On-premise

NetApp Solutions

NetApp
April 26, 2024

Sommario

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

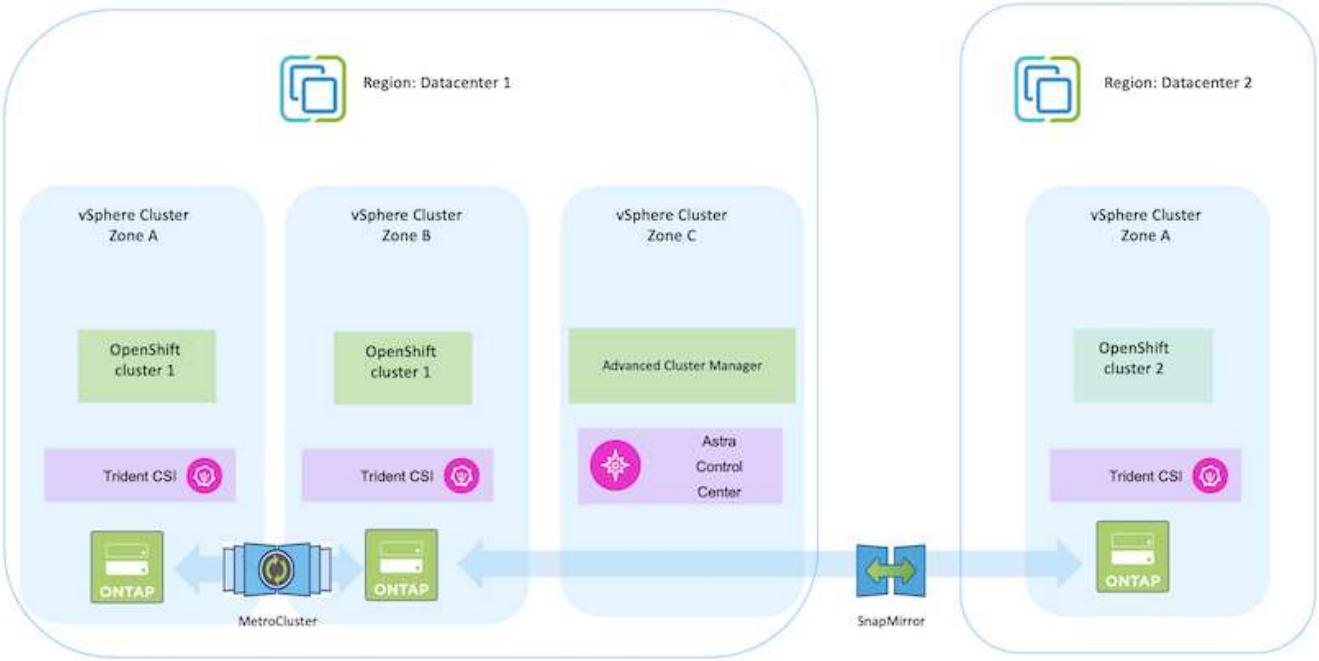
Se i clienti hanno la necessità di eseguire le loro moderne applicazioni containerizzate su un'infrastruttura nei propri data center privati, possono farlo. Devono pianificare e implementare la piattaforma container Red Hat OpenShift (OCP) per un ambiente pronto per la produzione di successo per l'implementazione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

