenendo una latenza sul lato server di poco inferiore a 1 ms.

Per le dimensioni dei blocchi da 64 KB e il 100% di letture sequenziali, abbiamo osservato i seguenti risultati:



Durante i test, abbiamo riscontrato che il sistema ha raggiunto circa 250.000 IOPS mantenendo una latenza sul lato server di poco inferiore a 1 ms.

Per le dimensioni dei blocchi da 64 KB e il 100% di scritture sequenziali, abbiamo osservato i seguenti risultati:



Durante i test, abbiamo riscontrato che il sistema ha raggiunto circa 120.000 IOPS mantenendo al contempo una latenza inferiore a 1 ms sul lato server.

"Prossimo: Conclusione."

Conclusione

"Precedente: Risultati del test."

Il throughput osservato per questa soluzione era pari a 14 Gbps e 220.000 IOPS per un carico di lavoro in lettura sequenziale con una latenza inferiore a 1 ms. Per i carichi di lavoro di lettura casuale, abbiamo raggiunto un throughput di 9,5 Gbps e 1,25 milioni di IOPS. La capacità di FlexPod di fornire queste performance con FC-NVMe può soddisfare le esigenze di qualsiasi applicazione mission-critical.

FlexPod Datacenter con VMware vSphere 7.0 U2 è la base ottimale per l'implementazione di FC-NVMe per una vasta gamma di carichi DI lavoro IT, offrendo così un accesso allo storage dalle performance elevate alle applicazioni che lo richiedono. Poiché FC-NVMe si evolve per includere alta disponibilità, multipathing e supporto aggiuntivo del sistema operativo, FlexPod è la piattaforma scelta, fornendo la scalabilità e l'affidabilità necessarie per supportare queste funzionalità.

Con FlexPod, Cisco e NetApp hanno creato una piattaforma flessibile e scalabile per diversi casi di utilizzo e applicazioni. Con FC-NVMe, FlexPod aggiunge un'altra funzionalità per aiutare le organizzazioni a supportare in modo efficiente ed efficace le applicazioni business-critical eseguite contemporaneamente dalla stessa infrastruttura condivisa. La flessibilità e la scalabilità di FlexPod consentono inoltre ai clienti di iniziare con un'infrastruttura di dimensioni adeguate, in grado di crescere e adattarsi ai loro requisiti di business in evoluzione.

Ulteriori informazioni

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

- Cisco Unified Computing System (UCS)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Scheda informativa su Cisco UCS 6400 Series Fabric Interconnects

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Chassis per server blade Cisco UCS serie 5100

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Server blade Cisco UCS serie B.

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Server rack Cisco UCS C-Series

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Cisco Unified Computing System Adapter

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Cisco UCS Manager

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Switch Cisco Nexus serie 9000

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Switch Cisco MDS 9000 Multilayer Fabric

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Switch Fibre Channel Cisco MDS 9132T a 32 porte da 32 Gbps

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF A-Series

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere

"https://www.vmware.com/products/vsphere"

- VMware vCenter Server

  "http://www.vmware.com/products/vcenter-server/overview.html"

- Best practice per LE SAN moderne

  "https://www.netapp.com/us/media/tr-4080.pdf"

- Presentazione di NVMe end-to-end per FlexPod

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

Matrici di interoperabilità

- Tool di matrice di interoperabilità NetApp

  "http://support.netapp.com/matrix/"

- Matrice di compatibilità hardware Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Guida alla compatibilità VMware

  "http://www.vmware.com/resources/compatibility"

Ringraziamenti

Gli autori desiderano ringraziare John George di Cisco e Scott Lane e Bobby Oommen di NetApp per l'assistenza e le indicazioni fornite durante l'esecuzione del progetto.

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

http://www.netapp.com/us/legal/netapptmlist.aspx

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/us/media/patents-page.pdf

Direttiva sulla privacy

https://www.netapp.com/us/legal/privacypolicy/index.aspx