Cloud ibrido FlexPod con Cloud Volumes ONTAP per Epic

FlexPod

NetApp
March 25, 2024

Sommario

Cloud ibrido FlexPod con Cloud Volumes ONTAP per Epic

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

In collaborazione con: CISCO

Kamini Singh, NetApp

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

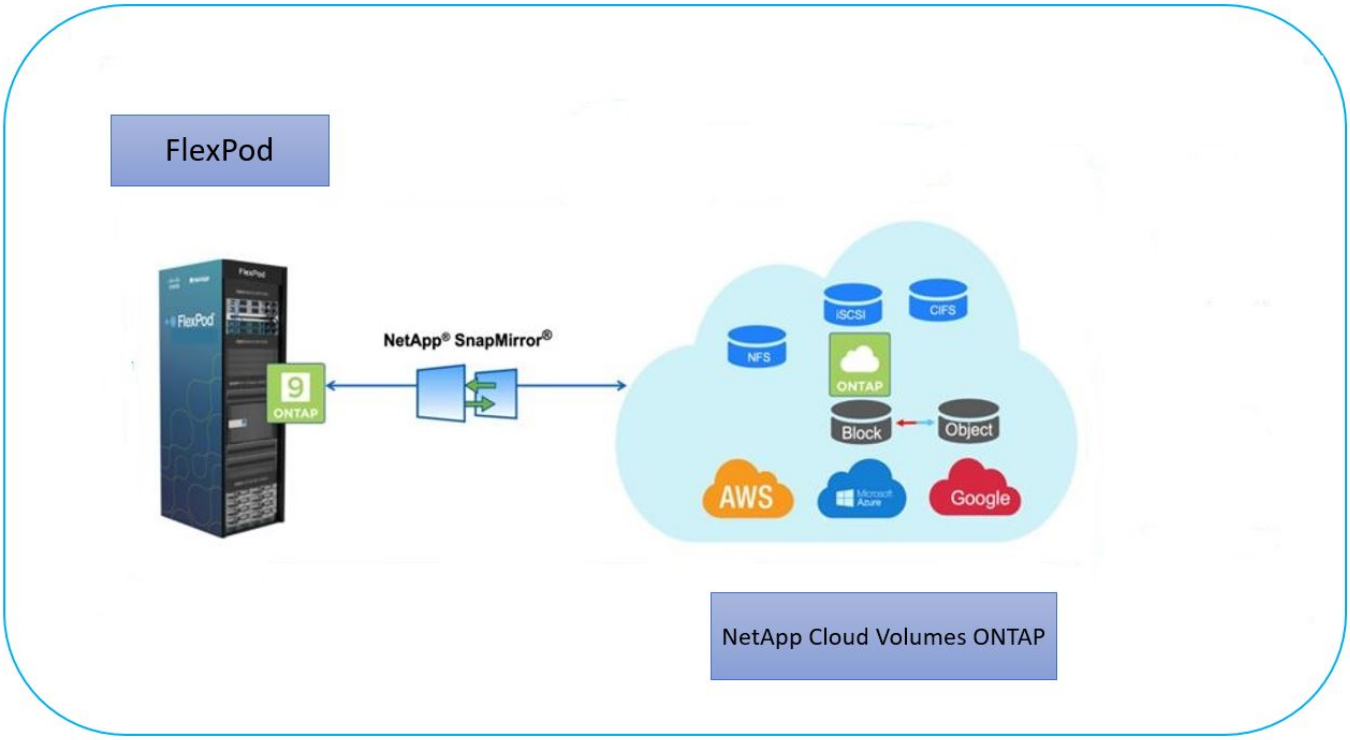
Le dimensioni in costante aumento dei dati sanitari e le preziose informazioni che questi dati possono fornire rendono i servizi dati sanitari e la protezione dei dati critici e impegnativi. Innanzitutto, i dati del settore sanitario devono essere sia disponibili che protetti per soddisfare i requisiti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

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

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

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

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



Pubblico

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

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

Vantaggi della soluzione

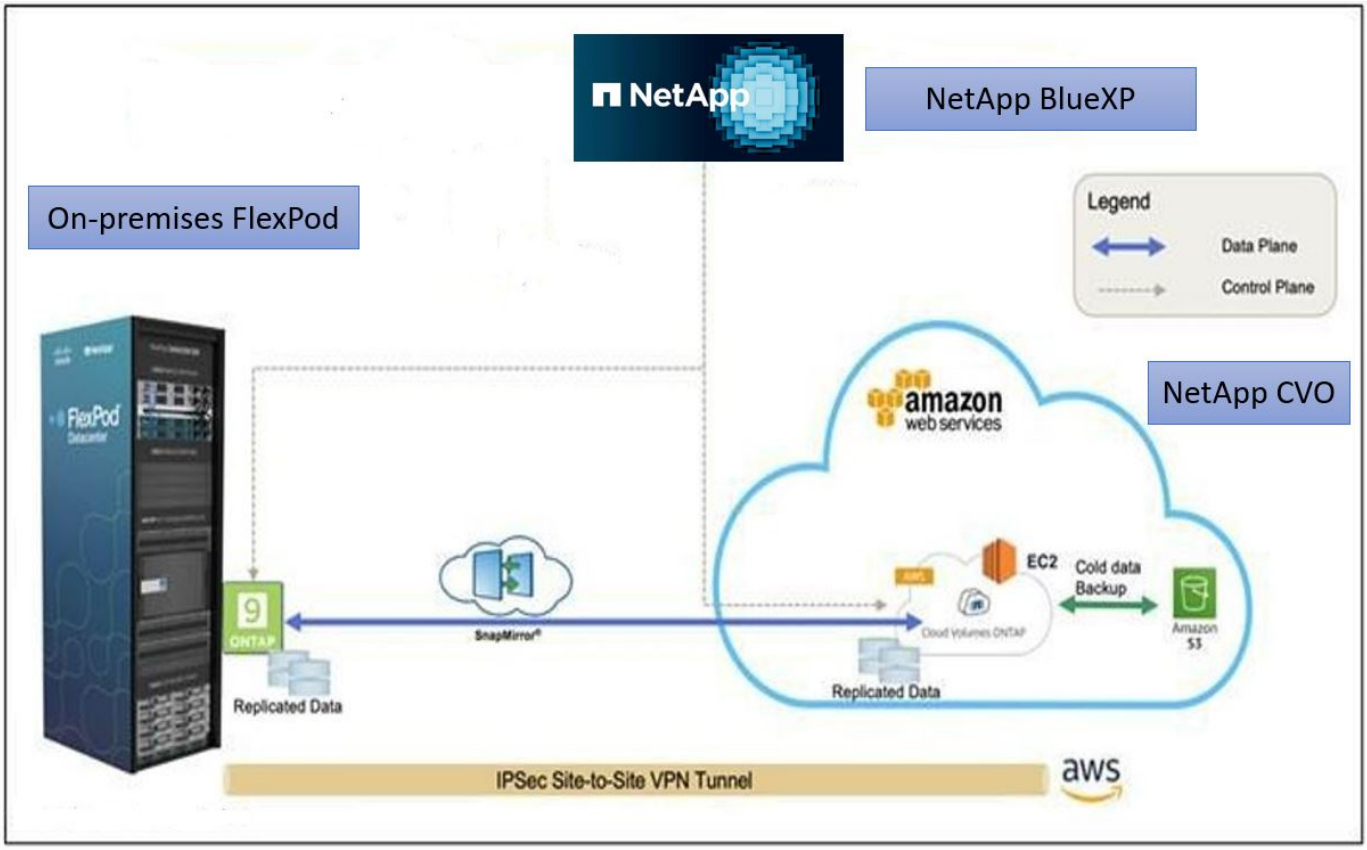
Il data center FlexPod integrato con NetApp Cloud Volumes ONTAP offre i seguenti vantaggi ai carichi di lavoro del settore sanitario:

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

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

Topologia della soluzione

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



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

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

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

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

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

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

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

EHR

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

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

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

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

NetApp BlueXP

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

Connettore

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

Il connettore è supportato nelle seguenti posizioni:

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

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

NetApp Cloud Volumes ONTAP

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

I vantaggi principali includono:

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

Per ulteriori informazioni, vedere "Cloud Volumes ONTAP".

NetApp Active IQ Unified Manager

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

macchina virtuale offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter analizzare l'intero percorso di i/o dall'host vSphere fino alla rete e infine allo storage.

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

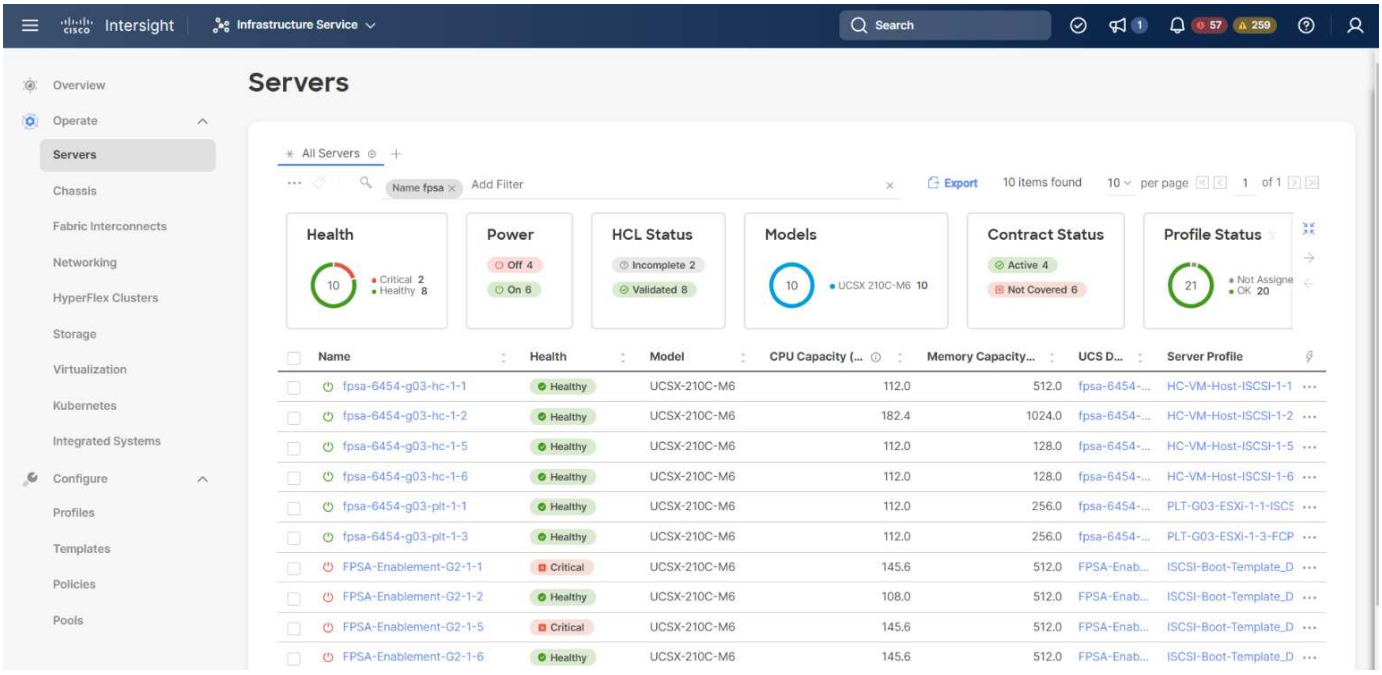
Per ulteriori informazioni, vedere "Active IQ Unified Manager".

Cisco Intersight

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

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

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



VMware vSphere 7.0

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

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

VMware vCenter Server

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

Per informazioni dettagliate, vedere "VMware vCenter".

Revisioni hardware e software

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

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

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

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

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

Vendor	Prodotto	Versione
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9.11

"Pagina successiva: Installazione e configurazione."

Installazione e configurazione

"Precedente: Componenti della soluzione."

