Openshift per ambienti on-premise

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-cloud/openshift/os-op-solution.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommario

Openshift per ambienti on-premise . . . 1
- Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware . . . 1
  - Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container utilizzando Trident Protect . . . 1
- Distribuisci e configura la piattaforma Red Hat OpenShift Container su VMware . . . 1
- Protezione dei dati tramite Astra . . . 4
  - Istantanea con ACC . . . 4
  - Backup e ripristino con ACC . . . 5
  - Hook di esecuzione specifici dell'applicazione . . . 5
  - Esempio di hook di esecuzione per il pre-Snapshot di un'applicazione Redis. . . . 5
  - Replica con ACC . . . 6
  - Continuità aziendale con MetroCluster . . . 7
- Migrazione dei dati tramite Trident Protect . . . 8
  - Migrazione dei dati tra diversi ambienti Kubernetes . . . 8

Openshift per ambienti on-premise

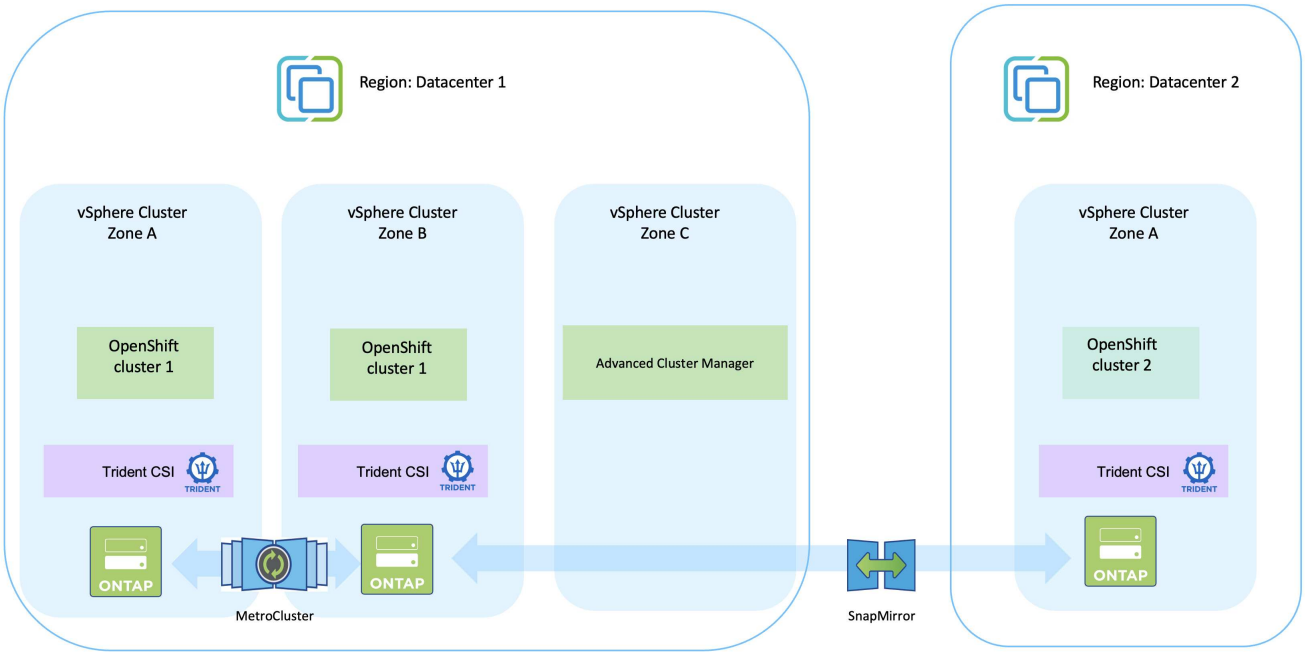
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift su VMware

Se i clienti hanno la necessità di eseguire le loro moderne applicazioni containerizzate sull'infrastruttura dei loro data center privati, possono farlo. Dovrebbero pianificare e distribuire la piattaforma container Red Hat OpenShift (OCP) per un ambiente di produzione di successo per la distribuzione dei carichi di lavoro dei container. I loro cluster OCP possono essere distribuiti su VMware o bare metal.

Lo storage NetApp ONTAP garantisce protezione dei dati, affidabilità e flessibilità per le distribuzioni di container. Trident funge da fornitore di storage dinamico per utilizzare lo storage ONTAP persistente per le applicazioni stateful dei clienti. NetApp Trident Protect può essere utilizzato per i numerosi requisiti di gestione dei dati delle applicazioni con stato, quali protezione dei dati, migrazione e continuità aziendale.

