Multicloud ibrido NetApp con Red Hat OpenShift

NetApp Solutions

NetApp
April 26, 2024

Sommario

Multicloud ibrido NetApp con carichi di lavoro container Red Hat OpenShift 1
Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift 1
Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift 14
Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift 25
Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift 42

Multicloud ibrido NetApp con carichi di lavoro container Red Hat OpenShift

Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

Panoramica

NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler

ONTAP feature highlights

Storage Administration

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

Security & Compliance

- Fpolicy & Vscan
- Active Directory integration
- LDAP & Kerberos
- Certificate based authentication

NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Proposte a valore delle soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

La maggior parte dei clienti non inizia a costruire ambienti basati su Kubernetes senza alcuna infrastruttura esistente. Forse si tratta di un negozio IT tradizionale che esegue la maggior parte delle applicazioni aziendali su macchine virtuali (ad esempio in ambienti VMware di grandi dimensioni). Quindi, iniziano a creare piccoli ambienti basati su container per soddisfare le esigenze dei moderni team di sviluppo delle applicazioni. Queste iniziative di solito iniziano a poco e iniziano a diventare più pervasive man mano che i team imparano queste nuove tecnologie e competenze, e iniziano a riconoscere i numerosi benefici derivanti dall'adozione di queste tecnologie. La buona notizia per i clienti è che NetApp può soddisfare le esigenze di entrambi gli ambienti. Questo set di soluzioni per il multicloud ibrido con Red Hat OpenShift consentirà ai clienti NetApp di adottare tecnologie e servizi cloud moderni senza dover rivedere l'intera infrastruttura e organizzazione. Sia che le applicazioni e i dati dei clienti siano ospitati on-premise, nel cloud, eseguiti su macchine virtuali o su container, NetApp è in grado di fornire gestione, protezione, sicurezza e portabilità dei dati coerenti. Con queste nuove soluzioni, lo stesso valore offerto da NetApp in ambienti di data center on-premise per decenni sarà disponibile nell'intero orizzonte dei dati dell'azienda, senza richiedere investimenti significativi per il ritool, l'acquisizione di nuove competenze o la creazione di nuovi team. NetApp è in grado di aiutare i clienti a risolvere queste sfide aziendali indipendentemente dalla fase del loro percorso cloud.

Multi-cloud ibrido NetApp con Red Hat OpenShift:

- Offre ai clienti design e pratiche validati che dimostrano i modi migliori per gestire, proteggere, proteggere e migrare i dati e le applicazioni quando utilizzano Red Hat OpenShift con le soluzioni di storage basate su NetApp.
- Presentare le Best practice per i clienti che utilizzano Red Hat OpenShift con lo storage NetApp in ambienti VMware, infrastruttura bare metal o una combinazione di entrambi.
- Dimostra strategie e opzioni per ambienti sia on-premise che cloud, nonché per ambienti ibridi in cui vengono utilizzati entrambi.

Soluzioni supportate di NetApp Hybrid Multibloud per i carichi di lavoro dei container Red Hat OpenShift

La soluzione verifica e convalida la migrazione e la protezione centralizzata dei dati con la piattaforma container OpenShift, l'Advanced Cluster Manager (ACM) OpenShift, NetApp ONTAP, NetApp BlueXP e il centro di controllo NetApp Astra (ACC).

Per questa soluzione, i seguenti scenari sono testati e validati da NetApp. La soluzione è suddivisa in più scenari in base alle seguenti caratteristiche:

- on-premise
- cloud
  - Cluster OpenShift autogestiti e storage NetApp autogestiti
  - Cluster OpenShift gestiti dal provider e storage NetApp gestito dal provider

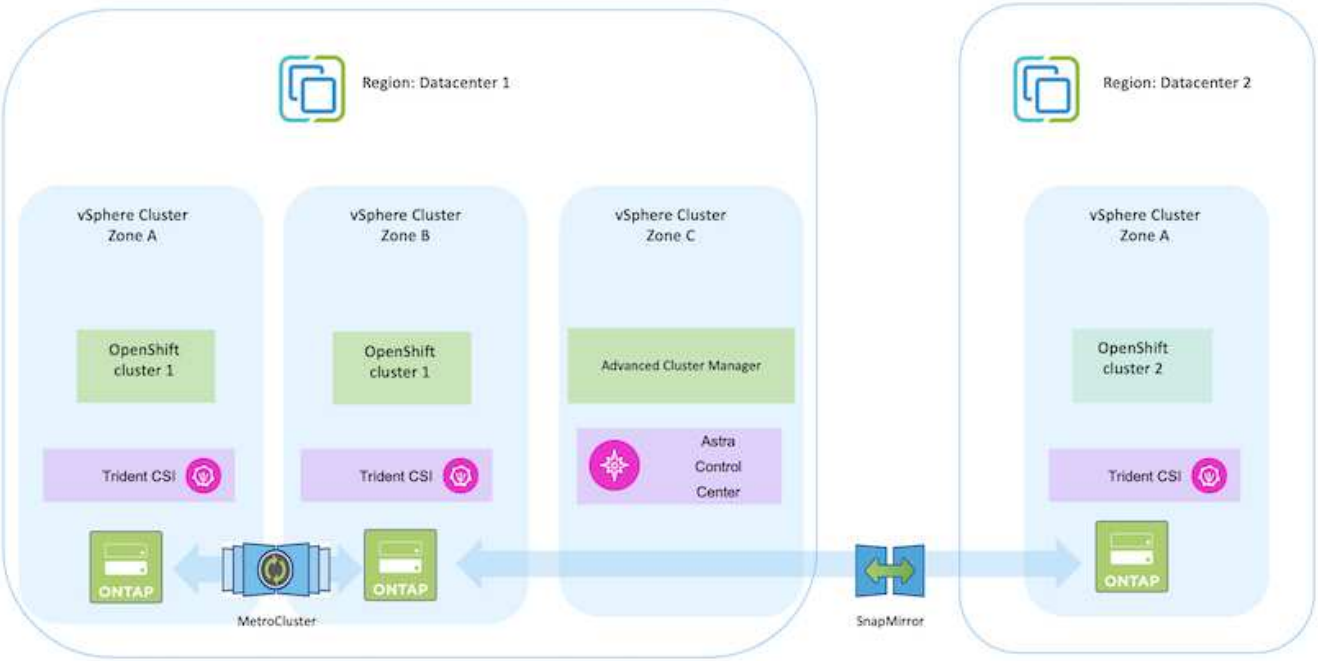
In futuro verranno sviluppate soluzioni e casi di utilizzo aggiuntivi.

Scenario 1: Protezione dei dati e migrazione all'interno dell'ambiente on-premise con ACC

On-premise: Cluster OpenShift autogestiti e storage NetApp autogestiti

- Utilizzando ACC, è possibile creare copie Snapshot, backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

Scenario 1

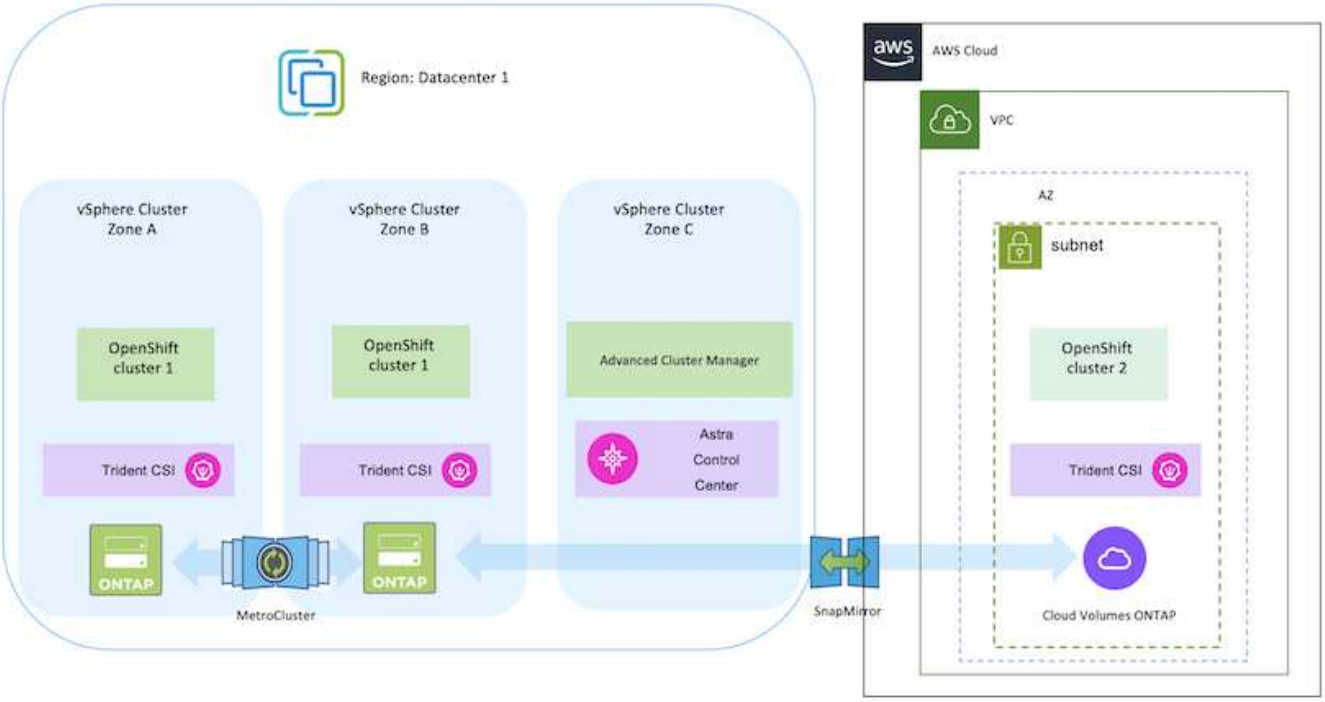


Scenario 2: Data Protection e migrazione dall'ambiente on-premise all'ambiente AWS con ACC

On-premise: Cluster OpenShift autogestiti e storage autogestiti AWS Cloud: Cluster OpenShift autogestiti e storage autogestiti

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

Scenario 2

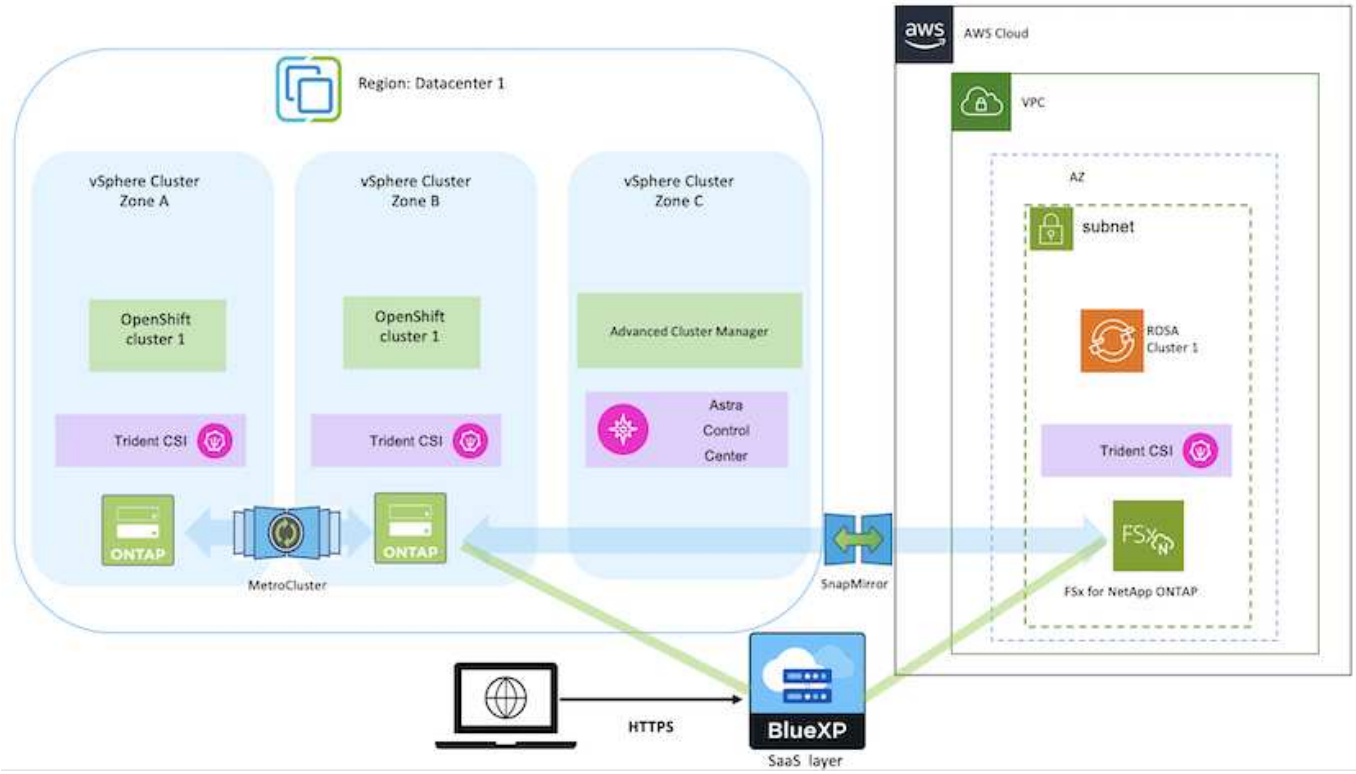


Scenario 3: Data Protection e migrazione dall'ambiente on-premise all'ambiente AWS

On-premise: Cluster OpenShift e storage autogestito AWS Cloud: Cluster OpenShift gestito dal provider (ROSA) e storage gestito dal provider (FSxN)

- Utilizzando BlueXP, eseguire la replica dei volumi persistenti (FSxN).
- Utilizzando OpenShift GitOps, ricreare i metadati dell'applicazione.

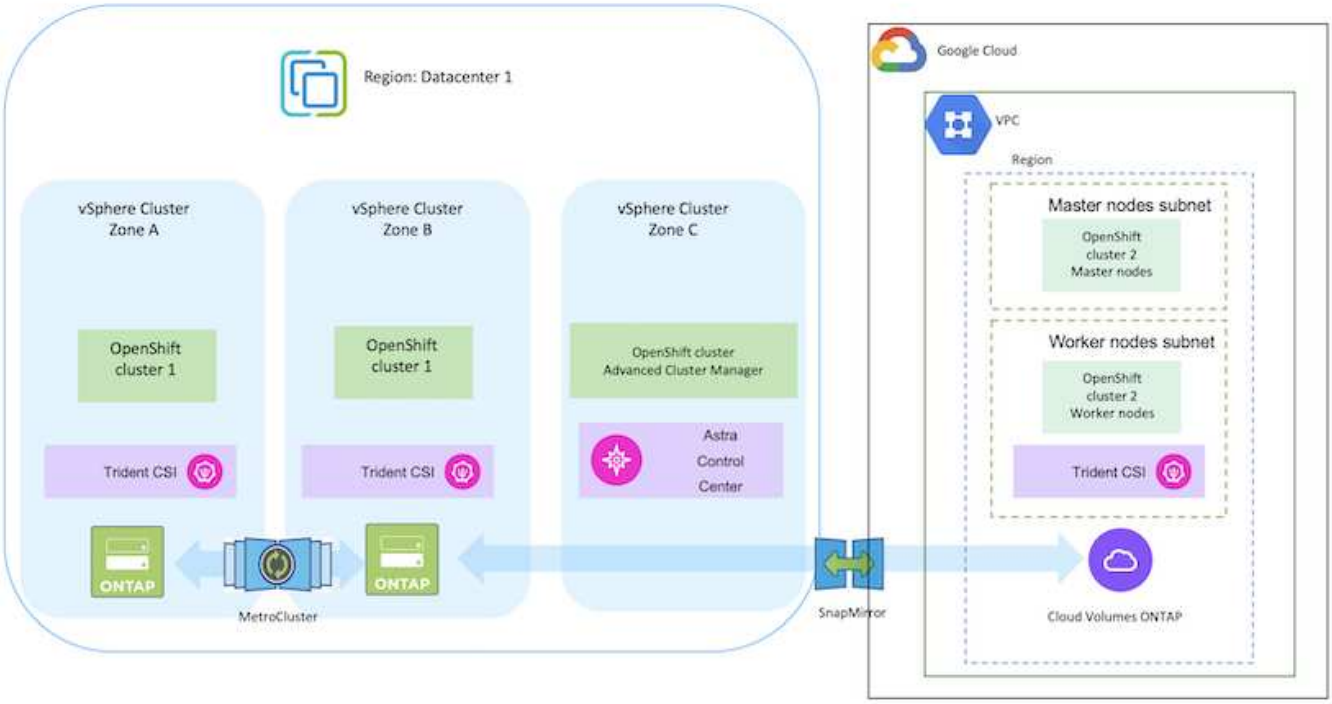
Scenario 3



Scenario 4: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente GCP tramite ACC

On-premise: Cluster OpenShift autogestito e storage autogestito
Google Cloud: Cluster OpenShift autogestito e storage autogestito

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.

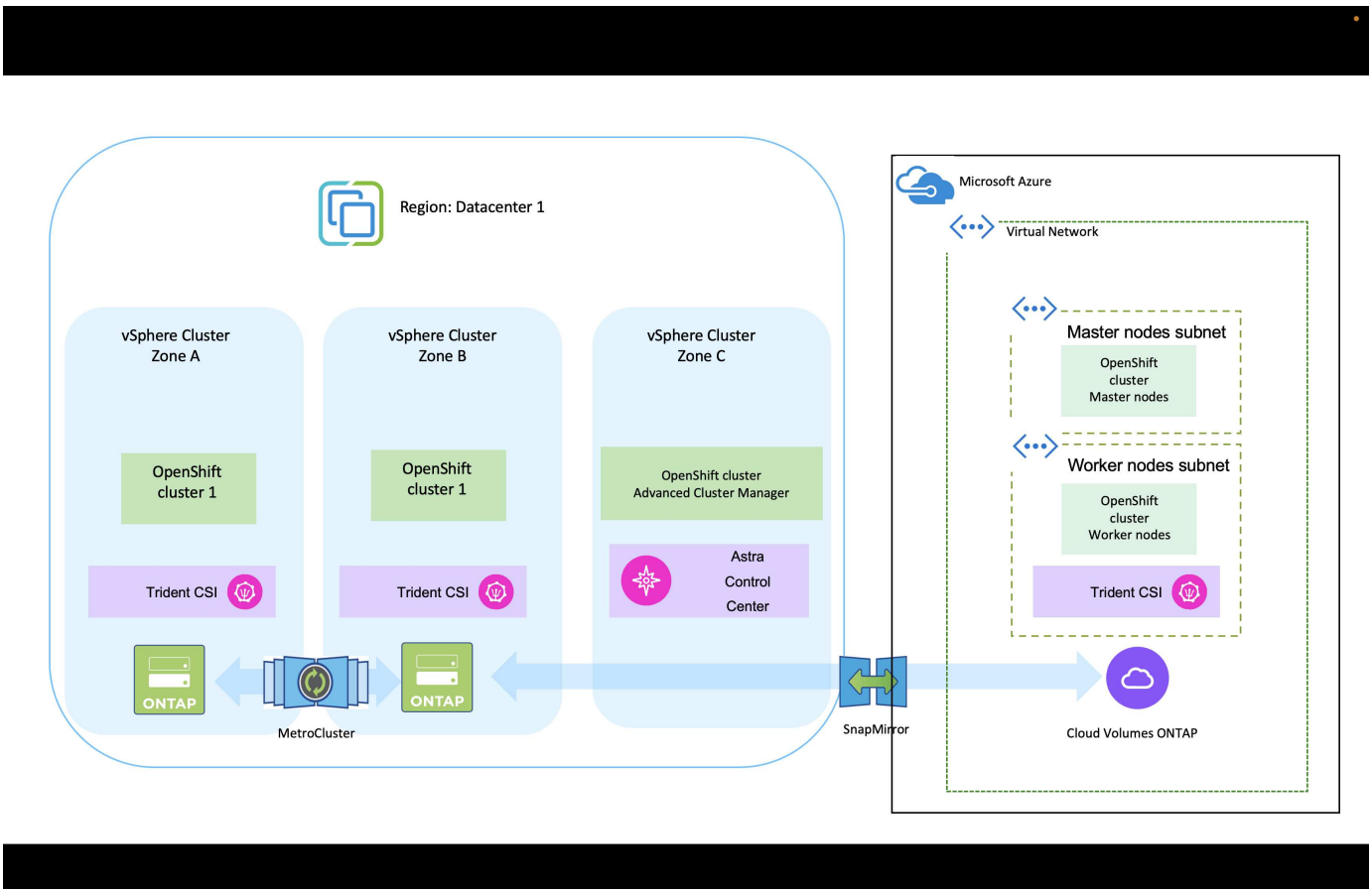


Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster, fare riferimento a. "qui".

Scenario 5: Protezione dei dati e migrazione dall'ambiente on-premise all'ambiente Azure con ACC

On-premise: Cluster OpenShift autogestito e storage autogestito
Azure Cloud: Cluster OpenShift autogestito e storage autogestito

- Utilizzando ACC, eseguire backup e ripristini per la protezione dei dati.
- Utilizzando ACC, eseguire una replica SnapMirror delle applicazioni container.



Per considerazioni sull'utilizzo di ONTAP in una configurazione MetroCluster, fare riferimento a. "qui".

Versioni dei vari componenti utilizzati nella convalida della soluzione

La soluzione testa e convalida la migrazione e la protezione centralizzata dei dati con la piattaforma container OpenShift, l'Advanced Cluster Manager OpenShift, NetApp ONTAP e il centro di controllo NetApp Astra.

