



# Container

## NetApp Solutions

NetApp  
April 26, 2024

This PDF was generated from [https://docs.netapp.com/it-it/netapp-solutions/containers/a-w-n\\_anthos\\_VMW.html](https://docs.netapp.com/it-it/netapp-solutions/containers/a-w-n_anthos_VMW.html) on April 26, 2024. Always check docs.netapp.com for the latest.

# Sommario

- Soluzioni container NetApp ..... 1
  - NVA-1165: Anthos con NetApp ..... 1
  - TR-4919: DevOps con NetApp Astra ..... 34
  - NVA-1160: Red Hat OpenShift con NetApp ..... 62
  - NVA-1166: VMware Tanzu con NetApp ..... 261
- Soluzioni archiviate ..... 306

# Soluzioni container NetApp

## NVA-1165: Anthos con NetApp

Banu Sundhar e Suresh Thoppay, NetApp

Questo documento di riferimento fornisce la convalida dell'implementazione della soluzione anthos con NetApp da parte di NetApp e dei nostri partner tecnici quando viene implementata in più ambienti di data center. Inoltre, illustra in dettaglio l'integrazione dello storage con i sistemi di storage NetApp utilizzando Astra Trident Storage orchestrator per la gestione dello storage persistente. Infine, esploriamo e documentiamo una serie di validazioni delle soluzioni e casi di utilizzo reali.

### Casi di utilizzo

La soluzione anthos con NetApp è progettata per offrire un valore eccezionale ai clienti con i seguenti casi di utilizzo:

- Facile da implementare e gestire l'ambiente anthos implementato utilizzando il fornito `bmctl` su metallo nudo o su `gkectl` Su VMware vSphere.
- Potenza combinata di container Enterprise e carichi di lavoro virtualizzati con anthos implementato virtualmente su vSphere o su bare metal con "[kubivirt](#)".
- Configurazione e casi di utilizzo reali che evidenziano le funzionalità di anthos quando utilizzate con lo storage NetApp e Astra Trident, l'orchestrator dello storage open-source per Kubernetes.

### Valore di business

Le aziende stanno adottando sempre più pratiche DevOps per creare nuovi prodotti, abbreviare i cicli di rilascio e aggiungere rapidamente nuove funzionalità. A causa della loro natura innata e agile, i container e i microservizi svolgono un ruolo cruciale nel supporto delle pratiche DevOps. Tuttavia, la pratica di DevOps su scala di produzione in un ambiente aziendale presenta le proprie sfide e impone determinati requisiti all'infrastruttura sottostante, come ad esempio:

- Alta disponibilità a tutti i livelli dello stack
- Procedure di implementazione semplici
- Operazioni e aggiornamenti senza interruzioni
- Infrastruttura programmabile e basata su API per restare al passo con l'agilità dei microservizi
- Multi-tenancy con garanzie di performance
- Possibilità di eseguire workload virtualizzati e containerizzati contemporaneamente
- Possibilità di scalare l'infrastruttura in modo indipendente in base alle esigenze dei carichi di lavoro

La soluzione anthos con NetApp riconosce queste sfide e presenta una soluzione che aiuta a risolvere ogni problema implementando l'implementazione completamente automatica di anthos in maniera prematura nell'ambiente di data center scelto dal cliente.

## Panoramica della tecnologia

La soluzione anthos con NetApp comprende i seguenti componenti principali:

### Anthos on Prem

Anthos on Prem è una piattaforma Kubernetes aziendale completamente supportata che può essere implementata nell'hypervisor VMware vSphere o su un'infrastruttura bare metal di tua scelta.

Per ulteriori informazioni su anthos, visitare il sito Web di anthos all'indirizzo ["qui"](#).

### Sistemi storage NetApp

NetApp dispone di diversi sistemi storage perfetti per data center aziendali e implementazioni di cloud ibrido. Il portfolio NetApp include NetApp ONTAP, Cloud Volumes ONTAP, Cloud Volumes Service, Azure NetApp Files, FSxN per i sistemi storage NetApp ONTAP, tutti in grado di fornire storage persistente per le applicazioni containerizzate.

Per ulteriori informazioni, visitare il sito Web di NetApp ["qui"](#).

### Integrazioni di storage NetApp

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, incluso Anthos.

Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

## Opzioni di configurazione avanzate

Questa sezione è dedicata alle personalizzazioni che gli utenti reali dovrebbero eseguire durante l'implementazione di questa soluzione in produzione, ad esempio la creazione di un registro di immagini private dedicato o l'implementazione di istanze personalizzate di bilanciamento del carico.

## Matrice di supporto corrente per le release validate

Vedere ["qui"](#) per la matrice di supporto per le release validate.

## Panoramica di anthos

Anthos con NetApp è un'architettura di cloud ibrido verificata e basata su Best practice per l'implementazione on-premise di un ambiente Google Kubernetes Engine (GKE) in modo affidabile e affidabile. Questo documento di riferimento sull'architettura verificata di NetApp funge sia da guida di progettazione che da convalida dell'implementazione della soluzione anthos con NetApp implementata in ambienti virtuali e bare metal.

L'architettura descritta in questo documento è stata convalidata da esperti in materia presso NetApp e Google Cloud per offrire i vantaggi dell'esecuzione di anthos nel tuo ambiente di data center aziendale.

### Anthos

Anthos è una soluzione per data center di Kubernetes con cloud ibrido che consente alle organizzazioni di costruire e gestire moderne infrastrutture di cloud ibrido adottando al contempo flussi di lavoro agili incentrati

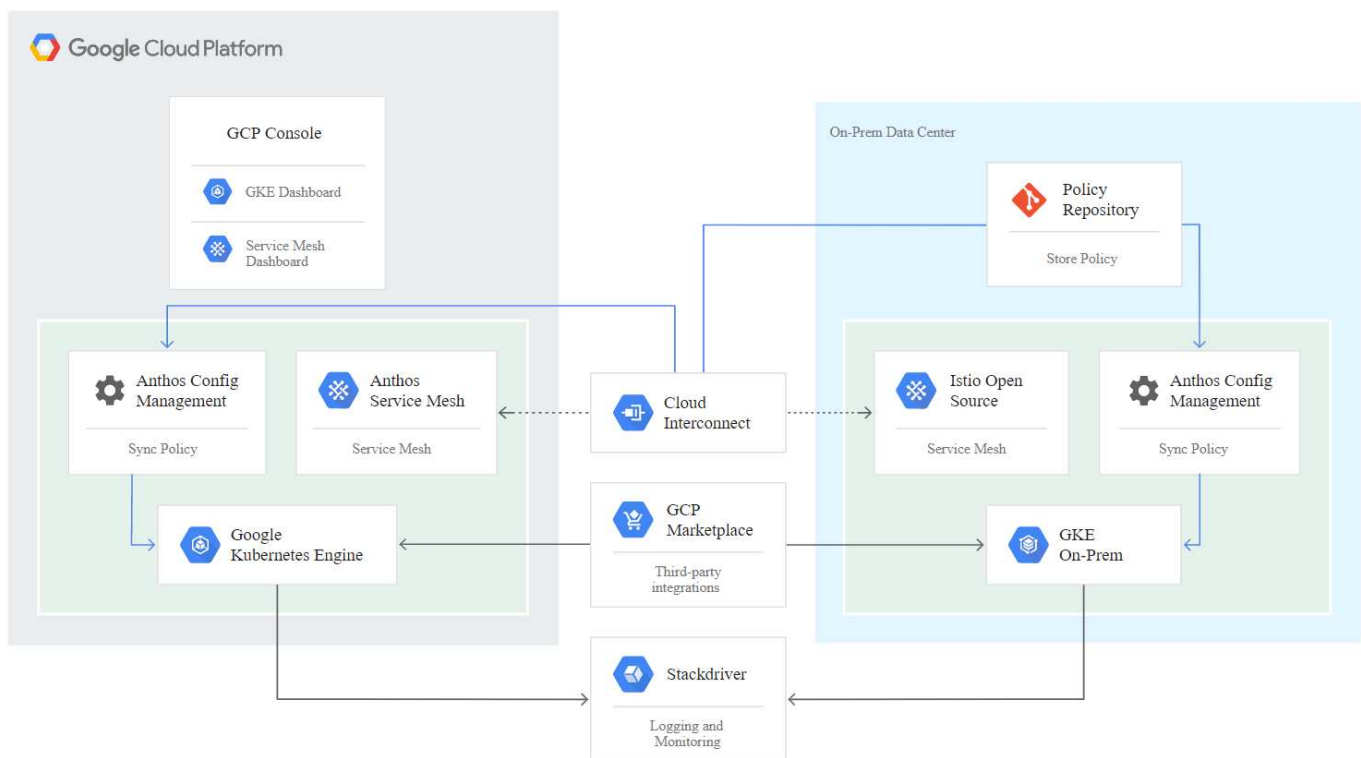


sullo sviluppo delle applicazioni. Anthos su VMware, una soluzione basata su tecnologie open-source, viene eseguita on-premise in un'infrastruttura basata su VMware vSphere, in grado di connettersi e interagire con Anthos GKE in Google Cloud. L'adozione di container, service mesh e altre tecnologie trasformative consente alle organizzazioni di sperimentare cicli di sviluppo delle applicazioni coerenti e carichi di lavoro pronti per la produzione in ambienti locali e basati sul cloud. La seguente figura illustra la soluzione anthos e il modo in cui un'implementazione in un data center on-premise si interconnette con l'infrastruttura nel cloud.

Per ulteriori informazioni su anthos, visitare il sito Web di anthos all'indirizzo ["qui"](#).

Anthos offre le seguenti funzionalità:

- **Anthos Configuration management.** automatizza le policy e la sicurezza delle implementazioni ibride di Kubernetes.
- **Anthos Service Mesh.** migliora l'osservabilità, la sicurezza e il controllo delle applicazioni con una mesh di servizi basata su Istio.
- **Google Cloud Marketplace for Kubernetes Applications.** un catalogo di applicazioni container curate disponibili per una facile implementazione.
- **Migrazione per anthos.** migrazione automatica di servizi fisici e macchine virtuali da on-premise al cloud.
- **Stackdriver.** Servizio di gestione offerto da Google per la registrazione e il monitoraggio delle istanze cloud.



## Metodi di implementazione per anthos

### Anthos su VMware

I cluster Anthos implementati negli ambienti VMware vSphere sono facili da implementare, gestire e scalare rapidamente per la maggior parte dei carichi di lavoro Kubernetes dell'utente finale.

Per ulteriori informazioni sui cluster anthos su VMware, implementati con NetApp, visita la pagina ["qui"](#).

## Anthos su bare metal

I cluster anthos implementati su server bare metal sono indipendenti dall'hardware e consentono di selezionare una piattaforma di calcolo ottimizzata per il tuo caso d'utilizzo personalizzato.

Per ulteriori informazioni su anthos sui cluster bare metal implementati con NetApp, visitare il sito ["qui"](#).

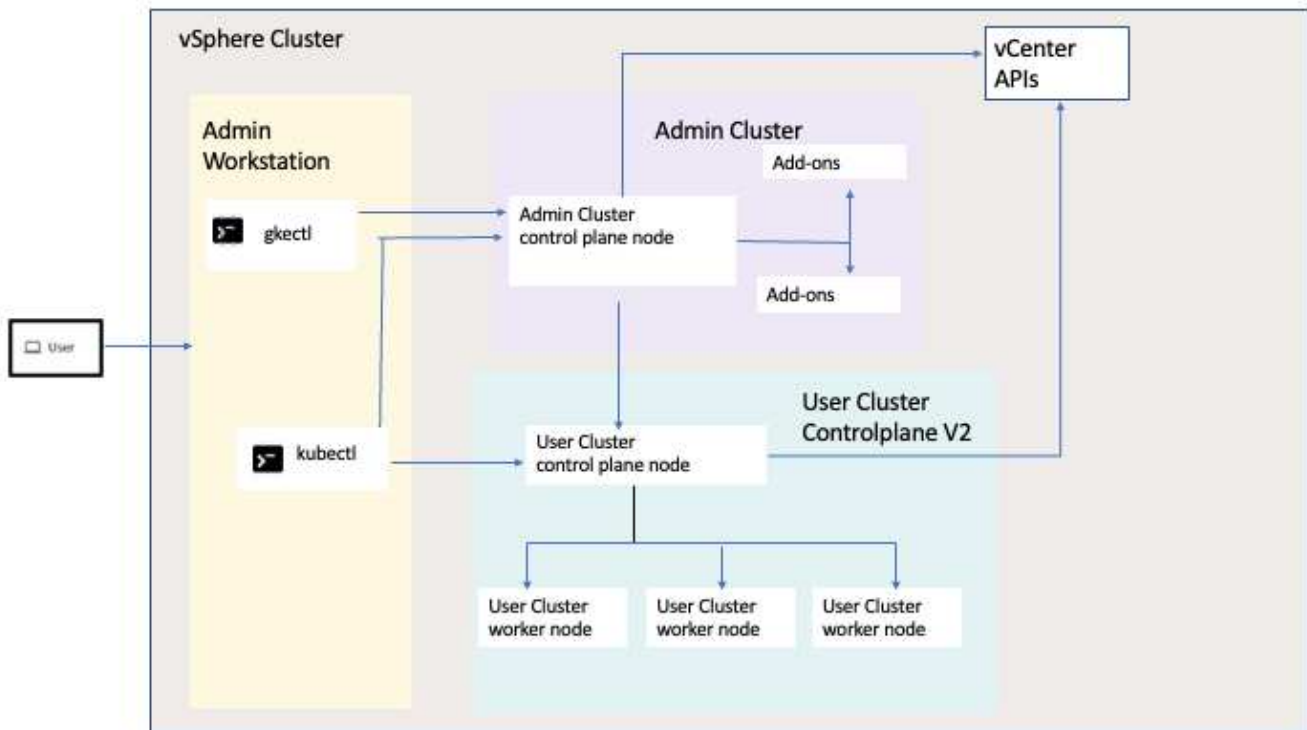
## Anthos Clusters su VMware

Anthos Clusters su VMware è un'estensione di Google Kubernetes Engine implementata nel data center privato di un utente finale. Un'organizzazione può implementare le stesse applicazioni progettate per essere eseguite in container in Google Cloud nei cluster Kubernetes on-premise. I cluster Anthos su VMware possono essere implementati in un ambiente VMware vSphere esistente nel data center, risparmiando sulle spese di capitale e consentendo operazioni di implementazione e scalabilità più rapide.

L'implementazione dei cluster anthos su VMware include i seguenti componenti:

- **Anthos admin workstation.** un host di implementazione da cui `gkectl` e `kubectl` i comandi possono essere eseguiti per implementare e interagire con le implementazioni di anthos.
- **Admin cluster.** il cluster iniziale implementato durante la configurazione dei cluster anthos su VMware. Questo cluster gestisce tutte le azioni del cluster utente subordinate, incluse l'implementazione, la scalabilità e l'aggiornamento.
- **Cluster utente.** ogni cluster utente viene implementato con la propria istanza o partizione di bilanciamento del carico, consentendo di agire come cluster Kubernetes standalone per singoli utenti o gruppi, contribuendo a ottenere una multi-tenancy completa.

La seguente figura mostra una descrizione di un'implementazione di anthos-Clusters-on-VMware.



## Benefici

I cluster Anthos su VMware offrono i seguenti vantaggi:

- **Multi-tenancy avanzata.** a ciascun utente finale può essere assegnato il proprio cluster utente, implementato con le risorse virtuali necessarie per il proprio ambiente di sviluppo.
- **Risparmi sui costi.** gli utenti finali possono ottenere risparmi significativi sui costi implementando più cluster di utenti nello stesso ambiente fisico e utilizzando le proprie risorse fisiche per le implementazioni delle applicazioni invece di fornire risorse nel proprio ambiente Google Cloud o su grandi cluster bare-metal.
- **Sviluppare e pubblicare.** le implementazioni on-premise possono essere utilizzate mentre le applicazioni sono in fase di sviluppo, il che consente di testare le applicazioni nella privacy di un data center locale prima di essere rese pubblicamente disponibili nel cloud.
- **Requisiti di sicurezza.** i clienti con maggiori problemi di sicurezza o set di dati sensibili che non possono essere memorizzati nel cloud pubblico sono in grado di eseguire le proprie applicazioni dalla sicurezza dei propri data center, soddisfacendo così i requisiti organizzativi.

## VMware vSphere

VMware vSphere è una piattaforma di virtualizzazione per la gestione centralizzata di un gran numero di server e reti virtualizzati in esecuzione sull'hypervisor ESXi.

Per ulteriori informazioni su VMware vSphere, consultare ["Sito Web di VMware vSphere"](#).

VMware vSphere offre le seguenti funzionalità:

- **VMware vCenter Server.** VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da una singola console e aggrega il monitoraggio delle performance di cluster, host e macchine virtuali.
- **VMware vSphere vMotion.** VMware vCenter consente di eseguire la migrazione a caldo delle macchine virtuali tra i nodi del cluster, su richiesta e senza interruzioni.
- **vSphere High Availability.** per evitare interruzioni in caso di guasti agli host, VMware vSphere consente di eseguire il clustering e la configurazione degli host in base all'alta disponibilità. Le macchine virtuali che vengono interrotte da un guasto dell'host vengono riavviate a breve su altri host del cluster, ripristinando i servizi.
- **Distributed Resource Scheduler (DRS).** Un cluster VMware vSphere può essere configurato per bilanciare il carico delle esigenze di risorse delle macchine virtuali ospitate. È possibile eseguire la migrazione a caldo delle macchine virtuali con risorse in altri nodi del cluster per assicurarsi che siano disponibili risorse sufficienti.

## Requisiti hardware

### Calcolo

Google Cloud richiede periodicamente la convalida aggiornata delle piattaforme server dei partner con le nuove release di Anthos attraverso il programma per partner della piattaforma Anthos Ready. È possibile trovare un elenco delle piattaforme server attualmente validate e delle versioni di Anthos supportate ["qui"](#).

### Sistema operativo

I cluster Anthos su VMware possono essere implementati in ambienti vSphere 7 e 8, scelti dal cliente per aiutare a creare un'infrastruttura di data center attuale.

La seguente tabella contiene un elenco delle versioni di vSphere utilizzate da NetApp e dai partner per la convalida della soluzione.

| Sistema operativo | Rilasciare | Versioni anthos |
|-------------------|------------|-----------------|
| VCenter           | 8.0.1      | 1,28            |

### Hardware aggiuntivo

Per completare l'implementazione di anthos con NetApp come soluzione completamente validata, NetApp e i nostri partner hanno testato altri componenti del data center per il networking e lo storage.

La tabella seguente contiene informazioni su questi componenti dell'infrastruttura aggiuntivi.

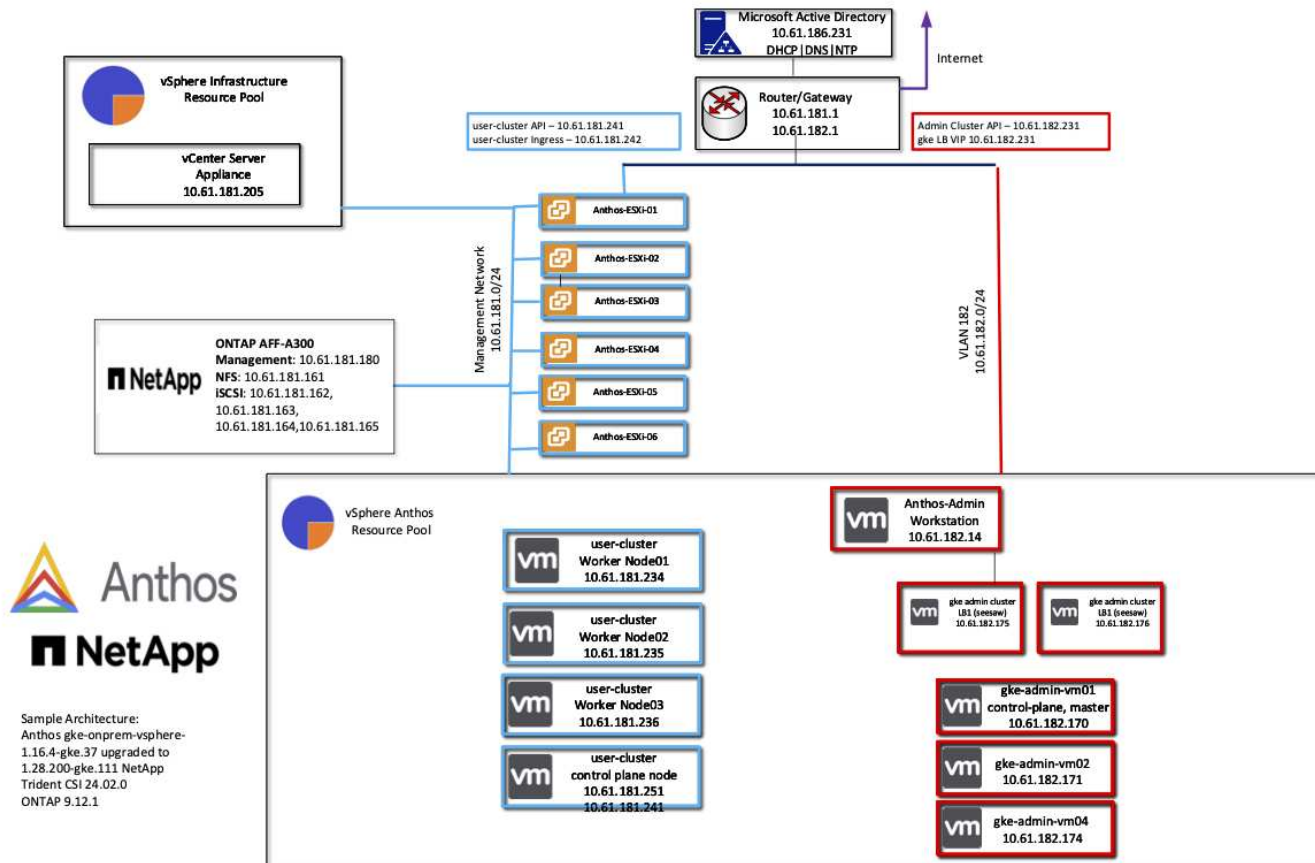
| Produttore | Componente hardware       |
|------------|---------------------------|
| Mellanox   | switch (rete dati)        |
| Cisco      | switch (rete di gestione) |
| NetApp     | Sistema storage AFF       |

### Software aggiuntivo

La seguente tabella include un elenco delle versioni software implementate nell'ambiente di convalida.

| Produttore | Software Name (Nome software) | Versione |
|------------|-------------------------------|----------|
| NetApp     | ONTAP                         | 9.12.1   |
| NetApp     | Astra Trident                 | 24.02.0  |

Durante la convalida della piattaforma anthos Ready eseguita da NetApp, l'ambiente di laboratorio è stato costruito sulla base del seguente diagramma, che ci ha consentito di testare diversi scenari utilizzando diversi backend di storage NetApp ONTAP.



## Risorse di supporto dell'infrastruttura di rete

Prima dell'implementazione di anthos, è necessario disporre della seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host accessibile dalla rete di gestione in-band e dalla rete VM.
- Almeno un server NTP accessibile dalla rete di gestione in-band e dalla rete VM.
- Un server DHCP disponibile per fornire locazioni di indirizzi di rete on-demand, nel caso in cui i cluster debbano scalare dinamicamente.
- (Opzionale) connettività Internet in uscita per la rete di gestione in banda e la rete VM.

## Best practice per le implementazioni in produzione

In questa sezione sono elencate diverse Best practice che un'organizzazione deve prendere in considerazione prima di implementare questa soluzione in produzione.

### Implementare anthos in un cluster ESXi di almeno tre nodi

Sebbene sia possibile installare anthos in un cluster vSphere di meno di tre nodi a scopo dimostrativo o di valutazione, questa operazione non è consigliata per i carichi di lavoro di produzione. Anche se due nodi consentono la tolleranza di base ha e fault tolerance, una configurazione del cluster anthos deve essere modificata per disattivare l'affinità host predefinita e questo metodo di implementazione non è supportato da Google Cloud.

## Configurare l'affinità della macchina virtuale e dell'host

La distribuzione dei nodi cluster anthos su più nodi hypervisor può essere ottenuta abilitando l'affinità di macchine virtuali e host.

Affinità o anti-affinità è un metodo per definire le regole per un insieme di macchine virtuali e/o host che determinano se le macchine virtuali vengono eseguite insieme sullo stesso host o su host del gruppo o su host diversi. Viene applicato alle macchine virtuali creando gruppi di affinità costituiti da macchine virtuali e/o host con un insieme di parametri e condizioni identici. A seconda che le macchine virtuali di un gruppo di affinità vengano eseguite sullo stesso host o su host del gruppo o separatamente su host diversi, i parametri del gruppo di affinità possono definire affinità positiva o affinità negativa.

Per configurare i gruppi di affinità, fare riferimento al collegamento appropriato riportato di seguito per la versione di VMware vSphere in uso.

"Documentazione vSphere 6.7: Utilizzo delle regole di affinità DRS".<https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-FF28F29C-8B67-4EFF-A2EF-63B3537E6934.html>["Documentazione vSphere 7.0: Utilizzo delle regole di affinità DRS"]].



Anthos dispone di un'opzione di configurazione in ogni singolo utente `cluster.yaml` File per creare automaticamente regole di affinità dei nodi che possono essere attivate o disattivate in base al numero di host ESXi nell'ambiente.

## Anthos su bare metal

### Benefici

Le funzionalità indipendenti dall'hardware di anthos on bare metal ti consentono di scegliere una piattaforma di calcolo ottimizzata per il tuo caso d'utilizzo personalizzato e di offrire molti vantaggi aggiuntivi.

Alcuni esempi includono:

- **Porta il tuo server.** puoi utilizzare server che corrispondono alla tua infrastruttura esistente per ridurre le spese di capitale e i costi di gestione.
- **Porta il tuo sistema operativo Linux.** scegliendo il sistema operativo Linux al quale desideri implementare l'ambiente anthos-on-bare-metal, puoi assicurarti che l'ambiente anthos si adatti perfettamente all'infrastruttura e agli schemi di gestione esistenti.
- **Prestazioni migliorate e costi ridotti.** senza la necessità di un hypervisor, i cluster anthos-on-bare-metal richiedono l'accesso diretto alle risorse hardware del server, inclusi i dispositivi hardware ottimizzati per le performance come le GPU.
- **Prestazioni di rete migliorate e latenza ridotta.** poiché i nodi server anthos-on-bare-metal sono collegati direttamente alla rete senza un livello di astrazione virtualizzato, possono essere ottimizzati per bassa latenza e performance.

### Requisiti hardware

### Calcolo

Google Cloud richiede periodicamente la convalida aggiornata delle piattaforme server dei partner con le nuove release di anthos attraverso il programma per partner della piattaforma anthos Ready. È possibile trovare un elenco delle piattaforme server attualmente validate e delle versioni di anthos supportate "qui".

La seguente tabella contiene le piattaforme server testate dai partner engineer NetApp e NetApp per la

convalida di anthos sulle implementazioni bare metal.

| Produttore | Fare     | Modello |
|------------|----------|---------|
| Cisco      | UCS      | B200 M5 |
| HPE        | ProLiant | DL360   |

### Sistema operativo

I nodi anthos-on-bare-metal possono essere configurati con diverse distribuzioni Linux scelte dal cliente per adattarsi all'attuale infrastruttura del data center.

La seguente tabella contiene un elenco dei sistemi operativi Linux utilizzati da NetApp e dai partner per la convalida della soluzione.

| Sistema operativo        | Rilasciare                                | Versioni anthos |
|--------------------------|---|-----------------|
| CentOS                   | 8.4.2105                                  | 1.14            |
| Red Hat Enterprise Linux | 8.4                                       | 1.14            |
| Ubuntu                   | 18.04.5 LTS (con kernel 5.4.0-81-generic) | 1.14            |
| Ubuntu                   | 20.04.2 LTS                               | 1.14            |

### Hardware aggiuntivo

Per completare l'implementazione di anthos su bare metal come soluzione completamente validata, NetApp e i nostri partner hanno testato componenti aggiuntivi per il data center per il networking e lo storage.

La tabella seguente contiene informazioni su questi componenti dell'infrastruttura aggiuntivi.

| Produttore | Nome hardware | Modello    |
|------------|---------------|------------|
| Cisco      | Nexus         | C9336C-FX2 |
| NetApp     | AFF           | A250, A220 |

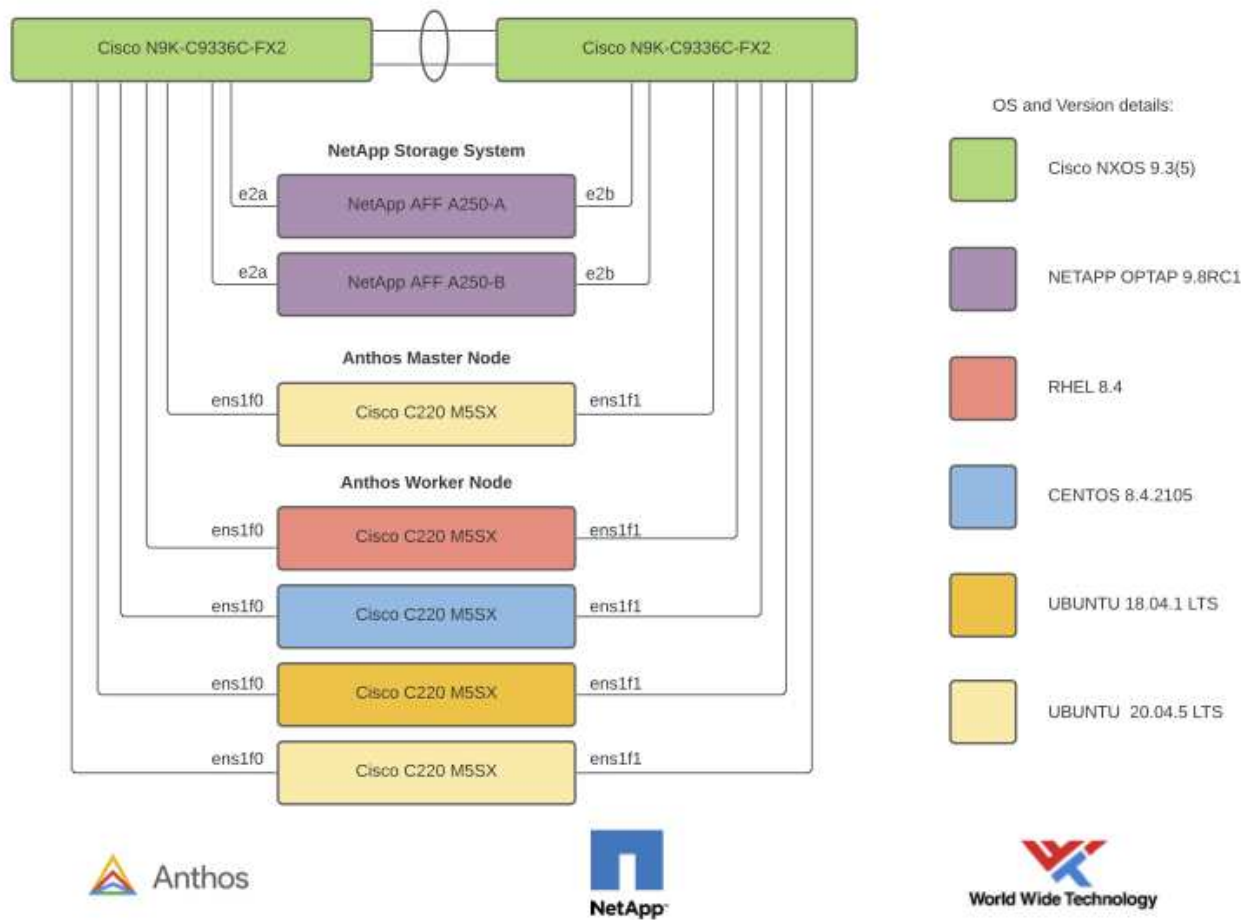
### Software aggiuntivo

La seguente tabella include un elenco delle versioni software aggiuntive implementate nell'ambiente di convalida.

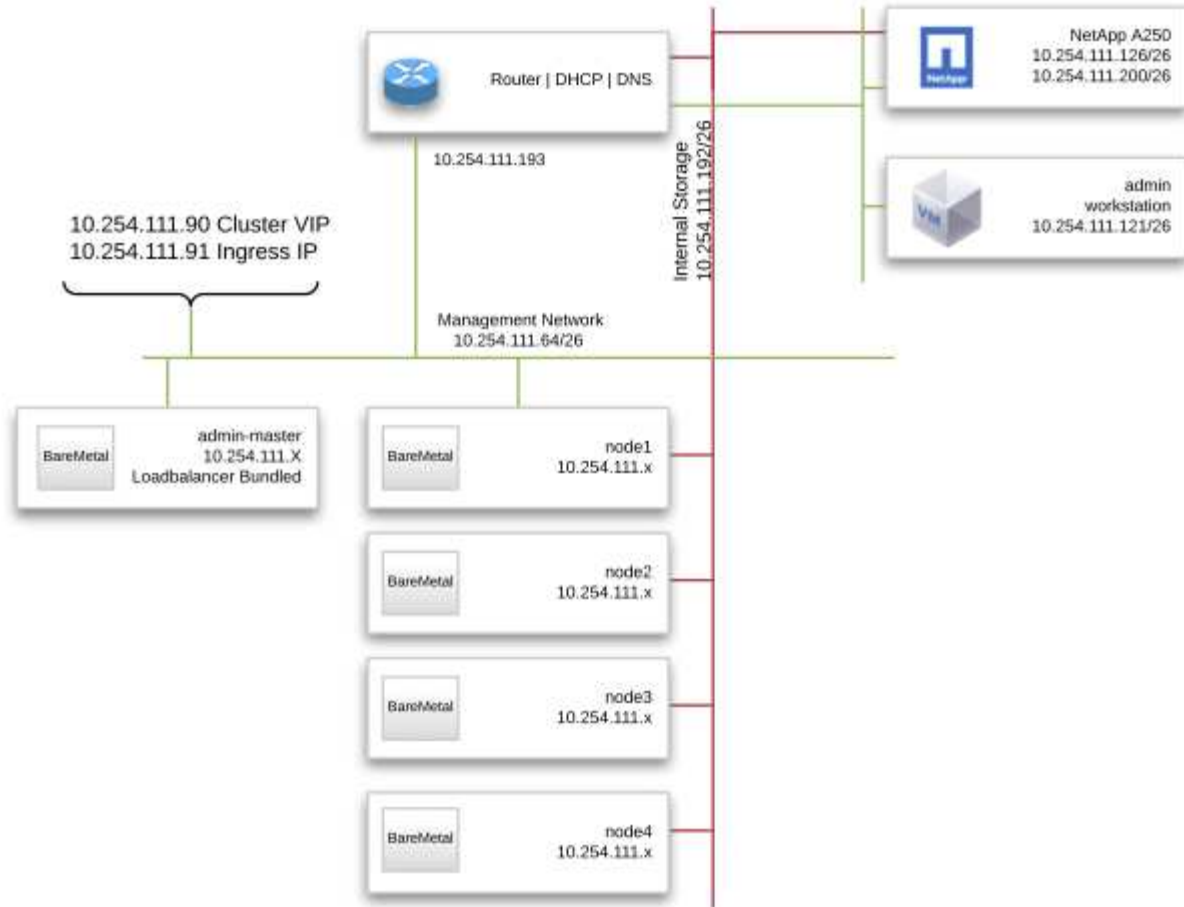
| Produttore | Nome del software | Versione |
|------------|-------------------|----------|
| Cisco      | NXOS              | 9.3(5)   |
| NetApp     | ONTAP             | 9.11.1P4 |
| NetApp     | Astra Trident     | 23.01.0  |

Durante la convalida della piattaforma anthos Ready eseguita da NetApp e dal nostro team di partner di World Wide Technology (WWT), l'ambiente di laboratorio è stato costruito sulla base del seguente diagramma, che ci ha consentito di testare la funzionalità di ogni tipo di server, sistema operativo, dispositivi di rete, e sistemi storage implementati nella soluzione.

## Anthos BareMetal Physical Hardware and Network Diagram







Questo ambiente multi-OS mostra l'interoperabilità con le versioni dei sistemi operativi supportate per la soluzione anthos-on-bare-metal. Prevediamo che i clienti si standardizzeranno su uno o un sottoinsieme di sistemi operativi per la loro implementazione.