Con VMware vSphere, gli strumenti NetApp ONTAP forniscono un plug-in vCenter che può essere utilizzato per il provisioning degli archivi dati. Applica i tag e utilizzali con OpenShift per memorizzare la configurazione e i dati del nodo. L'archiviazione basata su NVMe garantisce una latenza inferiore e prestazioni elevate.

Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container utilizzando Trident Protect



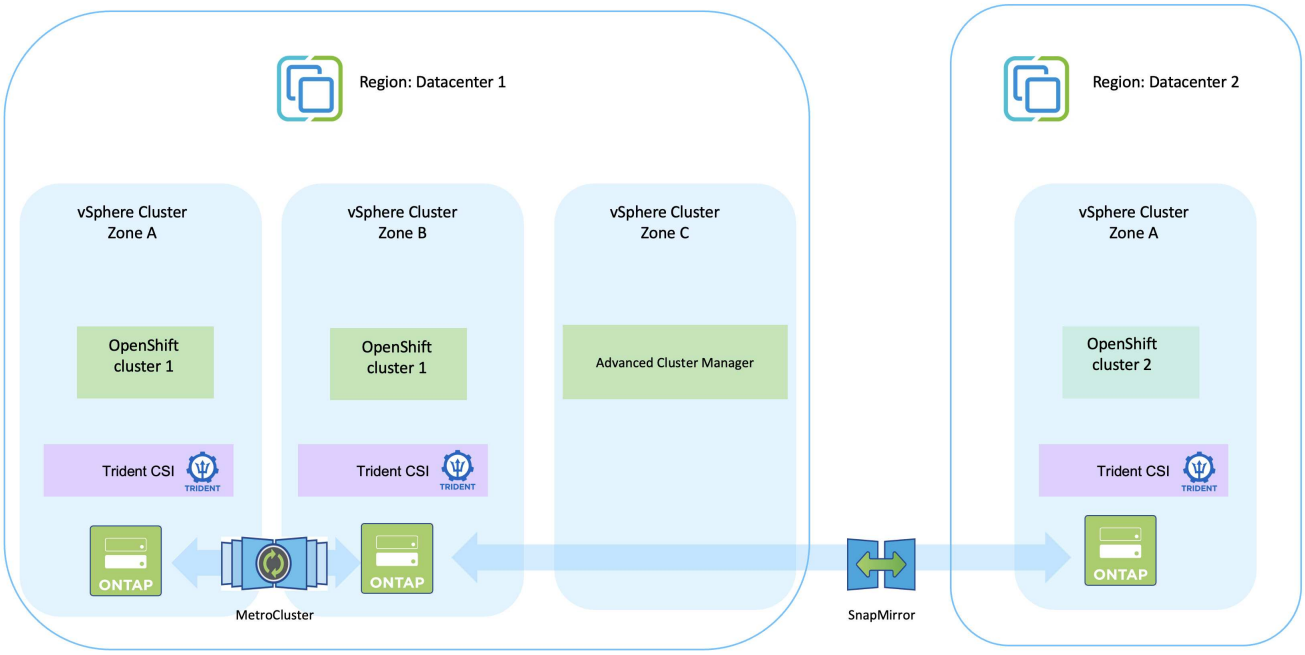
Distribuisci e configura la piattaforma Red Hat OpenShift Container su VMware

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i

cluster OpenShift e le applicazioni con stato su di essi. Mostra l'utilizzo di array di storage NetApp ONTAP con l'ausilio di Trident per fornire volumi persistenti.

> Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container. Questa descrizione di alto livello della configurazione fornisce link alla documentazione per il metodo specifico utilizzato. È possibile fare riferimento agli altri metodi nei link pertinenti forniti nel"sezione risorse" .

Ecco un diagramma che illustra i cluster distribuiti su VMware in un data center.



Il processo di configurazione può essere suddiviso nei seguenti passaggi:

Distribuisci e configura una VM CentOS

- Viene distribuito nell'ambiente VMware vSphere.
- Questa VM viene utilizzata per distribuire alcuni componenti della soluzione, come NetApp Trident e NetApp Trident Protect.
- Durante l'installazione, su questa VM viene configurato un utente root.