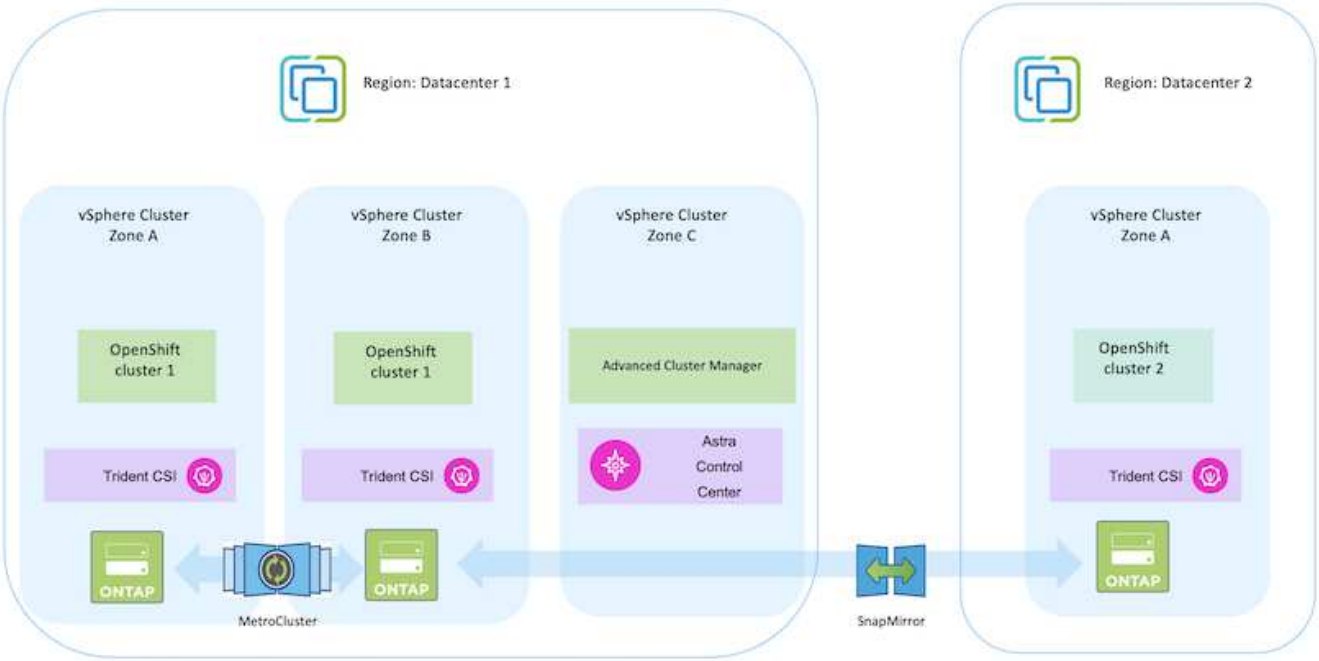


Implementare e configurare la piattaforma container Red Hat OpenShift su VMware

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.

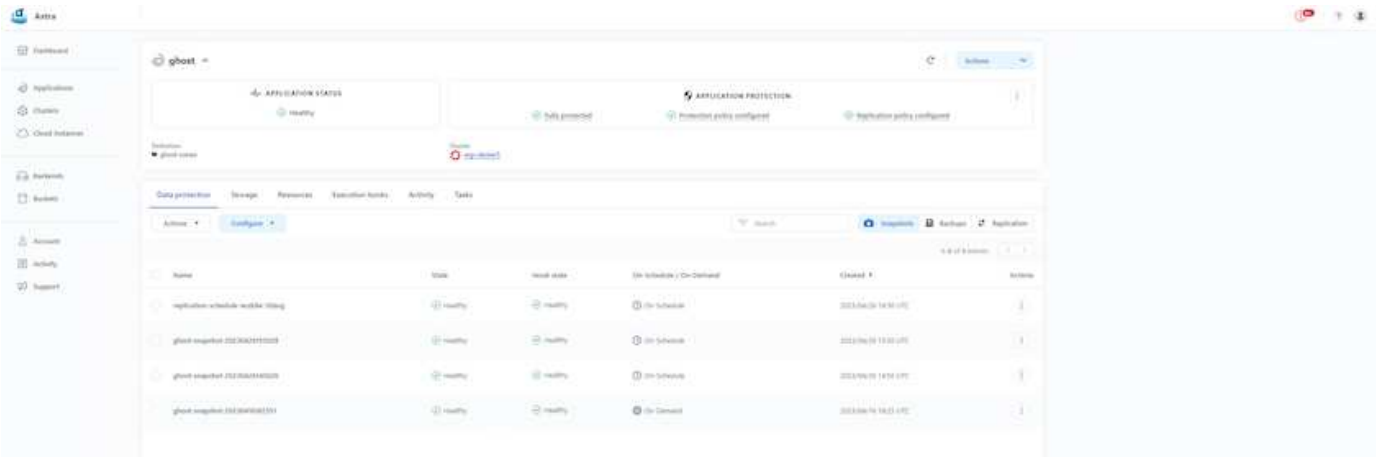
La protezione dei dati in ONTAP può essere ottenuta utilizzando ad-hoc o policy controllate - **Snapshot** - **backup e ripristino**