## Risorse di supporto dell'infrastruttura

Prima dell'implementazione di anthos su bare metal, deve essere implementata la seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host accessibile dalla rete di gestione.
- Almeno un server NTP accessibile dalla rete di gestione.
- (Opzionale) connettività Internet in uscita per la rete di gestione in banda.

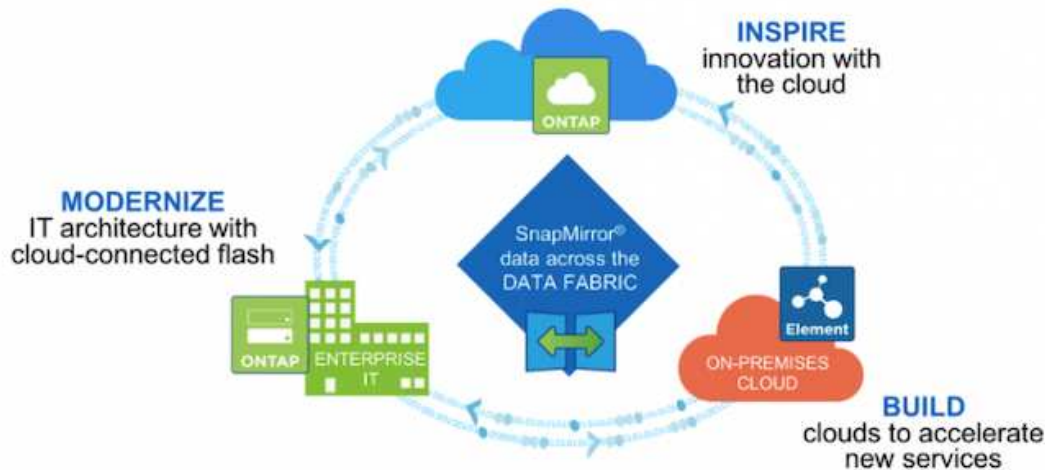


Nella sezione Video e demo di questo documento è disponibile un video dimostrativo su un'implementazione di anthos su bare metal.

## Panoramica dello storage NetApp

NetApp dispone di diverse piattaforme di storage qualificate con Astra Trident Storage

Orchestrator per il provisioning dello storage per le applicazioni implementate come container.



- I sistemi AFF e FAS eseguono NetApp ONTAP e forniscono storage per i casi di utilizzo basati su file (NFS) e basati su blocchi (iSCSI).
- Cloud Volumes ONTAP e ONTAP Select offrono gli stessi vantaggi rispettivamente nel cloud e nello spazio virtuale.
- NetApp Cloud Volumes Service (GCP) e Azure NetApp Files offrono storage basato su file nel cloud.
- Amazon FSX per NetApp ONTAP è un servizio completamente gestito su AWS che fornisce storage per casi di utilizzo basati su file.



Ogni sistema storage del portfolio NetApp può semplificare la gestione dei dati e lo spostamento tra i siti on-premise e il cloud, garantendo che i dati si trovino nella posizione in cui si trovano le applicazioni.

## NetApp ONTAP

NetApp ONTAP è un potente tool software per lo storage con funzionalità come GUI intuitiva, API REST con integrazione dell'automazione, analisi predittive e azioni correttive informate dell'ai, aggiornamenti hardware senza interruzioni e importazione di storage incrociato.

Per ulteriori informazioni sul sistema di storage NetApp ONTAP, visitare il sito ["Sito Web di NetApp ONTAP"](#).

ONTAP offre le seguenti funzionalità:

- Un sistema storage unificato con accesso e gestione simultanei dei dati di NFS, CIFS, iSCSI, FC, FCoE, E protocolli FC-NVMe.
- Diversi modelli di implementazione includono configurazioni hardware on-premise su all-flash, ibride e all-HDD, piattaforme di storage basate su VM su un hypervisor supportato come ONTAP Select e nel cloud

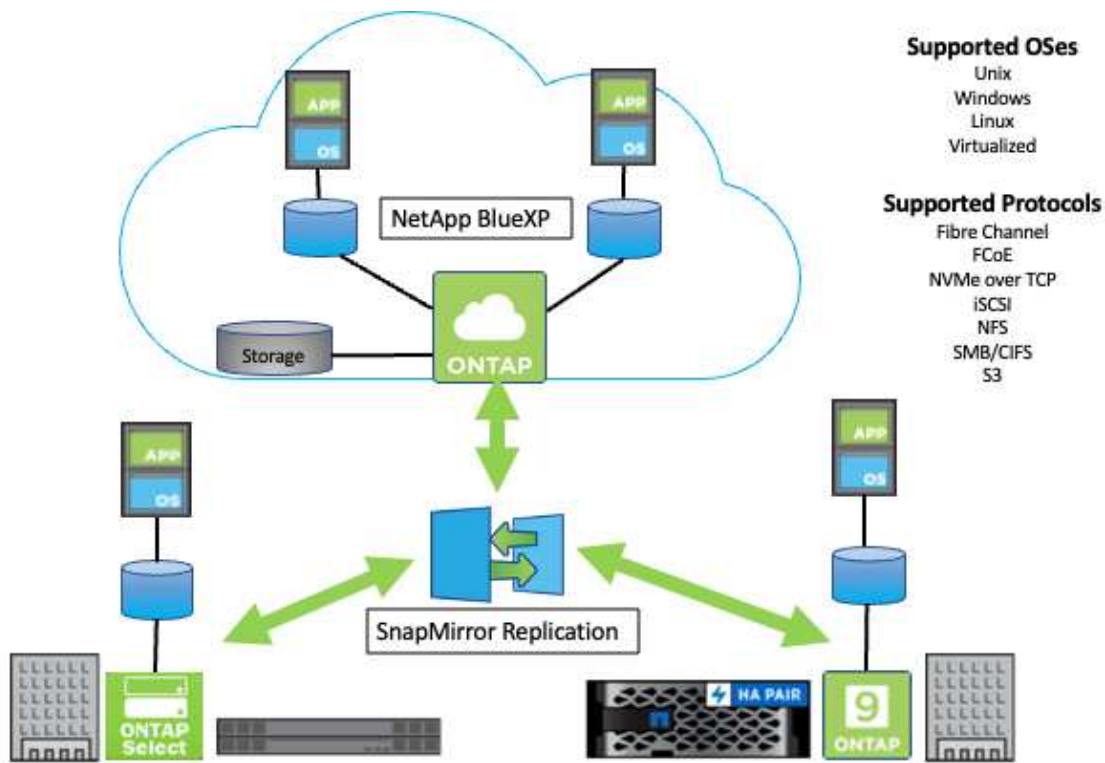
come Cloud Volumes ONTAP.

- Maggiore efficienza dello storage dei dati sui sistemi ONTAP con supporto per tiering automatico dei dati, compressione dei dati inline, deduplica e compaction.
- Storage basato su workload e controllato dalla QoS.
- Integrazione perfetta con un cloud pubblico per tiering e protezione dei dati. ONTAP offre inoltre solide funzionalità di protezione dei dati che lo differenziano in qualsiasi ambiente:
  - **NetApp Snapshot Copies.** Backup rapido e point-in-time dei dati utilizzando una quantità minima di spazio su disco senza alcun overhead delle performance aggiuntivo.
  - **NetApp SnapMirror.** Mirror le copie Snapshot dei dati da un sistema storage a un altro. ONTAP supporta il mirroring dei dati su altre piattaforme fisiche e servizi nativi del cloud.
  - **NetApp SnapLock.** Amministrazione efficiente dei dati non riscrivibili, scrivendo su volumi speciali che non possono essere sovrascritti o cancellati per un determinato periodo.
  - **NetApp SnapVault.** esegue il backup dei dati da più sistemi storage in una copia Snapshot centrale che funge da backup su tutti i sistemi designati.
  - **NetApp SyncMirror.** offre mirroring dei dati in tempo reale a livello RAID su due diversi plessi di dischi collegati fisicamente allo stesso controller.
  - **NetApp SnapRestore.** offre un rapido ripristino dei dati di backup on-demand dalle copie Snapshot.
  - **NetApp FlexClone.** fornisce il provisioning istantaneo di una copia leggibile e scrivibile di un volume NetApp basata su una copia Snapshot.

Per ulteriori informazioni su ONTAP, consultare ["Centro documentazione di ONTAP 9"](#).



NetApp ONTAP è disponibile on-premise, virtualizzato o nel cloud.



## Piattaforme NetApp

### NetApp AFF/FAS

NetApp offre solide piattaforme di storage all-flash (AFF) e ibride scale-out (FAS), realizzate su misura con performance a bassa latenza, protezione integrata dei dati e supporto multiprotocollo.

Entrambi i sistemi sono basati sul software per la gestione dei dati NetApp ONTAP, il software per la gestione dei dati più avanzato del settore per una gestione dello storage semplificata, integrata nel cloud e altamente disponibile, in grado di offrire la velocità, l'efficienza e la sicurezza di livello Enterprise di cui ha bisogno il data fabric.

Per ulteriori informazioni sulle piattaforme NETAPP AFF e FAS, fare clic su ["qui"](#).

### ONTAP Select

ONTAP Select è un'implementazione software-defined di NetApp ONTAP che può essere implementata su un hypervisor nel tuo ambiente. Può essere installato su VMware vSphere o su KVM e offre tutte le funzionalità e l'esperienza di un sistema ONTAP basato su hardware.

Per ulteriori informazioni su ONTAP Select, fare clic su ["qui"](#).

### Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è una versione di NetApp ONTAP implementata nel cloud e disponibile per l'implementazione in diversi cloud pubblici, tra cui: Amazon AWS, Microsoft Azure e Google Cloud.

Per ulteriori informazioni su Cloud Volumes ONTAP, fare clic su ["qui"](#).

## Panoramica sull'integrazione dello storage NetApp

### Programma per partner di storage anthos Ready.

Google Cloud richiede periodicamente la convalida aggiornata delle integrazioni di storage dei partner con le nuove release di anthos attraverso il programma per partner di storage anthos Ready. È possibile trovare un elenco delle soluzioni storage attualmente validate, dei driver CSI, delle funzionalità disponibili e delle versioni di anthos supportate ["qui"](#).

NetApp ha mantenuto una conformità regolare su base trimestrale con le richieste di validare il nostro orchestrator di storage conforme a Astra Trident CSI e il nostro sistema di storage ONTAP con le versioni di anthos.

La tabella seguente contiene le versioni anthos testate dai tecnici dei partner NetApp e NetApp per la convalida dei driver e delle funzionalità di NetApp Astra Trident CSI nell'ambito del programma per partner di storage anthos Ready:

| Tipo di implementazione | Versione | Sistema storage | Versione di Astra Trident | Protocollo | Caratteristiche   |
|-------------------------|----------|-----------------|---------------------------|------------|---|
| VMware                  | 1,28     | ONTAP 9.12.1    | 24,02                     | NAS        | Multiwriter, espansione dei volumi, snapshot, PVCDataSource |

|        |      |               |       |     |  |
|--------|------|---------------|-------|-----|--|
| VMware | 1,28 | ONTAP 9.12.1  | 24,02 | SAN | Blocco raw, espansione dei volumi, snapshot, PVCDDataSource  |
| VMware | 1.15 | ONTAP 9.12.1  | 23.04 | NAS | Multiwriter, espansione dei volumi, snapshot, PVCDDataSource |
| VMware | 1.15 | ONTAP 9.12.1  | 23.04 | SAN | Blocco raw, espansione dei volumi, snapshot, PVCDDataSource  |
| VMware | 1.14 | ONTAP 9.12.1  | 23.01 | NAS | Multiwriter, espansione dei volumi, snapshot, PVCDDataSource |
| VMware | 1.14 | ONTAP 9.12.1  | 23.01 | SAN | Blocco raw, espansione dei volumi, snapshot, PVCDDataSource  |
| VMware | 1.13 | ONTAP 9.12.1  | 22.10 | NAS | Multiwriter, espansione dei volumi, snapshot, PVCDDataSource |
| VMware | 1.13 | ONTAP 9.12.1  | 22.10 | SAN | Blocco raw, espansione dei volumi, snapshot, PVCDDataSource  |
| VMware | 1.11 | ONTAP 9.9.1   | 22.04 | NAS | Multiwriter, Volume Expansion, snapshot                      |
| VMware | 1.11 | ONTAP 9.9.1   | 22.04 | SAN | Blocco raw, espansione del volume, snapshot                  |
| VMware | 1.11 | Elemento 12.3 | 22.04 | SAN | Blocco raw, espansione del volume, snapshot                  |

|              |      |           |       |     |   |
|--------------|------|-----------|-------|-----|---|
| metallo nudo | 1.10 | ONTAP 9.8 | 22.01 | NAS | Multivriter, Volume Expansion, snapshot     |
| metallo nudo | 1.10 | ONTAP 9.8 | 22.01 | SAN | Blocco raw, espansione del volume, snapshot |

## Integrazioni di storage NetApp

NetApp offre una serie di prodotti che consentono di orchestrare e gestire i dati persistenti in ambienti basati su container come Anthos.

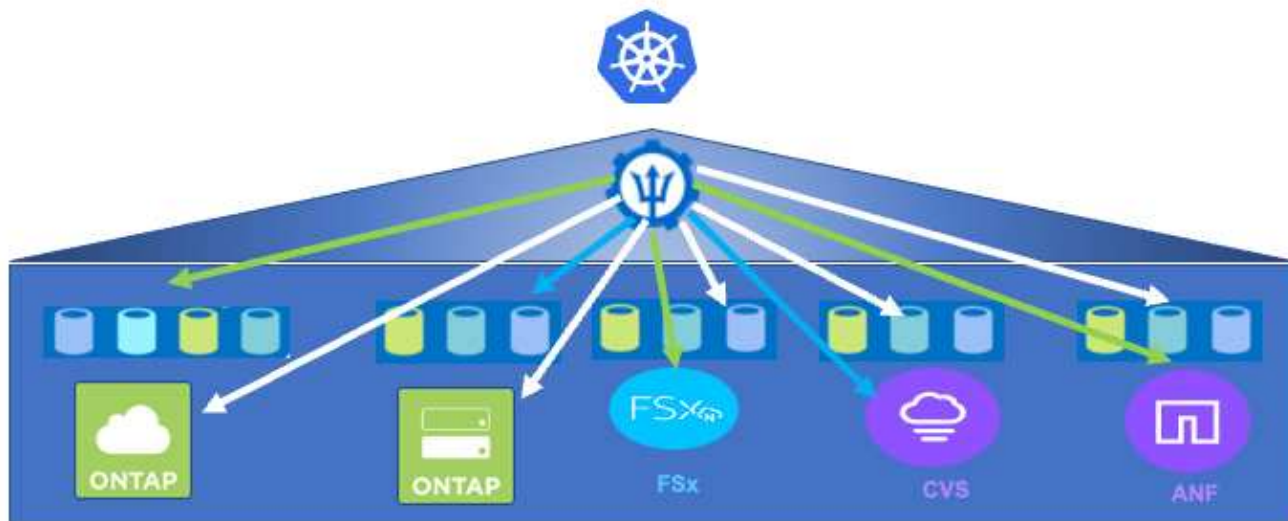
NetApp Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, incluso Anthos. Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

Le pagine seguenti contengono informazioni aggiuntive sui prodotti NetApp validati per la gestione delle applicazioni e dello storage persistente nella soluzione anthos con NetApp.

## Panoramica di Astra Trident

Astra Trident è un orchestrator di storage open-source completamente supportato per container e distribuzioni Kubernetes, incluso Anthos. Trident lavora con l'intero portfolio di storage NetApp, incluso NetApp ONTAP, e supporta anche connessioni NFS e iSCSI. Trident accelera il workflow DevOps consentendo agli utenti finali di eseguire il provisioning e gestire lo storage dai sistemi storage NetApp senza richiedere l'intervento di un amministratore dello storage.

Un amministratore può configurare una serie di backend di storage in base alle esigenze di progetto e ai modelli di sistemi di storage che consentono funzionalità di storage avanzate, tra cui compressione, tipi di dischi specifici e livelli di QoS che garantiscono un certo livello di performance. Una volta definiti, questi backend possono essere utilizzati dagli sviluppatori nei loro progetti per creare dichiarazioni di volume persistenti (PVC) e per collegare storage persistente ai propri container on-demand.



Astra Trident ha un rapido ciclo di sviluppo e, come Kubernetes, viene rilasciato quattro volte all'anno.

È possibile trovare la documentazione relativa all'ultima versione di Astra Trident ["qui"](#). Matrice di supporto per quale versione di Trident è stata testata con la quale è possibile trovare la distribuzione Kubernetes ["qui"](#).

A partire dalla versione 20.04, l'impostazione di Trident viene eseguita dall'operatore Trident. L'operatore semplifica le implementazioni su larga scala e fornisce supporto aggiuntivo, inclusa la riparazione automatica dei pod implementati nell'installazione di Trident.

Con la versione 22.04, è stato reso disponibile un grafico Helm per facilitare l'installazione dell'operatore Trident.

Per informazioni dettagliate sull'installazione di Astra Trident, vedere ["qui"](#).

### Creare un backend di sistema storage

Dopo aver completato l'installazione di Astra Trident Operator, è necessario configurare il backend per la piattaforma di storage NetApp specifica in uso. Seguire il link riportato di seguito per continuare l'installazione e la configurazione di Astra Trident. ["Creare un backend."](#)

### Creare una classe di storage

Dopo aver creato il backend, è necessario creare una classe di storage che gli utenti Kubernetes specificheranno quando desiderano un volume. Kubernetes consente agli utenti di eseguire il provisioning dei volumi utilizzando le dichiarazioni di volumi persistenti (PVC) che specificano una classe di storage in base al nome. Fare clic sul collegamento riportato di seguito per creare una classe di storage. ["Creare una classe di storage"](#)

### Eseguire il provisioning dinamico di un volume

È necessario creare un oggetto Kubernetes Persistent Volume claim (PVC) utilizzando la classe storage per eseguire il provisioning dinamico di un volume. Fare clic sul collegamento riportato di seguito per creare un

oggetto PVC. ["Creare un PVC"](#)

#### Utilizzare il volume

Il volume fornito nella fase precedente può essere utilizzato da un'applicazione montando il volume nel pod. Il link seguente mostra un esempio. ["Montare il volume in un pod"](#)

## Opzioni di configurazione avanzate

In genere, la soluzione più semplice da implementare è la migliore, ma in alcuni casi sono necessarie personalizzazioni avanzate per soddisfare i requisiti o le specifiche di un'applicazione specifica o dell'ambiente in cui la soluzione viene implementata. A tal fine, la soluzione Red Hat OpenShift con NetApp consente le seguenti personalizzazioni per soddisfare queste esigenze.



In questa sezione sono state documentate alcune opzioni di configurazione avanzate, come l'utilizzo di bilanciatori di carico di terze parti o la creazione di un registro privato per l'hosting di immagini container personalizzate, entrambi prerequisiti per l'installazione di NetApp Astra Control Center.

Le pagine seguenti contengono informazioni aggiuntive sulle opzioni di configurazione avanzate validate nella soluzione Red Hat OpenShift con NetApp:

### Analisi delle opzioni di bilanciamento del carico

Un'applicazione implementata in anthos è esposta al mondo da un servizio fornito da un bilanciamento del carico implementato nell'ambiente anthos on-premise.

Le seguenti pagine contengono informazioni aggiuntive sulle opzioni di bilanciamento del carico validate nella soluzione anthos con NetApp:

- ["Installazione di F5 BIG-IP load balancer"](#)
- ["Installazione dei bilanciatori di carico MetalLB"](#)
- ["Installazione di bilanciatori di carico seesaw"](#)

#### Installazione di F5 BIG-IP load balancer

F5 BIG-IP è un Application Delivery Controller (ADC) che offre un'ampia gamma di servizi avanzati di gestione del traffico e di sicurezza di livello produttivo come il bilanciamento del carico L4-L7, l'offload SSL/TLS, DNS, firewall e altro ancora. Questi servizi aumentano notevolmente la disponibilità, la sicurezza e le performance delle applicazioni.

F5 BIG-IP può essere implementato e utilizzato in vari modi, tra cui su hardware dedicato, nel cloud o come appliance virtuale on-premise. Fare riferimento alla documentazione qui per esplorare e implementare F5 BIG-IP.

F5 BIG-IP è stata la prima delle soluzioni di bilanciamento del carico in bundle disponibili con anthos on-Prem ed è stata utilizzata in una serie delle prime validazioni dei partner anthos Ready per la soluzione anthos con NetApp.





F5 BIG-IP può essere implementato in modalità standalone o cluster. Ai fini di questa convalida, F5 BIG-IP è stato implementato in modalità standalone. Tuttavia, per scopi di produzione, NetApp consiglia di creare un cluster di istanze BIG-IP per evitare un singolo punto di errore.



Un sistema F5 BIG-IP può essere implementato su hardware dedicato, nel cloud o come appliance virtuale on-premise con versioni superiori alla 12.x per l'integrazione con F5 CIS. Ai fini di questo documento, il sistema F5 BIG-IP è stato validato come appliance virtuale, ad esempio utilizzando l'edizione BIG-IP VE.

## Release validate

Questa soluzione utilizza l'appliance virtuale implementata in VMware vSphere. Il networking per l'appliance virtuale F5 Big-IP può essere configurato in una configurazione a due o tre armi in base all'ambiente di rete. L'implementazione di questo documento si basa sulla configurazione a due armi. Ulteriori informazioni sulla configurazione dell'appliance virtuale per l'utilizzo con Anthos sono disponibili ["qui"](#).

Il Solutions Engineering Team di NetApp ha convalidato le release riportate nella seguente tabella del nostro laboratorio per lavorare con le implementazioni di Anthos on-Prem:

| Fare | Tipo       | Versione      |
|------|------------|---------------|
| F5   | VE. BIG-IP | 15.0.1-0.0.11 |
| F5   | VE. BIG-IP | 16.1.0-0.0.19 |

## Installazione

Per installare F5 BIG-IP, attenersi alla seguente procedura:

1. Scaricare il file dell'applicazione virtuale Open Virtual Appliance (OVA) da F5 ["qui"](#).



Per scaricare l'appliance, l'utente deve registrarsi con F5. Forniscono una licenza demo di 30 giorni per Big-IP Virtual Edition Load Balancer. NetApp consiglia una licenza permanente da 10 Gbps per l'implementazione in produzione di un'appliance.

2. Fare clic con il pulsante destro del mouse su Infrastructure Resource Pool e selezionare Deploy OVF Template (implementa modello OVF). Viene avviata una procedura guidata che consente di selezionare il file OVA appena scaricato nella fase 1. Fare clic su Avanti.

## Deploy OVF Template

### 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

### Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

http | https://remoteserver-address/filetoinstall.ovf | .ova

☒ Local file

Choose Files

BIGIP-15.0.1-0.....ALL-vmware.ova

CANCEL

BACK

NEXT

3. Fare clic su Next (Avanti) per continuare con ogni passaggio e accettare i valori predefiniti per ciascuna schermata visualizzata fino a quando non viene visualizzata la schermata di selezione della memoria. Selezionare il VM\_Datastore in cui si desidera implementare la macchina virtuale, quindi fare clic su Avanti.
4. La schermata successiva presentata dalla procedura guidata consente di personalizzare le reti virtuali per l'utilizzo nell'ambiente. Selezionare VM\_Network per il campo External (esterno) e Management\_Network per il campo Management (Gestione). Interni e ha vengono utilizzati per le configurazioni avanzate dell'appliance F5 Big-IP e non sono configurati. Questi parametri possono essere lasciati soli oppure possono essere configurati per connettersi a gruppi di porte distribuiti non infrastrutturali. Fare clic su Avanti.

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks**
- 9 Ready to complete

### Select networks

Select a destination network for each source network.

| Source Network | Destination Network |
|----------------|---------------------|
| Internal       | BIG-IP-Internal     |
| External       | VM_Network          |
| HA             | BIG-IP-HA           |
| Management     | Management_Network  |

4 items

### IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

5. Esaminare la schermata di riepilogo dell'appliance e, se tutte le informazioni sono corrette, fare clic su fine per avviare l'implementazione.
6. Una volta implementata l'appliance virtuale, fare clic con il pulsante destro del mouse e accenderla. Dovrebbe ricevere un indirizzo DHCP sulla rete di gestione. L'appliance è basata su Linux e dispone di VMware Tools, in modo da poter visualizzare l'indirizzo DHCP ricevuto nel client vSphere.

The screenshot shows the vSphere VM Summary view for a virtual machine named 'BIGIP-15.0.1-0.0.11-vmware-B'. The VM is powered on. The summary includes details about the Guest OS (CentOS 4/5 or later (64-bit)), Compatibility (ESXi 5.5 and later (VM version 10)), and VMware Tools (Running, version:10245 (Guest Managed)). It also shows the DNS Name (localhost.localdomain), IP Addresses (127.20.0.254), and Host (172.21.224.101). A tooltip is visible over the IP Addresses field, showing the IP Addresses: 127.20.0.254, 127.1.1.254, and 172.21.224.20.

7. Aprire un browser Web e connettersi all'appliance utilizzando l'indirizzo IP indicato nella fase precedente. L'accesso predefinito è admin/admin e, dopo il primo accesso, l'appliance richiede immediatamente di modificare la password admin. Viene quindi visualizzata una schermata in cui è necessario accedere con le nuove credenziali.

**f5** BIG-IP Configuration Utility  
F5 Networks, Inc.

**Hostname**  
bigip1

**IP Address**  
172.21.224.20

**Username**  
admin

**Password**  
\*\*\*\*\*

Log in

Welcome to the BIG-IP Configuration Utility.  
Log in with your username and password using the fields on the left.

(c) Copyright 1996-2019, F5 Networks, Inc., Seattle, Washington. All rights reserved.  
[F5 Networks, Inc. Legal Notices](#)

8. La prima schermata richiede all'utente di completare l'utilità di configurazione. Avviare l'utility facendo clic su Next (Avanti).

Welcome

**Setup Utility**

To begin configuring this BIG-IP® system, please complete the Setup Utility. To begin, click the "Next" button.

Next...

9. La schermata successiva richiede l'attivazione della licenza per l'appliance. Fare clic su Activate (attiva) per iniziare. Quando richiesto nella pagina successiva, incollare la chiave di licenza di valutazione di 30 giorni ricevuta al momento della registrazione per il download o la licenza permanente acquistata al momento dell'acquisto dell'appliance. Fare clic su Avanti.

| General Properties           |  |
|------------------------------|--|
| Base Registration Key        | BFXBY-PVROQ-QIHCH-NZGSZ-AZCFDPX <span>Revert</span>  |
| Add-On Registration Key List | Add-On Key <input type="text"/> <span>Add</span><br><div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <span>Edit</span> <span>Delete</span> |
|                              |  |
| Activation Method            | <input checked="" type="radio"/> Automatic (requires outbound connectivity) <input type="radio"/> Manual   |
| Outbound Interface           | mgmt ▼   |
| License Comparison           | <input type="checkbox"/> Enable License Comparison   |
| <span>Next...</span>         |  |



Affinché il dispositivo esegua l'attivazione, la rete definita nell'interfaccia di gestione deve essere in grado di raggiungere Internet.

10. Nella schermata successiva, viene visualizzato il Contratto di licenza con l'utente finale (EULA). Se i termini della licenza sono accettabili, fare clic su Accept (Accetta).
11. La schermata successiva conta il tempo trascorso durante la verifica delle modifiche di configurazione apportate finora. Fare clic su Continue (continua) per riprendere la configurazione iniziale.

## BIG-IP system configuration has changed

Tue Nov 05 2019 18:10:20

The configuration for this device has been updated. Consequently, the features and functionality previously available on the BIG-IP system might have changed.

Elapsed Time: 49 seconds

✓ Please wait while the configuration changes are verified...  
The BIG-IP Configuration utility will be updated momentarily.

✓ Configuration changes have been verified  
You may now continue using the BIG-IP Configuration utility.

Continue

12. La finestra Modifica configurazione si chiude e l'Utilità di configurazione visualizza il menu Provisioning risorse. Questa finestra elenca le funzionalità attualmente concesse in licenza e le allocazioni delle risorse correnti per l'appliance virtuale e ciascun servizio in esecuzione.

| Current Resource Allocation |               |  |  |  |
|-----------------------------|---------------|--|--|--|
| CPU                         | MGMT TMM(55%) |  |  |  |
| Disk (24GB)                 | MGMT          |  |  |  |
| Memory (3.8GB)              | MGMT TMM      |  |  |  |

| Module                                     | Provisioning | License Status | Required Disk (GB) | Required Memory (MB) |
|--|--------------|----------------|--------------------|----------------------|
| Management (MGMT)                          | Small        | N/A            | 0                  | 1070                 |
| Local Traffic (LTM)                        | Nominal      | Licensed       | 0                  | 854                  |
| Application Security (ASM)                 | None         | Licensed       | 20                 | 1492                 |
| Fraud Protection Service (FPS)             | None         | N/A            | 12                 | 544                  |
| Global Traffic (DNS)                       | None         | Licensed       | 0                  | 148                  |
| Link Controller (LC)                       | None         | Unlicensed     | 0                  | 148                  |
| Access Policy (APM)                        | None         | Limited        | 12                 | 494                  |
| Application Visibility and Reporting (AVR) | None         | Licensed       | 16                 | 576                  |
| Policy Enforcement (PEM)                   | None         | Unlicensed     | 16                 | 1223                 |
| Advanced Firewall (AFM)                    | None         | Licensed       | 16                 | 1058                 |
| Application Acceleration Manager (AAM)     | None         | Unlicensed     | 32                 | 2050                 |
| Secure Web Gateway (SWG)                   | None         | Unlicensed     | 24                 | 4096                 |
| iRules Language Extensions (iRulesLX)      | None         | Licensed       | 0                  | 748                  |
| URLDB Minimal (URLDB)                      | None         | Unlicensed     | 36                 | 2048                 |
| SSL Orchestrator (SSLO)                    | None         | Unlicensed     | 0                  | 128                  |
| Carrier Grade NAT (CGNAT)                  | None         | Licensed       | 16                 | 336                  |

13. Facendo clic sull'opzione di menu Platform (piattaforma) a sinistra è possibile apportare ulteriori modifiche alla piattaforma. Le modifiche includono l'impostazione dell'indirizzo IP di gestione configurato con DHCP, l'impostazione del nome host e del fuso orario in cui è installato l'appliance e la protezione dell'appliance dall'accessibilità SSH.

| General Properties     |  |
|------------------------|--|
| Management Config IPv4 | <input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual |
| Management Config IPv6 | <input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual |
| Host Name              | <input type="text" value="Anthos-F5-Big-IP"/>                                  |
| Host IP Address        | <input type="text" value="Use Management Port IP Address"/>                    |
| Time Zone              | <input type="text" value="America/New York"/>                                  |

| User Administration |   |
|---------------------|---|
| Root Account        | <input type="checkbox"/> Disable login<br>Password: <input type="text"/><br>Confirm: <input type="text"/> |
| SSH Access          | <input checked="" type="checkbox"/> Enabled   |
| SSH IP Allow        | <input type="text" value="* All Addresses"/>  |

14. Fare clic sul menu Network (rete), che consente di configurare le funzioni di rete standard. Fare clic su Next (Avanti) per avviare la Configurazione di rete standard.

**Standard Network Configuration**  
Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- NTP
- DNS
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

**Advanced Network Configuration**  
Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

15. La prima pagina della procedura guidata configura la ridondanza; lasciare le impostazioni predefinite e fare clic su Avanti. La pagina successiva consente di configurare un'interfaccia interna sul bilanciamento del carico. L'interfaccia 1.1 viene mappata alla VMNIC etichettata Internal nella procedura guidata di implementazione di OVF.

**Internal Network Configuration**

|             |                |                 |
|-------------|----------------|-----------------|
| Self IP     | Address:       | 192.168.1.11    |
|             | Netmask:       | 255.255.255.0   |
|             | Port Lockdown: | Allow Default ▼ |
| Floating IP | Address:       | 192.168.1.10    |
|             | Port Lockdown: | Allow Default ▼ |

**Internal VLAN Configuration**

|             |   |
|-------------|---|
| VLAN Name   | Internal  |
| VLAN Tag ID | auto  |
| Interfaces  | VLAN Interfaces: 1.1 ▼  |
|             | Tagging: Select... ▼  |
|             | <input type="button" value="Add"/>  |
|             | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |



Gli spazi in questa pagina per l'indirizzo IP automatico, la netmask e l'indirizzo IP mobile possono essere riempiti con un indirizzo IP non instradabile da utilizzare come segnaposto. È inoltre possibile utilizzare una rete interna configurata come gruppo di porte distribuito per i guest virtuali se si sta implementando la configurazione a tre armi. Per continuare con la procedura guidata, è necessario completarli.

16. La pagina successiva consente di configurare una rete esterna utilizzata per mappare i servizi ai pod implementati in Kubernetes. Selezionare un IP statico dall'intervallo VM\_Network, la subnet mask appropriata e un IP mobile dello stesso intervallo. L'interfaccia 1.2 viene mappata alla VMNIC etichettata External nella procedura guidata di implementazione di OVF.

| External Network Configuration |  |
|--------------------------------|--|
| External VLAN                  | <input checked="" type="radio"/> Create VLAN external <input type="radio"/> Select existing VLAN   |
| Self IP                        | Address: <input type="text" value="10.63.172.101"/><br>Netmask: <input type="text" value="255.255.255.0"/><br>Port Lockdown: <input type="text" value="Allow None"/> |
| Default Gateway                | <input type="text" value="10.63.172.1"/>   |
| Floating IP                    | Address: <input type="text" value="10.63.172.100"/><br>Port Lockdown: <input type="text" value="Allow None"/>  |

| External VLAN Configuration |  |
|-----------------------------|--|
| VLAN Name                   | <input type="text" value="external"/>  |
| VLAN Tag ID                 | <input type="text" value="auto"/>  |
| Interfaces                  | VLAN Interfaces: <input type="text" value="1.2"/><br>Tagging: <input type="text" value="Select..."/><br><input type="button" value="Add"/><br><div style="border: 1px solid #ccc; height: 40px; margin-top: 5px;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

17. Nella pagina successiva, è possibile configurare una rete ha interna se si stanno implementando più appliance virtuali nell'ambiente. Per procedere, è necessario compilare i campi Self-IP Address (Indirizzo IP automatico) e Netmask (maschera di rete) e selezionare Interface 1.3 (interfaccia VLAN), che viene mappata alla rete ha definita dalla creazione guidata dei modelli OVF.