Distribuisci e configura un cluster OpenShift Container Platform su VMware vSphere (Hub Cluster)

Fare riferimento alle istruzioni per l'uso"Distribuzione assistita" metodo per distribuire un cluster OCP.

> Ricordare quanto segue: - Creare una chiave pubblica e privata ssh da fornire al programma di installazione. Queste chiavi verranno utilizzate per accedere ai nodi master e worker, se necessario. - Scaricare il programma di installazione dall'installatore assistito. Questo programma viene utilizzato per avviare le VM create nell'ambiente VMware vSphere per i nodi master e worker. - Le VM devono avere i requisiti minimi di CPU, memoria e disco rigido. (Fare riferimento ai comandi vm create su"Questo" pagina per il master e i nodi worker che forniscono queste informazioni) - Il diskUUID deve essere abilitato su tutte le VM. - Creare almeno 3 nodi per il master e 3 nodi per il worker. - Una volta rilevati dal programma di installazione, attivare il pulsante di integrazione VMware vSphere.

Installa Advanced Cluster Management sul cluster Hub

L'installazione avviene tramite l'Advanced Cluster Management Operator sul cluster Hub. Fare riferimento alle istruzioni"Qui" .

Installa due cluster OCP aggiuntivi (origine e destinazione)

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

Configurare l'archiviazione NetApp ONTAP

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

Installa NetApp Trident sui cluster OCP

- Installa NetApp Trident su tutti e tre i cluster: hub, origine e destinazione
- Fare riferimento alle istruzioni"Qui" .
- Creare un backend di archiviazione per ontap-nas.
- Creare una classe di archiviazione per ontap-nas.
- Fare riferimento alle istruzioni"Qui" .

Distribuire un'applicazione sul cluster di origine

Utilizzare OpenShift GitOps per distribuire un'applicazione. (ad esempio Postgres, Ghost)

Il passaggio successivo consiste nell'utilizzare Trident Protect per la protezione dei dati e la migrazione dei dati

dal cluster di origine a quello di destinazione. Fare riferimento"Qui" per istruzioni.

Protezione dei dati tramite Astra

Questa pagina mostra le opzioni di protezione dei dati per le applicazioni basate su Red Hat OpenShift Container in esecuzione su VMware vSphere mediante Trident Protect (ACC).

Mentre gli utenti intraprendono il loro percorso di modernizzazione delle applicazioni con Red Hat OpenShift, è necessario adottare una strategia di protezione dei dati per proteggerli da eliminazioni accidentali o da altri errori umani. Spesso è necessaria anche una strategia di protezione per motivi normativi o di conformità, per proteggere i dati da un disastro.

I requisiti di protezione dei dati variano dal ripristino di una copia in un dato momento al failover automatico su 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 numerose funzionalità, come multitenancy, multiprotocollo, elevate prestazioni e capacità, replicazione e memorizzazione nella cache per sedi multi-sito, sicurezza e flessibilità.

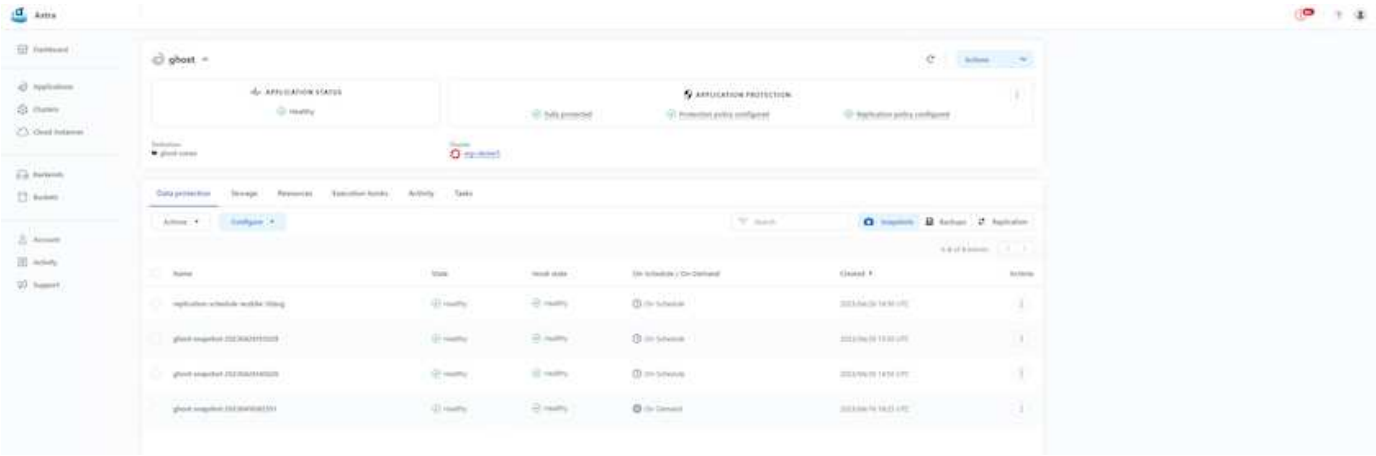
La protezione dei dati in ONTAP può essere ottenuta utilizzando ad hoc o policy controllate - **Snapshot** - **backup e ripristino**

