



# **FlexPod DataCenter con NetApp SnapMirror Business Continuity e ONTAP 9.10**

FlexPod

NetApp  
March 25, 2024

This PDF was generated from <https://docs.netapp.com/it-it/flexpod/flexpod-dc/sm-bcs-introduction.html> on March 25, 2024. Always check docs.netapp.com for the latest.

# Sommario

- FlexPod DataCenter con NetApp SnapMirror Business Continuity e ONTAP 9.10 ..... 1
  - TR-4920: Data center FlexPod con NetApp SnapMirror Business Continuity e ONTAP 9.10 ..... 1
  - Introduzione ..... 1
  - Soluzione FlexPod SM-BC ..... 3
  - Convalida della soluzione ..... 13
  - Conclusione ..... 54
  - Dove trovare informazioni aggiuntive e cronologia delle versioni ..... 55

# 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

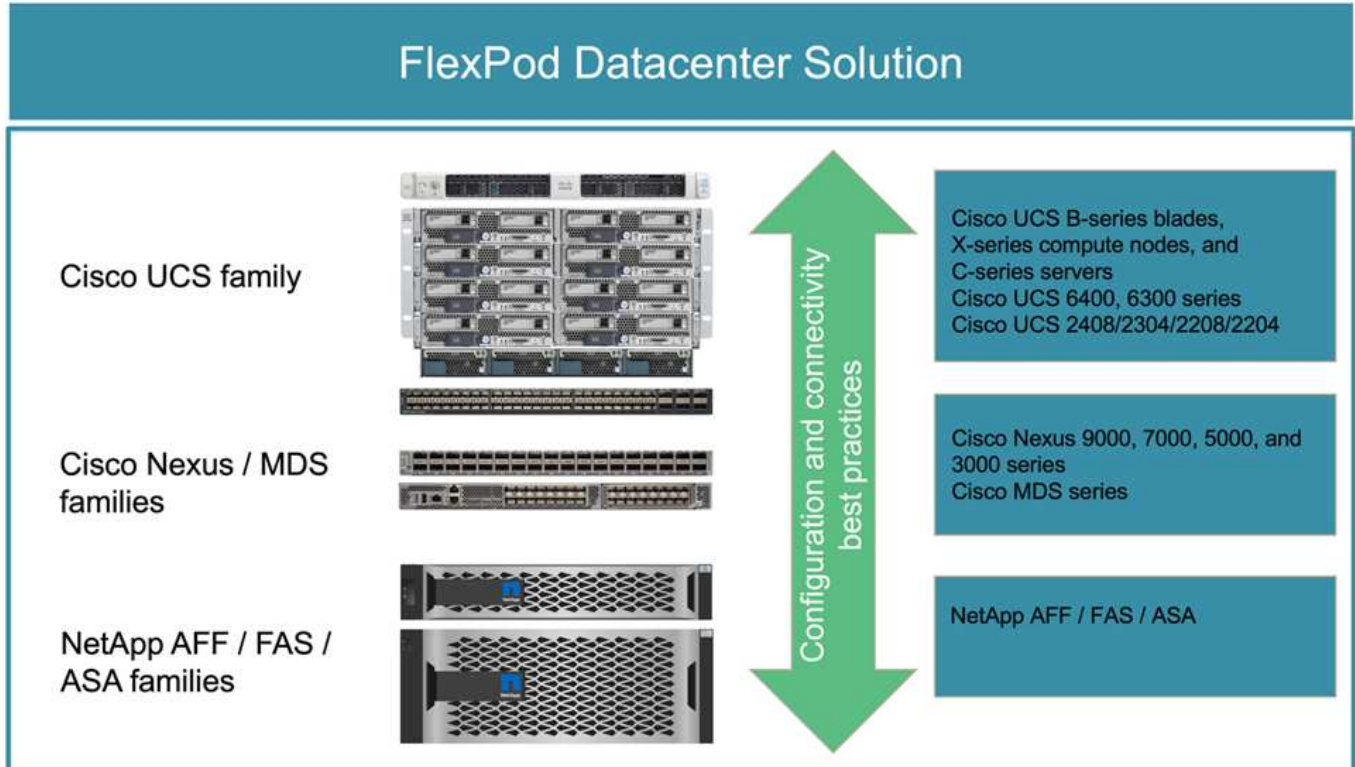
### Introduzione

#### 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**

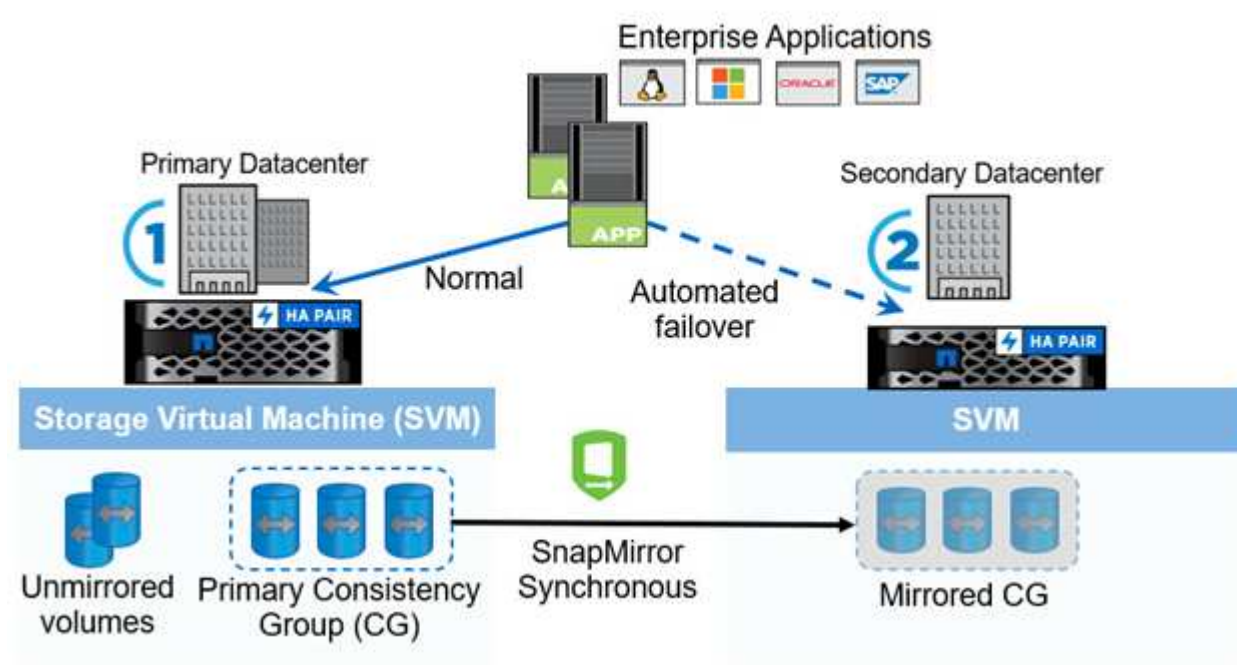
A partire da ONTAP 9.8, è possibile proteggere i carichi di lavoro SAN per il failover trasparente delle

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

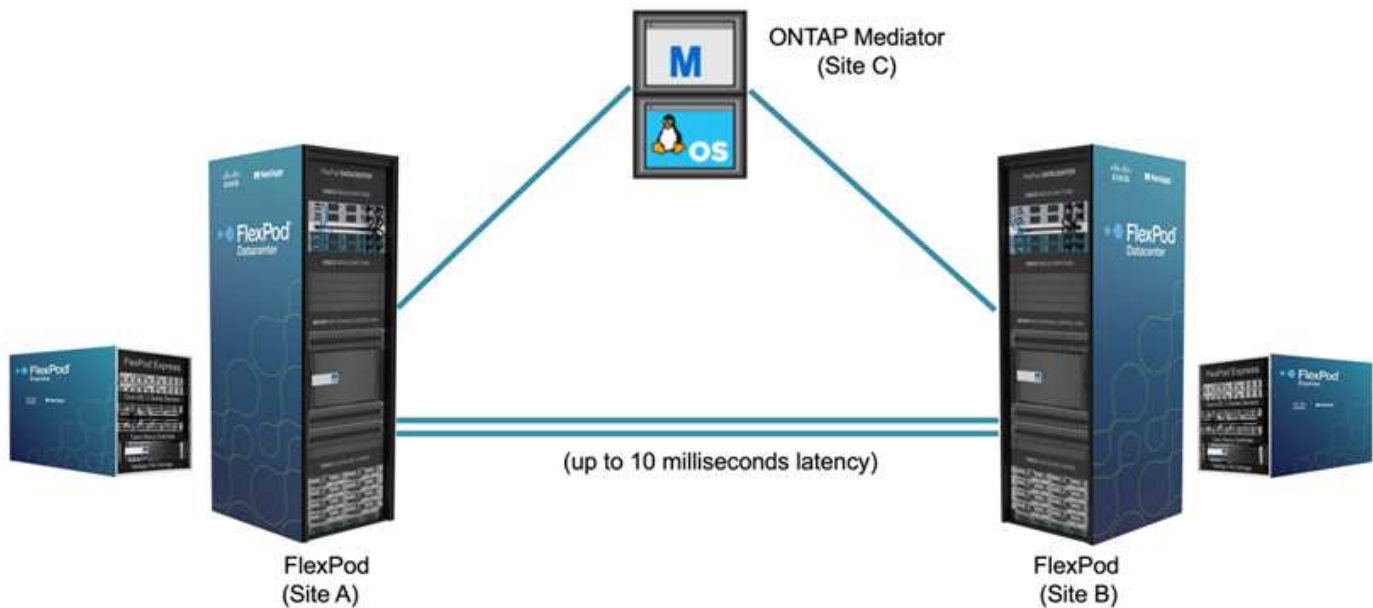
Ad alto livello, una soluzione FlexPod SM-BC è costituita da due sistemi FlexPod, situati in due siti separati da una certa distanza, collegati e accoppiati tra loro per fornire una soluzione di data center altamente disponibile, altamente flessibile e altamente affidabile in grado di garantire la continuità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

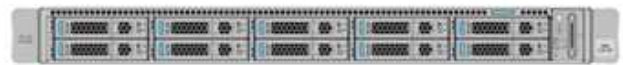
La figura seguente mostra alcuni esempi dei componenti server UCS, tra cui i server rack UCS C-Series, lo chassis UCS 5108 con server blade B-Series e il nuovo chassis UCS X9508 con nodi di calcolo X-Series. I server rack Cisco UCS C-Series sono disponibili in un fattore di forma a una e due unità rack (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.



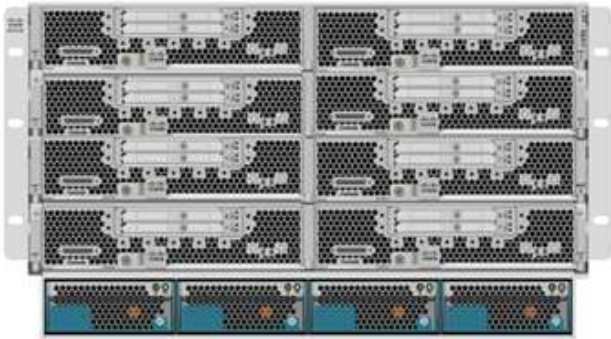
UCS C240/C245 M6



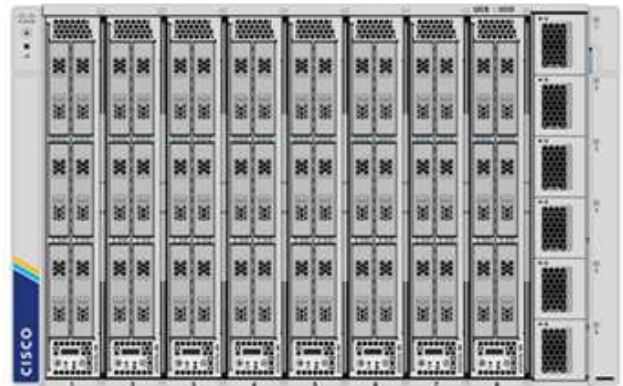
UCS C220/C225 M6



UCS B200 M6



UCS X210c M6



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.

UCS 2408



UCS 2208XP



UCS 2304



UCS 2204XP



UCSX 9108





## 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.



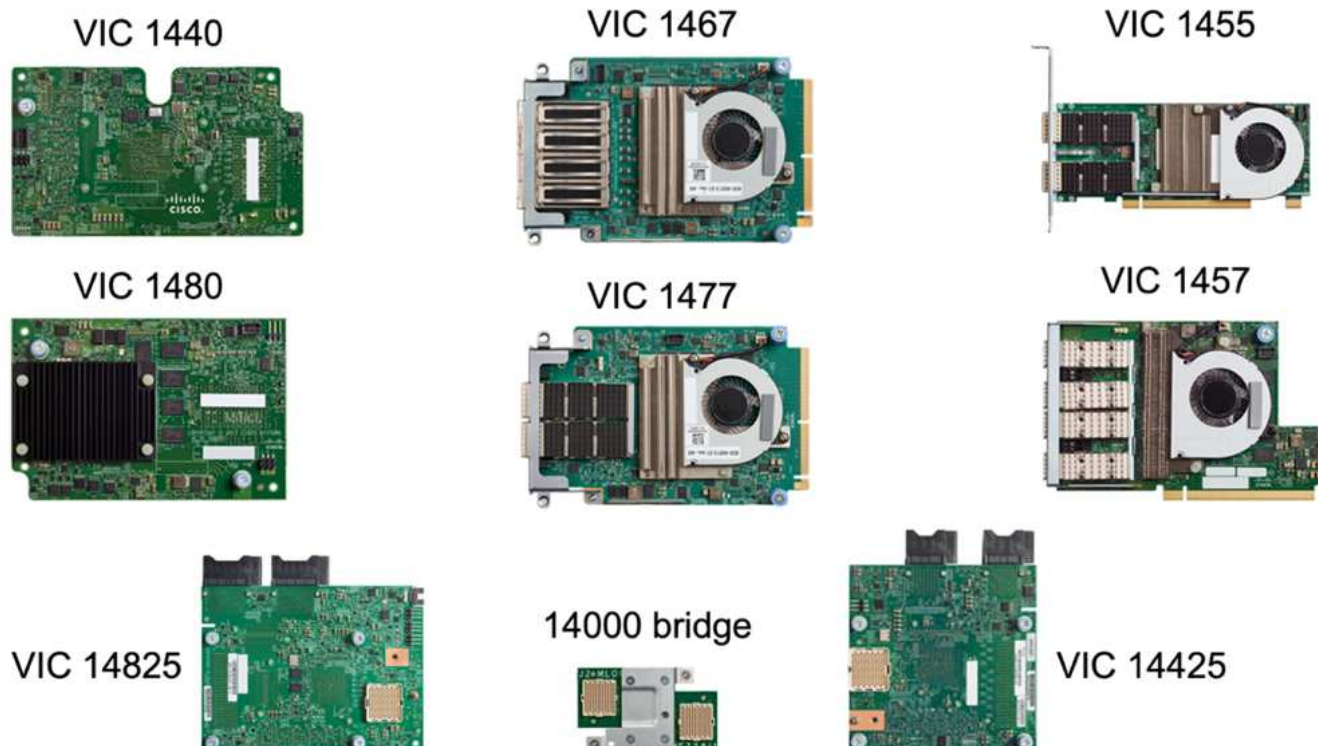
Per supportare lo chassis Cisco UCS X-Series, sono necessarie interconnessioni fabric di quarta generazione configurate in Intersight Managed Mode (IMM). Tuttavia, lo chassis Cisco UCS 5108 serie B può essere supportato sia in modalità IMM che in modalità gestita UCSM.



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  $2 \times 50\text{-G} + 2 \times 50\text{-G}$ , 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.

### Nexus 9336C-FX2



### Nexus 93180YC-FX3



### Nexus 3232C



Vedere "[Switch Cisco Data Center](#)" Per ulteriori informazioni sugli switch Nexus disponibili e sulle relative specifiche e documentazione.

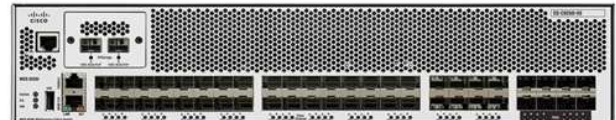
#### Switch MDS

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.

### MDS 9132T



### MDS 9250i



### MDS 9148T



### MDS 9396T



### MDS 9148S



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 semomodulari 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.

### AFF A700/A900, ASA A700



### AFF/ASA A400/A800



### AFF/ASA A250, AFF C190



### DS 224C/2246



### NS 224



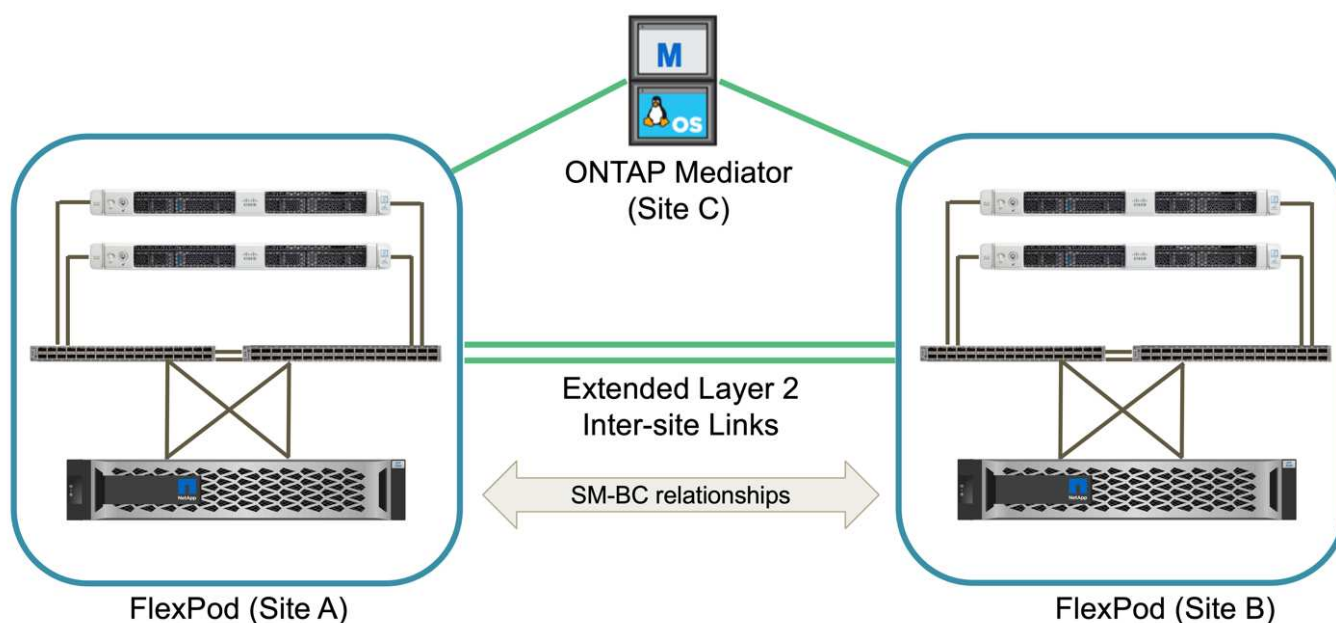


Famiglia di prodotti	Specifiche tecniche
Serie AFF	<a href="#">"Documentazione della serie AFF"</a>
Serie ASA	<a href="#">"Documentazione della serie ASA"</a>

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.