Implementazione di NetApp Cloud Volumes ONTAP

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

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

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

2. Configurare il gateway dell'endpoint VPC.

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

3. Accedi a NetApp BlueXP.

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

4. Implementare il connettore.

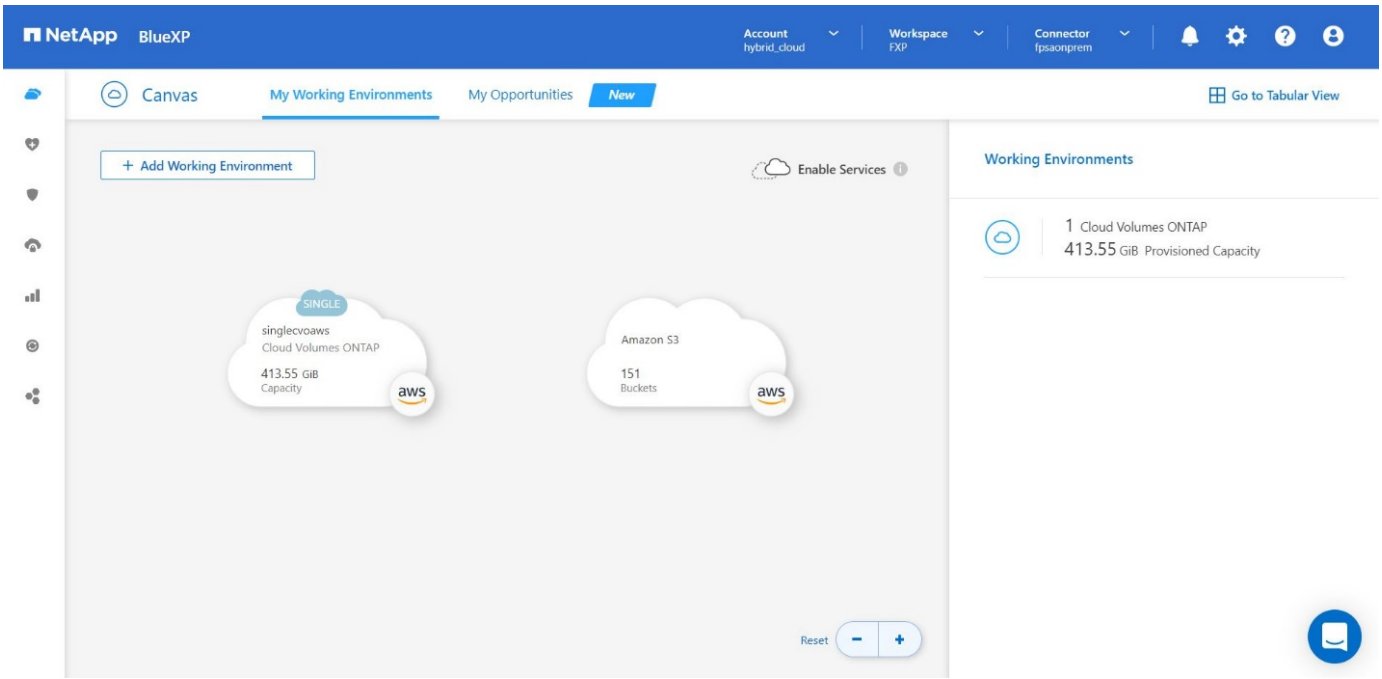
   Prima di aggiungere un ambiente di lavoro Cloud Volume ONTAP, è necessario implementare Connector. BlueXP richiede se si tenta di creare il primo ambiente di lavoro Cloud Volumes ONTAP senza il connettore. Per implementare il connettore in AWS da BlueXP, consulta questa sezione "collegamento".

5. Avviare Cloud Volumes ONTAP in AWS.

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

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

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



Implementazione FlexPod on-premise

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

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

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

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

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

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

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

Configurazione dello storage ONTAP on-premise

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

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

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

   To verify:

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

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

2. Creare un volume FlexVol.

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

3. Aggiunta di interfacce per l'accesso iSCSI.

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

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

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

4. Creare un LUN.

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

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

5. Creare un igroup.

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

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

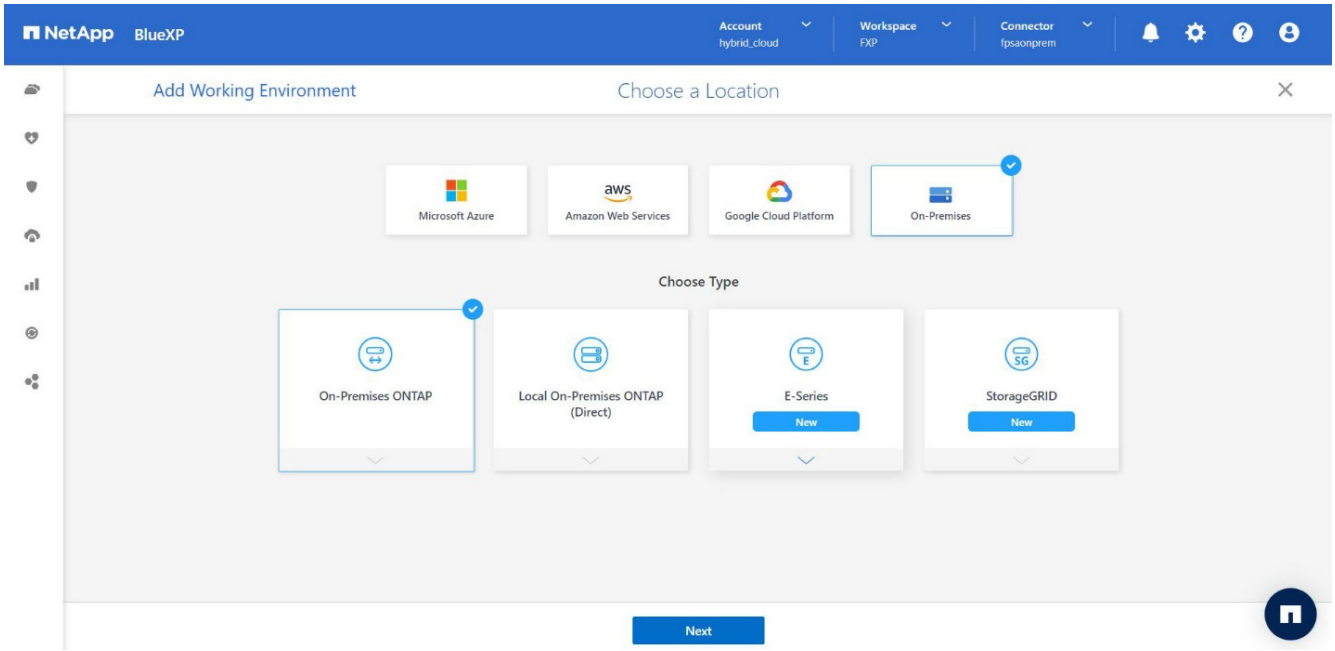
6. Mappare il LUN sull'igroup.

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

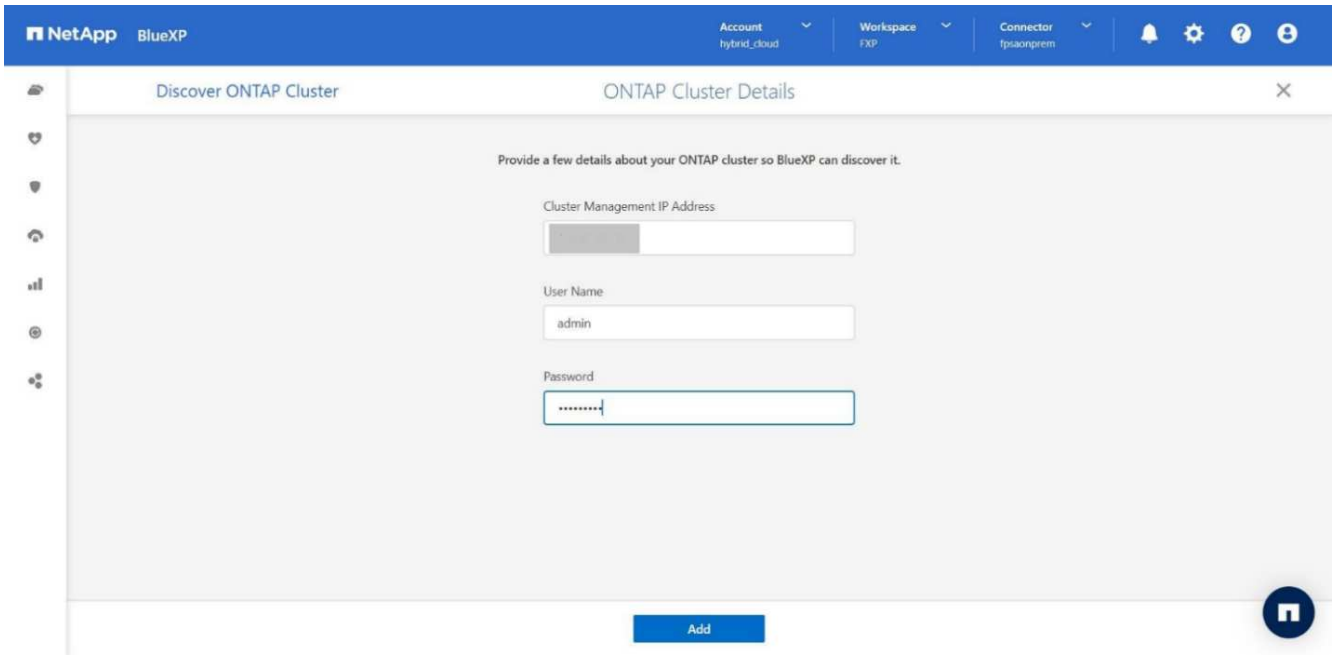
Aggiunta di storage FlexPod on-premise a BlueXP

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

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

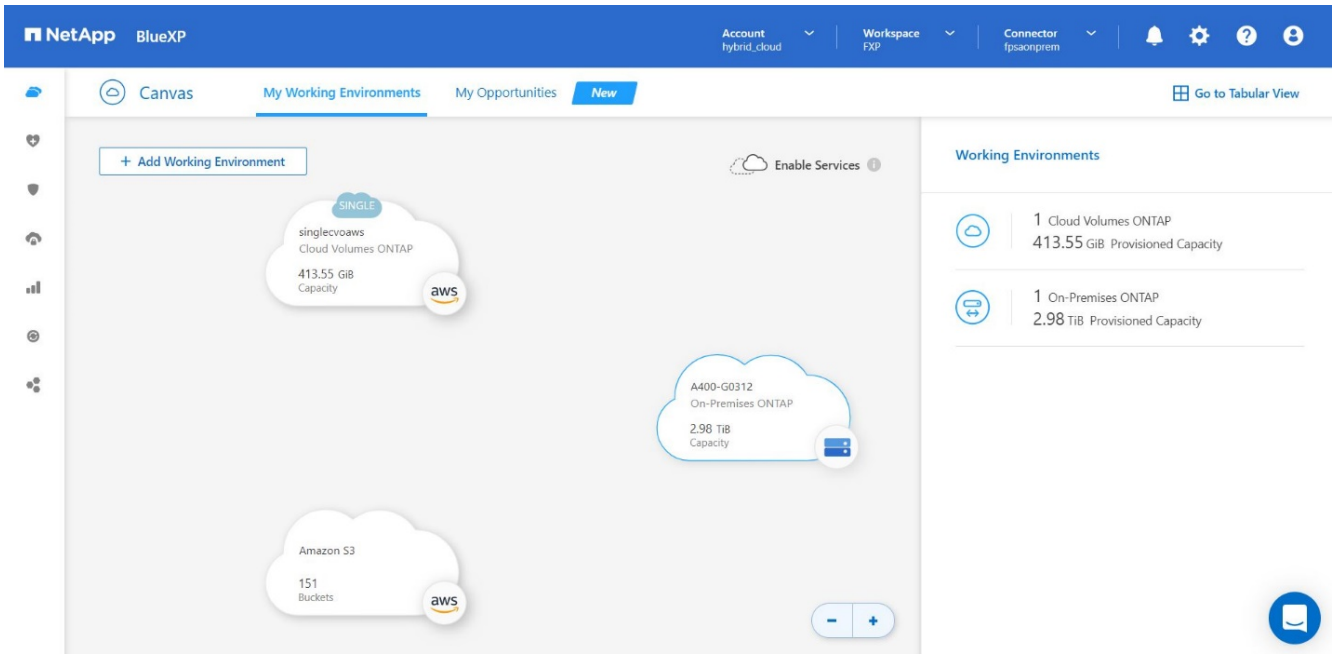


4. Nella pagina Dettagli cluster ONTAP, inserire l'indirizzo IP di gestione del cluster e la password per l'account utente admin. Quindi fare clic su **Aggiungi**.