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

Istantanea con ACC

È possibile acquisire una copia dei dati in un dato momento 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 su richiesta possono essere eseguite in qualsiasi momento e a intervalli più brevi rispetto alle copie Snapshot programmate. Le copie snapshot vengono archiviate sullo stesso volume fornito dell'app.

Configurazione di Snapshot con ACC

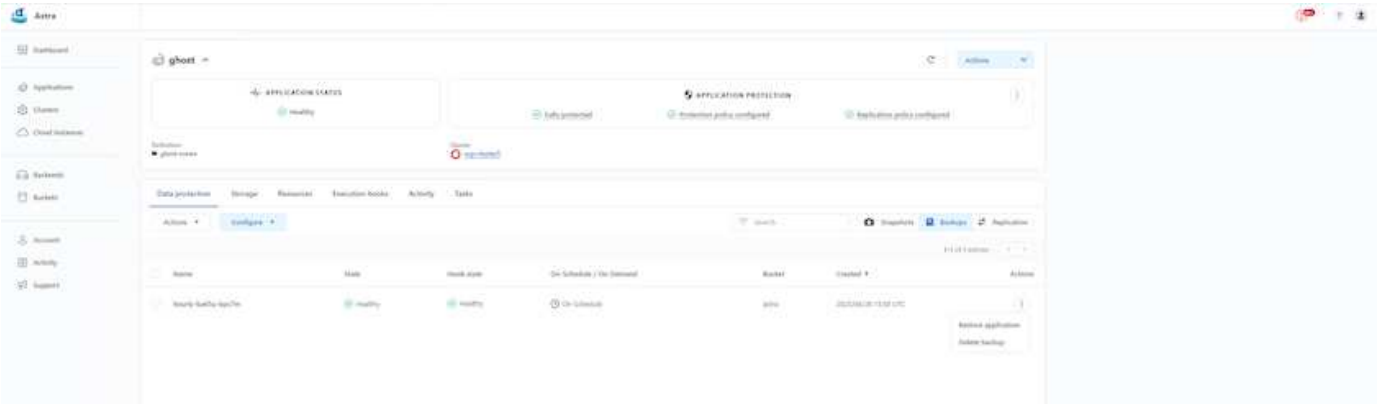


Backup e ripristino con ACC

Un backup si basa su uno Snapshot. Trident Protect può effettuare copie Snapshot tramite CSI ed eseguire il backup utilizzando la copia Snapshot in un dato momento. Il backup viene archiviato in un archivio 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 tramite ACC

