Cloud ibrido

FlexPod

NetApp
November 04, 2025

Sommario

Cloud ibrido

Cloud ibrido FlexPod con Cloud Volumes ONTAP per Epic

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

In collaborazione con: 

Kamini Singh, NetApp

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

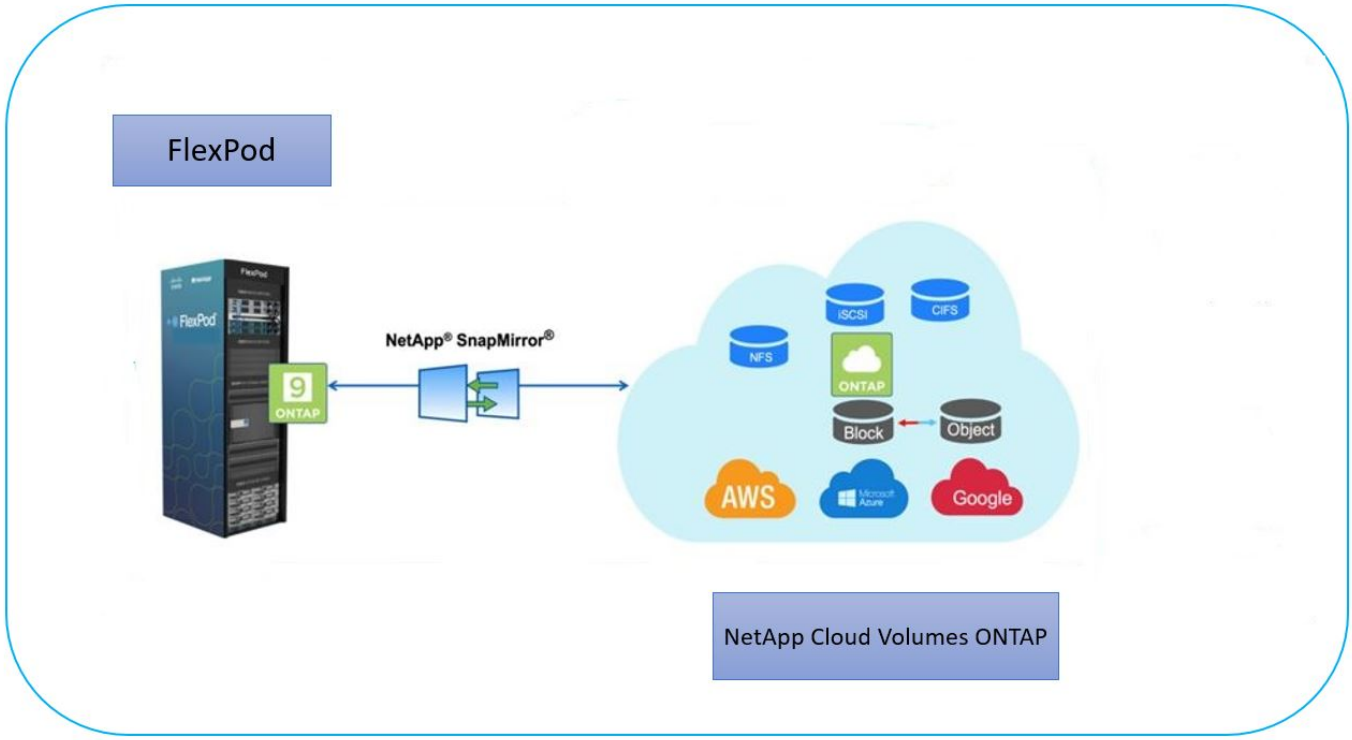
Le dimensioni in costante aumento dei dati sanitari e le preziose informazioni che questi dati possono fornire rendono i servizi dati sanitari e la protezione dei dati critici e impegnativi. Innanzitutto, i dati del settore sanitario devono essere sia disponibili che protetti per soddisfare i requisiti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

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

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

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

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



Pubblico

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

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

Vantaggi della soluzione

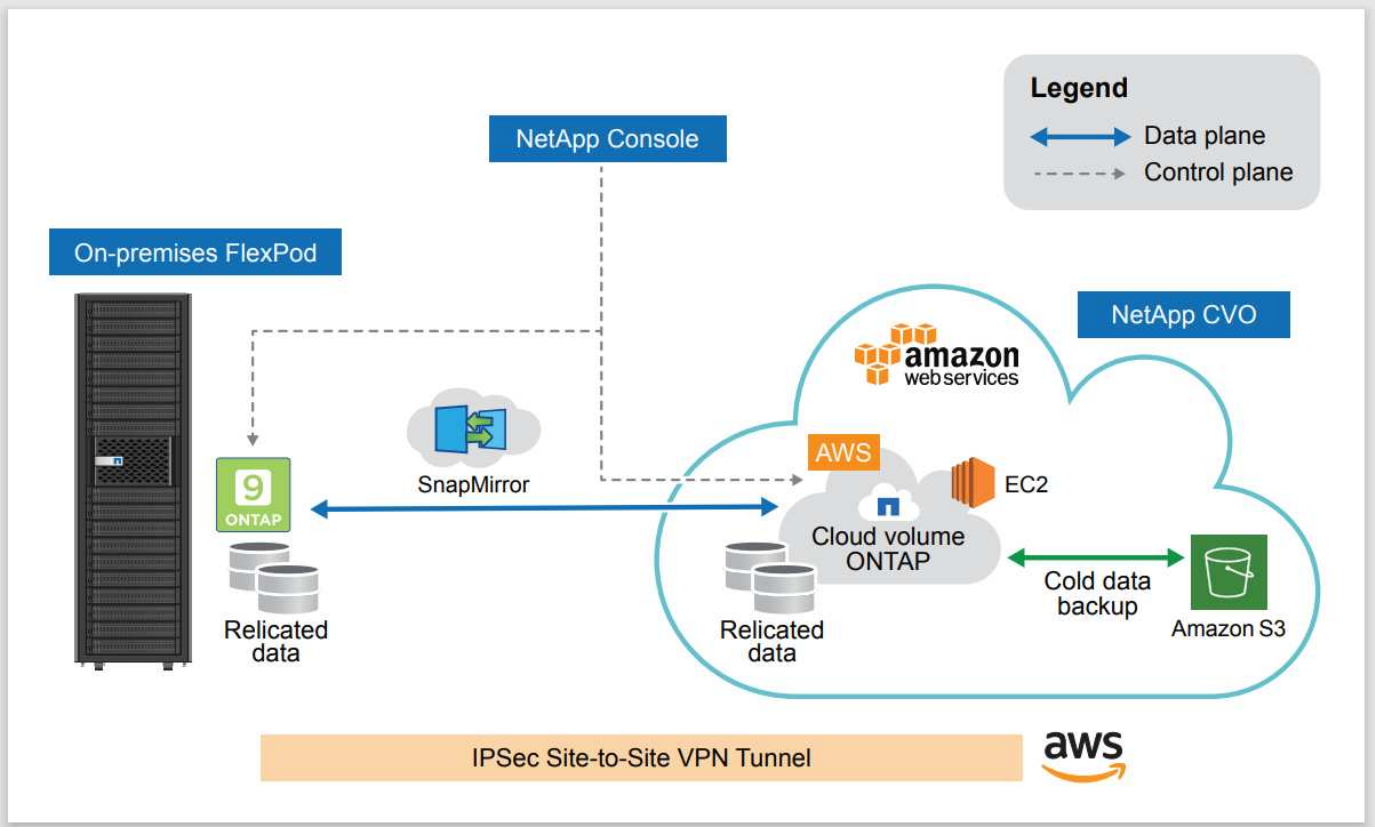
Il data center FlexPod integrato con NetApp Cloud Volumes ONTAP offre i seguenti vantaggi ai carichi di lavoro del settore sanitario:

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

- **Protezione ransomware.** La protezione ransomware NetApp Console analizza le fonti di dati in ambienti on-premise e cloud, rileva le vulnerabilità della sicurezza e fornisce il loro stato di sicurezza attuale e il punteggio di rischio. Fornisce quindi raccomandazioni pratiche che è possibile approfondire e seguire per porre rimedio. Ciò consente di proteggere i dati sanitari critici dagli attacchi ransomware.

Topologia della soluzione

Questa sezione descrive la topologia logica della soluzione. La figura seguente rappresenta la topologia della soluzione composta dall'ambiente FlexPod on-premise, NetApp Cloud Volumes ONTAP (CVO) in esecuzione su Amazon Web Services (AWS) e dalla piattaforma SaaS NetApp Console .



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 certificato EHR e supporta una piattaforma contenente Cisco Cisco UCS con processori Intel Xeon, Red Hat Enterprise Linux (RHEL) e virtualizzazione con VMware ESXi. Questa piattaforma, abbinata al livello di comfort elevato di EHR per lo storage NetApp che esegue ONTAP, consente di eseguire le applicazioni sanitarie in un cloud privato completamente gestito tramite FlexPod , che può anche essere connesso a qualsiasi provider di cloud pubblico.

NetApp Console

NetApp Console è una piattaforma di gestione di livello enterprise basata su SaaS che consente agli esperti IT e agli architetti cloud di gestire centralmente la propria infrastruttura multi-cloud ibrida utilizzando le soluzioni cloud NetApp . Fornisce un sistema centralizzato per la visualizzazione e la gestione dell'archiviazione on-premise e cloud, supportando account e provider cloud multipli e ibridi. Per maggiori informazioni, vedere "Documentazione NetApp Console".

Agente console

Un'istanza dell'agente Console consente alla Console di gestire risorse e processi all'interno di un ambiente cloud pubblico. Per molte delle funzionalità fornite dalla Console è necessario un agente Console, che può

essere distribuito nel cloud o nella rete locale.

Un agente Console è supportato nelle seguenti posizioni:

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

"Scopri di più sugli agenti della console".

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 informazioni più dettagliate, 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.

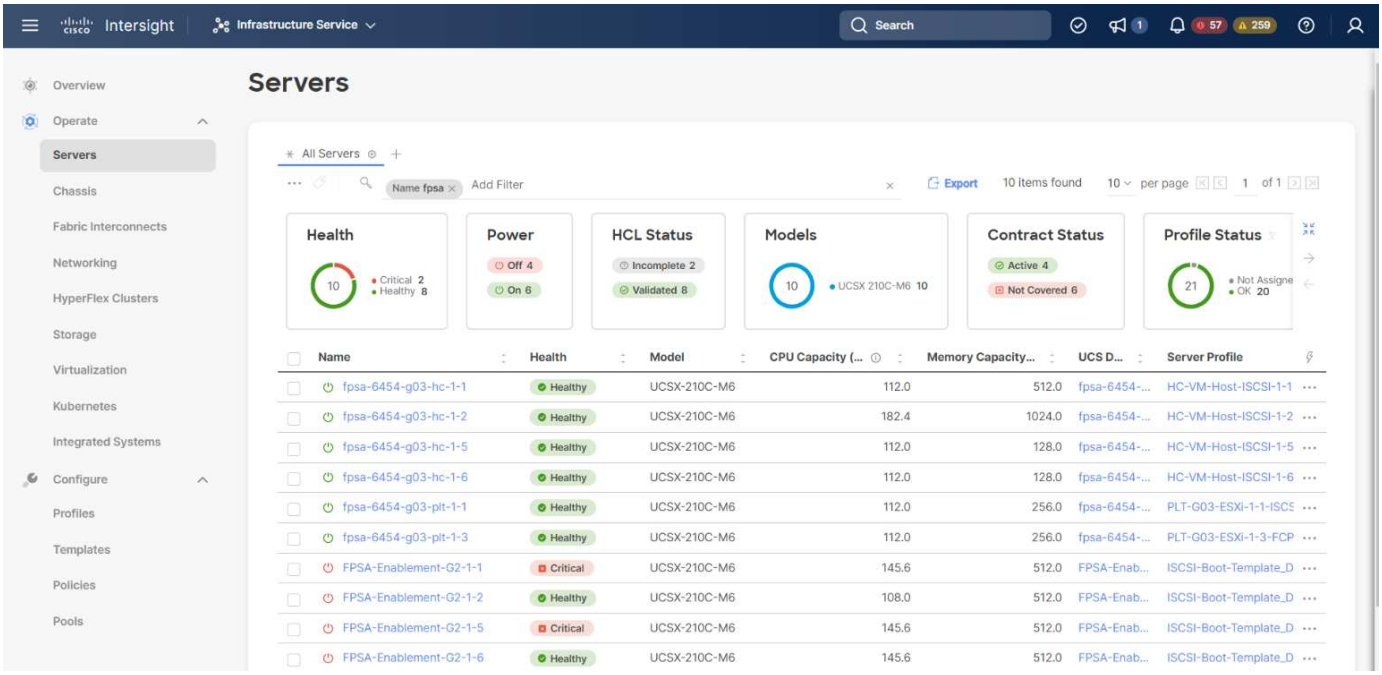
Per maggiori informazioni, vedere "Active IQ Unified Manager".

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 suoi 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 cloud ibrida può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware come definito nel"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)
	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

Nella tabella seguente sono riportate le versioni di Console e Cloud Volumes ONTAP .

Vendor	Prodotto	Versione
NetApp	Consolle	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 alla NetApp Console.

   Per accedere alla Console e ad altri servizi cloud, è necessario registrarsi su "NetApp Console" . Per impostare spazi di lavoro e utenti nell'account Console, vedere "Configurazione e amministrazione NetApp Console" . È necessario un account che disponga dell'autorizzazione per distribuire l'agente della Console nel provider cloud direttamente dalla Console. Per ottenere le autorizzazioni necessarie, fare riferimento a "Riepilogo delle autorizzazioni per NetApp Console" .

4. Distribuisci l'agente della console.

   Prima di aggiungere un sistema Cloud Volume ONTAP , è necessario distribuire un agente Console. La Console ti avvisa se provi a creare il tuo primo sistema Cloud Volumes ONTAP senza un agente della Console. Per distribuire un agente della console in AWS dalla console, vedere "Opzioni di installazione dell'agente console in AWS" .

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.

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
```

Aggiungi storage FlexPod on-premise alla NetApp Console

Completa i seguenti passaggi per aggiungere lo spazio di archiviazione FlexPod al sistema utilizzando la Console.

1. Dal menu di navigazione, seleziona **Archiviazione** > **Sistemi**.
2. Nella pagina Sistemi, fare clic su **Aggiungi sistema** e selezionare **In sede**.
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**.

   La Console rileva il cluster ONTAP e lo aggiunge come sistema nella pagina Sistemi.

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 delle LUN vengono generati con l'EHR
`Dgen.pl` sceneggiatura.  Lo script è progettato per creare dati simili a
quelli presenti in 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, seleziona **Archiviazione** > **Sistemi**.
2. In Sistemi, seleziona il sistema che contiene il volume di origine, trascinalo sul sistema su cui vuoi replicare il volume, quindi seleziona **Replica**.

   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".

La console avvia il processo di replicazione dei dati. A questo punto, puoi vedere il servizio **Replica** che è stato stabilito tra il tuo sistema ONTAP locale 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".
   ```

   Un aggiornamento SnapMirror può essere eseguito anche tramite l'interfaccia utente grafica NetApp Console nella scheda **Replica**.

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.

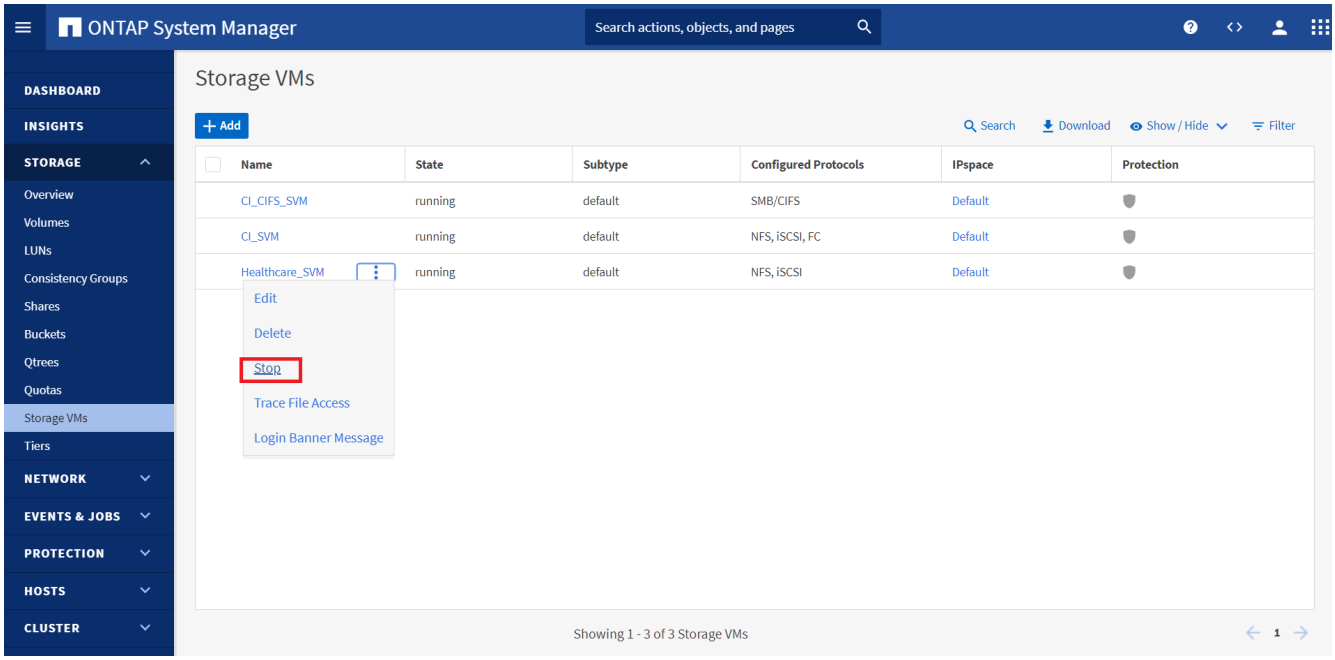
Disaster recovery

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 che l'SVM è stato arrestato, il `hc_iscsi_vol` il volume non è visibile nella Console.

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.

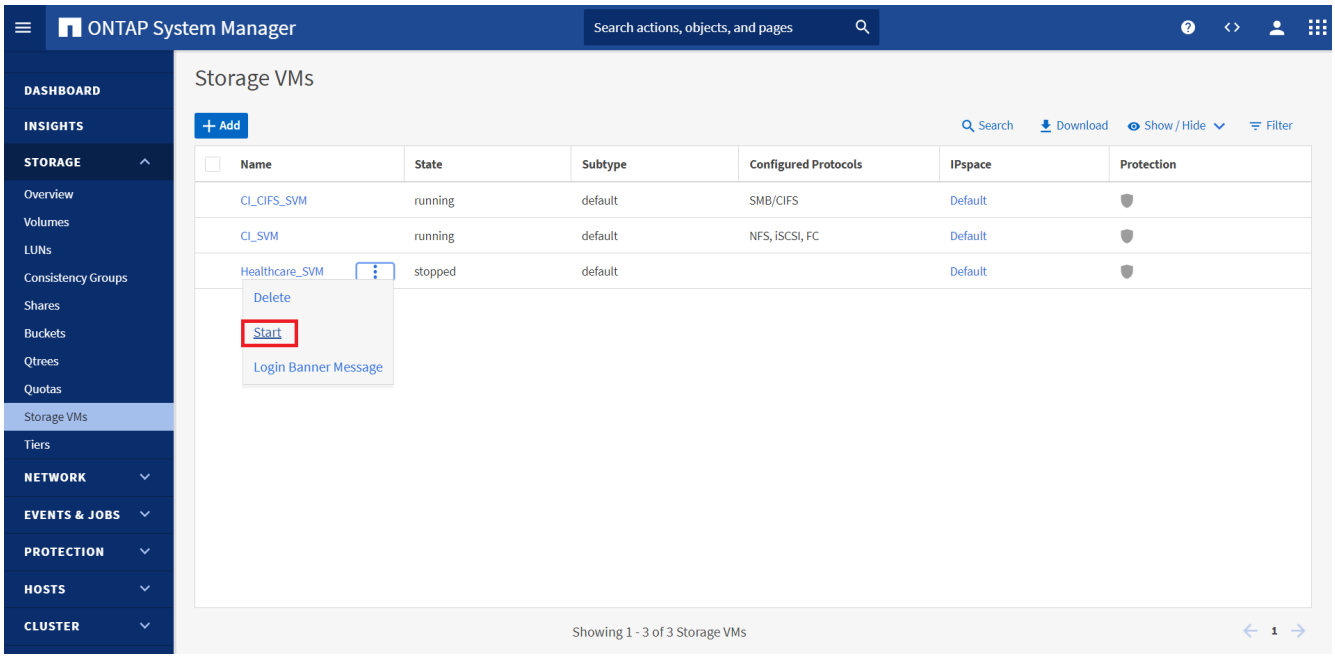
Verifica dei dati sul sito di produzione

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.

