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

FlexPod

NetApp
October 30, 2025

This PDF was generated from https://docs.netapp.com/it-it/flexpod/hybrid-cloud/flexpod-rho-cvo-solution-overview.html on October 30, 2025. Always check docs.netapp.com for the latest.

Sommario

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.

[Errore: Immagine grafica mancante]

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.

[Errore: Immagine grafica mancante]

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

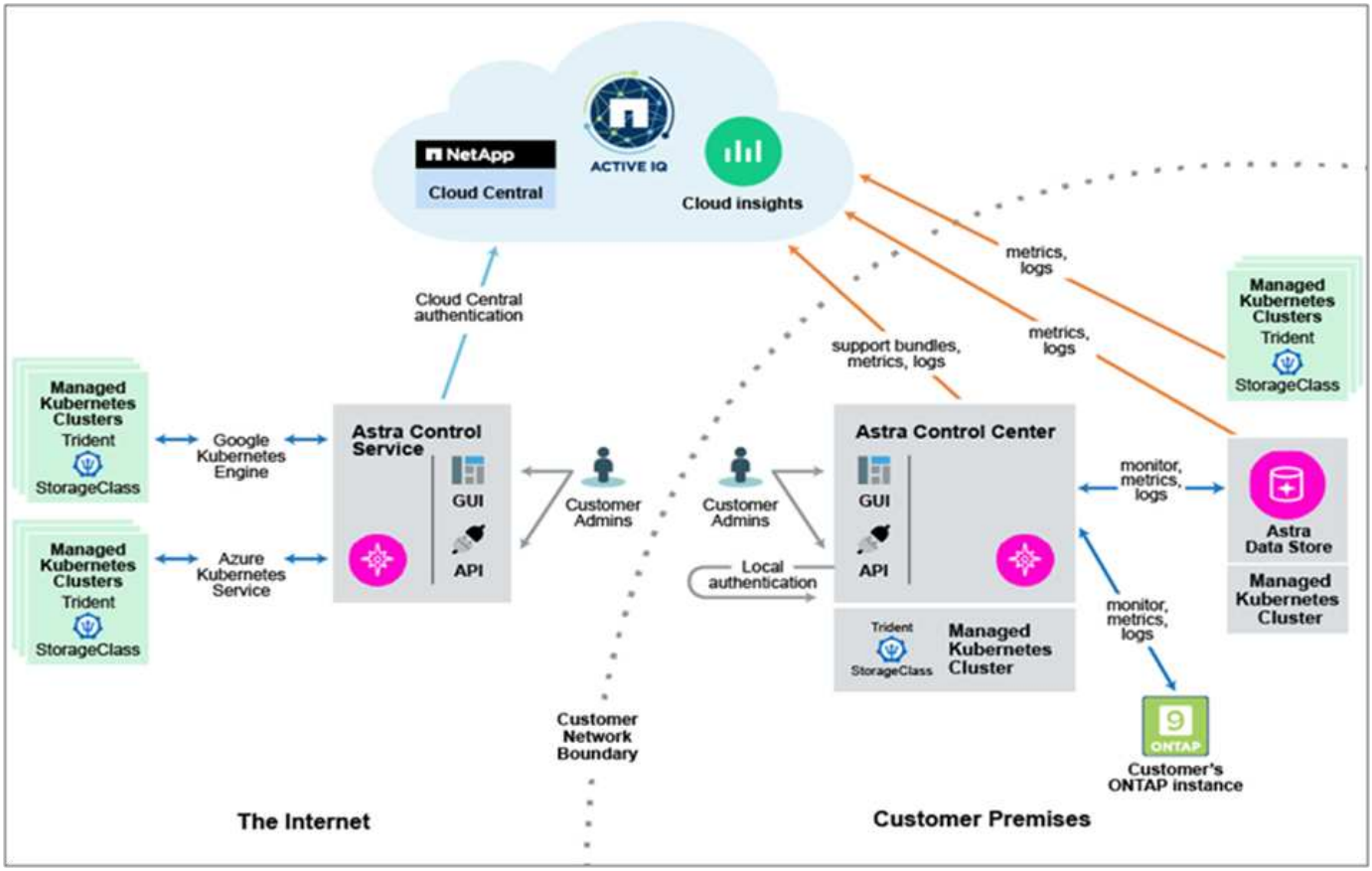
Astra Control è disponibile in due modelli di consumo:

- **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:

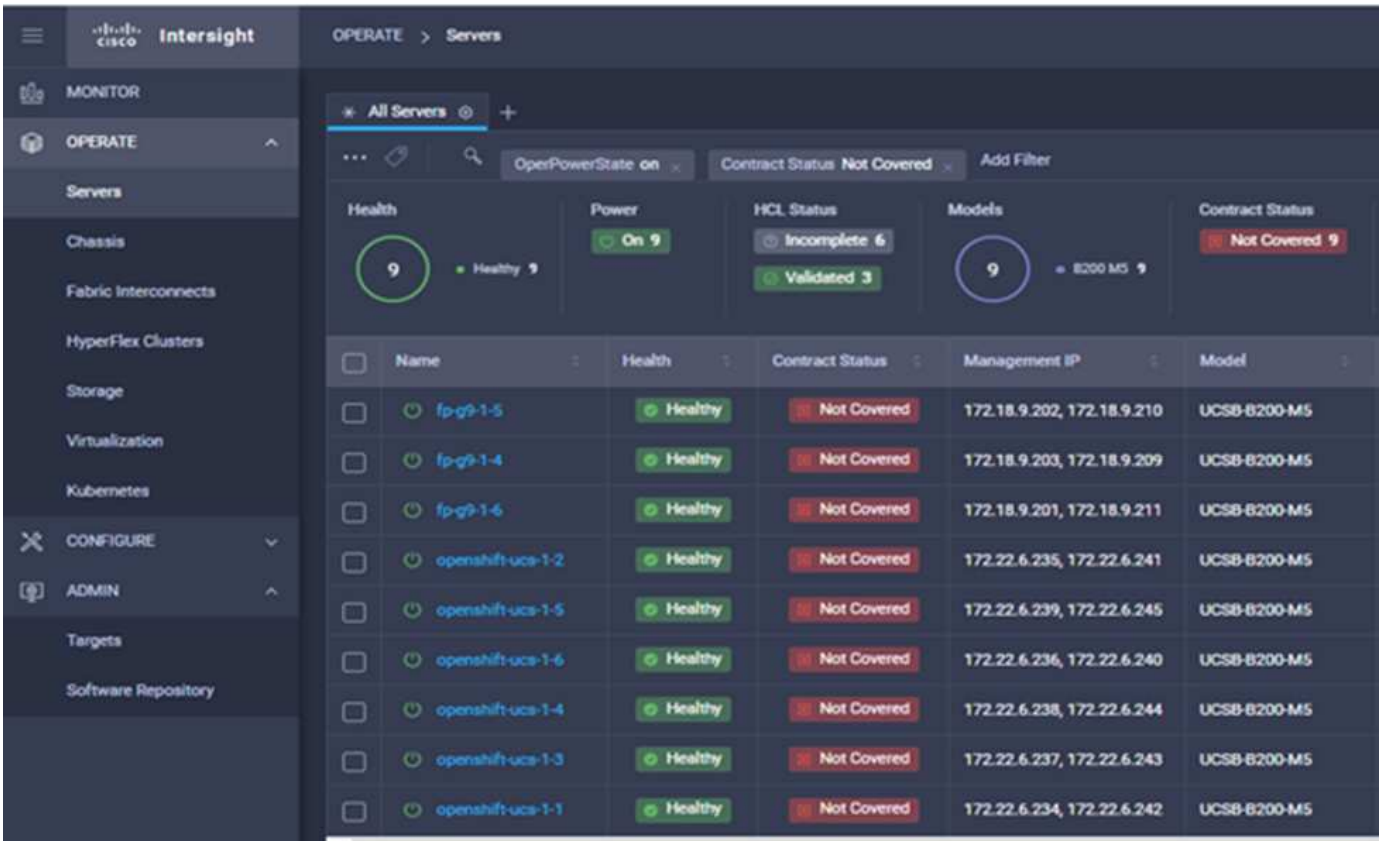
- **Delivery più rapida.** offerta come servizio dal cloud o nel data center del cliente con frequenti aggiornamenti e innovazione continua, grazie a un modello di sviluppo software agile. In questo modo, il cliente può semplicemente concentrarsi sull'accelerazione della consegna per la linea di business.
- **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.

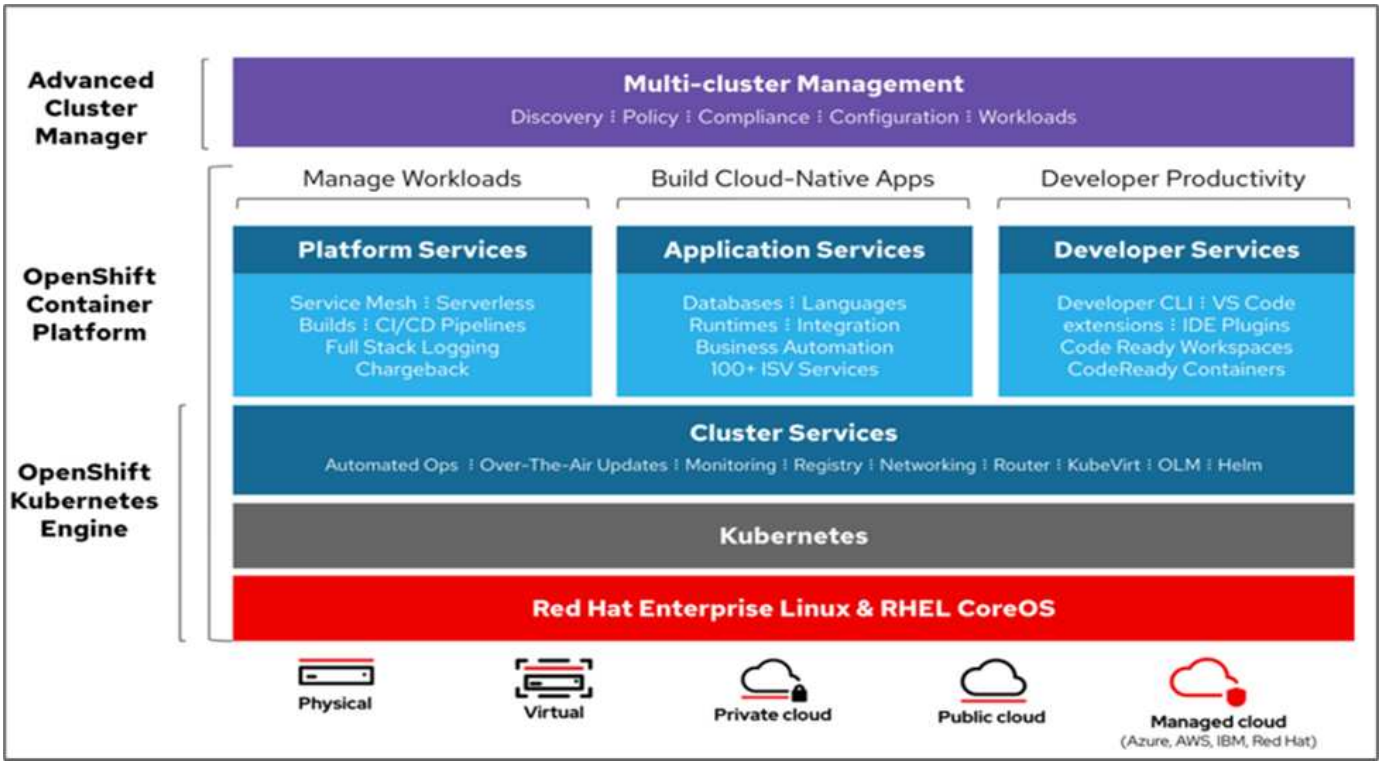


Red Hat OpenShift Container Platform

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."

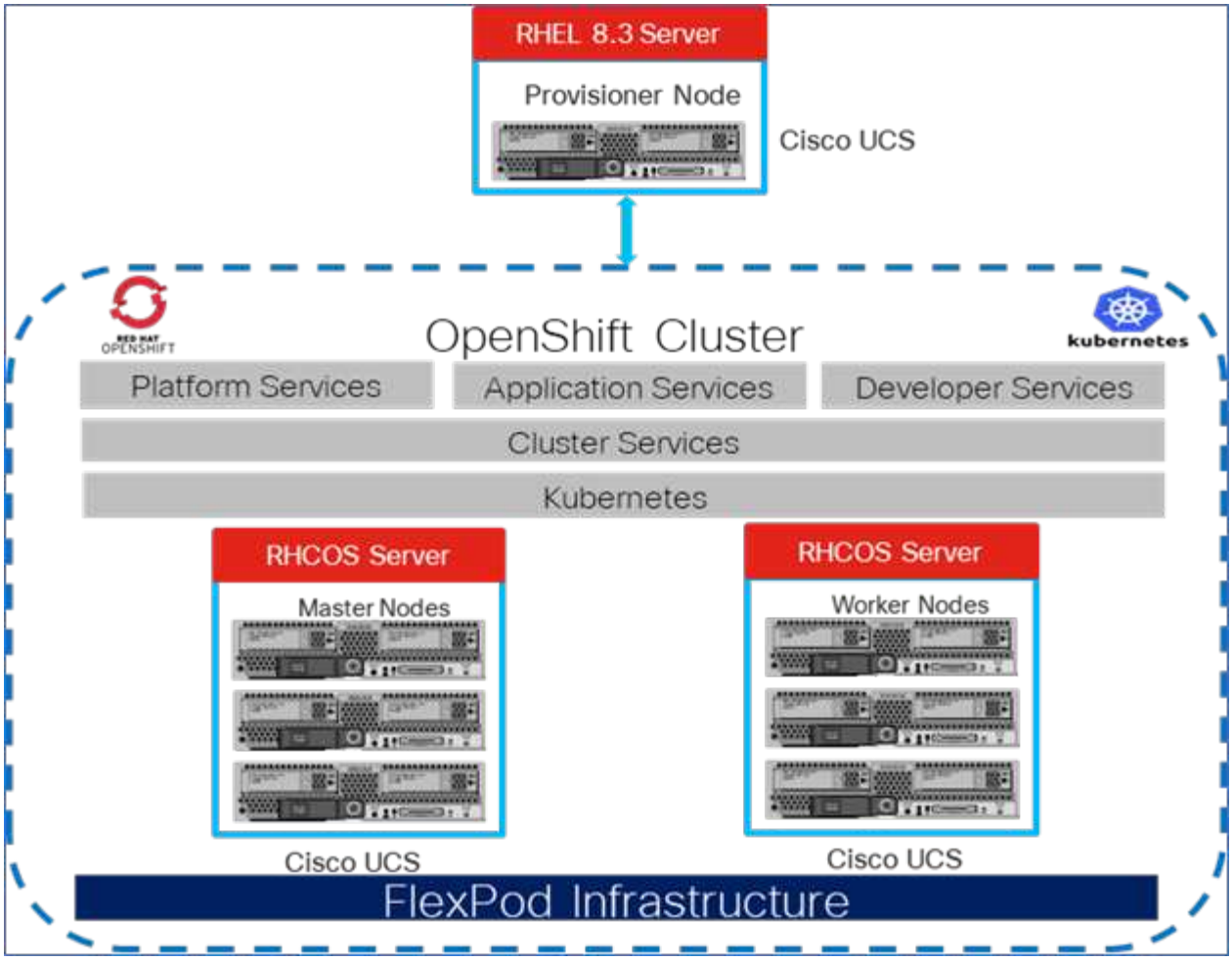
Installazione e configurazione

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.

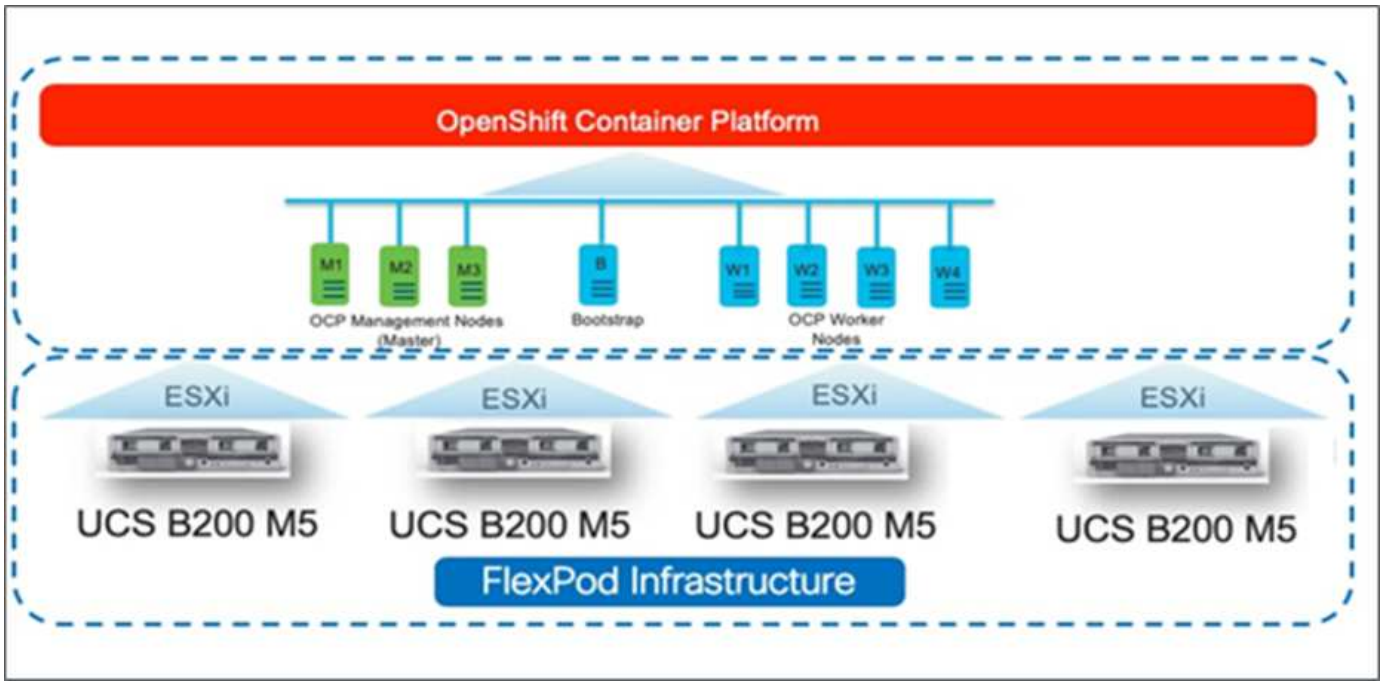
La figura seguente illustra la piattaforma container OpenShift 4 Bare Metal su FlexPod.



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.

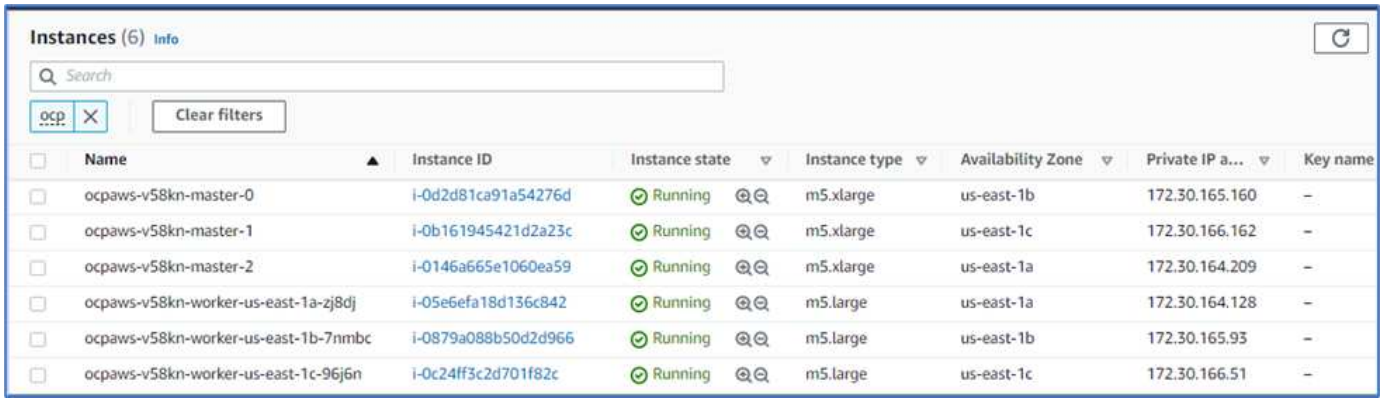


"Avanti: Red Hat OpenShift su AWS."