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



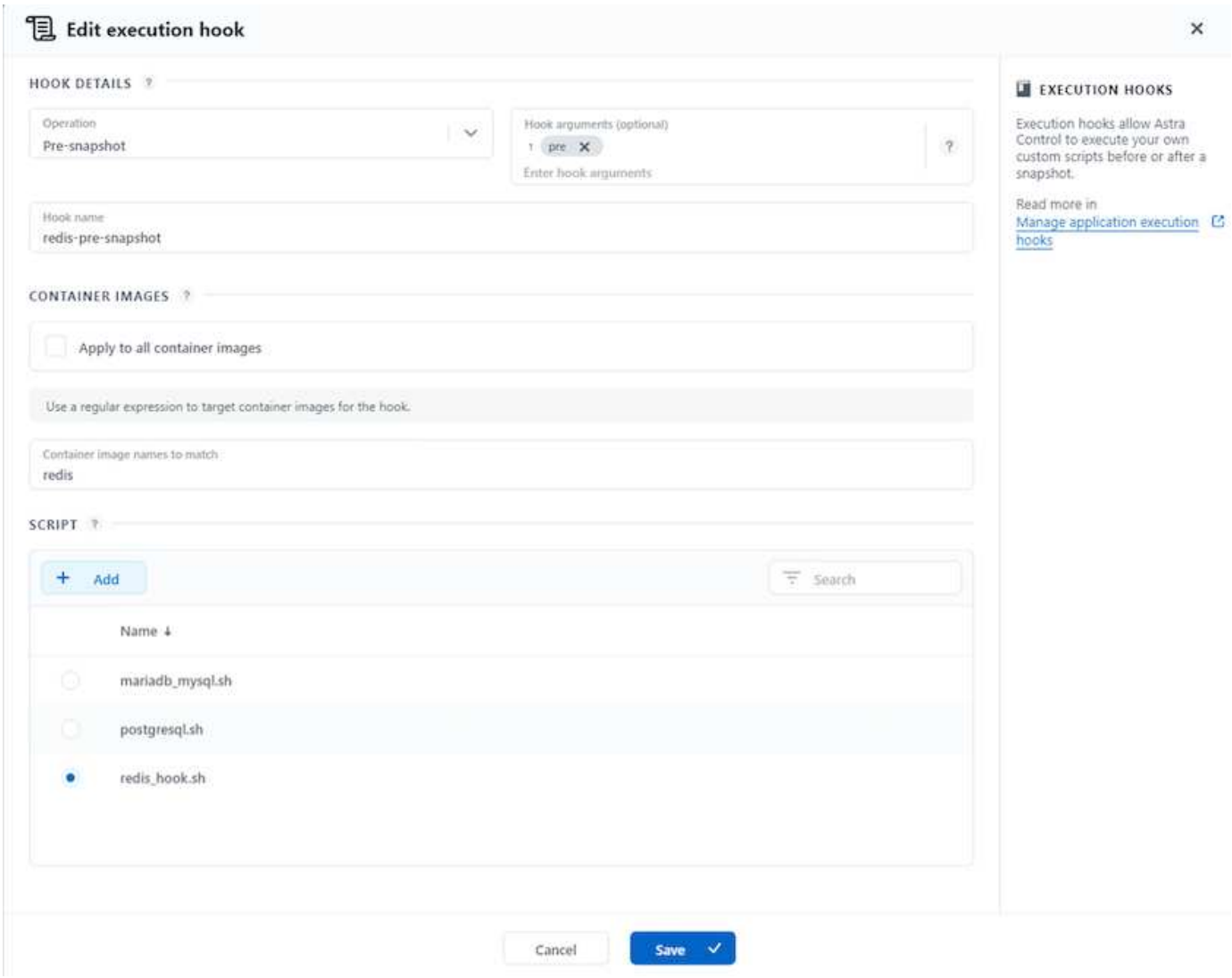
Hook di esecuzione specifici dell'applicazione

Inoltre, gli hook di esecuzione possono essere configurati per essere eseguiti insieme a un'operazione di protezione dei dati di un'app gestita. Sebbene siano disponibili funzionalità di protezione dei dati a livello di array di archiviazione, spesso sono necessari passaggi aggiuntivi per rendere i backup e i ripristini coerenti con l'applicazione. I passaggi aggiuntivi specifici dell'app 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'app codificati come script personalizzati denominati "execution hook".

"Progetto GitHub NetApp Verda"fornisce hook di esecuzione per le applicazioni cloud-native più diffuse per rendere la protezione delle applicazioni semplice, solida e facile da orchestrare. Sentiti libero di contribuire a quel progetto se hai informazioni sufficienti per un'applicazione che non è presente nel repository.

Esempio di hook di esecuzione per il pre-Snapshot di un'applicazione Redis.