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

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



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

"Pagina successiva: Configurazione SAN."

Configurazione SAN

"Precedente: Installazione e configurazione."

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

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

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

Kit di utility host NetApp

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

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

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

Scopri lo storage ONTAP

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

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

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

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

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

Configurare il multipathing

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

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

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

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

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

3. Attivare e avviare i servizi multipath.

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

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

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

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

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

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

Creare un volume fisico

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

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

Creare un gruppo di volumi

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

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

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

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

Creare un volume logico

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

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Questo comando crea un volume logico chiamato `datalv` che utilizza tutto lo spazio non allocato nel gruppo di volumi `datavg`.

Creare il file system

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Creare la cartella da montare

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Montare il file system

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

Per informazioni dettagliate su queste attività, vedere la pagina "Amministrazione di LVM con comandi CLI".

Generazione di dati

```
`Dgen.pl` È un generatore di dati di script perl per il simulatore i/o di
EHR (GenerateIO). I dati all'interno dei LUN vengono generati con l'EHR
`Dgen.pl` script. Lo script è progettato per creare dati simili a quelli
che si trovano all'interno di un database EHR.
```

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                 1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

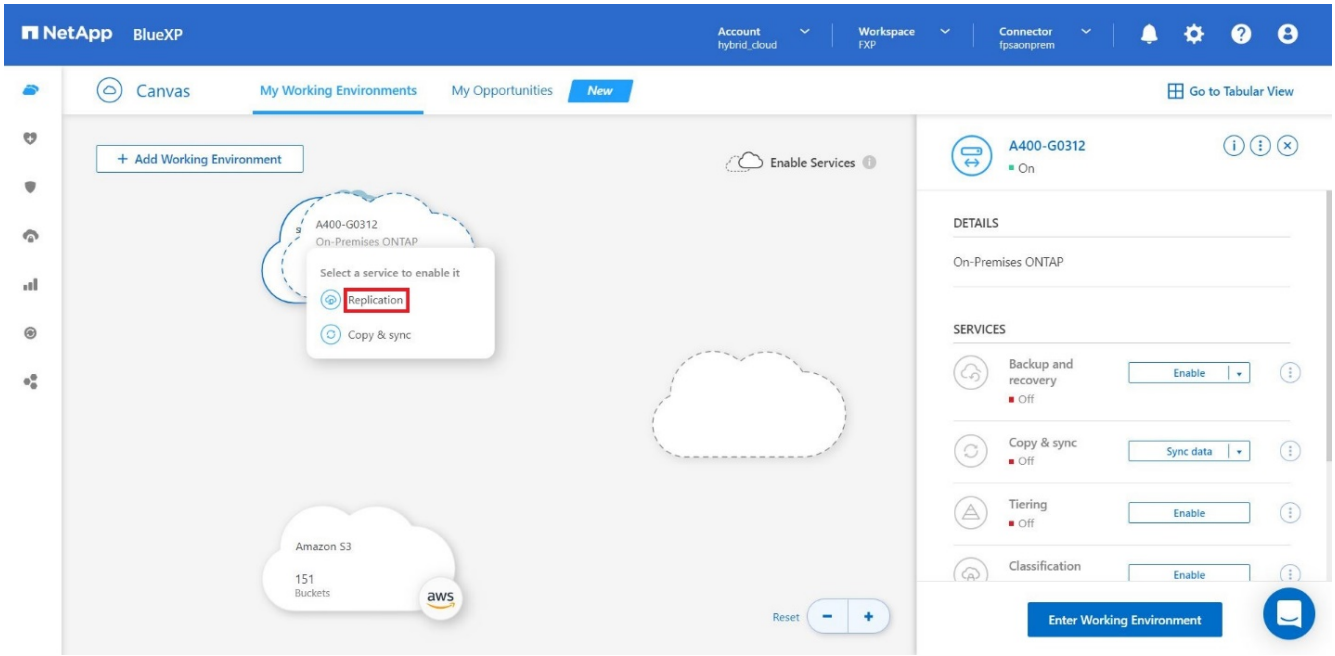
Durante la corsa `Dgen.pl` per impostazione predefinita, lo script utilizza il 85% del file system per la generazione dei dati.

Configurare la replica di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP

NetApp SnapMirror replica i dati a velocità elevate su LAN o WAN, in modo da ottenere un'elevata disponibilità dei dati e una replica rapida dei dati in ambienti virtuali e tradizionali. Quando si replicano i dati nei sistemi storage NetApp e si aggiornano continuamente i dati secondari, i dati vengono mantenuti aggiornati e rimangono disponibili ogni volta che ne hai bisogno. Non sono richiesti server di replica esterni.

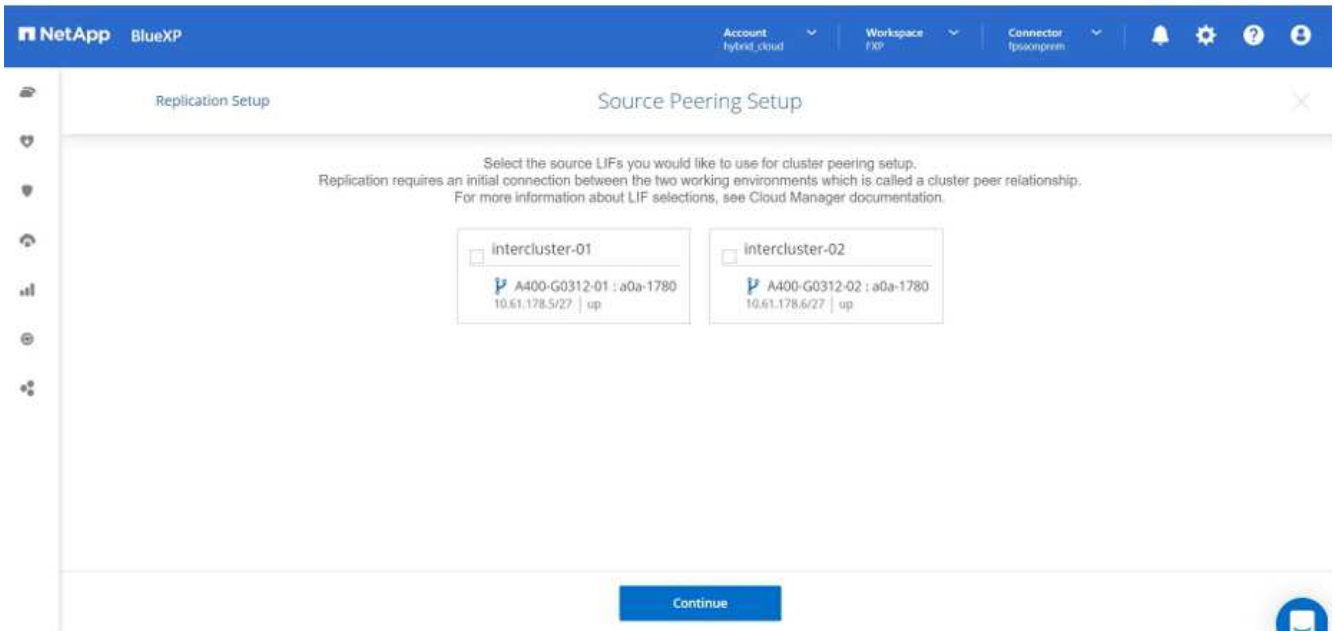
Completare i seguenti passaggi per configurare la replica di SnapMirror tra il sistema ONTAP on-premise e CVO.

1. Dal menu di navigazione, selezionare **Storage** > **Canvas**.
2. In Canvas, selezionare l'ambiente di lavoro che contiene il volume di origine, trascinarlo nell'ambiente di lavoro in cui si desidera replicare il volume, quindi selezionare **Replication**.

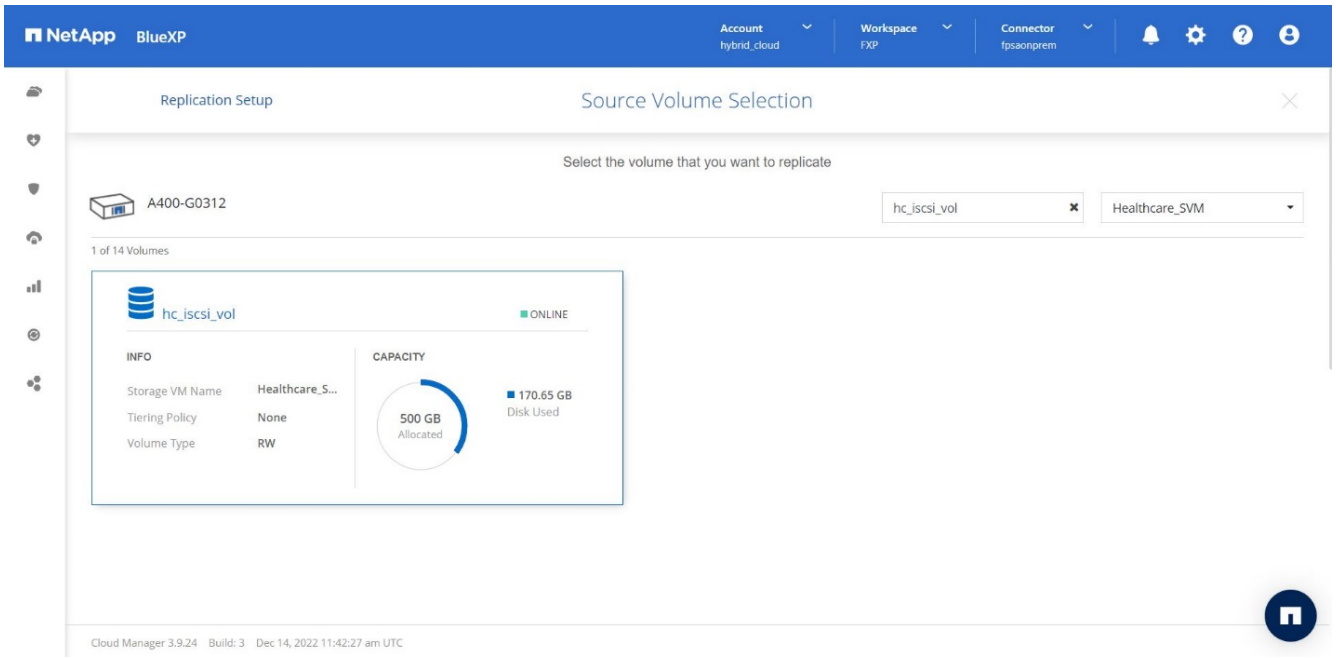


I passaggi rimanenti spiegano come creare una relazione sincrona tra cluster Cloud Volumes ONTAP e ONTAP on-premise.

