Cloud ibrido con componenti autogestiti

NetApp public and hybrid cloud solutions

NetApp
November 04, 2026

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-cloud/openshift/os-sm-solution.html on November 04, 2026. Always check docs.netapp.com for the latest.

Sommario

Cloud ibrido con componenti autogestiti . . . 1
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido . . . 1
Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container in un cloud ibrido utilizzando Trident Protect . . . 1
Distribuisci e configura la piattaforma Red Hat OpenShift Container su AWS . . . 2
Distribuisci e configura la piattaforma container Red Hat OpenShift su Google Cloud . . . 4
Distribuisci e configura la piattaforma Red Hat OpenShift Container su Azure . . . 6
Protezione dei dati tramite Trident Protect . . . 9

Cloud ibrido con componenti autogestiti

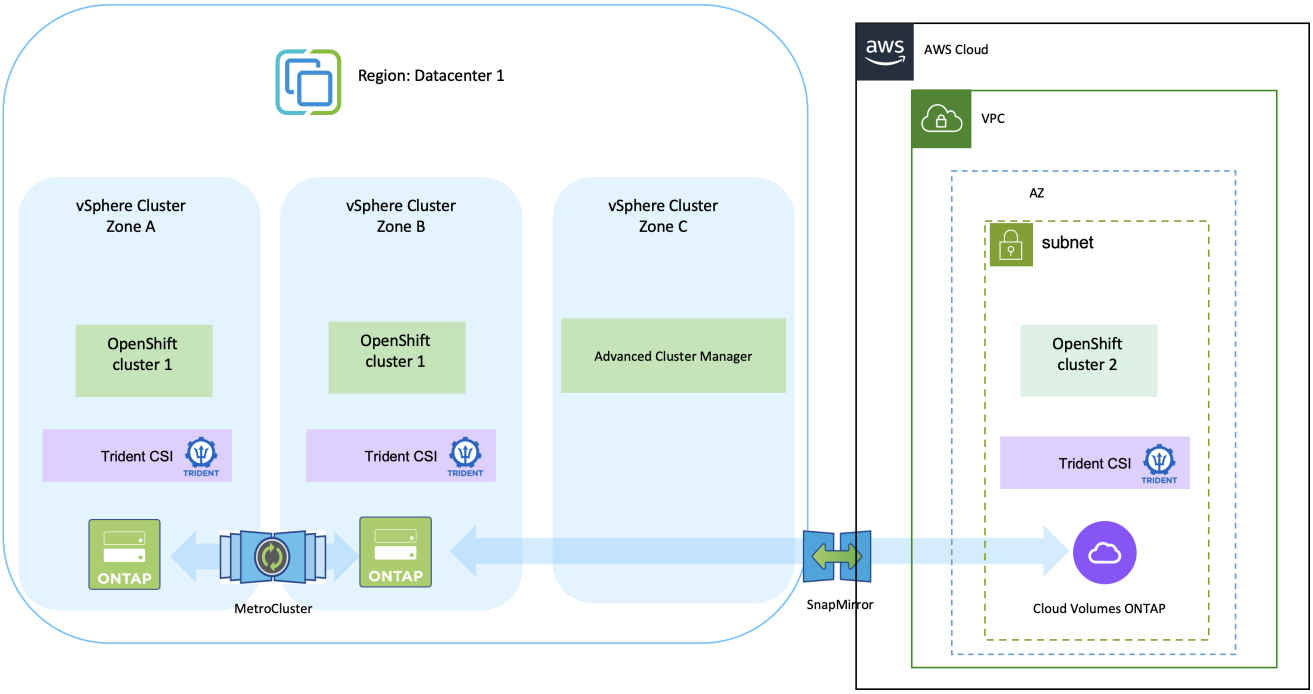
Soluzione NetApp con carichi di lavoro della piattaforma container Red Hat OpenShift nel cloud ibrido

