Cloud ibrido con componenti a gestione autonoma (on-premise/AWS/GCP/Azure)

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.

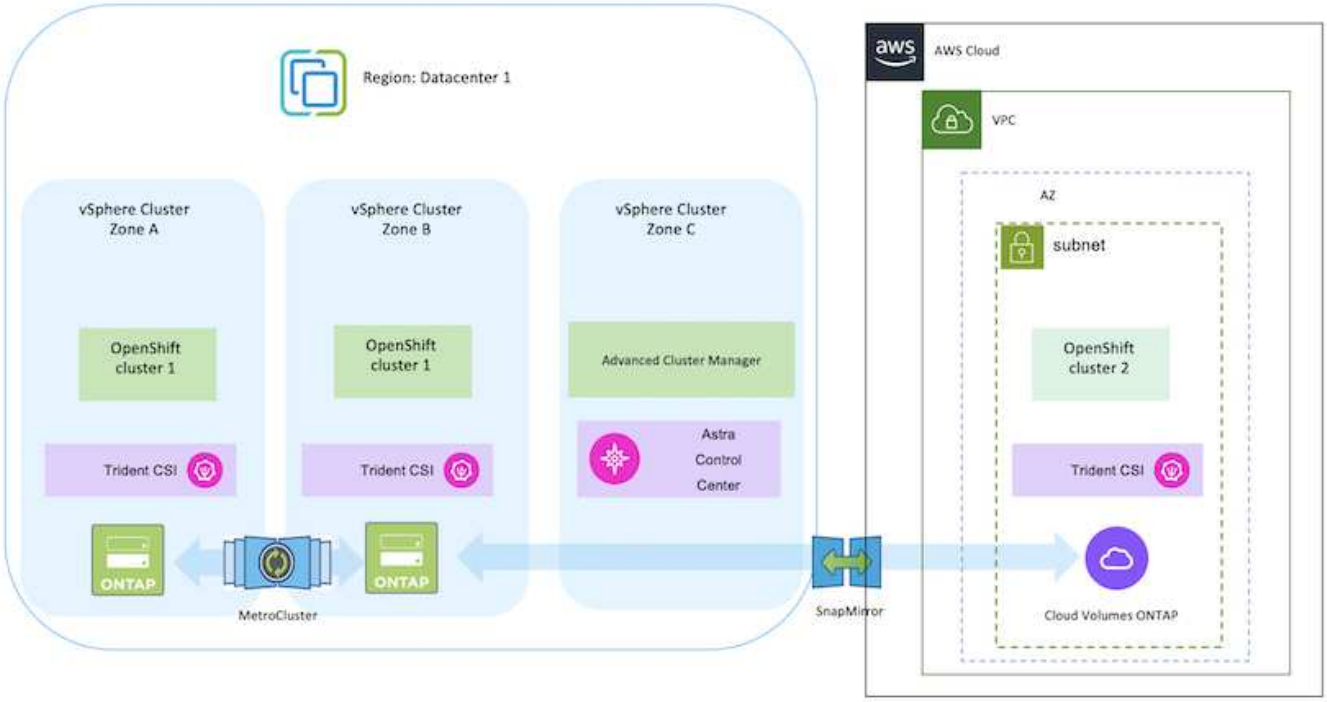
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido

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.