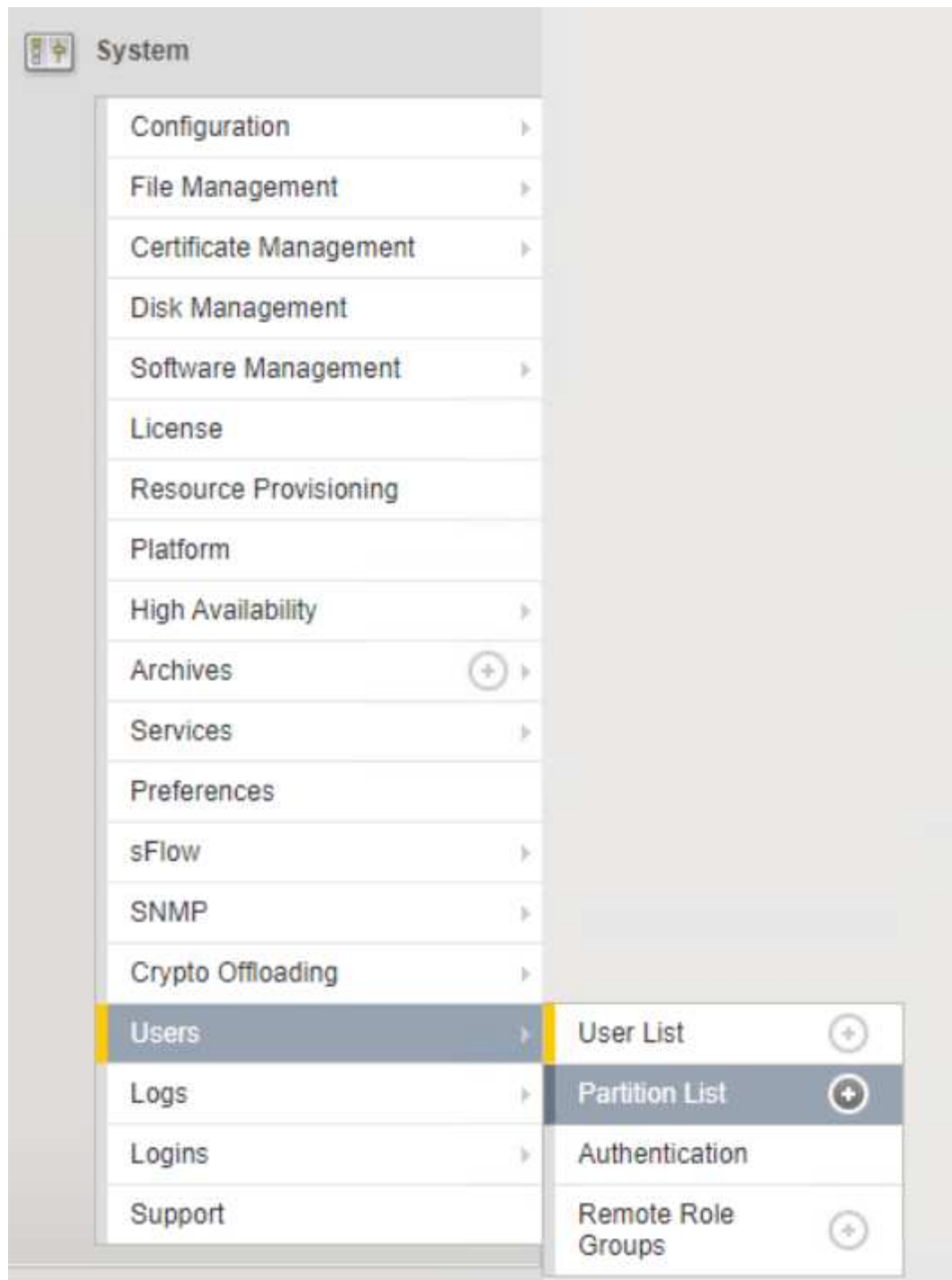
| High Availability Network Configuration |   |
|---|---|
| High Availability VLAN                  | <input checked="" type="radio"/> Create VLAN HA <input type="radio"/> Select existing VLAN                |
| Self IP                                 | Address: <input type="text" value="192.168.2.11"/><br>Netmask: <input type="text" value="255.255.255.0"/> |

| High Availability VLAN Configuration |  |
|--------------------------------------|--|
| VLAN Name                            | <input type="text" value="HA"/>  |
| VLAN Tag ID                          | <input type="text" value="auto"/>  |
| Interfaces                           | VLAN Interfaces: <input type="text" value="1.3"/><br>Tagging: <input type="text" value="Select..."/><br><input type="button" value="Add"/><br><div style="border: 1px solid #ccc; height: 40px; margin-top: 5px;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

18. La pagina successiva consente di configurare i server NTP. Fare clic su Next (Avanti) per continuare con la configurazione del DNS. I server DNS e l'elenco di ricerca dei domini devono essere già popolati dal server DHCP. Fare clic su Next (Avanti) per accettare le impostazioni predefinite e continuare.
19. Per il resto della procedura guidata, fare clic su Next (Avanti) per continuare con la configurazione avanzata del peering, la cui configurazione non rientra nell'ambito di questo documento. Quindi fare clic su fine per uscire dalla procedura guidata.
20. Creare singole partizioni per il cluster di amministrazione anthos e per ciascun cluster utente implementato nell'ambiente. Fare clic su System (sistema) nel menu a sinistra, selezionare Users (utenti) e fare clic su Partition List (elenco partizioni).





21. La schermata visualizzata mostra solo la partizione comune corrente. Fare clic su Create (Crea) a destra per creare la prima partizione aggiuntiva e assegnarle un nome GKE-Admin. Quindi fare clic su Repeat (Ripeti) e assegnare un nome alla partizione User-Cluster-1. Fare nuovamente clic sul pulsante Repeat (Ripeti) per assegnare un nome alla partizione successiva User-Cluster-2. Infine, fare clic su fine per completare la procedura guidata. Viene visualizzata nuovamente la schermata elenco partizioni con tutte le partizioni elencate.

| Search                                   |  | Create...                      |
|--|--|--------------------------------|
| <input checked="" type="checkbox"/> Name |  | Partition Default Route Domain |
| <input type="checkbox"/> Anthos-Admin    |  | 0                              |
| <input type="checkbox"/> Anthos-Cluster1 |  | 0                              |
| <input type="checkbox"/> Anthos-Cluster2 |  | 0                              |
| <input type="checkbox"/> Common          |  | 0                              |
| Delete...                                |  |                                |

## Integrazione con anthos

Ogni file di configurazione contiene una sezione, rispettivamente per il cluster di amministrazione e per ogni cluster di utenti che si sceglie di implementare per configurare il bilanciamento del carico in modo che venga gestito da anthos su Prem.

Il seguente script è un esempio della configurazione della partizione per il cluster GKE-Admin. I valori che devono essere non commentati e modificati vengono inseriti in grassetto di seguito:

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
    # # be the same across clusters
    # # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
  # the corresponding field below to provide the detailed spec
  kind: F5BigIP
  # # (Required when using "ManualLB" kind) Specify pre-defined nodeports
# manualLB:
  # # NodePort for ingress service's http (only needed for user cluster)
  # ingressHTTPONodePort: 0
  # # NodePort for ingress service's https (only needed for user
cluster)
  # ingressHTTPSNodePort: 0
  # # NodePort for control plane service
  # controlPlaneNodePort: 30968
  # # NodePort for addon service (only needed for admin cluster)
  # addonsNodePort: 31405
  # # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
  # # credentials
  f5BigIP:
    address: "172.21.224.21"
    credentials:
```

```

    username: "admin"
    password: "admin-password"
    partition: "GKE-Admin"
#   #   (Optional) Specify a pool name if using SNAT
#   # snatPoolName: ""
# (Required when using "Seesaw" kind) Specify the Seesaw configs
# seesaw:
#   (Required) The absolute or relative path to the yaml file to use for
IP allocation
#   for LB VMs. Must contain one or two IPs.
#   ipBlockFilePath: ""
#   (Required) The Virtual Router Identifier of VRRP for the Seesaw
group. Must
#   be between 1-255 and unique in a VLAN.
#   vrid: 0
#   (Required) The IP announced by the master of Seesaw group
#   masterIP: ""
#   (Required) The number CPUs per machine
#   cpus: 4
#   (Required) Memory size in MB per machine
#   memoryMB: 8192
#   (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
#   network)
#   vCenter:
#     vSphere network name
#     networkName: VM_Network
#   (Optional) Run two LB VMs to achieve high availability (default:
false)
#   enableHA: false

```

## Installazione dei bilanciatori di carico MetalLB

Questa pagina elenca le istruzioni di installazione e configurazione per il bilanciamento del carico gestito da MetalLB.

### Installazione del bilanciamento del carico MetalLB

Il bilanciamento del carico MetalLB è completamente integrato con i cluster anthos su VMware e ha eseguito l'implementazione automatica come parte delle configurazioni dei cluster Admin e User a partire dalla release 1.11. Vi sono blocchi di testo nei rispettivi `cluster.yaml` file di configurazione che è necessario modificare per fornire informazioni sul bilanciamento del carico. Viene eseguito in hosting automatico sul cluster anthos invece di richiedere l'implementazione di risorse esterne come le altre soluzioni di bilanciamento del carico supportate. Consente inoltre di creare un pool ip che assegna automaticamente gli indirizzi con la creazione di servizi Kubernetes di tipo bilanciamento del carico in cluster che non vengono eseguiti su un provider cloud.

## Integrazione con anthos

Quando si attiva il bilanciamento del carico di MetalLB per l'amministratore di anthos, è necessario modificare alcune righe in `loadBalancer:` che esiste in `admin-cluster.yaml` file. Gli unici valori che è necessario modificare sono l'impostazione di `controlPlaneVIP`: quindi impostare `kind`: Come MetalLB. Vedere il seguente frammento di codice per un esempio:

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
    features). Must
    # # be the same across clusters
    # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
  "MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```

Quando si abilita il bilanciamento del carico MetalLB per i cluster di utenti anthos, vi sono due aree in ciascuna `user-cluster.yaml` file da aggiornare. In primo luogo, in modo simile a `admin-cluster.yaml` modificare il `controlPlaneVIP`:, `ingressVIP`:, e `kind`: valori in `loadBalancer:` sezione. Vedere il seguente frammento di codice per un esempio:

```
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.240"
    # Shared by all services for ingress traffic
    ingressVIP: "10.61.181.244"
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
  "MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```



L'indirizzo IP `entressVIP` deve trovarsi all'interno del pool di indirizzi IP assegnati al bilanciamento del carico MetalLB in un secondo momento della configurazione.

Quindi, accedere a `metalLB:` sottosezione e modificare `addressPools`: assegnando un nome al pool in `- name: variabile`. È inoltre necessario creare un pool di indirizzi ip che MetalLB può assegnare ai servizi di tipo LoadBalancer fornendo un intervallo a `addresses: variabile`.

```
# # (Required when using "MetalLB" kind in user clusters) Specify the
MetalLB config
  metalLB:
    # # (Required) A list of non-overlapping IP pools used by load balancer
typed services.
    # # Must include ingressVIP of the cluster.
    addressPools:
      # # (Required) Name of the address pool
      - name: "default"
      # # (Required) The addresses that are part of this pool. Each address
must be either
      # # in the CIDR form (1.2.3.0/24) or range form (1.2.3.1-1.2.3.5).
      addresses:
        - "10.61.181.244-10.61.181.249"
```



Il pool di indirizzi può essere fornito come un intervallo come nell'esempio, limitandolo a un numero di indirizzi in una particolare subnet, oppure può essere fornito come notazione CIDR se l'intera subnet è resa disponibile.

1. Quando vengono creati servizi Kubernetes di tipo LoadBalancer, MetalLB assegna automaticamente un IP esterno ai servizi e annuncia l'indirizzo IP rispondendo alle richieste ARP.

#### Installazione di bilanciatori di carico seesaw

Questa pagina elenca le istruzioni di installazione e configurazione per il bilanciamento del carico gestito da seesaw.

Seesaw è il bilanciamento del carico di rete gestito predefinito installato in un cluster anthos su ambiente VMware dalle versioni 1.6 alla 1.10.

#### Installazione del bilanciamento del carico di scarico

Il bilanciamento del carico seesaw è completamente integrato con i cluster anthos su VMware e ha eseguito l'implementazione automatica come parte delle configurazioni dei cluster Admin e User. Sono presenti blocchi di testo in `cluster.yaml` i file di configurazione che devono essere modificati per fornire informazioni sul bilanciamento del carico, quindi prima dell'implementazione del cluster è necessario eseguire un ulteriore passaggio per implementare il bilanciamento del carico utilizzando il sistema integrato `gkectl` tool.



I bilanciatori di carico Seesaw possono essere implementati in modalità ha o non ha. Ai fini di questa convalida, il bilanciamento del carico di seesaw è stato implementato in modalità non ha, che è l'impostazione predefinita. Per scopi di produzione, NetApp consiglia di implementare seesaw in una configurazione ha per garantire tolleranza agli errori e affidabilità.

#### Integrazione con anthos

Ogni file di configurazione contiene una sezione, rispettivamente per il cluster di amministrazione e per ogni cluster di utenti che si sceglie di implementare, per configurare il bilanciamento del carico in modo che venga gestito da anthos on-Prem.

Il testo seguente è un esempio della configurazione della partizione per il cluster GKE-Admin. I valori che devono essere non commentati e modificati vengono inseriti in grassetto di seguito:

```
loadBalancer:
# (Required) The VIPs to use for load balancing
vips:
# Used to connect to the Kubernetes API
controlPlaneVIP: "10.61.181.230"
# # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
# # be the same across clusters
# # addonsVIP: ""
# (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
# the corresponding field below to provide the detailed spec
kind: Seesaw
# # (Required when using "ManualLB" kind) Specify pre-defined nodeports
# manualLB:
# # NodePort for ingress service's http (only needed for user cluster)
# ingressHTTPTNodePort: 0
# # NodePort for ingress service's https (only needed for user
cluster)
# ingressHTTPSNodePort: 0
# # NodePort for control plane service
# controlPlaneNodePort: 30968
# # NodePort for addon service (only needed for admin cluster)
# addonsNodePort: 31405
# # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
# # credentials
# f5BigIP:
# address:
# credentials:
# username:
# password:
# partition:
# # # (Optional) Specify a pool name if using SNAT
# # snatPoolName: ""
# (Required when using "Seesaw" kind) Specify the Seesaw configs
seesaw:
# (Required) The absolute or relative path to the yaml file to use for
IP allocation
# for LB VMs. Must contain one or two IPs.
ipBlockFilePath: "admin-seesaw-block.yaml"
# (Required) The Virtual Router IDentifier of VRRP for the Seesaw
group. Must
```

```
#   be between 1-255 and unique in a VLAN.
vrid: 100
#   (Required) The IP announced by the master of Seesaw group
masterIP: "10.61.181.236"
#   (Required) The number CPUs per machine
cpus: 1
#   (Required) Memory size in MB per machine
memoryMB: 2048
#   (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
#   network)
vCenter:
#   vSphere network name
networkName: VM_Network
#   (Optional) Run two LB VMs to achieve high availability (default:
false)
enableHA: false
```

Anche il bilanciamento del carico di sequilazione ha un'unità statica separata `seesaw-block.yaml` file che è necessario fornire per ogni implementazione del cluster. Questo file deve trovarsi nella stessa directory relativa a `cluster.yaml` il file di implementazione o il percorso completo devono essere specificati nella sezione precedente.

Un esempio di `admin-seesaw-block.yaml` il file è simile al seguente script:

```
blocks:
- netmask: "255.255.255.0"
  gateway: "10.63.172.1"
  ips:
- ip: "10.63.172.152"
  hostname: "admin-seesaw-vm"
```



Questo file fornisce il gateway e la netmask per la rete che il bilanciamento del carico fornisce al cluster sottostante, nonché l'IP di gestione e il nome host per la macchina virtuale che viene implementata per eseguire il bilanciamento del carico.

## Convalida della soluzione e casi di utilizzo

Gli esempi forniti in questa pagina sono validazioni di soluzioni e casi di utilizzo per anthos con NetApp.

["Installare un'applicazione utilizzando Google Cloud Console"](#)

## Video e demo

Il seguente video mostra alcune delle funzionalità descritte in questo documento:

## Dove trovare ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione NetApp

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Documentazione di NetApp Astra Trident

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- Documentazione di NetApp Astra Control Center

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Documentazione di Anthos Clusters su VMware

["https://cloud.google.com/anthos/clusters/docs/on-prem/latest/overview"](https://cloud.google.com/anthos/clusters/docs/on-prem/latest/overview)

- Anthos sulla documentazione bare metal

["https://cloud.google.com/anthos/clusters/docs/bare-metal/latest"](https://cloud.google.com/anthos/clusters/docs/bare-metal/latest)

- Documentazione VMware vSphere

["https://docs.vmware.com/"](https://docs.vmware.com/)

## TR-4919: DevOps con NetApp Astra

Alan Cowles e Nikhil M Kulkarni, NetApp

### Casi di utilizzo

La soluzione DevOps con NetApp Astra è progettata per offrire un valore eccezionale ai clienti con i seguenti casi di utilizzo:

- Facile da implementare e gestire applicazioni e ambienti di sviluppo implementati su distribuzioni Kubernetes supportate.
- Discussione di casi di utilizzo reali per i flussi di lavoro DevOps ed esempi di strumenti e metodi che NetApp può fornire per semplificare l'adozione e l'utilizzo di questi metodi.
- Esplorazione di come è possibile utilizzare snapshot, backup e cloni coerenti con l'applicazione per migliorare l'esperienza DevOps.



## Valore di business

Le aziende stanno adottando sempre più pratiche DevOps per creare nuovi prodotti, abbreviare i cicli di rilascio e aggiungere rapidamente nuove funzionalità. A causa della loro natura innata e agile, i container e i microservizi svolgono un ruolo cruciale nel supporto delle pratiche DevOps. Tuttavia, la pratica di DevOps su scala di produzione in un ambiente aziendale presenta le proprie sfide e impone determinati requisiti all'infrastruttura sottostante, come ad esempio:

- Alta disponibilità a tutti i livelli dello stack, in modo che i flussi di lavoro non vengano mai interrotti.
- Facilità di implementazione e procedure di gestione per l'utente finale.
- Infrastruttura programmabile e basata su API per restare al passo con i microservizi e l'agilità dello sviluppatore.
- Possibilità di scalare l'infrastruttura in modo indipendente e automatizzato, in base alle esigenze dei carichi di lavoro.
- La protezione delle applicazioni insieme ai set di dati persistenti di supporto per i flussi di lavoro DevOps accelera il time-to-market senza dover fare affidamento sulle ridistribuzioni o sulla copia manuale dei dati.

Riconoscendo queste funzionalità e queste sfide, questo report tecnico illustra il processo di miglioramento e semplificazione dei casi di utilizzo DevOps per le applicazioni containerizzate utilizzando l'ampio portfolio di prodotti NetApp.

## Panoramica della tecnologia

La soluzione DevOps con NetApp contiene i seguenti componenti principali:

### Procedure DevOps

Le pratiche DevOps si concentrano su operazioni automatizzate, ripetibili e facilmente gestibili che migliorano il flusso di lavoro di sviluppo consentendo all'utente finale di controllare l'ambiente in cui sta sviluppando il proprio codice. Questa soluzione fornisce diversi esempi e casi di utilizzo in cui la tecnologia NetApp può essere di maggior beneficio per tali operazioni.

### Orchestrazione di container

Attualmente sono in uso numerose piattaforme di orchestrazione dei container. Anche se la maggior parte di queste piattaforme si basa su Kubernetes, ognuna ha pro e contro. Pertanto, è importante comprendere i set di funzionalità e le integrazioni quando si seleziona una piattaforma di orchestrazione container per i flussi di lavoro DevOps. Con la suite di prodotti NetApp Astra, supportiamo le seguenti piattaforme per casi di utilizzo DevOps completi:

- ["Red Hat OpenShift" 4.6.8+](#)
- ["Rancher" 2.5+](#)
- ["Kubernetes" 1.20+](#)
- ["Griglia VMware Tanzu Kubernetes" 1.4+](#)
- ["VMware Tanzu Kubernetes Grid Integrated Edition" 1.12.2+](#)

### Sistemi storage NetApp

NetApp dispone di diversi sistemi storage perfetti per data center aziendali e implementazioni di cloud ibrido. Il portfolio NetApp include i sistemi storage NetApp ONTAP, NetApp Element e NetApp e-Series, tutti in grado di fornire storage persistente per le applicazioni containerizzate.

Per ulteriori informazioni, visitare il sito Web di NetApp ["qui"](#).

## **Integrazioni di storage NetApp**

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati NetApp.

Per ulteriori informazioni, visitare il sito Web di NetApp Astra ["qui"](#).

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud etc..

Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

## **Panoramica di DevOps**

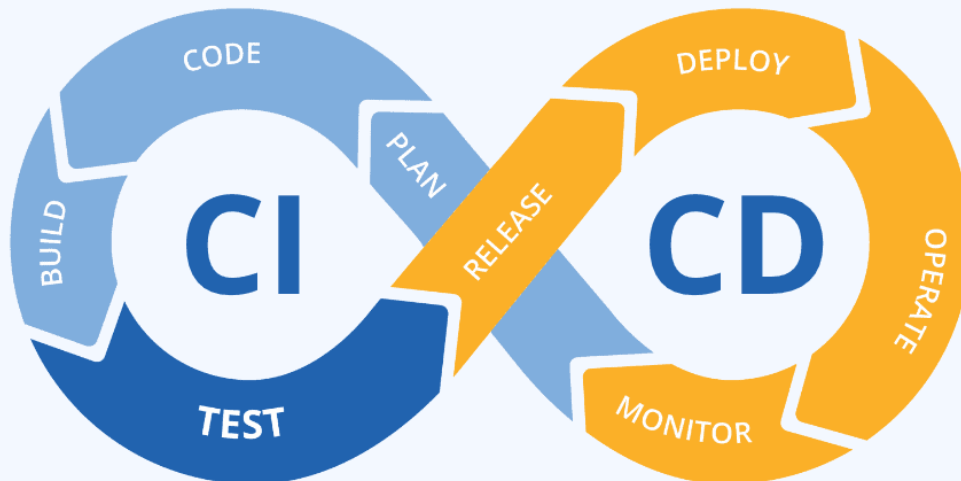
Negli ultimi anni, le organizzazioni che creano software hanno adottato i concetti di DevOps. Le pratiche DevOps abbattano le barriere organizzative, avvicinando i team di sviluppo e operativi. Le pratiche DevOps consentono inoltre ai team di accelerare l'erogazione, aumentare la disponibilità e rendere più stabili servizi e applicazioni, migliorando così la produttività del team. Inoltre, l'adozione di un framework di automazione è anche un elemento chiave del successo, dalla creazione, test e gestione di applicazioni su larga scala o dalla gestione di una piattaforma o stack di infrastruttura completamente automatizzati. Di seguito vengono illustrati alcuni casi di utilizzo principali per DevOps in cui è possibile implementare le soluzioni NetApp per migliorare le esperienze che i professionisti DevOps incontrano durante le loro pratiche quotidiane.

### **Casi di utilizzo DevOps**

Sebbene DevOps non disponga di una singola definizione universalmente accettata, le soluzioni per i professionisti DevOps contengono in genere costrutti o ideologie simili che consentono un'implementazione, una ripetizione e una gestione semplici su larga scala. Le sezioni seguenti descrivono i potenziali casi di utilizzo per i flussi di lavoro DevOps abilitati dalle soluzioni NetApp.

#### **Integrazione continua, erogazione continua e implementazione continua (ci/CD)**

Continuous Integration, Continuous Delivery e Continuous Deployment (ci/CD) è una filosofia di codifica che incoraggia gli sviluppatori a implementare e trasformare le proprie pratiche di codifica stabilendo un metodo per aggiornare, testare e implementare il proprio codice in modo automatizzato. Il metodo più diffuso con cui ci/CD viene implementato nella maggior parte dei flussi di lavoro DevOps è quello della pipeline ci/CD, e esistono diverse applicazioni software di terze parti che possono contribuire a ottenere questo risultato.



Di seguito sono riportati alcuni esempi di applicazioni comuni che possono essere di aiuto con i flussi di lavoro ci/CD-type:

"ArgoCD"

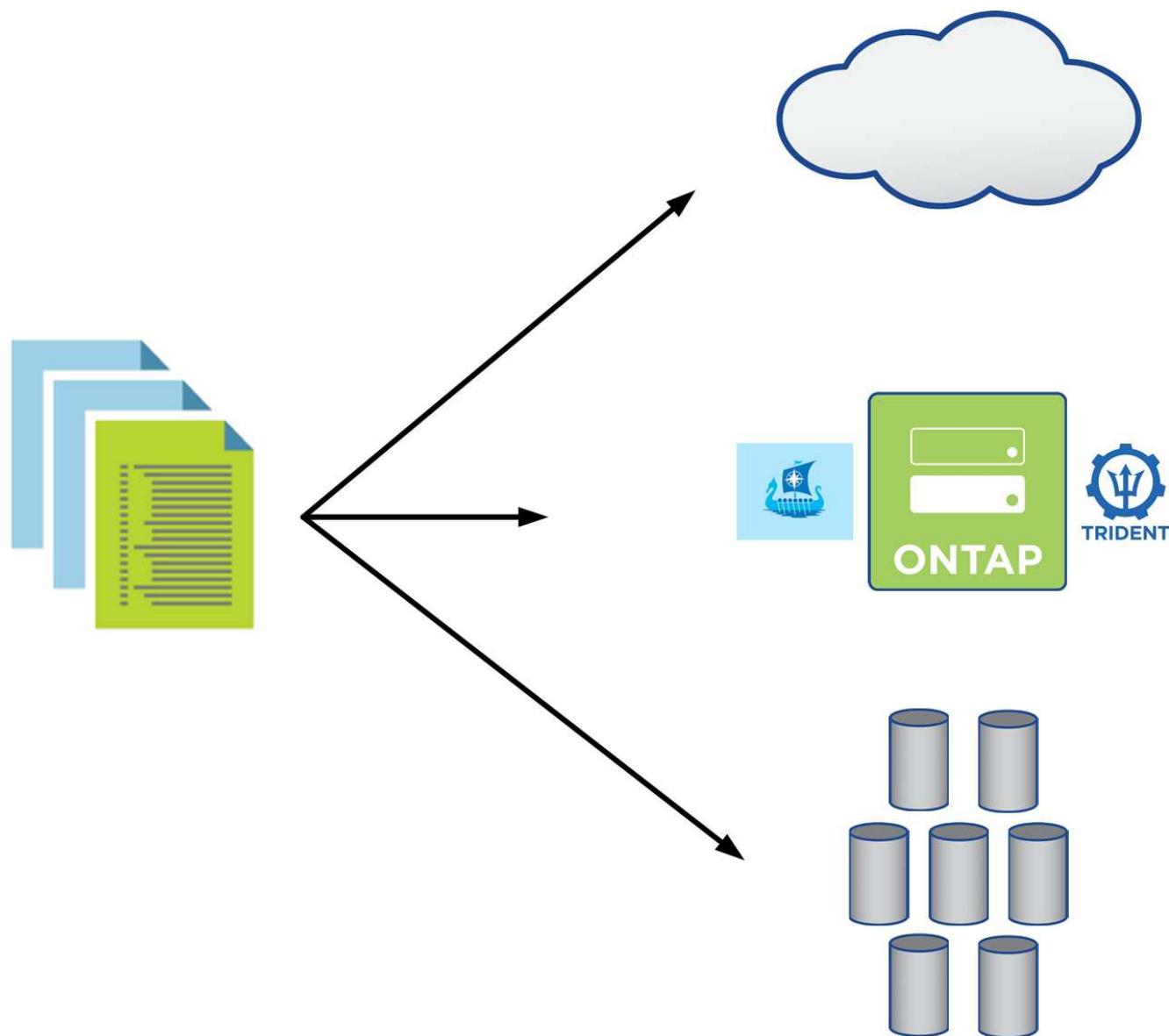
"Jenkins"

"Tekton"

Alcuni dei casi di utilizzo inclusi più avanti in questo report tecnico sono stati dimostrati in Jenkins, ma i principi ci/CD principali possono essere applicati a qualsiasi strumento implementato da un'organizzazione nelle proprie pratiche.

#### **Infrastruttura come codice**

L'infrastruttura come codice aiuta a fornire e gestire le risorse IT attraverso comandi automatizzati, API e kit di sviluppo software (SDK). Questo concetto migliora notevolmente l'esperienza DevOps eliminando i limiti fisici del data center o delle risorse che potrebbero impedire agli sviluppatori di raggiungere i propri obiettivi.

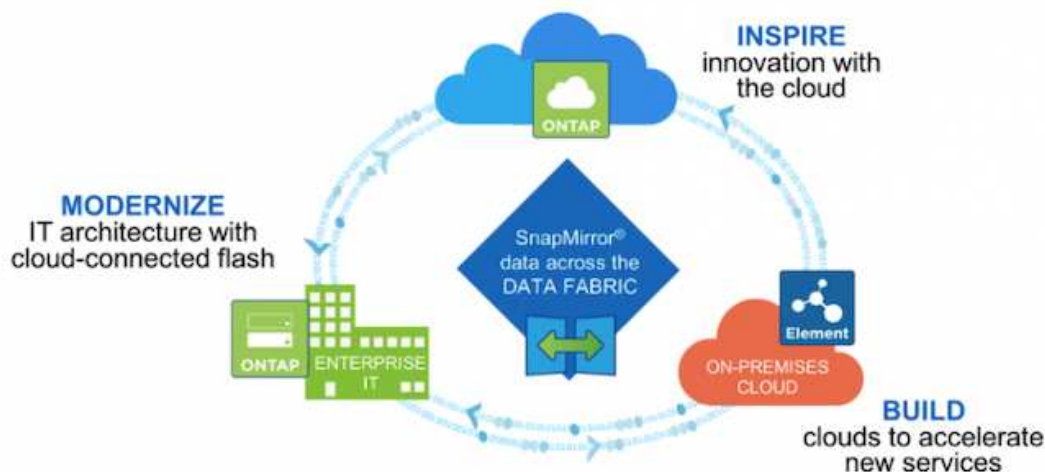


Gli utenti finali spesso utilizzano linguaggi di programmazione come ["Python"](#) o strumenti di automazione come ["Ansible"](#) oppure ["Marionetta"](#) per creare azioni di scalabilità dell'infrastruttura automatizzate e ripetibili che possono essere chiamate dagli sviluppatori quando necessario.

Sia NetApp ONTAP che Astra Control contengono API pubbliche e moduli ansible o toolkit di sviluppo software che rendono le operazioni di automazione molto semplici da adottare e integrare nei processi DevOps.

## Panoramica dei sistemi storage NetApp

NetApp dispone di diverse piattaforme storage qualificate con Astra Trident e Astra Control per il provisioning, la protezione e la gestione dei dati per le applicazioni containerizzate.



- I sistemi AFF e FAS eseguono NetApp ONTAP e forniscono storage per i casi di utilizzo basati su file (NFS) e basati su blocchi (iSCSI).
- Cloud Volumes ONTAP e ONTAP Select offrono gli stessi vantaggi rispettivamente nel cloud e nello spazio virtuale.
- NetApp Cloud Volumes Service (AWS/GCP) e Azure NetApp Files offrono storage basato su file nel cloud.



Ogni sistema storage del portfolio NetApp può semplificare la gestione dei dati e lo spostamento tra i siti on-premise e il cloud, in modo che i dati si trovino dove si trovano le applicazioni.

Le pagine seguenti contengono informazioni aggiuntive sui sistemi di storage NetApp validati nella soluzione DevOps with NetApp:

- ["NetApp ONTAP"](#)

## NetApp ONTAP

NetApp ONTAP è un potente tool software per lo storage con funzionalità come GUI intuitiva, API REST con integrazione dell'automazione, analisi predittive e azioni correttive informate dell'ai, aggiornamenti hardware senza interruzioni e importazione di storage incrociato.

Per ulteriori informazioni sul sistema di storage NetApp ONTAP, visitare il sito ["Sito Web di NetApp ONTAP"](#).

ONTAP offre le seguenti funzionalità:

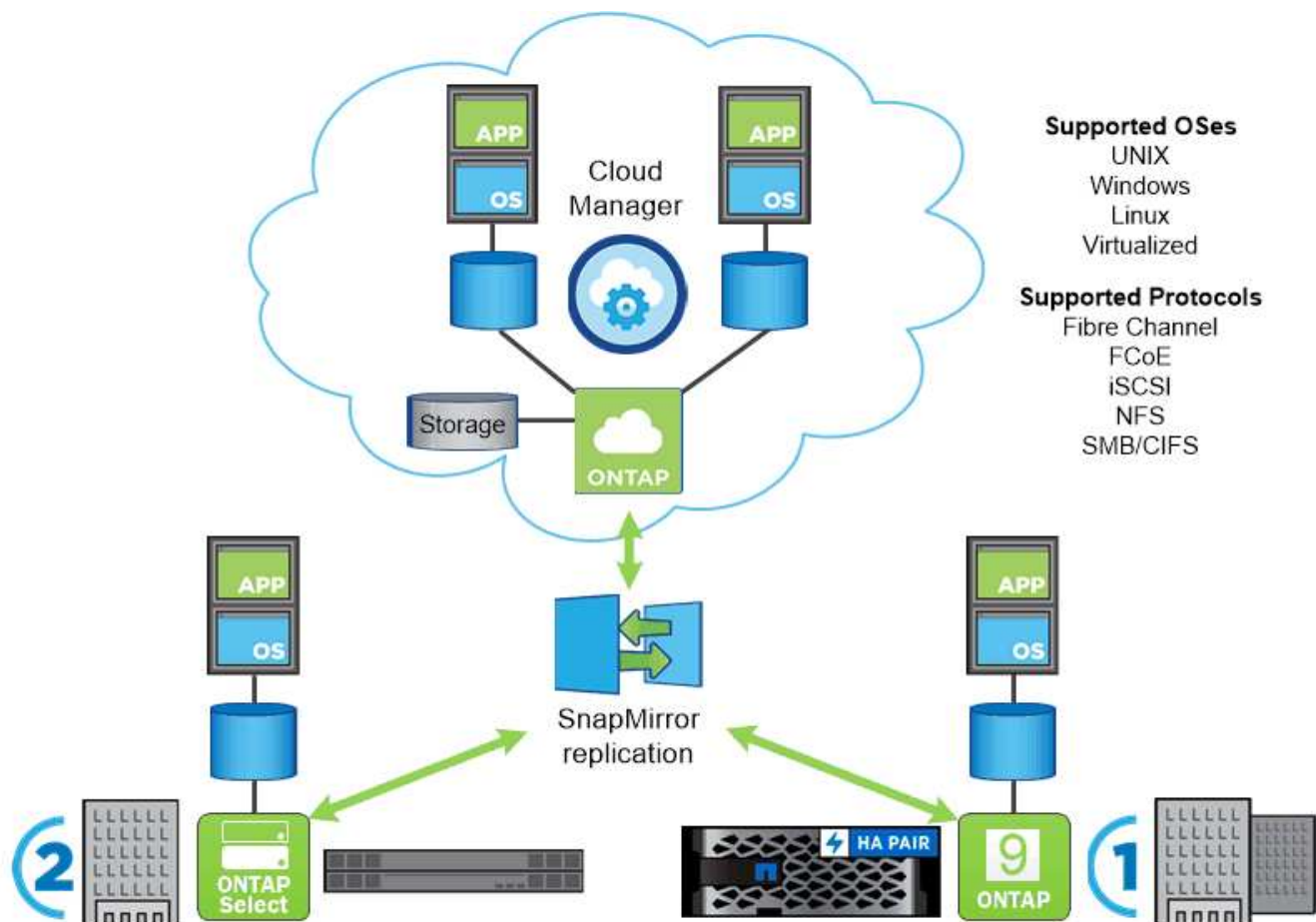
- Un sistema storage unificato con accesso e gestione simultanei dei dati di NFS, CIFS, iSCSI, FC, FCoE, E protocolli FC-NVMe.
- Diversi modelli di implementazione includono configurazioni hardware on-premise su all-flash, ibride e all-HDD, piattaforme di storage basate su VM su un hypervisor supportato come ONTAP Select e nel cloud come Cloud Volumes ONTAP.

- Maggiore efficienza dello storage dei dati sui sistemi ONTAP con supporto per tiering automatico dei dati, compressione dei dati inline, deduplica e compaction.
- Storage basato su workload e controllato dalla QoS.
- Integrazione perfetta con un cloud pubblico per tiering e protezione dei dati. ONTAP offre inoltre solide funzionalità di protezione dei dati che lo differenziano in qualsiasi ambiente:
  - **NetApp Snapshot Copies.** Backup rapido e point-in-time dei dati utilizzando una quantità minima di spazio su disco senza alcun overhead delle performance aggiuntivo.
  - **NetApp SnapMirror.** Mirror le copie Snapshot dei dati da un sistema storage a un altro. ONTAP supporta il mirroring dei dati su altre piattaforme fisiche e servizi nativi del cloud.
  - **NetApp SnapLock.** Amministrazione efficiente dei dati non riscrivibili, scrivendo su volumi speciali che non possono essere sovrascritti o cancellati per un determinato periodo.
  - **NetApp SnapVault.** esegue il backup dei dati da più sistemi storage in una copia Snapshot centrale che funge da backup su tutti i sistemi designati.
  - **NetApp SyncMirror.** offre mirroring dei dati in tempo reale a livello RAID su due diversi plessi di dischi collegati fisicamente allo stesso controller.
  - **NetApp SnapRestore.** offre un rapido ripristino dei dati di backup on-demand dalle copie Snapshot.
  - **NetApp FlexClone.** fornisce il provisioning istantaneo di una copia leggibile e scrivibile di un volume NetApp basata su una copia Snapshot.

Per ulteriori informazioni su ONTAP, consultare ["Centro documentazione di ONTAP 9"](#).



NetApp ONTAP è disponibile on-premise, virtualizzato o nel cloud.



## Piattaforme NetApp

### NetApp AFF/FAS

NetApp offre solide piattaforme di storage all-flash (AFF) e ibride scale-out (FAS), realizzate su misura con performance a bassa latenza, protezione integrata dei dati e supporto multiprotocollo.