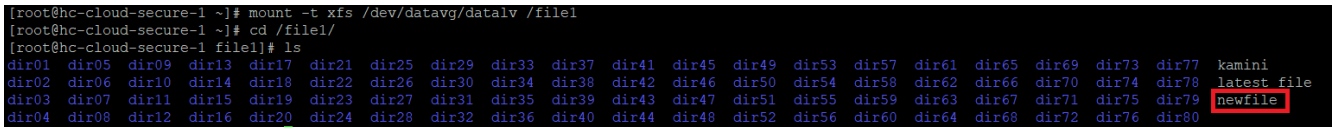
   Una volta interrotta la relazione di SnapMirror, il tipo di volume on-premise cambia da protezione dati (DP) a lettura/scrittura (RW).

```
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.



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 Console

  "https://console.netapp.com/"

- NetApp Cloud Volumes ONTAP

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

- Avvio rapido di Cloud Volumes ONTAP in AWS

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

- Replica di SnapMirror

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

- TR-3928: Best practice NetApp per Epic

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

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

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

- FlexPod per Epic

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

- Tool di matrice di interoperabilità NetApp

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

- Cisco UCS hardware and Software Interoperability Tool

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

- Guida alla compatibilità VMware

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

Cronologia delle versioni

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

Cloud ibrido FlexPod per piattaforma cloud Google con NetApp Cloud Volumes ONTAP e Cisco Intersight

TR-4939: Cloud ibrido FlexPod per piattaforma cloud Google con NetApp Cloud Volumes ONTAP e Cisco Intersight

Ruchika Lahoti, NetApp

Introduzione

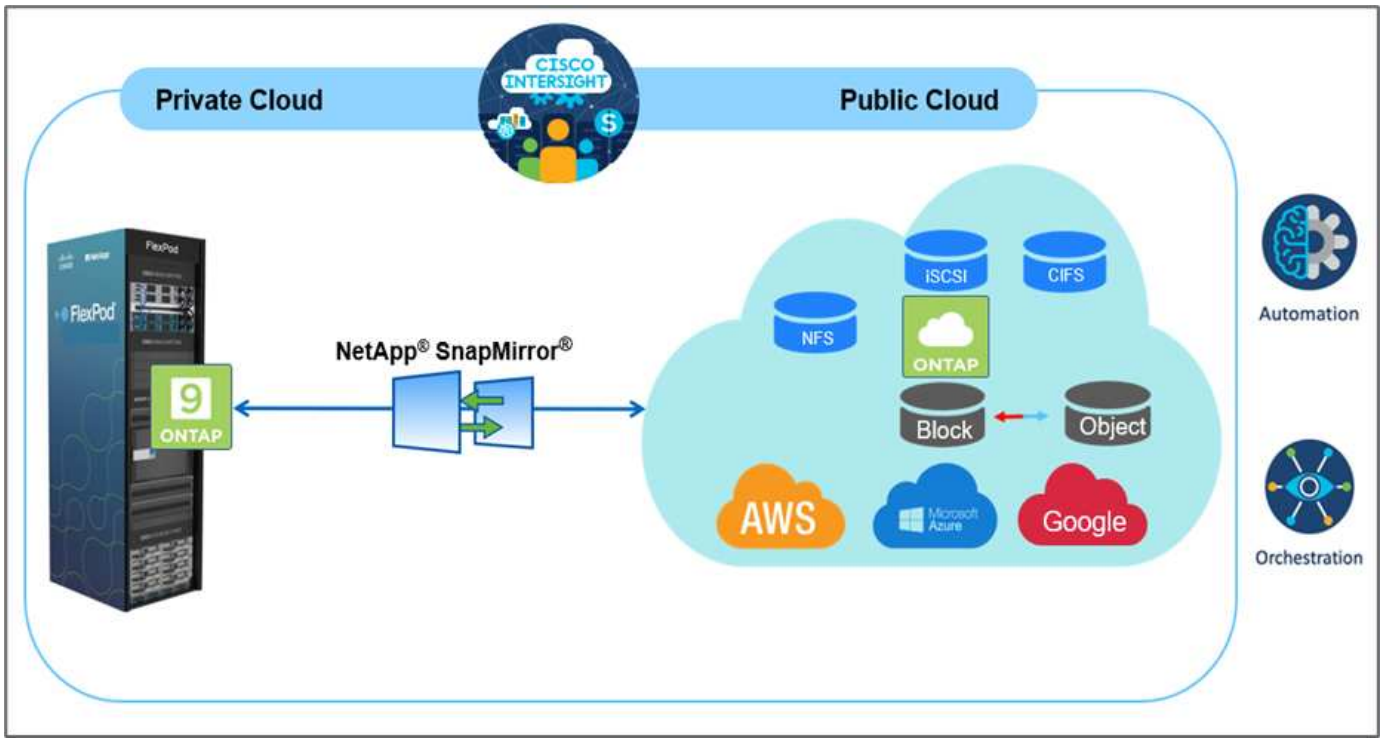
La protezione dei dati con il disaster recovery (DR) è un obiettivo critico per la business continuity. Il DR consente alle organizzazioni di eseguire il failover delle proprie operazioni di business in una posizione secondaria e di eseguire in seguito il ripristino e il failback sul sito primario in modo efficiente e affidabile. Diversi problemi, come disastri naturali, guasti di rete, vulnerabilità software ed errori umani, rendono lo sviluppo di una strategia di disaster recovery una priorità ASSOLUTA PER L'IT.

Per il DR, tutti i carichi di lavoro eseguiti sul sito primario devono essere riprodotti fedelmente sul sito DR. Un'organizzazione deve inoltre disporre di una copia aggiornata di tutti i dati aziendali, inclusi database, file service, storage NFS e iSCSI e così via. Poiché i dati nell'ambiente di produzione vengono costantemente aggiornati, le modifiche devono essere trasferite regolarmente al sito di DR.

L'implementazione di ambienti di disaster recovery è una sfida per la maggior parte delle organizzazioni a causa dei requisiti di indipendenza dell'infrastruttura e del sito. Il numero di risorse necessarie e i costi di configurazione, test e manutenzione di un data center secondario possono essere molto elevati, in genere avvicinandosi al costo dell'intero ambiente di produzione. È difficile mantenere un impatto minimo sui dati con una protezione adeguata, sincronizzando continuamente i dati e stabilendo un failover e un failback perfetti. Dopo aver creato il sito di DR, la sfida diventa replicare i dati dall'ambiente di produzione e mantenerli sincronizzati in futuro.

Questo report tecnico riunisce la soluzione di infrastruttura convergente FlexPod, NetApp Cloud Volumes ONTAP su Google Cloud e Cisco Intersight per formare un data center di cloud ibrido per il DR. In questa soluzione discuteremo della progettazione e dell'esecuzione di un workflow ONTAP on-premise utilizzando Cisco Intersight Cloud Orchestrator. Discutiamo inoltre dell'implementazione di NetApp Cloud Volumes ONTAP e dell'orchestrazione e dell'automazione della replica dei dati e del DR tra FlexPod e Cloud Volumes ONTAP utilizzando il servizio di interoperabilità Cisco per HashiCorp Terraform.

La figura seguente fornisce una panoramica della soluzione.



Questa soluzione offre diversi vantaggi, tra cui:

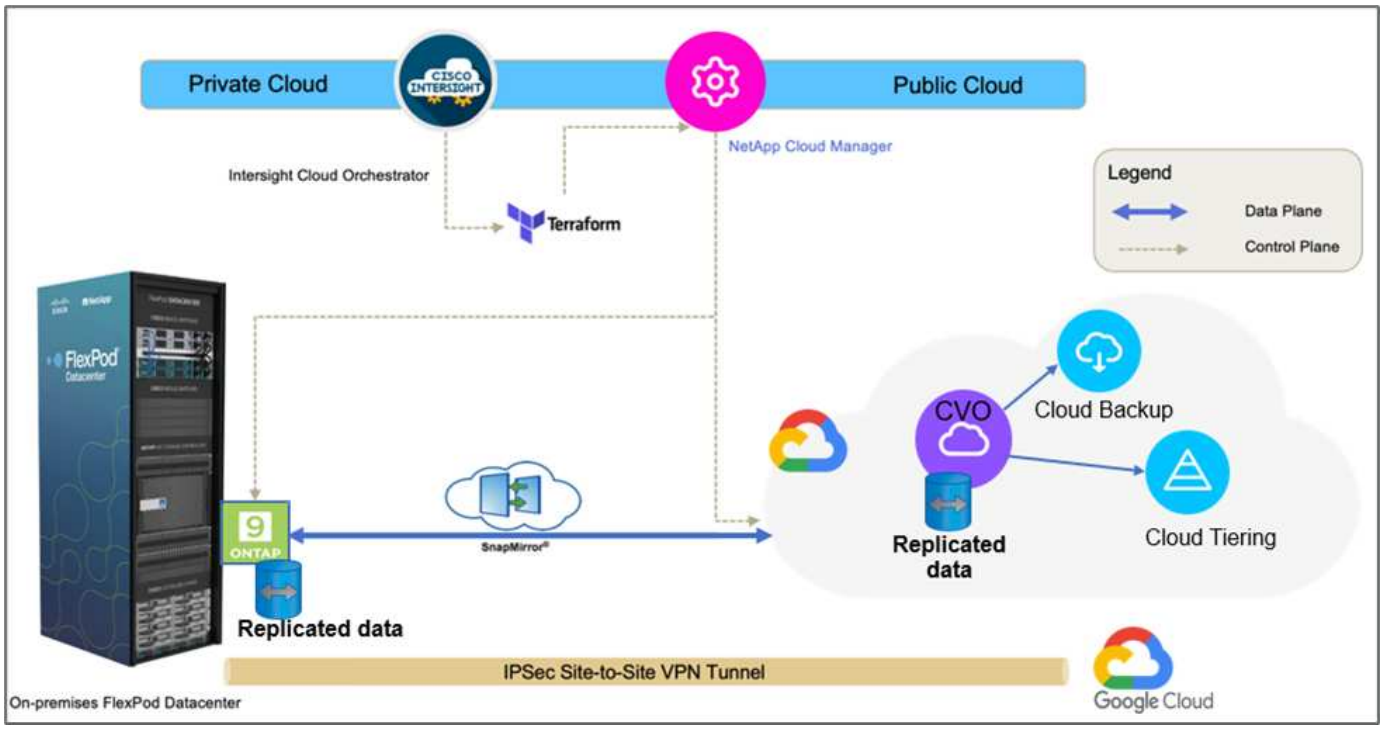
- **Orchestrazione e automazione.** Cisco Intersight semplifica le operazioni quotidiane dell'infrastruttura di cloud ibrido FlexPod fornendo framework di orchestrazione coerenti forniti tramite automazione.
- **Protezione personalizzata.** Cloud Volumes ONTAP offre replica dei dati a livello di blocco da ONTAP al cloud che mantiene aggiornata la destinazione attraverso aggiornamenti incrementali. Gli utenti possono specificare una pianificazione di sincronizzazione ogni 5 minuti o ogni ora, ad esempio, in base alle modifiche apportate all'origine che vengono trasferite.
- **Failover e failback perfetti.** in caso di disastro, gli amministratori dello storage possono eseguire rapidamente il failover sui volumi cloud. Quando il sito primario viene ripristinato, i nuovi dati creati nell'ambiente DR vengono sincronizzati di nuovo con i volumi di origine, ripristinando la replica dei dati secondari.
- **Efficienza:** lo spazio di storage e i costi per la copia del cloud secondario sono ottimizzati attraverso l'utilizzo di compressione dei dati, thin provisioning e deduplica. I dati vengono trasferiti a livello di blocco in forma compressa e deduplicata, migliorando la velocità di trasferimento. Inoltre, i dati vengono automaticamente suddivisi in livelli per lo storage a oggetti a basso costo e riportati allo storage dalle performance elevate solo quando si accede, ad esempio in uno scenario di DR. In questo modo si riducono significativamente i costi di storage in corso.
- **Aumento della produttività IT.** l'utilizzo di Intersight come singola piattaforma sicura e di livello Enterprise per la gestione del ciclo di vita dell'infrastruttura e delle applicazioni semplifica la gestione della configurazione e l'automazione delle attività manuali su larga scala per la soluzione.

Pubblico

I destinatari di questo documento includono, a titolo esemplificativo ma non esaustivo, tecnici di vendita, consulenti sul campo, servizi professionali, responsabili IT, Ingegneri partner, ingegneri dell'affidabilità del sito, architetti cloud, ingegneri cloud e clienti che vogliono sfruttare un'infrastruttura costruita per offrire efficienza IT e favorire l'innovazione IT.

Topologia della soluzione

In questa sezione viene descritta la topologia logica della soluzione. La figura seguente rappresenta la topologia della soluzione dell'ambiente FlexPod on-premise, NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud, Cisco Intersight e NetApp Cloud Manager.



I piani di controllo e i piani di dati sono chiaramente indicati tra gli endpoint. Il data plane utilizza una connessione VPN sicura da sito a sito per connettere l'istanza di ONTAP in esecuzione su FlexPod All Flash FAS all'istanza di NetApp Cloud Volumes ONTAP su Google Cloud.

La replica dei dati dei carichi di lavoro da FlexPod a NetApp Cloud Volumes ONTAP viene gestita da NetApp SnapMirror e il processo complessivo viene orchestrato utilizzando Cisco Intersight Cloud Orchestrator sia per gli ambienti on-premise che per gli ambienti cloud. Cisco Intersight Cloud Orchestrator utilizza i provider di risorse Terraform per NetApp Cloud Manager per eseguire operazioni relative all'implementazione di NetApp Cloud Volumes ONTAP e stabilire relazioni di replica dei dati.

Questa soluzione supporta anche il backup opzionale e il tiering dei dati cold che risiedono nell'istanza di NetApp Cloud Volumes ONTAP su Google Cloud Storage.

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp ONTAP, networking Cisco Nexus, storage networking Cisco MDS e Cisco Unified Computing System (Cisco UCS). Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare

più configurazioni.

Cisco Intersight

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

- **Delivery più rapida.** offerta come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può concentrarsi sull'accelerazione dell'erogazione per la linea di business.
- **Operazioni semplificate.** semplifica le operazioni utilizzando un unico tool sicuro fornito da SaaS con inventario, autenticazione e API comuni per lavorare nell'intero stack e in tutte le ubicazioni, eliminando i silos tra i team. Dalla gestione on-premise di server fisici e hypervisor a macchine virtuali, K8s, serverless, automazione, ottimizzazione e controllo dei costi su cloud pubblici e on-premise.
- **Ottimizzazione continua.** Ottimizza continuamente il tuo ambiente utilizzando l'intelligence fornita da Cisco Intersight su ogni livello e Cisco TAC. Questa intelligenza viene convertita in azioni consigliate e automatizzabili, in modo da poter adattare in tempo reale ad ogni cambiamento: Dallo spostamento dei carichi di lavoro al monitoraggio dello stato di salute dei server fisici ai consigli per la riduzione dei costi sui cloud pubblici con cui lavorate.

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

Licenze Cisco Intersight

Cisco Intersight utilizza una licenza basata su abbonamento con più livelli.

I livelli di licenza Cisco Intersight sono i seguenti:

- **Cisco Intersight Essentials.** include tutte le funzionalità di base e le seguenti funzionalità:
  - Cisco UCS Central
  - Diritto a Cisco IMC Supervisor
  - Configurazione basata su policy con profili server
  - Gestione del firmware
  - Valutazione della compatibilità con l'elenco di compatibilità hardware (HCL)
- **Cisco Intersight Advantage.** include le funzionalità e le funzionalità del Tier Essentials oltre alle seguenti funzionalità:
  - Widget, inventario, capacità, funzionalità di utilizzo e correlazione dell'inventario tra domini tra calcolo fisico, rete, storage, virtualizzazione VMware e cloud pubblico AWS.
  - Servizio Cisco Security Advisory in cui i clienti possono ricevere importanti avvisi di sicurezza e avvisi sul campo relativi ai dispositivi endpoint interessati.
- **Cisco Intersight Premier.** oltre alle funzionalità offerte dal livello Advantage, Cisco Intersight Premier offre quanto segue:
  - Intersight Cloud Orchestrator (ICO) per Cisco e terze parti per calcolo, rete, storage, sistemi integrati, virtualizzazione, piattaforme container e cloud pubblico
  - Diritto di iscrizione completo per Cisco UCS Director senza costi aggiuntivi.

Ulteriori informazioni sulle licenze Intersight e sulle funzionalità supportate in ciascuna licenza sono disponibili "qui".

> In questa soluzione, utilizziamo Intersight Cloud Orchestrator e Intersight Service per HashiCorp Terraform. Queste funzionalità sono disponibili per gli utenti con licenza Intersight Premier, pertanto questo livello di licenza deve essere attivato.

Integrazione del cloud terraform con ICO

È possibile utilizzare Cisco Intersight Cloud Orchestrator (ICO) per creare ed eseguire flussi di lavoro che chiamano le API di Terraform Cloud (TFC). L'attività Invoke Web API Request supporta Terraform Cloud come destinazione e può essere configurata con le API di Terraform Cloud utilizzando i metodi HTTP. Pertanto, il flusso di lavoro può avere una combinazione di attività che richiama più API di Terraform Cloud utilizzando attività API generiche e altre operazioni. È necessaria una licenza Premier per utilizzare la funzione ICO.

Cisco Intersight Assist

Cisco Intersight Assist consente di aggiungere dispositivi endpoint a Cisco Intersight. Un data center potrebbe avere più dispositivi che non si connettono direttamente a Cisco Intersight. Qualsiasi dispositivo supportato da Cisco Intersight ma non connesso direttamente ad esso richiede un meccanismo di connessione. Cisco Intersight Assist offre questo meccanismo di connessione e consente di aggiungere dispositivi a Cisco Intersight.

Cisco Intersight Assist è disponibile all'interno di Cisco Intersight Virtual Appliance, che viene distribuita come macchina virtuale implementabile contenuta in un formato di file OVA (Open Virtual Appliance). È possibile installare l'appliance su un server ESXi. Per ulteriori informazioni, consultare "Cisco Intersight Virtual Appliance Getting Started Guide".

Dopo aver richiesto Intersight Assist a Intersight, puoi richiedere i dispositivi endpoint utilizzando l'opzione Claim Through Intersight Assist. Per ulteriori informazioni, vedere "Per iniziare".

NetApp Cloud Volumes ONTAP

- Utilizzo della deduplica dei dati integrata, della compressione dei dati, del thin provisioning e della clonazione per ridurre al minimo i costi dello storage.
- Affidabilità aziendale e operazioni continue in caso di guasti nel tuo ambiente cloud.
- Cloud Volumes ONTAP utilizza NetApp SnapMirror, la tecnologia di replica leader del settore, per replicare i dati on-premise nel cloud, in modo che sia facile disporre di copie secondarie per diversi casi di utilizzo.
- Cloud Volumes ONTAP si integra anche con Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.
- Passaggio tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.
- Coerenza delle copie Snapshot con NetApp SnapCenter.
- Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.
- L'integrazione con Cloud Data Sense ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

Cloud Central

Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi ti consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il

backup dei dati SaaS e migrare e controllare in modo efficace i dati su più cloud. Per ulteriori informazioni, vedere "Cloud Central".

Cloud Manager

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

Connettore

Connector consente a Cloud Manager di gestire risorse e processi all'interno di un ambiente di cloud pubblico. Un'istanza di connettore è necessaria per utilizzare molte funzionalità fornite da Cloud Manager e può essere implementata nel cloud o nella rete on-premise. Il connettore è supportato nelle seguenti posizioni:

- AWS
- Microsoft Azure
- Google Cloud
- On-premise

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager consente di monitorare i cluster di storage ONTAP da un'unica interfaccia intuitiva, riprogettata, che offre intelligence basata su conoscenze della community e analytics ai. Fornisce informazioni complete su operazioni, performance e proattive sull'ambiente di storage e sulle macchine virtuali in esecuzione. Quando si verifica un problema con l'infrastruttura di storage, Unified Manager può notificare i dettagli del problema per identificare la causa principale. La dashboard della macchina virtuale offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter analizzare l'intero percorso di i/o dall'host vSphere fino alla rete e infine allo storage.

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

VMware vSphere

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

Per ulteriori informazioni su VMware vSphere, seguire "questo link".

VMware vSphere vCenter

VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da una singola console e aggrega il monitoraggio delle performance di cluster, host e macchine virtuali. VMware vCenter

Server offre agli amministratori una panoramica approfondita dello stato e della configurazione di cluster di calcolo, host, macchine virtuali, storage, sistema operativo guest, e altri componenti critici di un'infrastruttura virtuale. VMware vCenter gestisce l'insieme completo di funzionalità disponibili in un ambiente VMware vSphere.

Versioni hardware e software

Questa soluzione di cloud ibrido può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware, come definito nello strumento matrice di interoperabilità NetApp e nell'elenco di compatibilità hardware Cisco UCS.

La soluzione FlexPod utilizzata come piattaforma di riferimento nel nostro ambiente on-premise è stata implementata in base alle linee guida e alle specifiche descritte "qui".

La rete all'interno di questo ambiente è basata su ACI. Per ulteriori informazioni, vedere "qui".

- Per ulteriori informazioni, consultare i seguenti collegamenti:
- "Tool di matrice di interoperabilità NetApp"
- "Guida alla compatibilità VMware"
- "Cisco UCS hardware and Software Interoperability Tool"

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

Componente	Prodotto	Versione
Calcolo	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnects 6454	4.2(2a)
Rete	Cisco Nexus 9332C (colonna vertebrale)	14.2(7)
	Cisco Nexus 9336C-FX2 (Leaf)	14.2(7)
	Cisco ACI	4.2(7)
Storage	NetApp AFF A220	9.11.1
	Strumenti NetApp ONTAP per VMware vSphere	9.10
	NetApp NFS Plugin per VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Software	VSphere ESXi	7.0 (U3)
	Appliance VMware vCenter	7.0.3
	Appliance virtuale Cisco Intersight Assist	1.0.11-306

L'esecuzione delle configurazioni Terraform avviene sull'account Terraform Cloud for Business. La configurazione del terraform utilizza il provider Terraform per NetApp Cloud Manager.

La seguente tabella elenca i vendor, i prodotti e le versioni.

Componente	Prodotto	Versione
HashiCorp	Terraform	1.2.7

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

Componente	Prodotto	Versione
NetApp	Cloud Volumes ONTAP	9.11
	Cloud Manager	3.9.21

"Pagina successiva: Installazione e configurazione - implementazione di FlexPod."

Installazione e configurazione

Implementare FlexPod

"Precedente: Componenti della soluzione."

Per informazioni dettagliate sulla progettazione e l'implementazione di FlexPod, inclusa la configurazione dei vari elementi di progettazione e le Best practice associate, vedere "Cisco Validated Design per FlexPod".

FlexPod può essere implementato sia in modalità gestita UCS che in modalità gestita Cisco Intersight. Se si sta implementando FlexPod in modalità gestita UCS, è possibile trovare la versione più recente di Cisco Validated Design "qui".

Cisco Unified Compute System (Cisco UCS) X-Series è un nuovissimo sistema di calcolo modulare, configurato e gestito dal cloud. È progettato per soddisfare le esigenze delle applicazioni moderne e per migliorare l'efficienza operativa, l'agilità e la scalabilità attraverso un design modulare adattabile, pronto al futuro. È possibile trovare le indicazioni di progettazione relative all'integrazione della piattaforma UCS X-Series gestita da Cisco Intersight nell'infrastruttura FlexPod "qui".

È possibile trovare FlexPod con implementazione Cisco ACI "qui".

"Pagina successiva: Configurazione di Cisco Intersight."

Configurazione di Cisco Intersight

"Precedente: Implementare FlexPod."

Per configurare Cisco Intersight e Intersight Assist, consultare il documento Cisco Validated Designs for FlexPod Found "qui".

"Pagina successiva: Integrazione del cloud terraform con prerequisito ICO."

Integrazione del cloud terraform con prerequisito ICO

"Precedente: Configurazione di Cisco Intersight."

Procedura 1: Connettere Cisco Intersight e Terraform Cloud

1. Richiedi o crea un target cloud Terraform fornendo i dettagli dell'account Terraform Cloud pertinente.
2. Creare un target di Terraform Cloud Agent per i cloud privati in modo che i clienti possano installare l'agente nel data center e abilitare la comunicazione con Terraform Cloud.

   Per ulteriori informazioni, seguire "questo link".

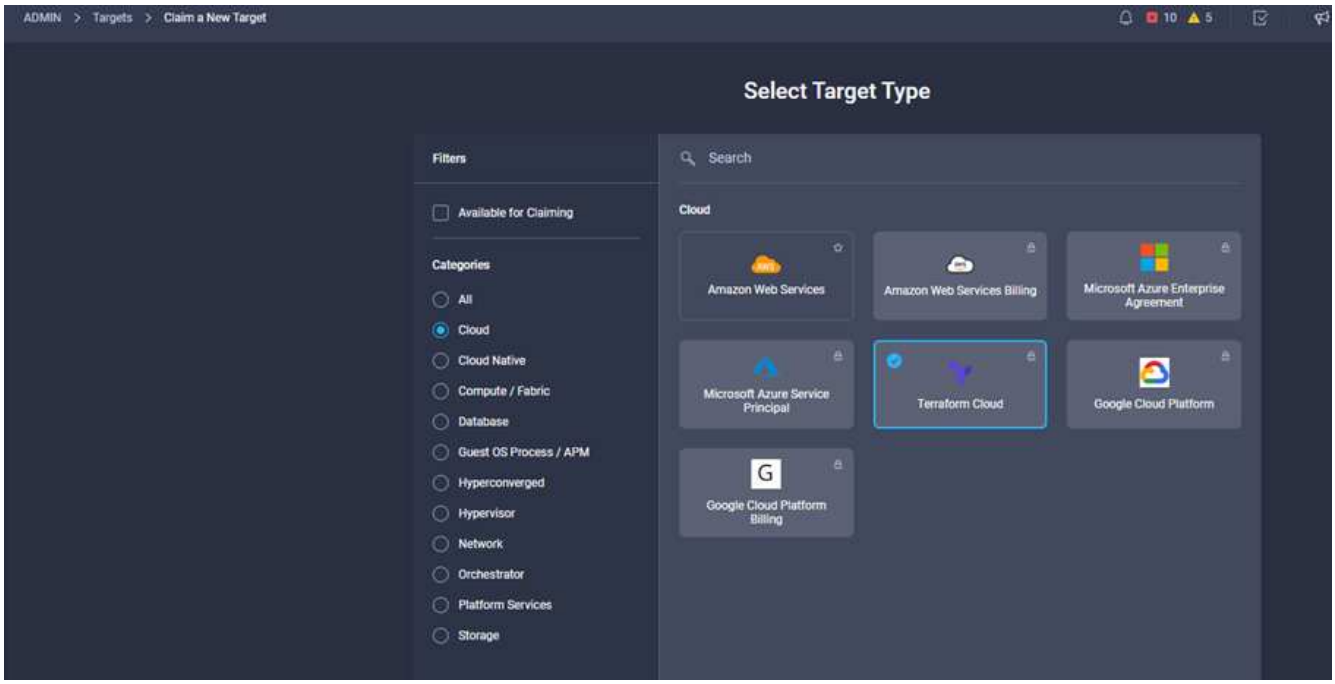
Procedura 2: Generazione del token utente

Come parte dell'aggiunta di una destinazione per Terraform Cloud, devi fornire il nome utente e il token API dalla pagina delle impostazioni di Terraform Cloud.

1. Accedi a Terraform Cloud e vai a **User Tokens**: "https://app.terraform.io/app/settings/tokens".
2. Fare clic su **Crea un nuovo token API**.
3. Assegnare un nome da ricordare e salvare il token in un luogo sicuro.

Procedura 3: Richiesta di rimborso del target cloud Terraform

1. Accedere a Intersight con i privilegi di account Administrator, Device Administrator o Device Technician.
2. Accedere a **ADMIN > Target > Richiedi un nuovo target**.
3. In **Categorie**, fare clic su **Cloud**.
4. Fare clic su **Terraform Cloud** e fare clic su **Start**.



5. Immettere un nome per la destinazione, il nome utente per Terraform Cloud, il token API e un'organizzazione predefinita in Terraform Cloud, come mostrato nell'immagine seguente.
6. Nel campo **Default Managed Hosts**, assicurarsi di aggiungere i seguenti collegamenti insieme ad altri host gestiti:
   - github.com
   - github-releases.githubusercontent.com

Se tutto viene inserito correttamente, il target di Terraform Cloud verrà visualizzato nella sezione **Intersight targets**.

Procedura 4: Aggiunta di agenti Terraform Cloud

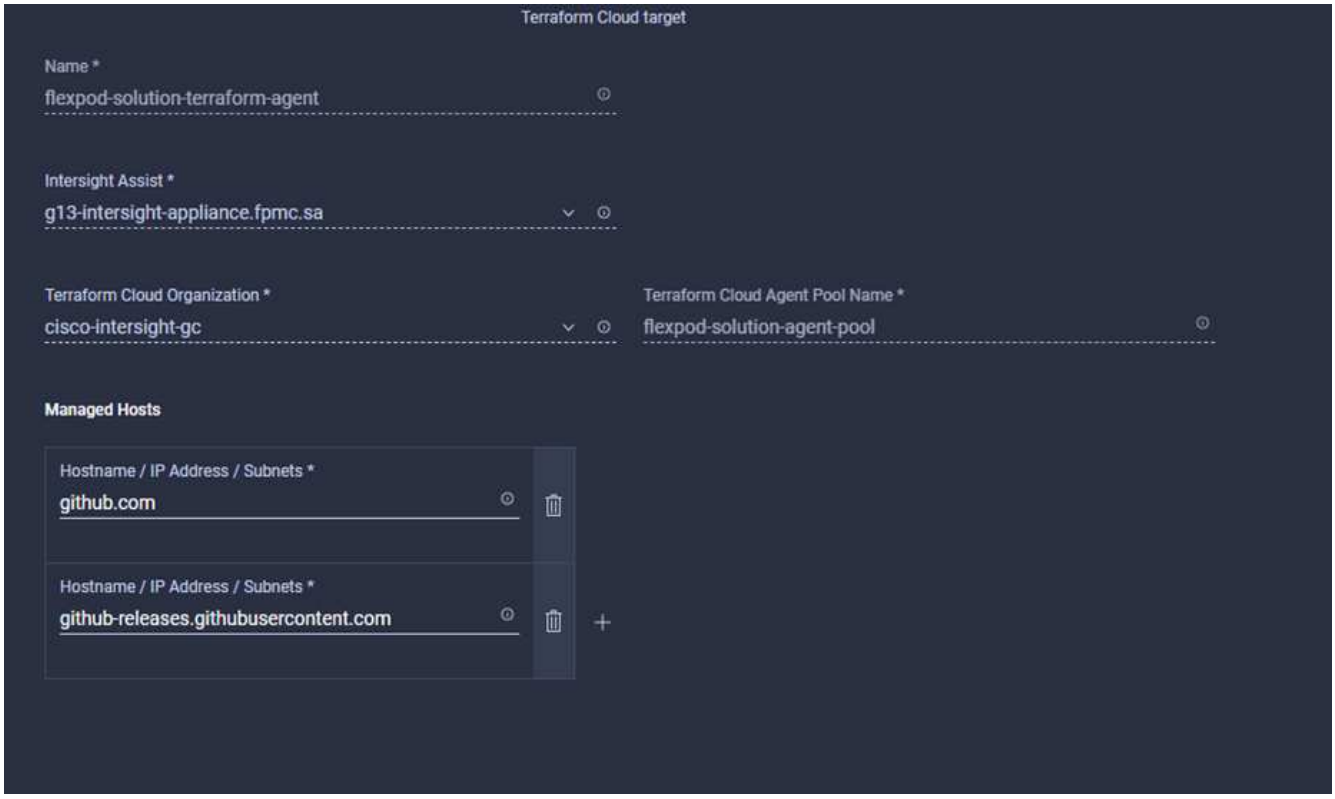
Prerequisiti:

- Destinazione di Terraform Cloud.
- Ha richiesto Intersight Assist in Intersight prima di implementare Terraform Cloud Agent.

> È possibile richiedere solo cinque agenti per ciascun Assist.

> Dopo aver creato la connessione a Terraform, è necessario eseguire lo spin up di un Terraform Agent per eseguire il codice Terraform.

1. Fare clic su **Claim Terraform Cloud Agent** dall'elenco a discesa della destinazione di Terraform Cloud.
2. Inserire i dettagli dell'agente Terraform Cloud. La seguente schermata mostra i dettagli di configurazione per l'agente Terraform.



È possibile aggiornare qualsiasi proprietà di Terraform Agent. Se la destinazione si trova nello stato **non connesso** e non si trova mai nello stato **connesso**, non è stato generato alcun token per l'agente Terraform.

Una volta completata la convalida dell'agente e generato un token, non è possibile riconfigurare l'organizzazione e/o il pool di agenti. La corretta implementazione di un agente Terraform è indicata dallo stato **connesso**.

Dopo aver attivato e richiesto l'integrazione di Terraform Cloud, puoi implementare uno o più agenti di Terraform Cloud in Cisco Intersight Assist. L'agente Terraform Cloud viene modellato come target figlio dell'obiettivo di Terraform Cloud. Quando si richiede l'obiettivo dell'agente, viene visualizzato un messaggio che indica che la richiesta di rimborso è in corso.

Dopo alcuni secondi, la destinazione viene spostata nello stato **connesso** e la piattaforma Intersight instrada i pacchetti HTTPS dall'agente al gateway Terraform Cloud.

Il tuo Agente Terraform deve essere correttamente richiesto e deve essere visualizzato sotto obiettivi come **connesso**.

"Avanti: Configurare il provider di servizi cloud pubblico."

Configurare il provider di servizi di cloud pubblico

"Precedente: Integrazione del cloud terraform con prerequisito ICO."

Procedura 1: Accesso a NetApp Cloud Manager

Per accedere a NetApp Cloud Manager e ad altri servizi cloud, devi iscriverti a. "NetApp Cloud Central".

Per configurare le aree di lavoro e gli utenti nell'account Cloud Central, fare clic su "qui".

Procedura 2: Implementare il connettore

Per implementare Connector in Google Cloud, consulta questa sezione "collegamento".

"Successivo: Implementazione automatica dello storage NetApp per il cloud ibrido."

Implementazione automatica dello storage NetApp per il cloud ibrido

"Precedente: Configurare il provider di servizi di cloud pubblico."

Google Cloud

È necessario innanzitutto abilitare le API e creare un account di servizio che fornisca a Cloud Manager le autorizzazioni per implementare e gestire i sistemi Cloud Volumes ONTAP che si trovano nello stesso progetto del connettore o in progetti diversi.

Prima di implementare un connettore in un progetto Google Cloud, assicurarsi che il connettore non sia in esecuzione in sede o in un altro provider cloud.

Prima di implementare un connettore direttamente da Cloud Manager, è necessario disporre di due set di autorizzazioni:

- È necessario implementare Connector utilizzando un account Google che disponga delle autorizzazioni per avviare l'istanza di Connector VM da Cloud Manager.
- Durante l'implementazione di Connector, viene richiesto di selezionare l'istanza della macchina virtuale. Cloud Manager ottiene le autorizzazioni dall'account del servizio per creare e gestire i sistemi Cloud Volumes ONTAP per conto dell'utente. Le autorizzazioni vengono fornite allegando un ruolo personalizzato all'account del servizio.è necessario impostare due file YAML che includono le autorizzazioni richieste per l'utente e l'account del servizio. Scopri come utilizzare "I file YAML per impostare le autorizzazioni" qui.

Vedere "questo video dettagliato" per tutti i prerequisiti richiesti.

Architettura e modalità di implementazione di Cloud Volumes ONTAP

Cloud Volumes ONTAP è disponibile in Google Cloud come sistema a nodo singolo e come coppia di nodi ad alta disponibilità (ha). In base ai requisiti, possiamo scegliere la modalità di implementazione di Cloud Volumes ONTAP. L'aggiornamento di un sistema a nodo singolo a una coppia ha non è supportato. Se si desidera passare da un sistema a nodo singolo a una coppia ha, è necessario implementare un nuovo sistema e replicare i dati dal sistema esistente al nuovo sistema.

Cloud Volumes ONTAP altamente disponibile in Google Cloud

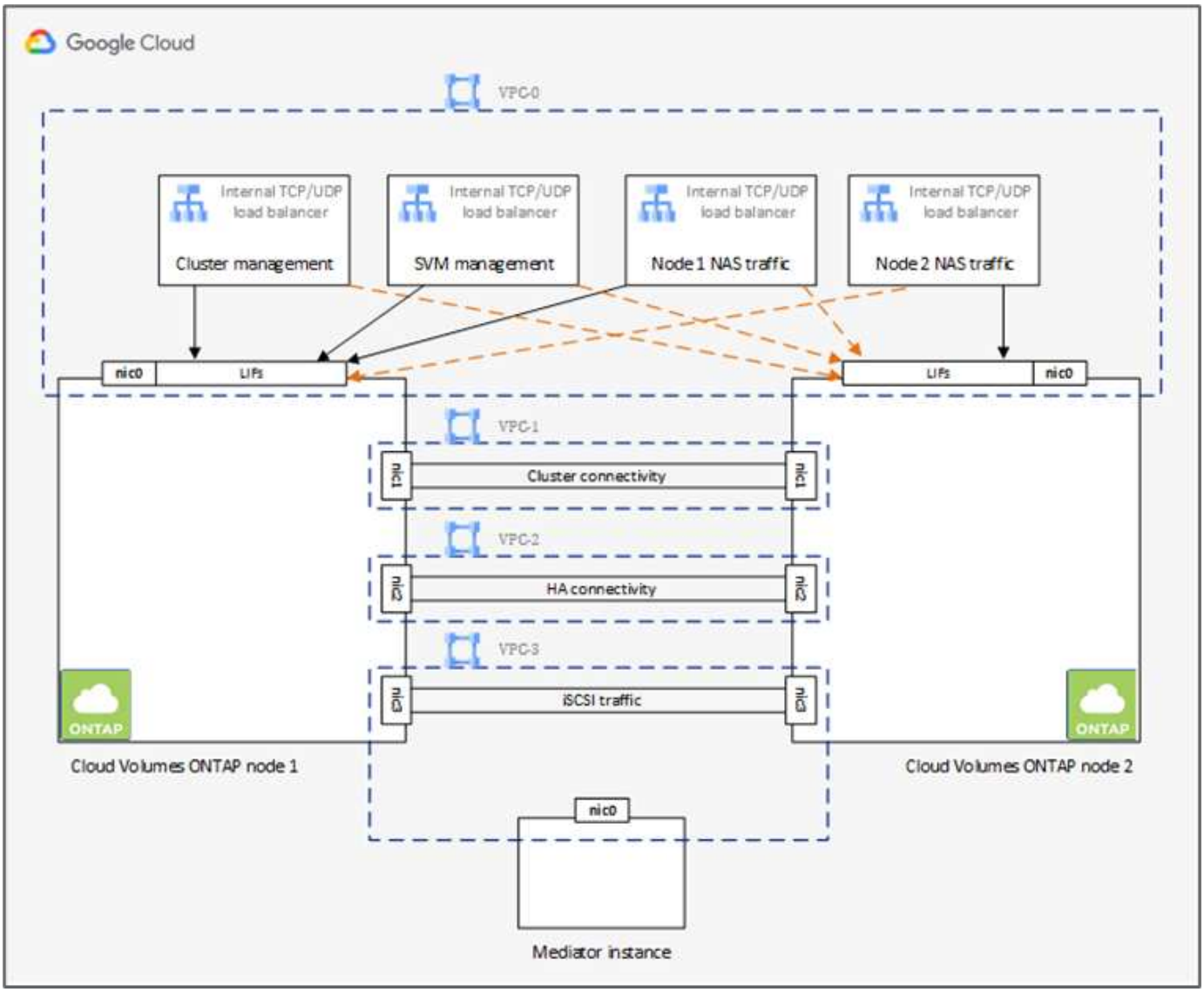
Google Cloud supporta l'implementazione di risorse in più aree geografiche e in più zone all'interno di una regione. L'implementazione ha è costituita da due nodi ONTAP che utilizzano potenti tipi di computer standard n1 o n2 disponibili in Google Cloud. I dati vengono replicati in modo sincrono tra i due nodi Cloud Volumes ONTAP per garantire la disponibilità in caso di guasto. L'implementazione HA di Cloud Volumes ONTAP richiede quattro VPC e una subnet privata in ciascun VPC. Le subnet dei quattro VPC devono essere dotate di intervalli CIDR non sovrapposti.

I quattro VPC vengono utilizzati per i seguenti scopi:

- VPC 0 consente la comunicazione in entrata ai nodi dati e Cloud Volumes ONTAP.

- VPC 1 offre connettività cluster tra nodi Cloud Volumes ONTAP.
- VPC 2 consente la replica RAM non volatile (NVRAM) tra i nodi.
- VPC 3 viene utilizzato per la connettività all'istanza del mediatore ha e per il traffico di replica del disco per le ricostruzioni dei nodi.

La seguente immagine mostra un Cloud Volumes ONTAP altamente disponibile in Goggle Cloud.



Per ulteriori informazioni, vedere "questo link".

Per i requisiti di rete per Cloud Volumes ONTAP in Google Cloud, consulta "questo link".

Per ulteriori informazioni sul tiering dei dati, vedere "questo link".

Impostare i prerequisiti dell'ambiente

La creazione automatica di cluster Cloud Volumes ONTAP, la configurazione di SnapMirror tra un volume on-premise e un volume cloud, la creazione di un volume cloud e così via vengono eseguite utilizzando la configurazione Terraform. Queste configurazioni Terraform sono ospitate su un account Terraform Cloud for Business. Utilizzando Intersight Cloud Orchestrator, puoi orchestrare attività come la creazione di un'area di lavoro in un account Terraform Cloud per Business, aggiungere tutte le variabili richieste all'area di lavoro,

eseguire un piano Terraform e così via.

Per queste attività di automazione e orchestrazione, sono necessari alcuni requisiti e dati, come descritto nelle sezioni seguenti.

Repository di GitHub

Devi disporre di un account GitHub per ospitare il tuo codice Terraform. Intersight Orchestrator crea un nuovo spazio di lavoro nell'account Terraform Cloud for Business. Questa area di lavoro è configurata con un flusso di lavoro di controllo della versione. A tale scopo, è necessario mantenere la configurazione Terraform in un repository GitHub e fornirla come input durante la creazione dello spazio di lavoro.

"Questo link GitHub" Fornisce la configurazione Terraform con diverse risorse. Puoi forare questo repository e fare una copia nel tuo account GitHub.

In questo repository, `provider.tf` Ha la definizione per il provider Terraform richiesto. Viene utilizzato il provider di terraform per NetApp Cloud Manager.

`variables.tf` contiene tutte le dichiarazioni variabili. Il valore di queste variabili viene immesso come input del workflow di Intersight Cloud Orchestrator. In questo modo è possibile passare i valori a un'area di lavoro ed eseguire la configurazione del Terraform.

`resources.tf` Definisce le varie risorse necessarie per aggiungere un ONTAP on-premise all'ambiente di lavoro, creare un cluster Cloud Volumes ONTAP a nodo singolo su Google Cloud, stabilire una relazione SnapMirror tra on-premise e Cloud Volumes ONTAP, creare un volume cloud su Cloud Volumes ONTAP e così via.

In questo repository:

- `provider.tf` Ha NetApp Cloud Manager come definizione per il Terraform provider richiesto.
- `variables.tf` Contiene le dichiarazioni variabili utilizzate come input per il flusso di lavoro di Intersight Cloud Orchestrator. In questo modo è possibile passare i valori all'area di lavoro ed eseguire la configurazione Terraform.
- `resources.tf` Definisce varie risorse per aggiungere un ONTAP on-premise all'ambiente di lavoro, creare un cluster Cloud Volumes ONTAP a nodo singolo su Google Cloud, stabilire una relazione SnapMirror tra on-premise e Cloud Volumes ONTAP, creare un volume cloud su Cloud Volumes ONTAP e così via.

È possibile aggiungere un ulteriore blocco di risorse per creare più volumi su Cloud Volumes ONTAP o utilizzare il conteggio o. `for_each` Costrutti di terraform.

Per connettere spazi di lavoro, moduli e set di policy Terraform a repository contenenti configurazioni Terraform, Terraform Cloud deve accedere al tuo repo GitHub.

Se si aggiunge un client, l'ID token OAuth del client viene utilizzato come input del flusso di lavoro di Intersight Cloud Orchestrator.

1. Accedi al tuo account Terraform Cloud per Business. Selezionare **Impostazioni > Provider**.
2. Fare clic su **Aggiungi un provider VCS**.
3. Selezionare la versione.
4. Seguire la procedura sotto **Configura provider**.
5. Il client aggiunto viene visualizzato in **VCS Providers**. Prendere nota dell'ID token OAuth.

Token di refresh per le operazioni API di NetApp Cloud Manager

Oltre all'interfaccia del browser Web, Cloud Manager dispone di un'API REST che fornisce agli sviluppatori software l'accesso diretto alla funzionalità Cloud Manager attraverso l'interfaccia SaaS. Il servizio Cloud Manager è costituito da diversi componenti distinti che formano collettivamente una piattaforma di sviluppo estensibile. Il token refresh consente di generare token di accesso che si aggiungono all'intestazione Authorization per ogni chiamata API.

Senza chiamare direttamente un'API, il provider netapp-cloudmanager utilizza un token di refresh e traduce le risorse Terraform in corrispondenti chiamate API. Devi generare un token di refresh per le operazioni API di NetApp Cloud Manager da "NetApp Cloud Central".

Per creare risorse su Cloud Manager, ad esempio la creazione di un cluster Cloud Volumes ONTAP, la configurazione di SnapMirror e così via, è necessario disporre dell'ID client di Cloud Manager Connector.

1. Accedi a Cloud Manager: "https://cloudmanager.netapp.com/".
2. Fare clic su **Connector** (connettore).
3. Fare clic su **Gestisci connettori**.
4. Fare clic sui puntini di sospensione e copiare l'ID del connettore.

Sviluppare il workflow di Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator è disponibile in Cisco Intersight se:

- È stata installata la licenza Intersight Premier.
- Sei un amministratore dell'account, un amministratore dello storage, un amministratore della virtualizzazione o un amministratore del server e hai almeno un server assegnato.

Progettazione workflow

Workflow Designer consente di creare nuovi flussi di lavoro (oltre a attività e tipi di dati) e modificare i flussi di lavoro esistenti per gestire le destinazioni in Cisco Intersight.

Per avviare Workflow Designer, accedere a **Orchestration > Workflow**. Una dashboard visualizza i seguenti dettagli nelle schede **My workflow**, **Sample workflow** e **All workflow**:

- Stato di convalida
- Ultimo stato di esecuzione
- Flussi di lavoro principali in base al numero di esecuzioni
- Categorie principali di flussi di lavoro
- Numero di flussi di lavoro definiti dal sistema
- Flussi di lavoro principali in base alle destinazioni

Utilizzando la dashboard, è possibile creare, modificare, clonare o eliminare una scheda. Per creare una scheda di visualizzazione personalizzata, fare clic su **+**, specificare un nome, quindi selezionare i parametri necessari da visualizzare nelle colonne, nelle colonne dei tag e nei widget. È possibile rinominare una scheda se non presenta l'icona **Lock**.

Sotto la dashboard è presente un elenco tabulare di flussi di lavoro che visualizza le seguenti informazioni:

- Nome visualizzato

- Descrizione
- Definito dal sistema
- Versione predefinita
- Esecuzioni
- Ultimo stato di esecuzione
- Stato di convalida
- Ultimo aggiornamento
- Organizzazione

La colonna Actions (azioni) consente di eseguire le seguenti azioni:

- **Esegui.** esegue il flusso di lavoro.
- **History.** Visualizza la cronologia di esecuzione del workflow.
- **Gestisci versioni.** Crea e gestisci le versioni per i flussi di lavoro.
- **Delete.** Elimina un flusso di lavoro.
- **Riprova.** Riprovare un flusso di lavoro non riuscito.

Workflow

Creare un flusso di lavoro composto dai seguenti passaggi:

- **Definizione di un flusso di lavoro.** specificare il nome visualizzato, la descrizione e altri attributi importanti.
- **Definire gli input e gli output del workflow.** specificare quali parametri di input sono obbligatori per l'esecuzione del workflow e gli output generati al momento dell'esecuzione
- **Aggiungi attività di workflow.** Aggiungi una o più attività di workflow in Workflow Designer che sono necessarie al workflow per svolgere la sua funzione.
- *Convalidare il flusso di lavoro. *Convalidare un workflow per garantire che non ci siano errori nella connessione degli input e output delle attività.

Creazione di flussi di lavoro per lo storage FlexPod on-premise

Per configurare un flusso di lavoro per lo storage FlexPod on-premise, vedere "questo link".

"Segue: Workflow di DR."

Workflow di DR

"Precedente: Implementazione automatica dello storage NetApp per il cloud ibrido."

La sequenza delle fasi è la seguente:

1. Definire il flusso di lavoro.
    - Creare un nome breve e intuitivo per il flusso di lavoro, ad esempio Disaster Recovery Workflow.
2. Definire l'input del flusso di lavoro. Gli input che prendiamo per questo flusso di lavoro includono quanto segue:

- Opzioni del volume (nome del volume, percorso di montaggio)
- Capacità del volume
- Data center associato al nuovo datastore
- Cluster su cui è ospitato il datastore
- Nome del nuovo datastore da creare in vCenter
- Tipo e versione del nuovo datastore
- Nome dell'organizzazione Terraform
- Spazio di lavoro terraform
- Descrizione dell'area di lavoro Terraform
- Variabili (sensibili e non sensibili) richieste per eseguire la configurazione Terraform
- Motivo dell'avvio del piano

3. Aggiungere le attività del flusso di lavoro.

   Le attività correlate alle operazioni in FlexPod includono quanto segue:

   - Creare un volume in FlexPod.
   - Aggiungere il criterio di esportazione dello storage al volume creato.
   - Mappare il volume appena creato su un datastore in VMware vCenter.

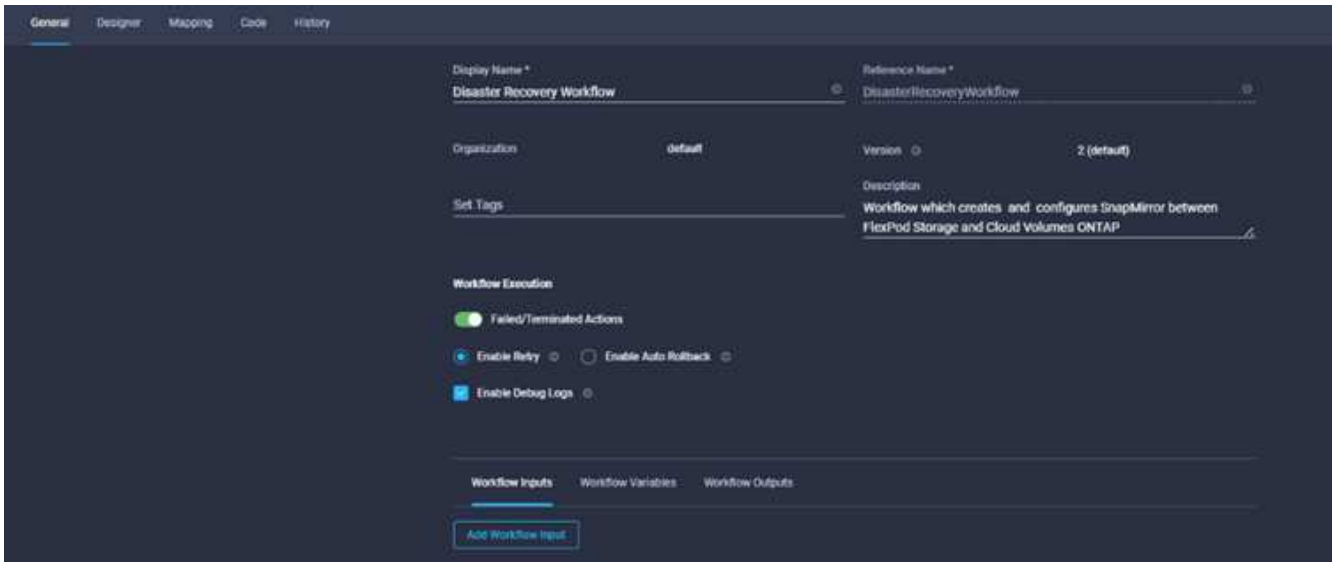
     Le attività relative alla creazione del cluster Cloud Volumes ONTAP:

   - Aggiungi spazio di lavoro Terraform
   - Aggiungere variabili terraform
   - Aggiungere variabili sensibili al terraform
   - Avvia un nuovo piano Terraform
   - Confermare l'esecuzione di Terraform

4. Validare il workflow.

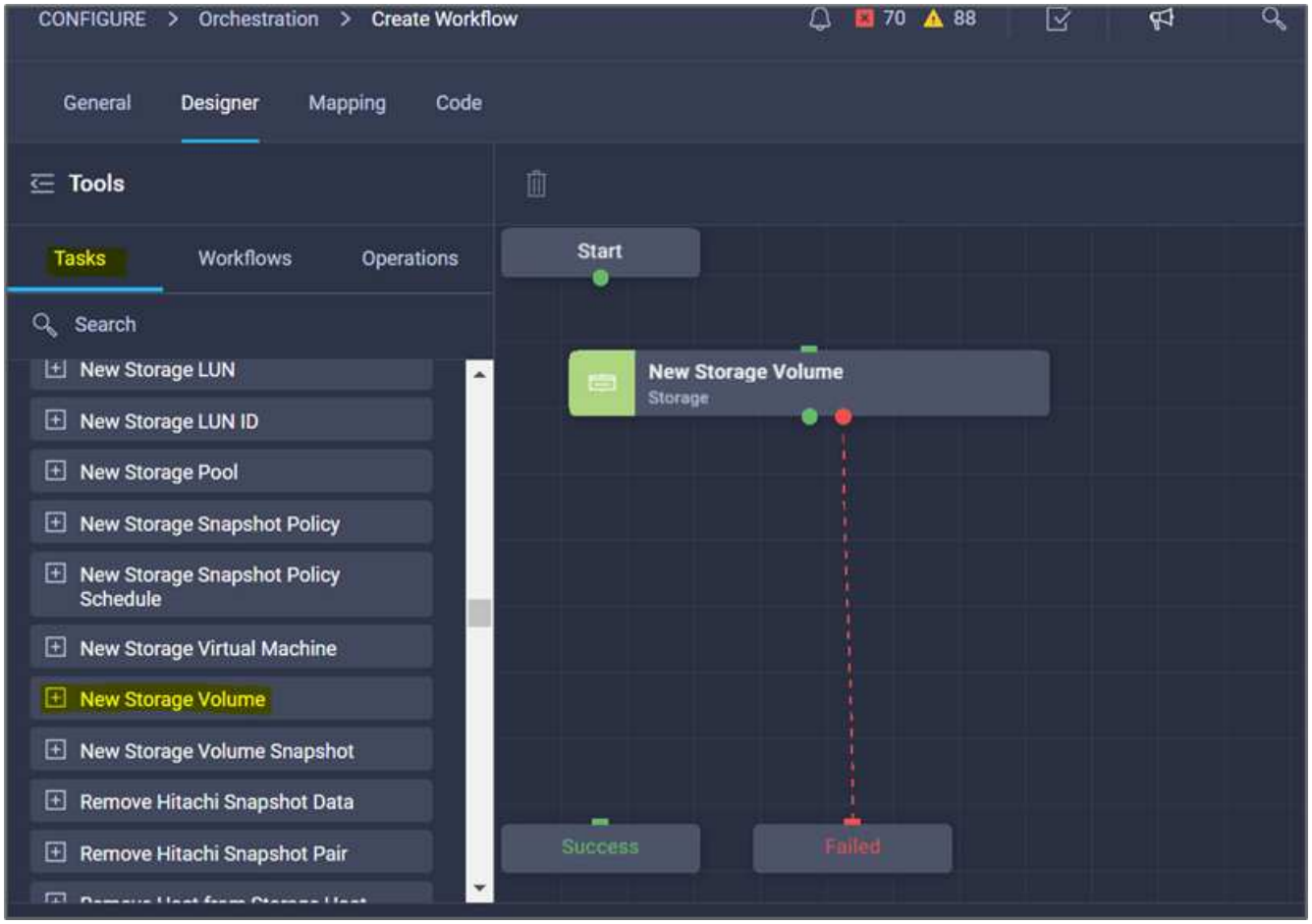
Procedura 1: Creazione del flusso di lavoro

1. Fare clic su **Orchestration** (orchestrazione) nel riquadro di navigazione a sinistra e fare clic su **Create Workflow** (Crea flusso di lavoro).
2. Nella scheda **Generale**:
   a. Fornire il nome visualizzato (flusso di lavoro di disaster recovery).
   b. Selezionare l'organizzazione, impostare i tag e fornire una descrizione.
3. Fare clic su Salva.

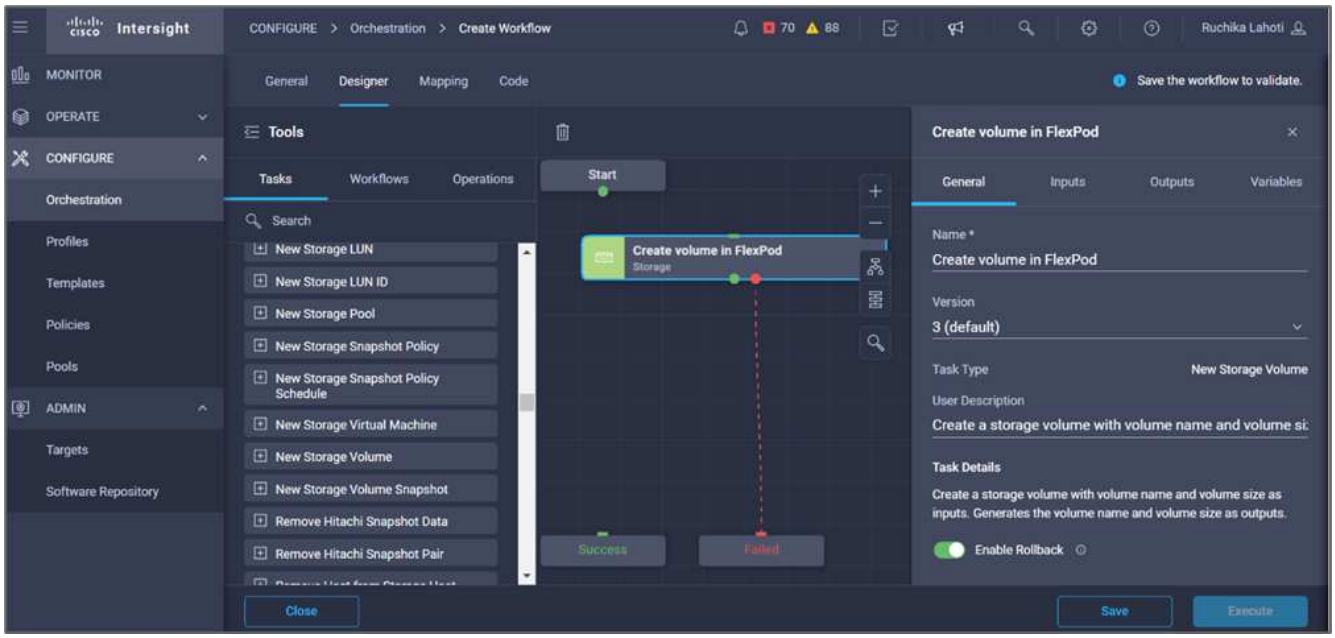


Procedura 2. Creare un nuovo volume in FlexPod

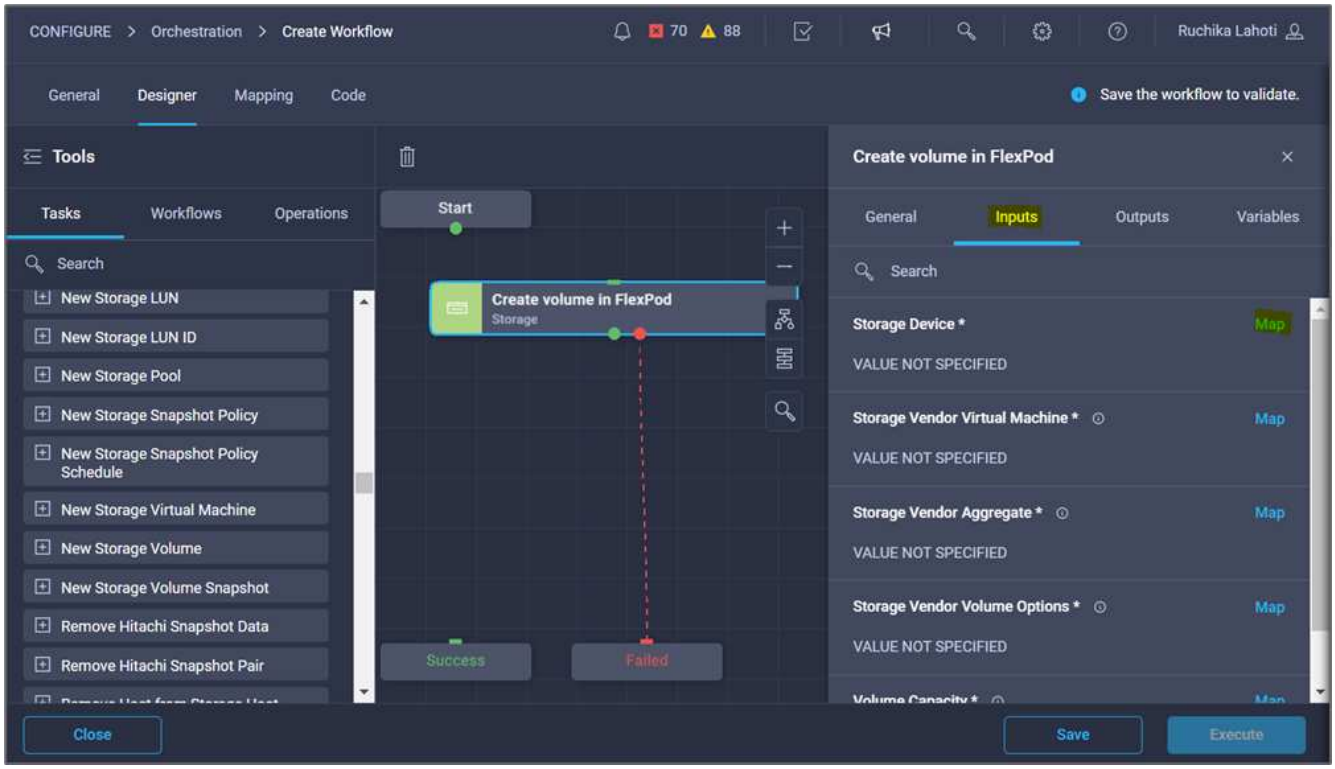
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Storage > New Storage Volume** (Storage > nuovo volume di storage) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Fare clic su **New Storage Volume** (nuovo volume di storage).



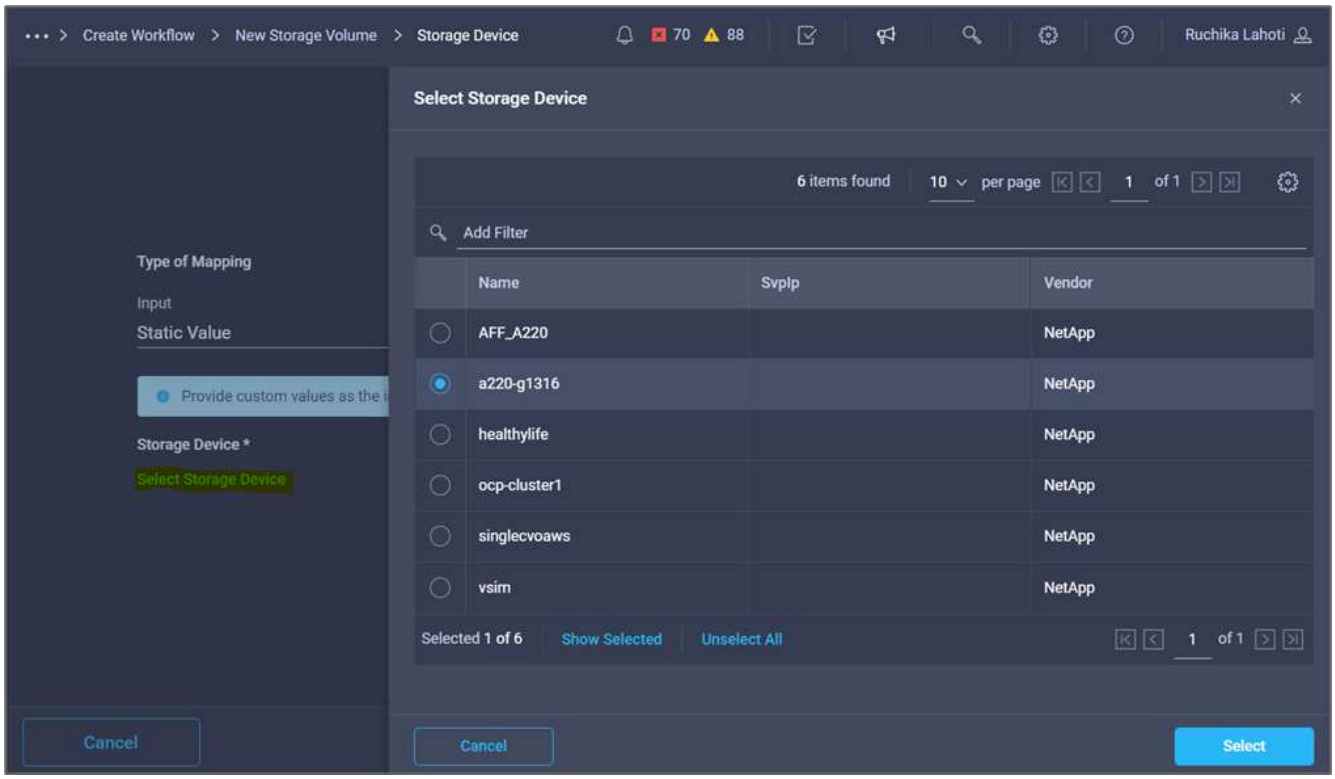
4. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Crea volume in FlexPod**.



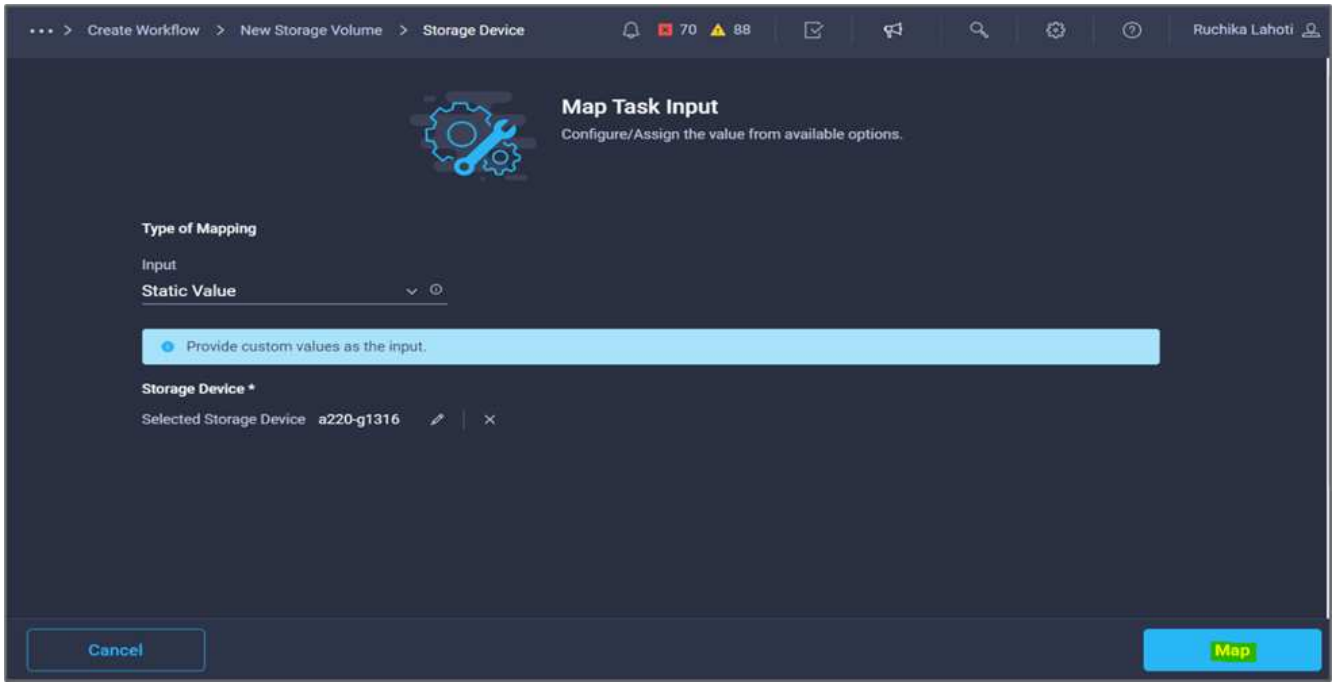
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Storage Device**.



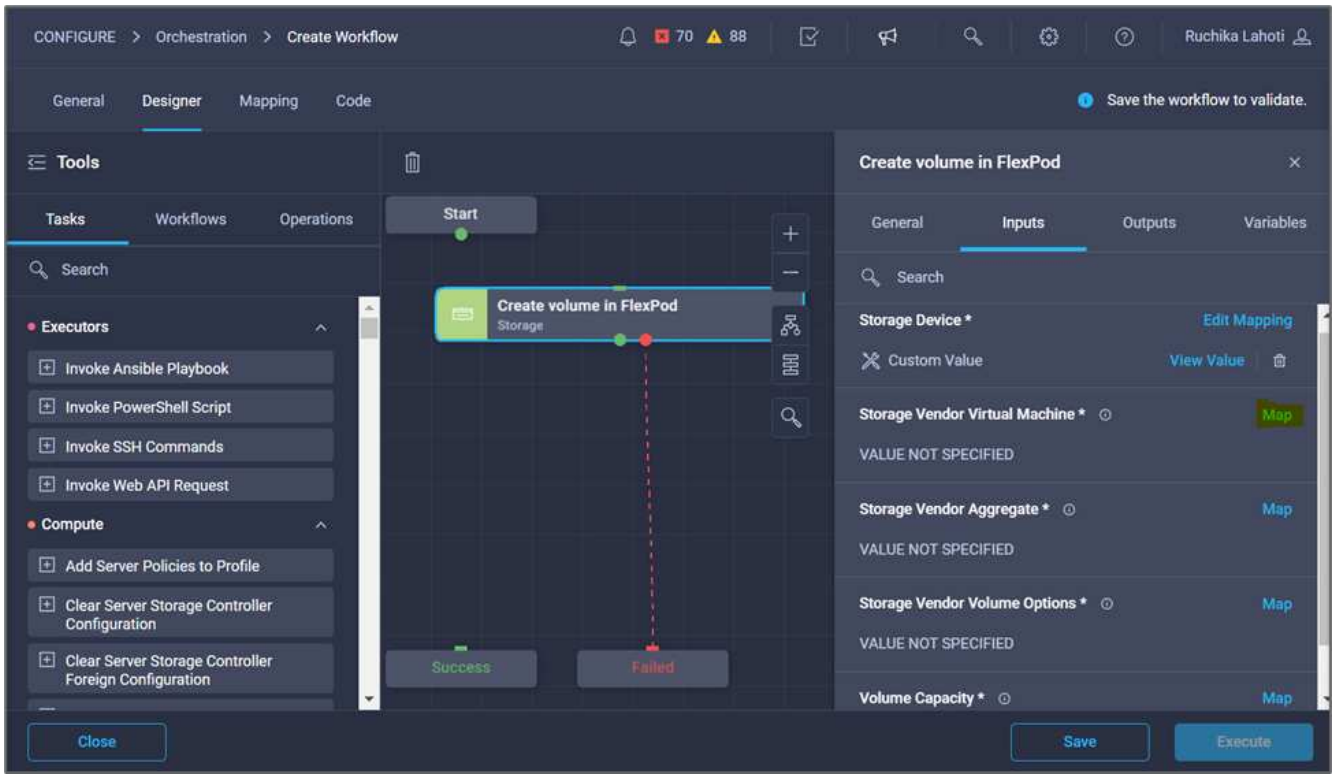
7. Scegliere **valore statico** e fare clic su **Seleziona dispositivo di storage**.
8. Fare clic sulla destinazione di storage aggiunta e fare clic su **Select** (Seleziona).



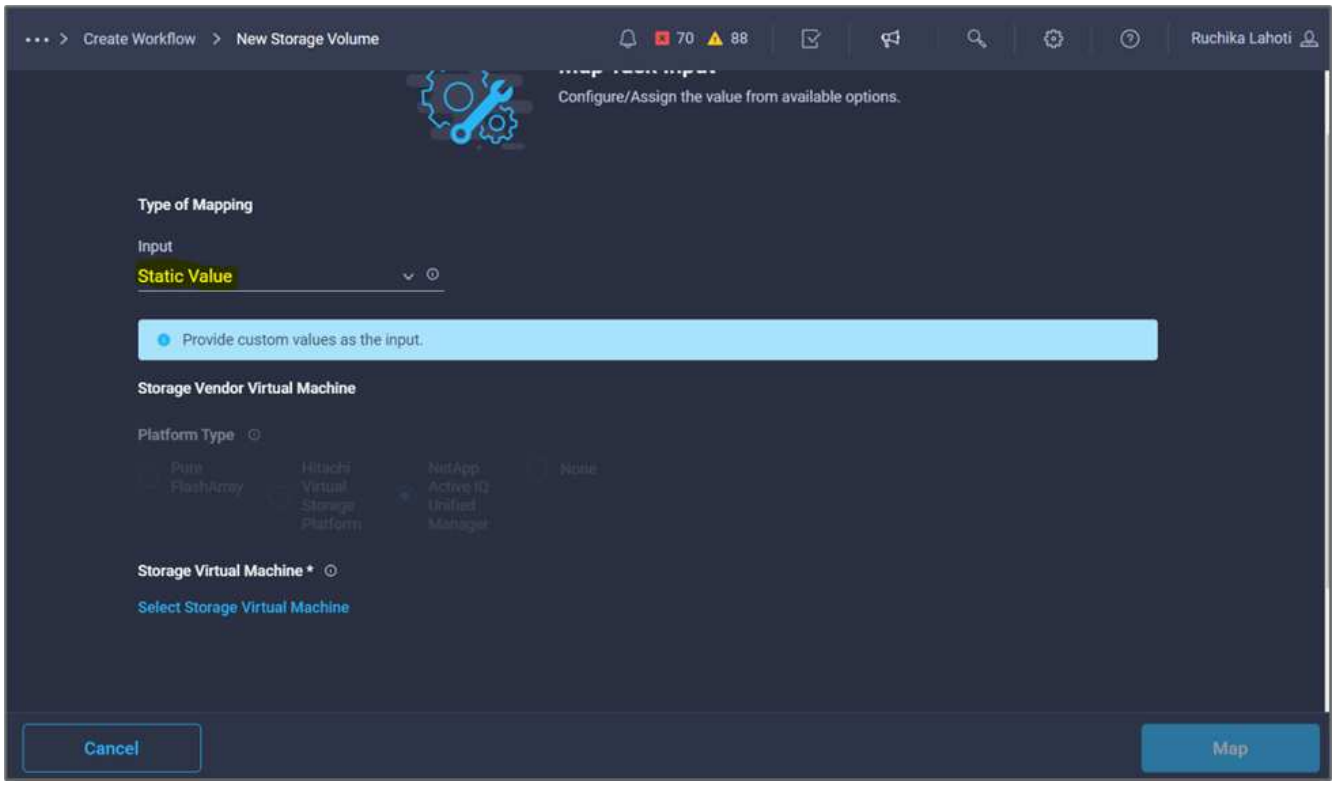
9. Fare clic su **Map** (Mappa).



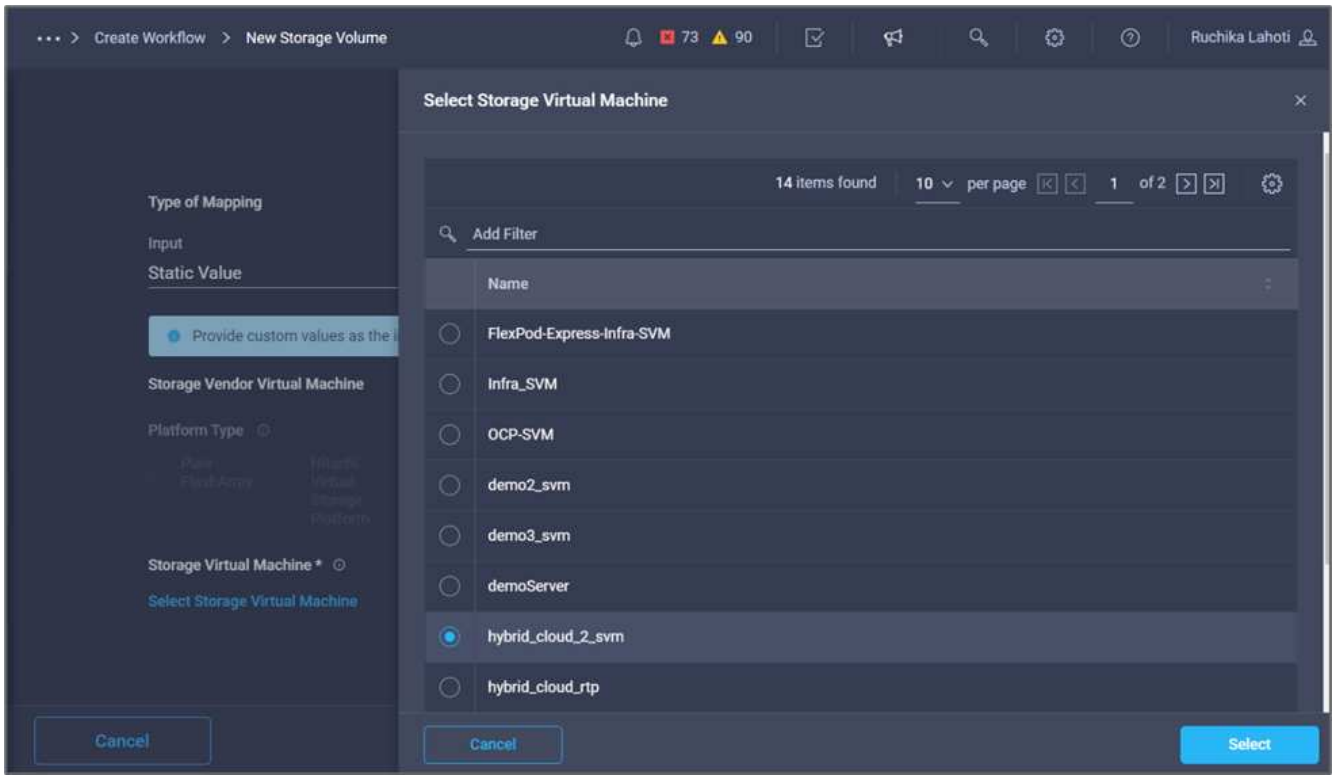
10. Fare clic su **Map** nel campo **Storage Vendor Virtual Machine**.



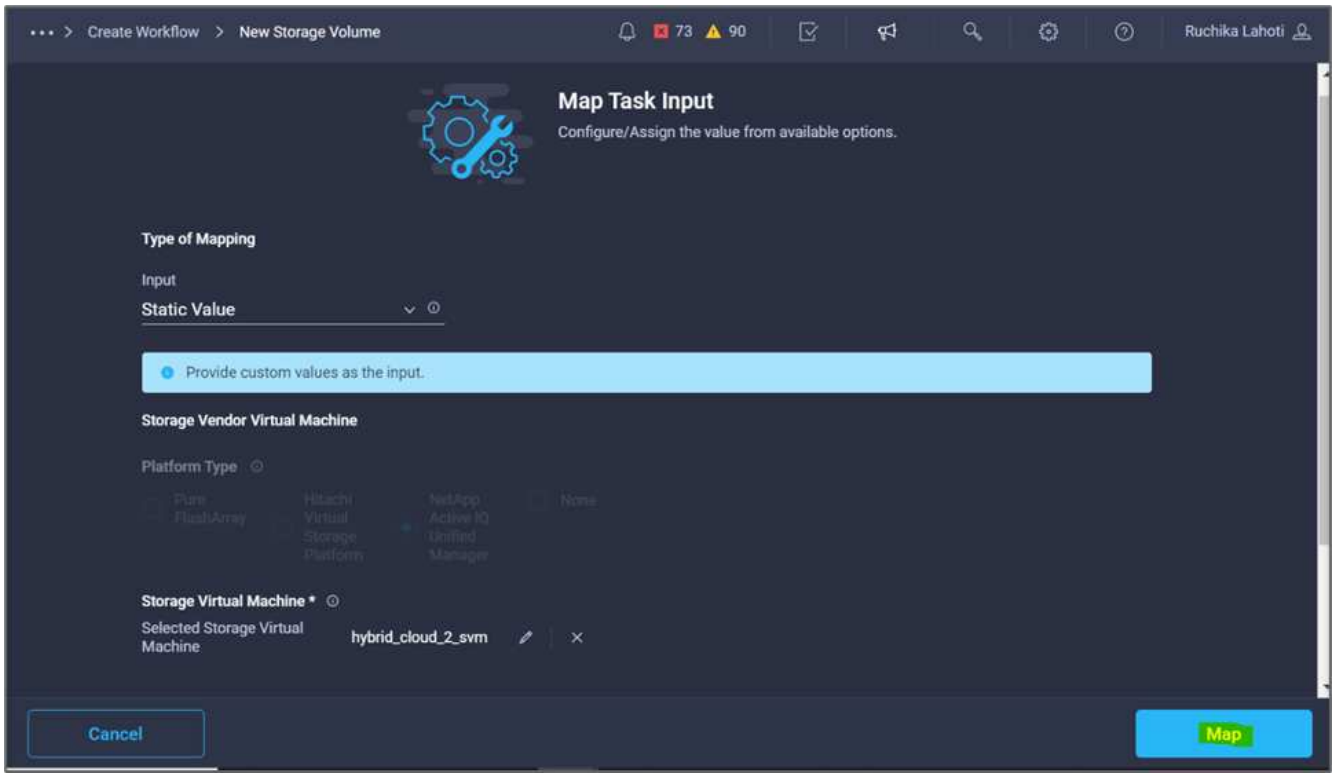
11. Scegliere **valore statico** e fare clic su **Seleziona Storage Virtual Machine**.



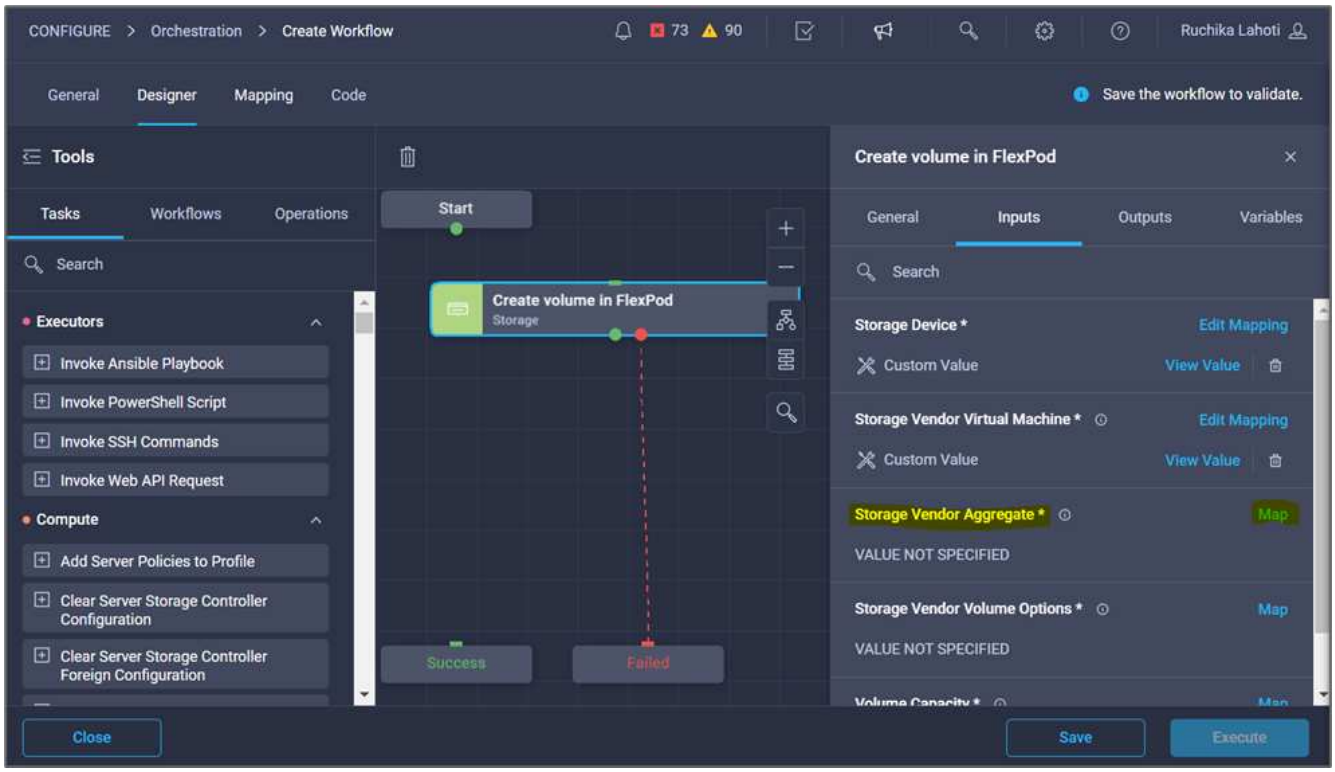
12. Selezionare la macchina virtuale di storage in cui creare il volume e fare clic su **Select** (Seleziona).



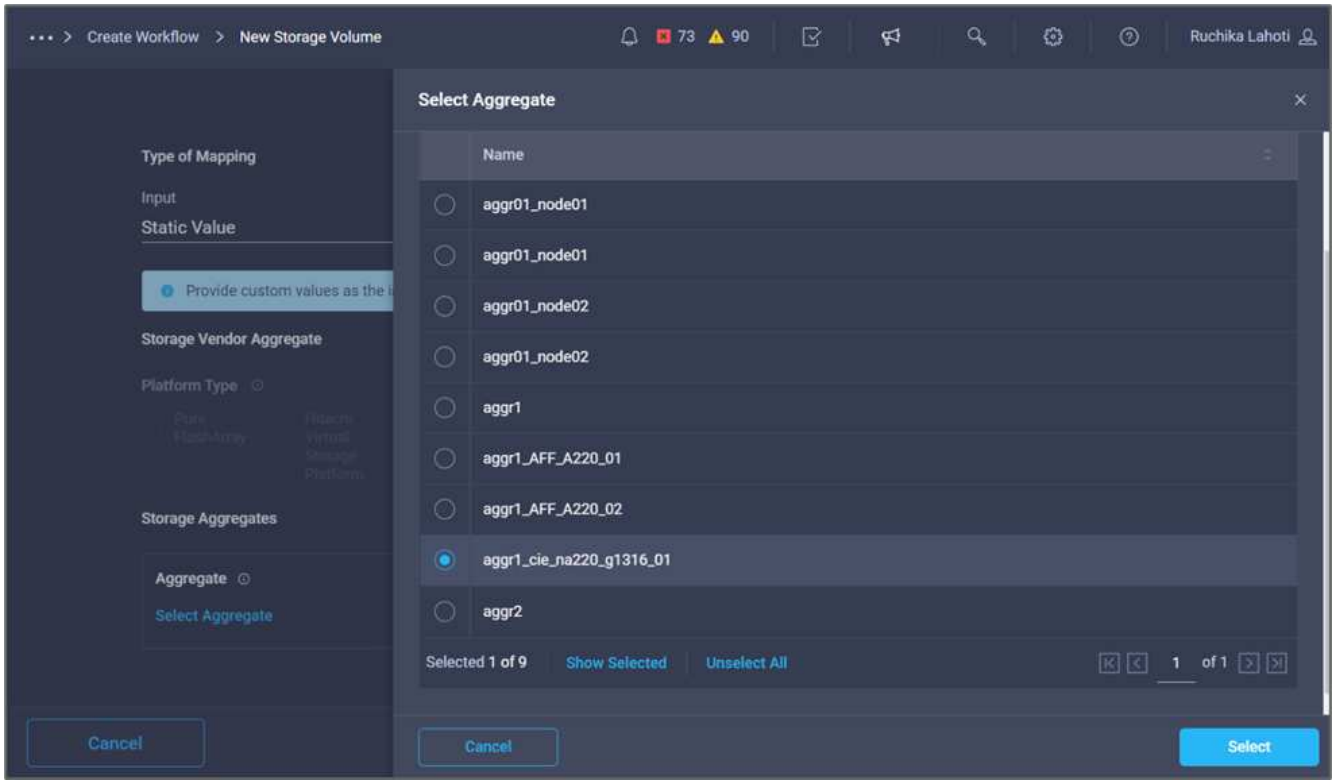
13. Fare clic su **Map** (Mappa).



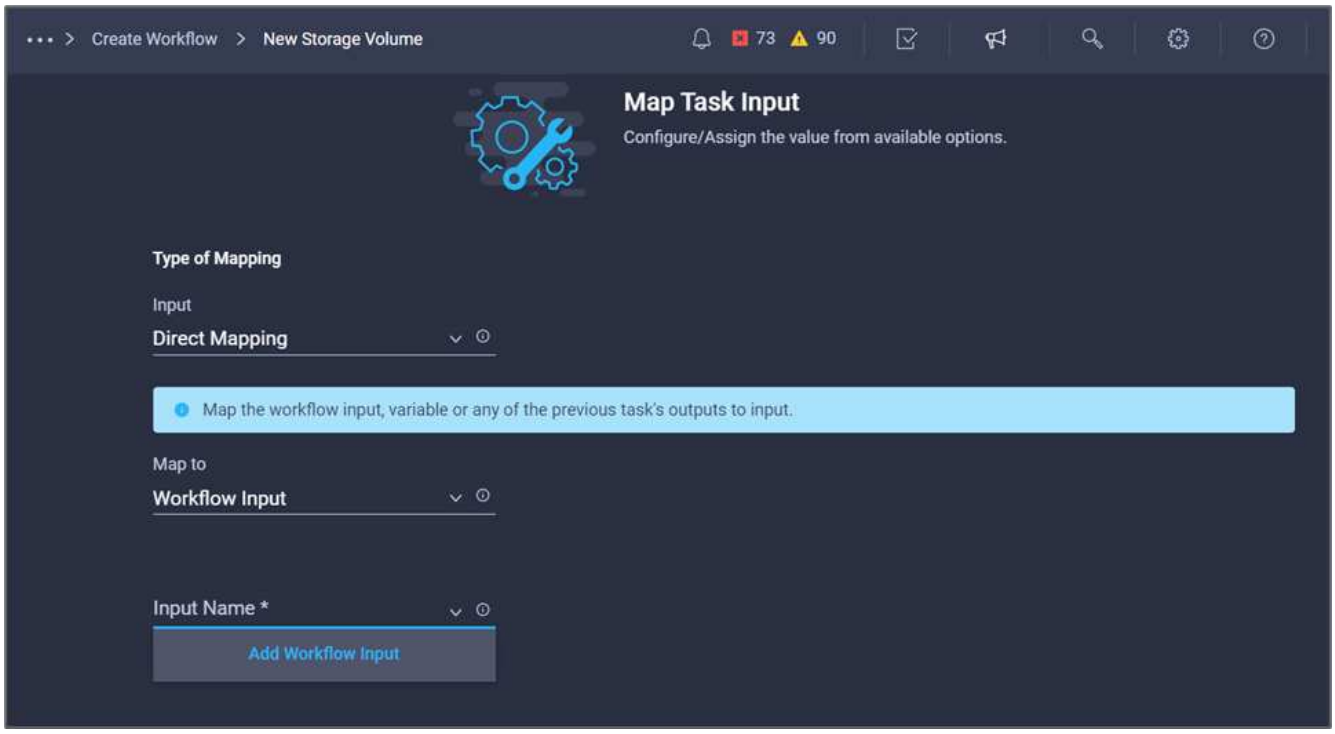
14. Fare clic su **Map** nel campo **Storage Vendor aggregate**.



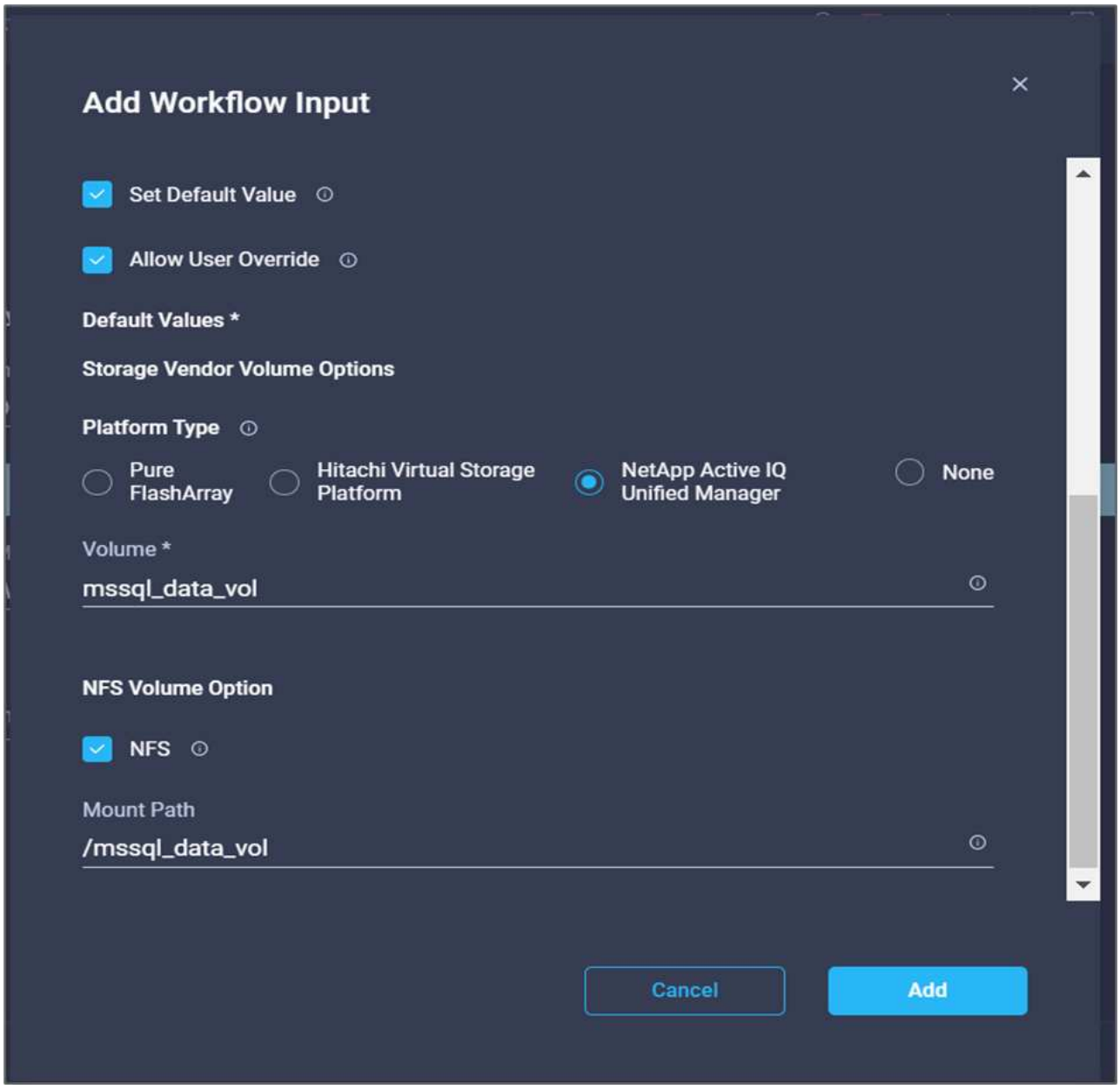
15. Scegliere **valore statico** e fare clic su **Seleziona aggregato di storage**. Scegliere l'aggregato e fare clic su **Select** (Seleziona).



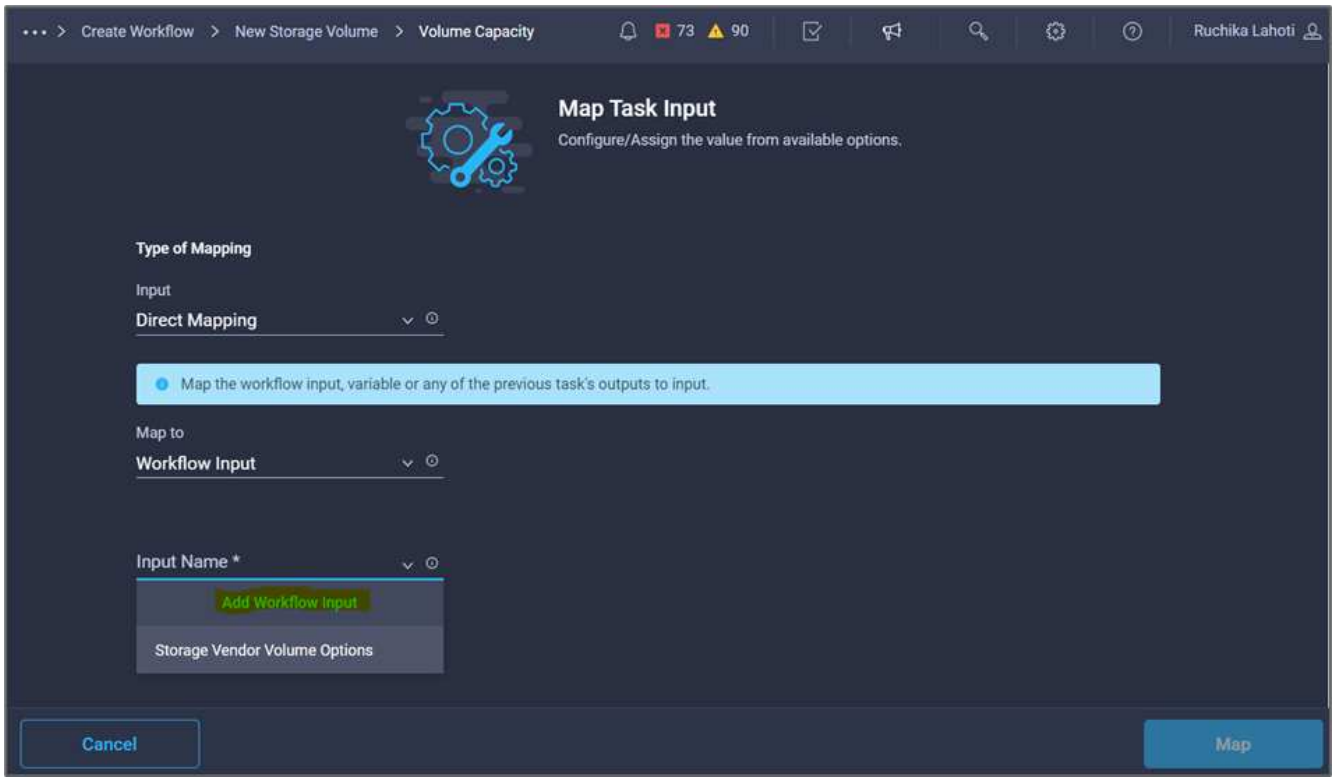
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Storage Vendor Volume Options**.
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.



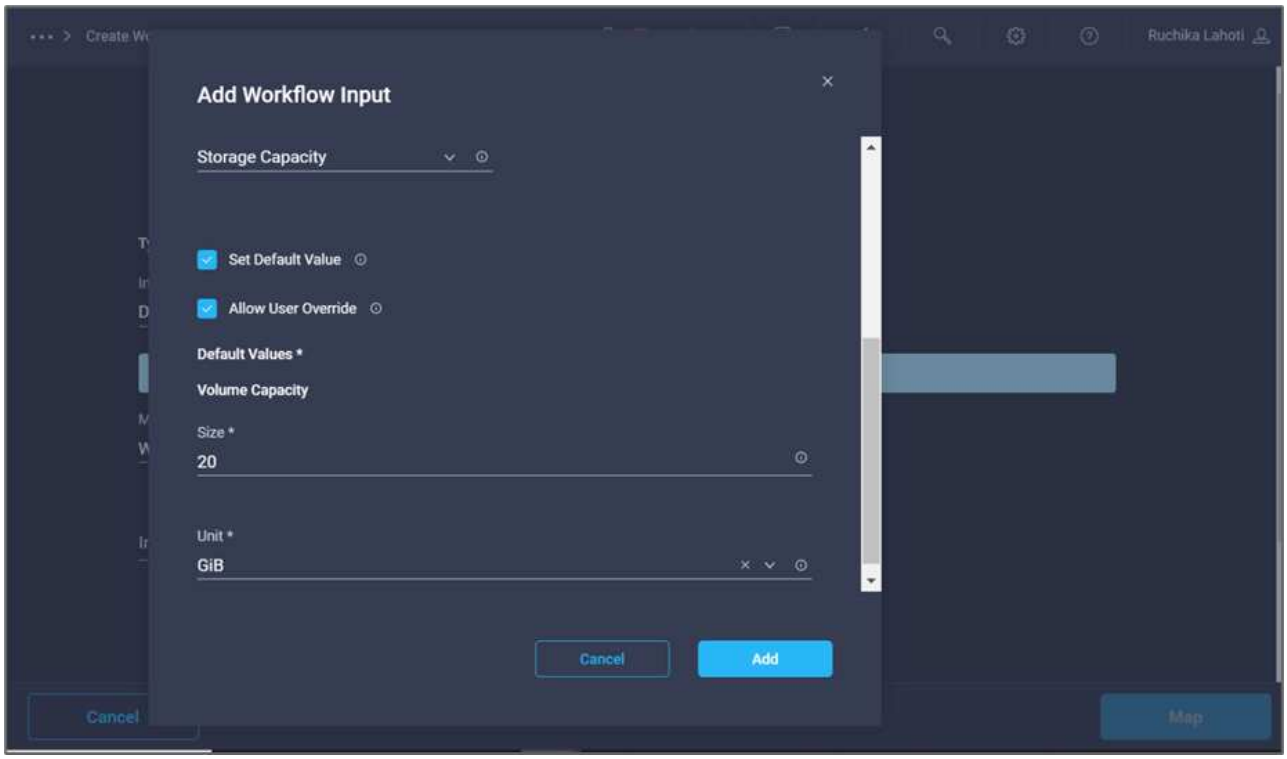
19. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi che l'opzione **Storage Vendor Volume Options** sia selezionata per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fare clic su **obbligatorio**.
    e. Impostare **tipo di piattaforma** su **NetApp Active IQ Unified Manager**.
    f. Fornire un valore predefinito per il volume creato in **Volume**.
    g. Fare clic su **NFS**. Se NFS è impostato, viene creato un volume NFS. Se questo valore è impostato su false, viene creato un volume SAN.
    h. Fornire un percorso di montaggio e fare clic su **Aggiungi**.



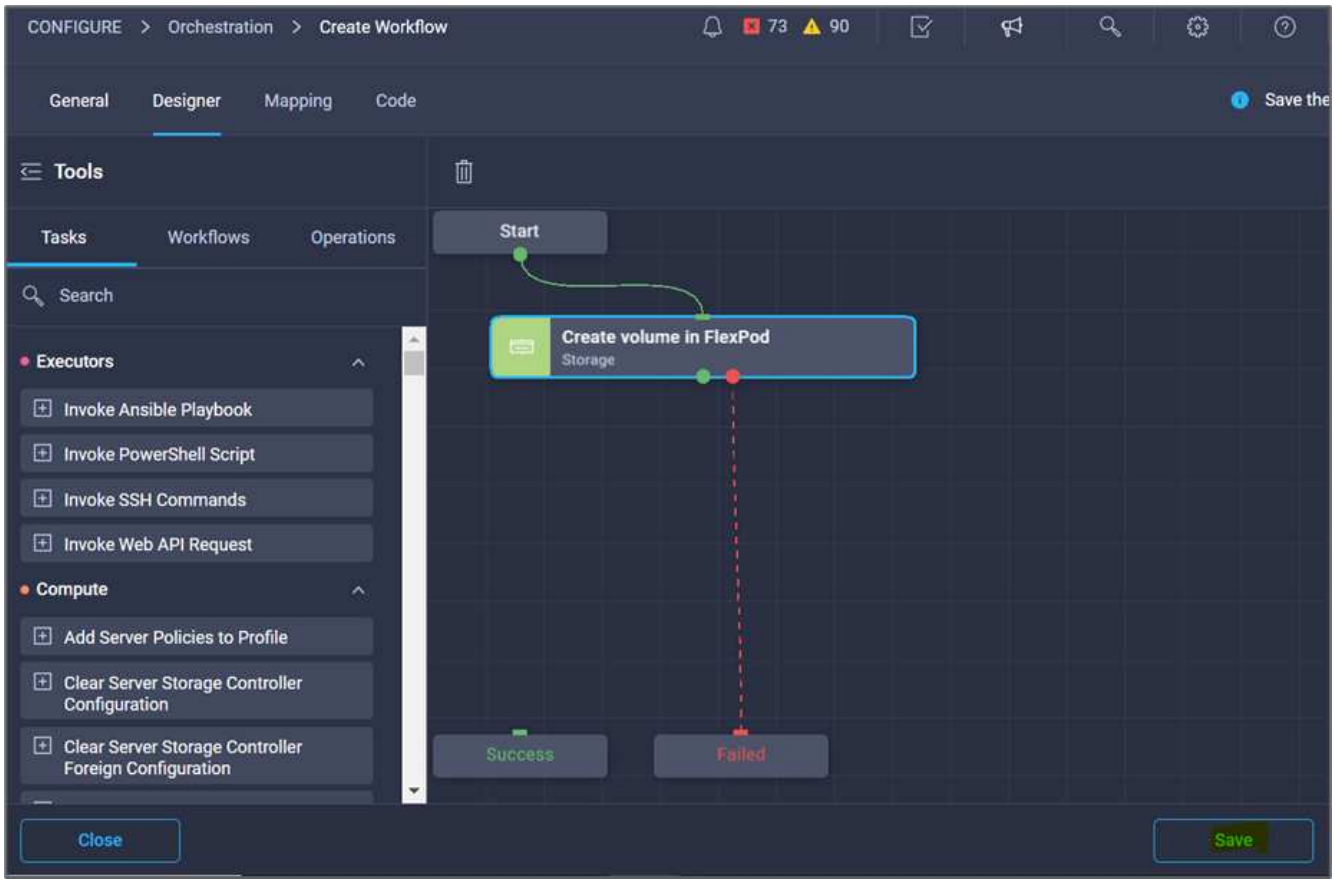
20. Fare clic su **Map** (Mappa).
21. Fare clic su **MAP** nel campo **Volume Capacity**.
22. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
23. Fare clic su **Input Name** e **Create Workflow Input**.



24. Nella procedura guidata Aggiungi input:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Per **Type**, selezionare **Storage Capacity**.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Fornire un valore predefinito per le dimensioni del volume e l'unità.
    f. Fare clic su **Aggiungi**.



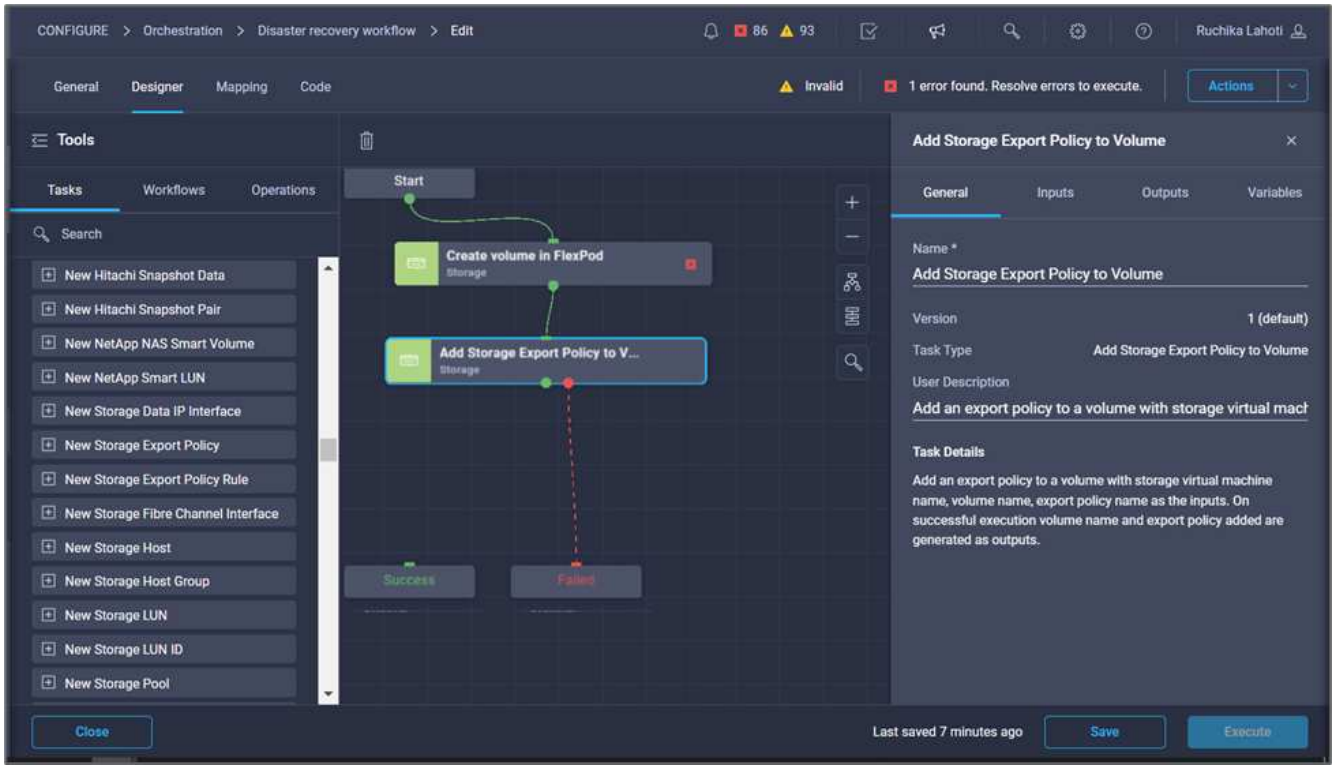
25. Fare clic su **Map** (Mappa).
26. Con Connector, creare una connessione tra le attività **Avvio** e **Crea volume in FlexPod**, quindi fare clic su **Salva**.



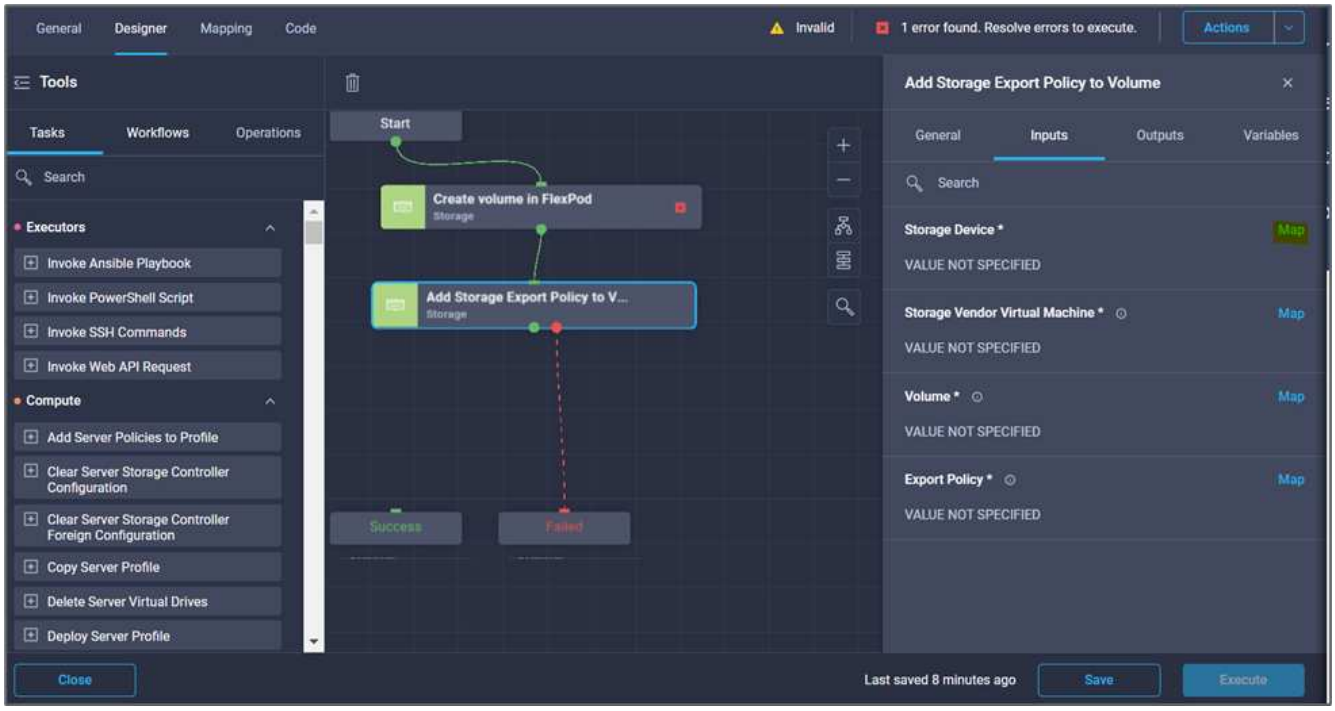
Ignorare l'errore per ora. Questo errore viene visualizzato perché non è presente alcuna connessione tra le attività **Crea volume in FlexPod** e **operazione riuscita**, necessaria per specificare la transizione corretta.

Procedura 3: Aggiunta della policy di esportazione dello storage

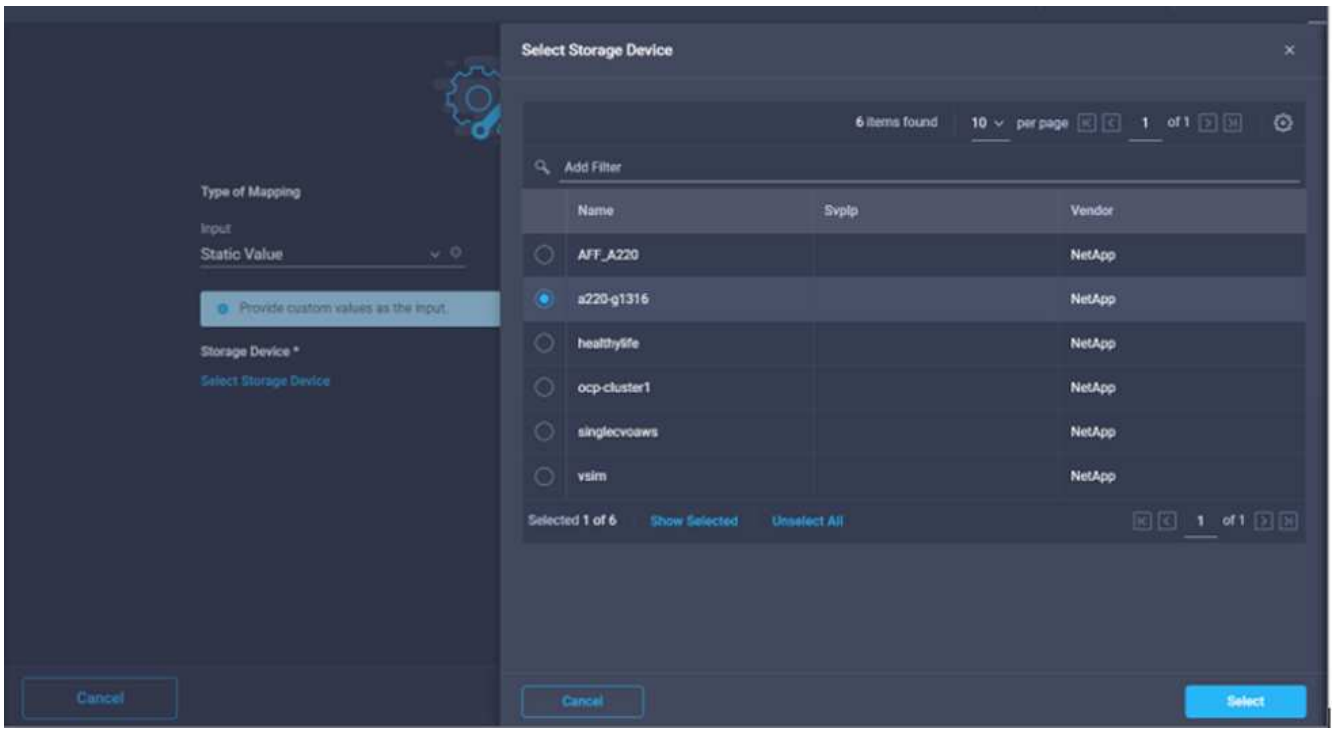
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Storage > Add Storage Export Policy to Volume** (archiviazione > Aggiungi policy di esportazione dello storage al volume) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Fare clic su **Add Storage Export Policy to Volume** (Aggiungi policy di esportazione storage al volume). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è Add Storage Export Policy (Aggiungi policy di esportazione dello storage).
4. Utilizzare Connector per stabilire una connessione tra le attività **Crea volume in FlexPod** e **Aggiungi policy di esportazione dello storage**. Fare clic su **Save** (Salva).



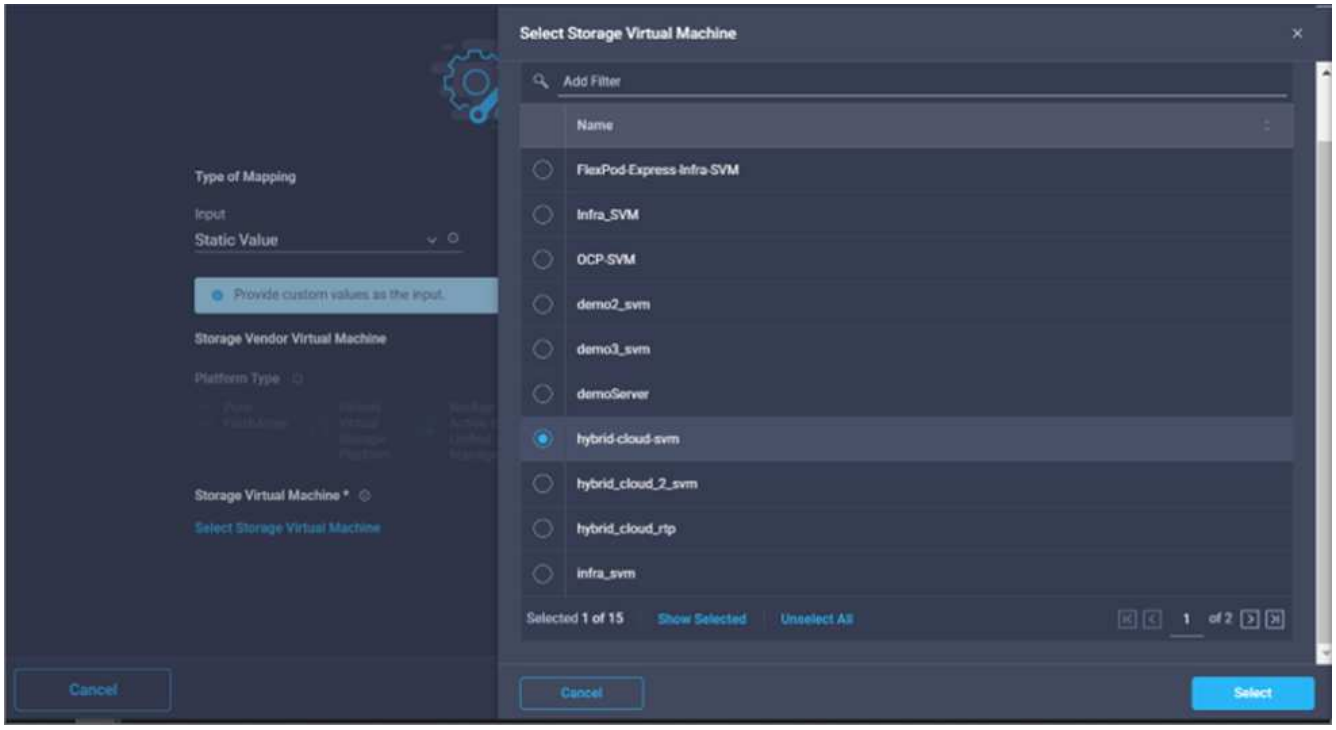
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Storage Device**.



7. Scegliere **valore statico** e fare clic su **Seleziona dispositivo di storage**. Selezionare la stessa destinazione di storage aggiunta durante la creazione dell'attività precedente di creazione di un nuovo volume di storage.
8. Fare clic su **Map** (Mappa).

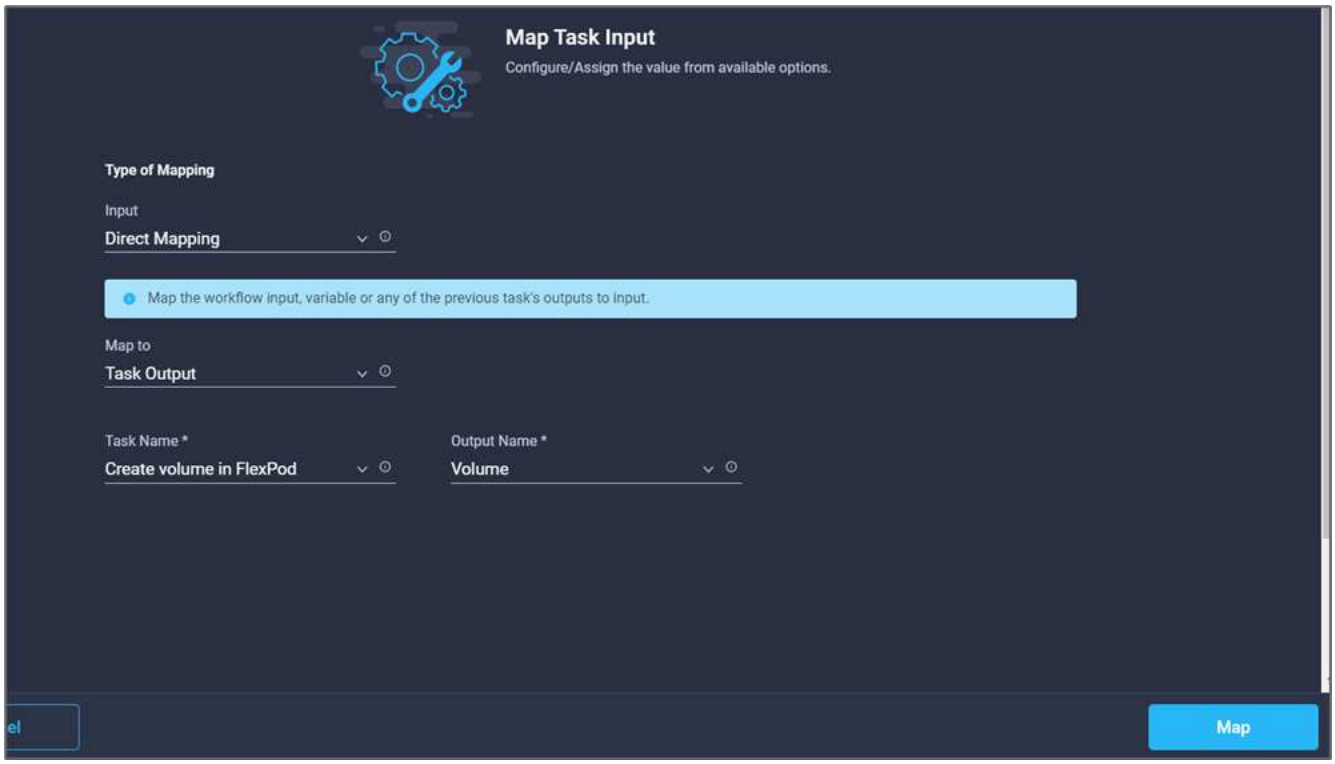


9. Fare clic su **Map** nel campo **Storage Vendor Virtual Machine**.
10. Scegliere **valore statico** e fare clic su **Seleziona Storage Virtual Machine**. Selezionare la stessa macchina virtuale di storage aggiunta durante la creazione dell'attività precedente di creazione di un nuovo volume di storage.

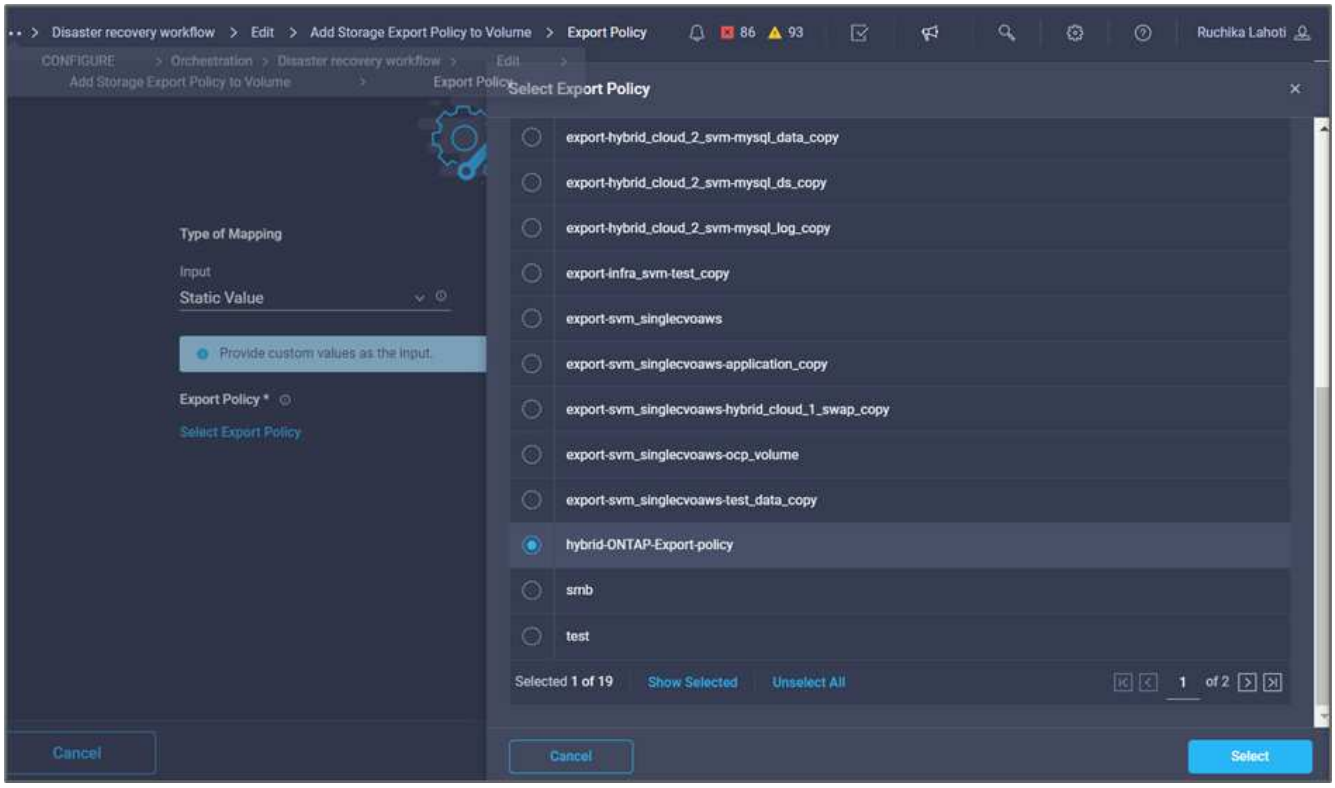


11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Volume**.
13. Fare clic su **Nome attività**, quindi su **Crea volume in FlexPod**. Fare clic su **Output Name** (Nome output), quindi su **Volume**.

> In Cisco Intersight Cloud Orchestrator, è possibile fornire l'output di un'attività precedente come input per una nuova attività. In questo esempio, i dettagli di **Volume** sono stati forniti dall'attività **Crea volume in FlexPod** come input per l'attività **Aggiungi policy di esportazione dello storage**.



14. Fare clic su **Map** (Mappa).
15. Fare clic su **Map** nel campo **Export Policy**.
16. Scegliere **valore statico** e fare clic su **Seleziona policy di esportazione**. Selezionare la policy di esportazione creata.

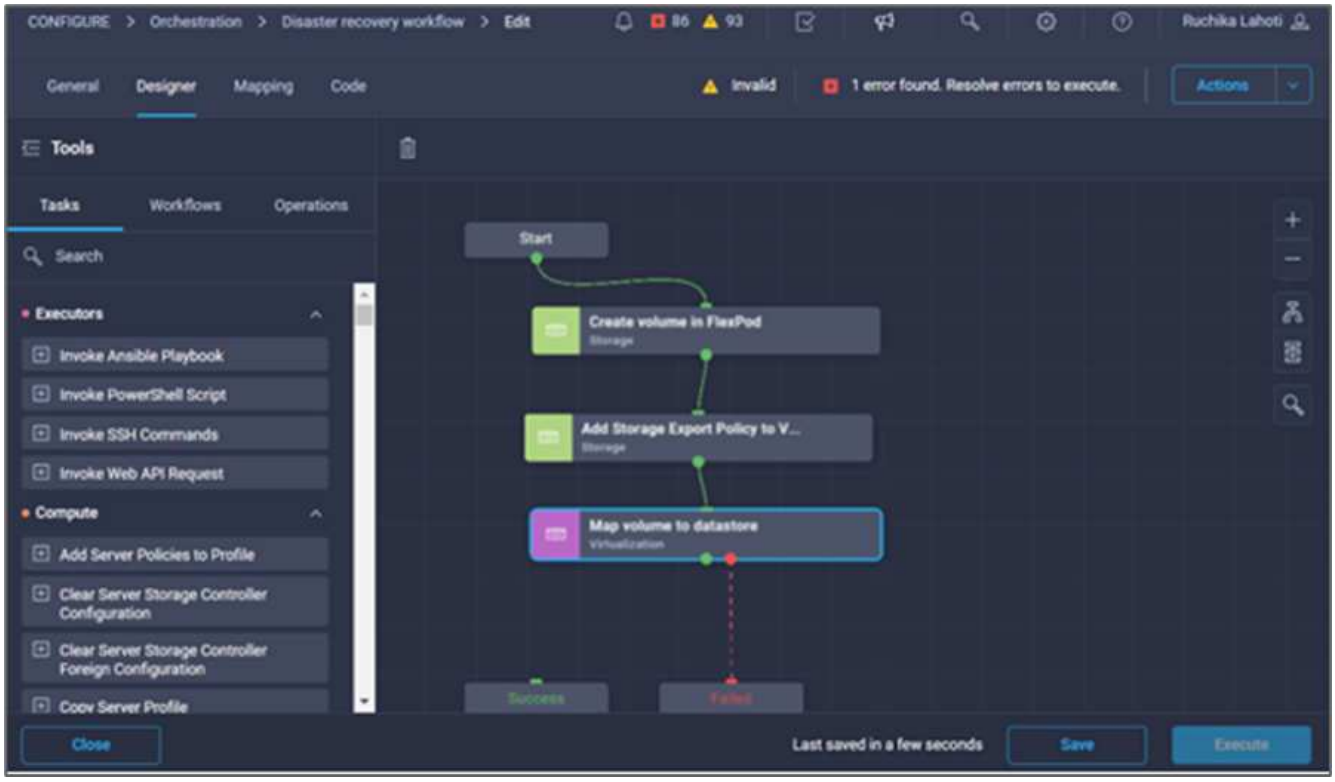


17. Fare clic su **Map** (Mappa), quindi su **Save** (Salva).

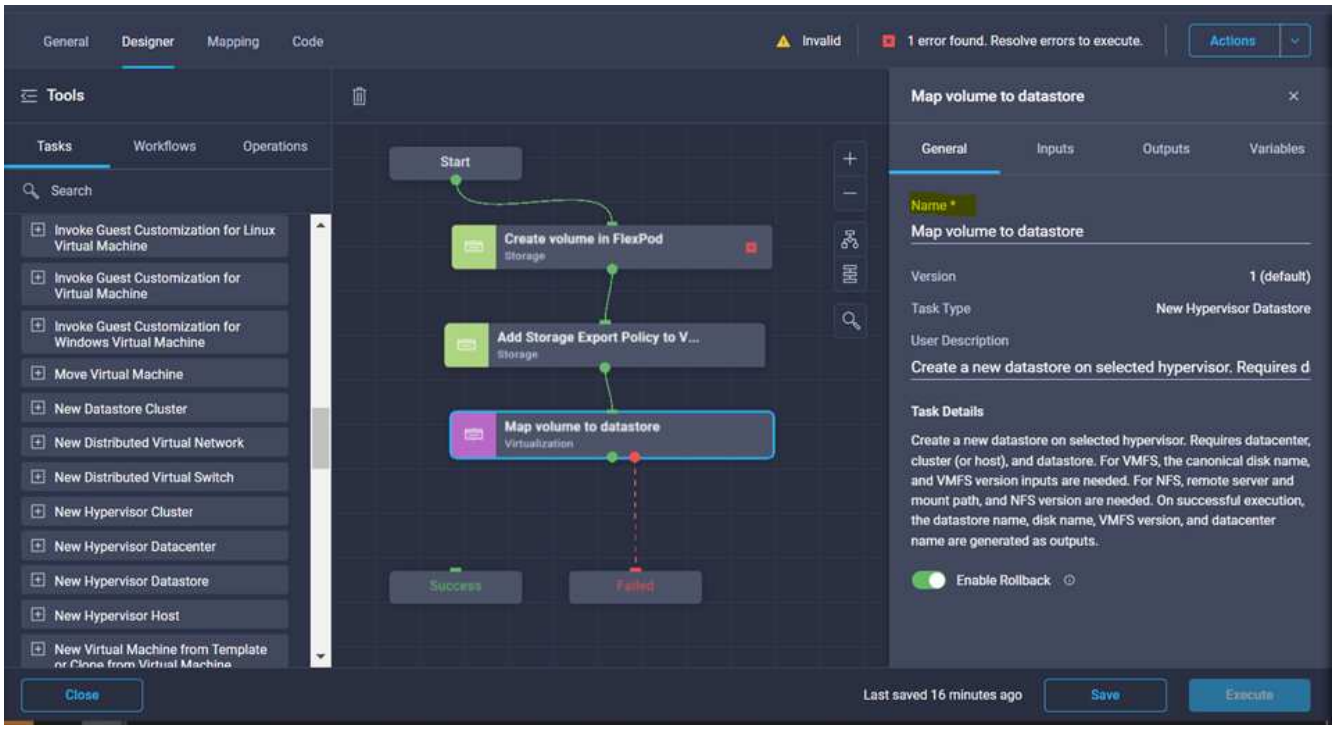
In questo modo, viene completata l'aggiunta di un criterio di esportazione al volume. Quindi, creare un nuovo datastore mappando il volume creato.

Procedura 4: Mappare il volume FlexPod all'archivio dati

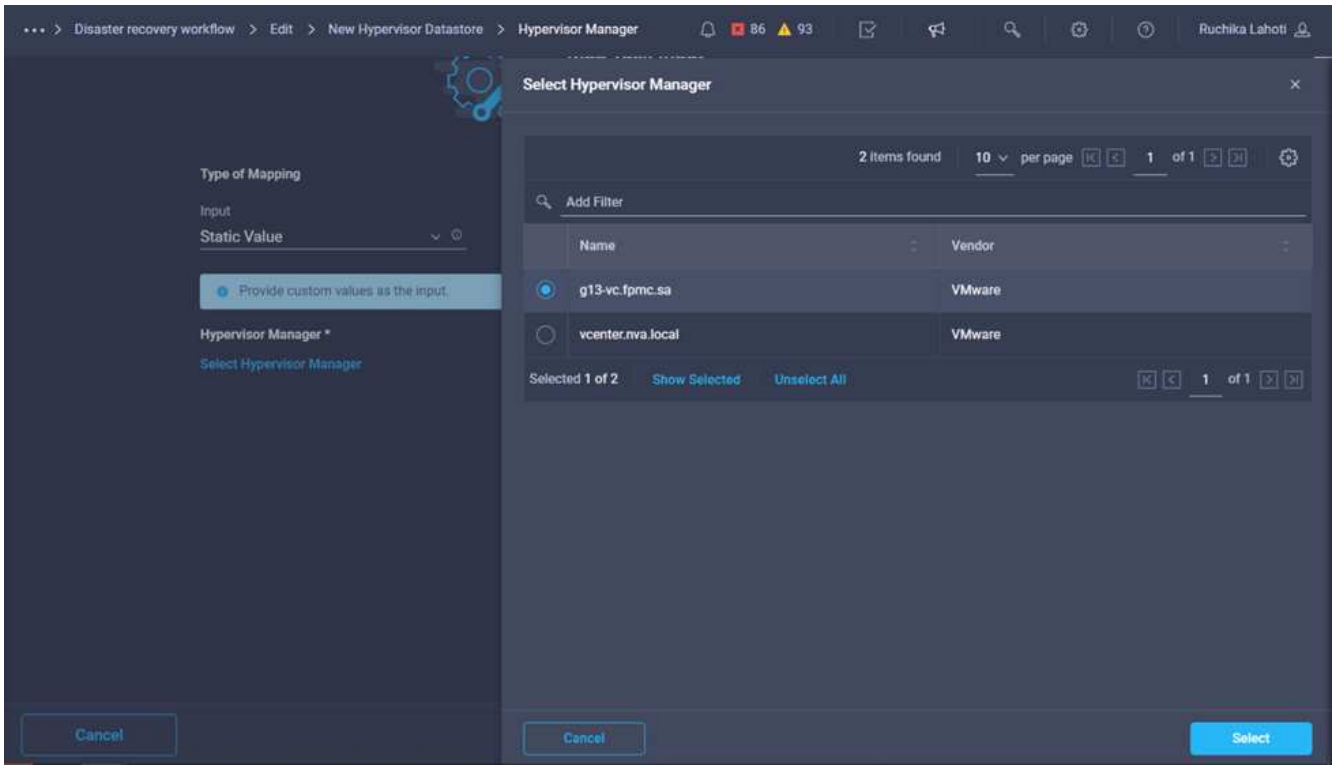
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Virtualization > New Hypervisor Datastore** (virtualizzazione > nuovo archivio dati hypervisor) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per stabilire una connessione tra le attività **Add Storage Export Policy** (Aggiungi policy di esportazione dello storage) e **New Hypervisor Datastore** (nuovo archivio dati hypervisor). Fare clic su **Save** (Salva).



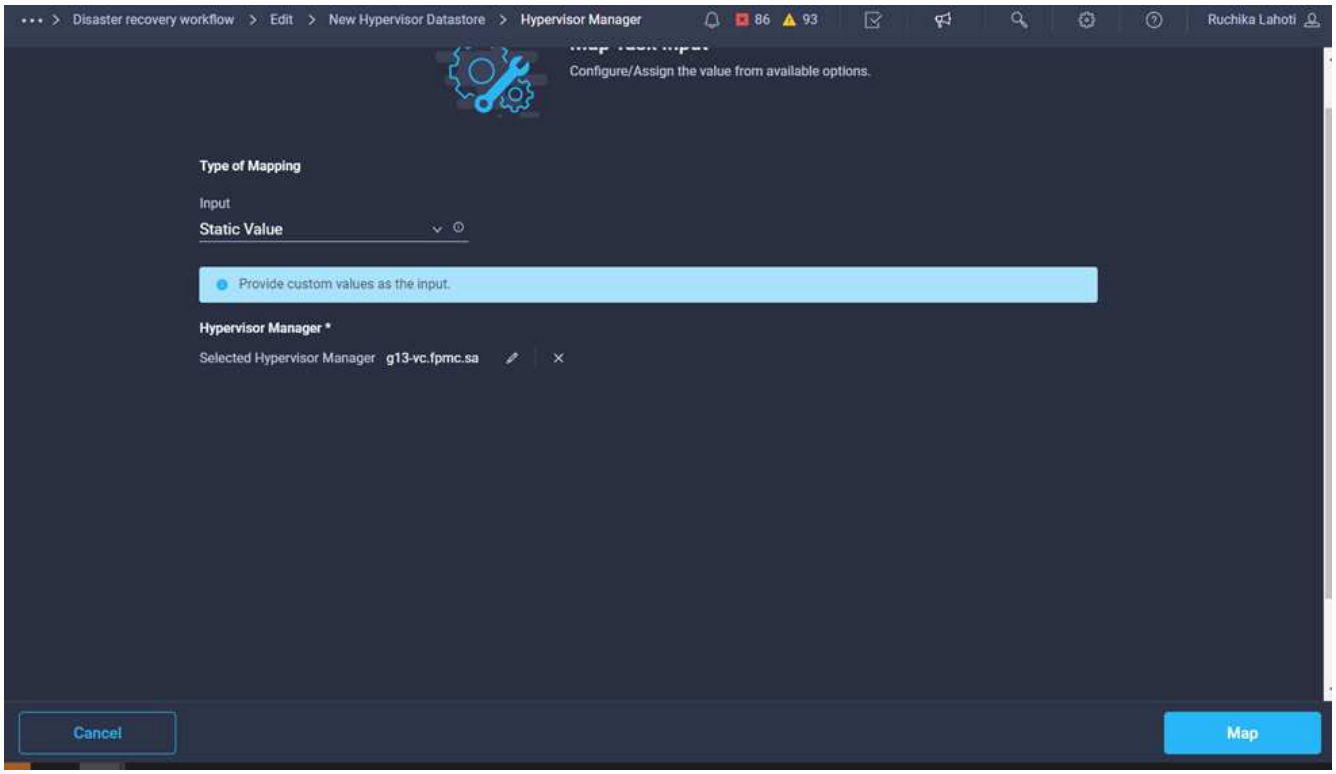
4. Fare clic su **New Hypervisor Datastore** (nuovo archivio dati hypervisor). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Mapp volume to Datastore**.



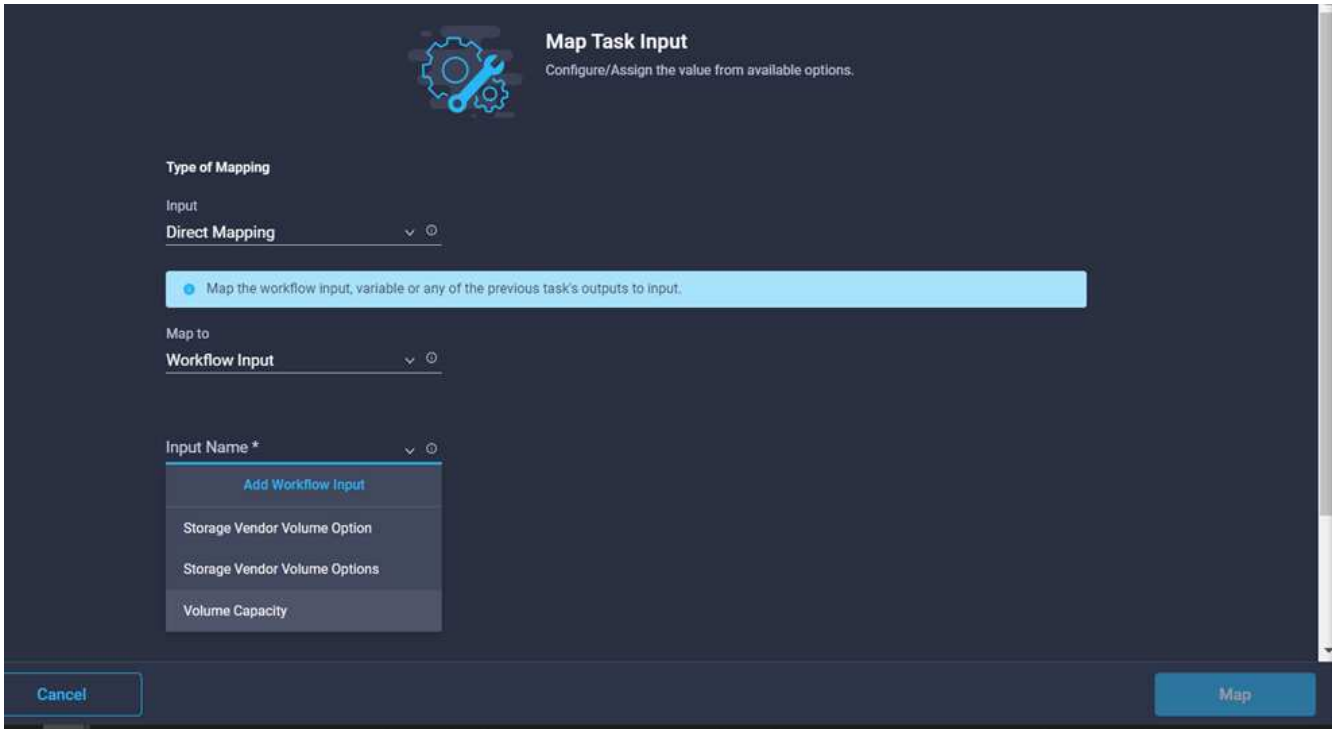
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Hypervisor Manager**.
7. Scegliere **Static Value** (valore statico) e fare clic su **Select Hypervisor Manager** (Seleziona gestore hypervisor). Fare clic sulla destinazione di VMware vCenter.



8. Fare clic su **Map** (Mappa).



9. Fare clic su **Map** nel campo **Data center**. Si tratta del data center associato al nuovo datastore.
10. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
11. Fare clic su **Input Name**, quindi su **Create Workflow Input**.

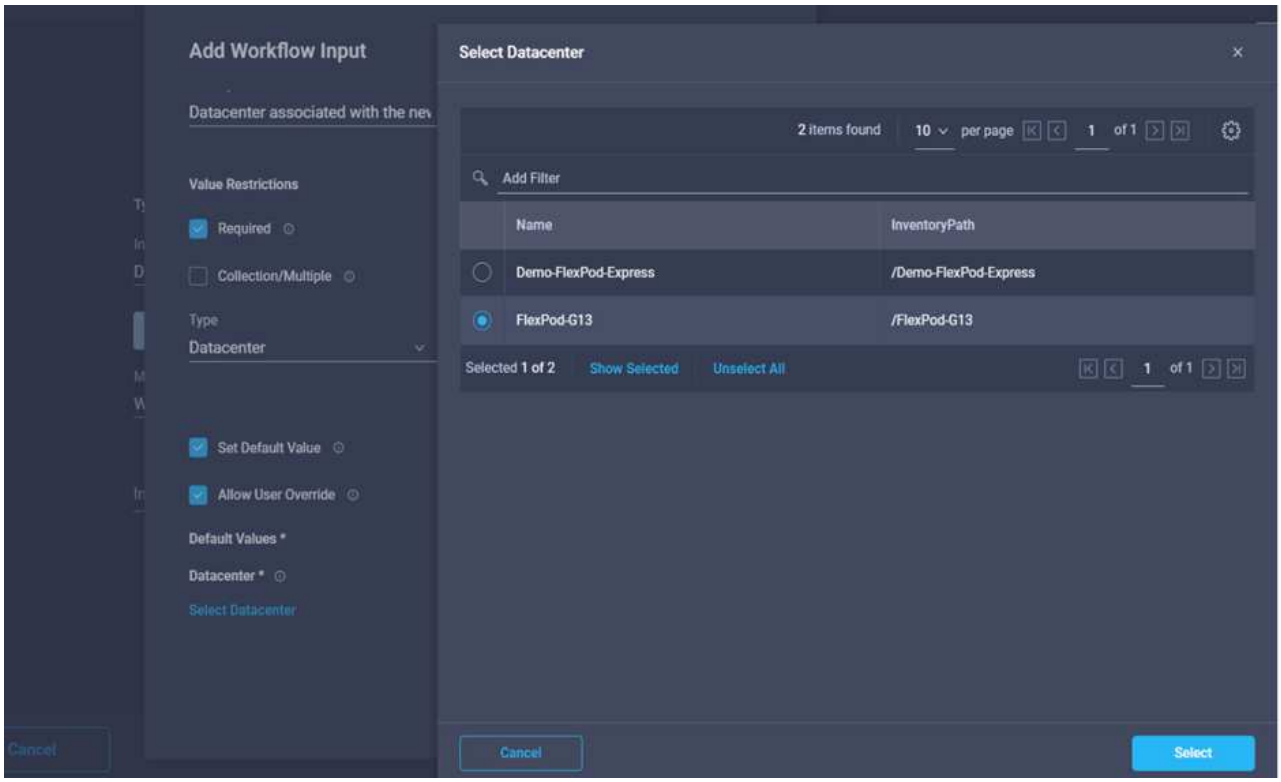


12. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Selezionare **Datacenter** come tipo.

c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).

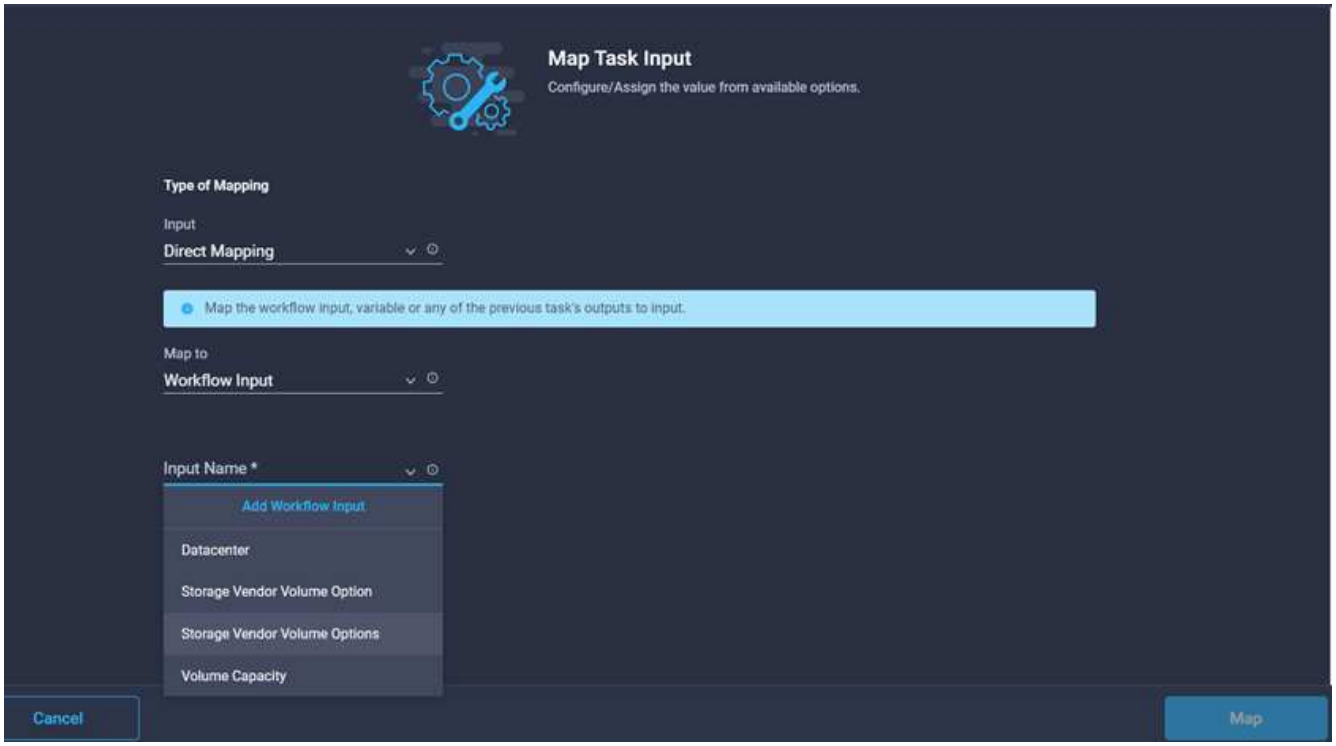
d. Fare clic su **Seleziona data center**.

e. Fare clic sul data center associato al nuovo datastore, quindi fare clic su **Select** (Seleziona).

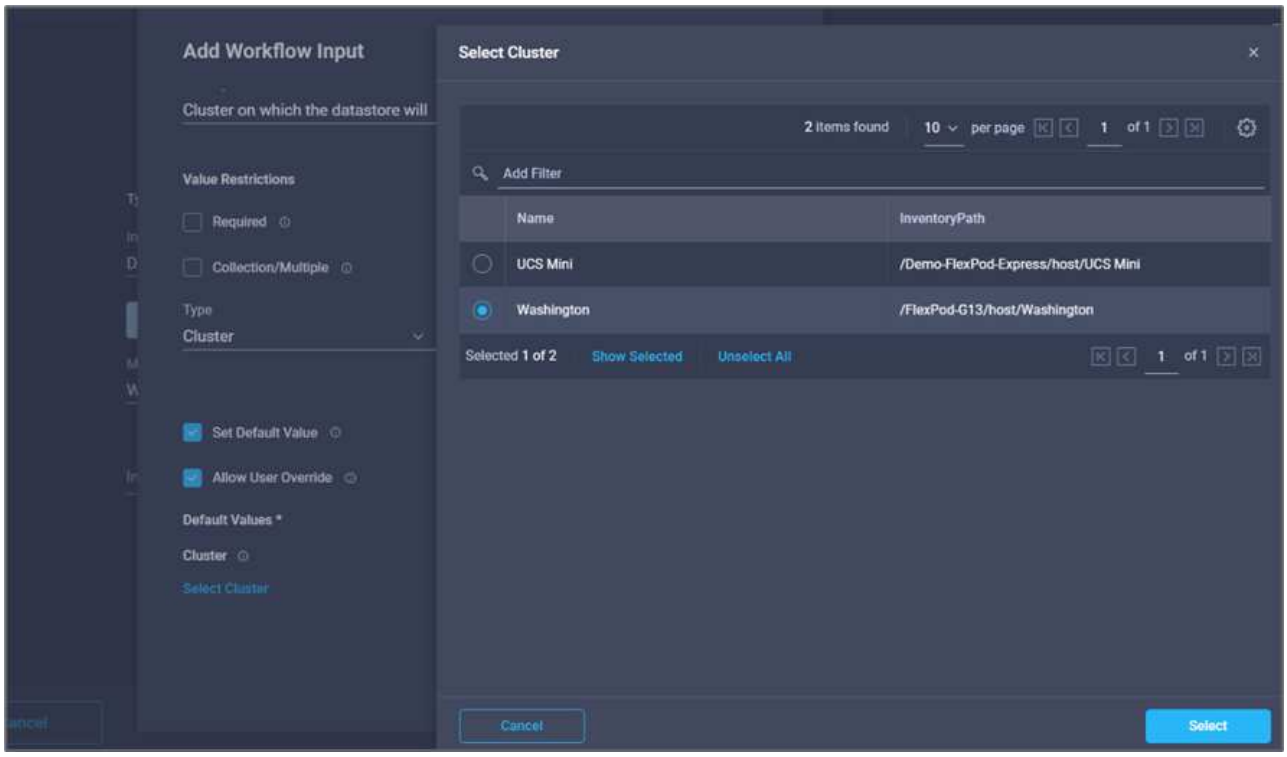


- Fare clic su **Aggiungi**.

13. Fare clic su **Map** (Mappa).
14. Fare clic su **Map** nel campo **Cluster**.
15. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.

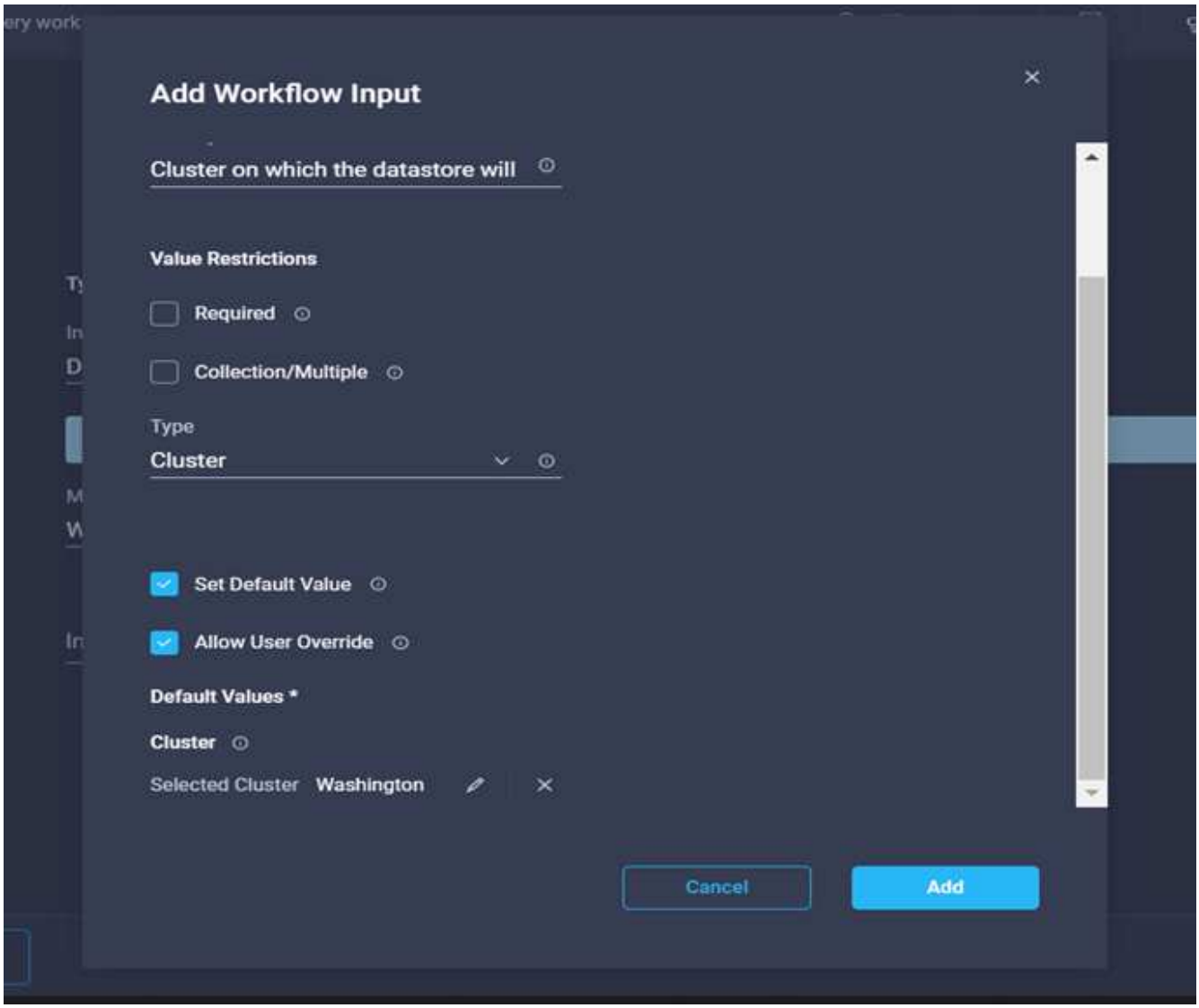


16. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Selezionare Cluster come tipo.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Fare clic su **Select Cluster** (Seleziona cluster).
    f. Fare clic sul cluster associato al nuovo datastore.
    g. Fare clic su **Seleziona**.

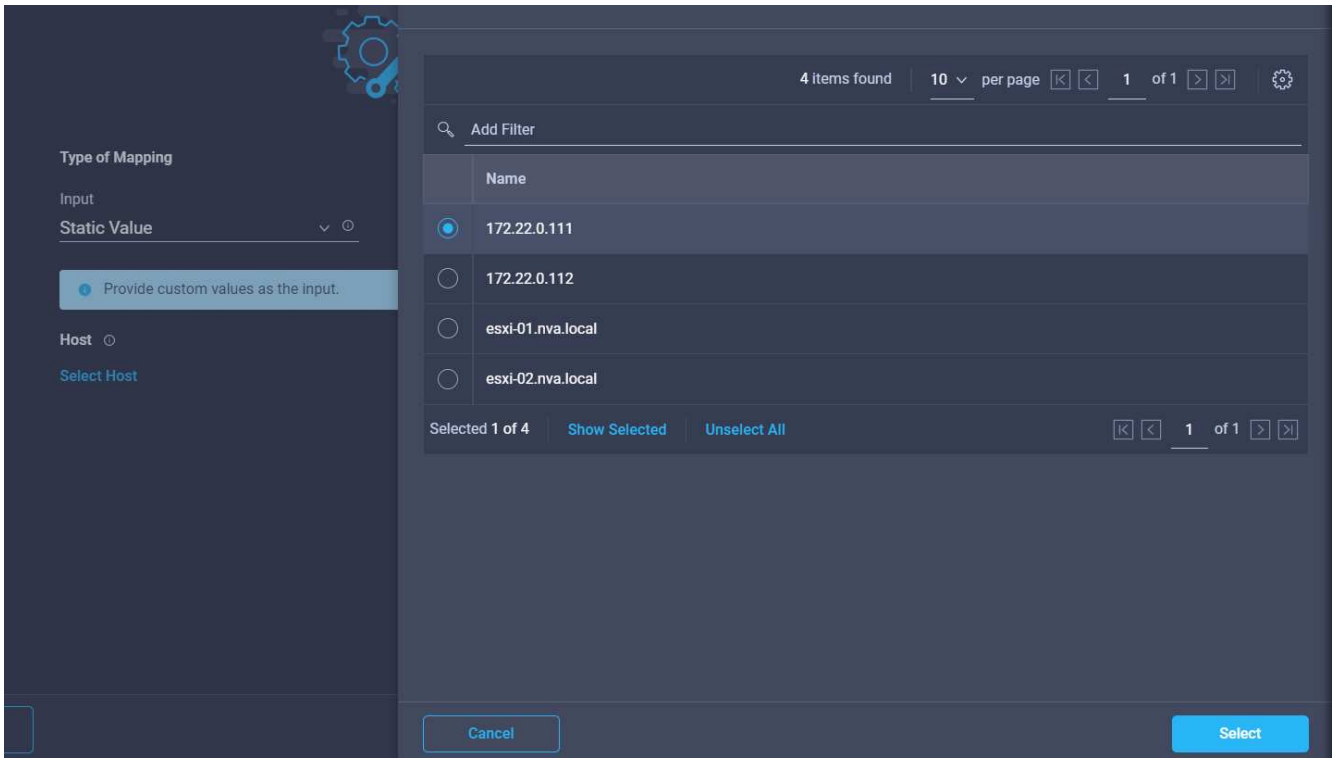


h. Fare clic su **Aggiungi**.

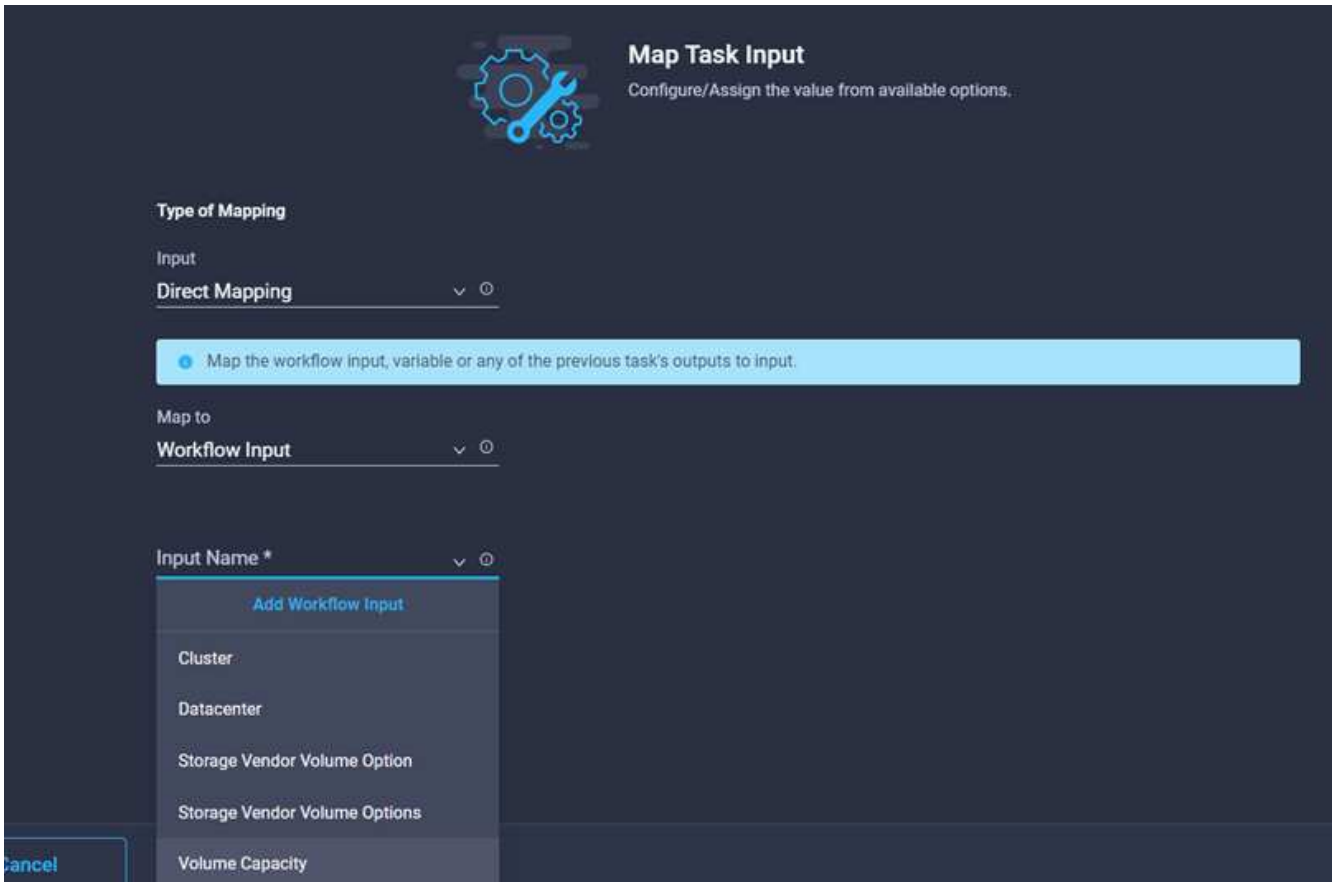
17. Fare clic su **Map** (Mappa).
18. Fare clic su **Map** nel campo **host**.



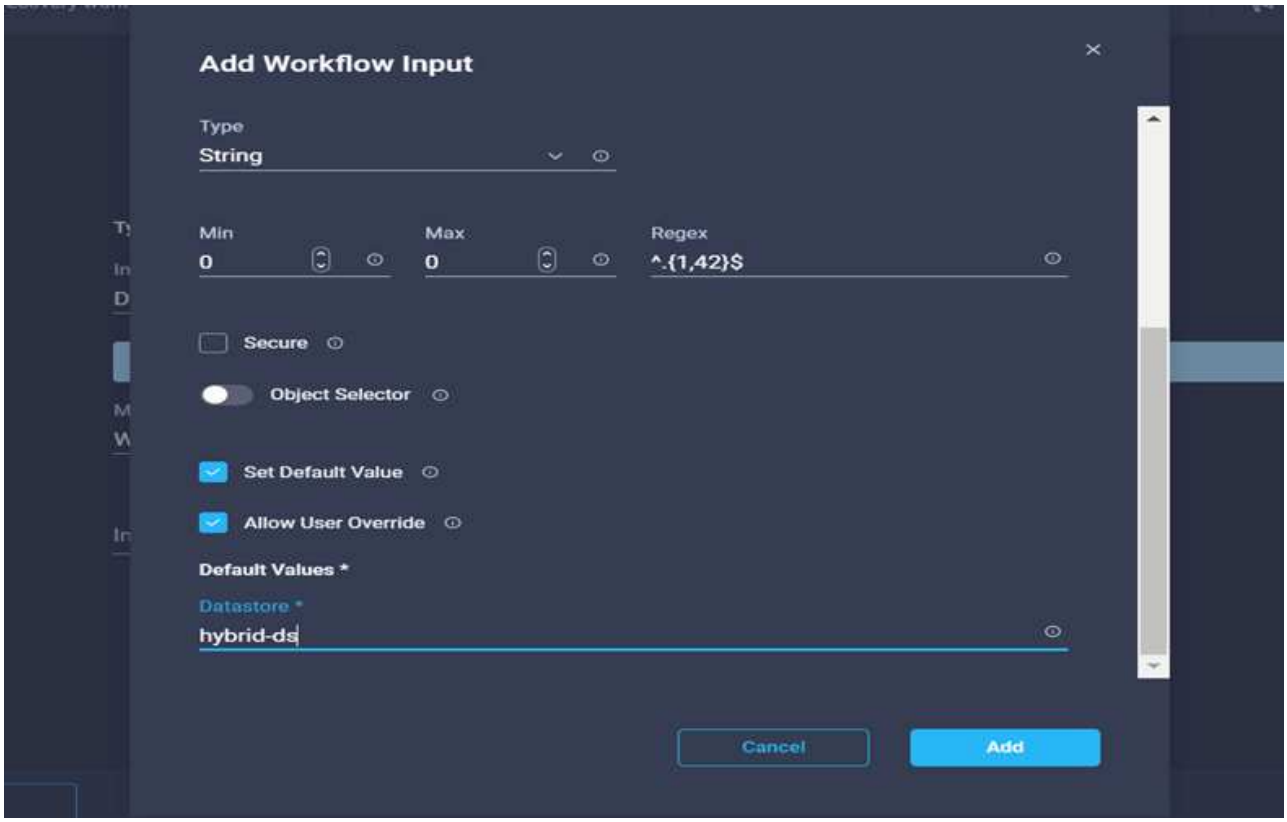
19. Scegliere **Static Value** (valore statico) e fare clic sull'host su cui verrà ospitato il datastore. Se viene specificato un cluster, l'host viene ignorato.



20. Fare clic su **Select and Map** (Seleziona e mappa).
21. Fare clic su **Map** nel campo **Datastore**.
22. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
23. Fare clic su **Input Name** e **Create Workflow Input**.

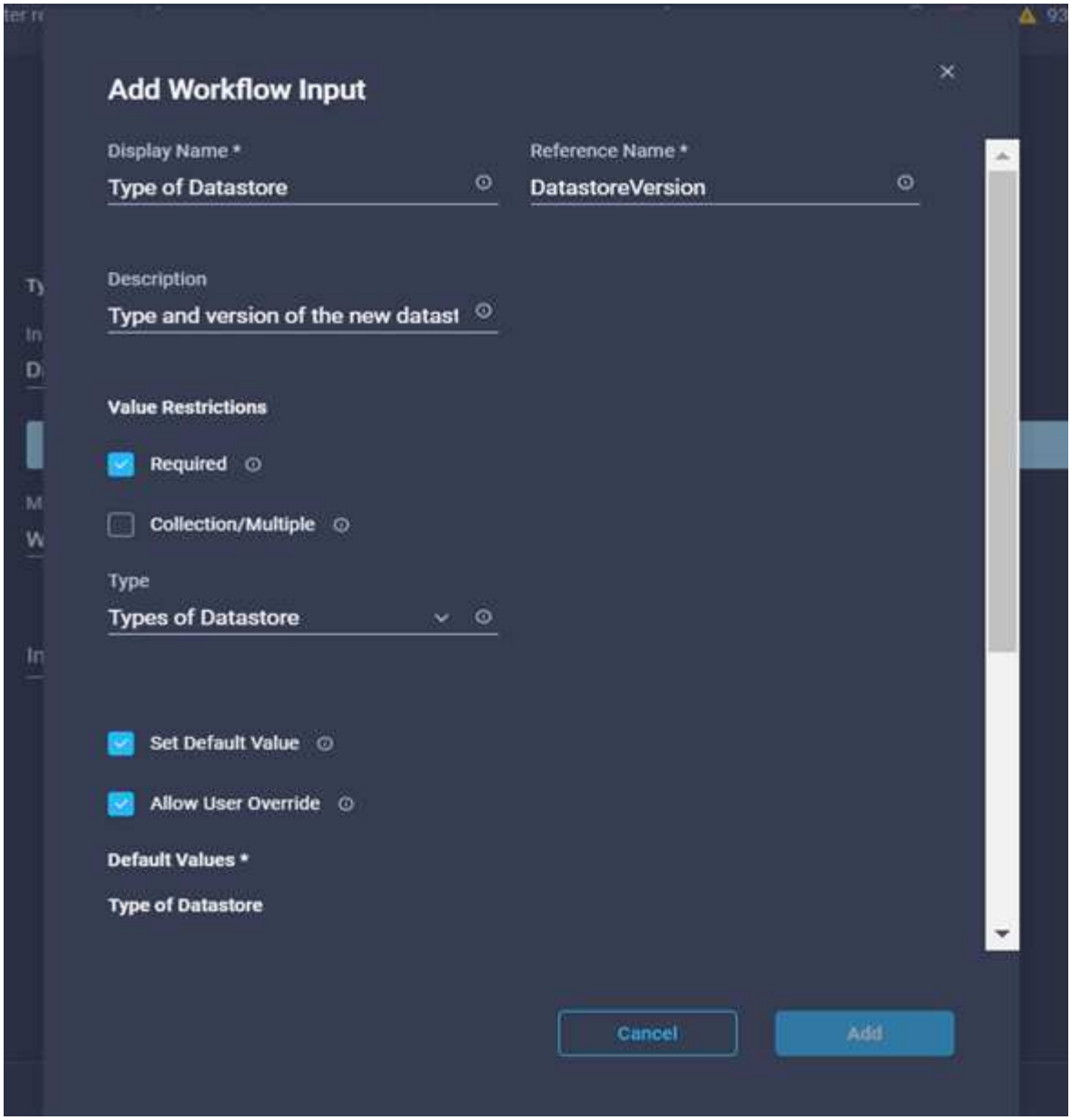


24. Nella procedura guidata Aggiungi input:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fornire un valore predefinito per l'archivio dati e fare clic su **Add** (Aggiungi).



25. Fare clic su **Map** (Mappa).
26. Fare clic su **Map** nel campo di immissione **Type of Datastore**.
27. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
28. Fare clic su **Input Name** e **Create Workflow Input**.

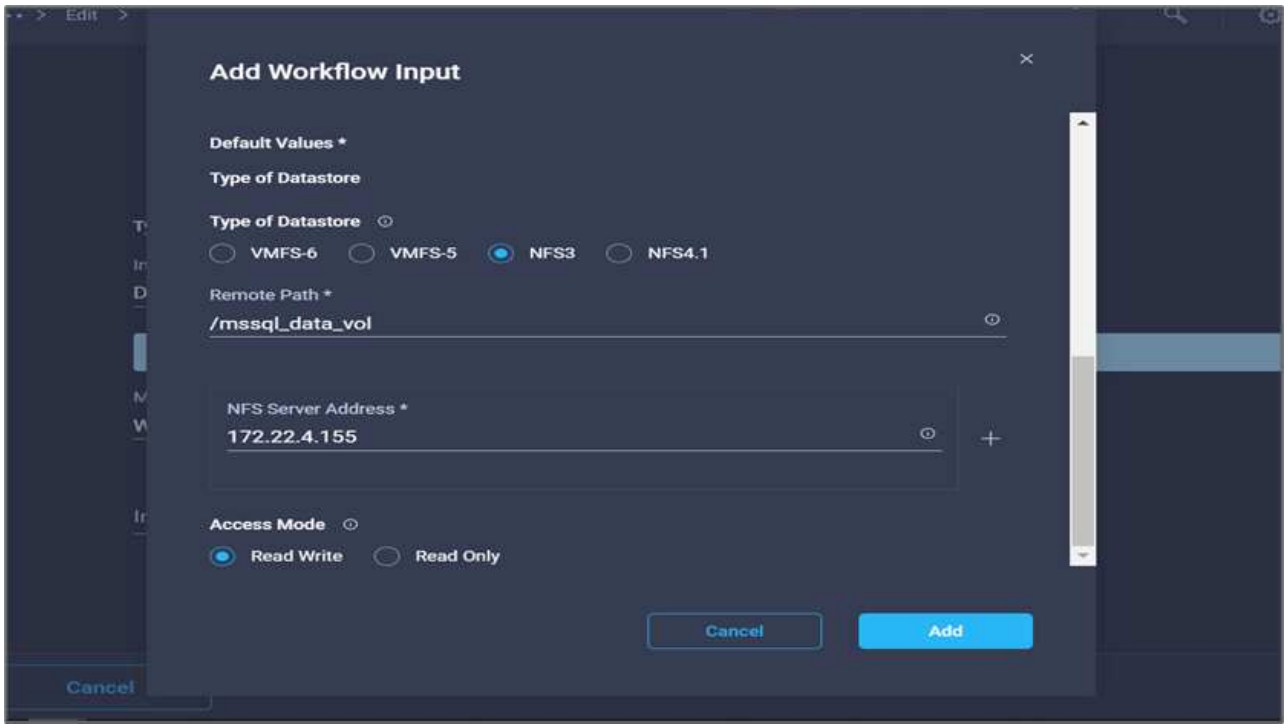
29. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo) e fare clic su **obbligatorio**.
    b. Assicurarsi di selezionare il tipo **tipi di datastore** e fare clic su **Imposta valore predefinito e Ignora**.



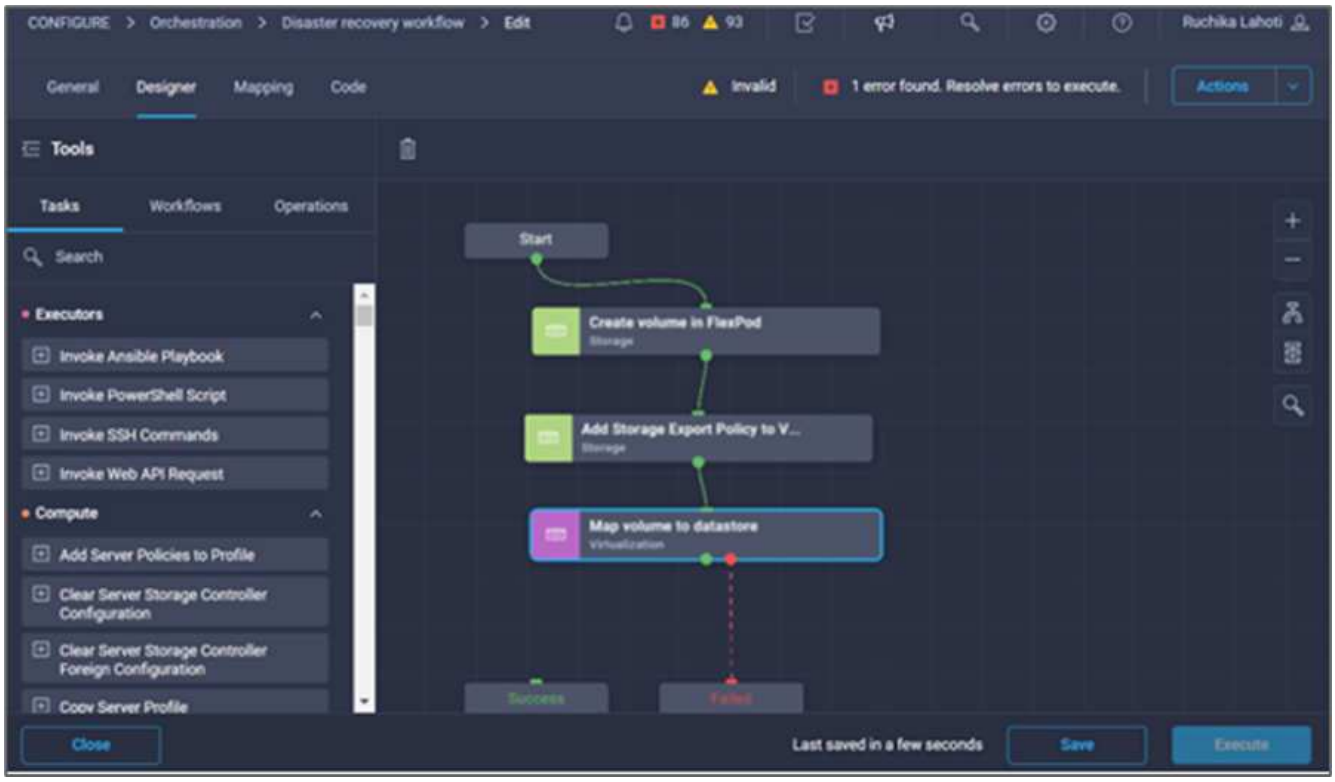
c. Fornire il percorso remoto. Questo è il percorso remoto del punto di montaggio NFS.

d. Fornire i nomi host o gli indirizzi IP del server NFS remoto in NFS Server Address (Indirizzo server NFS).

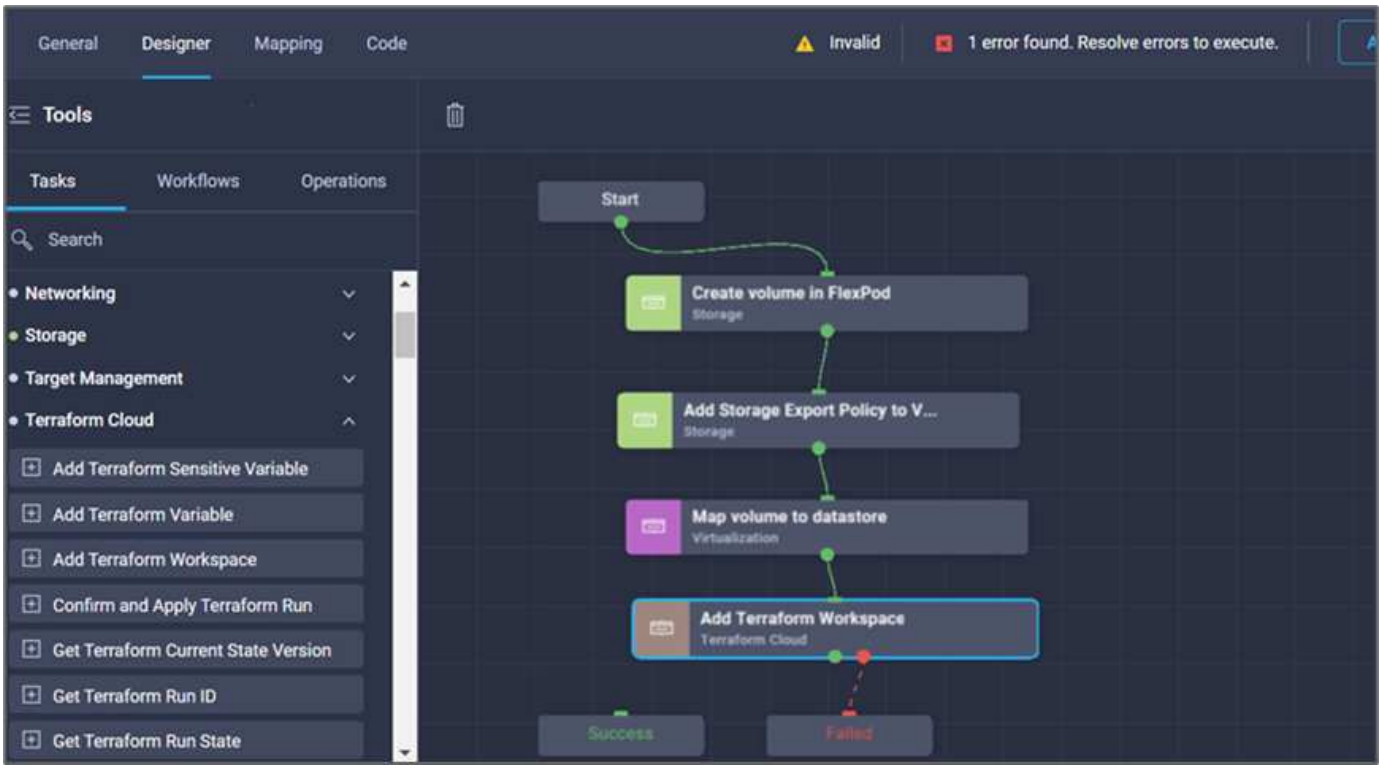
e. Fare clic su **Access Mode** (modalità di accesso). La modalità Access è per il server NFS. Fare clic su Read-only (sola lettura) se i volumi vengono esportati in sola lettura. Fare clic su **Aggiungi**.



30. Fare clic su **Map** (Mappa).
31. Fare clic su **Save** (Salva).

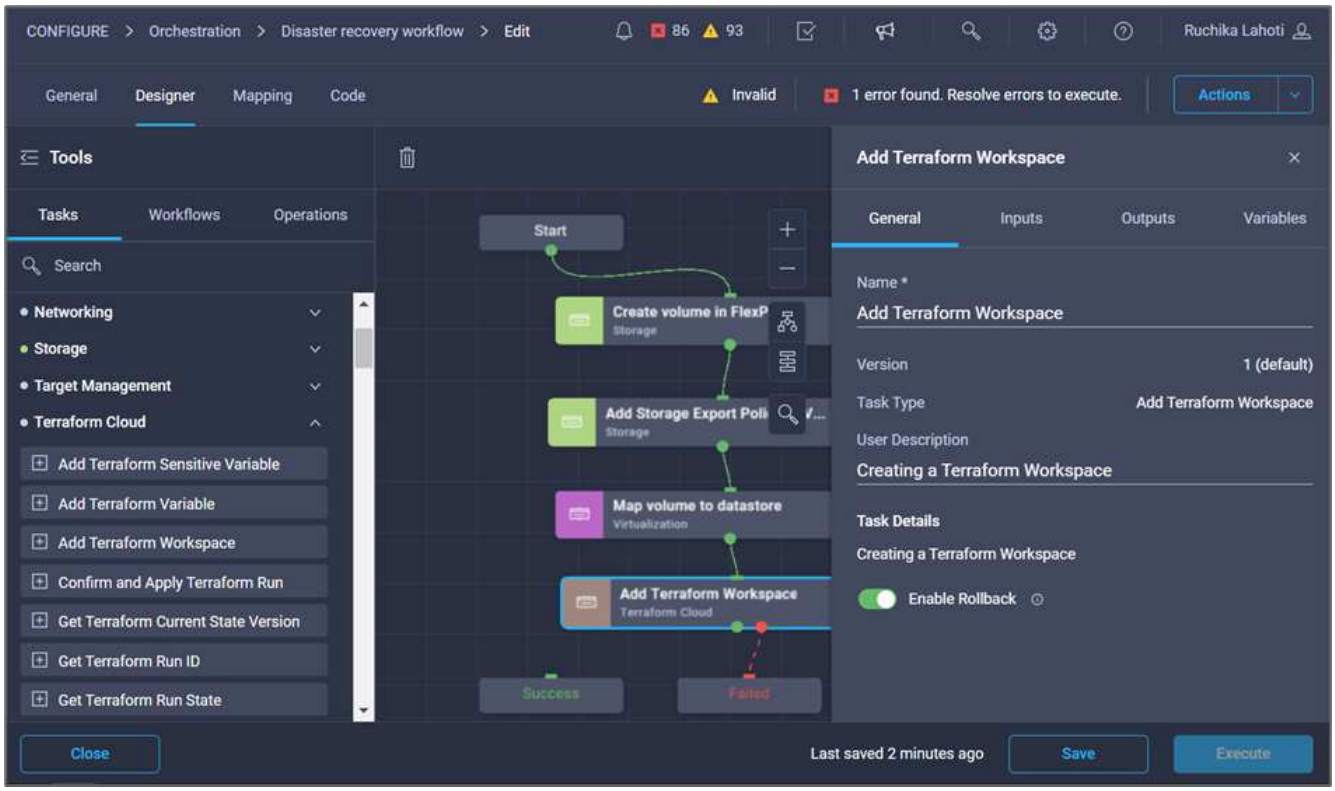


In questo modo viene completata l'attività di creazione dell'archivio dati. Tutte le attività eseguite nel data center FlexPod on-premise sono state completate.

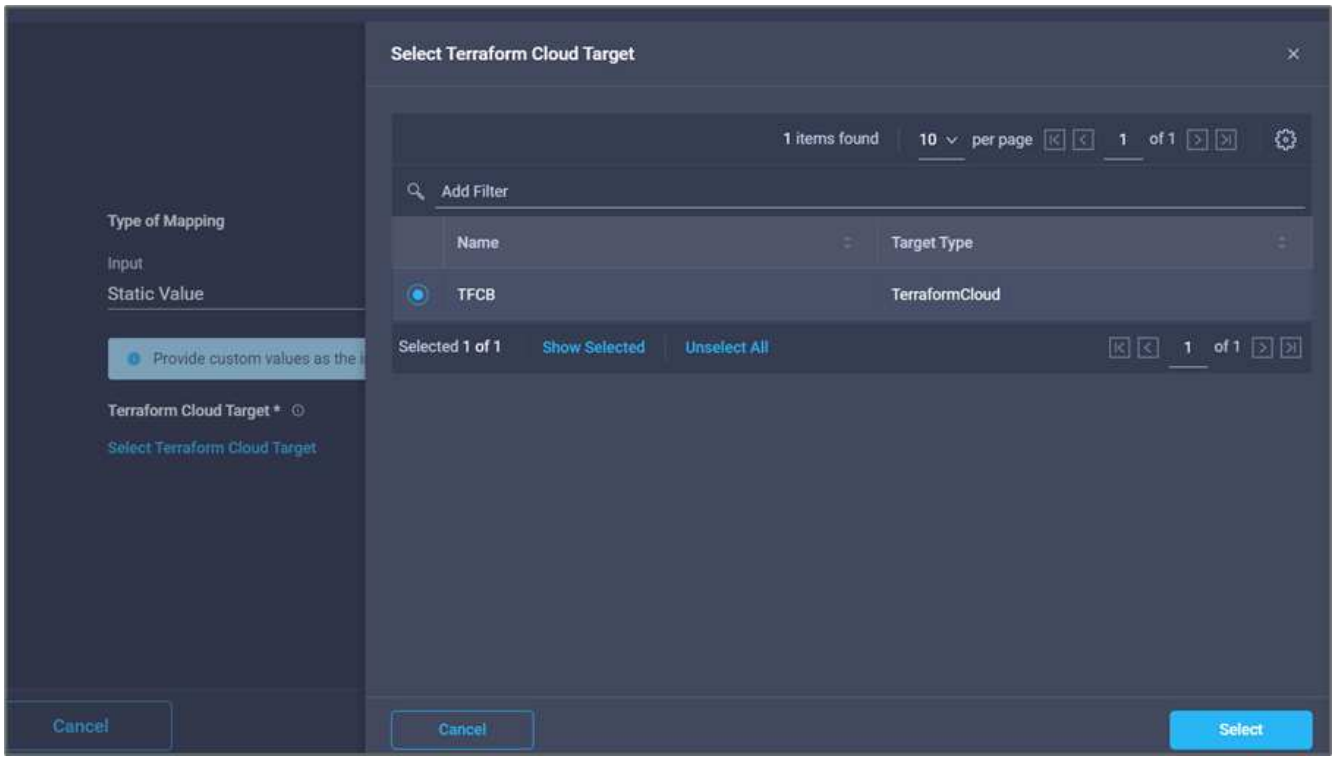


Procedura 5: Aggiungere una nuova area di lavoro Terraform

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Add Terraform Workspace** dalla sezione Tools (Strumenti) dell'area Design (progettazione).
3. Utilizzare Connector per connettere le attività **Map volume to Datastore** e **Add Terraform Workspace** e fare clic su **Save**.
4. Fare clic su **Aggiungi area di lavoro Terraform**. Nell'area Task Properties (Proprietà attività), fare clic sulla scheda **General** (Generale). In alternativa, è possibile modificare il nome e la descrizione dell'attività.

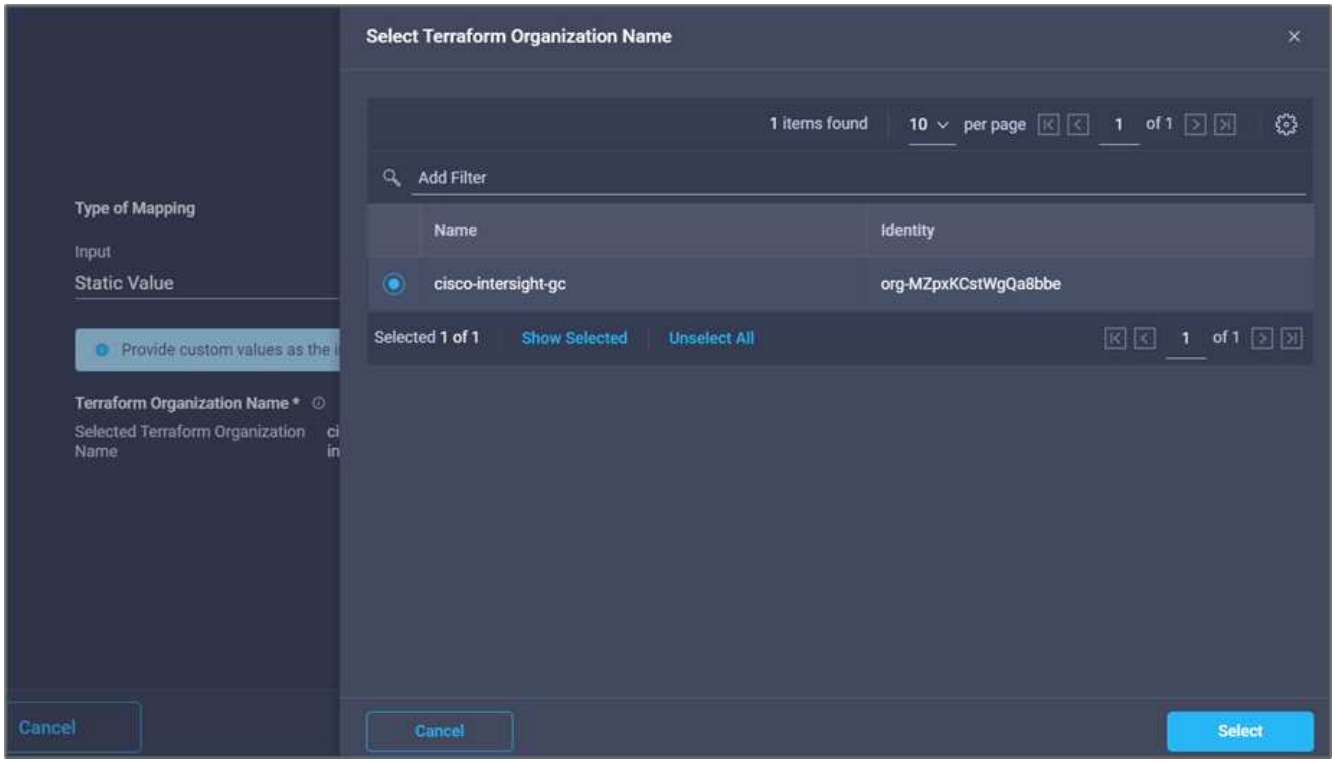


5. Nell'area Task Properties (Proprietà operazione), fare clic su **Input**.
6. Fare clic su **Map** nel campo di immissione **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto come spiegato in "Configurare Cisco Intersight Service per HashiCorp Terraform".".

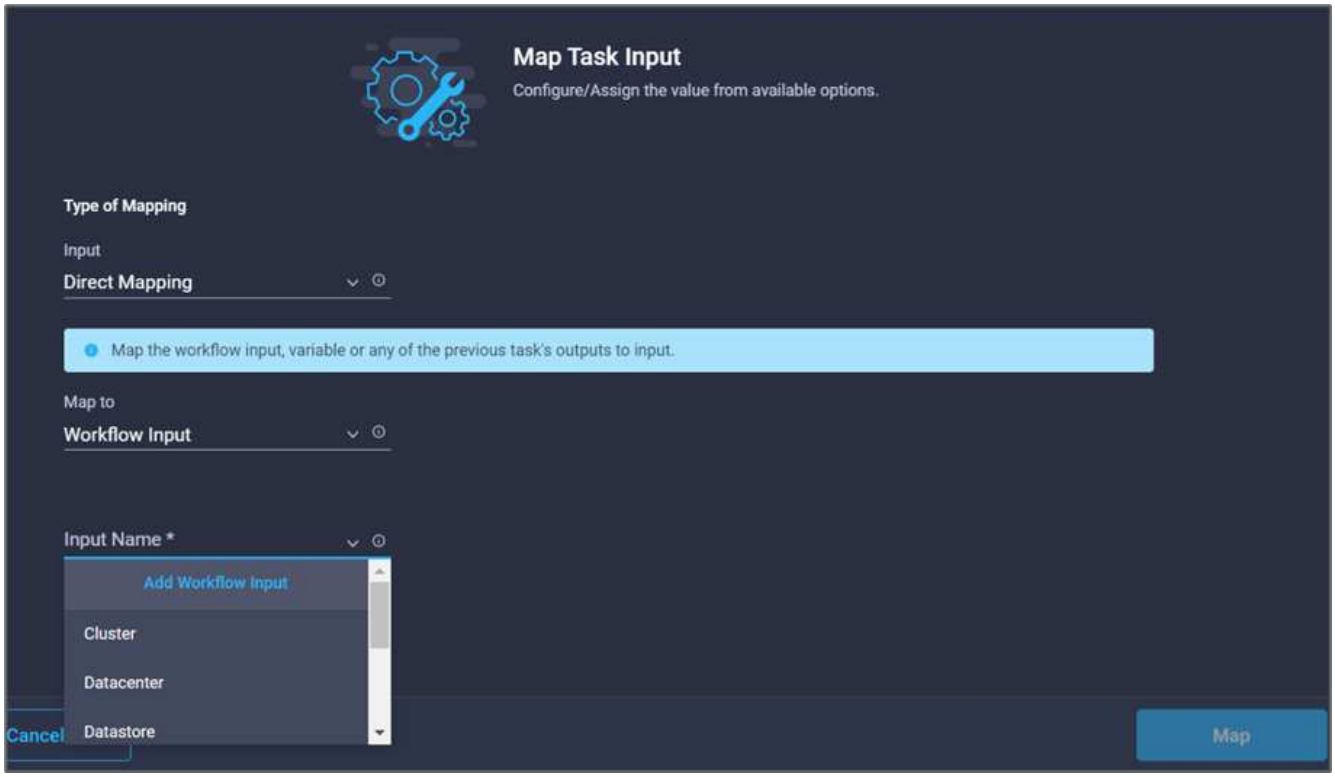


8. Fare clic su **Map** (Mappa).

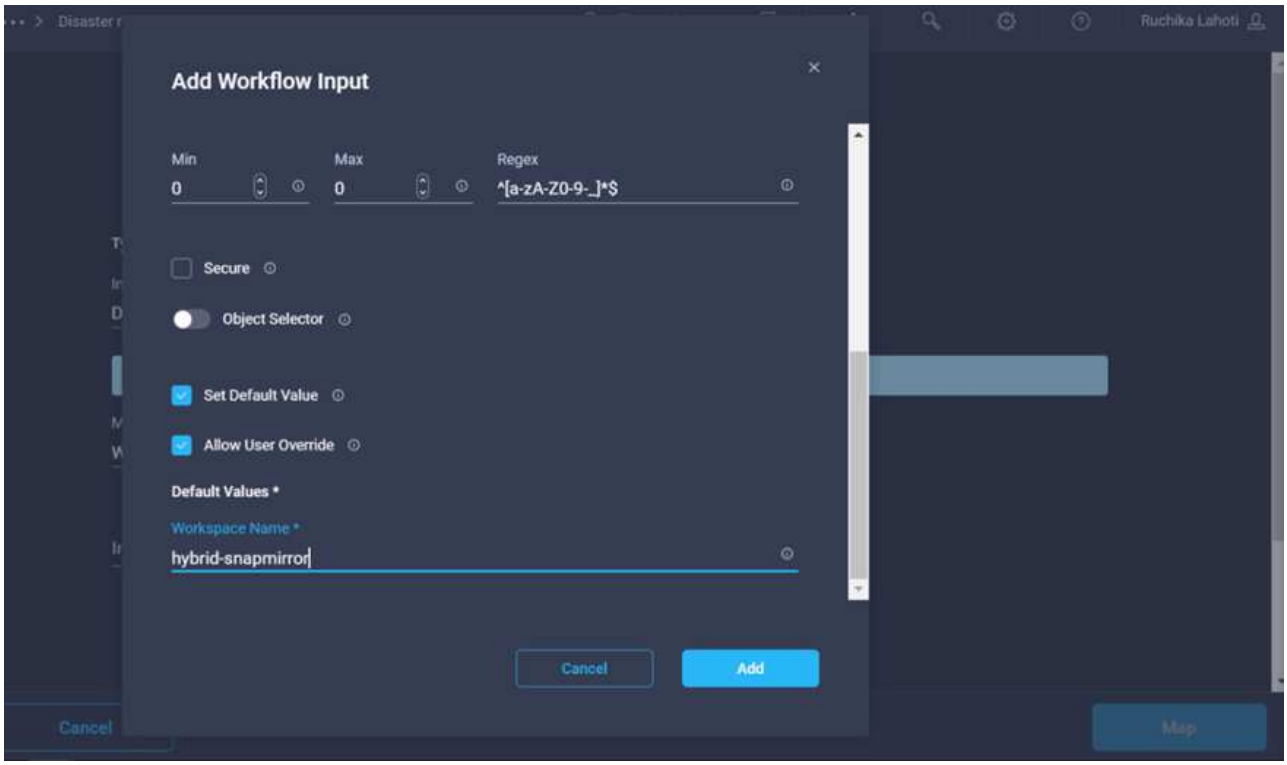
9. Fare clic su **Map** nel campo di immissione **Terraform Organization Name**.
10. Scegliere **Static Value** (valore statico), quindi fare clic su **Select Terraform Organization** (Seleziona organizzazione terraform). Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.



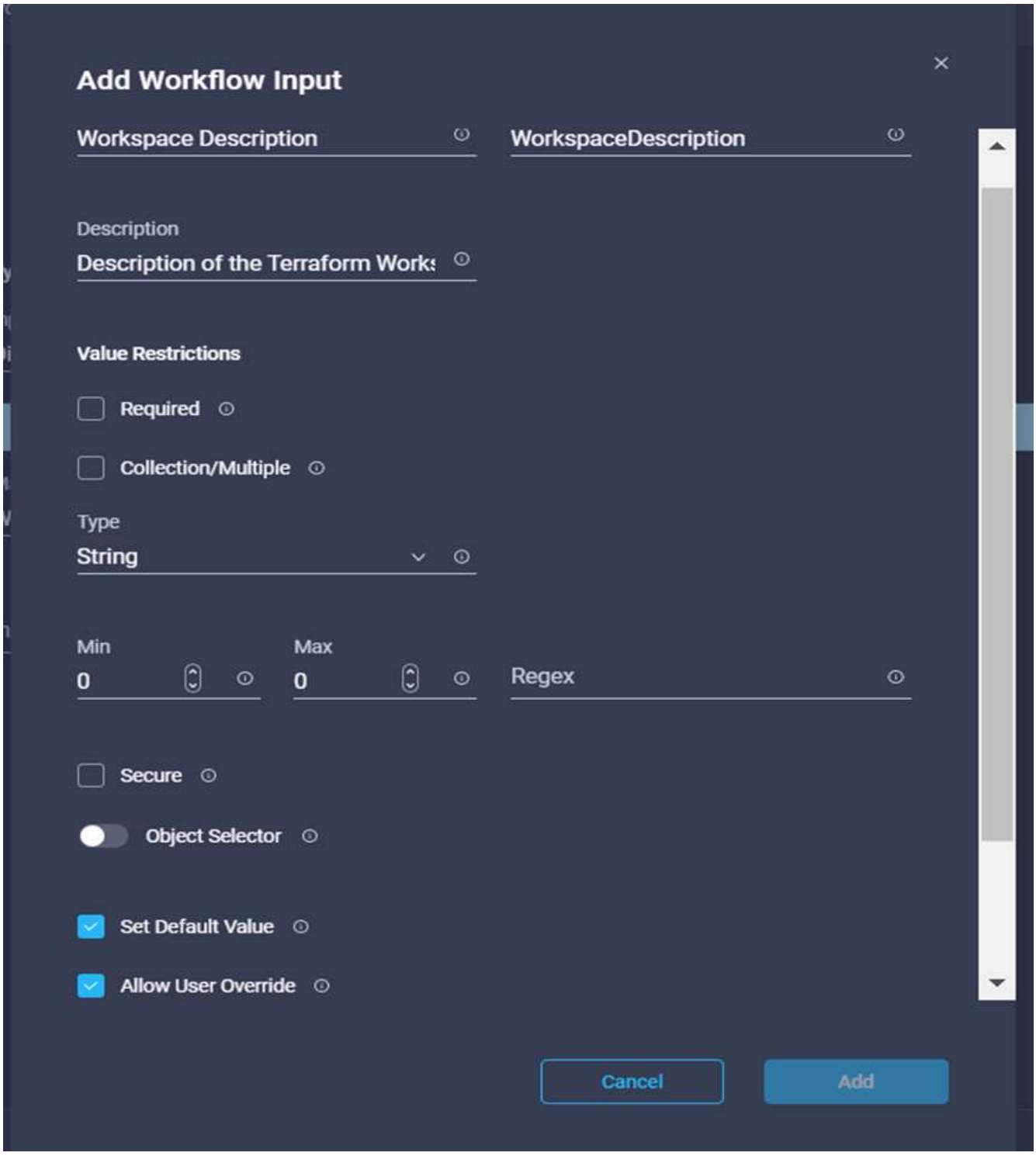
11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**. Questo è il nuovo spazio di lavoro nell'account Terraform Cloud for Business.
13. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
14. Fare clic su **Input Name** e **Create Workflow Input**.



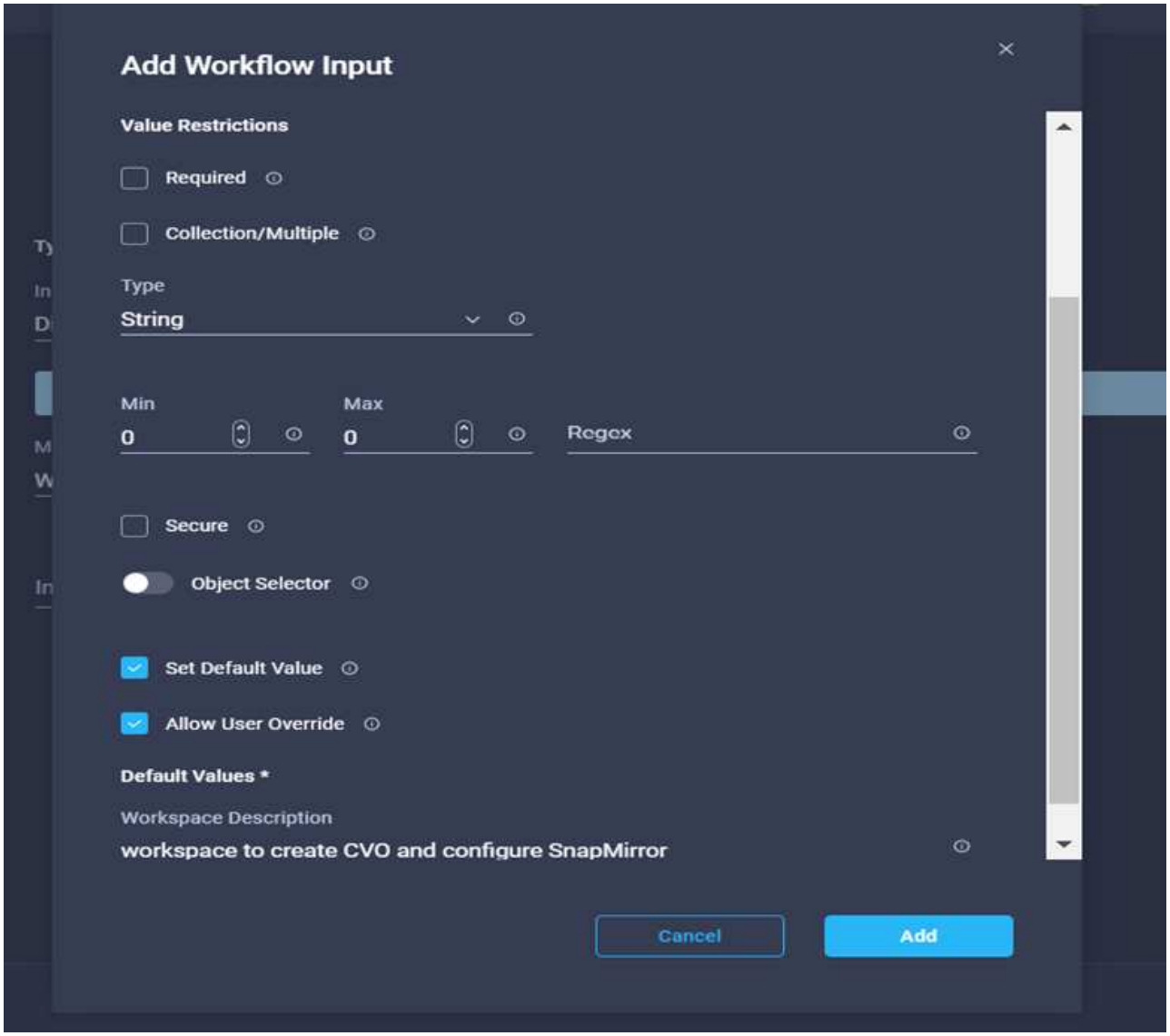
15. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Fare clic su **obbligatorio**.
    c. Assicurarsi di selezionare **String** per **Type**.
    d. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    e. Specificare un nome predefinito per l'area di lavoro.
    f. Fare clic su **Aggiungi**.



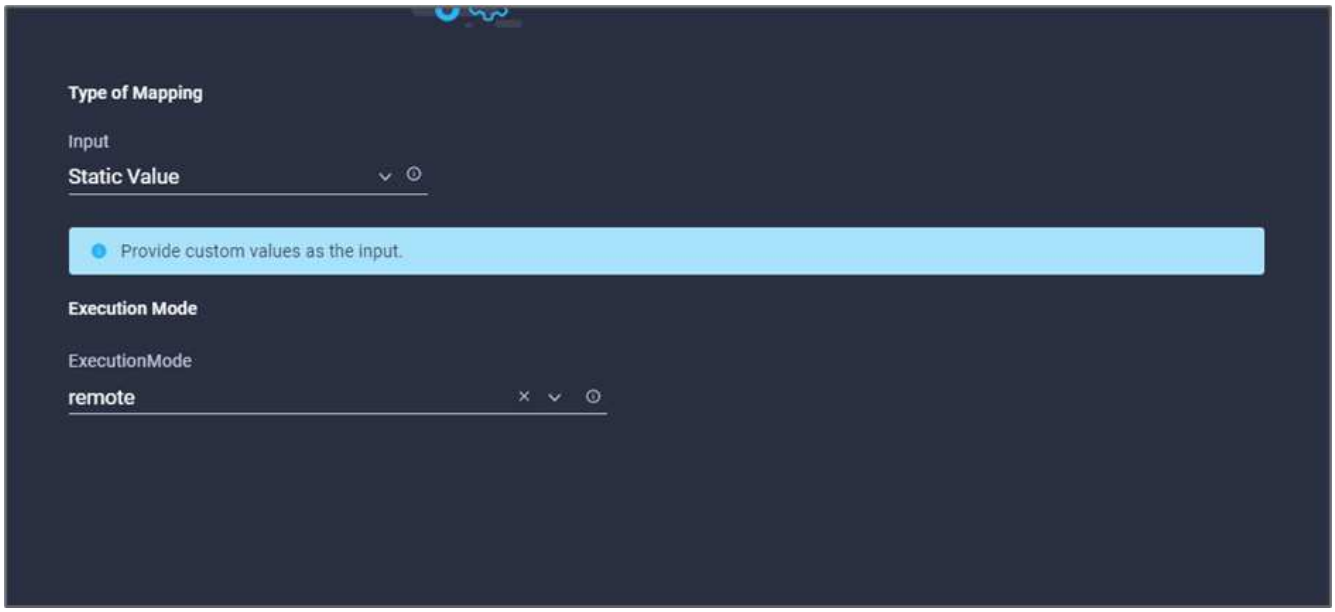
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** (Mappa) nel campo **Workspace Description** (Descrizione area di lavoro).
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.



20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fornire una descrizione dell'area di lavoro e fare clic su **Aggiungi**.



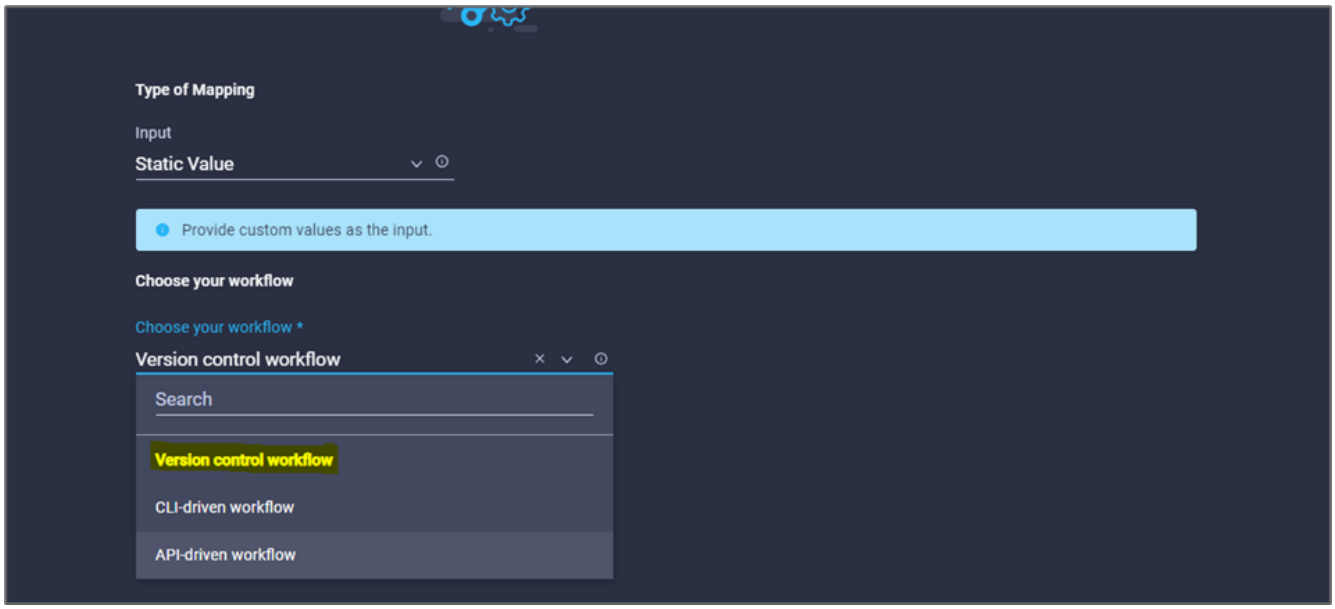
21. Fare clic su **Map** (Mappa).
22. Fare clic su **Map** nel campo **Execution Mode**.
23. Scegliere **valore statico**, fare clic su **modalità di esecuzione**, quindi fare clic su **remoto**.



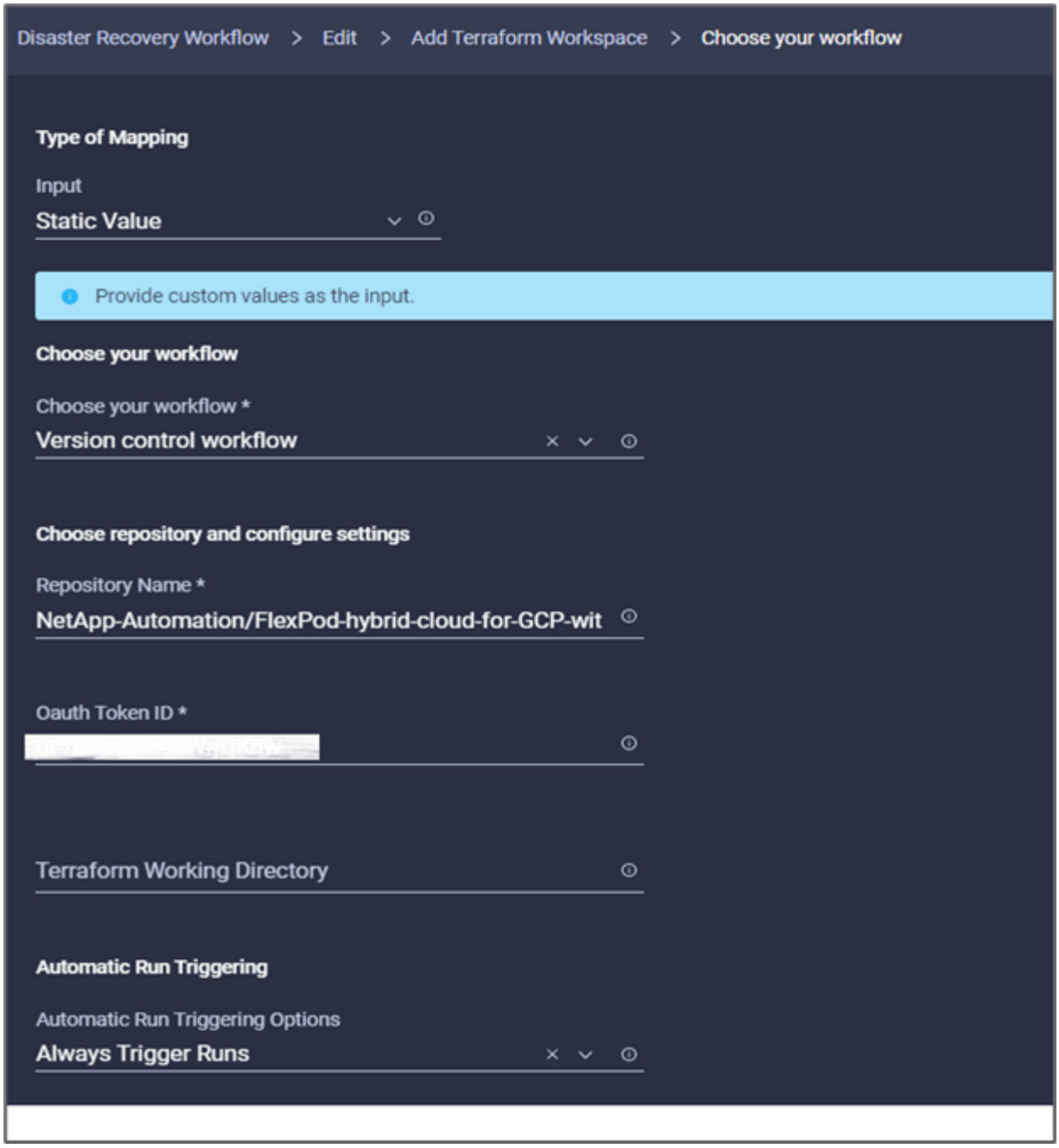
24. Fare clic su **Map** (Mappa).
25. Fare clic su **Map** nel campo **Apply Method** (Applica metodo).
26. Scegliere **valore statico** e fare clic su **Applica metodo**. Fare clic su **Manual Apply** (Applica manuale).

27. Fare clic su **Map** (Mappa).
28. Fare clic su **Map** (Mappa) nel campo **User Interface** (interfaccia utente).
29. Scegliere **Static Value** (valore statico) e fare clic su **User Interface** (interfaccia utente). Fare clic su **Console UI**.

30. Fare clic su **Map** (Mappa).
31. Fare clic su **Map** nel campo di immissione e selezionare il flusso di lavoro.
32. Selezionare **valore statico** e fare clic su **Scegli il flusso di lavoro**. Fare clic su **Version Control Workflow**.



33. Fornire i seguenti dettagli sul repository GitHub:
    a. In **Repository Name** (Nome repository), immettere il nome del repository descritto nella sezione ""Configurazione dei prerequisiti dell'ambiente"".
    b. Fornire l'ID token OAuth come descritto in dettaglio nella sezione ""Configurazione dei prerequisiti dell'ambiente"".
    c. Selezionare l'opzione **Automatic Run Triggering**.



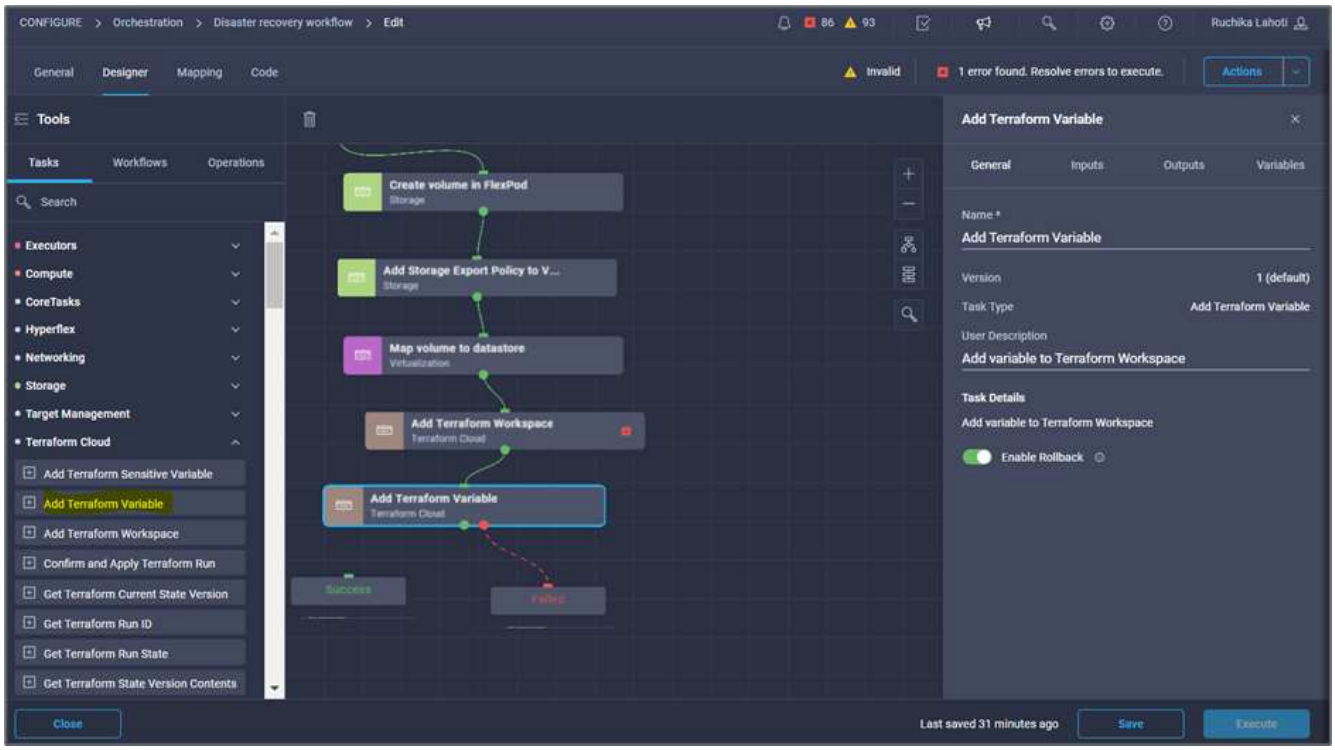
34. Fare clic su **Map** (Mappa).
35. Fare clic su **Save** (Salva).

In questo modo viene completata l'attività di creazione di uno spazio di lavoro in un account Terraform Cloud for Business.

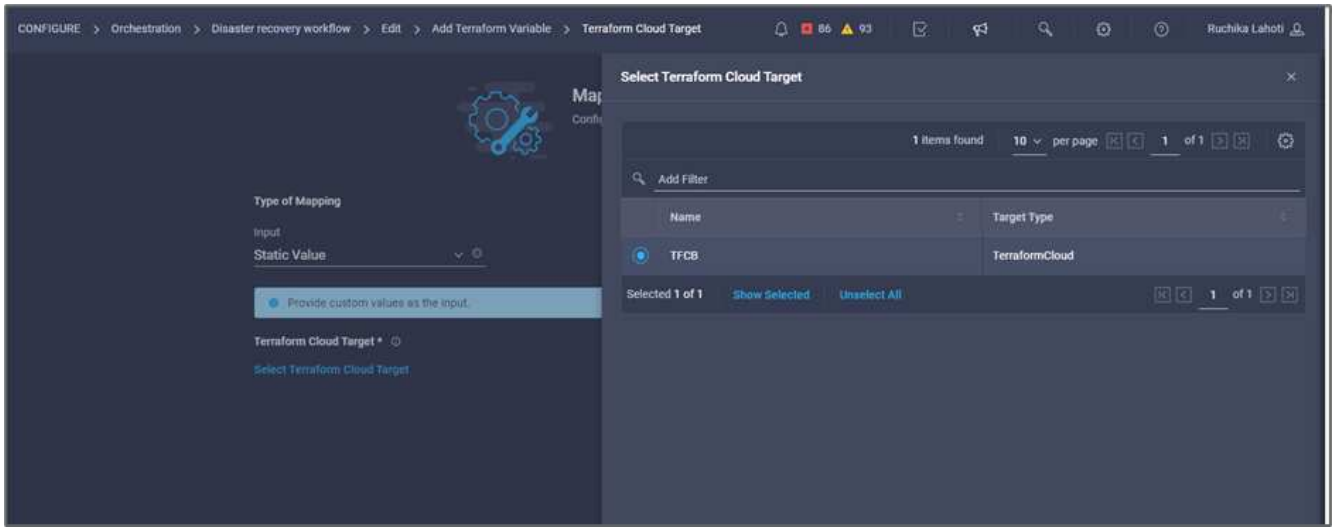
Procedura 6: Aggiunta di variabili non sensibili all'area di lavoro

1. Accedere alla scheda **Designer** e fare clic sulla sezione **flussi di lavoro da Strumenti**.
2. Trascinare il flusso di lavoro **Terraform > Add Terraform Variables** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le attività **Add Terraform Workspace** e **Add Terraform Variables**. Fare clic su **Save** (Salva).

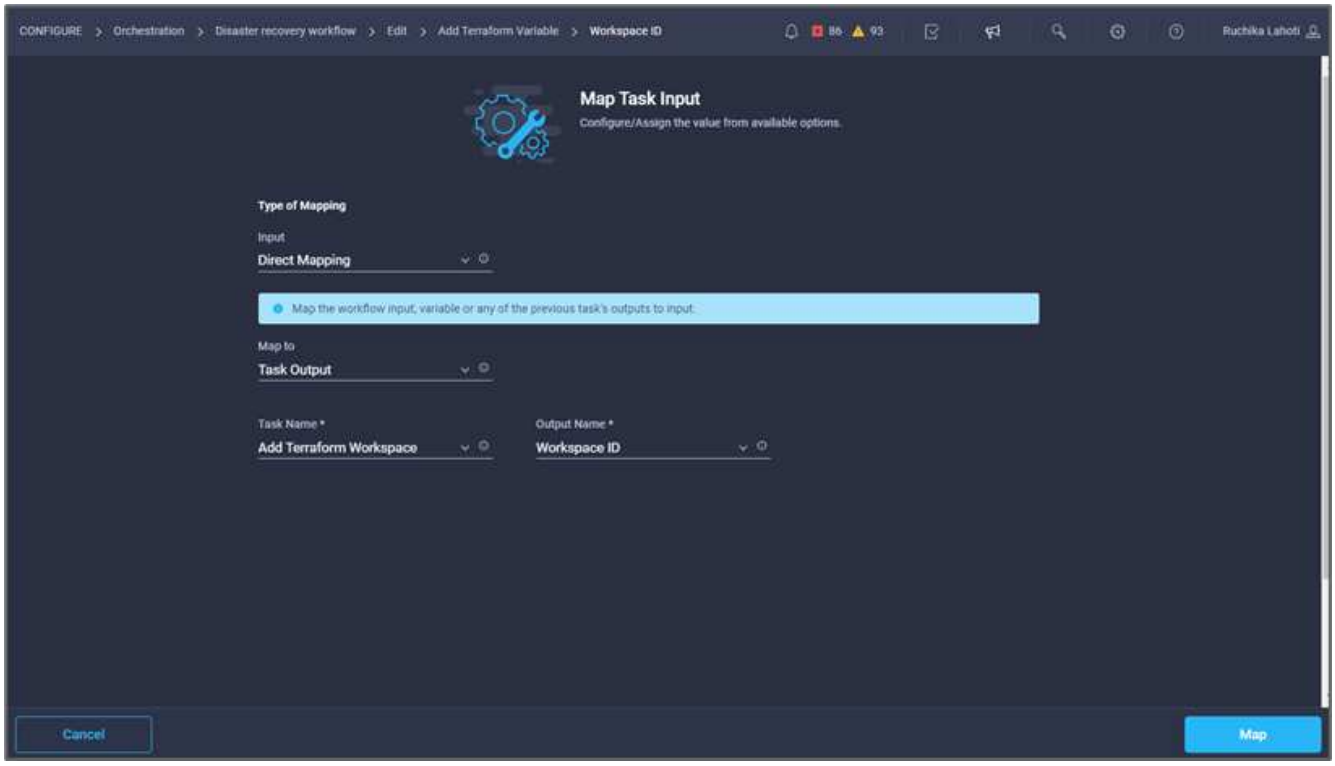
4. Fare clic su **Aggiungi variabili terraform**. Nell'area **Workflow Properties** (Proprietà flusso di lavoro), fare clic sulla scheda **General** (Generale). In alternativa, è possibile modificare il nome e la descrizione dell'attività.



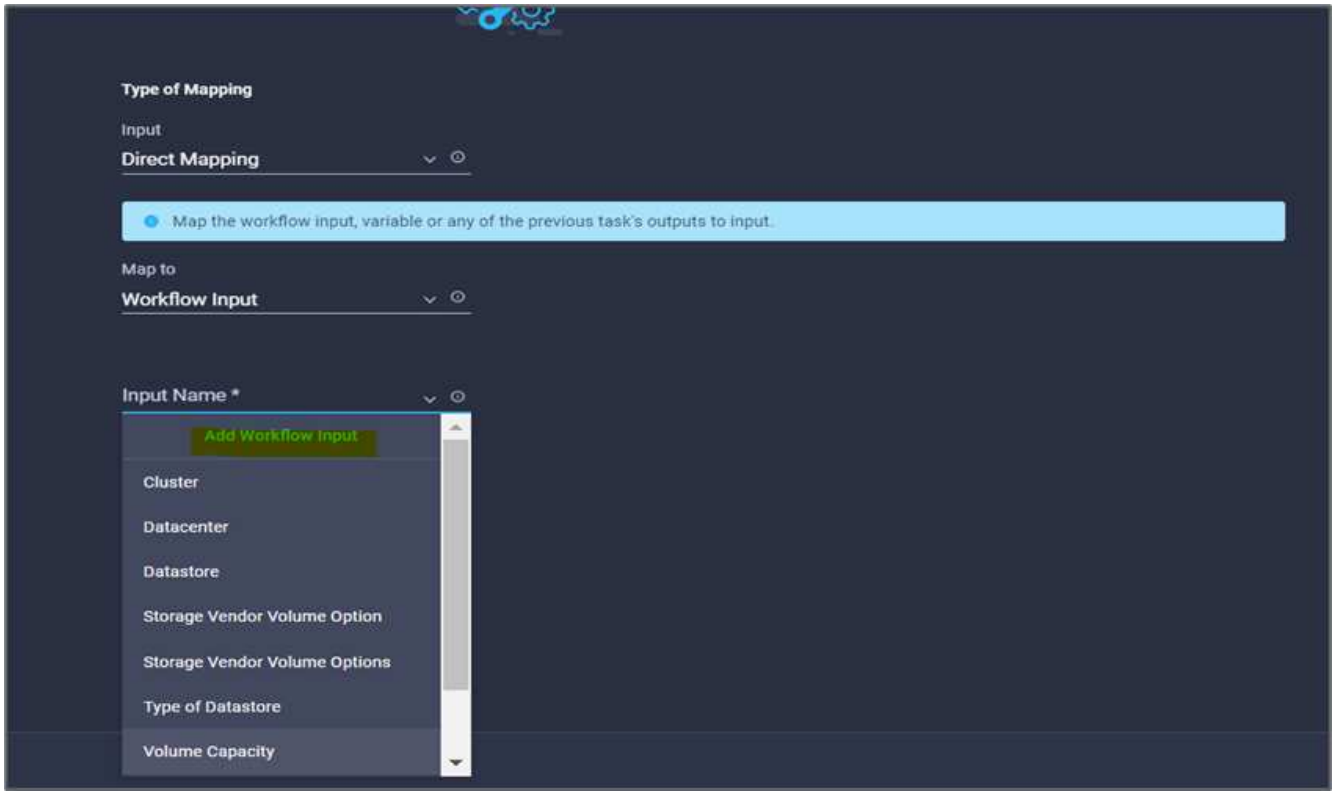
5. Nell'area **Workflow Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto come spiegato in "Configurare Cisco Intersight Service per HashiCorp Terraform".".



8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo *Terraform Organization Name *.
10. Scegliere **valore statico** e fare clic su **Seleziona organizzazione terraform**. Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.

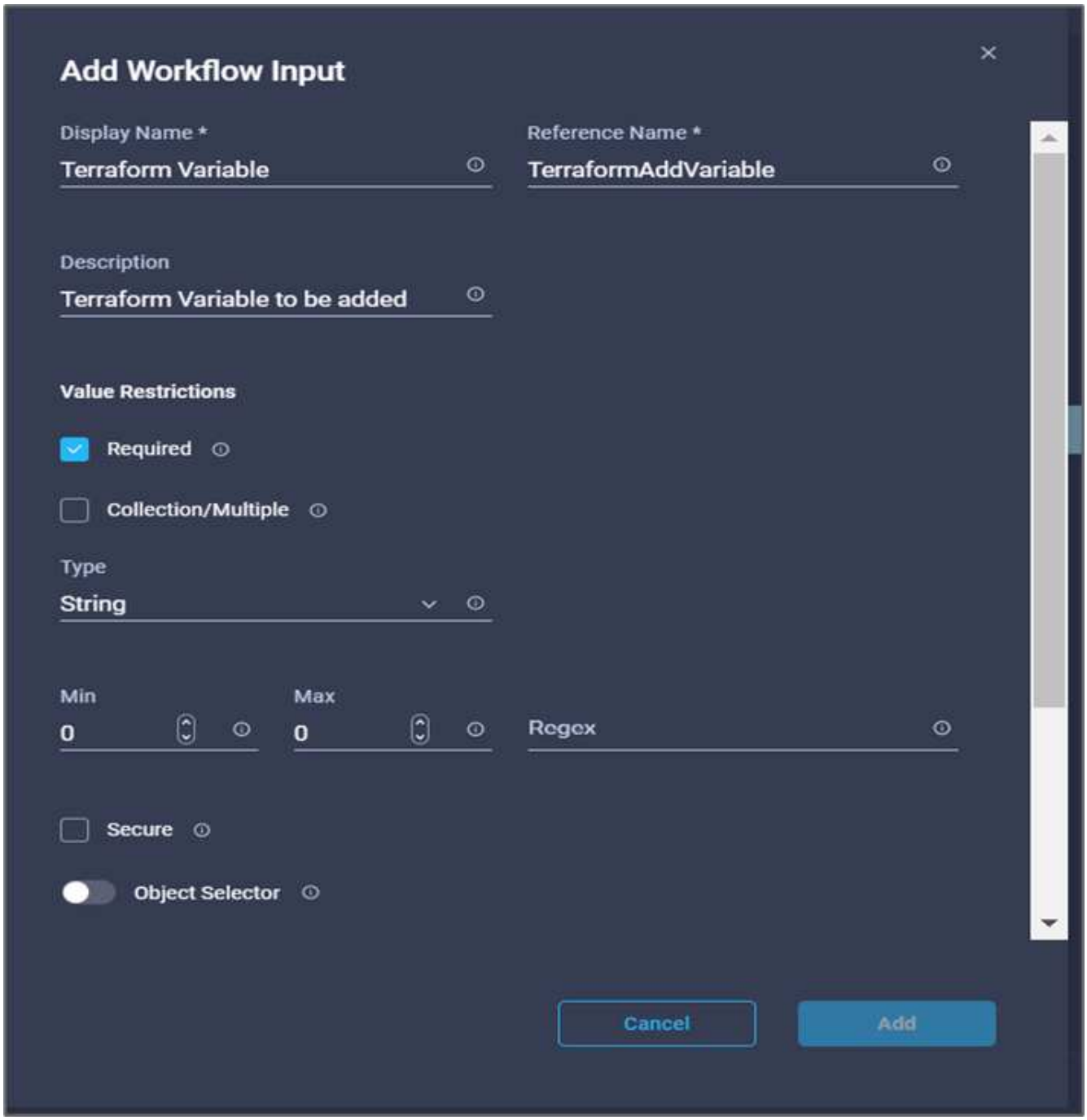


11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**.
13. Scegliere **Direct Mapping** e fare clic su **Task Output**.
14. Fare clic su **Nome attività** e fare clic su **Aggiungi area di lavoro terraform**.



15. Fare clic su **Output Name** (Nome output) e su **Workspace Name** (Nome area di lavoro).

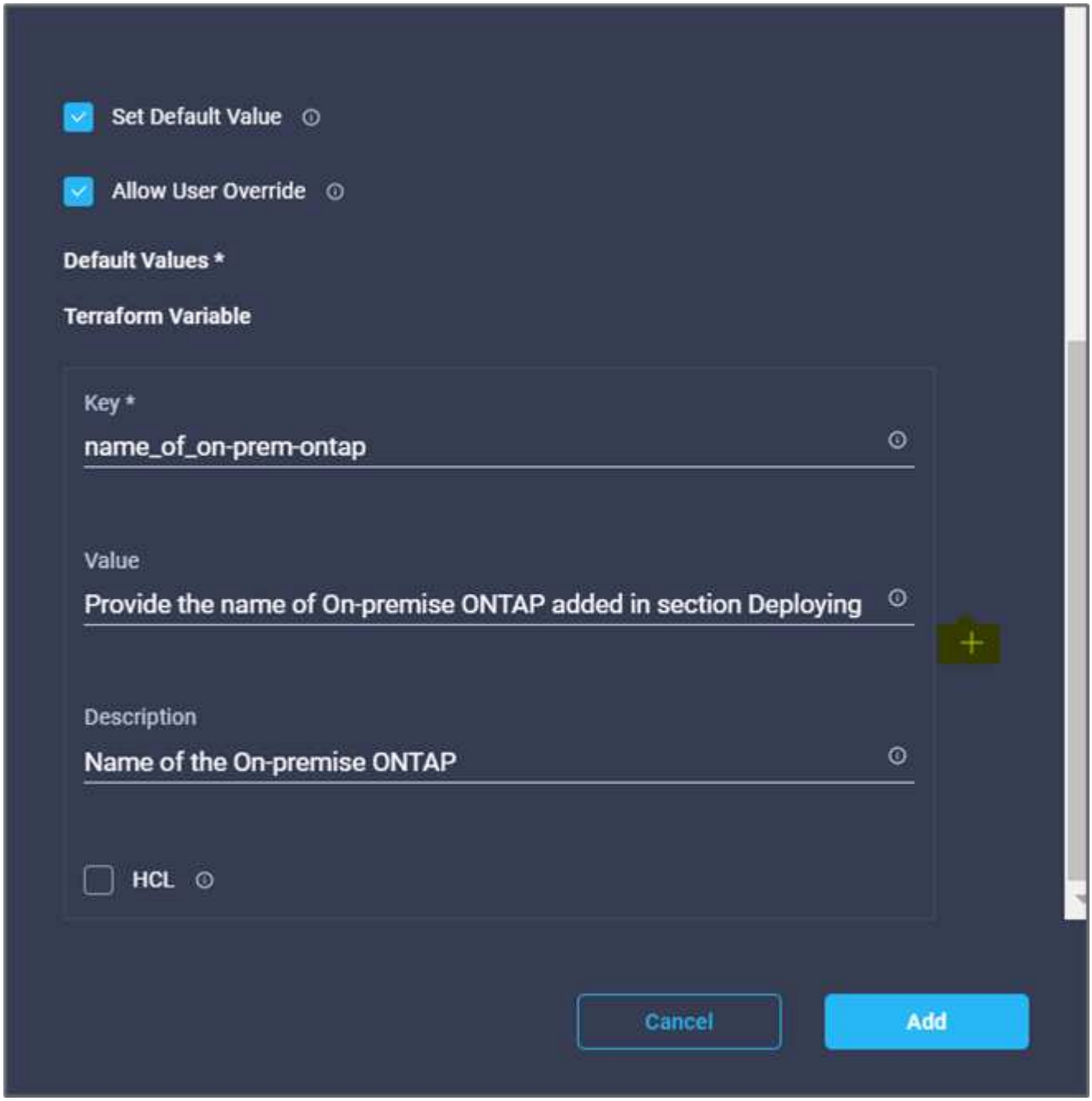
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Add Variables Options**.
18. Scegliere **Direct Mapping** e fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.



20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (opzionale).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Fare clic su **Variable Type** (tipo di variabile), quindi su **non-sensitive Variables** (variabili non

sensibili).

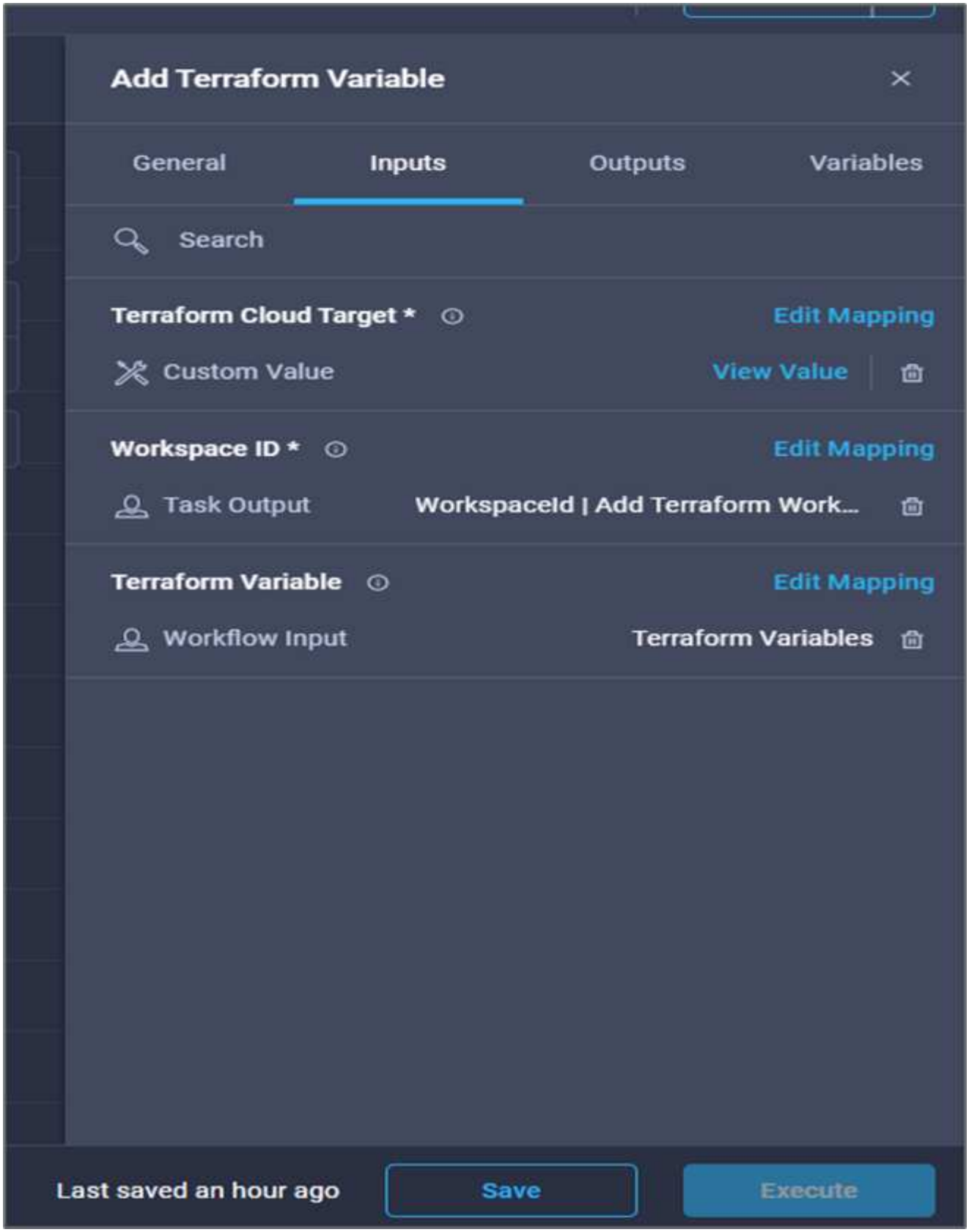
21. Nella sezione **Add Terraform Variables**, fornire le seguenti informazioni:
    - **Chiave.** `name_of_on-prem-ontap`
    - **Value.** indica il nome di on-premise ONTAP.
    - **Descrizione.** Nome del ONTAP on-premise.
22. Fare clic su **+** per aggiungere ulteriori variabili.



23. Aggiungere tutte le variabili Terraform come mostrato nella tabella seguente. È inoltre possibile specificare un valore predefinito.

Nome della variabile terraform	Descrizione
name_of_on-premise-ontap	Nome del FlexPod (on-premise ONTAP)
ip_cluster_ontap on-premise	L'indirizzo IP dell'interfaccia di gestione del cluster di storage
nome_utente_ontap_on-premise	Nome utente amministratore per il cluster di storage
Zona	Regione GCP in cui verrà creato l'ambiente di lavoro
subnet_id	id subnet GCP in cui verrà creato l'ambiente di lavoro
id_vpc	L'ID VPC in cui verrà creato l'ambiente di lavoro
nome_pacchetto_capacità	Il tipo di licenza da utilizzare
volume_origine	Il nome del volume di origine
source_storage_vm_name	Il nome della SVM di origine
destination_volume	Nome del volume su Cloud Volumes ONTAP
schedule_of_replication	L'impostazione predefinita è 1 ora
name_of_volume_to_create_on_cvo	Nome del volume cloud
id_area di lavoro	L'id_area di lavoro in cui verrà creato l'ambiente di lavoro
ID_progetto	l'id_progetto in cui verrà creato l'ambiente di lavoro
name_of_cvo_cluster	Il nome dell'ambiente di lavoro Cloud Volumes ONTAP
account_servizio_gcp	account_servizio_gcp dell'ambiente di lavoro Cloud Volumes ONTAP

24. Fare clic su **Map** (Mappa), quindi su **Save** (Salva).



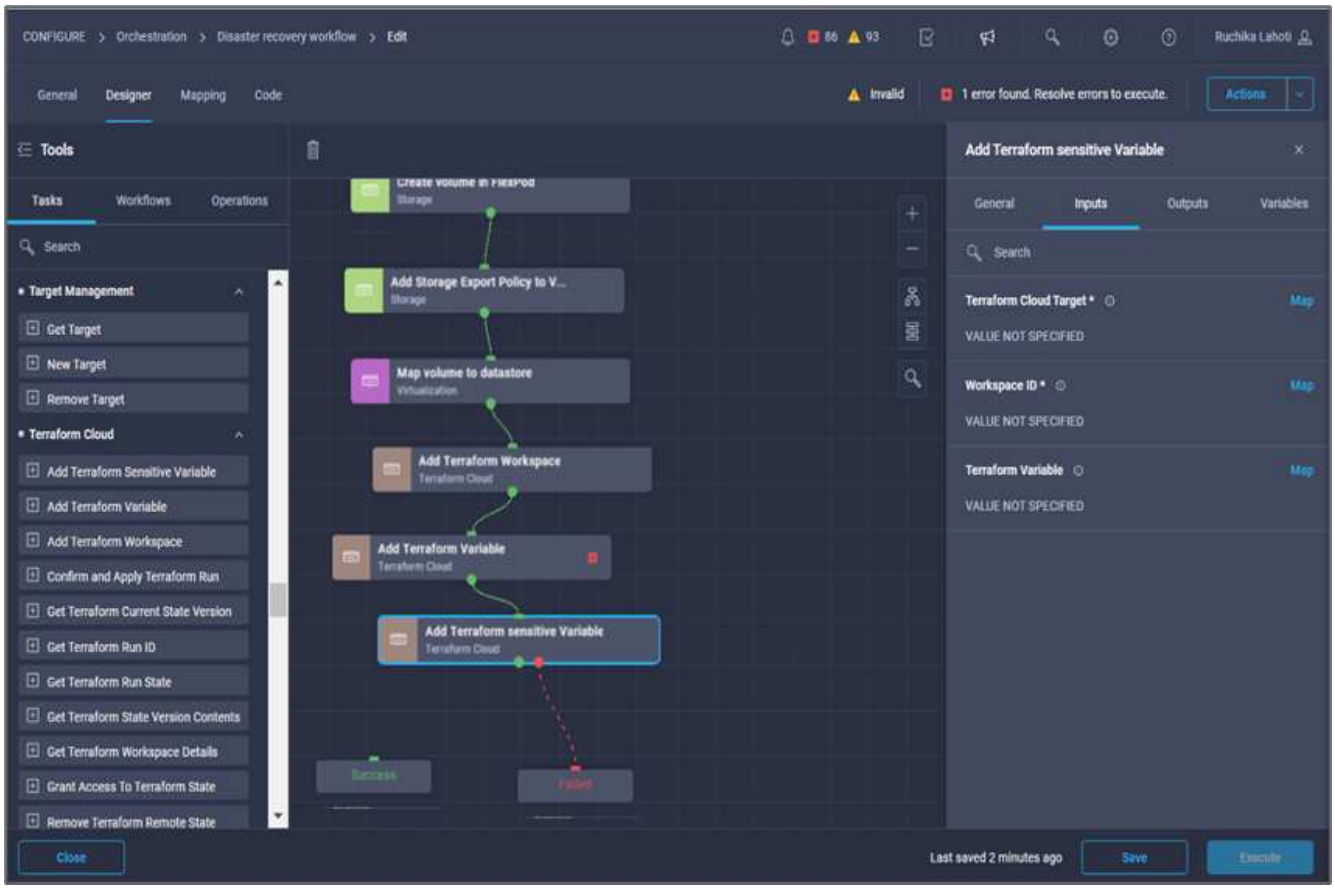
In questo modo viene completata l'attività di aggiunta delle variabili Terraform richieste all'area di lavoro. Quindi, aggiungere le variabili Terraform sensibili richieste all'area di lavoro. È inoltre possibile combinare entrambi in un'unica attività.

Procedura 7: Aggiunta di variabili sensibili a un'area di lavoro

1. Accedere alla scheda **Designer** e fare clic su **workflow** nella sezione **Strumenti**.
2. Trascinare il flusso di lavoro **Terraform > Add Terraform Variables** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le due attività **Add Terraform Workspace**. Fare clic su **Save** (Salva).

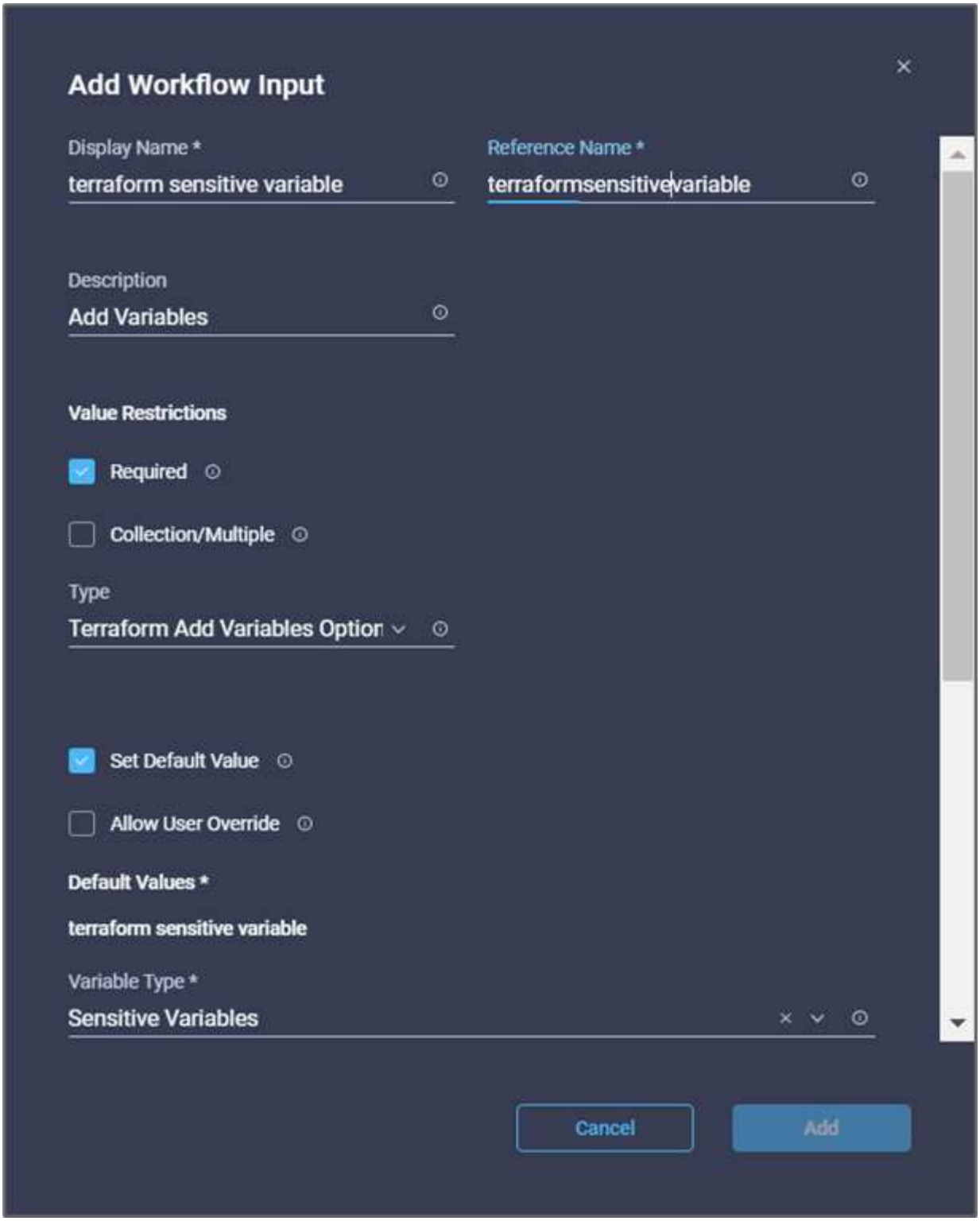
> Viene visualizzato un avviso che indica che le due attività hanno lo stesso nome. Ignorare l'errore per ora perché si modifica il nome dell'attività nel passaggio successivo.

4. Fare clic su **Aggiungi variabili terraform**. Nell'area **Workflow Properties** (Proprietà flusso di lavoro), fare clic sulla scheda **General** (Generale). Modificare il nome in **Aggiungi variabili sensibili al terraform**.



5. Nell'area **Workflow Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Seleziona l'account Terraform Cloud for Business che è stato aggiunto nella sezione "Configurare Cisco Intersight Service per HashiCorp Terraform"."
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Terraform Organization Name**.
10. Scegliere **valore statico** e fare clic su **Seleziona organizzazione terraform**. Seleziona il nome dell'organizzazione Terraform a cui fai parte nel tuo account Terraform Cloud for Business.
11. Fare clic su **Map** (Mappa).
12. Fare clic su **Map** nel campo **Terraform Workspace Name**.

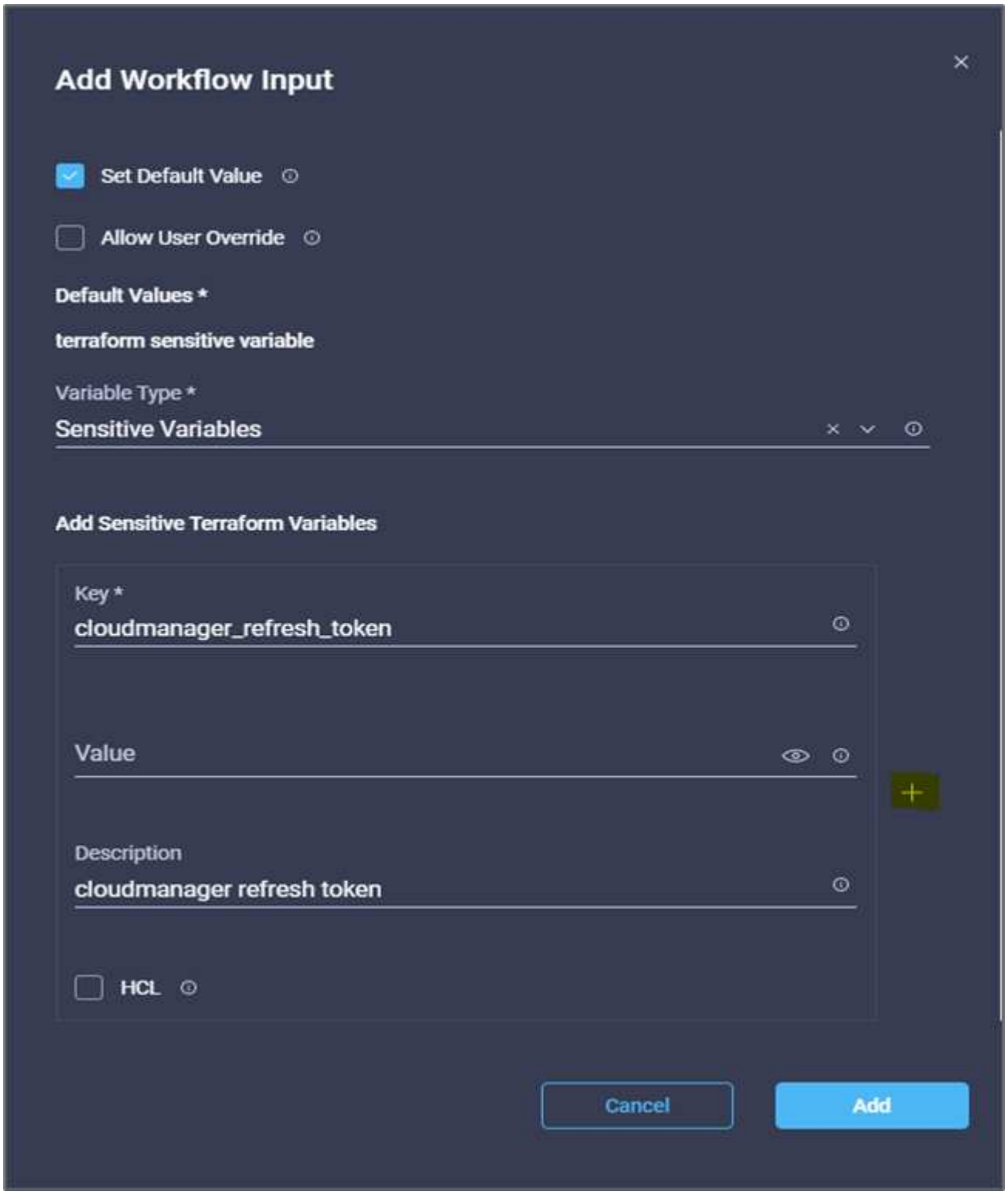
13. Scegliere **Direct Mapping** e fare clic su **Task Output**.
14. Fare clic su **Nome attività**, quindi su **Aggiungi area di lavoro terraform**.
15. Fare clic su **Output Name** (Nome output) e selezionare l'output **Workspace Name** (Nome area di lavoro).
16. Fare clic su **Map** (Mappa).
17. Fare clic su **Map** nel campo **Add Variables Options**.
18. Scegliere **Direct Mapping**, quindi fare clic su **Workflow Input**.
19. Fare clic su **Input Name** e **Create Workflow Input**.
20. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **Terraform Add Variables Options** per il tipo.
    c. Fare clic su **Set Default Value** (Imposta valore predefinito).
    d. Fare clic su **Variable Type** (tipo variabile), quindi su **Sensitive Variables** (variabili sensibili).
    e. Fare clic su **Aggiungi**.



21. Nella sezione **Add Terraform Variables**, fornire le seguenti informazioni:

    - **Chiave.** `cloudmanager_refresh_token`.
    - **Valore.** inserire il token di refresh per le operazioni API di NetApp Cloud Manager.
    - **Descrizione.** Aggiorna token.

Per ulteriori informazioni su come ottenere un token di refresh per le operazioni API di NetApp Cloud Manager, consulta la sezione ""Configurazione dei prerequisiti dell'ambiente"."



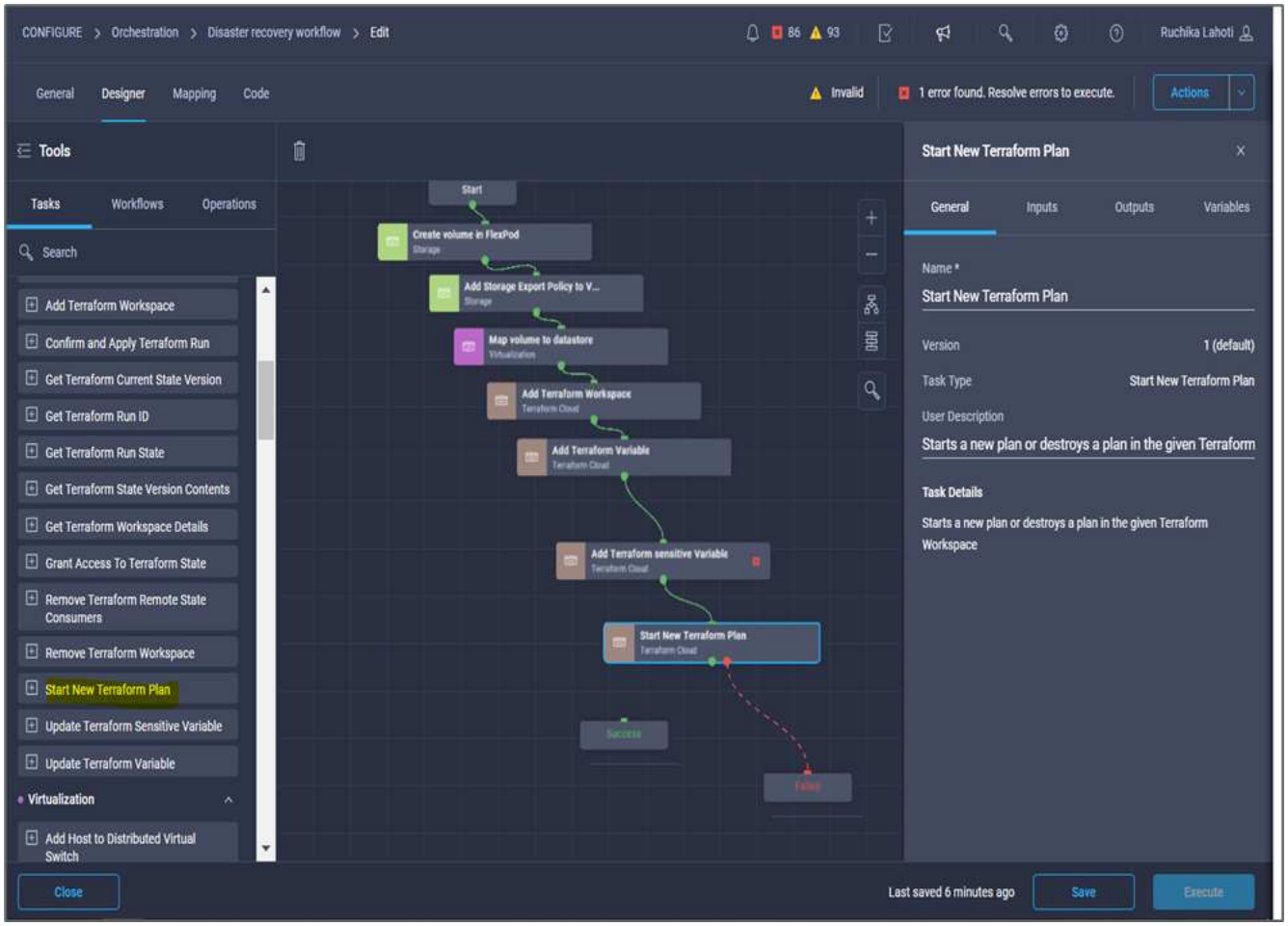
22. Aggiungere tutte le variabili sensibili al terraform come mostrato nella tabella seguente. È inoltre possibile specificare un valore predefinito.

Nome variabile sensibile al terraform	Descrizione
cloud_manager_refresh_token	Aggiorna token. Ottenerlo da:
id_connettore	L'ID client di Cloud Manager Connector. Ottenerlo da
cvo_admin_password	La password admin per Cloud Volumes ONTAP
on-premise-ontap_user_password	Password di amministratore per il cluster di storage

23. Fare clic su **Map** (Mappa) per completare l'operazione di aggiunta delle variabili sensibili al Terraform richieste all'area di lavoro. Quindi, avviare un nuovo piano Terraform nell'area di lavoro configurata.

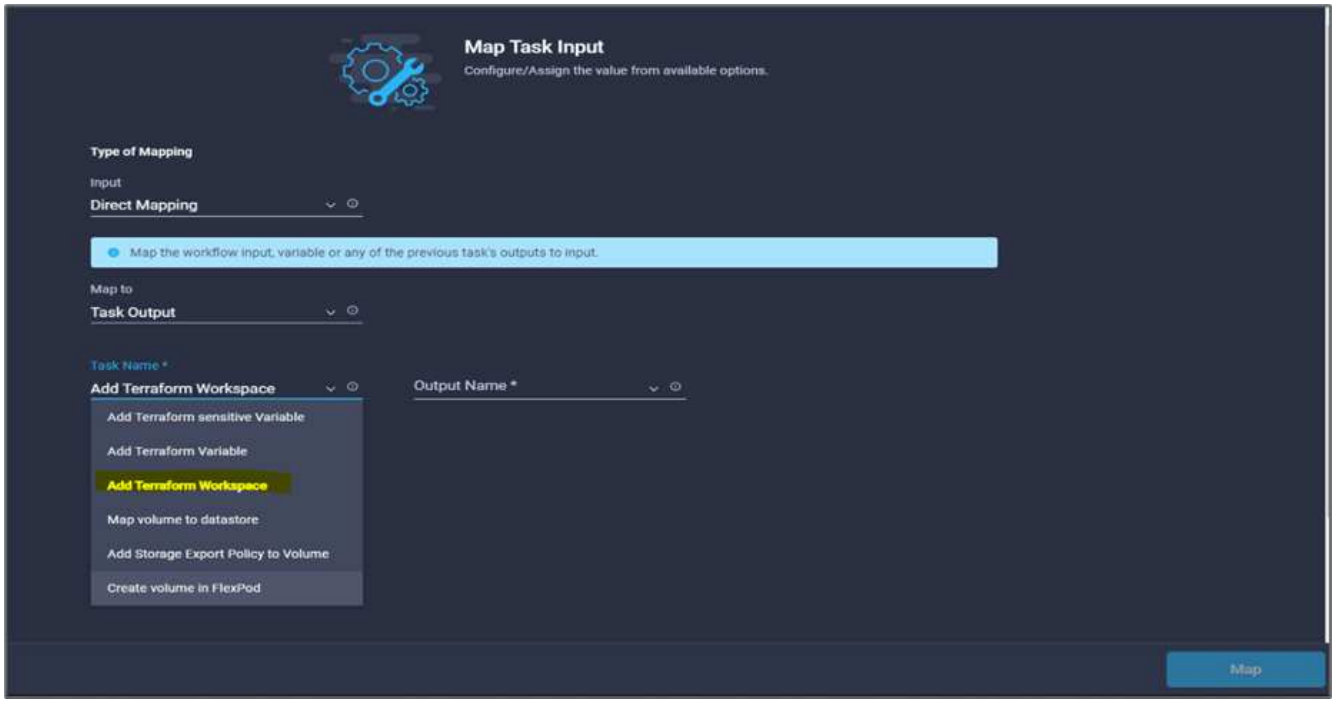
Procedura 8: Avviare un nuovo piano Terraform

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Start New Terraform Plan** (Avvia nuovo piano di terraform) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per connettersi tra le attività **Aggiungi variabili sensibili al terraform** e **Avvia nuove attività del piano di terraform**. Fare clic su **Save** (Salva).
4. Fare clic su **Start New Terraform Plan** (Avvia nuovo piano terraform). Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività.

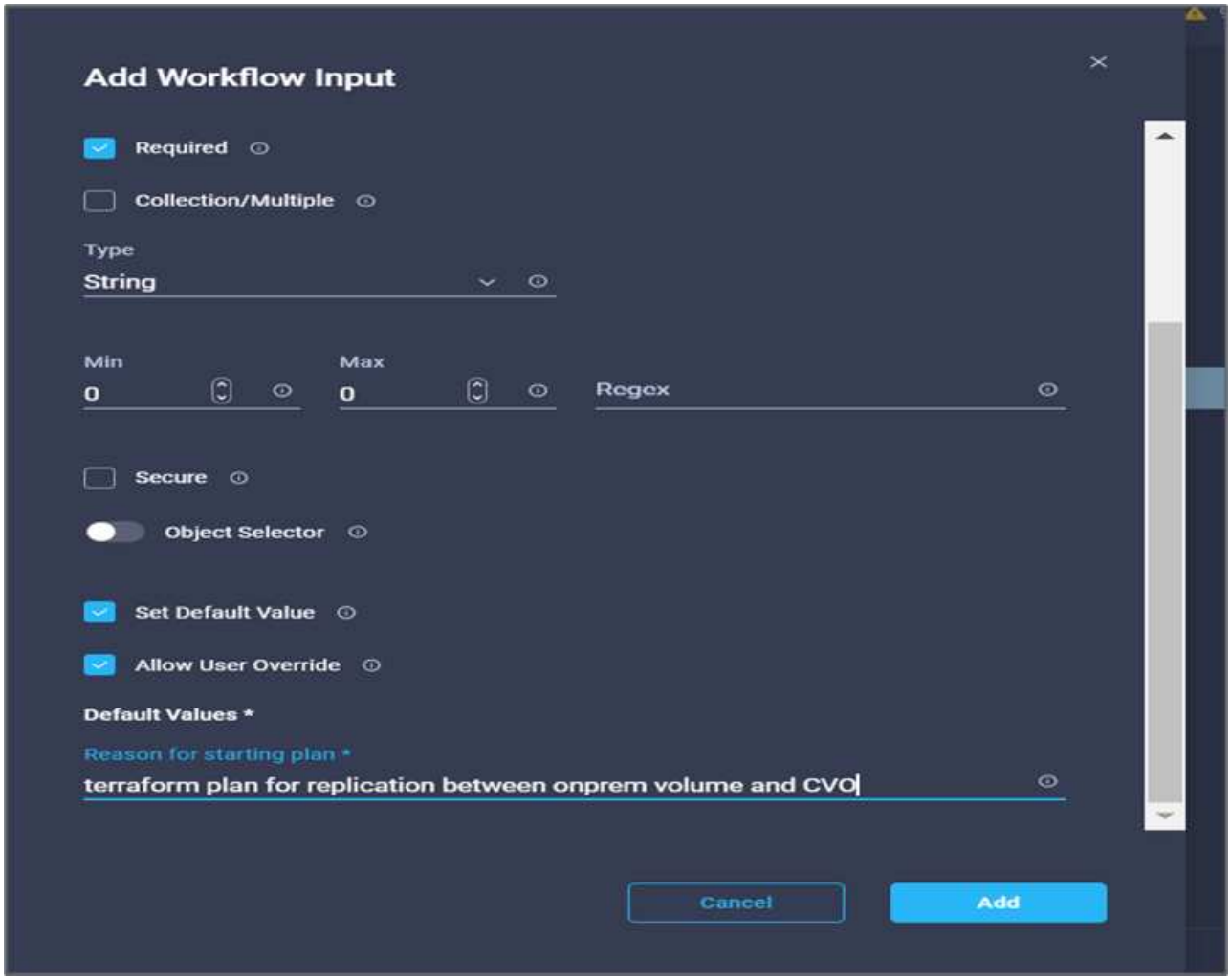


5. Nell'area **Task Properties**, fare clic su **Input**.

6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Selezionare l'account Terraform Cloud for Business aggiunto nella sezione "Configurazione di Cisco Intersight Service per HashiCorp Terraform".
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Workspace ID**.
10. Scegliere **Direct Mapping** e fare clic su **Task Output**.
11. Fare clic su **Nome attività**, quindi su **Aggiungi area di lavoro terraform**.



12. Fare clic su **Output Name**, **Workspace ID**, quindi su **Map**.
13. Fare clic su **Map** nel campo **Reason for Starting plan** (motivo del piano di avvio).
14. Scegliere **Direct Mapping**, quindi fare clic su **Workflow Input**.
15. Fare clic su **Input Name**, quindi su **Create Workflow Input**.
16. Nella procedura guidata Aggiungi input, completare i seguenti passaggi:
    a. Fornire un nome visualizzato e un nome di riferimento (facoltativo).
    b. Assicurarsi di selezionare **String** per **Type**.
    c. Fare clic su **Set Default Value and Override** (Imposta valore predefinito e ignora).
    d. Inserire un valore predefinito per **motivo dell'avvio del piano** e fare clic su **Aggiungi**.



17. Fare clic su **Map** (Mappa).
18. Fare clic su **Map** (Mappa) nel campo **Plan Operation** (operazione piano).
19. Scegliere **valore statico** e fare clic su **operazione piano**. Fare clic su **nuovo piano**.

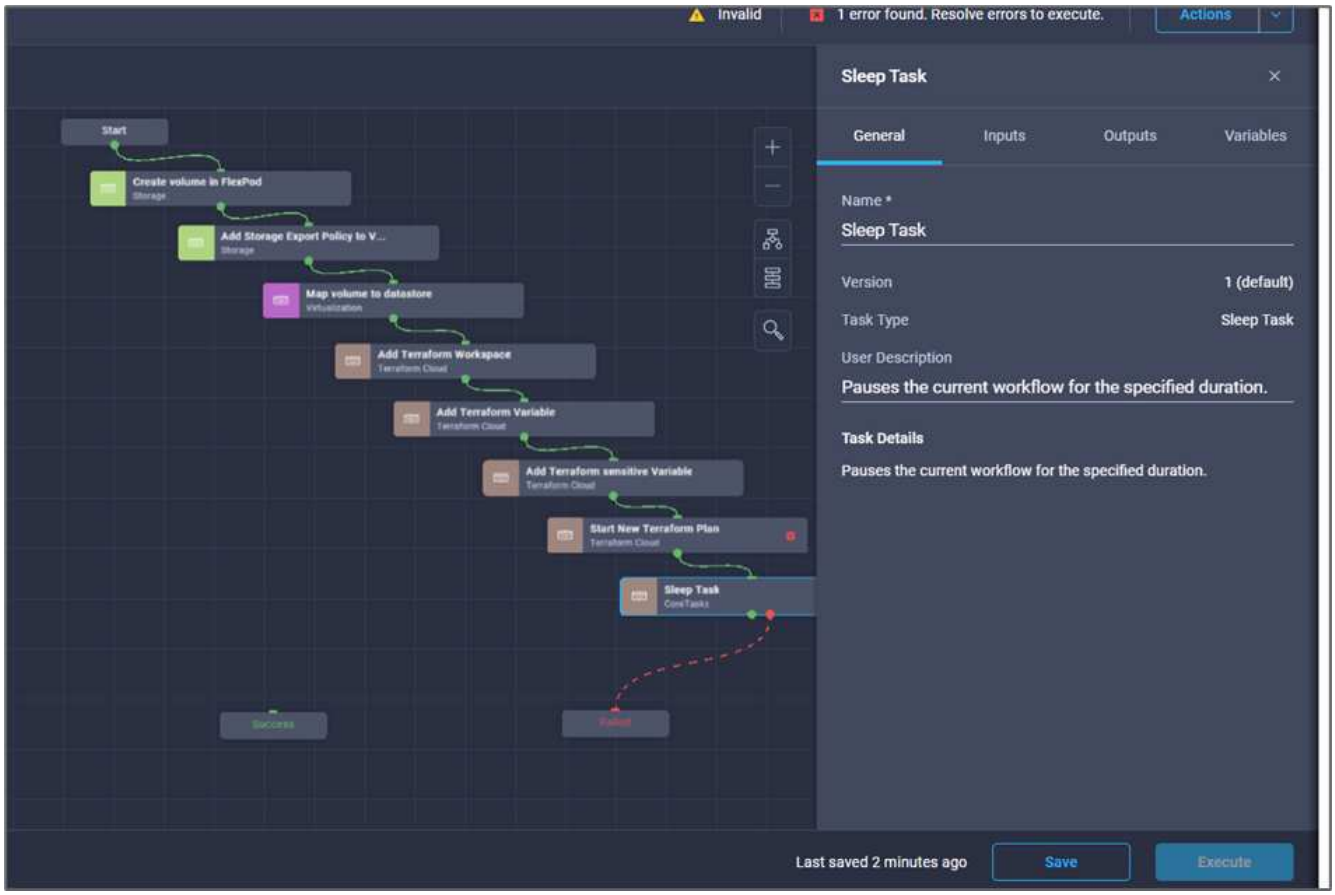
20. Fare clic su **Map** (Mappa).
21. Fare clic su **Save** (Salva).

In questo modo, viene completata l'attività di aggiunta di un piano Terraform in un account Terraform Cloud for Business. Quindi, creare un'attività di sospensione per alcuni secondi.

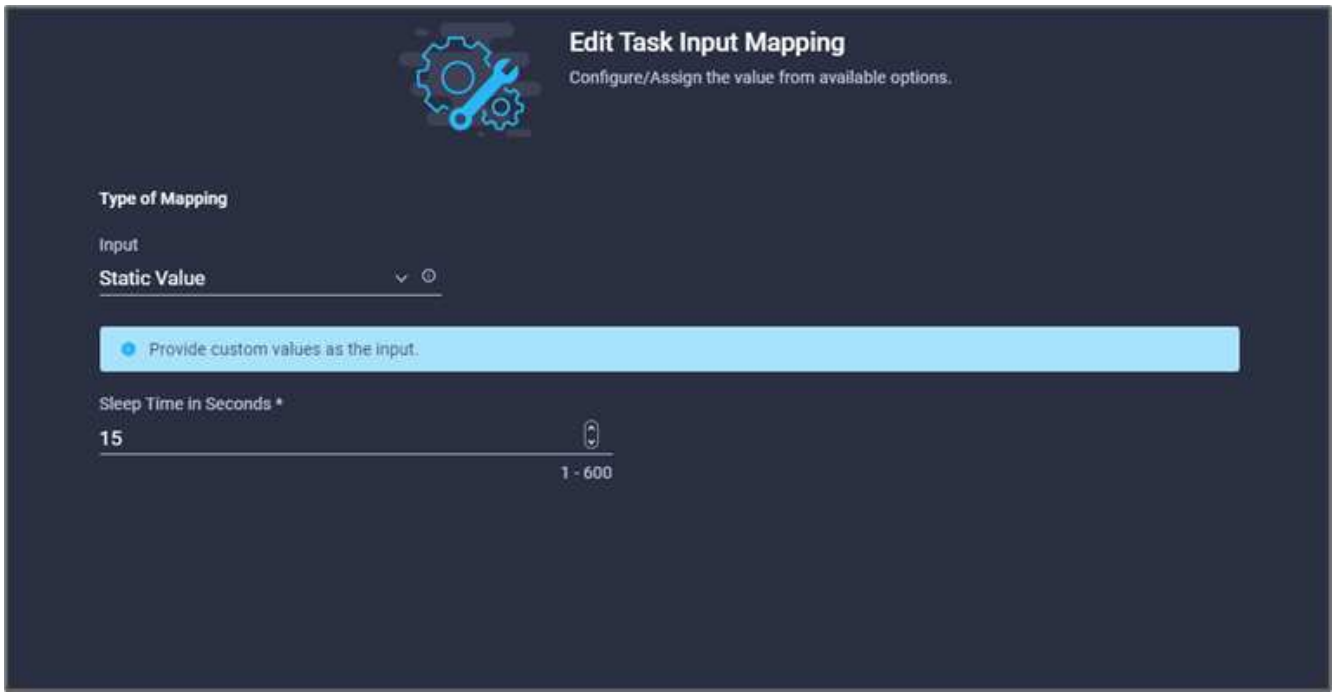
Procedura 9: Attività di sospensione per la sincronizzazione

Terraform Apply richiede RunID, che viene generato come parte dell'attività Terraform Plan. Attendere alcuni secondi tra il piano Terraform e le azioni Terraform Apply evita i problemi di tempistica.

1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare **Core Tasks > Sleep Task** dalla sezione **Tools** nell'area **Design**.
3. Utilizzare Connector per collegare le attività **Avvia nuovo piano terraform** e **sospensione attività**. Fare clic su **Save** (Salva).



4. Fare clic su **attività sospensione**. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività. In questo esempio, il nome dell'attività è **Synchronize**.
5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Sleep Time in seconds**.
7. Scegliere **valore statico** e inserire **15** in per il valore **tempo di pausa in secondi**.

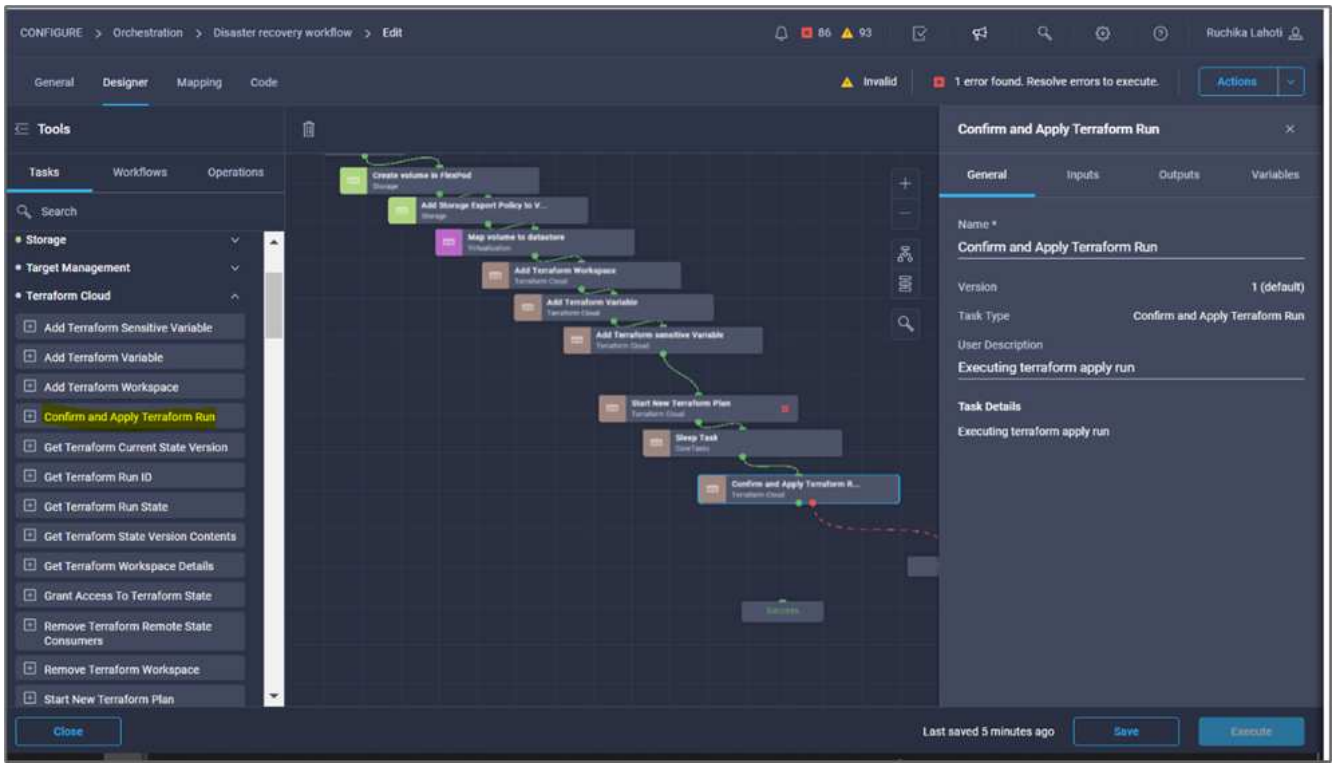


8. Fare clic su **Map** (Mappa).
9. Fare clic su **Save** (Salva).

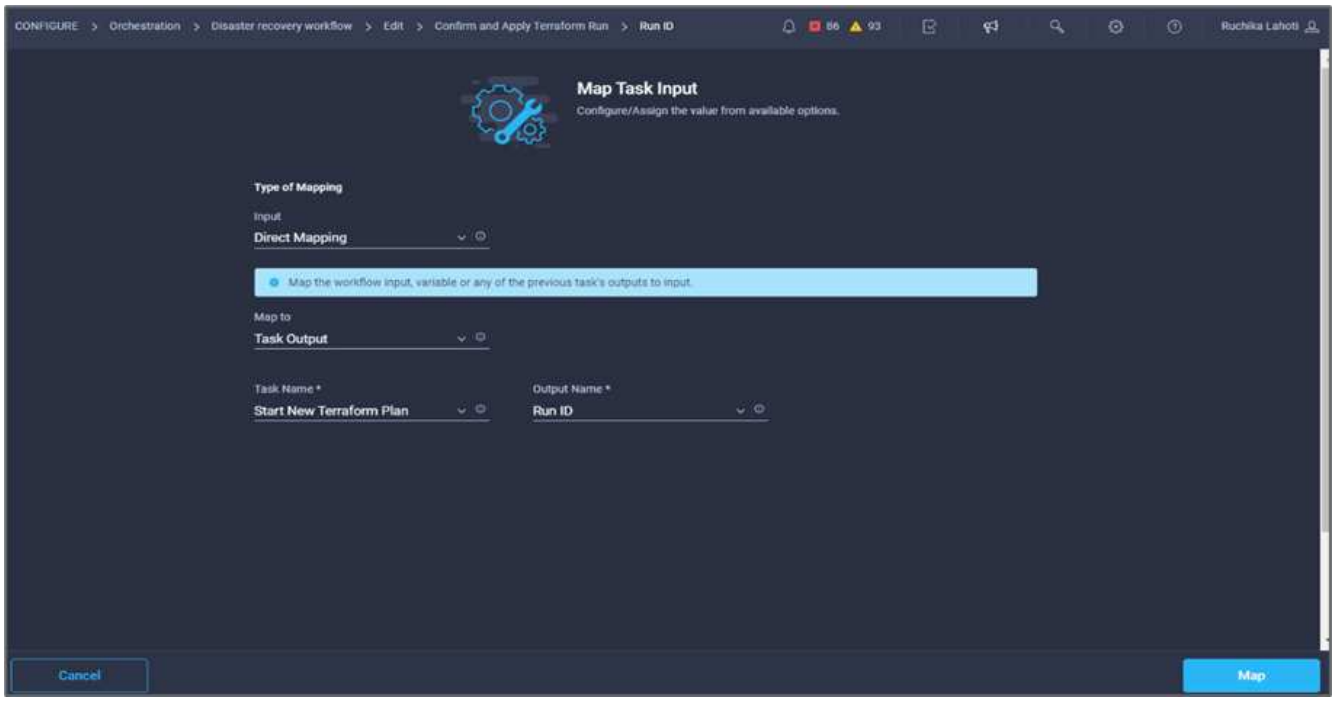
L'attività di sospensione viene completata. Quindi, creare l'ultima attività di questo flusso di lavoro, confermando e applicando Terraform Run.

Procedura 10: Confermare e applicare Terraform Run

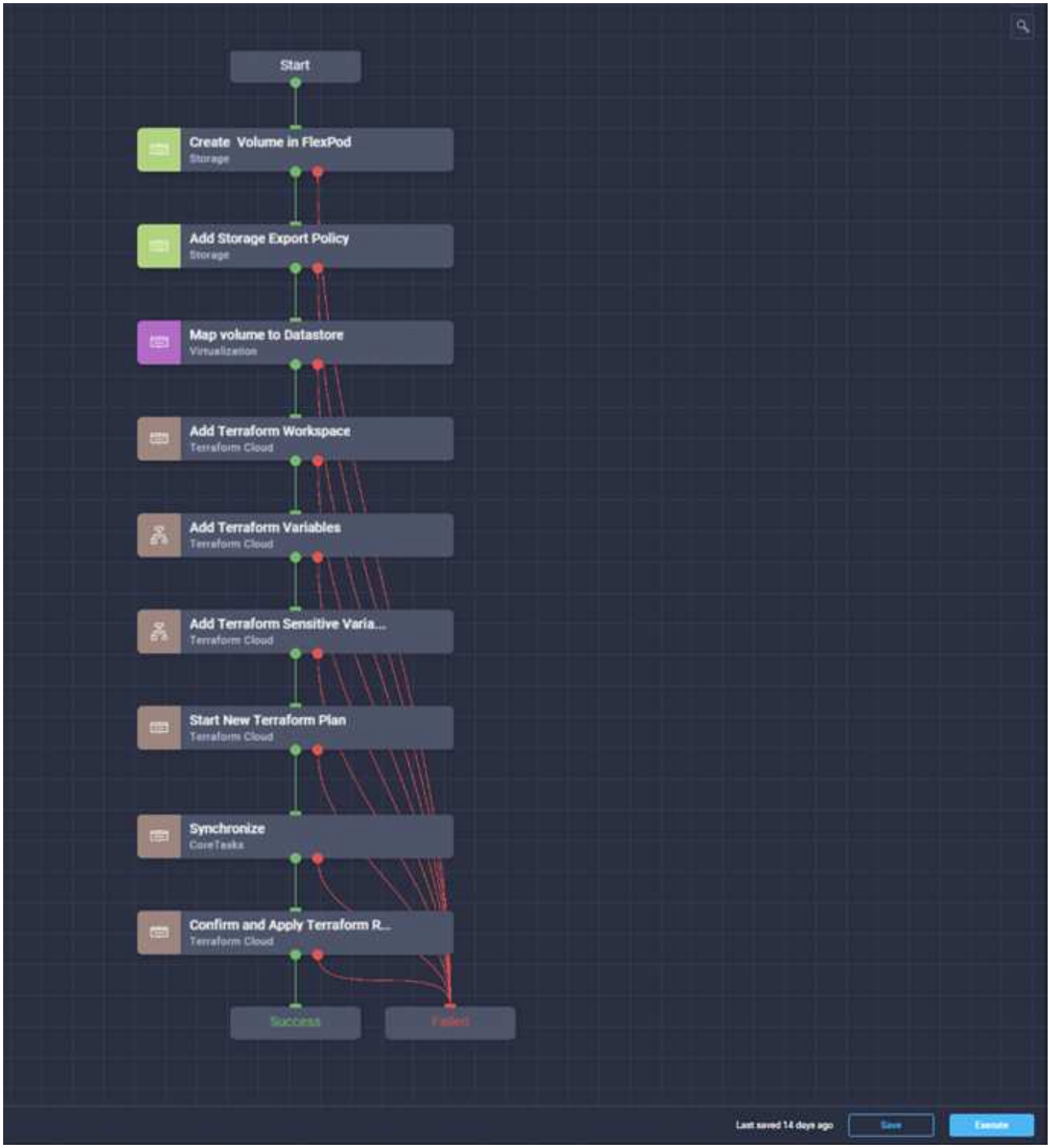
1. Selezionare la scheda **Designer** e fare clic su **Tasks** nella sezione **Tools**.
2. Trascinare l'attività **Terraform Cloud > Confirm and Apply Terraform Run** (Conferma e applica esecuzione terraform) dalla sezione **Tools** (Strumenti) nell'area **Design** (progettazione).
3. Utilizzare Connector per collegare le attività **Synchronize** e **Confirm and Apply Terraform Run**. Fare clic su **Save** (Salva).
4. Fare clic su **Conferma** e **Applica esecuzione terraform**. Nell'area **Proprietà attività**, fare clic sulla scheda **Generale**. In alternativa, è possibile modificare il nome e la descrizione dell'attività.



5. Nell'area **Task Properties**, fare clic su **Input**.
6. Fare clic su **Map** nel campo **Terraform Cloud Target**.
7. Scegliere **valore statico** e fare clic su **Seleziona destinazione cloud Terraform**. Seleziona l'account Terraform Cloud for Business aggiunto in "Configurare Cisco Intersight Service per HashiCorp Terraform"."
8. Fare clic su **Map** (Mappa).
9. Fare clic su **Map** nel campo **Run ID** (ID analisi).
10. Scegliere **Direct Mapping** e fare clic su **Task Output**.
11. Fare clic su **Nome attività** e fare clic su **Avvia nuovo piano di terraform**.
12. Fare clic su **Output Name** (Nome output), quindi su **Run ID** (ID esecuzione).



13. Fare clic su **Map** (Mappa).
14. Fare clic su **Save** (Salva).
15. Fare clic su **Auto Align Workflow** (allineamento automatico flusso di lavoro) per allineare tutte le attività. Fare clic su **Save** (Salva).



Questa operazione completa l'attività Confirm and Apply Terraform Run (Conferma e applica esecuzione terraform). Utilizzare Connector per connettersi tra le attività **Confirm and Apply Terraform Run** e le attività **Success** e **Failed**.

Procedura 11: Importazione di un flusso di lavoro creato da Cisco

Cisco Intersight Cloud Orchestrator consente di esportare i flussi di lavoro da un account Cisco Intersight al sistema e di importarli in un altro account. È stato creato un file JSON esportando il workflow creato che può essere importato nel tuo account.

In è disponibile un file JSON per il componente del flusso di lavoro "Repository di GitHub".

"Pagina successiva: Esecuzione del terraform dal controller."

Esecuzione del terraform dal controller

"Precedente: Workflow DR."

Possiamo eseguire il piano Terraform utilizzando un controller. Puoi saltare questa sezione se hai già eseguito il tuo piano Terraform utilizzando un workflow ICO.

Prerequisiti

La configurazione della soluzione inizia con una workstation di gestione che ha accesso a Internet e con un'installazione funzionante di Terraform.

È possibile trovare una guida per l'installazione di Terraform "qui".

Clonare GitHub repo

La prima fase del processo consiste nella clonazione del repo GitHub in una nuova cartella vuota della workstation di gestione. Per clonare il repository GitHub, attenersi alla seguente procedura:

1. Dalla workstation di gestione, creare una nuova cartella per il progetto. Creare una nuova cartella all'interno di questa cartella denominata `/root/snapmirror-cvo` E Clone il repo GitHub in esso.
2. Aprire un'interfaccia a riga di comando o console sulla workstation di gestione e modificare le directory nella nuova cartella appena creata.
3. Clonare l'insieme GitHub utilizzando il seguente comando:

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Modificare le directory nella nuova cartella denominata `snapmirror-cvo`.

Esecuzione terraform

- **Init.** Inizializza l'ambiente Terraform (locale). Di solito viene eseguita una sola volta per sessione.
- **Plan.** Confronta lo stato del terraform con lo stato as-in nel cloud e crea e visualizza un piano di esecuzione. Ciò non modifica la distribuzione (sola lettura).
- **Apply.** applicare il piano dalla fase del piano. In questo modo è possibile modificare l'implementazione (lettura e scrittura).
- **Destroy.** tutte le risorse gestite da questo specifico ambiente terraform.

  Per ulteriori informazioni, vedere "qui".

"Successivo: Convalida della soluzione."

Convalida della soluzione

"Precedente: Esecuzione del terraform dal controller."

In questa sezione, rivisitiamo la soluzione con un workflow di replica dei dati di esempio e effettuiamo alcune misurazioni per verificare l'integrità della replica dei dati dall'istanza di NetApp ONTAP in esecuzione in FlexPod a NetApp Cloud Volumes ONTAP in esecuzione su Google Cloud.

Abbiamo utilizzato Cisco Intersight workflow orchestrator in questa soluzione e continueremo a utilizzarla per il nostro caso d'utilizzo.

In particolare, la serie limitata di flussi di lavoro Cisco Intersight utilizzata in questa soluzione non rappresenta la serie completa di flussi di lavoro di cui Cisco Intersight è dotato. È possibile creare flussi di lavoro personalizzati in base ai requisiti specifici e attivarli da Cisco Intersight.

Per eseguire la convalida di uno scenario di disaster recovery di successo, spostare i dati da un volume in ONTAP che fa parte di FlexPod a Cloud Volumes ONTAP utilizzando SnapMirror. Quindi, puoi tentare di accedere ai dati dall'istanza di calcolo del cloud di Google seguita da un controllo dell'integrità dei dati.

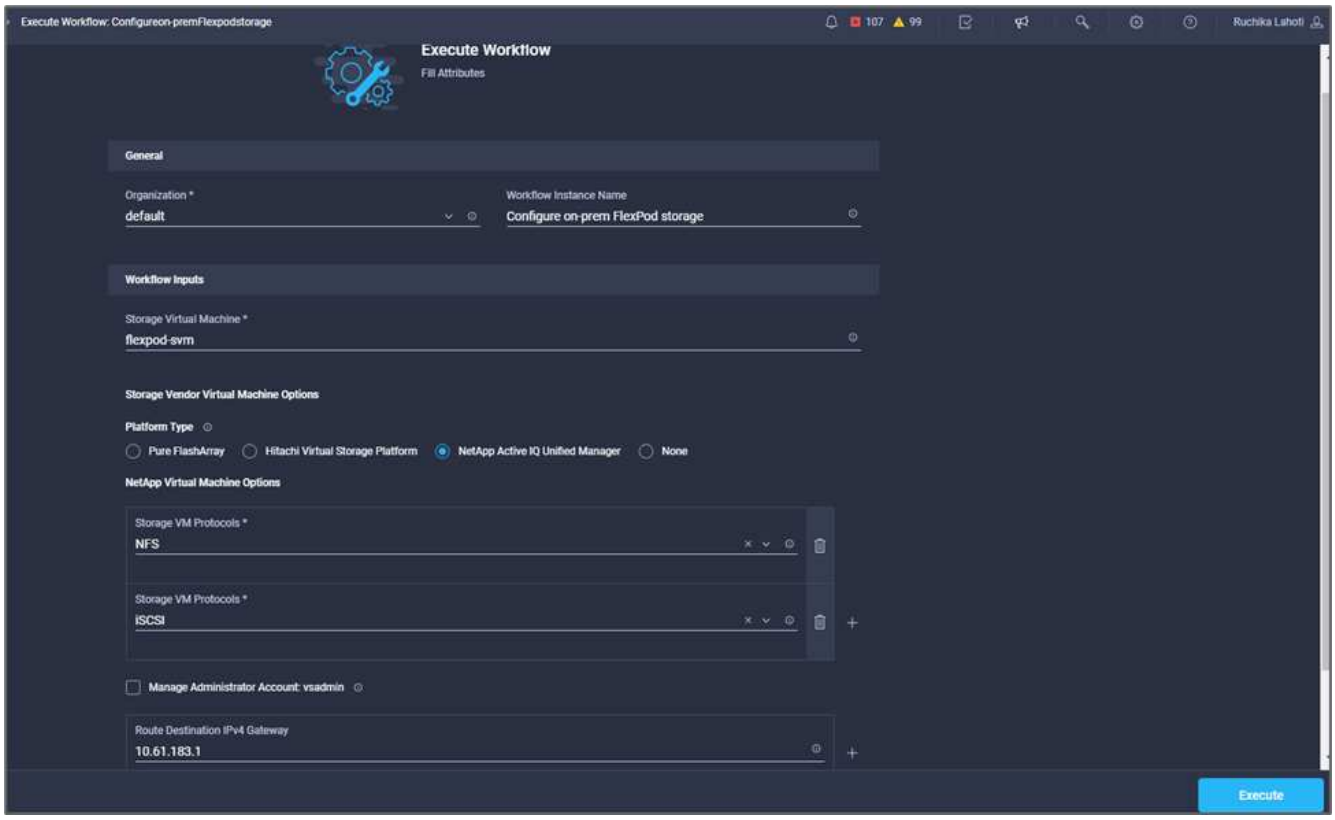
Per verificare i criteri di successo di questa soluzione, vengono utilizzati i seguenti passaggi di alto livello:

1. Generare un checksum SHA256 nel set di dati di esempio presente in un volume ONTAP in FlexPod.
2. Impostare una relazione di SnapMirror tra ONTAP in FlexPod e Cloud Volumes ONTAP.
3. Replicare il set di dati di esempio da FlexPod a Cloud Volumes ONTAP.
4. Interrompere la relazione di SnapMirror e promuovere il volume in Cloud Volumes ONTAP alla produzione.
5. Mappare il volume Cloud Volumes ONTAP con il dataset in un'istanza di calcolo in Google Cloud.
6. Generare un checksum SHA256 nel set di dati di esempio in Cloud Volumes ONTAP.
7. Confrontare il checksum sull'origine e sulla destinazione; presumibilmente, i checksum su entrambi i lati corrispondono.

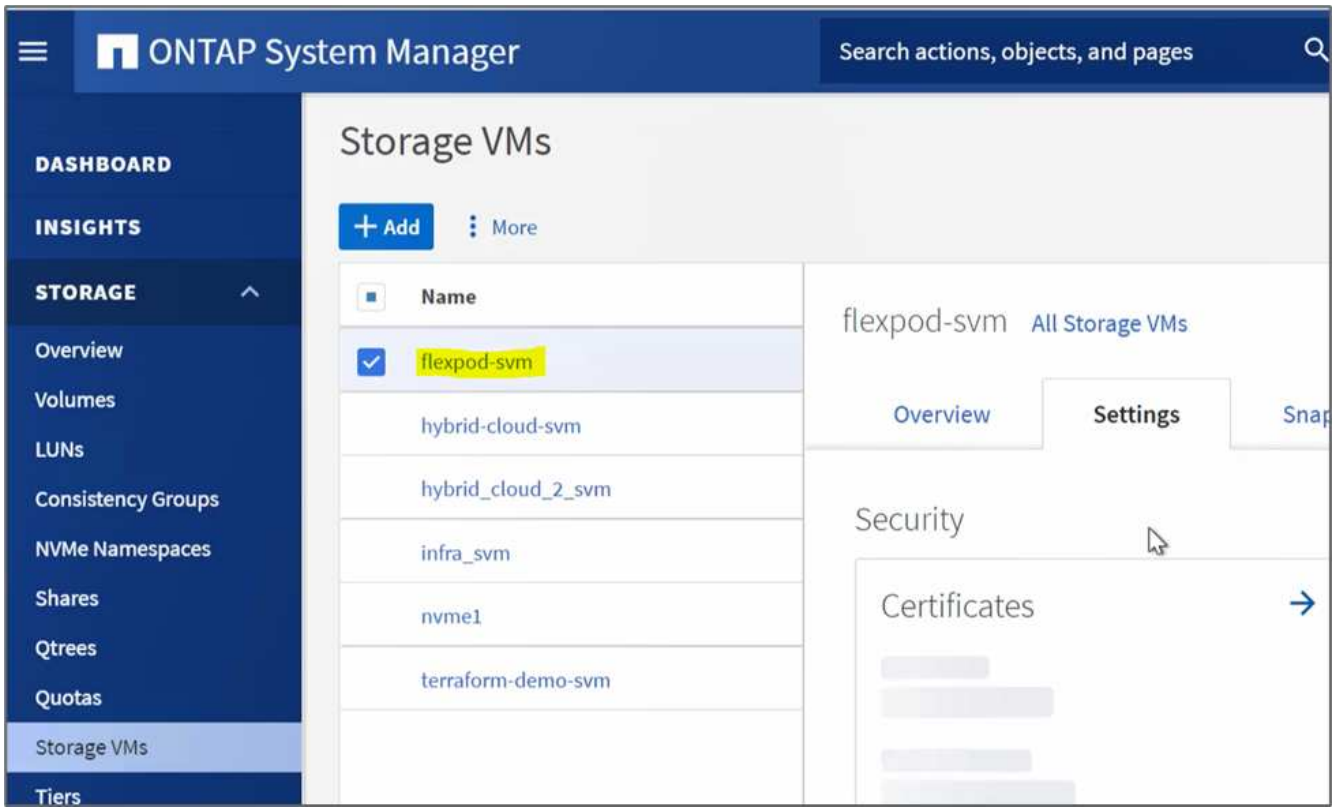
Per eseguire il flusso di lavoro on-premise, attenersi alla seguente procedura:

1. Crea un workflow in Intersight per FlexPod on-premise.

2. Fornire gli input richiesti ed eseguire il workflow.

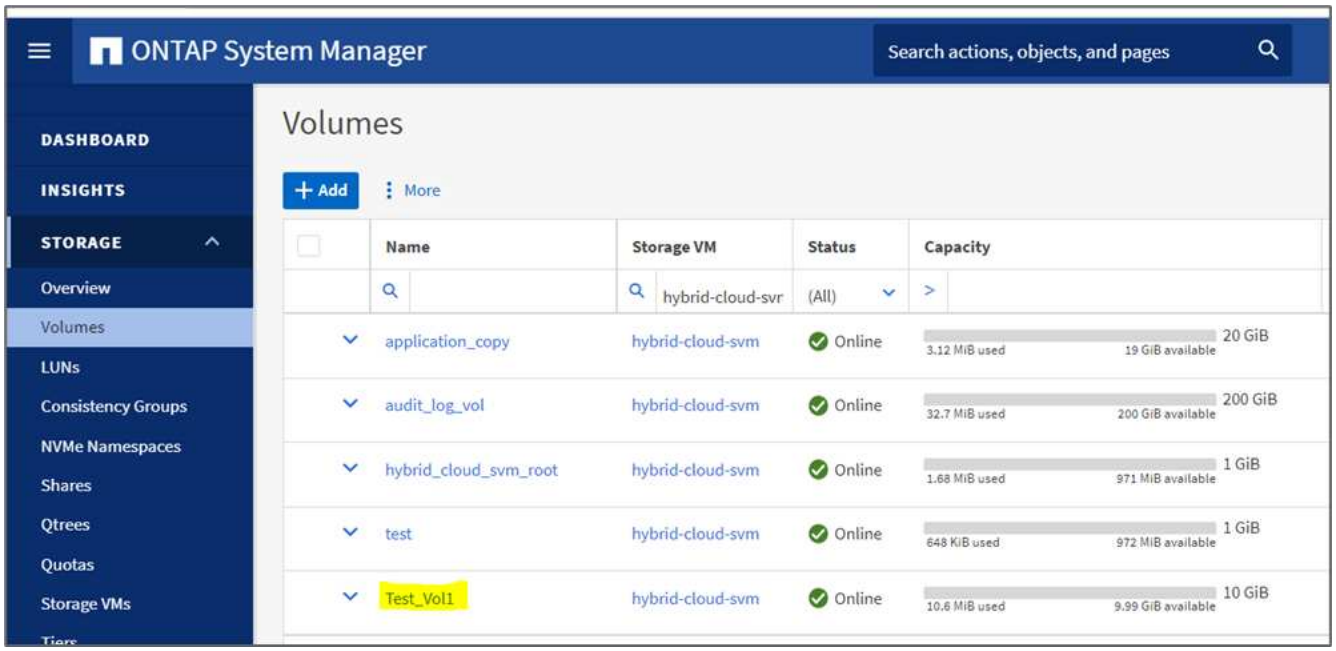


3. Verificare la SVM appena creata in System Manager.



4. Creare ed eseguire un altro flusso di lavoro di disaster recovery per creare un volume in FlexPod on-premise e stabilire una relazione SnapMirror tra questo volume in FlexPod e Cloud Volumes ONTAP.

5. Verificare il volume appena creato in ONTAP System Manager.

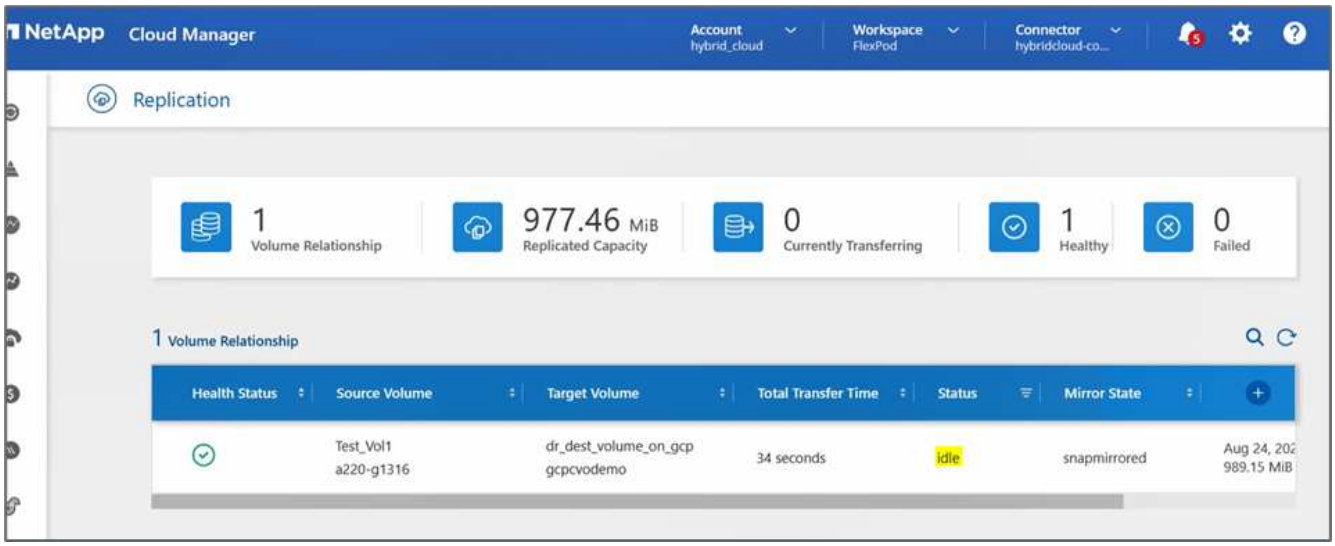


6. Montare lo stesso volume NFS su una macchina virtuale on-premise, quindi copiare il set di dati di esempio ed eseguire il checksum.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

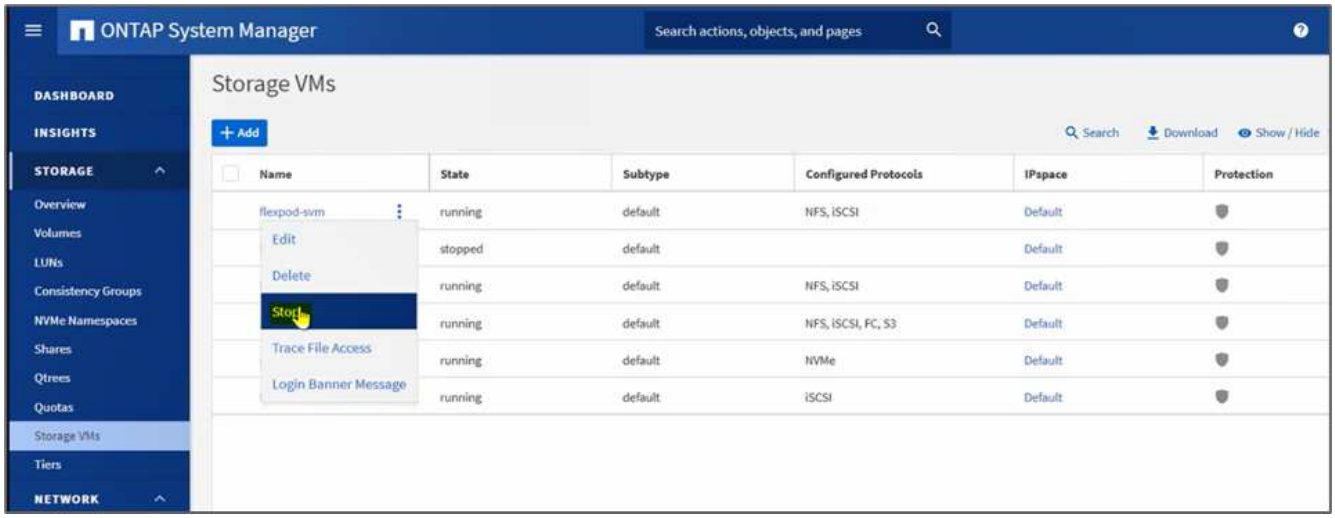
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Controllare lo stato della replica in Cloud Manager. Il trasferimento dei dati può richiedere alcuni minuti in base alle dimensioni dei dati. Al termine, lo stato di SnapMirror sarà **Idle**.

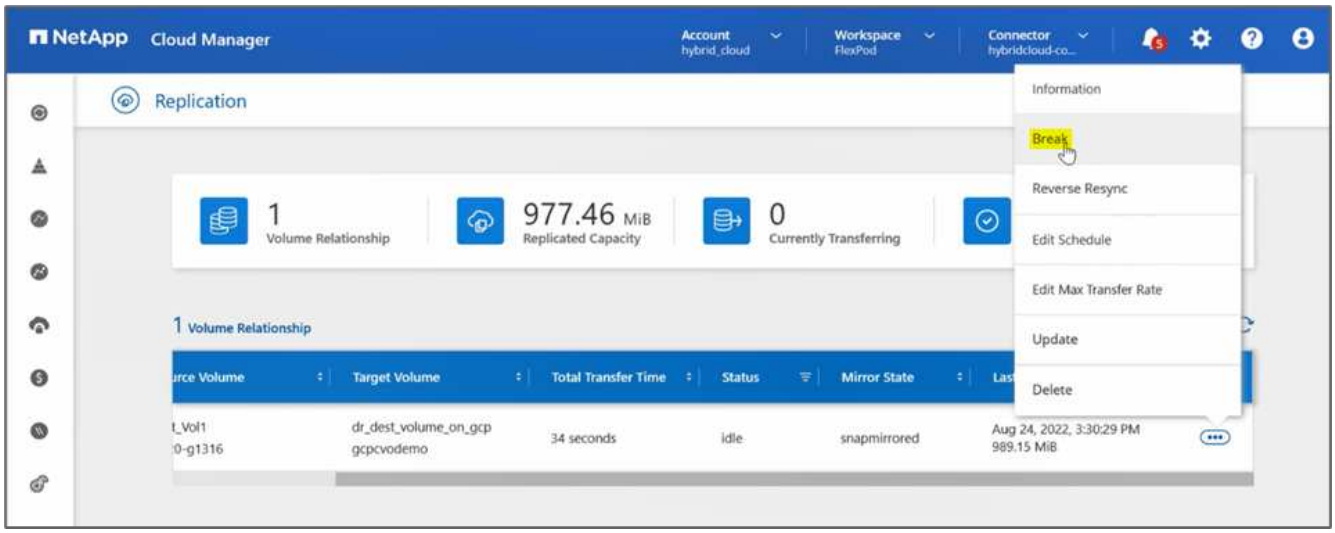


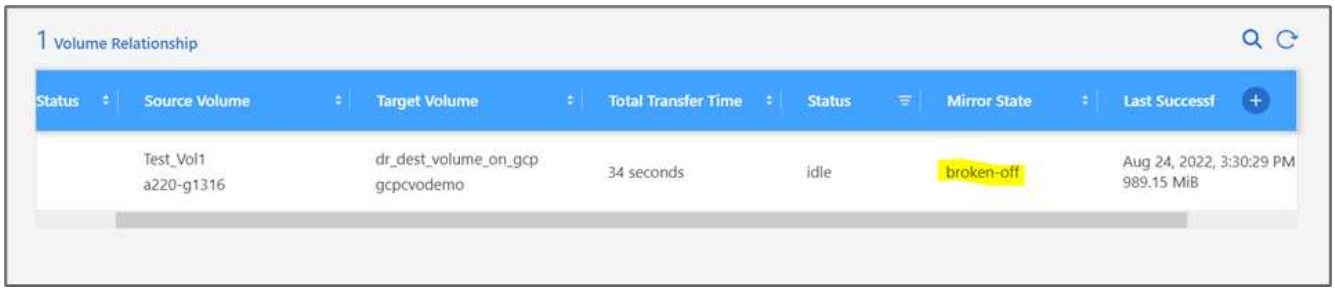
8. Una volta completato il trasferimento dei dati, simulare un disastro sul lato di origine arrestando la SVM che ospita `Test_vol1` volume.

   Dopo l'arresto di SVM, il `Test_vol1` Il volume non è visibile in Cloud Manager.

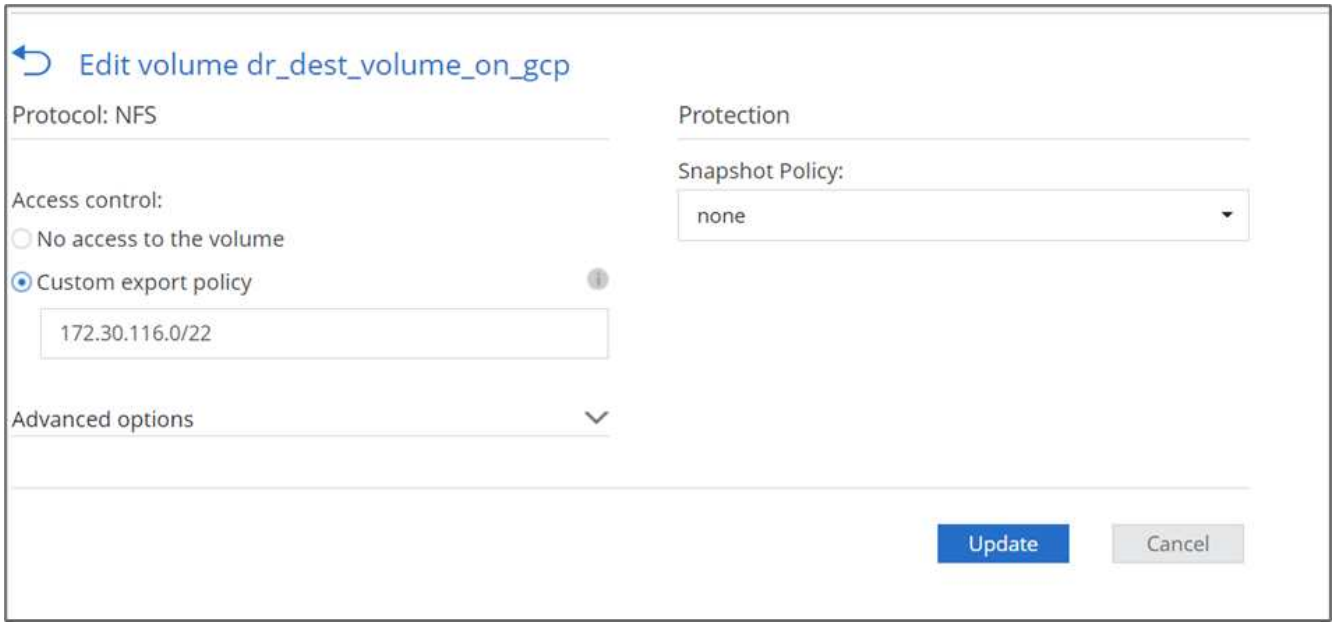


9. Interrompere la relazione di replica e promuovere il volume di destinazione Cloud Volumes ONTAP in produzione.

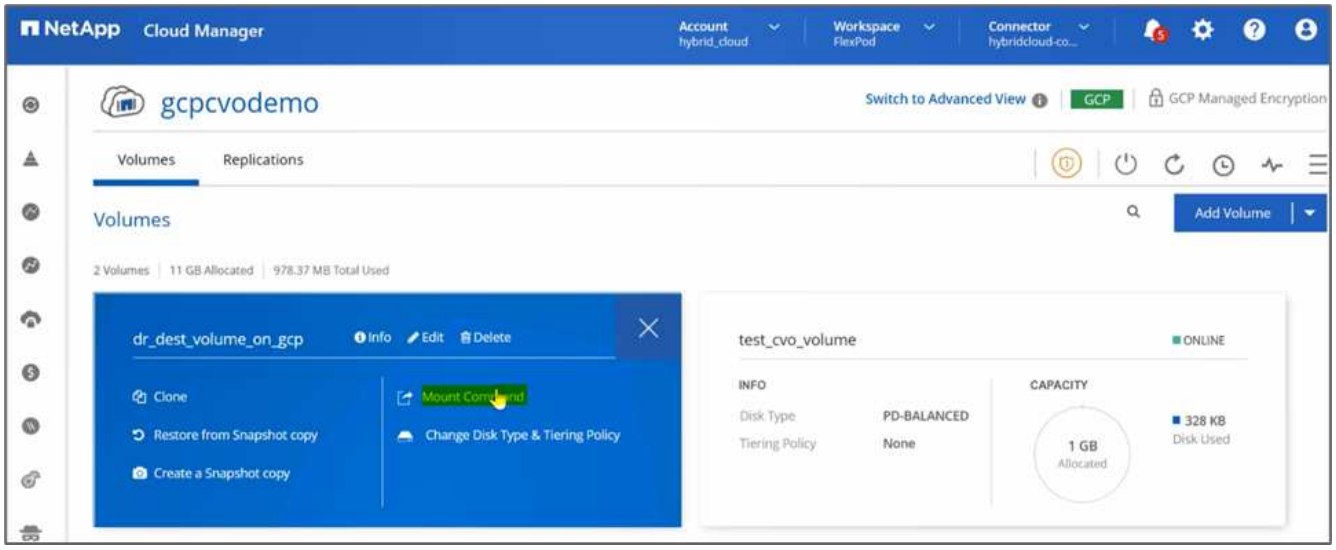




10. Modificare il volume e abilitare l'accesso client associandolo a un criterio di esportazione.



11. Ottenere il comando mount pronto all'uso per il volume.



12. Montare il volume su un'istanza di calcolo, verificare che i dati siano presenti nel volume di destinazione e generare il checksum SHA256 di `sample_dataset_2GB` file.

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Confrontare i valori del checksum sia in corrispondenza dell'origine (FlexPod) che in corrispondenza della destinazione (Cloud Volumes ONTAP).
14. I checksum corrispondono all'origine e alla destinazione.

È possibile confermare che la replica dei dati dall'origine alla destinazione sia stata completata correttamente e che l'integrità dei dati sia stata mantenuta. Questi dati possono ora essere consumati in modo sicuro dalle applicazioni per servire i client mentre il sito di origine passa attraverso il ripristino.

"Prossimo: Conclusione."

Conclusione

"Precedente: Convalida della soluzione."

In questa soluzione, il servizio dati cloud NetApp, Cloud Volumes ONTAP e l'infrastruttura del data center FlexPod sono stati utilizzati per creare una soluzione di DR con un cloud pubblico basato su Cisco Intersight Cloud Orchestrator. La soluzione FlexPod si è evoluta costantemente per consentire ai clienti di modernizzare le proprie applicazioni e i processi di business delivery. Con questa soluzione, è possibile creare un piano BCDR con il cloud pubblico come punto di accesso per un piano di disaster recovery transitorio o a tempo pieno, mantenendo al contempo bassi i costi della soluzione di disaster recovery.