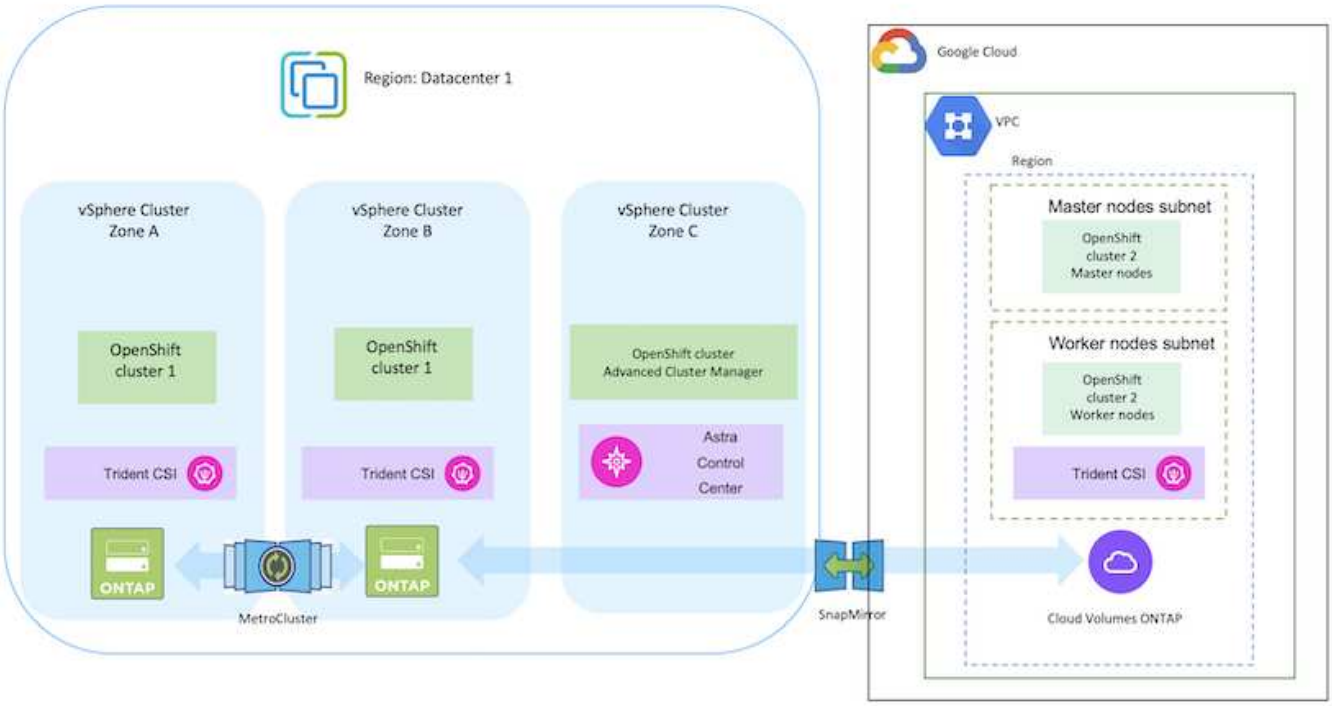
Lo storage NetApp Cloud Volumes ONTAP offre protezione dei dati, affidabilità e flessibilità per le implementazioni di container in AWS, Azure e Google Cloud. Astra Trident funge da provider di storage dinamico per consumare lo storage Cloud Volumes ONTAP persistente per le applicazioni stateful dei 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