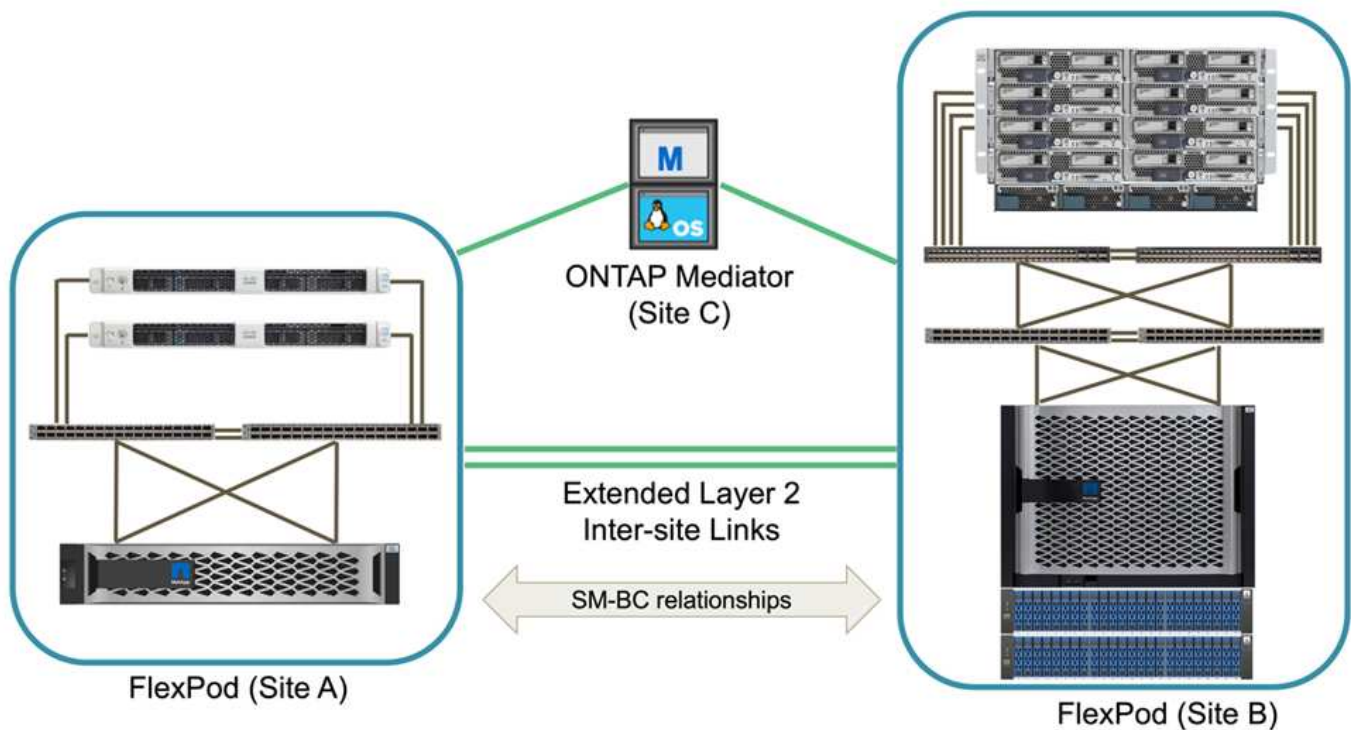
## Topologie delle soluzioni

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.



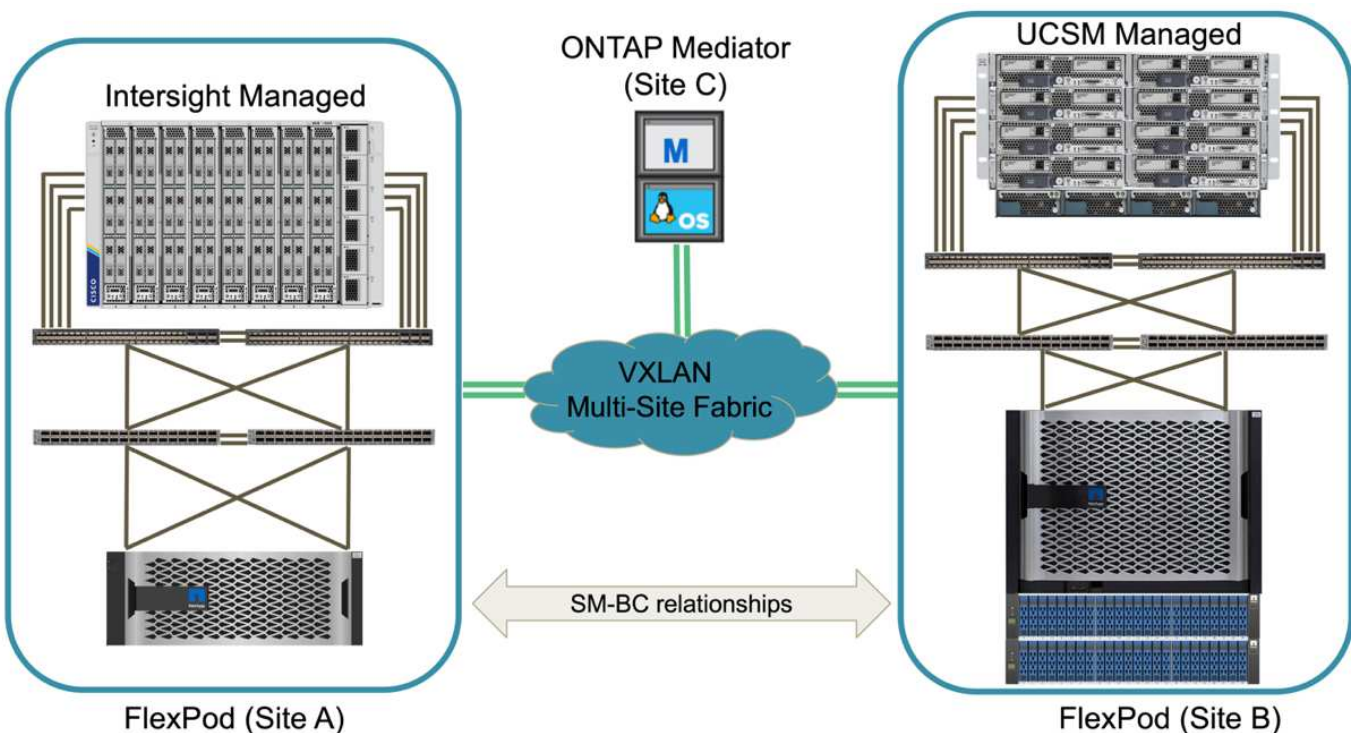
I componenti ridondanti di calcolo, rete e storage sono interconnessi con una connettività ridondante tra i componenti. Questo design ad alta disponibilità offre resilienza della soluzione e consente all'IT di resistere a scenari di singolo punto di errore. Il design multi-sito e le relazioni di replica 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.

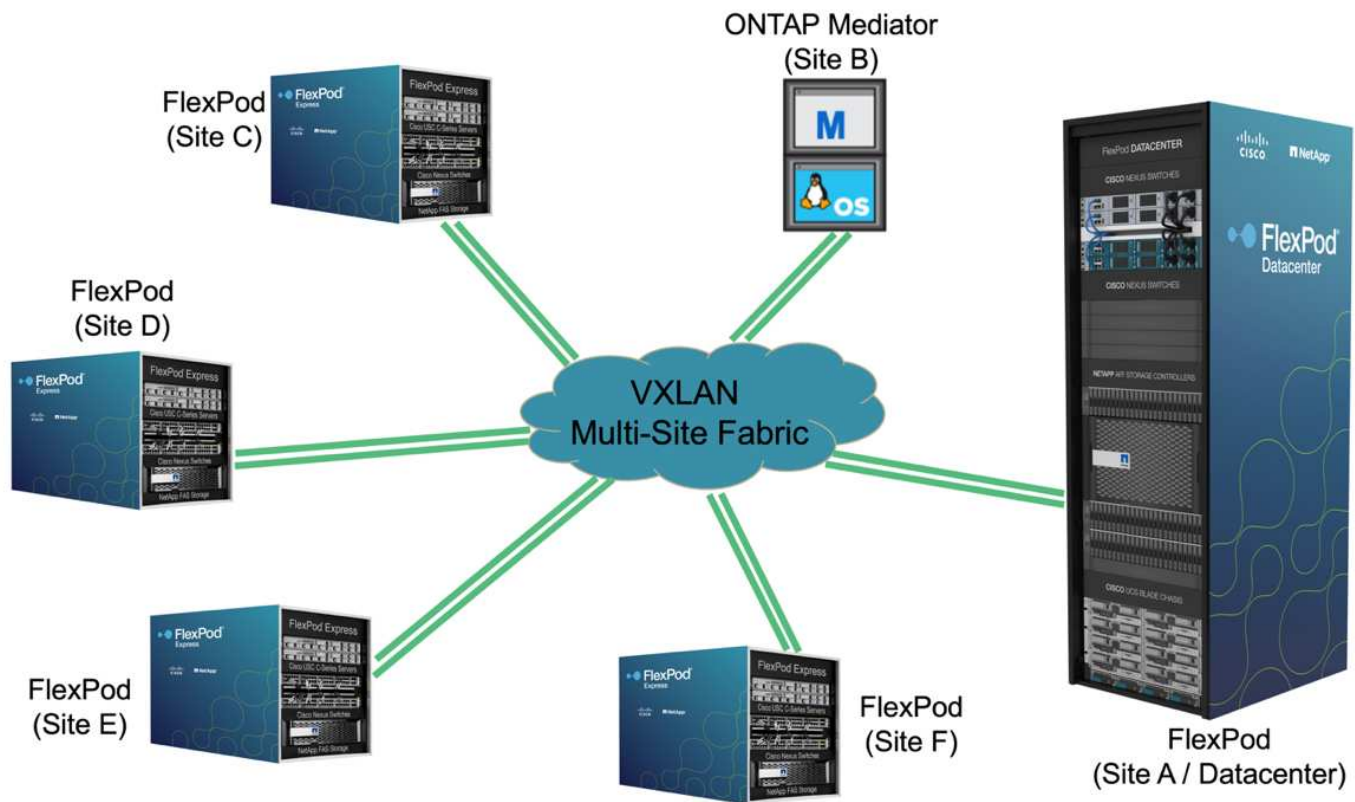


Per le aziende con requisiti di risorse di calcolo e storage più elevati e con più siti, un fabric multi-sito basato su VXLAN consente a più siti di disporre di un fabric di rete perfetto per facilitare la mobilità delle applicazioni, in modo che un'applicazione possa essere servita da qualsiasi sito.

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.

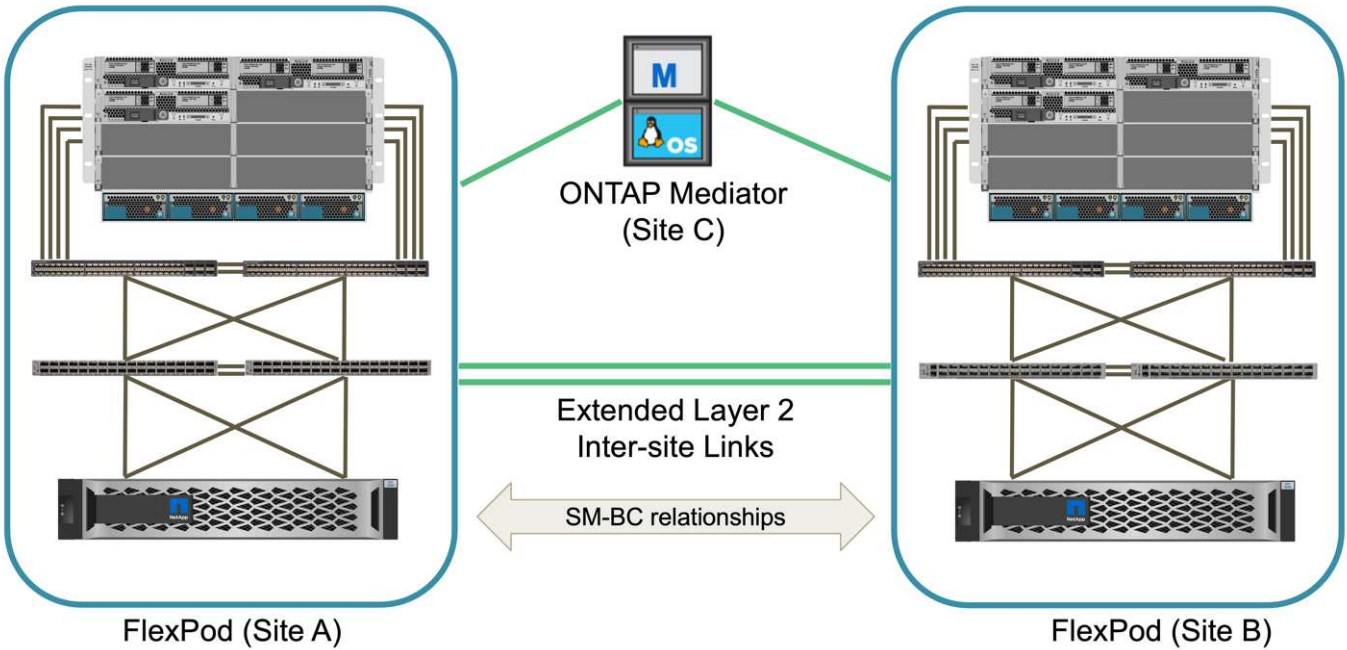
Poiché le soluzioni FlexPod sono di natura flessibile nelle relative configurazioni, è possibile utilizzare potenzialmente tutte le configurazioni e i componenti FlexPod supportati. Il resto di questa sezione fornisce informazioni sulle validazioni di implementazione eseguite per una soluzione di infrastruttura 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

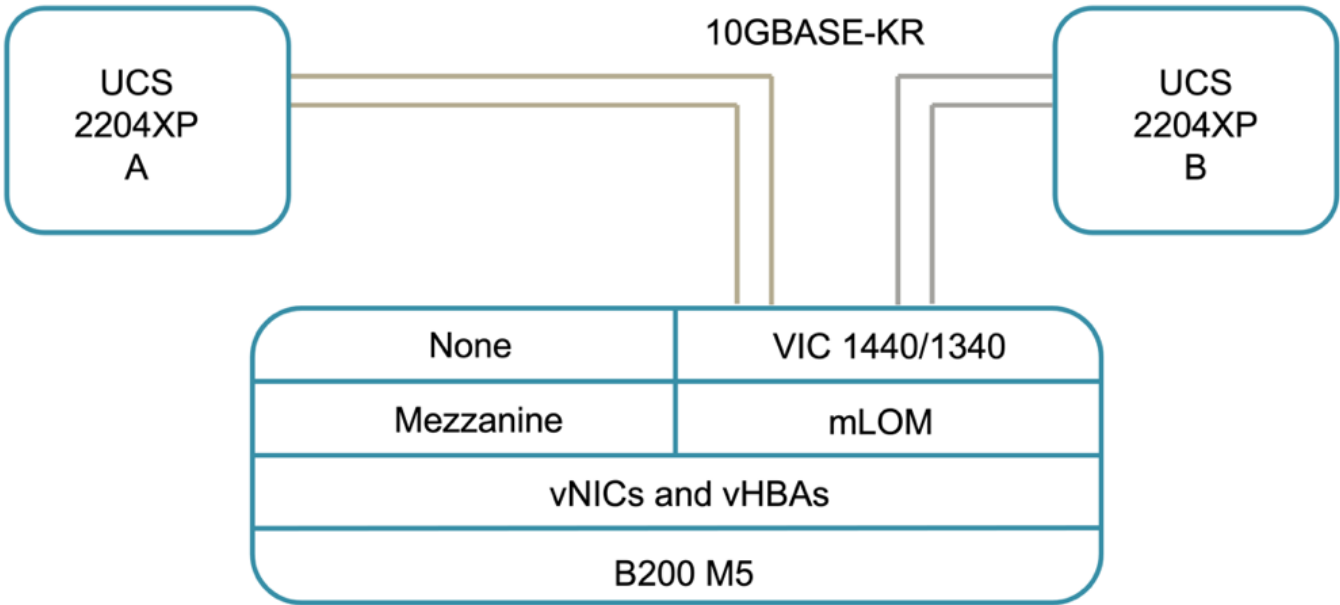
["Previous: Convalida della soluzione - Panoramica."](#)

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

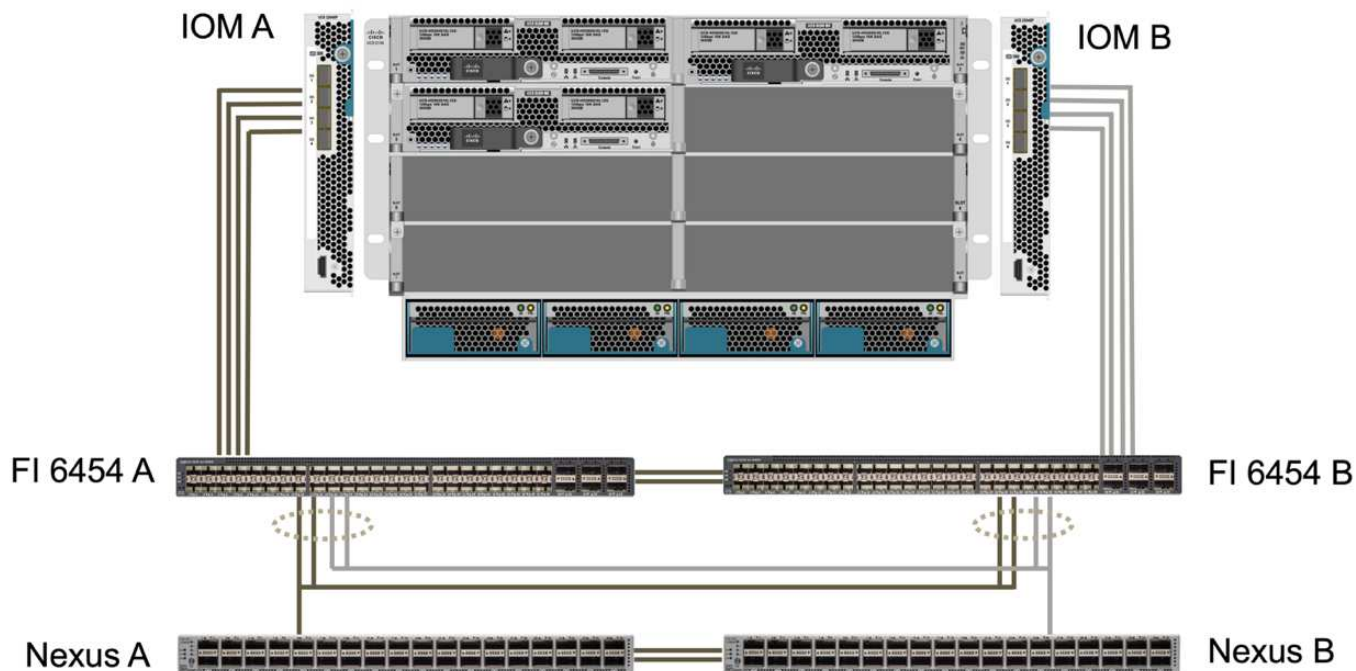
tipiche delle soluzioni FlexPod. Nelle sezioni seguenti vengono illustrate alcune delle configurazioni e della connettività utilizzate per la convalida. Vengono inoltre evidenziate alcune considerazioni relative a SM-BC per fornire riferimenti e indicazioni per l'implementazione.