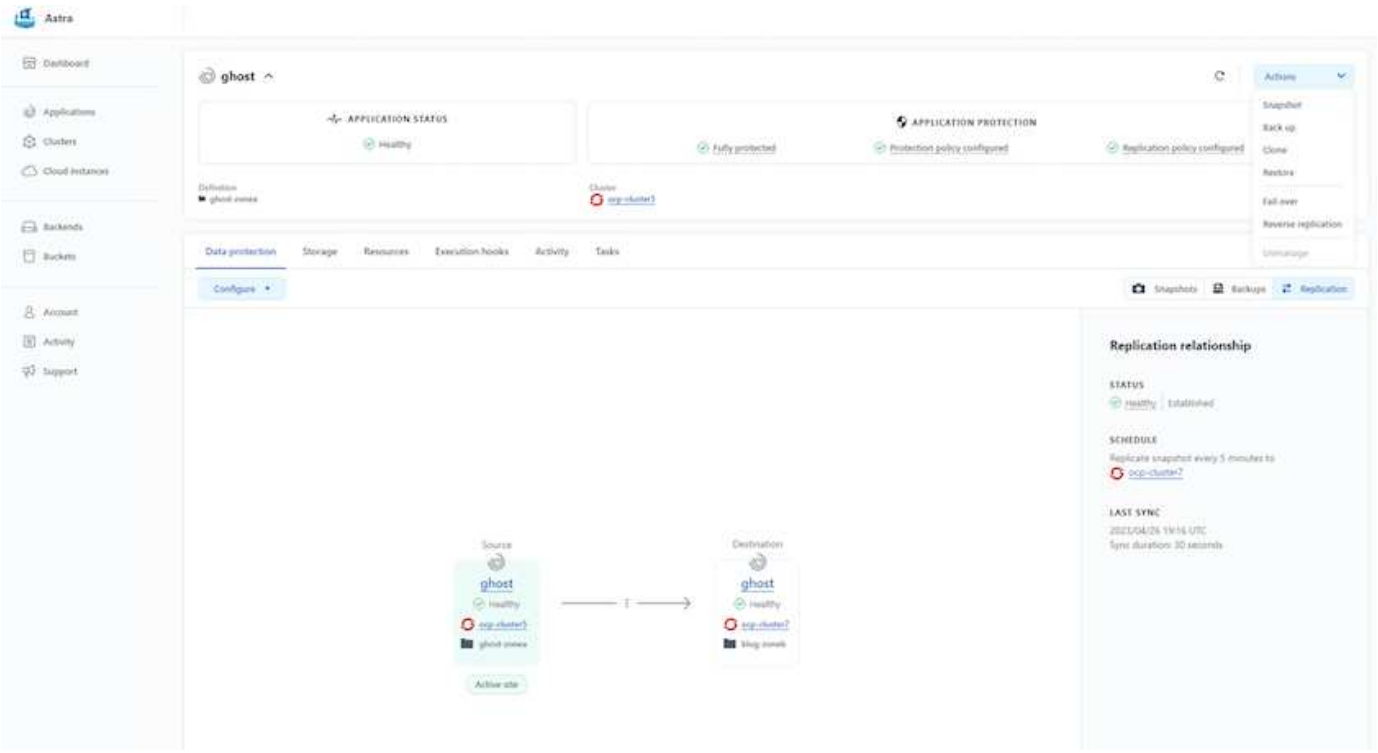
Replica con ACC

Per una protezione regionale o per una soluzione RPO e RTO bassi, un'applicazione può essere replicata su un'altra istanza di Kubernetes in esecuzione in un sito diverso, preferibilmente in un'altra regione. Trident Protect utilizza ONTAP async SnapMirror con RPO di appena 5 minuti. La replica viene eseguita tramite replica su ONTAP e quindi un failover crea le risorse Kubernetes nel cluster di destinazione.

> Si noti che la replica è diversa dal backup e dal ripristino, in quanto il backup viene eseguito su S3 e il ripristino viene eseguito da S3. Fare riferimento al collegamento: https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster [qui] per ottenere ulteriori dettagli sulle differenze tra i due tipi di protezione dei dati.

Fare riferimento"Qui" per le istruzioni di configurazione SnapMirror .

SnapMirror con ACC



I driver di archiviazione san-economy e nas-economy non supportano la funzionalità di replica. Fare riferimento"Qui" per ulteriori dettagli.

Video dimostrativo:

"Video dimostrativo del disaster recovery con Trident Protect"