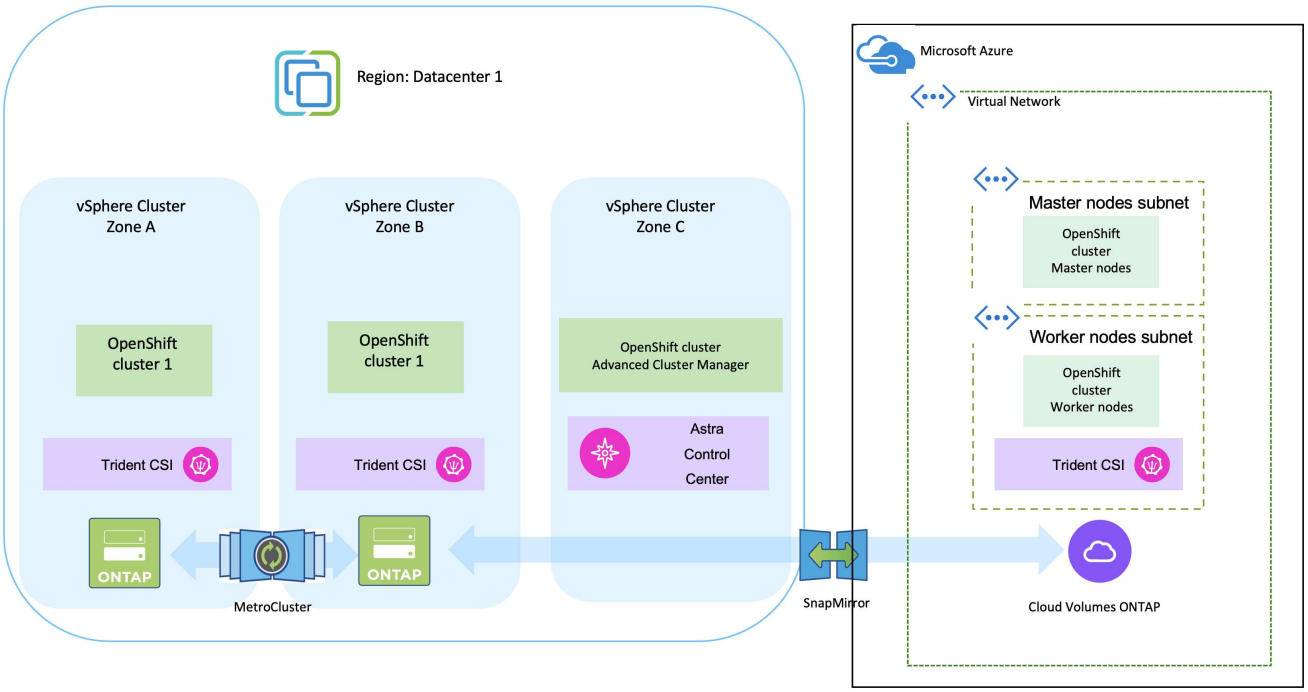
On-premise e in AWS



On-premise e Google Cloud



Azure Cloud e on-premise

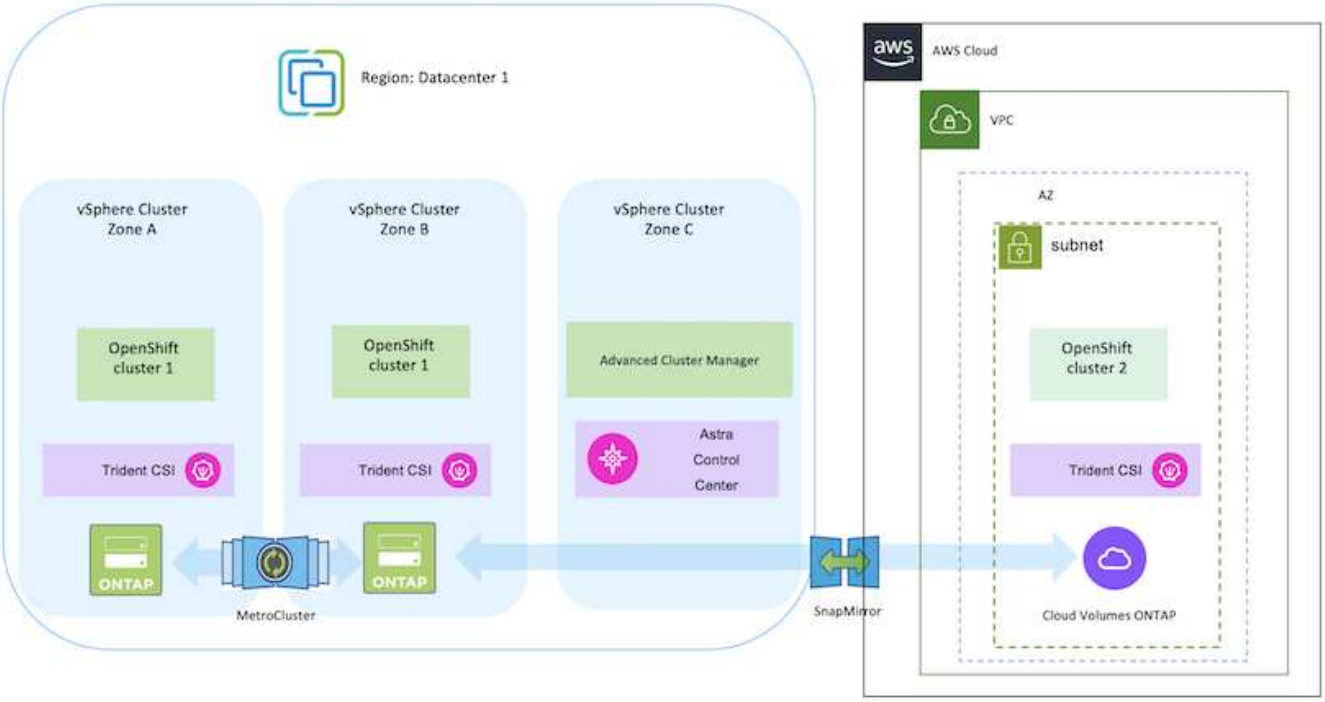


Implementa e configura la piattaforma container Red Hat OpenShift su AWS