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.



```
[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.

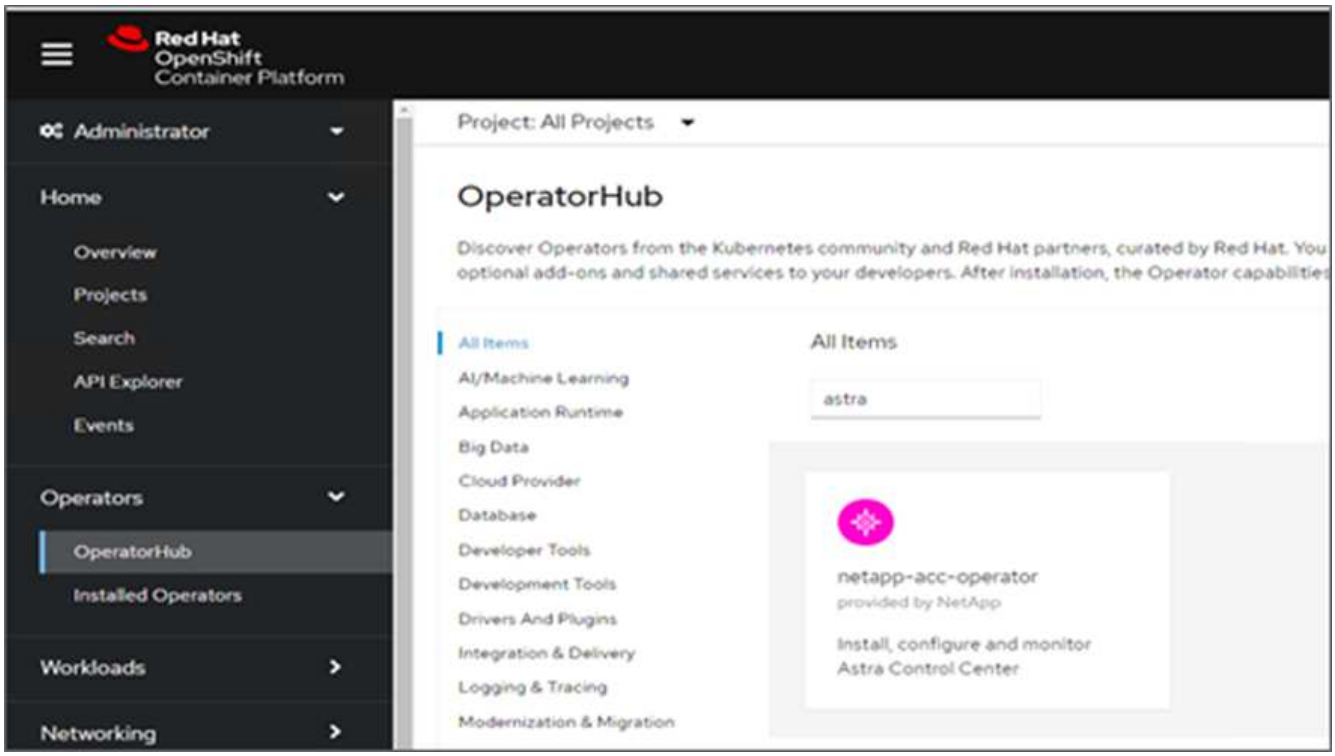
   Per Docker:

```
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:

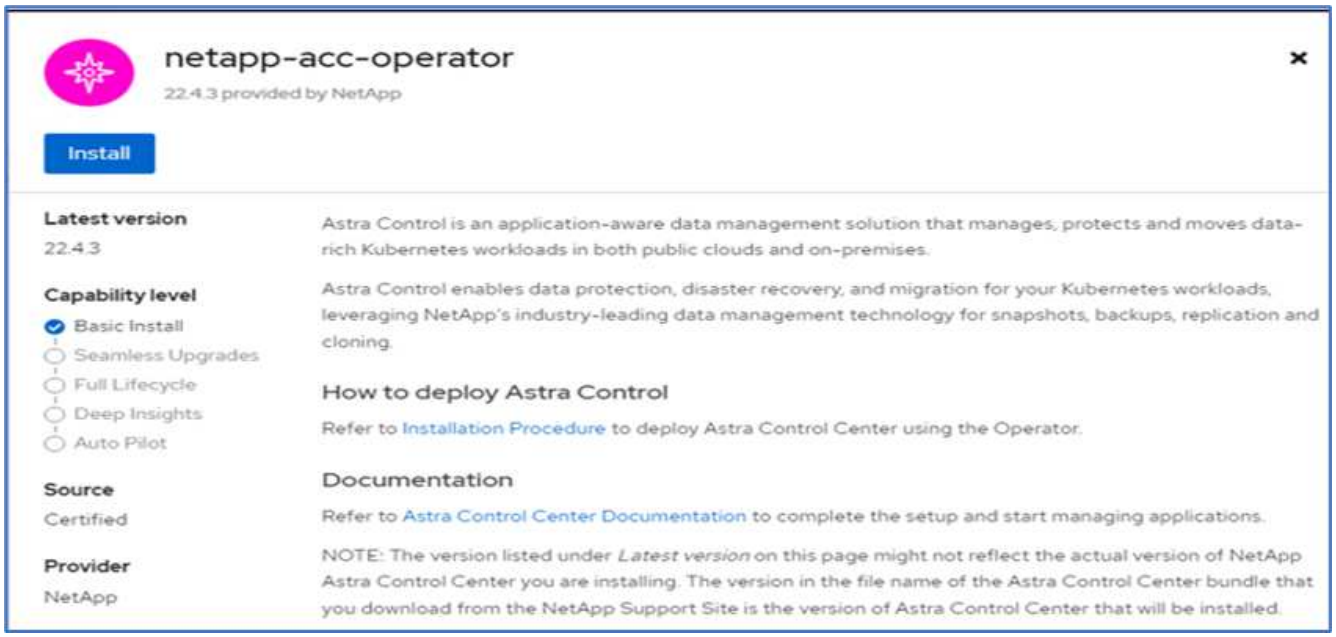
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed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

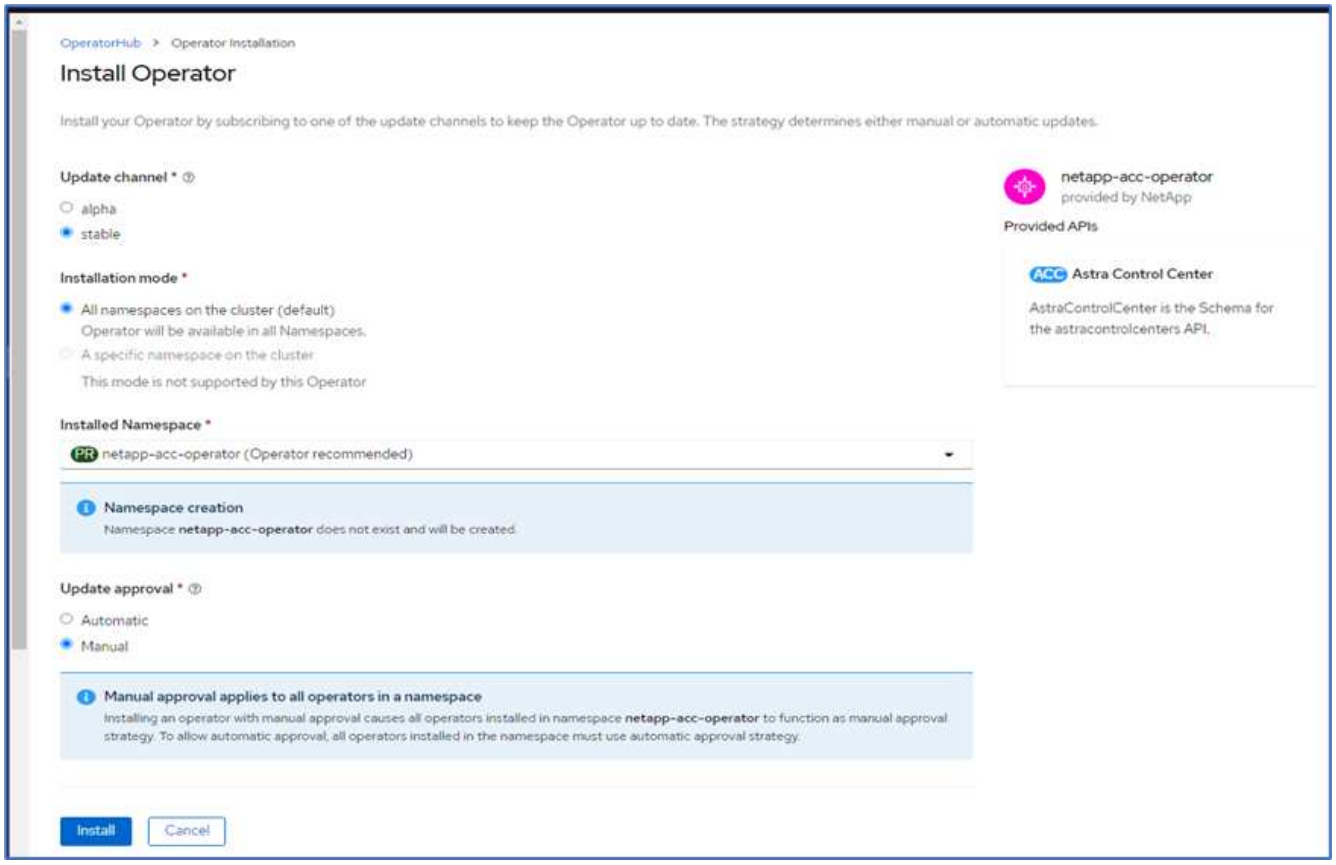


> `netapp-acc-operator` È un operatore Red Hat OpenShift certificato ed è elencato nel catalogo OperatorHub.

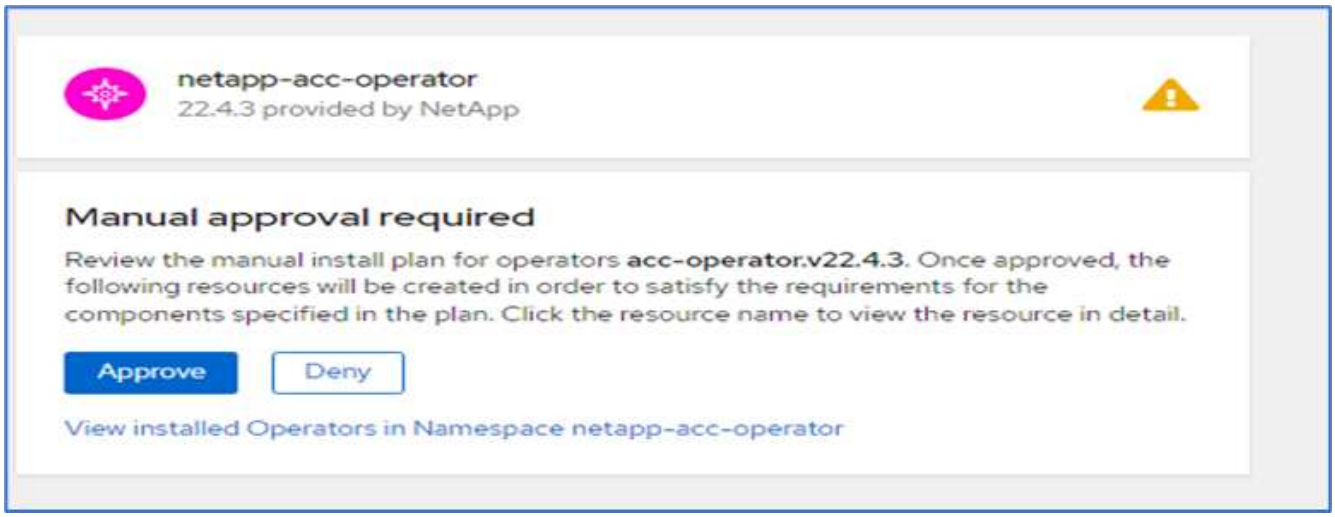
9. Selezionare `netapp-acc-operator` E fare clic su Installa.



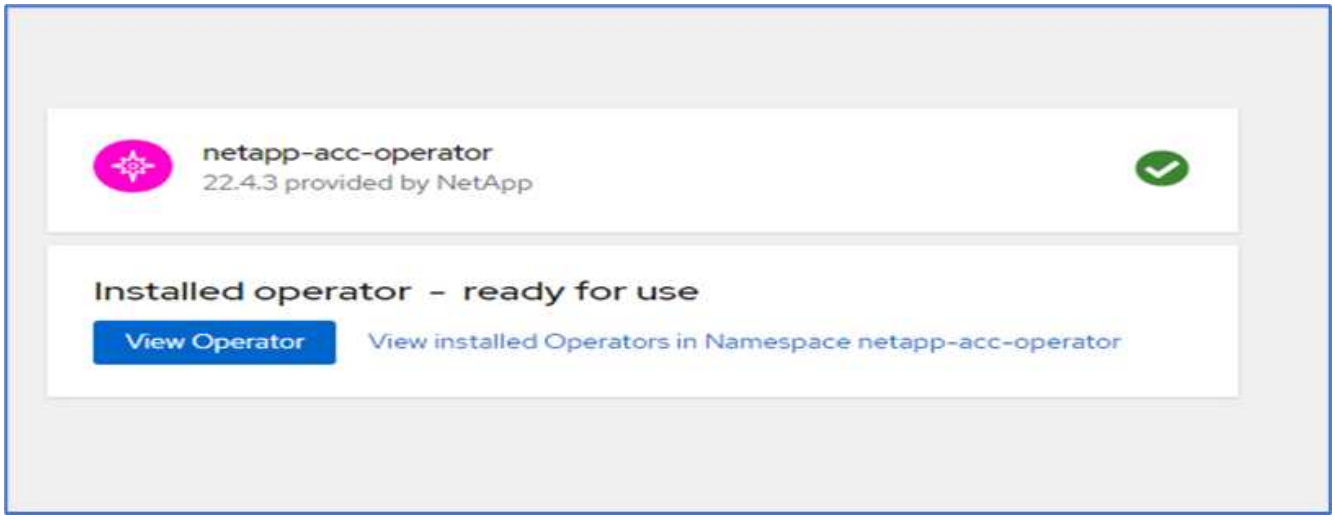
10. Selezionare le opzioni appropriate e fare clic su Install (Installa).



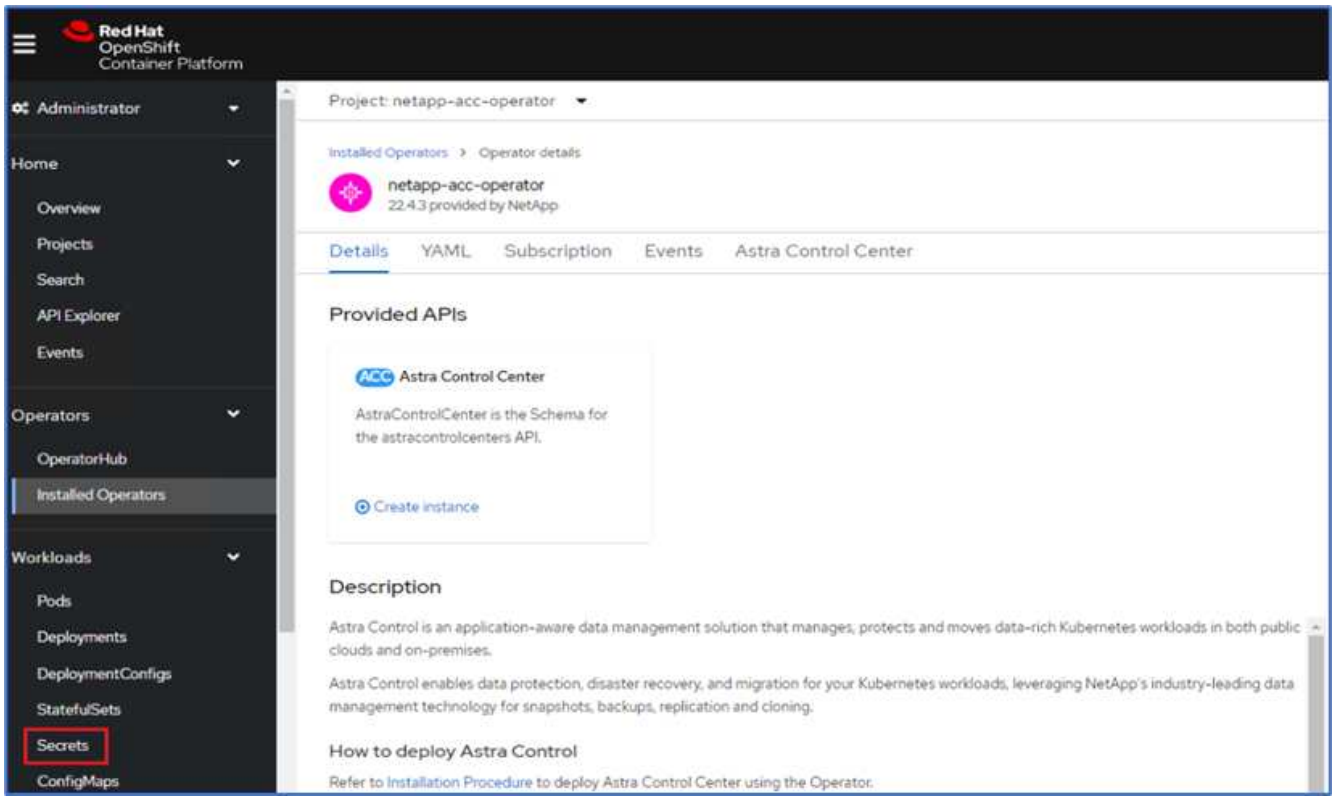
11. Approvare l'installazione e attendere l'installazione dell'operatore.



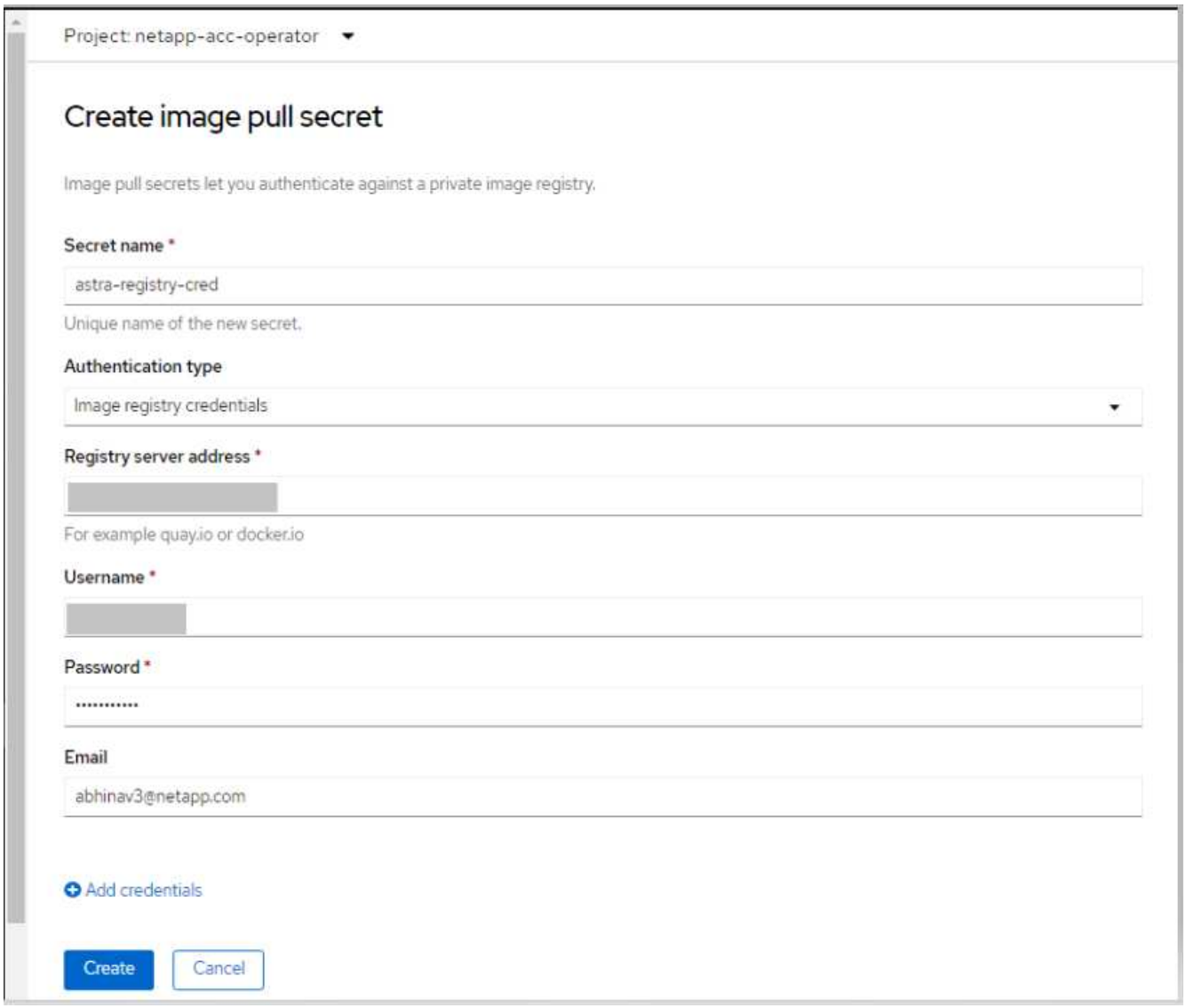
12. A questo punto, l'operatore viene installato correttamente e pronto per l'uso. Fare clic su View Operator (Visualizza operatore) per avviare l'installazione di Astra Control Center.



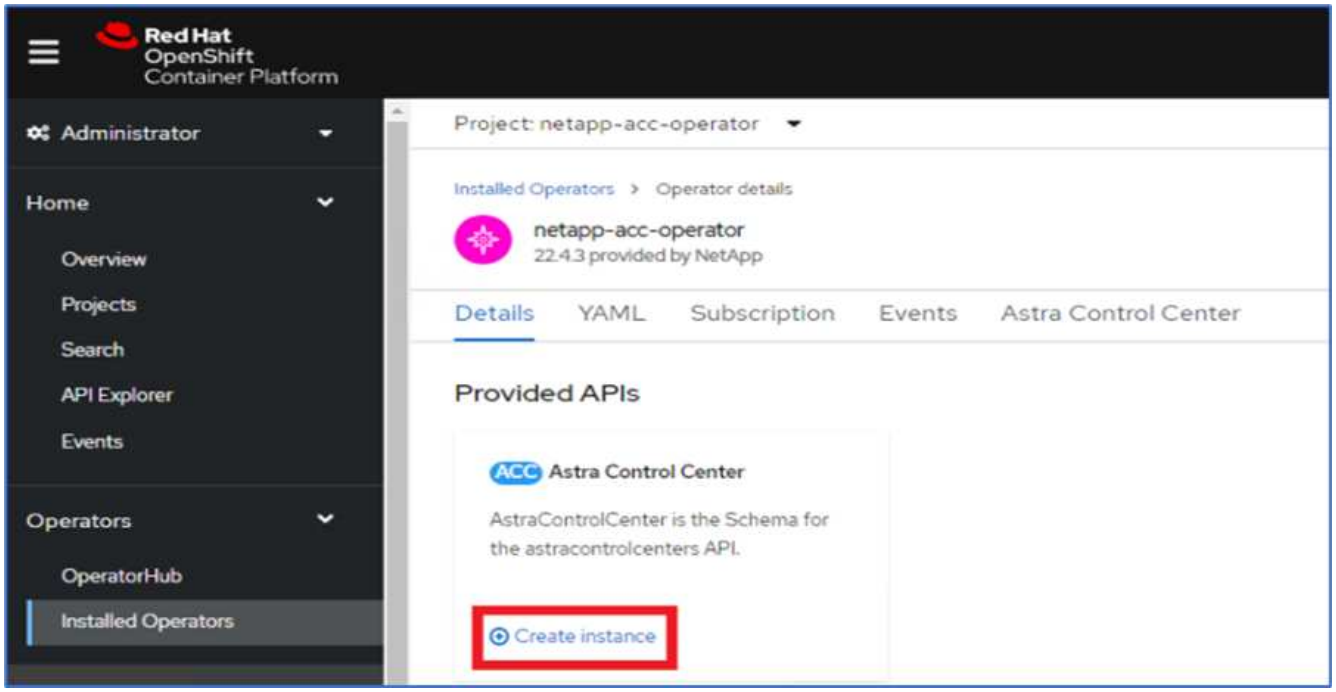
13. Prima di installare Astra Control Center, creare il segreto pull per scaricare le immagini Astra dal registro Docker precedentemente inserito.