**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
UCS 6454 FI B	L1	UCS 6454 FI B	L1
	L2		L2
	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus A.	1/13/3
	26		1/13/4
UCS 6454 FI B	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:

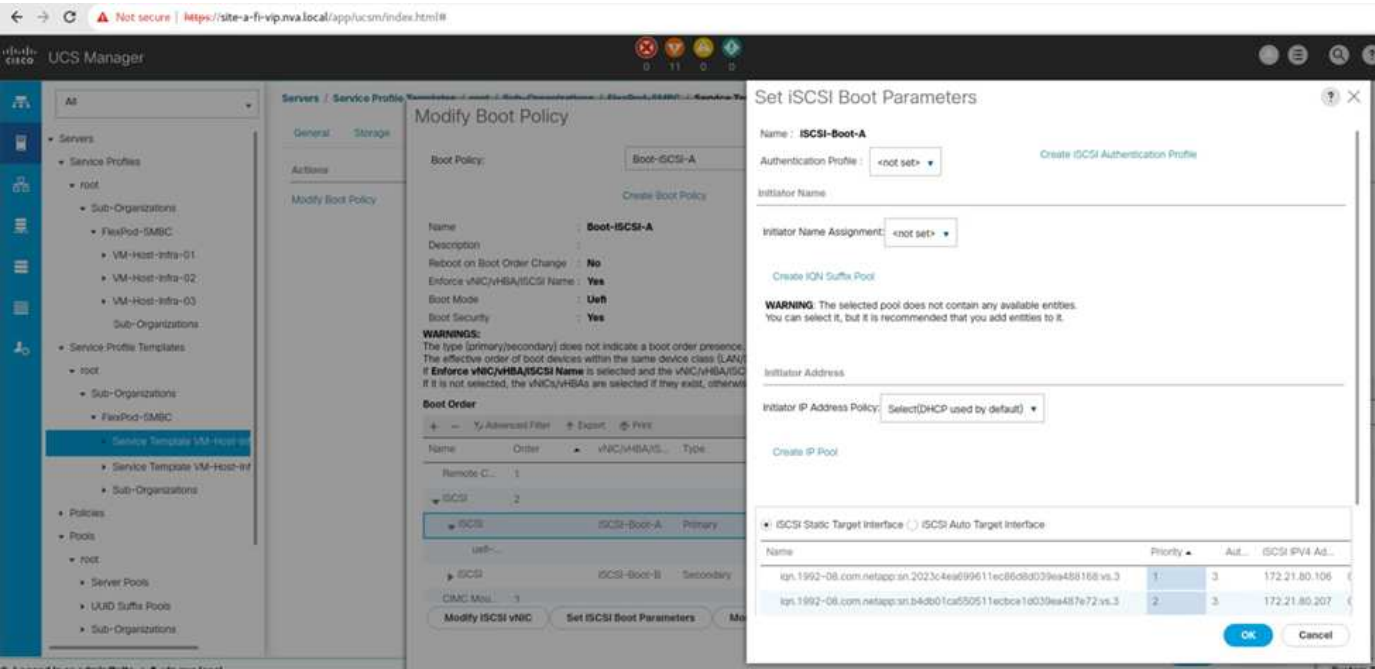
- Eseguire l'avvio SAN dallo storage AFF A250 in entrambi i siti utilizzando il protocollo iSCSI.
- Vengono create sei vNIC per i server in cui:
  - Due vNIC ridondanti (vSwitch0-A e vSwitch0-B) trasportano traffico di gestione in banda. Facoltativamente, questi vNIC possono essere utilizzati anche dai 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

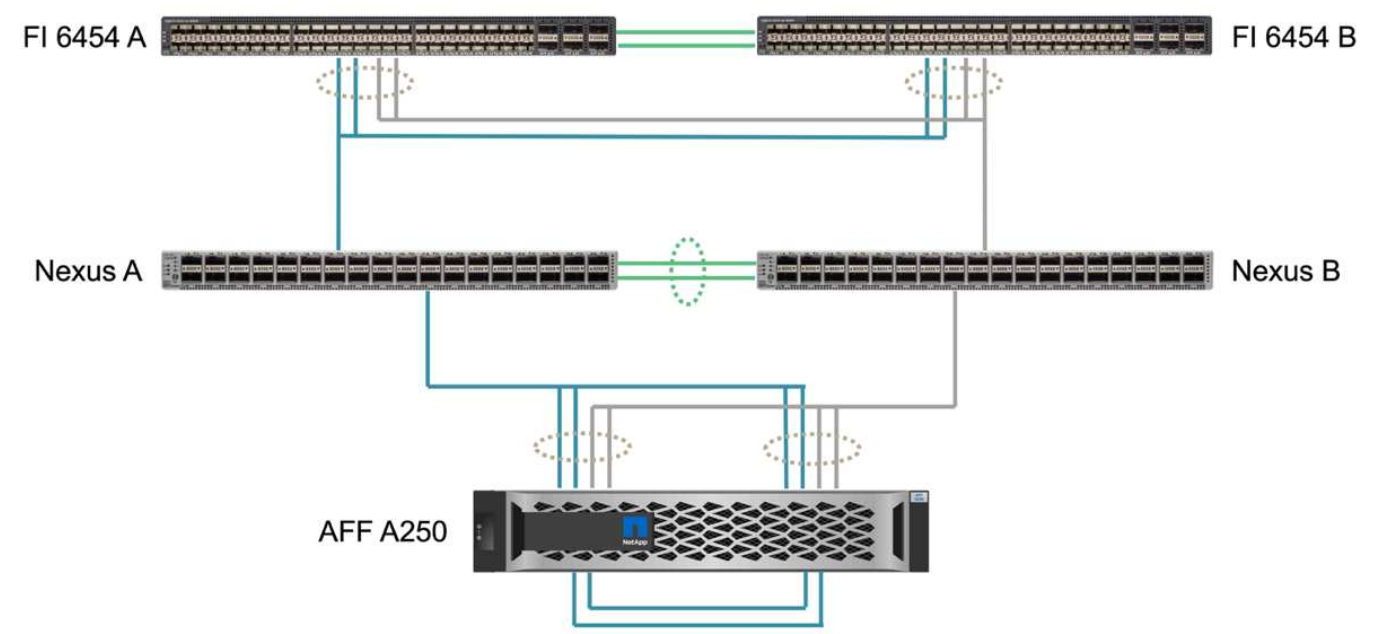
"Precedente: Convalida della soluzione - calcolo."

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.

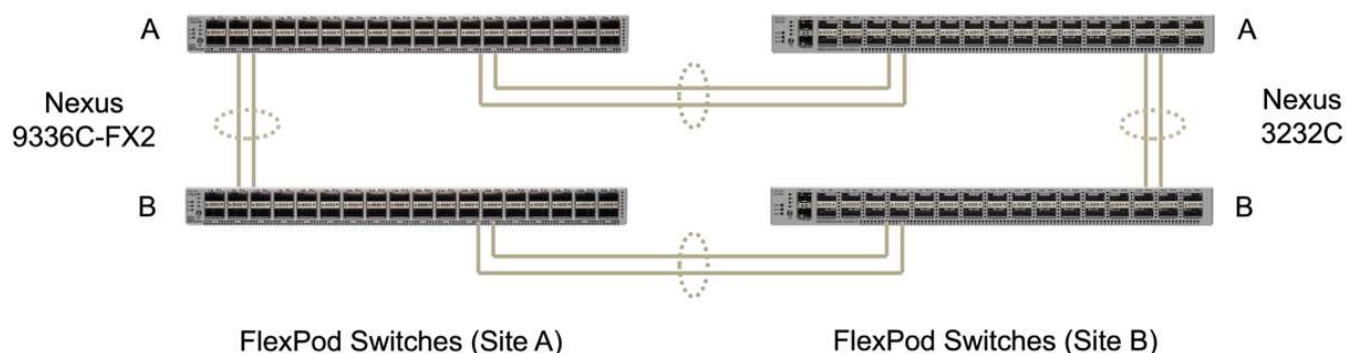


La seguente tabella mostra la connettività tra gli switch Nexus e i controller di storage AFF A250 in ogni sito.

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."](#)

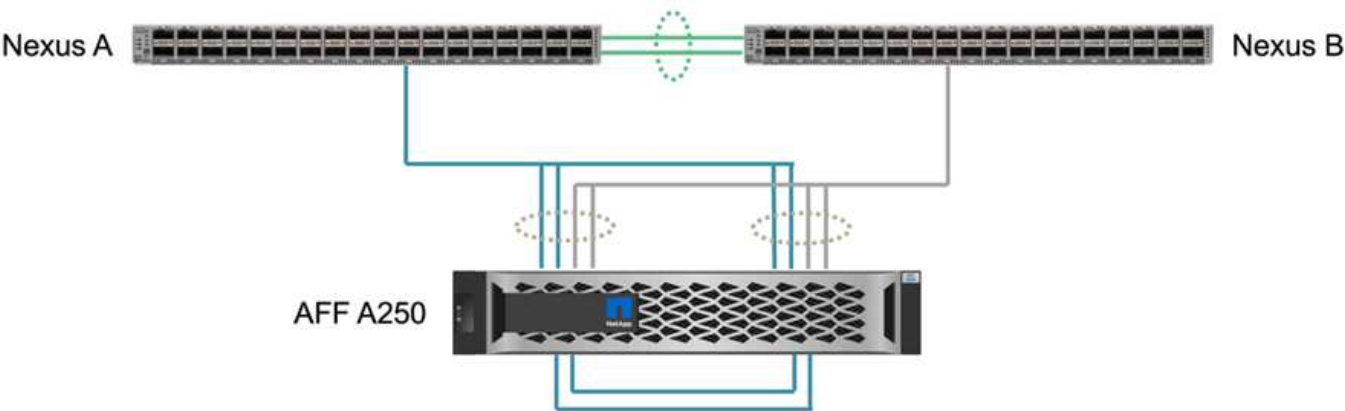
## Convalida della soluzione - Storage

["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.



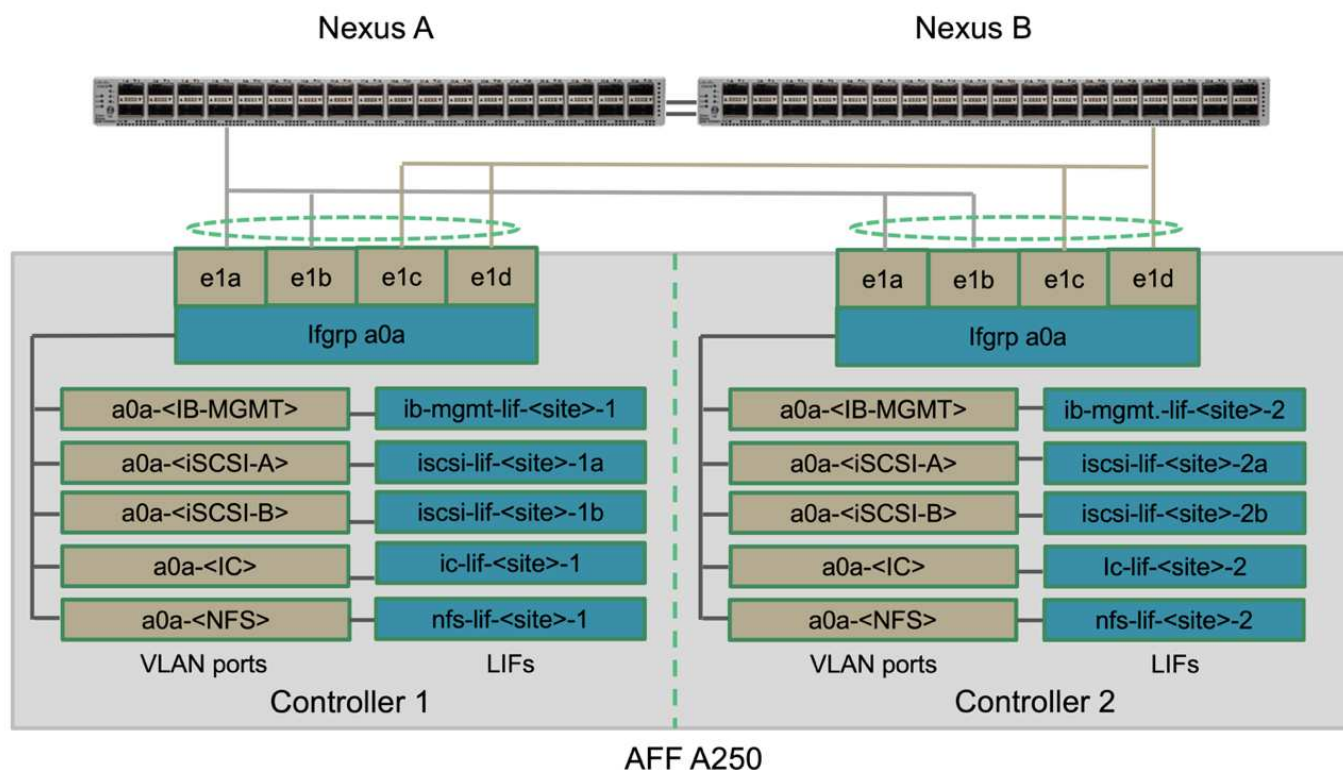
Dispositivo locale	Porta locale	Dispositivo remoto	Porta remota
AFF A250 A.	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A.	1/10/1
	e1b		1/10/2
	e1c	Nexus B	1/10/1

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.



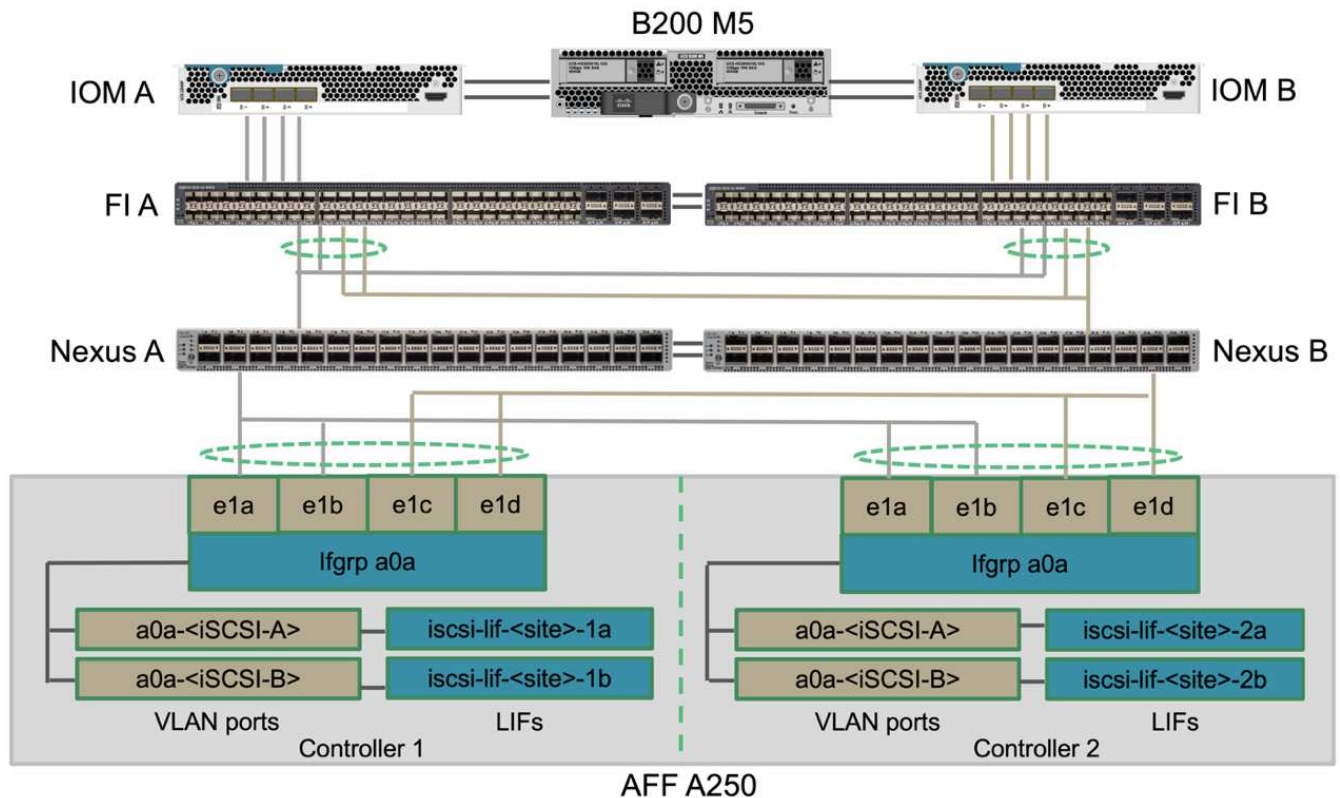
## Boot SAN

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.