Entrambi i sistemi sono basati sul software per la gestione dei dati NetApp ONTAP, il software per la gestione dei dati più avanzato del settore per una gestione dello storage semplificata, altamente disponibile e integrata nel cloud, per offrire velocità, efficienza e sicurezza di livello Enterprise per le tue esigenze di data fabric.

Per ulteriori informazioni sulle piattaforme NETAPP AFF/FAS, fare clic su ["qui"](#).

### ONTAP Select

ONTAP Select è un'implementazione software-defined di NetApp ONTAP che può essere implementata su un hypervisor nel tuo ambiente. Può essere installato su VMware vSphere o su KVM e offre tutte le funzionalità e l'esperienza di un sistema ONTAP basato su hardware.

Per ulteriori informazioni su ONTAP Select, fare clic su ["qui"](#).

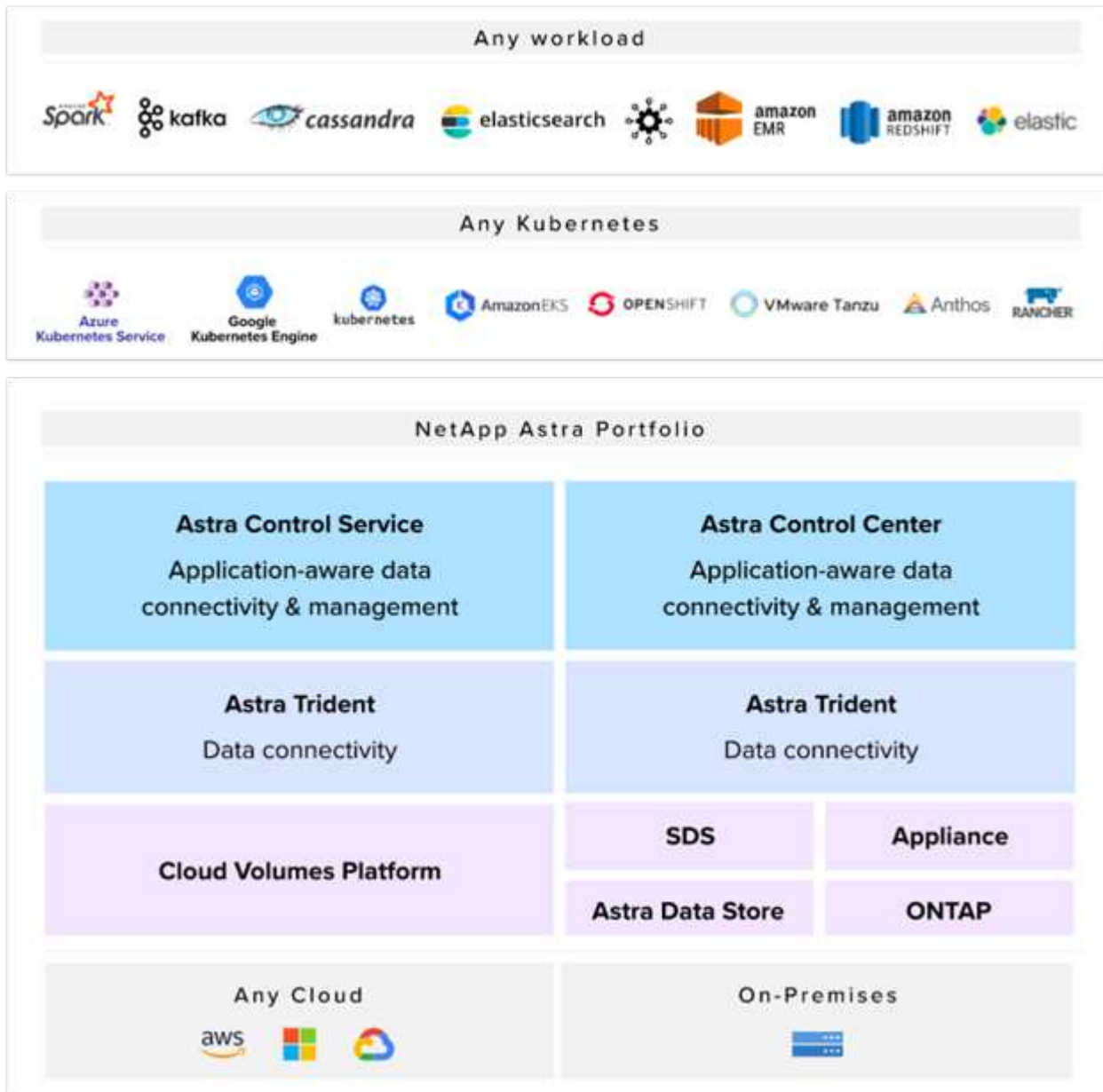
### Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è una versione di NetApp ONTAP implementata nel cloud che può essere implementata in diversi cloud pubblici, tra cui Amazon AWS, Microsoft Azure e Google Cloud.

Per ulteriori informazioni su Cloud Volumes ONTAP, fare clic su ["qui"](#).

## Panoramica sull'integrazione dello storage NetApp

NetApp offre una serie di prodotti che consentono di orchestrare, gestire, proteggere e migrare le applicazioni stateful containerizzate e i relativi dati.



NetApp Astra Control offre un set completo di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful basati sulla tecnologia di protezione dei dati di NetApp. Astra Control Service è disponibile per supportare carichi di lavoro stateful nelle implementazioni Kubernetes native nel cloud. Astra Control Center è disponibile per supportare carichi di lavoro stateful in implementazioni on-premise di piattaforme Enterprise Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito Web di NetApp Astra Control ["qui"](#).

NetApp Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

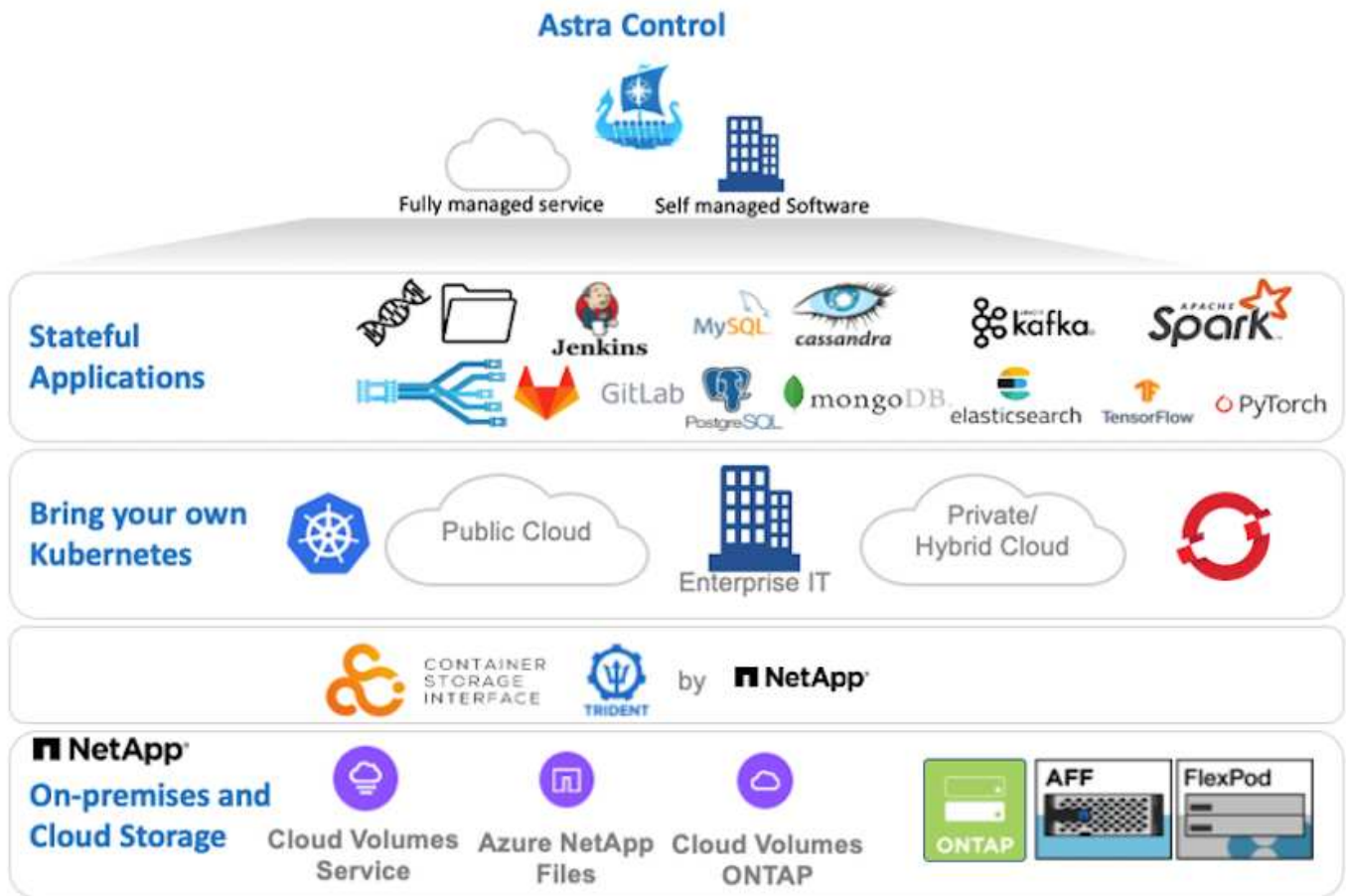


Le pagine seguenti contengono informazioni aggiuntive sui prodotti NetApp validati per la gestione delle applicazioni e dello storage persistente nella soluzione DevOps with NetApp:

- ["NetApp Astra Control Center"](#)
- ["NetApp Astra Trident"](#)

## Panoramica di NetApp Astra Control

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati basati su applicazioni e storage per carichi di lavoro Kubernetes stateful implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati di NetApp.



NetApp Astra Control Center può essere installato su un cluster Kubernetes che ha installato e configurato Astra Trident Storage orchestrator con classi di storage e backend di storage per i sistemi storage NetApp ONTAP.

Per ulteriori informazioni su Astra Trident, vedere ["questo documento qui"](#).

In un ambiente connesso al cloud, il centro di controllo Astra utilizza Cloud Insights per fornire monitoraggio avanzato e telemetria. In assenza di una connessione Cloud Insights, sono disponibili funzioni limitate di monitoraggio e telemetria (per un valore di sette giorni di metriche) ed esportate negli strumenti di monitoraggio nativi di Kubernetes (Prometheus e Grafana) attraverso endpoint di metriche aperte.

Il centro di controllo Astra è completamente integrato nell'ecosistema NetApp AutoSupport e Active IQ per fornire supporto agli utenti, fornire assistenza per la risoluzione dei problemi e visualizzare le statistiche di utilizzo.

Oltre alla versione a pagamento di Astra Control Center, è disponibile anche una licenza di valutazione di 90 giorni. La versione di valutazione è supportata tramite e-mail e il canale slack della community. I clienti hanno accesso a queste risorse, ad altri articoli della Knowledge base e alla documentazione disponibile nella dashboard di supporto dei prodotti.

Per ulteriori informazioni sul portfolio Astra, visitare il ["Sito web Astra"](#).

Per una guida dettagliata all'installazione e alle operazioni su Astra Control Center, seguire la documentazione ["qui"](#).

### Automazione di Astra Control Center

Astra Control Center dispone di un'API REST completamente funzionale per l'accesso programmatico. Gli utenti possono utilizzare qualsiasi linguaggio di programmazione o utility per interagire con gli endpoint API REST di Astra Control. Per ulteriori informazioni su questa API, consultare la documentazione ["qui"](#).

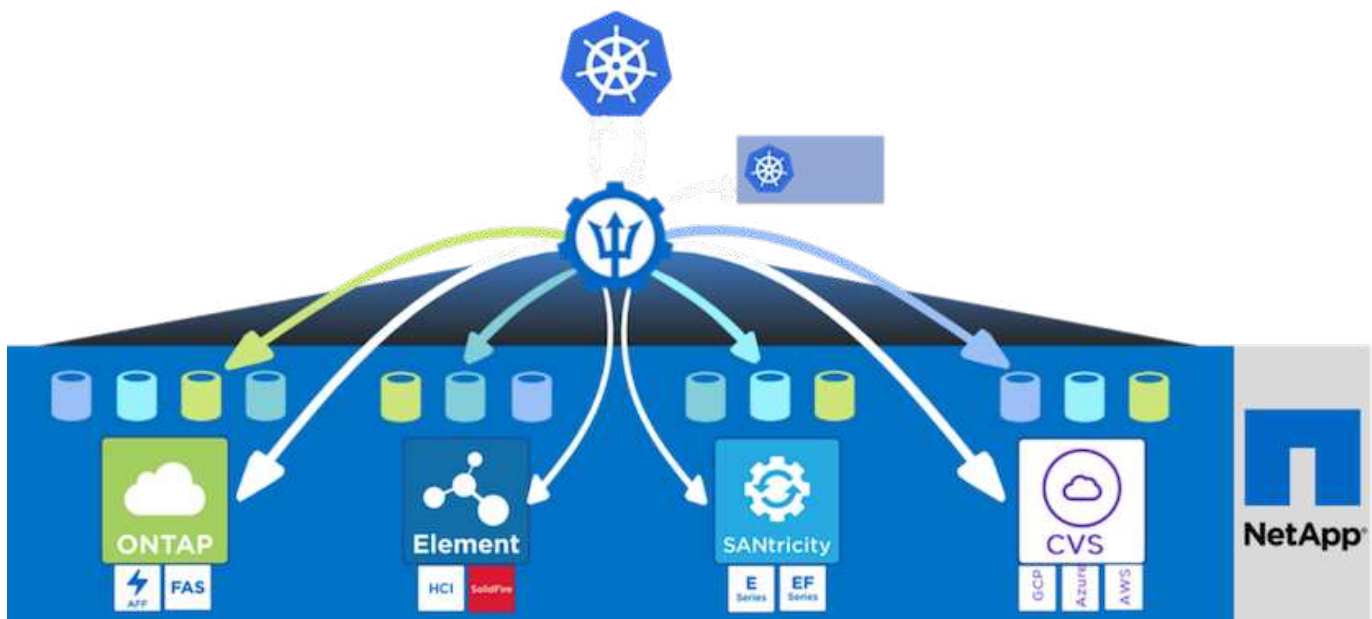
Se stai cercando un toolkit di sviluppo software pronto per interagire con le API REST di Astra Control, NetApp offre un toolkit con Astra Control Python SDK, che puoi scaricare ["qui"](#).

Se la programmazione non è adatta alla tua situazione e desideri utilizzare uno strumento di gestione della configurazione, puoi clonare ed eseguire i playbook Ansible pubblicati da NetApp ["qui"](#).

### Panoramica di Astra Trident

Astra Trident è uno storage orchestrator open-source completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident lavora con l'intero portfolio di storage NetApp, inclusi i sistemi storage NetApp ONTAP ed Element, e supporta anche connessioni NFS e iSCSI. Trident accelera il workflow DevOps consentendo agli utenti finali di eseguire il provisioning e gestire lo storage dai sistemi storage NetApp senza richiedere l'intervento di un amministratore dello storage.

Un amministratore può configurare una serie di backend di storage in base alle esigenze di progetto e ai modelli di sistemi di storage che consentono funzionalità di storage avanzate, tra cui compressione, tipi di dischi specifici o livelli di QoS che garantiscono un certo livello di performance. Una volta definiti, questi backend possono essere utilizzati dagli sviluppatori nei loro progetti per creare dichiarazioni di volume persistenti (PVC) e per collegare storage persistente ai propri container on-demand.



Astra Trident ha un rapido ciclo di sviluppo e, come Kubernetes, viene rilasciato quattro volte all'anno.

L'ultima versione di Astra Trident è la 22.04 rilasciata ad aprile 2022. Matrice di supporto per quale versione di Trident è stata testata con la quale è possibile trovare la distribuzione Kubernetes ["qui"](#).

A partire dalla versione 20.04, l'impostazione di Trident viene eseguita dall'operatore Trident. L'operatore semplifica le implementazioni su larga scala e fornisce supporto aggiuntivo, inclusa la riparazione automatica dei pod implementati nell'installazione di Trident.

Con la versione 21.01, è stato reso disponibile un grafico Helm per facilitare l'installazione dell'operatore Trident.

Consultare la documentazione ["qui"](#) Per installare e utilizzare Astra Trident.

## Validazione dei casi d'utilizzo: DevOps con NetApp Astra

I seguenti casi di utilizzo sono stati validati per DevOps con NetApp Astra:

- ["Integra la protezione nelle pipeline ci/CD con NetApp Astra Control"](#)
- ["Sfrutta Astra Control per facilitare l'analisi post-mortem e ripristinare l'applicazione"](#)
- ["Accelerazione dello sviluppo software con NetApp FlexClones"](#)

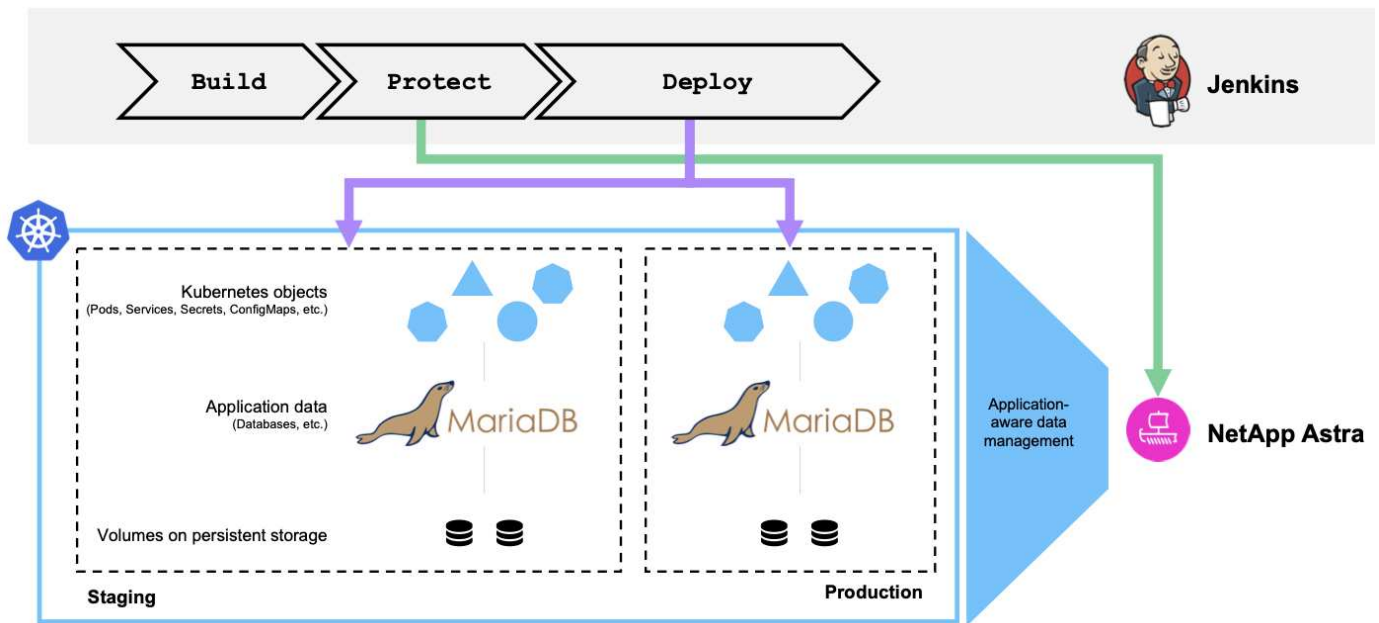
### Integra la protezione nelle pipeline ci/CD con NetApp Astra Control

#### Panoramica

Uno degli utilizzi più comuni dei flussi di lavoro DevOps è l'integrazione continua e le pipeline di implementazione continua (ci/CD) che creano, integrano ed eseguono suite di test automatizzate sulle applicazioni man mano che gli sviluppatori commettono nuovo codice. Gli ingegneri DevOps e gli SREs (Site-Reliability Engineer) dispongono di pipeline dedicate ai vari flussi di lavoro per lo sviluppo di nuove funzionalità, il test di regressione, la correzione di bug, la progettazione della qualità e altre funzioni del processo di sviluppo.

Man mano che i team aumentano il loro livello di automazione, il ritmo del cambiamento per le applicazioni in-produzione può sembrare schiacciante. Pertanto, alcuni team preferiscono proteggere le applicazioni o i servizi in-produzione. Oltre a proteggere il codice e le immagini dei container, desiderano proteggere lo stato dell'applicazione, i dati di configurazione (come gli oggetti Kubernetes e le risorse associate all'applicazione) e i dati persistenti di un'applicazione.

In questo caso di utilizzo, analizziamo più da vicino una pipeline di promozione-produzione che implementa una nuova versione di un'applicazione: Prima in un ambiente di staging e poi in un ambiente di produzione. Questo esempio si applica allo stesso modo ai principali cloud pubblici e anche a un ambiente on-premise. Anche se mostriamo l'implementazione di una versione dell'applicazione, la pipeline può essere utilizzata anche con altre strategie, come l'implementazione blu/verde o canary. Come parte della pipeline ci/CD, proteggeremo l'applicazione creando un backup completo dell'applicazione. Un backup applicativo-aware dell'applicazione in-production e dei relativi dati, stato e configurazione può essere utile per numerosi flussi di lavoro DevOps.



L'applicazione utilizzata per la convalida di questo caso di utilizzo è stata "**Magento**", Una soluzione di e-commerce con front-end basato su web; un'istanza di Elasticsearch per le funzionalità di ricerca e analisi; e un database MariaDB che tiene traccia di tutti i dettagli dell'inventario di acquisto e delle transazioni. Questa applicazione containerizzata è stata installata in un cluster Red Hat OpenShift. Ogni pod dell'applicazione utilizzava volumi persistenti per memorizzare i dati. I volumi persistenti sono stati creati automaticamente da NetApp Astra Trident, lo storage orchestrator per Kubernetes conforme a Container Storage Interface, che consente il provisioning dello storage sui sistemi storage NetApp. Inoltre, per utilizzare le funzionalità di protezione delle applicazioni di Astra Control Center, l'applicazione in questione è stata gestita da Astra Control, che è stata utilizzata per attivare i backup delle applicazioni che memorizzavano lo stato dell'applicazione insieme ai dati contenuti nei volumi persistenti. Abbiamo utilizzato "**SDK NetApp Astra Control Python**" Per automatizzare il processo di attivazione dei backup delle applicazioni, che è stato poi introdotto in una pipeline ci/CD. Questa pipeline è stata creata ed eseguita utilizzando un popolare tool ci/CD chiamato ["**Jenkins**"] per automatizzare il flusso di creazione, protezione e implementazione dell'applicazione.

Analizziamo i prerequisiti e la procedura per introdurre la protezione in una pipeline ci/CD.

#### Prerequisiti per la convalida del caso d'utilizzo

I seguenti strumenti o piattaforme sono stati implementati e configurati come prerequisiti:

1. Red Hat OpenShift Container Platform
2. NetApp Astra Trident installato su OpenShift con un sistema ONTAP di back-end configurato
3. Uno storageclass predefinito configurato, che punta a un backend NetApp ONTAP
4. NetApp Astra Control Center installato su un cluster OpenShift
5. Cluster OpenShift aggiunto come cluster gestito ad Astra Control Center
6. Jenkins è stato installato su un cluster OpenShift e configurato con un nodo Agent su cui è installato un motore Docker

#### Installazione dell'applicazione

Iniziamo con l'installazione iniziale dell'applicazione negli ambienti di staging e produzione. Ai fini di questo caso d'utilizzo, questo passaggio è un prerequisito, quindi viene eseguito manualmente. La pipeline ci/CD viene utilizzata per i flussi di lavoro di creazione e implementazione successivi come risultato delle nuove

versioni dell'applicazione.

L'ambiente di produzione in questo caso di utilizzo è uno spazio dei nomi chiamato `magento-prod` e il corrispondente ambiente di staging è uno spazio dei nomi chiamato `magento-staging` Configurato sul cluster Red Hat OpenShift. Per installare l'applicazione, attenersi alla seguente procedura:

1. Installare l'applicazione Magento utilizzando bitnami Helm Chart nell'ambiente di produzione. Utilizziamo RWX PVS per i pod Magento e MariaDB.

```
[netapp-user@rhel7 na_astra_control_suite]$ helm install --version 14
magento bitnami/magento -n magento-prod --create-namespace --set
image.tag=2.4.1-debian-10-
r11,magentoHost=10.63.172.243,persistence.magento.accessMode=ReadWriteMa
ny,persistence.apache.accessMode=ReadWriteMany,mariadb.master.persistenc
e.accessModes[0]=ReadWriteMany
```



Magento bitnami Helm Chart richiede un servizio LoadBalancer per esporre il servizio Magento GUI. Abbiamo utilizzato "[MetalLB](#)" per fornire un servizio di bilanciamento del carico on-premise in questo esempio.

2. Dopo alcuni minuti, verificare che tutti i pod e i servizi siano in esecuzione.

```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
NAME                                READY   STATUS
RESTARTS   AGE
magento-9d658fd96-qrxmt             1/1     Running
0         49m
magento-elasticsearch-coordinating-only-69869cc5-768rm 1/1     Running
0         49m
magento-elasticsearch-data-0        1/1     Running
0         49m
magento-elasticsearch-master-0      1/1     Running
0         49m
magento-mariadb-0                   1/1     Running
0         49m
```

3. Ripetere la stessa procedura per l'ambiente di staging.


### Gestire l'applicazione Magento in Astra Control Center

1. Accedere ad applicazioni e selezionare la scheda applicazioni rilevate.
2. Fare clic sui puntini di sospensione dell'applicazione Magento nell'ambiente di produzione (`magento-prod`), quindi fare clic su Manage (Gestisci).
3. L'applicazione Magento è ora gestita da Astra Control Center. Tutte le operazioni supportate da Astra Control possono essere eseguite sull'applicazione. Prendere nota anche della versione dell'applicazione.

App status

 Healthy

App protection status

 Partially Protected

Images

docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
docker.io/bitnami/magento:2.4.1-debian-10-r11  
docker.io/bitnami/mariadb:10.3.23-debian-10-r38

Protection schedule

Disabled

Group

 magento-prod

Cluster

 ocp-vmw

4. Ripetere i passaggi per la gestione dell'applicazione Magento nell'ambiente di staging (magento-staging).

### Pipeline ci/CD con protezione integrata

Quando lavoriamo con le nuove versioni delle applicazioni, utilizziamo una pipeline ci/CD per creare l'immagine container, eseguire backup degli ambienti di staging e produzione, implementare la nuova versione dell'applicazione nell'ambiente di staging, attendere l'approvazione per la promozione in produzione, quindi, implementare la nuova versione dell'applicazione nell'ambiente di produzione. Per utilizzare una pipeline ci/CD, attenersi alla seguente procedura:

1. Accedi a Jenkins e crea le credenziali richieste: Una per Magento creds, una per MariaDB admin creds e la terza per MariaDB root creds.
2. Accedere a Manage Jenkins > Manage Credentials (Gestisci Jenkins > Gestisci credenziali) e fare clic sul dominio appropriato.
3. Fare clic su Add Credentials (Aggiungi credenziali) e impostare il tipo su Username (Nome utente) con password e ambito impostati su Global (Globale). Immettere il nome utente, la password e un ID per le credenziali, quindi fare clic su OK.

Dashboard > Credentials > System > Global credentials (unrestricted) >

Back to credential domains
Add Credentials

Kind
Username with password
Scope
Global (Jenkins, nodes, items, all child items, etc)
Username
admin
☐ Treat username as secret
Password
ID
magento-cred
Description
OK

4. Ripetere la stessa procedura per le altre due credenziali.
5. Tornare alla dashboard, creare una pipeline facendo clic su New Item (nuovo elemento), quindi fare clic su Pipeline (pipeline).
6. Copiare la pipeline dal file Jenkinsfile "qui".



- Incollare la pipeline nella sezione della pipeline Jenkins, quindi fare clic su Save (Salva).
- Compilare i parametri della pipeline Jenkins con i relativi dettagli, tra cui la versione del grafico Helm, la versione dell'applicazione Magento a cui si desidera eseguire l'aggiornamento, la versione del toolkit Astra, l'FQDN di Astra Control Center, il token API e il relativo ID istanza. Specificare il registro del docker, lo spazio dei nomi e l'IP Magento degli ambienti di produzione e di staging e specificare anche gli ID delle credenziali create.

```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
PROD_NAMESPACE = 'magento-prod'
PROD_MAGENTO_IP = 'x.x.x.x'
STAGING_NAMESPACE = 'magento-staging'
STAGING_MAGENTO_IP = 'x.x.x.x'
MAGENTO_CREDS = credentials('magento-cred')
MAGENTO_MARIADB_CREDS = credentials('magento-mariadb-cred')
MAGENTO_MARIADB_ROOT_CREDS = credentials('magento-mariadb-root-cred')
```

- Fare clic su Crea ora. La pipeline inizia a essere eseguita e procede attraverso le fasi. L'immagine dell'applicazione viene creata e caricata nel registro del container.

| Build & Publish Segment | Build Docker Image | Publish Image to Registry | Protect & Deploy Segment | Install & Configure Pre-requisites | Download & Configure Astra Toolkit | Backup Tasks | Backup of Staging Env | Backup of Production Env | Deploy to Staging environment [Minor/Patch] | Deploy to Staging environment [Major] | Promote to Production? | Deploy to Production environment [Minor/Patch] | Deploy to Production environment [Major] | Delete temporary files |
|-------------------------|--------------------|---------------------------|--------------------------|------------------------------------|------------------------------------|--------------|-----------------------|--------------------------|---|---------------------------------------|------------------------|--|--|------------------------|
| 4s                      | 24s                | 5s                        | 213ms                    | 40s                                | 2s                                 | 290ms        | 1min 38s              | 1min 2s                  | 6min 29s                                    | 229ms                                 | 361ms                  | 2min 57s                                       | 200ms                                    | 850ms                  |
| 3s                      |                    |                           |                          |                                    |                                    |              |                       |                          |   |                                       |                        |  |  |                        |
| 18min 29s               |                    |                           |                          |                                    |                                    |              |                       |                          |   |                                       |                        |  |  |                        |

- I backup dell'applicazione vengono avviati tramite Astra Control.


**magento-prod**
Available

 App status  
Healthy

 App protection status  
Partially Protected

**Images**  
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
 docker.io/bitnami/magento:2.4.1-debian-10-r11  
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38

**Protection schedule**  
 Disabled

**Group**  
 magento-prod

**Cluster**  
 ocp-vmw

Overview

Data protection

Storage

Resources

Activity

Actions

Configure protection policy

Search

1-8 of 8 entries

| <input type="checkbox"/> | Name                             | Ready   | On-Schedule/On-Demand | Created ↑            | Actions   |
|--------------------------|----------------------------------|---|-----------------------|----------------------|---|
| <input type="checkbox"/> | upgrade-prod-2-4-1-debian-10-r20 |  | On-Demand             | 2021/10/29 14:43 UTC | Running  |

11. Una volta completate le fasi di backup, verificare i backup da Astra Control Center.


**magento-prod**
Available

 App status  
Healthy

 App protection status  
Partially Protected

**Images**  
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16  
 docker.io/bitnami/magento:2.4.1-debian-10-r11  
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38

**Protection schedule**  
 Disabled

**Group**  
 magento-prod

**Cluster**  
 ocp-vmw

Overview

Data protection

Storage

Resources

Activity

Actions

Configure protection policy

Search

1-8 of 8 entries

| <input type="checkbox"/> | Name                             | Ready   | On-Schedule/On-Demand | Created ↑            | Actions                          |
|--------------------------|----------------------------------|---|-----------------------|----------------------|----------------------------------|
| <input type="checkbox"/> | upgrade-prod-2-4-1-debian-10-r20 |  | On-Demand             | 2021/10/29 14:43 UTC | Available <span>Available</span> |

12. La nuova versione dell'applicazione viene quindi distribuita nell'ambiente di staging.



| Build & Publish Segment | Build Docker Image | Publish Image to Registry | Protect & Deploy Segment | Install & Configure Pre-requisites | Download & Configure Astra Toolkit | Backup Tasks | Backup of Staging Env | Backup of Production Env | Deploy to Staging environment [Minor/Patch] | Deploy to Staging environment [Major] | Promote to Production? | Deploy to Production environment [Minor/Patch] | Deploy to Production environment [Major] | Delete temporary files |
|-------------------------|--------------------|---------------------------|--------------------------|------------------------------------|------------------------------------|--------------|-----------------------|--------------------------|---|---------------------------------------|------------------------|--|--|------------------------|
| 4s                      | 47s                | 7s                        | 238ms                    | 1min 25s                           | 2s                                 | 273ms        | 1min 53s              | 1min 18s                 | 5min 20s                                    | 211ms                                 | 337ms                  | 2min 39s                                       | 187ms                                    | 780ms                  |
| 3s                      | 4min 16s           | 30s                       | 485ms                    | 7s                                 | 3s                                 | 153ms        | 6min 9s               | 5min 9s                  |   |                                       |                        |  |  |                        |

13. Al termine di questa fase, il programma attende che l'utente approvi la distribuzione in produzione. In questa fase, supponiamo che il team di QA esegua alcuni test manuali e approvi la produzione. Fare clic su Approve (approva) per distribuire la nuova versione dell'applicazione nell'ambiente di produzione.

| Deploy to Staging environment [Minor/Patch] | Deploy to Staging environment [Major] | Promote to Production? | Deploy to Production environment [Minor/Patch] | Deploy to Production environment [Major] | Delete temporary files |
|---|---------------------------------------|------------------------|--|--|------------------------|
| 3s  | 249ms                                 | 221ms                  | 159ms  | 178ms                                    | 210ms                  |

**Approval for promotion to Production?**

Proceed Abort

(paused for 1min 30s)

14. Verificare che anche l'applicazione di produzione sia aggiornata alla versione desiderata.

Available

App status
 

Healthy

App protection status
 

Partially Protected

**Images**

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
 docker.io/bitnami/mariadb:10.3.24-debian-10-r49  
 docker.io/niksleo415/magento:2.4.1-debian-10-r14

**Protection schedule**  
 Disabled

**Group**  
 magento-prod

**Cluster**  
 ocp-vmw

Come parte della pipeline ci/CD, abbiamo dimostrato la capacità di proteggere l'applicazione creando un backup completo e integrato con l'applicazione. Poiché il backup dell'intera applicazione è stato eseguito nell'ambito della pipeline di promozione-produzione, puoi sentirti più sicuro delle implementazioni altamente automatizzate delle applicazioni. Questo backup integrato con l'applicazione contenente i dati, lo stato e la configurazione dell'applicazione può essere utile per numerosi flussi di lavoro DevOps. Un importante flusso di lavoro potrebbe essere il ripristino della versione precedente dell'applicazione in caso di problemi imprevisti.

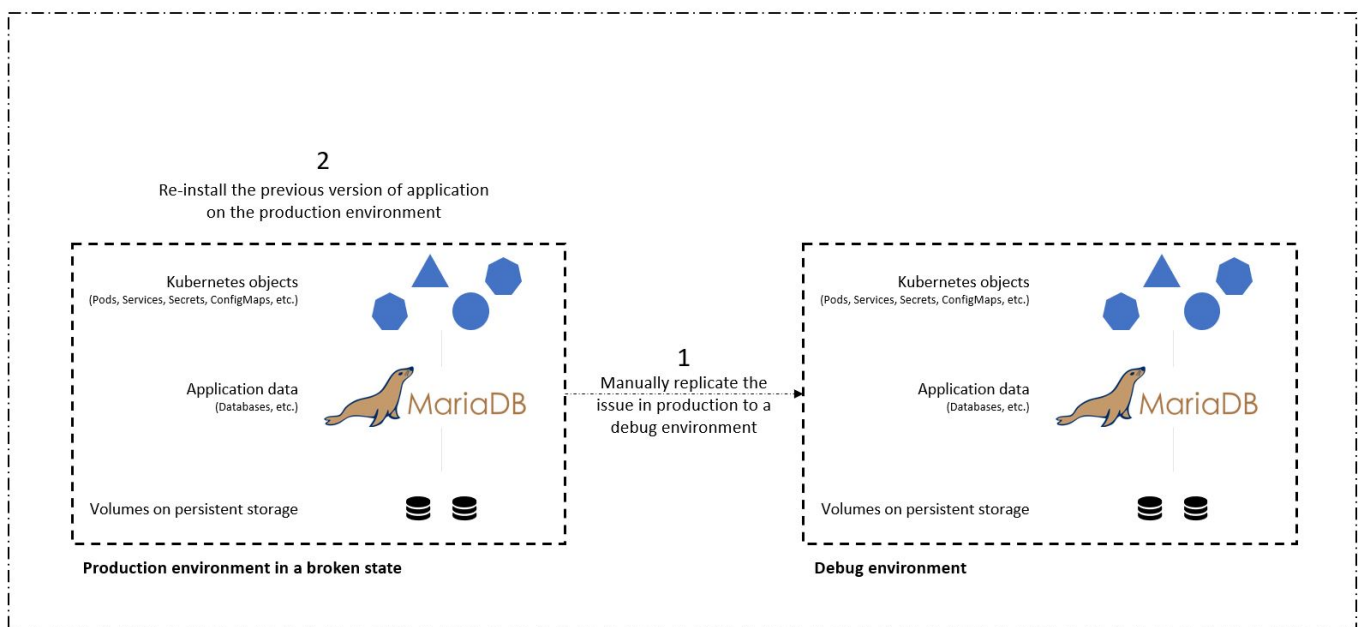
Anche se abbiamo dimostrato un workflow ci/CD attraverso lo strumento Jenkins, il concetto può essere estrapolato in modo semplice ed efficiente a diversi strumenti e strategie. Per vedere questo caso d'utilizzo in azione, guarda il video ["qui"](#).