Gli scenari 1, 2 e 3 della soluzione sono stati validati utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cluster hub	OpenShift 4.11.34

Clusters di origine e destinazione	OpenShift 4.12.9 on-premise e in AWS
NetApp Astra Trident	Trident Server e Client 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1
AWS FSX per NetApp ONTAP	AZ. Singola

Lo scenario 4 della soluzione è stato validato utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Cluster hub	OpenShift 4.13.13
Clusters di origine e destinazione	OpenShift 4.13.12 On-premise e in Google Cloud
NetApp Astra Trident	Trident Server e Client 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	AZ singolo, nodo singolo, 9.14.0

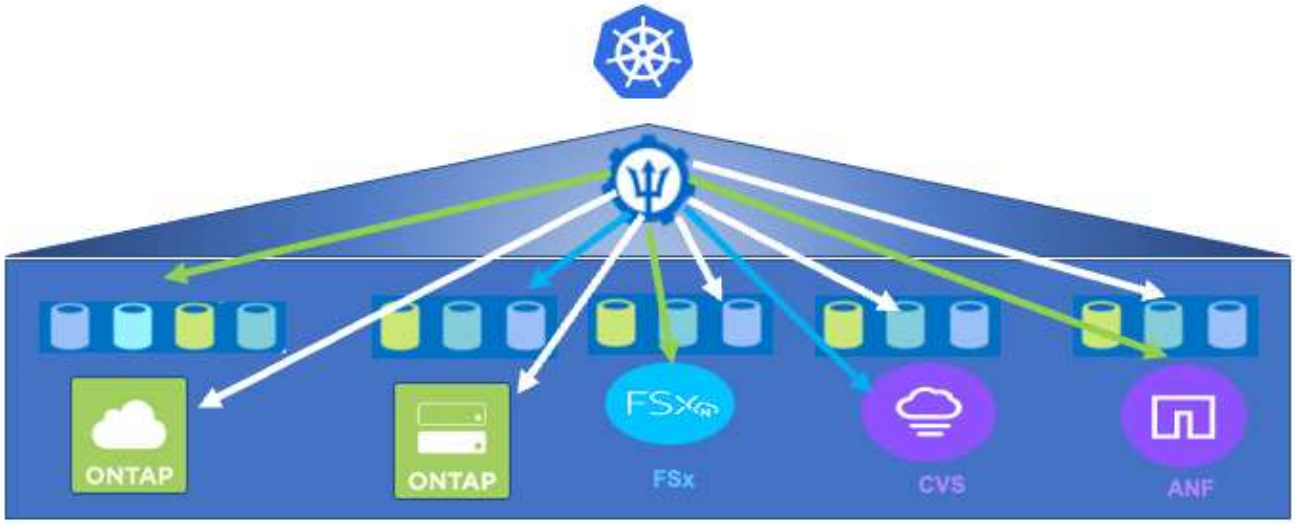
Lo scenario 5 della soluzione è stato validato utilizzando le versioni indicate nella tabella seguente:

Componente	Versione
VMware	VSphere Client versione 8.0.2.00000 VMware ESXi, 8,0.2, 22380479
Clusters di origine e destinazione	OpenShift 4.13.25 On-premise e in Azure
NetApp Astra Trident	Trident Server e Client e Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23,10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	AZ singolo, nodo singolo, 9.14.0

Integrazioni di storage NetApp supportate con Red Hat Open Shift Containers

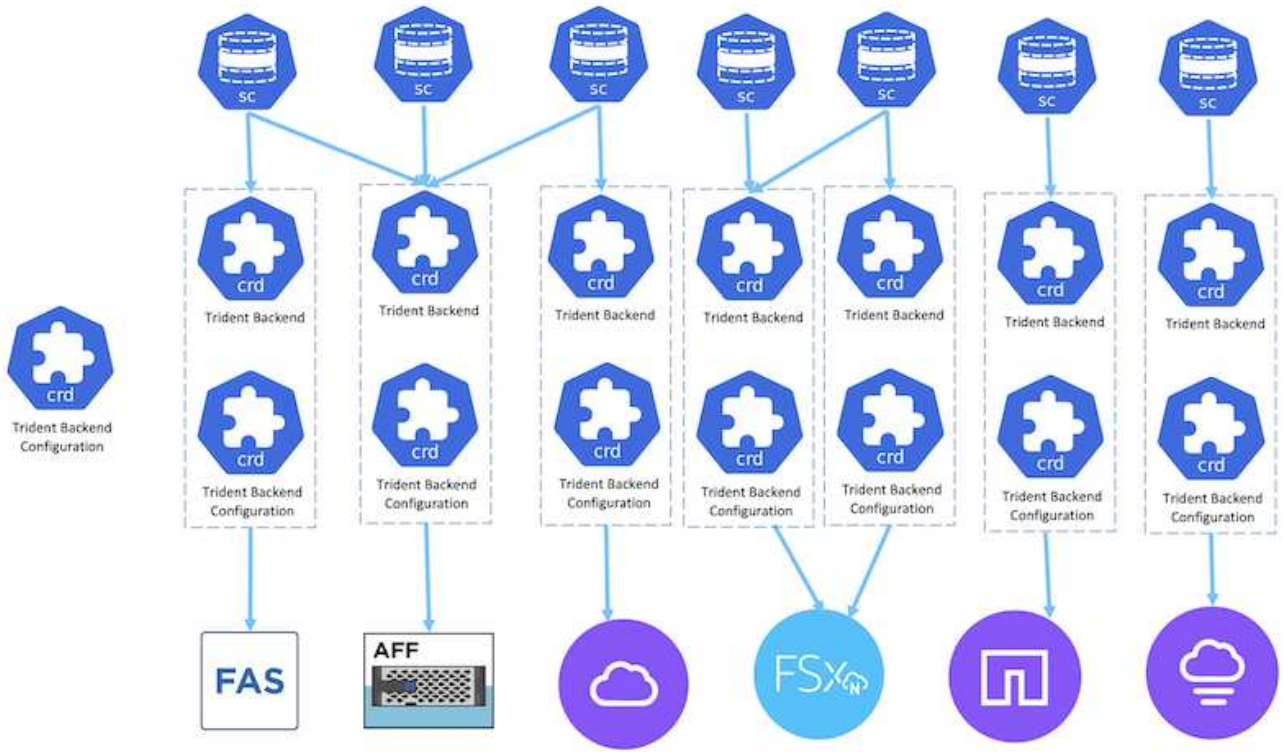
Sia che i container Red Hat Open Shift siano in esecuzione su VMware o negli hyperscaler, NetApp Astra Trident può essere utilizzato come provider CSI per i vari tipi di storage NetApp di back-end supportati.

Il seguente diagramma illustra i vari storage NetApp di back-end che possono essere integrati con i cluster OpenShift utilizzando NetApp Astra Trident.

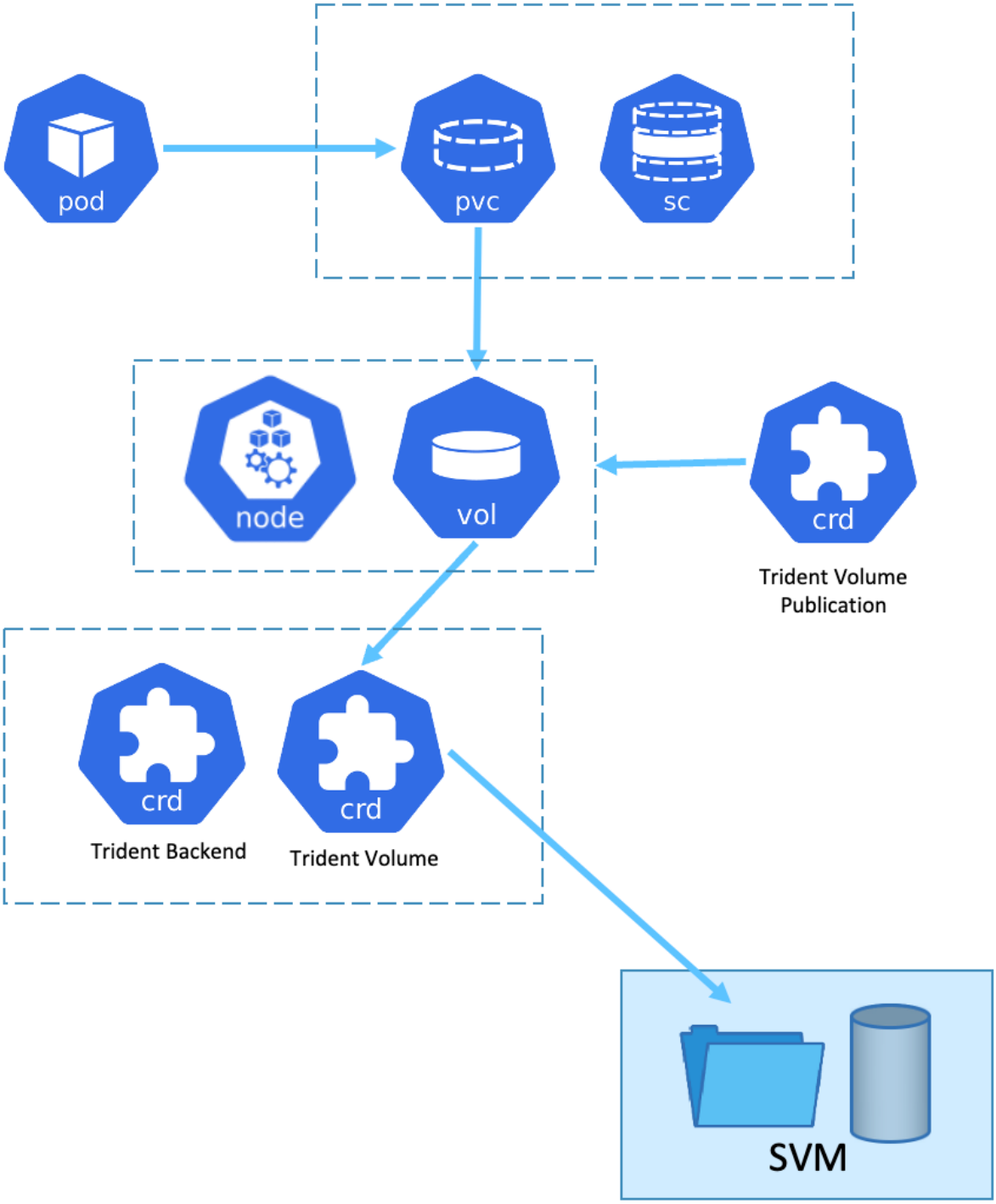


La macchina virtuale per lo storage ONTAP (SVM) offre una multi-tenancy sicura. Un singolo cluster OpenShift può connettersi a una singola SVM o a più SVM o persino a più cluster ONTAP. La classe di storage filtra lo storage back-end in base ai parametri o alle etichette. Gli amministratori dello storage definiscono i parametri per la connessione al sistema di storage utilizzando la configurazione backend trident. Una volta stabilita la connessione, crea il backend trident e popola le informazioni che la classe di storage può filtrare.

Di seguito viene illustrata la relazione tra lo storageclass e il backend.



Il proprietario dell'applicazione richiede un volume persistente utilizzando la classe di storage. La classe di storage filtra lo storage back-end. Di seguito viene illustrata la relazione tra il pod e lo storage back-end.



Opzioni CSI (Container Storage Interface)

Negli ambienti vSphere, i clienti possono scegliere il driver VMware CSI e/o Astra Trident CSI da integrare con ONTAP. Con VMware CSI, i volumi persistenti vengono consumati come dischi SCSI locali, mentre con Trident viene consumato con la rete. Poiché VMware CSI non supporta le modalità di accesso RWX con ONTAP, le applicazioni devono utilizzare Trident CSI se è richiesta la modalità RWX. Con le implementazioni basate su FC, VMware CSI è la soluzione preferita e SnapMirror Business Continuity (SMBC) offre disponibilità elevata a livello di zona.

Supporto di VMware CSI

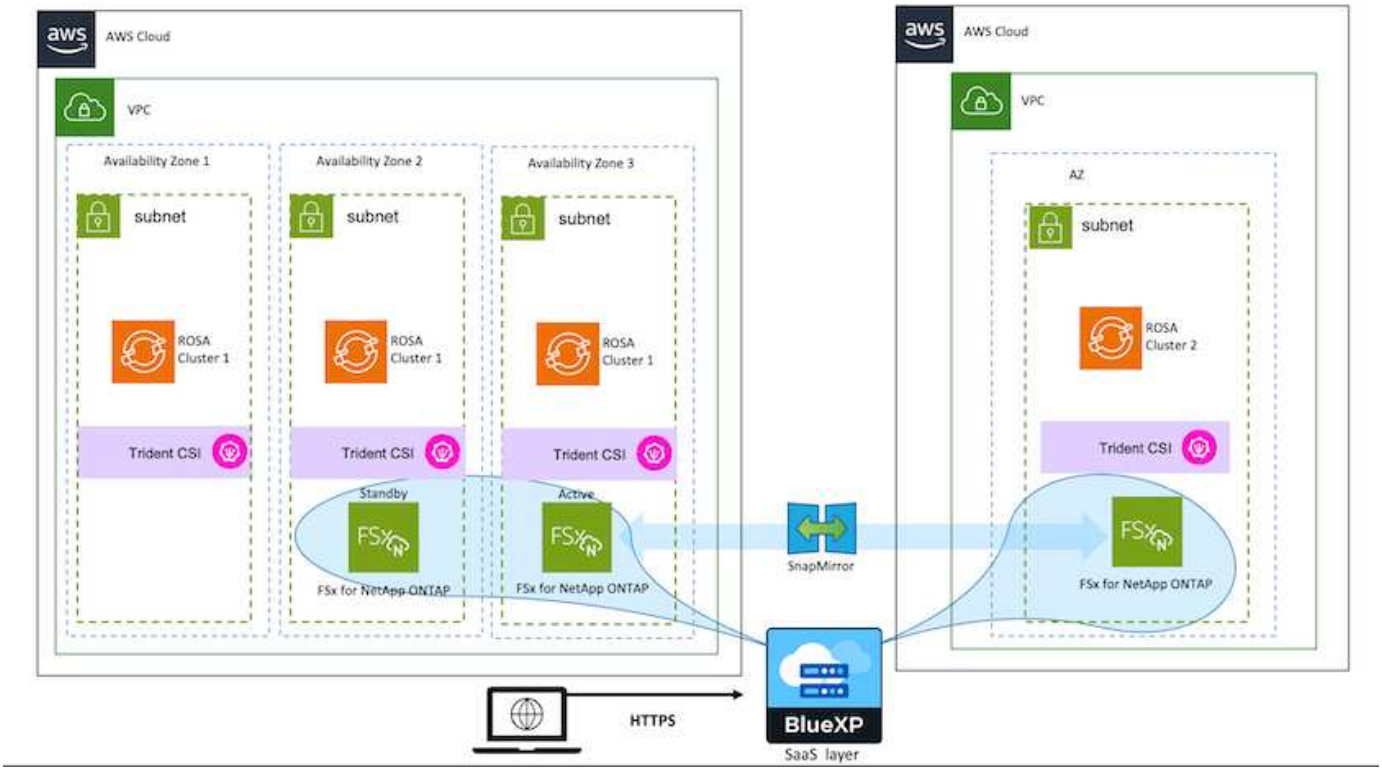
- Datastore basati su core block (FC, FCoE, iSCSI, NVMeoF)
- Archivi dati basati su file di base (NFS v3, v4)
- Datastore vVol (blocco e file)

Trident ha i seguenti driver per supportare ONTAP

- ontap-san (volume dedicato)
- ontap-san-economy (volume condiviso)
- ontap-nas (volume dedicato)
- ontap-nas-economy (volume condiviso)
- ontap-nas-flexgroup (volume dedicato su larga scala)

Per VMware CSI e Astra Trident CSI, ONTAP supporta nconnect, trunking di sessione, kerberos, ecc. per NFS e multipathing, autenticazione chap, ecc. per i protocolli a blocchi.

In AWS, FSX per NetApp ONTAP (FSxN) può essere implementato in una singola zona di disponibilità (AZ) o in più AZ. Per i carichi di lavoro di produzione che richiedono alta disponibilità, multi-AZ offre tolleranza di errore a livello zonale e una cache di lettura NVMe migliore rispetto a AZ singolo. Per ulteriori informazioni, consultare "Linee guida per le performance di AWS".
Per risparmiare sui costi del sito di disaster recovery, è possibile utilizzare un singolo ONTAP AZ FSX.



Per il numero di SVM supportati da FSX ONTAP, fare riferimento a. "Gestione della macchina virtuale per lo storage FSX ONTAP"

Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

Panoramica

NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler

ONTAP feature highlights

Storage Administration

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

Security & Compliance

- Fpolicy & Vscan
- Active Directory integration
- LDAP & Kerberos
- Certificate based authentication

NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware

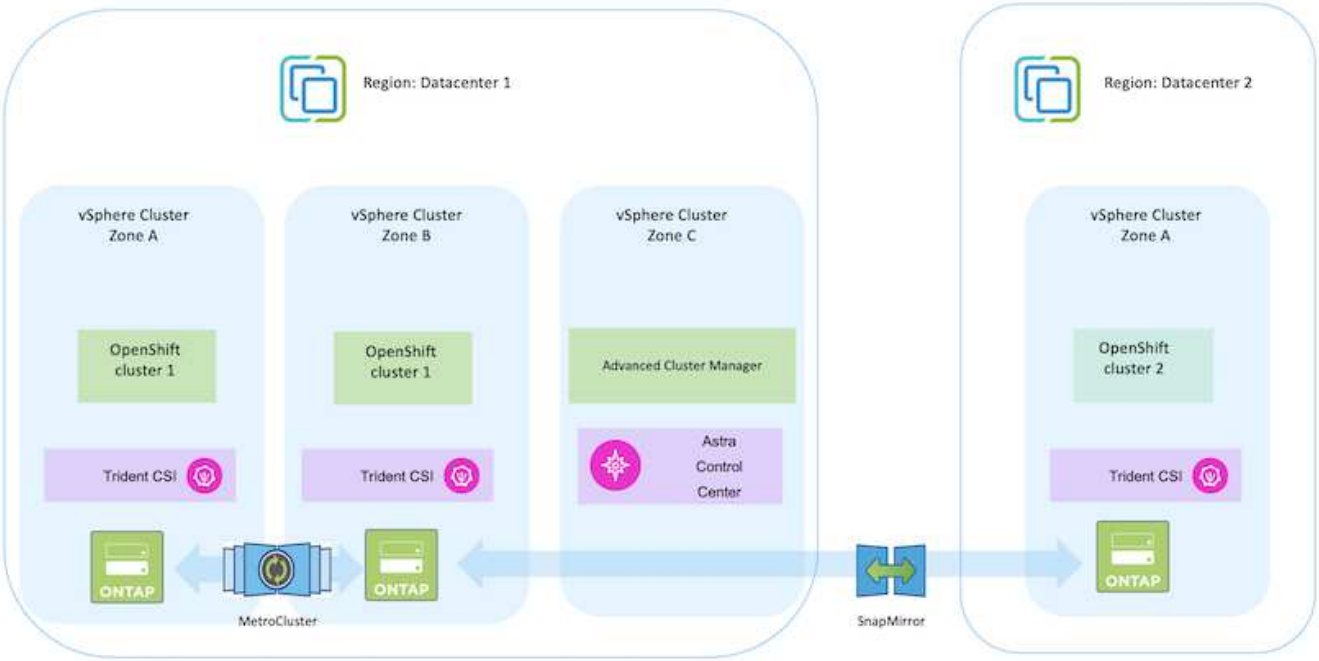
Se i clienti hanno la necessità di eseguire le loro moderne applicazioni containerizzate su un'infrastruttura nei propri data center privati, possono farlo. Devono pianificare e implementare la piattaforma container Red Hat OpenShift (OCP) per un ambiente pronto per la produzione di successo per l'implementazione dei carichi di lavoro dei container. I cluster OCP possono essere implementati su VMware o bare metal.

Lo storage NetApp ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container. Astra Trident funge da provider di storage dinamico per consumare storage ONTAP persistente per le applicazioni stateful dei clienti. Astra Control Center può essere utilizzato per orchestrare i numerosi requisiti di gestione dei dati delle applicazioni stateful come protezione dei dati, migrazione e business continuity.

Con VMware vSphere, i tool NetApp ONTAP forniscono un plug-in vCenter che può essere utilizzato per il provisioning dei datastore. Applica i tag e usali con OpenShift per memorizzare la configurazione del nodo e i dati. Lo storage basato su NVMe offre latenza inferiore e performance elevate.

Questa soluzione fornisce dettagli sulla protezione dei dati e sulla migrazione dei carichi di lavoro dei container utilizzando Astra Control Center. Per questa soluzione, i carichi di lavoro dei container vengono implementati nei cluster Red Hat OpenShift su vSphere all'interno dell'ambiente on-premise. NOTA: In futuro forniremo una soluzione per i carichi di lavoro container sui cluster OpenShift su bare metal.

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift con Astra Control Center

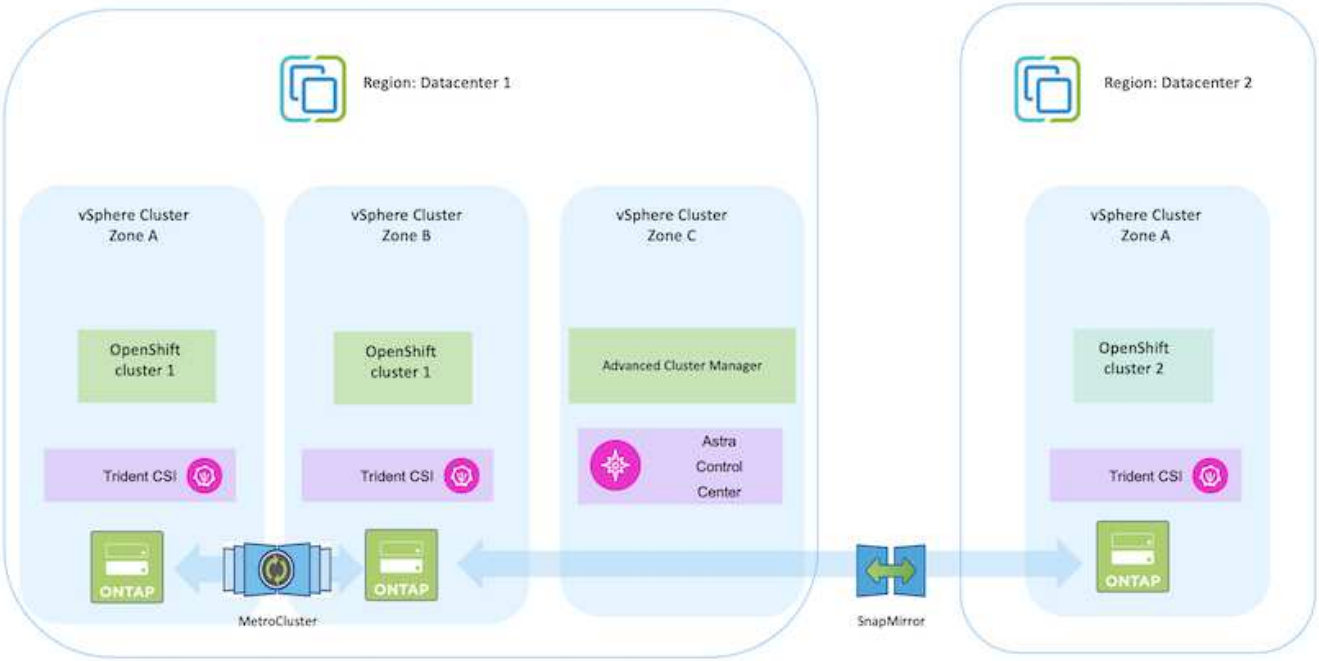


Implementare e configurare la piattaforma container Red Hat OpenShift su VMware

In questa sezione viene descritto un workflow di alto livello che illustra come configurare e gestire i cluster OpenShift e gestire le applicazioni stateful su di essi. Mostra l'utilizzo degli storage array NetApp ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

> Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Di seguito è riportato un diagramma che illustra i cluster implementati su VMware in un data center.



Il processo di installazione può essere suddiviso nei seguenti passaggi:

Implementare e configurare una macchina virtuale CentOS

- Viene implementato nell'ambiente VMware vSphere.
- Questa macchina virtuale viene utilizzata per l'implementazione di alcuni componenti come NetApp Astra Trident e NetApp Astra Control Center per la soluzione.
- Un utente root viene configurato su questa macchina virtuale durante l'installazione.

Implementare e configurare un cluster OpenShift Container Platform su VMware vSphere (Hub Cluster)

Fare riferimento alle istruzioni del "Implementazione assistita" Metodo per implementare un cluster OCP.

> Tenere presente quanto segue: - Creare una chiave pubblica e privata ssh da fornire all'installatore. Queste chiavi verranno utilizzate per accedere ai nodi master e worker, se necessario. - Scaricare il programma di installazione dal programma di installazione assistito. Questo programma viene utilizzato per avviare le macchine virtuali create nell'ambiente VMware vSphere per i nodi master e worker. Le macchine virtuali devono avere i requisiti minimi di CPU, memoria e disco rigido. (Fare riferimento ai comandi di creazione della macchina virtuale su "questo" Per i nodi master e worker che forniscono queste informazioni) - diskUID deve essere abilitato su tutte le macchine virtuali. - Creare un minimo di 3 nodi per master e 3 nodi per worker. Una volta rilevati dal programma di installazione, attivare il pulsante di attivazione/disattivazione dell'integrazione VMware vSphere.

Installare Advanced Cluster Management sul cluster Hub

Viene installato utilizzando Advanced Cluster Management Operator sul cluster Hub. Fare riferimento alle istruzioni "qui".

Installare un registro Red Hat Quay interno sul cluster Hub.

- Per inviare l'immagine Astra è necessario un registro interno. Un registro interno Quay viene installato utilizzando l'operatore nel cluster Hub.
- Fare riferimento alle istruzioni "qui"

Installare due cluster OCP aggiuntivi (origine e destinazione)

- I cluster aggiuntivi possono essere implementati utilizzando ACM sul cluster Hub.
- Fare riferimento alle istruzioni "qui".

Configurare lo storage NetApp ONTAP

- Installare un cluster ONTAP con connettività alle VM OCP nell'ambiente VMware.
- Creare una SVM.
- Configurare i dati NAS per accedere allo storage in SVM.

Installare NetApp Trident sui cluster OCP

- Installare NetApp Trident su tutti e tre i cluster: Hub, origine e destinazione
- Fare riferimento alle istruzioni "qui".
- Creare un backend di storage per ontap-nas .
- Creare una classe di storage per ontap-nas.
- Fare riferimento alle istruzioni "qui".

Installare NetApp Astra Control Center

- NetApp Astra Control Center viene installato utilizzando Astra Operator sul cluster Hub.
- Fare riferimento alle istruzioni "qui".