I clienti potrebbero trovarsi a un punto del loro percorso di modernizzazione in cui sono pronti a spostare alcuni carichi di lavoro selezionati o tutti i carichi di lavoro dai loro data center al cloud. Possono scegliere di utilizzare container OpenShift autogestiti e storage NetApp autogestito nel cloud per vari motivi. Dovrebbero pianificare e distribuire la piattaforma container Red Hat OpenShift (OCP) nel cloud per creare un ambiente di produzione di successo per la migrazione dei carichi di lavoro dei container dai loro data center. I loro cluster OCP possono essere distribuiti su VMware o Bare Metal nei loro data center e su AWS, Azure o Google Cloud nell'ambiente cloud.

NetApp Cloud Volumes ONTAP storage offre protezione dei dati, affidabilità e flessibilità per le distribuzioni di container in AWS, Azure e Google Cloud. Trident funge da dynamic storage provisioner per consumare lo storage persistente Cloud Volumes ONTAP per le applicazioni stateful dei clienti. Trident Protect può essere utilizzato per i requisiti di gestione dei dati delle applicazioni stateful, come protezione dei dati, migrazione e continuità aziendale.

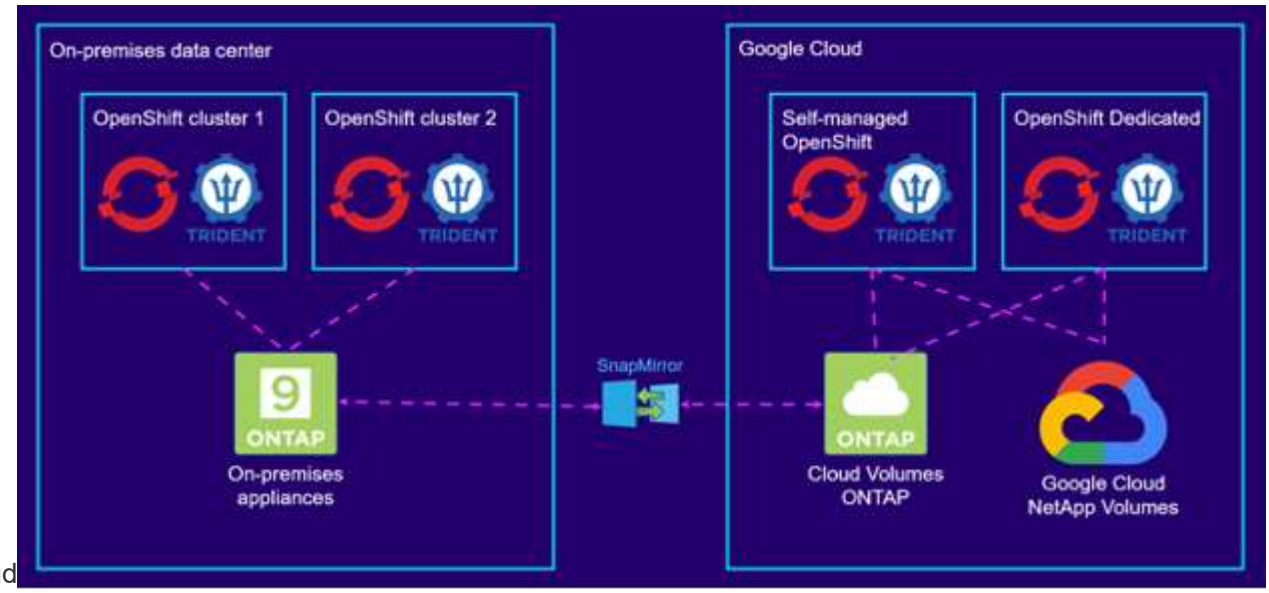
Soluzione di protezione e migrazione dei dati per carichi di lavoro OpenShift Container in un cloud ibrido utilizzando Trident Protect