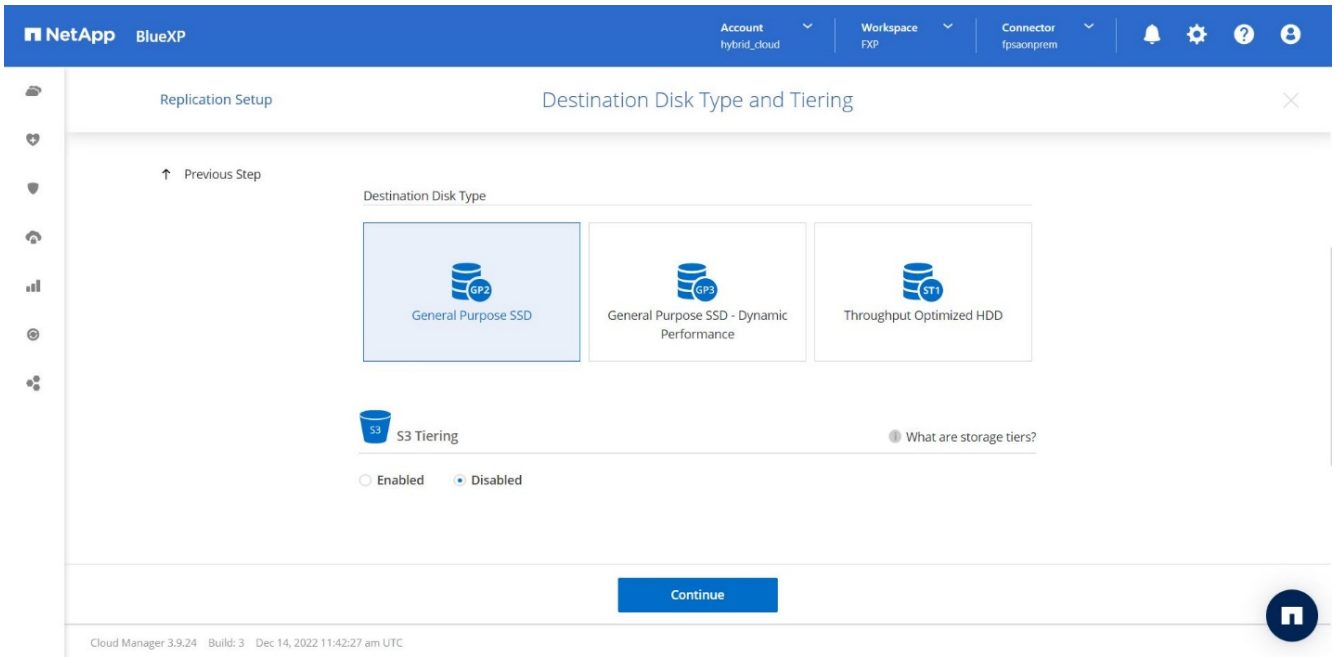
3. **Impostazione peering di origine e destinazione.** se viene visualizzata questa pagina, selezionare tutte le LIF dell'intercluster per la relazione peer del cluster.



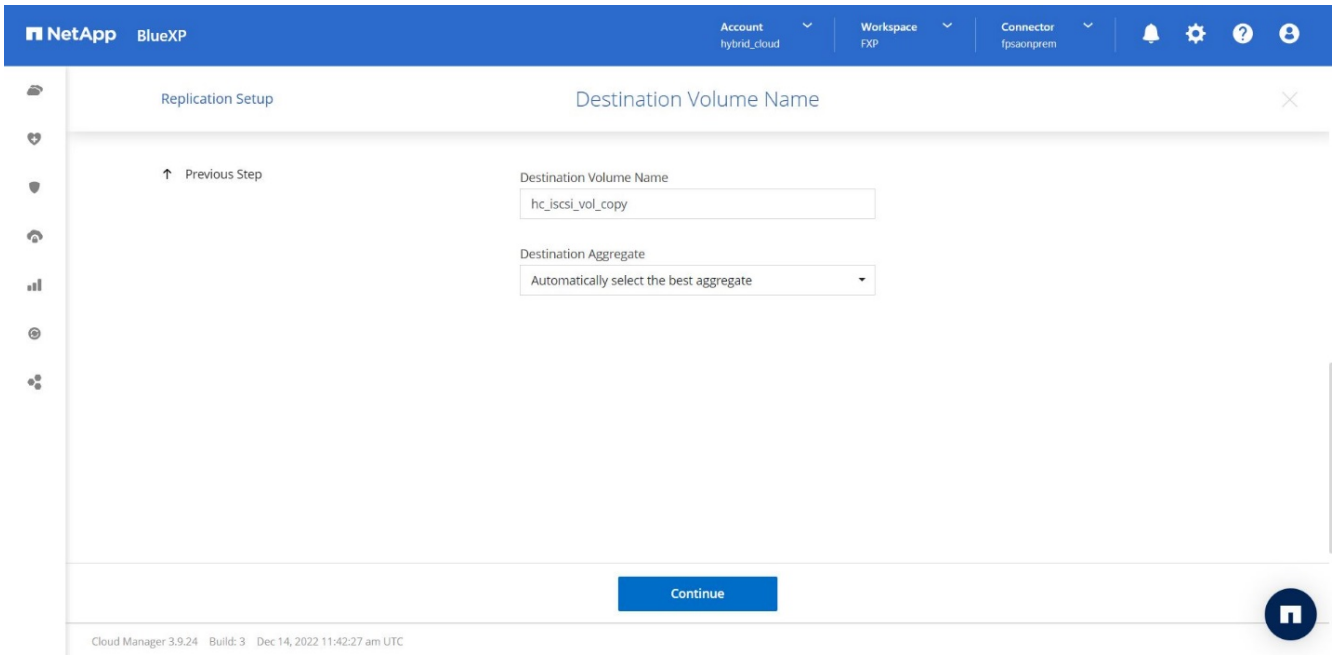
4. **Source Volume Selection.** selezionare il volume che si desidera replicare.



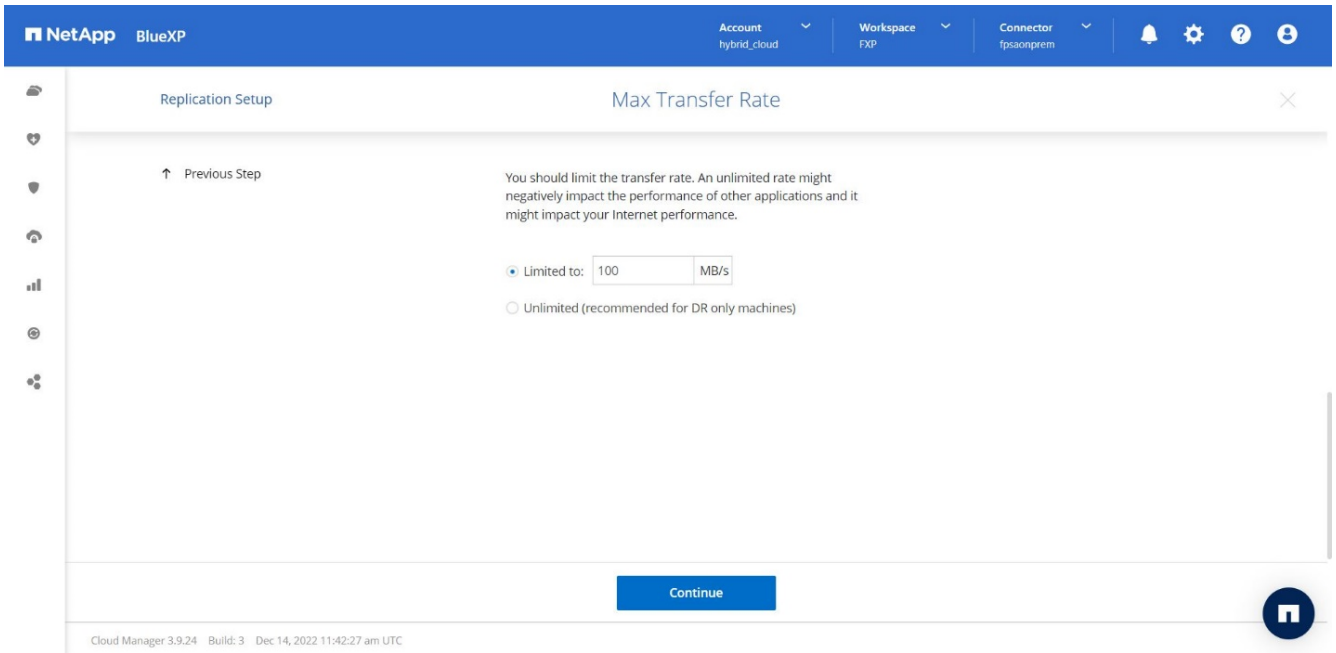
5. **Tipo di disco di destinazione e tiering.** se la destinazione è un sistema Cloud Volumes ONTAP, selezionare il tipo di disco di destinazione e scegliere se si desidera attivare il tiering dei dati.



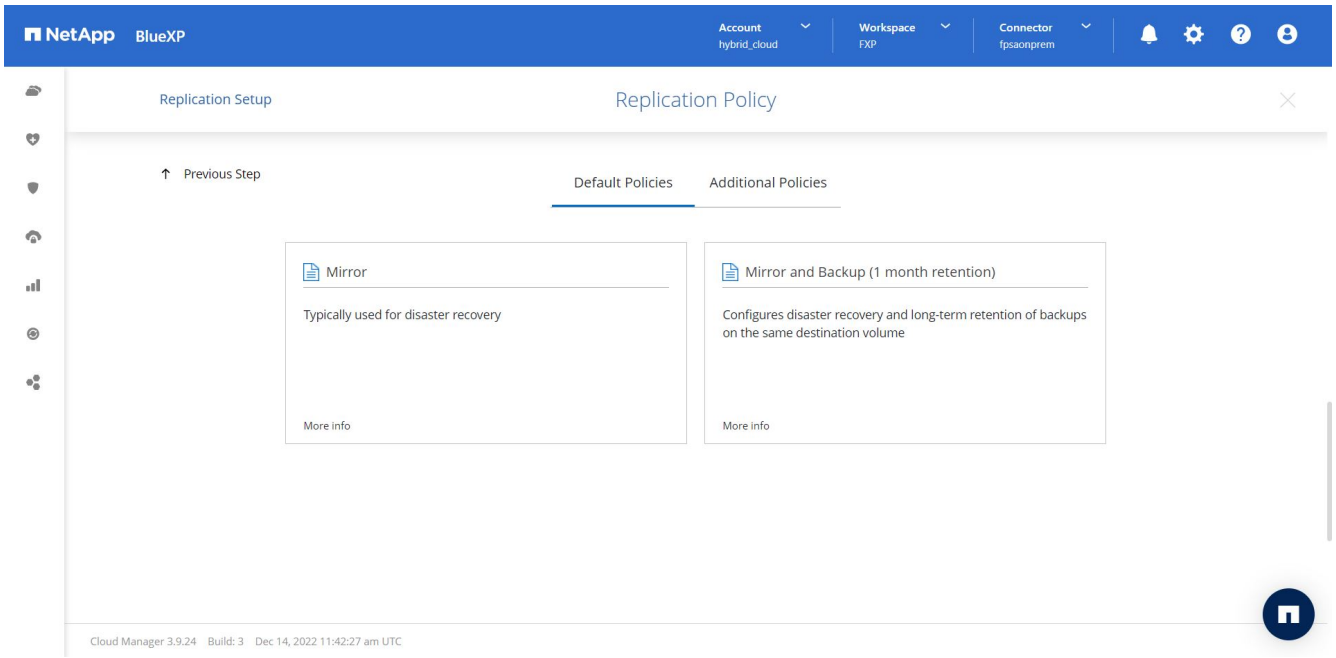
6. **Nome volume di destinazione:** specificare il nome del volume di destinazione e scegliere l'aggregato di destinazione. Se la destinazione è un cluster ONTAP, è necessario specificare anche la VM di storage di destinazione.