Punti da ricordare: * Scarica l'immagine di NetApp Astra Control Center dal sito di supporto. * Inserire l'immagine in un registro interno. * Fare riferimento alle istruzioni qui.

Implementare un'applicazione sul cluster di origine

Utilizza OpenShift GitOps per implementare un'applicazione. (es. Postgres, Ghost)

Aggiungere i cluster di origine e destinazione in Astra Control Center.

Dopo aver aggiunto un cluster alla gestione di Astra Control, è possibile installare le applicazioni sul cluster (all'esterno di Astra Control) e quindi passare alla pagina delle applicazioni in Astra Control per definire le applicazioni e le relative risorse. Fare riferimento a. "Inizia a gestire le app di Astra Control Center".

Il passaggio successivo consiste nell'utilizzare Astra Control Center per la protezione dei dati e la migrazione dei dati dal cluster di origine a quello di destinazione.

Protezione dei dati con Astra

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su container Red Hat OpenShift eseguite su VMware vSphere utilizzando Astra Control Center (ACC).

Mentre gli utenti intraprendono il percorso di modernizzazione delle proprie applicazioni con Red Hat OpenShift, è necessario adottare una strategia di protezione dei dati per proteggerli da cancellazioni accidentali o altri errori umani. Spesso, per proteggere i propri dati da un diaster, è necessaria anche una strategia di protezione a scopo normativo o di compliance.

I requisiti di protezione dei dati variano dal ritorno a una copia point-in-time al failover automatico a un dominio di errore diverso senza alcun intervento umano. Molti clienti scelgono ONTAP come piattaforma di storage preferita per le loro applicazioni Kubernetes per le sue ricche funzionalità come multi-tenancy, multi-protocollo, offerte di capacità e performance elevate, replica e caching per ubicazioni multi-sito, sicurezza e flessibilità.

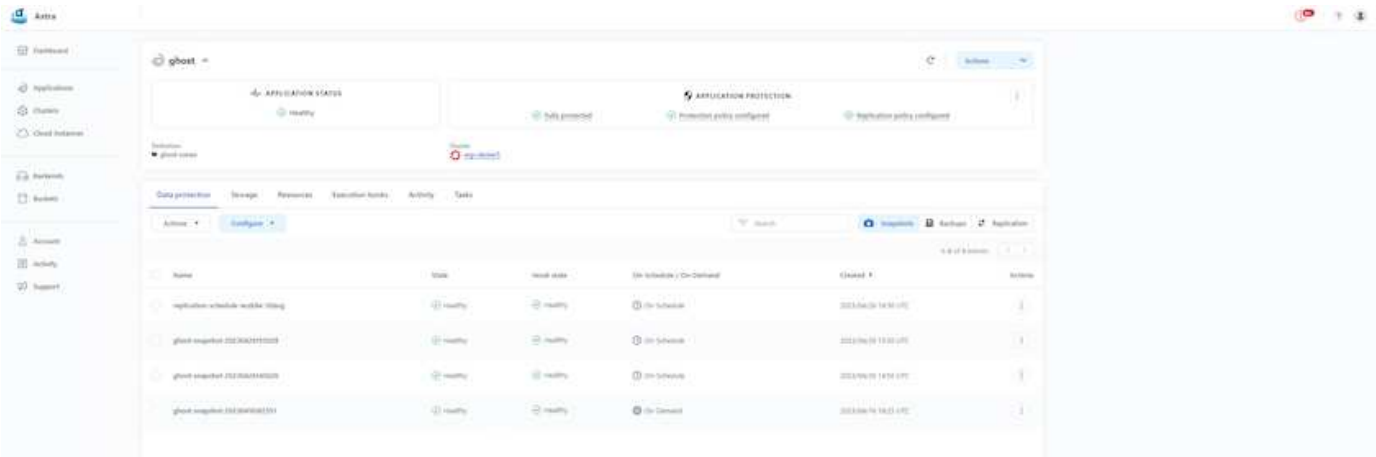
La protezione dei dati in ONTAP può essere ottenuta utilizzando ad-hoc o policy controllate - **Snapshot** - **backup e ripristino**

Sia le copie Snapshot che i backup proteggono i seguenti tipi di dati: - **I metadati dell'applicazione che rappresentano lo stato dell'applicazione** - **eventuali volumi di dati persistenti associati all'applicazione** - **eventuali artefatti delle risorse appartenenti all'applicazione**

Snapshot con ACC

È possibile acquisire una copia point-in-time dei dati utilizzando Snapshot con ACC. La policy di protezione definisce il numero di copie Snapshot da conservare. L'opzione di pianificazione minima disponibile è oraria. Le copie Snapshot manuali e on-demand possono essere eseguite in qualsiasi momento e a intervalli più brevi rispetto alle copie Snapshot pianificate. Le copie Snapshot vengono memorizzate sullo stesso volume sottoposto a provisioning dell'applicazione.

Configurazione di Snapshot con ACC

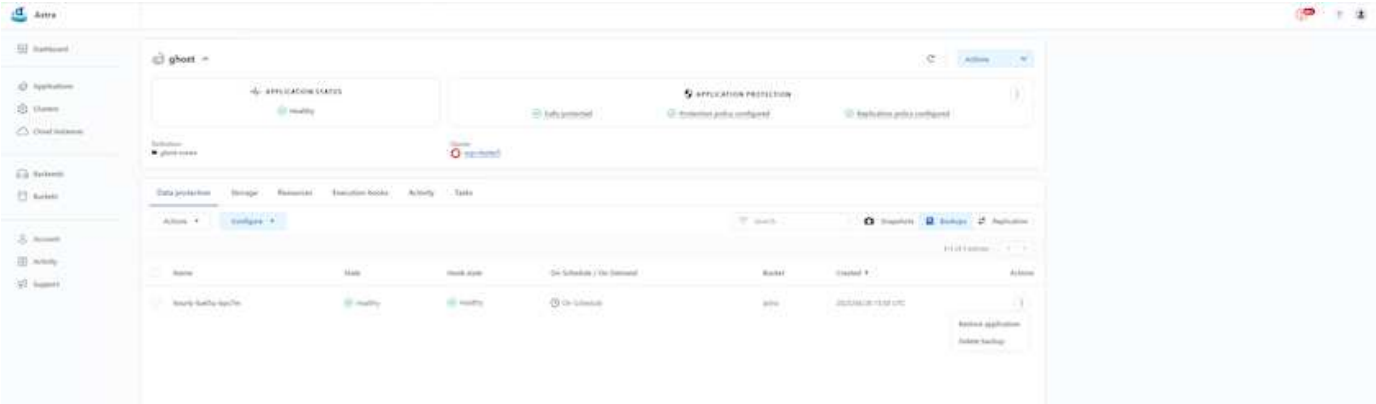


Backup e ripristino con ACC

Un backup si basa su un'istantanea. ACC può eseguire copie Snapshot utilizzando CSI ed eseguire il backup utilizzando la copia Snapshot point-in-time. Il backup viene memorizzato in un archivio di oggetti esterno (qualsiasi compatibile con s3, incluso ONTAP S3, in una posizione diversa). È possibile configurare i criteri di protezione per i backup pianificati e il numero di versioni di backup da conservare. L'RPO minimo è di un'ora.

Ripristino di un'applicazione da un backup mediante ACC

ACC ripristina l'applicazione dal bucket S3 in cui sono memorizzati i backup.



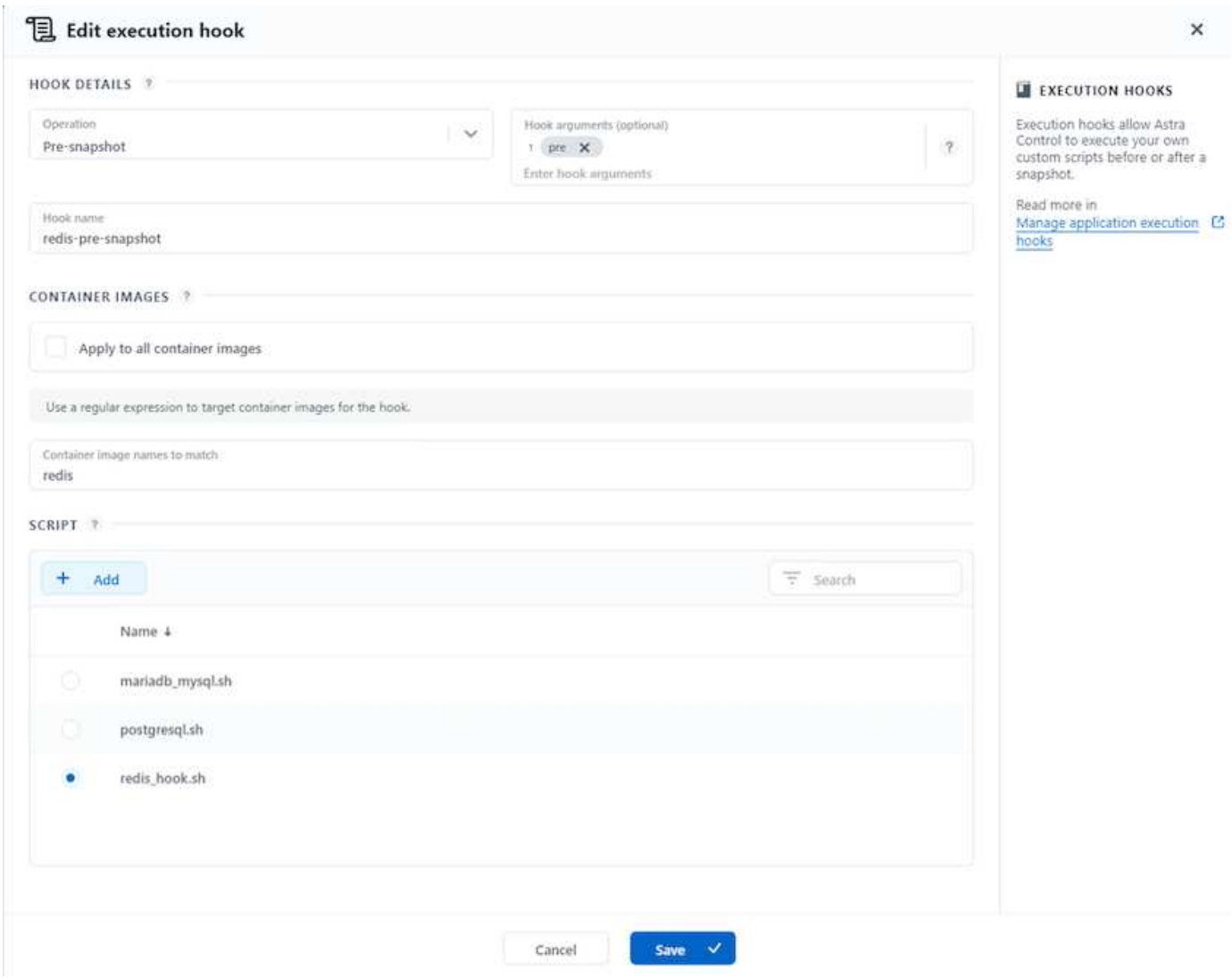
Hook di esecuzione specifici dell'applicazione

Inoltre, è possibile configurare gli hook di esecuzione per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Anche se sono disponibili funzionalità di protezione dei dati a livello di array di storage, spesso sono necessari ulteriori passaggi per rendere coerenti backup e ripristini. I passaggi aggiuntivi specifici dell'applicazione potrebbero essere: - Prima o dopo la creazione di una copia Snapshot. - prima o dopo la creazione di un backup. - Dopo il ripristino da una copia Snapshot o da un backup.

Astra Control può eseguire questi passaggi specifici dell'applicazione codificati come script personalizzati chiamati uncini di esecuzione.

"Progetto NetApp Verda GitHub" fornisce hook di esecuzione per le applicazioni native del cloud più diffuse per rendere la protezione delle applicazioni semplice, robusta e facile da orchestrare. Se si dispone di informazioni sufficienti per un'applicazione non presente nel repository, è possibile contribuire al progetto.

Esempio di gancio di esecuzione per pre-Snapshot di un'applicazione redis.



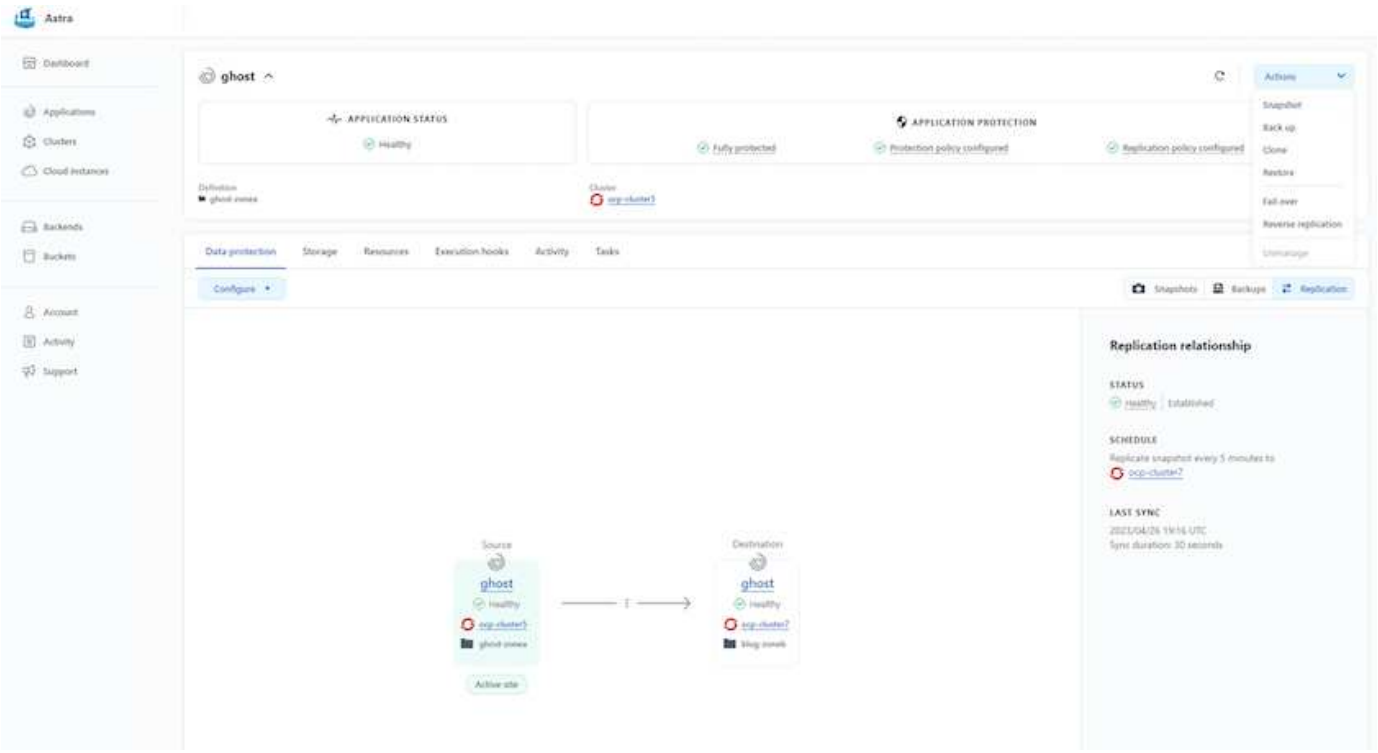
Replica con ACC

Per la protezione regionale o per una soluzione RPO e RTO bassa, un'applicazione può essere replicata in un'altra istanza di Kubernetes in esecuzione in un sito diverso, preferibilmente in un'altra regione. ACC utilizza SnapMirror asincrono ONTAP con RPO in soli 5 minuti. La replica viene eseguita replicando in ONTAP, quindi un failover crea le risorse Kubernetes nel cluster di destinazione.

> Tenere presente che la replica è diversa dal backup e ripristino, dove il backup viene eseguito in S3 e il ripristino viene eseguito da S3. Fare riferimento al xref:./rhhc/ here per ulteriori dettagli sulle differenze tra i due tipi di protezione dei dati.

Fare riferimento a. "qui" Per le istruzioni di installazione di SnapMirror.

SnapMirror con ACC



i driver di storage san-economy e nas-economy non supportano la funzione di replica. Fare riferimento a. "qui" per ulteriori dettagli.

Video dimostrativo:

"Video dimostrativo del disaster recovery con Astra Control Center"

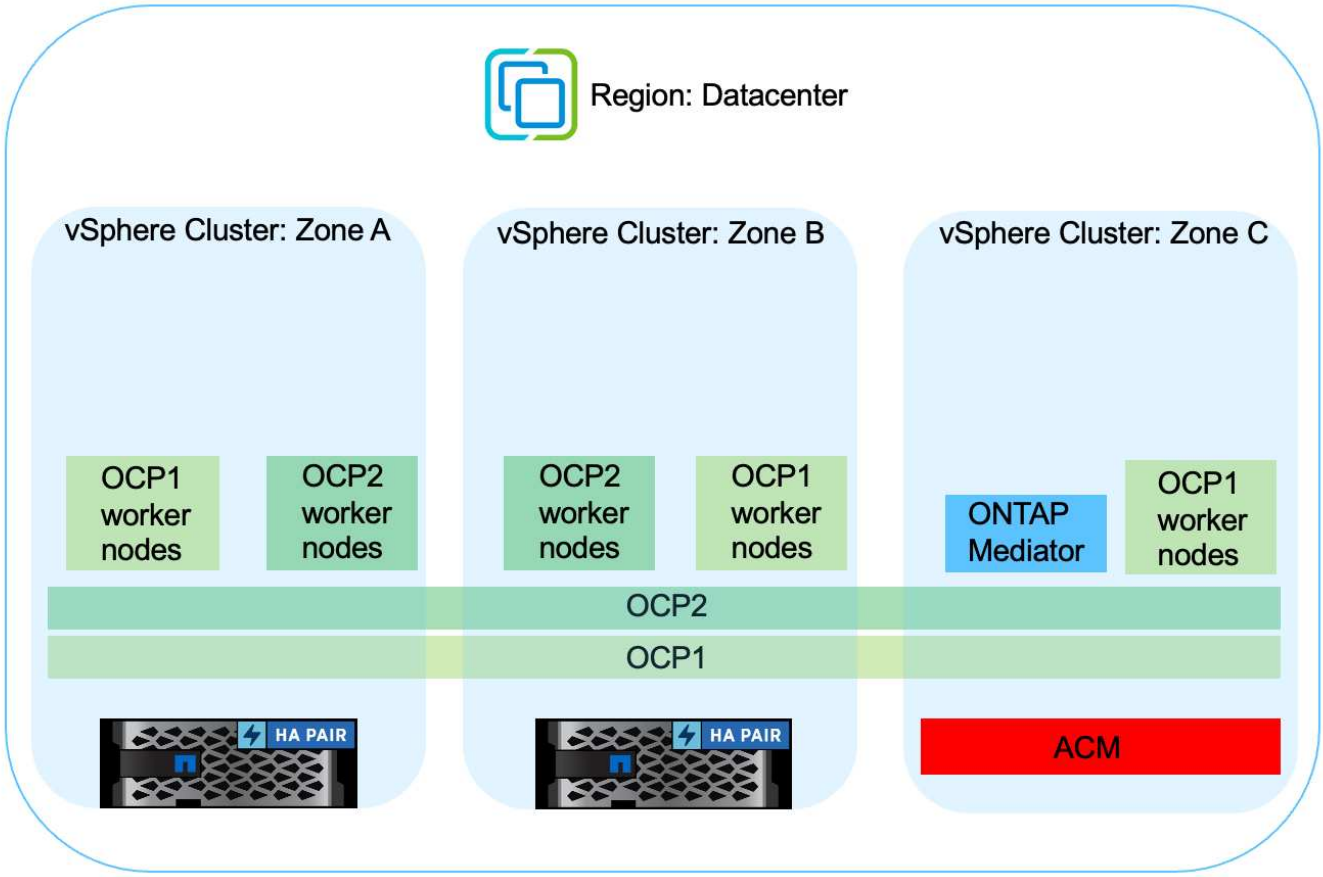
Data Protection con Astra Control Center

Continuità del business con MetroCluster

La maggior parte della nostra piattaforma hardware per ONTAP dispone di funzionalità ad alta disponibilità per la protezione dai guasti dei dispositivi, evitando la necessità di eseguire il disaster recovery. Tuttavia, per proteggere da incendi o altri disastri e continuare il business con un RPO zero e un RTO basso, spesso viene utilizzata una soluzione MetroCluster.

I clienti che attualmente dispongono di un sistema ONTAP possono estendere a MetroCluster aggiungendo sistemi ONTAP supportati entro i limiti di distanza per fornire il disaster recovery a livello di zona. Astra Trident, CSI (Container Storage Interface) supporta NetApp ONTAP, inclusa la configurazione MetroCluster e altre opzioni come Cloud Volumes ONTAP, Azure NetApp Files, AWS FSX per NetApp ONTAP, ecc. Astra Trident offre cinque opzioni di driver di storage per ONTAP, tutte supportate per la configurazione MetroCluster. Fare riferimento a. "qui" Per ulteriori informazioni sui driver di storage ONTAP supportati da Astra Trident.

La soluzione MetroCluster richiede un’estensione di rete Layer 2 o la capacità di accedere allo stesso indirizzo di rete da entrambi i domini di errore. Una volta eseguita la configurazione MetroCluster, la soluzione è trasparente per i proprietari delle applicazioni, in quanto tutti i volumi nella svm MetroCluster sono protetti e ottengono i benefici di SyncMirror (zero RPO).



Per la configurazione back-end Trident (TBC), non specificare dataLIF e SVM quando si utilizza la configurazione MetroCluster. Specificare l'IP di gestione SVM per la gestione LIF e utilizzare le credenziali del ruolo vsadmin.

Sono disponibili dettagli sulle funzioni di protezione dei dati di Astra Control Center "qui"

Migrazione dei dati con Astra Control Center

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster Red Hat OpenShift con Astra Control Center (ACC).

Le applicazioni Kubernetes spesso devono essere spostate da un ambiente all'altro. Per migrare un'applicazione insieme ai suoi dati persistenti, è possibile utilizzare NetApp ACC.

Migrazione dei dati tra diversi ambienti Kubernetes

ACC supporta diversi tipi di Kubernetes, tra cui Google anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Kubernetes upstream, ecc. Per ulteriori dettagli, fare riferimento a. "qui".

Per migrare l'applicazione da un cluster a un altro, è possibile utilizzare una delle seguenti funzionalità di ACC:

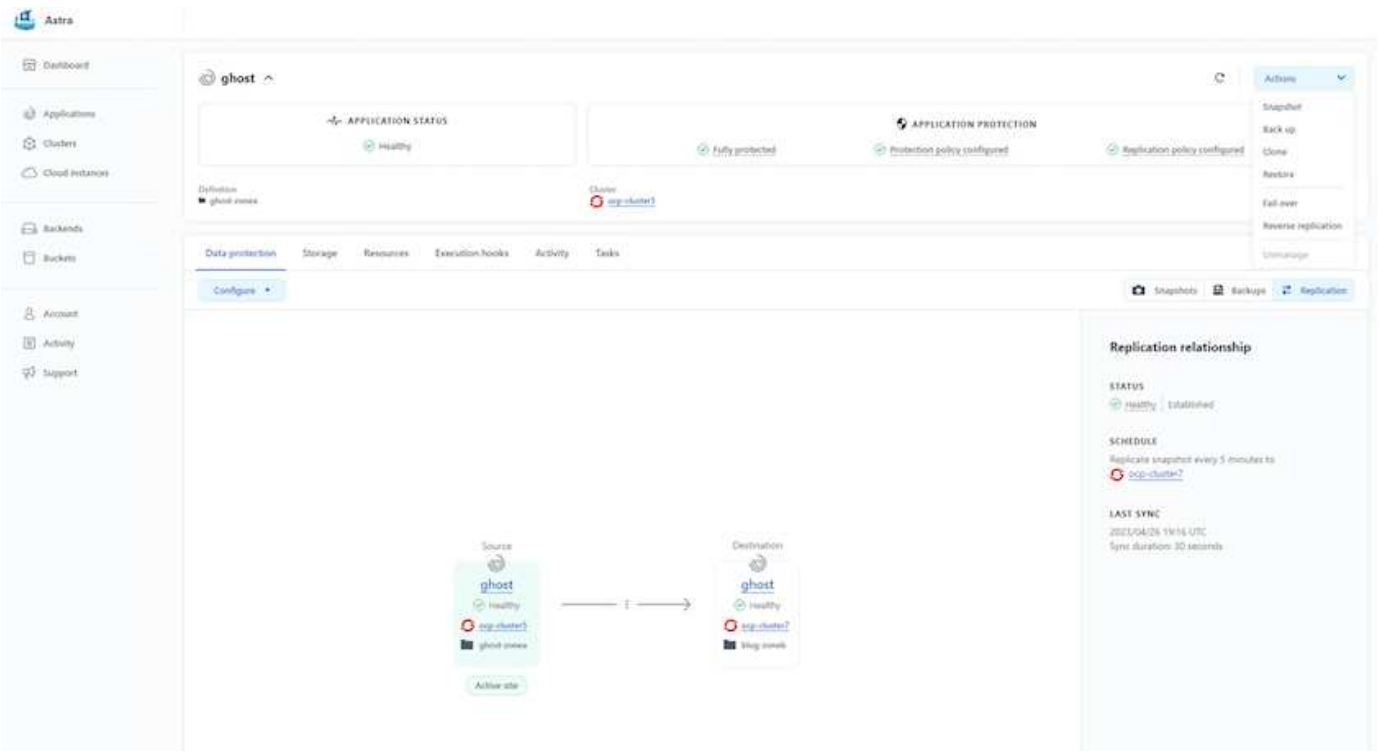
- **replica**
- **backup e ripristino**
- **clone**

Fare riferimento a. "sezione sulla protezione dei dati" per le opzioni **replica e backup e ripristino**.