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.

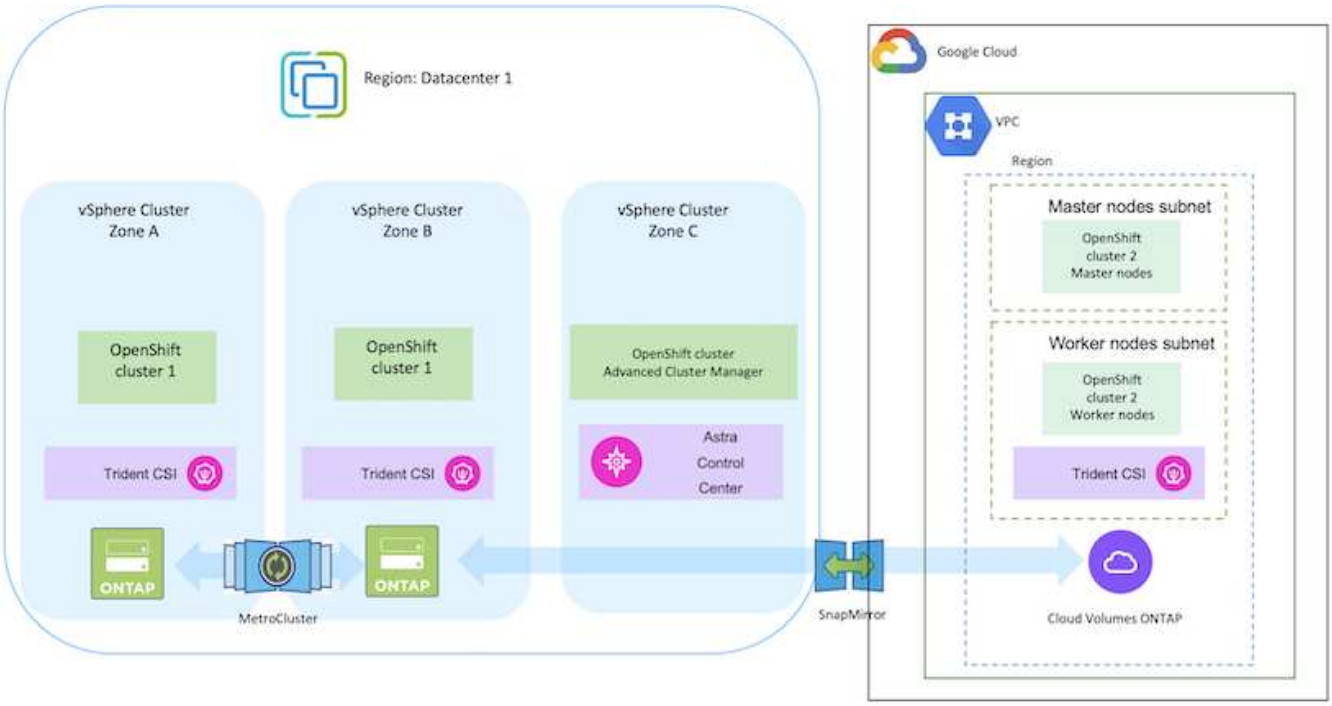
Implementare e configurare la piattaforma Red Hat OpenShift Container su GCP