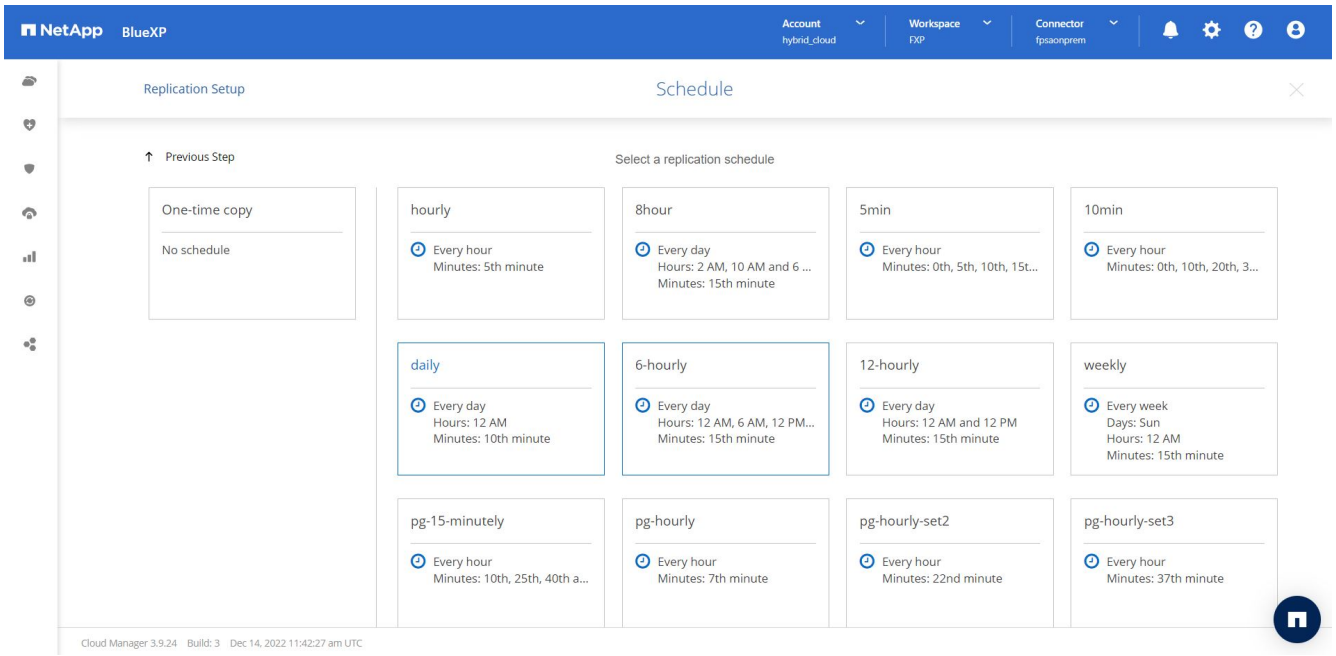
7. **Velocità di trasferimento massima.** specificare la velocità massima (in megabyte al secondo) alla quale trasferire i dati.



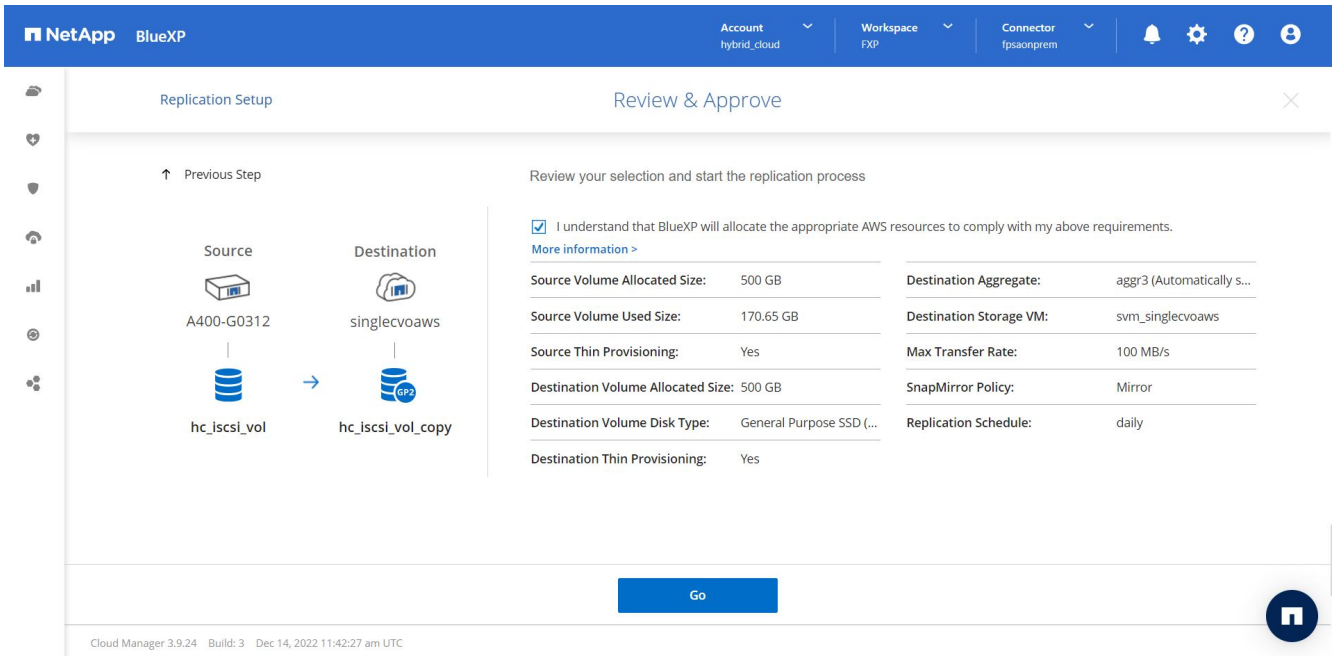
8. **Replication policy.** scegliere un criterio predefinito o fare clic su **Additional Policies**, quindi selezionare uno dei criteri avanzati. Per assistenza, "scopri le policy di replica".



9. **Pianificazione.** scegliere una copia singola o una pianificazione ricorrente. Sono disponibili diverse pianificazioni predefinite. Se si desidera una pianificazione diversa, è necessario creare una nuova pianificazione su `destination cluster` Utilizzo di System Manager.

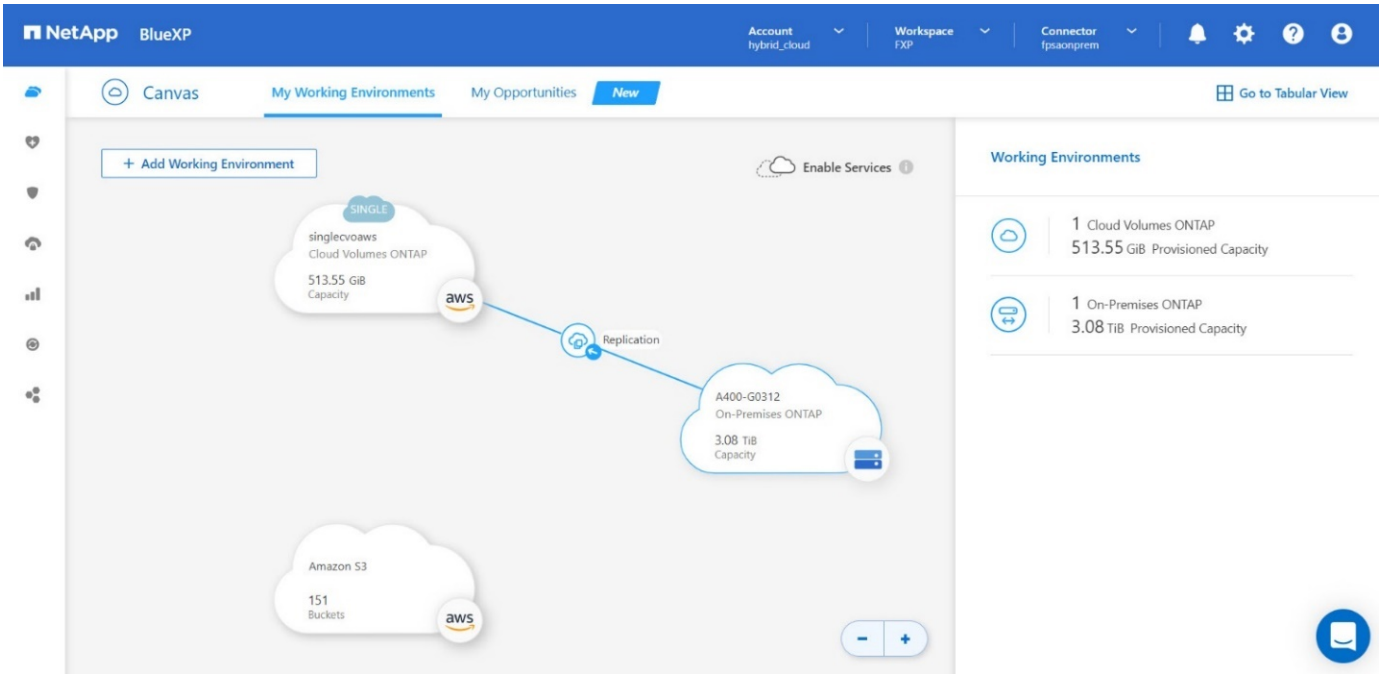


10. **Review.** Rivedi le tue selezioni e fai clic su **Go**.

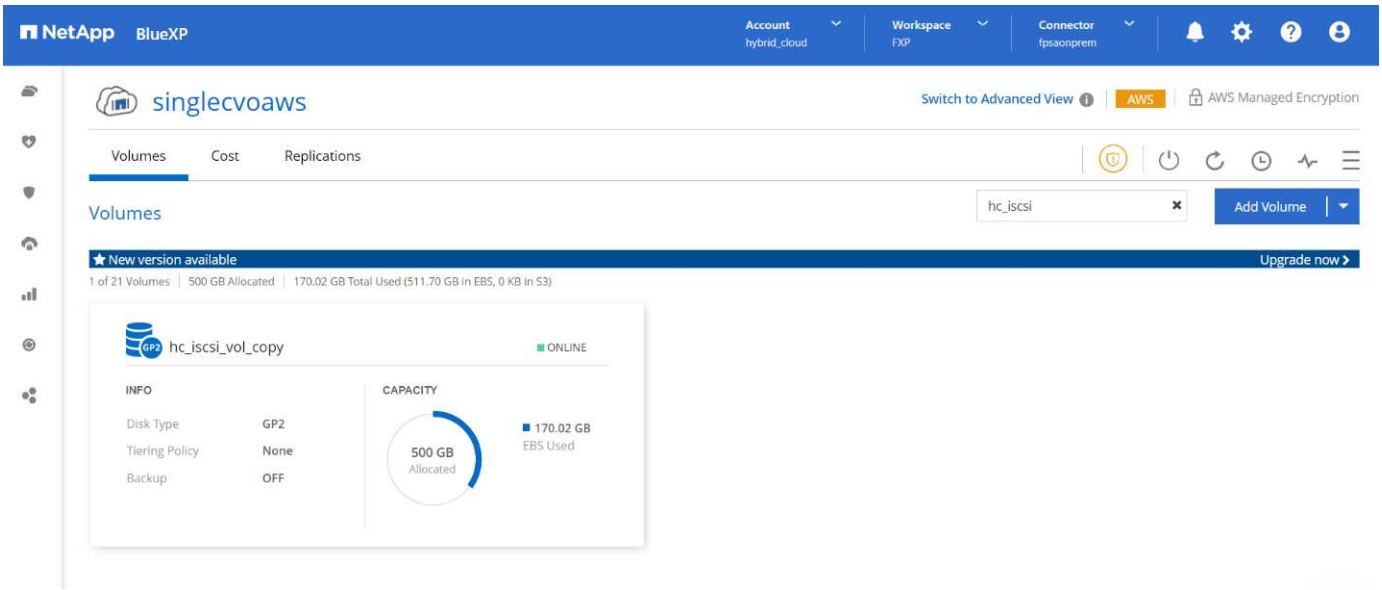


Per informazioni dettagliate su questi passaggi di configurazione, vedere "qui".