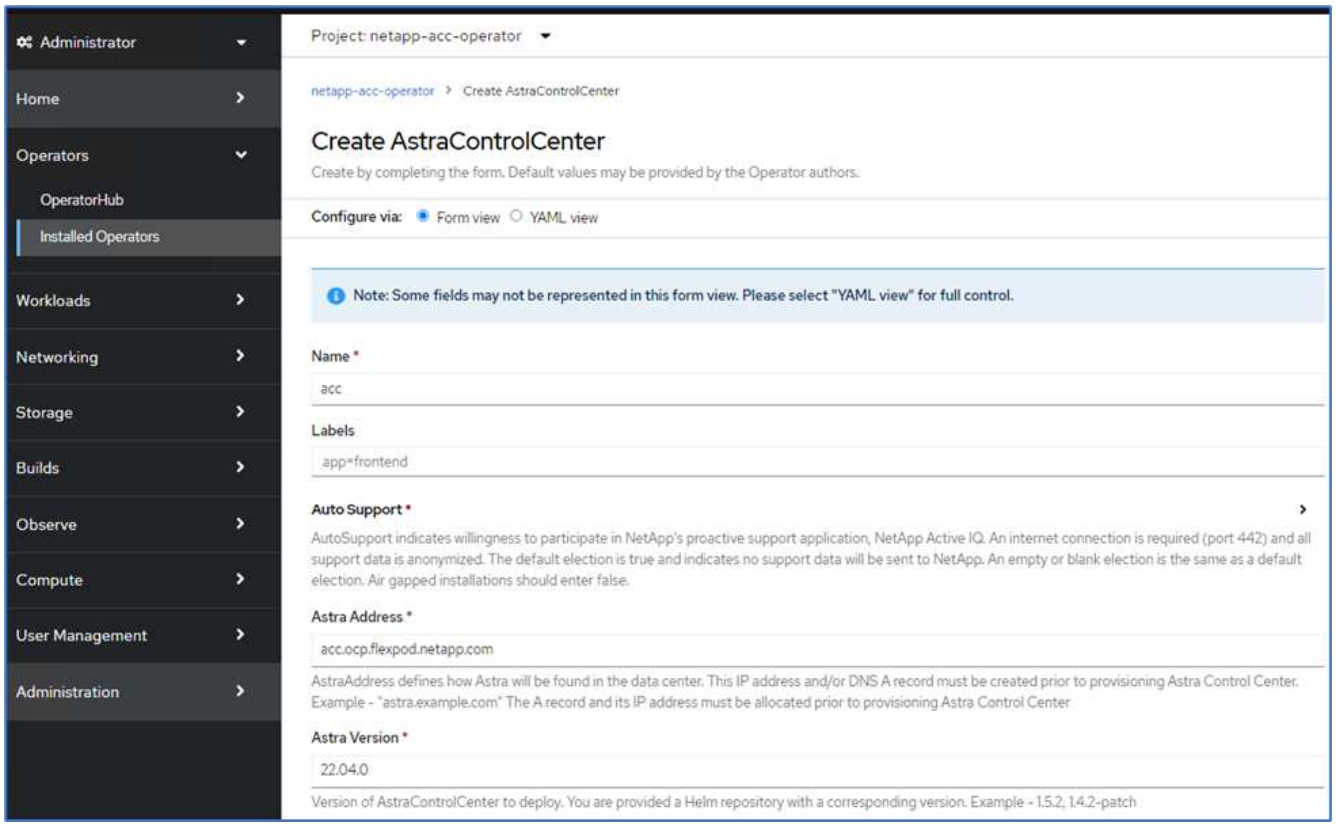
14. Per estrarre le immagini di Astra Control Center dal tuo repo privato Docker, crea un segreto in `netapp-acc-operator` namespace. Questo nome segreto viene fornito nel manifesto YAML di Astra Control Center in un passaggio successivo.



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



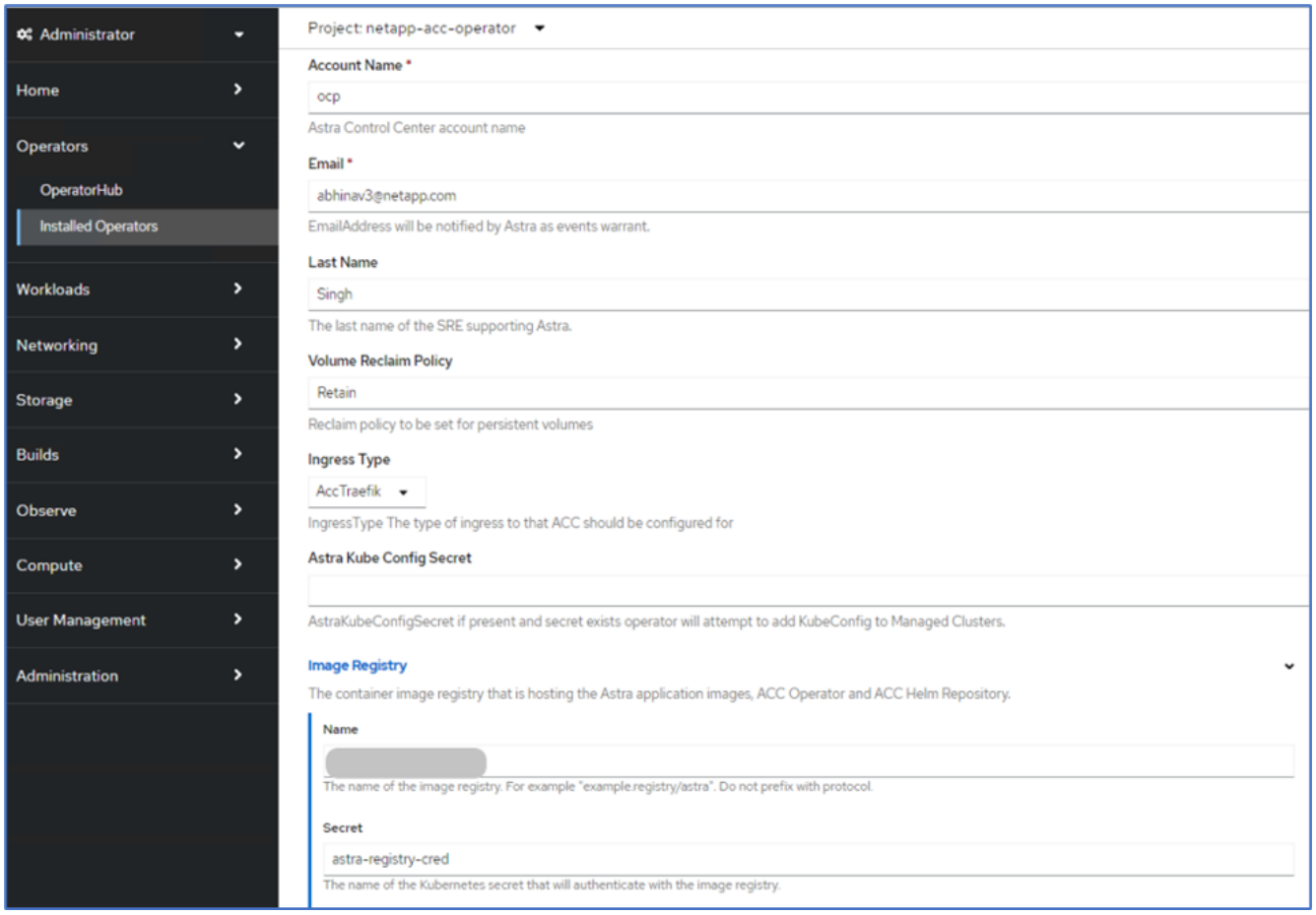
16. Completare il modulo Create AstraControlCenter. Fornire il nome, l'indirizzo Astra e la versione di Astra.



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.

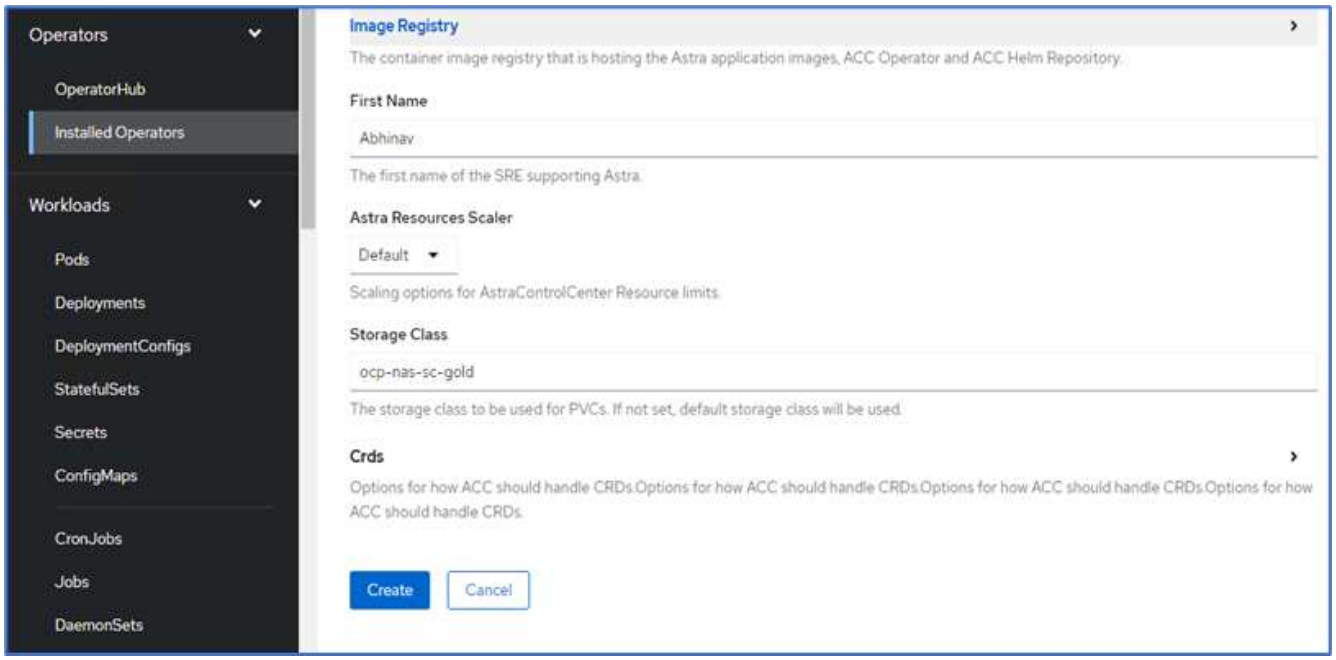
17. Immettere un nome account, un indirizzo e-mail, il cognome dell'amministratore e mantenere la policy di

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.

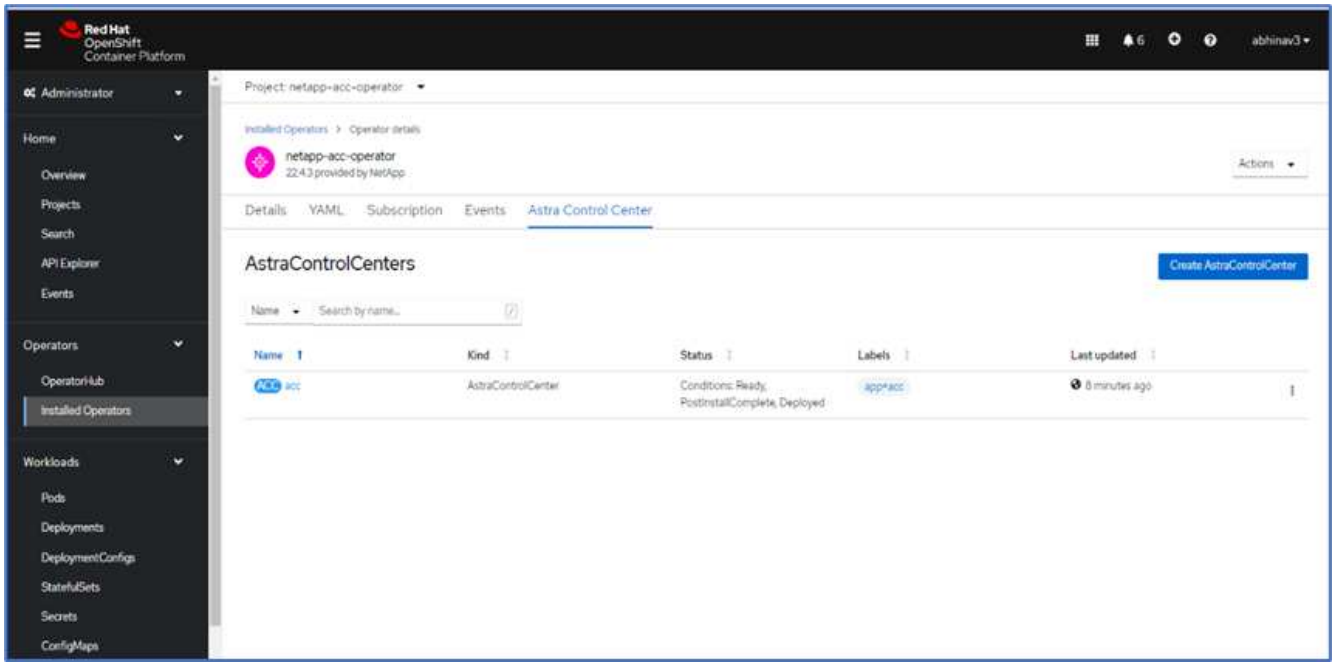


In questa soluzione viene utilizzato il bilanciamento del carico Metallb. Pertanto, il tipo di ingresso è AccTraefik. Questo espone il gateway traefik di Astra Control Center come un servizio Kubernetes di tipo LoadBalancer.

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
```

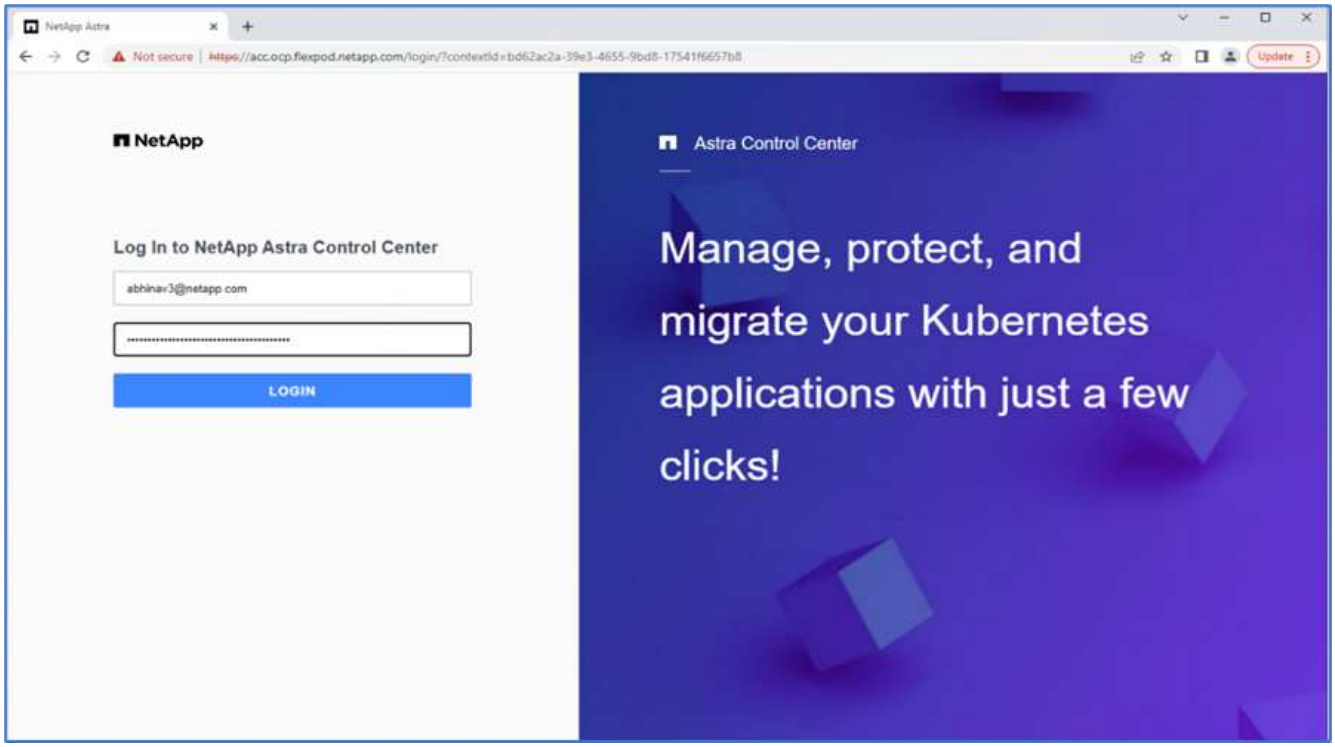
```
3m18s
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   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]).

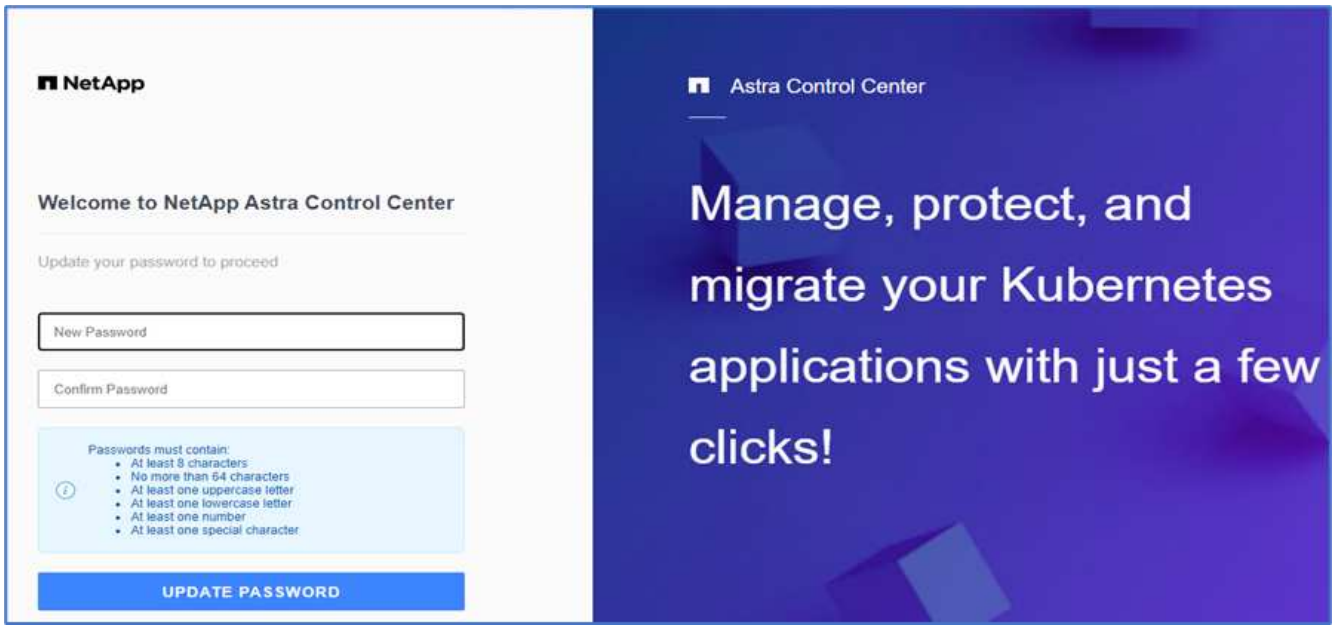
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

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.

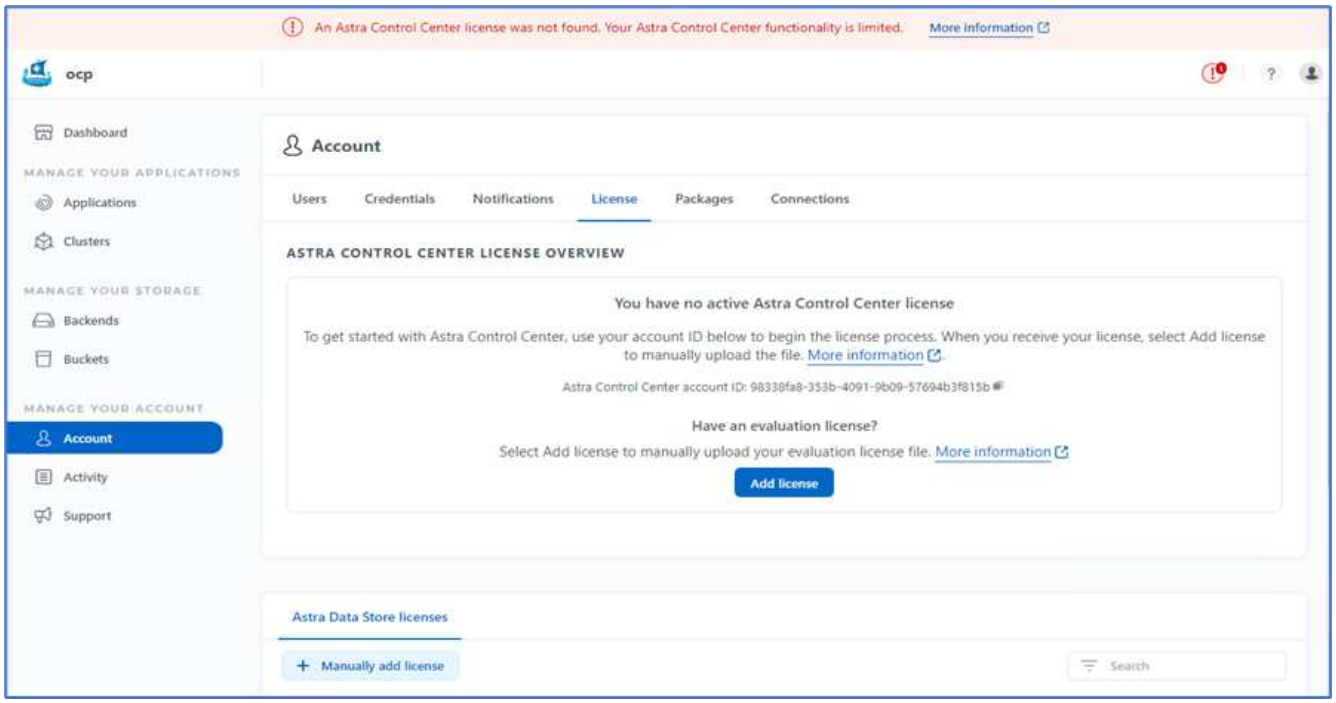


Per ulteriori informazioni sull'installazione di Astra Control Center, consultare "Panoramica dell'installazione di Astra Control Center" pagina.