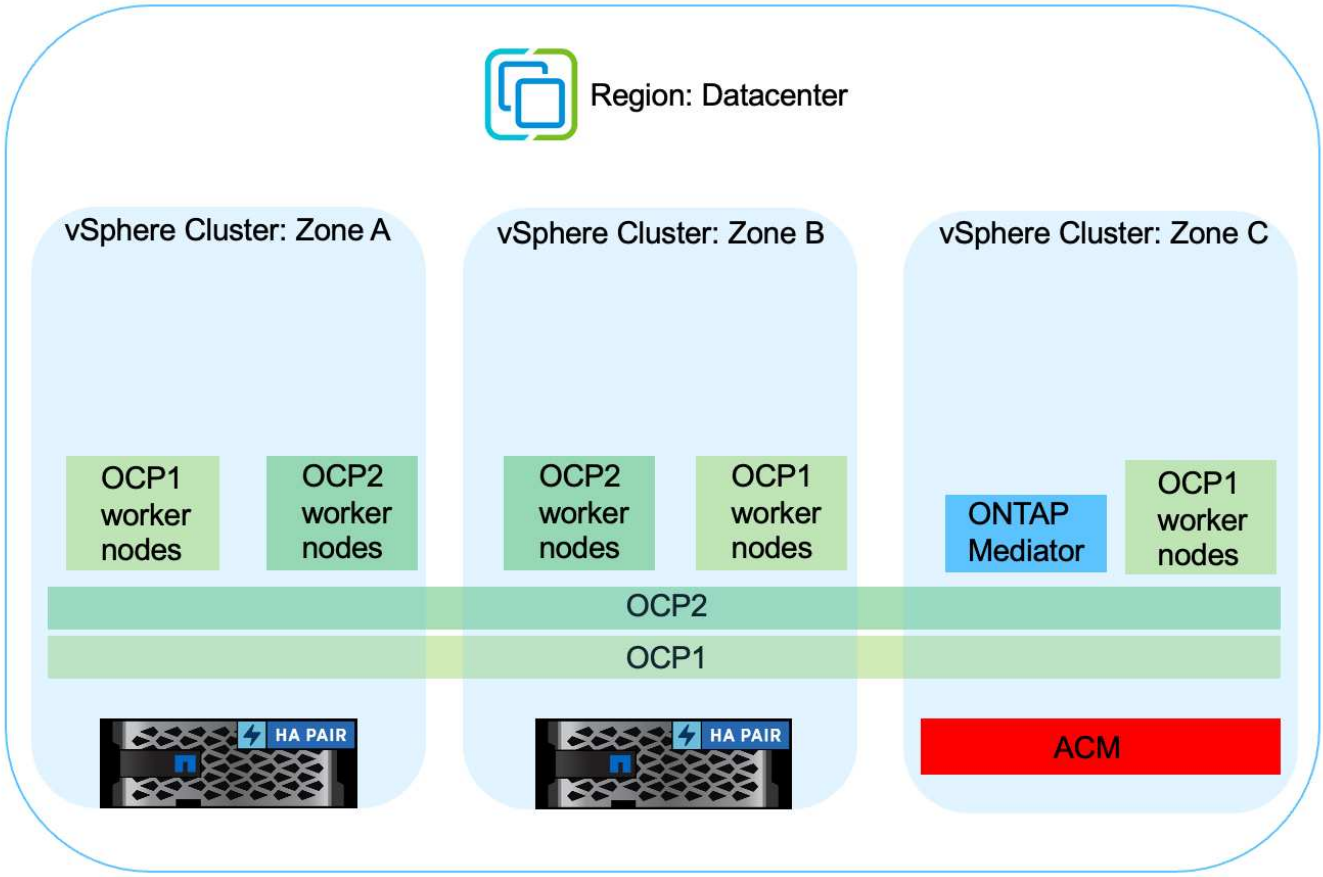
Protezione dei dati con Trident Protect

Continuità aziendale con MetroCluster

La maggior parte della nostra piattaforma hardware per ONTAP è dotata di funzionalità di elevata disponibilità per proteggere i dispositivi dai guasti, evitando la necessità di eseguire il ripristino di emergenza. Tuttavia, per proteggersi da incendi o altri disastri e continuare l'attività con RPO pari a zero e RTO basso, spesso si ricorre alla soluzione MetroCluster .

I clienti che attualmente dispongono di un sistema ONTAP possono estenderlo a MetroCluster aggiungendo sistemi ONTAP supportati entro i limiti di distanza per fornire il ripristino di emergenza a livello di zona. Trident, CSI (Container Storage Interface), supporta NetApp ONTAP, inclusa la configurazione MetroCluster , nonché altre opzioni come Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, ecc. Trident fornisce cinque opzioni di driver di archiviazione per ONTAP e sono tutte supportate per la configurazione MetroCluster . Fare riferimento"Qui" per ulteriori dettagli sui driver di archiviazione ONTAP supportati da Trident.

La soluzione MetroCluster richiede un'estensione di rete di livello 2 o la capacità di accedere allo stesso indirizzo di rete da entrambi i domini di errore. Una volta configurata MetroCluster , la soluzione è trasparente per i proprietari delle applicazioni, poiché tutti i volumi nella svm MetroCluster sono protetti e beneficiano dei vantaggi di SyncMirror (RPO zero).