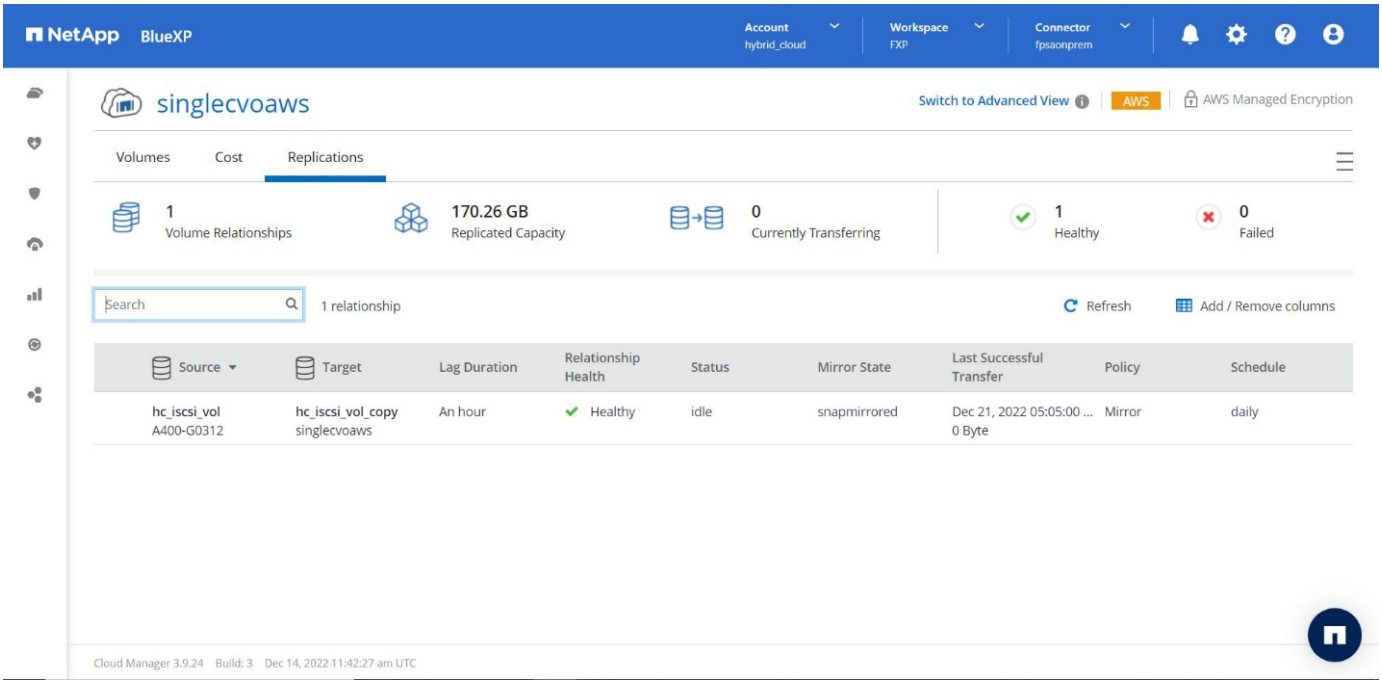
BlueXP avvia il processo di replica dei dati. A questo punto, è possibile visualizzare il servizio **Replication** stabilito tra il sistema ONTAP on-premise e Cloud Volumes ONTAP.



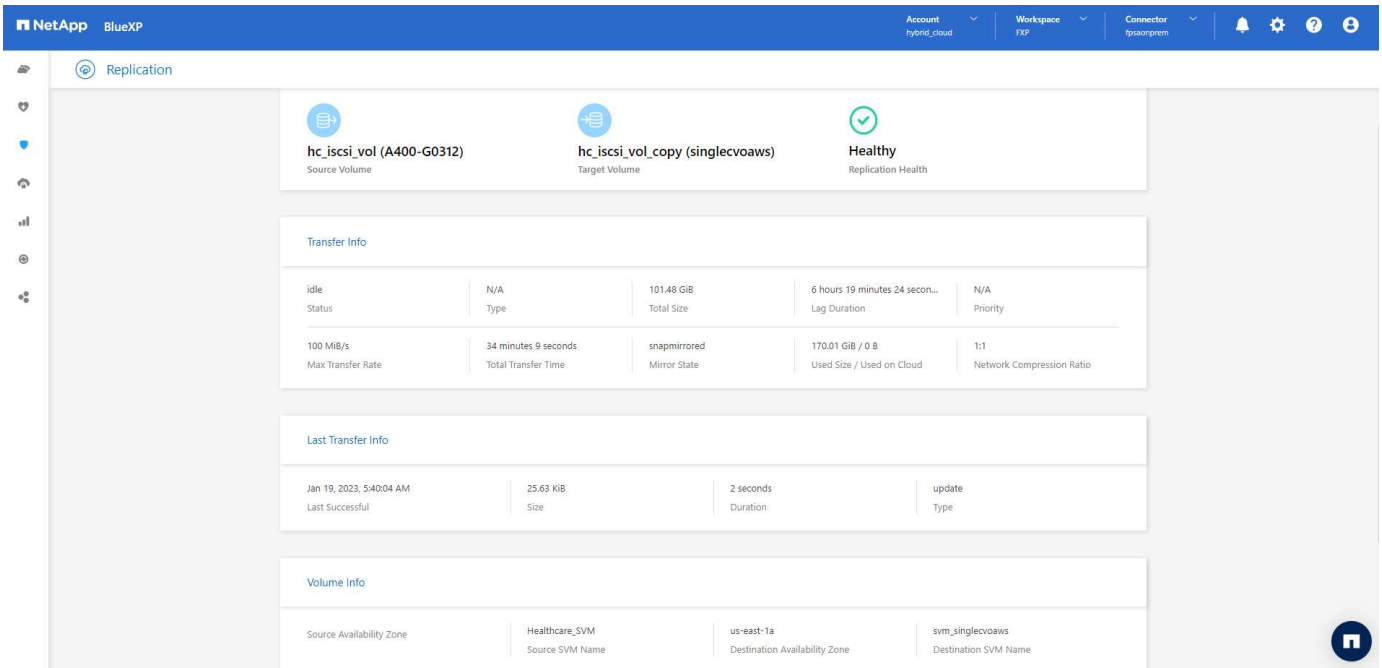
Nel cluster Cloud Volumes ONTAP, è possibile visualizzare il volume appena creato.



È inoltre possibile verificare che la relazione di SnapMirror sia stabilita tra il volume on-premise e il volume cloud.



Ulteriori informazioni sull'attività di replica sono disponibili nella scheda **Replication**.



"Successivo: Convalida della soluzione."

Convalida della soluzione

"Precedente: Configurazione SAN."

In questa sezione vengono esaminati alcuni casi di utilizzo della soluzione.

- Uno dei principali casi di utilizzo di SnapMirror è il backup dei dati. SnapMirror può essere utilizzato come strumento di backup primario replicando i dati all'interno dello stesso cluster o su destinazioni remote.
- Utilizzo dell'ambiente DR per eseguire test di sviluppo delle applicazioni (sviluppo/test).
- Dr in caso di disastro in produzione.
- Distribuzione dei dati e accesso remoto ai dati.

In particolare, i casi di utilizzo relativamente pochi validati in questa soluzione non rappresentano l'intera funzionalità della replica SnapMirror.

Sviluppo e test delle applicazioni (sviluppo/test)

Per accelerare lo sviluppo delle applicazioni, è possibile clonare rapidamente i dati replicati nel sito di DR e utilizzarli per lo sviluppo e il test delle applicazioni. La co-locazione degli ambienti di DR e di sviluppo/test può migliorare significativamente l'utilizzo delle strutture di backup o DR, mentre i cloni on-demand di sviluppo/test offrono il numero di copie di dati necessario per arrivare più rapidamente alla produzione.

La tecnologia FlexClone di NetApp consente di creare rapidamente una copia in lettura/scrittura di un volume FlexVol di destinazione SnapMirror nel caso in cui si desideri disporre dell'accesso in lettura/scrittura della copia secondaria per confermare la disponibilità di tutti i dati di produzione.

Completare i seguenti passaggi per utilizzare l'ambiente DR per eseguire lo sviluppo/test dell'applicazione:

1. Eseguire una copia dei dati di produzione. A tale scopo, eseguire un'istantanea applicativa di un volume on-premise. La creazione dello snapshot dell'applicazione prevede tre fasi: `Lock`, `Snap`, e. `Unlock`.

a. Interrompere il file system in modo che l'i/o venga sospeso e le applicazioni mantengano la coerenza. Qualsiasi applicazione scrive sul file system rimane in uno stato di attesa fino a quando non viene emesso il comando unquiesce nella fase c. I passaggi a, b e c vengono eseguiti attraverso un processo o un flusso di lavoro trasparente e che non influisce sullo SLA dell'applicazione.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

Questa opzione richiede il blocco del file system specificato in caso di nuove modifiche. Qualsiasi processo che tenta di scrivere nel file system bloccato viene bloccato fino a quando il file system non viene sbloccato.

b. Creare uno snapshot del volume on-premise.

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
hc_iscsi_vol -snapshot kamini
```

c. Riavviare i/o dal file system

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

Questa opzione viene utilizzata per sbloccare il file system e consentire il proseguimento delle operazioni. Tutte le modifiche al filesystem che sono state bloccate dal blocco vengono sbloccate e possono essere completate.

Lo snapshot coerente con l'applicazione può essere eseguito anche utilizzando NetApp SnapCenter, che ha l'orchestrazione completa del workflow descritto sopra come parte di SnapCenter. Per informazioni dettagliate, vedere "qui".

2. Eseguire un'operazione di aggiornamento di SnapMirror per mantenere sincronizzati i sistemi di produzione e DR.

```
singlecvoaws::> snapmirror update -destination-path
svm_singlecvoaws:hc_iscsi_vol_copy -source-path
Healthcare_SVM:hc_iscsi_vol