In locale e
AWS

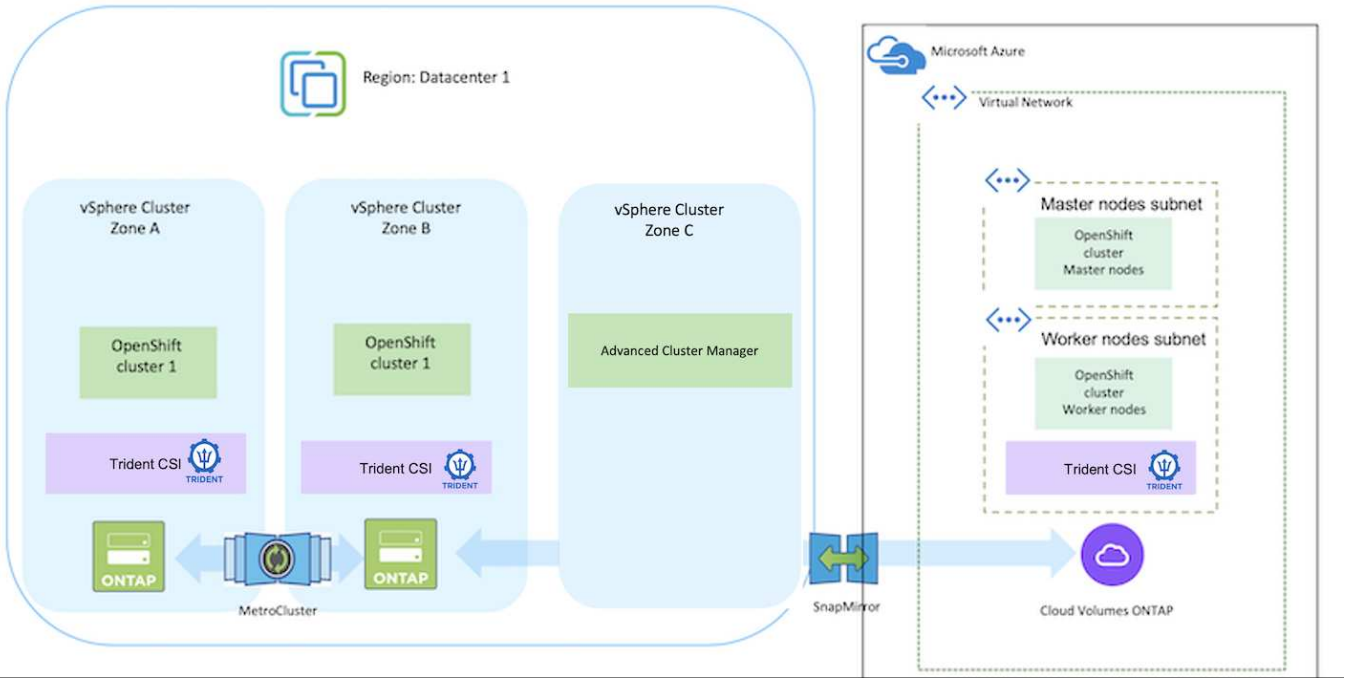


In locale e su Google

Cloud



In locale e nel cloud di Azure

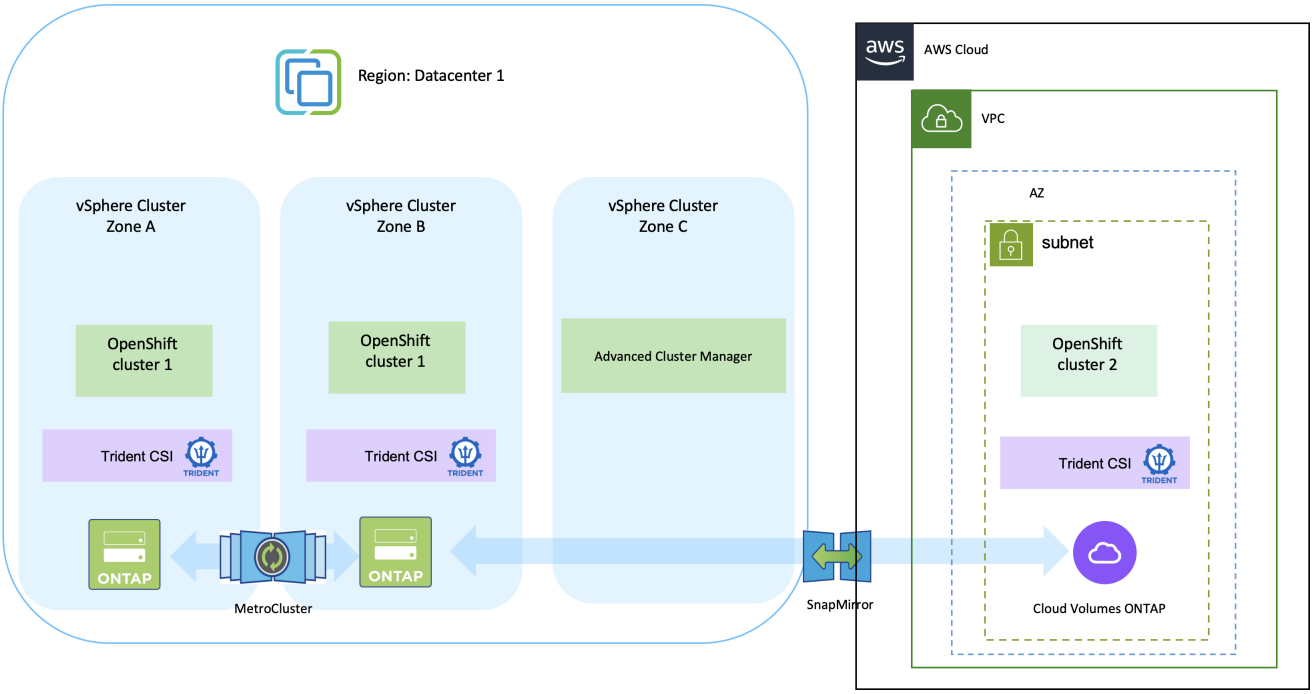


Distribuisci e configura la piattaforma Red Hat OpenShift Container su AWS

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in AWS e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Trident Protect per eseguire attività di protezione e migrazione dei dati per le applicazioni con stato.

Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container su AWS. 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 AWS e connessi al data center tramite una VPN.



Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Installa un cluster OCP su AWS da Advanced Cluster Management.**

- Crea una VPC con una connessione VPN da sito a sito (utilizzando pfsense) per connetterti alla rete locale.
- La rete locale è dotata di connettività Internet.
- Crea 3 subnet private in 3 diverse zone di disponibilità.
- Creare una zona ospitata privata Route 53 e un resolver DNS per la VPC.

Crea un cluster OpenShift su AWS dalla procedura guidata di Advanced Cluster Management (ACM). Consulta le istruzioni "Qui".

Puoi anche creare il cluster in AWS dalla console Hybrid Cloud di OpenShift. Consulta "Qui" per le istruzioni.

Quando si crea il cluster tramite ACM, è possibile personalizzare l'installazione modificando il file yaml dopo aver compilato i dettagli nella visualizzazione del modulo. Dopo aver creato il cluster, è possibile effettuare l'accesso tramite SSH ai nodi del cluster per la risoluzione dei problemi o per ulteriori configurazioni manuali. Utilizza la chiave ssh fornita durante l'installazione e il nome utente core per effettuare l'accesso.

▼ **Distribuisci Cloud Volumes ONTAP in AWS utilizzando BlueXP.**

- Installare il connettore nell'ambiente VMware locale. Fare riferimento alle istruzioni"Qui" .
- Distribuisci un'istanza CVO in AWS utilizzando il connettore. Fare riferimento alle istruzioni"Qui" .