## Utilizza Astra Control per facilitare l'analisi post-mortem e ripristinare l'applicazione

### Panoramica

In ["primo caso di utilizzo"](#), Abbiamo dimostrato come utilizzare NetApp Astra Control Center per proteggere le tue applicazioni in Kubernetes. In questa sezione viene descritto come integrare i backup delle applicazioni tramite Astra Control direttamente nel flusso di lavoro di sviluppo utilizzando l'SDK Python del toolkit NetApp Astra. Questo approccio consente la protezione degli ambienti di sviluppo e produzione automatizzando i backup on-demand durante il processo di integrazione continua e implementazione continua (ci/CD). Con questo ulteriore livello di protezione dei dati coerente con le applicazioni aggiunto alla pipeline ci/CD e alle applicazioni di produzione, i processi di sviluppo sono sicuri se qualcosa va storto nel processo, il che promuove buone pratiche di business-continuity.

In un workflow tradizionale, dopo aver riscontrato un errore quando l'applicazione viene aggiornata a una nuova versione, il team di sviluppo tentava di risolvere il problema in tempo reale in base ai report di bug forniti dai clienti. In alternativa, al primo segnale di problemi, il team potrebbe tentare di ridistribuire l'applicazione in un ambiente di debug parallelo per portare il processo offline. Potevano ridistribuire una base di codice precedente da una versione precedente in produzione, ripristinando l'applicazione in ordine di lavoro.



Anche se questo approccio funziona, il team dovrebbe assicurarsi che lo stato dell'applicazione di produzione guasta corrisponda a quello della versione vista in produzione quando si sono verificati i problemi. Inoltre, dovrebbero dedicare del tempo alla promozione della build sicuramente funzionante in produzione, recuperando il codice dal repository e ridistribuendo le immagini della macchina per ripristinare l'applicazione a un buon stato di esecuzione. Inoltre, in questo scenario, non abbiamo considerato se il database di produzione stesso fosse corrotto dal codice difettoso. Idealmente, esistono processi di backup separati per i dati del database, ma dobbiamo presumere che siano coerenti con lo stato dell'applicazione così come è stata pubblicata? È qui che i benefici di backup, ripristini e cloni stateful e coerenti con l'applicazione con Astra Control dimostrano davvero il loro valore.

Innanzitutto, possiamo utilizzare Astra Control per facilitare l'analisi post-mortem sullo stato dell'applicazione. Per farlo, cloniamo la versione di produzione buggy in un ambiente di test parallelo in modo coerente con

l'applicazione. La messa da parte di questo ambiente nello stato di bug-ridden ci consente di risolvere il problema in tempo reale.

Inoltre, Astra Control supporta la funzionalità di ripristino in-place che consente di ripristinare l'applicazione di produzione a un ultimo backup accettabile (che ha preceduto la versione del codice interessata). La versione ripristinata assume la posizione dell'applicazione di produzione precedente, in modo coerente e stateful con l'applicazione, incluso l'IP di ingresso precedentemente assegnato. Di conseguenza, i clienti che accedono al front-end non sarebbero a conoscenza della transizione alla versione di backup.



### Prerequisiti per la convalida del caso d'utilizzo

I seguenti strumenti o piattaforme sono stati implementati e configurati come prerequisiti:

- Red Hat OpenShift Container Platform.
- NetApp Astra Trident installato su OpenShift con un backend configurato su un sistema NetApp ONTAP.
- Uno storageclass predefinito configurato, che punta a un backend NetApp ONTAP.
- NetApp Astra Control Center installato su un cluster OpenShift.
- Cluster OpenShift aggiunto come cluster gestito ad Astra Control Center.
- Jenkins installato su un cluster OpenShift.
- Applicazione Magento installata nell'ambiente di produzione. In questo caso di utilizzo, l'ambiente di produzione è uno spazio dei nomi chiamato "lento-prod" in un cluster Red Hat OpenShift.
- Applicazione di produzione gestita da Astra Control Center.
- Backup sicuramente funzionanti dell'applicazione di produzione acquisita con Astra Control.

### Clonare e ripristinare la pipeline

Considerando che l'applicazione è stata aggiornata a una nuova versione, l'applicazione nell'ambiente di produzione (`magento-prod`) non si comporta come previsto dopo l'aggiornamento. Supponiamo che i dati restituiti dalle query front-end non corrispondano alla richiesta o che il database sia stato effettivamente danneggiato. Per clonare e ripristinare la pipeline, attenersi alla seguente procedura:



## This site can't be reached

10.63.172.243 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR\_CONNECTION\_TIMED\_OUT

Reload

Details

1. Accedere a Jenkins e creare una pipeline facendo clic su New Item (nuovo elemento), quindi su Pipeline (pipeline).
2. Copiare la pipeline dal file Jenkinsfile "qui".
3. Incollare la pipeline nella sezione della pipeline Jenkins, quindi fare clic su Save (Salva).
4. Compilare i parametri della pipeline Jenkins con i relativi dettagli, come la versione corrente dell'applicazione Magento in produzione, l'FQDN di Astra Control Center, il token API, l'ID dell'istanza e il nome dell'applicazione o lo spazio dei nomi degli ambienti di produzione e debug, nonché i nomi dei cluster di origine e destinazione. Ai fini di questo caso d'utilizzo, l'ambiente di produzione è uno spazio dei nomi chiamato 'lento-prod' e l'ambiente di debug è uno spazio dei nomi chiamato 'lento-debug' configurato su un cluster Red Hat OpenShift.

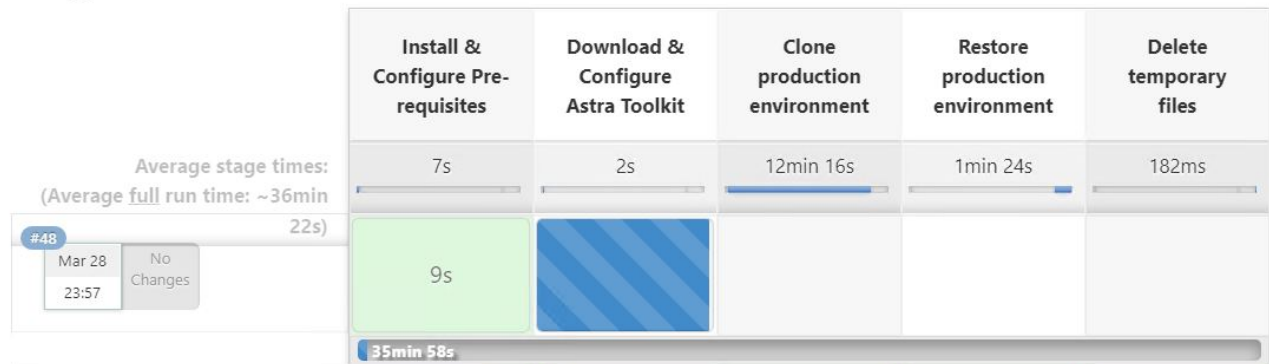
```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
PROD_APP_NAME = 'magento-prod'
DEBUG_APP_NAME = 'magento-debug'
DEBUG_NAMESPACE = 'magento-debug'
PROD_KUBERNETES_CLUSTER = 'ocp-vmw'
DEBUG_KUBERNETES_CLUSTER = 'ocp-vmw'
```

5. Fare clic su Crea ora. La pipeline inizia a essere eseguita e procede attraverso le fasi. L'applicazione viene prima clonata nello stato corrente in un ambiente di debug e quindi ripristinata al backup funzionante.

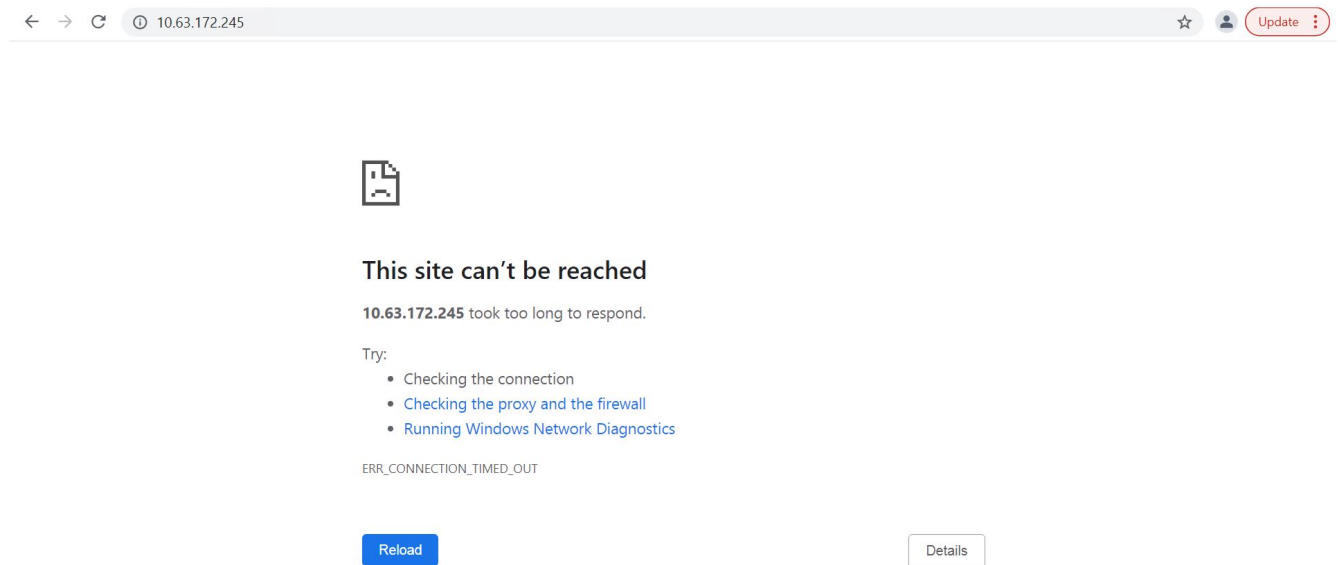
# Pipeline magento\_clone-for-triage\_restore-from-backup



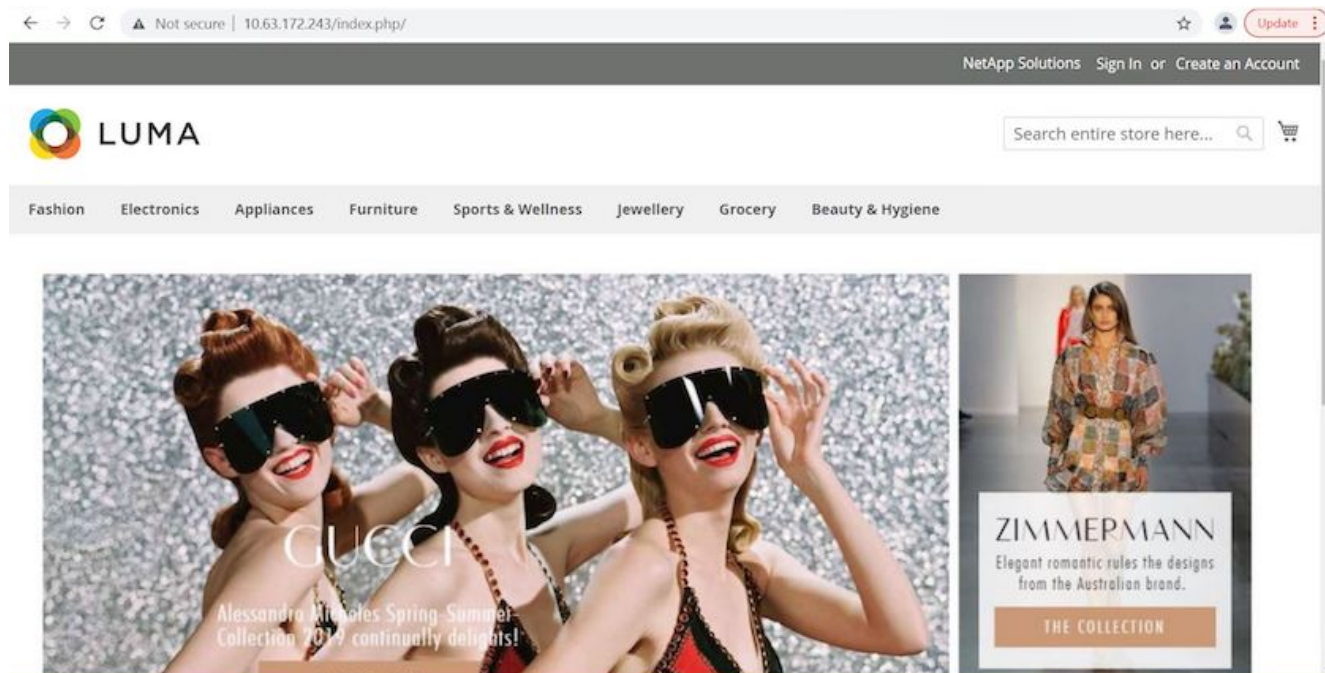
## Stage View



6. Verificare che l'applicazione clonata sia la versione contenente bug.



7. Verificare che l'ambiente di produzione sia ripristinato a un backup funzionante e che l'applicazione in produzione funzioni come previsto.



Queste due operazioni in tandem accelerano il ritorno alle normali operazioni di business. Per vedere questo caso d'utilizzo in azione, guarda il video "[qui](#)".

## Accelerazione dello sviluppo software con la tecnologia FlexClone di NetApp

### Panoramica

La clonazione di un'applicazione distribuita in un cluster Kubernetes è uno strumento molto utile per gli sviluppatori che desiderano accelerare i propri flussi di lavoro condividendo ambienti con i partner o testando nuove versioni di codice in un ambiente di sviluppo senza interferire con la versione su cui stanno attualmente lavorando. La clonazione stateful e coerente con l'applicazione di un'applicazione Kubernetes è una delle funzionalità principali incluse in NetApp Astra Control, insieme al backup e ripristino delle applicazioni. Come bonus, se un'applicazione viene clonata all'interno dello stesso cluster Kubernetes utilizzando lo stesso backend di storage, Astra Control utilizza per impostazione predefinita la tecnologia NetApp FlexClone per la duplicazione di volumi di dati persistenti, accelerando notevolmente il processo. Accelerando questo processo, l'ambiente clonato viene fornito e disponibile per l'utilizzo in pochi istanti, consentendo agli sviluppatori di riprendere il proprio lavoro con una breve pausa rispetto alla ridistribuzione dell'ambiente di test o sviluppo. Come ulteriore comodità, tutte le funzioni disponibili in NetApp Astra Control possono essere chiamate con un'API, che consente una facile integrazione in framework di automazione come Ansible. Pertanto, gli ambienti possono essere gestiti in tempi ancora più rapidi, perché sono necessarie solo modifiche di lieve entità in un manuale o in un ruolo per iniziare la procedura di cloning.

### Che cos'è la tecnologia FlexClone di NetApp?

La tecnologia NetApp FlexClone è una copia scrivibile e point-in-time basata su snapshot di un NetApp FlexVol. Vengono forniti quasi istantaneamente, contengono tutti i dati del volume di origine e non consumano spazio di storage aggiuntivo fino a quando i dati nel nuovo volume non iniziano a divergere dall'origine. Vengono spesso utilizzati in ambienti basati su modelli o di sviluppo quando più copie di dati sono utili per scopi di staging e i sistemi storage dispongono di risorse limitate per il provisioning di questi volumi. Rispetto a un sistema storage tradizionale in cui i dati devono essere copiati più volte, con un conseguente consumo di tempo e spazio di storage significativo, la tecnologia NetApp FlexClone accelera le attività dipendenti dallo storage.



## Traditional Data Copies



Traditional physical copies take additional time and consume additional storage space

## NetApp FlexClone Copies



NetApp FlexClone copies are near instantaneous and only consume space when written to

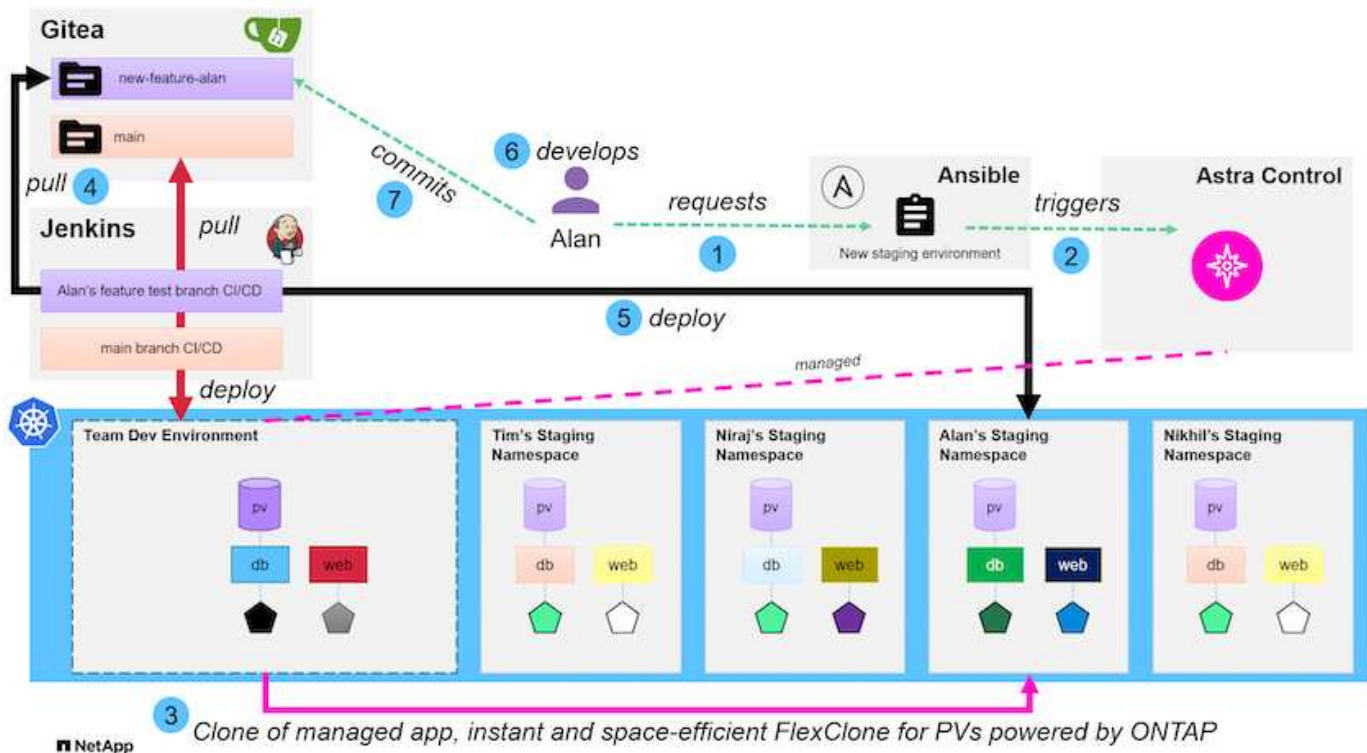
Per ulteriori informazioni sulla tecnologia FlexClone di NetApp, visita la pagina all'indirizzo "[Documenti NetApp](#)".

### Prerequisiti

1. Una distribuzione Kubernetes supportata, come Red Hat OpenShift 4.6.8+, Rancher 2.5+ o Kubernetes 1.19+.
2. NetApp Astra Control Center 21.12+.
3. Un sistema NetApp ONTAP con un backend di storage configurato tramite NetApp Astra Trident.
4. Ansible 2.9+.
5. Modelli per gli ambienti che si desidera clonare come applicazioni gestite in NetApp Astra Control.

### Introduzione al caso d'utilizzo

In questo caso di utilizzo, viene visualizzato un aspetto simile al seguente flusso di lavoro:



1. Un utente esegue il playbook ansible per creare un nuovo ambiente di staging.
2. Ansible utilizza il modulo URI-API per richiamare Astra Control per eseguire l'operazione di cloning.
3. Astra Control esegue un'operazione di cloning su un ambiente modello con provisioning anticipato, creando così una nuova applicazione gestita.



Questo ambiente può essere una singola applicazione standalone in fase di sviluppo o un intero ambiente di sviluppo come una pipeline Jenkins ci/CD.

4. L'utente quindi estrae una versione del proprio codice nell'ambiente di sviluppo clonato da un repository online come Gitea.
5. La nuova versione dell'applicazione viene implementata e gestita da NetApp Astra Control.

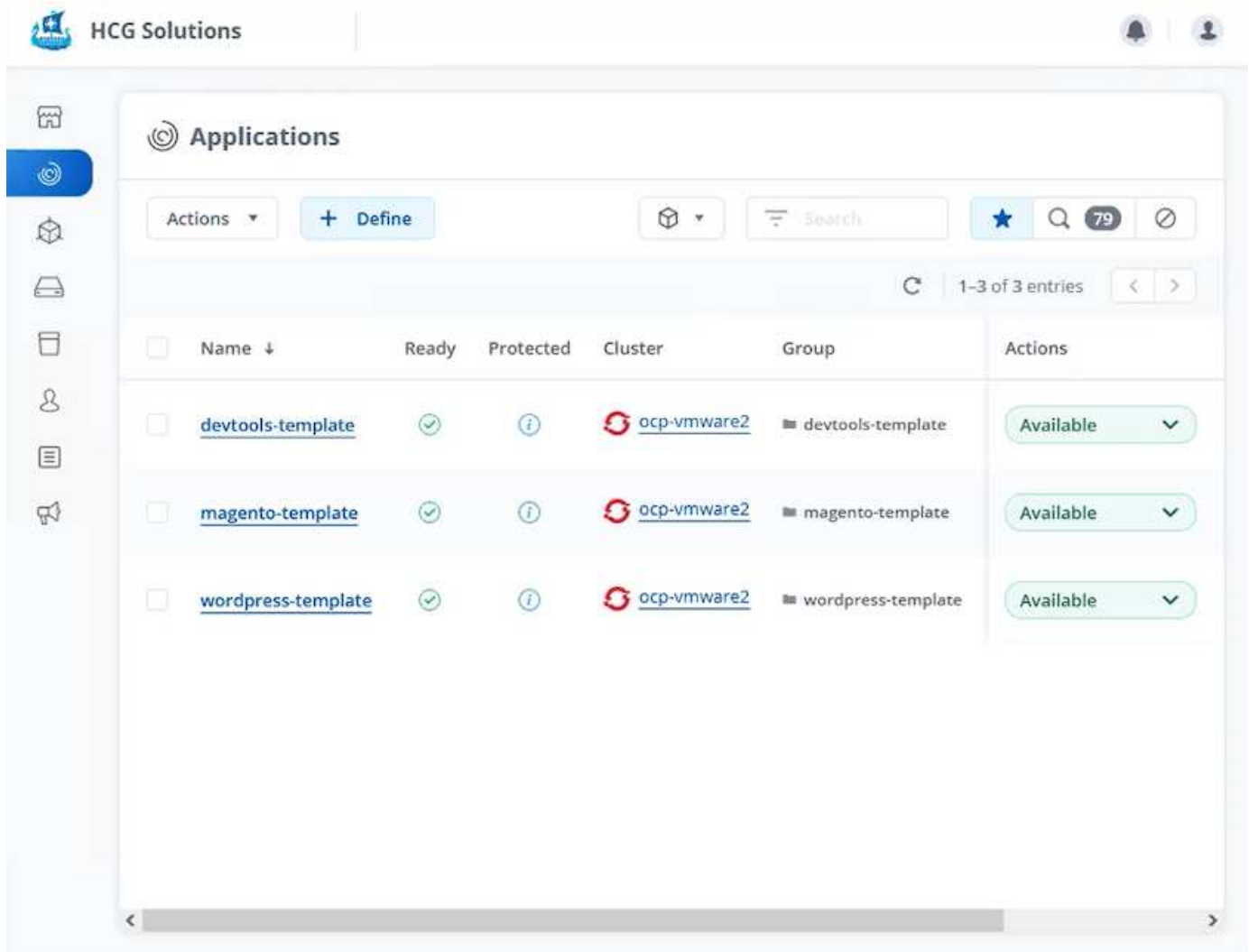


Entrambi questi processi possono essere automatizzati.

6. L'utente può sviluppare nuovo codice in questo ambiente clonato.
7. Quando l'utente è soddisfatto dei propri sforzi di sviluppo, può reinviare il codice al repository ospitato.

Il caso d'utilizzo qui presentato dipende dall'esistenza di modelli Golden per gli ambienti o le applicazioni che si desidera clonare. Nel nostro ambiente abbiamo creato tre modelli di questo tipo, uno per un'implementazione di WordPress, uno per un'implementazione di Magento e uno per un ambiente ci/CD di Jenkins con Gitea che abbiamo chiamato DevTools.





Ciascuno di questi ambienti è gestito da NetApp Astra Control, con volumi persistenti attualmente memorizzati su un sistema di storage NetApp ONTAP con un backend NFS fornito da NetApp Astra Trident.

#### Validazione del caso d'utilizzo

1. Clonare il toolkit ansible fornito dal team NetApp Solutions Engineering, che include il ruolo di cloning e il manuale di aggiornamento dell'applicazione.

```
[netapp-user@rhel7 ~]$ git clone https://github.com/NetApp-Automation/na_astra_control_suite.git
[netapp-user@rhel7 ~]$ cd na_astra_control_suite
```

2. Modifica `vars/clone_vars.yml` E compila i valori globali che si adattano al tuo ambiente Astra Control.

```
astra_control_fqdn: astra-control-center.example.com
astra_control_account_id: "xxxx-xxxx-xxxx-xxxx-xxxx"
astra_control_api_token: "xxxxx"
```



I valori dell'ambiente globale da compilare sono disponibili sotto l'icona del profilo utente in NetApp Astra Control nel menu API Access.



- Una volta completate le variabili globali, è possibile scegliere i valori per l'applicazione specifica che si desidera clonare. Per clonare l'ambiente devtools in un ambiente personale chiamato alan-devtools, eseguire le seguenti operazioni:

```
clone_details:
- clone_name: alan-devtools
  destination_namespace: alan-dev-namespace
  source_cluster_name: ocp-vmware2
  destination_cluster_name: ocp-vmware2
  source_application_name: devtools-template
```



Per sfruttare la tecnologia FlexClone di NetApp nel processo di cloning, src-cluster e dest-cluster deve essere lo stesso.

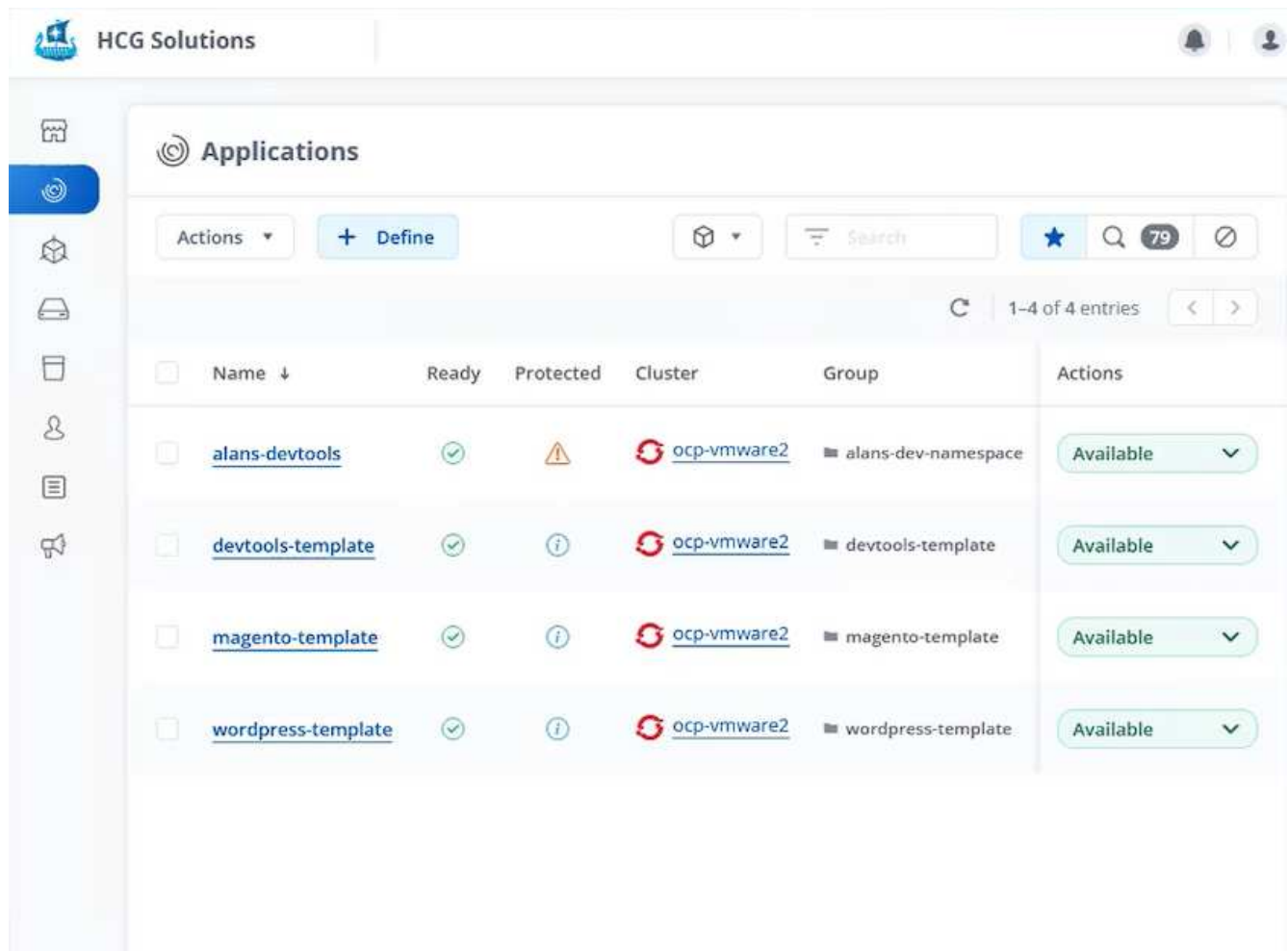
- È ora possibile eseguire il manuale per clonare l'applicazione.

```
[netapp-user@rhel7 na_astra_control_suite]$ ansible-playbook -K clone_app_playbook.yml]
```



Il playbook così come è stato scritto deve essere eseguito dall'utente root o da un utente che può eseguire l'escalation attraverso il processo sudo passando l'argomento "-K".

- Quando il playbook completa la sua esecuzione, l'applicazione clonata viene visualizzata come disponibile nella console di Astra Control Center.



- Un utente può quindi accedere all'ambiente Kubernetes in cui è stata implementata l'applicazione, verificare che l'applicazione sia esposta con un nuovo indirizzo IP e iniziare il lavoro di sviluppo.

Per una dimostrazione di questo caso di utilizzo e un esempio di aggiornamento di un'applicazione, vedere ["qui"](#).

## Video e demo: DevOps con NetApp Astra

I seguenti video mostrano alcune delle funzionalità descritte in questo documento:

[Data Protection in pipeline ci/CD con Astra Control Center](#)

[Sfrutta NetApp Astra Control per eseguire l'analisi post-mortem e ripristinare l'applicazione](#)

## Ulteriori informazioni: DevOps con NetApp Astra

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione NetApp

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Documentazione di Astra Trident

["https://docs.netapp.com/us-en/trident/"](https://docs.netapp.com/us-en/trident/)

- Documentazione di NetApp Astra Control Center

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Documentazione Ansible

["https://docs.ansible.com/"](https://docs.ansible.com/)

- Documentazione di Red Hat OpenShift

["https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.8/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/)

- Documentazione del rancher

["https://rancher.com/docs/"](https://rancher.com/docs/)

- Documentazione Kubernetes

["https://kubernetes.io/docs/home/"](https://kubernetes.io/docs/home/)

## NVA-1160: Red Hat OpenShift con NetApp

Alan Cowles e Nikhil M Kulkarni, NetApp

Questo documento di riferimento fornisce la convalida dell'implementazione della soluzione Red Hat OpenShift, implementata tramite l'infrastruttura IPI (Installer Provided Infrastructure) in diversi ambienti di data center come validati da NetApp. Inoltre, descrive in dettaglio l'integrazione dello storage con i sistemi di storage NetApp utilizzando Astra Trident Storage orchestrator per la gestione dello storage persistente. Infine, vengono analizzate e documentate una serie di validazioni delle soluzioni e casi di utilizzo reali.

### Casi di utilizzo

La soluzione Red Hat OpenShift con NetApp è progettata per offrire un valore eccezionale ai clienti con i seguenti casi di utilizzo:

- Facile da implementare e gestire Red Hat OpenShift implementato utilizzando IPI (Installer Provided Infrastructure) su bare metal, Red Hat OpenStack Platform, Red Hat Virtualization e VMware vSphere.
- Potenza combinata dei container aziendali e dei carichi di lavoro virtualizzati con Red Hat OpenShift

implementato virtualmente su OSP, RHV o vSphere o su bare metal con la virtualizzazione OpenShift.

- Configurazione e casi d'utilizzo reali che evidenziano le funzionalità di Red Hat OpenShift se utilizzato con lo storage NetApp e Astra Trident, l'orchestrator dello storage open source per Kubernetes.

## Valore di business

Le aziende stanno adottando sempre più pratiche DevOps per creare nuovi prodotti, abbreviare i cicli di rilascio e aggiungere rapidamente nuove funzionalità. A causa della loro natura innata e agile, i container e i microservizi svolgono un ruolo cruciale nel supporto delle pratiche DevOps. Tuttavia, la pratica di DevOps su scala di produzione in un ambiente aziendale presenta le proprie sfide e impone determinati requisiti all'infrastruttura sottostante, come ad esempio:

- Alta disponibilità a tutti i livelli dello stack
- Procedure di implementazione semplici
- Operazioni e aggiornamenti senza interruzioni
- Infrastruttura programmabile e basata su API per restare al passo con l'agilità dei microservizi
- Multi-tenancy con garanzie di performance
- Possibilità di eseguire contemporaneamente carichi di lavoro virtualizzati e containerizzati
- Possibilità di scalare l'infrastruttura in modo indipendente in base alle esigenze dei carichi di lavoro

Red Hat OpenShift con NetApp riconosce queste sfide e presenta una soluzione che aiuta a risolvere ogni problema implementando l'implementazione completamente automatizzata di RedHat OpenShift IPI nell'ambiente del data center scelto dal cliente.

## Panoramica della tecnologia

La soluzione Red Hat OpenShift con NetApp comprende i seguenti componenti principali:

### Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform è una piattaforma aziendale Kubernetes completamente supportata. Red Hat apporta diversi miglioramenti a Kubernetes open-source per offrire una piattaforma applicativa con tutti i componenti completamente integrati per la creazione, l'implementazione e la gestione delle applicazioni containerizzate.

Per ulteriori informazioni, visita il sito Web di OpenShift ["qui"](#).

### Sistemi storage NetApp

NetApp dispone di diversi sistemi storage perfetti per data center aziendali e implementazioni di cloud ibrido. Il portfolio NetApp include i sistemi storage NetApp ONTAP, NetApp Element e NetApp e-Series, tutti in grado di fornire storage persistente per le applicazioni containerizzate.

Per ulteriori informazioni, visitare il sito Web di NetApp ["qui"](#).