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

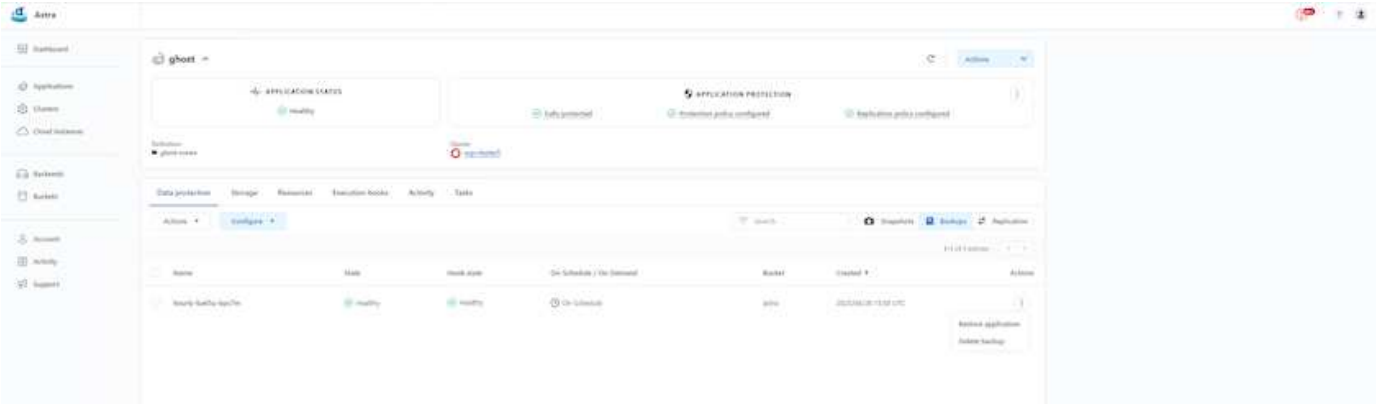


Backup e ripristino con ACC

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.



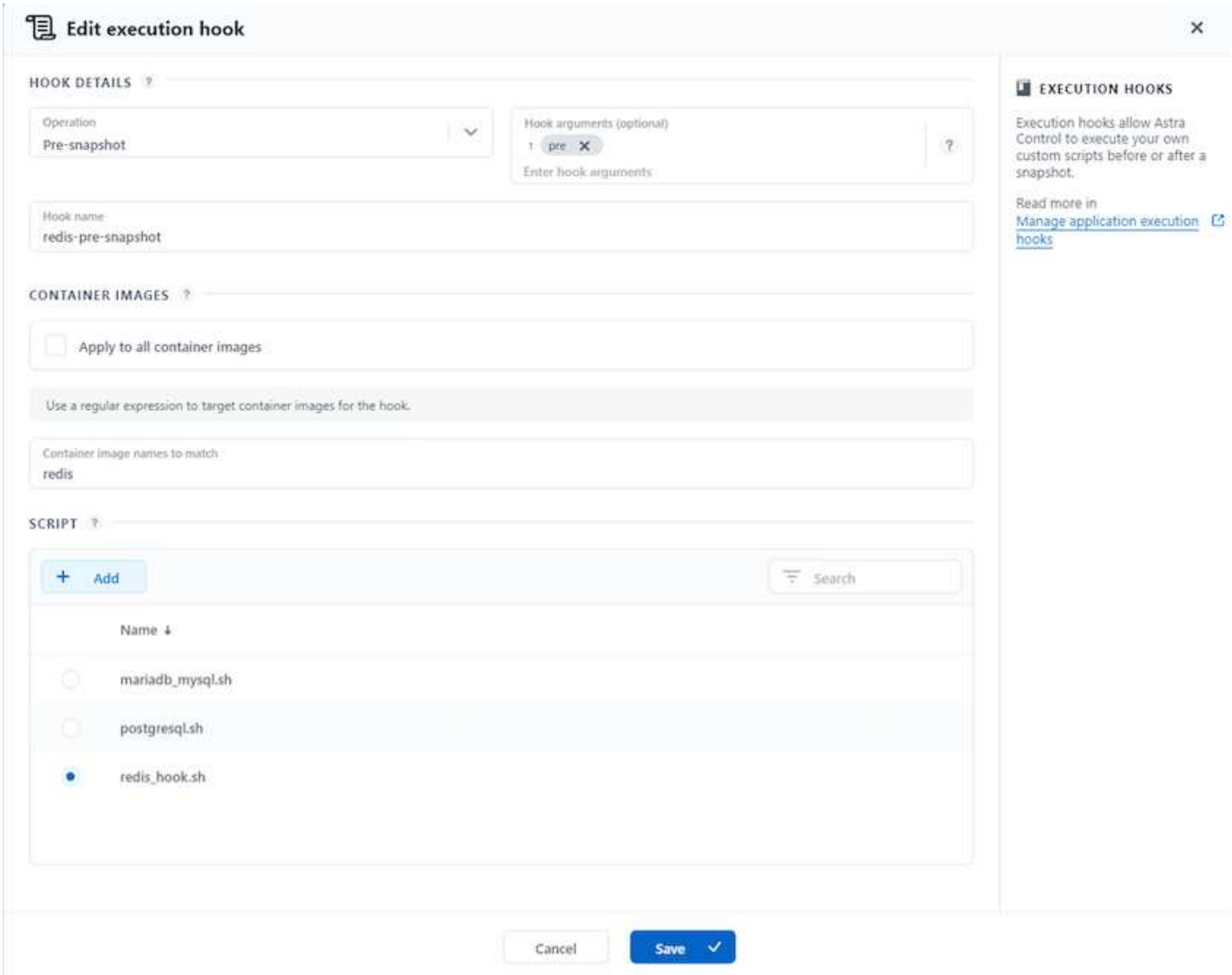
Hook di esecuzione specifici dell'applicazione