Fare riferimento a. "qui" per ulteriori dettagli sulla clonazione **.

> La funzione di replica Astra è supportata solo con Trident Container Storage Interface (CSI). Tuttavia, la replica non è supportata dai driver nas-economy e san-economy.

Esecuzione della replica dei dati con ACC



Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

Panoramica

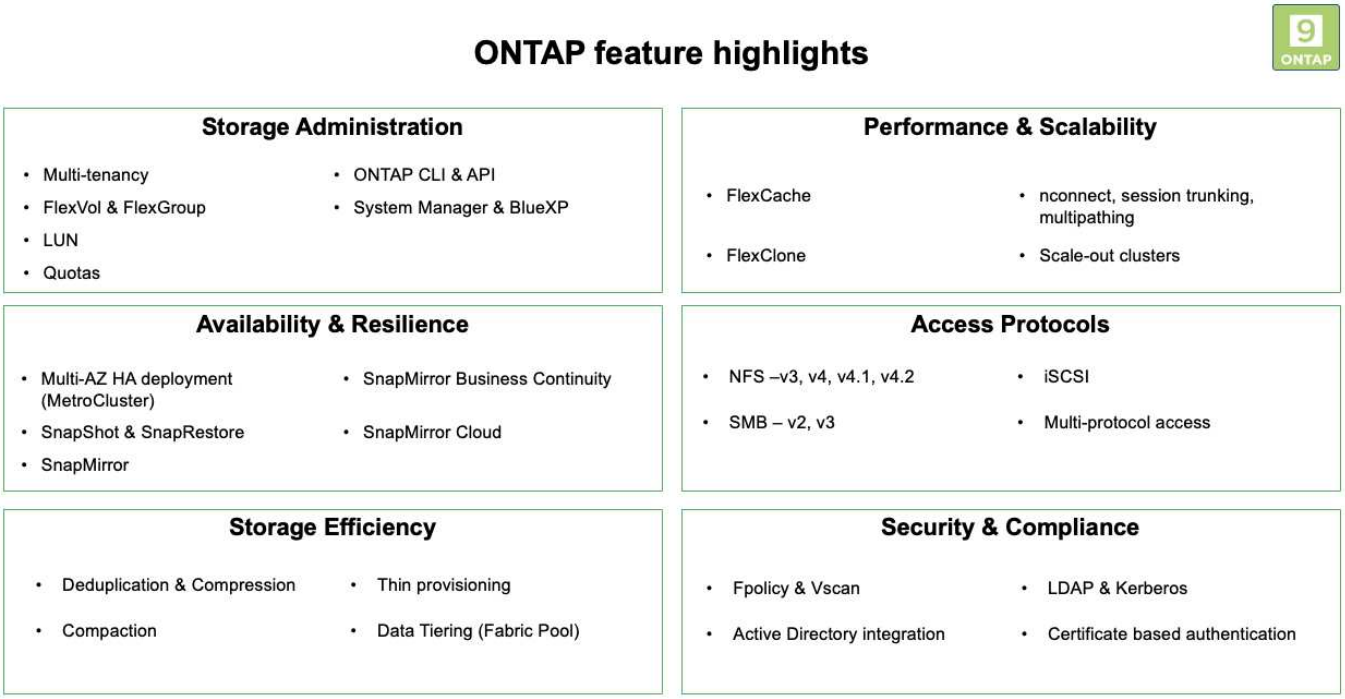
NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

- Storage autogestita on-premise:

    - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
    - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
    - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
    - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido

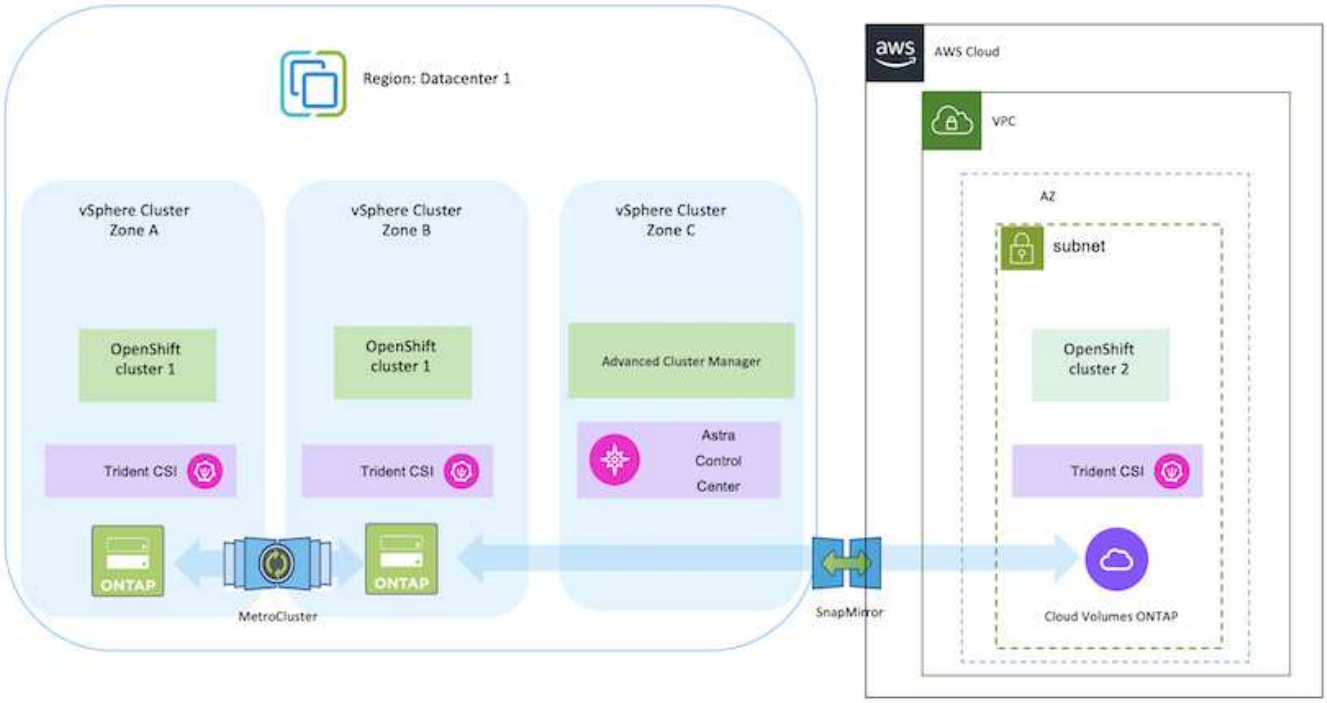
I clienti potrebbero trovarsi in un punto del loro percorso di modernizzazione quando sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i carichi di lavoro dai data center al cloud. Possono scegliere di utilizzare container OpenShift autogestiti e storage NetApp autogestiti nel cloud per diversi motivi. Devono pianificare e implementare la

piattaforma container Red Hat OpenShift (OCP) nel cloud per un ambiente pronto per la produzione di successo per la migrazione dei carichi di lavoro dei container dai data center. I loro cluster OCP possono essere implementati su VMware o bare metal nei loro data center e su AWS, Azure o Google Cloud nell'ambiente cloud.

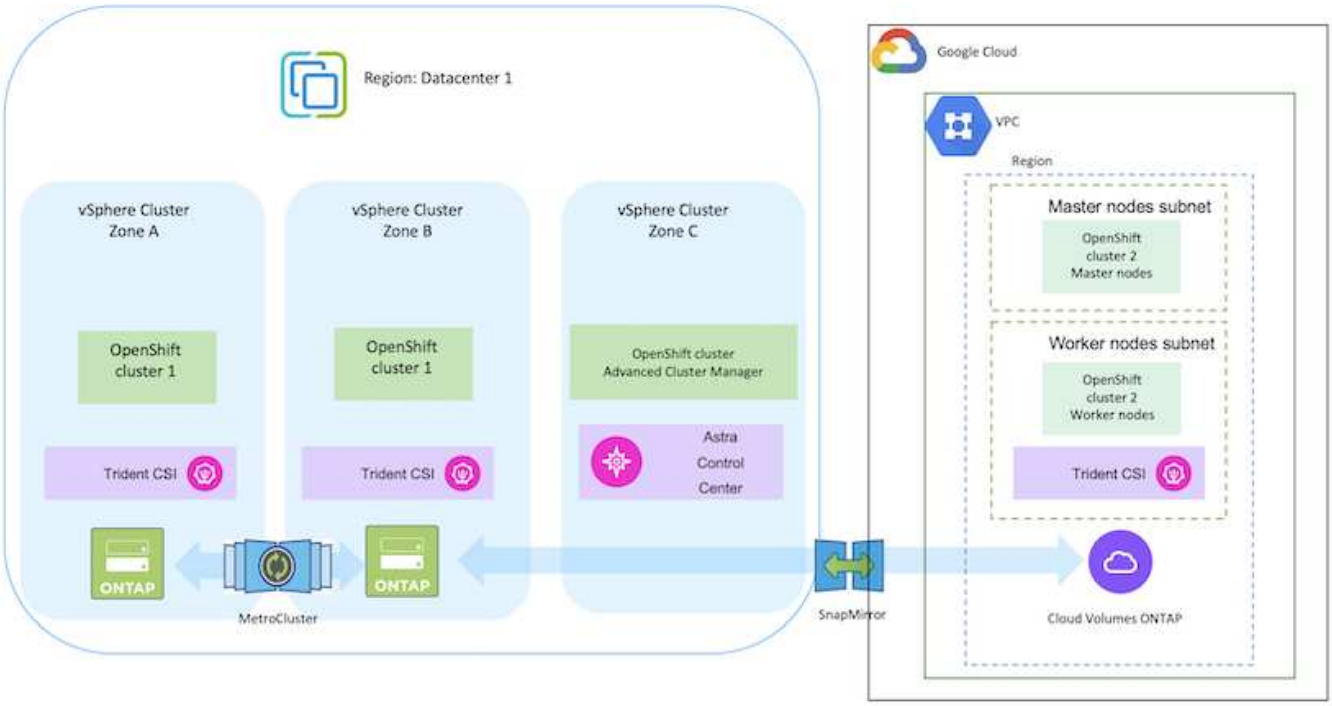
Lo storage NetApp Cloud Volumes ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container in AWS, Azure e Google Cloud. Astra Trident funge da provider di storage dinamico per consumare lo storage Cloud Volumes ONTAP persistente per le applicazioni stateful dei clienti. Astra Control Center può essere utilizzato per orchestrare i numerosi requisiti di gestione dei dati delle applicazioni stateful come protezione dei dati, migrazione e business continuity.

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift in un cloud ibrido con Astra Control Center

On-premise e in AWS

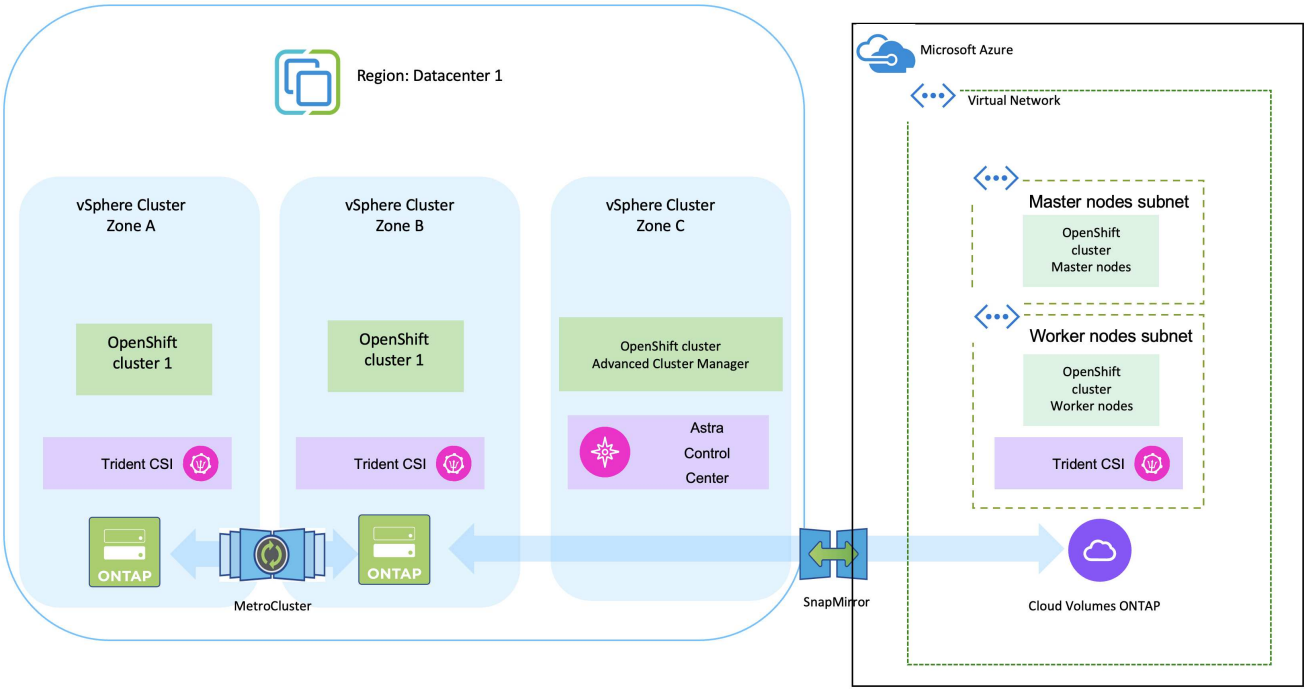


On-premise e Google Cloud



Azure Cloud e on-premise

[redacted]



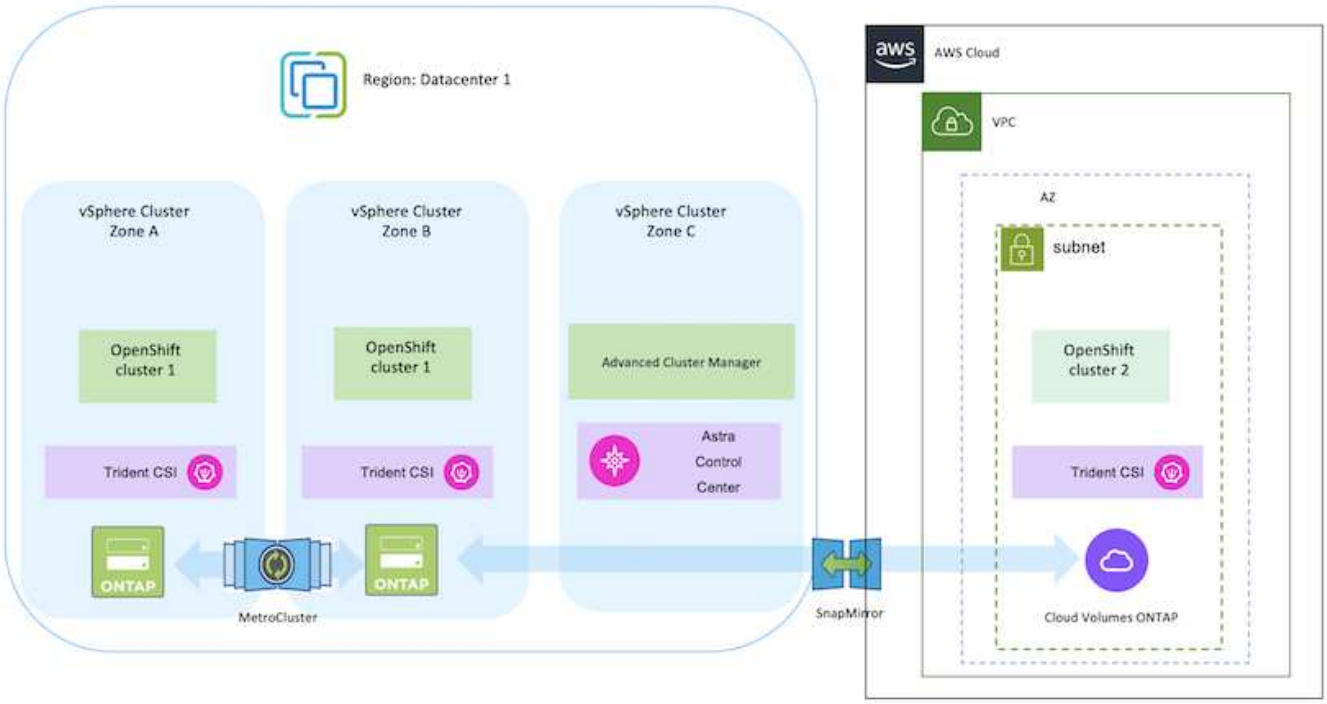
[redacted]

Implementa e configura la piattaforma container Red Hat OpenShift su AWS

In questa sezione viene descritto un workflow di alto livello che illustra come configurare e gestire i cluster OpenShift in AWS e come implementare applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

> Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift su AWS. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Di seguito è riportato un diagramma che illustra i cluster implementati su AWS e connessi al data center mediante una VPN.



Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP su AWS da Advanced Cluster Management.

- Creare un VPC con una connessione VPN sito-sito (utilizzando pfsense) per connettersi alla rete on-premise.
- La rete on-premise dispone di connettività Internet.
- Creare 3 subnet private in 3 diversi AZS.
- Creare una zona host privata Route 53 e un resolver DNS per il VPC.

Creare il cluster OpenShift su AWS dalla procedura guidata Advanced Cluster Management (ACM). Fare riferimento alle istruzioni "qui".

Puoi anche creare il cluster in AWS dalla console OpenShift Hybrid Cloud. Fare riferimento a. "qui" per istruzioni.

Quando si crea il cluster utilizzando ACM, è possibile personalizzare l'installazione modificando il file yaml dopo aver inserito i dettagli nella vista del modulo. Una volta creato il cluster, è possibile accedere ssh ai nodi del cluster per la risoluzione dei problemi o per un'ulteriore configurazione manuale. Utilizzare la chiave ssh fornita durante l'installazione e il nome utente principale per effettuare il login.

Implementare Cloud Volumes ONTAP in AWS utilizzando BlueXP.

- Installare il connettore in ambiente VMware on-premise. Fare riferimento alle istruzioni "qui".
- Implementare un'istanza CVO in AWS utilizzando il connettore. Fare riferimento alle istruzioni "qui".

Il connettore può essere installato anche nell'ambiente cloud. Fare riferimento a. "qui" per ulteriori informazioni.

Installare Astra Trident nel cluster OCP

- Implementare Trident Operator utilizzando Helm. Fare riferimento alle istruzioni "qui"
- Creare un backend e una classe di storage. Fare riferimento alle istruzioni "qui".

Aggiungere il cluster OCP su AWS all'Astra Control Center.

Aggiungere il cluster OCP in AWS ad Astra Control Center.

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

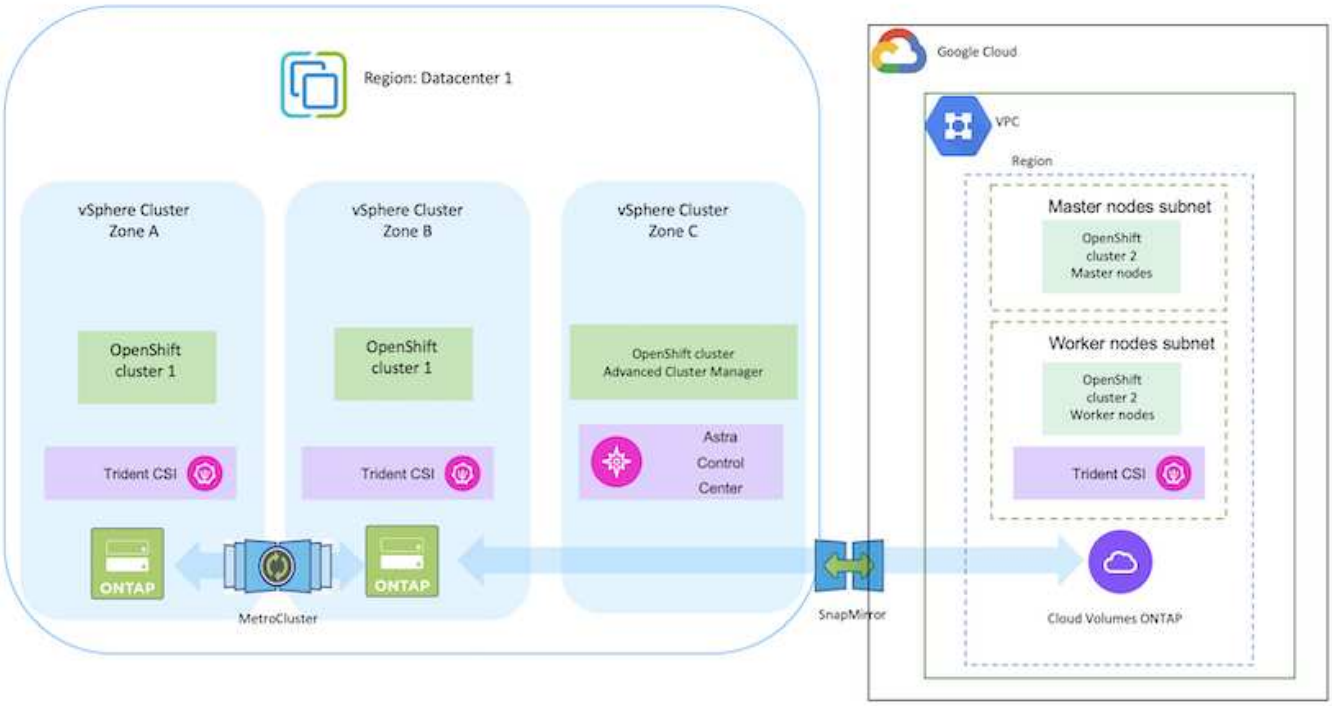
> Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Implementare e configurare la piattaforma Red Hat OpenShift Container su GCP

Implementare e configurare la piattaforma Red Hat OpenShift Container su GCP

In questa sezione viene descritto un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in GCP e distribuire le applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Segue un diagramma che mostra i cluster implementati in GCP e connessi al data center tramite una VPN.



Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift in GCP. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP su GCP dalla CLI.

- Assicurarsi di aver soddisfatto tutti i prerequisiti indicati "qui".
- Per la connettività VPN tra on-premise e GCP, è stata creata e configurata una macchina virtuale pfsense. Per istruzioni, vedere "qui".
  - L'indirizzo del gateway remoto in pfsense può essere configurato solo dopo aver creato un gateway VPN in Google Cloud Platform.
  - Gli indirizzi IP della rete remota per la fase 2 possono essere configurati solo dopo l'esecuzione del programma di installazione del cluster OpenShift e la creazione dei componenti dell'infrastruttura per il cluster.
  - La VPN in Google Cloud può essere configurata solo dopo che i componenti di infrastruttura per il cluster sono stati creati dal programma di installazione.
- Installare ora il cluster OpenShift su GCP.
  - Ottenere il programma di installazione e il segreto pull e distribuire il cluster seguendo i passaggi forniti nella documentazione "qui".
  - L'installazione crea una rete VPC in Google Cloud Platform. Inoltre, crea una zona privata in DNS cloud e aggiunge record.
    - Utilizzare l'indirizzo del blocco CIDR della rete VPC per configurare pfsense e stabilire la connessione VPN. Assicurarsi che i firewall siano configurati correttamente.
    - Aggiungere Un record nel DNS dell'ambiente on-premise utilizzando l'indirizzo IP nei record A del DNS di Google Cloud.
  - L'installazione del cluster viene completata e viene fornito un file kubeconfig e un nome utente e una password per accedere alla console del cluster.