Operation is queued: snapmirror update of destination
"svm_singlecvoaws:hc_iscsi_vol_copy".
```

È possibile eseguire un aggiornamento di SnapMirror anche tramite l'interfaccia utente grafica di BlueXP nella scheda **Replication**.

3. Creare un'istanza di FlexClone in base all'istantanea dell'applicazione acquisita in precedenza.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

Per l'attività precedente, è possibile creare anche una nuova snapshot, ma è necessario seguire le stesse procedure descritte in precedenza per garantire la coerenza dell'applicazione.

4. Attivare un volume FlexClone per visualizzare l'istanza EHR nel cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                 /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. Eseguire i seguenti comandi sull'istanza EHR nel cloud per accedere ai dati o al file system.
   a. Scopri lo storage ONTAP. Controllare lo stato del multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. Attivare il gruppo di volumi.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. Montare il file system e visualizzare il riepilogo delle informazioni sul file system.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

In questo modo è possibile utilizzare l'ambiente DR per lo sviluppo/test delle applicazioni. L'esecuzione di test/sviluppo dell'applicazione sullo storage DR consente di utilizzare più risorse che altrimenti potrebbero rimanere inattive per gran parte del tempo.

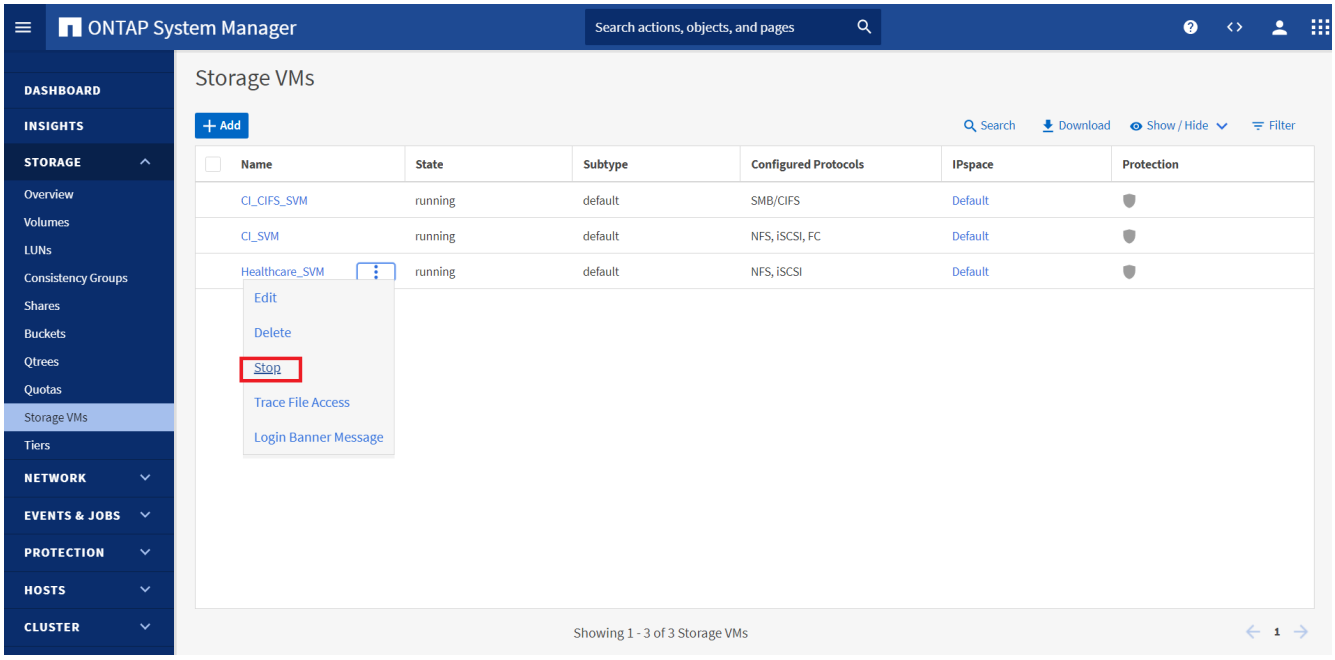
Disaster recovery

La tecnologia SnapMirror viene utilizzata anche come parte dei piani di DR. Se i dati critici vengono replicati in una posizione fisica diversa, un disastro grave non deve causare lunghi periodi di indisponibilità dei dati per le applicazioni business-critical. I client possono accedere ai dati replicati in rete fino al ripristino del sito di produzione da corruzione, eliminazione accidentale, disastro naturale e così via.

In caso di failback al sito primario, SnapMirror offre un mezzo efficiente per risincronizzare il sito DR con il sito primario, trasferendo solo i dati modificati o nuovi al sito primario dal sito DR semplicemente invertendo la relazione SnapMirror. Dopo che il sito di produzione primario riprende le normali operazioni applicative, SnapMirror continua il trasferimento al sito DR senza richiedere un altro trasferimento di riferimento.

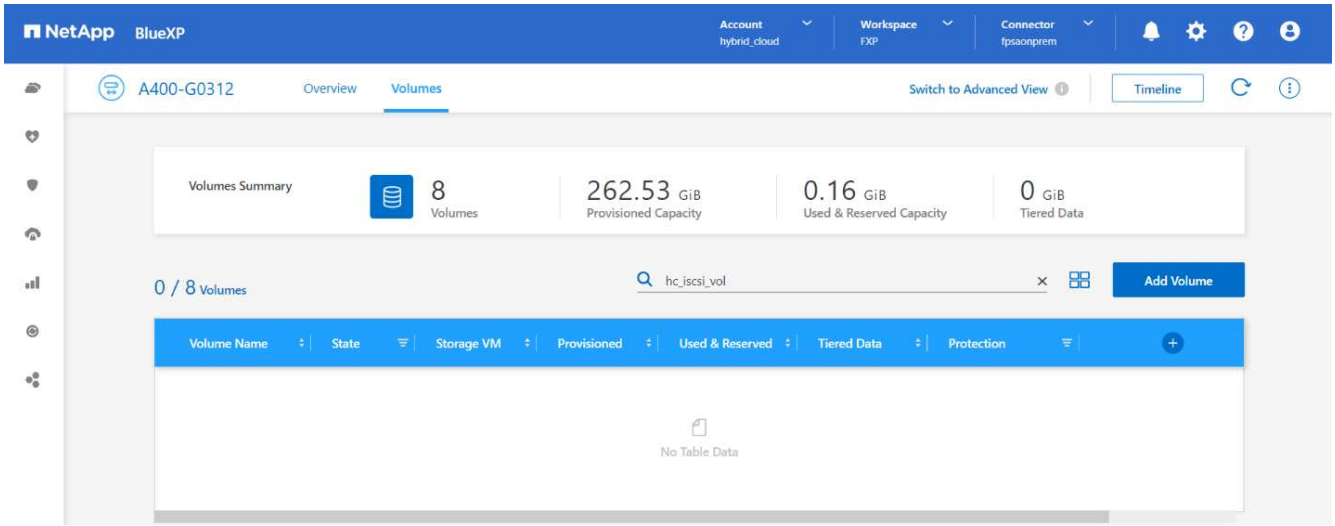
Per eseguire la convalida di uno scenario di disaster recovery corretto, attenersi alla seguente procedura:

1. Simulare un disastro sul lato di origine (produzione) arrestando la SVM che ospita il volume ONTAP on-premise (`hc_iscsi_vol`).



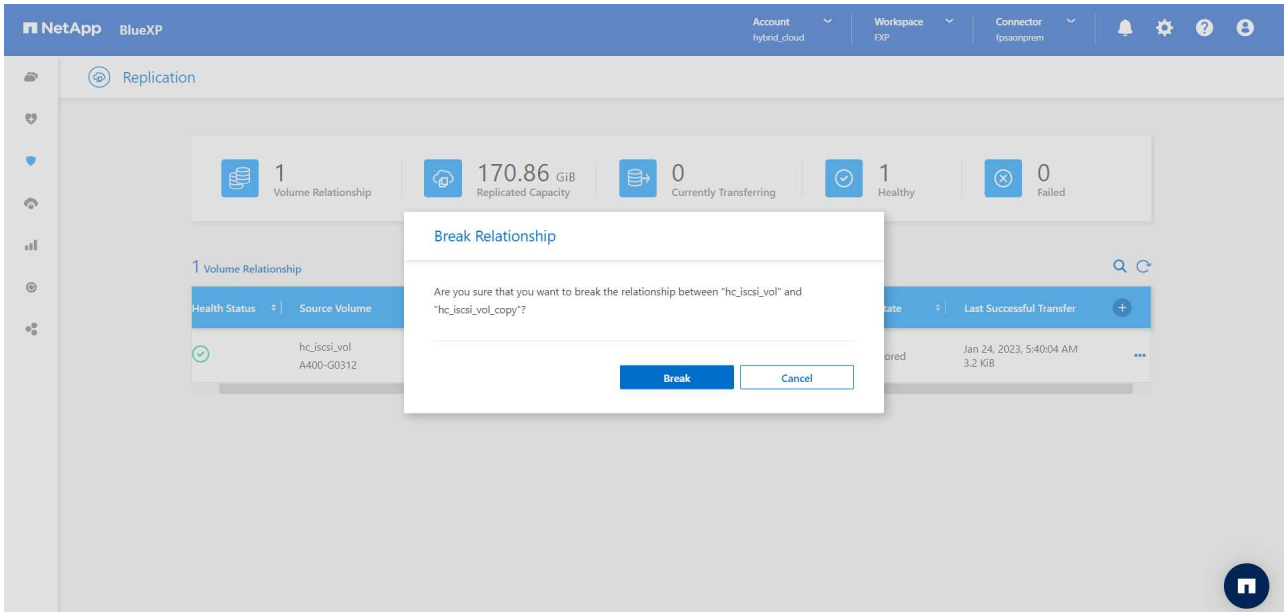
   Assicurarsi che la replica di SnapMirror sia già impostata tra ONTAP on-premise nell'istanza di FlexPod e Cloud Volumes ONTAP in AWS, in modo da poter creare snapshot delle applicazioni frequenti.

   Dopo l'arresto di SVM, il `hc_iscsi_vol` Il volume non è visibile in BlueXP.



2. Attivare DR in CVO.

   a. Interrompere la relazione di replica di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP e promuovere il volume di destinazione CVO (`hc_iscsi_vol_copy`) alla produzione.



   Una volta interrotta la relazione di SnapMirror, il tipo di volume di destinazione cambia da protezione dati (DP) a lettura/scrittura (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume             type
--------------- ----------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Attivare il volume di destinazione in Cloud Volumes ONTAP per visualizzare l'istanza EHR su un'istanza EC2 nel cloud.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. Per accedere ai dati e al file system sull'istanza EHR nel cloud, individuare prima lo storage ONTAP e verificare lo stato del multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. Quindi attivare il gruppo di volumi.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

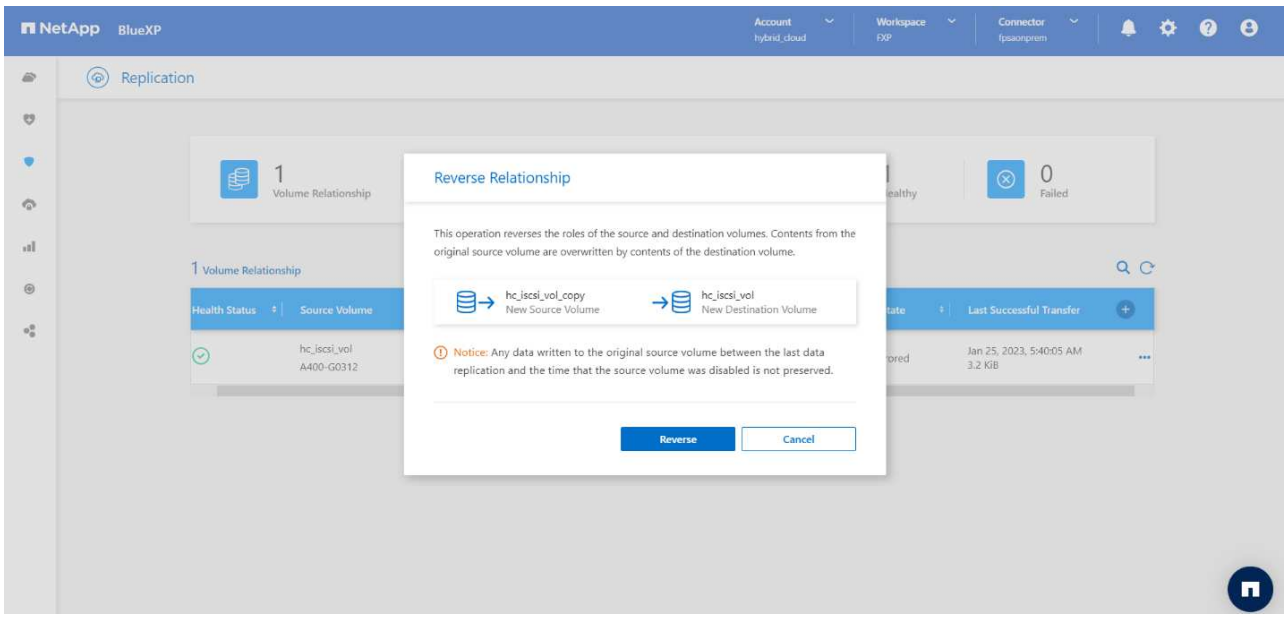
e. Infine, montare il file system e visualizzare le informazioni sul file system.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                  1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

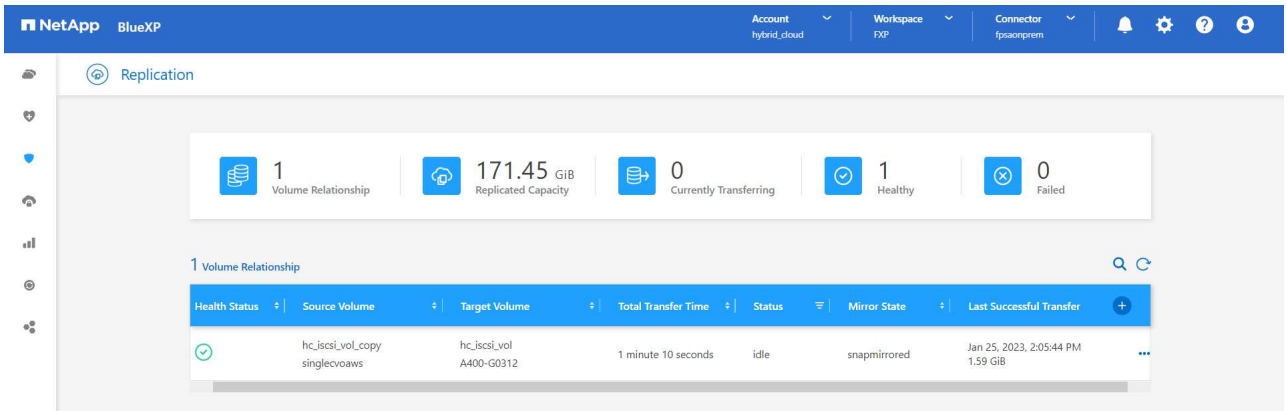
Questo output mostra che gli utenti possono accedere ai dati replicati attraverso la rete fino al ripristino del sito di produzione da un disastro.

f. Invertire la relazione di SnapMirror. Questa operazione inverte i ruoli dei volumi di origine e di destinazione.



Quando viene eseguita questa operazione, i contenuti del volume di origine originale vengono sovrascritti dai contenuti del volume di destinazione. Questa operazione è utile quando si desidera riattivare un volume di origine che è stato offline.

Ora il volume CVO (`hc_iscsi_vol_copy`) diventa il volume di origine e il volume on-premise (`hc_iscsi_vol`) diventa il volume di destinazione.



Tutti i dati scritti nel volume di origine tra l'ultima replica dei dati e l'ora in cui il volume di origine è stato disattivato non vengono conservati.

a. Per verificare l'accesso in scrittura al volume CVO, creare un nuovo file sull'istanza EHR nel cloud.