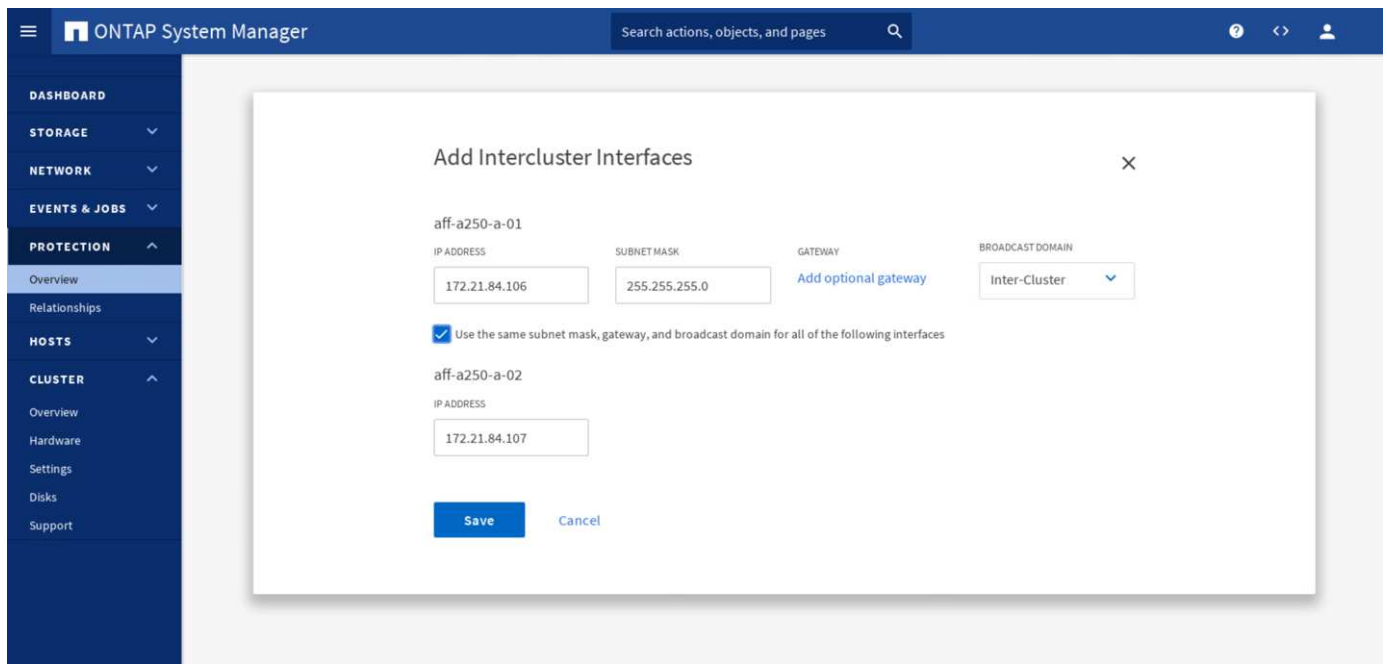
La figura seguente mostra la connettività per l'avvio SAN iSCSI del server Cisco UCS dallo storage NetApp. Nell'avvio SAN iSCSI, a ciascun server Cisco UCS vengono assegnate due vNIC iSCSI (una per ciascun fabric SAN) che forniscono una connettività ridondante dal server fino allo storage. Le porte di 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.



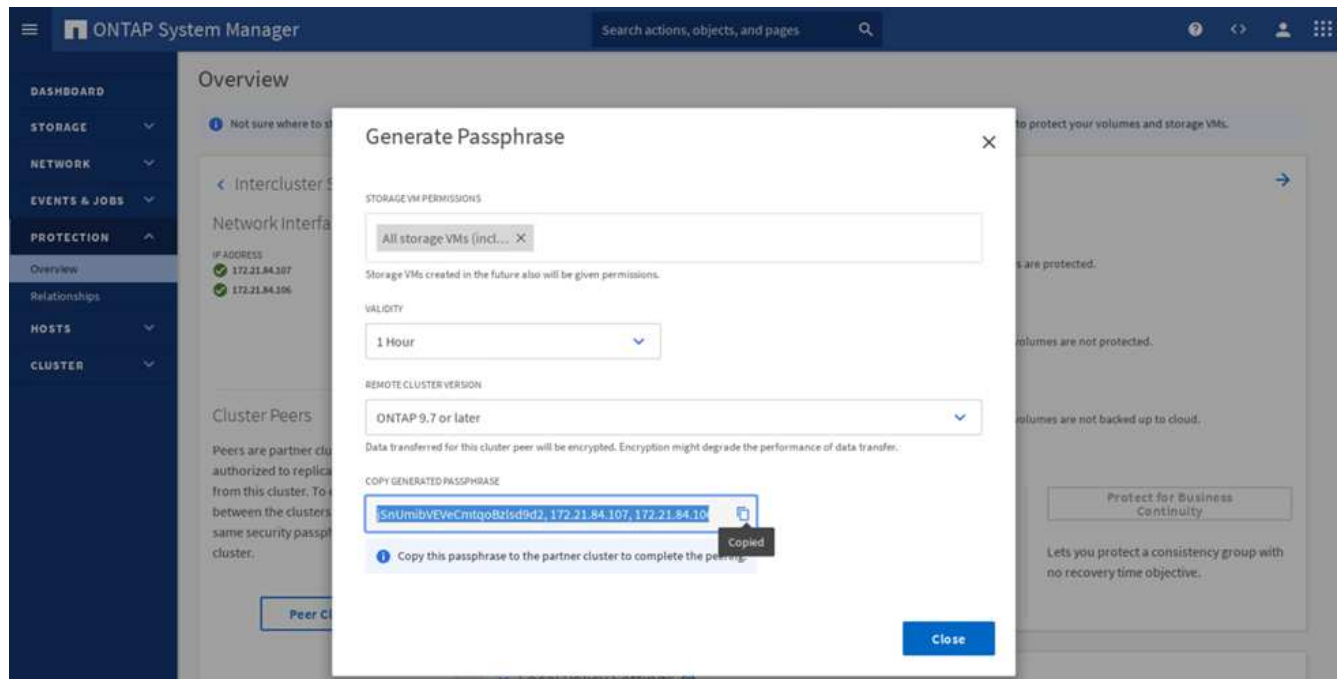
### Peering dei cluster

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.

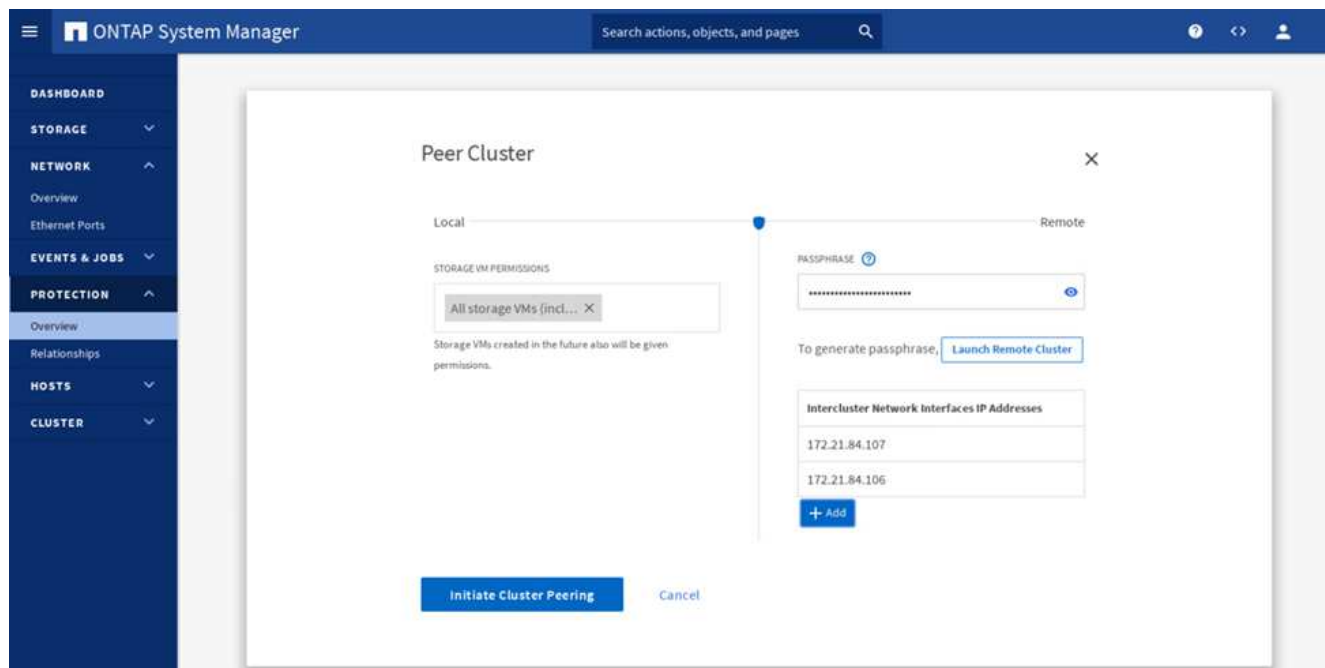


Per unire i due cluster, completare i seguenti passaggi:

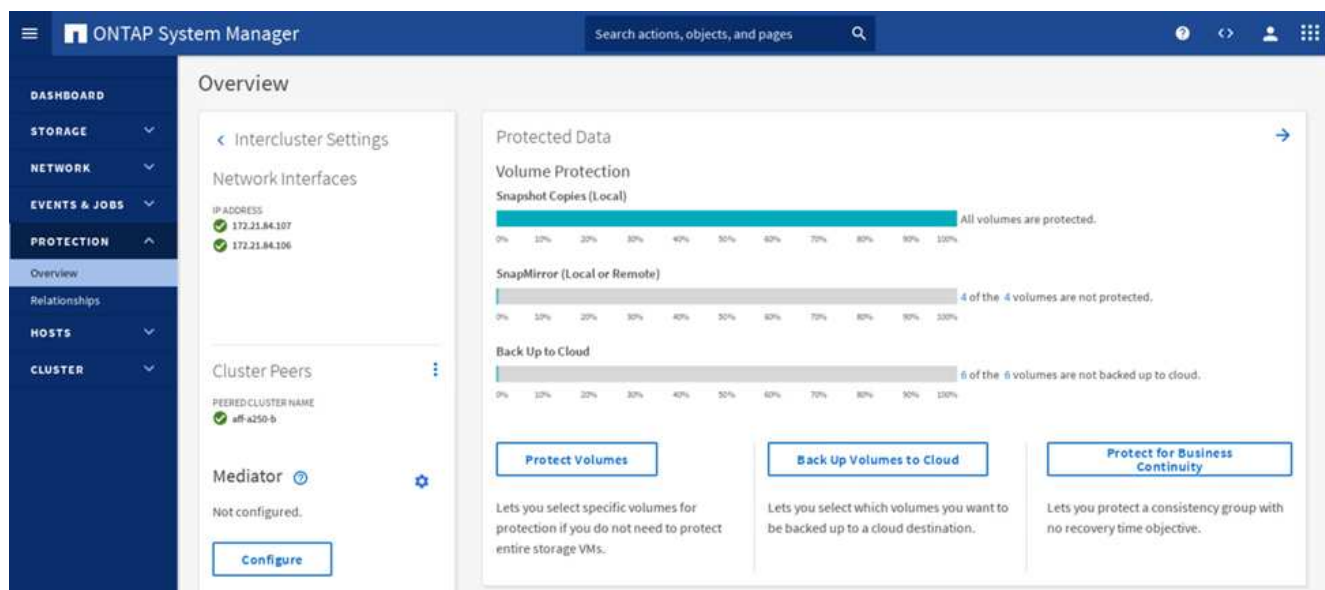
1. Generare la passphrase di peering del cluster nel primo cluster.



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.



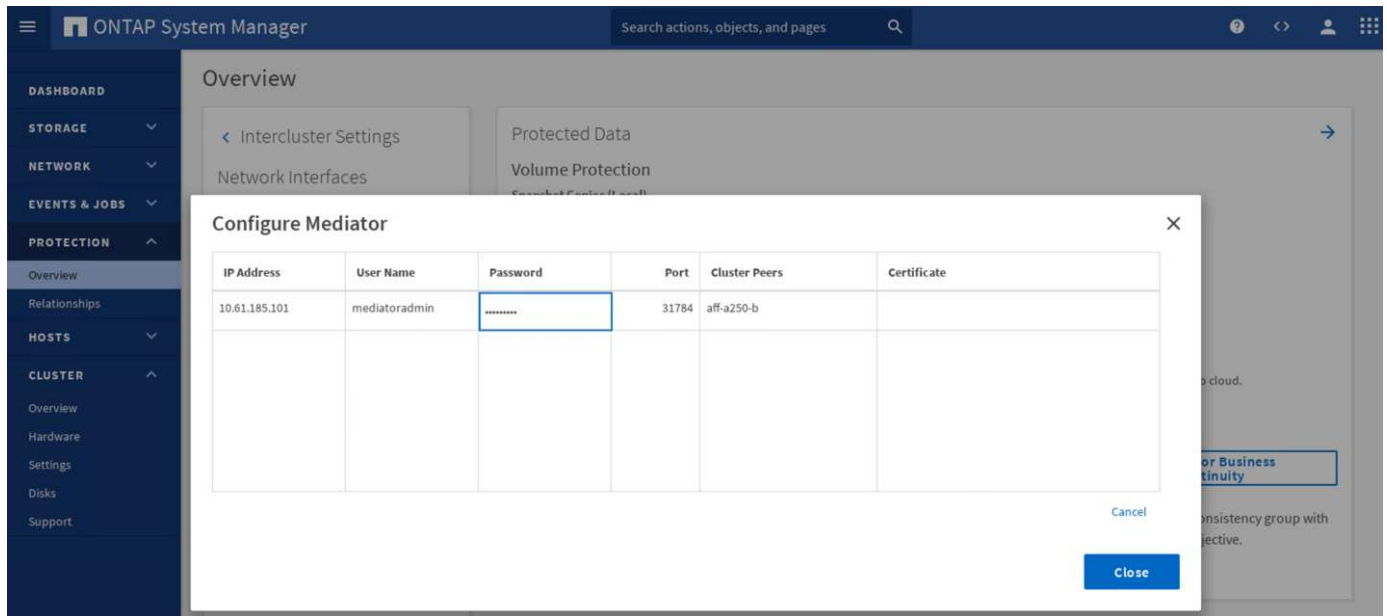
## Installazione e configurazione del mediatore ONTAP

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.

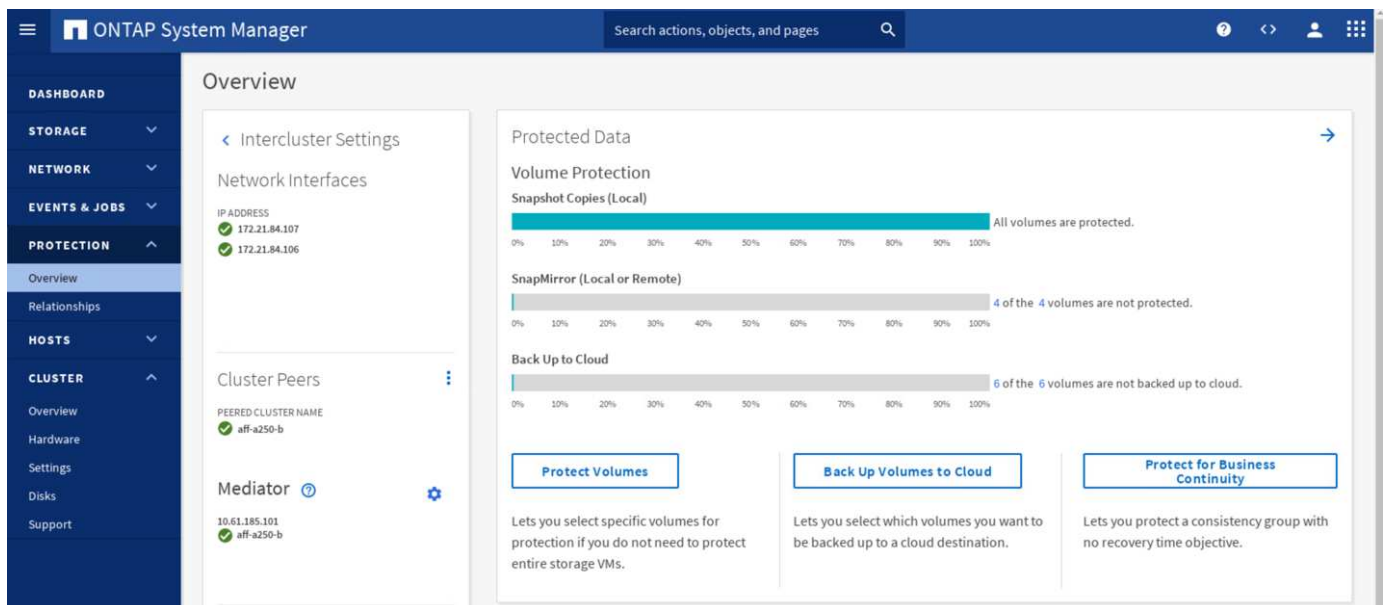
Prima di installare il mediatore ONTAP, consultare ["Installare o aggiornare il servizio di supporto ONTAP"](#) Pagina per i prerequisiti, le versioni di Linux supportate e le procedure per l'installazione sui vari sistemi operativi Linux supportati.