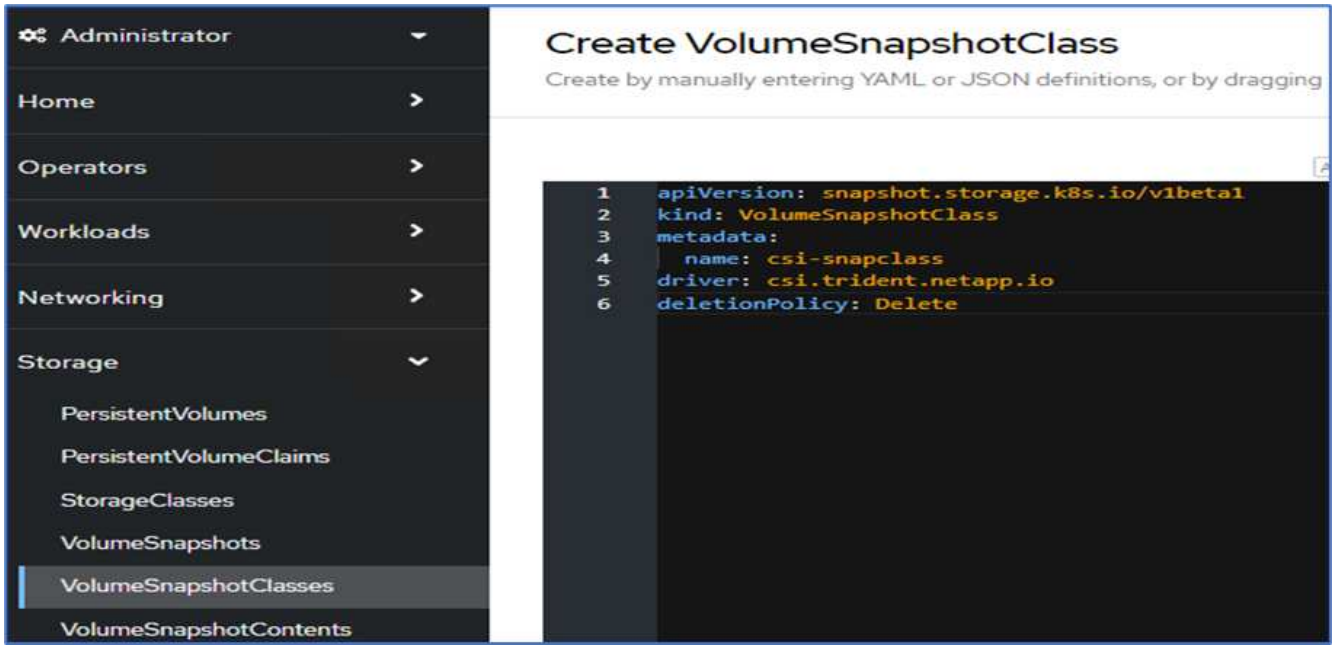
Configurare Astra Control Center

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

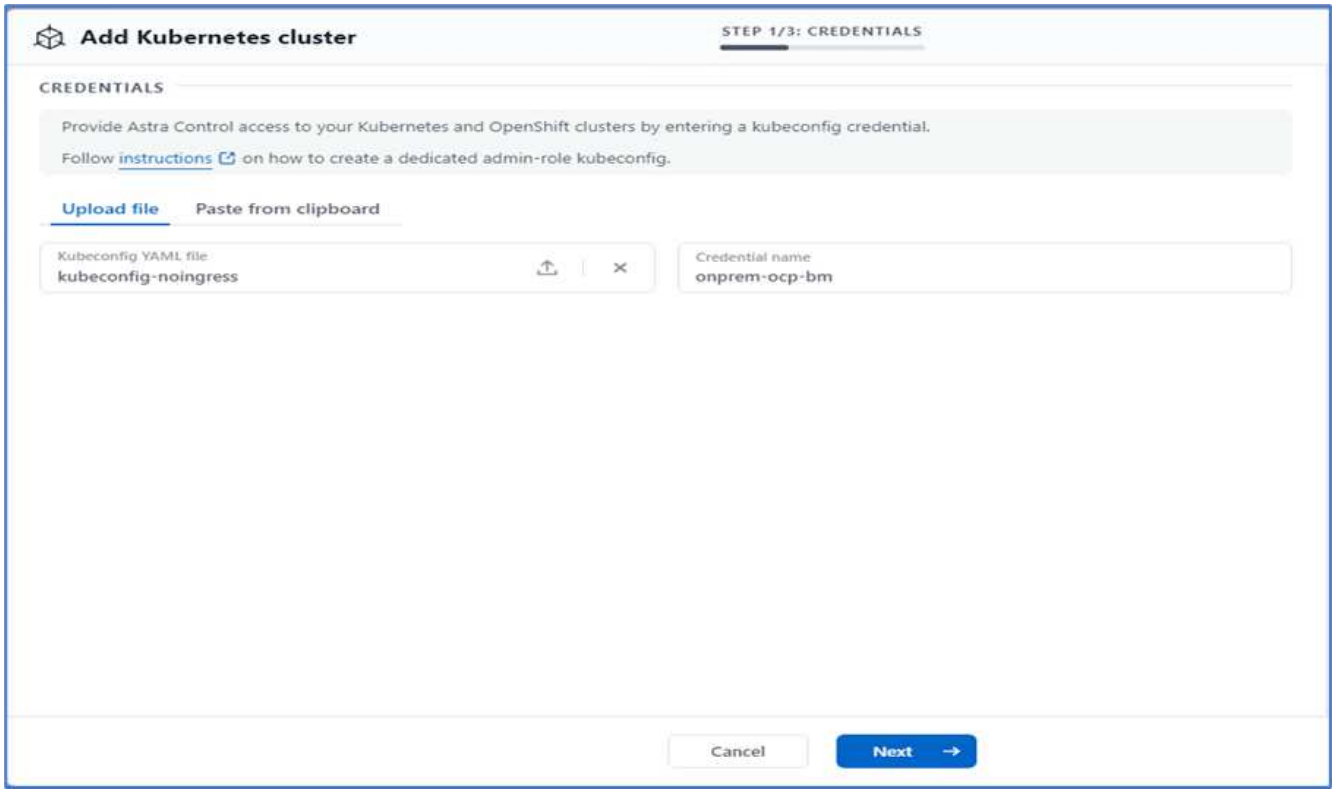
1. Nella home page, sotto account, andare alla scheda License (licenza) e selezionare Add License (Aggiungi licenza) per caricare la licenza Astra.



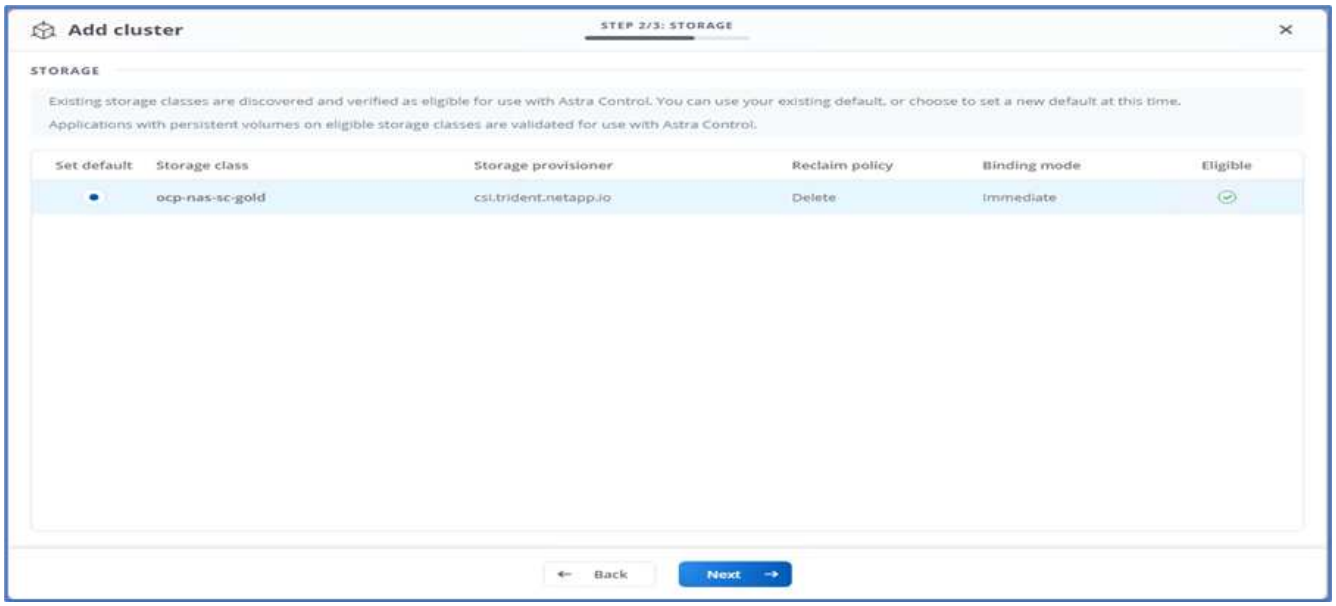
2. Prima di aggiungere il cluster OpenShift, creare una classe di snapshot Astra Trident Volume dalla console Web OpenShift. La classe Volume snapshot viene configurata con `csi.trident.netapp.io` driver.



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.



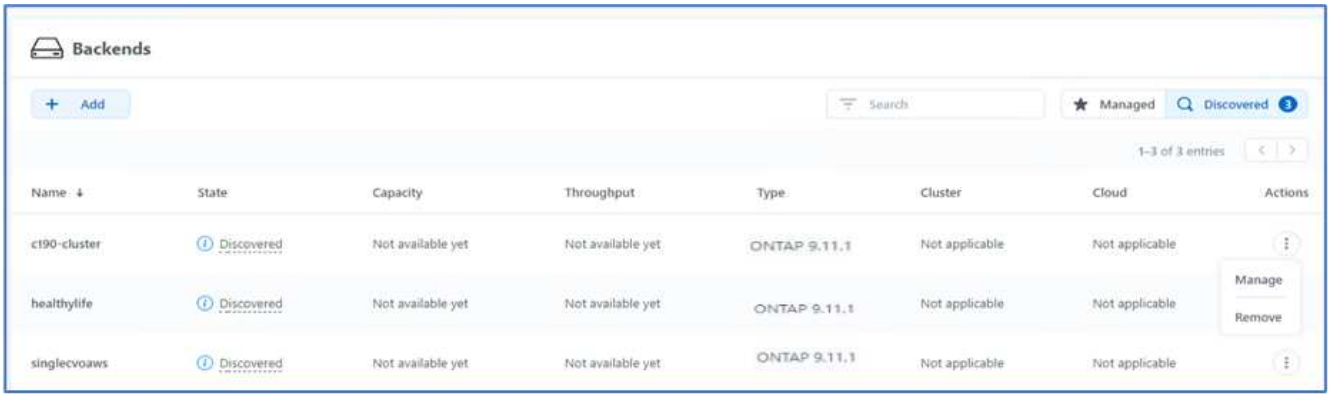
4. Le classi di storage esistenti vengono rilevate automaticamente. Selezionare la classe di storage predefinita, fare clic su Next (Avanti), quindi su Add cluster (Aggiungi cluster).



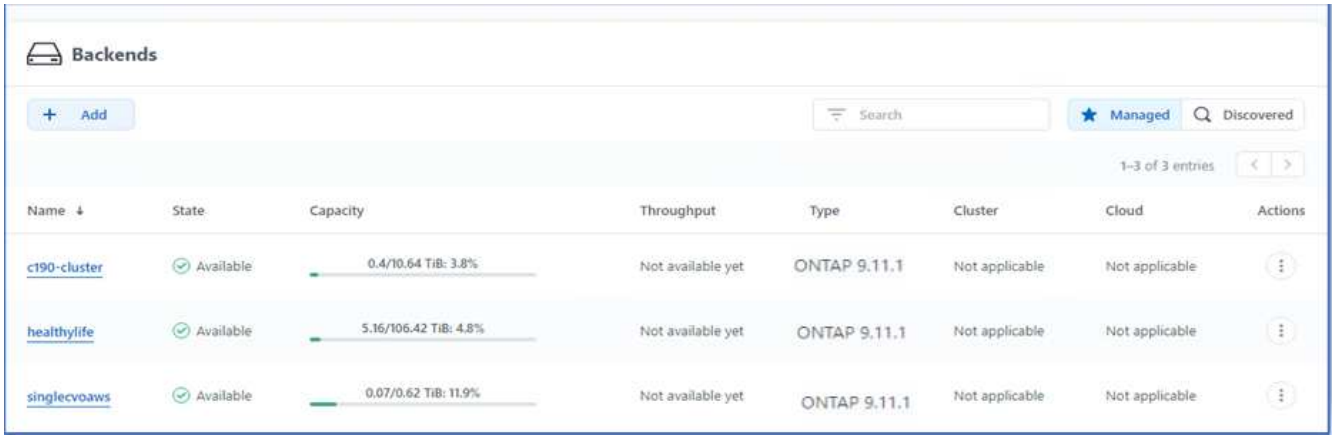
5. Il cluster viene aggiunto in pochi minuti. Per aggiungere altri cluster OpenShift Container Platform, ripetere i passaggi 1–4.

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

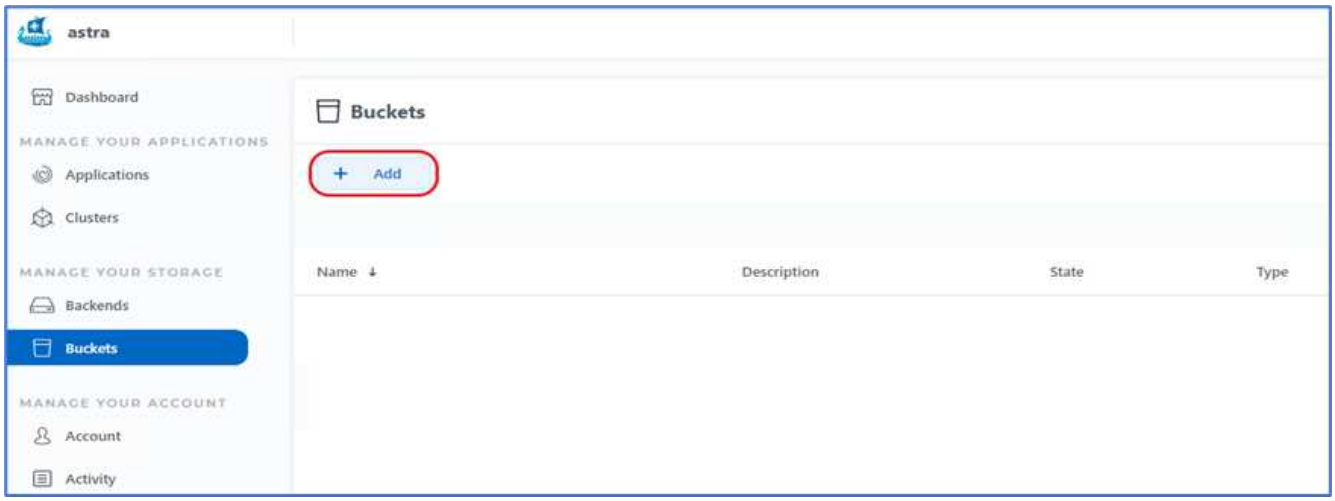
6. Per gestire lo storage, accedere a Backend, fare clic sui tre punti in azioni rispetto al backend che si desidera gestire. Fare clic su Gestisci.



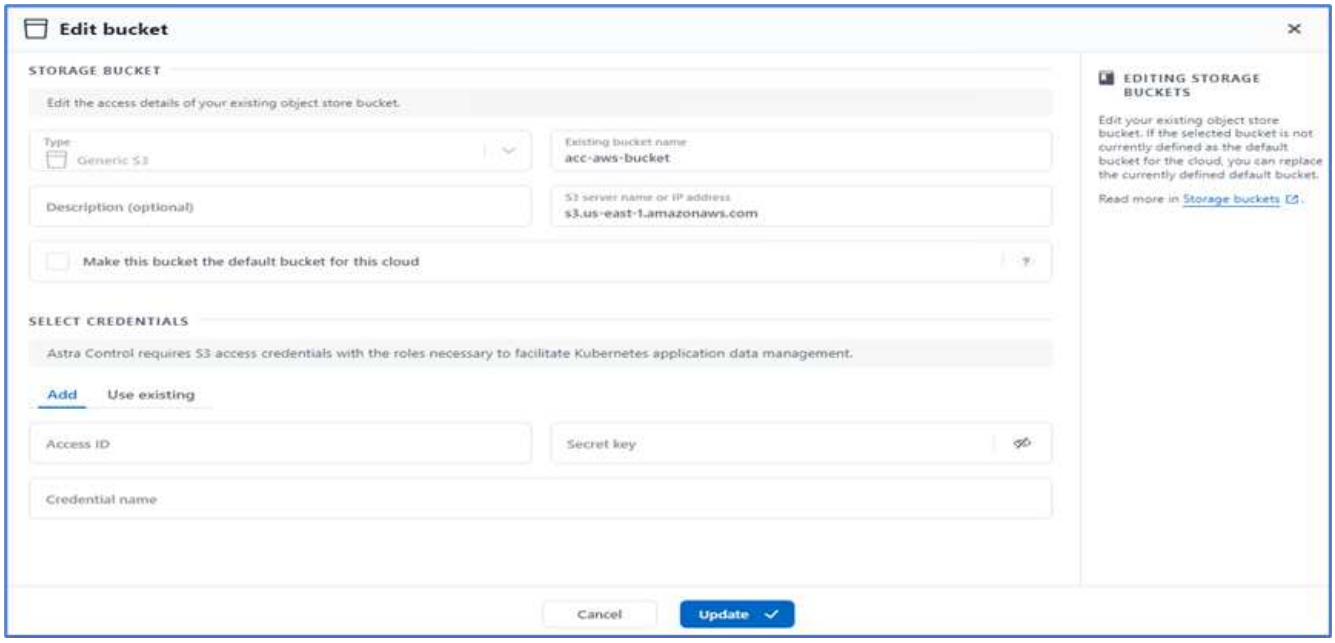
7. Fornire le credenziali ONTAP e fare clic su Avanti. Esaminare le informazioni e fare clic su Managed (gestito). I backend dovrebbero essere simili all'esempio seguente.



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

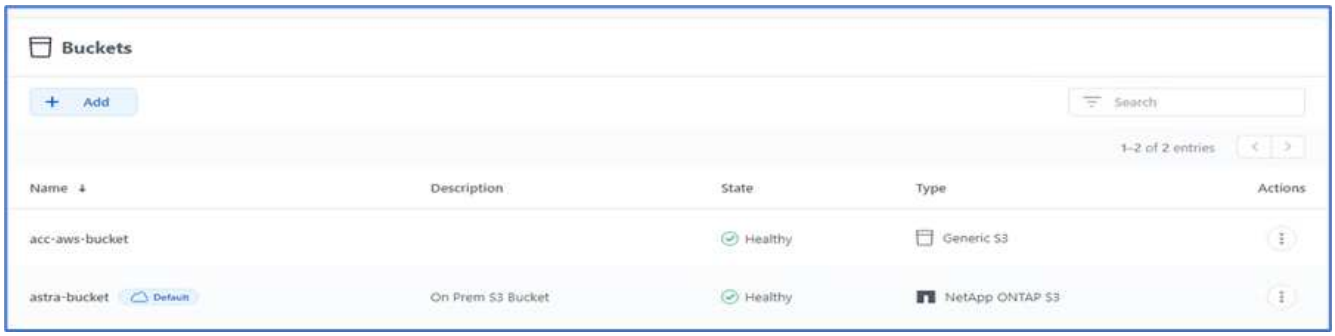


9. Selezionare il tipo di bucket e fornire il nome del bucket, il nome del server S3 o l'indirizzo IP e la credenziale S3. Fare clic su Aggiorna.



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."

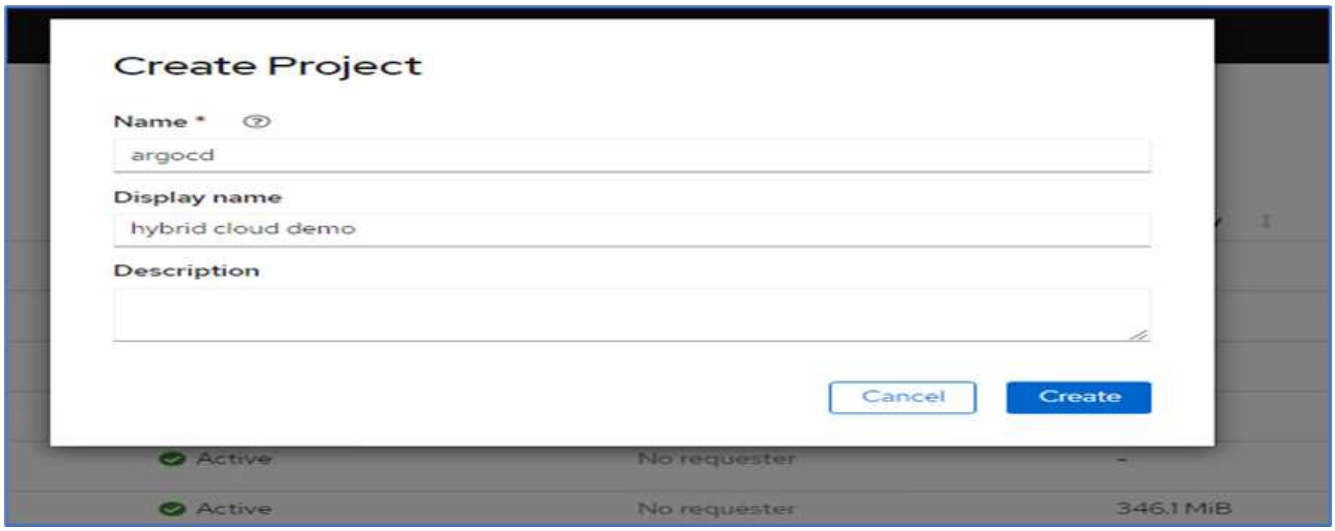
Con Astra, puoi eseguire un backup completo coerente con l'applicazione che può

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.

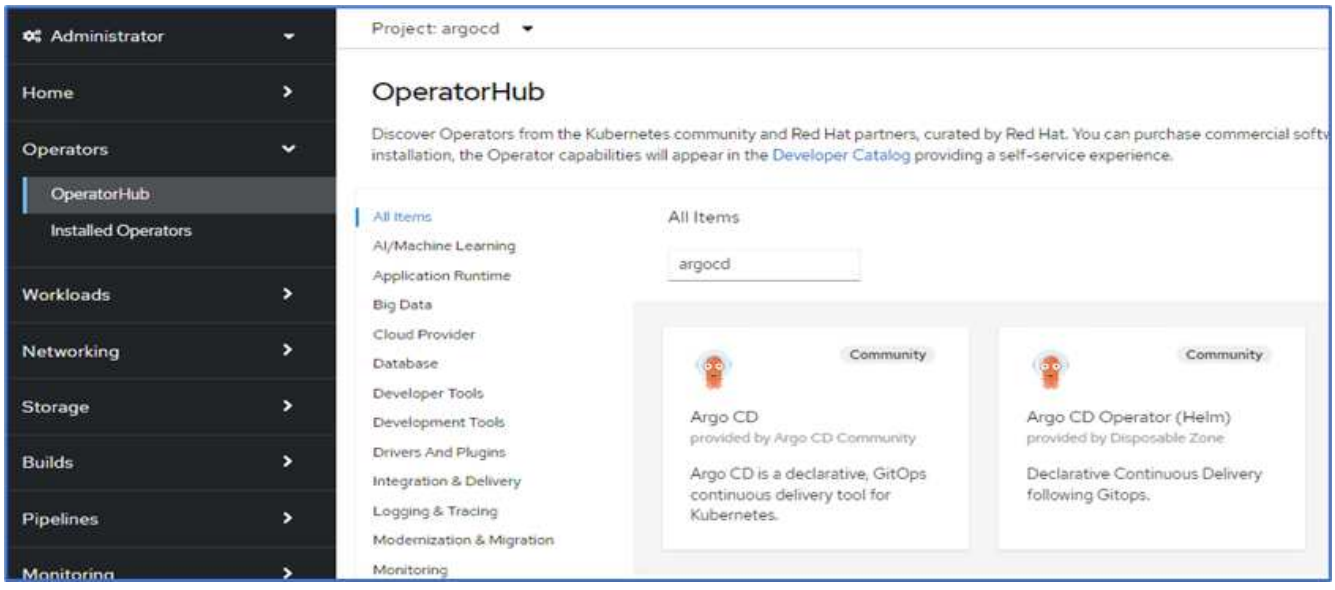
Per convalidare un ripristino dell'applicazione di successo, simulare un errore on-premise di un'applicazione in esecuzione sul sistema FlexPod e ripristinare l'applicazione su un cluster K8s in esecuzione nel cloud utilizzando un backup remoto.