La replica dei dati tra FlexPod on-premise e NetApp Cloud Volumes ONTAP è stata gestita dalla comprovata tecnologia SnapMirror, ma è anche possibile selezionare altri strumenti di trasferimento e sincronizzazione dei dati NetApp come Cloud Sync per i requisiti di mobilità dei dati. Sicurezza dei dati in volo grazie alle tecnologie di crittografia integrate basate su TLS/AES.

Sia che si disponga di un piano di DR temporaneo per un'applicazione o di un piano di DR a tempo pieno per un'azienda, il portfolio di prodotti utilizzati in questa soluzione può soddisfare entrambi i requisiti su larga scala. Basato su Cisco Intersight Workflow Orchestrator, lo stesso può essere automatizzato con flussi di lavoro predefiniti che non solo eliminano la necessità di ricostruire i processi, ma accelerano anche l'implementazione di un piano BCDR.

La soluzione consente la gestione on-premise di FlexPod e la replica dei dati in un cloud ibrido in modo molto semplice e conveniente con l'automazione e l'orchestrazione fornite da Cisco Intersight Cloud Orchestrator.

Dove trovare ulteriori informazioni

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

GitHub

- Tutte le configurazioni terraform utilizzate

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- File JSON per l'importazione dei flussi di lavoro

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centro assistenza Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentazione di Cisco Intersight Cloud Orchestrator:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Cisco Intersight Service per documentazione HashiCorp Terraform

"https://intersight.com/help/saas/features/terraform_cloud/admin"

- Scheda informativa su Cisco Intersight

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Scheda informativa di Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Scheda informativa di Cisco Intersight Service per HashiCorp Terraform

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

  "FlexPod Datacenter con Cisco UCS 4.2(1) in modalità gestita UCS, VMware vSphere 7.0 U2 e guida alla progettazione di NetApp ONTAP 9.9"

- Data center FlexPod con Cisco UCS serie X.

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

Interoperabilità

- Tool di matrice di interoperabilità NetApp

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

- Cisco UCS hardware and Software Interoperability Tool

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

- Guida alla compatibilità VMware

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

Documenti di riferimento NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

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

- Calcolatore del TCO di Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Cloud Assessment Tool

  https://cloud.netapp.com/assessments

- Cloud ibrido NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentazione API di Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Risoluzione dei problemi

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Cloud terraformo

  "https://www.terraform.io/cloud"

- Documentazione terraform

  "https://www.terraform.io/docs/"

- Registro di NetApp Cloud Manager

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- Alta disponibilità ONTAP per GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- Requisito GCP

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Cloud ibrido FlexPod con NetApp Astra e Cisco Intersight per Red Hat OpenShift

TR-4936: Cloud ibrido FlexPod con NetApp Astra e Cisco Intersight per Red Hat OpenShift

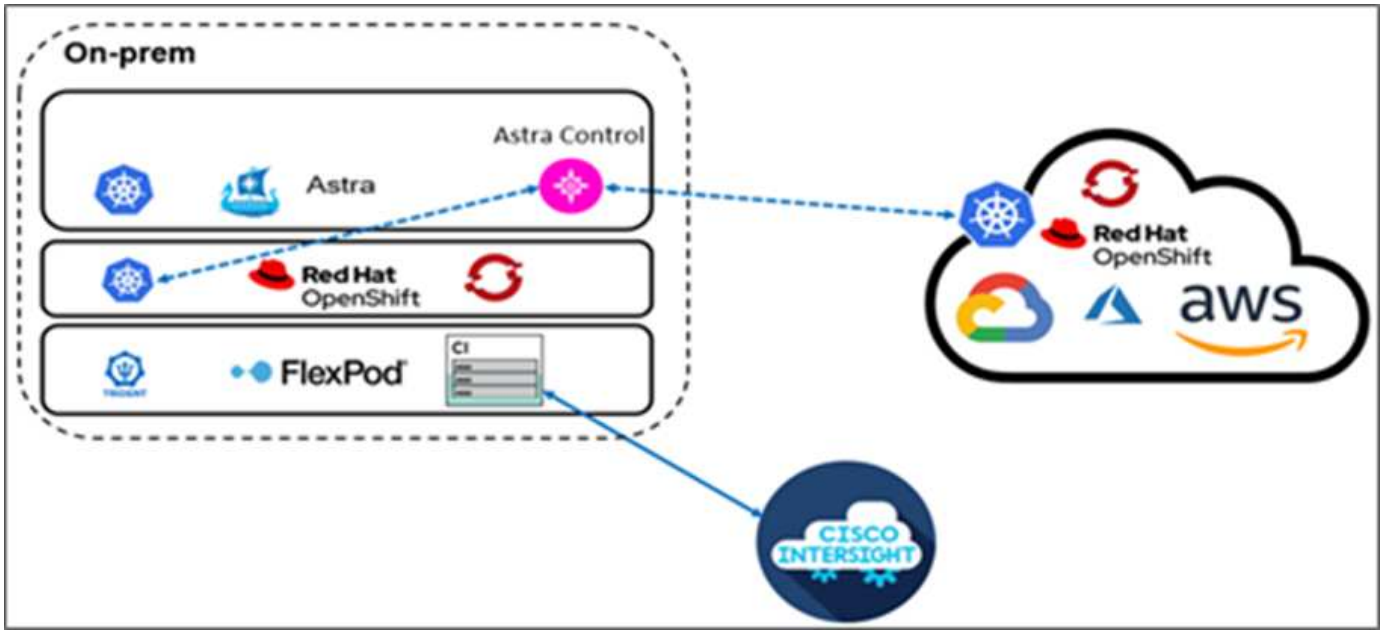
Abhinav Singh

Introduzione

Mentre container e Kubernetes diventano la scelta de facto per lo sviluppo, l'implementazione, l'esecuzione, la gestione e la scalabilità delle applicazioni containerizzate, le aziende eseguono sempre più applicazioni business-critical su di esse. Le applicazioni business-critical dipendono in larga misura dallo stato. Un'applicazione stateful dispone di informazioni sullo stato, sui dati e sulla configurazione associate e dipende dalle transazioni dei dati precedenti per eseguire la propria logica di business. Le applicazioni business-critical eseguite su Kubernetes continuano ad avere requisiti di disponibilità e business continuity come le applicazioni tradizionali. Un'interruzione del servizio può compromettere seriamente la perdita di ricavi, produttività e reputazione dell'azienda. Pertanto, è molto importante proteggere, ripristinare e spostare rapidamente e facilmente i workload Kubernetes all'interno e tra cluster, data center on-premise e ambienti cloud ibridi. Le aziende hanno riscontrato i vantaggi derivanti dal passaggio del business a un modello di cloud ibrido e la modernizzazione delle applicazioni a un fattore di forma nativo del cloud è un fattore di importanza fondamentale.

Questo report tecnico riunisce il centro di controllo Astra di NetApp con la piattaforma container OpenShift di Red Hat su una soluzione di infrastruttura convergente FlexPod e si estende ai servizi web Amazon (AWS) per formare un data center di cloud ibrido. Sulla base della familiarità con "FlexPod e Red Hat OpenShift", Questo documento illustra NetApp Astra Control Center, a partire dall'installazione, dalla configurazione, dai flussi di lavoro per la protezione delle applicazioni e dalla migrazione delle applicazioni tra on-premise e cloud. Vengono inoltre illustrati i vantaggi delle funzionalità di gestione dei dati application-aware (come backup e recovery, business continuity) quando si utilizza NetApp Astra Control Center per le applicazioni containerizzate eseguite su Red Hat OpenShift.

La figura seguente illustra la panoramica della soluzione.



Pubblico

Il pubblico di riferimento di questo documento comprende Chief Technology Officer (CTO), sviluppatori di applicazioni, architetti di soluzioni cloud, tecnici dell'affidabilità del sito (SRE), ingegneri DevOps, ITOps e team di servizi professionali che si occupano della progettazione, dell'hosting e della gestione delle applicazioni containerizzate.

NetApp Astra Control – casi di utilizzo chiave

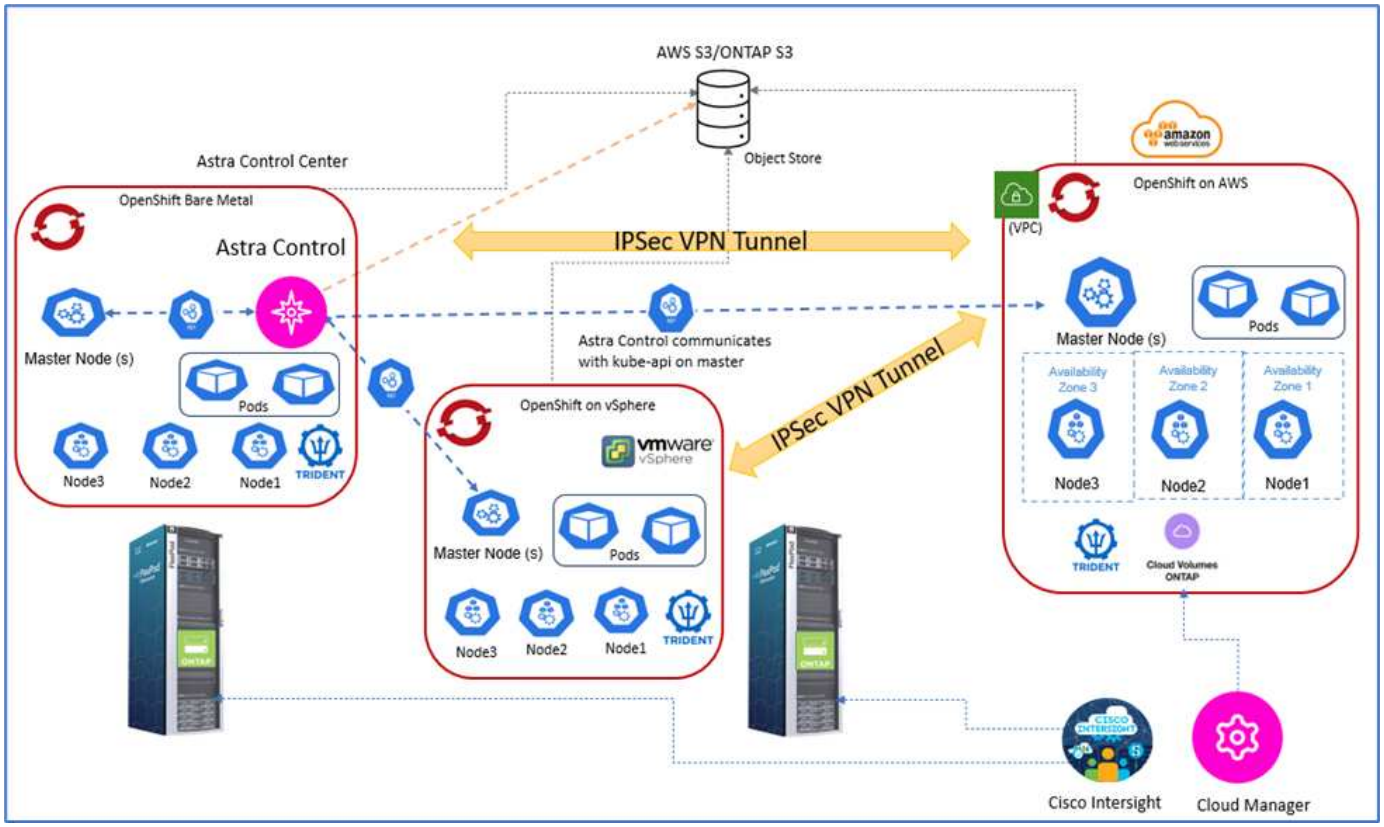
NetApp Astra Control mira a semplificare la protezione delle applicazioni per i clienti che si occupano di microservizi nativi del cloud:

- **Rappresentazione applicativa point-in-time (PIT) con snapshot.** con Astra Control è possibile creare snapshot end-to-end delle applicazioni containerizzate che includono i dettagli di configurazione dell'applicazione in esecuzione su Kubernetes e lo storage persistente associato. In caso di incidente, è possibile ripristinare le applicazioni a uno stato sicuramente funzionante facendo clic sul pulsante.
- **Backup completo dell'applicazione.** con Astra Control è possibile eseguire un backup completo dell'applicazione in base a una pianificazione predefinita che può essere utilizzata per ripristinare l'applicazione sullo stesso cluster K8s o su un cluster K8s diverso on-demand in modo automatizzato.
- **Portabilità dell'applicazione e migrazione con cloni.** con Astra Control è possibile clonare un'intera applicazione insieme ai relativi dati da un cluster Kubernetes a un altro o all'interno dello stesso cluster K8s. Questa funzionalità consente inoltre di eseguire il porting o la migrazione di un'applicazione tra cluster K8s, indipendentemente da dove si trovano i cluster (è sufficiente eliminare l'istanza dell'applicazione di origine dopo la clonazione).
- **Personalizza la coerenza delle applicazioni.** con Astra Control puoi assumere il controllo della definizione degli stati di quiesce delle applicazioni sfruttando gli hook di esecuzione. Rilasciare i ganci di esecuzione 'pre' e 'post' nei flussi di lavoro di snapshot e backup, le applicazioni verranno interrotti a modo proprio prima di eseguire un'istantanea o un backup.
- **Automatizzare il disaster recovery (DR) a livello applicativo.** con Astra Control è possibile configurare un piano di disaster recovery per la business continuity (BCDR) per le applicazioni containerizzate. NetApp SnapMirror viene utilizzato nel back-end e l'implementazione completa del flusso di lavoro DR viene automatizzata.

Topologia della soluzione

In questa sezione viene descritta la topologia logica della soluzione.

La seguente illustrazione rappresenta la topologia della soluzione che comprende l'ambiente on-premise di FlexPod con cluster di piattaforme container OpenShift e un cluster di piattaforme container OpenShift autogestiti su AWS con NetApp Cloud Volumes ONTAP, Cisco Intersight e la piattaforma SaaS di NetApp Cloud Manager.



Il primo cluster della piattaforma container OpenShift è un'installazione bare-metal su FlexPod, il secondo cluster della piattaforma container OpenShift è implementato su VMware vSphere in esecuzione su FlexPod e il terzo cluster della piattaforma container OpenShift è implementato come "cluster privato" In un cloud privato virtuale (VPC) esistente su AWS come infrastruttura autogestiva.

In questa soluzione, FlexPod è connesso ad AWS attraverso una VPN sito-sito, tuttavia i clienti possono anche utilizzare le implementazioni di connessione diretta per estendersi a un cloud ibrido. Cisco Intersight viene utilizzato per gestire i componenti dell'infrastruttura FlexPod.

In questa soluzione, Astra Control Center gestisce l'applicazione containerizzata ospitata sul cluster della piattaforma container OpenShift in esecuzione su FlexPod e AWS. Astra Control Center è installato sull'istanza bare-metal di OpenShift in esecuzione su FlexPod. Astra Control comunica con kube-api sul nodo master e controlla continuamente il cluster Kubernetes per eventuali modifiche. Tutte le nuove applicazioni aggiunte al cluster K8s vengono automaticamente rilevate e rese disponibili per la gestione.

Le rappresentazioni PIT delle applicazioni containerizzate possono essere acquisite come snapshot utilizzando Astra Control Center. Le snapshot delle applicazioni possono essere attivate tramite una policy di protezione pianificata o on-demand. Per le applicazioni supportate da Astra, lo snapshot è coerente con il crash. Uno snapshot applicativo costituisce uno snapshot dei dati dell'applicazione nei volumi persistenti e dei metadati dell'applicazione delle varie risorse Kubernetes associate a tale applicazione.

È possibile creare una copia di backup completa di un'applicazione utilizzando Astra Control utilizzando una pianificazione di backup predefinita o on-demand. Viene utilizzato uno storage a oggetti per memorizzare il backup dei dati dell'applicazione. NetApp ONTAP S3, NetApp StorageGRID e qualsiasi implementazione generica S3 possono essere utilizzati come archivio di oggetti.

"Successivo: Componenti della soluzione."

Componenti della soluzione

"Precedente: Panoramica della soluzione."

FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp ONTAP, networking Cisco Nexus, storage networking Cisco MDS, Cisco Unified Computing System (Cisco UCS). Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare più configurazioni.

Controllo Astra

Astra Control offre servizi di protezione dei dati application-aware per applicazioni native del cloud ospitate sia in cloud pubblici che on-premise. Astra Control offre funzionalità di protezione dei dati, disaster recovery e migrazione per le applicazioni containerizzate in esecuzione su Kubernetes.

Caratteristiche

Astra Control offre funzionalità critiche per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes:

- Gestire automaticamente lo storage persistente
- Creazione di snapshot e backup on-demand coerenti con l'applicazione
- Operazioni automatizzate di backup e snapshot basate su policy
- Migrare le applicazioni e i dati associati da un cluster Kubernetes a un altro in una configurazione di cloud ibrido
- Clonare un'applicazione nello stesso cluster K8s o in un altro cluster K8s
- Visualizzare lo stato di protezione dell'applicazione
- Fornisce un'interfaccia utente grafica e un elenco completo di API REST per implementare tutti i flussi di lavoro di protezione da strumenti interni esistenti.

Astra Control offre un singolo pannello di visualizzazione per le applicazioni containerizzate che include informazioni sulle risorse associate create sul cluster Kubernetes. Puoi visualizzare tutti i tuoi cluster, tutte le tue applicazioni, in tutti i cloud o in tutti i data center utilizzando un unico portale. È possibile utilizzare le API di controllo Astra in tutti gli ambienti (cloud pubblici o on-premise) per implementare i flussi di lavoro di gestione dei dati.

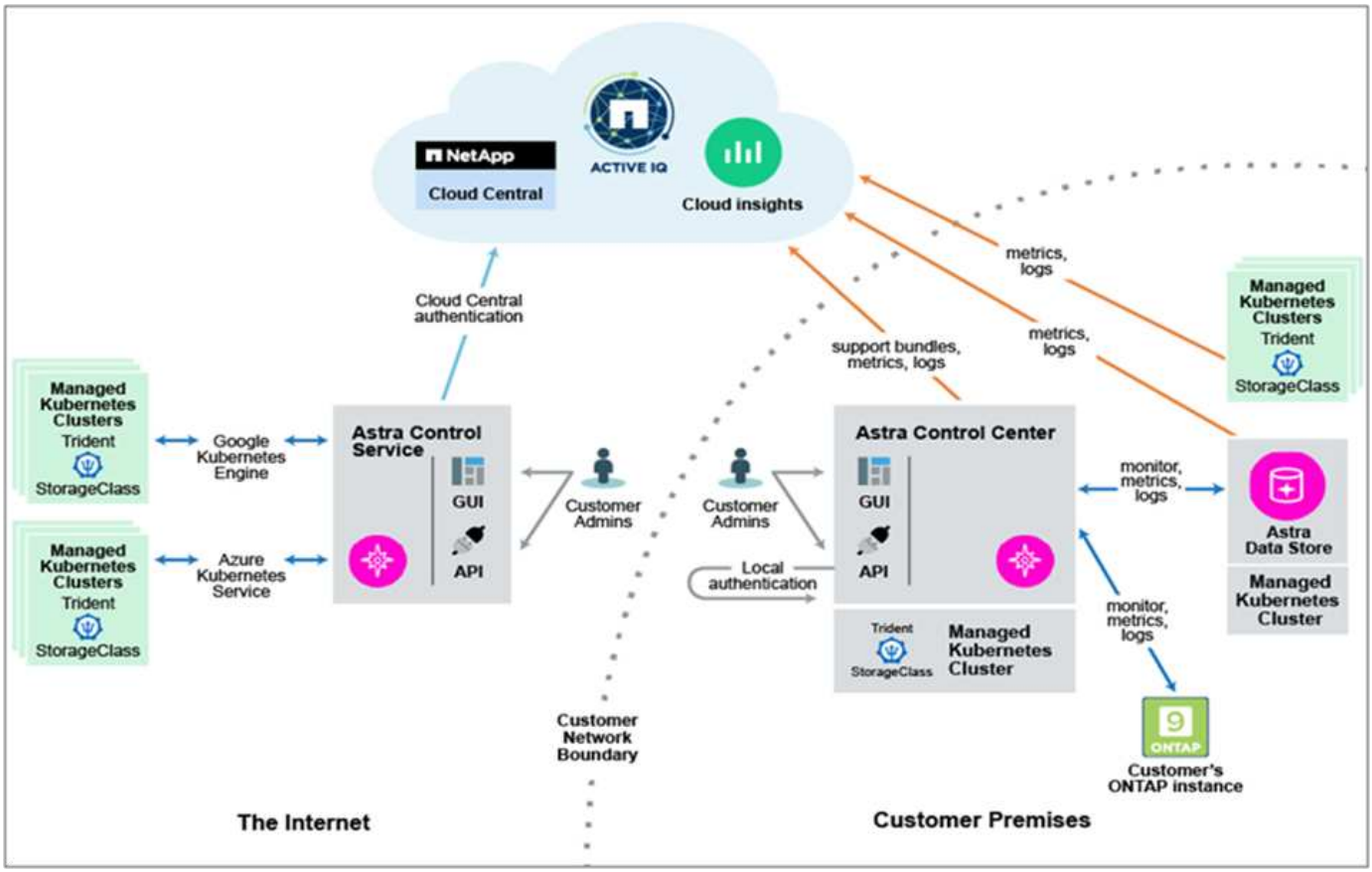
Modelli di consumo Astra Control

Astra Control è disponibile in due modelli di consumo:

- **Astra Control Service.** un servizio completamente gestito ospitato da NetApp che fornisce la gestione dei dati application-aware dei cluster Kubernetes in Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS).
- **Astra Control Center.** Software autogestito che fornisce la gestione dei dati applicativa dei cluster Kubernetes in esecuzione nel tuo ambiente di cloud ibrido e on-premise.

Questo report tecnico sfrutta Astra Control Center per la gestione delle applicazioni native del cloud eseguite su Kubernetes.

L'immagine seguente mostra l'architettura di Astra Control.



Astra Trident

Astra Trident è uno storage orchestrator open-source completamente supportato per container e distribuzioni Kubernetes. È stato progettato fin dall'inizio per soddisfare le esigenze di persistenza delle applicazioni containerizzate utilizzando interfacce standard di settore, come "CSI (Container Storage Interface)". Con Astra Trident, i microservizi e le applicazioni containerizzate possono sfruttare i servizi storage di livello Enterprise forniti dal portfolio di sistemi storage NetApp.

Astra Trident viene distribuito su cluster Kubernetes come pod e fornisce servizi di orchestrazione dinamica dello storage per i carichi di lavoro Kubernetes. Consente alle applicazioni containerizzate di utilizzare in modo rapido e semplice l'archiviazione persistente dall'ampio portfolio di NetApp, che include NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, Cloud e Amazon FSx for NetApp ONTAP), il software NetApp Element (NetApp SolidFire) e il servizio Azure NetApp Files . In un ambiente FlexPod , Astra Trident viene utilizzato per effettuare il provisioning e gestire dinamicamente volumi persistenti per contenitori supportati da volumi NetApp FlexVol e LUN ospitati su una piattaforma di storage ONTAP come i sistemi NetApp AFF e FAS e Cloud Volumes ONTAP. Trident svolge inoltre un ruolo fondamentale nell'implementazione degli schemi di protezione delle applicazioni forniti da Astra Control. Per maggiori informazioni su Astra Trident, vedere "Documentazione di Astra Trident."

Back-end dello storage

Per utilizzare Astra Trident, è necessario il backend dello storage supportato. Un backend Trident definisce la relazione tra Trident e un sistema storage. Spiega a Trident come comunicare con quel sistema storage e come Trident dovrebbe eseguire il provisioning dei volumi da esso. Trident offrirà automaticamente pool di storage da backend che insieme soddisfano i requisiti definiti da una classe di storage.

- Backend di storage ONTAP AFF e FAS. In qualità di piattaforma hardware e software per lo storage, ONTAP offre servizi di storage di base, supporto per più protocolli di accesso allo storage e funzionalità di gestione dello storage, come copie Snapshot e mirroring NetApp.
- Back-end dello storage Cloud Volumes ONTAP
- "Archivio dati Astra" back-end dello storage

NetApp Cloud Volumes ONTAP

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

I vantaggi principali includono:

- Sfrutta la deduplica dei dati integrata, la compressione dei dati, il thin provisioning e la clonazione per ridurre al minimo i costi dello storage.
- Garantisci l'affidabilità aziendale e le operazioni continue in caso di guasti nel tuo ambiente cloud.
- Cloud Volumes ONTAP sfrutta SnapMirror, la tecnologia di replica leader del settore di NetApp, per replicare i dati on-premise nel cloud, in modo da poter disporre facilmente di copie secondarie per diversi casi di utilizzo.
- Cloud Volumes ONTAP si integra anche con Cloud Backup Service per offrire funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cloud.
- Passa tra pool di storage on-demand a performance elevate e basse senza portare le applicazioni offline.
- Garantire la coerenza delle copie Snapshot con NetApp SnapCenter.
- Cloud Volumes ONTAP supporta la crittografia dei dati e fornisce protezione contro virus e ransomware.
- L'integrazione con Cloud Data Sense ti aiuta a comprendere il contesto dei dati e a identificare i dati sensibili.

Cloud Central

Cloud Central offre una posizione centralizzata per accedere e gestire i servizi dati cloud di NetApp. Questi servizi consentono di eseguire applicazioni critiche nel cloud, creare siti di DR automatizzati, eseguire il backup dei dati e migrare e controllare in modo efficace i dati su più cloud. Per ulteriori informazioni, vedere "Cloud Central."

Cloud Manager

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

Connettore

Connector è un'istanza che consente a Cloud Manager di gestire risorse e processi all'interno dell'ambiente di cloud pubblico. È necessario un connettore per utilizzare molte funzionalità offerte da Cloud Manager. Un connettore può essere implementato nel cloud o nella rete on-premise.

Il connettore è supportato nelle seguenti posizioni:

- AWS
- Microsoft Azure
- Google Cloud
- On-premise

Per ulteriori informazioni su Connector, vedere "questo link."

NetApp Cloud Insights

Cloud Insights, uno strumento di monitoraggio dell'infrastruttura cloud di NetApp, consente di monitorare le performance e l'utilizzo dei cluster Kubernetes gestiti dal centro di controllo Astra. Cloud Insights mette in relazione l'utilizzo dello storage con i carichi di lavoro. Quando si attiva la connessione Cloud Insights in Astra Control Center, le informazioni di telemetria vengono visualizzate nelle pagine dell'interfaccia utente di Astra Control Center.

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager consente di monitorare i cluster di storage ONTAP da un'unica interfaccia intuitiva e ridisegnata che offre intelligence basata su saggezza della community e analisi ai. Fornisce informazioni complete su operazioni, performance e attività proattive nell'ambiente di storage e nelle macchine virtuali (VM) in esecuzione sull'ambiente IT. Quando si verifica un problema con l'infrastruttura di storage, Unified Manager può notificare i dettagli del problema per identificare la causa principale. Il dashboard delle macchine virtuali offre una vista delle statistiche delle performance della macchina virtuale, in modo da poter analizzare l'intero percorso di i/o dall'host VMware vSphere fino alla rete e infine allo storage. Alcuni eventi forniscono anche azioni correttive che possono essere intraprese per risolvere il problema. È possibile configurare avvisi personalizzati per gli eventi in modo che, quando si verificano problemi, venga inviata una notifica tramite e-mail e trap SNMP. Active IQ Unified Manager consente di pianificare i requisiti di storage degli utenti prevedendo le tendenze di capacità e utilizzo per agire in modo proattivo prima che si verifichino problemi, evitando decisioni reattive a breve termine che possono portare a ulteriori problemi a lungo termine.

Cisco Intersight

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

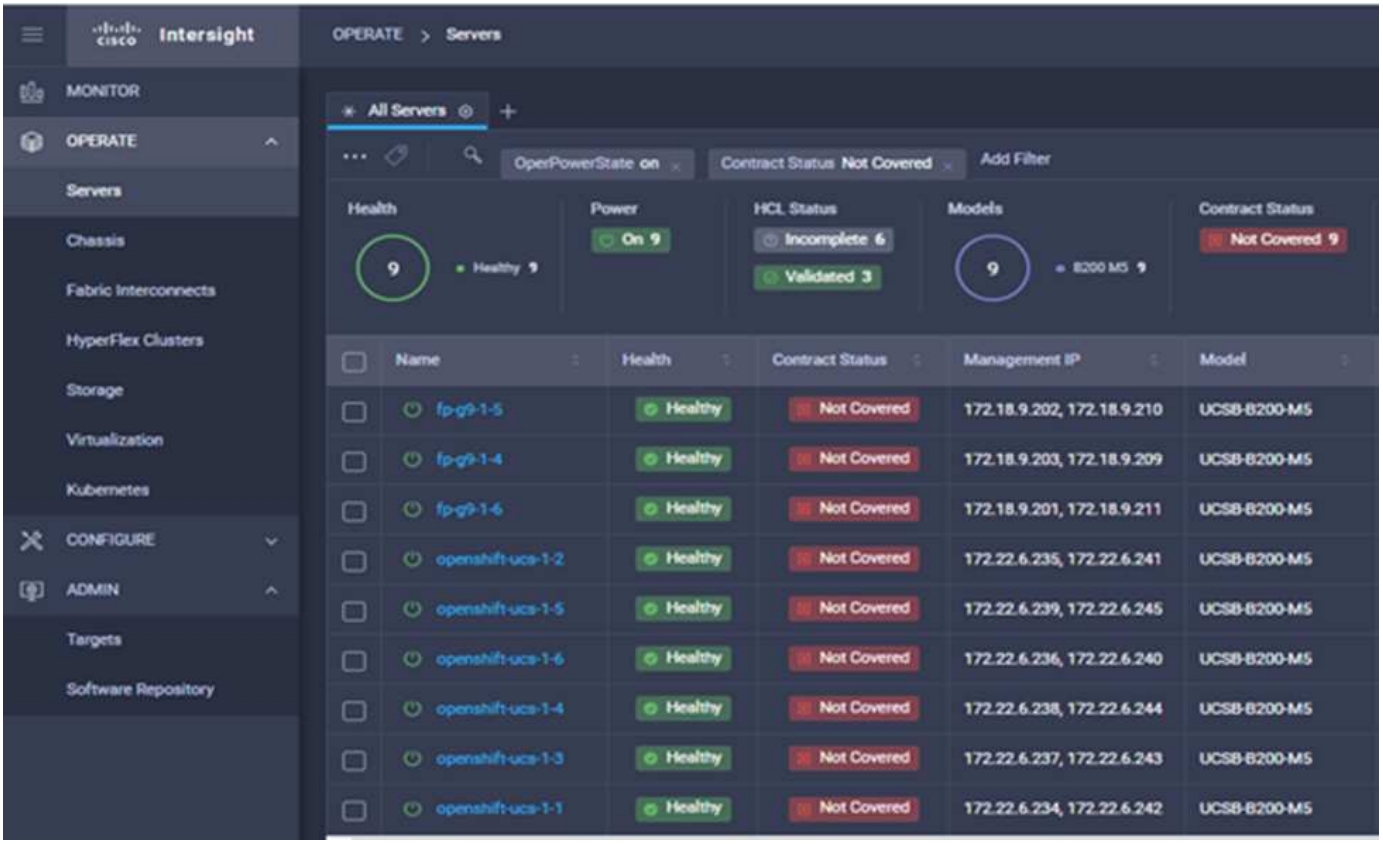
Cisco Intersight offre i seguenti vantaggi:

- **Delivery più rapida.** offerta come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può semplicemente concentrarsi sull'accelerazione della consegna per la linea di business.
- **Operazioni semplificate.** semplifica le operazioni utilizzando un unico tool sicuro fornito da SaaS con inventario, autenticazione e API comuni per lavorare in stack completi e in tutte le ubicazioni, eliminando i silos tra i team. Dalla gestione on-premise di server fisici e hypervisor a macchine virtuali, K8s, serverless, automazione, ottimizzazione e controllo dei costi su cloud pubblici e on-premise.
- **Ottimizzazione continua.** Ottimizza continuamente il tuo ambiente utilizzando l'intelligence fornita da Cisco Intersight su ogni livello e Cisco TAC. Questa intelligenza viene convertita in azioni consigliate e automatizzabili, in modo da poter adattare in tempo reale ad ogni cambiamento: Dallo spostamento dei carichi di lavoro al monitoraggio dello stato di salute dei server fisici al dimensionamento automatico dei cluster K8s, ai consigli per la riduzione dei costi sui cloud pubblici con cui lavorate.

Cisco Intersight offre due modalità di gestione: UCSM Managed Mode (UMM) e Intersight Managed Mode

(IMM). È possibile selezionare L'UMM o IMM nativo per i sistemi Cisco UCS collegati al fabric durante la configurazione iniziale delle interconnessioni fabric. In questa soluzione viene utilizzato UMM nativo.

La seguente immagine mostra la dashboard di Cisco Intersight.

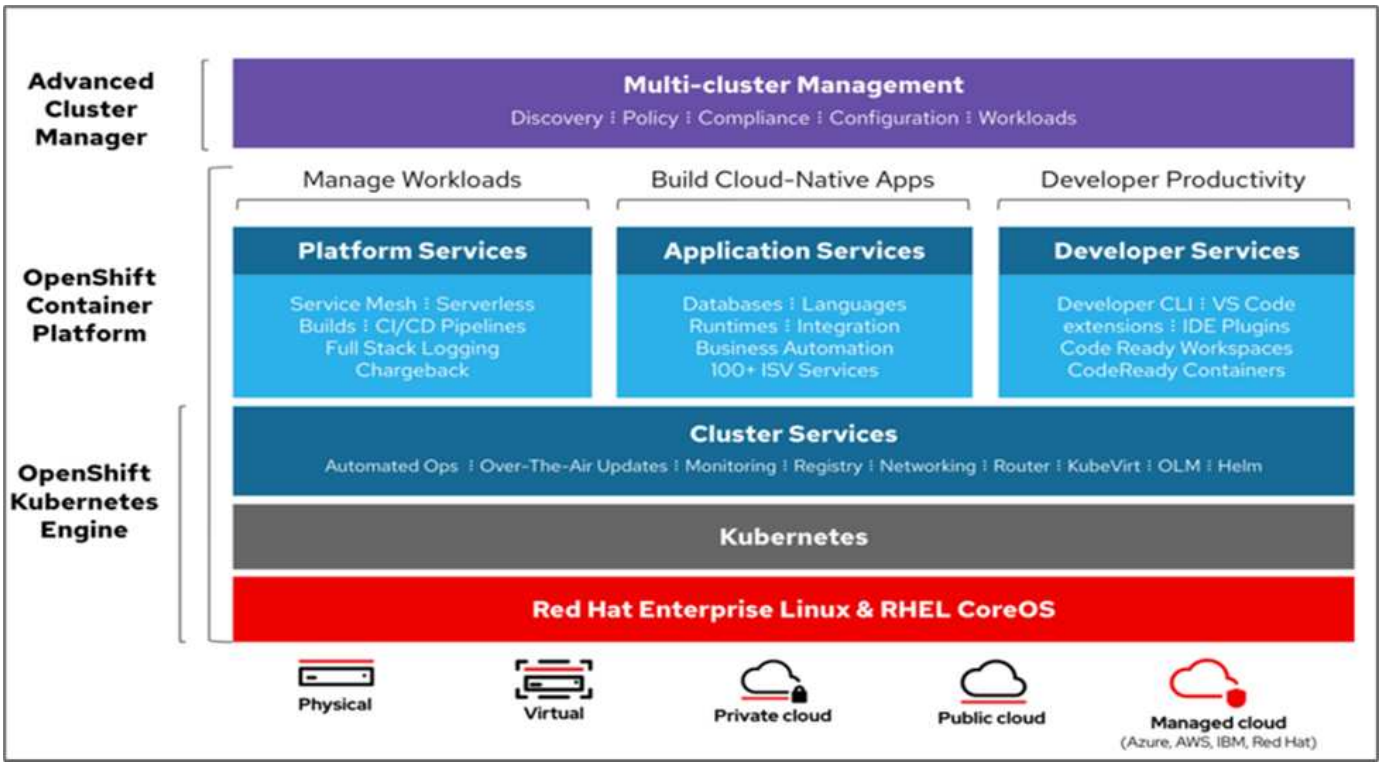


Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform è una piattaforma applicativa container che riunisce CRI-o e Kubernetes e fornisce un'API e un'interfaccia web per gestire questi servizi. CRI-o è un'implementazione della Kubernetes Container Runtime Interface (CRI) per consentire l'utilizzo di runtime compatibili con Open Container Initiative (OCI). Si tratta di un'alternativa leggera all'utilizzo di Docker come runtime per Kubernetes.

OpenShift Container Platform consente ai clienti di creare e gestire container. I container sono processi standalone che vengono eseguiti all'interno del proprio ambiente, indipendentemente dal sistema operativo e dall'infrastruttura sottostante. OpenShift Container Platform aiuta a sviluppare, implementare e gestire applicazioni basate su container. Offre una piattaforma self-service per creare, modificare e implementare applicazioni on-demand, consentendo cicli di sviluppo e rilascio più rapidi. OpenShift Container Platform dispone di un'architettura basata su microservizi di unità più piccole e separate che funzionano insieme. Viene eseguito su un cluster Kubernetes, con i dati sugli oggetti memorizzati in etcd, un archivio chiavi-valore in cluster affidabile.

L'immagine seguente è una panoramica della piattaforma container Red Hat OpenShift.



Infrastruttura Kubernetes

All'interno di OpenShift Container Platform, Kubernetes gestisce le applicazioni containerizzate su un set di host runtime CRI-o e fornisce meccanismi per l'implementazione, la manutenzione e la scalabilità delle applicazioni. Il servizio CRI-o crea pacchetti, crea istanze ed esegue applicazioni containerizzate.

Un cluster Kubernetes è costituito da uno o più master e da un insieme di nodi di lavoro. Questa progettazione della soluzione include funzionalità ad alta disponibilità (ha) sull'hardware e sullo stack software. Un cluster Kubernetes è progettato per essere eseguito in modalità ha con tre nodi master e un minimo di due nodi di lavoro per garantire che il cluster non abbia un singolo punto di errore.

So Red Hat Core

OpenShift Container Platform utilizza Red Hat Enterprise Linux CoreOS (RHCOS), un sistema operativo orientato ai container che combina alcune delle migliori funzionalità dei sistemi operativi CoreOS e Red Hat Atomic host. RHCOS è progettato appositamente per l'esecuzione di applicazioni containerizzate da OpenShift Container Platform e lavora con nuovi tool per fornire installazione rapida, gestione basata sull'operatore e aggiornamenti semplificati.

RHCOS include le seguenti funzionalità:

- Ignition, che OpenShift Container Platform utilizza come prima configurazione del sistema di boot per l'avvio iniziale e la configurazione delle macchine.
- CRI-o, un'implementazione nativa del runtime di container di Kubernetes che si integra a stretto contatto con il sistema operativo per offrire un'esperienza Kubernetes efficiente e ottimizzata. CRI-o offre funzionalità per l'esecuzione, l'arresto e il riavvio dei container. Sostituisce completamente Docker Container Engine, utilizzato in OpenShift Container Platform 3.
- Kubernetes, il principale agente di nodo di Kubernetes, è responsabile del lancio e del monitoraggio dei container.

VMware vSphere 7.0

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

Per ulteriori informazioni, vedere "VMware vSphere".

VMware vSphere vCenter

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

Revisioni hardware e software

Questa soluzione può essere estesa a qualsiasi ambiente FlexPod che esegue versioni supportate di software, firmware e hardware, come definito nella "Tool di matrice di interoperabilità NetApp" e. "Elenco di compatibilità hardware Cisco UCS." Il cluster OpenShift viene installato su FlexPod in maniera bare metal e su VMware vSphere.

Solo una singola istanza di Astra Control Center è necessaria per gestire più cluster OpenShift (k8s), mentre Trident CSI è installato su ciascun cluster OpenShift. Astra Control Center può essere installato su uno qualsiasi di questi cluster OpenShift. In questa soluzione, Astra Control Center viene installato sul cluster bare-metal OpenShift.

La seguente tabella elenca le revisioni hardware e software di FlexPod per OpenShift.

Componente	Prodotto	Versione
Calcolo	Cisco UCS Fabric Interconnects 6454	4.1(3c)
	Server Cisco UCS B200 M5	4.1(3c)
Rete	Sistema operativo Cisco Nexus 9336C-FX2 NX	9.3(8)
Storage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9.11
Software	Driver Ethernet Nenico VMware ESXi	1.0.35.0
	VSphere ESXi	7.0 (U2)
	Appliance VMware vCenter	7.0 U2b

Componente	Prodotto	Versione
	Appliance virtuale Cisco Intersight Assist	1.0.9-342
	Piattaforma container OpenShift	4.9
	Nodo master della piattaforma container OpenShift	RHCOS 4.9
	Nodo di lavoro della piattaforma container OpenShift	RHCOS 4.9

La seguente tabella elenca le versioni software di OpenShift su AWS.

Componente	Prodotto	Versione
Calcolo	Tipo istanza master: m5.xlarge	n/a.
	Tipo di istanza di lavoro: m5.Large	n/a.
Rete	Virtual Private Cloud Transit Gateway	n/a.
Storage	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Software	Piattaforma container OpenShift	4.9
	Nodo master della piattaforma container OpenShift	RHCOS 4.9
	Nodo di lavoro della piattaforma container OpenShift	RHCOS 4.9

"Avanti: Installazione bare-metal di FlexPod per la piattaforma container OpenShift 4."

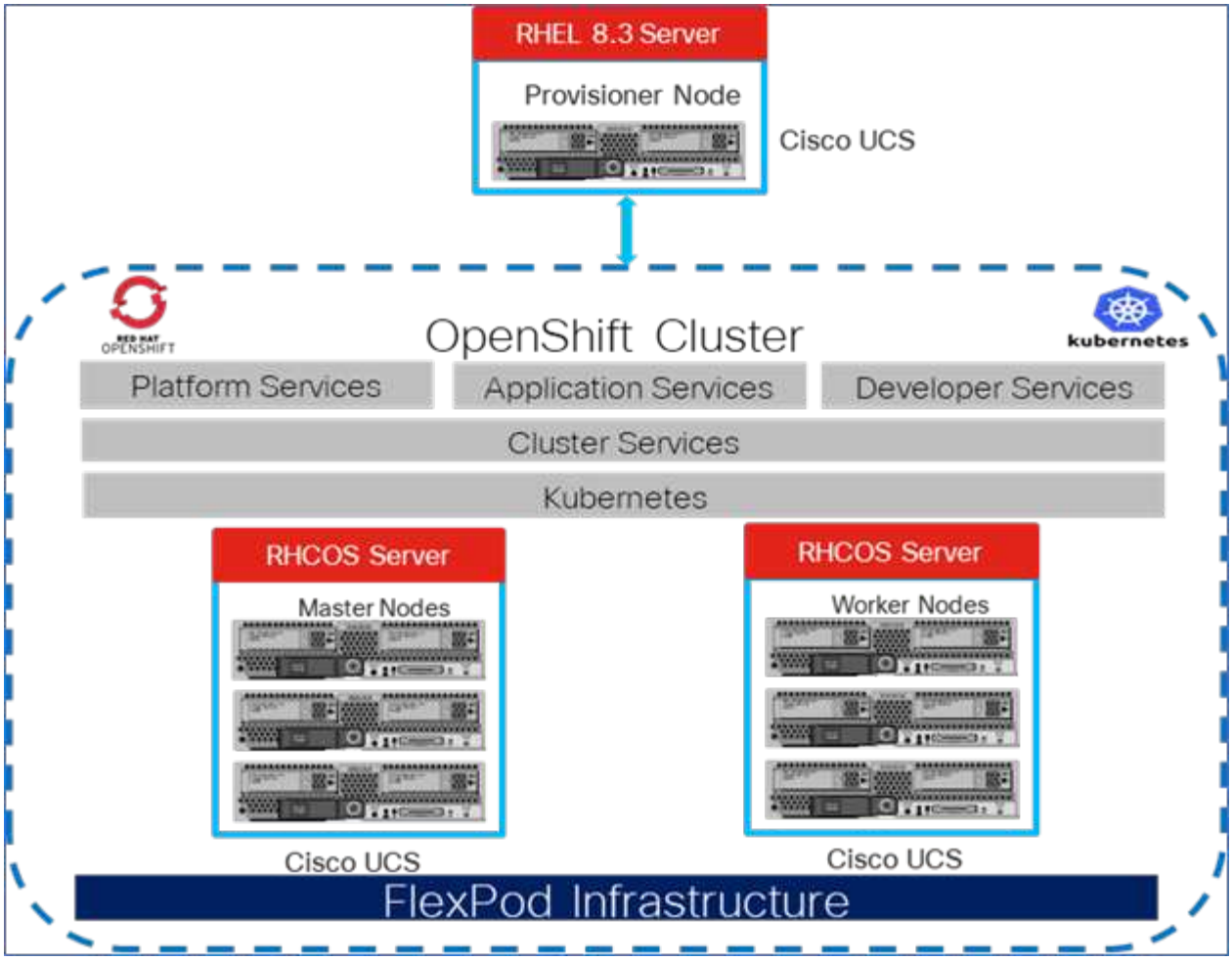
Installazione e configurazione

Installazione bare-metal di FlexPod per piattaforma container OpenShift 4

"Precedente: Componenti della soluzione."

Per informazioni sulla progettazione bare-metal di FlexPod per la piattaforma container OpenShift 4, sui dettagli di implementazione e sull'installazione e configurazione di NetApp Astra Trident, vedere "FlexPod con OpenShift Guida alla progettazione e all'implementazione validate di Cisco (CVD)". Questo CVD copre l'implementazione di FlexPod e della piattaforma container OpenShift utilizzando Ansible. Il CVD fornisce inoltre informazioni dettagliate sulla preparazione dei nodi di lavoro, sull'installazione di Astra Trident, sul backend dello storage e sulle configurazioni di classe storage, che sono i pochi prerequisiti per l'implementazione e la configurazione di Astra Control Center.

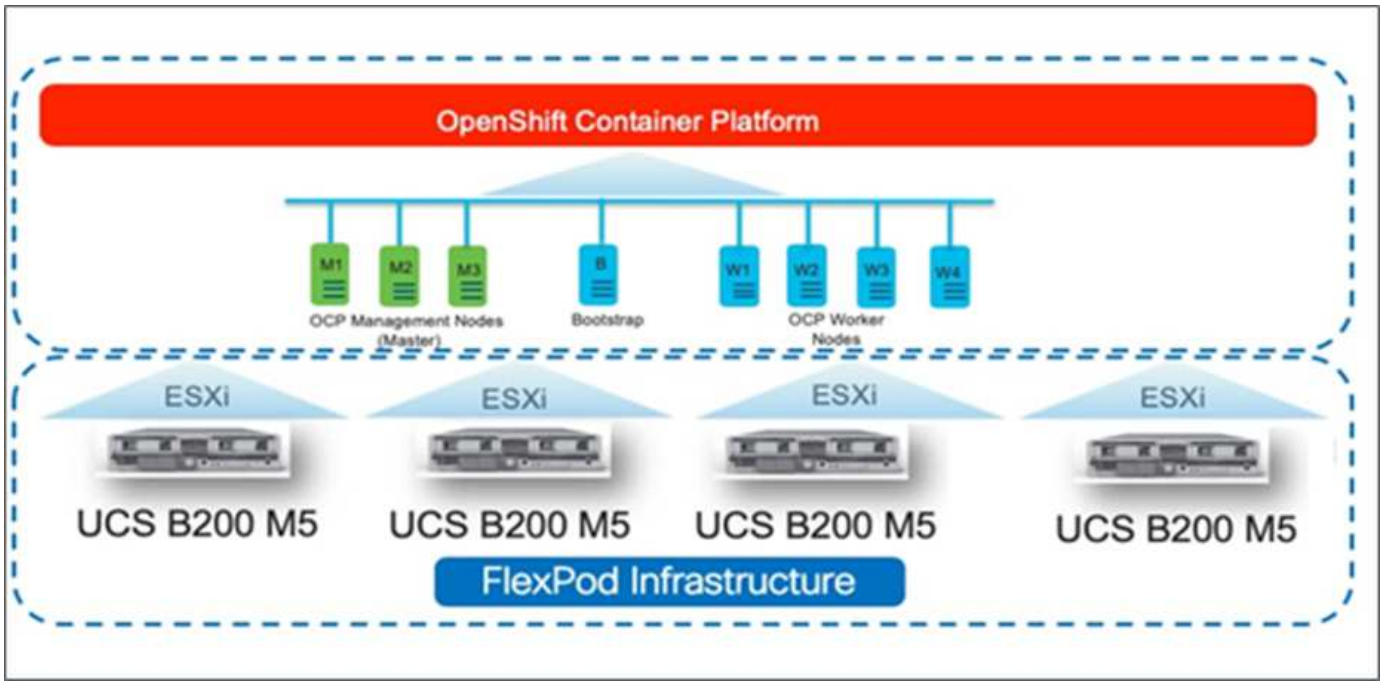
La figura seguente illustra la piattaforma container OpenShift 4 Bare Metal su FlexPod.



Installazione di FlexPod per piattaforma container OpenShift 4 su VMware

Per ulteriori informazioni sull'implementazione di Red Hat OpenShift Container Platform 4 su FlexPod con VMware vSphere, vedere "Data center FlexPod per piattaforma container OpenShift 4".

La figura seguente illustra FlexPod per piattaforma container OpenShift 4 su vSphere.



"Avanti: Red Hat OpenShift su AWS."

Red Hat OpenShift su AWS

"Precedente: Installazione bare-metal di FlexPod per piattaforma container OpenShift 4."

Un cluster OpenShift Container Platform 4 separato e autogestito viene implementato su AWS come sito di DR. I nodi master e worker si estendono in tre zone di disponibilità per garantire l'alta disponibilità.

Instances (6) Info

Search

ocp | Clear filters

Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift viene implementato come "cluster privato" In un VPC esistente su AWS. Un cluster OpenShift Container Platform privato non espone endpoint esterni ed è accessibile solo da una rete interna e non è visibile su Internet. Un NetApp Cloud Volumes ONTAP a nodo singolo viene implementato utilizzando NetApp Cloud Manager, che fornisce un backend di storage ad Astra Trident.

Per ulteriori informazioni sull'installazione di OpenShift su AWS, vedere "Documentazione di OpenShift".

"Pagina successiva: NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Precedente: Red Hat OpenShift su AWS."

L'istanza di NetApp Cloud Volumes ONTAP viene implementata su AWS e funge da storage back-end per Astra Trident. Prima di aggiungere un ambiente di lavoro Cloud Volumes ONTAP, è necessario implementare un connettore. Cloud Manager ti chiede se provi a creare il tuo primo ambiente di lavoro Cloud Volumes ONTAP senza un connettore. Per implementare un connettore in AWS, vedere "Creare un connettore".

Per implementare Cloud Volumes ONTAP su AWS, vedere "Quick Start per AWS".

Una volta implementato Cloud Volumes ONTAP, è possibile installare Astra Trident e configurare il backend dello storage e la classe Snapshot sul cluster della piattaforma container OpenShift.

"Avanti: Installazione di Astra Control Center su OpenShift Container Platform."

Installazione di Astra Control Center su OpenShift Container Platform

"Precedente: NetApp Cloud Volumes ONTAP."

È possibile installare Astra Control Center sul cluster OpenShift in esecuzione su FlexPod o su AWS con un backend di storage Cloud Volumes ONTAP. In questa soluzione, Astra Control Center viene implementato sul cluster bare-metal OpenShift.

Astra Control Center può essere installato utilizzando il processo standard descritto "qui" Oppure da Red Hat OpenShift OperatorHub. Astra Control Operator è un operatore certificato Red Hat. In questa soluzione, Astra Control Center viene installato utilizzando Red Hat OperatorHub.

Requisiti ambientali

- Astra Control Center supporta più distribuzioni Kubernetes; per Red Hat OpenShift, le versioni supportate

includono Red Hat OpenShift Container Platform 4.8 o 4.9.

- Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse applicative dell'ambiente e dell'utente finale:

Componenti	Requisito
Capacità di back-end dello storage	Almeno 500 GB disponibili
Nodi di lavoro	Almeno 3 nodi di lavoro, con 4 core CPU e 12 GB di RAM ciascuno
Indirizzo FQDN (Fully Qualified Domain Name)	Un indirizzo FQDN per Astra Control Center
Astra Trident	Astra Trident 21.04 o versione successiva installata e configurata
Controller di ingresso o bilanciamento del carico	Configurare il controller di ingresso per esporre Astra Control Center con un URL o un bilanciamento del carico per fornire l'indirizzo IP che verrà risolto nell'FQDN

- È necessario disporre di un registro di immagini privato esistente in cui trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui vengono caricate le immagini.

Alcune immagini vengono estratte durante l'esecuzione di determinati flussi di lavoro e i container vengono creati e distrutti quando necessario.

- Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Centro di controllo Astra supporta i seguenti driver ONTAP forniti da Astra Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-economy

Supponiamo che i cluster OpenShift implementati abbiano Astra Trident installato e configurato con un backend ONTAP e sia definita anche una classe di storage predefinita.

- Per la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per modificare il criterio di esportazione ONTAP in modo da consentire queste operazioni, eseguire i seguenti comandi:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Per aggiungere un secondo ambiente operativo OpenShift come risorsa di calcolo gestita, assicurarsi che la funzione Astra Trident Volume snapshot sia attivata. Per abilitare e testare le snapshot dei volumi con Astra Trident, consulta la pagina ufficiale "Istruzioni di Astra Trident".

- R "VolumeSnapClass" Deve essere configurato su tutti i cluster Kubernetes da cui vengono gestite le applicazioni. Questo potrebbe includere anche il cluster K8s su cui è installato Astra Control Center. Astra Control Center è in grado di gestire le applicazioni sul cluster K8s su cui è in esecuzione.

Requisiti di gestione delle applicazioni

- **Licensing.** per gestire le applicazioni utilizzando Astra Control Center, è necessaria una licenza Astra Control Center.
- **Namespaces.** Uno spazio dei nomi è l'entità più grande che può essere gestita come applicazione da Astra Control Center. È possibile scegliere di filtrare i componenti in base alle etichette dell'applicazione e alle etichette personalizzate in uno spazio dei nomi esistente e gestire un sottoinsieme di risorse come applicazione.
- **StorageClass.** se si installa un'applicazione con un StorageClass esplicitamente impostato ed è necessario clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la StorageClass originariamente specificata. La clonazione di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass ha esito negativo.
- **Kubernetes resources.** le applicazioni che utilizzano risorse Kubernetes non acquisite da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati applicativi. Astra Control può acquisire le seguenti risorse Kubernetes:

Risorse Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	CustomResource	Lavoro di cassa
DemonSet	HorizontalPodAutoscaler	Ingresso
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
NetworkPolicy	ReplicaSet	Ruolo
RoleBinding	Percorso	Segreto
ValidatingWebhook		

Installare Astra Control Center utilizzando OpenShift OperatorHub

La seguente procedura consente di installare Astra Control Center utilizzando Red Hat OperatorHub. In questa soluzione, Astra Control Center viene installato su un cluster OpenShift bare-metal in esecuzione su FlexPod.

1. Scarica il bundle Astra Control Center (`astra-control-center-[version].tar.gz`) da "Sito di supporto NetApp".
2. Scaricare il file .zip per i certificati e le chiavi di Astra Control Center da "Sito di supporto NetApp".
3. Verificare la firma del bundle.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Estrarre le immagini Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Passare alla directory Astra.