Implementa Cloud Volumes ONTAP in GCP usando BlueXP.

- Installare un connettore in Google Cloud. Fare riferimento alle istruzioni "qui".
- Implementa un'istanza CVO in Google Cloud usando Connector. Fare riferimento alle istruzioni riportate di seguito. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Installare Astra Trident nel cluster OCP in GCP

- Esistono molti metodi per implementare Astra Trident, come illustrato "qui".
- Per questo progetto, Astra Trident è stato installato distribuendo manualmente l'operatore Astra Trident utilizzando le istruzioni "qui".
- Creare classi di storage e backend. Fare riferimento alle istruzioni "qui".

Aggiungere il cluster OCP su GCP all'Astra Control Center.

- Creare un file KubeConfig separato con un ruolo cluster che contenga le autorizzazioni minime necessarie per gestire un cluster da Astra Control. Le istruzioni sono disponibili "qui".
- Aggiungere il cluster ad Astra Control Center seguendo le istruzioni "qui"

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Video dimostrativo

Installazione del cluster OpenShift su Google Cloud Platform

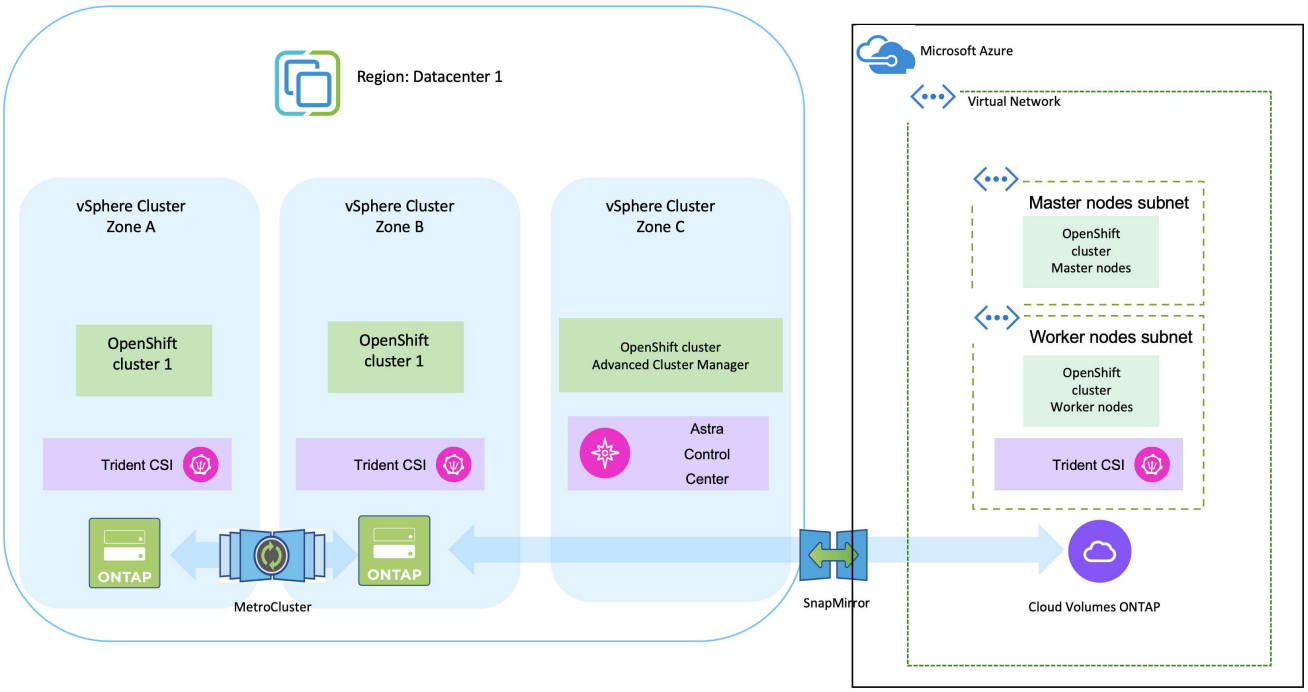
Importazione dei cluster OpenShift in Astra Control Center

Implementa e configura la piattaforma Red Hat OpenShift Container su Azure

Implementa e configura la piattaforma Red Hat OpenShift Container su Azure

In questa sezione viene descritto un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in Azure e distribuire applicazioni stateful su di essi. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'aiuto di Astra Trident/Astra Control Provivioner per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Astra Control Center per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful.

Segue un diagramma che mostra i cluster implementati in Azure e connessi al data center tramite una VPN.



Esistono diversi modi per implementare i cluster di piattaforme container Red Hat OpenShift in Azure. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare un cluster OCP in Azure dalla CLI.

- Assicurarsi di aver soddisfatto tutti i prerequisiti indicati "qui".
- Creare una VPN, subnet, gruppi di protezione della rete e una zona DNS privata. Creare un gateway VPN e una connessione VPN da sito a sito.
- Per la connettività VPN tra on-premise e Azure, è stata creata e configurata una macchina virtuale pfsense. Per istruzioni, vedere "qui".
- Ottenere il programma di installazione e il segreto pull e distribuire il cluster seguendo i passaggi forniti nella documentazione "qui".
- L'installazione del cluster viene completata e viene fornito un file kubeconfig e un nome utente e una password per accedere alla console del cluster.

Di seguito è riportato un esempio di file install-config.yaml.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
```

```
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

Implementa Cloud Volumes ONTAP in Azure utilizzando BlueXP.

- Installa un connettore in Azure. Fare riferimento alle istruzioni "qui".
- Implementa un'istanza CVO in Azure usando Connector. Fare riferimento alle istruzioni link:https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [qui].

Installa Astra Control Provisioner nel cluster OCP in Azure

- Per questo progetto, Astra Control Provisioner (ACP) è stato installato in tutti i cluster (cluster on-premise, cluster on-premise in cui viene implementato Astra Control Center e il cluster in Azure). Scopri di più su Astra Control Provisioner "qui".
- Creare classi di storage e backend. Fare riferimento alle istruzioni "qui".

Aggiungi il cluster OCP in Azure all'Astra Control Center.

- Creare un file KubeConfig separato con un ruolo cluster che contenga le autorizzazioni minime necessarie per gestire un cluster da Astra Control. Le istruzioni sono disponibili "qui".
- Aggiungere il cluster ad Astra Control Center seguendo le istruzioni "qui"

Utilizzo della funzionalità topologia CSI di Trident per architetture multi-zona

I cloud provider, oggi, consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi dei cluster basati su zone. I nodi possono essere collocati in diverse zone di disponibilità all'interno di una regione o in diverse regioni. Per facilitare il provisioning dei volumi per i carichi di lavoro in un'architettura multi-zona, Astra Trident utilizza la topologia CSI. Utilizzando la funzionalità topologia CSI, l'accesso ai volumi può essere limitato a un sottoinsieme di nodi, in base alle aree geografiche e alle zone di disponibilità. Fare riferimento a. "qui" per ulteriori dettagli.

> Kubernetes supporta due modalità di binding del volume: - Quando ***VolumeBindingMode* è impostato su *immediate*** (default), Astra Trident crea il volume senza alcuna consapevolezza della topologia. I volumi persistenti vengono creati senza alcuna dipendenza dai requisiti di pianificazione del pod richiedente. - Quando ***VolumeBindingMode* viene impostato su *WaitForFirstConsumer***, la creazione e il binding di un volume persistente per un PVC viene ritardata fino a quando un pod che utilizza il PVC viene pianificato e creato. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di storage Astra Trident possono essere progettati per eseguire il provisioning selettivo dei volumi in base alle zone di disponibilità (back-end compatibile con la topologia). Per StorageClasses che utilizzano tale backend, un volume viene creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass consapevole della topologia) fare riferimento "qui" per ulteriori dettagli.

Video dimostrativo

Utilizzo di Astra Control per il failover e il failback delle applicazioni

Protezione dei dati mediante Astra Control Center

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su container Red Hat OpenShift in esecuzione su VMware vSphere o nel cloud tramite Astra Control Center (ACC).

Mentre gli utenti intraprendono il percorso di modernizzazione delle proprie applicazioni con Red Hat OpenShift, è necessario adottare una strategia di protezione dei dati per proteggerli da cancellazioni accidentali o altri errori umani. Spesso, per proteggere i propri dati da un diaster, è necessaria anche una strategia di protezione a scopo normativo o di compliance.

I requisiti di protezione dei dati variano dal ritorno a una copia point-in-time al failover automatico a un dominio di errore diverso senza alcun intervento umano. Molti clienti scelgono ONTAP come piattaforma di storage preferita per le loro applicazioni Kubernetes per le sue ricche funzionalità come multi-tenancy, multi-protocollo, offerte di capacità e performance elevate, replica e caching per ubicazioni multi-sito, sicurezza e flessibilità.

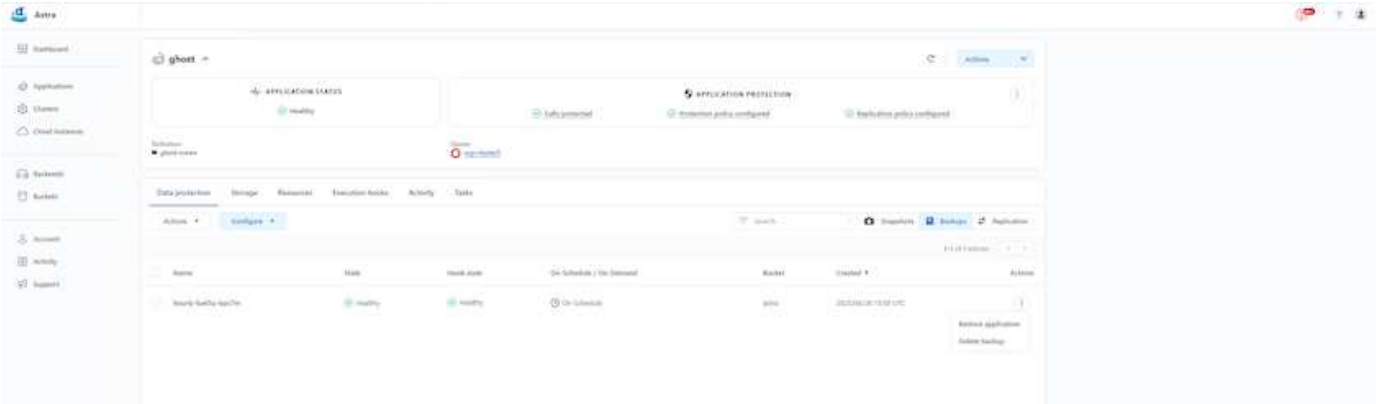
I clienti possono avere un ambiente cloud configurato come estensione del data center, in modo che possano sfruttare i benefici del cloud e essere in grado di spostare i propri carichi di lavoro in un momento futuro. Per

tali clienti, il backup delle applicazioni OpenShift e dei dati nell'ambiente cloud diventa una scelta inevitabile. Possono quindi ripristinare le applicazioni e i dati associati su un cluster OpenShift nel cloud o nel data center.

Backup e ripristino con ACC

I proprietari delle applicazioni possono rivedere e aggiornare le applicazioni rilevate da ACC. ACC può eseguire copie Snapshot utilizzando CSI ed eseguire il backup utilizzando la copia Snapshot point-in-time. La destinazione del backup può essere un archivio di oggetti nell'ambiente cloud. È possibile configurare i criteri di protezione per i backup pianificati e il numero di versioni di backup da conservare. L'RPO minimo è di un'ora.

Ripristino di un'applicazione da un backup mediante ACC

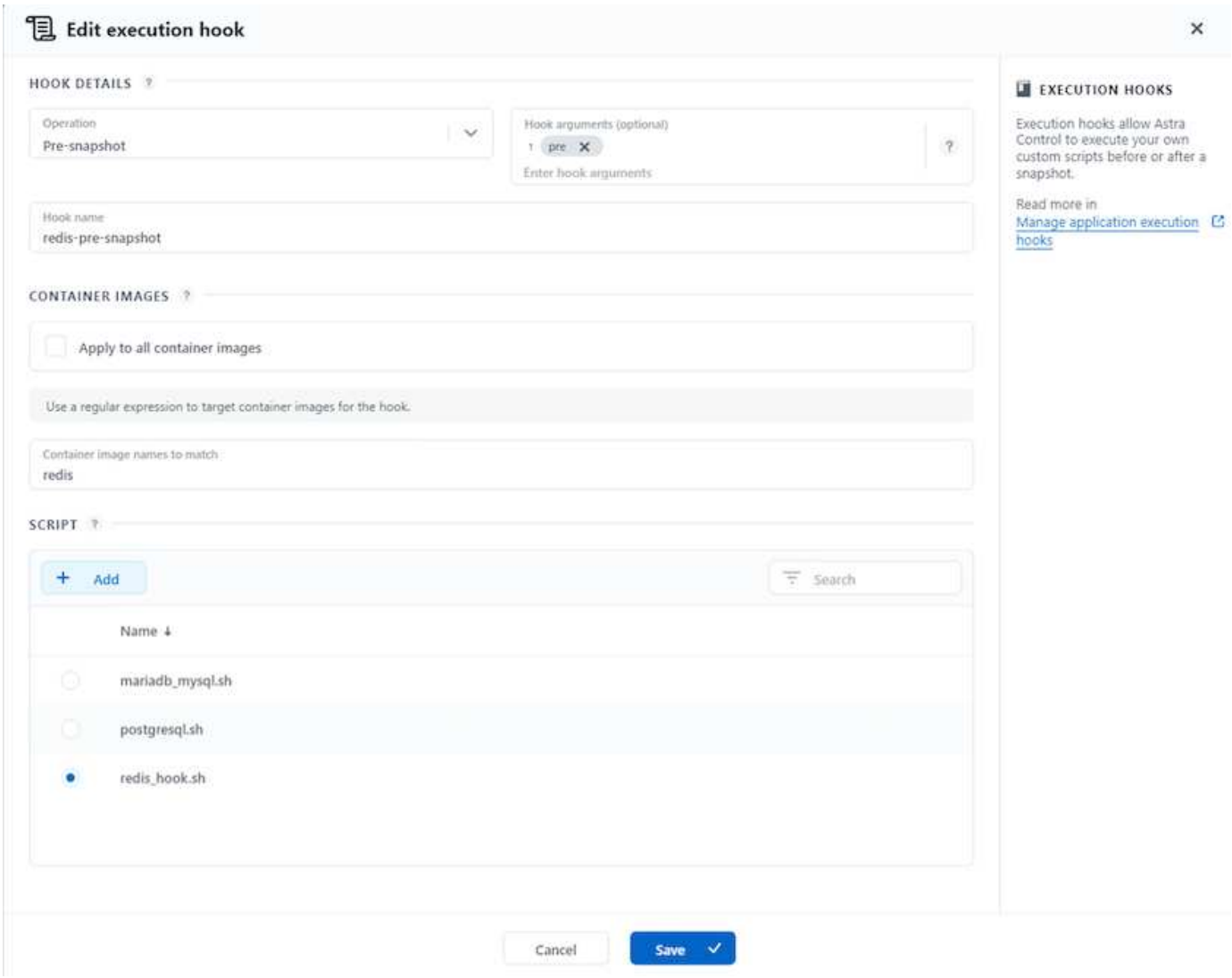


Hook di esecuzione specifici dell'applicazione

Anche se sono disponibili funzionalità di protezione dei dati a livello di array di storage, spesso sono necessari ulteriori passaggi per rendere coerenti le applicazioni di backup e ripristino. I passaggi aggiuntivi specifici dell'applicazione potrebbero essere: - Prima o dopo la creazione di una copia Snapshot. - prima o dopo la creazione di un backup. - Dopo il ripristino da una copia Snapshot o da un backup. Astra Control può eseguire questi passaggi specifici dell'applicazione codificati come script personalizzati chiamati uncini di esecuzione.

Di NetApp "Progetto open source Verda" fornisce hook di esecuzione per le applicazioni native del cloud più diffuse per rendere la protezione delle applicazioni semplice, robusta e facile da orchestrare. Se si dispone di informazioni sufficienti per un'applicazione non presente nel repository, è possibile contribuire al progetto.

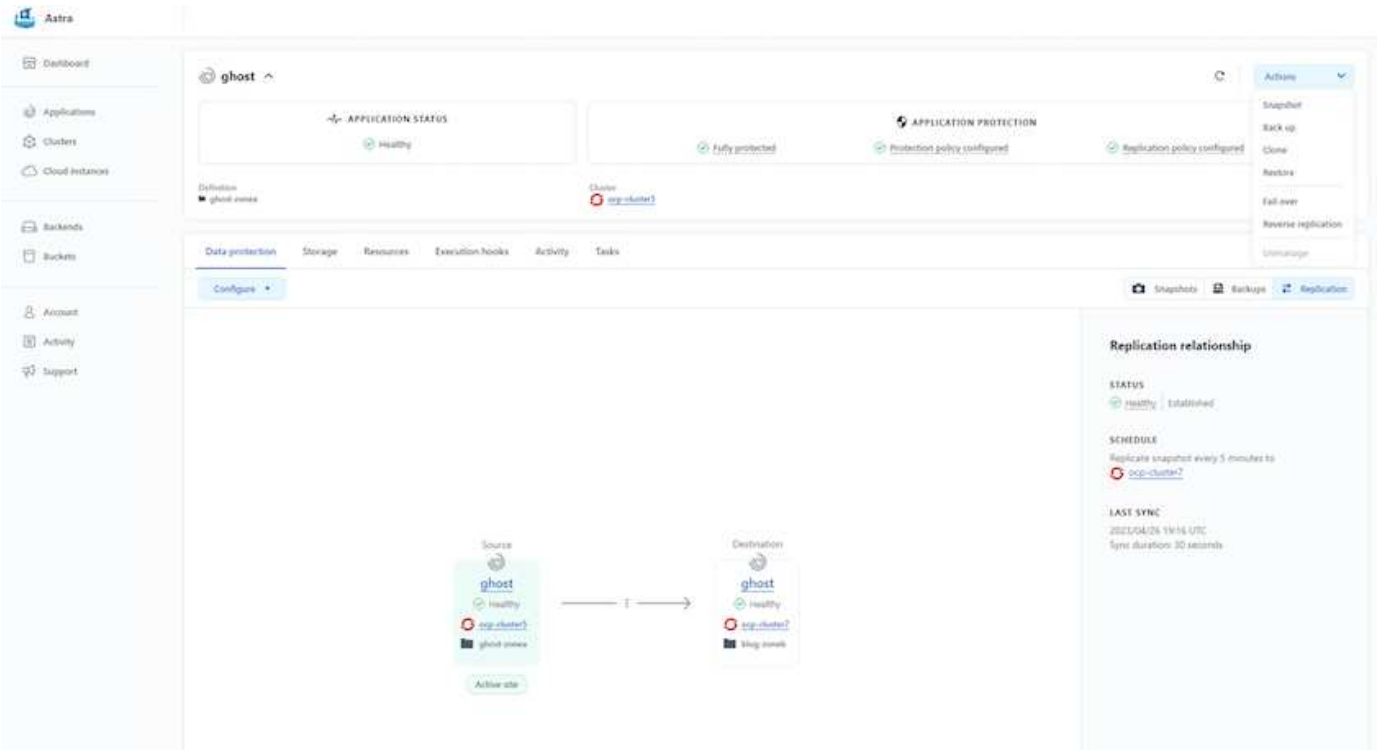
Esempio di gancio di esecuzione per pre-Snapshot di un'applicazione redis.



Replica con ACC

Per la protezione regionale o per una soluzione RPO e RTO bassa, un'applicazione può essere replicata in un'altra istanza di Kubernetes in esecuzione in un sito diverso, preferibilmente in un'altra regione. ACC utilizza SnapMirror asincrono ONTAP con RPO in soli 5 minuti. Fare riferimento a. "qui" Per le istruzioni di installazione di SnapMirror.

SnapMirror con ACC



i driver di storage san-economy e nas-economy non supportano la funzione di replica. Fare riferimento a. "qui" per ulteriori dettagli.

Video dimostrativo:

"Video dimostrativo del disaster recovery con Astra Control Center"

Data Protection con Astra Control Center

Sono disponibili dettagli sulle funzioni di protezione dei dati di Astra Control Center "qui"

Disaster recovery (failover e failback con replica) con ACC

Utilizzo di Astra Control per il failover e il failback delle applicazioni

Migrazione dei dati con Astra Control Center

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster Red Hat OpenShift con Astra Control Center (ACC). In particolare, i clienti possono utilizzare l'ACC per trasferire alcuni workload selezionati o tutti i workload dai data center on-premise al cloud, clonare le loro applicazioni nel cloud a scopo di test o passare dal data center al cloud

Migrazione dei dati

Per migrare l'applicazione da un ambiente a un altro, è possibile utilizzare una delle seguenti funzionalità di ACC:

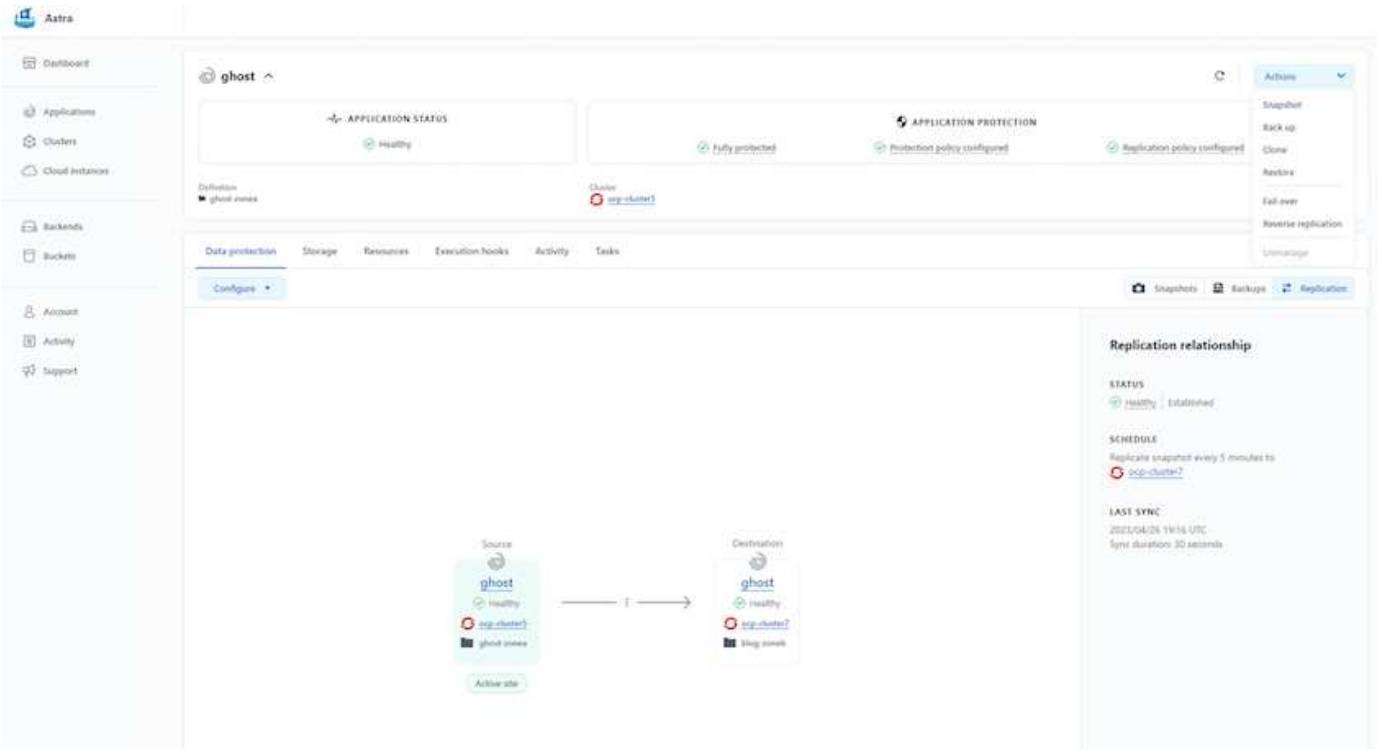
- **replica**

- **backup e ripristino**
- **clone**

Fare riferimento a. "sezione sulla protezione dei dati" per le opzioni **replica e backup e ripristino**. Fare riferimento a. "qui" per ulteriori dettagli sulla clonazione **.