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.

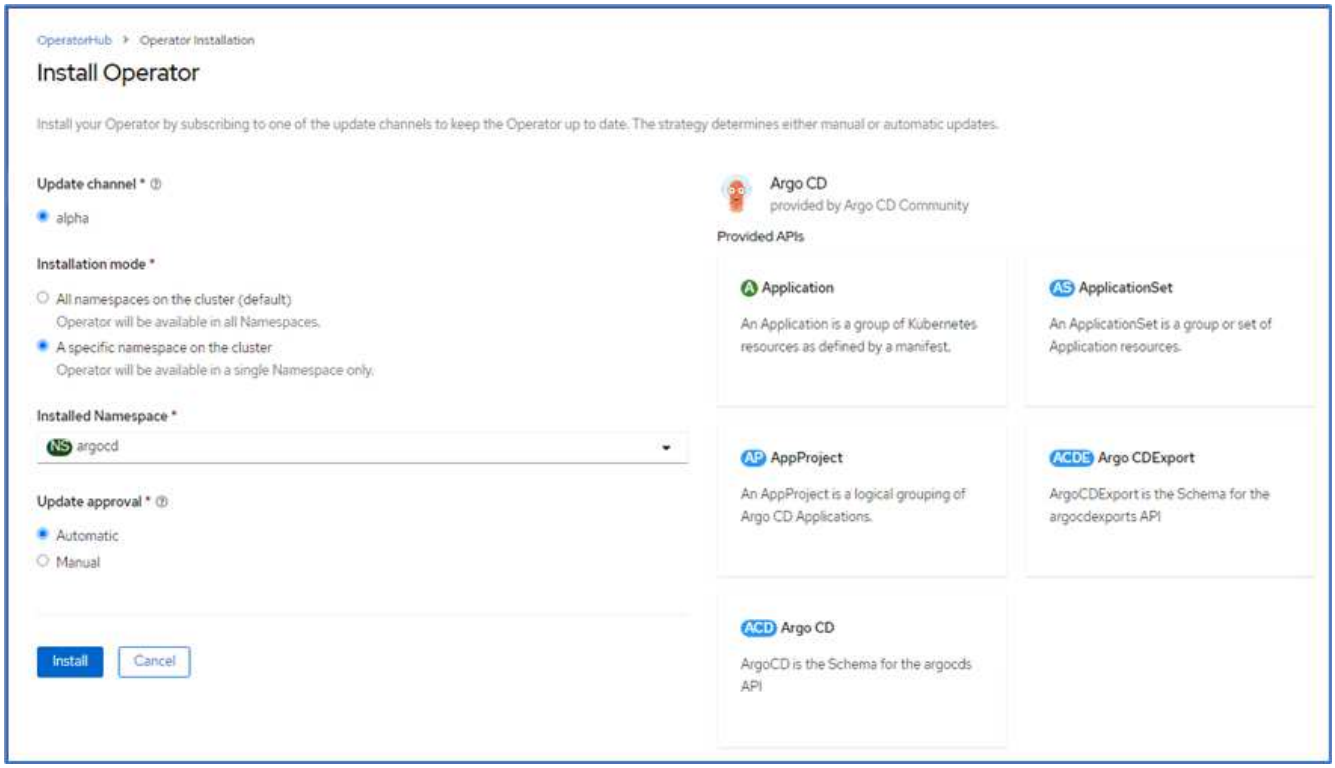
1. Accedi al cluster OpenShift on-premise e crea un nuovo progetto con il nome `argocd`.



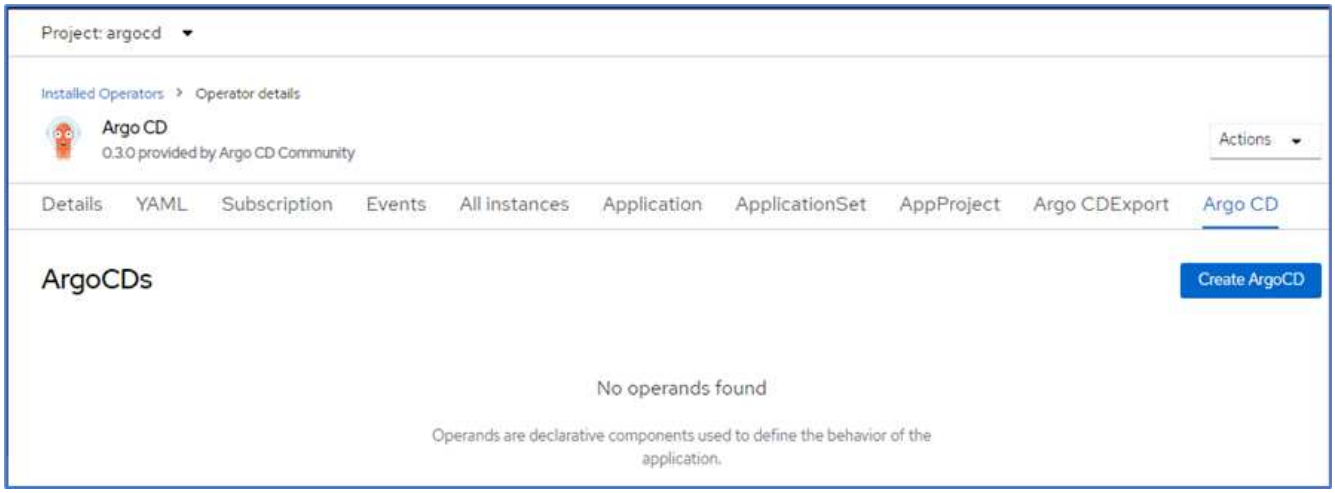
2. In OperatorHub, cercare `argocd` E selezionare Argo CD operator.



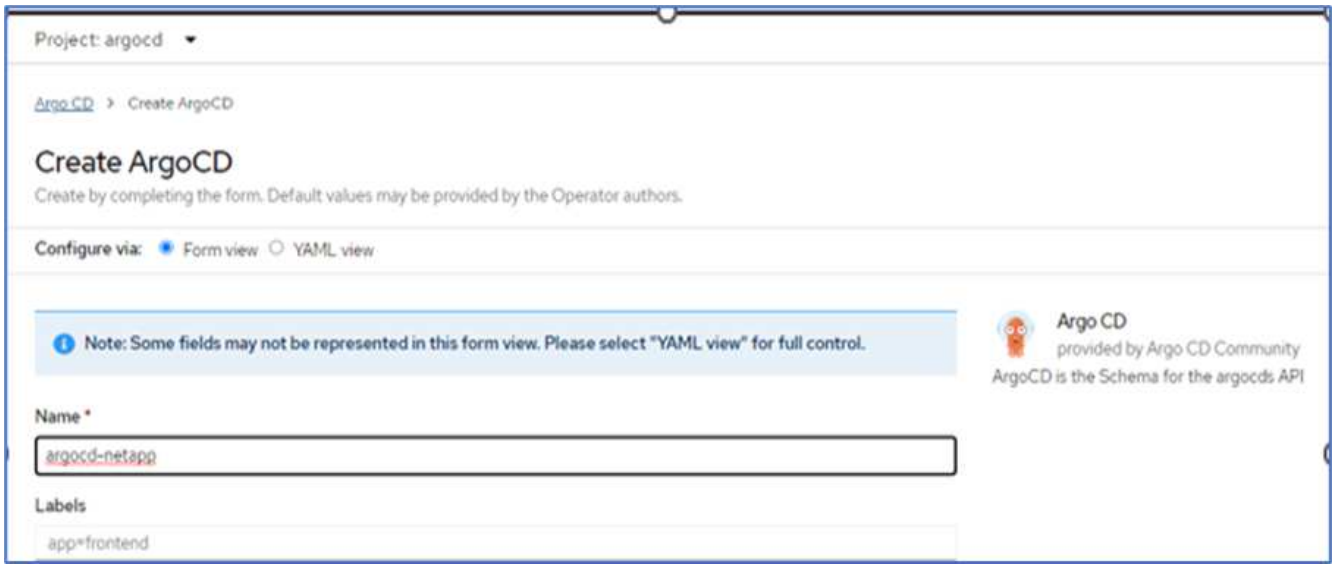
3. Installare l'operatore in `argocd` namespace.



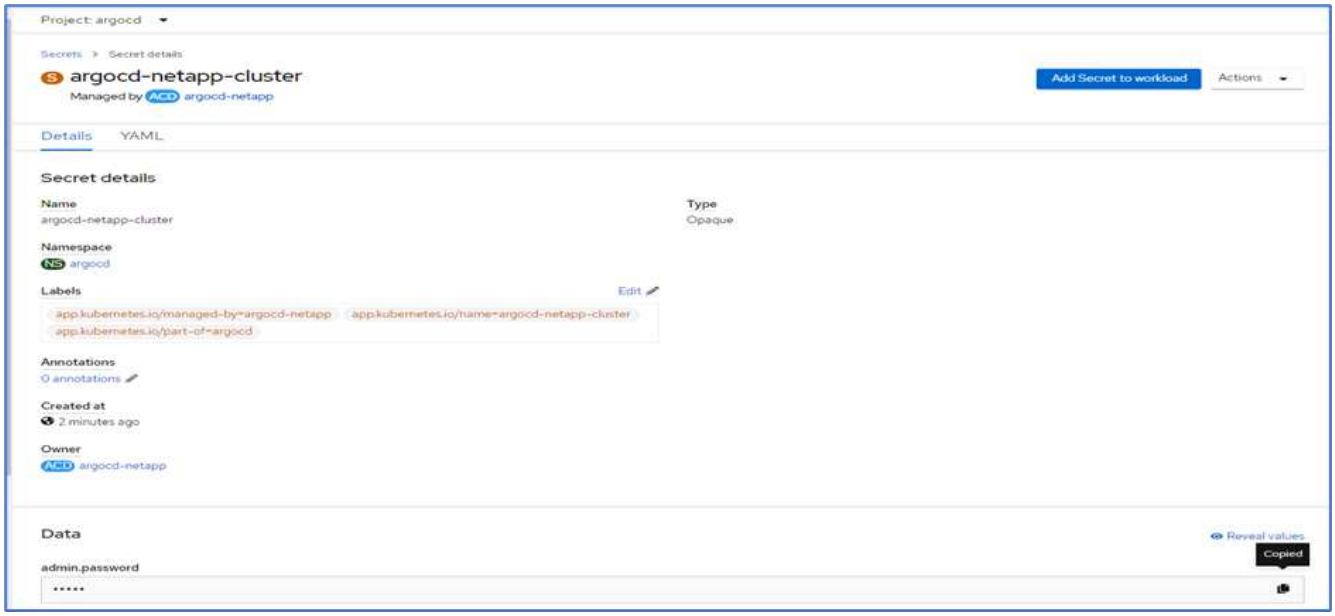
4. Accedere all'operatore e fare clic su Create ArgoCD (Crea ArgoCD).



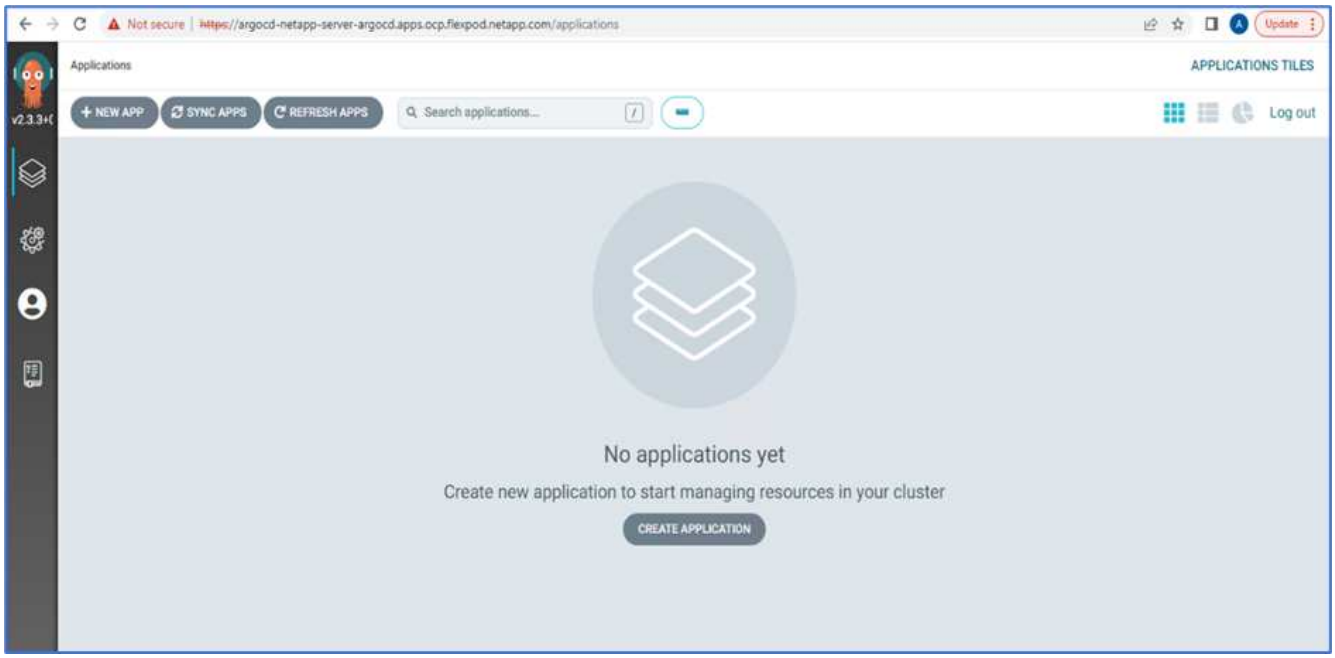
5. Per distribuire l'istanza del CD Argo in `argocd` Assegnare un nome e fare clic su Create (Crea).



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`.



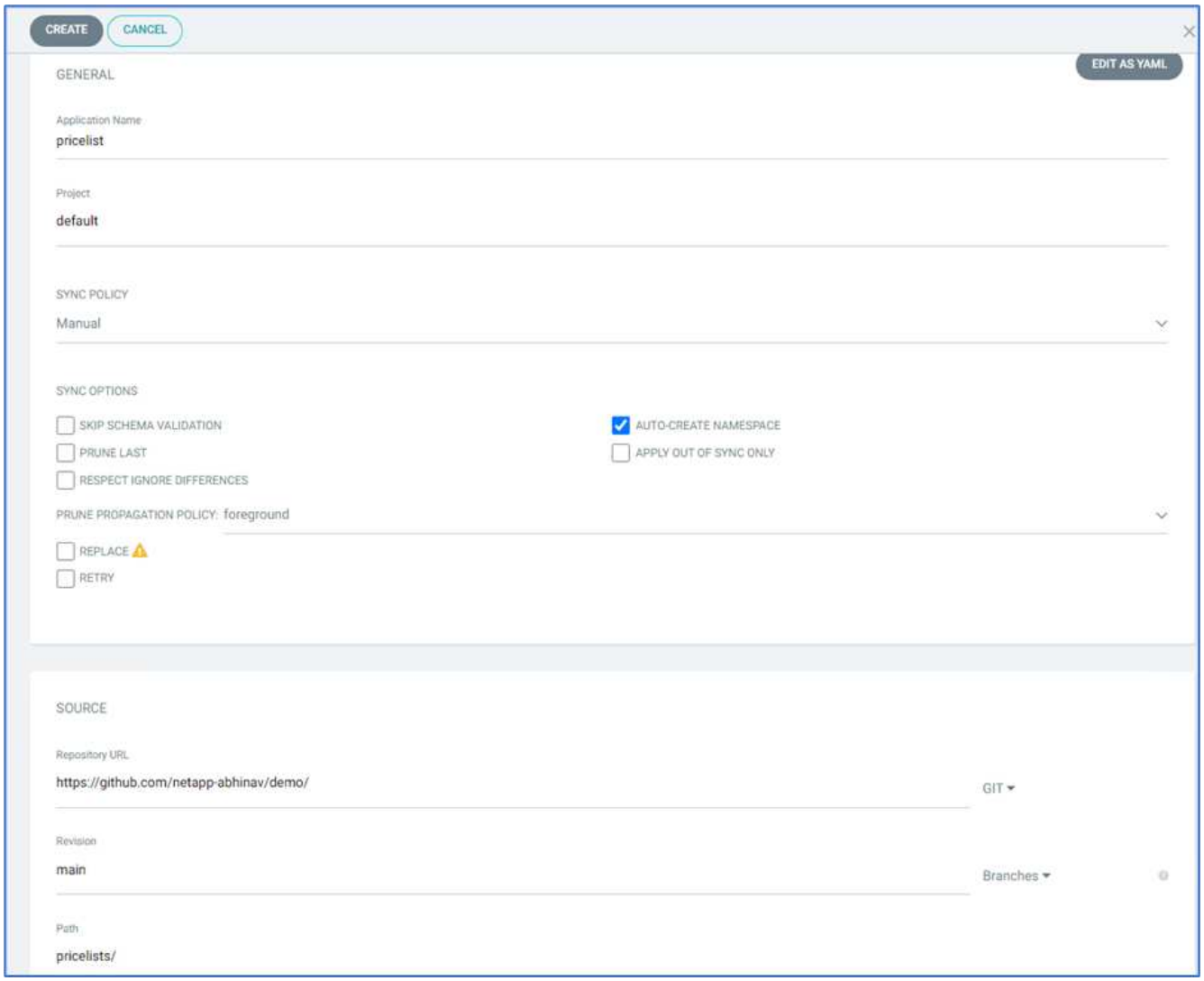
7. Dal menu laterale, selezionare routes > Location (percorsi > Località) e fare clic sull'URL del `argocd` percorsi. Immettere il nome utente e la password.



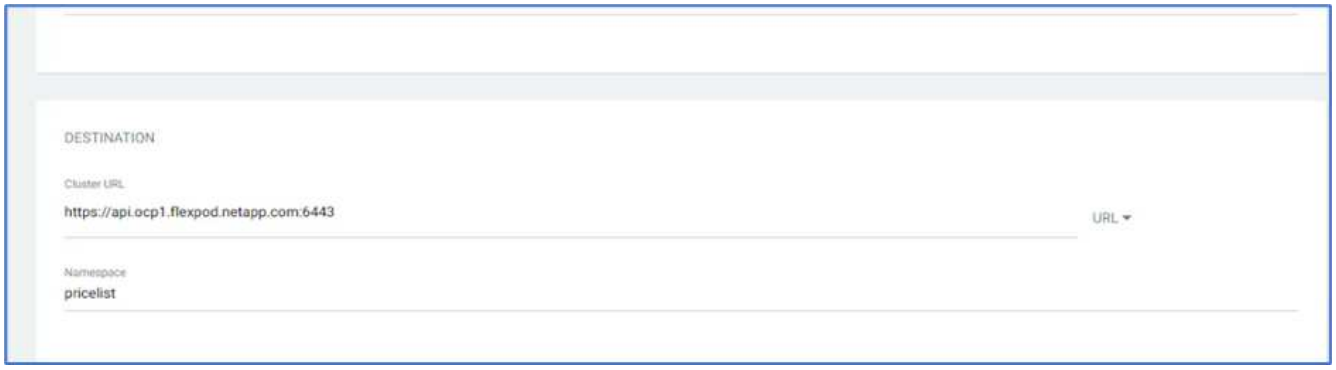
8. Aggiungere il cluster OpenShift on-premise al CD Argo attraverso la CLI.

```
####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
```

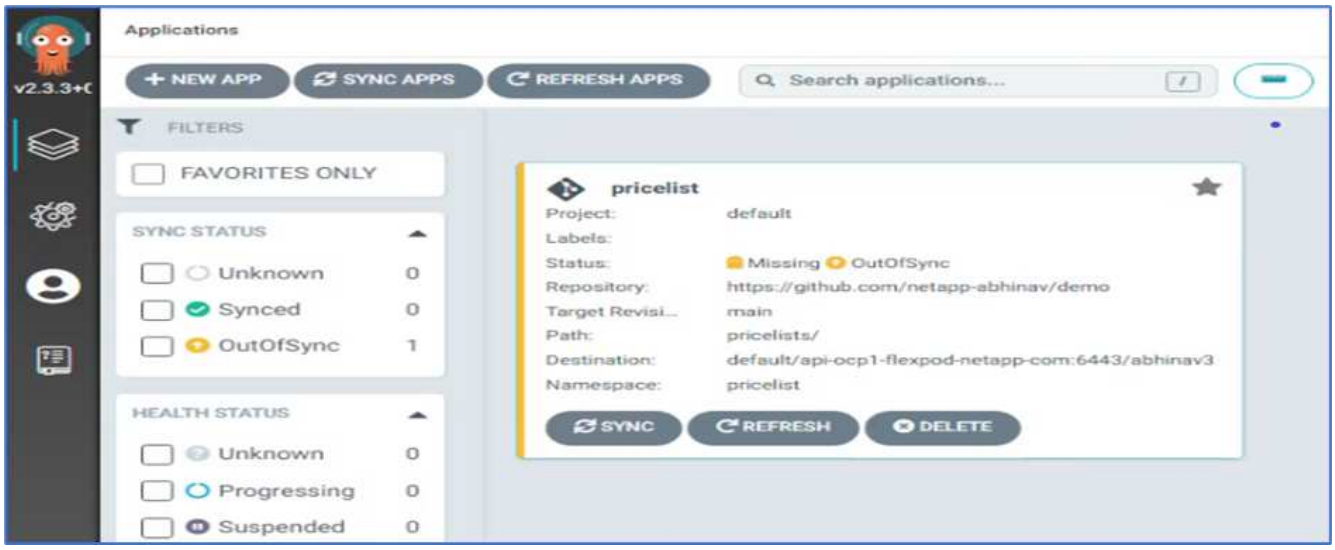
9. Nell'interfaccia utente di ArgoCD, fare clic SU NEW APP (NUOVA APPLICAZIONE) e immettere i dettagli relativi al nome dell'applicazione e al repository di codice.