```
cd astra-control-center-[version]
```

6. Aggiungere le immagini al registro locale.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilizzare lo script appropriato per caricare le immagini, etichettarle e inserirle nel registro locale.

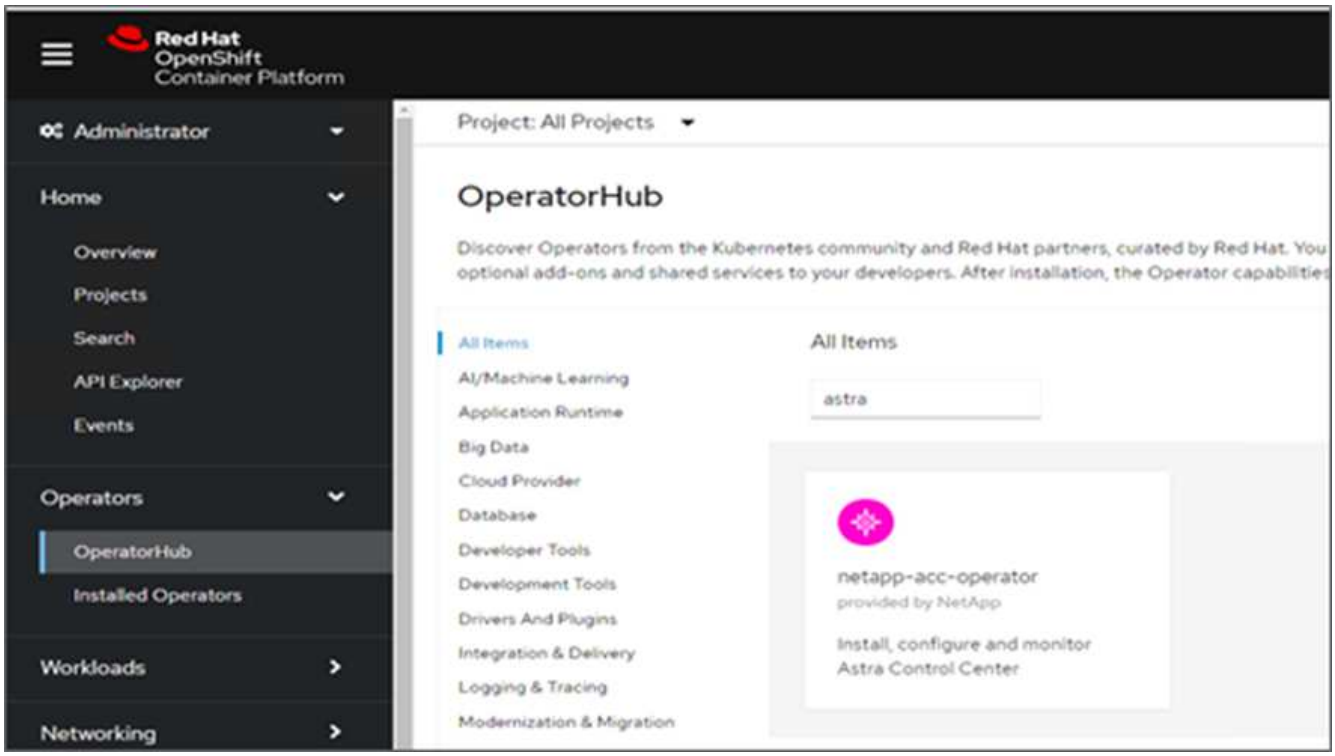
   Per Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

   Per Podman:

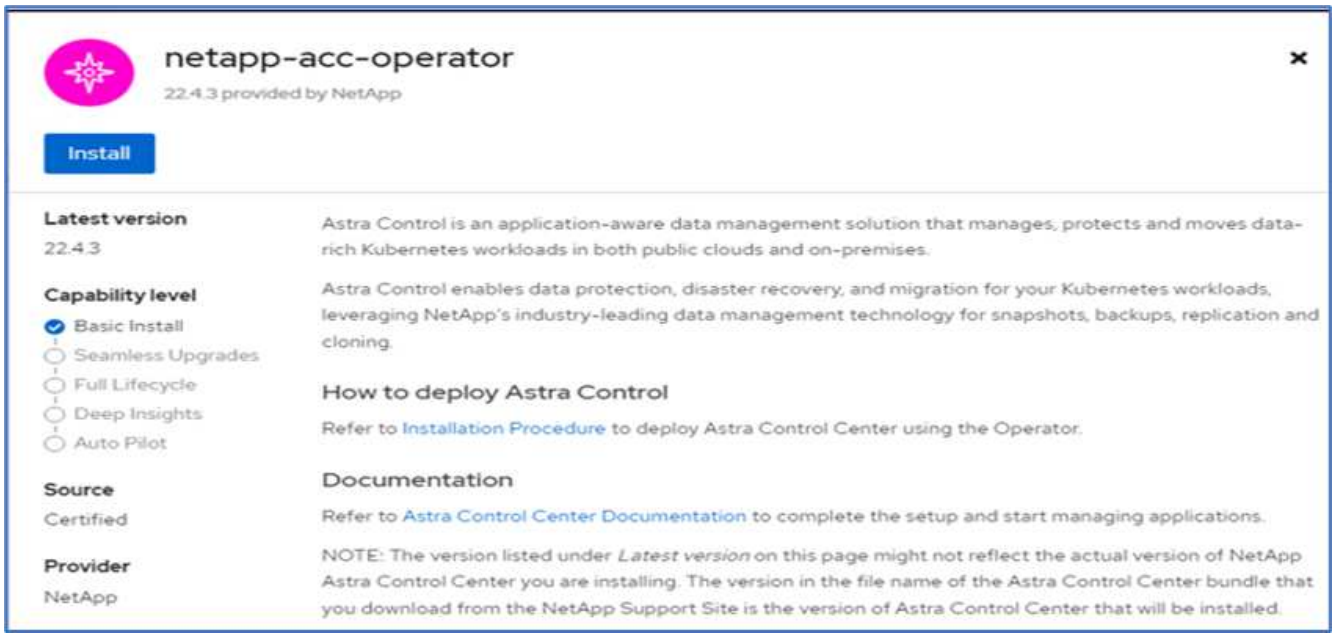
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Accedere alla console web del cluster OpenShift bare-metal. Dal menu laterale, selezionare Operator (operatori) > OperatorHub. Invio `astra` per visualizzare l'elenco di `netapp-acc-operator`.

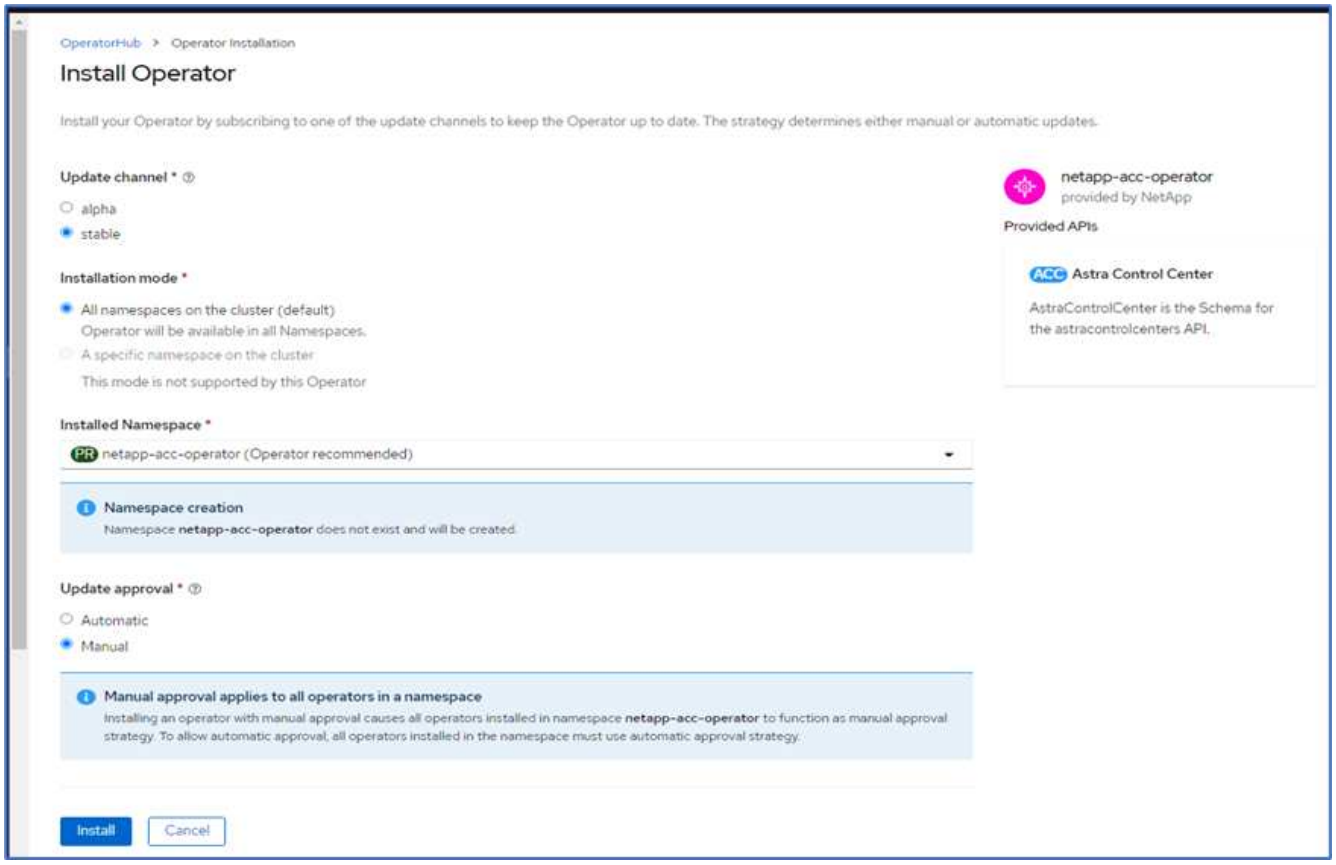


> `netapp-acc-operator` È un operatore Red Hat OpenShift certificato ed è elencato nel catalogo OperatorHub.

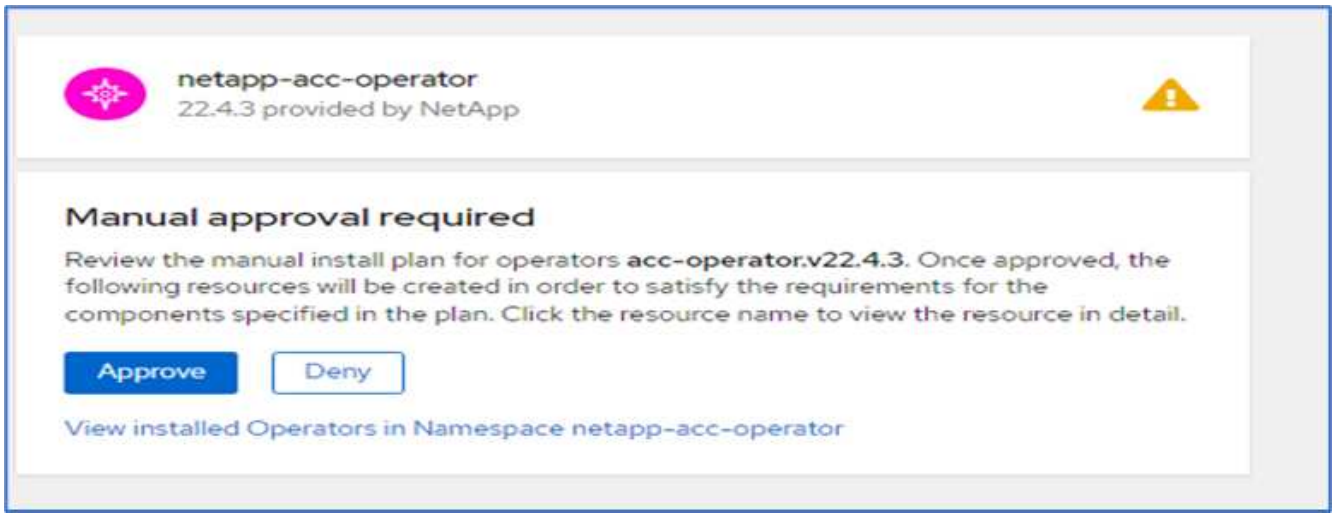
9. Selezionare `netapp-acc-operator` E fare clic su Installa.



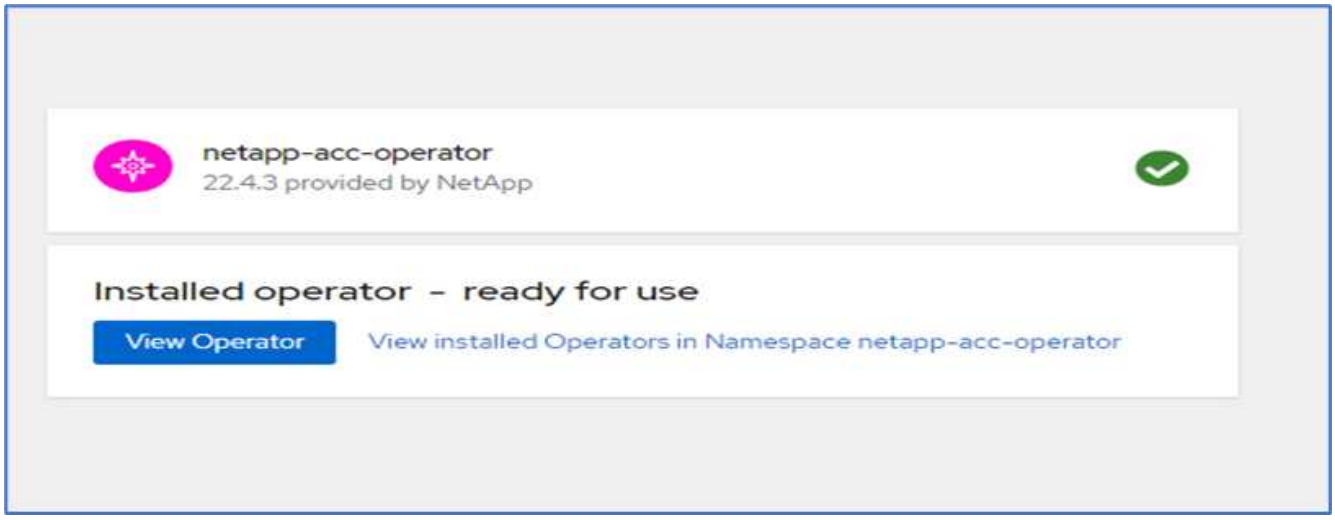
10. Selezionare le opzioni appropriate e fare clic su Install (Installa).



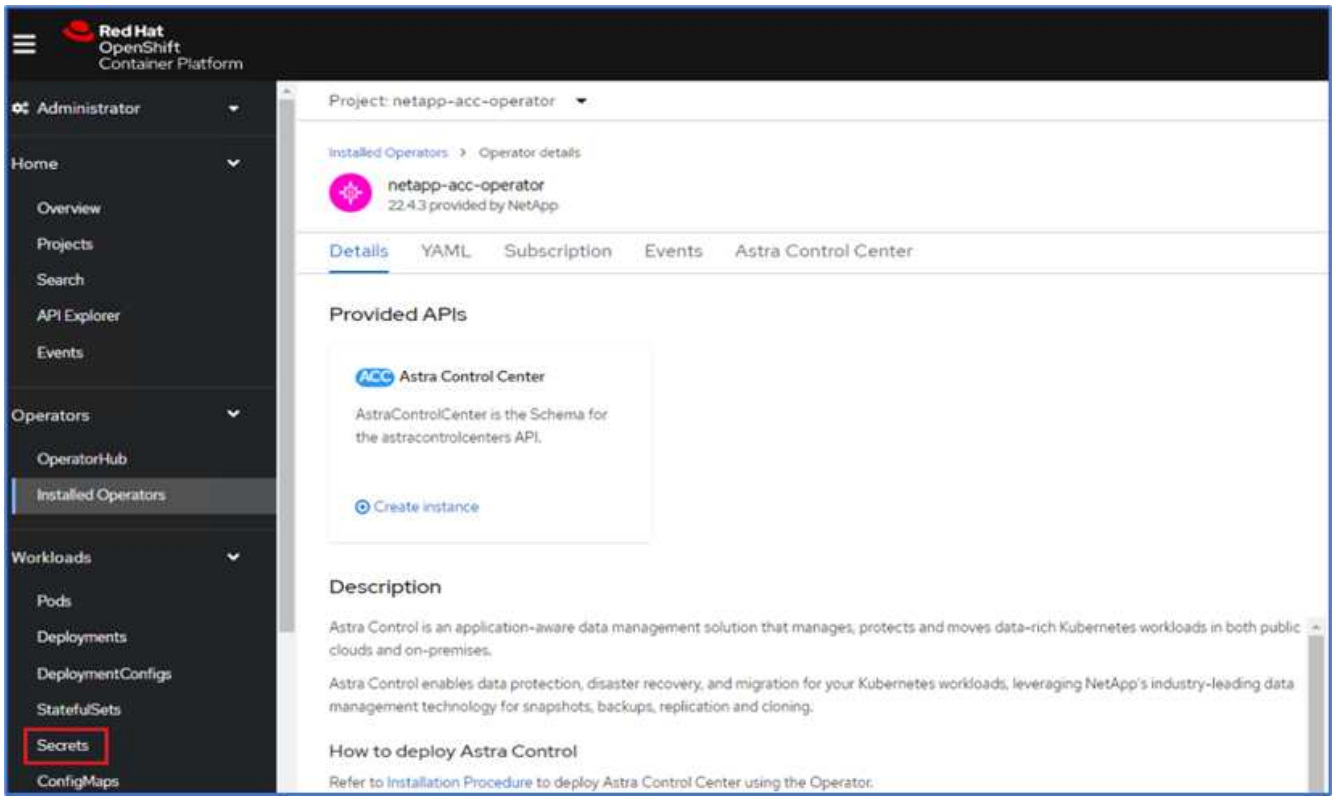
11. Approvare l'installazione e attendere l'installazione dell'operatore.



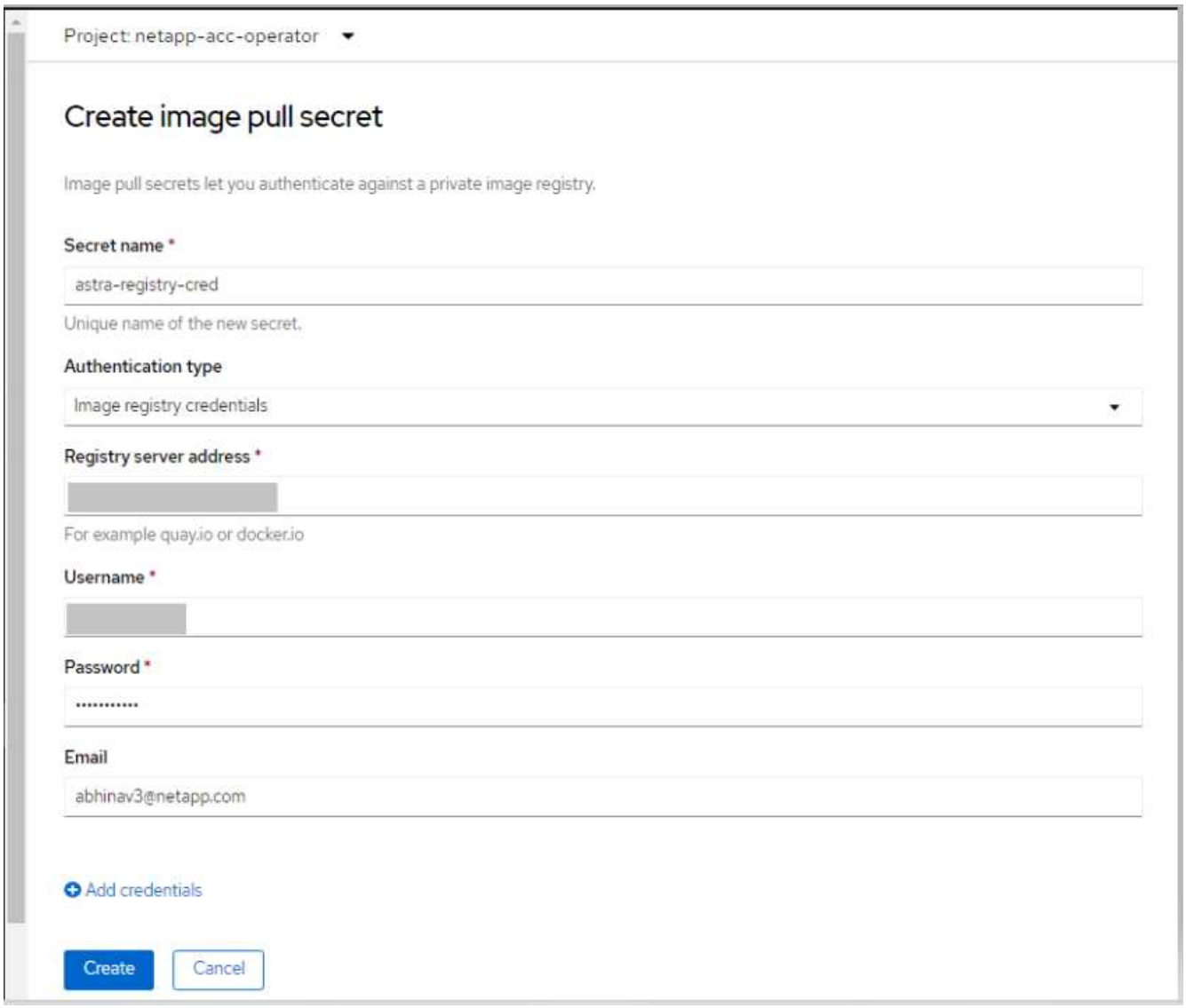
12. A questo punto, l'operatore viene installato correttamente e pronto per l'uso. Fare clic su View Operator (Visualizza operatore) per avviare l'installazione di Astra Control Center.



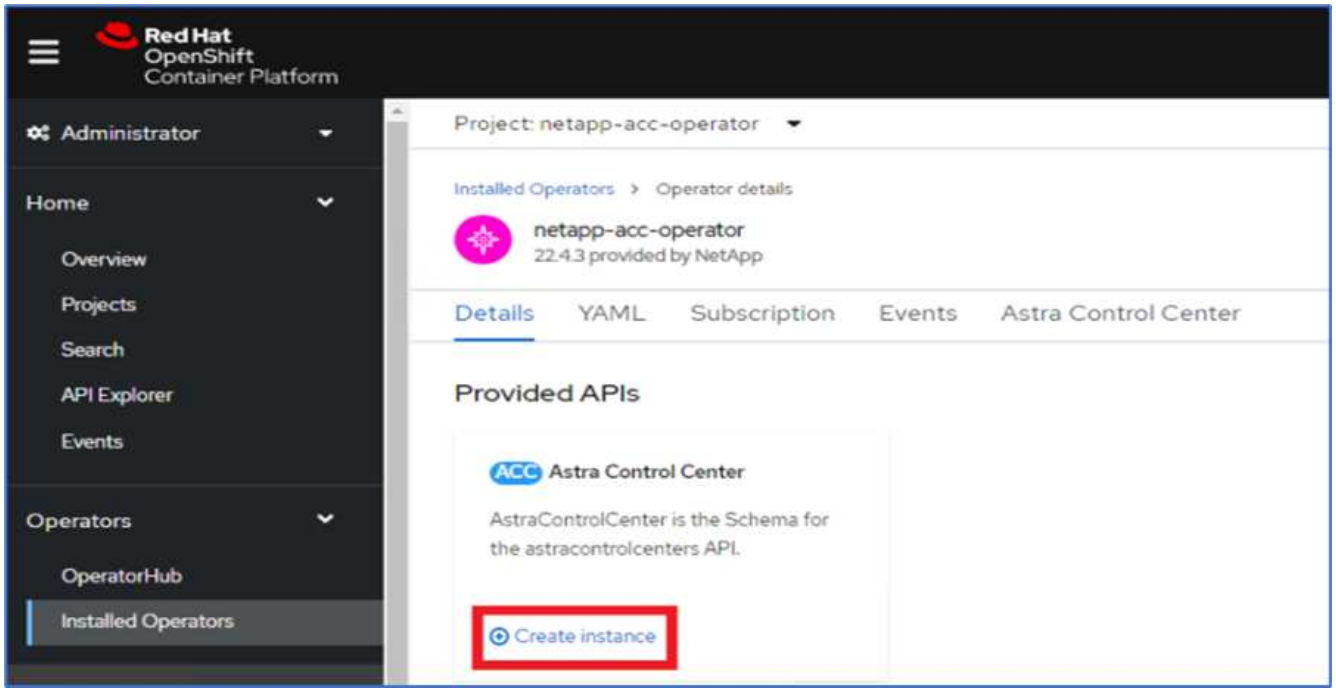
13. Prima di installare Astra Control Center, creare il segreto pull per scaricare le immagini Astra dal registro Docker precedentemente inserito.



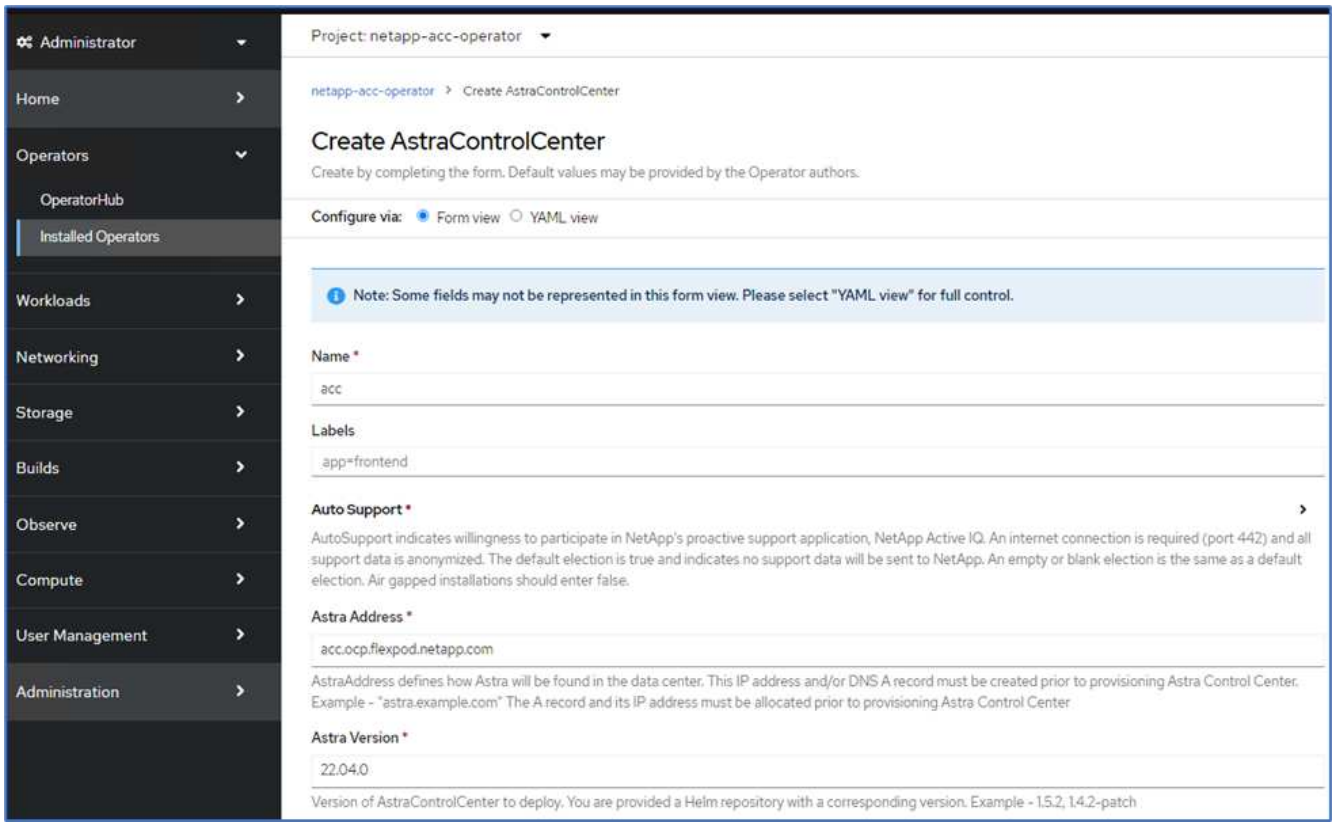
14. Per estrarre le immagini di Astra Control Center dal tuo repo privato Docker, crea un segreto in `netapp-acc-operator` namespace. Questo nome segreto viene fornito nel manifesto YAML di Astra Control Center in un passaggio successivo.



15. Dal menu laterale, selezionare Operator > Installed Operators (operatori > operatori installati) e fare clic su Create Instance (Crea istanza) nella sezione delle API fornite.



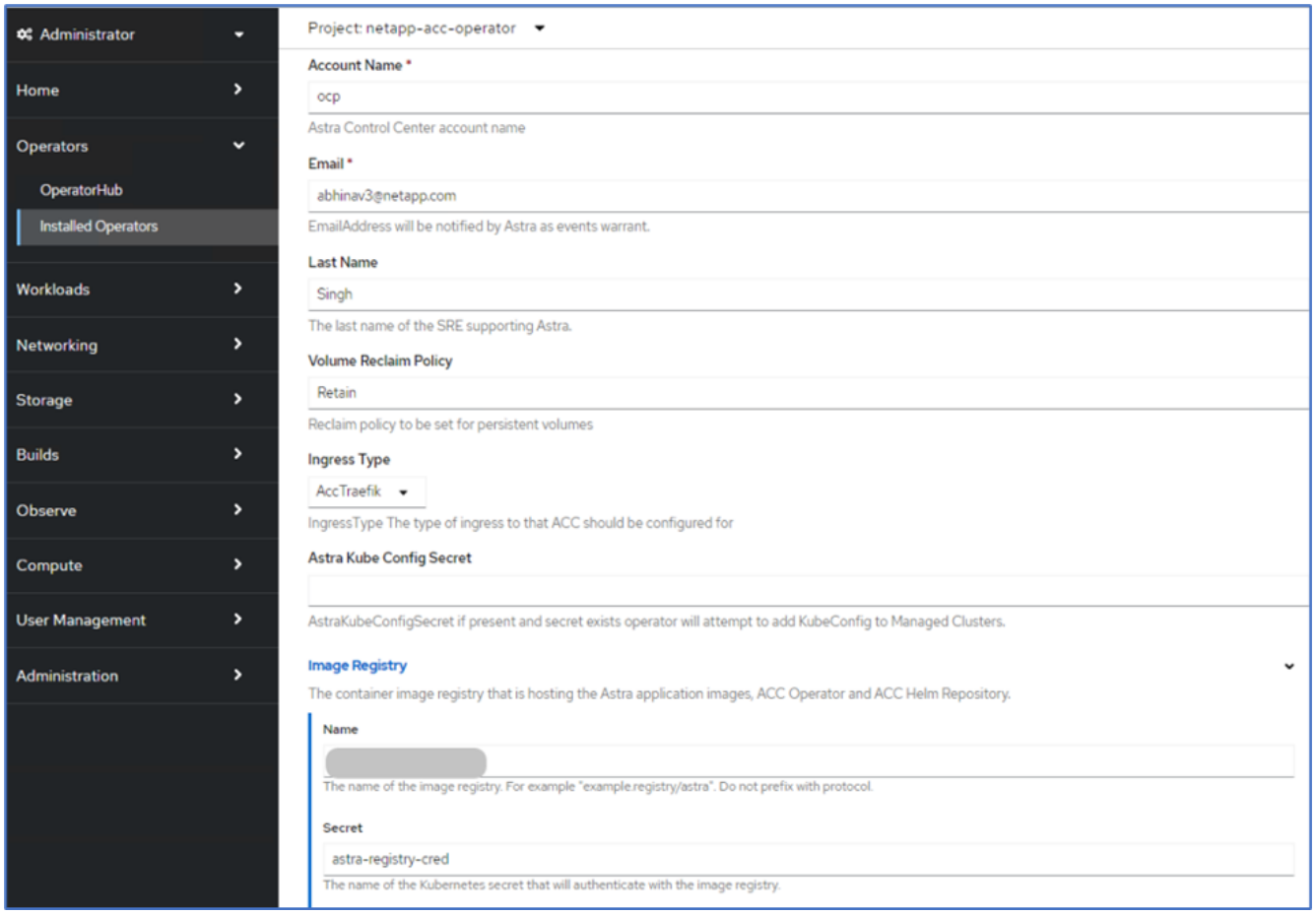
16. Completare il modulo Create AstraControlCenter. Fornire il nome, l'indirizzo Astra e la versione di Astra.



In Astra Address (Indirizzo Astra), fornire l'indirizzo FQDN per Astra Control Center. Questo indirizzo viene utilizzato per accedere alla console Web di Astra Control Center. Il nome FQDN deve anche essere impostato su una rete IP raggiungibile e deve essere configurato nel DNS.

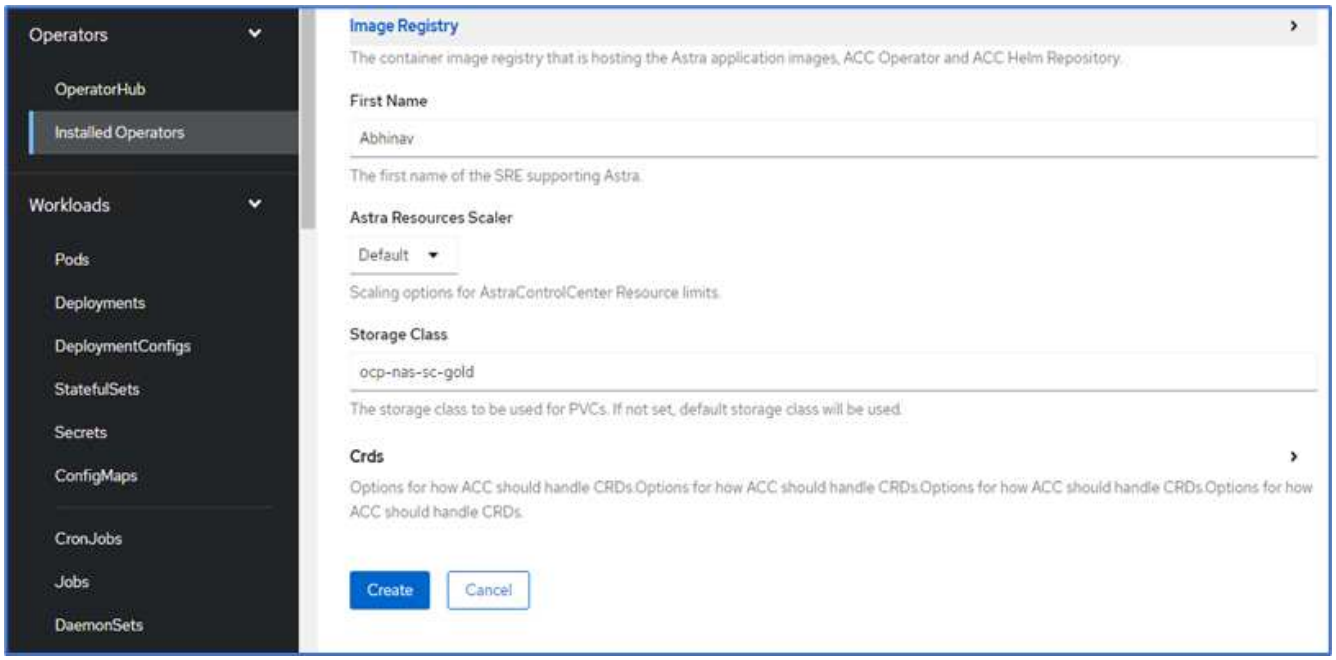
17. Immettere un nome account, un indirizzo e-mail, il cognome dell'amministratore e mantenere la policy di

recupero del volume predefinita. Se si utilizza un bilanciamento del carico, impostare il tipo di ingresso su `AccTraefik`. In caso contrario, selezionare Generico per `Ingress.Controller`. In Image Registry (Registro immagini), immettere il percorso e il segreto del Registro di sistema dell'immagine contenitore.

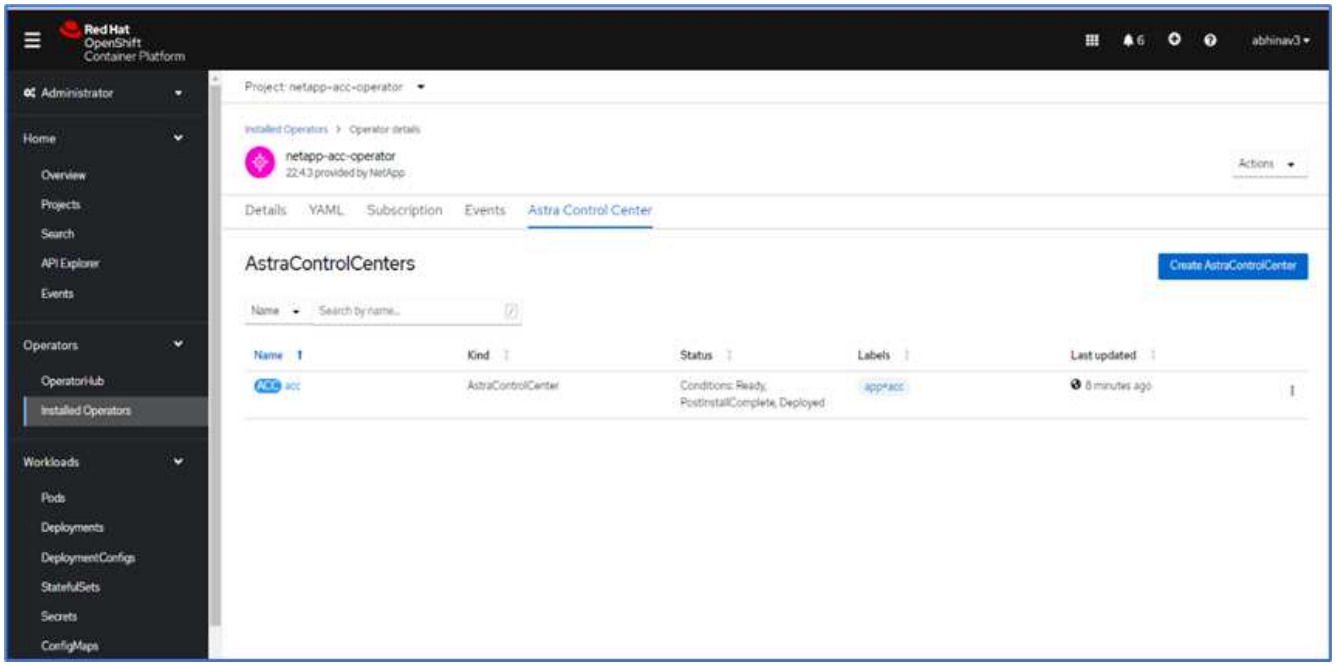


In questa soluzione viene utilizzato il bilanciamento del carico Metallb. Pertanto, il tipo di ingresso è AccTraefik. Questo espone il gateway traefik di Astra Control Center come un servizio Kubernetes di tipo LoadBalancer.

18. Inserire il nome admin, configurare la scalabilità delle risorse e fornire la classe di storage. Fare clic su Crea.



Lo stato dell'istanza di Astra Control Center deve passare da Deploying (implementazione) a Ready (Pronto).



19. Verificare che tutti i componenti del sistema siano stati installati correttamente e che tutti i pod siano in esecuzione.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
```

```
13m
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
```

```
3m35s
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
```