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

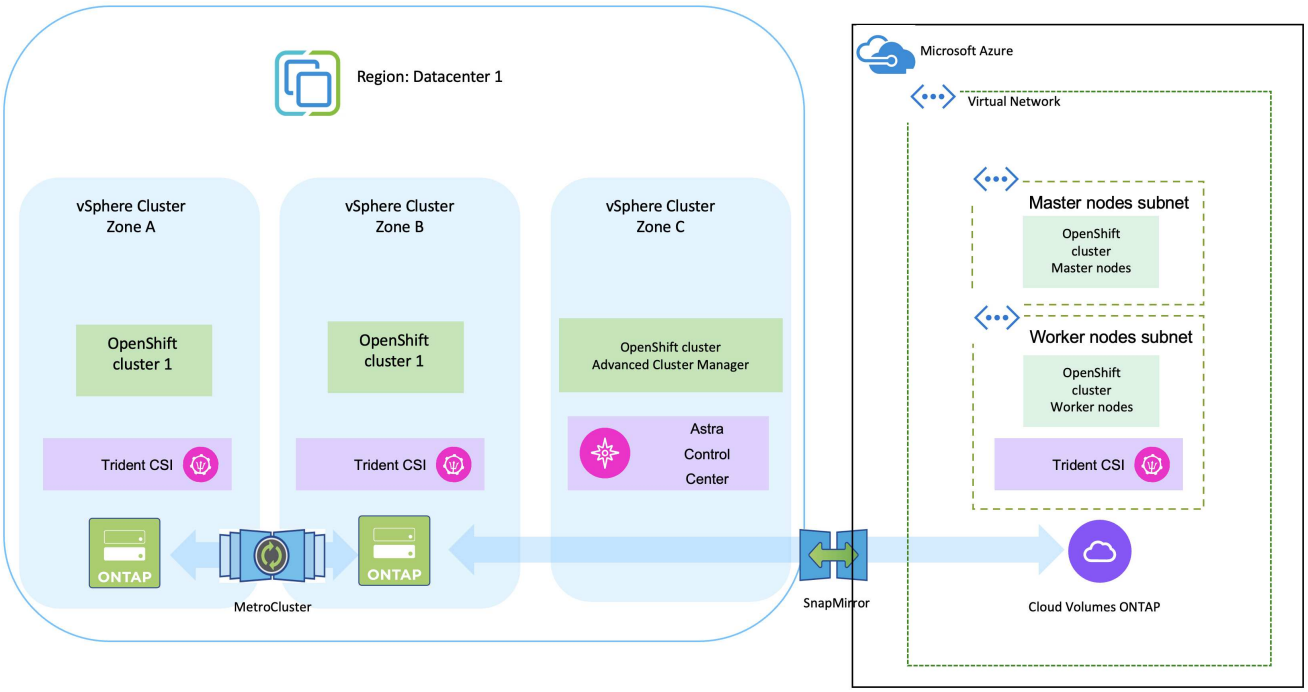
Importazione dei cluster OpenShift in Astra Control Center

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.

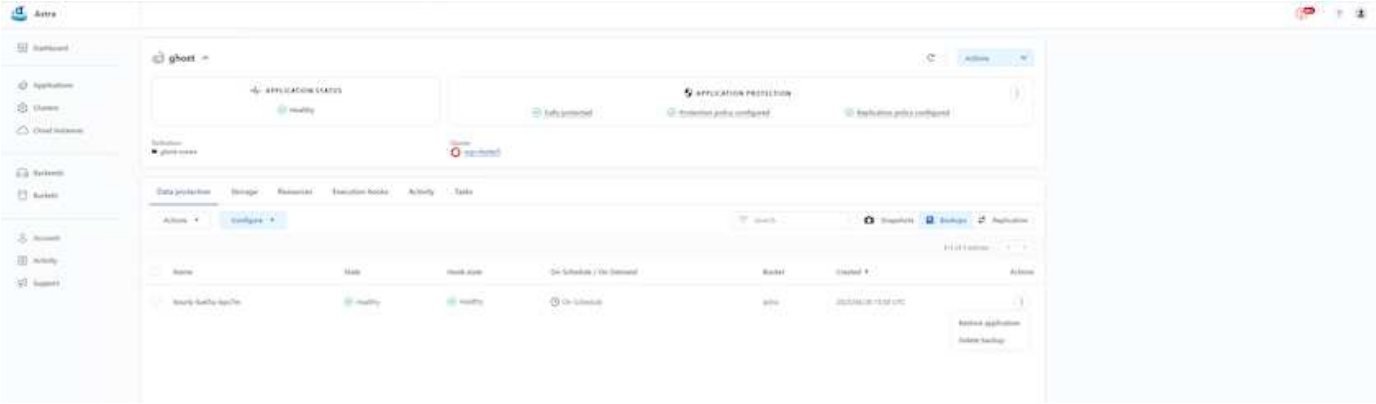
I clienti possono avere un ambiente cloud configurato come estensione del data center, in modo che possano sfruttare i benefici del cloud e essere in grado di spostare i propri carichi di lavoro in un momento futuro. Per