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

▼ **Installa Trident nel cluster OCP**

- Distribuisci Trident Operator tramite Helm. Consulta le istruzioni "Qui"
- Creare un backend e una classe di archiviazione. Fare riferimento alle istruzioni"Qui" .

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

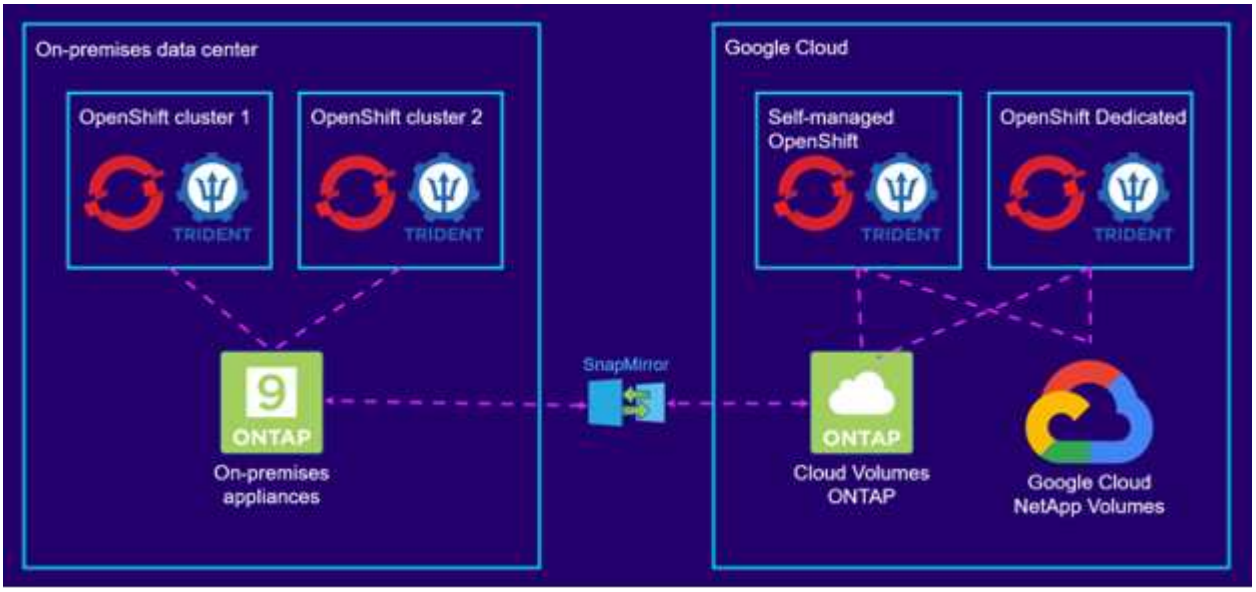
Oggi i provider cloud consentono agli amministratori di cluster Kubernetes/OpenShift di generare nodi di cluster basati su zone. I nodi possono essere ubicati in diverse zone di disponibilità all'interno di una regione o tra regioni diverse. Per facilitare il provisioning dei volumi per i carichi di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

> Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Distribuisci e configura la piattaforma container Red Hat OpenShift su Google Cloud

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in GCP e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage Google Cloud NetApp Volumes e NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti.

Ecco un diagramma che mostra i cluster distribuiti su GCP e connessi al data center tramite una VPN.



Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container in GCP. 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" .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