### Integrazioni di storage NetApp

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful, implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati NetApp.

Per ulteriori informazioni, visitare il sito Web di NetApp Astra ["qui"](#).

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, incluso Red Hat OpenShift.

Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

## Opzioni di configurazione avanzate

Questa sezione è dedicata alle personalizzazioni che gli utenti reali dovrebbero eseguire durante l'implementazione di questa soluzione in produzione, ad esempio la creazione di un registro di immagini private dedicato o l'implementazione di istanze personalizzate di bilanciamento del carico.

## Matrice di supporto corrente per le release validate

| Tecnologia                    | Scopo   | Versione del software |
|-------------------------------|---|-----------------------|
| NetApp ONTAP                  | Storage   | 9.8, 9.9.1            |
| NetApp Element                | Storage   | 12.3                  |
| NetApp Astra Control Center   | Gestione dei dati consapevole dell'applicazione | 21.12.60              |
| NetApp Astra Trident          | Orchestrazione dello storage                    | 22.01.0               |
| Red Hat OpenShift             | Orchestrazione di container                     | 4.6 EUS, 4.7, 4.8     |
| Piattaforma Red Hat OpenStack | Infrastruttura di cloud privato                 | 16.1                  |
| Virtualizzazione Red Hat      | Virtualizzazione del data center                | 4.4                   |
| VMware vSphere                | Virtualizzazione del data center                | 6.7U3                 |

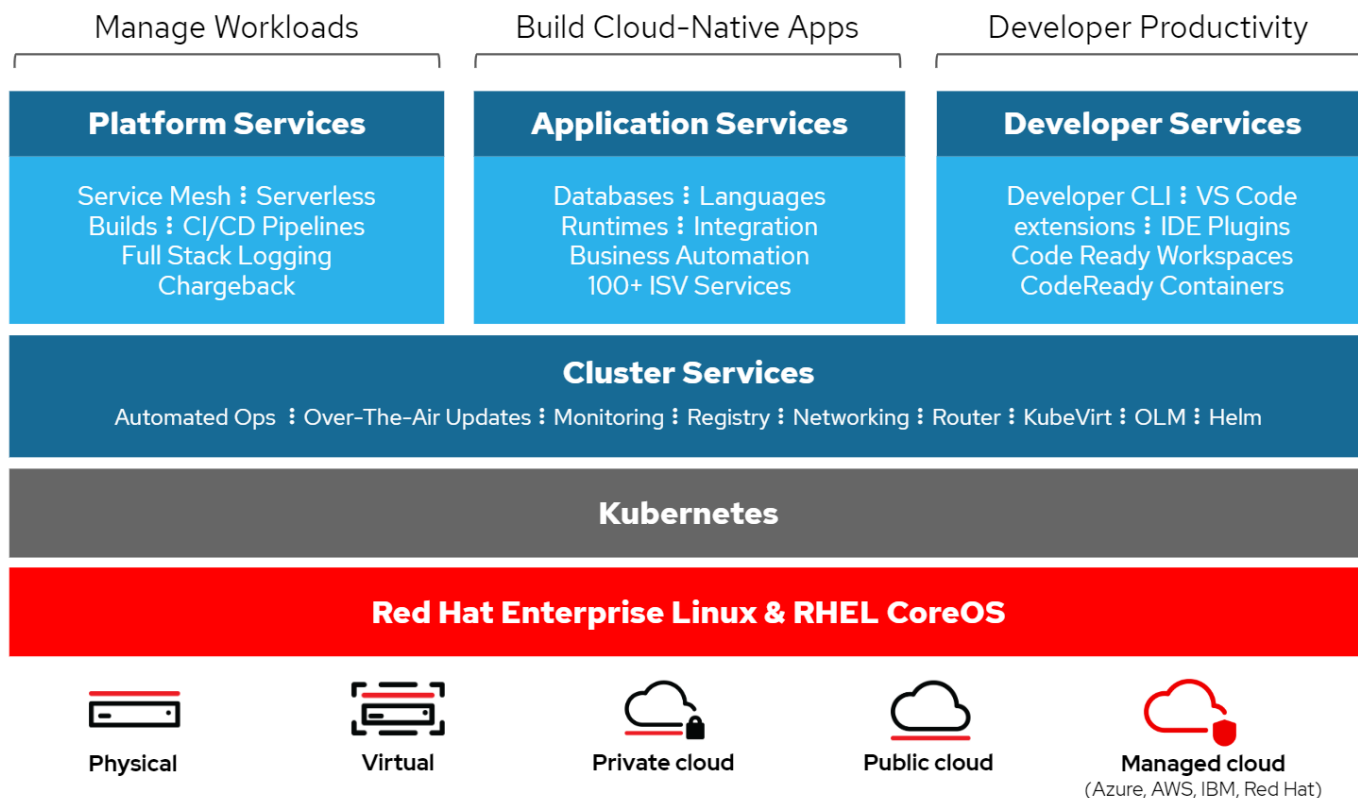
## Panoramica di OpenShift

Red Hat OpenShift Container Platform unisce le operazioni IT e di sviluppo su un'unica piattaforma per creare, implementare e gestire le applicazioni in modo coerente tra infrastrutture cloud ibride e on-premise. Red Hat OpenShift si basa su innovazioni open-source e standard di settore, tra cui Kubernetes e Red Hat Enterprise Linux CoreOS, la distribuzione Linux aziendale leader a livello mondiale progettata per carichi di lavoro basati su container. OpenShift fa parte del programma Cloud Native Computing Foundation (CNCF) Certified Kubernetes, che offre portabilità e interoperabilità dei carichi di lavoro dei container.

### Red Hat OpenShift offre le seguenti funzionalità:

- **Provisioning self-service** gli sviluppatori possono creare applicazioni su richiesta in modo rapido e semplice utilizzando gli strumenti più utilizzati, mentre le operazioni mantengono il pieno controllo sull'intero ambiente.
- **Storage persistente** grazie al supporto per lo storage persistente, OpenShift Container Platform consente di eseguire sia applicazioni stateful che applicazioni stateless native del cloud.
- **Integrazione continua e sviluppo continuo (ci/CD)** questa piattaforma di codice sorgente gestisce le immagini di build e distribuzione su larga scala.

- **Standard open-source** questi standard incorporano l'Open Container Initiative (OCI) e Kubernetes per l'orchestrazione dei container, oltre ad altre tecnologie open-source. Non ti limiterai alla tecnologia o alla roadmap di business di un vendor specifico.
- **Pipeline ci/CD** OpenShift fornisce un supporto immediato per le pipeline ci/CD, in modo che i team di sviluppo possano automatizzare ogni fase del processo di distribuzione dell'applicazione e assicurarsi che venga eseguito ad ogni modifica apportata al codice o alla configurazione dell'applicazione.
- **RBAC (Role-Based Access Control)** questa funzionalità fornisce il monitoraggio di team e utenti per aiutare a organizzare un gruppo di sviluppatori di grandi dimensioni.
- **Automated Build and Deploy** OpenShift offre agli sviluppatori la possibilità di creare le proprie applicazioni containerizzate o di far costruire i contenitori dal codice sorgente dell'applicazione o anche dai file binari. La piattaforma automatizza quindi l'implementazione di queste applicazioni nell'infrastruttura in base alle caratteristiche definite per le applicazioni. Ad esempio, la quantità di risorse da allocare e la posizione dell'infrastruttura da implementare per garantire la conformità con le licenze di terze parti.
- **Ambienti coerenti** OpenShift garantisce che l'ambiente fornito agli sviluppatori e per tutto il ciclo di vita dell'applicazione sia coerente dal sistema operativo alle librerie, alla versione runtime (ad esempio Java runtime), e persino il runtime dell'applicazione in uso (ad esempio, tomcat) per eliminare i rischi derivanti da ambienti incoerenti.
- **Gestione della configurazione** la configurazione e la gestione dei dati sensibili sono integrate nella piattaforma per garantire che all'applicazione venga fornita una configurazione di applicazione coerente e indipendente dall'ambiente, indipendentemente dalle tecnologie utilizzate per creare l'applicazione o dall'ambiente in cui si trova implementati.
- **Registri delle applicazioni e parametri metrici.** il feedback rapido è un aspetto importante dello sviluppo delle applicazioni. Il monitoraggio integrato e la gestione dei log di OpenShift forniscono agli sviluppatori metriche immediate per studiare il comportamento dell'applicazione tra le modifiche e per risolvere i problemi il prima possibile nel ciclo di vita dell'applicazione.
- **Catalogo sicurezza e container** OpenShift offre la multi-tenancy e protegge l'utente dall'esecuzione di codice dannoso utilizzando la sicurezza stabilita con Security-Enhanced Linux (SELinux), CGroups e Secure Computing Mode (seccomp) per isolare e proteggere i contenitori. Fornisce inoltre la crittografia tramite certificati TLS per i vari sottosistemi e l'accesso ai container certificati Red Hat ([access.redhat.com/containers](https://access.redhat.com/containers)) sottoposti a scansione e classificati con un'enfasi specifica sulla sicurezza per fornire container applicativi certificati, affidabili e sicuri agli utenti finali.



## Metodi di implementazione per Red Hat OpenShift

A partire da Red Hat OpenShift 4, i metodi di implementazione di OpenShift includono implementazioni manuali che utilizzano l'infrastruttura con provisioning utente (UPI) per implementazioni altamente personalizzate o implementazioni completamente automatizzate che utilizzano l'infrastruttura con provisioning dell'installatore (IPI).

Il metodo di installazione IPI è il metodo preferito nella maggior parte dei casi, perché consente la rapida implementazione dei cluster OpenShift per gli ambienti di sviluppo, test e produzione.

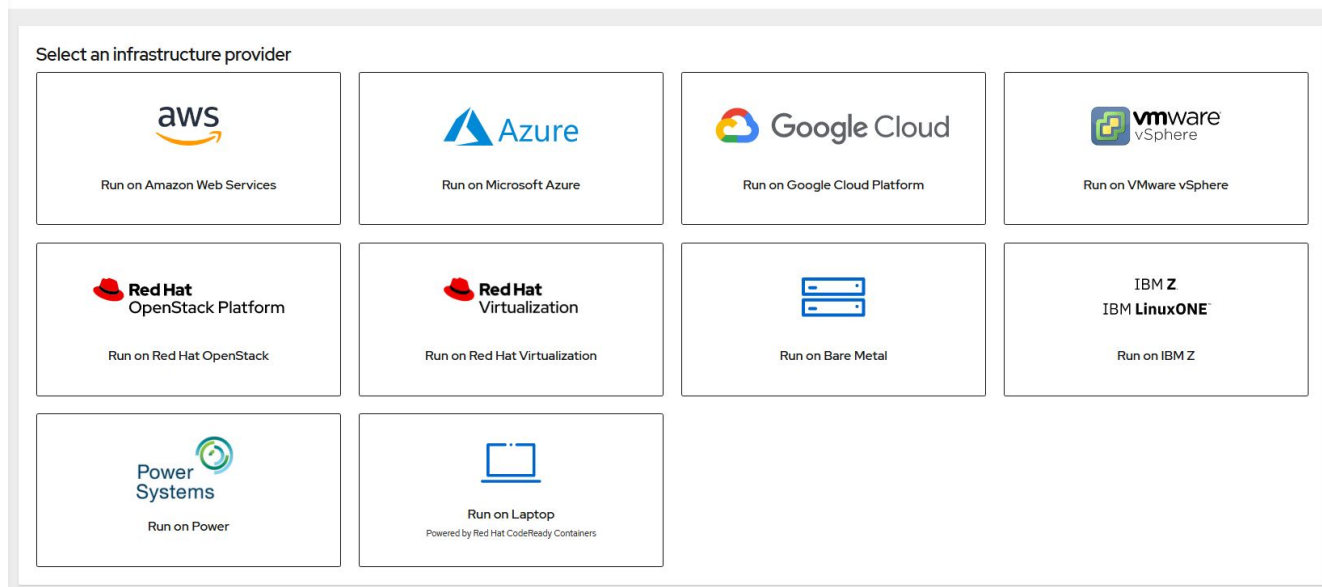
### Installazione IPI di Red Hat OpenShift

La distribuzione dell'infrastruttura IPI (Installer Provided Infrastructure) di OpenShift prevede questi passaggi di alto livello:

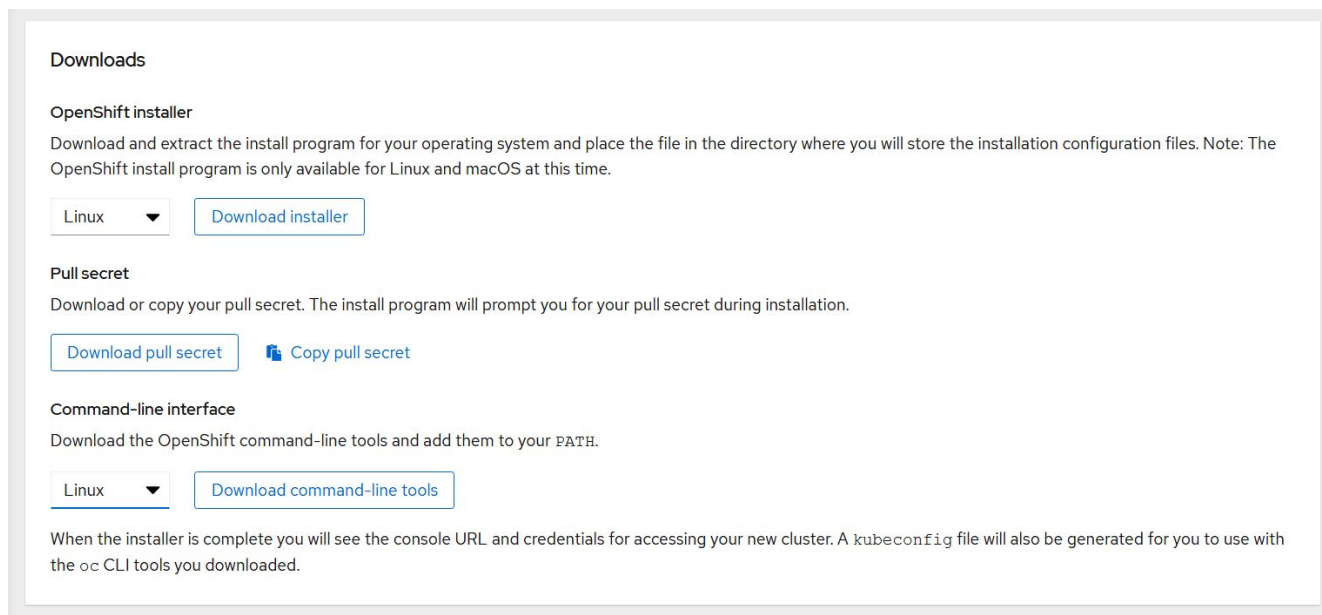
1. Visita Red Hat OpenShift "[sito web](#)" E accedi con le tue credenziali SSO.
2. Seleziona l'ambiente in cui desideri implementare Red Hat OpenShift.



## Install OpenShift Container Platform 4



3. Nella schermata successiva, scaricare il programma di installazione, l'esclusivo segreto pull e gli strumenti CLI per la gestione.



4. Seguire la ["istruzioni per l'installazione"](#) Fornito da Red Hat per l'implementazione nel vostro ambiente preferito.

#### Implementazioni OpenShift validate da NetApp

NetApp ha testato e validato l'implementazione di Red Hat OpenShift nei propri laboratori utilizzando il metodo di implementazione IPI (Installer Provided Infrastructure) in ciascuno dei seguenti ambienti di data center:

- ["OpenShift su bare metal"](#)
- ["OpenShift sulla piattaforma Red Hat OpenStack"](#)
- ["OpenShift sulla virtualizzazione Red Hat"](#)

- ["OpenShift su VMware vSphere"](#)

## OpenShift su bare metal

OpenShift su bare metal offre un'implementazione automatica della piattaforma container OpenShift sui server commodity.

OpenShift su bare metal è simile alle implementazioni virtuali di OpenShift, che offrono facilità di implementazione, provisioning rapido e scalabilità dei cluster OpenShift, supportando al contempo i carichi di lavoro virtualizzati per le applicazioni non pronte per essere containerizzate. L'implementazione su bare metal non richiede l'overhead aggiuntivo necessario per gestire l'ambiente dell'hypervisor host oltre all'ambiente OpenShift. Implementando direttamente sui server bare metal, è possibile ridurre anche i limiti di overhead fisico dovuti alla condivisione delle risorse tra l'host e l'ambiente OpenShift.

**OpenShift su bare metal offre le seguenti funzionalità:**

- **Implementazione IPI o assistita** con un cluster OpenShift distribuito da IPI (Installer Provisioning Infrastructure) su server bare metal, i clienti possono implementare un ambiente OpenShift altamente versatile e facilmente scalabile direttamente su commodity server, senza la necessità di gestire un livello di hypervisor.
- **Compact cluster design** per ridurre al minimo i requisiti hardware, OpenShift su bare metal consente agli utenti di implementare cluster di soli 3 nodi, consentendo ai nodi del piano di controllo OpenShift di agire anche come nodi di lavoro e contenitori host.
- **Virtualizzazione OpenShift** OpenShift può eseguire macchine virtuali all'interno dei container utilizzando OpenShift Virtualization. Questa virtualizzazione nativa per container esegue l'hypervisor KVM all'interno di un container e collega volumi persistenti per lo storage delle macchine virtuali.
- **Infrastruttura ottimizzata per ai/ML** implementate applicazioni come Kubeflow per applicazioni di apprendimento automatico incorporando nodi di lavoro basati su GPU nel vostro ambiente OpenShift e sfruttando OpenShift Advanced Scheduling.

## Progettazione di rete

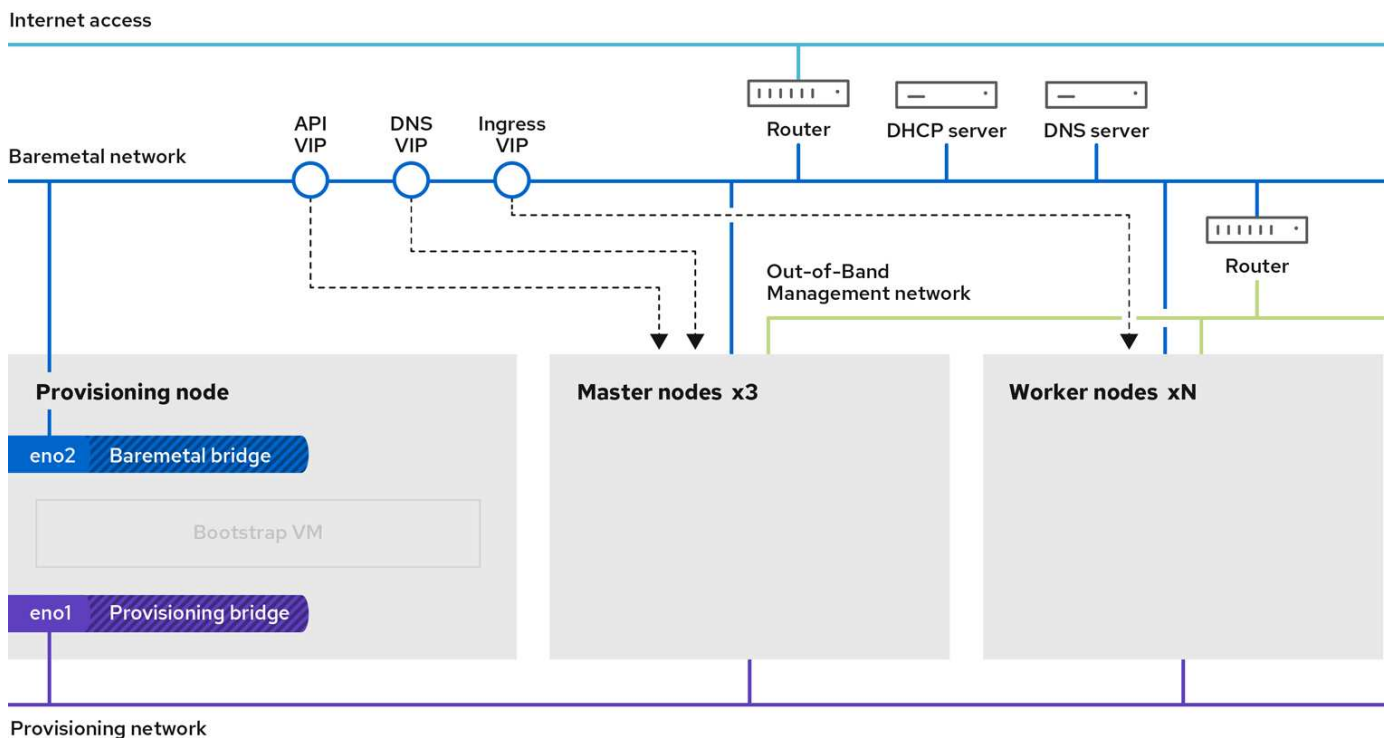
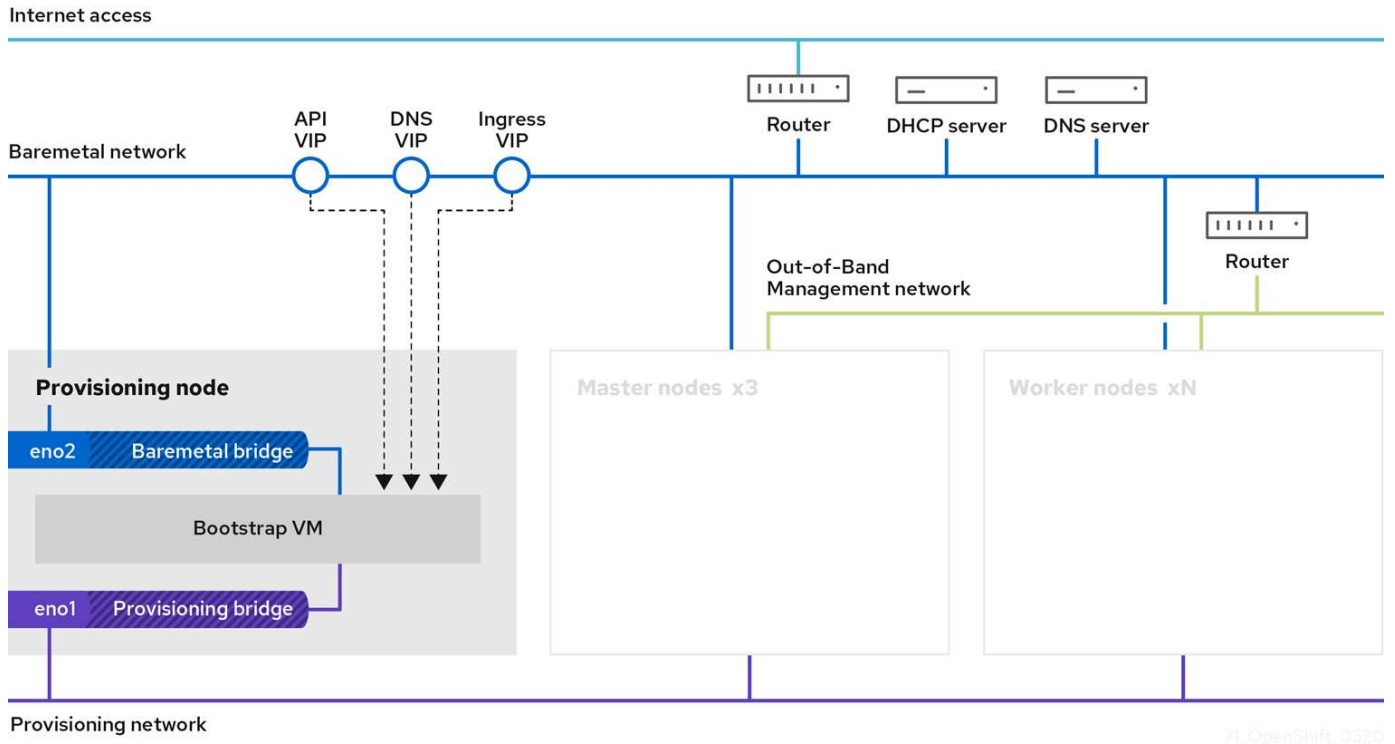
La soluzione Red Hat OpenShift su NetApp utilizza due switch dati per fornire connettività dati primaria a 25 Gbps. Utilizza inoltre due switch di gestione che forniscono connettività a 1 Gbps per la gestione in-band dei nodi di storage e gestione out-of-band per la funzionalità IPMI.

Per l'implementazione di OpenShift Bare-Metal IPI, è necessario creare un nodo di provisioning, una macchina Red Hat Enterprise Linux 8 che deve avere interfacce di rete collegate a reti separate.

- **Provisioning network** questa rete viene utilizzata per avviare i nodi bare-metal e installare le immagini e i pacchetti necessari per distribuire il cluster OpenShift.
- **Rete bare-metal** questa rete viene utilizzata per la comunicazione pubblica del cluster dopo la sua distribuzione.

Per la configurazione del nodo di provisioning, il cliente crea interfacce di bridge che consentono al traffico di instradare correttamente sul nodo stesso e sulla macchina virtuale Bootstrap fornita a scopo di implementazione. Una volta implementato il cluster, l'API e gli indirizzi VIP di ingresso vengono migrati dal nodo di boot strap al cluster appena implementato.

Le immagini seguenti illustrano l'ambiente sia durante l'implementazione IPI che al termine dell'implementazione.



## Requisiti VLAN

La soluzione Red Hat OpenShift con NetApp è progettata per separare logicamente il traffico di rete per scopi diversi utilizzando Virtual Local Area Network (VLAN).

| VLAN                         | Scopo   | ID VLAN |
|------------------------------|---|---------|
| Rete di gestione fuori banda | Gestione per nodi bare metal e IPMI                                   | 16      |
| Rete bare-metal              | Rete per i servizi OpenShift una volta che il cluster è disponibile   | 181     |
| Rete di provisioning         | Rete per l'avvio PXE e l'installazione di nodi bare metal tramite IPI | 3485    |



Sebbene ciascuna di queste reti sia virtualmente separata da VLAN, ciascuna porta fisica deve essere impostata in modalità di accesso con la VLAN primaria assegnata, poiché non esiste alcun modo di passare un tag VLAN durante una sequenza di avvio PXE.

## Risorse di supporto dell'infrastruttura di rete

Prima dell'implementazione della piattaforma container OpenShift, è necessario installare la seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host accessibile dalla rete di gestione in-band e dalla rete VM.
- Almeno un server NTP accessibile dalla rete di gestione in-band e dalla rete VM.
- (Opzionale) connettività Internet in uscita per la rete di gestione in banda e la rete VM.

## OpenShift sulla piattaforma Red Hat OpenStack

La piattaforma Red Hat OpenStack offre una base integrata per creare, implementare e scalare un cloud privato OpenStack sicuro e affidabile.

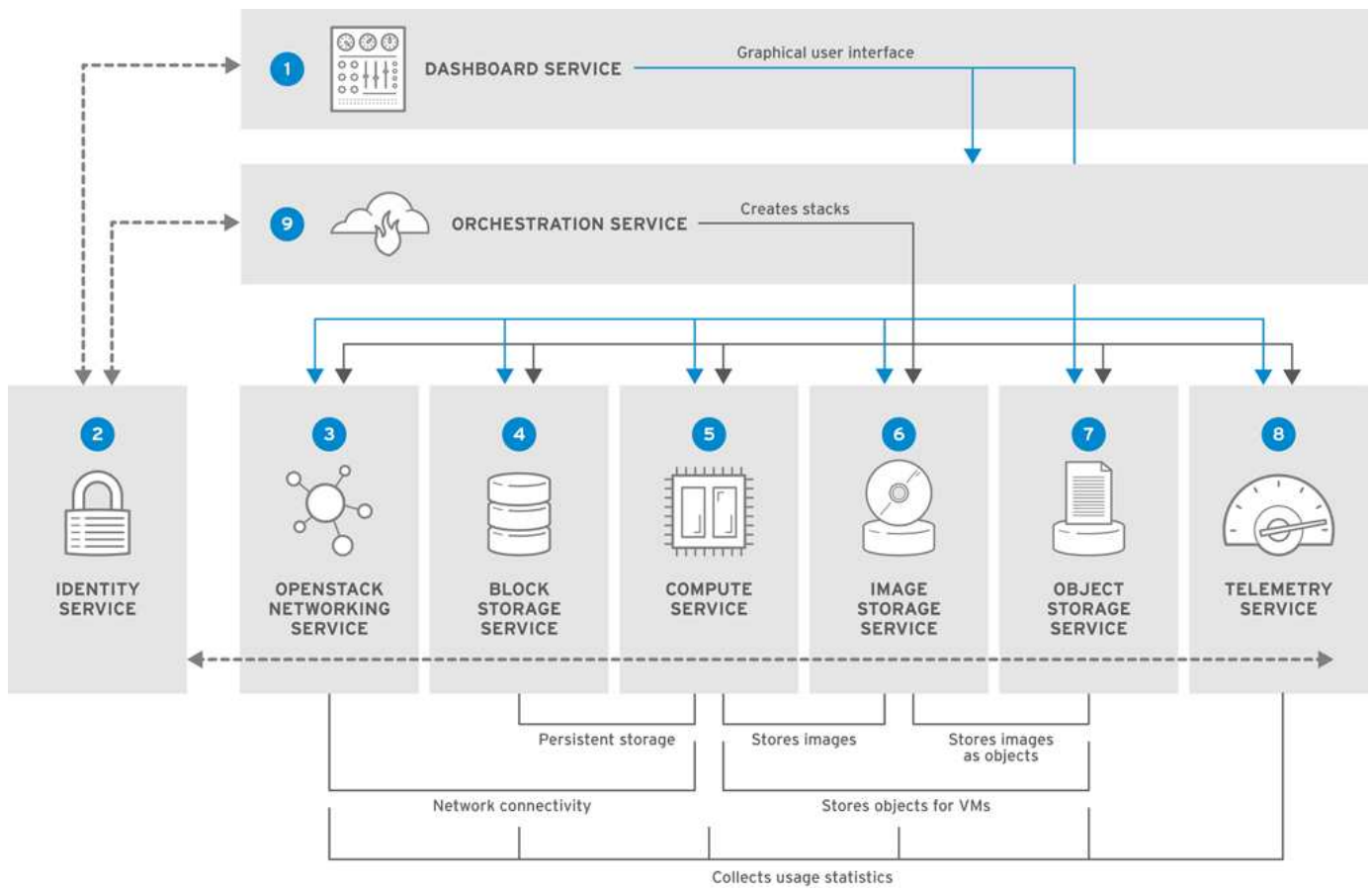
OSP è un cloud Infrastructure-as-a-service (IaaS) implementato da una raccolta di servizi di controllo che gestiscono risorse di calcolo, storage e networking. L'ambiente viene gestito tramite un'interfaccia basata su web che consente ad amministratori e utenti di controllare, eseguire il provisioning e automatizzare le risorse di OpenStack. Inoltre, l'infrastruttura OpenStack è facilitata da un'ampia interfaccia a riga di comando e API che consentono funzionalità di automazione complete per amministratori e utenti finali.

Il progetto OpenStack è un progetto della community sviluppato rapidamente che fornisce release aggiornate ogni sei mesi. Inizialmente Red Hat OpenStack Platform ha mantenuto il passo con questo ciclo di release pubblicando una nuova release insieme a ogni release upstream e fornendo supporto a lungo termine per ogni terza release. Di recente, con la release di OSP 16.0 (basata su OpenStack Train), Red Hat ha scelto di non tenere il passo con i numeri di release, ma ha invece trasferito le nuove funzionalità nelle subrelease. La versione più recente è Red Hat OpenStack Platform 16.1, che include funzionalità avanzate con backport delle release Usuri e Victoria in upstream.

Per ulteriori informazioni su OSP, vedere ["Sito Web della piattaforma Red Hat OpenStack"](#).

## Servizi OpenStack

I servizi della piattaforma OpenStack vengono implementati come container, isolando i servizi l'uno dall'altro e consentendo facili aggiornamenti. La piattaforma OpenStack utilizza un set di container creati e gestiti con Kolla. L'implementazione dei servizi viene eseguita estraendo le immagini container dal Red Hat Custom Portal. Questi container di servizio vengono gestiti utilizzando il comando Podman e vengono implementati, configurati e gestiti con Red Hat OpenStack Director.



| Servizio             | Nome del progetto | Descrizione   |
|----------------------|-------------------|---|
| Dashboard            | Orizzonte         | Dashboard basato su browser Web che consente di gestire i servizi OpenStack.  |
| Identità             | Keystone          | Servizio centralizzato per l'autenticazione e l'autorizzazione dei servizi OpenStack e per la gestione di utenti, progetti e ruoli. |
| Networking OpenStack | Neutroni          | Fornisce connettività tra le interfacce dei servizi OpenStack.  |
| Storage a blocchi    | Cinder            | Gestisce volumi di storage a blocchi persistenti per macchine virtuali (VM).  |
| Calcolo              | Nova              | Gestisce ed esegue il provisioning delle macchine virtuali in esecuzione sui nodi di calcolo.                                       |
| Immagine             | Panoramica        | Servizio di registro utilizzato per memorizzare risorse come immagini di macchine virtuali e snapshot di volumi.                    |
| Storage a oggetti    | Rapido            | Consente agli utenti di memorizzare e recuperare file e dati arbitrari.   |
| Telemetria           | Ceilometro        | Fornisce misurazioni dell'utilizzo delle risorse cloud.   |
| Orchestrazione       | Calore            | Motore di orchestrazione basato su modelli che supporta la creazione automatica di stack di risorse.                                |

## Progettazione di rete

La soluzione Red Hat OpenShift con NetApp utilizza due switch dati per fornire connettività dati primaria a 25 Gbps. Utilizza inoltre due switch di gestione aggiuntivi che forniscono connettività a 1 Gbps per la gestione in-band dei nodi di storage e gestione out-of-band per la funzionalità IPMI.

Red Hat OpenStack Director richiede la funzionalità IPMI per implementare la piattaforma Red Hat OpenStack utilizzando il servizio di provisioning bare-metal ironico.

## Requisiti VLAN

Red Hat OpenShift con NetApp è progettato per separare logicamente il traffico di rete per scopi diversi utilizzando Virtual Local Area Network (VLAN). Questa configurazione può essere scalata per soddisfare le esigenze dei clienti o per fornire un ulteriore isolamento per servizi di rete specifici. La seguente tabella elenca le VLAN necessarie per implementare la soluzione durante la convalida della soluzione in NetApp.

| VLAN                         | Scopo  | ID VLAN |
|------------------------------|--|---------|
| Rete di gestione fuori banda | Rete utilizzata per la gestione dei nodi fisici e servizio IPMI per ironico.   | 16      |
| Infrastruttura storage       | Rete utilizzata per i nodi controller per mappare i volumi direttamente per supportare servizi di infrastruttura come Swift.   | 201     |
| Storage Cinder               | Rete utilizzata per mappare e collegare i volumi a blocchi direttamente alle istanze virtuali implementate nell'ambiente.  | 202     |
| API interna                  | Rete utilizzata per la comunicazione tra i servizi OpenStack utilizzando la comunicazione API, i messaggi RPC e la comunicazione con il database.  | 301     |
| Tenant                       | Neutron fornisce a ciascun tenant le proprie reti tramite il tunneling tramite VXLAN. Il traffico di rete viene isolato all'interno di ciascuna rete tenant. A ciascuna rete tenant è associata una subnet IP e gli spazi dei nomi di rete indicano che più reti tenant possono utilizzare lo stesso intervallo di indirizzi senza causare conflitti.        | 302     |
| Gestione dello storage       | OpenStack Object Storage (Swift) utilizza questa rete per sincronizzare gli oggetti dati tra i nodi di replica partecipanti. Il servizio proxy funge da interfaccia intermedia tra le richieste degli utenti e il livello di storage sottostante. Il proxy riceve le richieste in entrata e individua la replica necessaria per recuperare i dati richiesti. | 303     |
| PXE                          | OpenStack Director offre l'avvio PXE come parte dell'ironico servizio di provisioning bare metal per orchestrare l'installazione di OSP Overcloud.   | 3484    |
| Esterno                      | Rete pubblicamente disponibile che ospita OpenStack Dashboard (Horizon) per la gestione grafica e consente alle chiamate API pubbliche di gestire i servizi OpenStack.   | 3485    |
| Rete di gestione in-band     | Fornisce l'accesso a funzioni di amministrazione del sistema come accesso SSH, traffico DNS e traffico NTP (Network Time Protocol). Questa rete funge anche da gateway per i nodi non controller.  | 3486    |

## Risorse di supporto dell'infrastruttura di rete

Prima dell'implementazione della piattaforma container OpenShift, è necessario installare la seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host.
- Almeno tre server NTP in grado di mantenere sincronizzato il tempo per i server della soluzione.
- (Opzionale) connettività Internet in uscita per l'ambiente OpenShift.