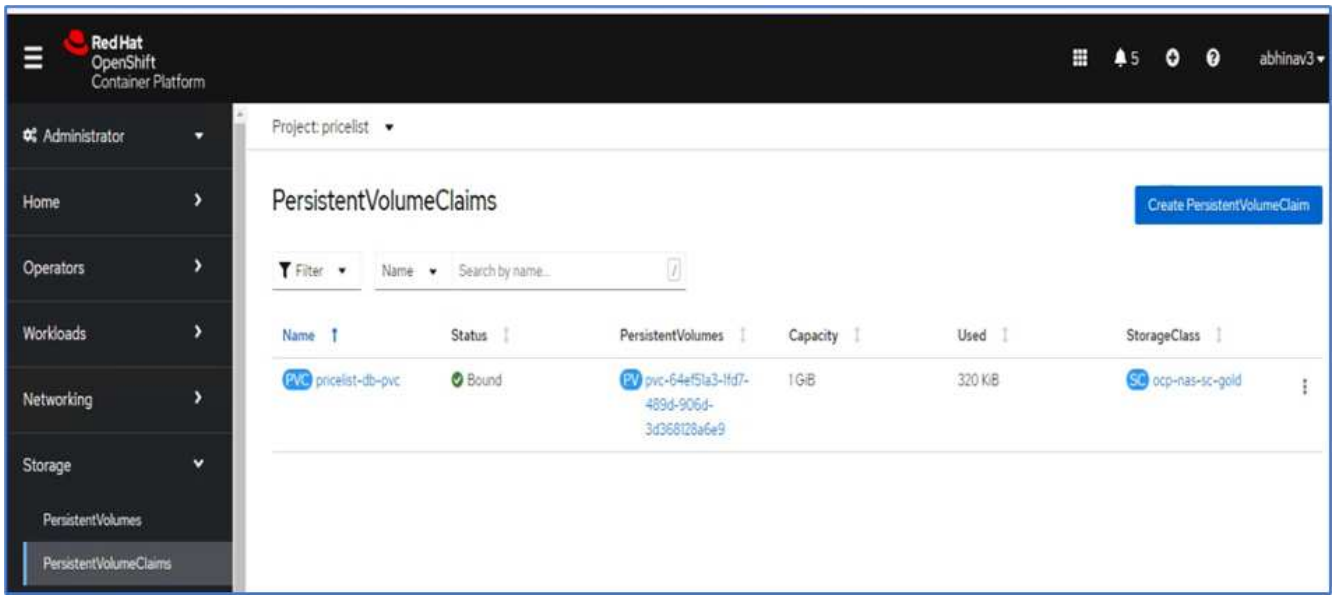
10. Inserire il cluster OpenShift in cui l'applicazione verrà implementata insieme allo spazio dei nomi.



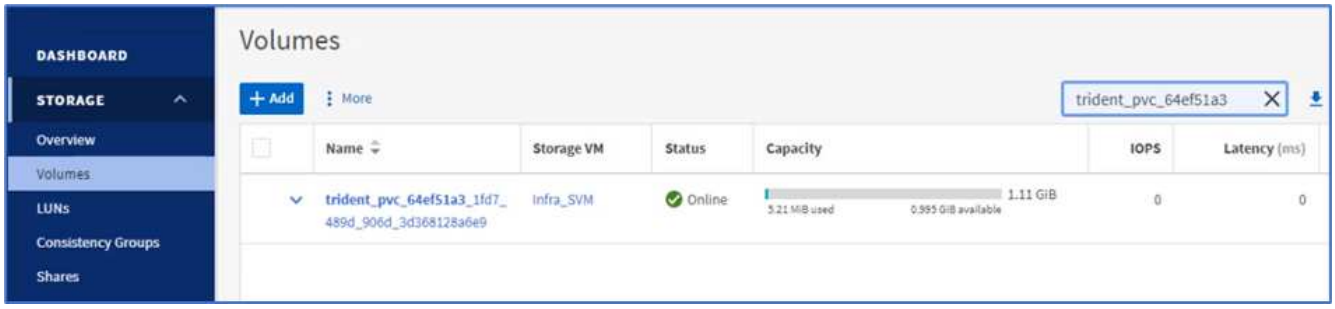
11. Per implementare l'applicazione sul cluster OpenShift on-premise, fare clic su SYNC.



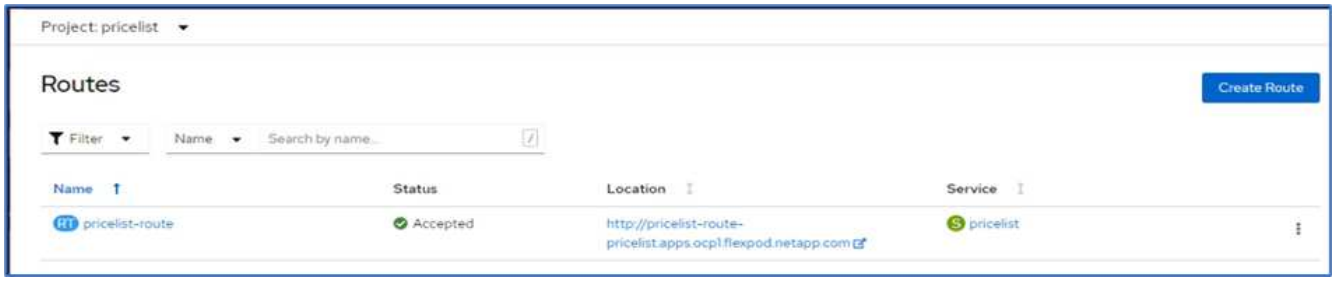
12. Nella console di OpenShift Container Platform, accedere a Preventivo progetto e, in Storage, verificare il nome e le dimensioni del PVC.



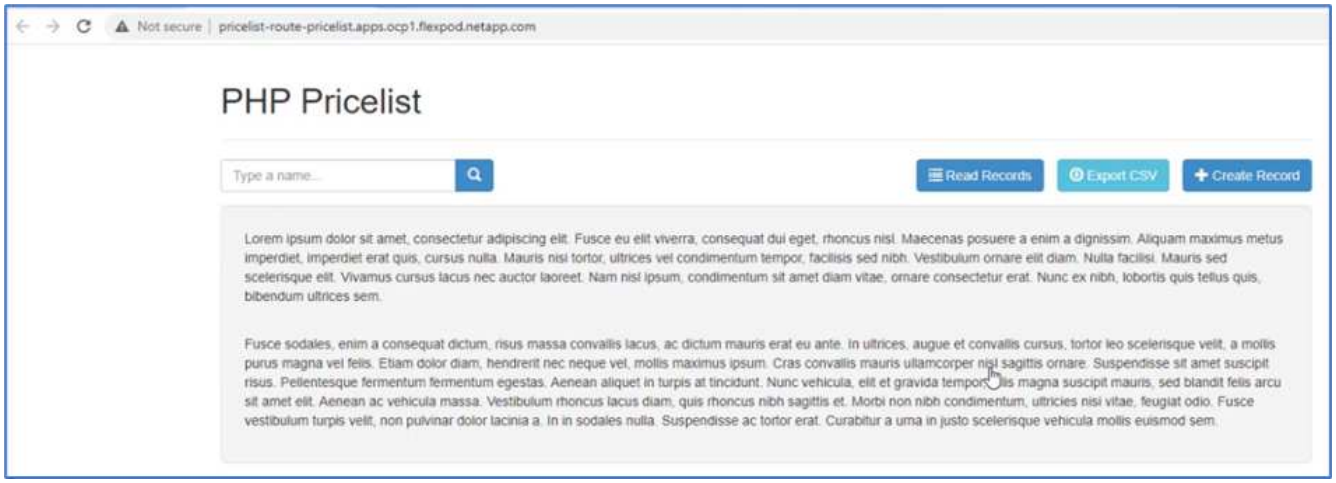
13. Accedere a System Manager e verificare il PVC.



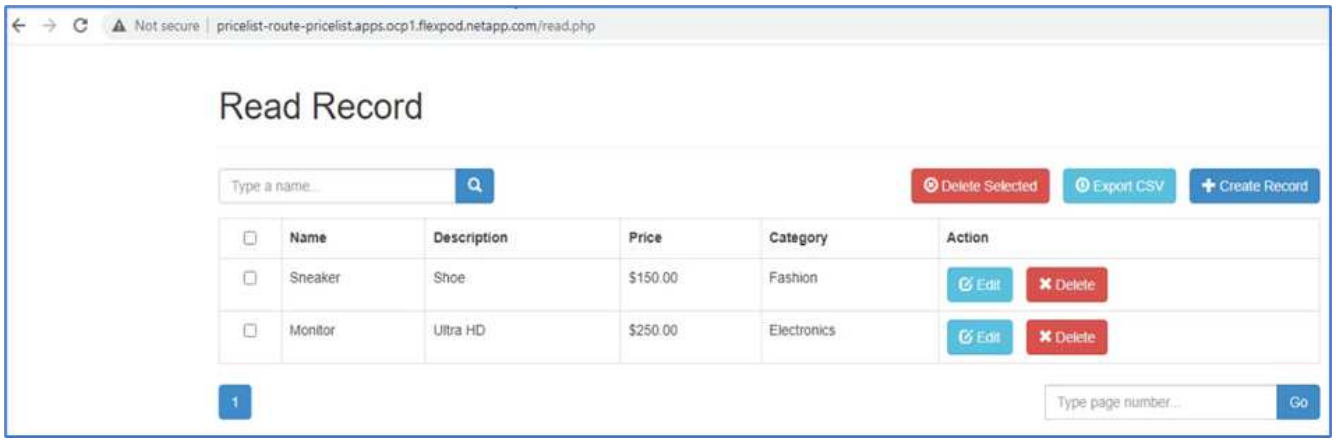
14. Una volta eseguiti i pod, selezionare rete > percorsi dal menu laterale, quindi fare clic sull'URL in posizione.



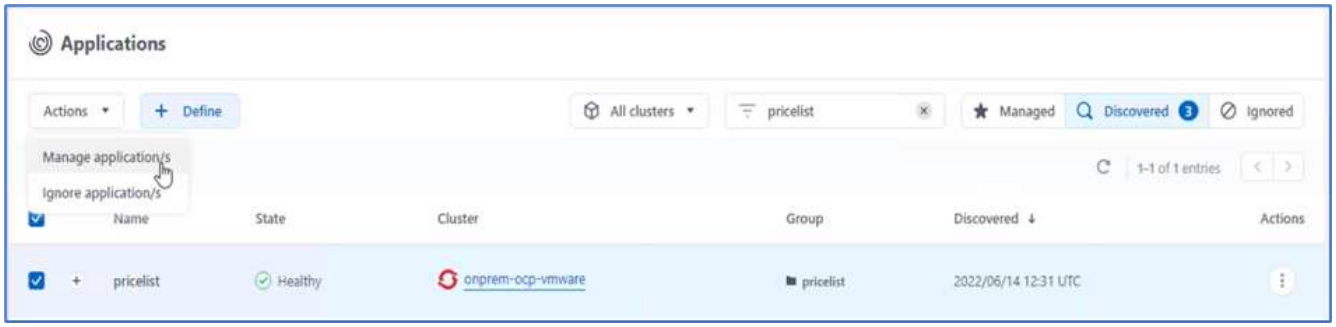
15. Viene visualizzata la pagina iniziale dell'applicazione Pricelist.



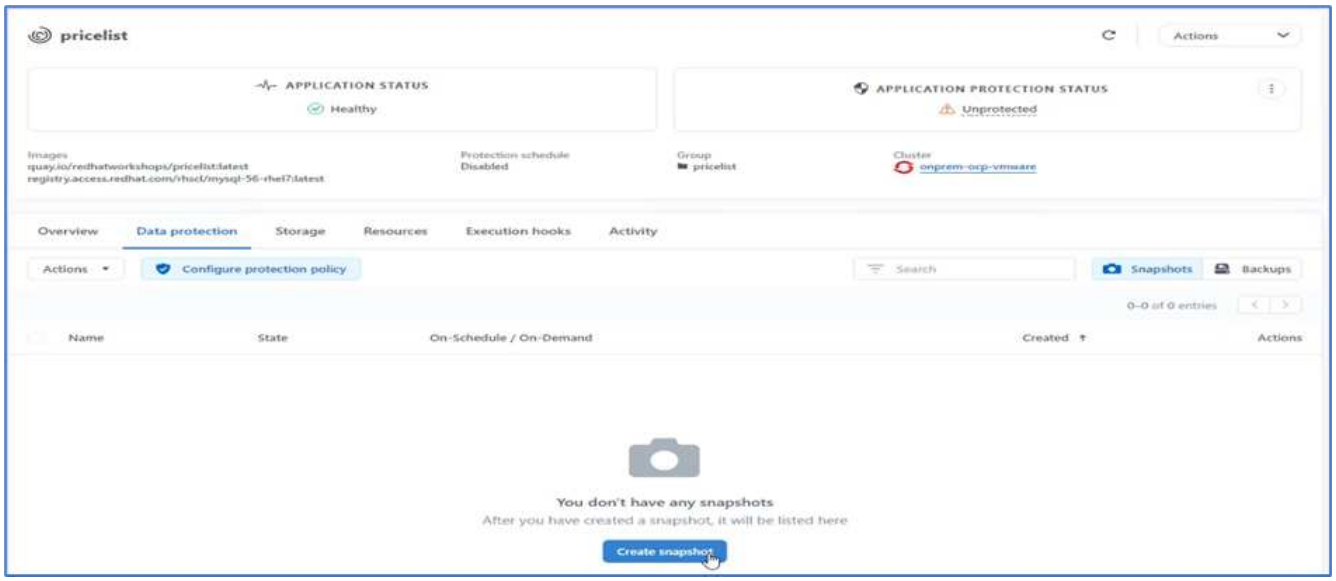
16. Creare alcuni record nella pagina Web.



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.

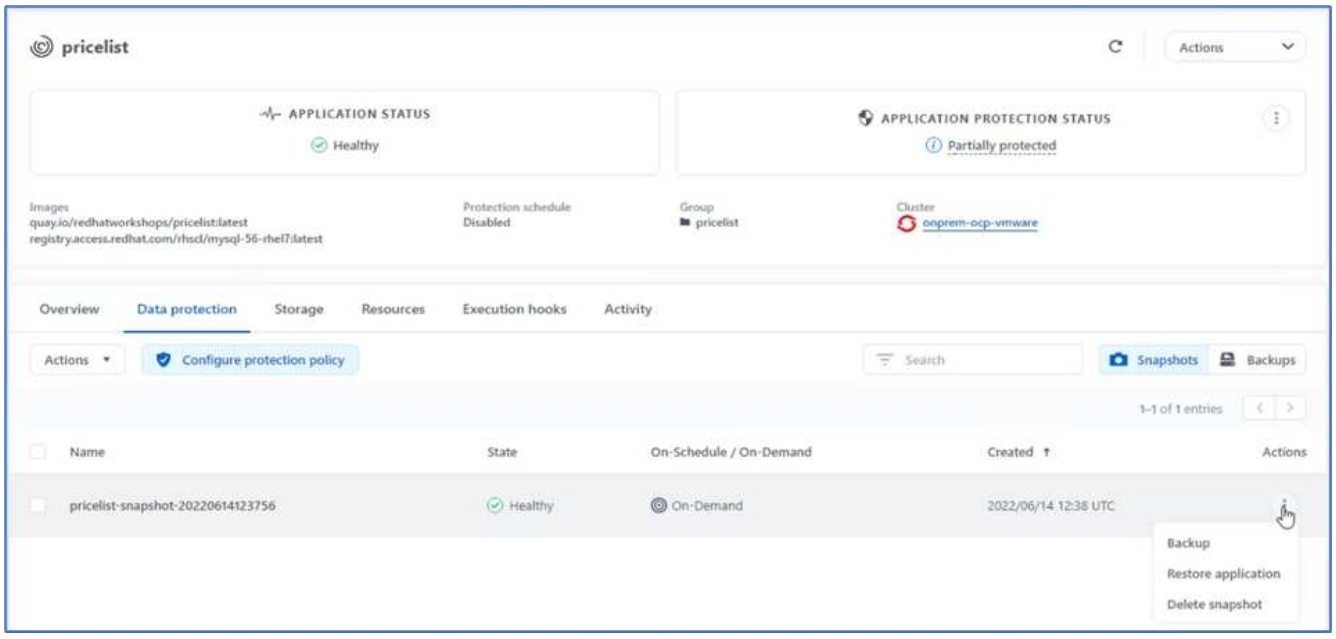


18. Fare clic sull'applicazione Listino prezzi e selezionare Data Protection (protezione dati). A questo punto, non dovrebbero esserci snapshot o backup. Fare clic su Create Snapshot (Crea istantanea) per creare un'istantanea on-demand.

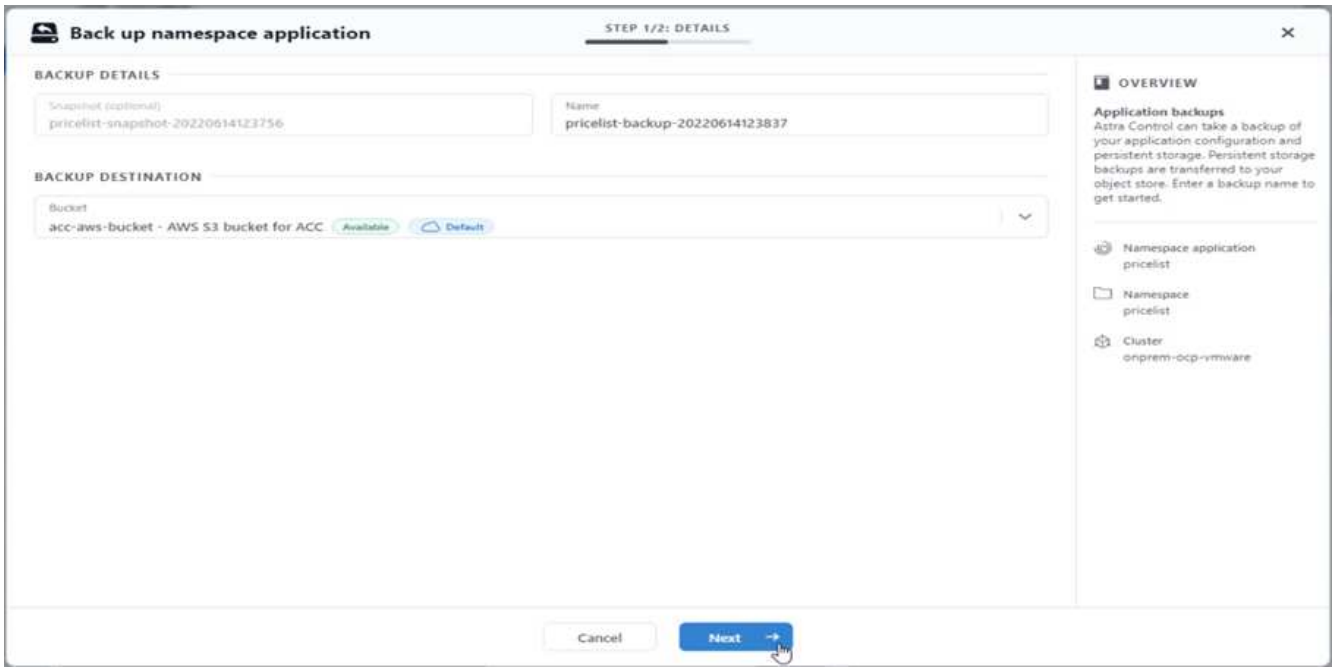


NetApp Astra Control Center supporta backup e snapshot on-demand e pianificati.

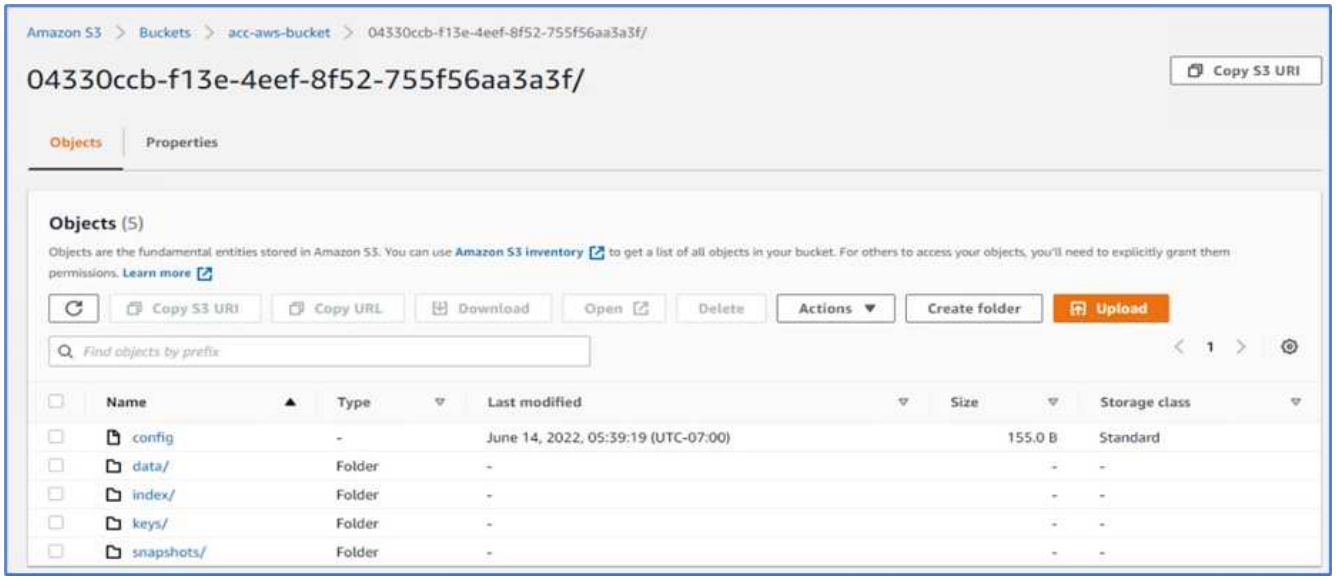
19. Una volta creata la snapshot e lo stato è integro, creare un backup remoto utilizzando tale snapshot. Questo backup viene memorizzato nel bucket S3.



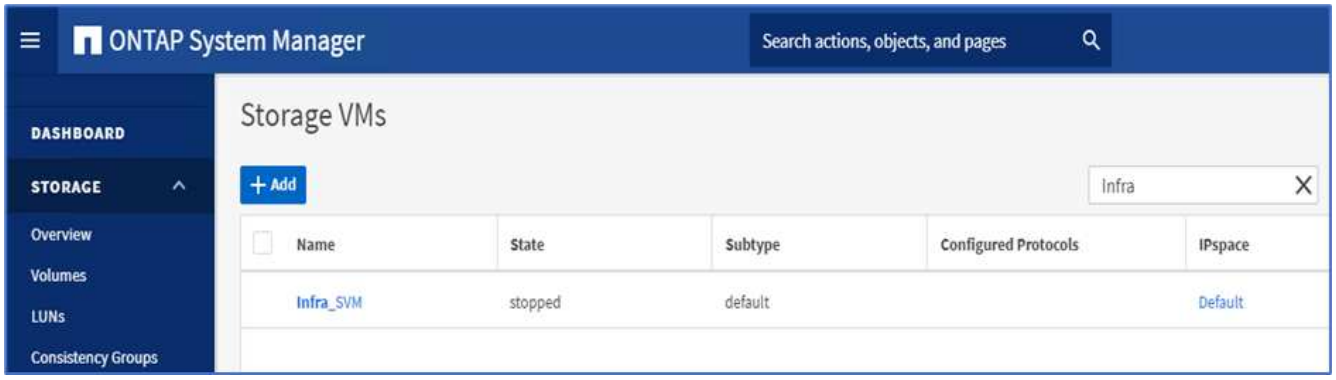
20. Selezionare il bucket AWS S3 e avviare l'operazione di backup.