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

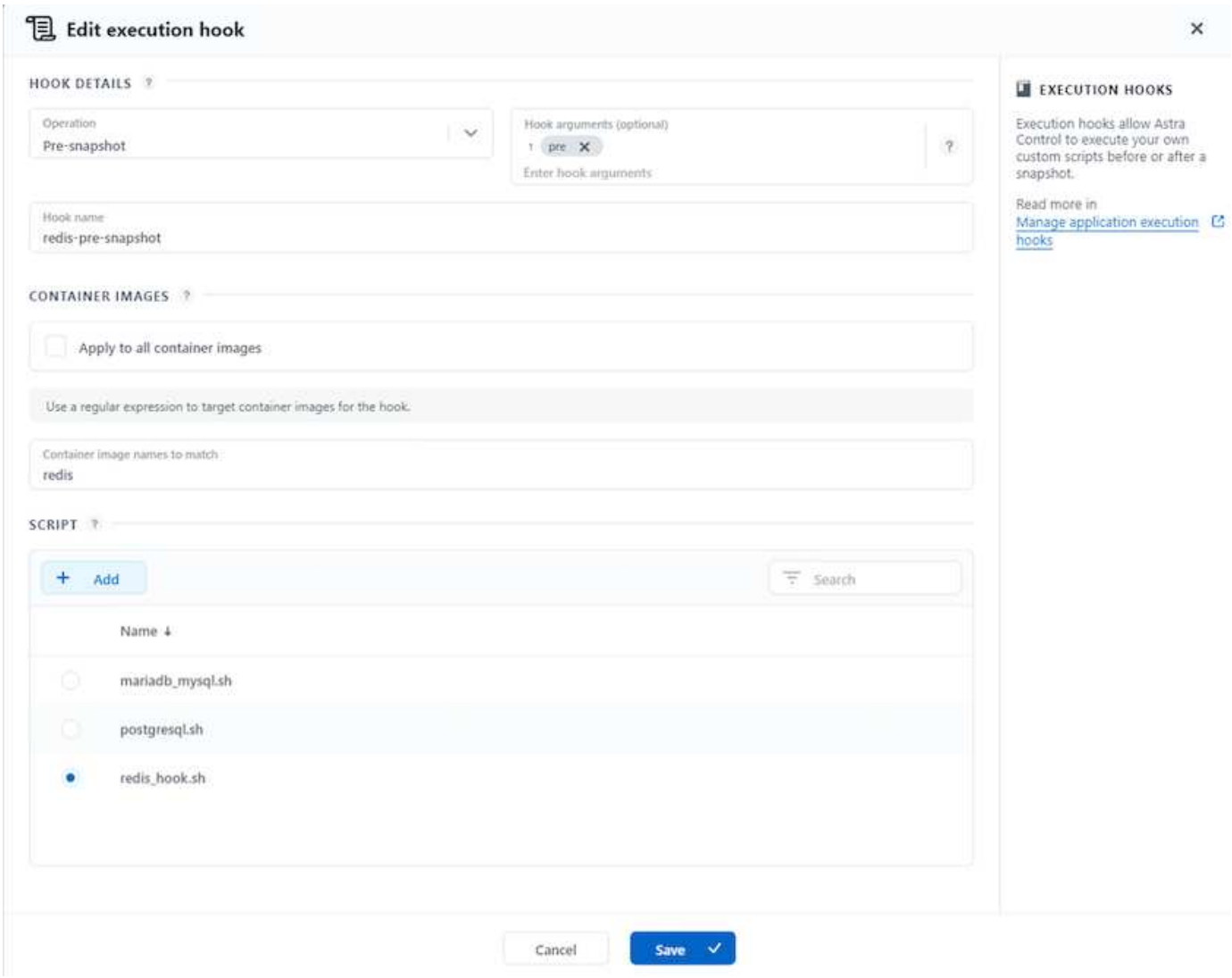


Hook di esecuzione specifici dell'applicazione

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.