### Best practice per le implementazioni in produzione

In questa sezione sono elencate diverse Best practice che un'organizzazione deve prendere in considerazione prima di implementare questa soluzione in produzione.

### Implementa OpenShift su un cloud privato OSP con almeno tre nodi di calcolo

L'architettura verificata descritta in questo documento presenta l'implementazione hardware minima adatta per le operazioni ha implementando tre nodi controller OSP e due nodi di calcolo OSP. Questa architettura garantisce una configurazione a tolleranza di errore in cui entrambi i nodi di calcolo possono lanciare istanze virtuali e le macchine virtuali implementate possono migrare tra i due hypervisor.

Poiché Red Hat OpenShift inizialmente viene implementato con tre nodi master, una configurazione a due nodi potrebbe causare l'occupazione di almeno due master nello stesso nodo, il che può causare un'interruzione di OpenShift se tale nodo specifico non è disponibile. Pertanto, è una Best practice di Red Hat implementare almeno tre nodi di calcolo OSP in modo che i master OpenShift possano essere distribuiti in modo uniforme e la soluzione riceva un ulteriore livello di tolleranza agli errori.

### Configurare l'affinità di macchine virtuali/host

La distribuzione dei master OpenShift tra più nodi hypervisor può essere ottenuta abilitando l'affinità VM/host.

Affinity è un modo per definire le regole per un insieme di macchine virtuali e/o host che determinano se le macchine virtuali vengono eseguite insieme sullo stesso host o su host del gruppo o su host diversi. Viene applicato alle macchine virtuali creando gruppi di affinità costituiti da macchine virtuali e/o host con un insieme di parametri e condizioni identici. A seconda che le macchine virtuali di un gruppo di affinità vengano eseguite sullo stesso host o su host del gruppo o separatamente su host diversi, i parametri del gruppo di affinità possono definire affinità positiva o affinità negativa. Nella piattaforma Red Hat OpenStack, è possibile creare e applicare le regole di affinità e anti-affinità degli host creando gruppi di server e configurando i filtri in modo che le istanze distribuite da Nova in un gruppo di server vengano distribuite su nodi di calcolo diversi.

Un gruppo di server dispone di un massimo predefinito di 10 istanze virtuali per le quali può gestire il posizionamento. È possibile modificare questa impostazione aggiornando le quote predefinite per Nova.



Esiste un limite specifico di affinità/anti-affinità per i gruppi di server OSP; se non sono disponibili risorse sufficienti per l'implementazione su nodi separati o se non sono disponibili risorse sufficienti per consentire la condivisione dei nodi, la macchina virtuale non viene avviata.

Per configurare i gruppi di affinità, vedere ["Come si configurano affinità e anti-affinità per le istanze di OpenStack?"](#).

### Utilizzare un file di installazione personalizzato per la distribuzione di OpenShift

IPI semplifica l'implementazione dei cluster OpenShift attraverso la procedura guidata interattiva descritta in precedenza in questo documento. Tuttavia, potrebbe essere necessario modificare alcuni valori predefiniti come parte di una distribuzione del cluster.

In questi casi, è possibile eseguire ed eseguire le procedure guidate senza implementare immediatamente un cluster; al contrario, viene creato un file di configurazione da cui il cluster può essere distribuito in un secondo



momento. Questa funzione è molto utile se si desidera modificare le impostazioni predefinite dell'IPI o se si desidera implementare più cluster identici nell'ambiente per altri utilizzi, ad esempio la multi-tenancy. Per ulteriori informazioni sulla creazione di una configurazione di installazione personalizzata per OpenShift, vedere ["Red Hat OpenShift Installazione di un cluster su OpenStack con personalizzazioni"](#).

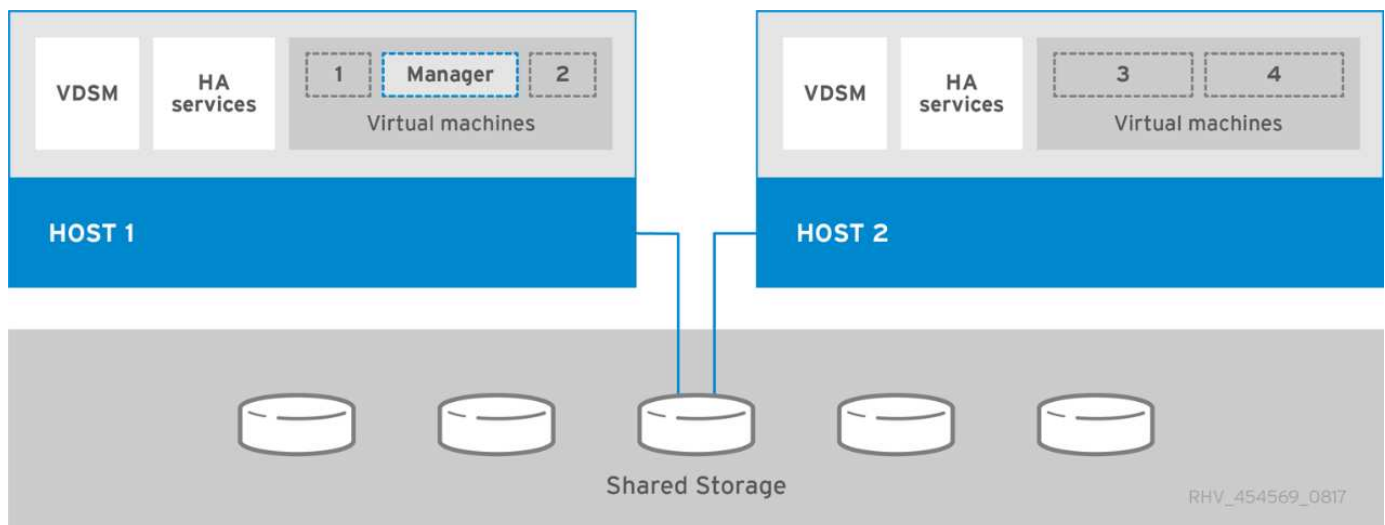
## OpenShift sulla virtualizzazione Red Hat

Red Hat Virtualization (RHV) è una piattaforma per data center virtuale aziendale che viene eseguita su Red Hat Enterprise Linux (RHEL) e utilizza l'hypervisor KVM.

Per ulteriori informazioni su RHV, consultare ["Sito Web Red Hat Virtualization"](#).

RHV offre le seguenti funzionalità:

- **Gestione centralizzata di VM e host** il manager RHV viene eseguito come macchina fisica o virtuale (VM) nella distribuzione e fornisce una GUI basata sul Web per la gestione della soluzione da un'interfaccia centrale.
- **Motore auto-ospitato** per ridurre al minimo i requisiti hardware, RHV consente a RHV Manager (RHV-M) di essere installato come VM sugli stessi host che eseguono VM guest.
- **Alta disponibilità** per evitare interruzioni in caso di guasti all'host, RHV consente di configurare le VM per l'alta disponibilità. Le macchine virtuali ad alta disponibilità vengono controllate a livello di cluster utilizzando policy di resilienza.
- **Elevata scalabilità** Un singolo cluster RHV può avere fino a 200 host hypervisor che consentono al reparto IT di supportare i requisiti di macchine virtuali di grandi dimensioni per ospitare carichi di lavoro di classe Enterprise avidi di risorse.
- **La sicurezza avanzata** ereditata dalle tecnologie RHV, Secure Virtualization (sVirt) e Security Enhanced Linux (SELinux) è impiegata da RHV per scopi di elevata sicurezza e protezione avanzata per host e VM. Il vantaggio principale di queste funzionalità è l'isolamento logico di una macchina virtuale e delle risorse associate.



## Progettazione di rete

La soluzione Red Hat OpenShift su NetApp utilizza due switch dati per fornire connettività dati primaria a 25 Gbps. Utilizza inoltre due switch di gestione aggiuntivi che forniscono connettività a 1 Gbps per la gestione in banda dei nodi di storage e gestione out-of-band per la funzionalità IPMI. OCP utilizza la rete logica della macchina virtuale su RHV per la gestione del cluster. Questa sezione descrive la disposizione e lo scopo di



ciascun segmento di rete virtuale utilizzato nella soluzione e illustra i prerequisiti per l'implementazione della soluzione.

## Requisiti VLAN

Red Hat OpenShift su RHV è progettato per separare logicamente il traffico di rete per scopi diversi utilizzando Virtual Local Area Network (VLAN). Questa configurazione può essere scalata per soddisfare le esigenze dei clienti o per fornire un ulteriore isolamento per servizi di rete specifici. La seguente tabella elenca le VLAN necessarie per implementare la soluzione durante la convalida della soluzione in NetApp.

| VLAN                         | Scopo   | ID VLAN |
|------------------------------|---|---------|
| Rete di gestione fuori banda | Gestione per nodi fisici e IPMI                             | 16      |
| Rete di macchine virtuali    | Accesso alla rete guest virtuale                            | 1172    |
| Rete di gestione in-band     | Gestione dei nodi RHV-H, RHV-Manager e della rete ovirtmgmt | 3343    |
| Rete di storage              | Rete storage per iSCSI NetApp Element                       | 3344    |
| Rete di migrazione           | Rete per la migrazione dei guest virtuali                   | 3345    |

## Risorse di supporto dell'infrastruttura di rete

Prima dell'implementazione della piattaforma container OpenShift, è necessario installare la seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host accessibile dalla rete di gestione in-band e dalla rete VM.
- Almeno un server NTP accessibile dalla rete di gestione in-band e dalla rete VM.
- (Opzionale) connettività Internet in uscita per la rete di gestione in banda e la rete VM.

## Best practice per le implementazioni in produzione

In questa sezione sono elencate diverse Best practice che un'organizzazione deve prendere in considerazione prima di implementare questa soluzione in produzione.

## Implementare OpenShift in un cluster RHV di almeno tre nodi

L'architettura verificata descritta in questo documento presenta l'implementazione hardware minima adatta per le operazioni ha implementando due nodi hypervisor RHV-H e garantendo una configurazione a tolleranza di errore in cui entrambi gli host possono gestire il motore in hosting e le macchine virtuali implementate possono migrare tra i due hypervisor.

Poiché Red Hat OpenShift viene inizialmente implementato con tre nodi master, in una configurazione a due nodi è garantito che almeno due master occuperanno lo stesso nodo, il che può causare un'interruzione di OpenShift se quel nodo specifico non è disponibile. Pertanto, è una Best practice di Red Hat che almeno tre nodi di hypervisor RHV-H siano implementati come parte della soluzione, in modo che i master OpenShift possano essere distribuiti in modo uniforme e la soluzione riceva un ulteriore grado di tolleranza agli errori.

## Configurare l'affinità di macchine virtuali/host

È possibile distribuire i master OpenShift su più nodi hypervisor abilitando l'affinità VM/host.

Affinity è un modo per definire le regole per un insieme di macchine virtuali e/o host che determinano se le macchine virtuali vengono eseguite insieme sullo stesso host o su host del gruppo o su host diversi. Viene applicato alle macchine virtuali creando gruppi di affinità costituiti da macchine virtuali e/o host con un insieme di parametri e condizioni identici. A seconda che le macchine virtuali di un gruppo di affinità vengano eseguite sullo stesso host o su host del gruppo o separatamente su host diversi, i parametri del gruppo di affinità possono definire affinità positiva o affinità negativa.

Le condizioni definite per i parametri possono essere l'applicazione forzata o forzata. La rigida applicazione garantisce che le macchine virtuali di un gruppo di affinità seguano sempre l'affinità positiva o negativa rigorosamente senza alcun riferimento alle condizioni esterne. La soft enforcement garantisce che venga impostata una preferenza più elevata per le macchine virtuali di un gruppo di affinità per seguire l'affinità positiva o negativa quando possibile. Nella configurazione di due o tre hypervisor descritta in questo documento, l'impostazione consigliata è affinità soft. Nei cluster più grandi, la hard affinità può distribuire correttamente i nodi OpenShift.

Per configurare i gruppi di affinità, vedere ["Red Hat 6.11. Documentazione di Affinity Groups"](#).

### Utilizzare un file di installazione personalizzato per la distribuzione di OpenShift

IPI semplifica l'implementazione dei cluster OpenShift attraverso la procedura guidata interattiva descritta in precedenza in questo documento. Tuttavia, è possibile che alcuni valori predefiniti debbano essere modificati nell'ambito dell'implementazione del cluster.

In questi casi, è possibile eseguire e gestire la procedura guidata senza implementare immediatamente un cluster. Viene invece creato un file di configurazione da cui è possibile implementare il cluster in un secondo momento. Questo è molto utile se si desidera modificare le impostazioni predefinite IPI o se si desidera implementare più cluster identici nel proprio ambiente per altri utilizzi, ad esempio la multi-tenancy. Per ulteriori informazioni sulla creazione di una configurazione di installazione personalizzata per OpenShift, vedere ["Red Hat OpenShift Installazione di un cluster su RHV con personalizzazioni"](#).

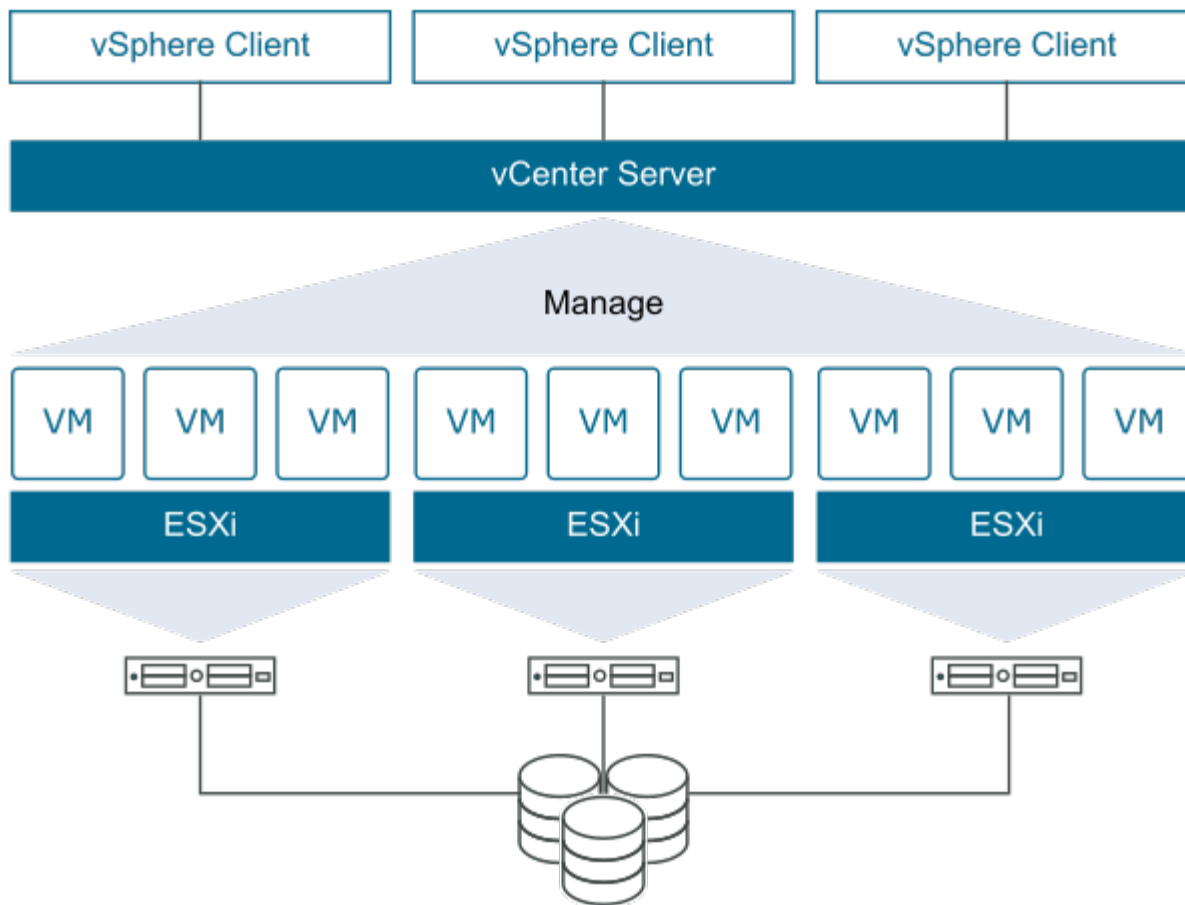
### OpenShift su VMware vSphere

VMware vSphere è una piattaforma di virtualizzazione per la gestione centralizzata di un gran numero di server e reti virtualizzati in esecuzione sull'hypervisor ESXi.

Per ulteriori informazioni su VMware vSphere, consultare ["Sito Web di VMware vSphere"](#).

VMware vSphere offre le seguenti funzionalità:

- **VMware vCenter Server** VMware vCenter Server offre una gestione unificata di tutti gli host e le macchine virtuali da un'unica console e aggrega il monitoraggio delle prestazioni di cluster, host e macchine virtuali.
- **VMware vSphere vMotion** VMware vCenter consente di eseguire la migrazione a caldo delle macchine virtuali tra i nodi del cluster su richiesta in modo non disgregativo.
- **vSphere High Availability** per evitare interruzioni in caso di errori dell'host, VMware vSphere consente di raggruppare gli host e di configurarli per l'alta disponibilità. Le macchine virtuali che vengono interrotte da un guasto dell'host vengono riavviate a breve su altri host del cluster, ripristinando i servizi.
- **Distributed Resource Scheduler (DRS)** È possibile configurare Un cluster VMware vSphere per bilanciare il carico delle risorse richieste dalle VM che ospita. È possibile eseguire la migrazione a caldo delle macchine virtuali con risorse in altri nodi del cluster per assicurarsi che siano disponibili risorse sufficienti.



## Progettazione di rete

La soluzione Red Hat OpenShift su NetApp utilizza due switch dati per fornire connettività dati primaria a 25 Gbps. Utilizza inoltre due switch di gestione aggiuntivi che forniscono connettività a 1 Gbps per la gestione in-band dei nodi di storage e gestione out-of-band per la funzionalità IPMI. OCP utilizza la rete logica VM su VMware vSphere per la gestione del cluster. Questa sezione descrive la disposizione e lo scopo di ciascun segmento di rete virtuale utilizzato nella soluzione e illustra i prerequisiti per l'implementazione della soluzione.

## Requisiti VLAN

Red Hat OpenShift su VMware vSphere è progettato per separare logicamente il traffico di rete per scopi diversi utilizzando Virtual Local Area Network (VLAN). Questa configurazione può essere scalata per soddisfare le esigenze dei clienti o per fornire un ulteriore isolamento per servizi di rete specifici. La seguente tabella elenca le VLAN necessarie per implementare la soluzione durante la convalida della soluzione in NetApp.

| VLAN                         | Scopo  | ID VLAN |
|------------------------------|--|---------|
| Rete di gestione fuori banda | Gestione per nodi fisici e IPMI                      | 16      |
| Rete di macchine virtuali    | Accesso alla rete guest virtuale                     | 181     |
| Rete di storage              | Rete di storage per NFS ONTAP                        | 184     |
| Rete di storage              | Rete storage per iSCSI ONTAP                         | 185     |
| Rete di gestione in-band     | Gestione per nodi ESXi, server vCenter, ONTAP Select | 3480    |

| VLAN               | Scopo                                     | ID VLAN |
|--------------------|---|---------|
| Rete di storage    | Rete storage per iSCSI NetApp Element     | 3481    |
| Rete di migrazione | Rete per la migrazione dei guest virtuali | 3482    |

## Risorse di supporto dell'infrastruttura di rete

Prima dell'implementazione della piattaforma container OpenShift, è necessario installare la seguente infrastruttura:

- Almeno un server DNS che fornisce una risoluzione completa del nome host accessibile dalla rete di gestione in-band e dalla rete VM.
- Almeno un server NTP accessibile dalla rete di gestione in-band e dalla rete VM.
- (Opzionale) connettività Internet in uscita per la rete di gestione in banda e la rete VM.

## Best practice per le implementazioni in produzione

In questa sezione sono elencate diverse Best practice che un'organizzazione deve prendere in considerazione prima di implementare questa soluzione in produzione.

### Implementare OpenShift in un cluster ESXi di almeno tre nodi

L'architettura verificata descritta in questo documento presenta l'implementazione hardware minima adatta per le operazioni ha implementando due nodi hypervisor ESXi e garantendo una configurazione con tolleranza di errore abilitando VMware vSphere ha e VMware vMotion. Questa configurazione consente alle macchine virtuali implementate di migrare tra i due hypervisor e di riavviare il sistema in caso di mancata disponibilità di un host.

Poiché Red Hat OpenShift inizialmente viene implementato con tre nodi master, almeno due master in una configurazione a due nodi possono occupare lo stesso nodo in alcune circostanze, il che può causare un'interruzione di OpenShift se quel nodo specifico non è disponibile. Pertanto, è una Best practice di Red Hat che devono essere implementati almeno tre nodi di hypervisor ESXi in modo che i master OpenShift possano essere distribuiti in modo uniforme, fornendo un ulteriore grado di tolleranza agli errori.

### Configurare l'affinità della macchina virtuale e dell'host

Garantire la distribuzione dei master OpenShift su più nodi hypervisor abilitando l'affinità di macchine virtuali e host.

Affinità o anti-affinità è un metodo per definire le regole per un insieme di macchine virtuali e/o host che determinano se le macchine virtuali vengono eseguite insieme sullo stesso host o su host del gruppo o su host diversi. Viene applicato alle macchine virtuali creando gruppi di affinità costituiti da macchine virtuali e/o host con un insieme di parametri e condizioni identici. A seconda che le macchine virtuali di un gruppo di affinità vengano eseguite sullo stesso host o su host del gruppo o separatamente su host diversi, i parametri del gruppo di affinità possono definire affinità positiva o affinità negativa.

Per configurare i gruppi di affinità, vedere ["Documentazione vSphere 6.7: Utilizzo delle regole di affinità DRS"](#).

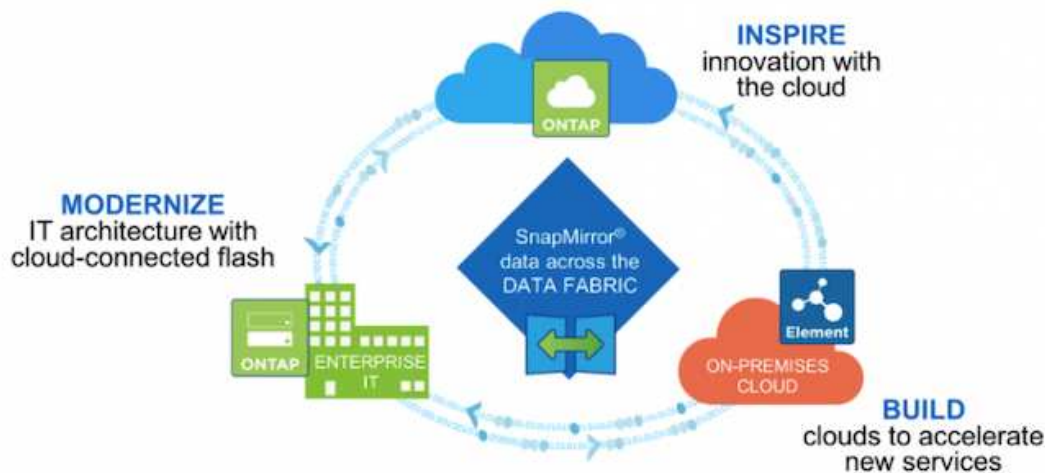
### Utilizzare un file di installazione personalizzato per la distribuzione di OpenShift

IPI semplifica l'implementazione dei cluster OpenShift attraverso la procedura guidata interattiva descritta in precedenza in questo documento. Tuttavia, potrebbe essere necessario modificare alcuni valori predefiniti come parte di una distribuzione del cluster.

In questi casi, è possibile eseguire la procedura guidata senza implementare immediatamente un cluster, ma la procedura guidata crea un file di configurazione da cui il cluster può essere distribuito in un secondo momento. Questa funzione è molto utile se si desidera modificare le impostazioni predefinite dell'IPI o se si desidera implementare più cluster identici nell'ambiente per altri utilizzi, ad esempio la multi-tenancy. Per ulteriori informazioni sulla creazione di una configurazione di installazione personalizzata per OpenShift, vedere ["Red Hat OpenShift Installazione di un cluster su vSphere con personalizzazioni"](#).

## Panoramica dello storage NetApp

NetApp dispone di diverse piattaforme di storage qualificate con Astra Trident Storage Orchestrator per il provisioning dello storage per le applicazioni implementate su Red Hat OpenShift.



- I sistemi AFF e FAS eseguono NetApp ONTAP e forniscono storage per i casi di utilizzo basati su file (NFS) e basati su blocchi (iSCSI).
- Cloud Volumes ONTAP e ONTAP Select offrono gli stessi vantaggi rispettivamente nel cloud e nello spazio virtuale.
- NetApp Cloud Volumes Service (AWS/GCP) e Azure NetApp Files offrono storage basato su file nel cloud.
- I sistemi storage NetApp Element offrono casi di utilizzo basati su blocchi (iSCSI) in un ambiente altamente scalabile.



Ogni sistema storage del portfolio NetApp può semplificare la gestione dei dati e lo spostamento tra i siti on-premise e il cloud, garantendo che i dati si trovino nella posizione in cui si trovano le applicazioni.

Le pagine seguenti contengono informazioni aggiuntive sui sistemi di storage NetApp validati nella soluzione Red Hat OpenShift con NetApp:

- ["NetApp ONTAP"](#)
- ["NetApp Element"](#)

## NetApp ONTAP

NetApp ONTAP è un potente tool software per lo storage con funzionalità come GUI intuitiva, API REST con integrazione dell'automazione, analisi predittive e azioni correttive informate dell'AI, aggiornamenti hardware senza interruzioni e importazione di storage incrociato.

Per ulteriori informazioni sul sistema di storage NetApp ONTAP, visitare il sito ["Sito Web di NetApp ONTAP"](#).

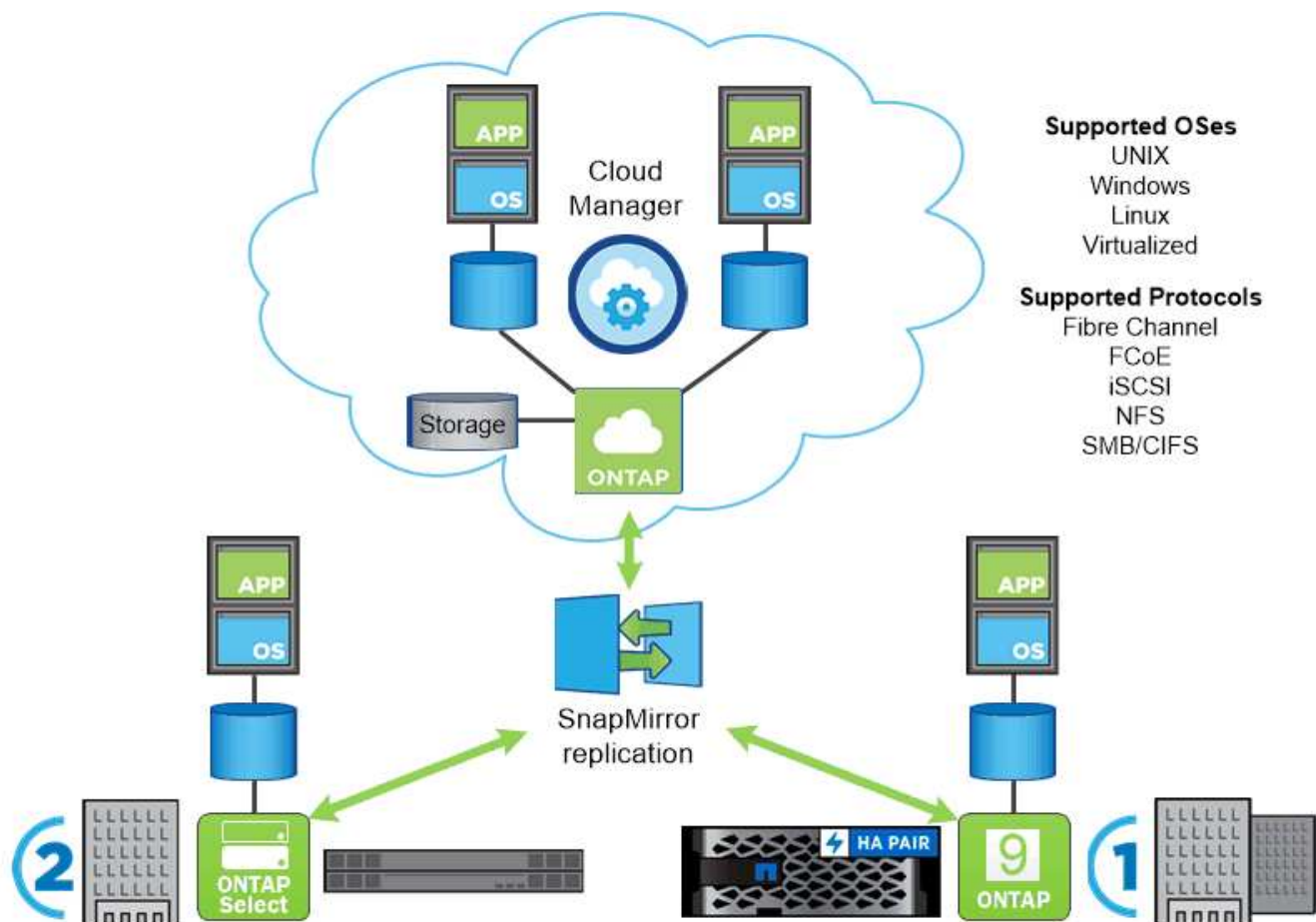
ONTAP offre le seguenti funzionalità:

- Un sistema storage unificato con accesso e gestione simultanei dei dati di NFS, CIFS, iSCSI, FC, FCoE, E protocolli FC-NVMe.
- Diversi modelli di implementazione includono configurazioni hardware on-premise su all-flash, ibride e all-HDD, piattaforme di storage basate su VM su un hypervisor supportato come ONTAP Select e nel cloud come Cloud Volumes ONTAP.
- Maggiore efficienza dello storage dei dati sui sistemi ONTAP con supporto per tiering automatico dei dati, compressione dei dati inline, deduplica e compaction.
- Storage basato su workload e controllato dalla QoS.
- Integrazione perfetta con un cloud pubblico per tiering e protezione dei dati. ONTAP offre inoltre solide funzionalità di protezione dei dati che lo differenziano in qualsiasi ambiente:
  - **NetApp Snapshot Copies.** Backup rapido e point-in-time dei dati utilizzando una quantità minima di spazio su disco senza alcun overhead delle performance aggiuntivo.
  - **NetApp SnapMirror.** Mirror le copie Snapshot dei dati da un sistema storage a un altro. ONTAP supporta il mirroring dei dati su altre piattaforme fisiche e servizi nativi del cloud.
  - **NetApp SnapLock.** Amministrazione efficiente dei dati non riscrivibili, scrivendo su volumi speciali che non possono essere sovrascritti o cancellati per un determinato periodo.
  - **NetApp SnapVault.** esegue il backup dei dati da più sistemi storage in una copia Snapshot centrale che funge da backup su tutti i sistemi designati.
  - **NetApp SyncMirror.** offre mirroring dei dati in tempo reale a livello RAID su due diversi plessi di dischi collegati fisicamente allo stesso controller.
  - **NetApp SnapRestore.** offre un rapido ripristino dei dati di backup on-demand dalle copie Snapshot.
  - **NetApp FlexClone.** fornisce il provisioning istantaneo di una copia leggibile e scrivibile di un volume NetApp basata su una copia Snapshot.

Per ulteriori informazioni su ONTAP, consultare ["Centro documentazione di ONTAP 9"](#).



NetApp ONTAP è disponibile on-premise, virtualizzato o nel cloud.



## Piattaforme NetApp

### NetApp AFF/FAS

NetApp offre solide piattaforme di storage all-flash (AFF) e ibride scale-out (FAS), realizzate su misura con performance a bassa latenza, protezione integrata dei dati e supporto multiprotocollo.

Entrambi i sistemi sono basati sul software per la gestione dei dati NetApp ONTAP, il software per la gestione dei dati più avanzato del settore per una gestione dello storage semplificata, integrata nel cloud e ad alta disponibilità, in grado di offrire velocità, efficienza e sicurezza di livello Enterprise di cui ha bisogno il data fabric.

Per ulteriori informazioni sulle piattaforme NETAPP AFF/FAS, fare clic su ["qui"](#).

### ONTAP Select

ONTAP Select è un'implementazione software-defined di NetApp ONTAP che può essere implementata su un hypervisor nel tuo ambiente. Può essere installato su VMware vSphere o su KVM e offre tutte le funzionalità e l'esperienza di un sistema ONTAP basato su hardware.

Per ulteriori informazioni su ONTAP Select, fare clic su ["qui"](#).



## Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è una versione di NetApp ONTAP implementata nel cloud e disponibile per l'implementazione in diversi cloud pubblici, tra cui: Amazon AWS, Microsoft Azure e Google Cloud.

Per ulteriori informazioni su Cloud Volumes ONTAP, fare clic su ["qui"](#).

## NetApp Element: Red Hat OpenShift con NetApp

Il software NetApp Element offre performance modulari e scalabili, con ogni nodo di storage che offre capacità e throughput garantiti all'ambiente. I sistemi NetApp Element possono scalare da 4 a 100 nodi in un singolo cluster e offrire una serie di funzionalità avanzate di gestione dello storage.



Per ulteriori informazioni sui sistemi di storage NetApp Element, visitare il sito ["Sito Web di NetApp SolidFire"](#).

### Reindirizzamento dell'accesso iSCSI e funzionalità di riparazione automatica

Il software NetApp Element sfrutta il protocollo di storage iSCSI, un metodo standard per incapsulare i comandi SCSI su una rete TCP/IP tradizionale. Quando gli standard SCSI cambiano o quando le performance delle reti Ethernet migliorano, il protocollo di storage iSCSI beneficia senza la necessità di modifiche.

Sebbene tutti i nodi storage dispongano di un IP di gestione e di un IP di storage, il software NetApp Element annuncia un singolo indirizzo IP virtuale di storage (indirizzo SVIP) per tutto il traffico di storage nel cluster. Come parte del processo di accesso iSCSI, lo storage può rispondere che il volume di destinazione è stato spostato in un indirizzo diverso e quindi non può procedere con il processo di negoziazione. L'host quindi invia nuovamente la richiesta di accesso al nuovo indirizzo in un processo che non richiede alcuna riconfigurazione sul lato host. Questo processo è noto come reindirizzamento dell'accesso iSCSI.

Il reindirizzamento dell'accesso iSCSI è una parte chiave del cluster software NetApp Element. Quando viene ricevuta una richiesta di accesso all'host, il nodo decide quale membro del cluster deve gestire il traffico in base agli IOPS e ai requisiti di capacità per il volume. I volumi vengono distribuiti nel cluster software NetApp Element e ridistribuiti se un singolo nodo gestisce un volume eccessivo di traffico per i volumi o se viene aggiunto un nuovo nodo. Più copie di un determinato volume vengono allocate nell'array.

In questo modo, se un guasto di un nodo è seguito da una redistribuzione del volume, non vi è alcun effetto sulla connettività dell'host oltre a una disconnessione e all'accesso con reindirizzamento alla nuova posizione. Con il reindirizzamento dell'accesso iSCSI, un cluster software NetApp Element è un'architettura scale-out con riparazione automatica in grado di eseguire operazioni e aggiornamenti senza interruzioni.