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



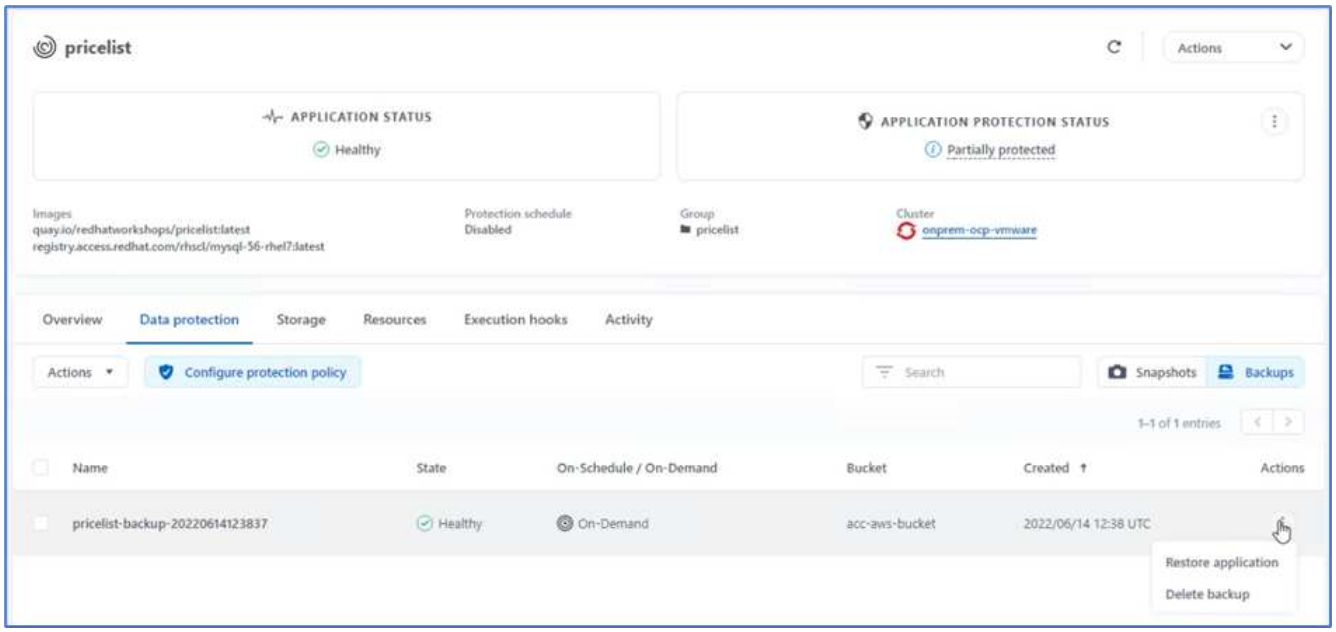
22. Una volta completato il backup remoto, simulare un disastro on-premise arrestando la storage virtual machine (SVM) che ospita il volume di backup per il PV.



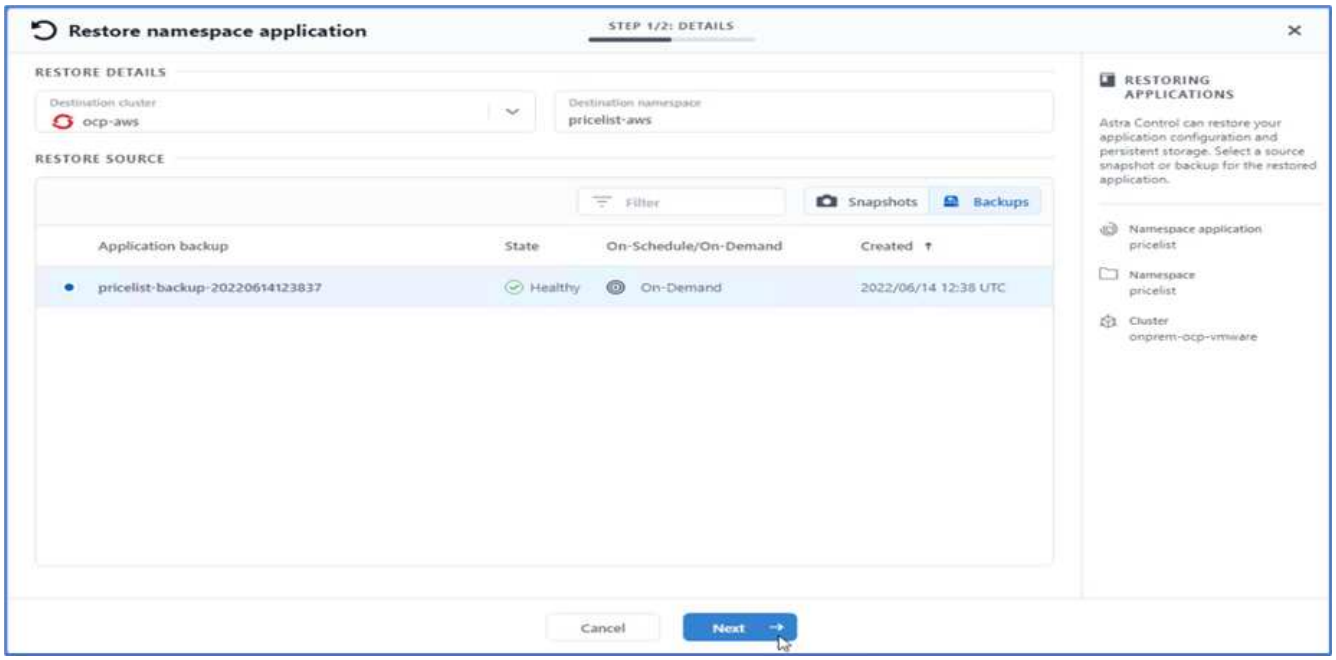
23. Aggiornare la pagina Web per confermare l'interruzione. La pagina web non è disponibile.

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.

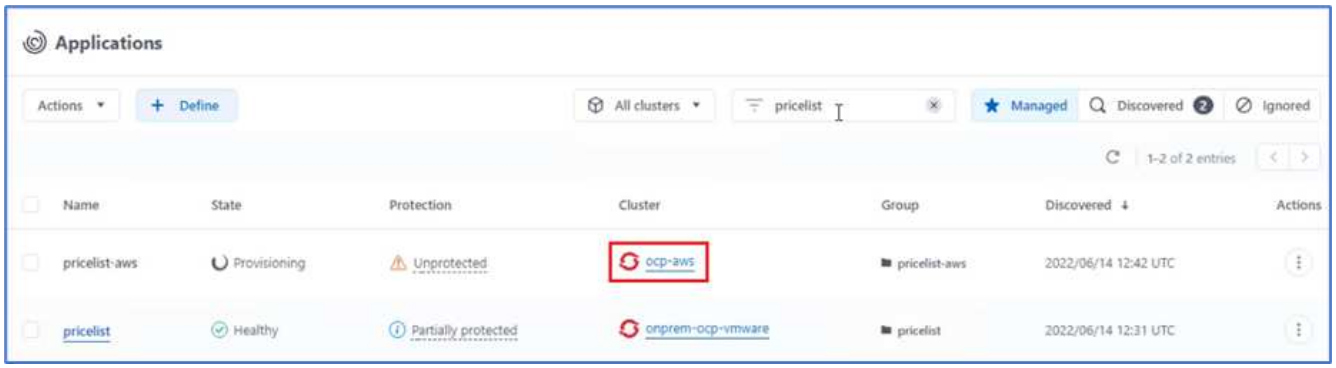
24. In Astra Control Center, fare clic sull'applicazione Pricelist e selezionare Data Protection > Backups (protezione dati > Backup). Selezionare il backup e fare clic su Restore Application (Ripristina applicazione) sotto Action (azione).



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).

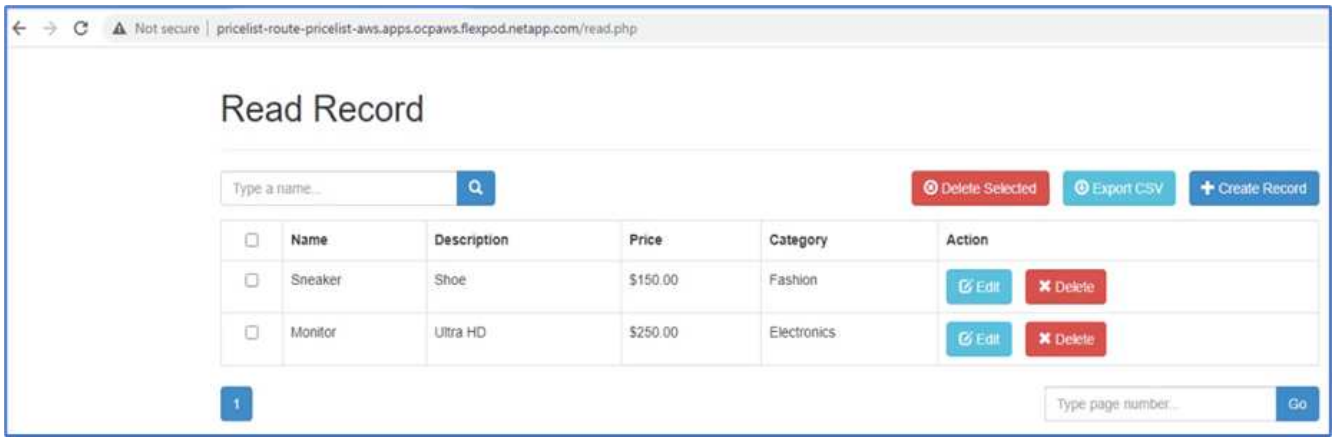


26. Una nuova applicazione con il nome `pricelist-app` Viene eseguito il provisioning sul cluster OpenShift in esecuzione in AWS.



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.

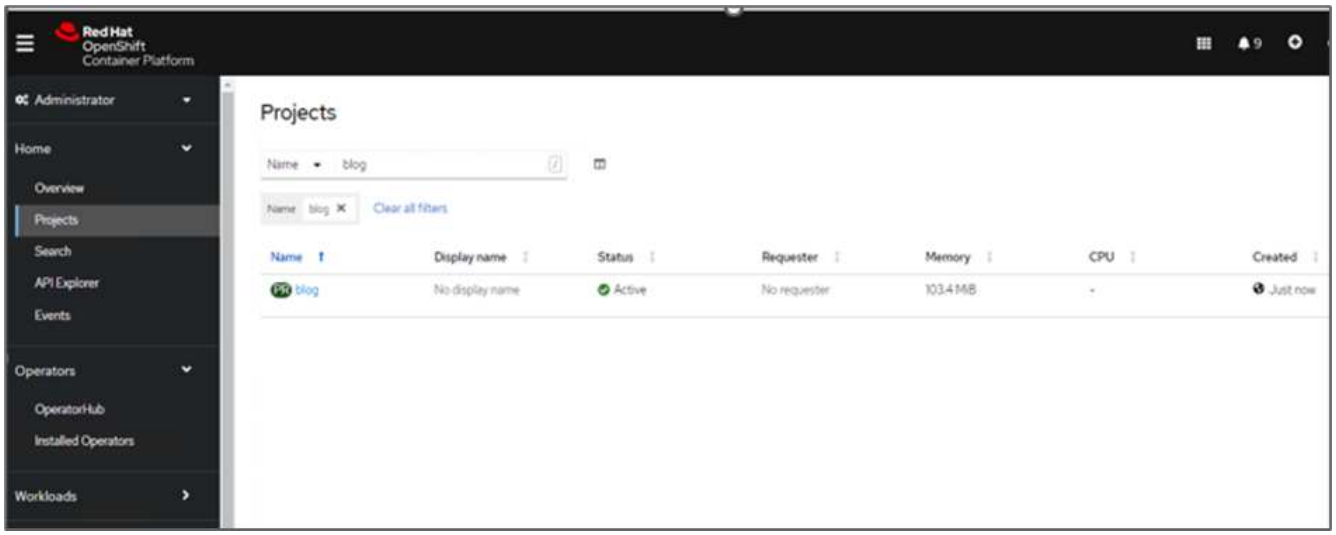
Parte 1

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.

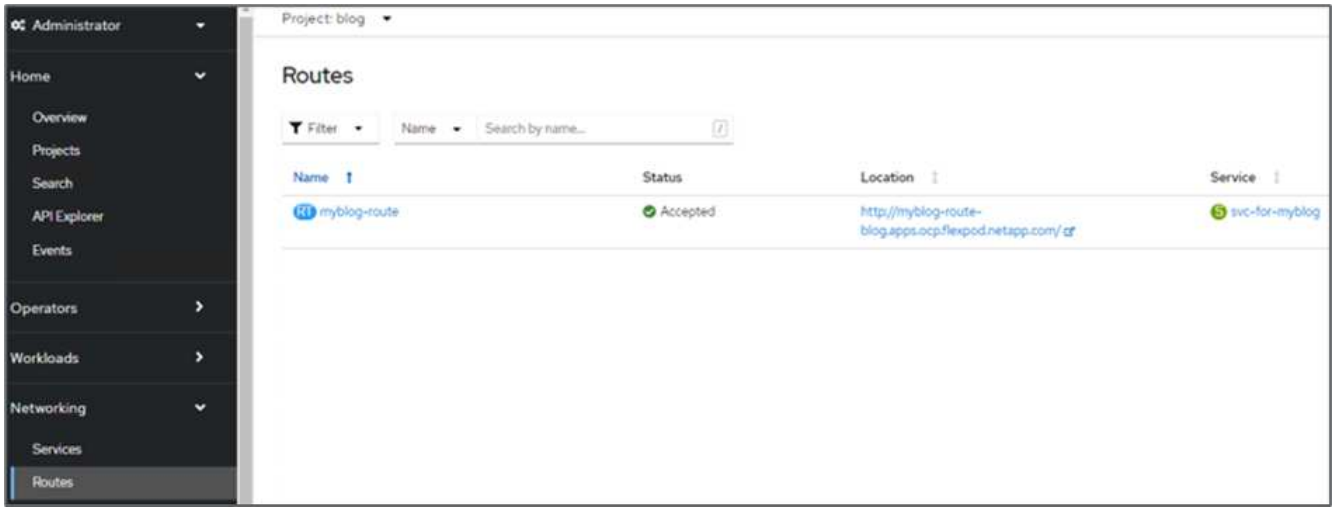
In questo scenario, un team di sviluppo e test (DevTest) implementa un'applicazione stateful di esempio (sito blog) che è un'applicazione blog Ghost, aggiunge alcuni contenuti e aggiorna l'applicazione alla versione più recente disponibile. L'applicazione Ghost utilizza SQLite per il database. Prima 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.

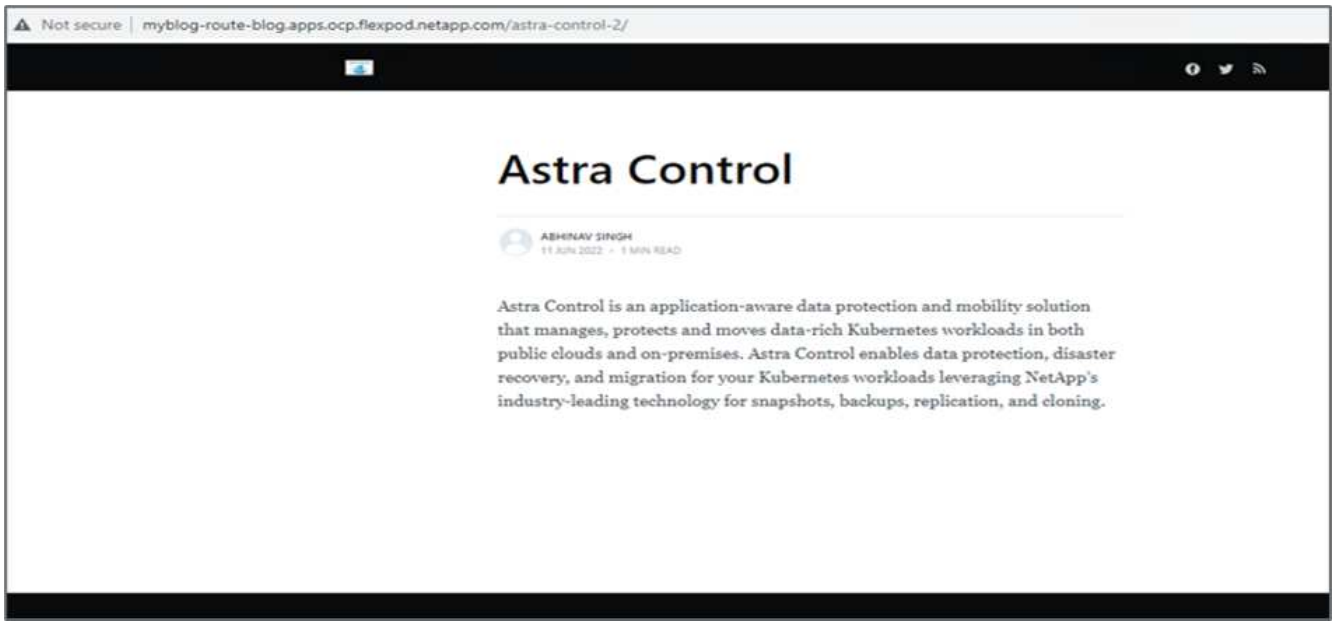
2. Accedere al primo cluster OpenShift, selezionare Project (progetto) e inserire Blog nella barra di ricerca.



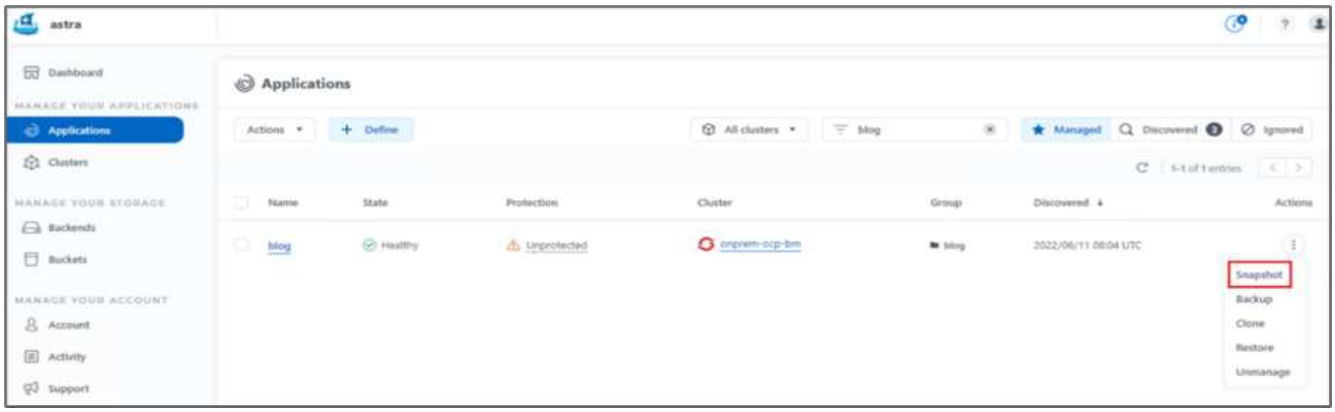
3. Dal menu laterale, selezionare rete > percorsi e fare clic sull'URL.



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



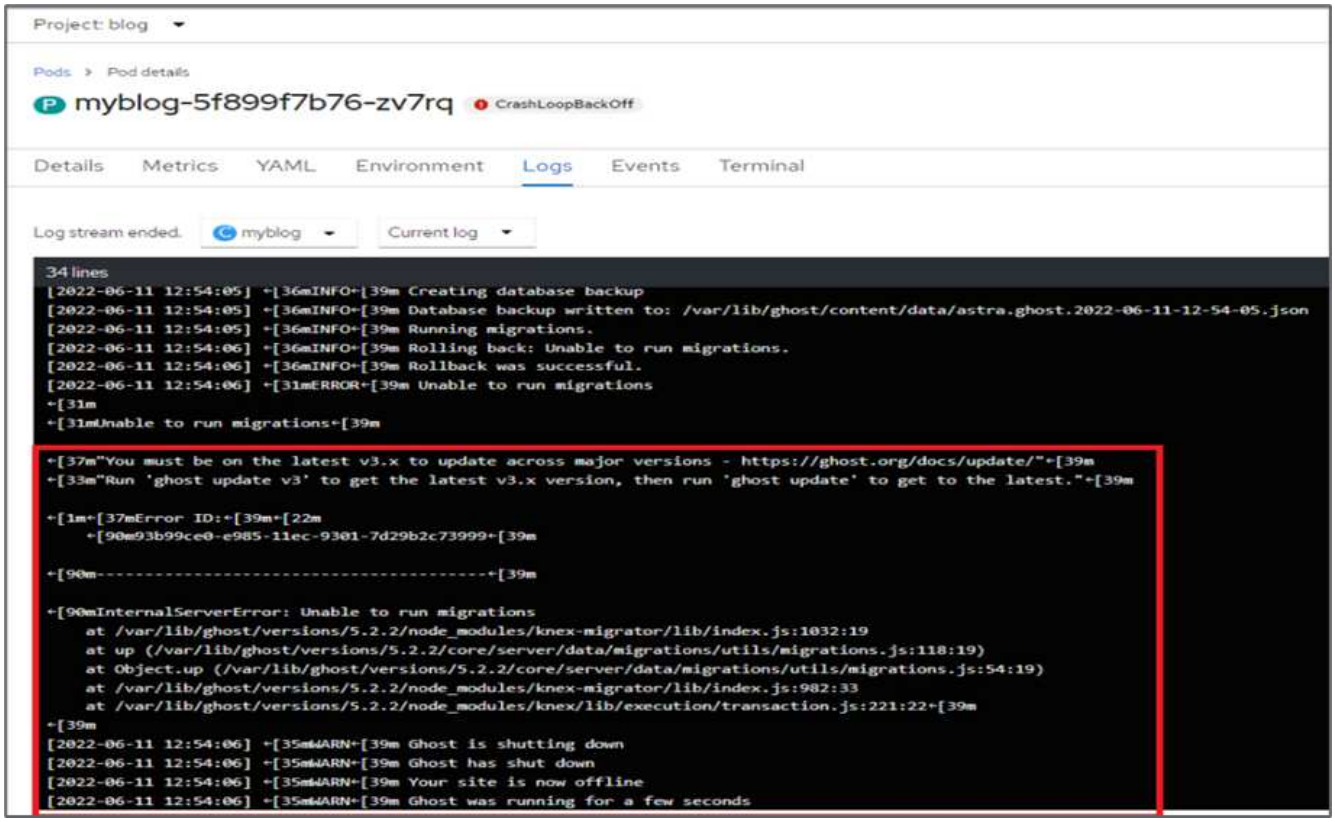
5. Accedere a Astra Control Center. Gestire l'applicazione dalla scheda rilevato, quindi eseguire una copia Snapshot.



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".