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.

Protect Consistency Group

PROTECTION POLICY

AutomatedFailOver

Source

CLUSTER

aff-a250-a

CONSISTENCY GROUP

Existing

New

NAME

cg\_esxi\_a

VOLUMES

esxi\_a

Destination

CLUSTER

aff-a250-b

Refresh

STORAGEVM

infra-SVM-b

Destination Settings

If the consistency group contains LUNs, you should manually update the host information for the newly created LUNs on the destination cluster.

Save

Cancel

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.

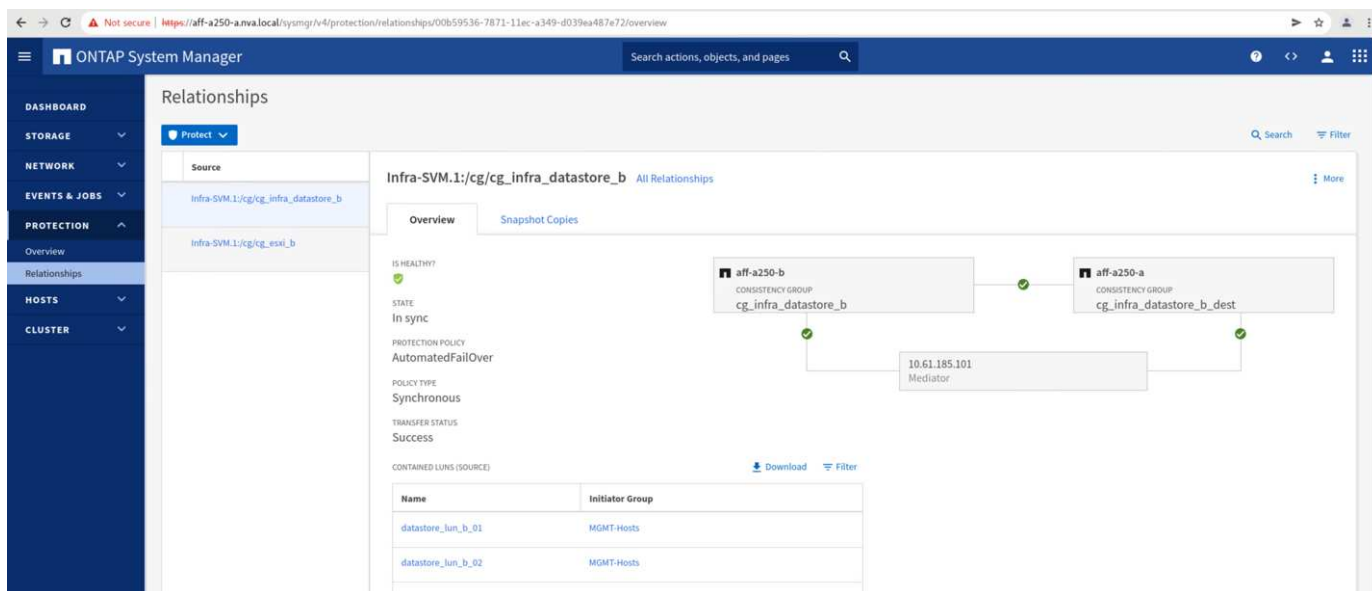
Questa schermata mostra le relazioni dei gruppi di coerenza nel sito A.

Source	Destination	Protection Policy	Relationship Health	State	Lag
Infra-SVM.1/cg/cg_infra_datastore_b	Infra-SVM-a:/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1/cg/cg_esxi_b	Infra-SVM-a:/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

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

Source	Destination	Protection Policy	Relationship Health	State	Lag
Infra-SVM.1/cg/cg_esxi_a	Infra-SVM-b:/cg/cg_esxi_a_dest	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1/cg/cg_infra_datastore_a	Infra-SVM-b:/cg/cg_infra_datastore_a_dest	AutomatedFailOver	Healthy	In sync	0 second

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."](#)

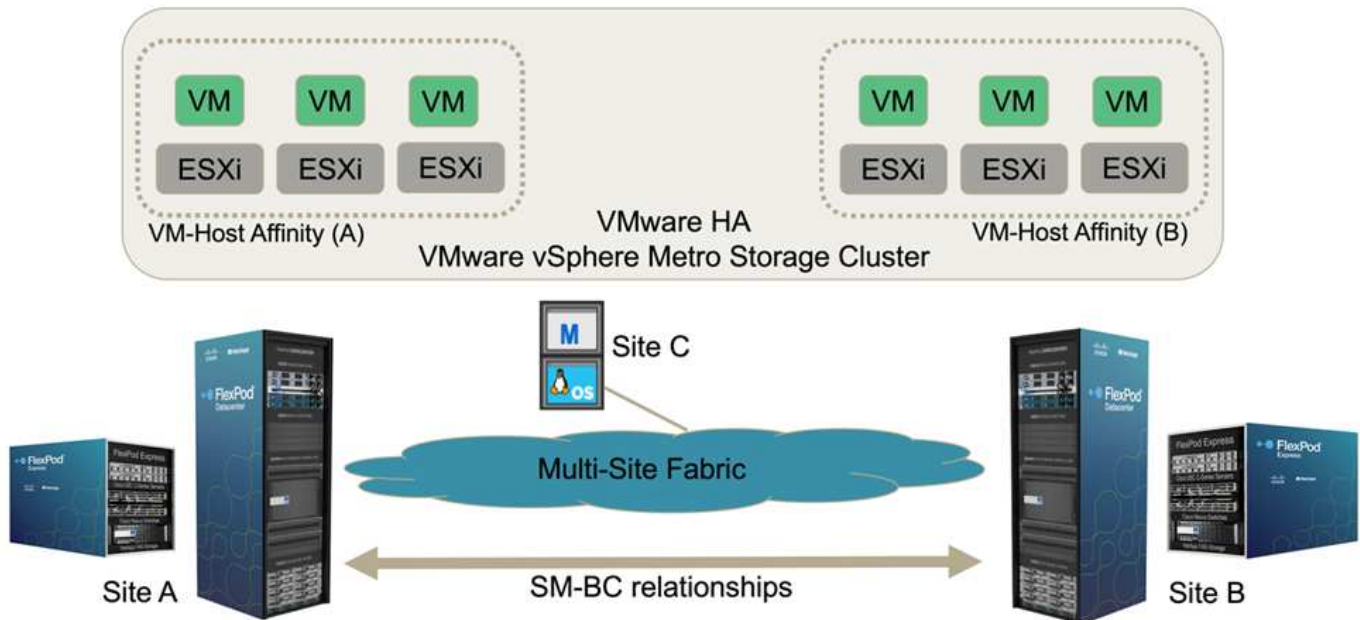
Nella soluzione multi-sito FlexPod SM-BC, un singolo VMware vCenter gestisce le risorse dell'infrastruttura virtuale per l'intera soluzione. Gli host di entrambi i data center partecipano al singolo cluster VMware ha che copre entrambi i data center. Gli host hanno accesso alla soluzione NetApp SM-BC, 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.

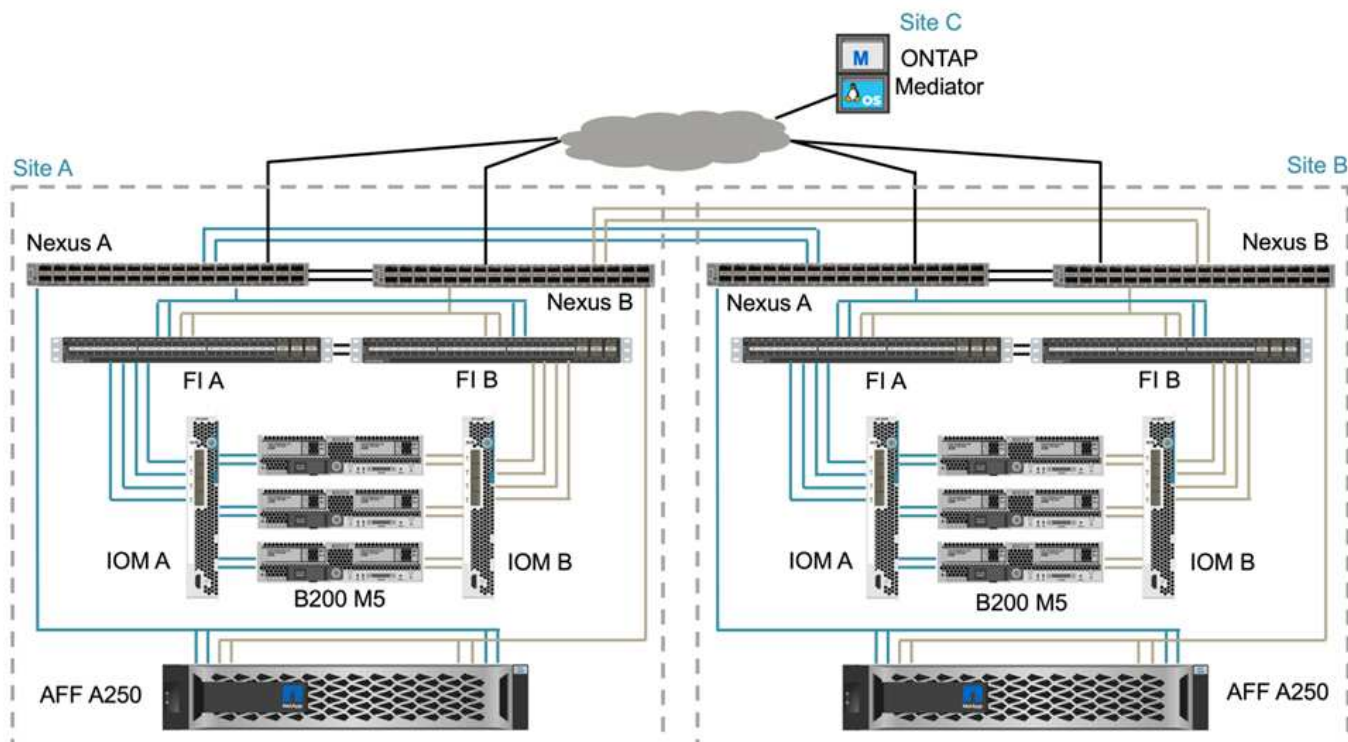
La figura seguente mostra una vista di alto livello sulla virtualizzazione della soluzione FlexPod SM-BC che include sia le funzionalità VMware ha che vMSC per fornire un'elevata disponibilità per i servizi di calcolo e storage. L'architettura della soluzione di data center Active-Active consente la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





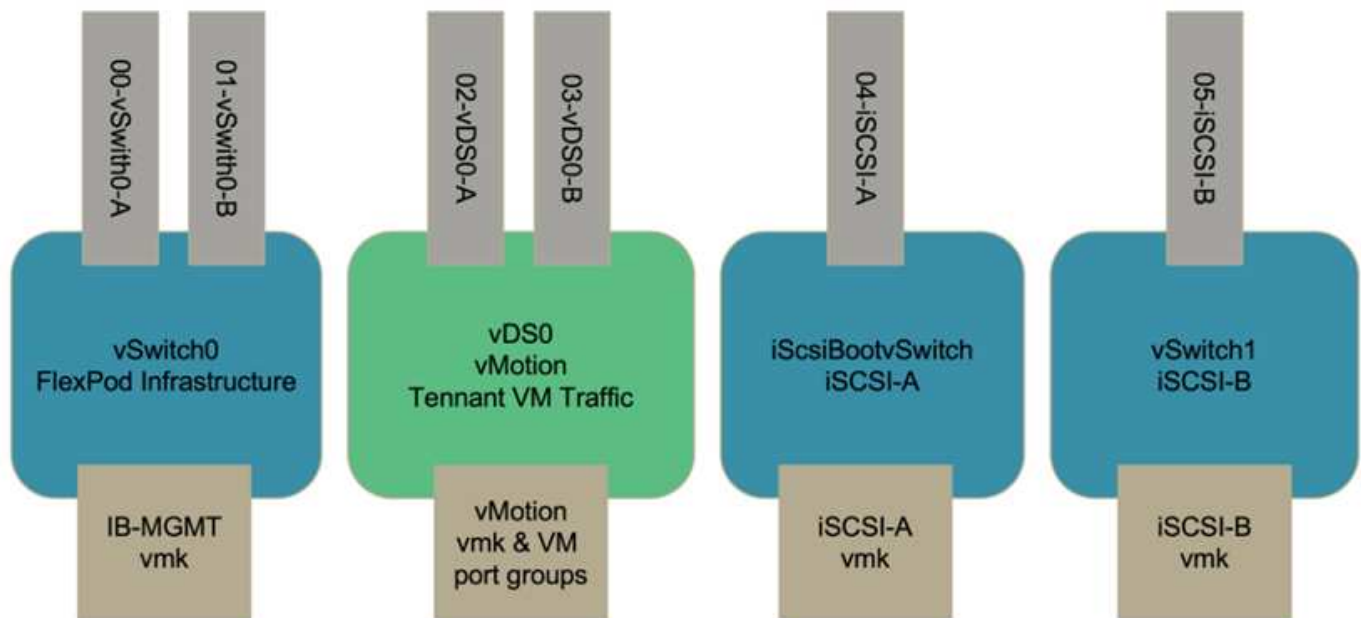
L'architettura di implementazione di FlexPod è identica in ogni sito per la convalida di questa soluzione. Tuttavia, la soluzione supporta implementazioni asimmetriche e può essere aggiunta a soluzioni FlexPod esistenti se soddisfano i requisiti.

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.

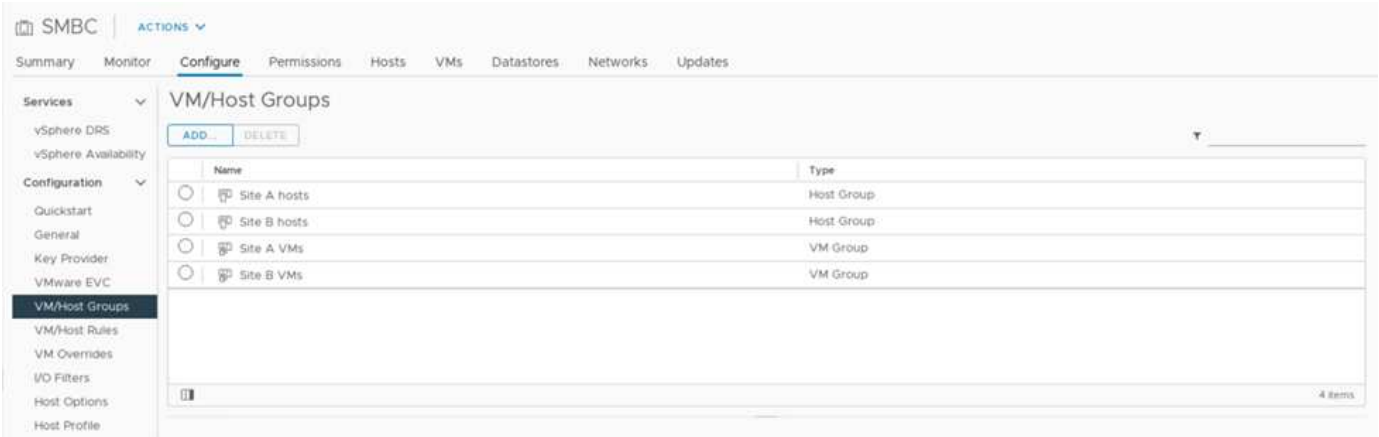
### Regole e gruppi di affinità VM-host

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.