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

Sono disponibili dettagli sulle funzionalità di protezione dei dati Trident Protect"Qui"

Migrazione dei dati tramite Trident Protect

Questa pagina mostra le opzioni di migrazione dei dati per i carichi di lavoro dei container sui cluster Red Hat OpenShift con Trident Protect.

Spesso è necessario spostare le applicazioni Kubernetes da un ambiente all'altro. Per migrare un'applicazione insieme ai suoi dati persistenti, è possibile utilizzare NetApp Trident Protect.

Migrazione dei dati tra diversi ambienti Kubernetes

ACC supporta vari tipi di Kubernetes, tra cui Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Upstream Kubernetes, ecc. Per ulteriori dettagli, fare riferimento"Qui" .

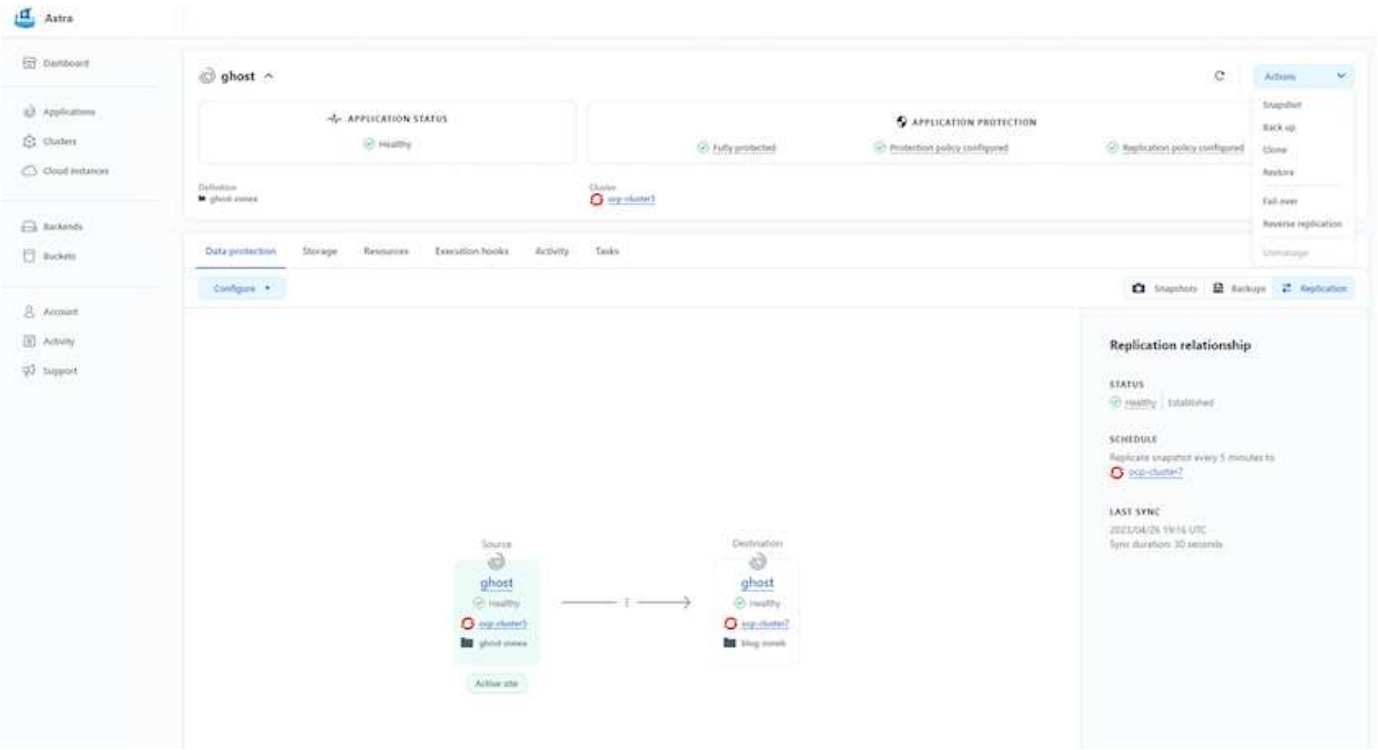
Per migrare l'applicazione da un cluster a un altro, è possibile utilizzare una delle seguenti funzionalità di ACC:

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

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

Fare riferimento"Qui" per ulteriori dettagli sulla **clonazione**.

Esecuzione della replica dei dati tramite ACC



Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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