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.



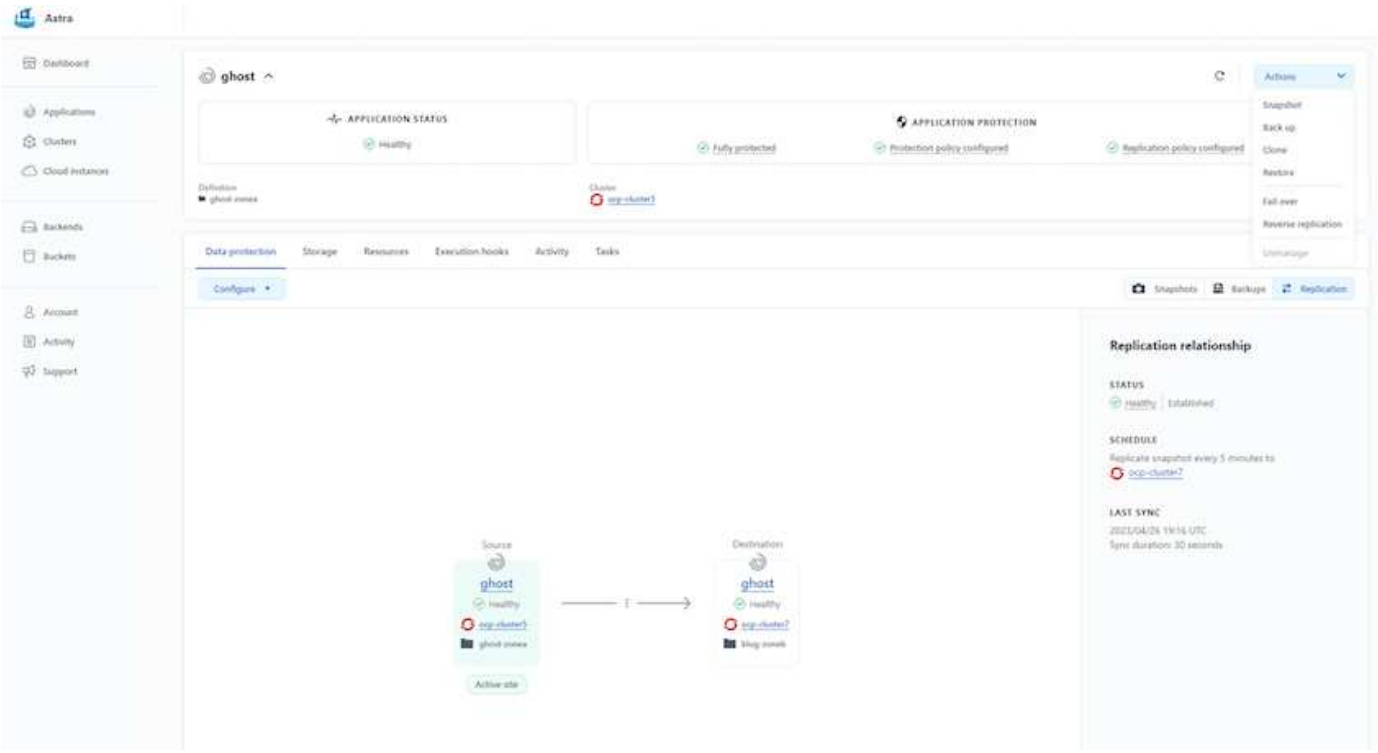
Replica con ACC

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"