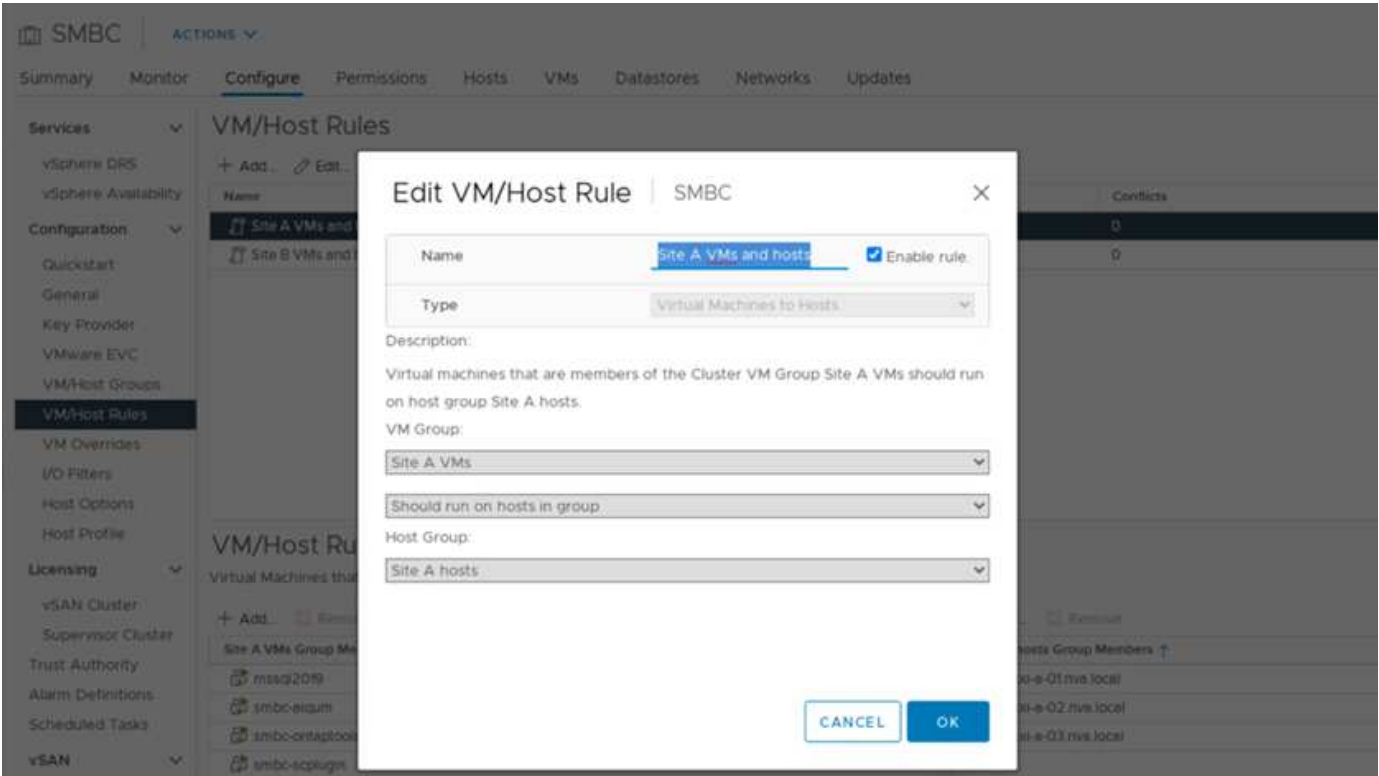
Per una macchina virtuale che utilizza datastore locali, l'accesso ai dischi virtuali diventa remoto se viene migrato a un host nel sito remoto e quindi aumenta la latenza delle operazioni di lettura a causa della distanza fisica tra i siti. Pertanto, è consigliabile mantenere le macchine virtuali sugli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

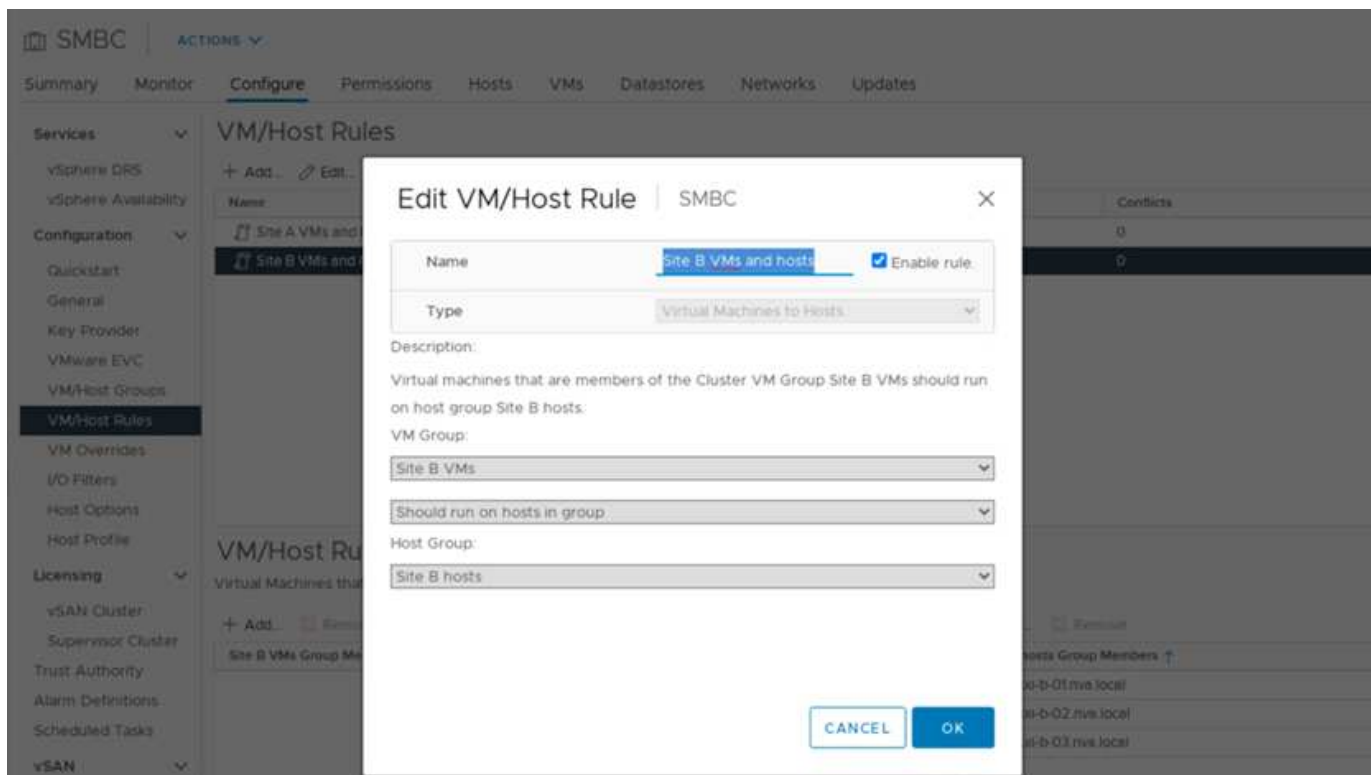
Utilizzando un meccanismo di affinità VM/host, è possibile utilizzare i gruppi VM/host per creare un gruppo VM e un gruppo host per macchine virtuali e host situati in un determinato sito. Utilizzando le regole VM/host, è possibile specificare il criterio per le macchine virtuali e gli host da seguire. 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".

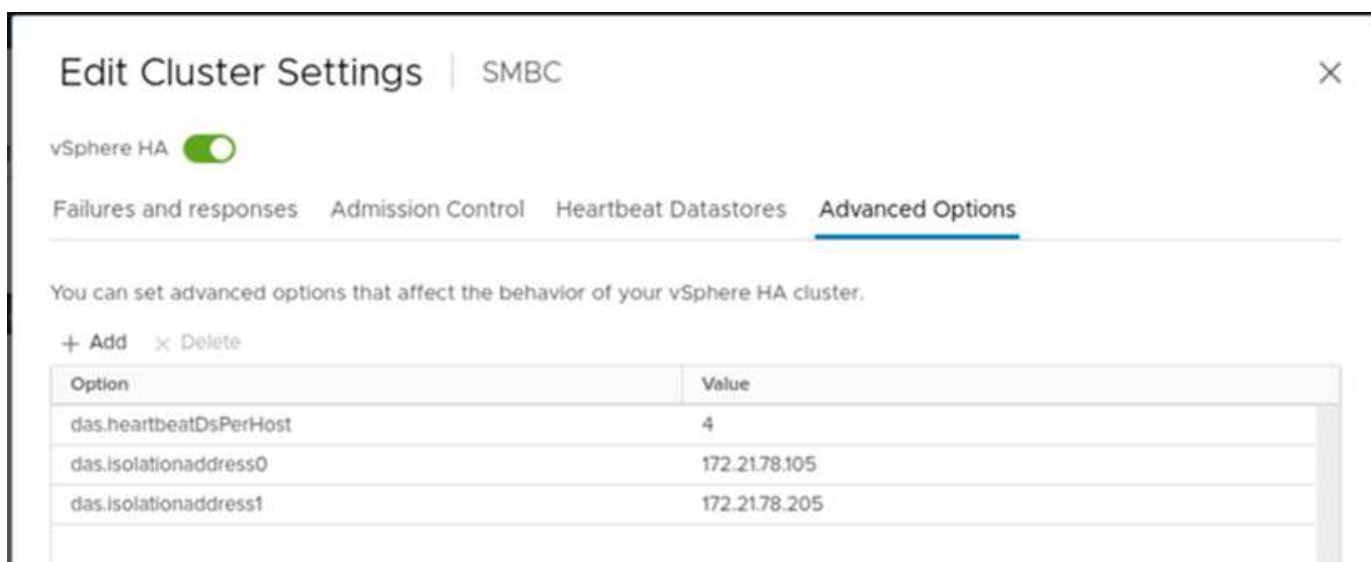




## VSphere ha heartbeat

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.

Edit Cluster Settings
SMBC

vSphere HA

Failures and responses
Admission Control
Heartbeat Datastores
Advanced Options

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 2 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

☐ Automatically select datastores accessible from the hosts  
☐ Use datastores only from the specified list  
☒ Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name	Datastore Cluster	Hosts Mounting Datastore ↓
<input type="checkbox"/>	infra_swap_a	N/A	6
<input type="checkbox"/>	infra_swap_b	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_b_02	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_a_01	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_a_02	N/A	6
<input checked="" type="checkbox"/>	infra_datastore_b_01	N/A	6

CANCEL
OK

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.

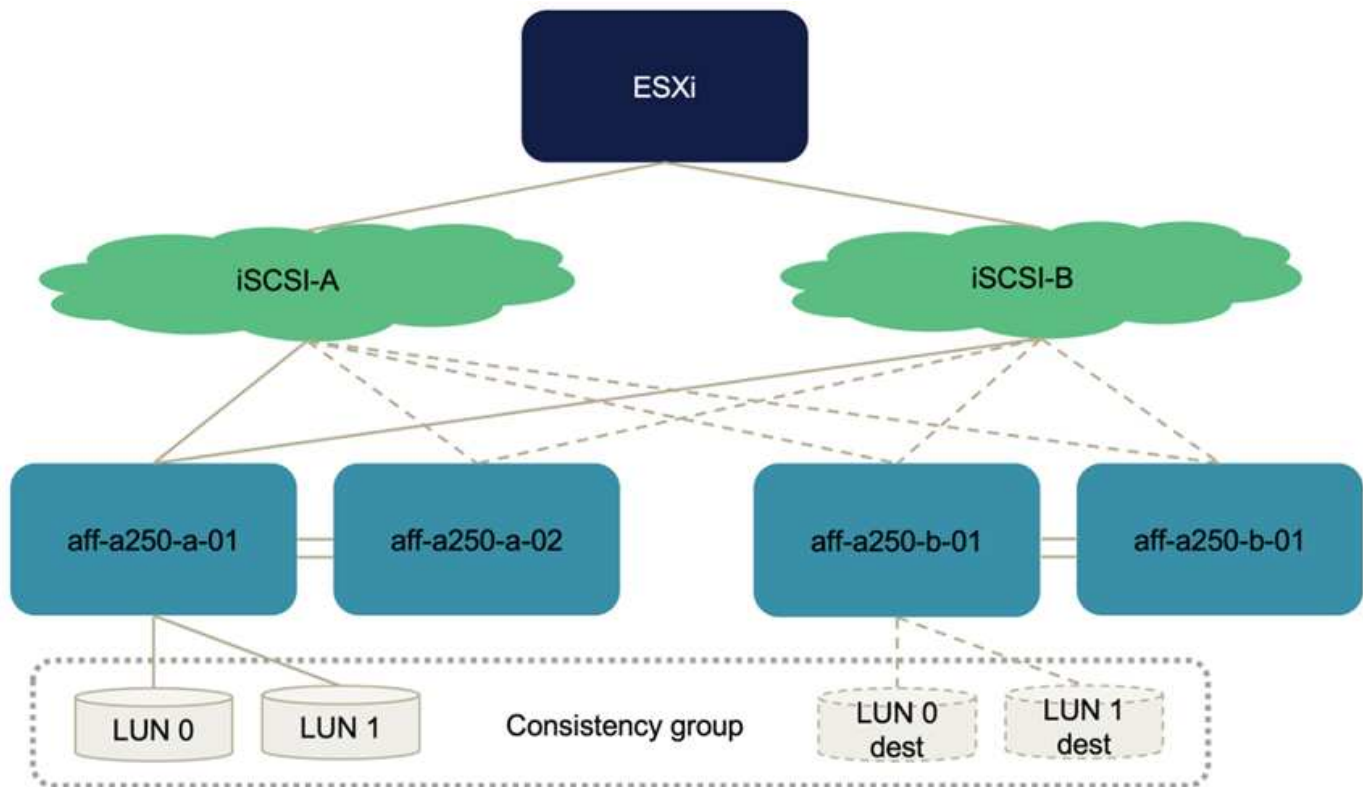
Oltre all'avvio di un host ESXi situato in un sito dalla propria LUN di avvio iSCSI locale, sono stati eseguiti test anche per avviare l'host ESXi quando il controller dello storage locale si trova in uno stato di Takeover o quando il cluster di storage locale non è completamente disponibile. Questi 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.





esxi-a-01.nva.local

ACTIONS

Summary

Monitor

Configure

Permissions

VMs

Datastores

Networks

Updates

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

TCP/IP configuration

Virtual Machines

VM Startup/Shutdown

Agent VM Settings

Default VM Compatibility

Swap File Location

System

Licensing

Host Profile

Time Configuration

Authentication Services

Storage Adapters

+

Add Software Adapter

↻

Refresh

🗑️

Rescan Storage...

🔄

Rescan Adapter

✖

Remove

Adapter	Type	Status	Identifier	Targets	Devices	Paths
Model: iSCSI Software Adapter						
vmhba64	iSCSI	Online	iscsi:vmkign.2010-11.com:flexpod-ucs-embc-a-1	8	7	56
Model: Lewisburg SATA AHCI Controller						
vmhba0	Block SCSI	Unknown	-	0	0	0

Copy All

2 items

Properties

Devices

Paths

Dynamic Discovery

Static Discovery

Network Port Binding

Advanced Options

Enable

Disable

Runtime Name	Target	LUN	Status
vmhba64.C0.T0.L0	iqn.1992-08.com:netapp.sn.2023c4ee6996f1ec86d8d039ee488168 vs. 3.172.2180.106.3260	0	Active (i/O)
vmhba64.C3.T0.L0	iqn.1992-08.com:netapp.sn.2023c4ee6996f1ec86d8d039ee488168 vs. 3.172.2180.107.3260	0	Active
vmhba64.C2.T0.L0	iqn.1992-08.com:netapp.sn.2023c4ee6996f1ec86d8d039ee488168 vs. 3.172.218106.3260	0	Active (i/O)
vmhba64.C1.T0.L0	iqn.1992-08.com:netapp.sn.2023c4ee6996f1ec86d8d039ee488168 vs. 3.172.218107.3260	0	Active
vmhba64.C0.T1.L0	iqn.1992-08.com:netapp.sn.b4db0fca5505f1ecbce10039ee487e72 vs. 3.172.2180.206.3260	0	Active
vmhba64.C1.T1.L0	iqn.1992-08.com:netapp.sn.b4db0fca5505f1ecbce10039ee487e72 vs. 3.172.2180.207.3260	0	Active
vmhba64.C2.T1.L0	iqn.1992-08.com:netapp.sn.b4db0fca5505f1ecbce10039ee487e72 vs. 3.172.2181.206.3260	0	Active
vmhba64.C3.T1.L0	iqn.1992-08.com:netapp.sn.b4db0fca5505f1ecbce10039ee487e72 vs. 3.172.2181.207.3260	0	Active

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.

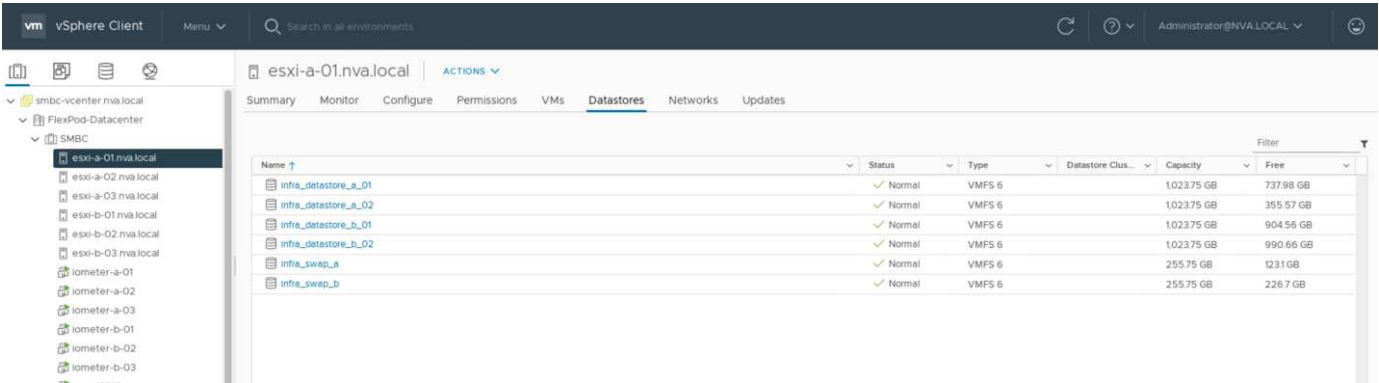
**Test di affinità di VMware vMotion e VM/host**

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.