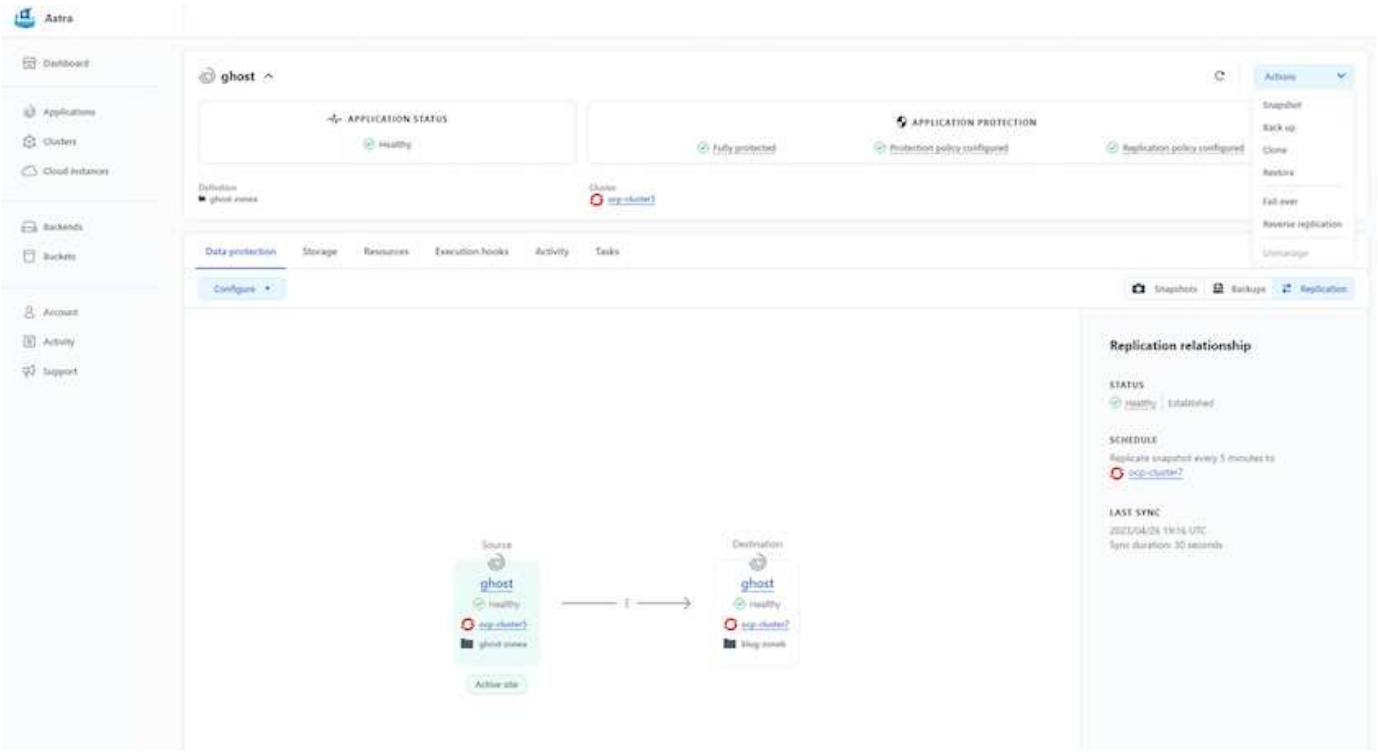
Esempio di gancio di esecuzione per pre-Snapshot di un'applicazione redis.



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