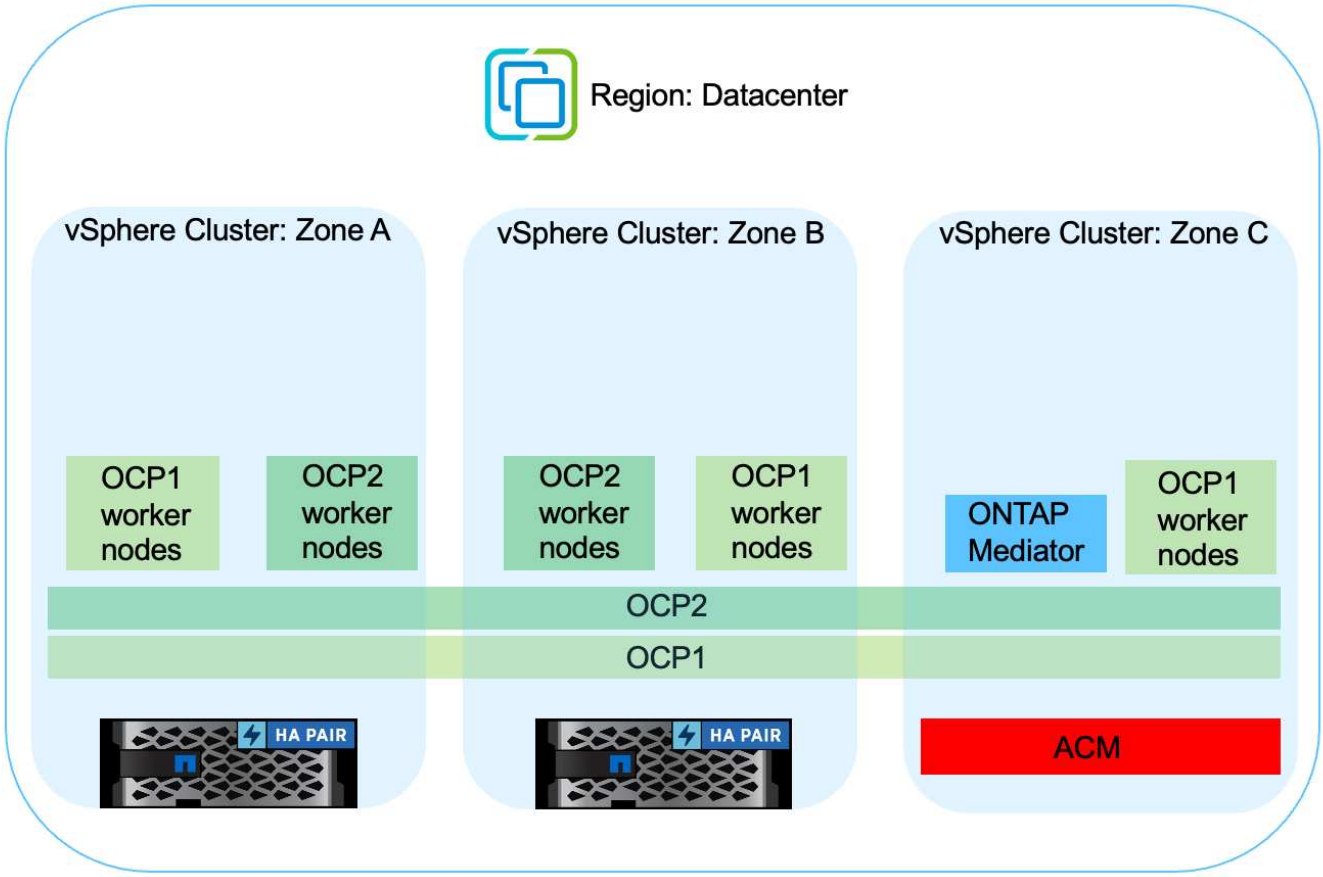
Data Protection con Astra Control Center

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