## Migrate | iometer-a-01

✓ 1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

VM origin ⓘ

BATCH CONFIGURE

CONFIGURE PER DISK

CONFIGURE

<input type="checkbox"/>	Virtual Machine	File	Storage	Disk format	VM Storage Policy
<input type="checkbox"/>	iometer-a-01	Configuration File	infra_datastore_a_01	N/A	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 1 (64.00 GB)	infra_datastore_a_02	Same format as sour...	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 2 (20.00 GB)	infra_datastore_b_01	Same format as sour...	Datastore Default
<input type="checkbox"/>	iometer-a-01	Hard disk 3 (20.00 GB)	infra_datastore_b_02	Same format as sour...	Datastore Default



4 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

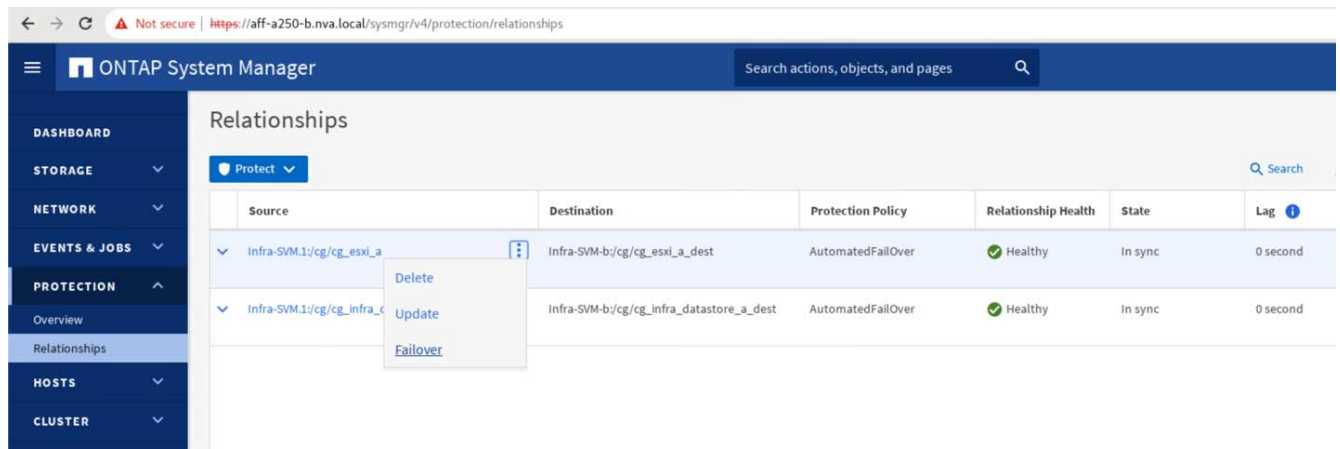
I test di vMotion delle macchine virtuali su un host diverso nello stesso sito e tra diversi siti sono stati eseguiti e sono stati eseguiti con successo. Dopo la migrazione manuale di una macchina virtuale tra i siti, la regola di affinità VM/host attiva e trasferisce nuovamente la macchina virtuale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

### Failover dello storage pianificato

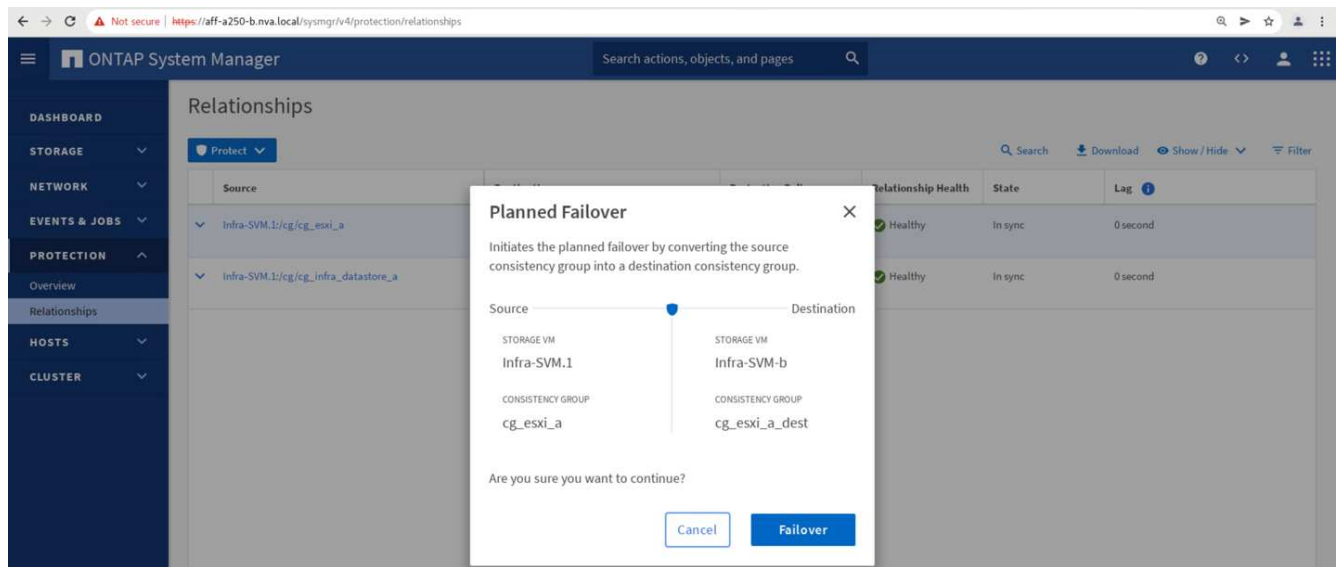
Le operazioni pianificate di failover dello storage devono essere eseguite sulla soluzione dopo la configurazione iniziale per determinare se la soluzione funziona correttamente dopo il failover dello storage. Il test può aiutare a identificare eventuali problemi di connettività o configurazione che 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.

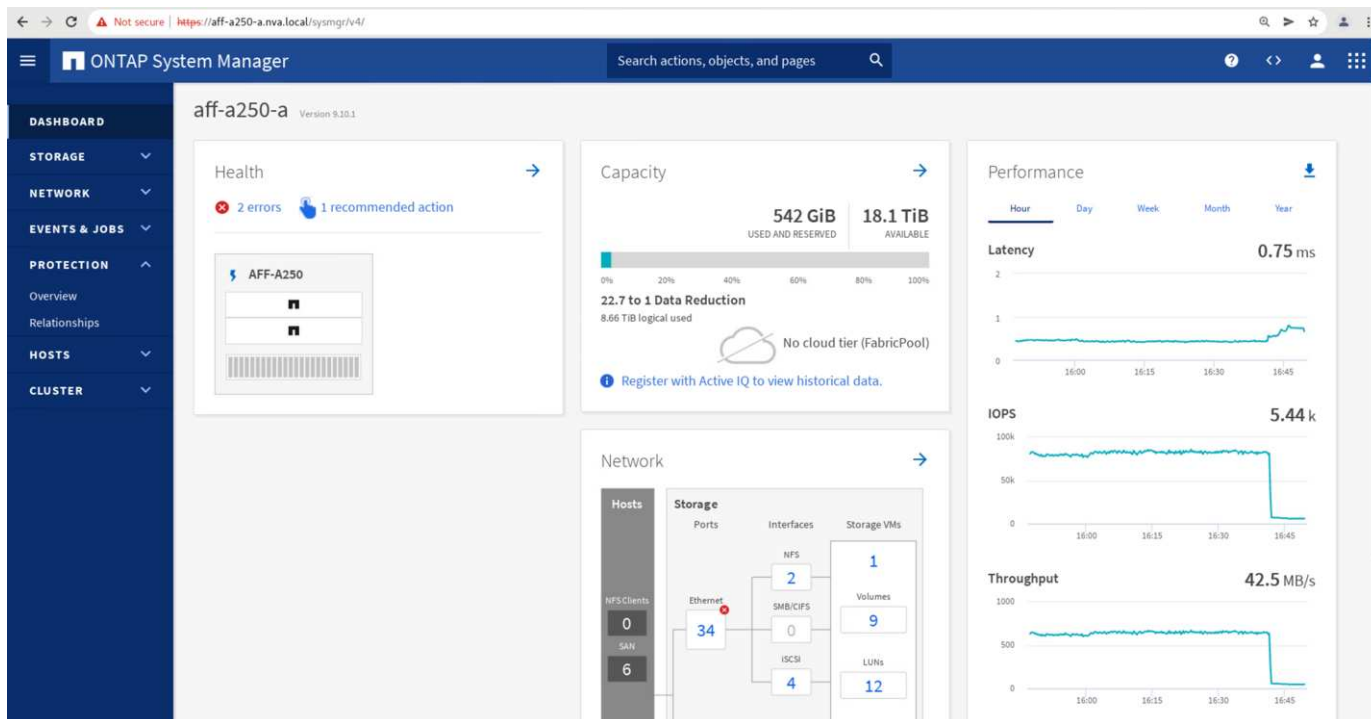
1. Accedere alla schermata protezione > Relazioni per verificare che lo stato della relazione del gruppo di coerenza sia In Sync. Se si trova ancora in Synchronizing state (stato), attendere che lo stato diventi In Sync prima di eseguire un failover.
2. Espandere i punti accanto al nome di origine e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



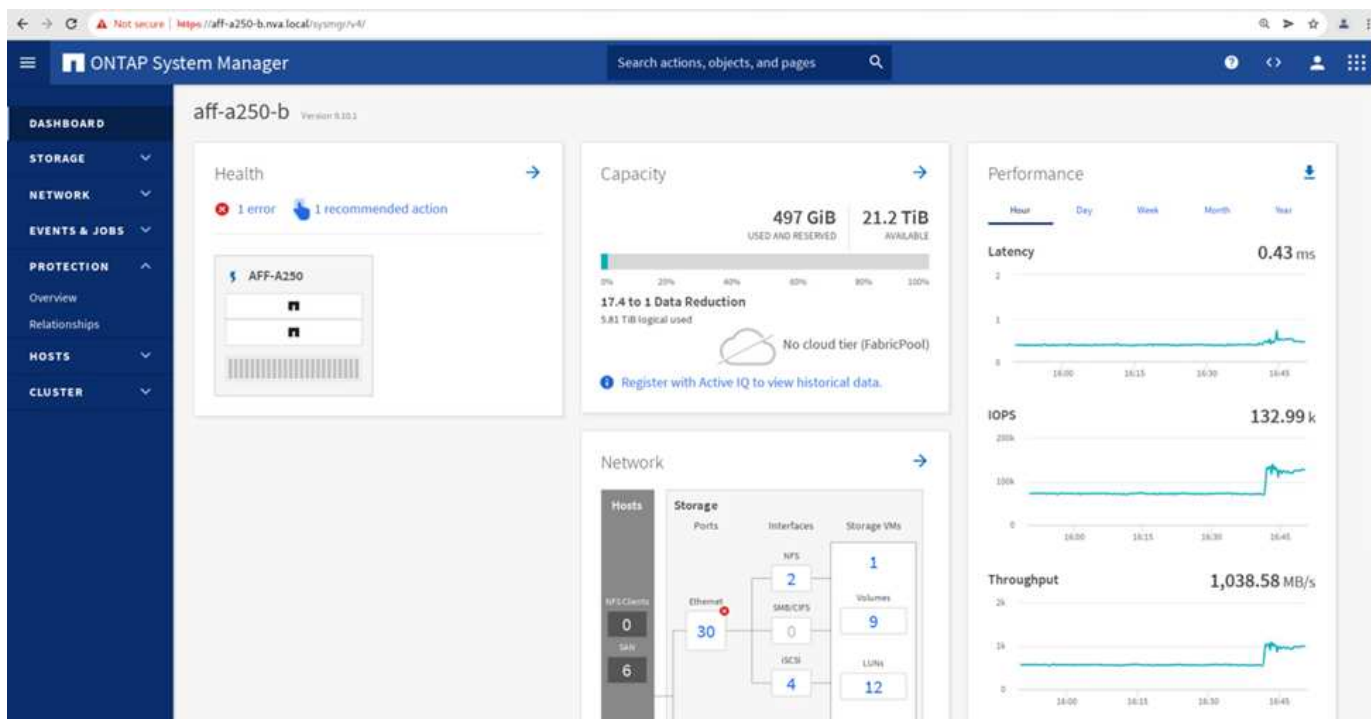
3. Confermare il failover per l'avvio dell'azione.



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.

Not secure | https://aff-a250-a.nva.local/sysmgr/v4/protection/relationships

ONTAP System Manager

Search actions, objects, and pages

Relationships

Protect

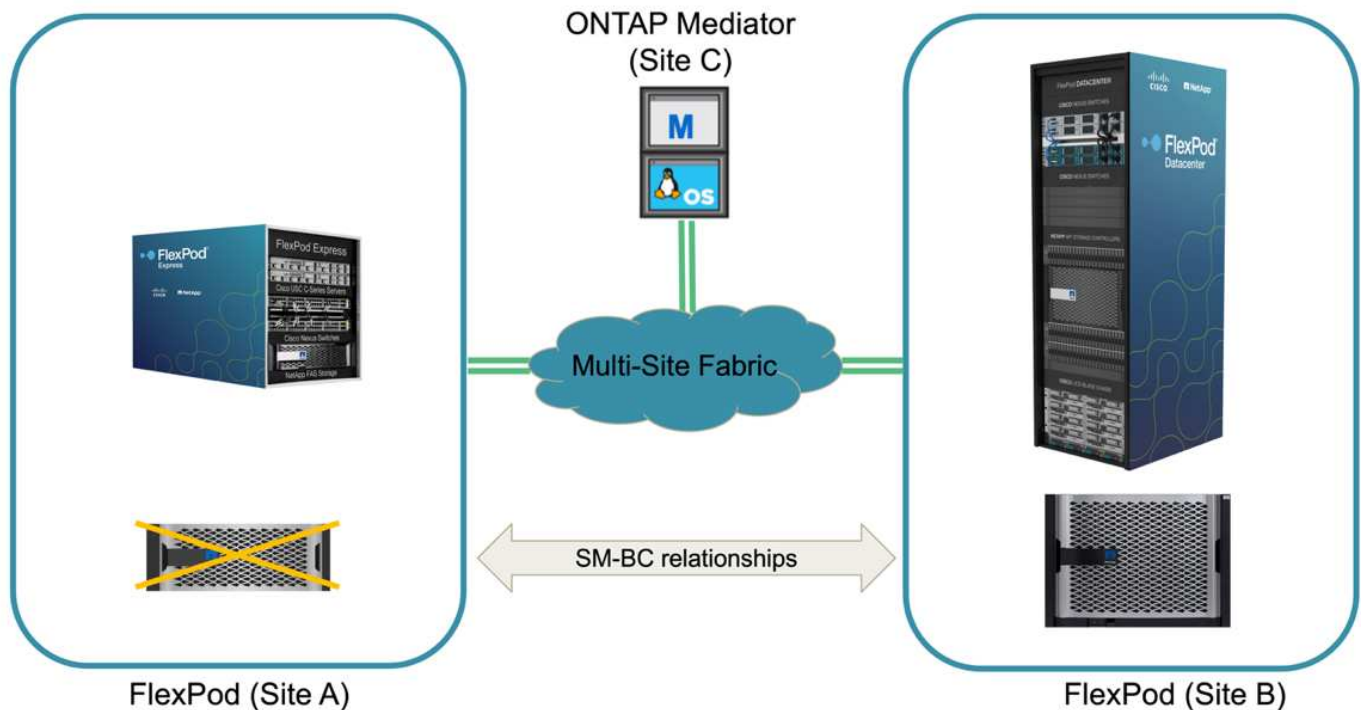
Search Download Show/Hide Filter

Source	Destination	Protection Policy	Relationship Health	State	Lag
Infra-SVM.1:/cg/cg_infra_datastore_b	Infra-SVM-a:/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1:/cg/cg_esxi_a_dest	Infra-SVM-a:/cg/cg_esxi_a	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1:/cg/cg/	Infra-SVM-a:/cg/cg_infra_datastore_a	AutomatedFailOver	Healthy	In sync	0 second
Infra-SVM.1:/cg/cg/	Infra-SVM-a:/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

Delete Update Failover

## 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.



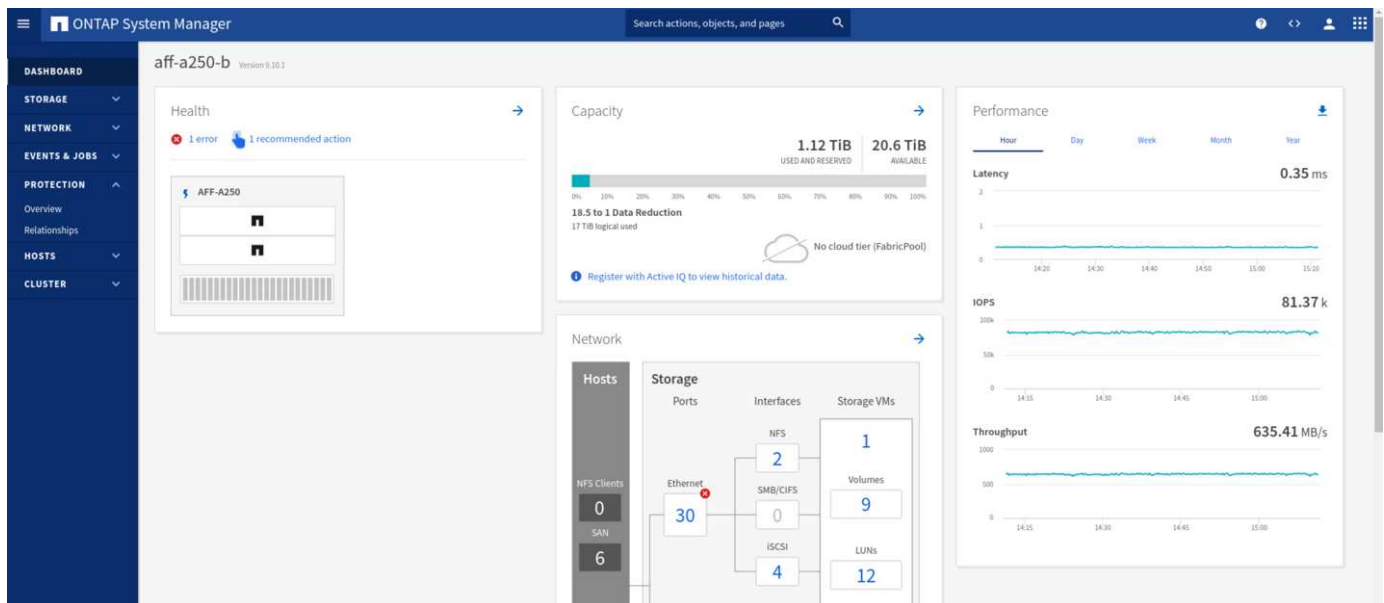
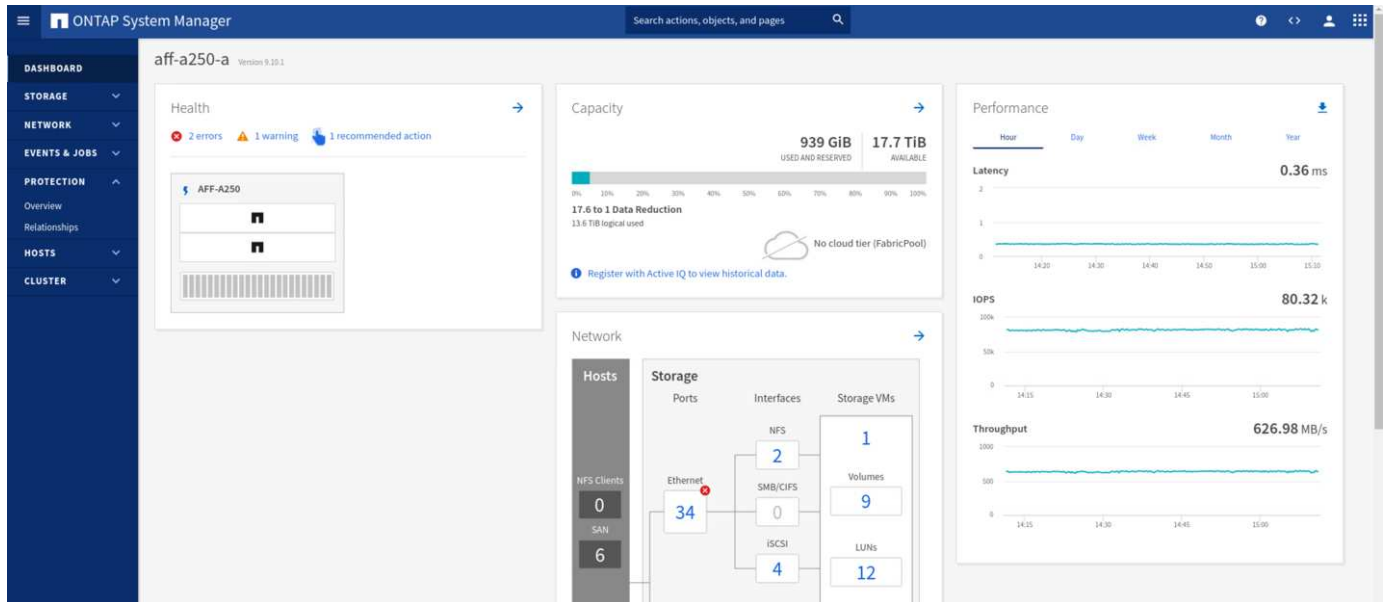
Per simulare un disastro dello storage nel sito A, è possibile spegnere entrambi i controller dello storage nel sito A spegnendo fisicamente l'interruttore di alimentazione per interrompere l'alimentazione dei controller, oppure utilizzando il comando di gestione dell'alimentazione del sistema dei processori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