> La funzione di replica Astra è supportata solo con Trident Container Storage Interface (CSI). Tuttavia, la replica non è supportata dai driver nas-economy e san-economy.

Esecuzione della replica dei dati con ACC



Soluzioni NetApp ibride multicloud per i carichi di lavoro dei container Red Hat OpenShift

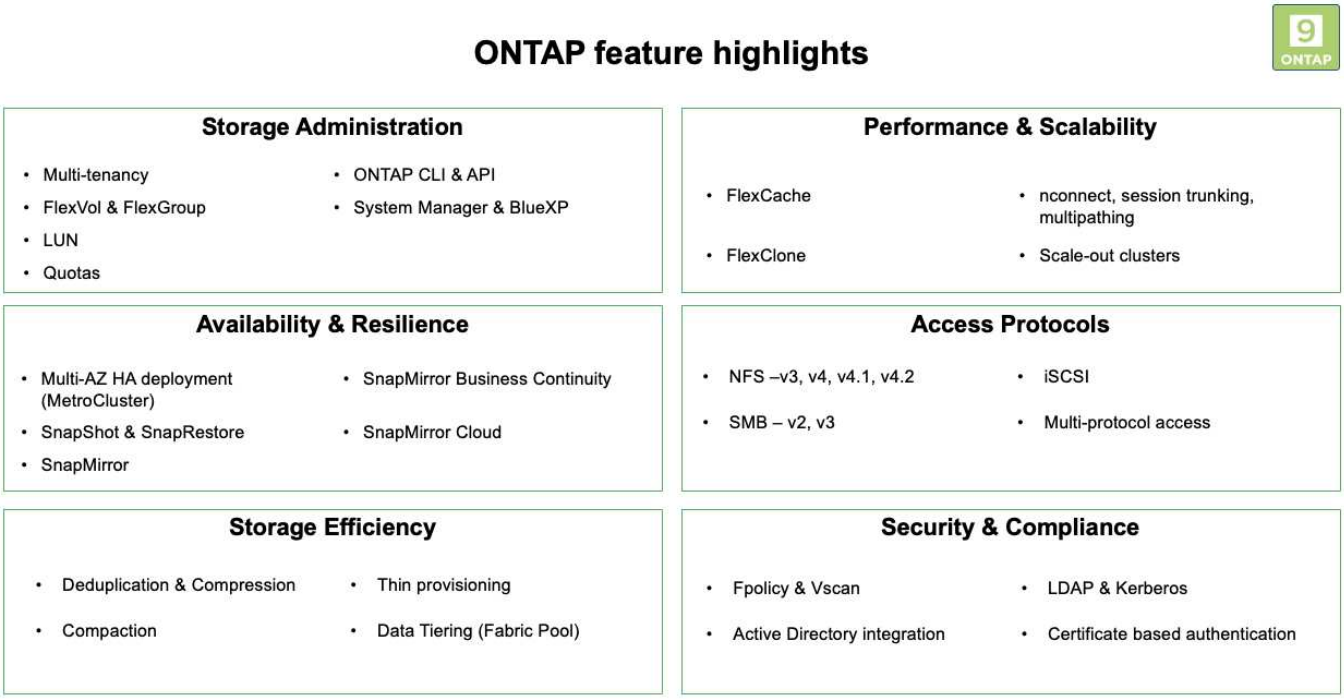
Panoramica

NetApp sta assistendo a un significativo aumento dei clienti nella modernizzazione delle applicazioni aziendali legacy e nella creazione di nuove applicazioni utilizzando container e piattaforme di orchestrazione basate su Kubernetes. Red Hat OpenShift Container Platform è un esempio che vediamo adottato da molti dei nostri clienti.

Man mano che un numero sempre maggiore di clienti inizia ad adottare container all'interno delle proprie aziende, NetApp si trova nella posizione ideale per soddisfare le esigenze di storage persistenti delle proprie applicazioni stateful e le esigenze di gestione dei dati classiche, come protezione dei dati, sicurezza dei dati e migrazione dei dati. Tuttavia, queste esigenze vengono soddisfatte utilizzando strategie, strumenti e metodi diversi.

Le opzioni di storage basate su NetApp ONTAP elencate di seguito offrono sicurezza, protezione dei dati, affidabilità e flessibilità per le implementazioni di container e Kubernetes.

- Storage autogestita on-premise:
  - NetApp Fabric Attached Storage (FAS), NetApp All Flash FAS Array (AFF), NetApp All SAN Array (ASA) e ONTAP Select
- Storage gestito dal provider on-premise:
  - NetApp Keystone offre storage as a service (STaaS)
- Storage autogestita nel cloud:
  - NetApp Cloud Volumes ONTAP (CVO) offre storage autogestiti negli hyperscaler
- Storage gestito dal provider nel cloud:
  - Cloud Volumes Service per Google Cloud (CVS), Azure NetApp Files (ANF) e Amazon FSX per NetApp ONTAP offrono storage completamente gestito negli hyperscaler



NetApp BlueXP consente di gestire tutte le risorse di storage e dati da un singolo piano di controllo/interfaccia.

È possibile utilizzare BlueXP per creare e amministrare lo storage cloud (ad esempio, Cloud Volumes ONTAP e Azure NetApp Files), per spostare, proteggere e analizzare i dati e per controllare molti dispositivi storage on-premise e edge.

NetApp Astra Trident è un orchestratore di storage conforme a CSI che consente un consumo rapido e semplice dello storage persistente supportato da una serie di opzioni di storage NetApp sopra menzionate. Si tratta di un software open-source gestito e supportato da NetApp.

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

I carichi di lavoro dei container business-critical richiedono molto di più dei semplici volumi persistenti. I loro requisiti di gestione dei dati richiedono anche la protezione e la migrazione degli oggetti di kubernetes dell'applicazione.

> I dati dell'applicazione includono oggetti kubernetes oltre ai dati dell'utente: Alcuni esempi sono i seguenti: - Kubernetes oggetti come specifiche di pod, PVC, implementazioni, servizi - oggetti di configurazione personalizzati come mappe di configurazione e segreti - dati persistenti come copie Snapshot, backup, cloni - risorse personalizzate come CRS e CRD

NetApp Astra Control, disponibile sia come software completamente gestito che autogestita, offre un'orchestrazione per una solida gestione dei dati applicativi. Fare riferimento a. "Documentazione Astra" Per ulteriori informazioni sulla famiglia di prodotti Astra.

Questa documentazione di riferimento fornisce la convalida della migrazione e della protezione delle applicazioni basate su container, implementate sulla piattaforma container RedHat OpenShift, utilizzando NetApp Astra Control Center. Inoltre, la soluzione fornisce dettagli di alto livello per l'implementazione e l'utilizzo di Red Hat Advanced Cluster Management (ACM) per la gestione delle piattaforme container. Il documento evidenzia inoltre i dettagli per l'integrazione dello storage NetApp con le piattaforme container Red Hat OpenShift che utilizzano Astra Trident CSI Provisioner. Astra Control Center viene implementato nel cluster dell'hub e viene utilizzato per gestire le applicazioni container e il loro ciclo di vita dello storage persistente. Infine, offre una soluzione per la replica, il failover e il fail-back per i carichi di lavoro dei container su cluster Red Hat OpenShift gestiti in AWS (ROSA) utilizzando Amazon FSX per NetApp ONTAP (FSxN) come storage persistente.

Soluzione NetApp con workload gestiti della piattaforma container Red Hat OpenShift su AWS

Soluzione NetApp con workload gestiti della piattaforma container Red Hat OpenShift su AWS

I clienti possono "nascere nel cloud" o trovarsi in un punto del loro percorso di modernizzazione quando sono pronti a spostare alcuni carichi di lavoro selezionati o tutti

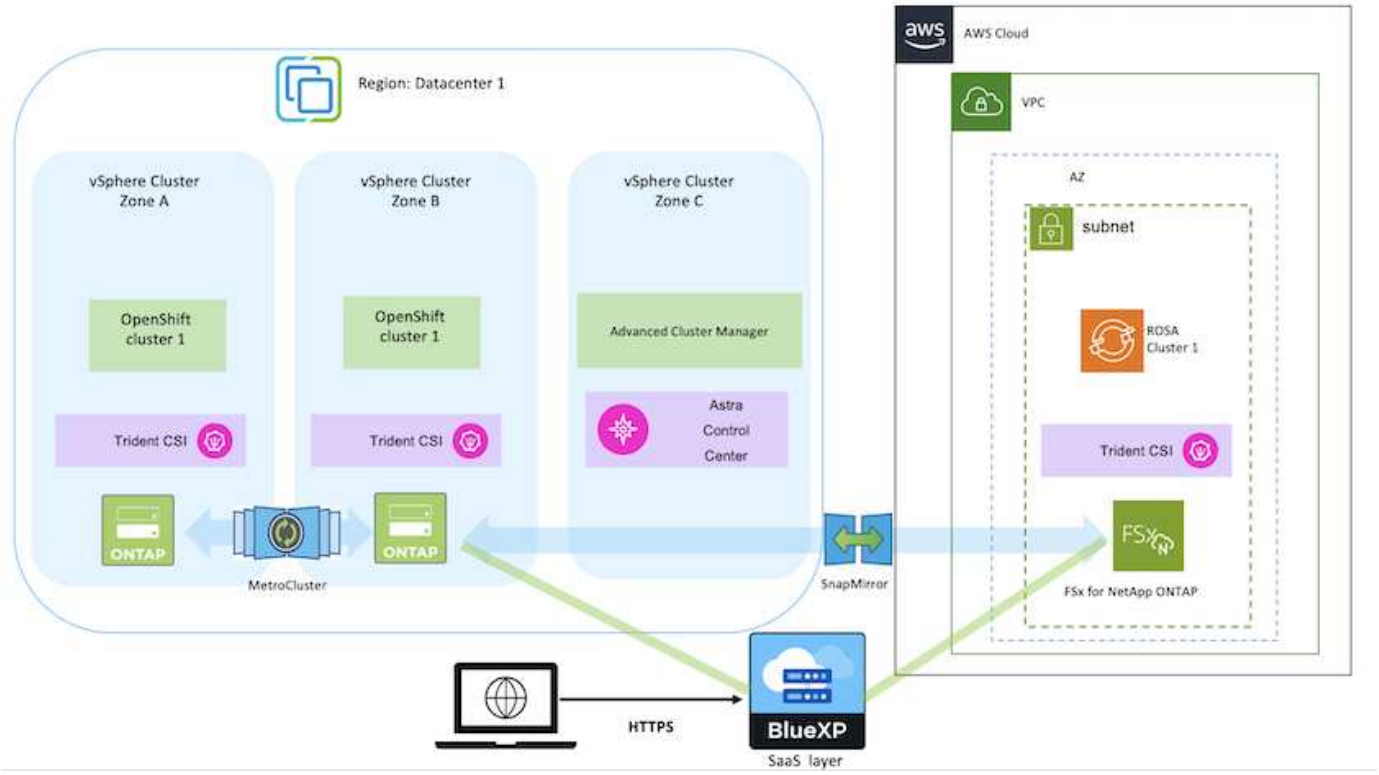
i carichi di lavoro dai data center al cloud. Possono scegliere di utilizzare container OpenShift gestiti da provider e storage NetApp gestito da provider nel cloud per l'esecuzione dei carichi di lavoro. Devono pianificare e implementare i cluster di container gestiti Red Hat OpenShift (ROSA) nel cloud per un ambiente pronto per la produzione di successo per i carichi di lavoro dei container. Quando si trovano nel cloud AWS, potrebbero anche implementare FSX per NetApp ONTAP per le esigenze di storage.

FSX per NetApp ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container in AWS. Astra Trident funge da provider di storage dinamico per consumare lo storage FSxN persistente per le applicazioni stateful dei clienti.

Poiché ROSA può essere implementato in modalità ha con nodi del piano di controllo distribuiti in più zone di disponibilità, FSX ONTAP può anche essere fornito con l'opzione Multi-AZ che fornisce alta disponibilità e protegge dai guasti AZ.

> Non sono previsti costi per il trasferimento dei dati quando si accede a un file system Amazon FSX dalla zona di disponibilità preferita (AZ) del file system. Per ulteriori informazioni sui prezzi, fare riferimento a. "qui".

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift

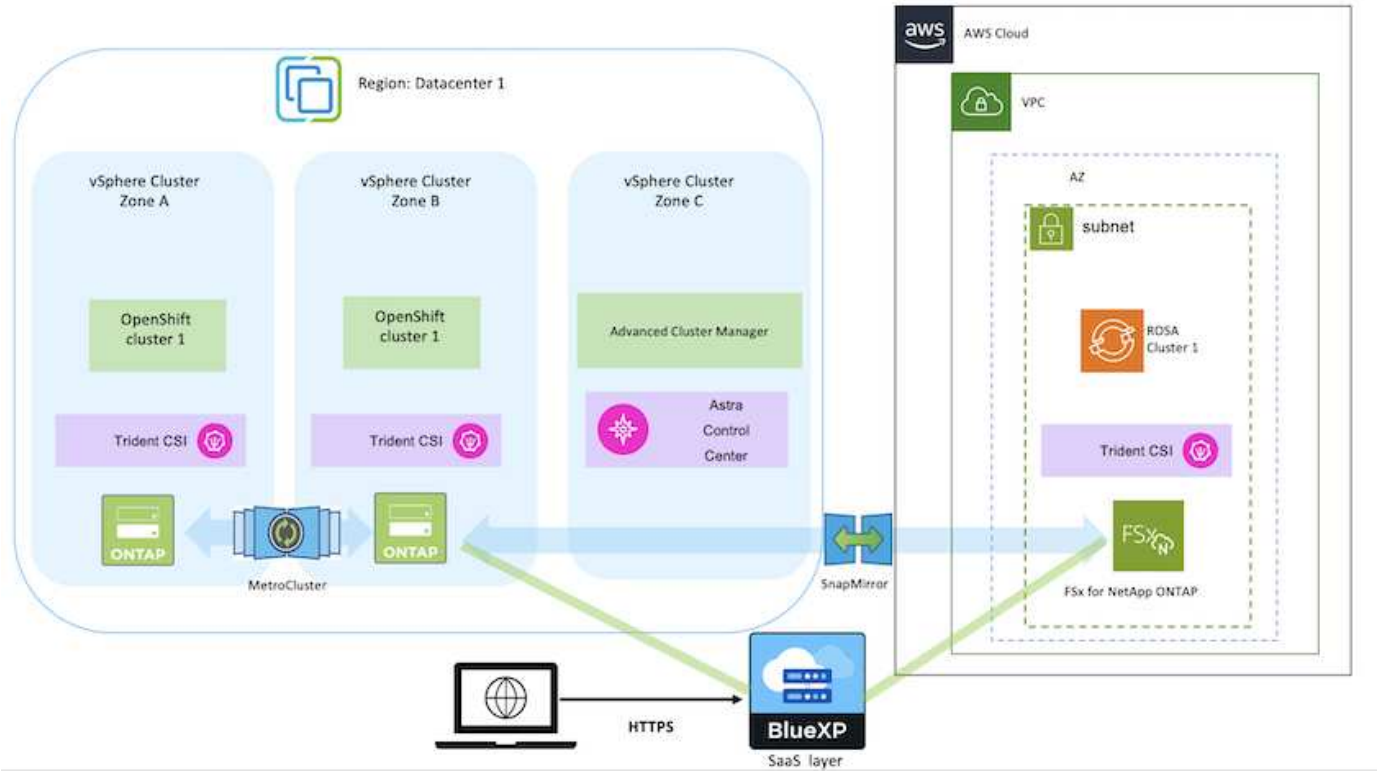


Implementa e configura la piattaforma container Managed Red Hat OpenShift su AWS

Questa sezione descrive un workflow di alto livello per la configurazione dei cluster Managed Red Hat OpenShift su AWS(ROSA). Mostra l'utilizzo di FSX gestito per NetApp ONTAP (FSxN) come back-end di storage di Astra Trident per fornire volumi persistenti. Vengono forniti dettagli sull'implementazione di FSxN su AWS utilizzando BlueXP. Inoltre,

vengono forniti dettagli sull'utilizzo di BlueXP e OpenShift GitOps (Argo CD) per eseguire attività di migrazione e protezione dei dati per le applicazioni stateful sui cluster ROSA.

Di seguito è riportato un diagramma che illustra i cluster ROSA implementati su AWS e che utilizzano FSxN come storage back-end.



Questa soluzione è stata verificata utilizzando due cluster ROSA in due VPC in AWS. Ogni cluster ROSA è stato integrato con FSxN utilizzando Astra Trident. Esistono diversi modi per implementare I cluster ROSA e FSxN in AWS. Questa descrizione di alto livello dell'installazione fornisce collegamenti alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei relativi collegamenti forniti in "sezione risorse".

Il processo di installazione può essere suddiviso nei seguenti passaggi:

Installare I cluster ROSA

- Creare due VPC e configurare la connettività di peering VPC tra i VPC.
- Fare riferimento a. "qui" Per istruzioni sull'installazione dei cluster ROSA.

Installare FSxN

- Installare FSxN sui VPC da BlueXP. Fare riferimento a. "qui" Per la creazione di un account BlueXP e per iniziare. Fare riferimento a. "qui" Per l'installazione di FSxN. Fare riferimento a. "qui" Per creare un connettore in AWS per gestire FSxN.
- Implementare FSxN utilizzando AWS. Fare riferimento a. "qui" Per l'implementazione utilizzando la console AWS.

Installare Trident sui cluster ROSA (utilizzando il grafico Helm)

- USA il grafico Helm per installare Trident sui cluster ROSA. url del grafico Helm: https://netapp.github.io/trident-helm-chart

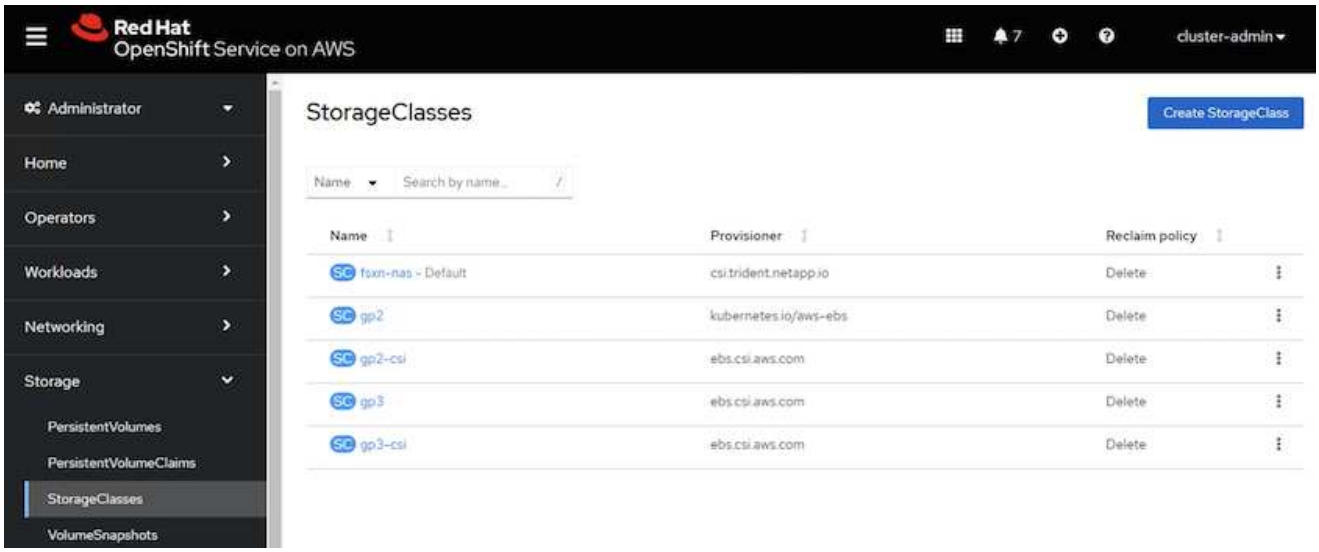
Integrazione di FSxN con Astra Trident per i cluster ROSA

OpenShift GitOps può essere utilizzato per implementare Astra Trident CSI su tutti i cluster gestiti, man mano che vengono registrati su ArgoCD utilizzando ApplicationSet.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Creare classi di storage e backend utilizzando Trident (per FSxN)

- Fare riferimento a. "qui" per informazioni dettagliate sulla creazione di classe di storage e backend.
- Rendere la classe di storage creata per FsxN con Trident CSI come predefinita da OpenShift Console. Vedere la schermata riportata di seguito:



Implementare un'applicazione utilizzando OpenShift GitOps (CD Argo)

- Installare l'operatore OpenShift GitOps sul cluster. Fare riferimento alle istruzioni "qui".
- Configurare una nuova istanza del CD Argo per il cluster. Fare riferimento alle istruzioni "qui".

Aprire la console del CD Argo e implementare un'applicazione. Ad esempio, puoi implementare un'applicazione Jenkins utilizzando il CD Argo con Helm Chart. Durante la creazione dell'applicazione, sono stati forniti i seguenti dettagli: Progetto: Cluster predefinito: https://kubernetes.default.svcSpazio dei nomi: Jenkins l'URL per il grafico Helm: https://charts.bitnami.com/bitnami

Parametri Helm: Global.storageClass: Fsxn-nas

Protezione dei dati

Questa pagina mostra le opzioni di protezione dei dati per i cluster Managed Red Hat OpenShift on AWS (ROSA) utilizzando Astra Control Service. Astra Control Service (ACS) offre un'interfaccia grafica utente di facile utilizzo che consente di aggiungere cluster, definire le applicazioni in esecuzione ed eseguire attività di gestione dei dati integrate con le applicazioni. È possibile accedere alle funzioni ACS anche utilizzando un'API che consente l'automazione dei workflow.

L'alimentazione di Astra Control (ACS o ACC) è NetApp Astra Trident. Astra Trident integra diversi tipi di cluster Kubernetes come Red Hat OpenShift, EKS, AKS, SUSE Rancher, anthos ecc., con varie soluzioni di storage NetApp ONTAP come FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files e Amazon FSX per NetApp ONTAP.

Questa sezione fornisce dettagli sulle seguenti opzioni di protezione dei dati con ACS:

- Un video che mostra il backup e il ripristino di un'applicazione ROSA in esecuzione in una regione e il ripristino in un'altra regione.
- Un video che mostra l'istantanea e il ripristino di un'applicazione ROSA.
- Dettagli dettagliati sull'installazione di un cluster ROSA, Amazon FSX per NetApp ONTAP, utilizzando NetApp Astra Trident per l'integrazione con il backend di storage, installazione di un'applicazione postgresql su un cluster ROSA, utilizzando ACS per creare una snapshot dell'applicazione e il ripristino dell'applicazione da esso.
- Un blog che mostra i dettagli passo per passo della creazione e del ripristino da uno snapshot per un'applicazione mysql su un cluster ROSA con FSX per ONTAP usando ACS.

Backup/Ripristino da backup

Il video seguente mostra il backup di un'applicazione ROSA in esecuzione in una regione e il ripristino in un'altra regione.

FSX NetApp ONTAP per il servizio Red Hat OpenShift su AWS

Snapshot/Ripristina da snapshot

Il video seguente mostra come scattare un'istantanea di un'applicazione ROSA e come eseguire il ripristino dall'istantanea dopo.