Installa un cluster OCP su GCP dalla CLI

- Assicurati di aver soddisfatto tutti i prerequisiti indicati "Qui".
- Per la connettività VPN tra locale e GCP, è stata creata e configurata una VM pfsense. Per le 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 di rete remoti per la Fase 2 possono essere configurati solo dopo l'esecuzione del programma di installazione del cluster OpenShift e la creazione dei componenti infrastrutturali per il cluster.
  - La VPN in Google Cloud può essere configurata solo dopo che i componenti dell'infrastruttura per il cluster sono stati creati dal programma di installazione.
- Ora installa il cluster OpenShift su GCP.
  - Ottieni il programma di installazione e il pull secret e distribuisci il cluster seguendo i passaggi indicati nella documentazione "Qui".
  - L'installazione crea una rete VPC in Google Cloud Platform. Crea anche una zona privata in Cloud DNS e aggiunge record A.
    - 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 record A nel DNS dell'ambiente locale utilizzando l'indirizzo IP nei record A del DNS di Google Cloud.
  - L'installazione del cluster è completata e verranno forniti un file kubeconfig, nonché nome utente e password per accedere alla console del cluster.

Distribuisci Google Cloud NetApp Volumes

- Google Cloud NetApp Volumes può essere aggiunto ai tuoi progetti come descritto"Qui" .

Distribuisci Cloud Volumes ONTAP in GCP utilizzando BlueXP

- Installa un connettore in Google Cloud. Fare riferimento alle istruzioni "Qui" .
- Distribuisci un'istanza CVO in Google Cloud utilizzando il connettore. Fare riferimento alle istruzioni qui. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Installa Trident nel cluster OCP in GCP

- Esistono molti metodi per implementare Trident, come mostrato "Qui".
- Per questo progetto, hai installato Trident distribuendo manualmente Trident Operator seguendo le istruzioni "Qui".
- Creare classi di backend e di archiviazione. Fare riferimento alle istruzioni"Qui" .

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

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

> Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Video dimostrativo

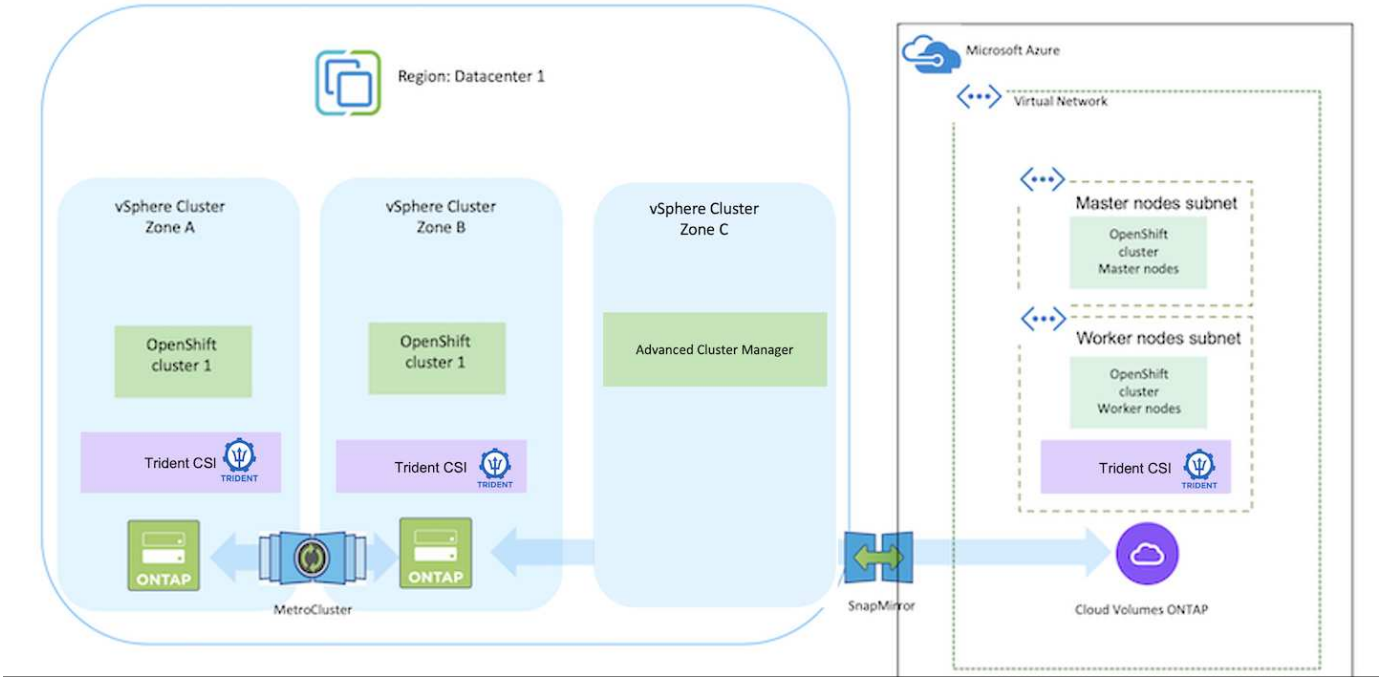
Installazione di OpenShift Cluster su Google Cloud Platform