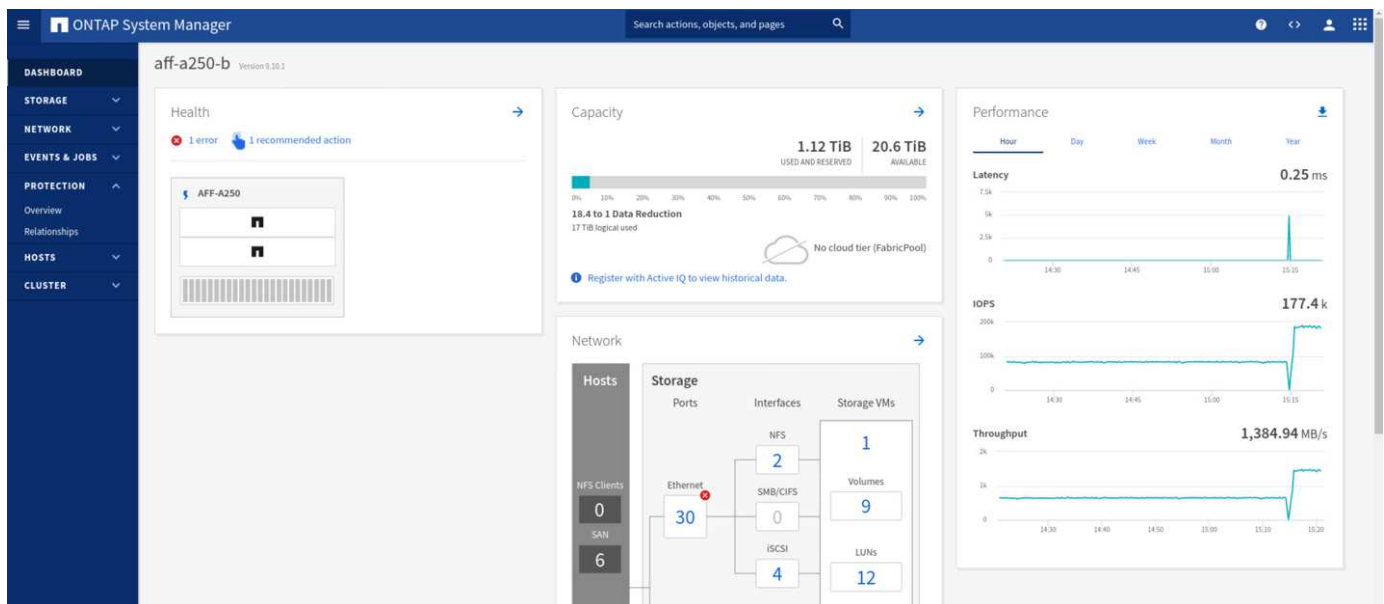
stato del percorso per i LUN e quindi riprende l'i/o sui percorsi disponibili per i controller di storage del sito B sopravvissuti.

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 riaccesso 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.

The screenshot shows the ONTAP System Manager Relationships page. The table lists the following relationships:

Source	Destination	Protection Policy	Relationship Health	State	Lag
infra-SVM.1/cg/cg_esxi_a	infra-SVM-b/cg/cg_esxi_a_dest	AutomatedFailOver	Healthy	Out of sync	1 hour, 22 minutes and 56 seconds
infra-SVM.1/cg/cg_infra_datastore_a	infra-SVM-b/cg/cg_infra_datastore_a_dest	AutomatedFailOver	Healthy	Out of sync	1 hour, 29 minutes and 35 seconds

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 ripristinate 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.

The screenshot shows the ONTAP System Manager Relationships page. The table lists the following relationships:

Source	Destination	Protection Policy	Relationship Health	State	Lag
infra-SVM.1/cg/cg_infra_datastore_b	infra-SVM-a/cg/cg_infra_datastore_b_dest	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_esxi_a_dest	infra-SVM-a/cg/cg_esxi_a	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_infra_datastore_a_dest	infra-SVM-a/cg/cg_infra_datastore_a	AutomatedFailOver	Healthy	In sync	0 second
infra-SVM.1/cg/cg_esxi_b	infra-SVM-a/cg/cg_esxi_b_dest	AutomatedFailOver	Healthy	In sync	0 second

## 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.

Edit VM/Host Rule

SMBC

×

Name

Site A VMs and hosts

☒ Enable rule.

Type

Virtual Machines to Hosts

▼

Description:

Virtual machines that are members of the Cluster VM Group Site A VMs must run on host group Site B hosts.

VM Group:

Site A VMs

▼

Must run on hosts in group

▼

Host Group:

Site B hosts

▼

CANCEL

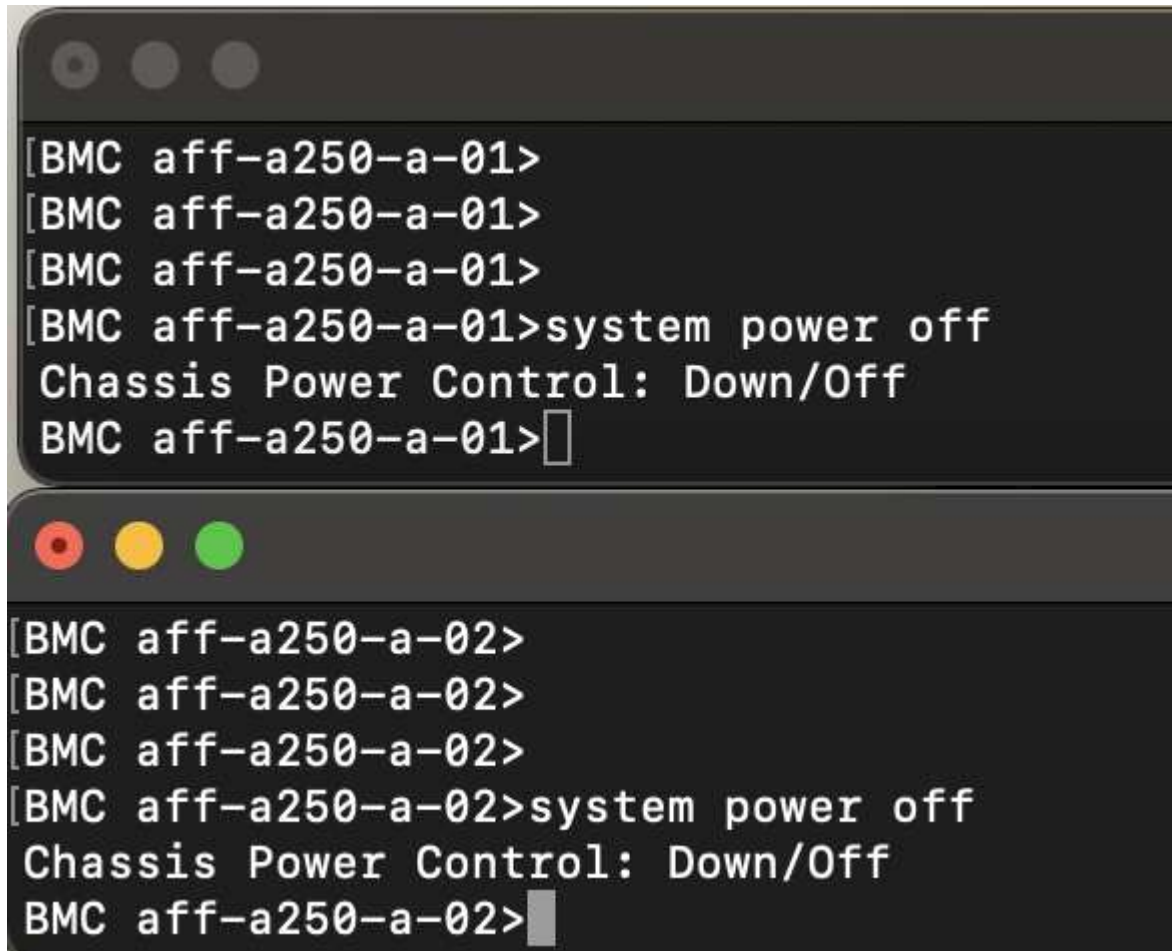
OK

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 rilevato 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 storage è stata utilizzata per spegnere il sito. Di un cluster in modo brusco per simulare un disastro dello storage nel sito.



```
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>
[BMC aff-a250-a-01>system power off
Chassis Power Control: Down/Off
BMC aff-a250-a-01>

[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>
[BMC aff-a250-a-02>system power off
Chassis Power Control: Down/Off
BMC aff-a250-a-02>
```

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 NAbbox 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 downtime 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.

Microsoft SQL Server TPROC-C Build Options

Build Options

SQL Server: (local)

TCP: ☐

SQL Server Port: 1433

Azure: ☐

SQL Server ODBC Driver: ODBC Driver 17 for SQL Server

Authentication: ☒ Windows Authentication  
☐ SQL Server Authentication

SQL Server User ID: sa

SQL Server User Password: admin

TPROC-C SQL Server Database: tpcc

In-Memory OLTP: ☐

In-Memory Hash Bucket Multiplier: 1

In-Memory Durability: ☒ SCHEMA\_AND\_DATA  
☐ SCHEMA\_ONLY

Number of Warehouses: 100

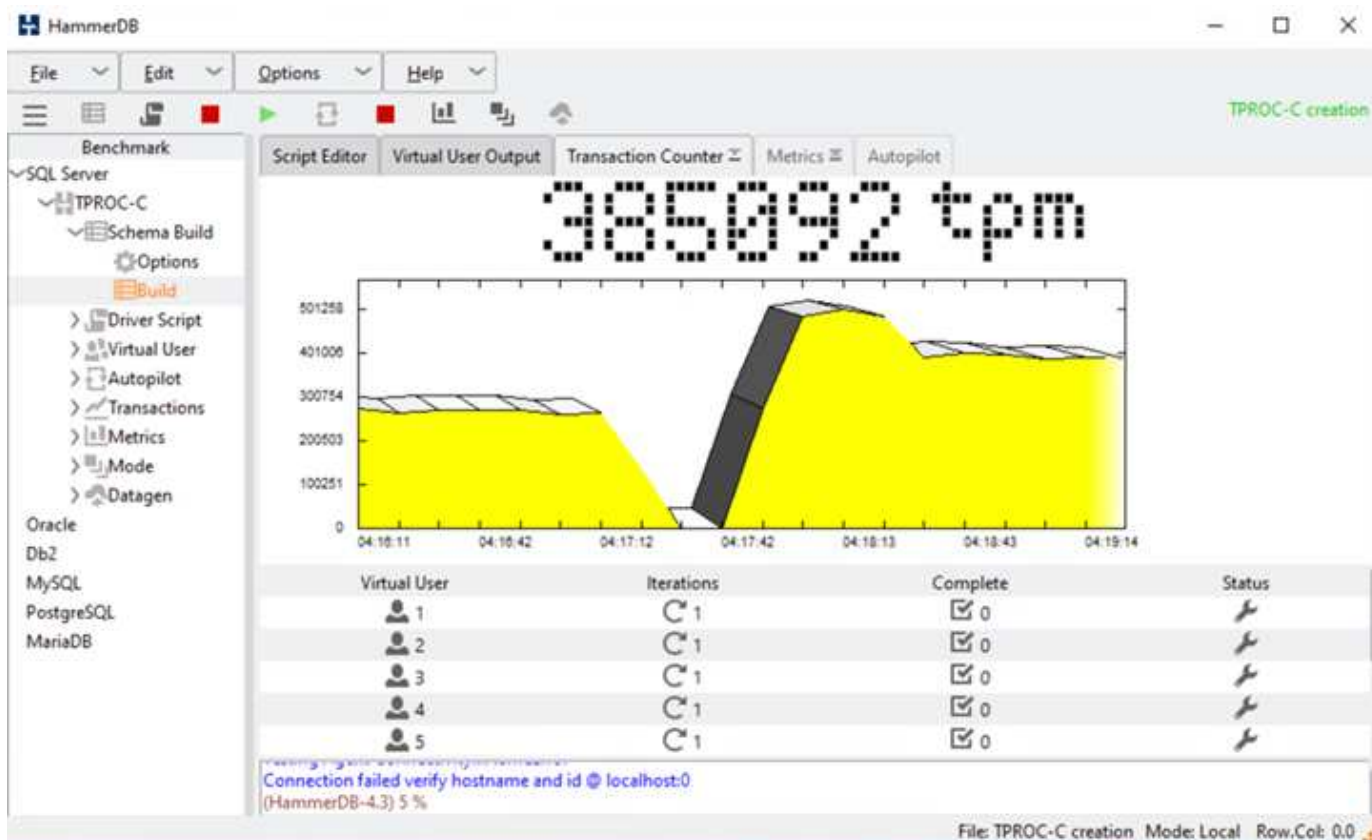
Virtual Users to Build Schema: 10

OK Cancel

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.

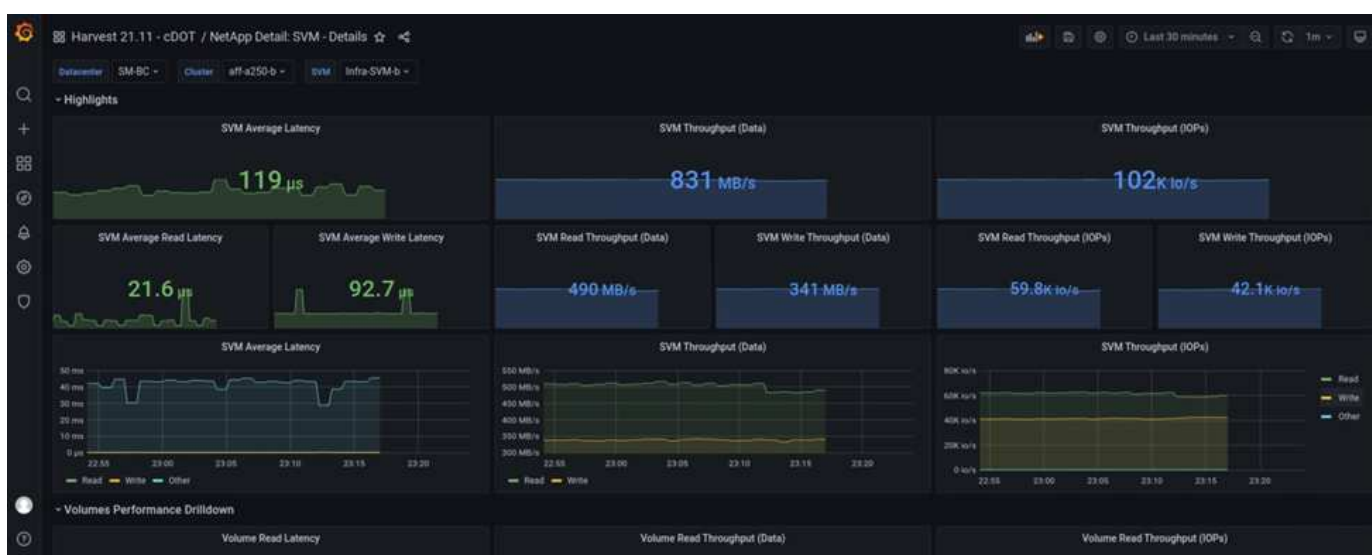
Dopo una breve pausa delle transazioni del database, è stato attivato il failover automatico per la risoluzione dei problemi e le transazioni sono state riavviate. La seguente schermata mostra la schermata di HammerDB Transaction Counter. Poiché il database per Microsoft SQL Server risiede normalmente 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 storage sono state acquisite utilizzando il tool NAbbox 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 metriche 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 NAbbox 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"](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"](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"](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/"](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"](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"](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"](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"](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"](https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf)

- NAbbox

["https://nabox.org"](https://nabox.org)

- NetApp Harvest

["https://github.com/NetApp/harvest/releases"](https://github.com/NetApp/harvest/releases)

## SM-BC

- SM-BC

["https://docs.netapp.com/us-en/ontap/smbc/index.html"](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"](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"](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"](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"](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"](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"](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-vmcsc"](https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmcsc)

- Procedure consigliate per VMware vSphere Metro Storage Cluster

["https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"](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"](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"](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"](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"](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"](https://www.hammerdb.com)

## Matrice di compatibilità

- Matrice di compatibilità hardware Cisco UCS

["https://ucshcltool.cloudapps.cisco.com/public/"](https://ucshcltool.cloudapps.cisco.com/public/)

- Tool di matrice di interoperabilità NetApp

["https://support.netapp.com/matrix/"](https://support.netapp.com/matrix/)

- NetApp Hardware Universe

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

- Guida alla compatibilità VMware

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

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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