Snapshot/ripristino per le applicazioni su Red Hat OpenShift Service su cluster AWS (ROSA) con Amazon FSX per lo storage NetApp ONTAP

Blog in inglese

- "Utilizzo di Astra Control Service per la gestione dei dati delle app su cluster ROSA con storage Amazon FSX"

Dettagli dettagliati per creare snapshot e ripristinarle

Impostazione dei prerequisiti

- "Account AWS"
- "Account Red Hat OpenShift"
- Utente IAM con "autorizzazioni appropriate" Per creare e accedere al cluster ROSA
- "CLI AWS"
- "ROSA CLI"
- "CLI OpenShift"(oc)
- VPC con subnet e gateway e percorsi appropriati
- "ROSA Cluster installato" Nel VPC
- "Amazon FSX per NetApp ONTAP" Creato nello stesso VPC
- Accesso al gruppo ROSA da "Console di cloud ibrido OpenShift"

Passi successivi

1. Creare un utente amministratore e accedere al cluster.

2. Creare un file kubeconfig per il cluster.
3. Installare Astra Trident nel cluster.
4. Creare una configurazione backend, di classe storage e di classe Snapshot utilizzando il provisioner Trident CSI.
5. Implementare un'applicazione postgresql nel cluster.
6. Creare un database e aggiungere un record.
7. Aggiungere il cluster in ACS.
8. Definire l'applicazione in ACS.
9. Creare uno snapshot utilizzando ACS.
10. Eliminare il database nell'applicazione postgresql.
11. Ripristino da uno snapshot utilizzando ACS.
12. Verifica che l'app sia stata ripristinata dall'istantanea.

1. Creare un utente amministratore e accedere al cluster

Accedere al cluster ROSA creando un utente amministratore con il seguente comando: (È necessario creare un utente amministratore solo se non è stato creato uno al momento dell'installazione)

```
rosa create admin --cluster=<cluster-name>
```

Il comando fornirà un output simile a quello riportato di seguito. Accedere al cluster utilizzando `oc login` comando fornito nell'output.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

> È inoltre possibile accedere al cluster utilizzando un token. Se hai già creato un utente admin al momento della creazione del cluster, puoi accedere al cluster dalla console Red Hat OpenShift Hybrid Cloud con le credenziali admin-user. Quindi, facendo clic sull'angolo in alto a destra in cui viene visualizzato il nome dell'utente connesso, è possibile ottenere `oc login` comando (accesso token) per la riga di comando.

2. Creare un file kubeconfig per il cluster

Seguire le procedure "qui" Per creare un file kubeconfig per il cluster ROSA. Questo file kubeconfig verrà utilizzato in seguito quando si aggiunge il cluster in ACS.

3. Installare Astra Trident sul cluster

Installare Astra Trident (versione più recente) sul cluster ROSA. A tale scopo, è possibile seguire una qualsiasi delle procedure indicate "qui". Per installare Trident utilizzando helm dalla console del cluster, creare prima un progetto chiamato Trident.

Quindi, dalla vista sviluppatore, creare un archivio grafico Helm. Per il campo URL utilizzare `'https://netapp.github.io/trident-helm-chart'`. Quindi, creare una release helm per l'operatore Trident.

Project: trident

Create Helm Chart Repository

Add helm chart repository.

Configure via: (●) Form view ( ) YAML view

Scope type

( ) Namespaced scoped (ProjectHelmChartRepository)

Add Helm Chart Repository in the selected namespace.

(●) Cluster scoped (HelmChartRepository)

Add Helm Chart Repository at the cluster level and in all namespaces.

Name *

trident

A unique name for the Helm Chart repository.

Display name

Astra Trident

A display name for the Helm Chart repository.

Description

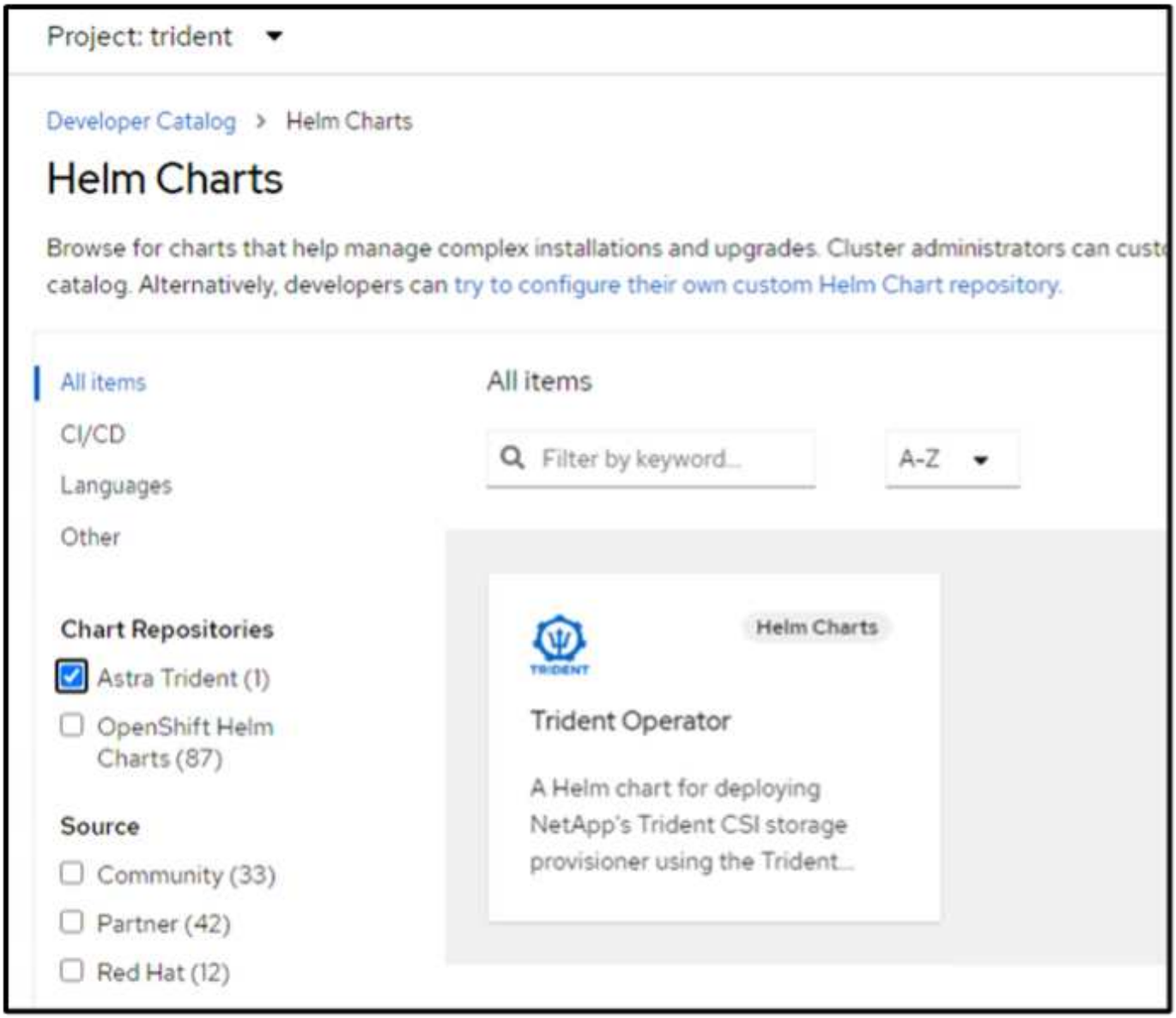
NetApp Astra Trident

A description for the Helm Chart repository.

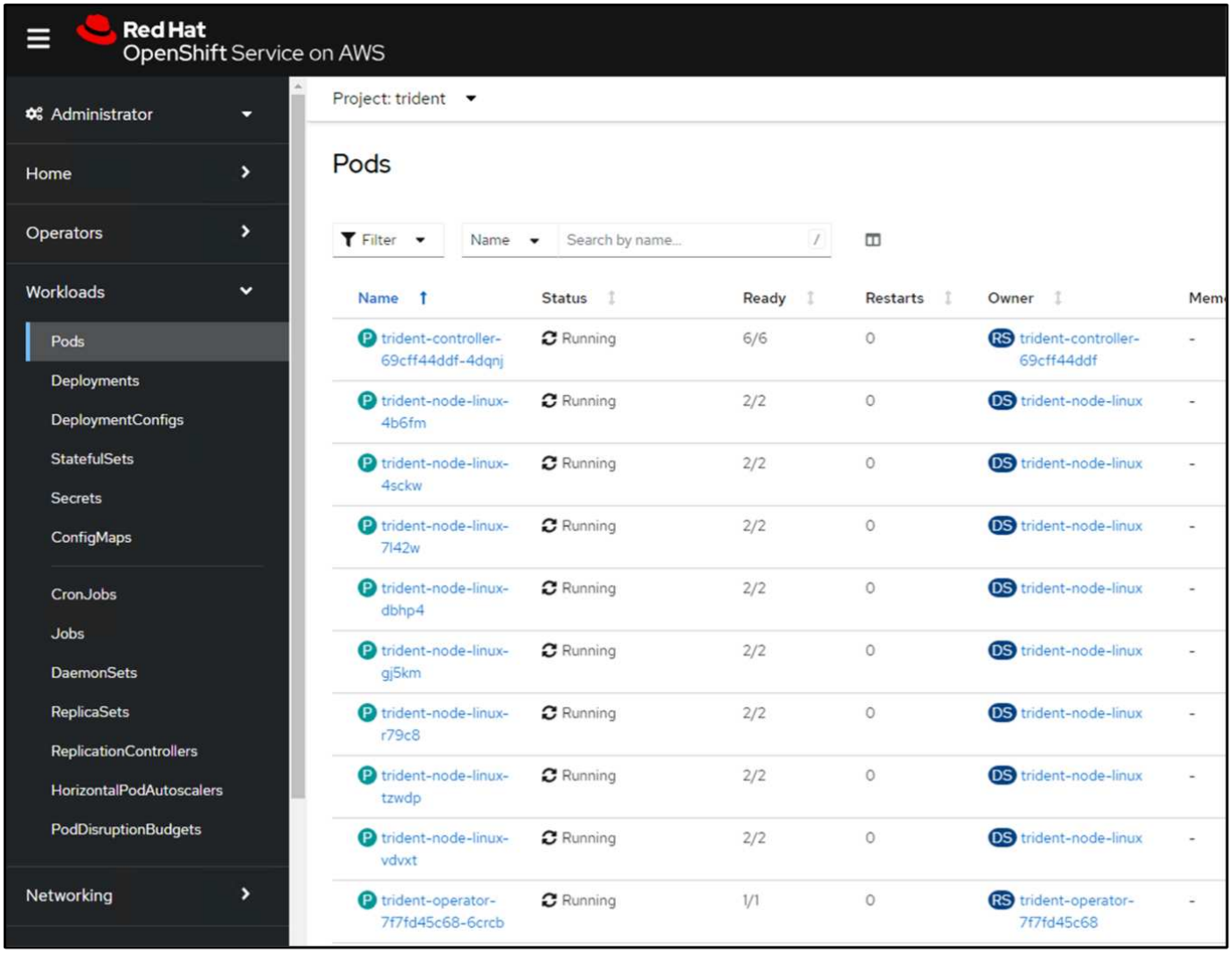
[ ] Disable usage of the repo in the developer catalog.

URL *

https://netapp.github.io/trident-helm-chart



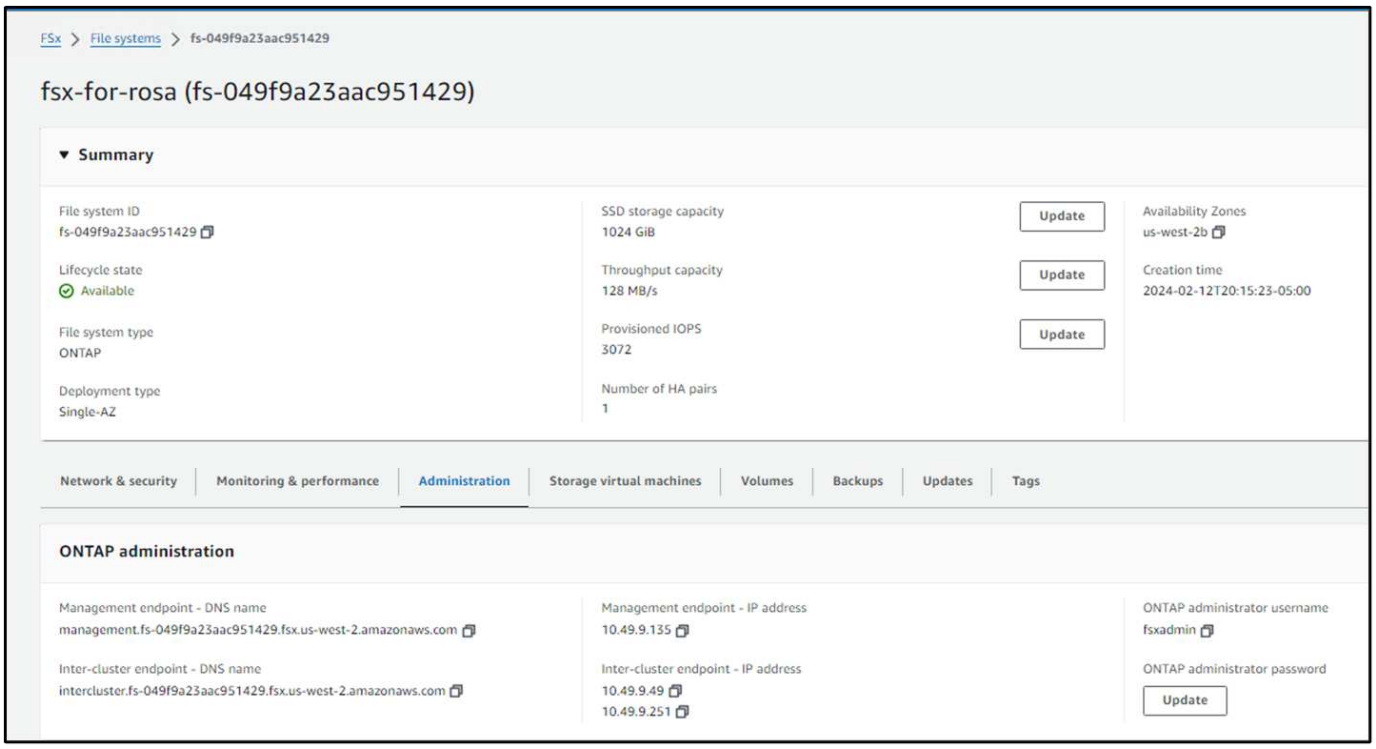
Verificare che tutti i pod di trident siano in esecuzione tornando alla vista Amministratore sulla console e selezionando i pod nel progetto trident.



4. Creare una configurazione backend, di classe storage e di classe snapshot utilizzando il provisioner Trident CSI

Utilizzare i file yaml illustrati di seguito per creare un oggetto backend tridente, un oggetto di classe di archiviazione e l'oggetto Volumesnapshot. Assicurati di fornire le credenziali al file system Amazon FSX per NetApp ONTAP che hai creato, la LIF di gestione e il nome del vserver del tuo file system nella configurazione yaml per il back-end. Per visualizzare questi dettagli, vai alla console AWS per Amazon FSX e seleziona il file system, quindi accedi alla scheda Administration (Amministrazione). Inoltre, fare clic su Update (Aggiorna) per impostare la password di `fsxadmin` utente.

> È possibile utilizzare la riga di comando per creare gli oggetti o con i file yaml dalla console del cloud ibrido.



Configurazione del backend Trident

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Classe di stoccaggio

```yaml
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

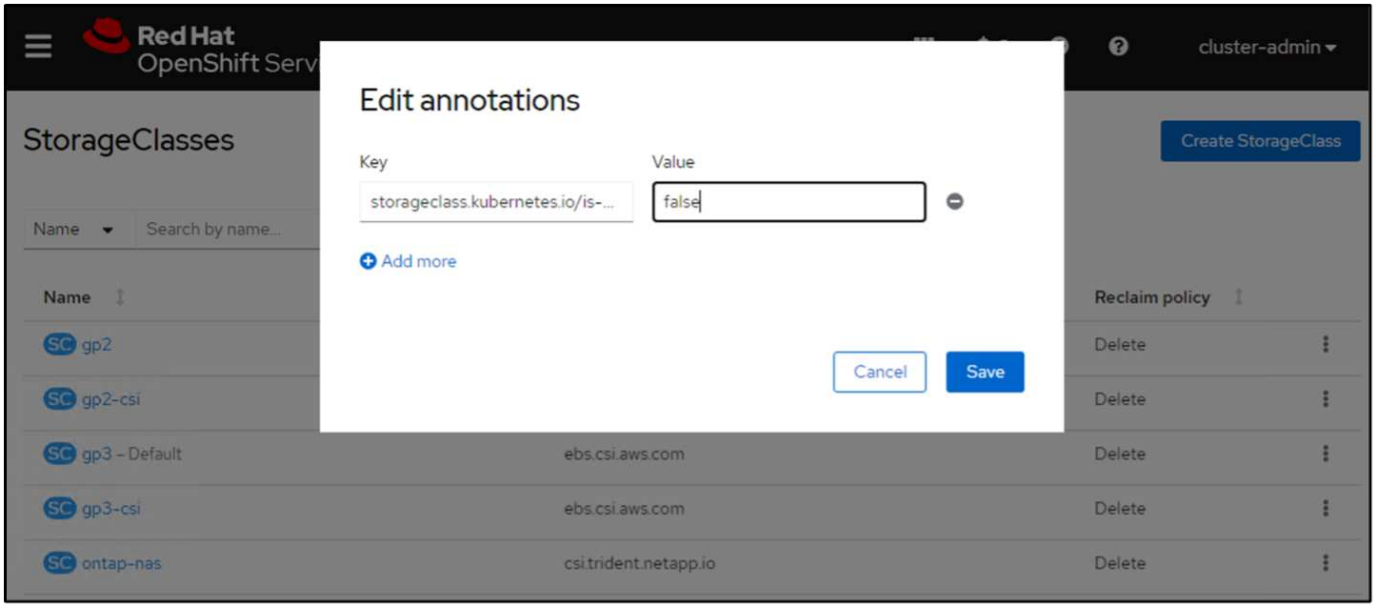
classe istantanea

```yaml
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Verificare che gli oggetti backend, di storage e trident-snapshotclass siano creati inviando i comandi indicati di seguito.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

In questo momento, un'importante modifica da apportare è impostare ontap-nas come classe di storage predefinita invece di GP3, in modo che l'app postgresql implementata in seguito possa utilizzare la classe di storage predefinita. Nella console OpenShift del cluster, in Storage selezionare StorageClasses. Modificare l'annotazione della classe predefinita corrente in modo che sia false e aggiungere l'impostazione della classe annotation storageclass.kuPensioni.io/is-default-class su true per la classe storage ontap-nas.



5. Distribuire un’applicazione postgresql sul cluster

È possibile distribuire l’applicazione dalla riga di comando nel modo seguente:

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Se i pod delle applicazioni non sono in esecuzione, potrebbe essersi verificato un errore dovuto ai vincoli del contesto di protezione.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                     TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql       ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl    ClusterIP   None            <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON                  OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer    persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate        statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate            statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Correggere l'errore modificando `runAsUser` e. `fsGroup` campi in `statefuleset.apps/postgresql` oggetto con l'uid che si trova nell'output di `oc get project` comando come illustrato di seguito.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

L'app postgresql deve essere in esecuzione e utilizzare volumi persistenti supportati da Amazon FSX per lo storage NetApp ONTAP.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME            READY   STATUS    RESTARTS   AGE
postgresql-0    1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

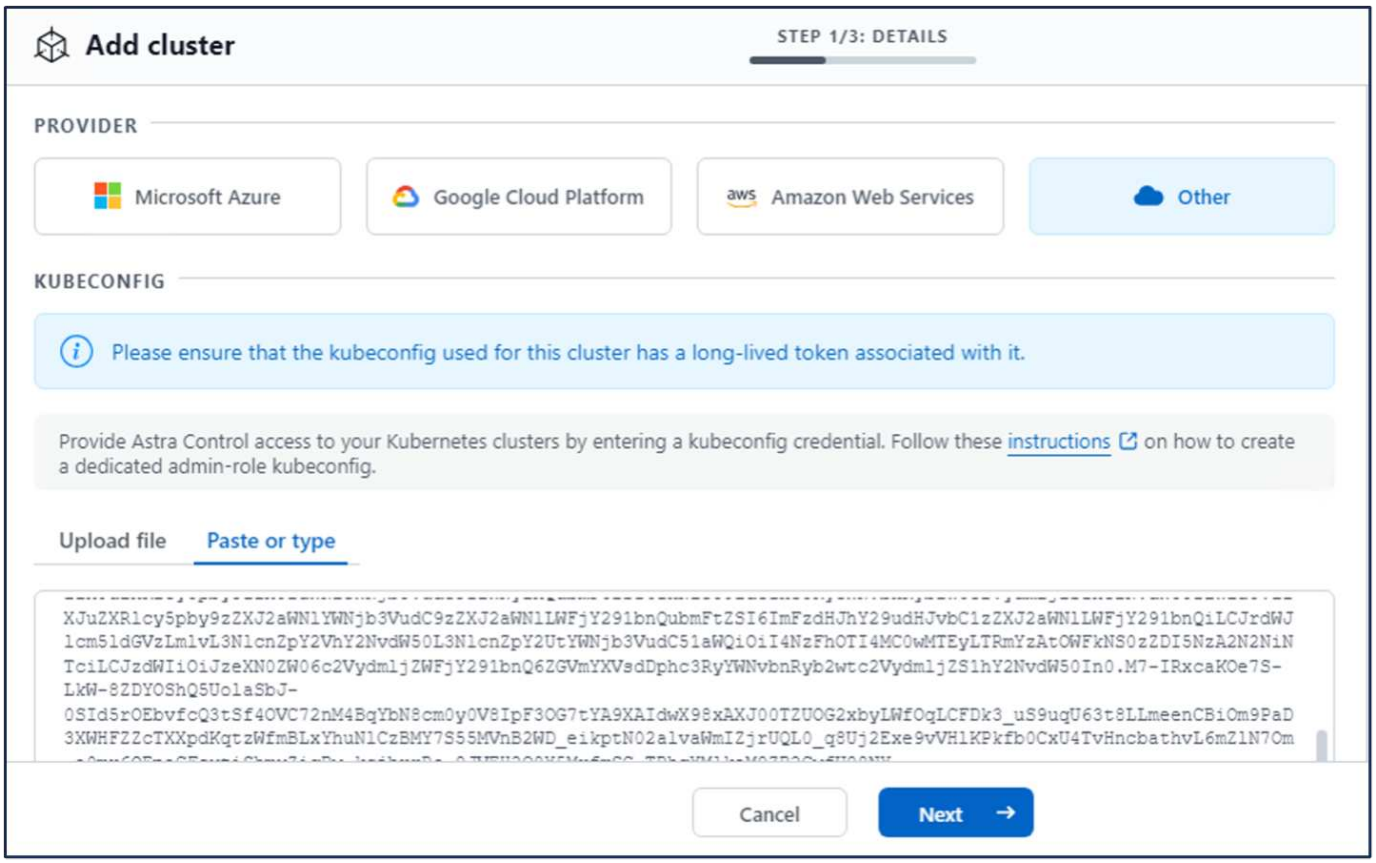
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Creare un database e aggiungere un record

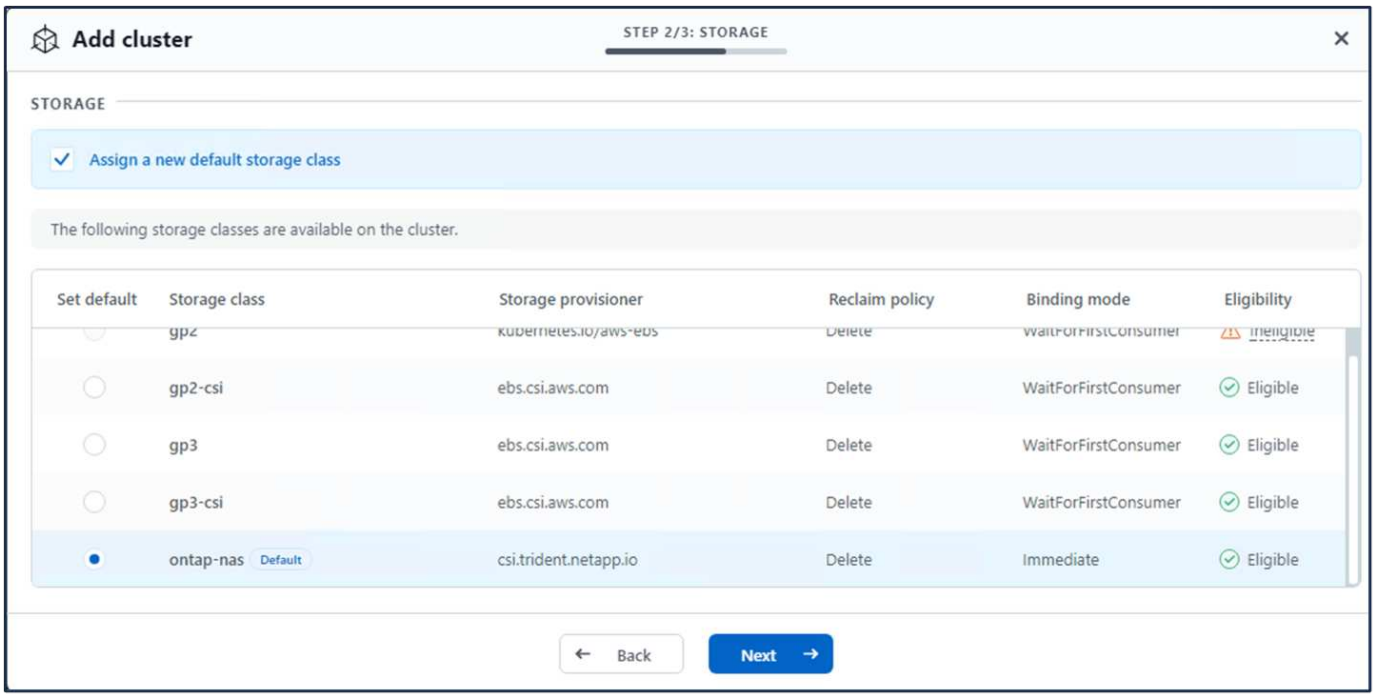
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
          List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Aggiungere il cluster in ACS

Accedere a ACS. Selezionare cluster e fare clic su Add. Selezionare Altro e caricare o incollare il file kubeconfig.