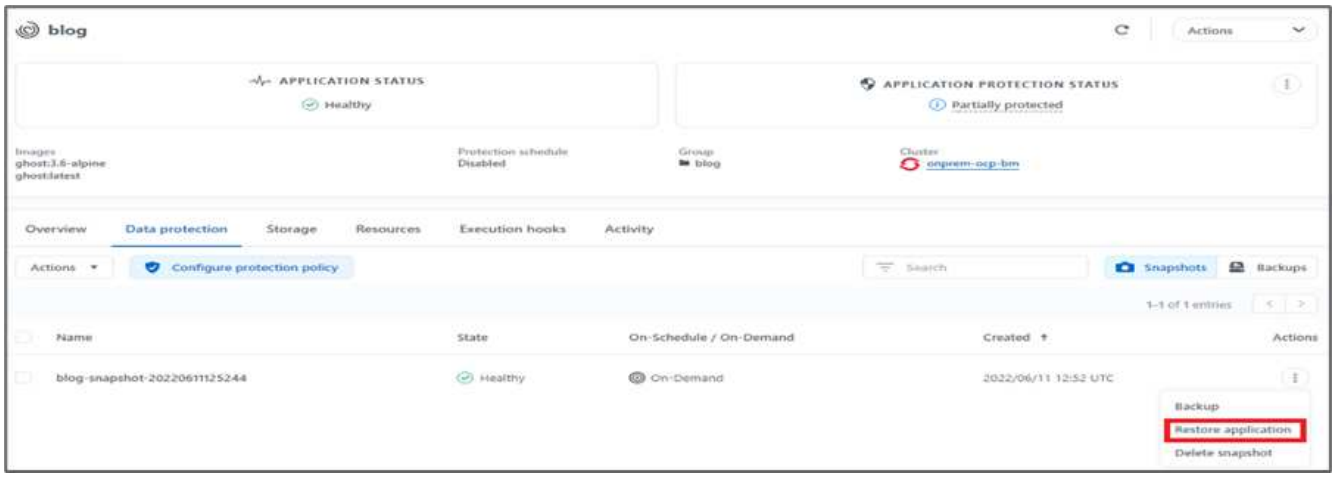
6. Una volta creata correttamente l'istantanea on-Demand, aggiorna l'applicazione alla versione più recente. La versione corrente dell'immagine è `ghost: 3.6-alpine` e la versione di destinazione è `ghost:latest`. Per aggiornare l'applicazione, apportare le modifiche direttamente al repository Git e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

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.

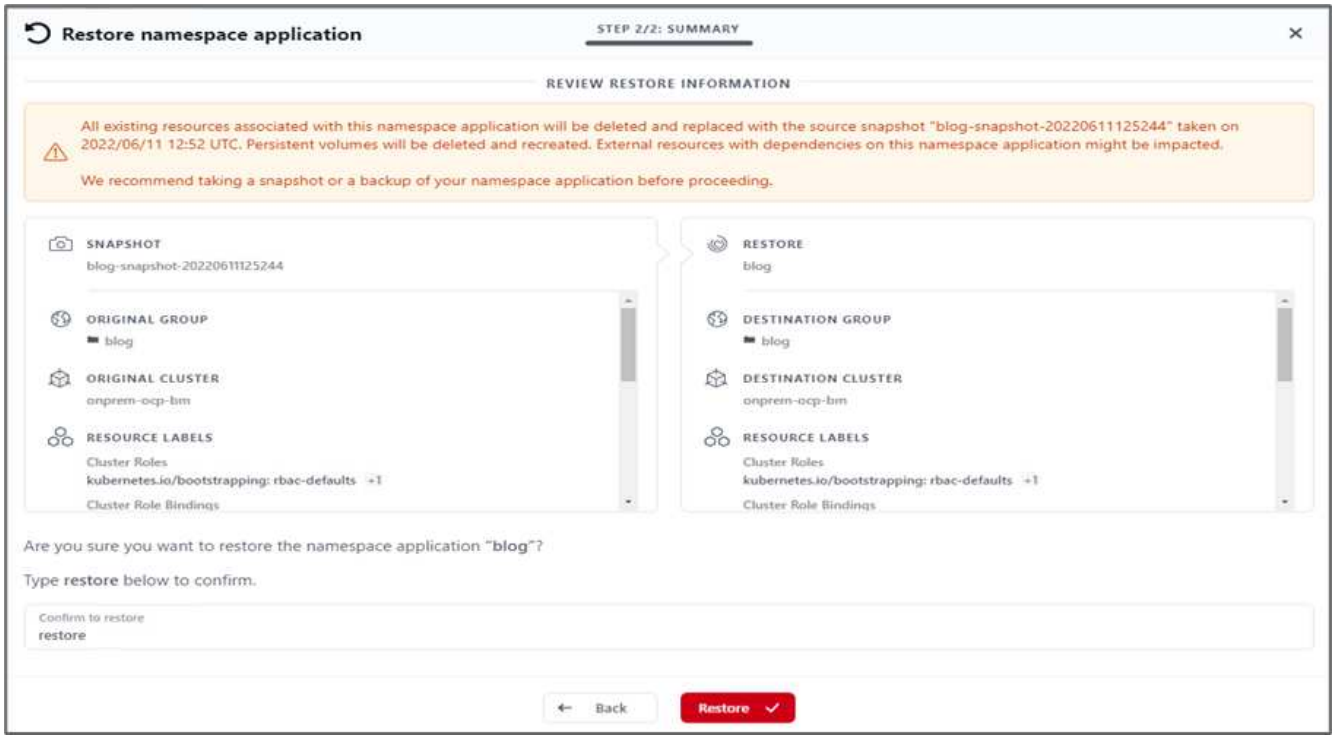


8. Per confermare la non disponibilità del sito del blog, aggiornare l'URL.

9. Ripristinare l'applicazione dallo snapshot.



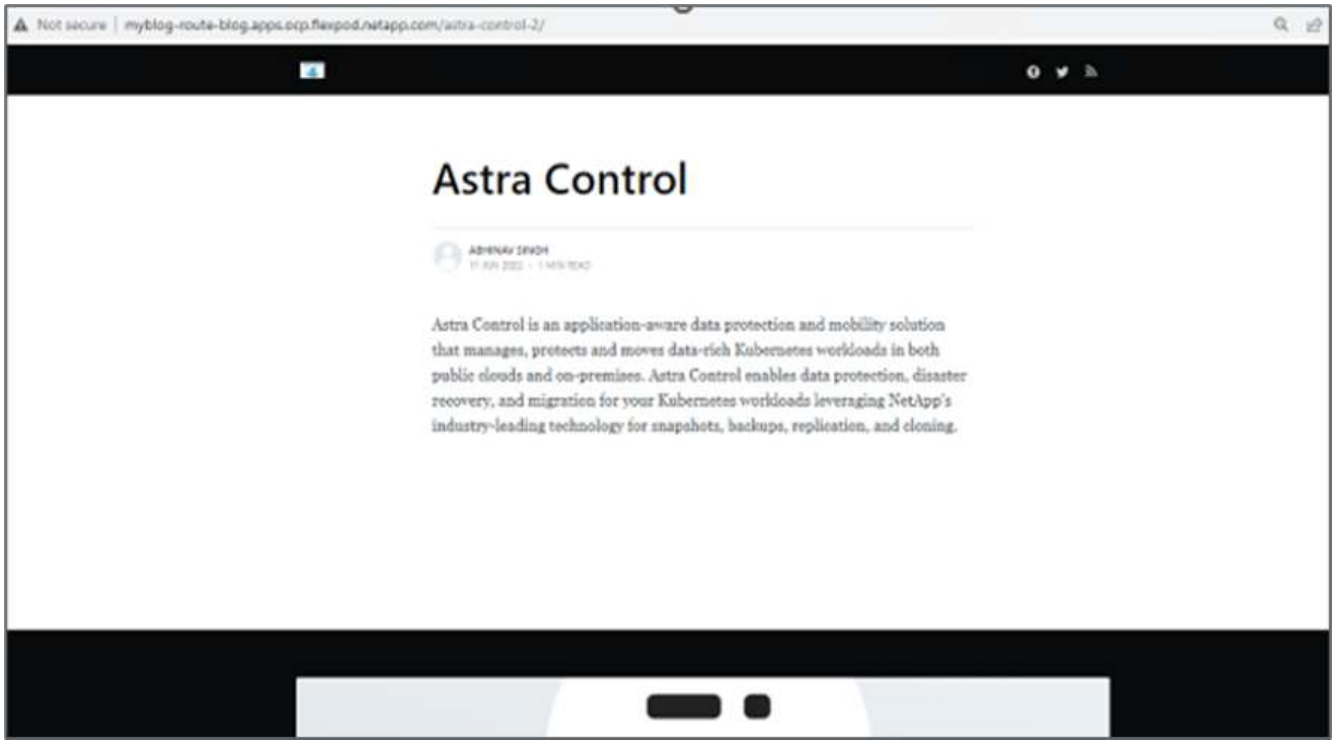
10. L'applicazione viene ripristinata sullo stesso cluster OpenShift.



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.

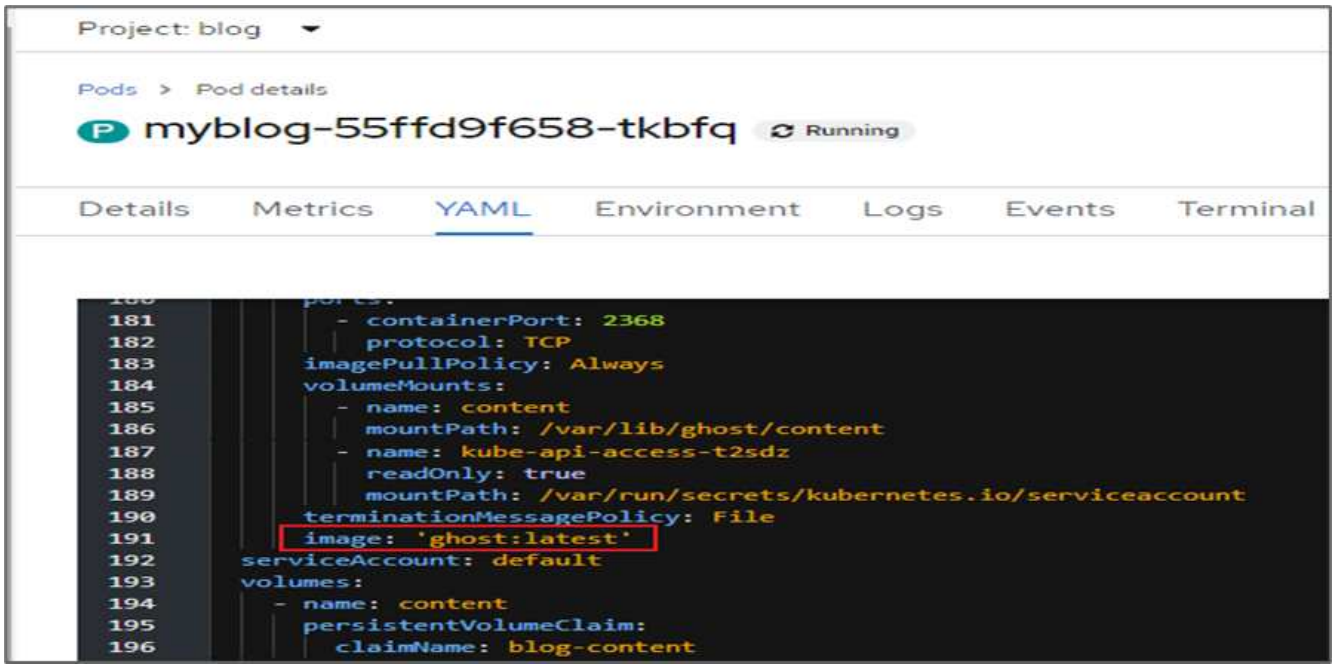


Con l'aiuto di Astra Control Center, un team DevTest può ripristinare con successo un'applicazione del sito del blog e i dati associati utilizzando lo snapshot.

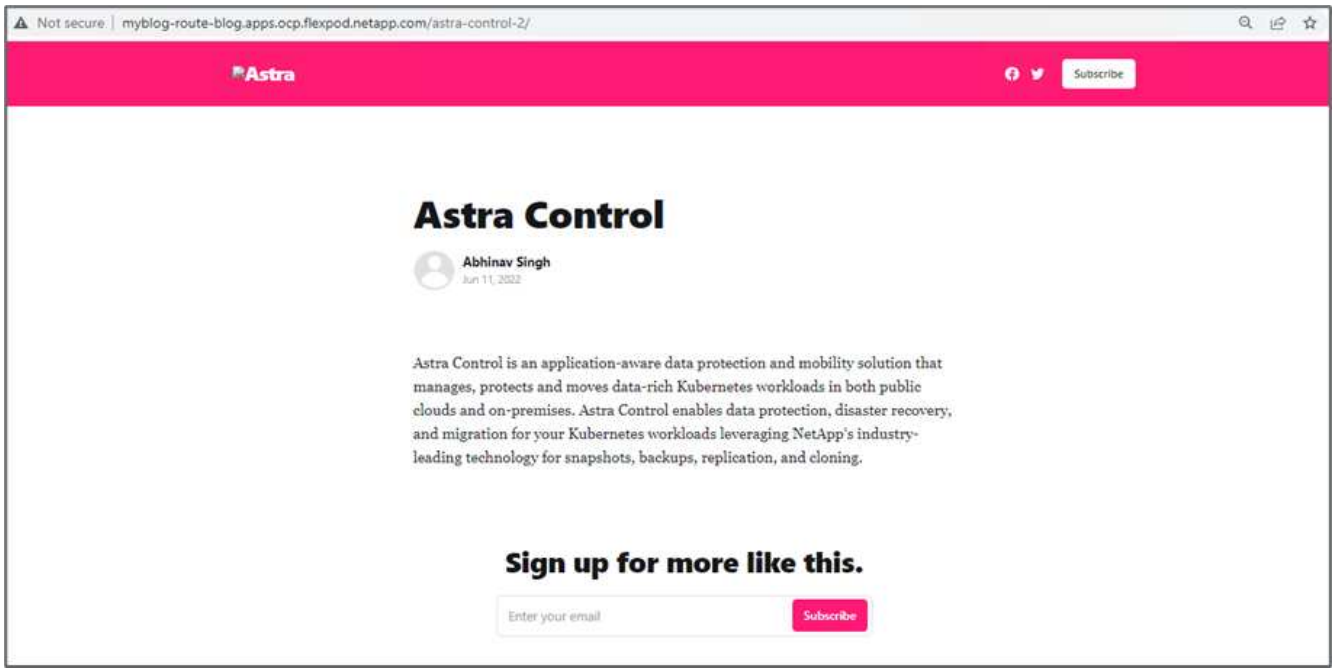
Parte 2

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).

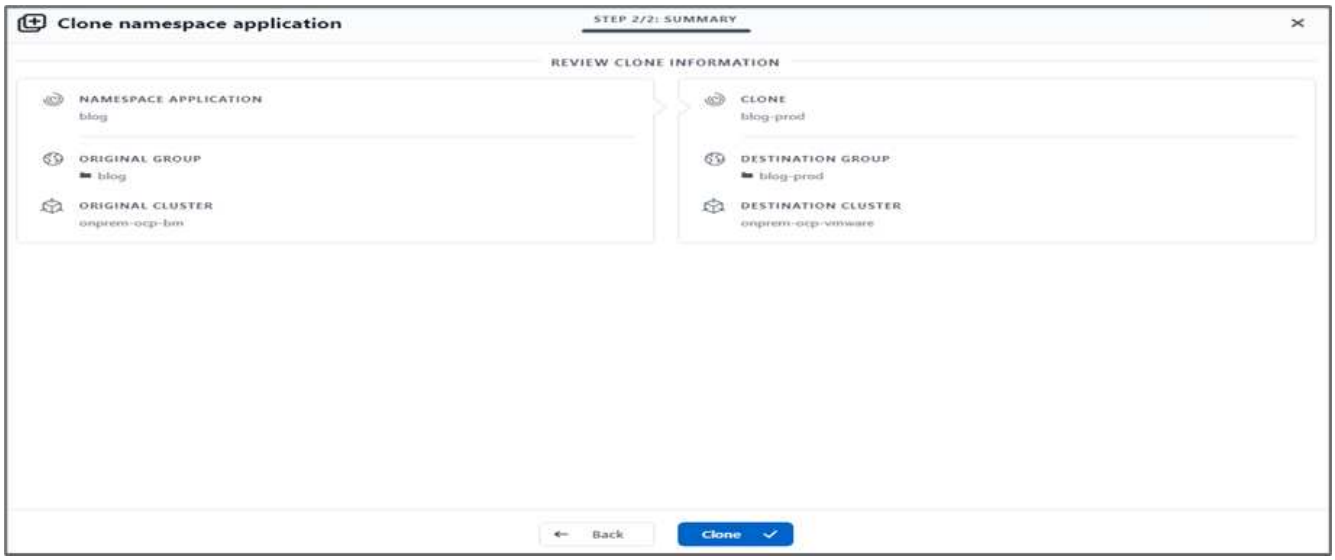
1. Il team DevTest aggiorna inizialmente l'applicazione alla versione supportata (`ghost-4.6-alpine`) prima di eseguire l'aggiornamento alla versione finale (`ghost-latest`) per preparare la produzione it. Quindi, postano un aggiornamento dell'applicazione clonata nel cluster OpenShift di produzione 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.



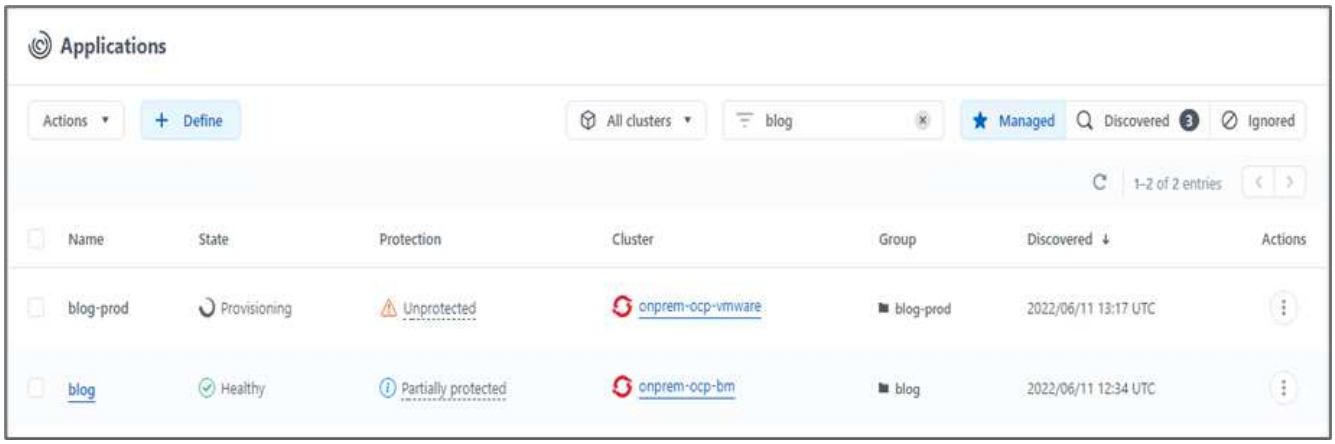
3. Per verificare il nuovo tema, aggiornare il sito del blog.



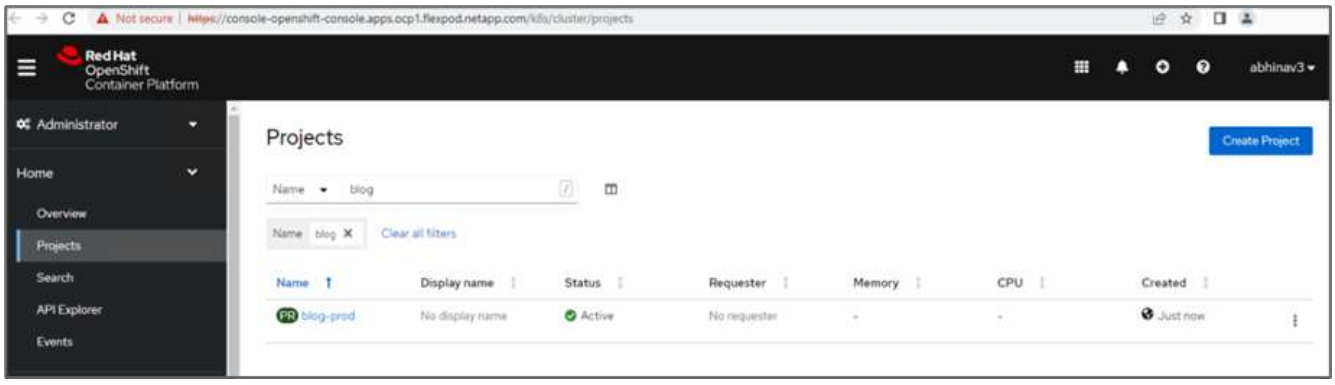
4. Da Astra Control Center, clonare l'applicazione sull'altro cluster OpenShift in produzione in esecuzione su VMware vSphere.



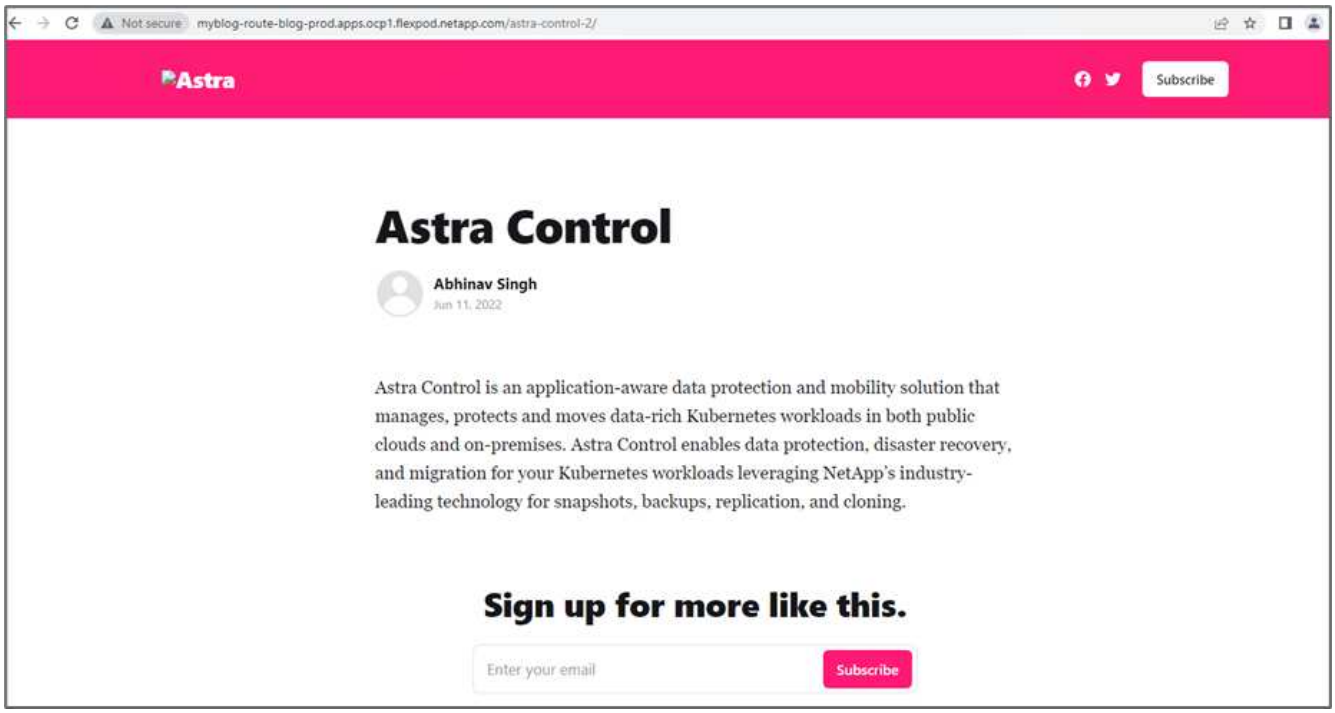
Nel cluster OpenShift di produzione viene ora eseguito il provisioning di un nuovo clone dell'applicazione.



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.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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