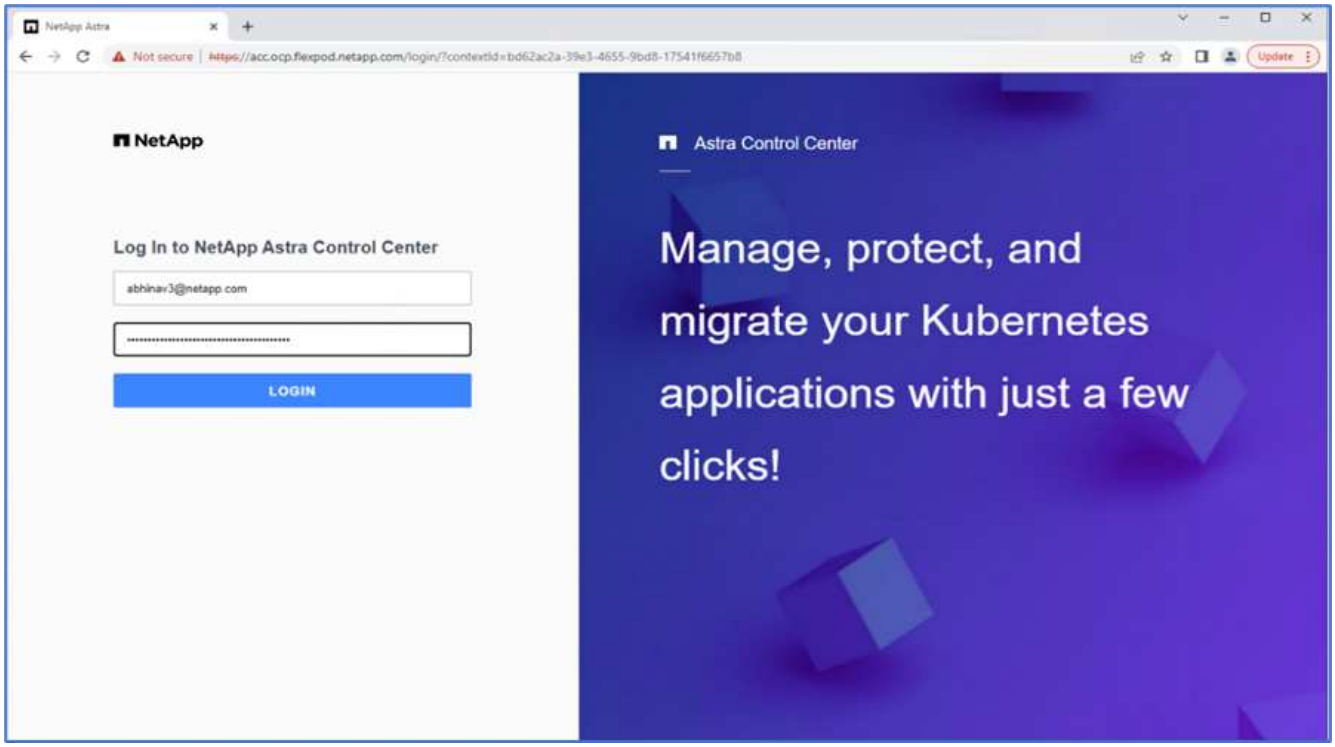
```
3m18s
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Ogni pod deve avere lo stato di esecuzione. L'implementazione dei pod di sistema potrebbe richiedere alcuni minuti.

20. Quando tutti i pod sono in esecuzione, eseguire il seguente comando per recuperare la password monouso. Nella versione YAML dell'output, selezionare `status.deploymentState` per il valore implementato, quindi copiare `status.uuid` valore. La password è `ACC-` Seguito dal valore UUID. (ACC-[UUID]).

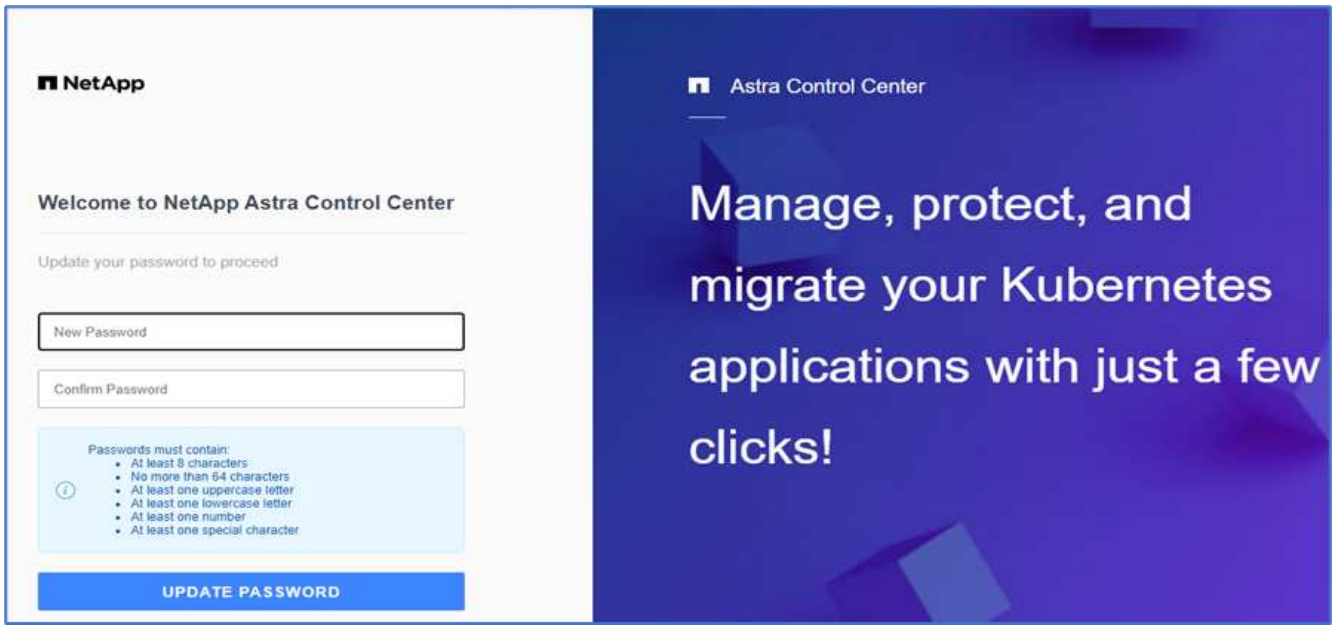
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. In un browser, accedere all'URL utilizzando l'FQDN fornito.
22. Effettuare l'accesso utilizzando il nome utente predefinito, ovvero l'indirizzo e-mail fornito durante l'installazione e la password monouso ACC-[UUID].



Se si immette una password errata per tre volte, l'account amministratore viene bloccato per 15 minuti.

23. Modificare la password e procedere.

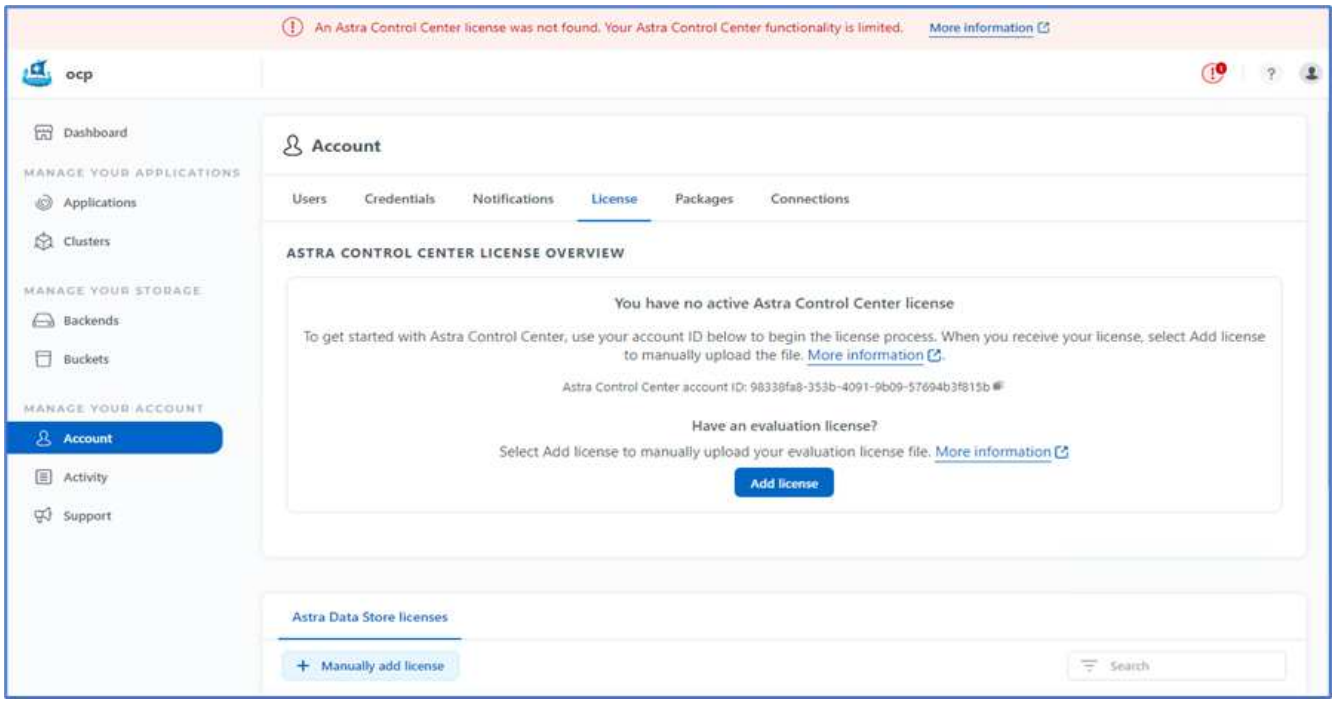


Per ulteriori informazioni sull'installazione di Astra Control Center, consultare "Panoramica dell'installazione di Astra Control Center" pagina.

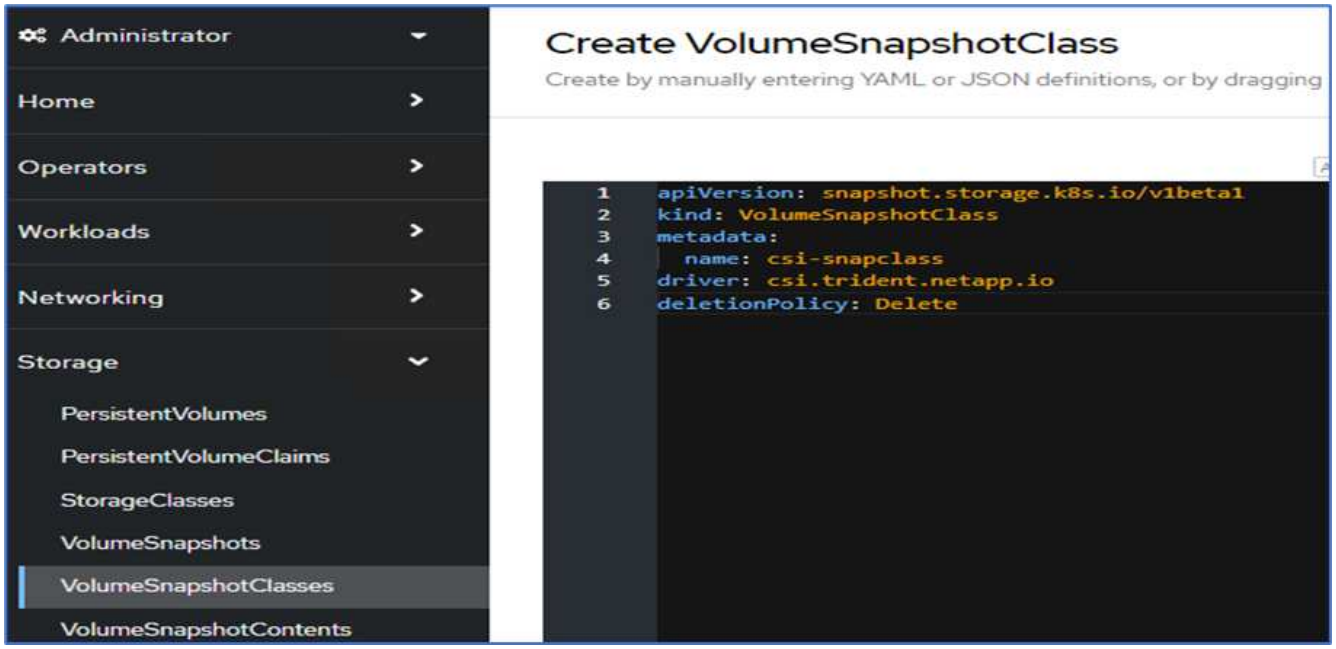
Configurare Astra Control Center

Dopo aver installato Astra Control Center, accedere all'interfaccia utente, caricare la licenza, aggiungere cluster, gestire lo storage e aggiungere bucket.

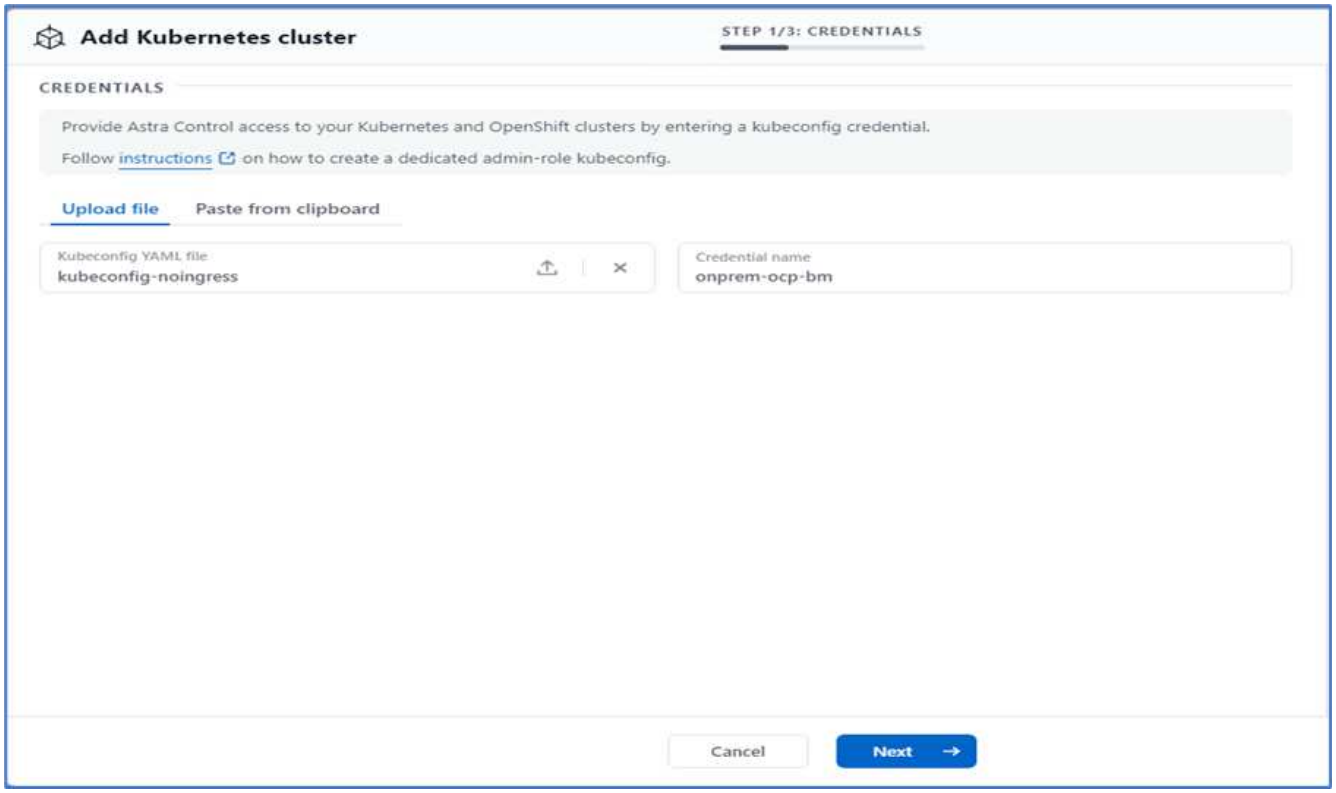
1. Nella home page, sotto account, andare alla scheda License (licenza) e selezionare Add License (Aggiungi licenza) per caricare la licenza Astra.



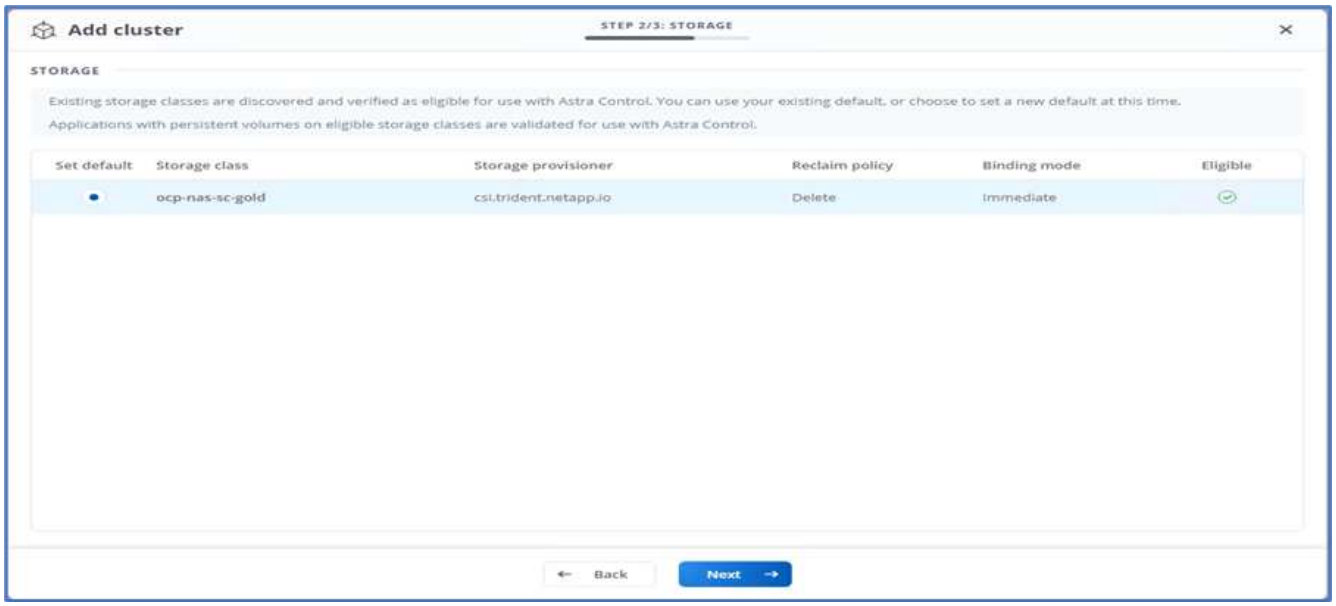
2. Prima di aggiungere il cluster OpenShift, creare una classe di snapshot Astra Trident Volume dalla console Web OpenShift. La classe Volume snapshot viene configurata con `csi.trident.netapp.io` driver.



3. Per aggiungere il cluster Kubernetes, accedere a Clusters nella home page e fare clic su Add Kubernetes Cluster (Aggiungi cluster Kubernetes). Quindi caricare `kubeconfig` per il cluster e fornire un nome di credenziale. Fare clic su Avanti.



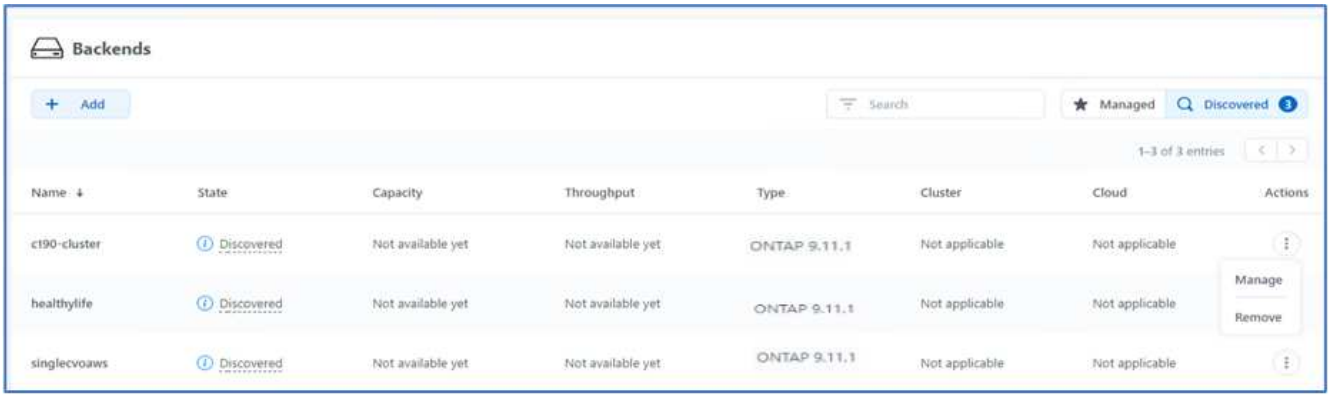
4. Le classi di storage esistenti vengono rilevate automaticamente. Selezionare la classe di storage predefinita, fare clic su Next (Avanti), quindi su Add cluster (Aggiungi cluster).



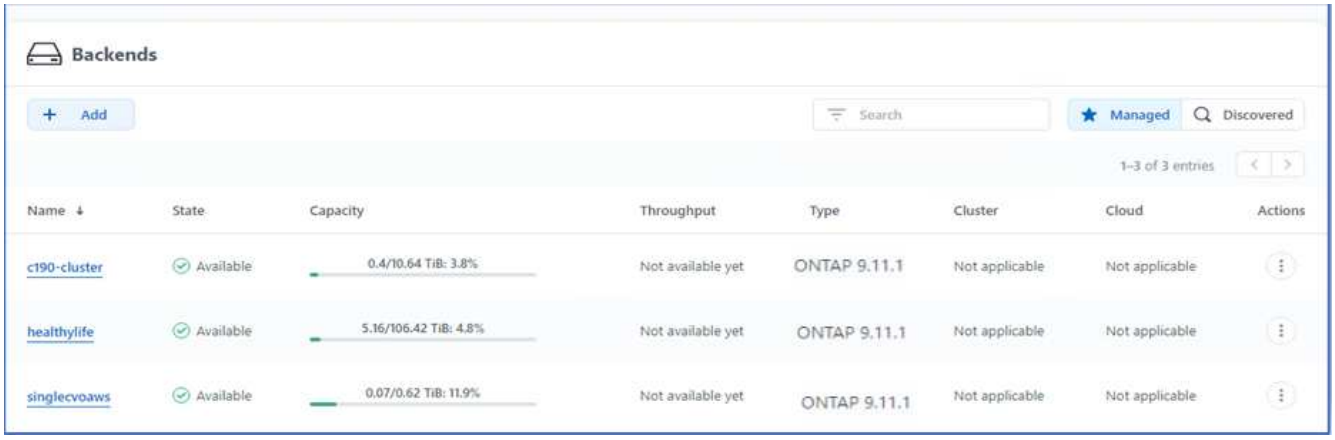
5. Il cluster viene aggiunto in pochi minuti. Per aggiungere altri cluster OpenShift Container Platform, ripetere i passaggi 1–4.

> Per aggiungere un ambiente operativo OpenShift aggiuntivo come risorsa di calcolo gestita, assicurarsi che Astra Trident "Oggetti VolumeSnapshotClass" sono definiti.

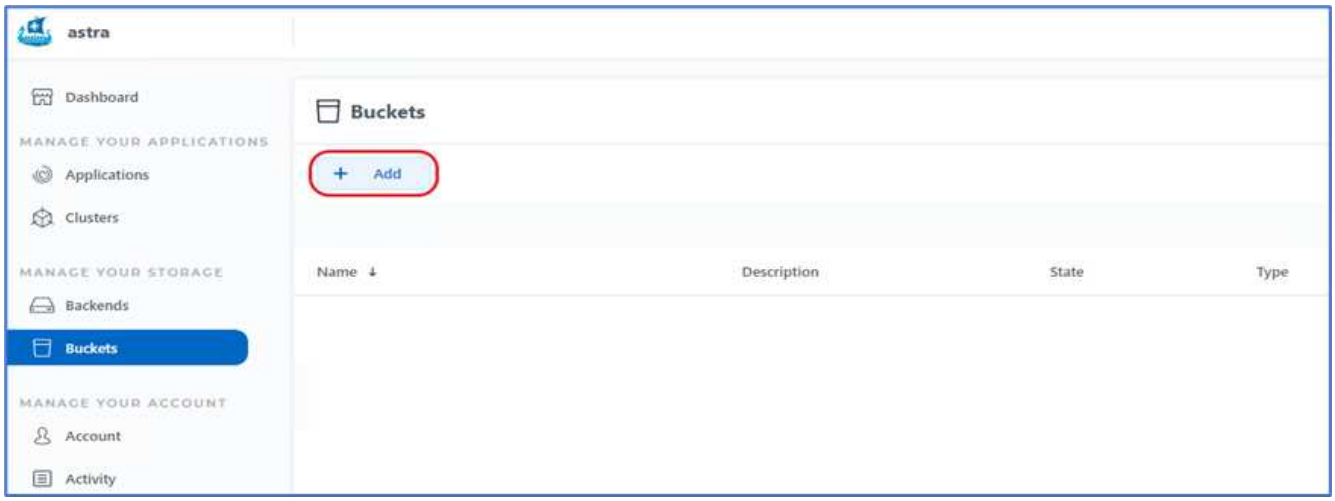
6. Per gestire lo storage, accedere a Backend, fare clic sui tre punti in azioni rispetto al backend che si desidera gestire. Fare clic su Gestisci.



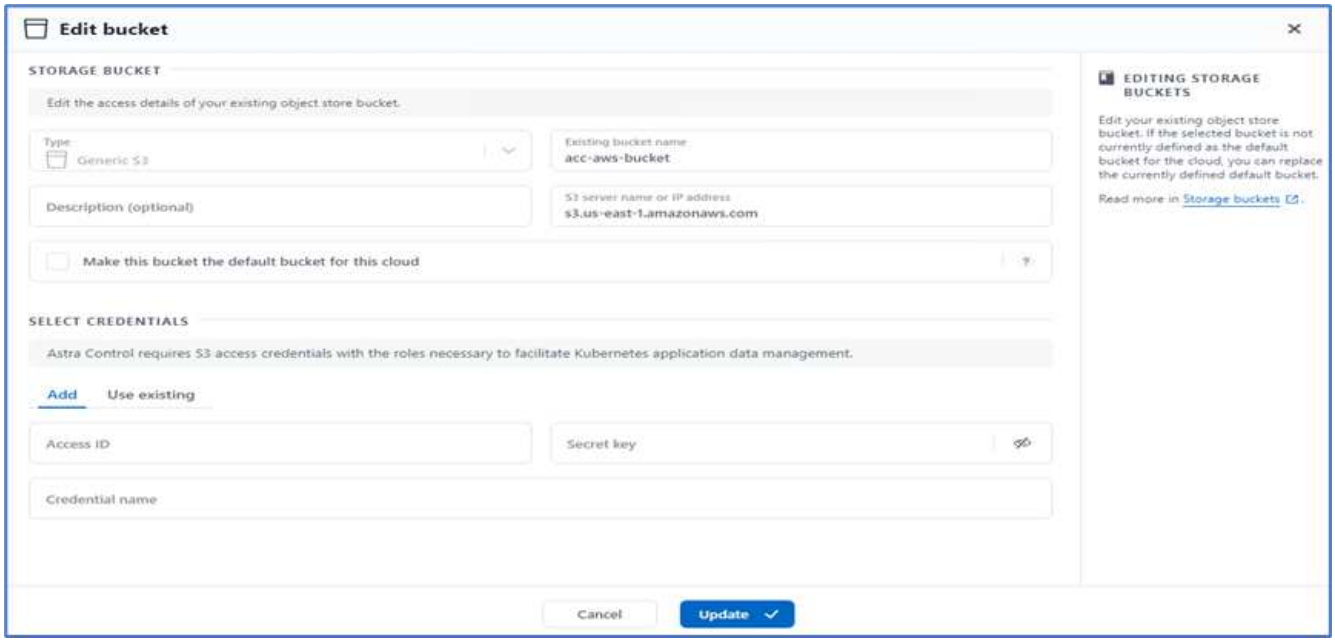
7. Fornire le credenziali ONTAP e fare clic su Avanti. Esaminare le informazioni e fare clic su Managed (gestito). I backend dovrebbero essere simili all'esempio seguente.



8. Per aggiungere un bucket ad Astra Control, selezionare Bucket e fare clic su Add (Aggiungi).

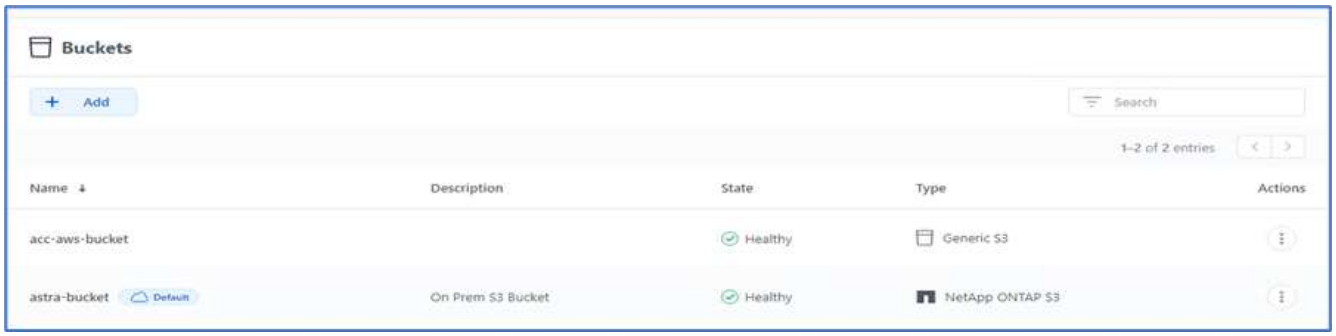


9. Selezionare il tipo di bucket e fornire il nome del bucket, il nome del server S3 o l'indirizzo IP e la credenziale S3. Fare clic su Aggiorna.



In questa soluzione vengono utilizzati entrambi i bucket AWS S3 e ONTAP S3. È anche possibile utilizzare StorageGRID.

Lo stato del bucket deve essere integro.



Come parte della registrazione del cluster Kubernetes con Astra Control Center per la gestione dei dati applicativa, Astra Control crea automaticamente associazioni di ruoli e uno spazio dei nomi di monitoraggio NetApp per raccogliere metriche e log dai pod di applicazioni e dai nodi di lavoro. Impostare una delle classi di storage basate su ONTAP supportate come predefinita.

Dopo di lei "Aggiungere un cluster alla gestione di Astra Control", È possibile installare le applicazioni sul cluster (al di fuori di Astra Control) e quindi andare alla pagina Apps (applicazioni) in Astra Control per gestire le applicazioni e le relative risorse. Per ulteriori informazioni sulla gestione delle applicazioni con Astra, consultare "Requisiti di gestione delle applicazioni".

"Pagina successiva: Panoramica sulla convalida della soluzione."

Convalida della soluzione

Panoramica

"Precedente: Installazione di Astra Control Center su OpenShift Container Platform."

In questa sezione, rivisudiamo la soluzione con alcuni casi di utilizzo:

- Ripristino di un'applicazione stateful da un backup remoto a un altro cluster OpenShift in esecuzione nel cloud.
- Ripristino di un'applicazione stateful nello stesso namespace nel cluster OpenShift.
- Mobilità applicativa mediante cloning da un sistema FlexPod (piattaforma container OpenShift Bare Metal) a un altro sistema FlexPod (piattaforma container OpenShift su VMware).

In particolare, in questa soluzione vengono validati solo pochi casi di utilizzo. Questa convalida non rappresenta in alcun modo l'intera funzionalità di Astra Control Center.

"Successivo: Ripristino delle applicazioni con backup remoti."

Recovery dell'applicazione con backup remoti

"Precedente: Panoramica sulla convalida della soluzione."

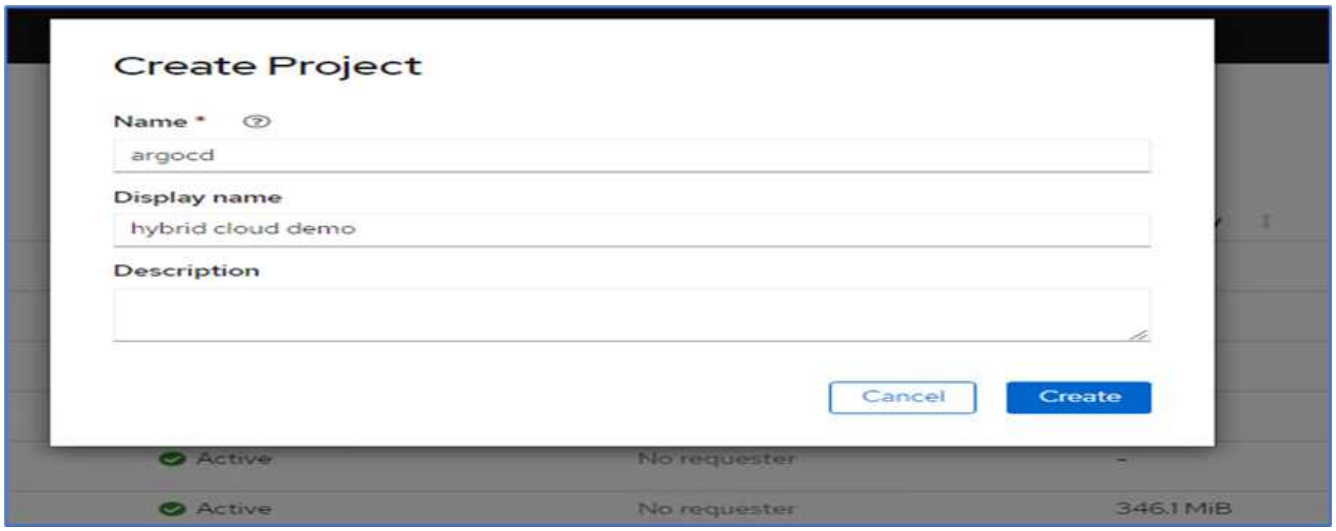
Con Astra, puoi eseguire un backup completo coerente con l'applicazione che può

essere utilizzato per ripristinare l'applicazione con i suoi dati in un cluster Kubernetes diverso in esecuzione in un data center on-premise o in un cloud pubblico.

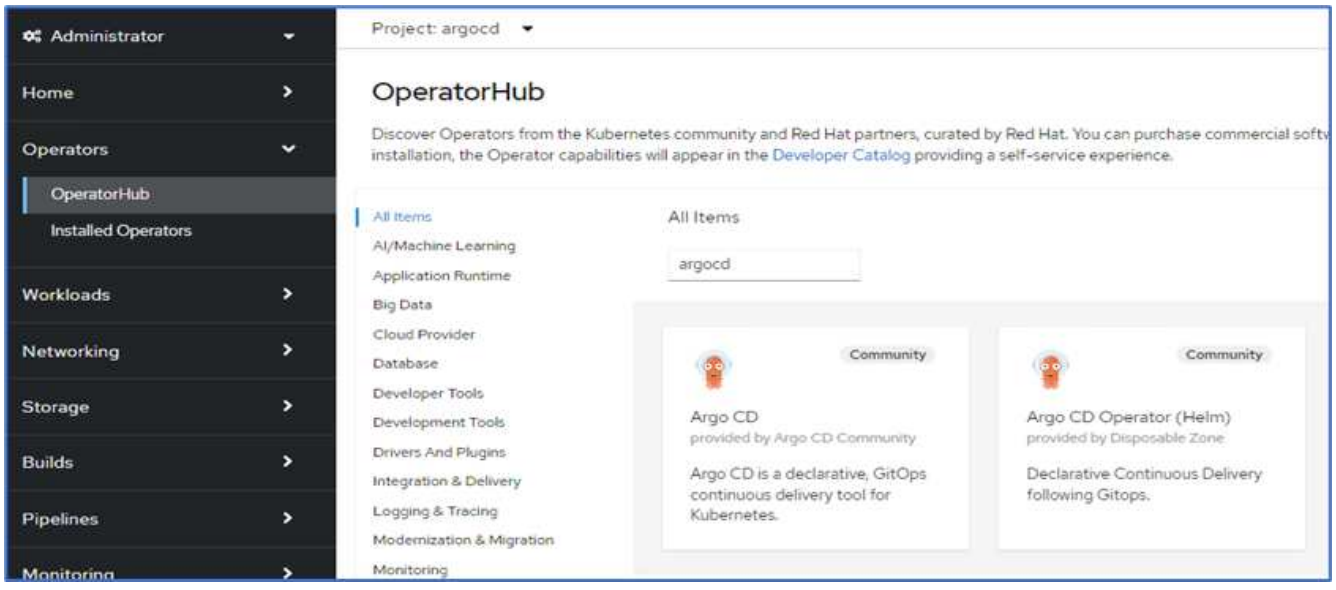
Per convalidare un ripristino dell'applicazione di successo, simulare un errore on-premise di un'applicazione in esecuzione sul sistema FlexPod e ripristinare l'applicazione su un cluster K8s in esecuzione nel cloud utilizzando un backup remoto.

L'applicazione di esempio è un'applicazione di listino prezzi che utilizza MySQL per il database. Per automatizzare l'implementazione, abbiamo utilizzato "CD Argo" tool. Argo CD è uno strumento dichiarativo, GitOps, per la consegna continua di Kubernetes.

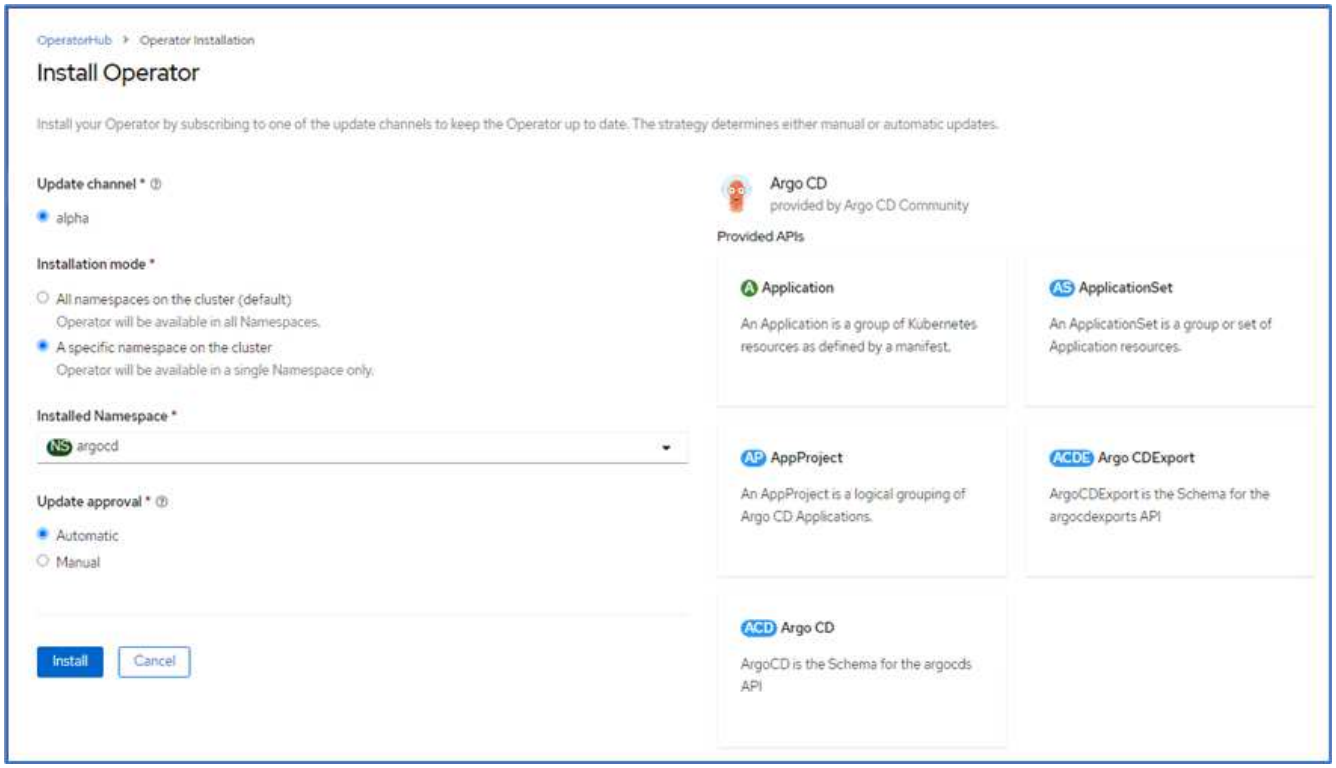
1. Accedi al cluster OpenShift on-premise e crea un nuovo progetto con il nome `argocd`.



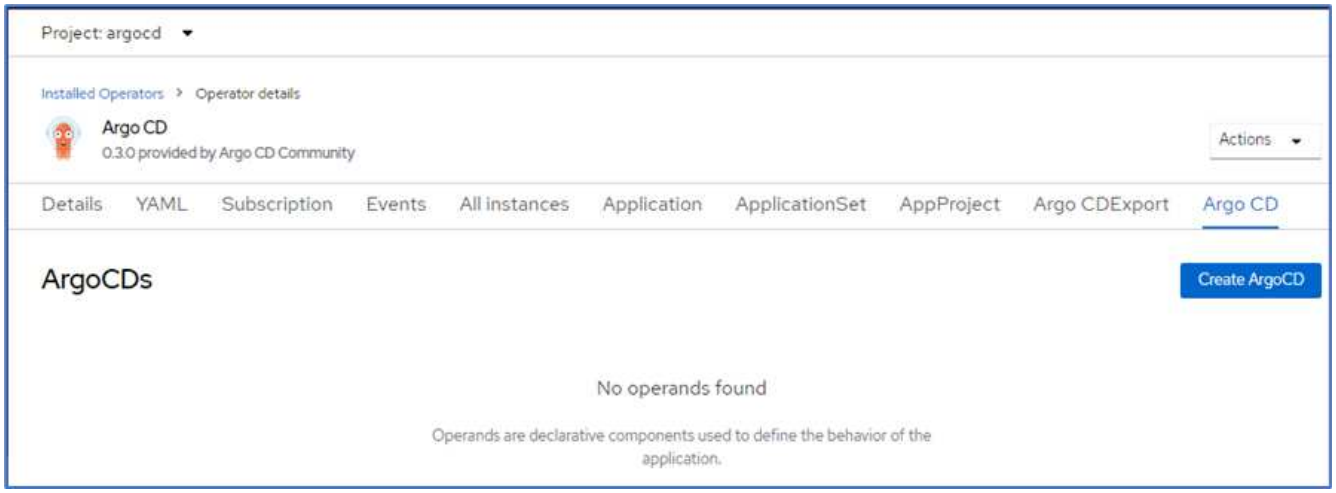
2. In OperatorHub, cercare `argocd` E selezionare Argo CD operator.



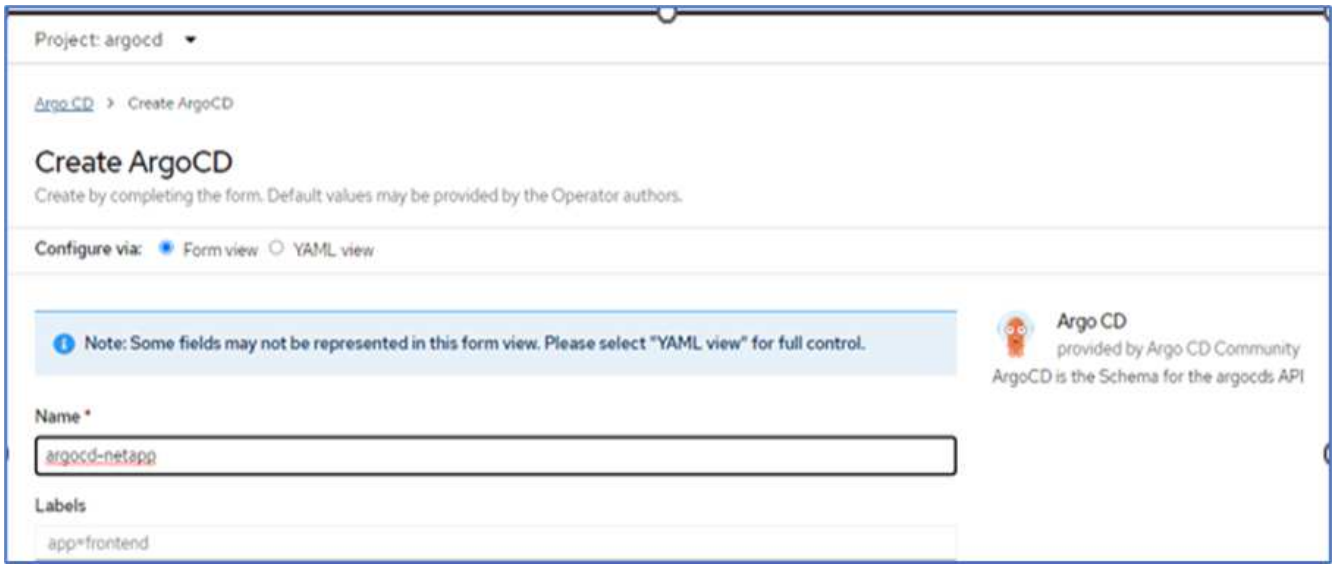
3. Installare l'operatore in `argocd` namespace.



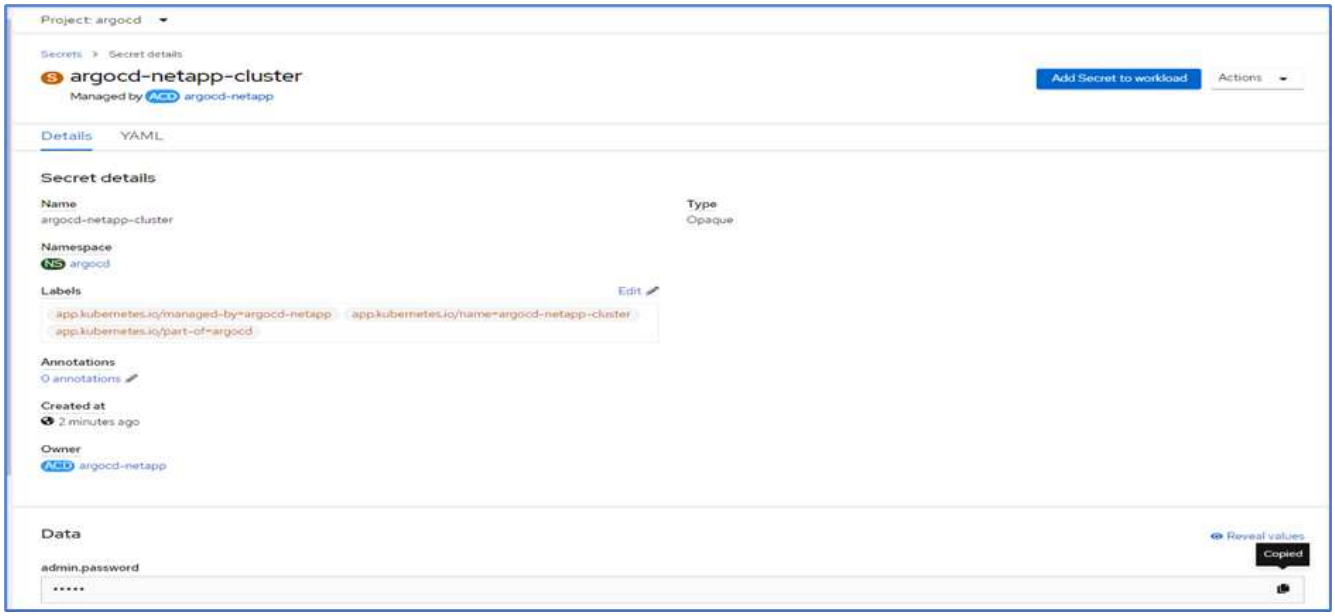
4. Accedere all'operatore e fare clic su Create ArgoCD (Crea ArgoCD).



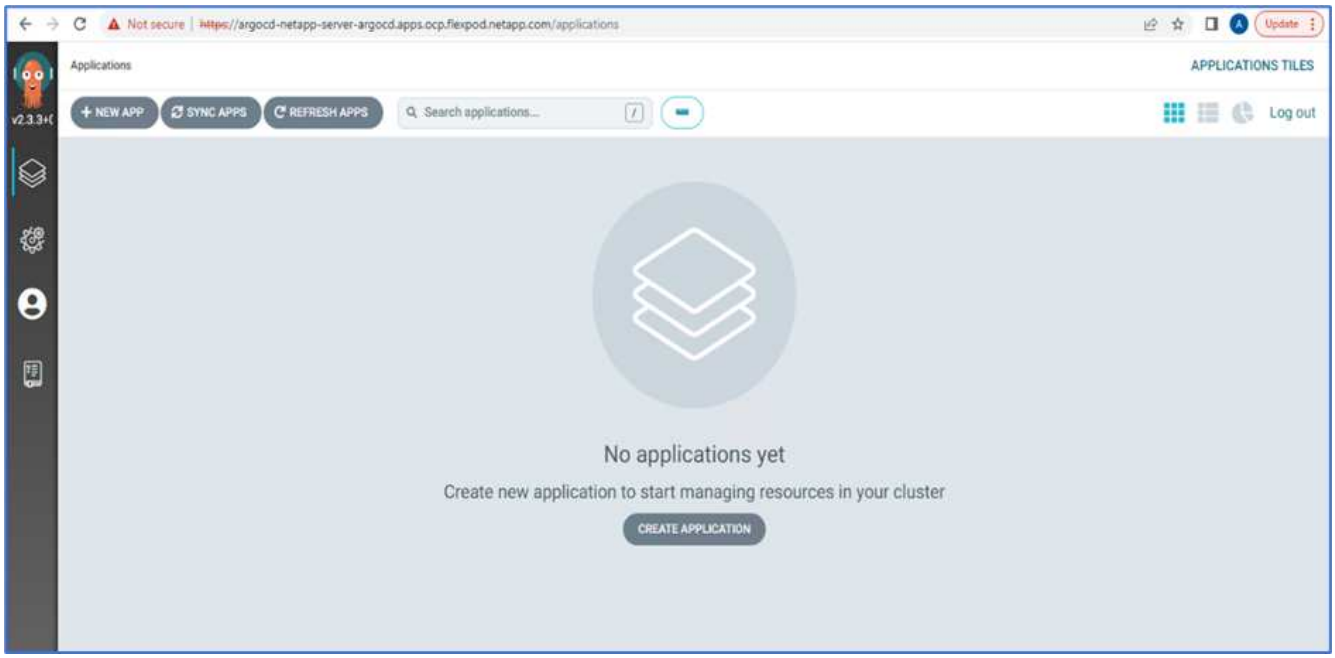
5. Per distribuire l'istanza del CD Argo in `argocd` Assegnare un nome e fare clic su Create (Crea).



6. Per accedere a Argo CD, l'utente predefinito è admin e la password si trova in un file segreto con il nome `argocd-netapp-cluster`.



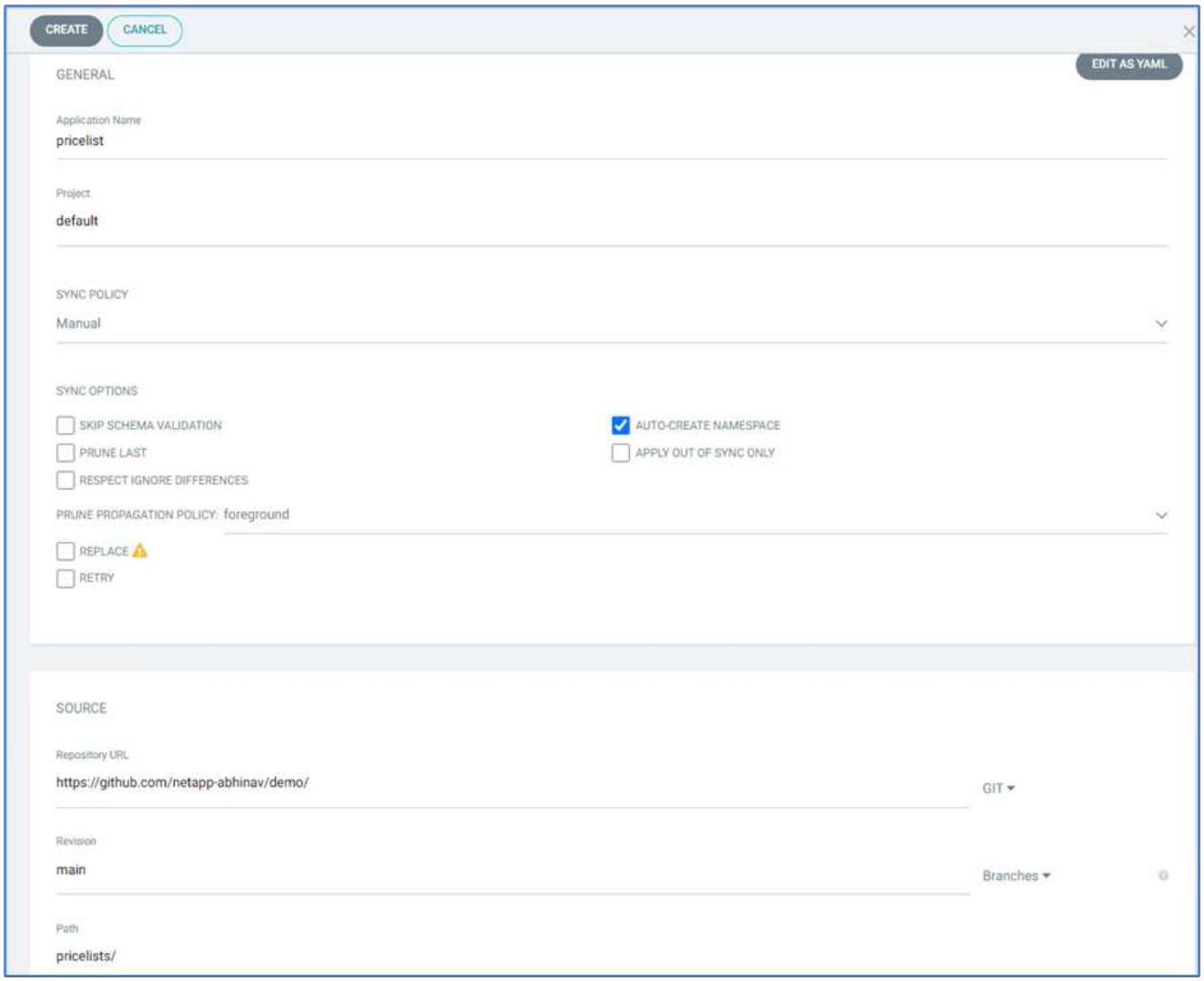
7. Dal menu laterale, selezionare routes > Location (percorsi > Località) e fare clic sull'URL del `argocd` percorsi. Immettere il nome utente e la password.



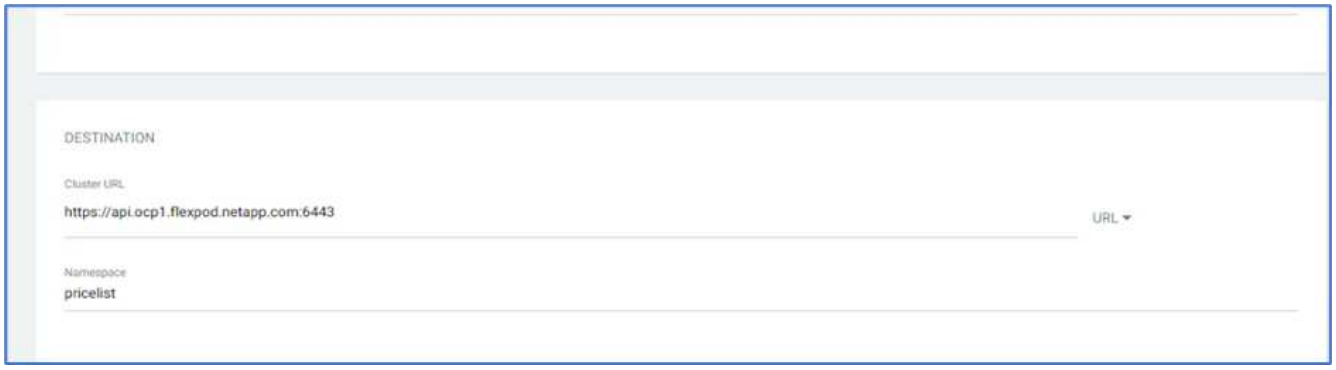
8. Aggiungere il cluster OpenShift on-premise al CD Argo attraverso la CLI.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

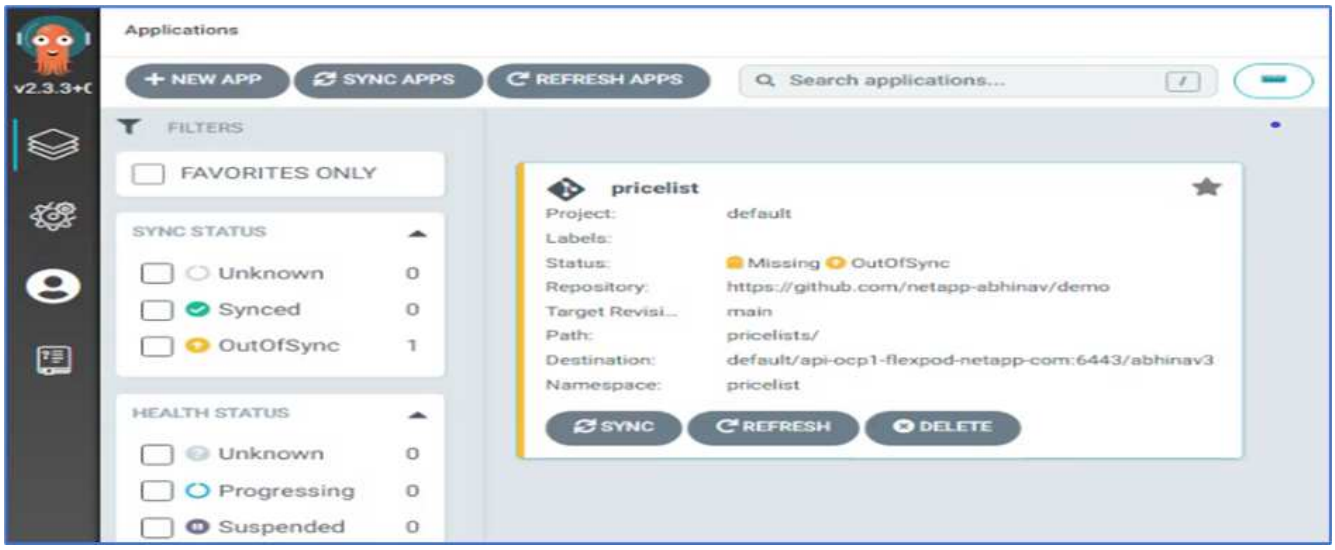
9. Nell'interfaccia utente di ArgoCD, fare clic SU NEW APP (NUOVA APPLICAZIONE) e immettere i dettagli relativi al nome dell'applicazione e al repository di codice.



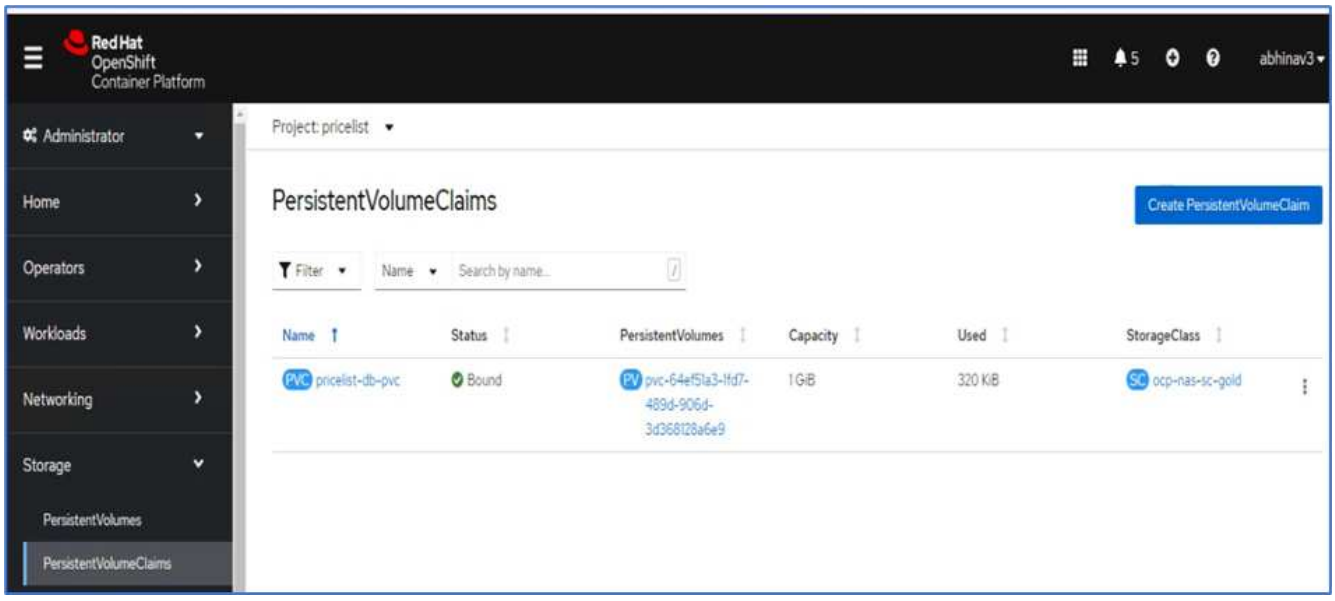
10. Inserire il cluster OpenShift in cui l'applicazione verrà implementata insieme allo spazio dei nomi.



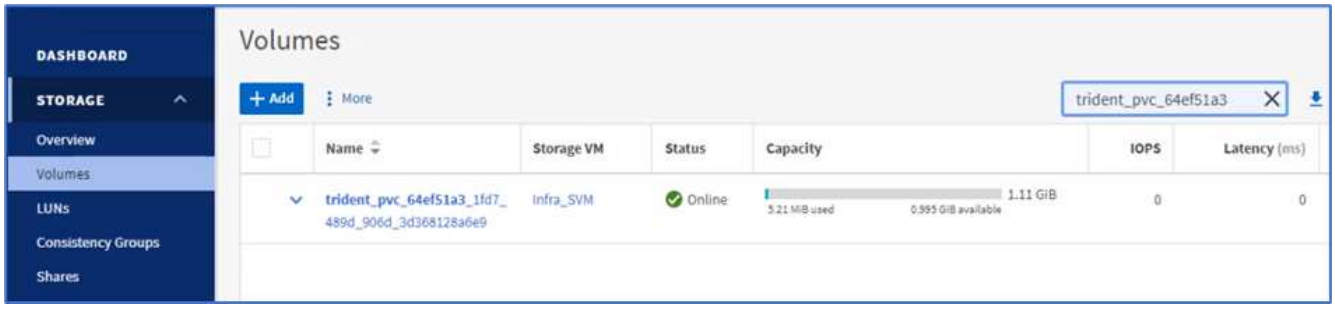
11. Per implementare l'applicazione sul cluster OpenShift on-premise, fare clic su SYNC.



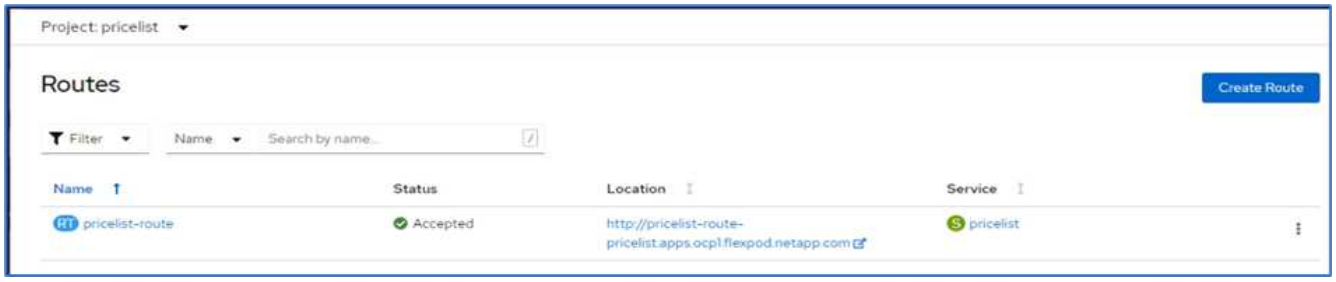
12. Nella console di OpenShift Container Platform, accedere a Preventivo progetto e, in Storage, verificare il nome e le dimensioni del PVC.



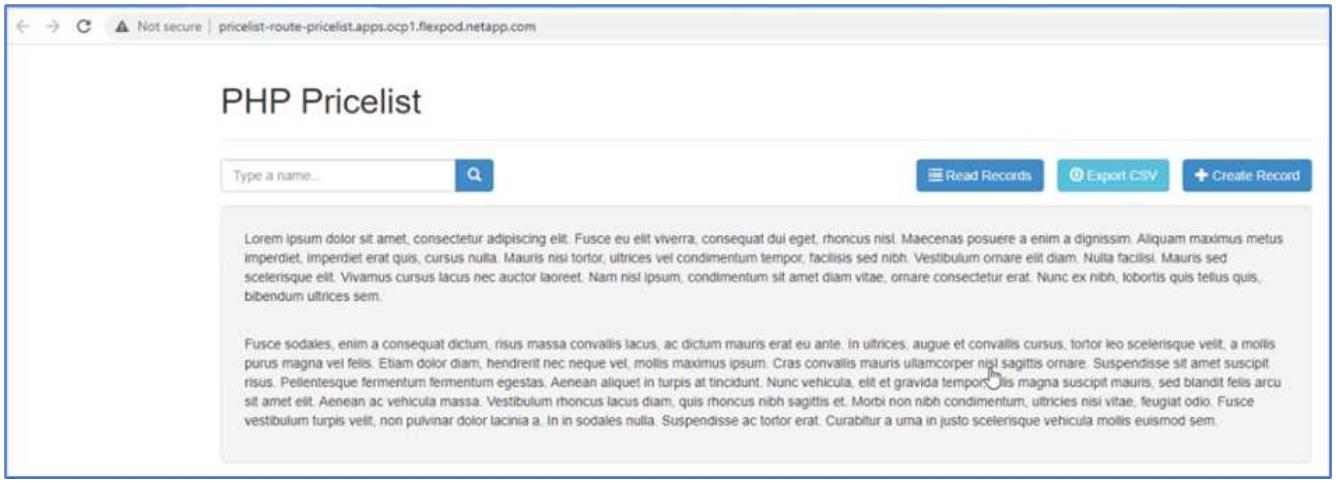
13. Accedere a System Manager e verificare il PVC.



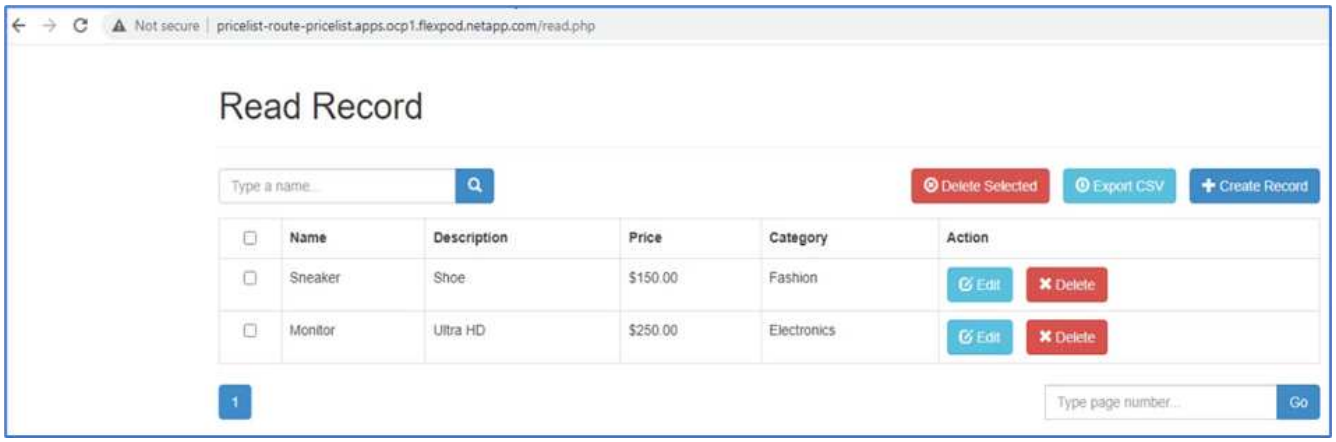
14. Una volta eseguiti i pod, selezionare rete > percorsi dal menu laterale, quindi fare clic sull'URL in posizione.



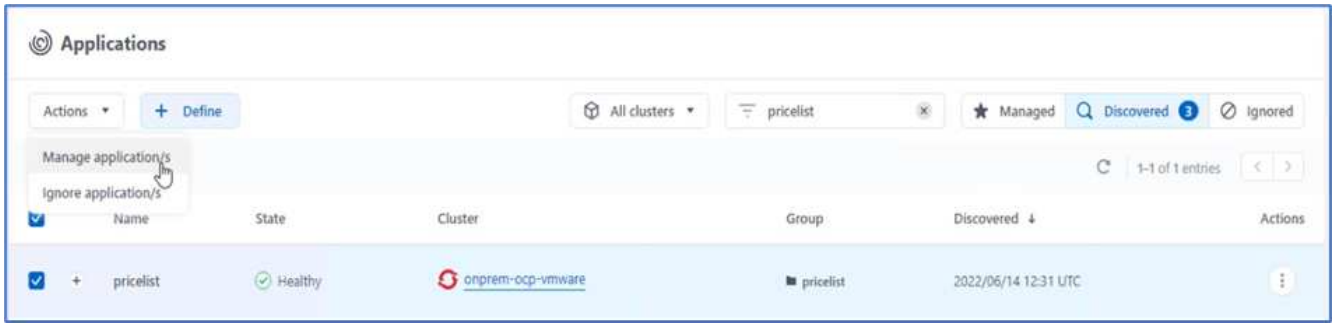
15. Viene visualizzata la pagina iniziale dell'applicazione Pricelist.



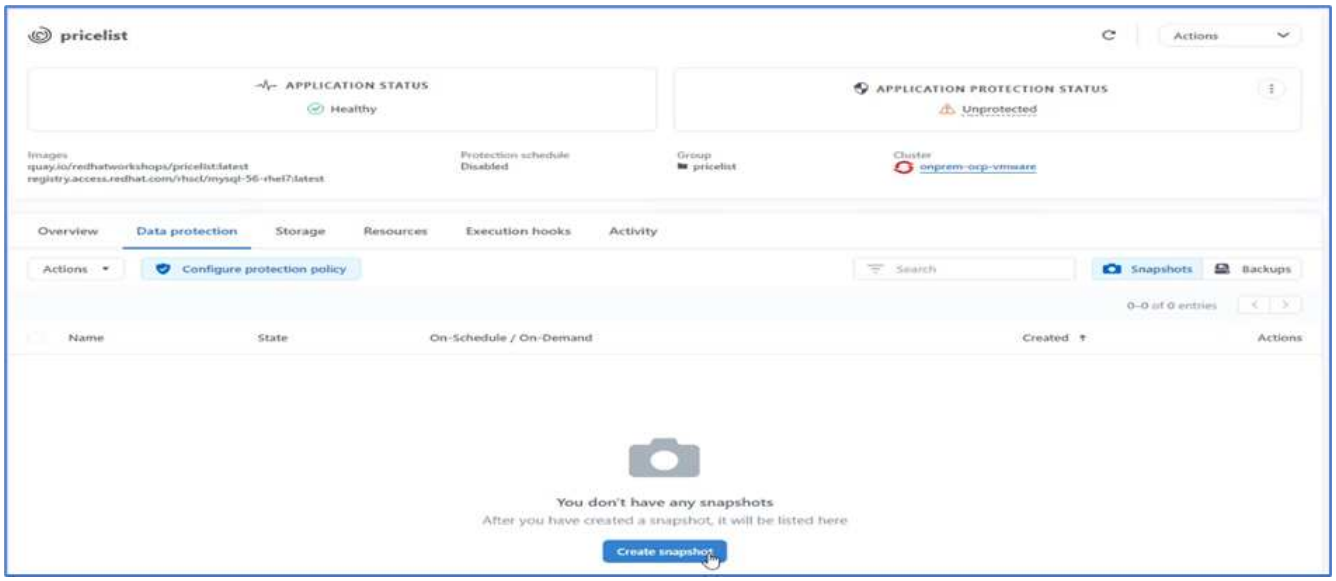
16. Creare alcuni record nella pagina Web.



17. L'applicazione viene scoperta in Astra Control Center. Per gestire l'applicazione, accedere ad applicazioni > rilevate, selezionare l'applicazione Listino prezzi e fare clic su Gestisci applicazioni in azioni.

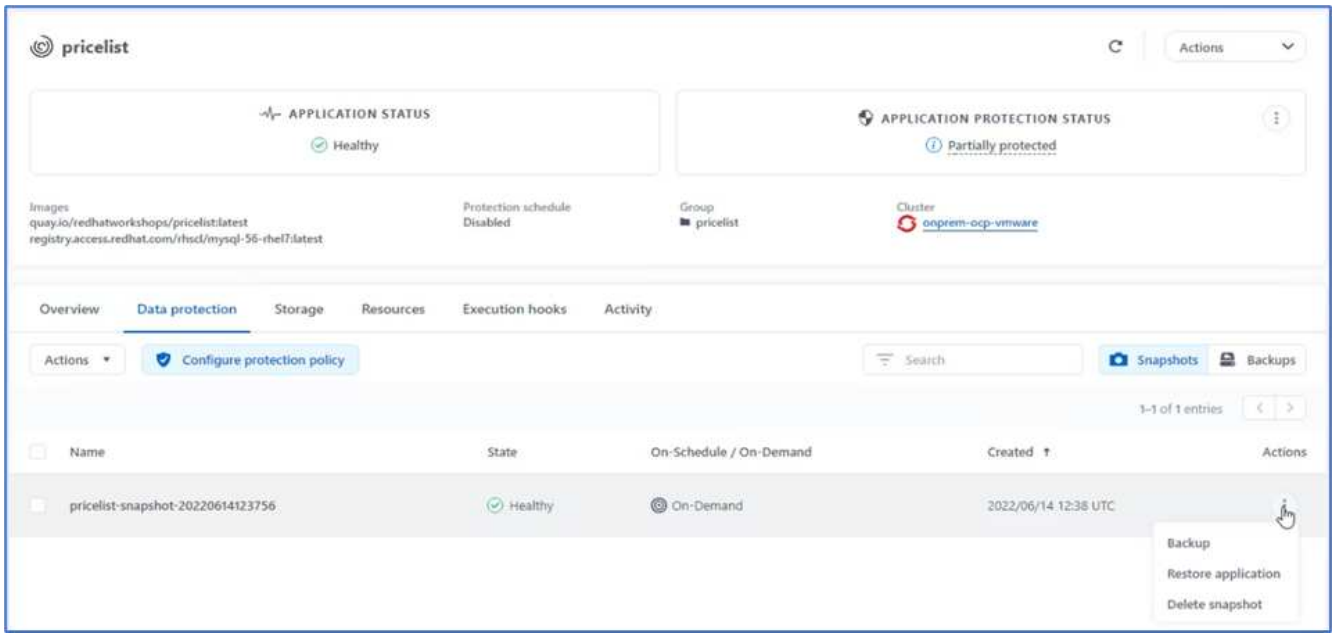


18. Fare clic sull'applicazione Listino prezzi e selezionare Data Protection (protezione dati). A questo punto, non dovrebbero esserci snapshot o backup. Fare clic su Create Snapshot (Crea istantanea) per creare un'istantanea on-demand.

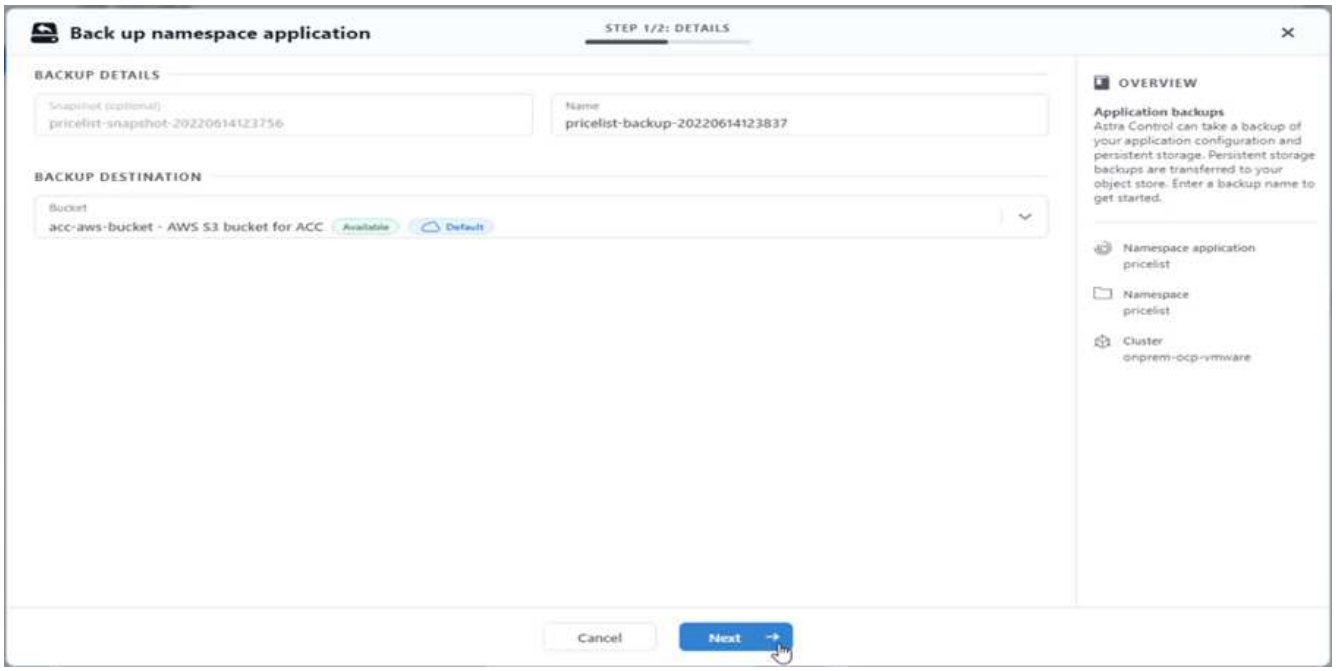


NetApp Astra Control Center supporta backup e snapshot on-demand e pianificati.

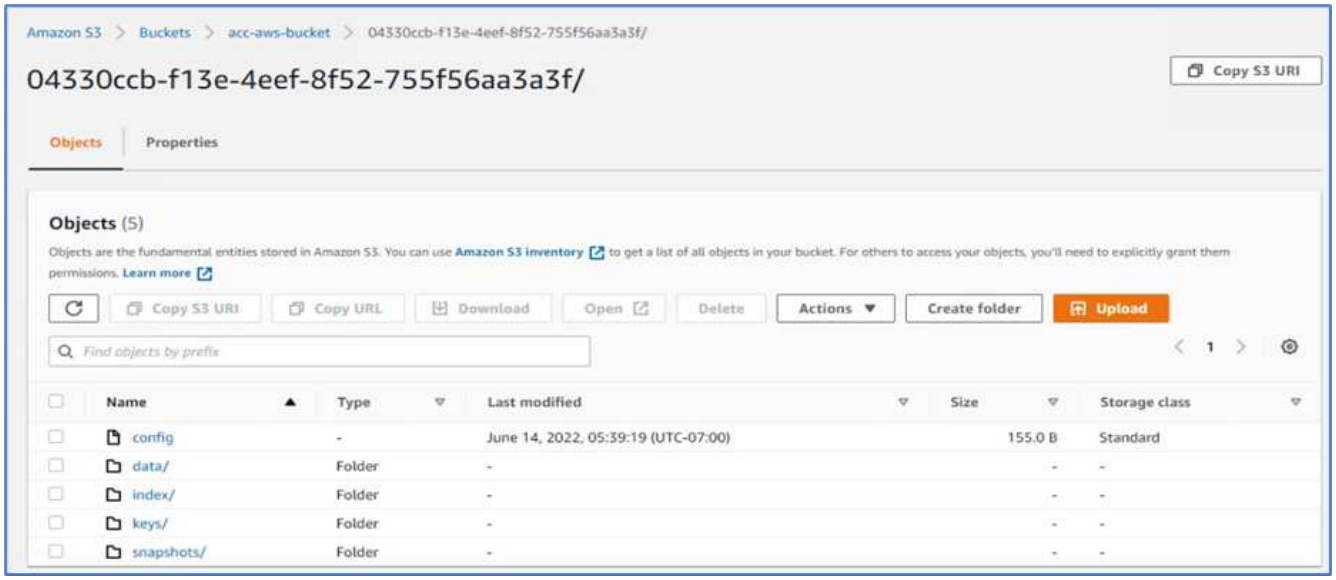
19. Una volta creata la snapshot e lo stato è integro, creare un backup remoto utilizzando tale snapshot. Questo backup viene memorizzato nel bucket S3.



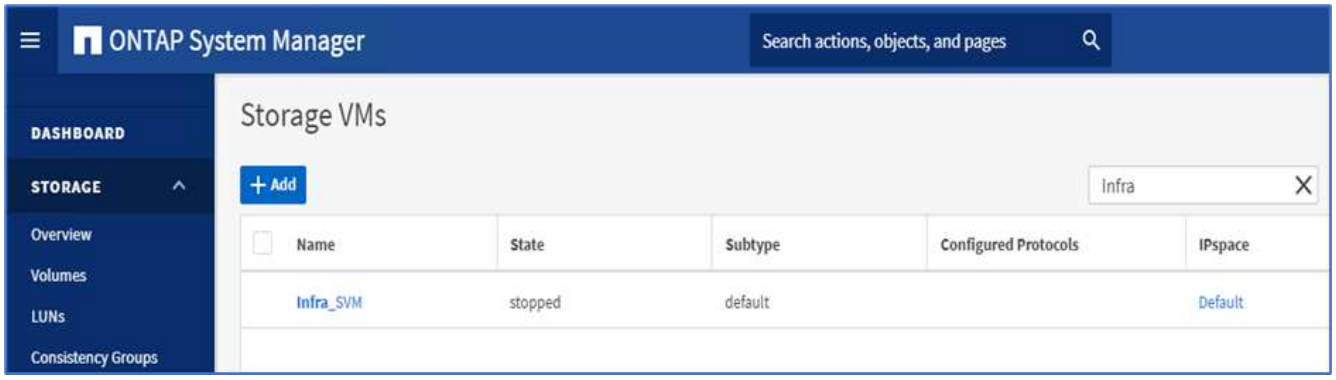
20. Selezionare il bucket AWS S3 e avviare l'operazione di backup.



21. L'operazione di backup deve creare una cartella con più oggetti nel bucket AWS S3.



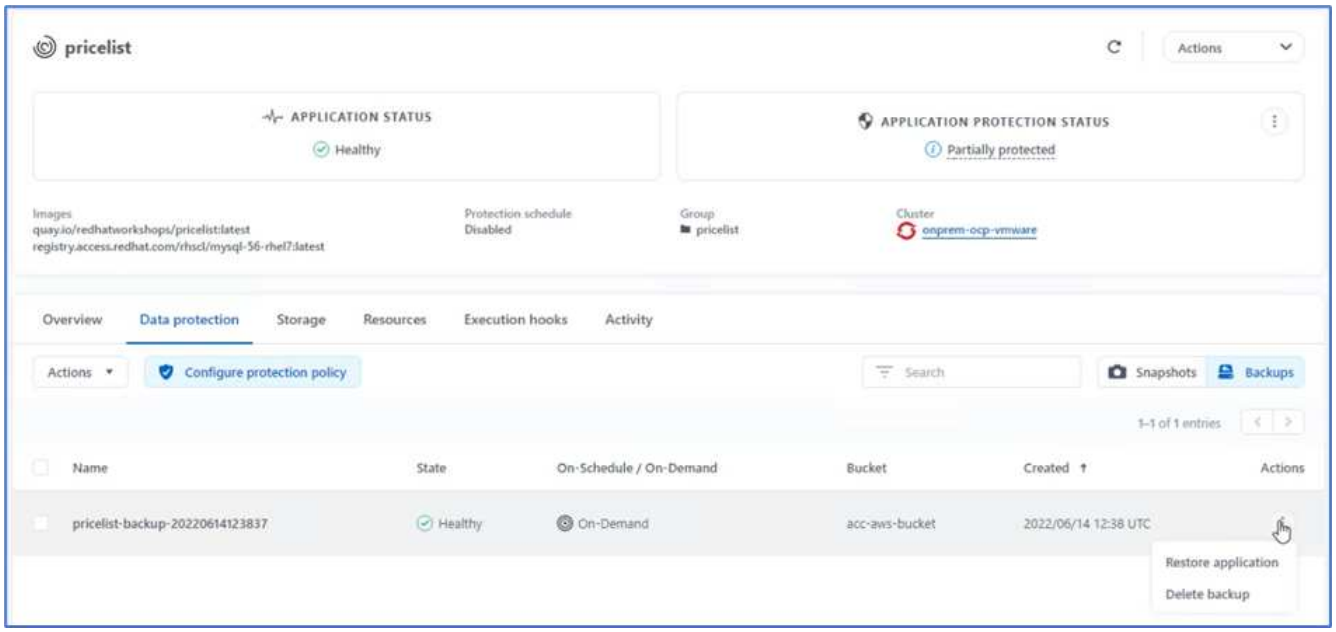
22. Una volta completato il backup remoto, simulare un disastro on-premise arrestando la storage virtual machine (SVM) che ospita il volume di backup per il PV.



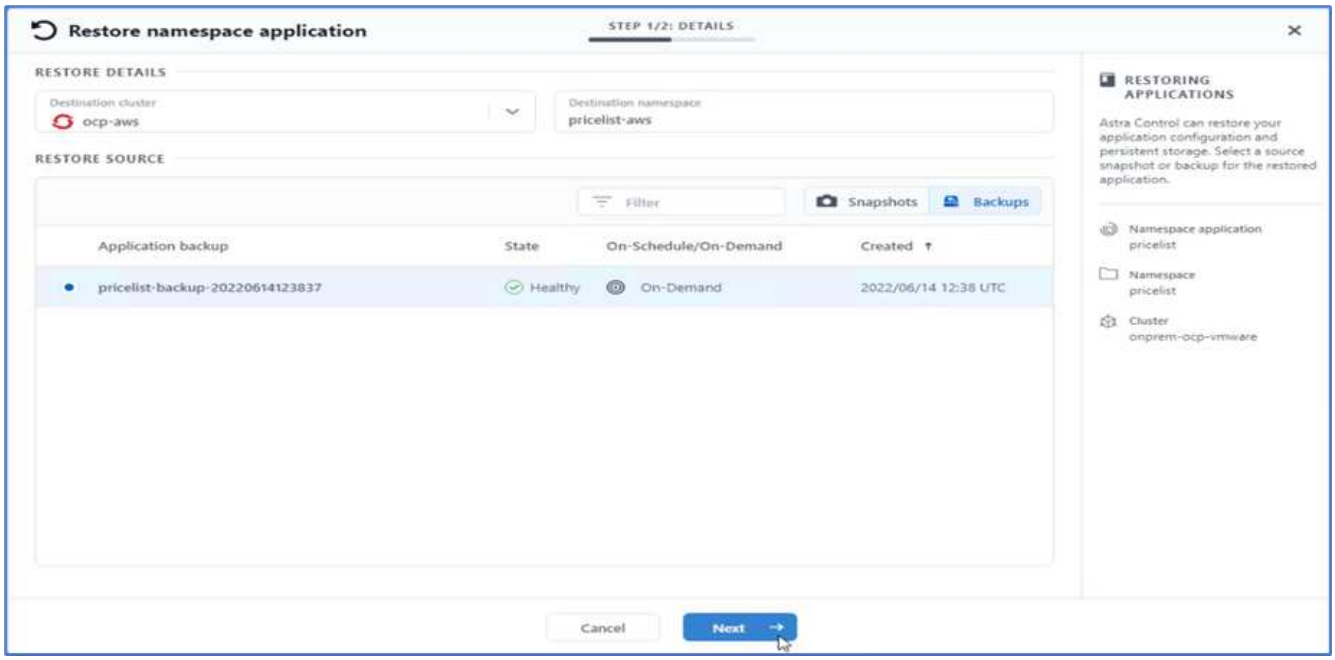
23. Aggiornare la pagina Web per confermare l'interruzione. La pagina web non è disponibile.

Come previsto, il sito Web non è disponibile, quindi ripristiniamo rapidamente l'applicazione dal backup remoto utilizzando Astra al cluster OpenShift in esecuzione in AWS.

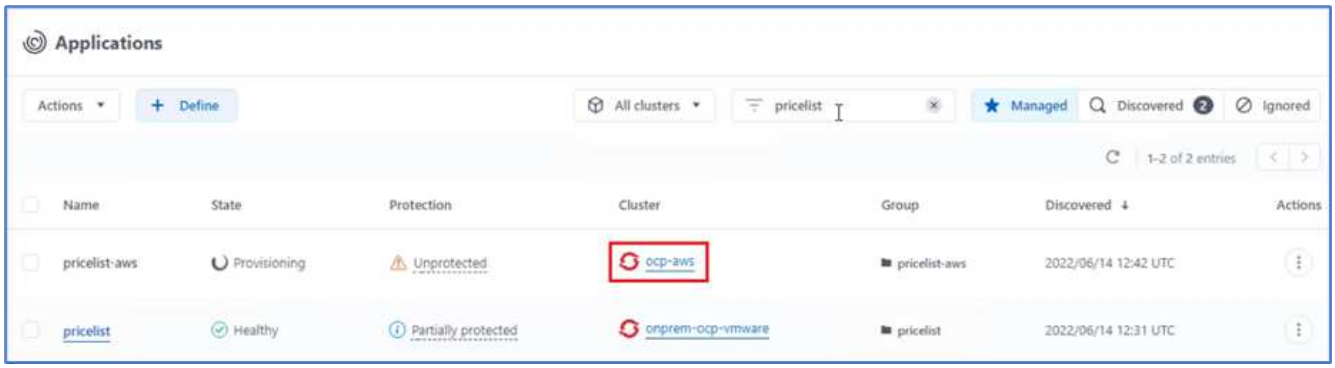
24. In Astra Control Center, fare clic sull'applicazione Pricelist e selezionare Data Protection > Backups (protezione dati > Backup). Selezionare il backup e fare clic su Restore Application (Ripristina applicazione) sotto Action (azione).



25. Selezionare `ocp-aws` come cluster di destinazione e assegnare un nome allo spazio dei nomi. Fare clic sul backup on-demand, su Next (Avanti), quindi su Restore (Ripristina).

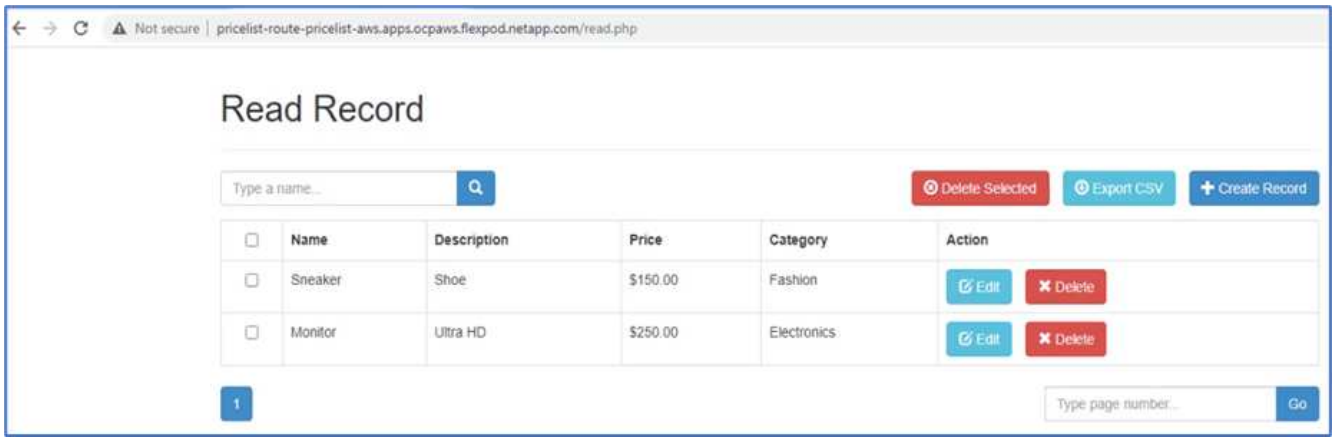


26. Una nuova applicazione con il nome `pricelist-app` Viene eseguito il provisioning sul cluster OpenShift in esecuzione in AWS.



27. Verificare lo stesso nella console Web di OpenShift.

28. Dopo tutti i pod sotto `pricelist-aws` Il progetto è in esecuzione, accedere a routes e fare clic sull'URL per avviare la pagina Web.



Questo processo convalida che l'applicazione Pricelist è stata ripristinata correttamente e che l'integrità dei dati è stata mantenuta sul cluster OpenShift che funziona perfettamente su AWS con l'aiuto di Astra Control Center.

Protezione dei dati con copie Snapshot e mobilità applicativa per DevTest

Questo caso d'utilizzo è costituito da due parti, come descritto nelle sezioni seguenti.

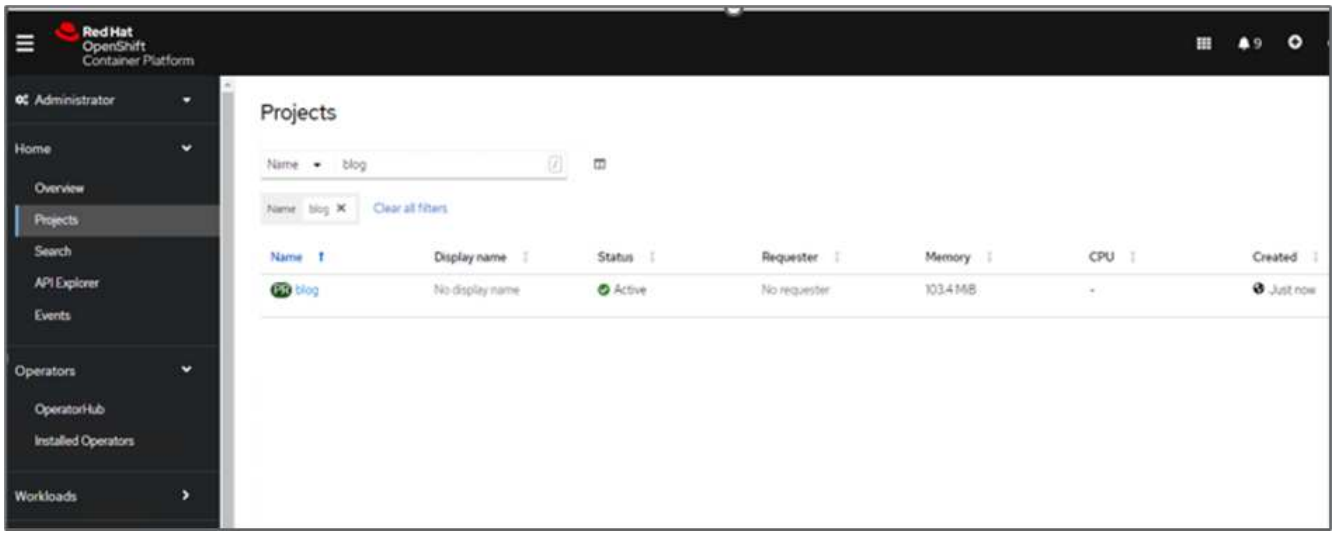
Parte 1

Con Astra Control Center, puoi creare snapshot application-aware per la protezione dei dati locali. In caso di eliminazione o danneggiamento accidentale dei dati, è possibile ripristinare le applicazioni e i dati associati a uno stato sicuramente funzionante utilizzando uno snapshot precedentemente registrato.

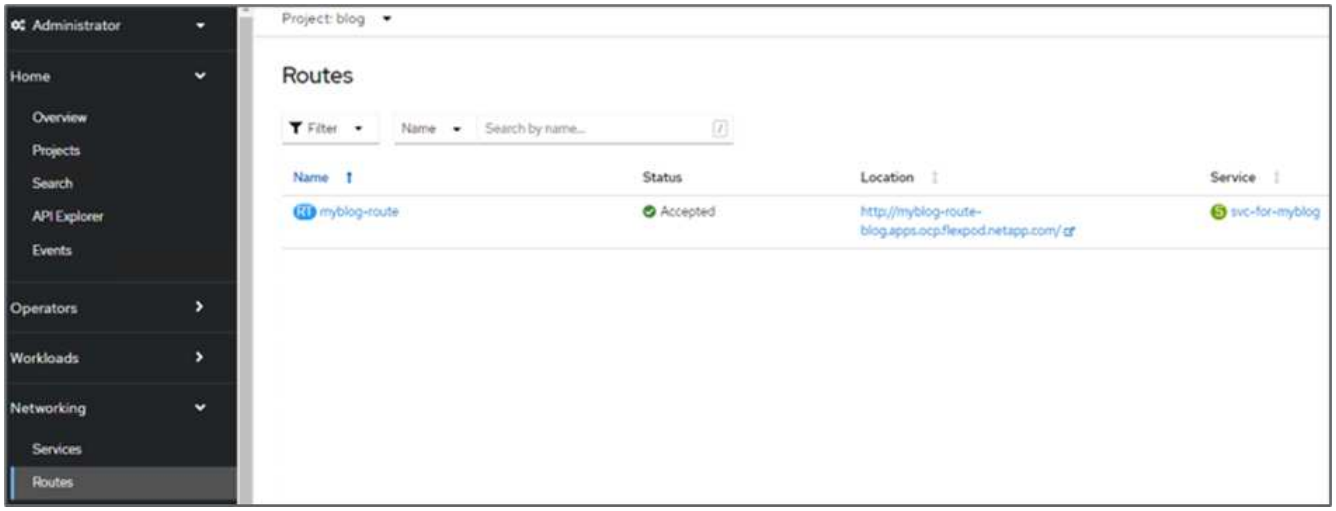
In questo scenario, un team di sviluppo e test (DevTest) implementa un'applicazione stateful di esempio (sito blog) che è un'applicazione blog Ghost, aggiunge alcuni contenuti e aggiorna l'applicazione alla versione più recente disponibile. L'applicazione Ghost utilizza SQLite per il database. Prima di aggiornare l'applicazione, viene eseguita una snapshot (on-demand) utilizzando Astra Control Center per la protezione dei dati. I passaggi dettagliati sono i seguenti:

1. Implementa l'app blogging di esempio e sincronizzala da ArgoCD.

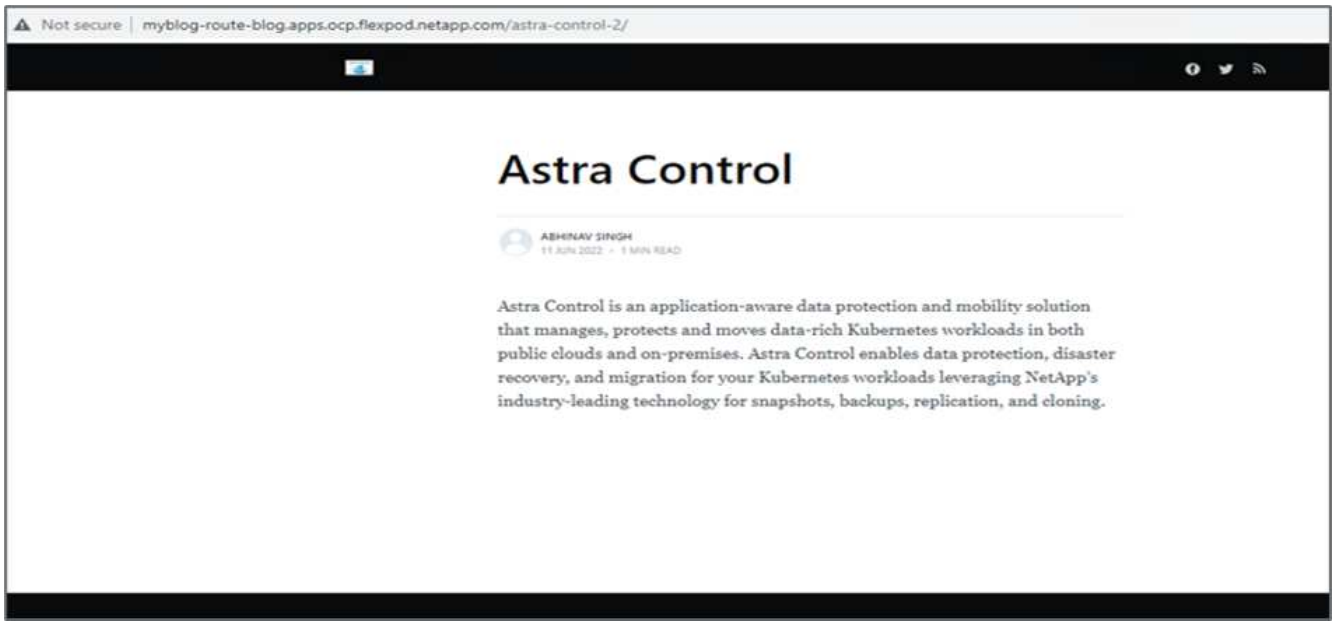
2. Accedere al primo cluster OpenShift, selezionare Project (progetto) e inserire Blog nella barra di ricerca.



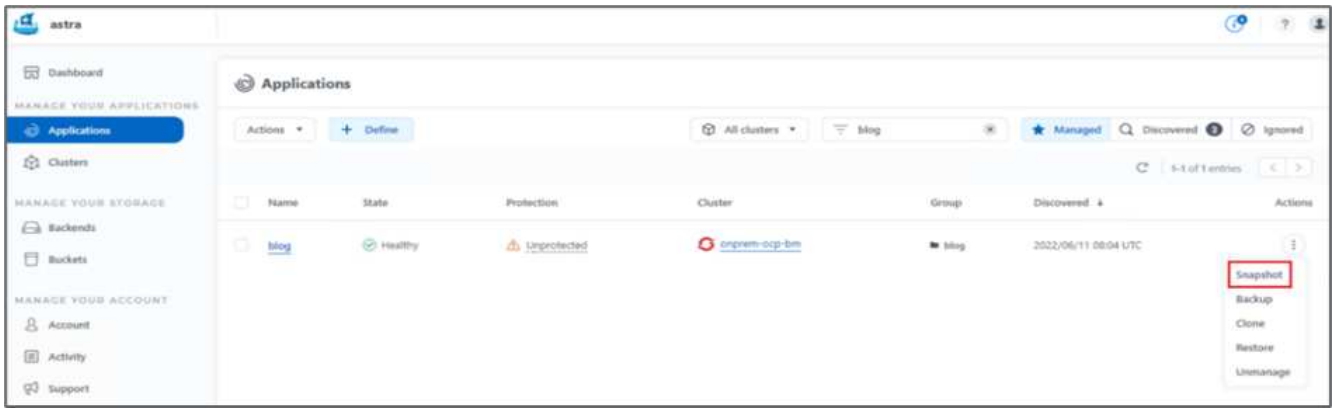
3. Dal menu laterale, selezionare rete > percorsi e fare clic sull'URL.



4. Viene visualizzata la home page del blog. Aggiungi alcuni contenuti al sito del blog e pubblicali.



5. Accedere a Astra Control Center. Gestire l'applicazione dalla scheda rilevato, quindi eseguire una copia Snapshot.

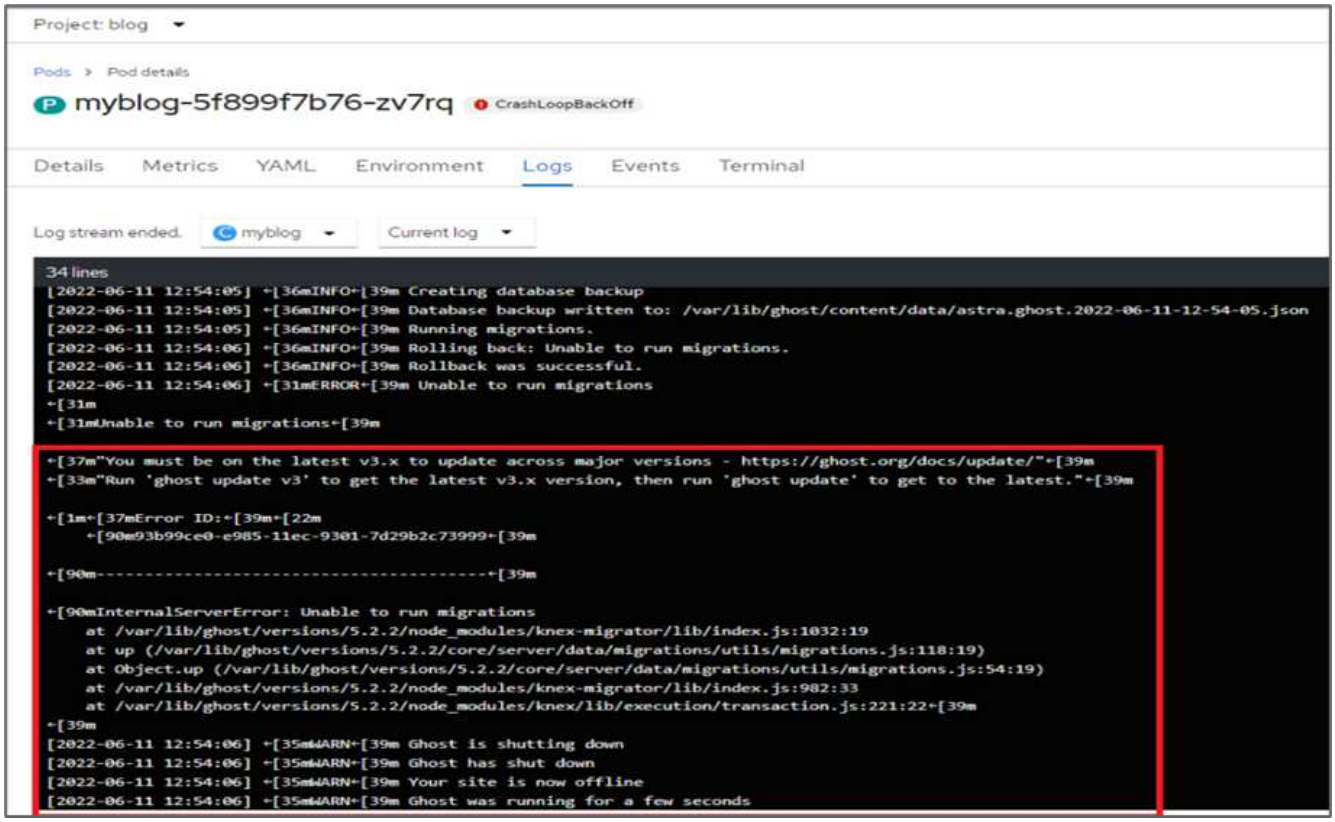


Puoi anche proteggere le tue applicazioni creando snapshot, backup o entrambi in base a una pianificazione definita. Per ulteriori informazioni, vedere "Proteggi le app con snapshot e backup".

6. Una volta creata correttamente l'istantanea on-Demand, aggiorna l'applicazione alla versione più recente. La versione corrente dell'immagine è `ghost: 3.6-alpine` e la versione di destinazione è `ghost:latest`. Per aggiornare l'applicazione, apportare le modifiche direttamente al repository Git e sincronizzarle con il CD Argo.

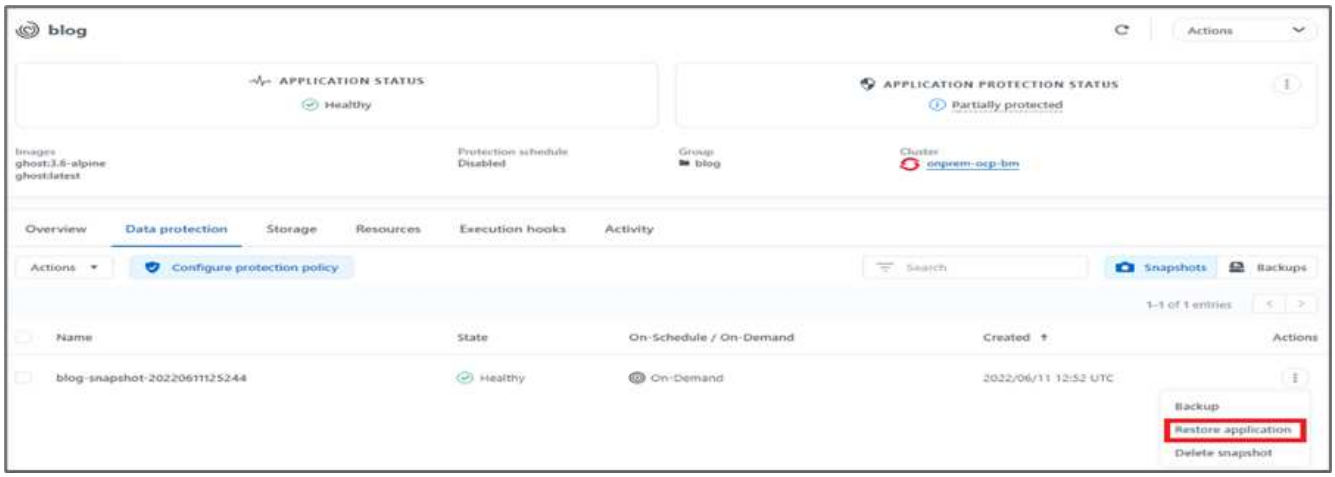
```
spec:
  containers:
  - name: myblog
    image: ghost:latest
    imagePullPolicy: Always
    ports:
    - containerPort: 2368
```

7. L'aggiornamento diretto alla versione più recente non è supportato a causa della disattivazione del sito del blog e del danneggiamento dell'intera applicazione.

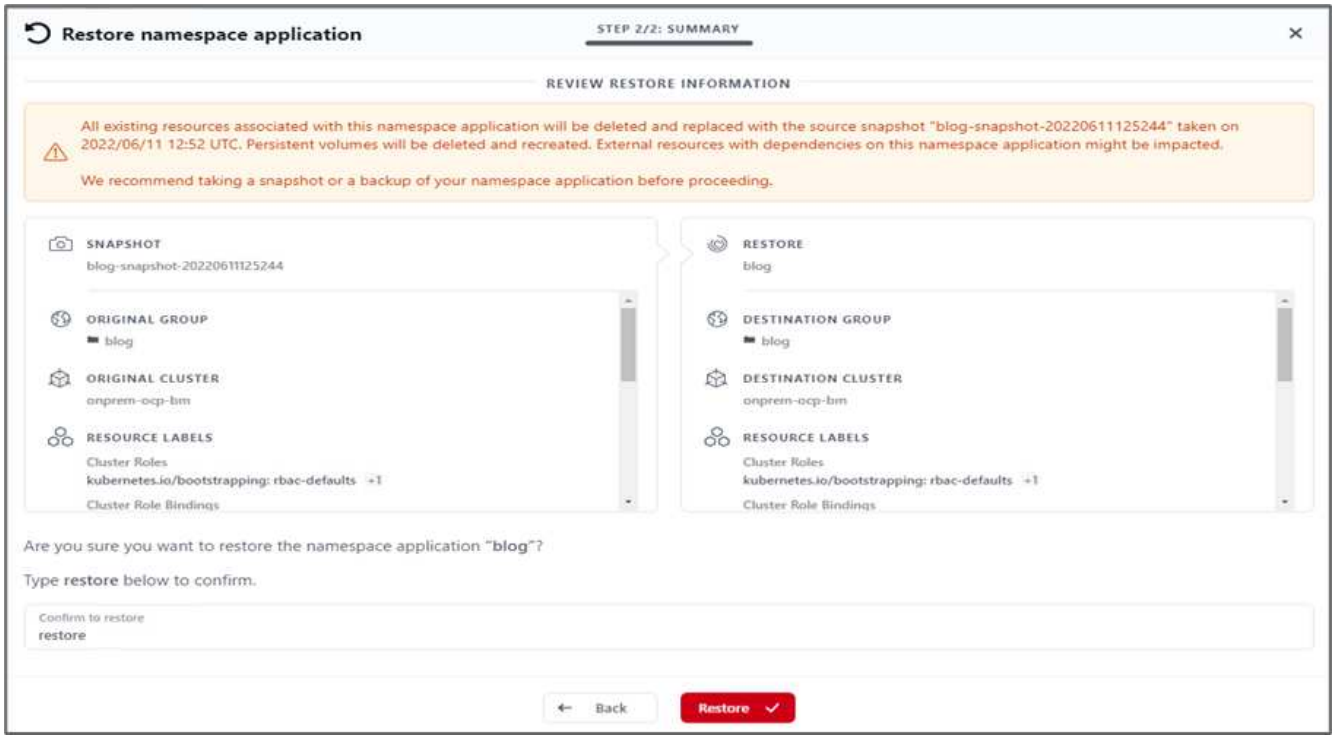


8. Per confermare la non disponibilità del sito del blog, aggiornare l'URL.

9. Ripristinare l'applicazione dallo snapshot.



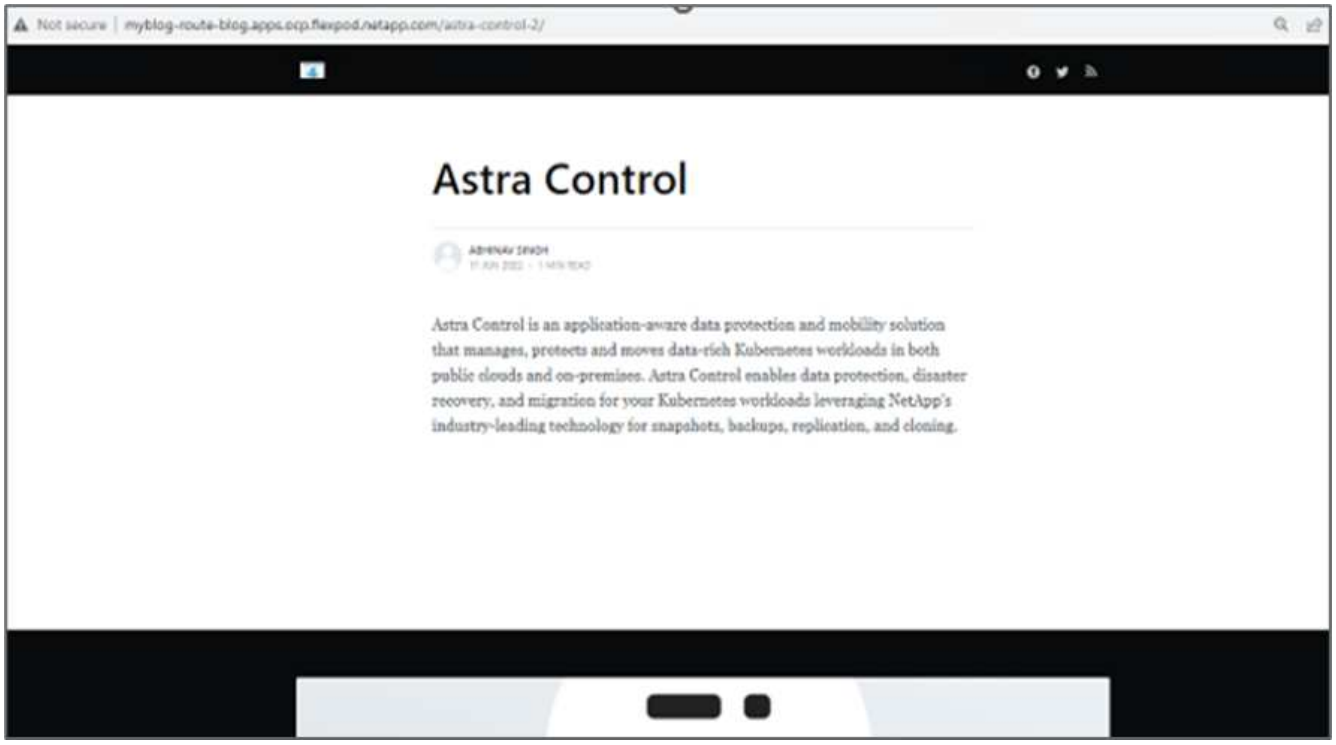
10. L'applicazione viene ripristinata sullo stesso cluster OpenShift.



11. Il processo di ripristino dell'applicazione viene avviato immediatamente.

12. In pochi minuti, l'applicazione viene ripristinata correttamente dallo snapshot disponibile.

13. Per verificare se la pagina Web è disponibile, aggiornare l'URL.

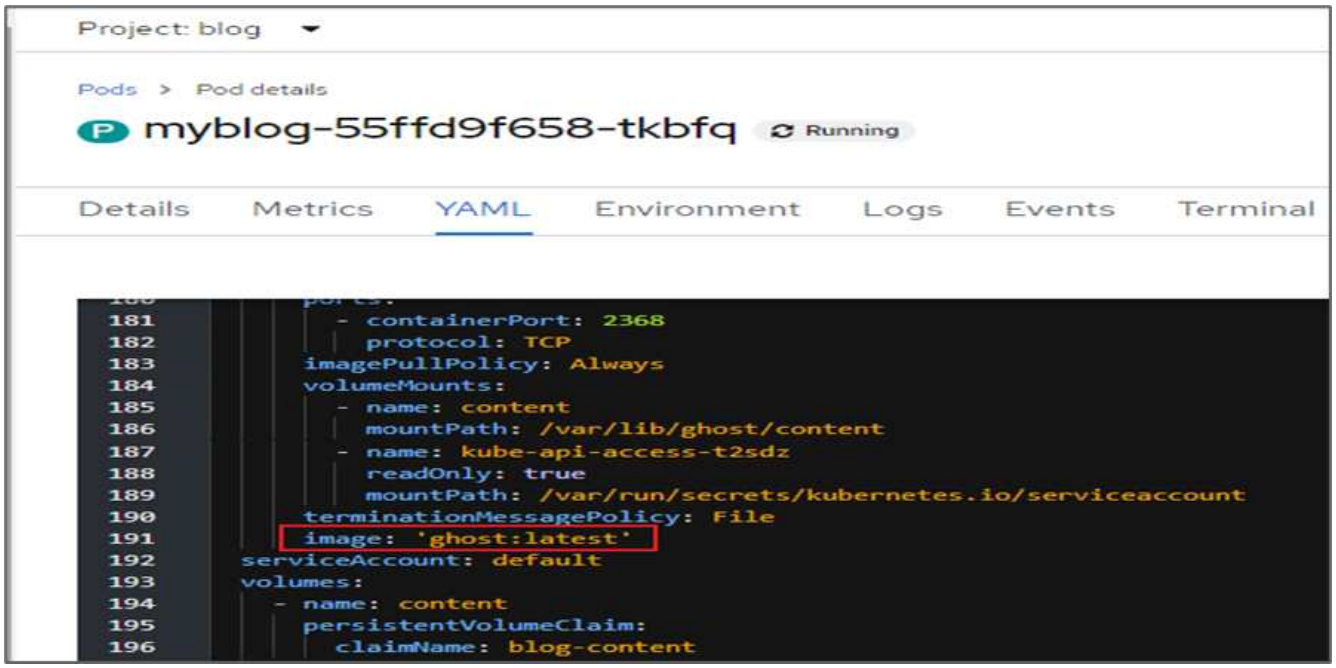


Con l'aiuto di Astra Control Center, un team DevTest può ripristinare con successo un'applicazione del sito del blog e i dati associati utilizzando lo snapshot.

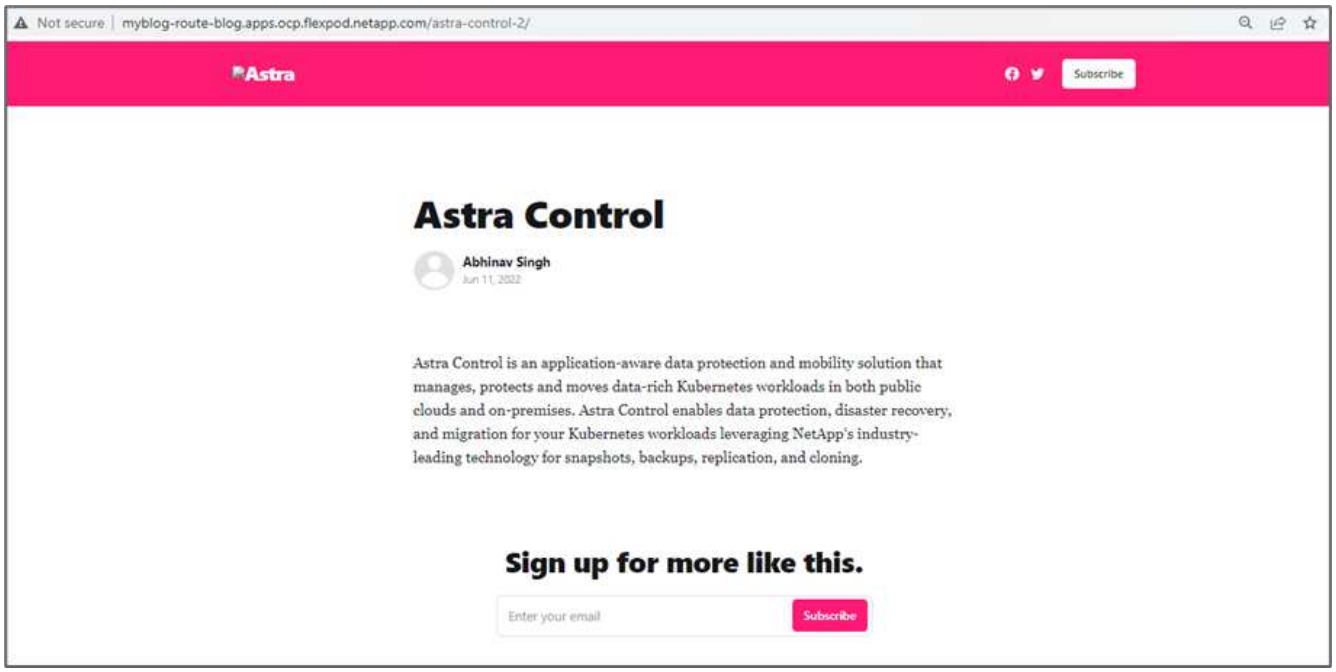
Parte 2

Con Astra Control Center, puoi spostare un'intera applicazione insieme ai suoi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trovano i cluster (on-premise o nel cloud).

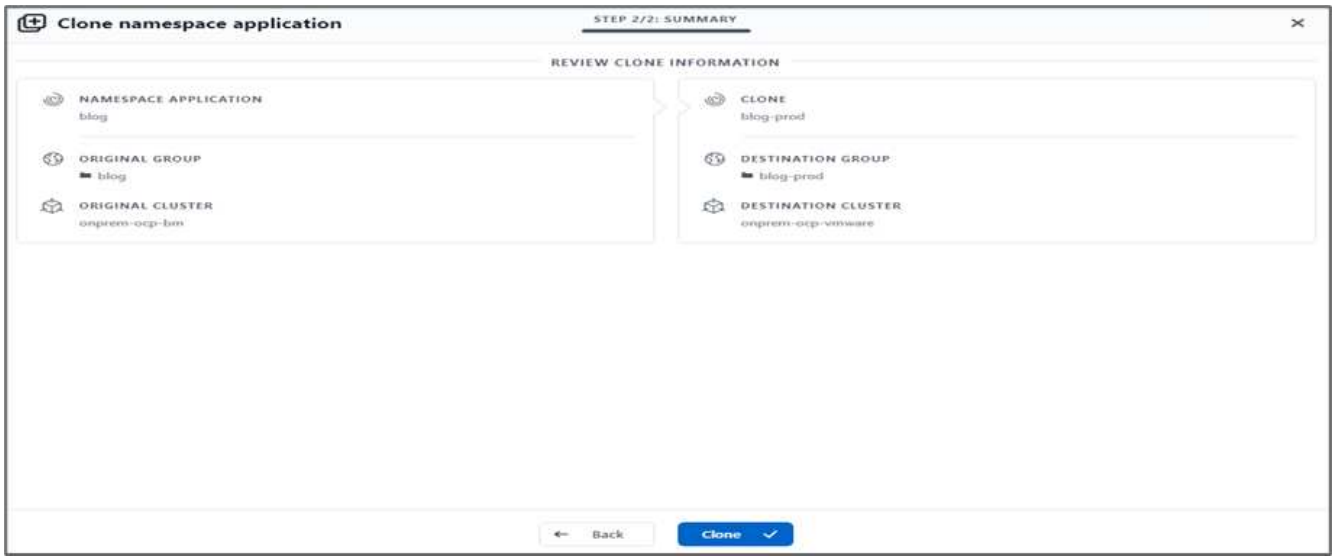
1. Il team DevTest aggiorna inizialmente l'applicazione alla versione supportata (`ghost-4.6-alpine`) prima di eseguire l'aggiornamento alla versione finale (`ghost-latest`) per preparare la produzione it. Quindi, postano un aggiornamento dell'applicazione clonata nel cluster OpenShift di produzione in esecuzione su un sistema FlexPod diverso.
2. A questo punto, l'applicazione viene aggiornata alla versione più recente e pronta per essere clonata nel cluster di produzione.



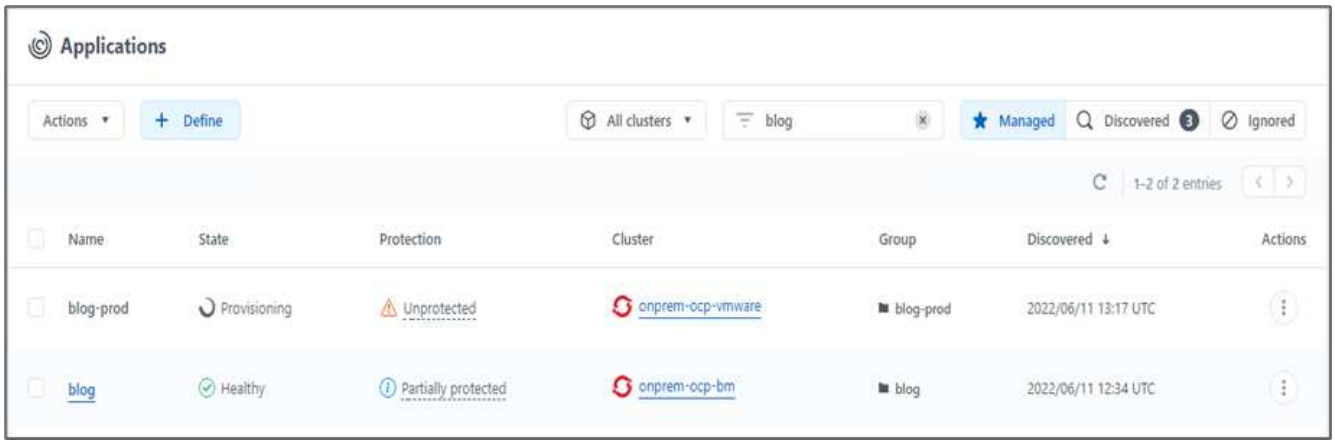
3. Per verificare il nuovo tema, aggiornare il sito del blog.



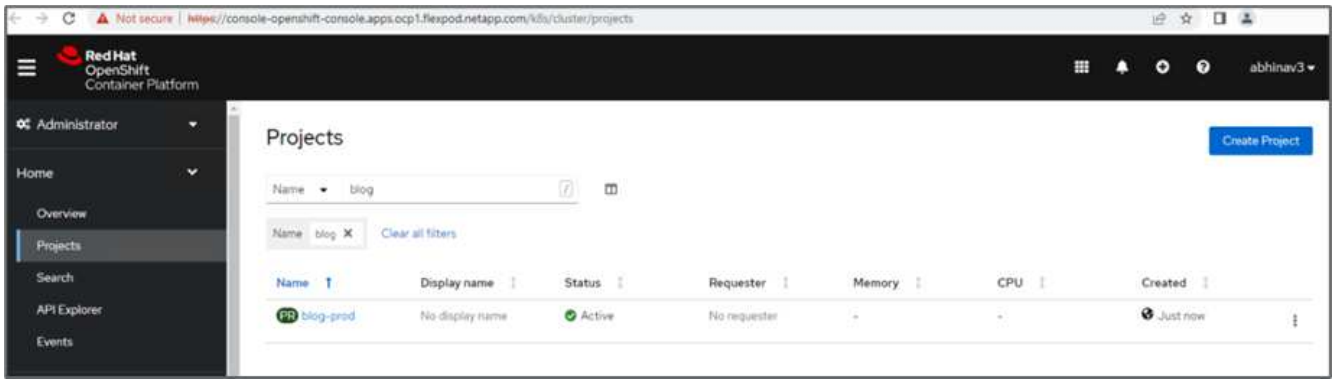
4. Da Astra Control Center, clonare l'applicazione sull'altro cluster OpenShift in produzione in esecuzione su VMware vSphere.



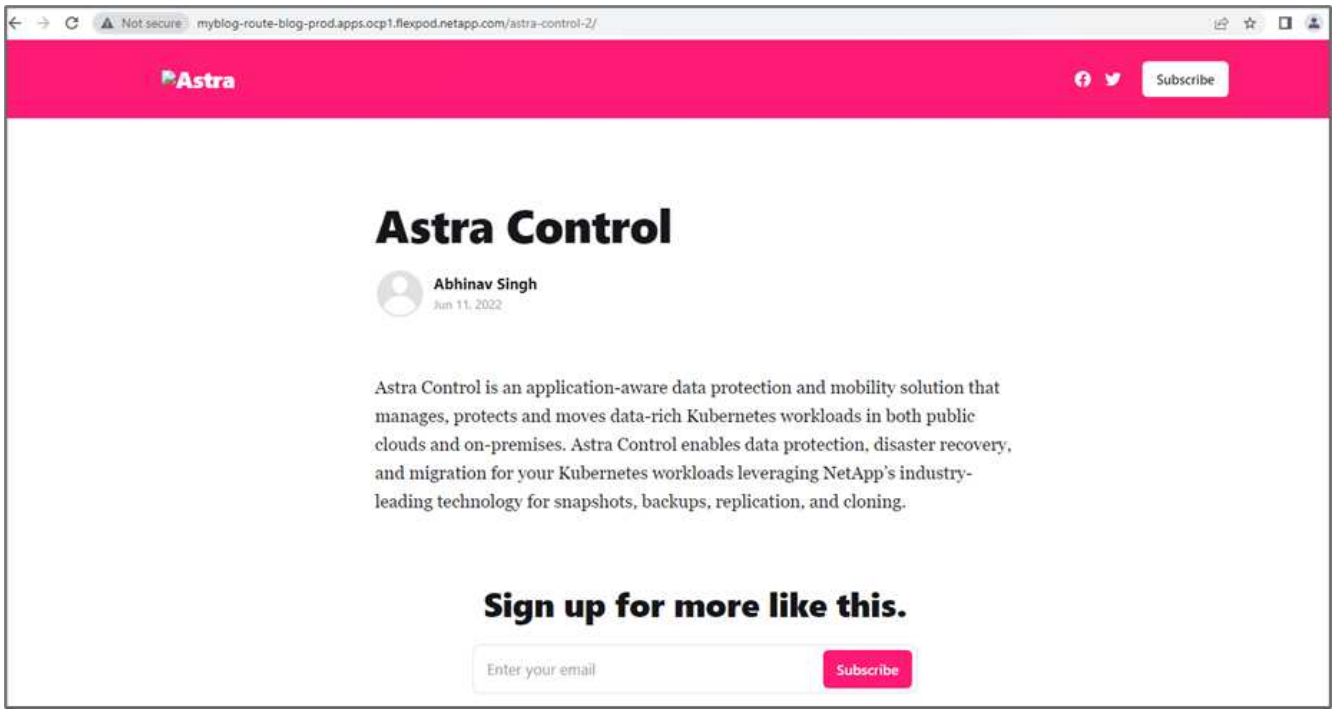
Nel cluster OpenShift di produzione viene ora eseguito il provisioning di un nuovo clone dell'applicazione.



5. Accedi al cluster OpenShift di produzione e cerca il blog del progetto.



6. Dal menu laterale, selezionare rete > percorsi e fare clic sull'URL in posizione. Viene visualizzata la stessa home page con il contenuto.



Si conclude così la convalida della soluzione Astra Control Center. È ora possibile clonare un'intera applicazione e i relativi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trova il cluster Kubernetes.

"Prossimo: Conclusione."

Conclusione

"Precedente: Ripristino dell'applicazione con backup remoti."

In questa soluzione, abbiamo implementato un piano di protezione per le applicazioni containerizzate eseguite su FlexPod e AWS utilizzando il portfolio NetApp Astra. Il centro di controllo Astra e Astra Trident di NetApp, insieme a Cloud Volumes ONTAP, Red Hat OpenShift e all'infrastruttura FlexPod, hanno costituito i componenti principali di questa soluzione.

Abbiamo dimostrato la protezione delle applicazioni acquisendo snapshot e abbiamo eseguito backup completi per ripristinare le applicazioni in diversi cluster K8s in esecuzione in ambienti cloud e on-premise.

Abbiamo anche dimostrato la clonazione delle applicazioni nei cluster K8s, consentendo così ai clienti di migrare le proprie applicazioni nei cluster K8s scelti nelle posizioni desiderate.

FlexPod si è evoluta costantemente in modo che i suoi clienti possano modernizzare le loro applicazioni e i processi di delivery aziendale. Con questa soluzione, i clienti FlexPod possono costruire con sicurezza il proprio piano BCDR per le applicazioni native del cloud con il cloud pubblico come luogo per un piano di DR transitorio o a tempo pieno, mantenendo al contempo bassi i costi della soluzione.

Astra Control consente di spostare un'intera applicazione insieme ai relativi dati da un cluster Kubernetes a un altro, indipendentemente da dove si trovano i cluster. Può anche aiutarti ad accelerare l'implementazione, le operazioni e la protezione per le tue applicazioni native del cloud.

Risoluzione dei problemi

Per informazioni sulla risoluzione dei problemi, consultare "documentazione online".

Dove trovare ulteriori informazioni

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

- Pagina iniziale di FlexPod

  "https://www.flexpod.com"

- Guide di progettazione e implementazione validate Cisco per FlexPod

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

- Implementazione di FlexPod con infrastruttura come codice per VMware utilizzando Ansible

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

- Implementazione di FlexPod con infrastruttura come codice per Red Hat OpenShift Bare Metal con Ansible

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

- Cisco UCS hardware and Software Interoperability Tool

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

- Scheda informativa su Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentazione NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

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

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Tool di matrice di interoperabilità NetApp

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

Cronologia delle versioni

Versione	Data	Cronologia delle versioni del documento
Versione 1.0	Luglio 2022	Release per ACC 22.04.0.

NetApp Cloud Insights per FlexPod

TR-4868: NetApp Cloud Insights per FlexPod

Alan Cowles, NetApp

In collaborazione con: 

La soluzione descritta in questo report tecnico è la configurazione del servizio NetApp Cloud Insights per il monitoraggio del sistema di storage NetApp AFF A800 con NetApp ONTAP, implementato come parte di una soluzione per data center FlexPod.

Valore per il cliente

La soluzione qui descritta offre valore ai clienti interessati a una soluzione di monitoraggio completa per i propri ambienti di cloud ibrido, in cui ONTAP viene implementato come sistema di storage primario. Sono inclusi gli ambienti FlexPod che utilizzano i sistemi storage NetApp AFF e FAS.

Casi di utilizzo

Questa soluzione si applica ai seguenti casi di utilizzo:

- Organizzazioni che desiderano monitorare varie risorse e utilizzo nel proprio sistema di storage ONTAP implementato come parte di una soluzione FlexPod.
- Organizzazioni che desiderano risolvere i problemi e ridurre i tempi di risoluzione degli incidenti che si verificano nella propria soluzione FlexPod con i sistemi AFF o FAS.
- Organizzazioni interessate a proiezioni di ottimizzazione dei costi, tra cui dashboard personalizzati per fornire informazioni dettagliate sulle risorse sprecate e dove è possibile realizzare risparmi sui costi nel proprio ambiente FlexPod, incluso ONTAP.

Pubblico di riferimento

Il pubblico di riferimento per la soluzione comprende i seguenti gruppi:

- Dirigenti IT e responsabili dell'ottimizzazione dei costi e della business continuity.
- Architetti di soluzioni interessati alla progettazione e alla gestione di data center o cloud ibrido.
- Tecnici del supporto tecnico responsabili della risoluzione dei problemi e della risoluzione degli incidenti.

È possibile configurare Cloud Insights in modo da fornire diversi tipi di dati utili che possono essere utilizzati per la pianificazione, la risoluzione dei problemi, la manutenzione e la garanzia di business continuity. Monitorando la soluzione di data center FlexPod con Cloud Insights e presentando i dati aggregati in dashboard personalizzate facilmente digeribili; non solo è possibile prevedere quando le risorse di un'implementazione devono essere scalate per soddisfare le esigenze, ma anche identificare applicazioni o volumi di storage specifici che causano problemi all'interno del sistema. In questo modo si garantisce che l'infrastruttura monitorata sia prevedibile e funzioni in base alle aspettative, consentendo a un'organizzazione di rispettare SLA definiti e di scalare l'infrastruttura in base alle necessità, eliminando sprechi e costi aggiuntivi.

Architettura

In questa sezione, esaminano l'architettura di un'infrastruttura convergente per data center FlexPod, incluso un sistema NetApp AFF A800 monitorato da Cloud Insights.

Tecnologia della soluzione

Una soluzione per data center FlexPod è costituita dai seguenti componenti minimi per fornire un ambiente di infrastruttura convergente altamente disponibile, facilmente scalabile, validato e supportato.

- Due nodi storage NetApp ONTAP (una coppia ha)
- Due switch di rete per data center Cisco Nexus
- Due switch Cisco MDS Fabric (opzionali per implementazioni FC)
- Due interconnessioni fabric Cisco UCS
- Uno chassis blade Cisco UCS con due server blade Cisco UCS serie B.

Oppure

- Due server Cisco UCS C-Series per il montaggio in rack

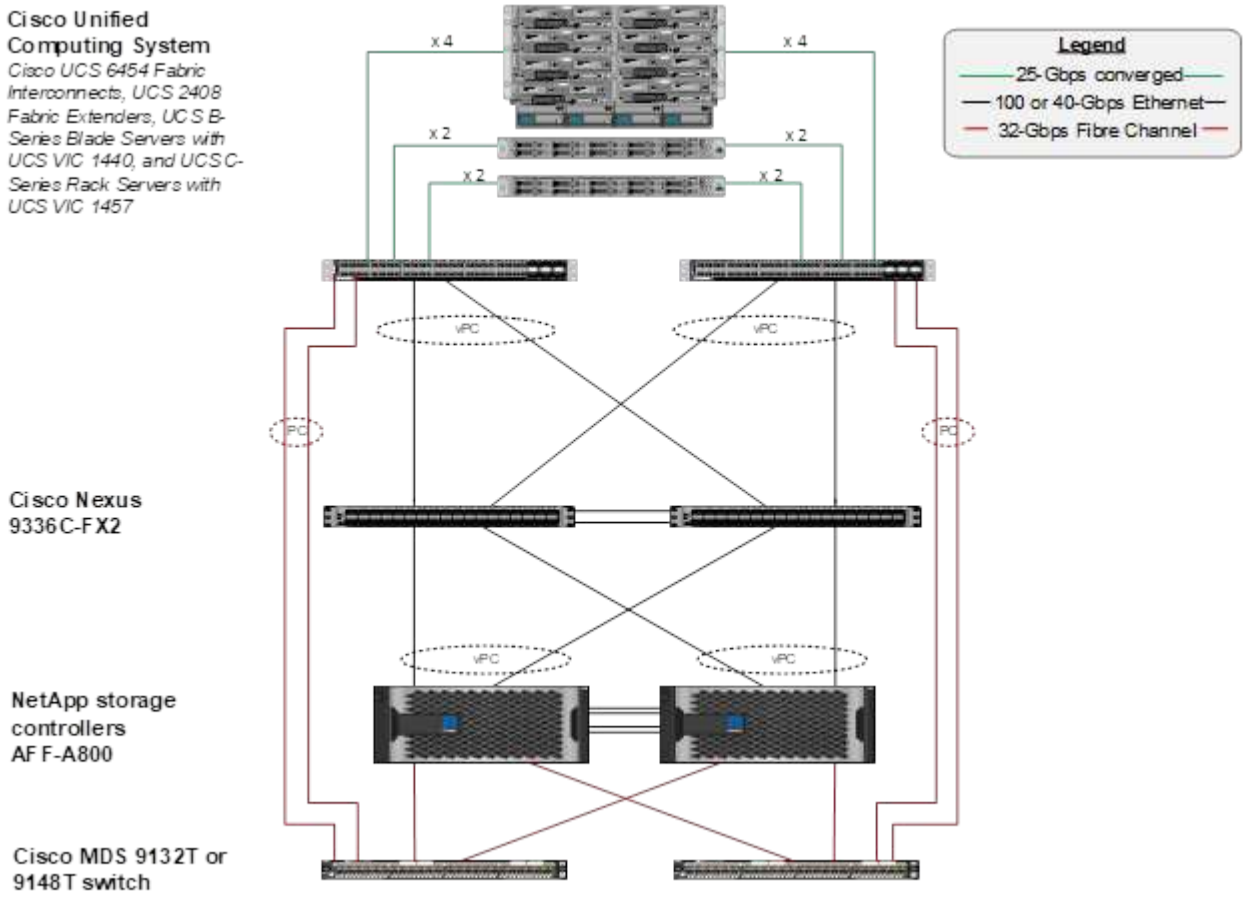
Per consentire a Cloud Insights di raccogliere i dati, un'organizzazione deve implementare un'unità di acquisizione come macchina virtuale o fisica all'interno del proprio ambiente FlexPod Datacenter o in una posizione in cui può contattare i componenti da cui sta raccogliendo i dati. È possibile installare il software Acquisition Unit su un sistema che esegue diversi sistemi operativi Windows o Linux supportati. La seguente tabella elenca i componenti della soluzione per questo software.

Sistema operativo	Versione
Microsoft Windows	10
Server Microsoft Windows	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7.2 – 7.6
CentOS	7.2 – 7.6

Sistema operativo	Versione
Oracle Enterprise Linux	7.5
Debian	9
Ubuntu	18.04 LTS

Diagramma dell'architettura

La figura seguente mostra l'architettura della soluzione.



Requisiti hardware

La seguente tabella elenca i componenti hardware necessari per implementare la soluzione. I componenti hardware utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Hardware	Quantità
Cisco Nexus 9336C-FX2	2
Cisco UCS 6454 Fabric Interconnect	2
Chassis blade Cisco UCS 5108	1
Cisco UCS 2408 Fabric Extender	2
Blade Cisco UCS B200 M5	2

Hardware	Quantità
NetApp AFF A800	2

Requisiti software

La seguente tabella elenca i componenti software necessari per implementare la soluzione. I componenti software utilizzati in una particolare implementazione della soluzione possono variare in base ai requisiti del cliente.

Software	Versione
Firmware Cisco Nexus	9.3(5)
Versione Cisco UCS	4.1(2a)
Versione di NetApp ONTAP	9.7
Versione di NetApp Cloud Insights	Settembre 2020, Basic
Red Hat Enterprise Linux	7.6
VMware vSphere	6.7U3

Utilizza i dettagli del caso

Questa soluzione si applica ai seguenti casi di utilizzo:

- Analisi dell'ambiente con i dati forniti al consulente digitale NetApp Active IQ per la valutazione dei rischi del sistema storage e consigli per l'ottimizzazione dello storage.
- Risoluzione dei problemi nel sistema storage ONTAP implementato in una soluzione FlexPod Datacenter esaminando le statistiche di sistema in tempo reale.
- Creazione di dashboard personalizzate per monitorare facilmente punti di interesse specifici per i sistemi storage ONTAP implementati in un'infrastruttura convergente del data center FlexPod.

Considerazioni di progettazione

La soluzione per data center FlexPod è un'infrastruttura convergente progettata da Cisco e NetApp per fornire un ambiente di data center dinamico, altamente disponibile e scalabile per l'esecuzione di carichi di lavoro aziendali. Le risorse di calcolo e di rete della soluzione sono fornite dai prodotti Cisco UCS e Nexus, mentre le risorse di storage sono fornite dal sistema di storage ONTAP. La progettazione della soluzione viene migliorata regolarmente, quando sono disponibili modelli hardware aggiornati o versioni software e firmware. Questi dettagli, insieme alle Best practice per la progettazione e l'implementazione della soluzione, vengono acquisiti nei documenti Cisco Validated Design (CVD) o NetApp Verified Architecture (NVA) e pubblicati regolarmente.

È disponibile il più recente documento CVD che descrive la progettazione della soluzione per data center FlexPod "qui".

Implementare Cloud Insights per FlexPod

Per implementare la soluzione, è necessario completare le seguenti attività:

1. Iscriviti al servizio Cloud Insights
2. Creare una macchina virtuale VMware (VM) da configurare come unità di acquisizione
3. Installare l'host Red Hat Enterprise Linux (RHEL)
4. Creare un'istanza dell'unità di acquisizione nel portale Cloud Insights e installare il software
5. Aggiungi il sistema storage monitorato dal data center FlexPod a Cloud Insights.

Iscriviti al servizio NetApp Cloud Insights

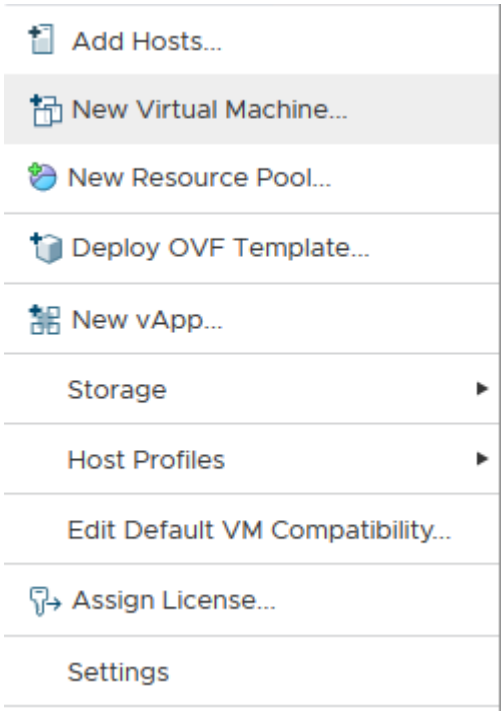
Per iscriversi al servizio NetApp Cloud Insights, attenersi alla seguente procedura:

1. Passare a. "https://cloud.netapp.com/cloud-insights"
2. Fare clic sul pulsante al centro dello schermo per avviare la prova gratuita di 14 giorni oppure sul collegamento nell'angolo in alto a destra per registrarsi o accedere a un account NetApp Cloud Central esistente.

Creare una macchina virtuale VMware da configurare come unità di acquisizione

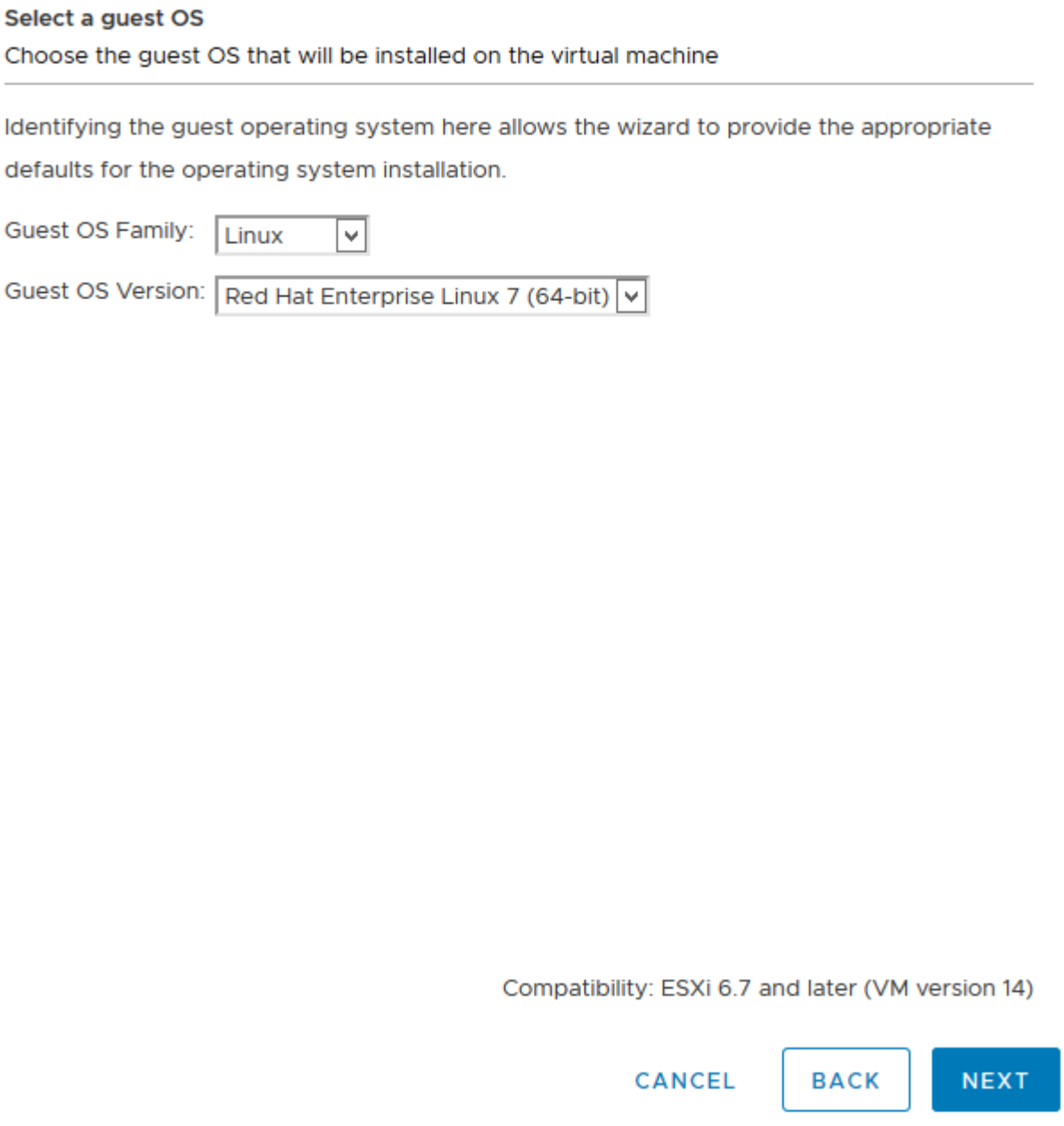
Per creare una macchina virtuale VMware da configurare come unità di acquisizione, attenersi alla seguente procedura:

1. Avviare un browser Web, accedere a VMware vSphere e selezionare il cluster che si desidera ospitare.
2. Fare clic con il pulsante destro del mouse sul cluster e selezionare Create A Virtual Machine (Crea una macchina virtuale) dal menu.



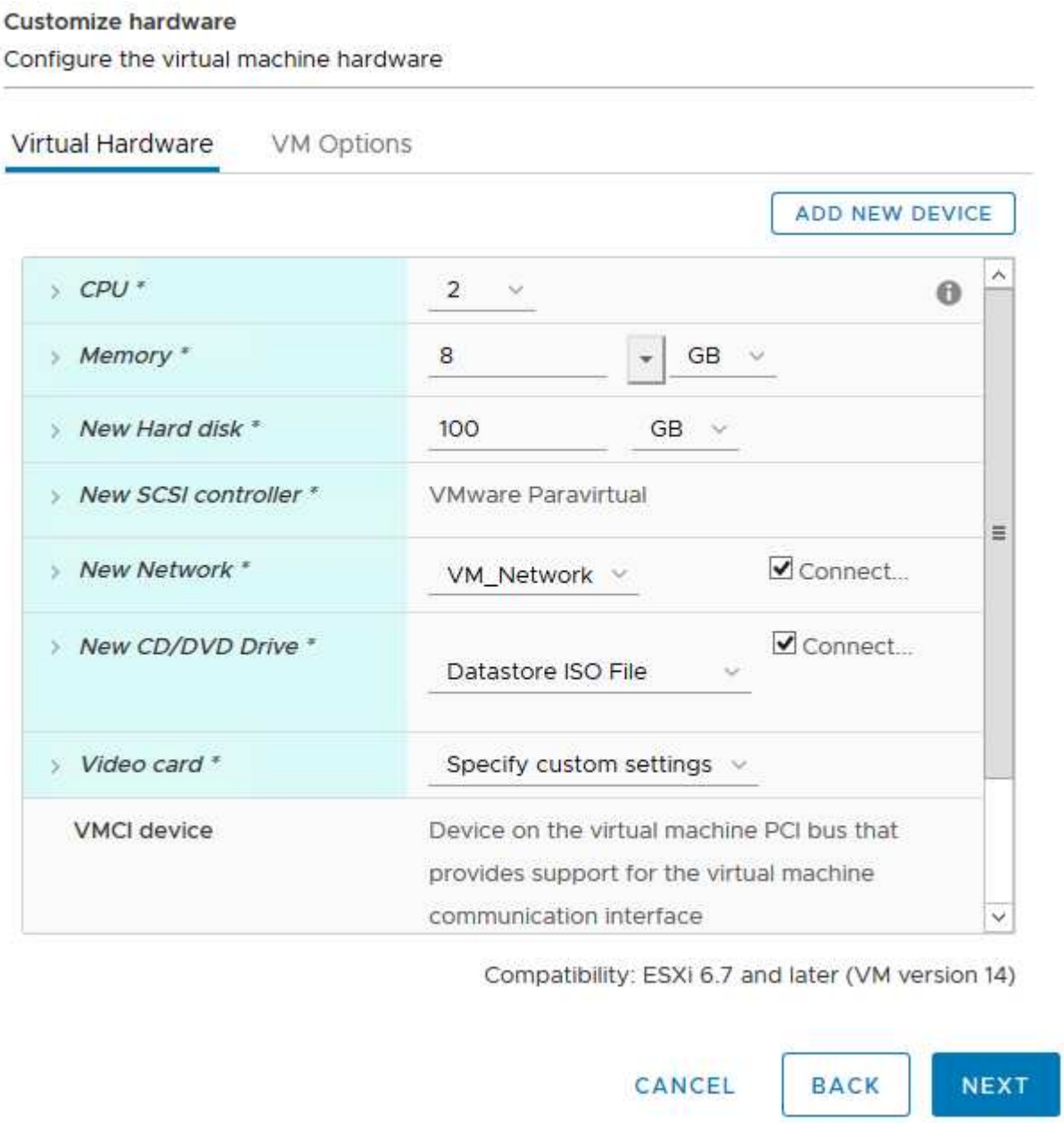
3. Nella procedura guidata Nuova macchina virtuale, fare clic su Avanti.

4. Specificare il nome della macchina virtuale e selezionare il data center in cui si desidera installarla, quindi fare clic su Next (Avanti).
5. Nella pagina seguente, selezionare il cluster, i nodi o il gruppo di risorse in cui si desidera installare la macchina virtuale, quindi fare clic su Avanti.
6. Selezionare il datastore condiviso che ospita le macchine virtuali e fare clic su Next (Avanti).
7. Verificare che la modalità di compatibilità per la macchina virtuale sia impostata su `ESXi 6.7 or later` E fare clic su Next (Avanti).
8. Selezionare la famiglia di sistemi operativi guest Linux, versione del sistema operativo guest: Red Hat Enterprise Linux 7 (64 bit).



9. La pagina successiva consente di personalizzare le risorse hardware sulla macchina virtuale. L'unità di acquisizione Cloud Insights richiede le seguenti risorse. Una volta selezionate le risorse, fare clic su Next (Avanti):

a. Due CPU
b. 8 GB di RAM
c. 100 GB di spazio su disco rigido
d. Una rete in grado di raggiungere le risorse nel data center FlexPod e nel server Cloud Insights tramite una connessione SSL sulla porta 443.
e. Immagine ISO della distribuzione Linux scelta (Red Hat Enterprise Linux) da cui eseguire l'avvio.

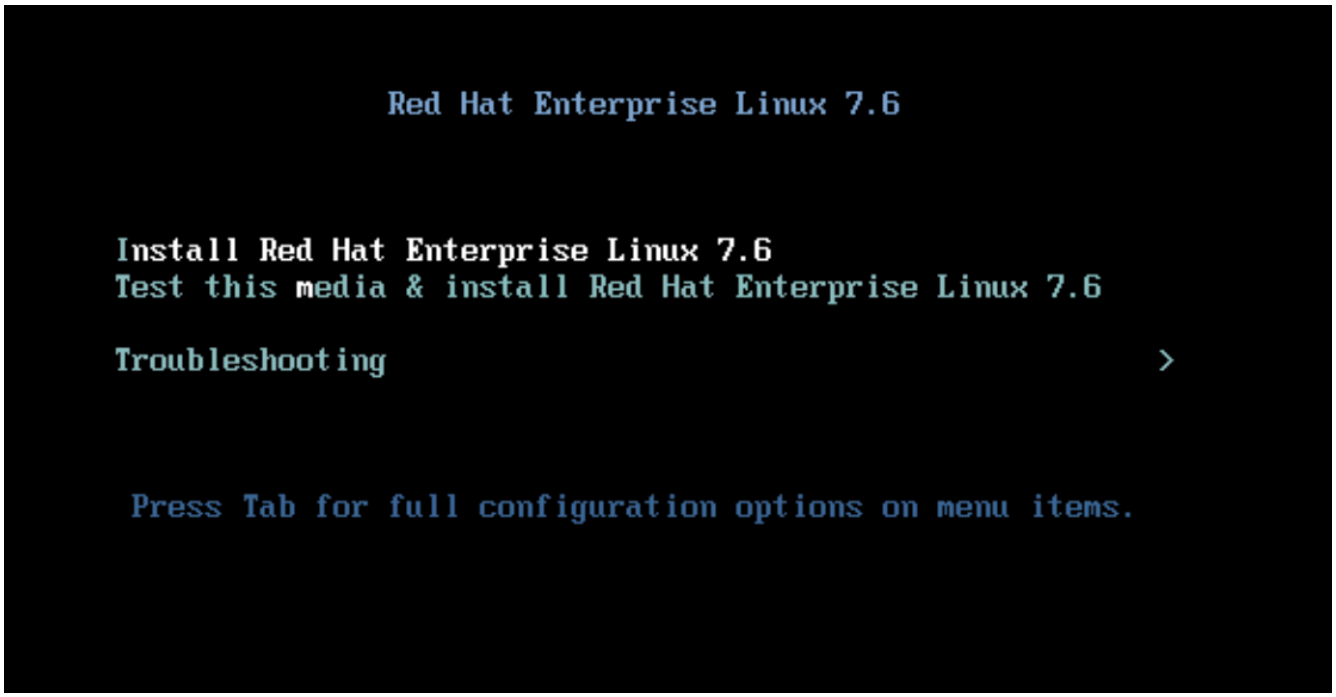


10. Per creare la macchina virtuale, nella pagina Ready to complete (Pronto per il completamento), rivedere le impostazioni e fare clic su Finish (fine).

Installare Red Hat Enterprise Linux

Per installare Red Hat Enterprise Linux, attenersi alla seguente procedura:

1. Accendere la macchina virtuale, fare clic sulla finestra per avviare la console virtuale, quindi selezionare l'opzione Installa Red Hat Enterprise Linux 7.6.

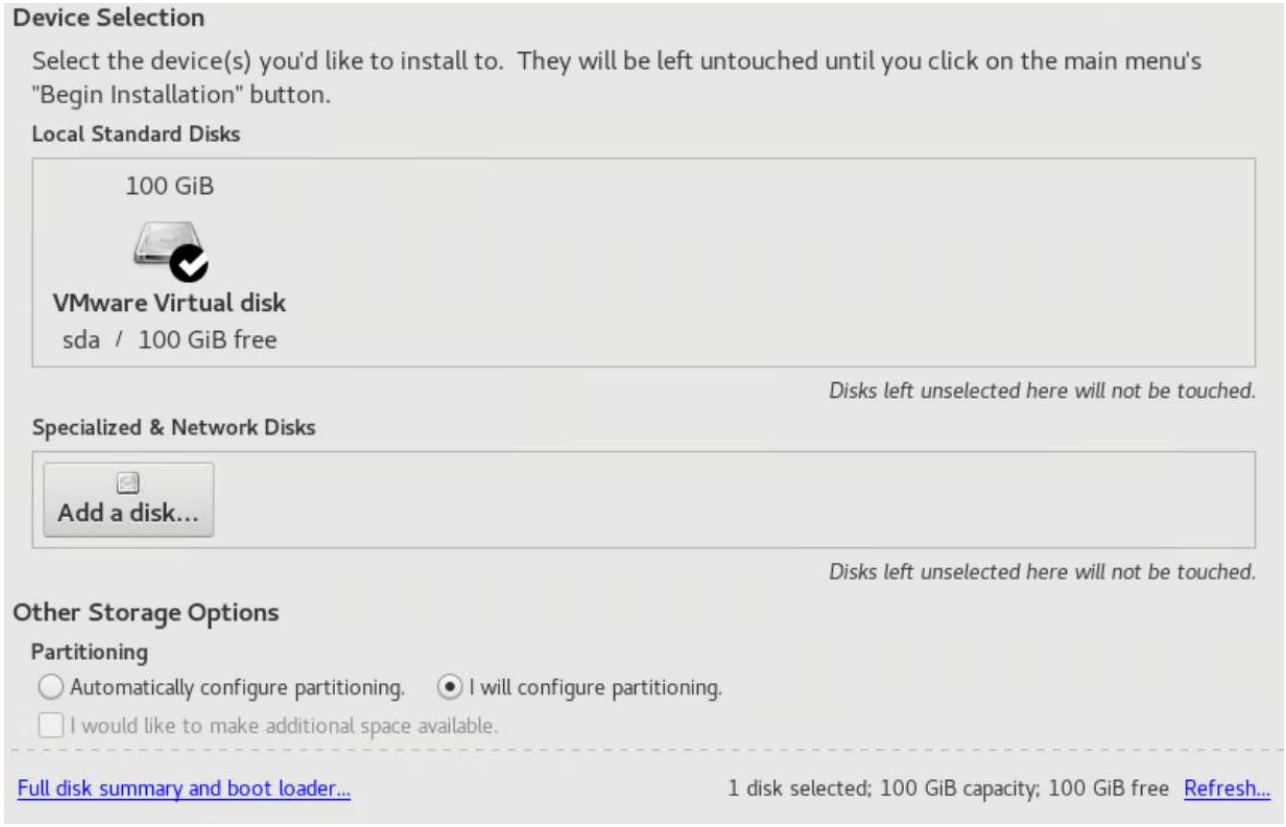


2. Selezionare la lingua desiderata e fare clic su continua.

   La pagina successiva è Riepilogo dell'installazione. Le impostazioni predefinite dovrebbero essere accettabili per la maggior parte di queste opzioni.

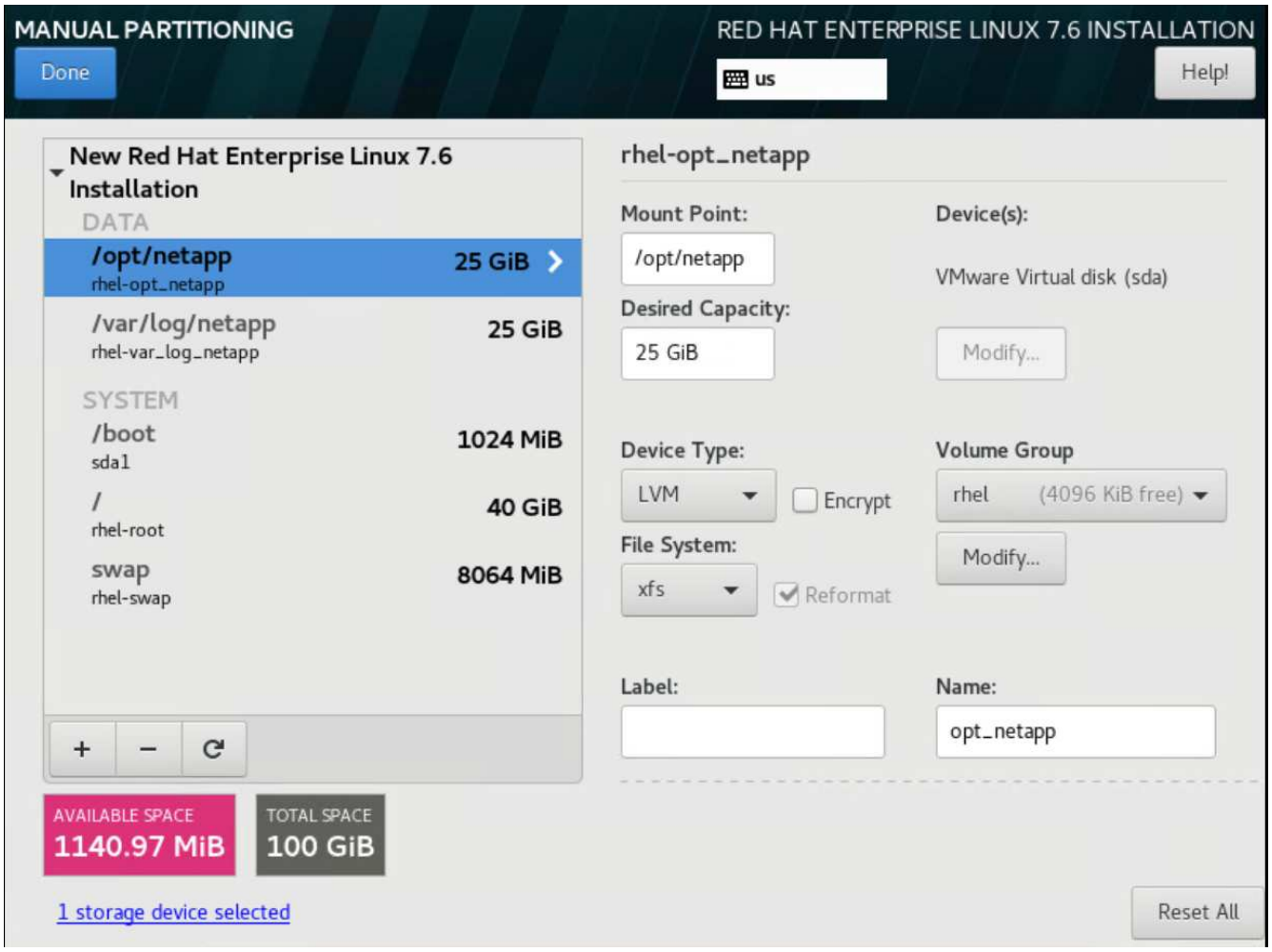
3. È necessario personalizzare il layout dello storage eseguendo le seguenti opzioni:

   a. Per personalizzare la partizione per il server, fare clic su destinazione installazione.
   b. Verificare che il disco virtuale VMware di 100GiB sia selezionato con un segno di spunta nero e selezionare il pulsante di opzione i Will Configure Partitioning (i Will Configure Partitioning).



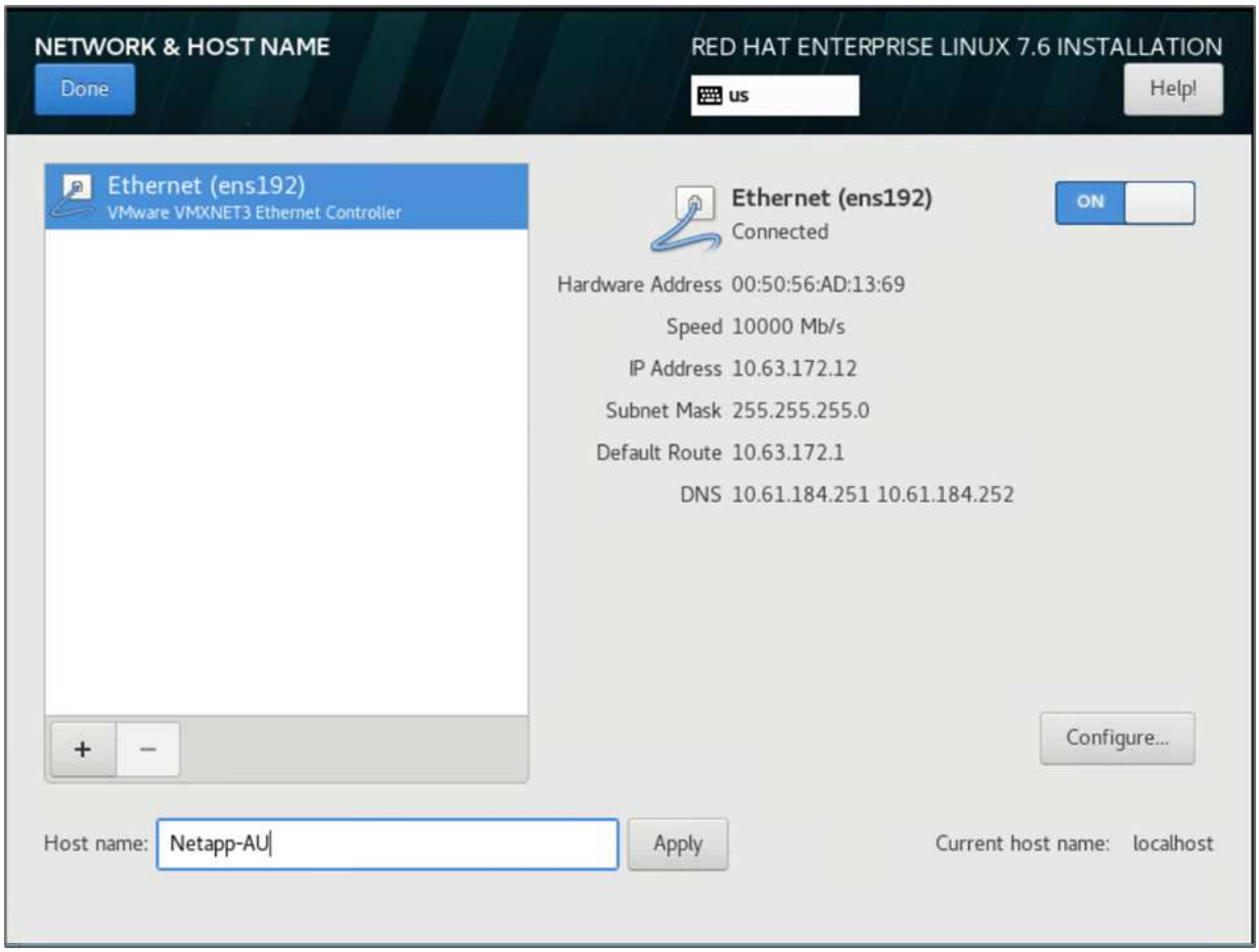
c. Fare clic su fine.

   Viene visualizzato un nuovo menu che consente di personalizzare la tabella delle partizioni. Dedicare 25 GB ciascuno a. `/opt/netapp` e. `/var/log/netapp`. È possibile allocare automaticamente il resto dello storage nel sistema.



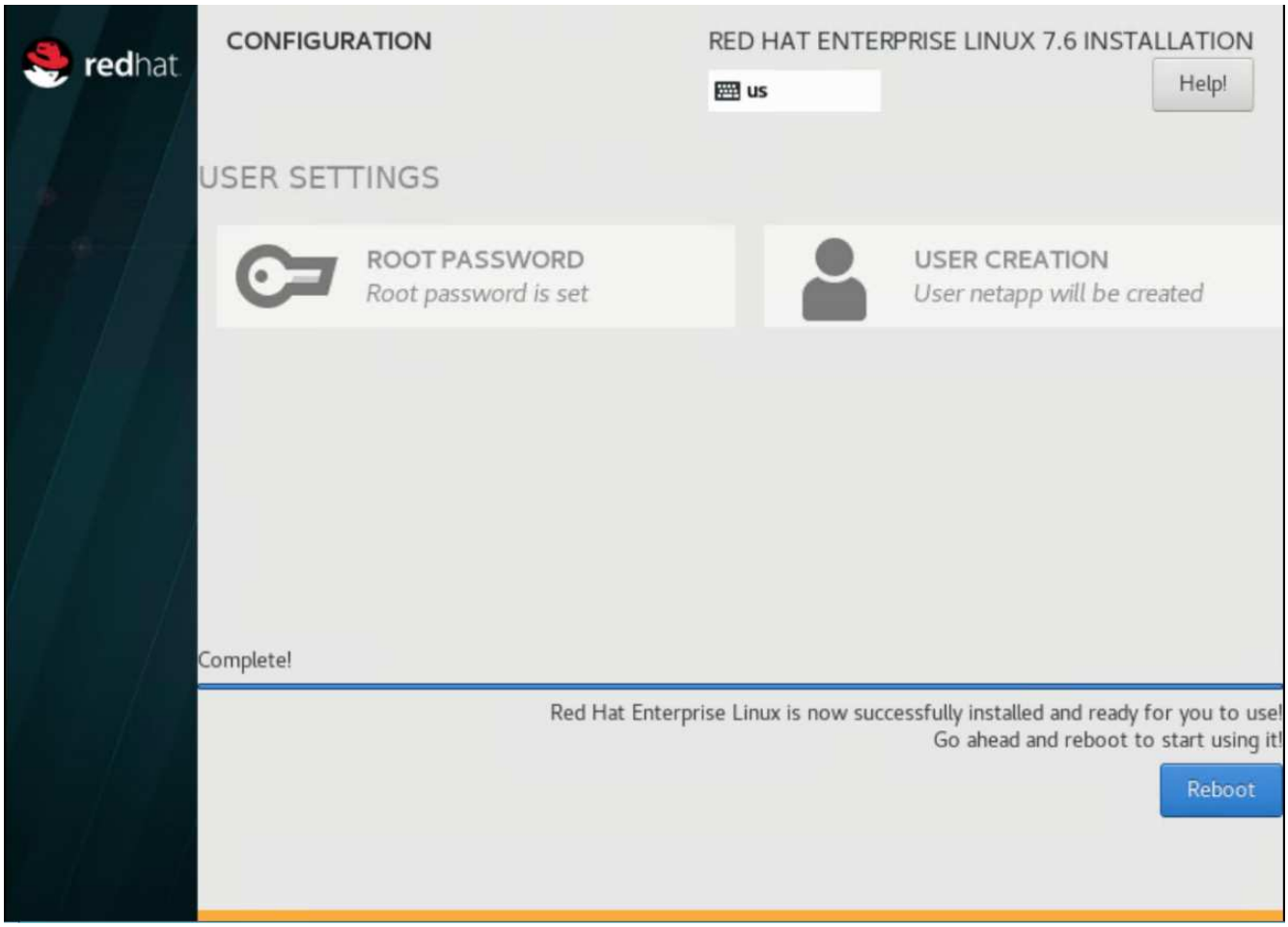
a. Per tornare al Riepilogo dell'installazione, fare clic su fine.

4. Fare clic su Network and host Name (rete e nome host)
   a. Immettere un nome host per il server.
   b. Accendere la scheda di rete facendo clic sul pulsante a scorrimento. Se il protocollo DHCP (Dynamic host Configuration Protocol) è configurato sulla rete, si riceverà un indirizzo IP. In caso contrario, fare clic su Configure (Configura) e assegnare manualmente un indirizzo.



c. . Fare clic su Done (fine) per tornare al Riepilogo dell'installazione.

5. Nella pagina Installation Summary (Riepilogo dell'installazione), fare clic su Begin Installation
6. Nella pagina Installation Progress (avanzamento installazione), è possibile impostare la password root o creare un account utente locale. Al termine dell'installazione, fare clic su Reboot (Riavvia) per riavviare il server.



7. Una volta riavviato il sistema, accedere al server e registrarlo con Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

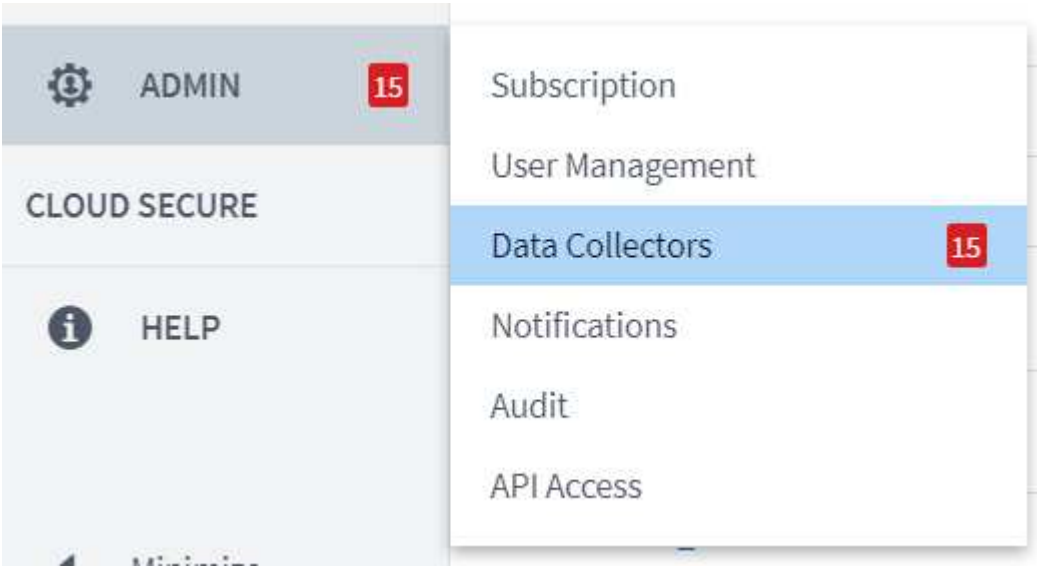
8. Allega un abbonamento disponibile per Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Creare un'istanza dell'unità di acquisizione nel portale Cloud Insights e installare il software

Per creare un'istanza dell'unità di acquisizione nel portale Cloud Insights e installare il software, attenersi alla seguente procedura:

1. Dalla home page di Cloud Insights, passare il mouse sulla voce Amministratore nel menu principale a sinistra e selezionare Data Collector dal menu.

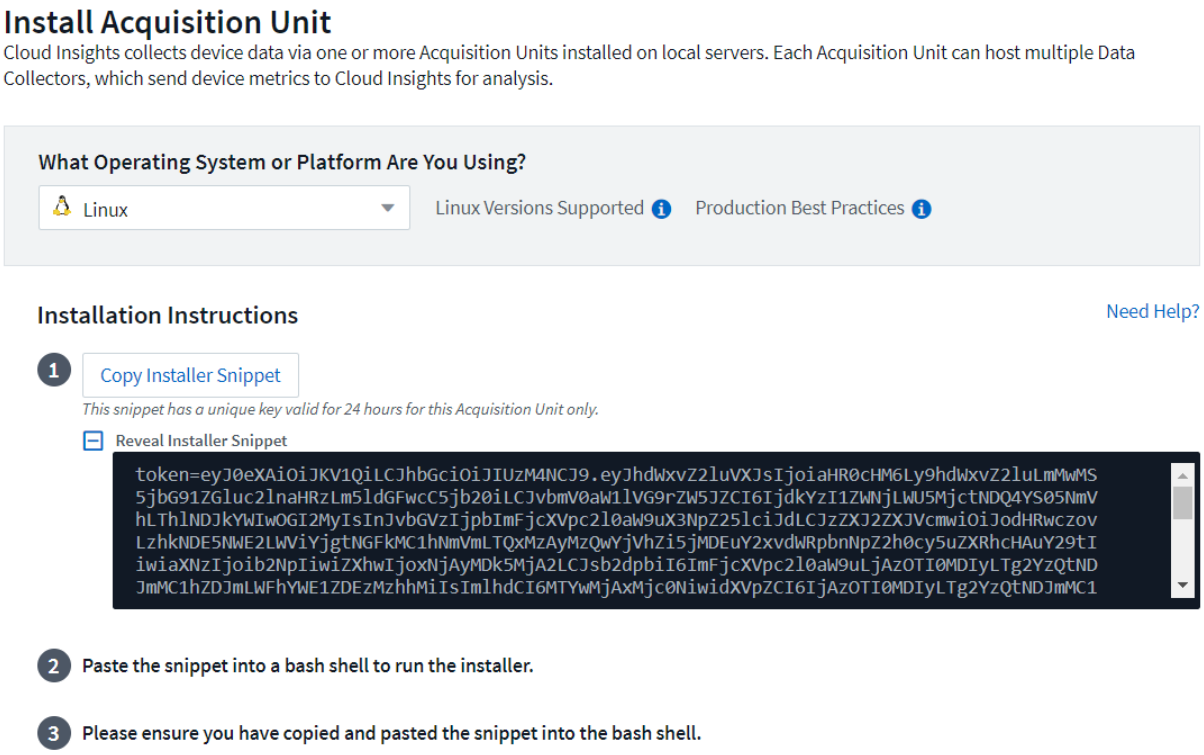


2. Nella parte superiore centrale della pagina Data Collector, fare clic sul collegamento Acquisition Units (unità di acquisizione).

3. Per creare una nuova unità di acquisizione, fare clic sul pulsante a destra.

4. Selezionare il sistema operativo che si desidera utilizzare per ospitare l'unità di acquisizione e seguire le istruzioni per copiare lo script di installazione dalla pagina Web.

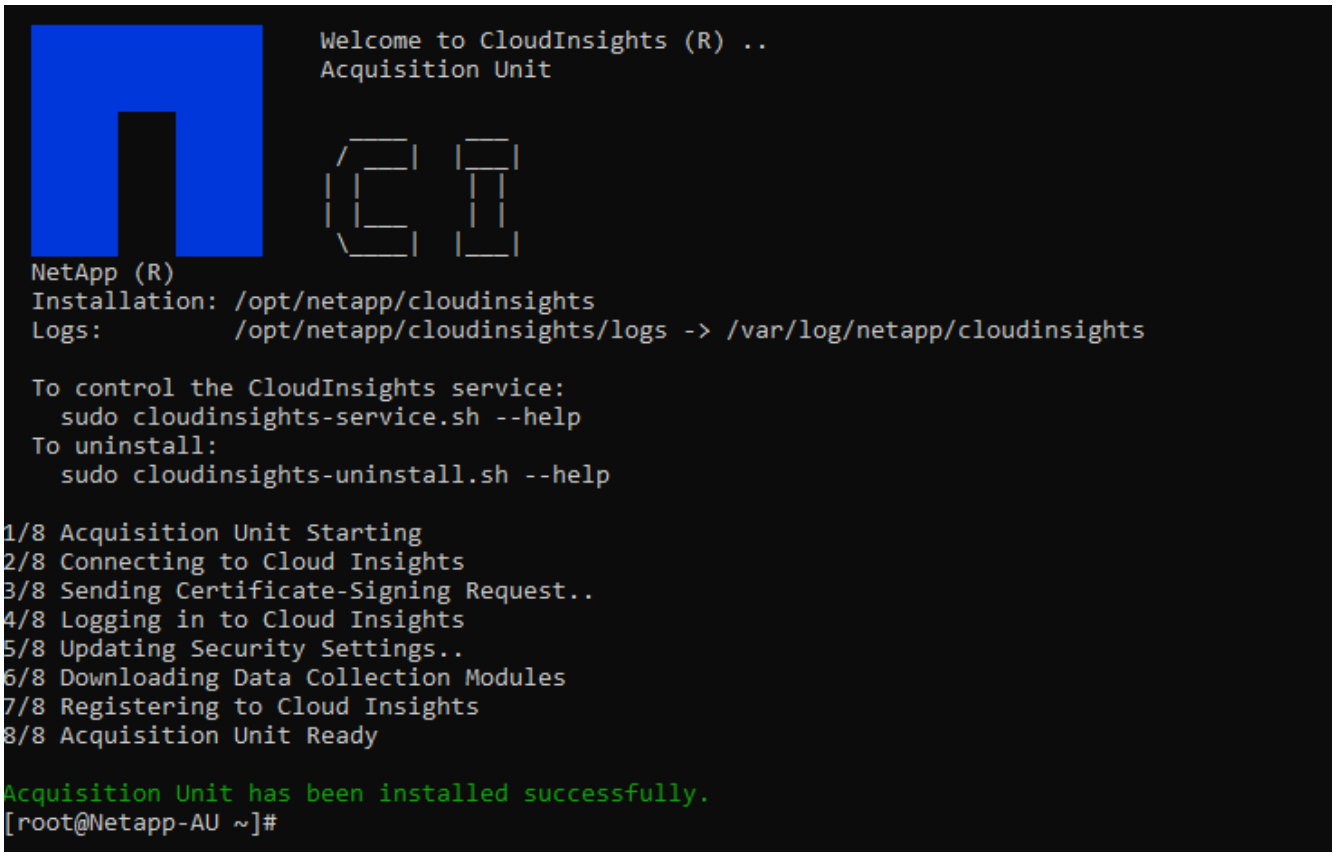
   In questo esempio, si tratta di un server Linux, che fornisce un frammento e un token da incollare nella CLI sul nostro host. La pagina Web attende la connessione dell'unità di acquisizione.



5. Incollare il frammento nella CLI della macchina Red Hat Enterprise Linux che ha eseguito il provisioning e fare clic su Invio.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0c
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

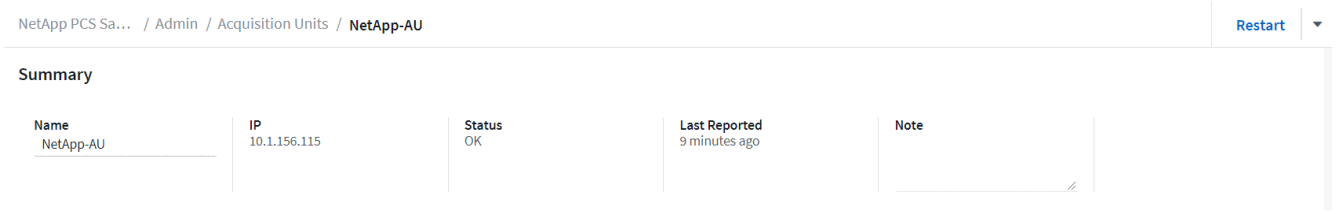
Il programma di installazione scarica un pacchetto compresso e avvia l'installazione. Una volta completata l'installazione, viene visualizzato un messaggio che indica che l'unità di acquisizione è stata registrata con NetApp Cloud Insights.



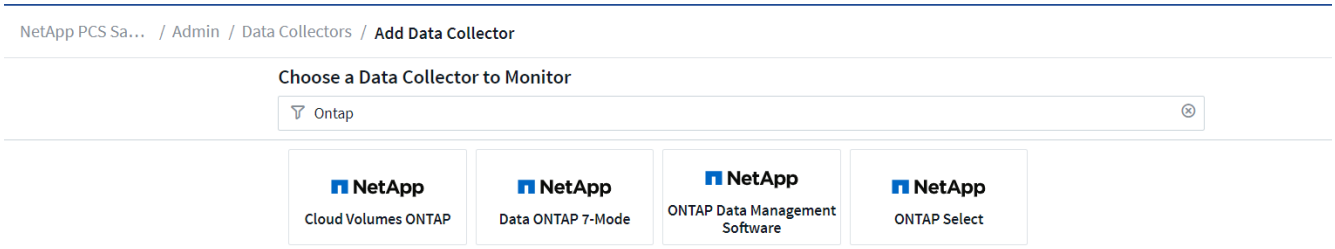
Aggiungi il sistema storage monitorato dal data center FlexPod a Cloud Insights

Per aggiungere il sistema di storage ONTAP da un'implementazione FlexPod, attenersi alla seguente procedura:

1. Tornare alla pagina unità di acquisizione sul portale Cloud Insights e individuare l'unità appena registrata elencata. Per visualizzare un riepilogo del reparto, fare clic sull'unità.

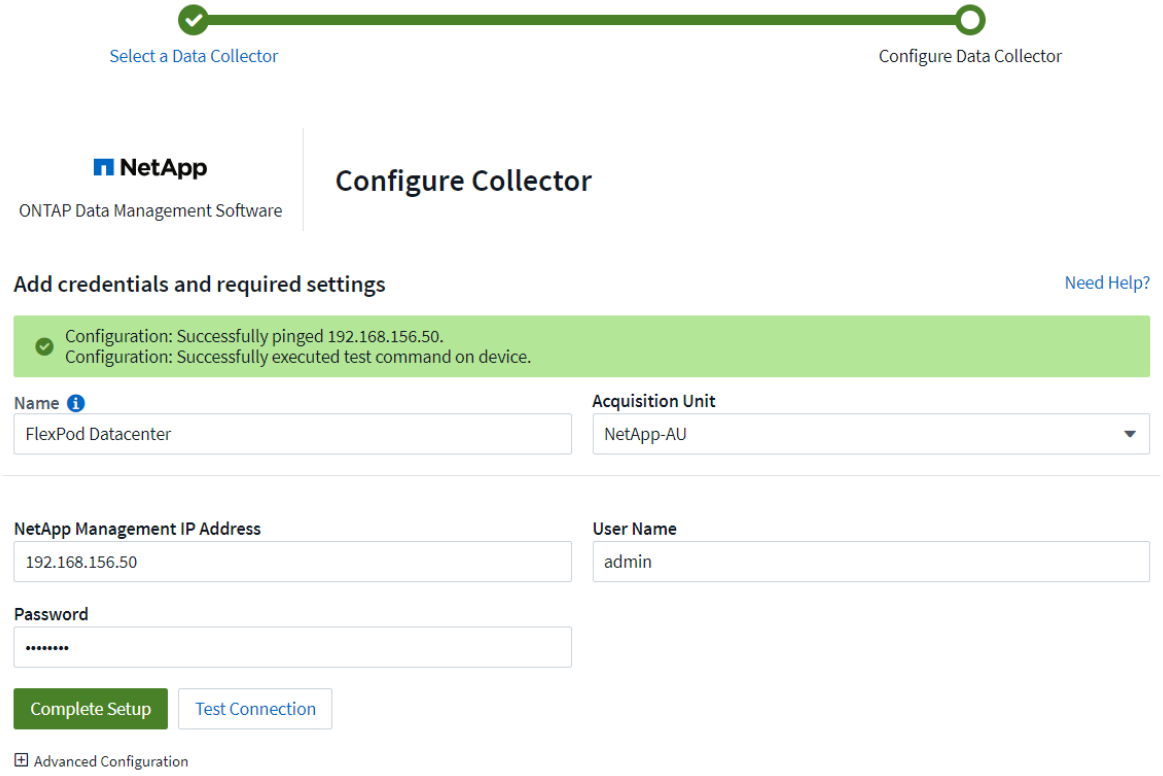


2. Per avviare una procedura guidata per aggiungere il sistema di storage, nella pagina Summary (Riepilogo), fare clic sul pulsante per creare un data collector. La prima pagina visualizza tutti i sistemi da cui è possibile raccogliere i dati. Utilizzare la barra di ricerca per cercare ONTAP.



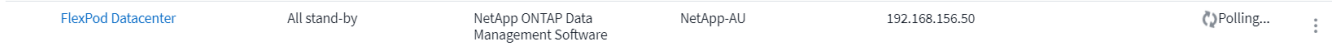
3. Selezionare il software di gestione dei dati ONTAP.

   Viene visualizzata una pagina che consente di assegnare un nome all'implementazione e selezionare l'unità di acquisizione da utilizzare. È possibile fornire le informazioni di connettività e le credenziali per il sistema ONTAP e verificare la connessione per confermare.



4. Fare clic su complete Setup (completa installazione)

   Il portale torna alla pagina Data Collector e il Data Collector inizia il primo polling per raccogliere i dati dal sistema di storage ONTAP nel data center FlexPod.



Casi di utilizzo

Con la configurazione e la configurazione di Cloud Insights per il monitoraggio della

soluzione FlexPod Datacenter, possiamo esplorare alcune delle attività che è possibile eseguire sulla dashboard per valutare e monitorare il tuo ambiente. In questa sezione, vengono evidenziati cinque casi di utilizzo principali per Cloud Insights:

- Integrazione di Active IQ
- Analisi delle dashboard in tempo reale
- Creazione di dashboard personalizzati
- Risoluzione avanzata dei problemi
- Ottimizzazione dello storage

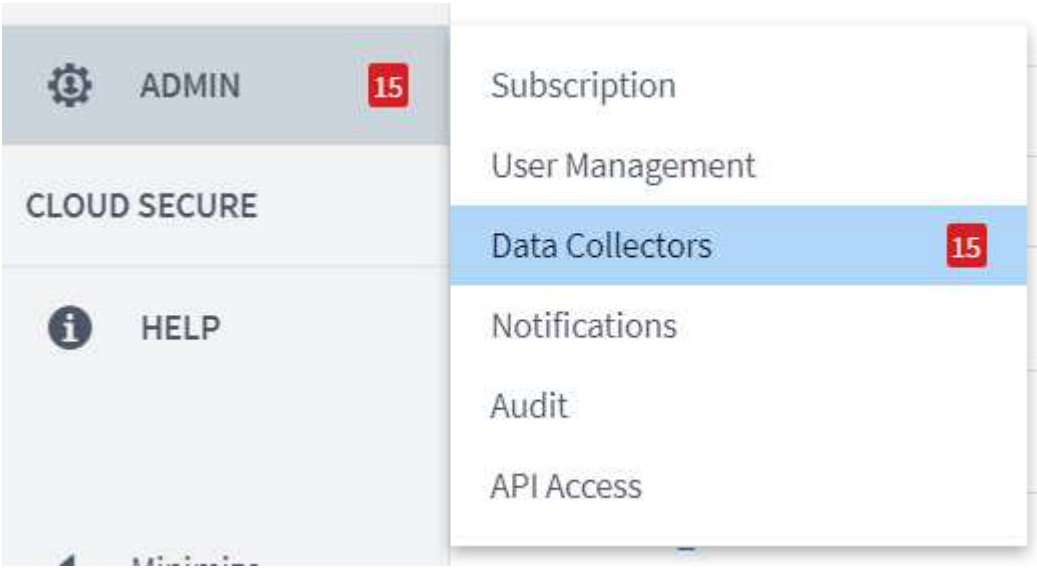
Integrazione di Active IQ

Cloud Insights è completamente integrato nella piattaforma di monitoraggio dello storage Active IQ. Un sistema ONTAP, implementato come parte di una soluzione FlexPod Datacenter, viene configurato automaticamente per inviare informazioni a NetApp attraverso la funzione AutoSupport, integrata in ciascun sistema. Questi report vengono generati in base a una pianificazione o in modo dinamico ogni volta che viene rilevato un guasto nel sistema. I dati comunicati tramite AutoSupport vengono aggregati e visualizzati in dashboard facilmente accessibili nel menu Active IQ di Cloud Insights.

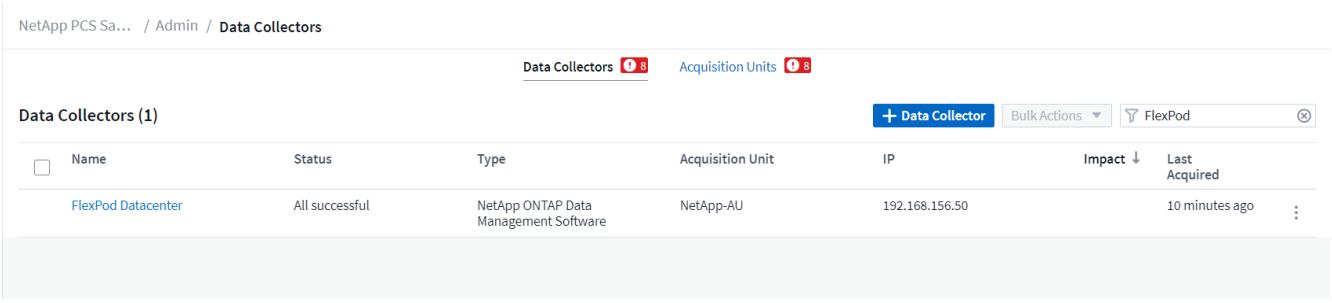
Accedere alle informazioni Active IQ dalla dashboard di Cloud Insights

Per accedere alle informazioni Active IQ dalla dashboard di Cloud Insights, attenersi alla seguente procedura:

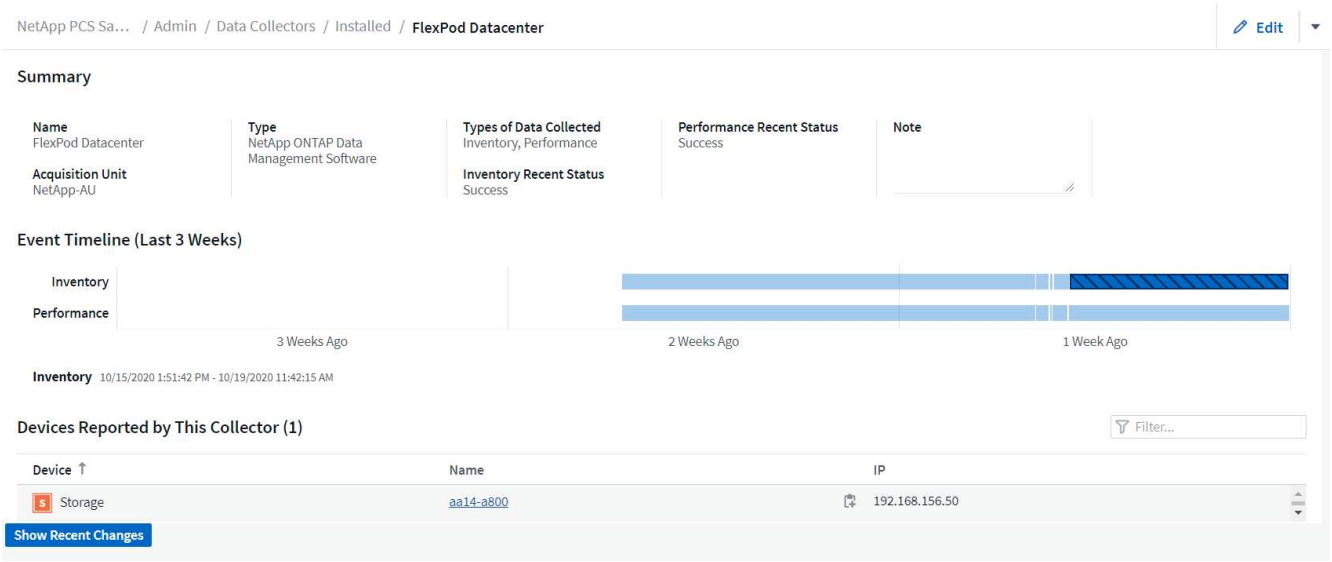
1. Fare clic sull'opzione Data Collector (raccolta dati) nel menu Admin (Amministrazione) a sinistra.



2. Filtro per il Data Collector specifico nel tuo ambiente. In questo esempio, filtriamo in base al termine FlexPod.

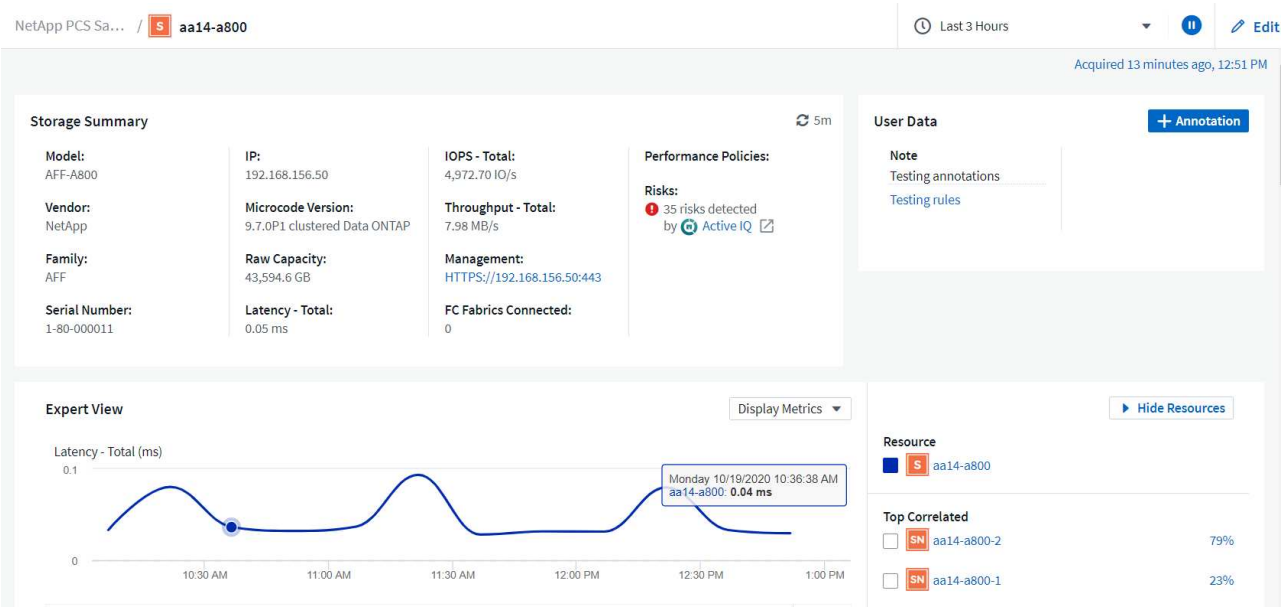


3. Fare clic su Data Collector per visualizzare un riepilogo dell'ambiente e dei dispositivi monitorati da tale collector.

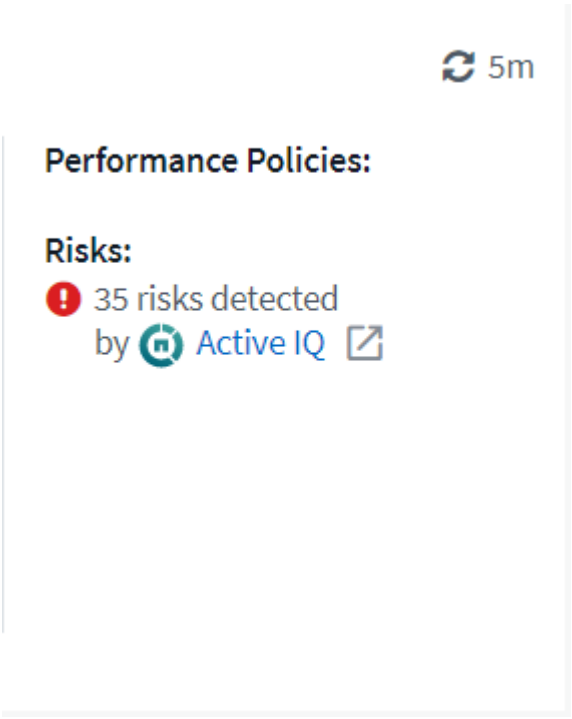


Nell'elenco dei dispositivi in basso, fare clic sul nome del sistema di storage ONTAP monitorato. Viene visualizzata una dashboard contenente le informazioni raccolte sul sistema, inclusi i seguenti dettagli:

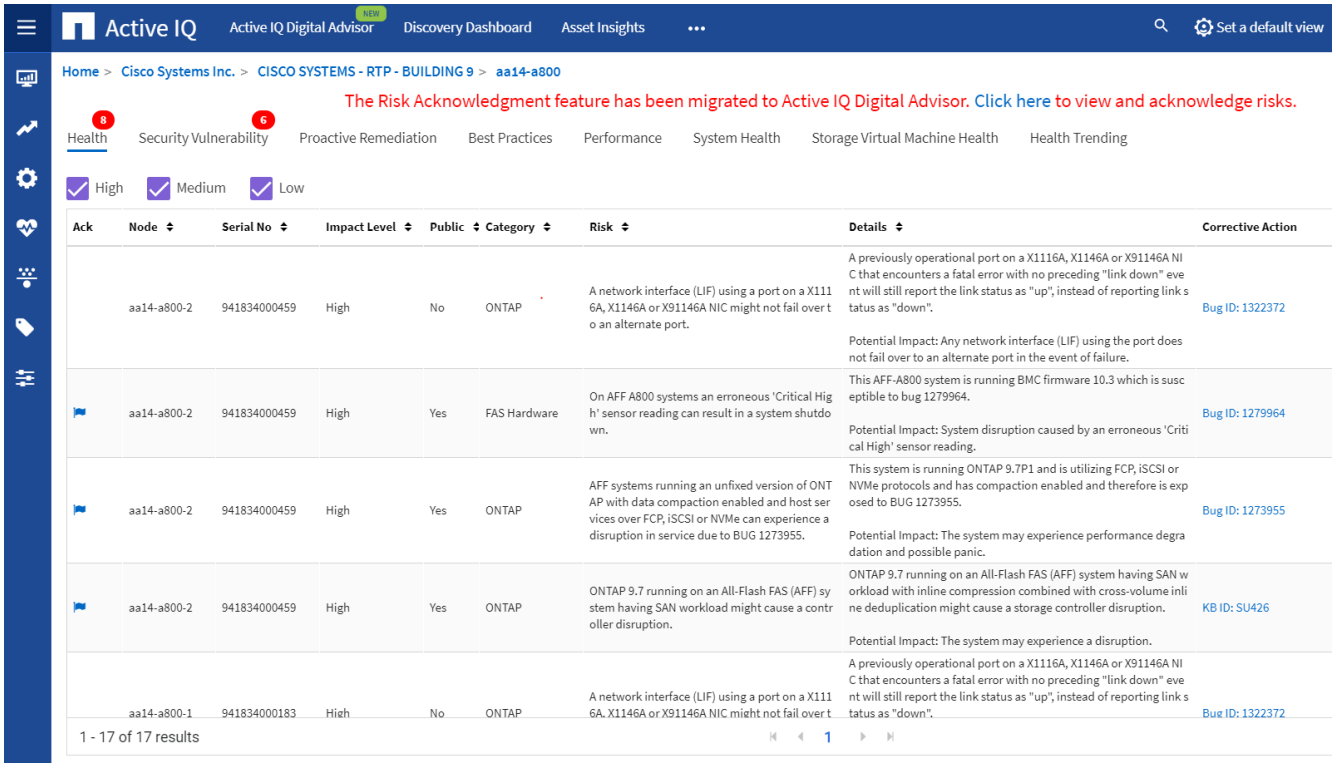
- Modello
- Famiglia
- Versione di ONTAP
- Capacità raw
- IOPS medi
- Latenza media
- Throughput medio



Inoltre, in questa pagina, nella sezione Criteri di performance, è disponibile un link a NetApp Active IQ.



4. Per aprire una nuova scheda del browser e accedere alla pagina di riduzione dei rischi, che mostra quali nodi sono interessati, quanto critici sono i rischi e quali sono le azioni appropriate da intraprendere per correggere i problemi identificati, fare clic sul link per Active IQ.

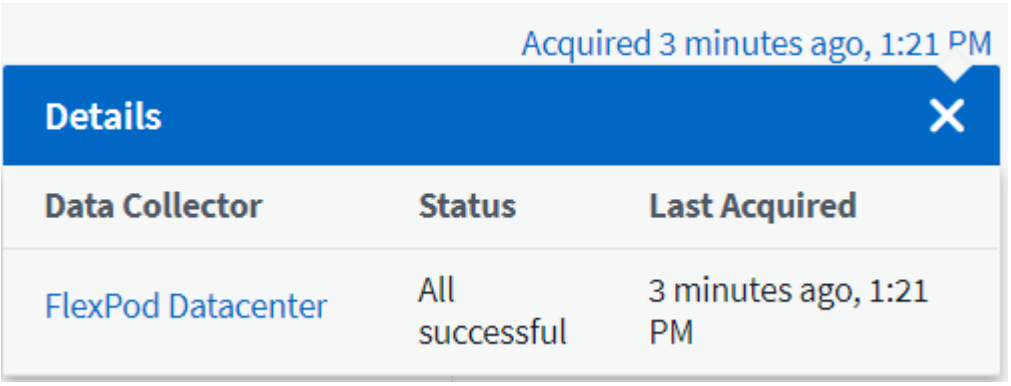


Esplora le dashboard in tempo reale

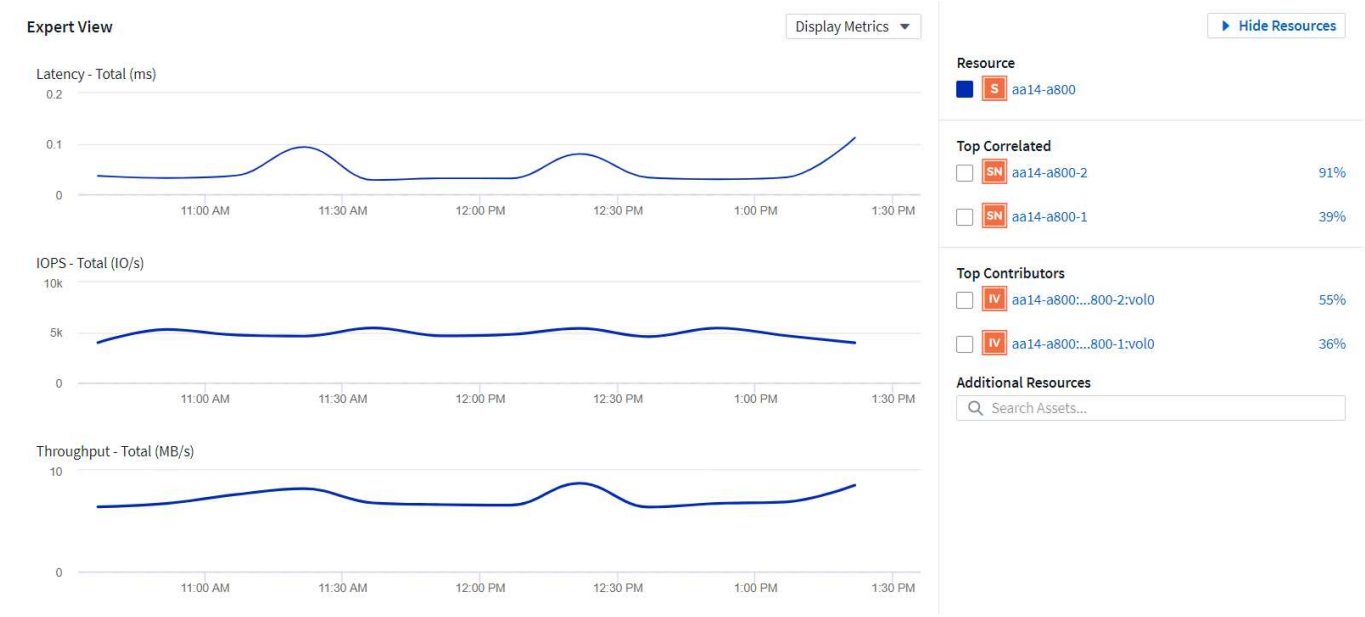
Cloud Insights può visualizzare dashboard in tempo reale delle informazioni raccolte dal sistema di storage ONTAP implementato in una soluzione FlexPod per data center. L'unità di acquisizione Cloud Insights raccoglie i dati a intervalli regolari e compila il dashboard del sistema di storage predefinito con le informazioni raccolte.

Accedi ai grafici in tempo reale dalla dashboard di Cloud Insights

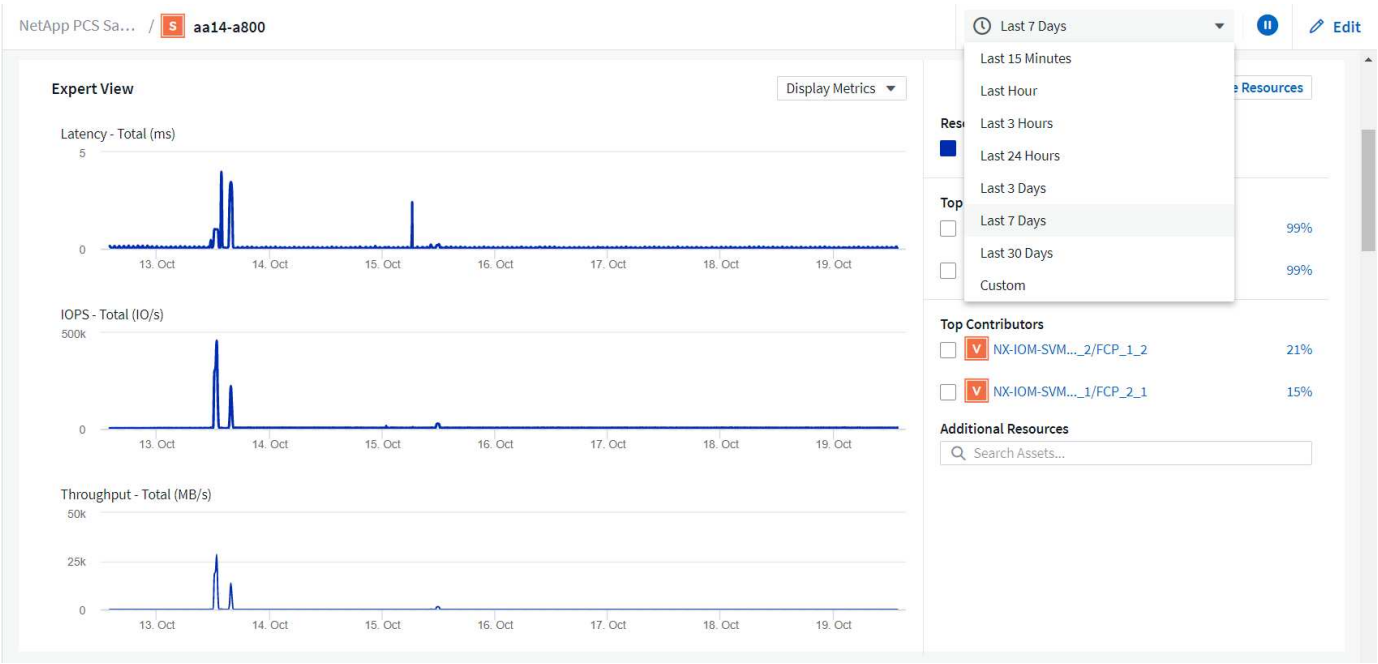
Dalla dashboard del sistema di storage, è possibile visualizzare l'ultima volta che Data Collector ha aggiornato le informazioni. Un esempio è illustrato nella figura seguente.



Per impostazione predefinita, la dashboard del sistema di storage visualizza diversi grafici interattivi che mostrano le metriche a livello di sistema dal sistema di storage sottoposto a polling o da ogni singolo nodo, tra cui latenza, IOPS e throughput, nella sezione visualizzazione avanzata. Esempi di questi grafici predefiniti sono illustrati nella figura seguente.



Per impostazione predefinita, i grafici mostrano le informazioni delle ultime tre ore, ma è possibile impostarle su un numero di valori diversi o su un valore personalizzato dall'elenco a discesa in alto a destra nella dashboard del sistema di storage. Questo è mostrato nella figura seguente.



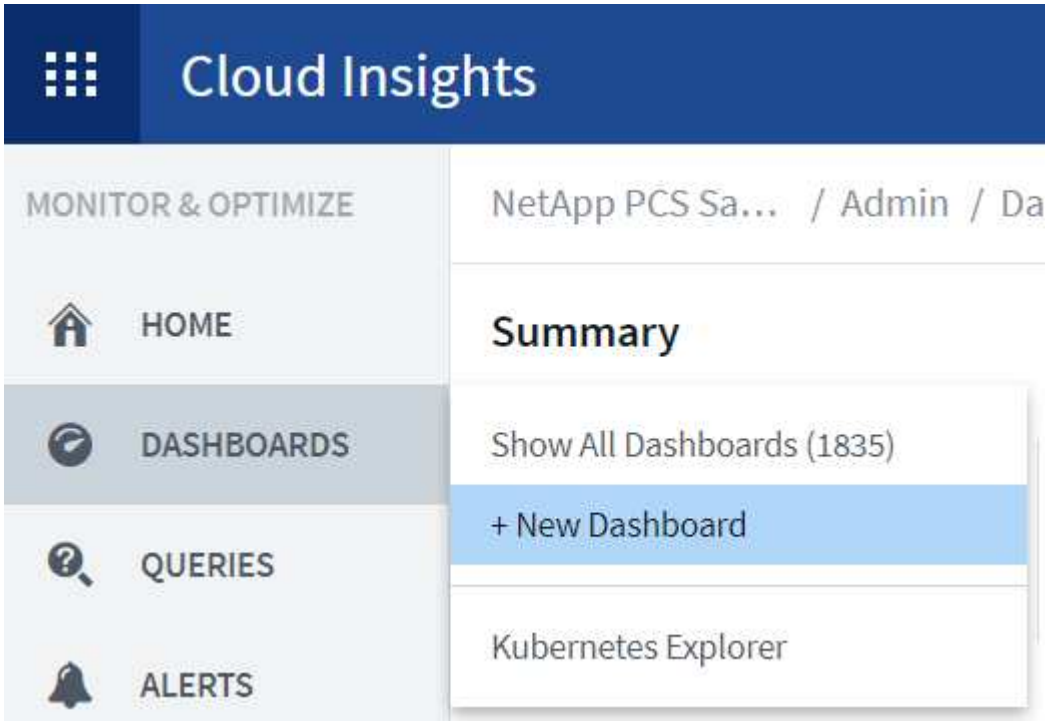
Creare dashboard personalizzati

Oltre a utilizzare i dashboard predefiniti che visualizzano informazioni a livello di sistema, è possibile utilizzare Cloud Insights per creare dashboard completamente personalizzati che consentono di concentrarsi sull'utilizzo delle risorse per volumi di storage specifici nella soluzione FlexPod Datacenter, e quindi le applicazioni implementate nell'infrastruttura convergente che dipendono da questi volumi per funzionare in modo efficace. In questo modo è possibile creare una migliore visualizzazione di applicazioni specifiche e delle risorse che consumano nell'ambiente del data center.

Creare una dashboard personalizzata per valutare le risorse di storage

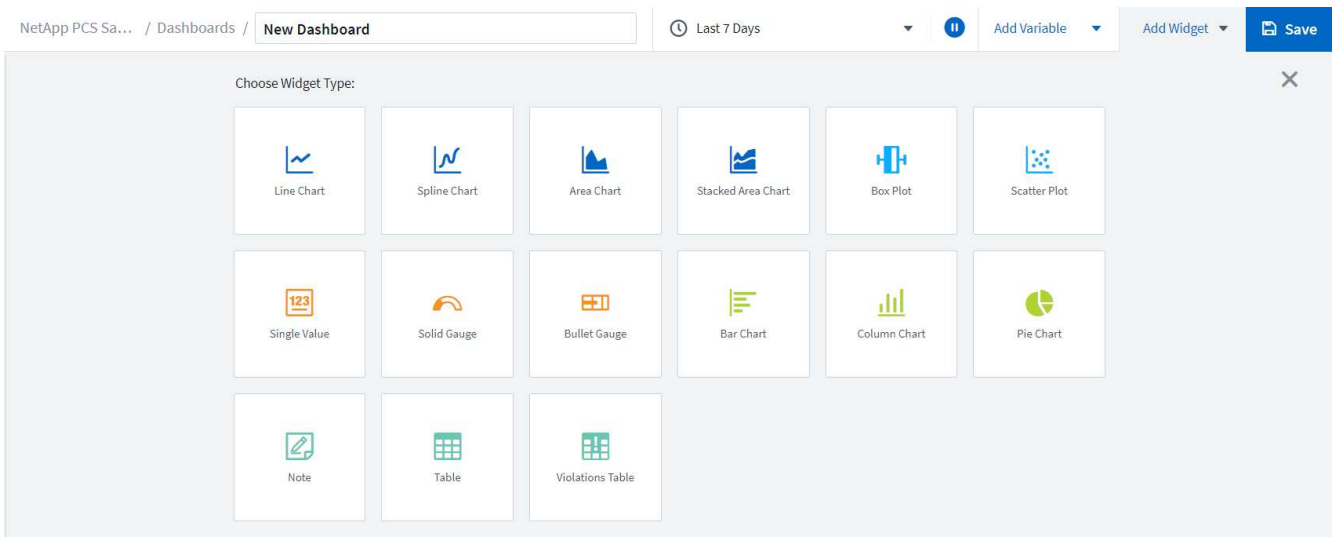
Per creare una dashboard personalizzata per la valutazione delle risorse di storage, attenersi alla seguente procedura:

1. Per creare una dashboard personalizzata, passare il mouse su dashboard nel menu principale di Cloud Insights e fare clic su + nuovo dashboard nell'elenco a discesa.



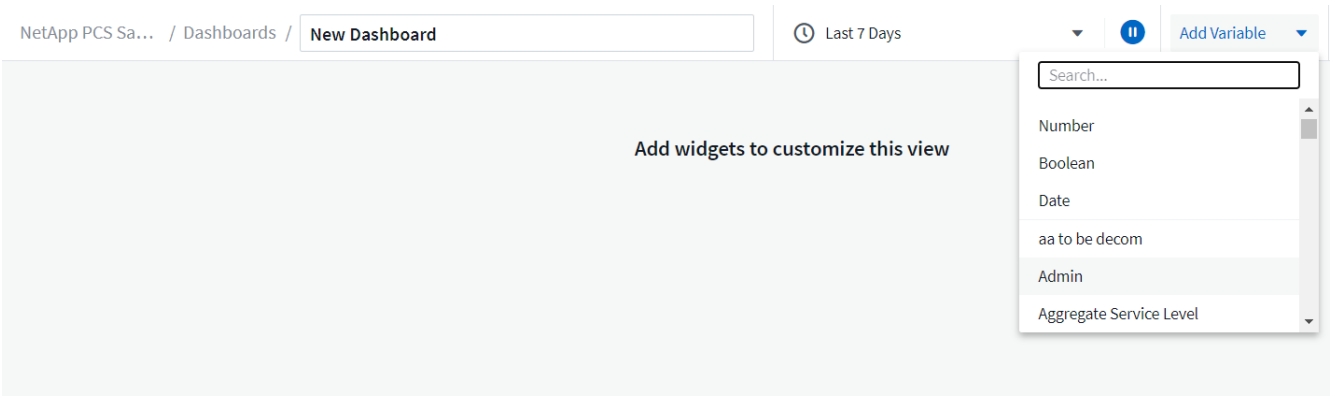
   Viene visualizzata la finestra New Dashboard (nuovo dashboard).

2. Assegnare un nome alla dashboard e selezionare il tipo di widget utilizzato per visualizzare i dati. È possibile scegliere tra diversi tipi di grafici o persino note o tipi di tabelle per visualizzare i dati raccolti.



3. Scegliere variabili personalizzate dal menu Aggiungi variabile.

   In questo modo, i dati presentati sono incentrati sulla visualizzazione di fattori più specifici o specializzati.



4. Per creare una dashboard personalizzata, selezionare il tipo di widget che si desidera utilizzare, ad esempio un grafico a torta per visualizzare l'utilizzo dello storage in base al volume:

   a. Selezionare il widget grafico a torta dall'elenco a discesa Aggiungi widget.

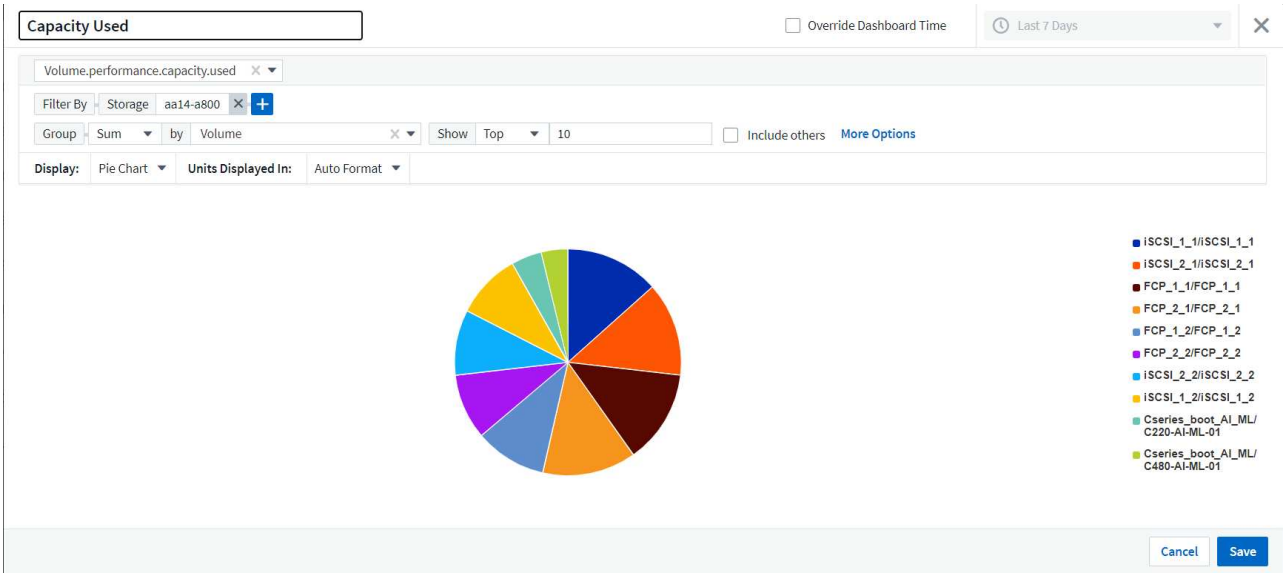
   b. Assegnare un nome al widget con un identificatore descrittivo, ad esempio `Capacity Used`.

   c. Selezionare l'oggetto che si desidera visualizzare. Ad esempio, è possibile effettuare una ricerca in base al volume dei termini chiave e selezionare `volume.performance.capacity.used`.

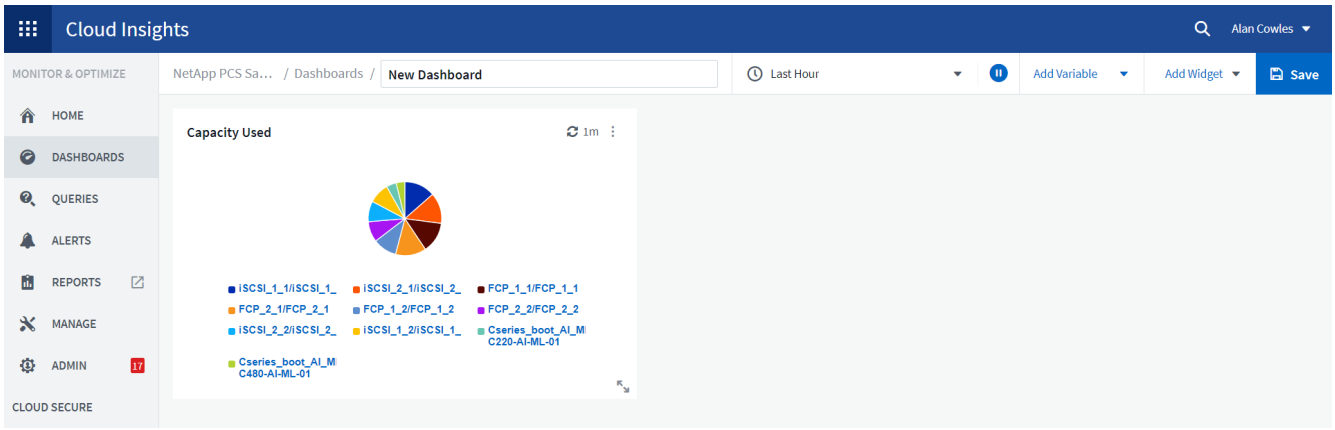
   d. Per filtrare in base ai sistemi storage, utilizzare il filtro e digitare il nome del sistema storage nella soluzione FlexPod Datacenter.

   e. Personalizzare le informazioni da visualizzare. Per impostazione predefinita, questa selezione mostra i volumi di dati ONTAP ed elenca i primi 10 volumi.

   f. Per salvare la dashboard personalizzata, fare clic sul pulsante Save (Salva).



   Dopo aver salvato il widget personalizzato, il browser torna alla pagina New Dashboard, dove viene visualizzato il widget appena creato e consente di eseguire azioni interattive, come la modifica del periodo di polling dei dati.



Risoluzione avanzata dei problemi

Cloud Insights consente di applicare metodi avanzati di troubleshooting a qualsiasi ambiente di storage in un'infrastruttura convergente FlexPod Datacenter. Utilizzando i componenti di ciascuna delle funzionalità menzionate in precedenza: Integrazione Active IQ, dashboard predefiniti con statistiche in tempo reale e dashboard personalizzati, i problemi che potrebbero insorgere vengono rilevati in anticipo e risolti rapidamente. Utilizzando l'elenco dei rischi in Active IQ, un cliente può trovare errori di configurazione segnalati che potrebbero causare problemi o scoprire bug che sono stati segnalati e versioni di codice con patch che possono rimediare. L'osservazione delle dashboard in tempo reale sulla home page di Cloud Insights può aiutare a individuare modelli di performance del sistema che potrebbero essere un indicatore precoce di un problema in aumento e contribuire a risolverlo in modo rapido. Infine, la possibilità di creare dashboard personalizzati consente ai clienti di concentrarsi sulle risorse più importanti della propria infrastruttura e di monitorarle direttamente per garantire che possano raggiungere i propri obiettivi di business continuity.

Ottimizzazione dello storage

Oltre alla risoluzione dei problemi, è possibile utilizzare i dati raccolti da Cloud Insights per ottimizzare il sistema di storage ONTAP implementato in una soluzione di infrastruttura convergente per data center FlexPod. Se un volume mostra una latenza elevata, forse perché diverse macchine virtuali con esigenze di performance elevate condividono lo stesso datastore, tali informazioni vengono visualizzate nella dashboard di Cloud Insights. Con queste informazioni, un amministratore dello storage può scegliere di migrare una o più macchine virtuali su altri volumi, migrare i volumi di storage tra Tier di aggregati o tra nodi nel sistema storage ONTAP, ottenendo un ambiente ottimizzato per le performance. Le informazioni ottenute dall'integrazione di Active IQ con Cloud Insights possono evidenziare i problemi di configurazione che portano a performance inferiori a quelle previste e fornire l'azione correttiva consigliata che, se implementata, può risolvere qualsiasi problema e garantire un sistema storage ottimizzato in modo ottimale.

Video e demo

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per valutare le risorse in un ambiente on-premise "qui".

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per monitorare l'infrastruttura e impostare soglie di allarme per l'infrastruttura "qui".

È possibile vedere una dimostrazione video sull'utilizzo di NetApp Cloud Insights per valutare le singole applicazioni nell'ambiente "qui".

Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione sui prodotti Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Data center FlexPod

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com"

FlexPod con FabricPool - Tiering dei dati inattivi su Amazon AWS S3

TR-4801: FlexPod con FabricPool - Tiering dei dati inattivi su Amazon AWS S3

Scott Kovacs, NetApp

I prezzi dello storage flash continuano a scendere, rendendolo disponibile per carichi di lavoro e applicazioni che non erano stati precedentemente considerati candidati per lo storage flash. Tuttavia, l'utilizzo più efficiente dell'investimento nello storage è ancora di fondamentale importanza per i responsabili IT. I reparti IT continuano a essere solleciti per offrire servizi dalle performance più elevate con un aumento minimo o nullo del budget. Per aiutare a soddisfare queste esigenze, NetApp FabricPool consente di sfruttare l'economia del cloud spostando i dati utilizzati di rado dal costoso storage flash on-premise a un Tier di storage più conveniente nel cloud pubblico. Lo spostamento nel cloud dei dati con accesso non frequente libera spazio prezioso di storage flash sui sistemi AFF o FAS per offrire maggiore capacità per i carichi di lavoro business-critical al Tier flash ad elevate performance.

Questo report tecnico analizza la funzionalità di tiering dei dati FabricPool di NetApp ONTAP nel contesto di un'architettura di infrastruttura convergente FlexPod di NetApp e Cisco. Per trarre il massimo vantaggio dai concetti discussi in questo report tecnico, è necessario conoscere l'architettura dell'infrastruttura convergente del data center FlexPod e il software di storage ONTAP. Sulla base della familiarità con FlexPod e ONTAP, discutiamo di FabricPool, del suo funzionamento e di come può essere utilizzato per ottenere un utilizzo più efficiente dello storage flash on-premise. Gran parte del contenuto di questo report viene trattato in maniera più dettagliata in "TR-4598 FabricPool Best practice" E altra documentazione sui prodotti ONTAP. Il contenuto è stato condensato per un'infrastruttura FlexPod e non copre completamente tutti i casi di utilizzo di FabricPool. Tutte le funzionalità e i concetti esaminati sono disponibili in ONTAP 9.6.

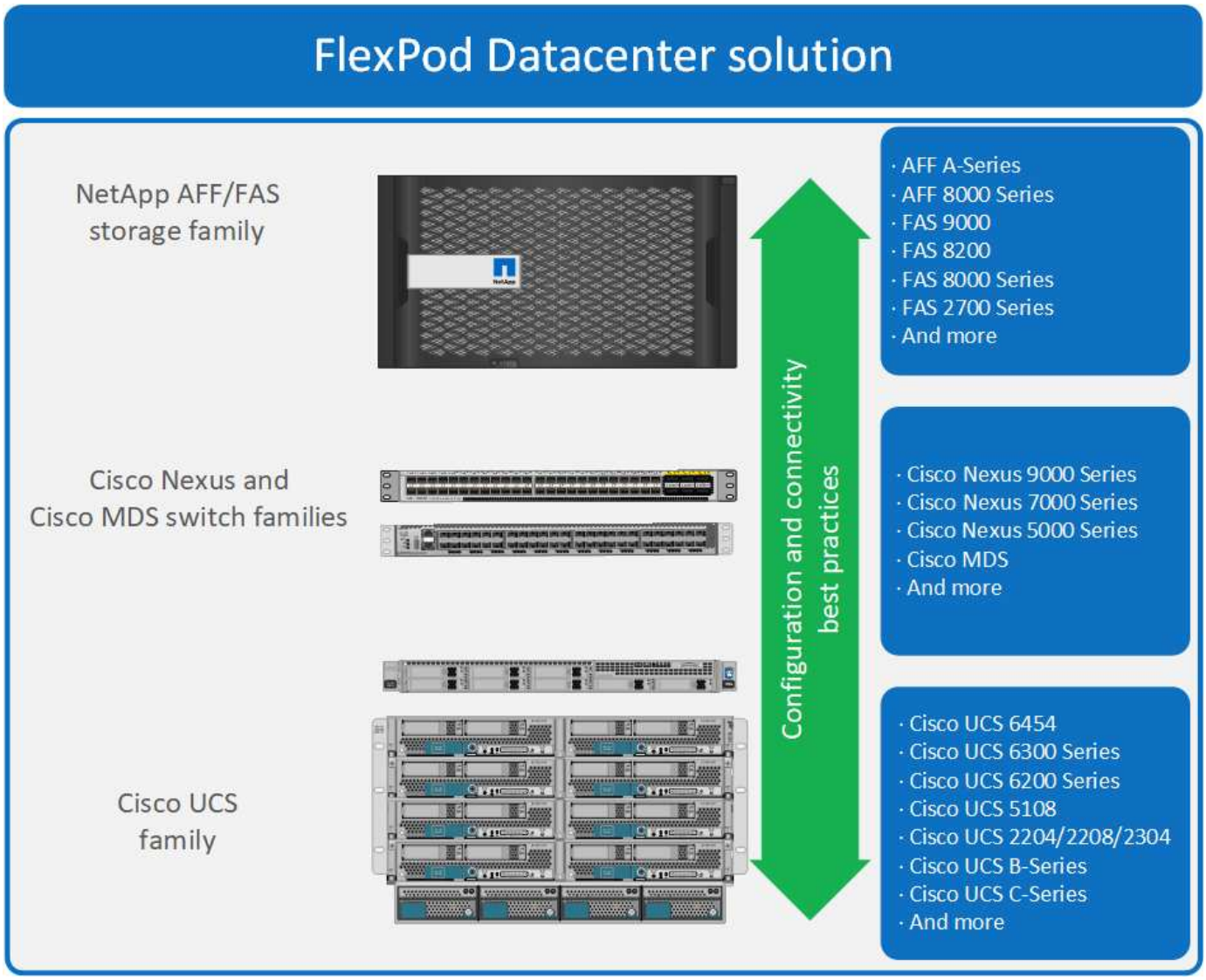
Ulteriori informazioni su FlexPod sono disponibili in "Specifiche tecniche del data center TR-4036 FlexPod".

Panoramica e architettura di FlexPod

Panoramica di FlexPod

FlexPod è un set definito di hardware e software che costituisce una base integrata per le soluzioni virtualizzate e non. FlexPod include storage NetApp AFF, networking Cisco Nexus, storage networking Cisco MDS, Cisco Unified Computing System (Cisco UCS) e software VMware vSphere in un unico pacchetto. Il design è abbastanza flessibile da consentire il collegamento in rete, il calcolo e lo storage in un rack del data center oppure può essere implementato in base alla progettazione del data center del cliente. La densità delle porte consente ai componenti di rete di ospitare più configurazioni.

Uno dei vantaggi dell'architettura FlexPod è la possibilità di personalizzare o flettere l'ambiente in base alle esigenze del cliente. Un'unità FlexPod può essere facilmente scalata in base ai requisiti e alla domanda. Un'unità può essere scalata sia in su (aggiungendo risorse a un'unità FlexPod) che in out (aggiungendo altre unità FlexPod). L'architettura di riferimento di FlexPod evidenzia la resilienza, i vantaggi in termini di costi e la facilità di implementazione di una soluzione di storage basata su Fibre Channel e IP. Un sistema storage in grado di servire più protocolli in un'unica interfaccia offre ai clienti una scelta e protegge il loro investimento perché si tratta di un'architettura wire-once. La figura seguente mostra molti dei componenti hardware di FlexPod.

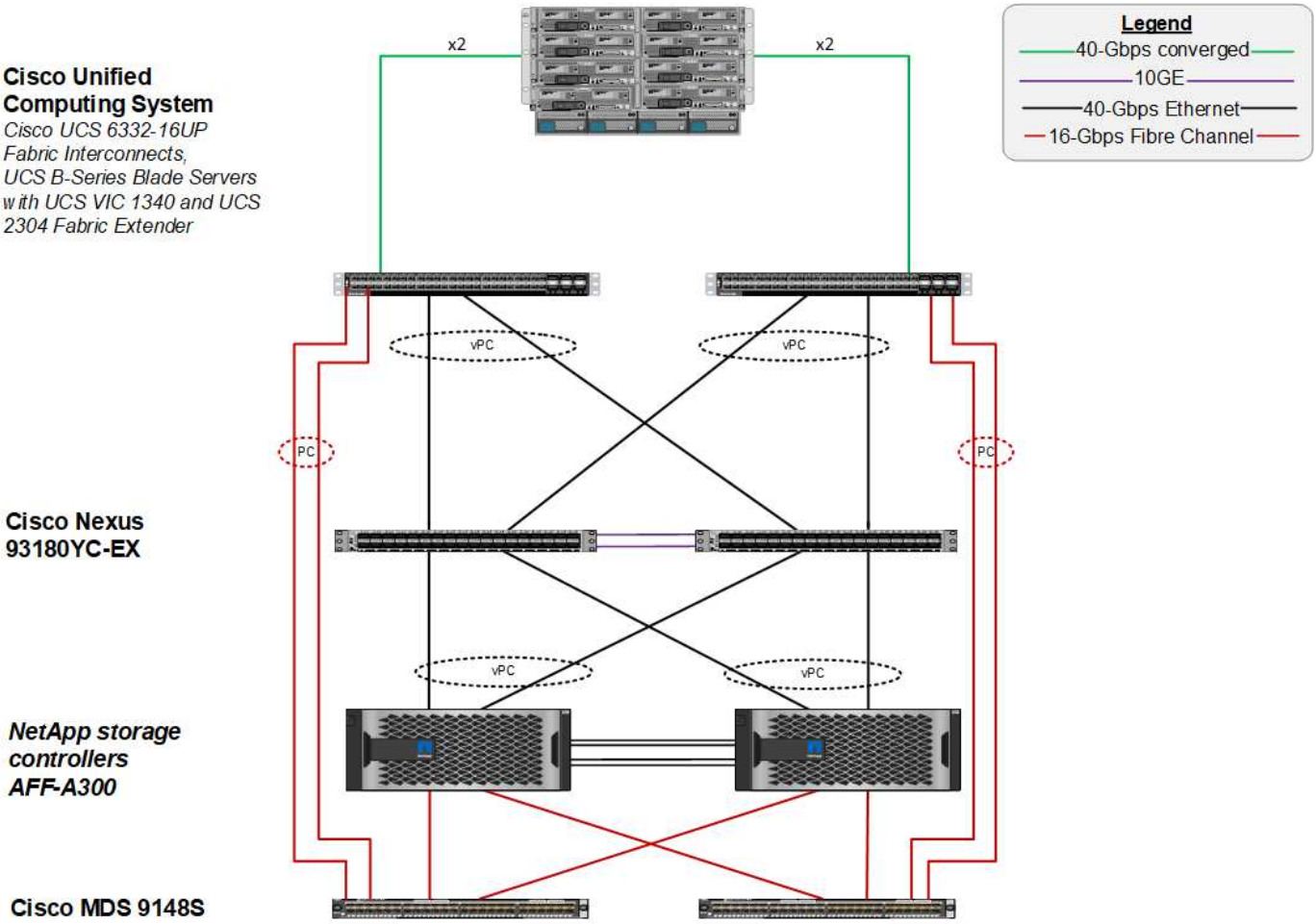


Architettura FlexPod

La figura seguente mostra i componenti di una soluzione VMware vSphere e FlexPod e le connessioni di rete necessarie per le interconnessioni fabric Cisco UCS 6454. Questo progetto ha i seguenti componenti:

- Connessioni Ethernet da 40 GB con canale di porta tra lo chassis blade Cisco UCS 5108 e le interconnessioni fabric Cisco UCS
- Connessioni Ethernet da 40 GB tra Cisco UCS Fabric Interconnect e Cisco Nexus 9000
- Connessioni Ethernet da 40 GB tra Cisco Nesxus 9000 e lo storage array NetApp AFF A300

Queste opzioni di infrastruttura sono state ampliate con l'introduzione degli switch Cisco MDS che si trovano tra l'interconnessione fabric Cisco UCS e NetApp AFF A300. Questa configurazione fornisce host con avvio FC con accesso a livello di blocco FC da 16 GB allo storage condiviso. L'architettura di riferimento rafforza la strategia wire-once, perché, con l'aggiunta di storage aggiuntivo all'architettura, non è richiesta alcuna ricablaggio dagli host all'interconnessione fabric Cisco UCS.



FabricPool

Panoramica di FabricPool

FabricPool è una soluzione di storage ibrido in ONTAP che utilizza un aggregato all-flash (SSD) come Tier di performance e un archivio di oggetti in un servizio di cloud pubblico come Tier di cloud. Questa configurazione consente lo spostamento dei dati basato su policy, a seconda che i dati siano o meno utilizzati frequentemente. FabricPool è supportato in ONTAP per aggregati AFF e all-SSD su piattaforme FAS. L'elaborazione dei dati

viene eseguita a livello di blocco, con blocchi di dati ad accesso frequente nel Tier di performance all-flash contrassegnati come blocchi a caldo e ad accesso non frequente contrassegnati come cold.

L'utilizzo di FabricPool consente di ridurre i costi dello storage senza compromettere performance, efficienza, sicurezza o protezione. FabricPool è trasparente per le applicazioni aziendali e sfrutta l'efficienza del cloud riducendo il TCO dello storage senza dover riprogettare l'infrastruttura applicativa.

FlexPod può trarre vantaggio dalle funzionalità di tiering dello storage di FabricPool per un utilizzo più efficiente dello storage flash ONTAP. Le macchine virtuali inattive (VM), i modelli di macchine virtuali utilizzati di rado e i backup delle macchine virtuali da NetApp SnapCenter per vSphere possono consumare spazio prezioso nel volume del datastore. Lo spostamento dei dati cold nel Tier cloud libera spazio e risorse per applicazioni mission-critical ad alte performance ospitate nell'infrastruttura FlexPod.

> I protocolli Fibre Channel e iSCSI in genere impiegano più tempo prima di riscontrare un timeout (da 60 a 120 secondi), ma non riprovano a stabilire una connessione nello stesso modo dei protocolli NAS. In caso di timeout di un protocollo SAN, l'applicazione deve essere riavviata. Anche una breve interruzione potrebbe essere disastrosa per le applicazioni di produzione che utilizzano i protocolli SAN perché non esiste alcun modo per garantire la connettività ai cloud pubblici. Per evitare questo problema, NetApp consiglia di utilizzare cloud privati quando si tierano i dati a cui si accede dai protocolli SAN.

In ONTAP 9.6, FabricPool si integra con tutti i principali provider di cloud pubblico: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage e Microsoft Azure Blob Storage. Questo report si concentra sullo storage Amazon AWS S3 come livello di oggetti cloud preferito.

L'aggregato composito

Un'istanza di FabricPool viene creata associando un aggregato flash ONTAP a un archivio di oggetti cloud, ad esempio un bucket AWS S3, per creare un aggregato composito. Quando i volumi vengono creati all'interno dell'aggregato composito, possono sfruttare le funzionalità di tiering di FabricPool. Quando i dati vengono scritti nel volume, ONTAP assegna una temperatura a ciascuno dei blocchi di dati. Quando il blocco viene scritto per la prima volta, viene assegnata una temperatura di caldo. Con il passare del tempo, se i dati non sono accessibili, vengono sottoposti a un processo di raffreddamento fino a quando non viene assegnato uno stato Cold. Questi blocchi di dati ad accesso non frequente vengono quindi suddivisi in tiering dall'aggregato SSD delle performance e nell'archivio di oggetti cloud.

Il periodo di tempo che intercorre tra il momento in cui un blocco viene designato come cold e il momento in cui viene spostato nello storage a oggetti cloud viene modificato dalla policy di tiering del volume in ONTAP. Un'ulteriore granularità si ottiene modificando le impostazioni di ONTAP che controllano il numero di giorni necessari per far sì che un blocco diventi freddo. I candidati per il tiering dei dati sono le snapshot dei volumi tradizionali, i backup di SnapCenter per vSphere VM e altri backup basati su Snapshot di NetApp e tutti i blocchi utilizzati di rado in un datastore vSphere, come i modelli di macchine virtuali e i dati delle macchine virtuali a cui si accede di rado.

Reporting dei dati inattivi

Il reporting dei dati inattivi (IDR) è disponibile in ONTAP per valutare la quantità di dati cold che possono essere suddivisi in più livelli da un aggregato. IDR è attivato per impostazione predefinita in ONTAP 9.6 e utilizza un criterio di raffreddamento predefinito di 31 giorni per determinare quali dati nel volume sono inattivi.

> La quantità di dati cold a più livelli dipende dai criteri di tiering impostati sul volume. Questa quantità può essere diversa dalla quantità di dati cold rilevata da IDR utilizzando il periodo di raffreddamento predefinito di 31 giorni.

Creazione di oggetti e spostamento dei dati

FabricPool lavora a livello di NetApp WAFL Block, raffreddando i blocchi, concatenandoli in oggetti storage e migrando tali oggetti a un livello cloud. Ogni oggetto FabricPool è di 4 MB ed è composto da 1,024 blocchi da 4 KB. La dimensione dell'oggetto è fissa a 4 MB in base ai consigli sulle performance dei principali cloud provider e non può essere modificata. Se i blocchi cold vengono letti e resi hot, vengono recuperati solo i blocchi richiesti nell'oggetto da 4 MB e spostati di nuovo nel Tier di performance. L'intero oggetto e l'intero file non vengono migrati di nuovo. Vengono migrati solo i blocchi necessari.

Se ONTAP rileva un'opportunità di readhead sequenziali, richiede i blocchi dal Tier cloud prima di essere letti per migliorare le performance.

Per impostazione predefinita, i dati vengono spostati nel Tier cloud solo quando l'aggregato delle performance viene utilizzato oltre il 50%. Questa soglia può essere impostata su una percentuale inferiore per consentire lo spostamento di una minore quantità di storage dei dati sul Tier flash delle performance nel cloud. Questo potrebbe essere utile se la strategia di tiering è quella di spostare i dati cold solo quando l'aggregato si avvicina alla capacità.

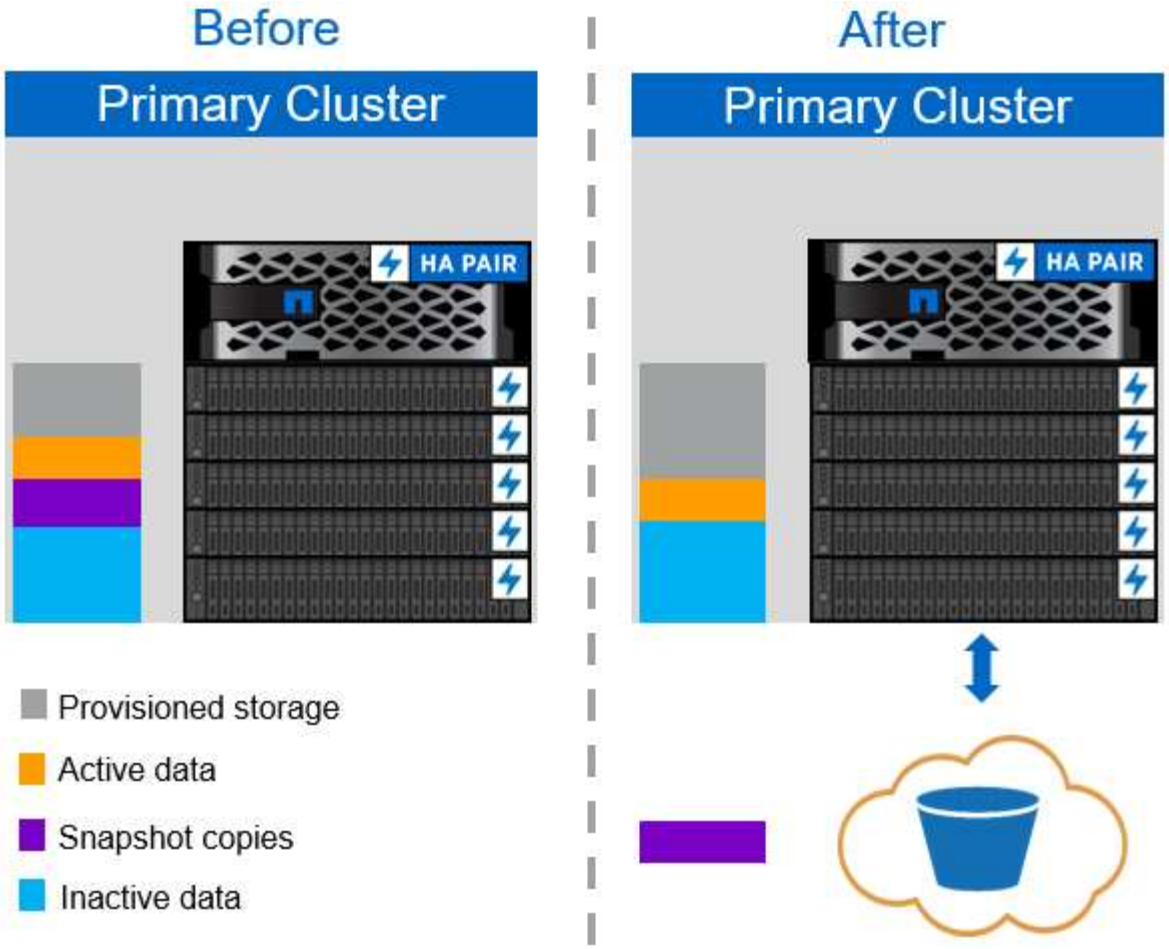
Se l'utilizzo del Tier di performance è superiore al 70% della capacità, i dati cold vengono letti direttamente dal Tier cloud senza essere riscritti nel Tier di performance. Impedendo il write-back dei dati cold su aggregati fortemente utilizzati, FabricPool preserva l'aggregato per i dati attivi.

Recuperare lo spazio del Tier di performance

Come discusso in precedenza, il caso d'utilizzo principale di FabricPool è quello di facilitare l'utilizzo più efficiente dello storage flash on-premise dalle performance elevate. I dati cold sotto forma di snapshot di volumi e backup di macchine virtuali dell'infrastruttura virtuale FlexPod possono occupare una quantità significativa di costoso storage flash. È possibile liberare lo storage Tier dalle performance preziose implementando una delle due policy di tiering: Snapshot-only o Auto.

Policy di tiering solo Snapshot

La policy di tiering Snapshot-Only, illustrata nella figura seguente, sposta i dati snapshot dei volumi cold e i backup SnapCenter per vSphere delle macchine virtuali che occupano spazio ma non condividono blocchi con il file system attivo in un archivio di oggetti cloud. La policy di tiering Snapshot-Only sposta i blocchi di dati cold nel Tier cloud. Se è necessario un ripristino, i blocchi freddi nel cloud vengono resi hot e spostati di nuovo sul Tier flash delle performance on-premise.

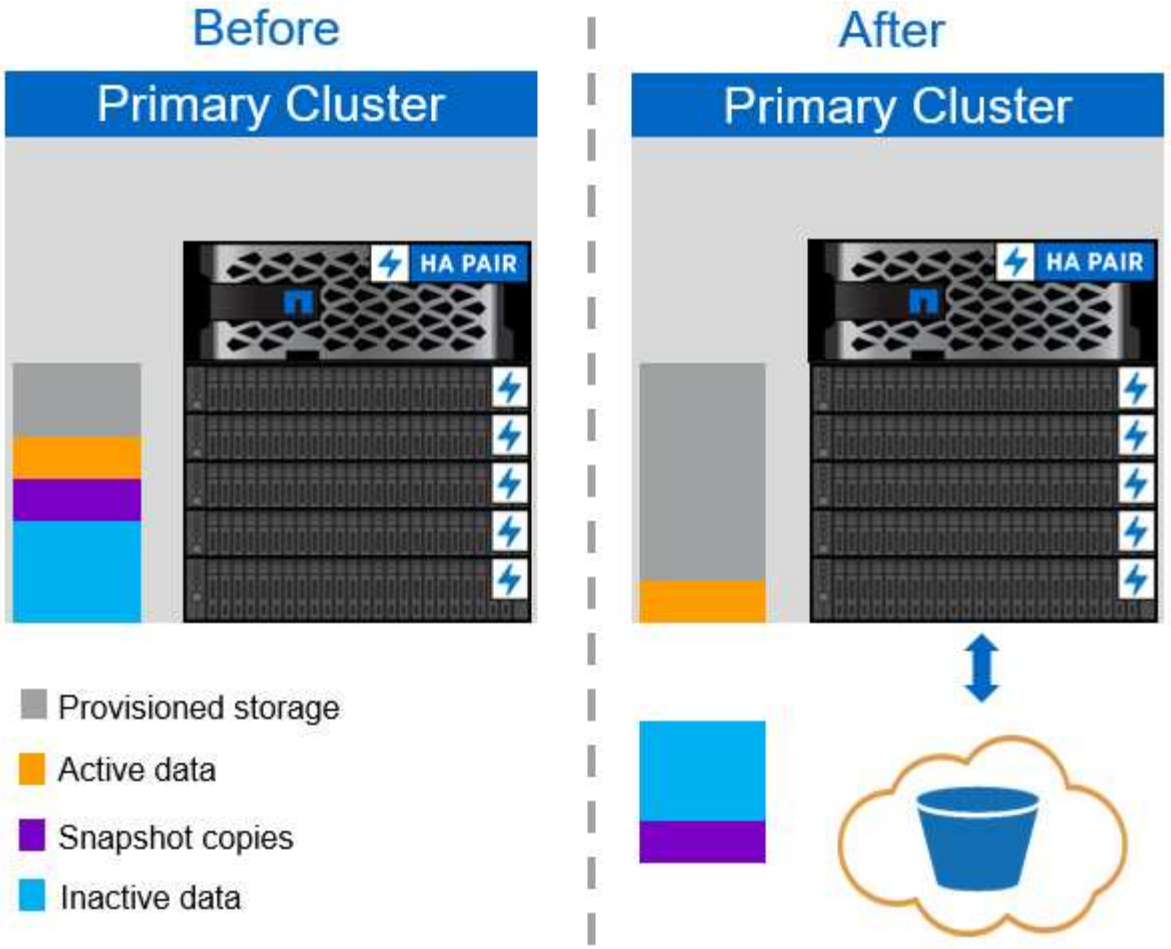


Policy di tiering automatico

La policy di tiering automatico di FabricPool, illustrata nella figura seguente, non solo sposta i blocchi di dati cold snapshot nel cloud, ma sposta anche i blocchi cold nel file system attivo. Questo può includere modelli di macchine virtuali ed eventuali dati di macchine virtuali inutilizzati nel volume dell'archivio dati. I blocchi a freddo che vengono spostati sono controllati da `tiering-minimum-cooling-days` impostazione del volume. Se un'applicazione legge casualmente i blocchi freddi nel Tier cloud, questi vengono resi hot e riportati al Tier di performance. Tuttavia, se i blocchi freddi vengono letti da un processo sequenziale come un antivirus scanner, i blocchi rimangono freddi e persistono nell'archivio di oggetti cloud; non vengono spostati di nuovo al livello di performance.

Quando si utilizza la policy di tiering automatico, i blocchi a cui si accede raramente e che vengono resi a caldo vengono ritirati dal Tier cloud alla velocità della connettività cloud. Questo può influire sulle prestazioni delle macchine virtuali se l'applicazione è sensibile alla latenza, che deve essere presa in considerazione prima di utilizzare il criterio di tiering automatico nel datastore. NetApp consiglia di posizionare le LIF Intercluster su porte con una velocità di 10 GbE per ottenere performance adeguate.

Il profiler dell'archivio di oggetti deve essere utilizzato per verificare la latenza e il throughput nell'archivio di oggetti prima di associarlo a un aggregato FabricPool.



Policy di tiering

A differenza delle policy Auto e Snapshot-Only, la policy all tiering sposta immediatamente interi volumi di dati nel Tier cloud. Questa policy è più adatta alla protezione dei dati secondari o ai volumi di archiviazione per i quali i dati devono essere conservati per scopi storici o normativi, ma a cui si accede raramente. La policy all non è consigliata per i volumi del datastore VMware perché qualsiasi dato scritto nel datastore viene immediatamente spostato nel Tier cloud. Le successive operazioni di lettura vengono eseguite dal cloud e potrebbero potenzialmente introdurre problemi di performance per le macchine virtuali e le applicazioni che risiedono nel volume del datastore.

Sicurezza

La sicurezza è una preoccupazione centrale per il cloud e per FabricPool. Tutte le funzionalità di sicurezza native di ONTAP sono supportate nel Tier di performance e lo spostamento dei dati è protetto quando vengono trasferiti al Tier cloud. FabricPool utilizza "AES-256-GCM" algoritmo di crittografia sul tier di performance e mantiene la crittografia end-to-end nel tier cloud. I blocchi di dati spostati nell'archivio di oggetti cloud sono protetti con TLS (Transport Layer Security) v1.2 per mantenere la riservatezza e l'integrità dei dati tra i livelli di storage.

La comunicazione con l'archivio di oggetti cloud tramite una connessione non crittografata è supportata ma non consigliata da NetApp.

Crittografia dei dati

La crittografia dei dati è fondamentale per la protezione della proprietà intellettuale, delle informazioni

commerciali e delle informazioni personali dei clienti. FabricPool supporta completamente la crittografia dei volumi NetApp (NVE) e la crittografia dello storage NetApp (NSE) per mantenere le strategie di protezione dei dati esistenti. Tutti i dati crittografati nel Tier di performance rimangono crittografati quando vengono spostati nel Tier cloud. Le chiavi di crittografia lato client sono di proprietà di ONTAP e le chiavi di crittografia dell'archivio di oggetti lato server sono di proprietà del rispettivo archivio di oggetti cloud. Tutti i dati non crittografati con NVE vengono crittografati con l'algoritmo AES-256-GCM. Non sono supportati altri tipi di crittografia AES-256.

L'utilizzo di NSE o NVE è opzionale e non è richiesto per l'utilizzo di FabricPool.

Requisiti FabricPool

FabricPool richiede ONTAP 9.2 o versione successiva e l'utilizzo di aggregati di SSD su qualsiasi piattaforma elencata in questa sezione. I requisiti FabricPool aggiuntivi dipendono dal livello cloud collegato. Per le piattaforme AFF entry-level con una capacità fissa e relativamente ridotta come NetApp AFF C190, FabricPool può essere estremamente efficace per lo spostamento dei dati inattivi nel Tier cloud.

Piattaforme

FabricPool è supportato sulle seguenti piattaforme:

- NetApp AFF
  - R800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 E AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 E FAS8040
  - FAS2750, FAS2720
  - FAS2650, FAS2620

Solo gli aggregati di SSD sulle piattaforme FAS possono utilizzare FabricPool.

- Tier cloud
  - Alibaba Cloud Object Storage Service (accesso standard e non frequente)
  - Amazon S3 (Standard, Standard-IA, One zone-IA, Intelligent-Tiering)
  - Amazon Commercial Cloud Services (C2S)
  - Google Cloud Storage (multi-regionale, regionale, nearline, coldline)
  - IBM Cloud Object Storage (Standard, Vault, Cold Vault, Flex)

- Storage Blob Microsoft Azure (caldo e freddo)

LIF di intercluster

Le coppie di cluster ad alta disponibilità (ha) che utilizzano FabricPool richiedono due interfacce logiche intercluster (LIFF) per comunicare con il livello cloud. NetApp consiglia di creare una LIF intercluster su coppie ha aggiuntive per collegare perfettamente i Tier cloud anche agli aggregati su tali nodi.

La LIF utilizzata da ONTAP per connettersi all'archivio di oggetti AWS S3 deve trovarsi su una porta a 10 Gbps.

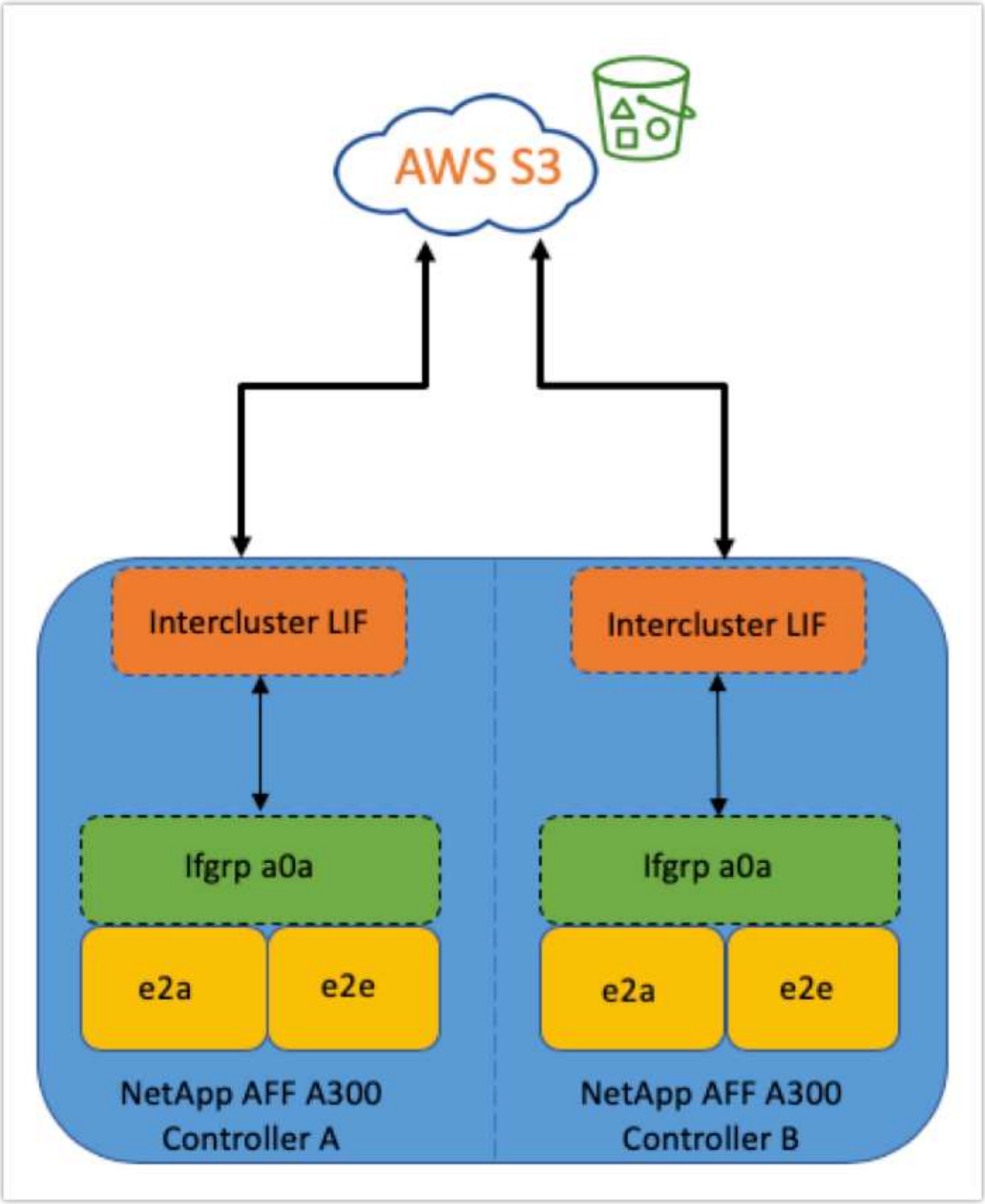
Se su un nodo con routing diverso viene utilizzato più LIF Intercluser, NetApp consiglia di inserirli in spazi IPdiversi. Durante la configurazione, FabricPool può selezionare diversi spazi IP, ma non è in grado di selezionare specifici LIF di intercluster all'interno di uno spazio IPSpace.

La disattivazione o l'eliminazione di un LIF intercluster interrompe la comunicazione con il livello cloud.

Connettività

La latenza di lettura FabricPool è una funzione della connettività al livello cloud. Le LIF di intercluster che utilizzano porte a 10 Gbps, illustrate nella figura seguente, offrono performance adeguate. NetApp consiglia di validare la latenza e il throughput dello specifico ambiente di rete per determinare l'effetto che ha sulle performance di FabricPool.

Quando si utilizza FabricPool in ambienti a basse performance, i requisiti minimi di performance per le applicazioni client devono continuare a essere soddisfatti e gli obiettivi dei tempi di recovery devono essere adeguati di conseguenza.



Profiler dell'archivio di oggetti

Il profiler dell'archivio di oggetti, un esempio del quale è illustrato di seguito ed è disponibile tramite l'interfaccia CLI di ONTAP, verifica la latenza e le performance di throughput degli archivi di oggetti prima che siano collegati a un aggregato FabricPool.

Il Tier cloud deve essere aggiunto a ONTAP prima di poter essere utilizzato con il profiler dell'archivio di oggetti.

Avviare il profiler dell'archivio di oggetti dalla modalità avanzata dei privilegi in ONTAP con il seguente comando:

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Per visualizzare i risultati, eseguire il seguente comando:

```
storage aggregate object-store profiler show
```

I Tier cloud non offrono performance simili a quelle riscontrate nel Tier di performance (in genere GB al secondo). Sebbene gli aggregati FabricPool possano facilmente fornire performance simili a quelle di SATA, possono tollerare anche latenze fino a 10 secondi e un basso throughput per le soluzioni di tiering che non richiedono performance simili a quelle di SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

Volumi

Il thin provisioning dello storage è una pratica standard per l'amministratore dell'infrastruttura virtuale FlexPod. NetApp Virtual Storage Console (VSC) esegue il provisioning dei volumi di storage per gli archivi dati VMware senza alcuna garanzia di spazio (thin provisioning) e con impostazioni di efficienza dello storage ottimizzate in base alle Best practice NetApp. Se si utilizza VSC per creare datastore VMware, non è necessaria alcuna azione aggiuntiva, in quanto non è necessario assegnare alcuna garanzia di spazio al volume del datastore.

FabricPool non può collegare un Tier cloud a un aggregato che contiene volumi utilizzando una garanzia di spazio diversa da Nessuno (ad esempio, volume).

```
volume modify -space-guarantee none
```

Impostazione di `space-guarantee none` il parametro fornisce il thin provisioning per il volume. La quantità

di spazio consumata dai volumi con questo tipo di garanzia aumenta man mano che vengono aggiunti i dati, anziché essere determinata dalla dimensione iniziale del volume. Questo approccio è essenziale per FabricPool perché il volume deve supportare i dati del Tier cloud che diventano "hot" e vengono riportati al Tier di performance.

Licensing

FabricPool richiede una licenza basata sulla capacità quando si collegano provider di storage a oggetti di terze parti (come Amazon S3) come Tier cloud per sistemi flash ibridi AFF e FAS.

Le licenze FabricPool sono disponibili in formato perpetuo o a termine (1 o 3 anni).

Il tiering al Tier cloud si interrompe quando la quantità di dati (capacità utilizzata) memorizzati nel Tier cloud raggiunge la capacità concessa in licenza. I dati aggiuntivi, incluse le copie SnapMirror sui volumi che utilizzano la policy di tiering completo, non possono essere suddivisi in più livelli fino a quando la capacità della licenza non viene aumentata. Anche se il tiering si ferma, i dati sono ancora accessibili dal Tier cloud. I dati cold aggiuntivi rimangono sugli SSD fino all'aumento della capacità concessa in licenza.

Con l'acquisto di qualsiasi nuovo cluster ONTAP 9.5 o successivo, viene fornita una licenza FabricPool a termine gratuita da 10 TB di capacità, anche se potrebbero essere applicati costi di supporto aggiuntivi. Le licenze FabricPool (inclusa la capacità aggiuntiva per le licenze esistenti) possono essere acquistate con incrementi di 1 TB.

Una licenza FabricPool può essere eliminata solo da un cluster che non contiene aggregati FabricPool.

> Le licenze FabricPool sono disponibili in tutto il cluster. L'UUID dovrebbe essere disponibile al momento dell'acquisto di una licenza (`cluster identify show`). Per ulteriori informazioni sulla licenza, fare riferimento a. "Knowledge base di NetApp".

Configurazione

Revisioni del software

La seguente tabella illustra le versioni hardware e software validate.

Layer	Dispositivo	Immagine	Commenti
Storage	NetApp AFF A300	ONTAP 9.6P2	
Calcolo	Server blade Cisco UCS B200 M5 con Cisco UCS VIC 1340	Versione 4.0(4b)	
Rete	Interconnessione fabric Cisco Nexus 6332-16UP	Versione 4.0(4b)	
	Switch Cisco Nexus 93180YC-EX in modalità standalone NX-OS	Versione 7.0(3)I7(6)	
Rete di storage	Cisco MDS 9148S	Versione 8.3(2)	

Layer	Dispositivo	Immagine	Commenti
Hypervisor		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		VMware vCenter Server	VCenter server 6.7.0.30000 build 13639309
Cloud provider		Amazon AWS S3	Bucket S3 standard con opzioni predefinite

I requisiti di base per FabricPool sono descritti nella "Requisiti FabricPool". Una volta soddisfatti tutti i requisiti di base, completare la seguente procedura per configurare FabricPool:

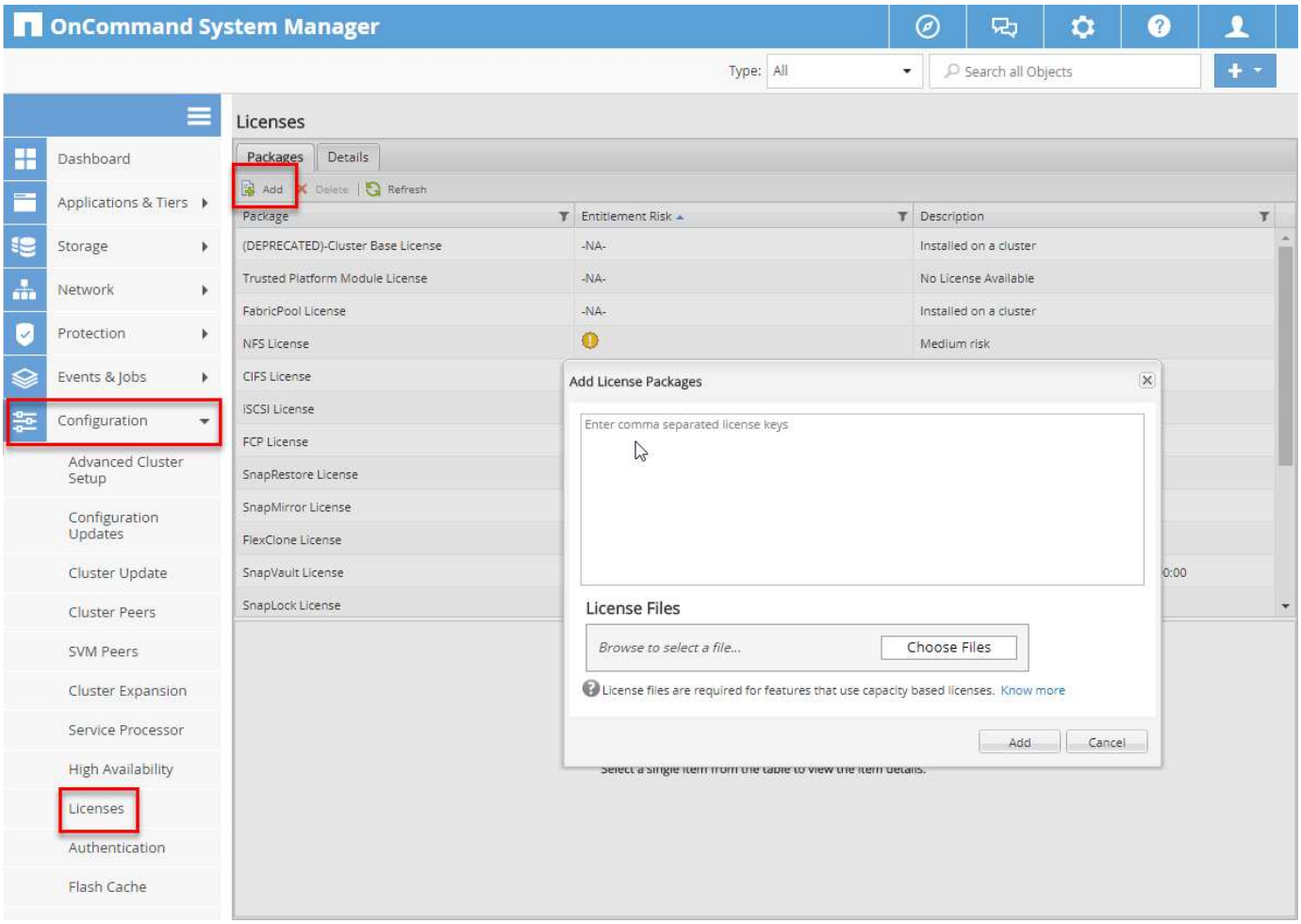
1. Installare una licenza FabricPool.
2. Creare un bucket dello store di oggetti AWS S3.
3. Aggiungi un Tier cloud a ONTAP.
4. Collegare il Tier cloud a un aggregato.
5. Impostare il criterio di tiering del volume.

"Avanti: Installare la licenza FabricPool."

Installare la licenza FabricPool

Dopo aver acquisito un file di licenza NetApp, è possibile installarlo con Gestione di sistema di OnCommand. Per installare il file di licenza, attenersi alla seguente procedura:

1. Fare clic su configurazioni.
2. Fare clic su Cluster.
3. Fare clic su licenze.
4. Fare clic su Aggiungi.
5. Fare clic su Choose Files (Scegli file) per sfogliare e selezionare un file.
6. Fare clic su Aggiungi.



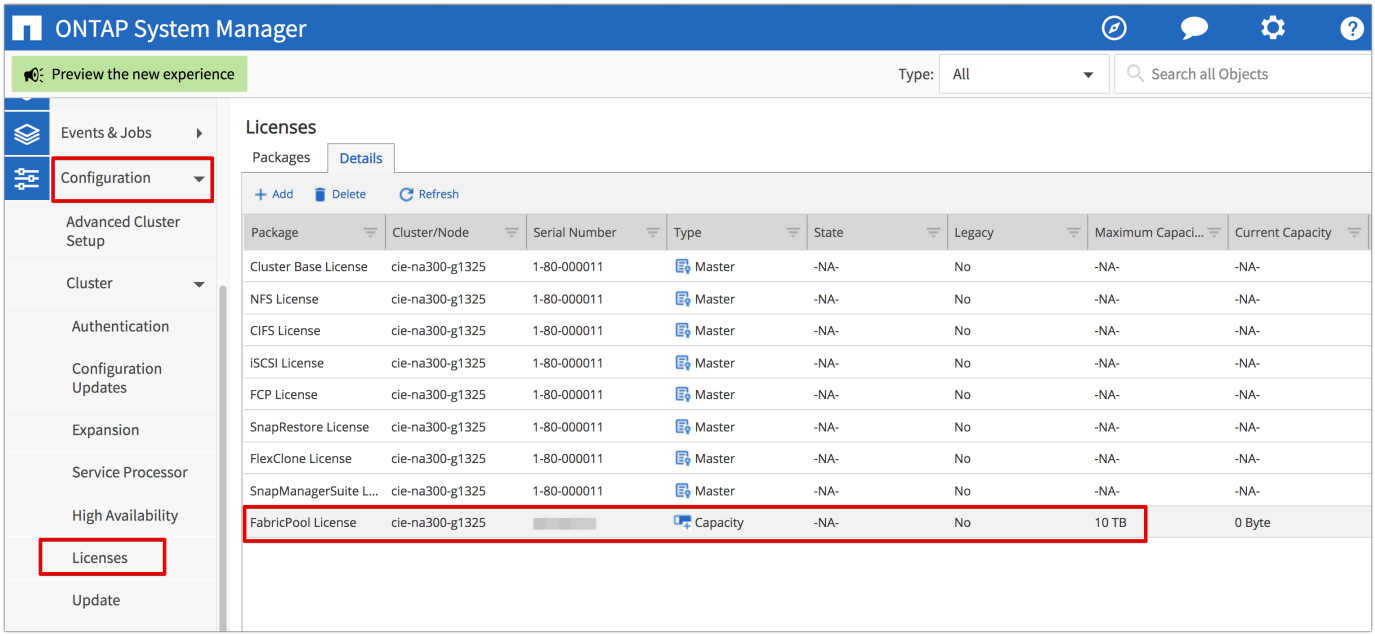
Capacità di licenza

È possibile visualizzare la capacità della licenza utilizzando l'interfaccia utente di ONTAP o Gestione di sistema di OnCommand. Per visualizzare la capacità concessa in licenza, eseguire il seguente comando nell'interfaccia utente di ONTAP:

```
system license show-status
```

In Gestore di sistema di OnCommand, attenersi alla seguente procedura:

1. Fare clic su configurazioni.
2. Fare clic su licenze.
3. Fare clic sulla scheda Dettagli.



La capacità massima e la capacità corrente sono elencate nella riga licenza FabricPool.

"Creare il bucket AWS S3."

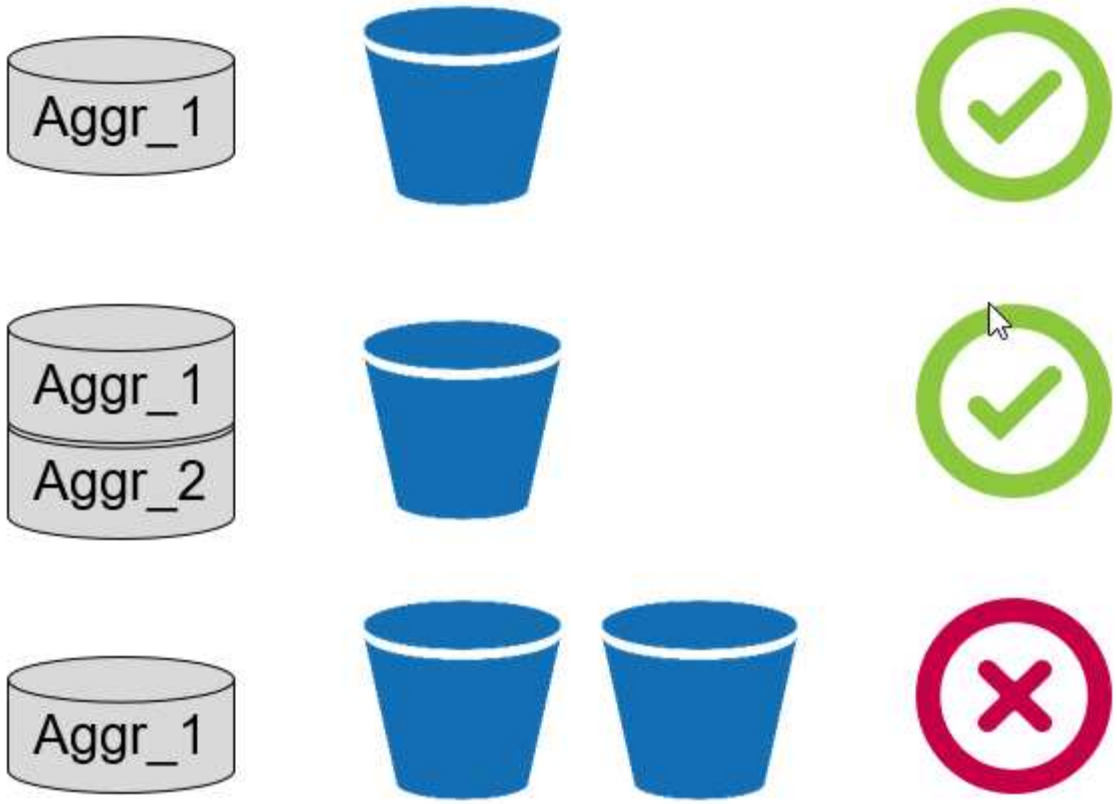
Creare il bucket AWS S3

I bucket sono contenitori di archivi di oggetti che contengono dati. È necessario fornire il nome e la posizione del bucket in cui i dati vengono memorizzati prima di poter essere aggiunti a un aggregato come Tier cloud.

I bucket non possono essere creati utilizzando Gestione di sistema di OnCommand, Gestore unificato di OnCommand o ONTAP.

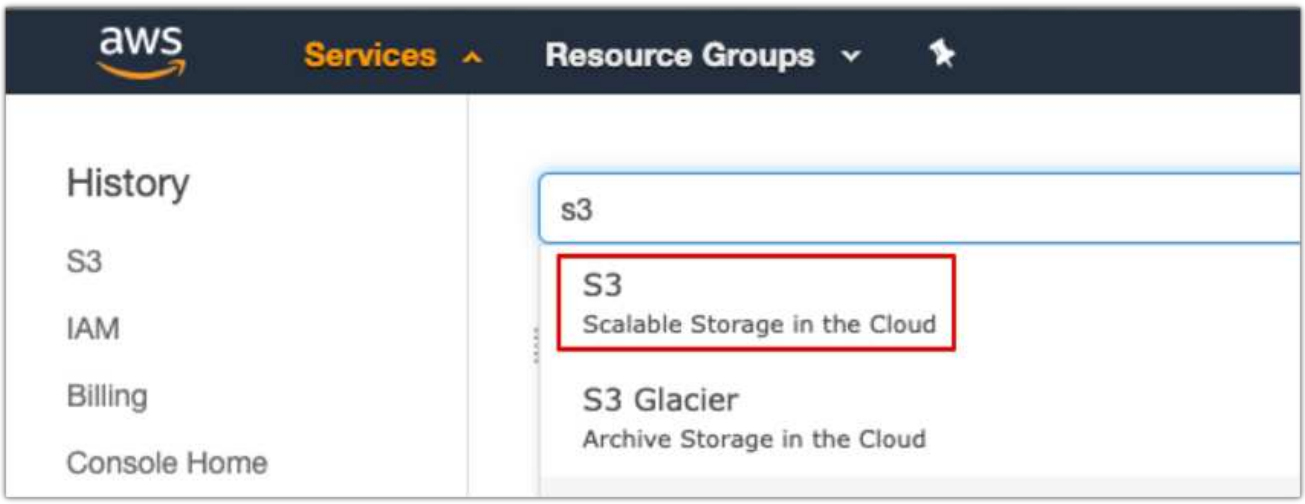
FabricPool supporta l'attacco di un bucket per aggregato, come illustrato nella figura seguente. Un singolo bucket può essere collegato a un singolo aggregato e un singolo bucket può essere collegato a più aggregati. Tuttavia, un singolo aggregato non può essere collegato a più bucket. Sebbene sia possibile collegare un singolo bucket a più aggregati in un cluster, NetApp sconsiglia di collegare un singolo bucket ad aggregati in più cluster.

Quando si pianifica un'architettura di storage, considerare come la relazione bucket-to-aggregate potrebbe influire sulle performance. Molti provider di archivi di oggetti impostano un numero massimo di IOPS supportati a livello di bucket o container. Gli ambienti che richiedono le massime performance devono utilizzare più bucket per ridurre la possibilità che le limitazioni IOPS dello storage a oggetti possano influire sulle performance di più aggregati FabricPool. Collegare un singolo bucket o container a tutti gli aggregati FabricPool in un cluster potrebbe essere più vantaggioso per gli ambienti che apprezzano la gestibilità rispetto alle performance di livello cloud.

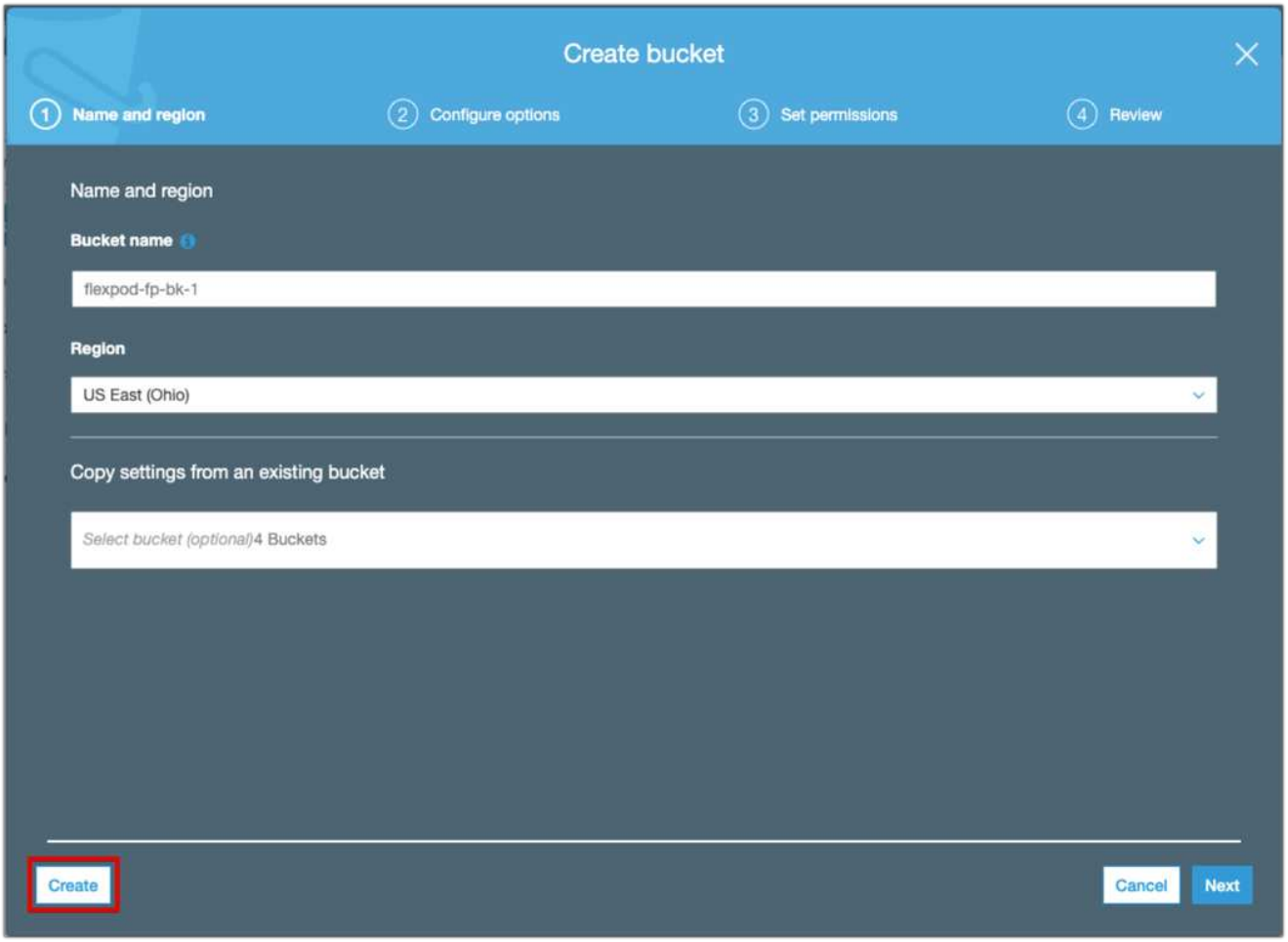


Creare un bucket S3

1. Nella console di gestione AWS dalla home page, immettere S3 nella barra di ricerca.
2. Seleziona lo storage scalabile S3 nel cloud.



3. Nella home page di S3, selezionare Create Bucket (Crea bucket).
4. Immettere un nome conforme al DNS e scegliere la regione in cui creare il bucket.



5. Fare clic su Create (Crea) per creare il bucket dell'archivio di oggetti.

"Avanti: Aggiungi un Tier cloud a ONTAP"

Aggiungi un Tier cloud a ONTAP

Prima di poter collegare un archivio di oggetti a un aggregato, è necessario aggiungerlo e identificarlo da ONTAP. Questa attività può essere completata con Gestore di sistema di OnCommand o l'interfaccia utente di ONTAP.

FabricPool supporta Amazon S3, storage cloud a oggetti IBM e archivi di oggetti storage blob Microsoft Azure come Tier cloud.

Sono necessarie le seguenti informazioni:

- Nome del server (FQDN); ad esempio, `s3.amazonaws.com`
- ID chiave di accesso
- Chiave segreta
- Nome del container (nome del bucket)

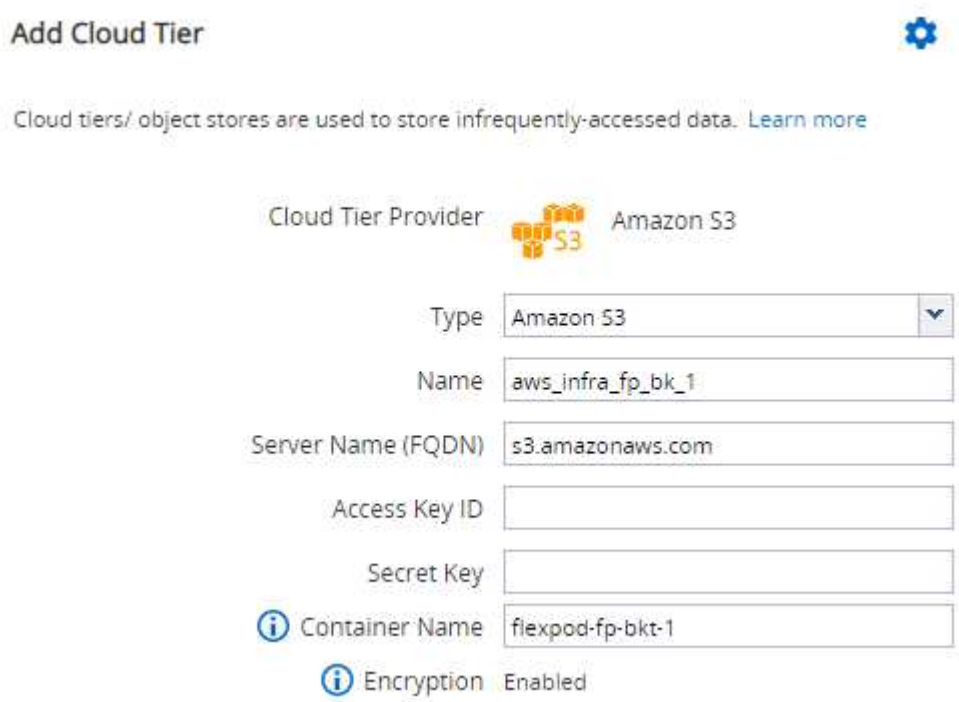
Gestore di sistema di OnCommand

Per aggiungere un livello cloud con Gestione di sistema OnCommand, attenersi alla seguente procedura:

1. Avviare Gestore di sistema di OnCommand.
2. Fare clic su Storage (archiviazione)
3. Fare clic su aggregati e dischi.
4. Fare clic su livelli cloud.
5. Selezionare un provider di archivi di oggetti.
6. Completare i campi di testo richiesti per il provider dell'archivio di oggetti.

   Nel campo Container Name (Nome contenitore), immettere il nome del bucket o del container dell'archivio di oggetti.

7. Fare clic su Save and Allega aggregati.



CLI ONTAP

Per aggiungere un livello cloud con l'interfaccia utente di ONTAP, immettere i seguenti comandi:

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Successivo: Collega un Tier cloud a un aggregato ONTAP."

Collegare un Tier cloud a un aggregato ONTAP

Una volta aggiunto e identificato da ONTAP, un archivio di oggetti deve essere collegato a un aggregato per creare un FabricPool. Questa attività può essere completata utilizzando Gestore di sistema di OnCommand o l'interfaccia utente di ONTAP.

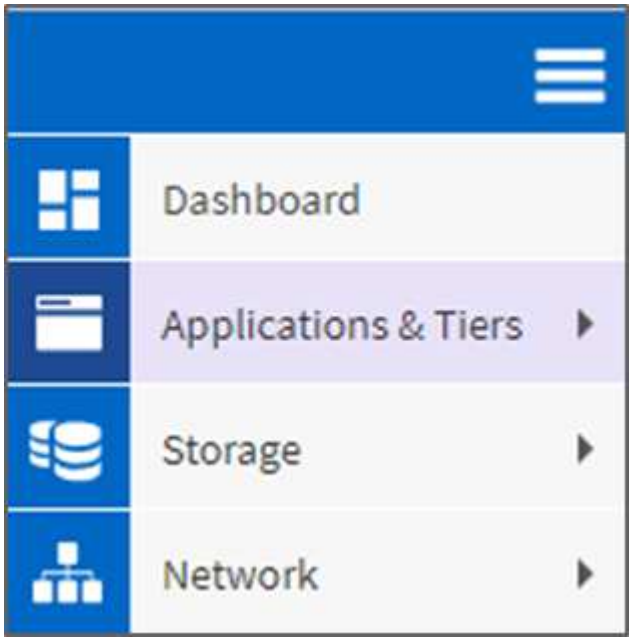
È possibile collegare più di un tipo di archivio di oggetti a un cluster, ma è possibile collegare un solo tipo di archivio di oggetti a ciascun aggregato. Ad esempio, un aggregato può utilizzare Google Cloud e un altro aggregato può utilizzare Amazon S3, ma un aggregato non può essere associato a entrambi.

Collegare un Tier cloud a un aggregato è un'azione permanente. Un Tier cloud non può essere disconnesso da un aggregato a cui è stato collegato.

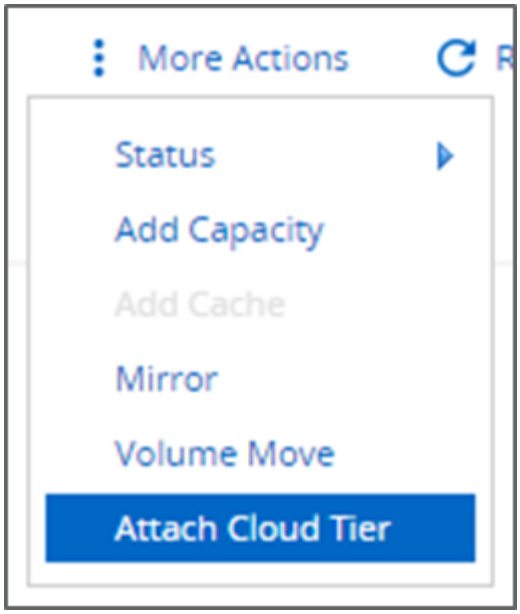
Gestore di sistema di OnCommand

Per associare un Tier cloud a un aggregato utilizzando Gestione di sistema di OnCommand, completare i seguenti passaggi:

1. Avviare Gestore di sistema di OnCommand.
2. Fare clic su applicazioni e livelli.



3. Fare clic su Storage Tier.
4. Fare clic su un aggregato.
5. Fare clic su azioni e selezionare Allega Tier cloud.



6. Seleziona un livello cloud.
7. Visualizzare e aggiornare i criteri di tiering per i volumi sull'aggregato (facoltativo). Per impostazione predefinita, il criterio di tiering del volume è impostato su Snapshot-Only (solo snapshot).
8. Fare clic su Salva.

CLI ONTAP

Per collegare un Tier cloud a un aggregato utilizzando l'interfaccia utente di ONTAP, eseguire i seguenti comandi:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Esempio:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Successivo: Impostare la policy di tiering dei volumi."

Impostare la policy di tiering dei volumi

Per impostazione predefinita, i volumi utilizzano il criterio None volume Tiering. Dopo la creazione del volume, è possibile modificare il criterio di tiering del volume utilizzando Gestione di sistema di OnCommand o l'interfaccia utente di ONTAP.

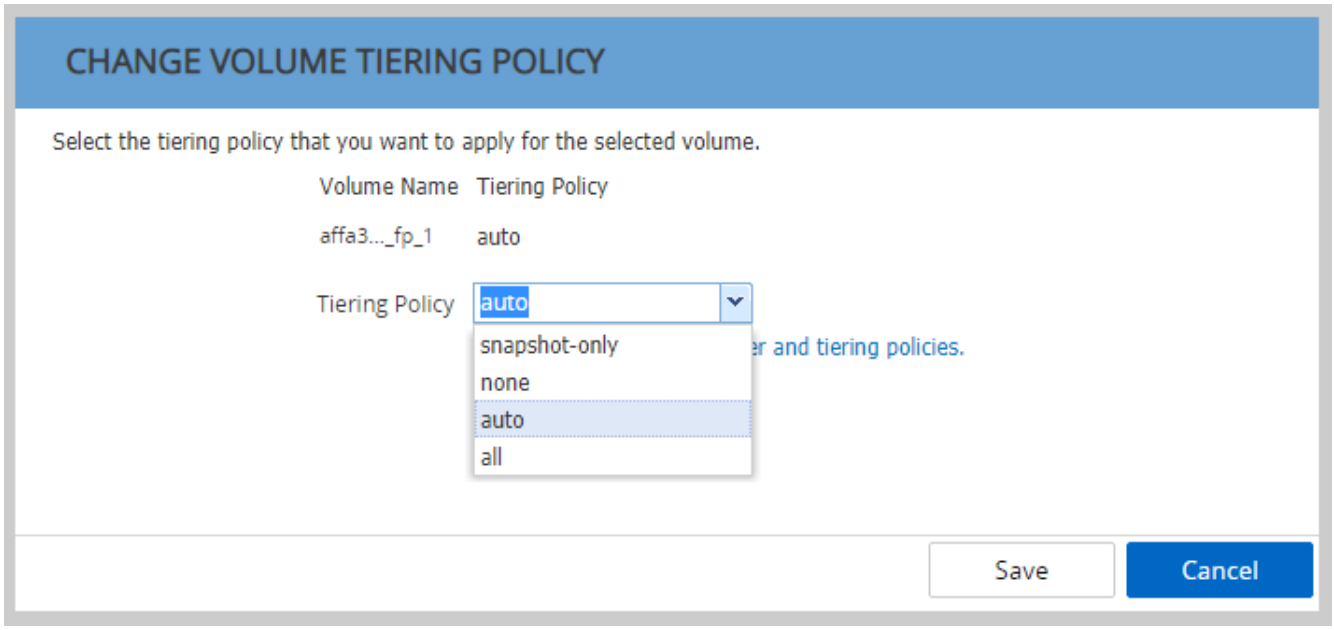
Se utilizzato con FlexPod, FabricPool offre tre criteri di tiering dei volumi, automatico, solo snapshot e Nessuno.

- **Auto**
  - Tutti i cold block nel volume vengono spostati nel Tier cloud. Supponendo che l'aggregato sia utilizzato oltre il 50%, occorrono circa 31 giorni affinché i blocchi inattivi diventino freddi. Il periodo di raffreddamento automatico può essere regolato tra 2 giorni e 63 giorni utilizzando `tiering-minimum-cooling-days` impostazione.
  - Quando i cold block in un volume con una policy di tiering impostata su Auto vengono letti in modo casuale, vengono resi hot e scritti nel Tier di performance.
  - Quando i blocchi freddi in un volume con una policy di tiering impostata su Auto vengono letti in sequenza, rimangono freddi e rimangono sul livello cloud. Non sono scritti nel Tier di performance.
- **Solo Snapshot**
  - I blocchi Cold Snapshot nel volume non condivisi con il file system attivo vengono spostati nel Tier cloud. Supponendo che l'aggregato sia utilizzato oltre il 50%, sono necessari circa 2 giorni affinché i blocchi snapshot inattivi diventino freddi. Il periodo di raffreddamento solo Snapshot può essere regolato da 2 a 63 giorni utilizzando `tiering-minimum-cooling-days` impostazione.
  - Quando i blocchi a freddo in un volume con una policy di tiering impostata su Snapshot-only vengono letti, vengono resi a caldo e scritti nel Tier di performance.
- **Nessuno (impostazione predefinita)**
  - I volumi impostati per l'utilizzo di None come policy di tiering non suddividono i dati cold nel Tier cloud.
  - L'impostazione del criterio di tiering su None impedisce il nuovo tiering.
  - I dati del volume precedentemente spostati nel Tier cloud rimangono nel Tier cloud fino a quando non diventano caldi e vengono automaticamente spostati di nuovo nel Tier di performance.

Gestore di sistema di OnCommand

Per modificare la policy di tiering di un volume utilizzando Gestione di sistema di OnCommand, attenersi alla seguente procedura:

1. Avviare Gestore di sistema di OnCommand.
2. Selezionare un volume.
3. Fare clic su altre azioni e selezionare Cambia policy di tiering.
4. Selezionare il criterio di tiering da applicare al volume.
5. Fare clic su Salva.



CLI ONTAP

Per modificare il criterio di tiering di un volume utilizzando l'interfaccia utente di ONTAP, eseguire il seguente comando:

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Successivo: Impostare i giorni minimi di raffreddamento per il tiering del volume."

Impostare i giorni minimi di raffreddamento per il tiering del volume

Il `tiering-minimum-cooling-days` L'impostazione determina il numero di giorni che devono trascorrere prima che i dati inattivi in un volume utilizzando il criterio Auto o Snapshot-Only siano considerati freddi e idonei per il tiering.

Automatico

L'impostazione predefinita `tiering-minimum-cooling-days` L'impostazione per il criterio di tiering automatico è 31 giorni.

Poiché le letture mantengono calde le temperature dei blocchi, l'aumento di questo valore potrebbe ridurre la quantità di dati che possono essere suddivisi in livelli e aumentare la quantità di dati conservati nel Tier di performance.

Se si desidera ridurre questo valore dai 31 giorni predefiniti, tenere presente che i dati non devono più essere attivi prima di essere contrassegnati come cold. Ad esempio, se si prevede che un carico di lavoro di più giorni esegua un numero significativo di scritture il giorno 7, il volume `tiering-minimum-cooling-days` l'impostazione non deve essere inferiore a 8 giorni.

Lo storage a oggetti non è transazionale come lo storage a file o a blocchi. Apportare modifiche ai file memorizzati come oggetti nei volumi con giorni di raffreddamento minimi eccessivamente aggressivi può causare la creazione di nuovi oggetti, la frammentazione degli oggetti esistenti e l'aggiunta di inefficienze dello storage.

Solo Snapshot

L'impostazione predefinita `tiering-minimum-cooling-days` L'impostazione per la policy di tiering Snapshot-Only è di 2 giorni. Un minimo di 2 giorni offre un tempo aggiuntivo per i processi in background per fornire la massima efficienza dello storage e impedisce ai processi di protezione dei dati quotidiani di dover leggere i dati dal Tier cloud.

CLI ONTAP

Per modificare un volume `tiering-minimum-cooling-days` Impostando utilizzando l'interfaccia utente di ONTAP, eseguire il seguente comando:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

È necessario il livello di privilegio avanzato.

La modifica della policy di tiering tra Auto e Snapshot-Only (o viceversa) ripristina il periodo di inattività dei blocchi sul Tier di performance. Ad esempio, un volume che utilizza il criterio di tiering automatico del volume con i dati sul Tier di performance inattivi per 20 giorni avrà l'inattività dei dati del Tier di performance reimpostata su 0 giorni se il criterio di tiering è impostato su Snapshot-Only.

Considerazioni sulle performance

Dimensionare il Tier di performance

Quando si prende in considerazione il dimensionamento, tenere presente che il Tier di performance deve essere in grado di svolgere le seguenti attività:

- Supporto dei dati hot
- Supporto dei dati cold fino a quando la scansione di tiering non sposta i dati nel Tier cloud
- Supporto dei dati del Tier cloud che diventano "hot" e vengono riscritti nel Tier di performance
- Supporto dei metadati WAFL associati al Tier cloud allegato

Per la maggior parte degli ambienti, un rapporto performance-capacità 1:10 sugli aggregati FabricPool è estremamente conservativo, fornendo al contempo risparmi significativi sullo storage. Ad esempio, se l'intento è quello di tierare 200 TB al livello cloud, l'aggregato del Tier di performance dovrebbe essere di almeno 20 TB.

Le scritture dal Tier cloud al Tier performance sono disattivate se la capacità del Tier performance è superiore al 70%. In questo caso, i blocchi vengono letti direttamente dal livello cloud.

Dimensionare il Tier cloud

Quando si considera il dimensionamento, l'archivio di oggetti che agisce come Tier cloud deve essere in grado di svolgere le seguenti attività:

- Supporto delle letture dei dati cold esistenti
- Supporto delle scritture di nuovi dati cold
- Supporto dell'eliminazione e della deframmentazione degli oggetti

Costo di proprietà

Il "Calcolatore economico di FabricPool" È disponibile attraverso la società di analisi IT indipendente Evaluator Group per contribuire a proiettare i risparmi sui costi tra on-premise e cloud per lo storage dei dati cold. Il calcolatore fornisce un'interfaccia semplice per determinare il costo di archiviazione dei dati con accesso non frequente su un Tier di performance rispetto all'invio a un Tier cloud per il resto del ciclo di vita dei dati. In base a un calcolo di 5 anni, i quattro fattori chiave (capacità di origine, crescita dei dati, capacità di snapshot e percentuale di dati cold) vengono utilizzati per determinare i costi di storage nel periodo di tempo.

Conclusione

Il percorso verso il cloud varia tra le organizzazioni, tra le business unit e persino tra le business unit all'interno delle organizzazioni. Alcuni scelgono un'adozione rapida, mentre altri adottano un approccio più conservativo. FabricPool si inserisce nella strategia cloud delle organizzazioni indipendentemente dalle loro dimensioni e dalla loro velocità di adozione del cloud, dimostrando ulteriormente i vantaggi in termini di efficienza e scalabilità di un'infrastruttura FlexPod.

Dove trovare ulteriori informazioni

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

- Best practice FabricPool

  "www.netapp.com/us/media/tr-4598.pdf"

- Documentazione sui prodotti NetApp

  "https://docs.netapp.com"

- TR-4036: Specifiche tecniche del data center FlexPod

  "https://www.netapp.com/us/media/tr-4036.pdf"

Data center FlexPod per cloud ibrido con Cisco CloudCenter e storage privato NetApp - progettazione

Haseeb Niazi, Cisco David Arnette, NetApp

Cisco Validated Designs (CVD) offre sistemi e soluzioni progettati, testati e documentati per facilitare e migliorare le implementazioni dei clienti. Questi design incorporano un'ampia gamma di tecnologie e prodotti in un portfolio di soluzioni sviluppate per soddisfare le esigenze di business dei clienti e per guidarli dalla progettazione all'implementazione.

"Data center FlexPod per cloud ibrido con Cisco CloudCenter e storage privato NetApp - progettazione"

Informazioni sul copyright

Informazioni sul marchio commerciale