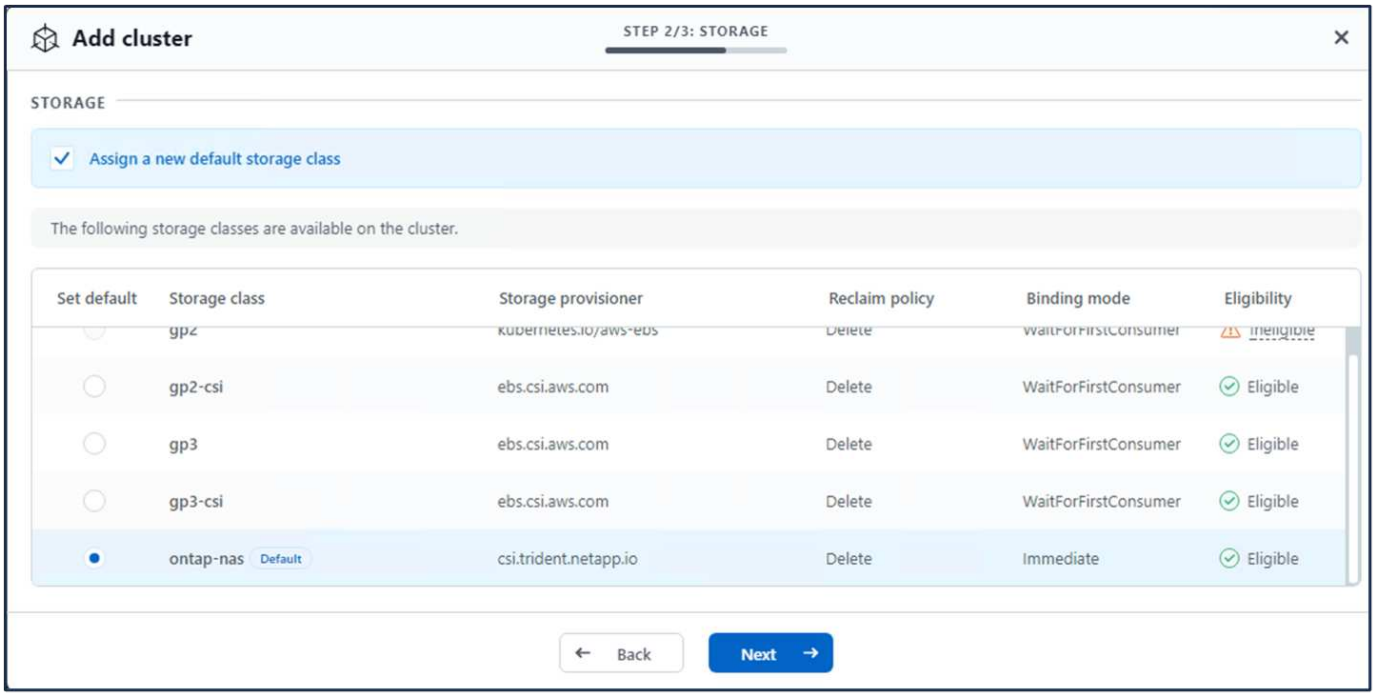
Fare clic su **Avanti** e selezionare ontap-nas come classe di storage predefinita per ACS. Fare clic su **Avanti**, rivedere i dettagli e **Aggiungi** il cluster.



8. Definire l'applicazione in ACS

Definire l'applicazione postgresql in ACS. Dalla pagina di destinazione, selezionare **applicazioni**, **Definisci** e inserire i dettagli appropriati. Fare clic su **Avanti** un paio di volte, rivedere i dettagli e fare clic su **Definisci**.

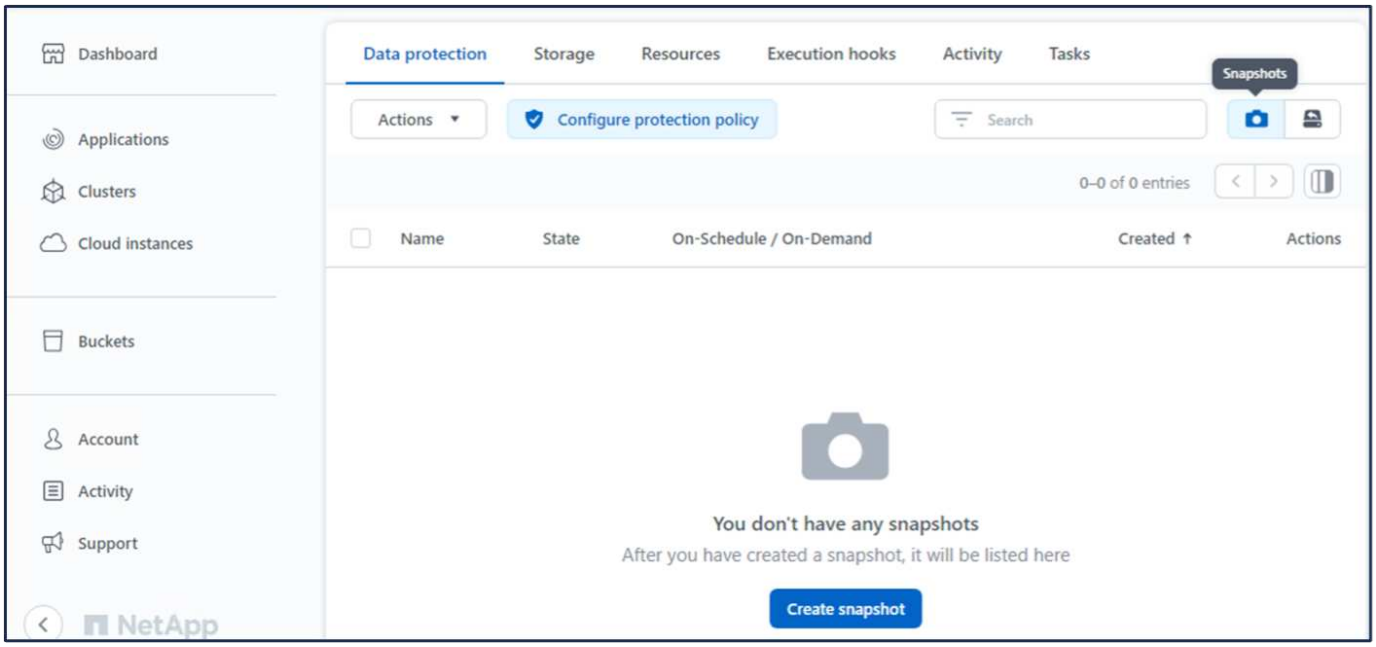
L'applicazione viene aggiunta a ACS.

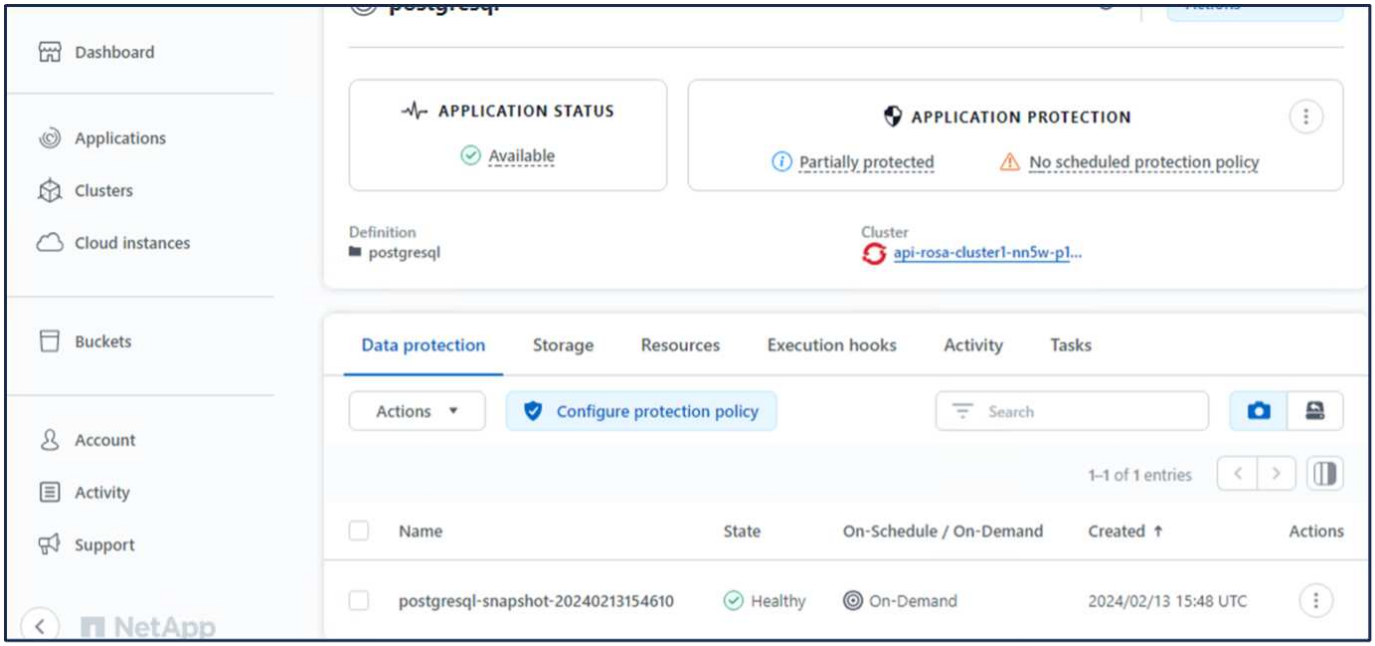


9. Creare un'istantanea utilizzando ACS

Esistono molti modi per creare uno snapshot in ACS. È possibile selezionare l'applicazione e creare un'istantanea dalla pagina che mostra i dettagli dell'applicazione. È possibile fare clic su Create Snapshot (Crea snapshot) per creare uno snapshot on-demand o configurare una policy di protezione.

Per creare un'istantanea su richiesta, è sufficiente fare clic su **Crea istantanea**, fornire un nome, rivedere i dettagli e fare clic su **istantanea**. Lo stato dell'istantanea diventa sano al termine dell'operazione.





10. Eliminare il database nell'applicazione postgresql

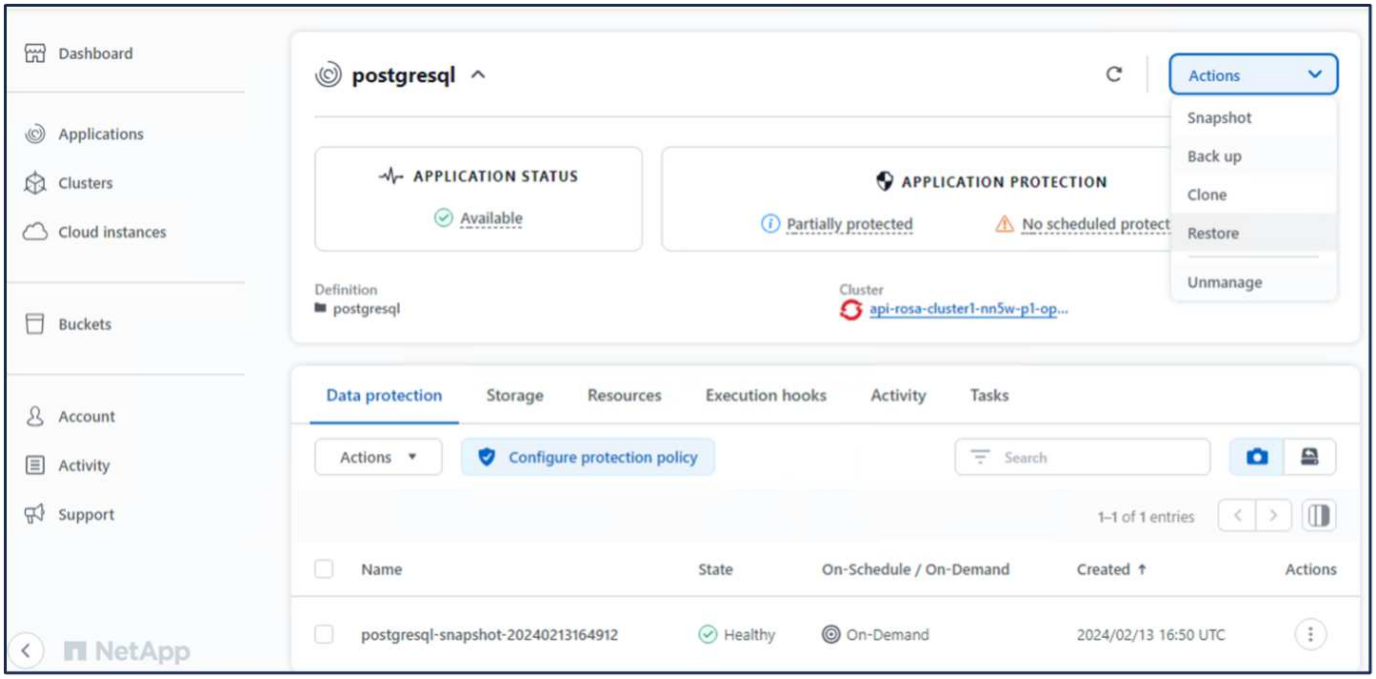
Accedere nuovamente a postgresql, elencare i database disponibili, eliminare quello creato in precedenza ed elencare nuovamente per assicurarsi che il database sia stato eliminato.

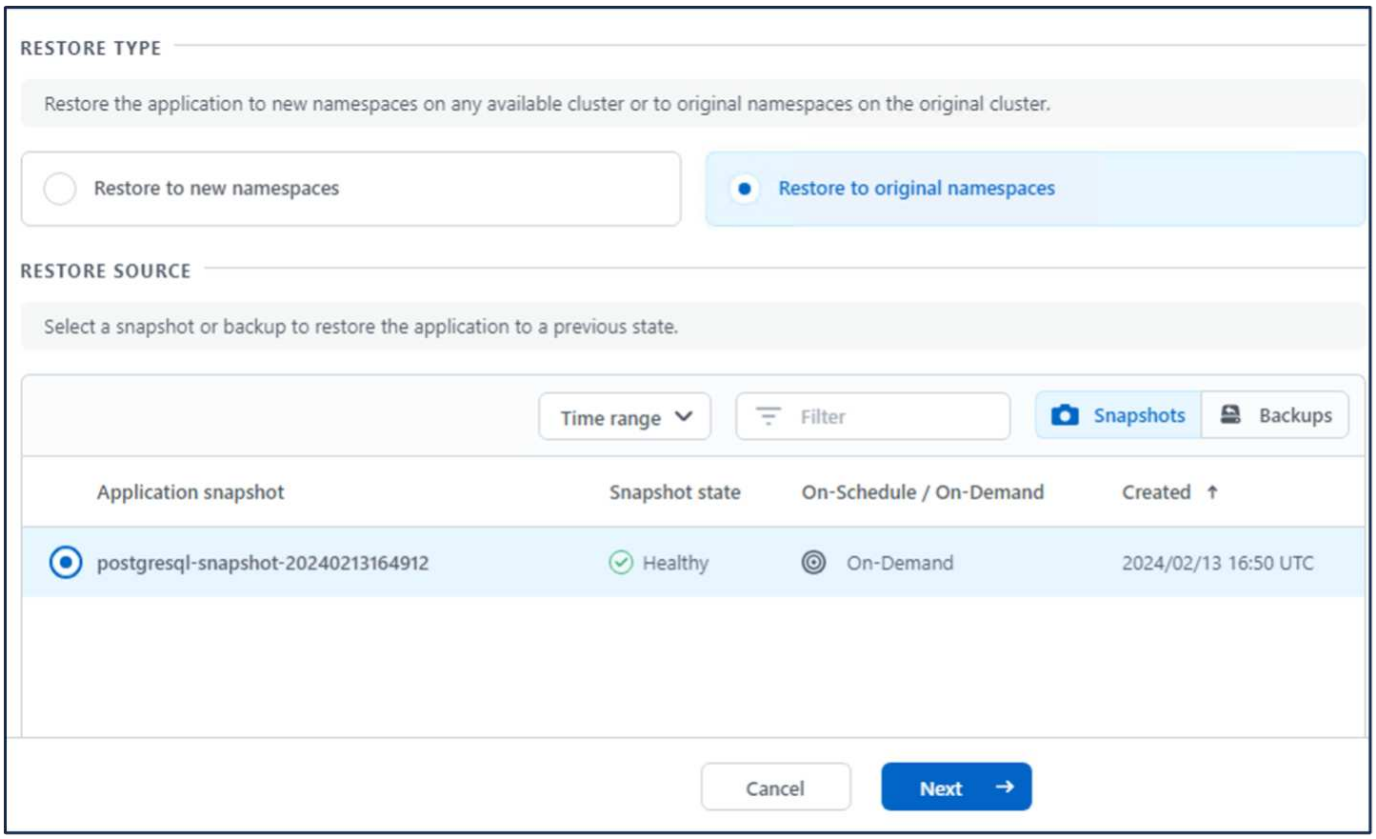
```
postgres=# \l
                                                    List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+---------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+          |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+          |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                    List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+---------------
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+          |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+          |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

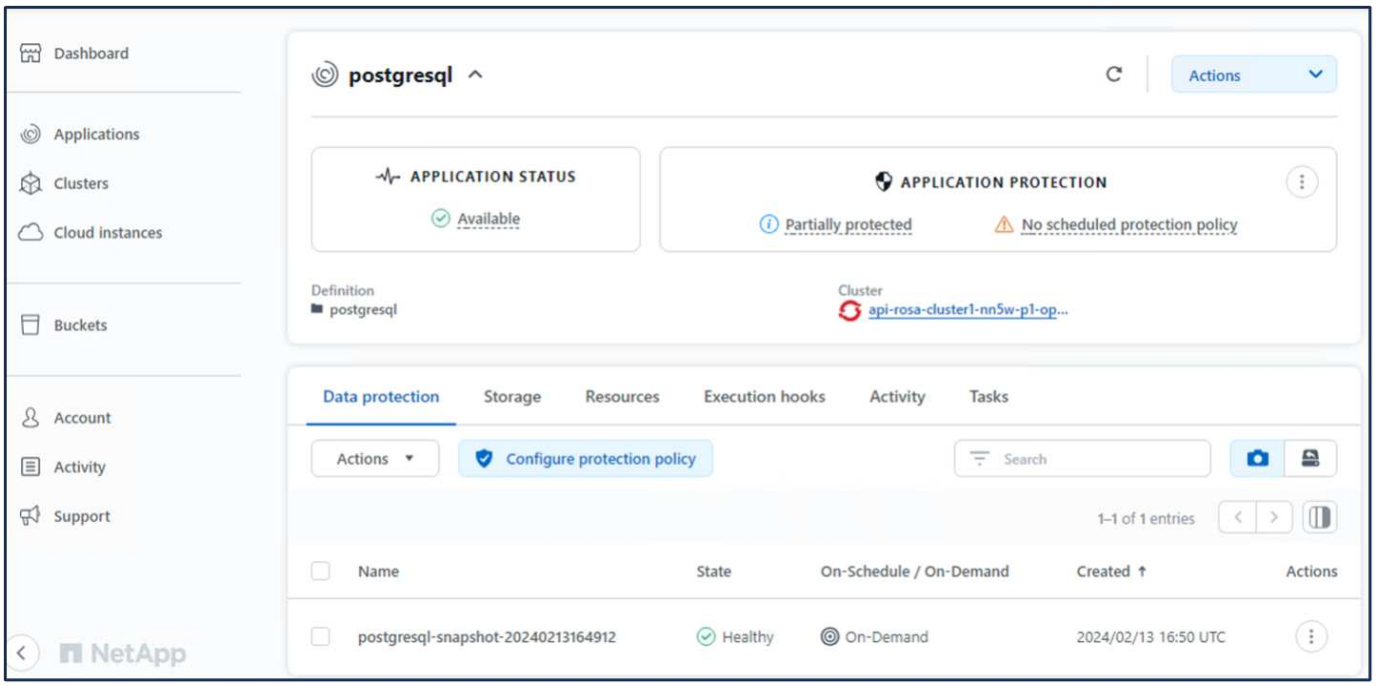
11. Ripristino da uno snapshot utilizzando ACS

Per ripristinare l'applicazione da uno snapshot, andare alla pagina di destinazione dell'interfaccia utente ACS,

selezionare l'applicazione e selezionare Ripristina. È necessario scegliere uno snapshot o un backup da cui eseguire il ripristino. (In genere, si creerebbero più criteri in base a un criterio configurato). Effettuare le scelte appropriate nelle due schermate successive, quindi fare clic su **Ripristina**. Lo stato dell'applicazione passa da Ripristino a disponibile dopo il ripristino dallo snapshot.







12. Verifica che l'app sia stata ripristinata dall'istantanea

Accedere al client postgresql e si dovrebbe ora vedere la tabella e il record nella tabella che si aveva in precedenza. Tutto qui. Basta fare clic su un pulsante per ripristinare lo stato precedente dell'applicazione. Con Astra Control, possiamo renderla semplice per i nostri clienti.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                   List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
          List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

Migrazione dei dati

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro container sui cluster gestiti Red Hat OpenShift che utilizzano FSX per NetApp ONTAP per lo storage persistente.

Migrazione dei dati

Il servizio Red Hat OpenShift su AWS e FSX per NetApp ONTAP (FSxN) fanno parte del loro portfolio di servizi di AWS. FSxN è disponibile nelle opzioni AZ singolo o AZ multiplo. L'opzione Multi-Az offre la protezione dei dati dai guasti della zona di disponibilità. FSxN può essere integrato con Astra Trident per fornire storage persistente per le applicazioni sui cluster ROSA.

Integrazione di FSxN con Trident utilizzando Helm Chart

Integrazione cluster ROSA con Amazon FSX per ONTAP

La migrazione delle applicazioni container comporta:

- Volumi persistenti: Questa operazione può essere eseguita utilizzando BlueXP. Un'altra opzione consiste nell'utilizzare Astra Control Center per gestire le migrazioni delle applicazioni container dall'ambiente on-premise a quello cloud. L'automazione può essere utilizzata per lo stesso scopo.
- Metadati dell'applicazione: È possibile eseguire questa operazione utilizzando OpenShift GitOps (Argo CD).

Failover e fail-back delle applicazioni sul cluster ROSA utilizzando FSxN per lo storage persistente

Il seguente video è una dimostrazione degli scenari di failover e fail-back delle applicazioni che utilizzano BlueXP e il CD Argo.

Failover e failback delle applicazioni sul cluster ROSA

Soluzione per la migrazione e la protezione dei dati per i carichi di lavoro dei container OpenShift