```
cd /file1/
sudo touch newfile
```

Quando il sito di produzione non è attivo, i client possono comunque accedere ai dati ed eseguire operazioni di scrittura nel volume Cloud Volumes ONTAP, che ora è il volume di origine.

In caso di failback al sito primario, SnapMirror offre un mezzo efficiente per risincronizzare il sito DR con il sito primario, trasferendo solo i dati modificati o nuovi al sito primario dal sito DR semplicemente invertendo la relazione SnapMirror. Dopo che il sito di produzione primario riprende le normali operazioni applicative, SnapMirror continua il trasferimento al sito DR senza richiedere un altro trasferimento di riferimento.

In questa sezione viene illustrata la corretta risoluzione di uno scenario di disaster recovery quando il sito di produzione viene colpito da un disastro. I dati possono ora essere consumati in modo sicuro dalle applicazioni che possono ora servire i client mentre il sito di origine passa attraverso il ripristino.

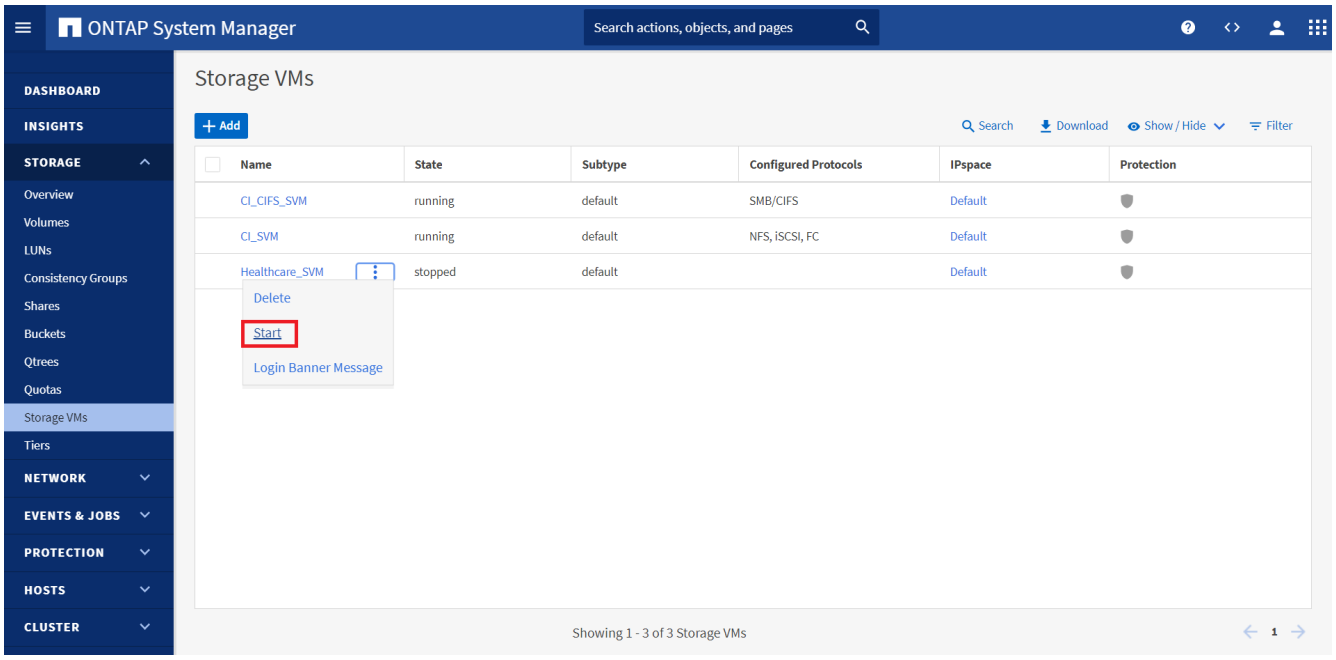
Verifica dei dati sul sito di produzione

Una volta ripristinato il sito di produzione, è necessario assicurarsi che la configurazione originale sia ripristinata e che i client siano in grado di accedere ai dati dal sito di origine.

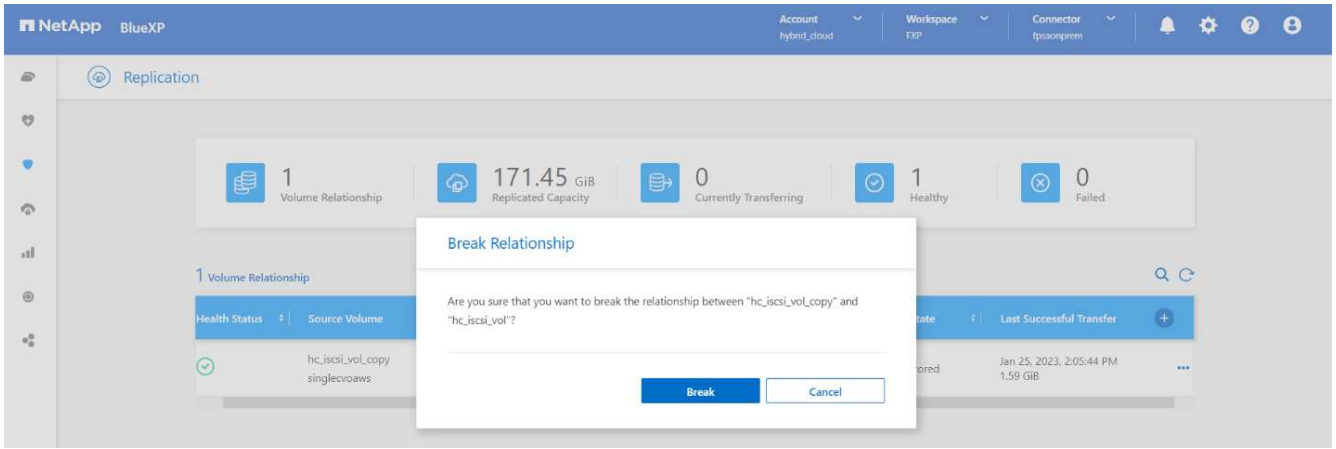
In questa sezione, parleremo di come attivare il sito di origine, ripristinare la relazione di SnapMirror tra ONTAP on-premise e Cloud Volumes ONTAP e infine eseguire un controllo dell'integrità dei dati sul lato di origine

Per la verifica dei dati sul sito di produzione è possibile utilizzare la seguente procedura:

1. Assicurarsi che il sito di origine sia attivo. A tale scopo, avviare la SVM che ospita il volume ONTAP on-premise (`hc_iscsi_vol`).



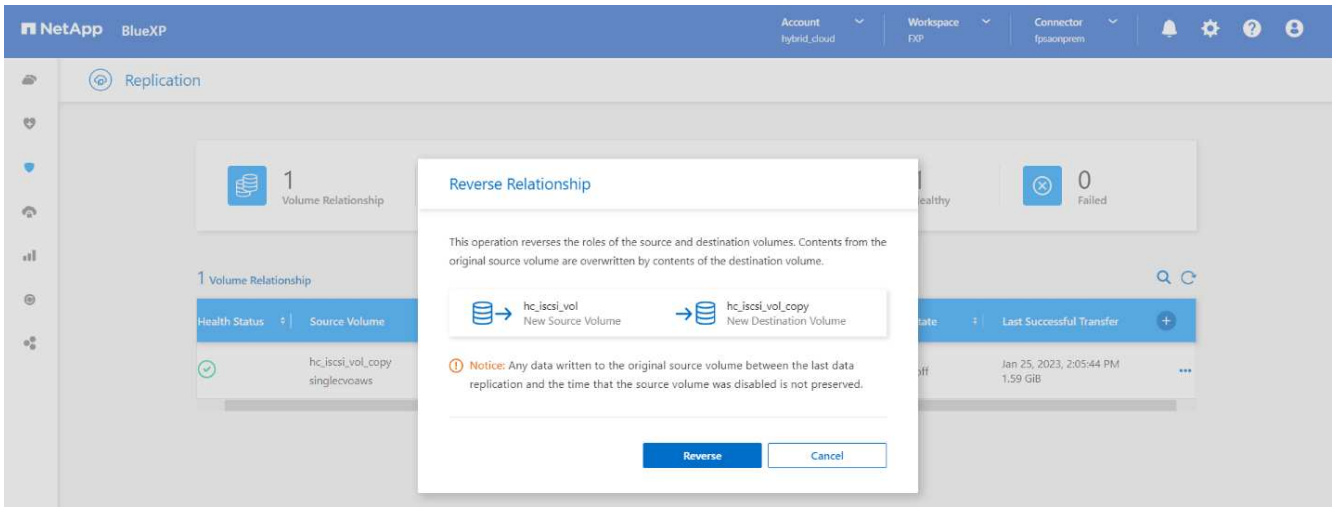
2. Interrompere la relazione di replica di SnapMirror tra Cloud Volumes ONTAP e ONTAP on-premise e promuovere il volume on-premise (`hc_iscsi_vol`) torna alla produzione.



Una volta interrotta la relazione di SnapMirror, il tipo di volume on-premise cambia da protezione dati (DP) a lettura/scrittura (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver         volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. Invertire la relazione di SnapMirror. Ora, il volume on-premise ONTAP (`hc_iscsi_vol`) Diventa il volume di origine e il volume Cloud Volumes ONTAP (`hc_iscsi_vol_copy`) diventa il volume di destinazione.



Seguendo questa procedura, la configurazione originale è stata ripristinata correttamente.

4. Riavviare l'istanza EHR on-premise. Montare il file system e verificare che `newfile` Esiste anche qui quello che hai creato sull'istanza EHR nel cloud quando la produzione era inattiva.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

Possiamo dedurre che la replica dei dati dall'origine alla destinazione è stata completata correttamente e che l'integrità dei dati è stata mantenuta. Questa operazione completa la verifica dei dati sul sito di produzione.

"Prossimo: Conclusione."

Conclusione

"Precedente: Convalida della soluzione."

La creazione di un cloud ibrido è un obiettivo per la maggior parte delle organizzazioni sanitarie di fornire la disponibilità dei dati in qualsiasi momento. In questa soluzione, abbiamo implementato una soluzione di cloud ibrido FlexPod con Cloud Volumes ONTAP, utilizzando la tecnologia di replica SnapMirror di NetApp per convalidare alcuni casi di utilizzo per il backup e il ripristino di applicazioni e carichi di lavoro nel settore sanitario.

FlexPod, un'infrastruttura convergente rigorosamente testata e prevalidata dalla partnership strategica di Cisco e NetApp, è progettata per offrire performance di sistema prevedibili a bassa latenza e alta disponibilità. Questo approccio offre elevati livelli di comfort EHR e, in ultima analisi, il miglior tempo di risposta per gli utenti del sistema EHR.

Con NetApp, puoi eseguire la produzione EHR, il disaster recovery, il backup o il tiering nel cloud proprio come faresti con le funzionalità di storage NetApp in un data center on-premise. Con NetApp Cloud Volumes ONTAP, NetApp offre le funzionalità di livello Enterprise e le performance necessarie per eseguire in modo efficace i servizi EHR nel cloud. Le opzioni cloud di NetApp offrono Block-over-iSCSI e file-over-NFS o SMB.

Questa soluzione soddisfa le esigenze delle organizzazioni sanitarie e consente loro di fare un passo verso la loro trasformazione digitale. Può anche aiutarli a gestire le applicazioni e i carichi di lavoro in modo efficiente.

"Avanti: Dove trovare ulteriori informazioni."

Dove trovare ulteriori informazioni

"Precedente: Conclusione."

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

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

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

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- Avvio rapido di Cloud Volumes ONTAP in AWS

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- Replica di SnapMirror

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928: Best practice NetApp per Epic

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693: Guida all'implementazione di FlexPod Datacenter per Epic EHR

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod per Epic

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

- Tool di matrice di interoperabilità NetApp

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

- Cisco UCS hardware and Software Interoperability Tool

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guida alla compatibilità VMware

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

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Marzo 2023	Versione iniziale