Importazione di cluster OpenShift in Trident Protect

Distribuisci e configura la piattaforma Red Hat OpenShift Container su Azure

Questa sezione descrive un flusso di lavoro di alto livello su come configurare e gestire i cluster OpenShift in Azure e distribuire su di essi applicazioni con stato. Mostra l'utilizzo dello storage NetApp Cloud Volumes ONTAP con l'ausilio di Trident per fornire volumi persistenti. Vengono forniti dettagli sull'utilizzo di Trident Protect per eseguire attività di protezione e migrazione dei dati per le applicazioni con stato.

Ecco un diagramma che mostra i cluster distribuiti su Azure e connessi al data center tramite una VPN.



Esistono diversi modi per distribuire i cluster della piattaforma Red Hat OpenShift Container in Azure. 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" .

Il processo di configurazione può essere suddiviso nei seguenti passaggi:

▼ **Installare un cluster OCP su Azure dalla CLI.**

- Assicurati di aver soddisfatto tutti i prerequisiti indicati "Qui".
- Creare una VPN, subnet e gruppi di sicurezza di rete e una zona DNS privata. Crea un gateway VPN e una connessione VPN da sito a sito.
- Per la connettività VPN tra locale e Azure, è stata creata e configurata una VM pfsense. Per le istruzioni, vedere"Qui" .
- Ottieni il programma di installazione e il pull secret e distribuisci il cluster seguendo i passaggi indicati nella documentazione "Qui".
- L'installazione del cluster è completata e verranno forniti un file kubeconfig, nonché nome utente e 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:
```

▼ **Distribuisci Cloud Volumes ONTAP in Azure utilizzando BlueXP.**

- Installa un connettore in Azure. Fare riferimento alle istruzioni "Qui" .
- Distribuisci un'istanza CVO in Azure utilizzando il connettore. Fare riferimento al collegamento alle istruzioni: https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [qui.]

Utilizzo della funzionalità CSI Topology di Trident per architetture multizona

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

Kubernetes supporta due modalità di associazione del volume: - Quando ***VolumeBindingMode*** **è impostato su** ***Immediate*** (predefinito), 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*** **è impostato su** ***WaitForFirstConsumer***, la creazione e l'associazione di un volume persistente per un PVC vengono ritardate finché non viene pianificato e creato un pod che utilizza il PVC. In questo modo, i volumi vengono creati per soddisfare i vincoli di pianificazione imposti dai requisiti di topologia. I backend di archiviazione Trident possono essere progettati per fornire volumi in modo selettivo in base alle zone di disponibilità (backend con riconoscimento della topologia). Per le StorageClass che utilizzano tale backend, un volume verrà creato solo se richiesto da un'applicazione pianificata in una regione/zona supportata. (StorageClass con riconoscimento della topologia) Fare riferimento"Qui" per ulteriori dettagli.

Protezione dei dati tramite Trident Protect

Per dettagli sulla protezione e la migrazione dei carichi di lavoro dei container utilizzando Trident Protect, consultare la seguente sezione: - "Proteggi e migra le app Container utilizzando Trident Protect"

Informazioni sul copyright

Copyright © 2026 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.