### QoS del cluster software NetApp Element

Un cluster software NetApp Element consente di configurare dinamicamente la qualità del servizio in base al volume. È possibile utilizzare le impostazioni QoS per volume per controllare le performance dello storage in base agli SLA definiti dall'utente. I seguenti tre parametri configurabili definiscono la QoS:



- **IOPS minimi.** il numero minimo di IOPS sostenuti che il cluster software NetApp Element fornisce a un volume. Il livello minimo di IOPS configurato per un volume è il livello garantito di performance per un volume. Le performance per volume non scendono al di sotto di questo livello.
- **IOPS massimo.** numero massimo di IOPS sostenuti che il cluster software NetApp Element fornisce a un determinato volume.
- **IOPS burst.** numero massimo di IOPS consentito in uno scenario a burst breve. L'impostazione della durata del burst è configurabile, con un valore predefinito di 1 minuto. Se un volume è stato eseguito al di sotto del livello IOPS massimo, vengono accumulati i crediti burst. Quando i livelli di performance diventano molto elevati e vengono spinti, sul volume sono consentiti brevi burst di IOPS oltre i massimi IOPS.

## Multi-tenancy

La multi-tenancy sicura si ottiene con le seguenti funzionalità:

- **Autenticazione sicura.** il protocollo CHAP (Challenge-Handshake Authentication Protocol) viene utilizzato per l'accesso sicuro ai volumi. Il protocollo LDAP (Lightweight Directory Access Protocol) viene utilizzato per l'accesso sicuro al cluster per la gestione e la creazione di report.
- **Volume Access Group (VAG).** facoltativamente, i VAG possono essere utilizzati al posto dell'autenticazione, mappando qualsiasi numero di iSCSI Initiator-Specific iSCSI Qualified Name (IQN) in uno o più volumi. Per accedere a un volume in un VAG, l'IQN dell'iniziatore deve essere nell'elenco IQN consentito per il gruppo di volumi.
- **LAN virtuali tenant (VLAN).** a livello di rete, la sicurezza di rete end-to-end tra gli iniziatori iSCSI e il cluster software NetApp Element è facilitata dall'utilizzo di VLAN. Per qualsiasi VLAN creata per isolare un carico di lavoro o un tenant, il software NetApp Element crea un indirizzo SVIP di destinazione iSCSI separato accessibile solo attraverso la VLAN specifica.
- **VLAN abilitate per VRF.** per supportare ulteriormente la sicurezza e la scalabilità nel data center, il software NetApp Element consente di abilitare qualsiasi VLAN tenant per funzionalità simili a VRF. Questa funzionalità aggiunge queste due funzionalità chiave:
  - **Routing L3 a un indirizzo SVIP tenant.** questa funzione consente di posizionare gli iniziatori iSCSI su una rete o VLAN separata da quella del cluster software NetApp Element.
  - **Subnet IP sovrapposte o duplicate.** questa funzione consente di aggiungere un modello agli ambienti tenant, consentendo a ciascuna VLAN tenant di essere assegnata a indirizzi IP della stessa subnet IP. Questa funzionalità può essere utile per gli ambienti dei provider di servizi in cui la scalabilità e la conservazione di IPspace sono importanti.

## Efficienze dello storage aziendale

Il cluster software NetApp Element aumenta l'efficienza e le performance generali dello storage. Le seguenti funzioni vengono eseguite inline, sono sempre attive e non richiedono alcuna configurazione manuale da parte dell'utente:

- **Deduplica.** il sistema memorizza solo blocchi 4K univoci. Tutti i blocchi 4K duplicati vengono automaticamente associati a una versione dei dati già memorizzata. I dati si trovano su dischi a blocchi e vengono mirrorati utilizzando la protezione dei dati del software NetApp Element Helix. Questo sistema riduce significativamente il consumo di capacità e le operazioni di scrittura all'interno del sistema.
- **Compressione.** la compressione viene eseguita inline prima che i dati vengano scritti nella NVRAM. I dati vengono compressi, memorizzati in blocchi 4K e rimangono compressi nel sistema. Questa compressione riduce significativamente il consumo di capacità, le operazioni di scrittura e il consumo di larghezza di banda nel cluster.

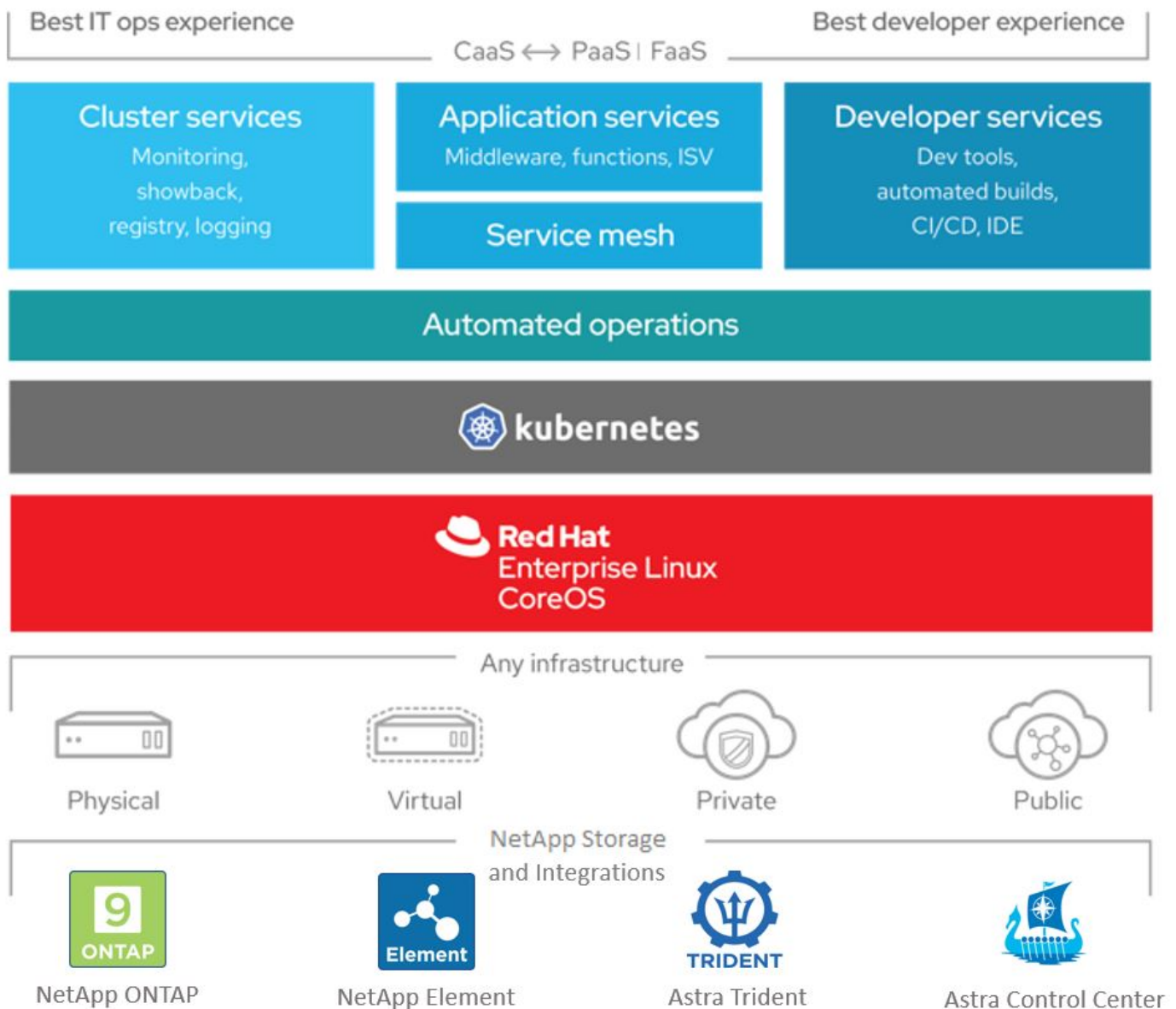
- **Thin-provisioning.** questa funzionalità fornisce la giusta quantità di storage al momento necessario, eliminando il consumo di capacità causato da volumi con overprovisioning o volumi sottoutilizzati.
- **Helix.** i metadati di un singolo volume vengono memorizzati su un'unità di metadati e replicati su un'unità di metadati secondaria per la ridondanza.



Element è stato progettato per l'automazione. Tutte le funzionalità di storage sono disponibili tramite API. Queste API sono l'unico metodo utilizzato dall'interfaccia utente per controllare il sistema.

## Panoramica sull'integrazione dello storage NetApp

NetApp offre una serie di prodotti per aiutarvi nell'orchestrazione e nella gestione dei dati persistenti in ambienti basati su container, come Red Hat OpenShift.



NetApp Astra Control offre un set completo di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful, basati sulla tecnologia di protezione dei dati di NetApp. Astra Control Service è disponibile per supportare carichi di lavoro stateful nelle implementazioni Kubernetes native nel

cloud. Astra Control Center è disponibile per supportare carichi di lavoro stateful in implementazioni on-premise, come Red Hat OpenShift. Per ulteriori informazioni, visita il sito Web di NetApp Astra Control ["qui"](#).

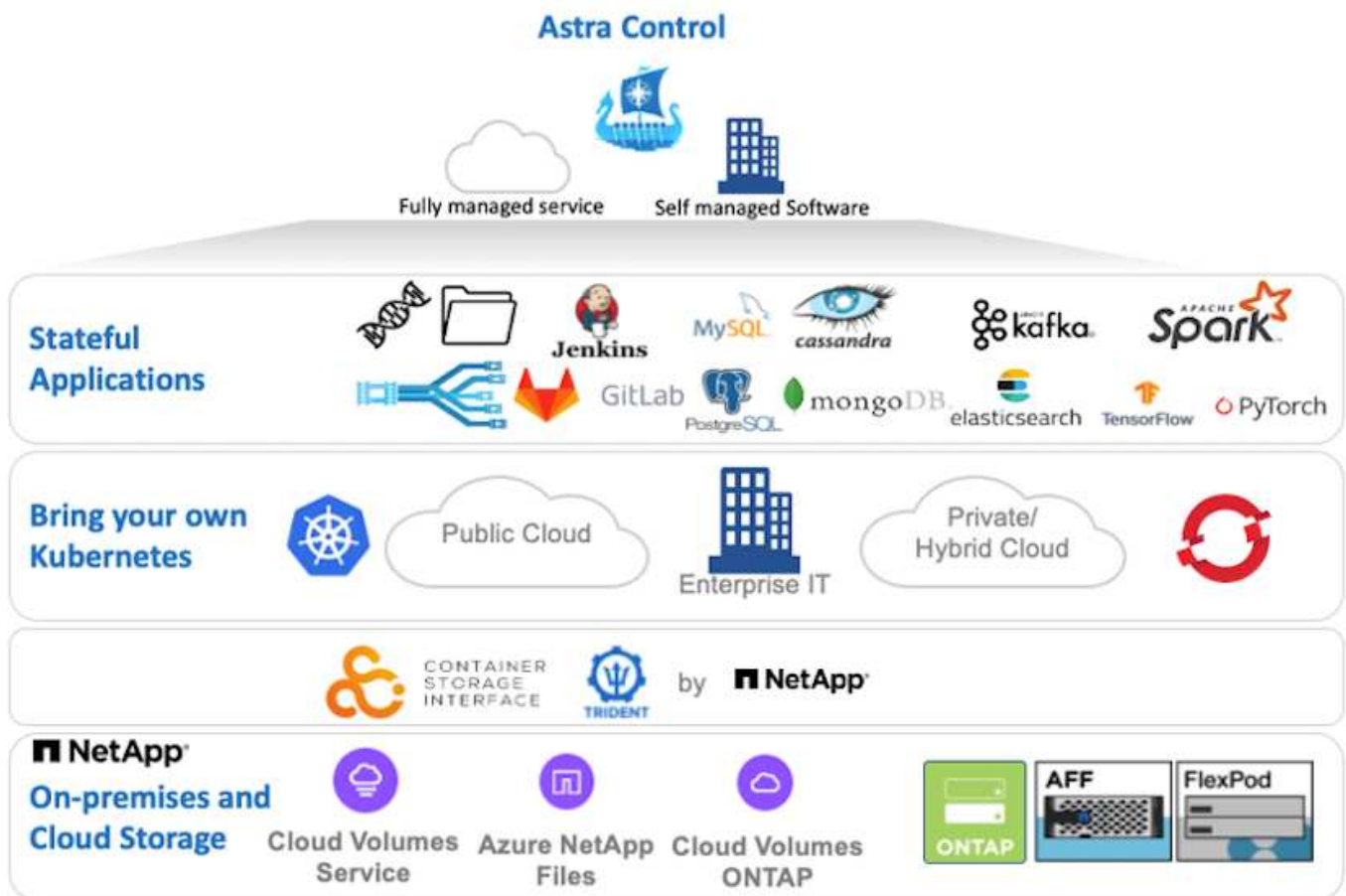
NetApp Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, tra cui Red Hat OpenShift. Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

Le pagine seguenti contengono informazioni aggiuntive sui prodotti NetApp validati per la gestione delle applicazioni e dello storage persistente nella soluzione Red Hat OpenShift con NetApp:

- ["NetApp Astra Control Center"](#)
- ["NetApp Astra Trident"](#)

## Panoramica di NetApp Astra Control Center

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati basati su applicazioni e storage per carichi di lavoro Kubernetes stateful implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati di NetApp.



È possibile installare NetApp Astra Control Center su un cluster Red Hat OpenShift che dispone di Astra Trident Storage orchestrator implementato e configurato con classi di storage e backend di storage per i sistemi storage NetApp ONTAP.

Per l'installazione e la configurazione di Astra Trident per il supporto di Astra Control Center, vedere ["questo documento qui"](#).

In un ambiente connesso al cloud, il centro di controllo Astra utilizza Cloud Insights per fornire monitoraggio avanzato e telemetria. In assenza di una connessione Cloud Insights, sono disponibili funzioni limitate di monitoraggio e telemetria (7 giorni di metriche) ed esportate negli strumenti di monitoraggio nativi di Kubernetes (Prometheus e Grafana) attraverso endpoint di metriche aperte.

Il centro di controllo Astra è completamente integrato nell'ecosistema NetApp AutoSupport e Active IQ per fornire supporto agli utenti, fornire assistenza per la risoluzione dei problemi e visualizzare le statistiche di utilizzo.

Oltre alla versione a pagamento di Astra Control Center, è disponibile una licenza di valutazione di 90 giorni. La versione di valutazione è supportata tramite e-mail e community (canale slack). I clienti hanno accesso a questi e ad altri articoli della Knowledge base e alla documentazione disponibile nella dashboard di supporto dei prodotti.

Per iniziare a utilizzare NetApp Astra Control Center, visita il ["Sito web Astra"](#).

#### Prerequisiti per l'installazione di Astra Control Center

1. Uno o più cluster Red Hat OpenShift. Le versioni 4.6 EUS e 4.7 sono attualmente supportate.
2. Astra Trident deve essere già installato e configurato su ogni cluster Red Hat OpenShift.
3. Uno o più sistemi storage NetApp ONTAP con ONTAP 9.5 o superiore.



Per ogni installazione di OpenShift in un sito è consigliabile disporre di una SVM dedicata per lo storage persistente. Le implementazioni multi-sito richiedono sistemi storage aggiuntivi.

4. È necessario configurare un backend di storage Trident su ciascun cluster OpenShift con una SVM supportata da un cluster ONTAP.
5. StorageClass predefinita configurata su ciascun cluster OpenShift con Astra Trident come storage provisioning.
6. È necessario installare e configurare un bilanciamento del carico su ciascun cluster OpenShift per il bilanciamento del carico e l'esposizione dei servizi OpenShift.



Vedere il link ["qui"](#) per informazioni sui bilanciatori di carico validati per questo scopo.

7. È necessario configurare un registro di immagini privato per ospitare le immagini di NetApp Astra Control Center.



Vedere il link ["qui"](#) Per installare e configurare un registro privato OpenShift a tale scopo.

8. È necessario disporre dell'accesso Cluster Admin al cluster Red Hat OpenShift.
9. È necessario disporre dell'accesso come amministratore ai cluster NetApp ONTAP.
10. Una workstation di amministrazione con i tool docker o podman, tridentctl e oc o kubectl installati e aggiunti al percorso dei dollari.



Le installazioni di Docker devono avere una versione di Docker superiore alla 20.10 e le installazioni di Podman devono avere una versione di podman superiore alla 3.0.



## Utilizzo di OperatorHub

1. Accedere al NetApp Support Site e scaricare l'ultima versione di NetApp Astra Control Center. Per farlo, è necessaria una licenza allegata al tuo account NetApp. Dopo aver scaricato il tarball, trasferirlo sulla workstation di amministrazione.



Per iniziare a utilizzare una licenza di prova per Astra Control, visitare il sito "[Sito di registrazione Astra](#)".

2. Disimballare il tar ball e modificare la directory di lavoro nella cartella risultante.

```
[netapp-user@rhel7 ~]$ tar -vxzf astra-control-center-21.12.60.tar.gz
[netapp-user@rhel7 ~]$ cd astra-control-center-21.12.60
```

3. Prima di iniziare l'installazione, trasferire le immagini di Astra Control Center in un registro di immagini. Puoi scegliere di farlo con Docker o Podman; in questo passaggio vengono fornite le istruzioni per entrambi.

## Podman

- a. Esportare 'reFQDN del Registro di sistema con il nome dell'organizzazione/namespace/progetto come variabile di ambiente 'gistry'.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- b. Accedere al Registro di sistema.

```
[netapp-user@rhel7 ~]$ podman login -u ocp-user -p password --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```



Se si utilizza kubeadmin utente per accedere al registro privato, quindi utilizzare il token invece della password -podman login -u ocp-user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com.



In alternativa, è possibile creare un account di servizio, assegnare un ruolo di editor del Registro di sistema e/o di visualizzatore del Registro di sistema (a seconda che si richieda l'accesso push/pull) e accedere al Registro di sistema utilizzando il token dell'account di servizio.

- c. Creare un file script della shell e incollarne il contenuto seguente.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded
    image trimming the 'Loaded images: '
    astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image(s): //' )
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
    # Tag with local image repo.
    podman tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    podman push ${REGISTRY}/${astraImage}
done
```



Se si utilizzano certificati non attendibili per il Registro di sistema, modificare lo script della shell e utilizzare --tls-verify=false per il comando podman push podman push \$REGISTRY/\$(echo \$astraImage | sed 's/!\[]\+\:\/\/') --tls-verify=false.

d. Rendere il file eseguibile.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. Eseguire lo script della shell.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```



## Docker

- a. Esportare 'reFQDN del Registro di sistema con il nome dell'organizzazione/namespace/progetto come variabile di ambiente 'gistry'.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- b. Accedere al Registro di sistema.

```
[netapp-user@rhel7 ~]$ docker login -u ocp-user -p password astra-registry.apps.ocp-vmw.cie.netapp.com
```



Se si utilizza kubeadmin utente per accedere al registro privato, quindi utilizzare il token invece della password - `docker login -u ocp-user -p token astra-registry.apps.ocp-vmw.cie.netapp.com`.



In alternativa, è possibile creare un account di servizio, assegnare un ruolo di editor del Registro di sistema e/o di visualizzatore del Registro di sistema (a seconda che si richieda l'accesso push/pull) e accedere al Registro di sistema utilizzando il token dell'account di servizio.

- c. Creare un file script della shell e incollarne il contenuto seguente.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded
    image trimming the 'Loaded images: '
    astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //' )
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
    # Tag with local image repo.
    docker tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    docker push ${REGISTRY}/${astraImage}
done
```

- d. Rendere il file eseguibile.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

- e. Eseguire lo script della shell.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

4. Quando si utilizzano registri di immagini private non pubblicamente attendibili, caricare i certificati TLS del registro di immagini nei nodi OpenShift. A tale scopo, creare una configurazione nello spazio dei nomi openshift-config utilizzando i certificati TLS e applicarla alla configurazione dell'immagine del cluster per rendere attendibile il certificato.

```
[netapp-user@rhel7 ~]$ oc create configmap default-ingress-ca -n  
openshift-config --from-file=astra-registry.apps.ocp  
-vmw.cie.netapp.com=tls.crt  
  
[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster  
--patch '{"spec":{"additionalTrustedCA":{"name":"default-ingress-  
ca"}}}' --type=merge
```



Se si utilizza un registro interno di OpenShift con certificati TLS predefiniti dall'operatore di ingresso con un percorso, è comunque necessario seguire la procedura precedente per applicare la patch ai certificati con il nome host del percorso. Per estrarre i certificati dall'operatore di ingresso, è possibile utilizzare il comando `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`.

5. Creare uno spazio dei nomi netapp-acc-operator Per Astra Control Center.

```
[netapp-user@rhel7 ~]$ oc create ns netapp-acc-operator  
  
namespace/netapp-acc-operator created
```


6. Creare un segreto con le credenziali per accedere al registro delle immagini in netapp-acc-operator namespace.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-  
registry-cred --docker-server=astra-registry.apps.ocp  
-vmw.cie.netapp.com --docker-username=ocp-user --docker  
-password=password -n netapp-acc-operator  
  
secret/astra-registry-cred created
```

7. Accedi alla console GUI di Red Hat OpenShift con accesso cluster-admin.
8. Selezionare Administrator (Amministratore) dal menu a discesa Perspective (prospettiva).
9. Accedere a Operator > OperatorHub e cercare Astra.



10. Selezionare `netapp-acc-operator` affiancare e fare clic su `Install`.



**netapp-acc-operator**  
21.12.63-1 provided by NetApp

✕

Install

---

**Latest version**  
21.12.63-1

**Capability level**  
☒ Basic Install  
☐ Seamless Upgrades  
☐ Full Lifecycle  
☐ Deep Insights  
☐ Auto Pilot

**Provider type**  
Certified

**Provider**  
NetApp

Astra Control is an application-aware data management solution that manages, protects and moves data-rich Kubernetes workloads in both public clouds and on-premises.

Astra Control enables data protection, disaster recovery, and migration for your Kubernetes workloads, leveraging NetApp's industry-leading data management technology for snapshots, backups, replication and cloning.

### How to deploy Astra Control

Refer to [Installation Procedure](#) to deploy Astra Control Center using the Operator.

### Documentation

Refer to [Astra Control Center Documentation](#) to complete the setup and start managing applications.

11. Nella schermata `Install Operator` (Installa operatore), accettare tutti i parametri predefiniti e fare clic su `Install`.

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

### Update channel \*

- ☐ alpha
- ☒ stable

### Installation mode \*

- ☒ All namespaces on the cluster (default)  
Operator will be available in all Namespaces.
- ☐ A specific namespace on the cluster  
This mode is not supported by this Operator

### Installed Namespace \*

PR netapp-acc-operator (Operator recommended)

#### ⚠ Namespace already exists


Namespace **netapp-acc-operator** already exists and will be used. Other users can already have access to this namespace.

### Approval strategy \*

- ☒ Automatic
- ☐ Manual

Install

Cancel

 **netapp-acc-operator**  
provided by NetApp

#### Provided APIs

 **Astra Control Center**

AstraControlCenter is the Schema for the astracontrolcenters API

12. Attendere il completamento dell'installazione da parte dell'operatore.



**netapp-acc-operator**  
21.12.63-1 provided by NetApp



## Installing Operator

InstallWaiting: installing; waiting for deployment acc-operator-controller-manager to become ready; Waiting for rollout to finish: 0 of 1 updated replicas are available...

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace netapp-acc-operator](#)

13. Una volta completata l'installazione dell'operatore, selezionare per fare clic su View Operator.



netapp-acc-operator

21.12.63-1 provided by NetApp



## Installed operator - ready for use

[View Operator](#)

[View installed Operators in Namespace netapp-acc-operator](#)

14. Quindi fare clic su `Create Instance` Nel riquadro Astra Control Center dell'operatore.

[Installed Operators](#) > [Operator details](#)



netapp-acc-operator

21.12.63-1 provided by NetApp

[Details](#)

[YAML](#)

[Subscription](#)

[Events](#)

[Astra Control Center](#)

## Provided APIs

**ACC** Astra Control Center

AstraControlCenter is the Schema for the astracontrolcenters API

[+ Create instance](#)

15. Riempire `Create AstraControlCenter` campi del modulo e fare clic su `Create`.

- Se si desidera, modificare il nome dell'istanza di Astra Control Center.
- Se si desidera, attivare o disattivare il supporto automatico. Si consiglia di mantenere la funzionalità di supporto automatico.
- Inserire il nome FQDN per Astra Control Center.
- Inserire la versione di Astra Control Center; per impostazione predefinita viene visualizzata la

versione più recente.

- e. Inserisci un nome account per Astra Control Center e i dettagli dell'amministratore come nome, cognome e indirizzo e-mail.
- f. Inserire il criterio di recupero del volume, l'impostazione predefinita è Mantieni.
- g. In Image Registry (Registro immagini), immettere l'FQDN del registro insieme al nome dell'organizzazione assegnato durante l'invio delle immagini al registro (in questo esempio, `astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra`)
- h. Se si utilizza un registro che richiede l'autenticazione, inserire il nome segreto nella sezione Registro immagini.
- i. Configurare le opzioni di scalabilità per i limiti delle risorse di Astra Control Center.
- j. Inserire il nome della classe di storage se si desidera inserire PVC in una classe di storage non predefinita.
- k. Definire le preferenze di gestione CRD.

Project: netapp-acc-operator ▼

---

**Name \***

**Labels**

**Account Name \***

Astra Control Center account name

**Astra Address \***

AstraAddress defines how Astra will be found in the data center. This IP address and/or DNS A record must be created prior to provisioning Astra Control Center. Example - "astra.example.com" The A record and its IP address must be allocated prior to provisioning Astra Control Center

**Astra Version \***

Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch

**Email \***

EmailAddress will be notified by Astra as events warrant.

**Auto Support \*** >

AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. The default election is true and indicates support data will be sent to NetApp. An empty or blank election is the same as a default election. Air gapped installations should enter false.

**First Name**

The first name of the SRE supporting Astra.

**Last Name**

Admin

The last name of the SRE supporting Astra.

**Image Registry**

The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

**Name**

astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra

The name of the image registry. For example "example.registry/astra". Do not prefix with protocol.

**Secret**

astra-registry-cred

The name of the Kubernetes secret that will authenticate with the image registry.

**Volume Reclaim Policy**

Retain

Reclaim policy to be set for persistent volumes

**Astra Resources Scaler**

Default

Scaling options for AstraControlCenter Resource limits.

**Storage Class**

The storage class to be used for PVCs. If not set, default storage class will be used.

**Crds**

Options for how ACC should handle CRDs.

Create

Cancel

**Automatizzato [Ansible]**

1. Per utilizzare i playbook Ansible per implementare Astra Control Center, è necessaria una macchina Ubuntu/RHEL con Ansible installato. Seguire le procedure ["qui"](#) Per Ubuntu e RHEL.
2. Clonare il repository GitHub che ospita il contenuto Ansible.

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. Accedi al sito NetApp Support e scarica l'ultima versione di NetApp Astra Control Center. Per farlo, è necessaria una licenza allegata al tuo account NetApp. Dopo aver scaricato il tarball, trasferirlo sulla workstation.



Per iniziare a utilizzare una licenza di prova per Astra Control, visitare il sito ["Sito di registrazione Astra"](#).

4. Creare o ottenere il file kubeconfig con accesso amministratore al cluster OpenShift su cui deve essere installato Astra Control Center.

5. Modificare la directory in na\_astra\_control\_suite.

```
cd na_astra_control_suite
```

6. Modificare il vars/vars.yml e inserire le variabili con le informazioni richieste.

```
#Define whether or not to push the Astra Control Center images to
your private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or
"Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer
type service to access ACC, requires MetallB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the
kubernetes/openshift cluster Astra Control Center needs to be
installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-
kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want
to accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the
PVCs to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
```



```

storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values:
yes, no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image
registry credentials
#Usually, the registry namespace and usernames are same for
individual users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kubernetes/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the
playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

7. Esegui il manuale per implementare Astra Control Center. Il playbook richiede privilegi root per alcune configurazioni.

Se l'utente che esegue il playbook è root o ha configurato sudo senza password, eseguire il seguente comando per eseguire il playbook.

```
ansible-playbook install_acc_playbook.yml
```

Se l'utente ha configurato l'accesso sudo basato su password, eseguire il seguente comando per eseguire il manuale, quindi inserire la password sudo.

```
ansible-playbook install_acc_playbook.yml -K
```

## Fasi successive all'installazione

1. Il completamento dell'installazione potrebbe richiedere alcuni minuti. Verificare che tutti i pod e i servizi in `netapp-astra-cc` namespace in esecuzione.

```
[netapp-user@rhel7 ~]$ oc get all -n netapp-astra-cc
```

2. Controllare `acc-operator-controller-manager` registri per garantire che l'installazione sia completata.

```
[netapp-user@rhel7 ~]$ oc logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```



Il seguente messaggio indica la corretta installazione di Astra Control Center.

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[21.12.60]"}

```

3. Il nome utente per l'accesso ad Astra Control Center è l'indirizzo e-mail dell'amministratore fornito nel file CRD e la password è una stringa ACC- Aggiunto all'UUID di Astra Control Center. Eseguire il seguente comando:

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME      UUID
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



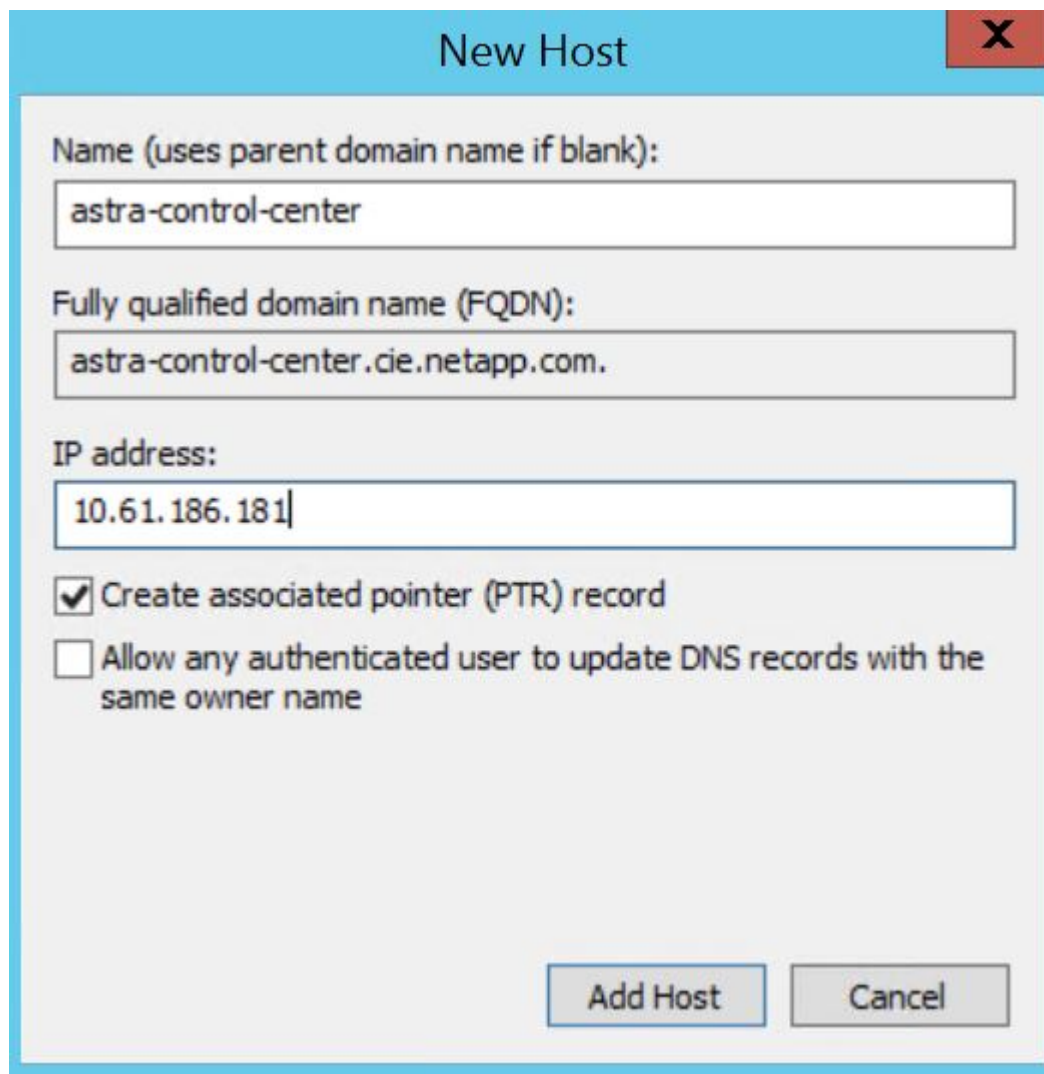
In questo esempio, la password è ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f.

4. Ottieni l'IP del bilanciamento del carico del servizio traefik.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep 'EXTERNAL|traefik'
```

| NAME          | TYPE                        | CLUSTER-IP    |
|---------------|-----------------------------|---------------|
| EXTERNAL-IP   | PORT(S)                     |               |
| AGE           |                             |               |
| traefik       | LoadBalancer                | 172.30.99.142 |
| 10.61.186.181 | 80:30343/TCP, 443:30060/TCP |               |
| 16m           |                             |               |

5. Aggiungere una voce nel server DNS che punta all'FQDN fornito nel file CRD di Astra Control Center  
EXTERNAL-IP del servizio traefik.



**New Host**

Name (uses parent domain name if blank):  
astra-control-center

Fully qualified domain name (FQDN):  
astra-control-center.cie.netapp.com.

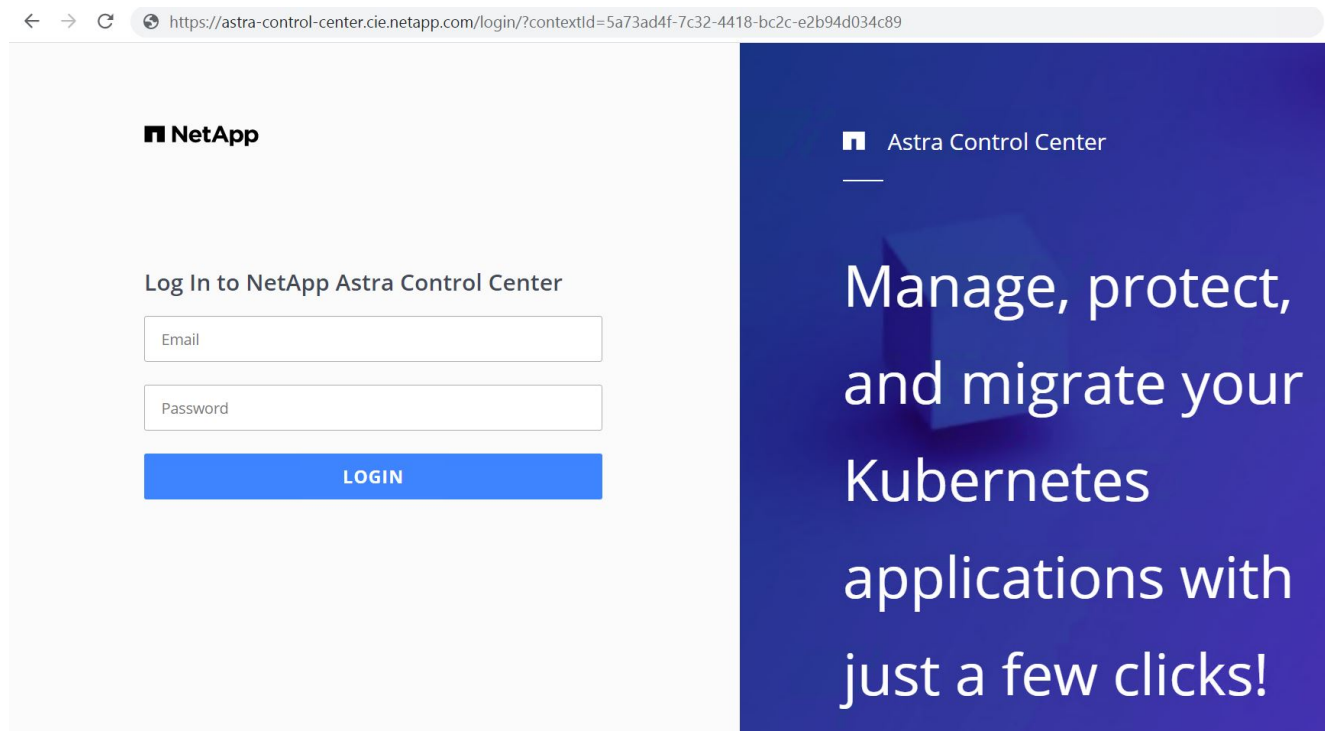
IP address:  
10.61.186.181

☒ Create associated pointer (PTR) record

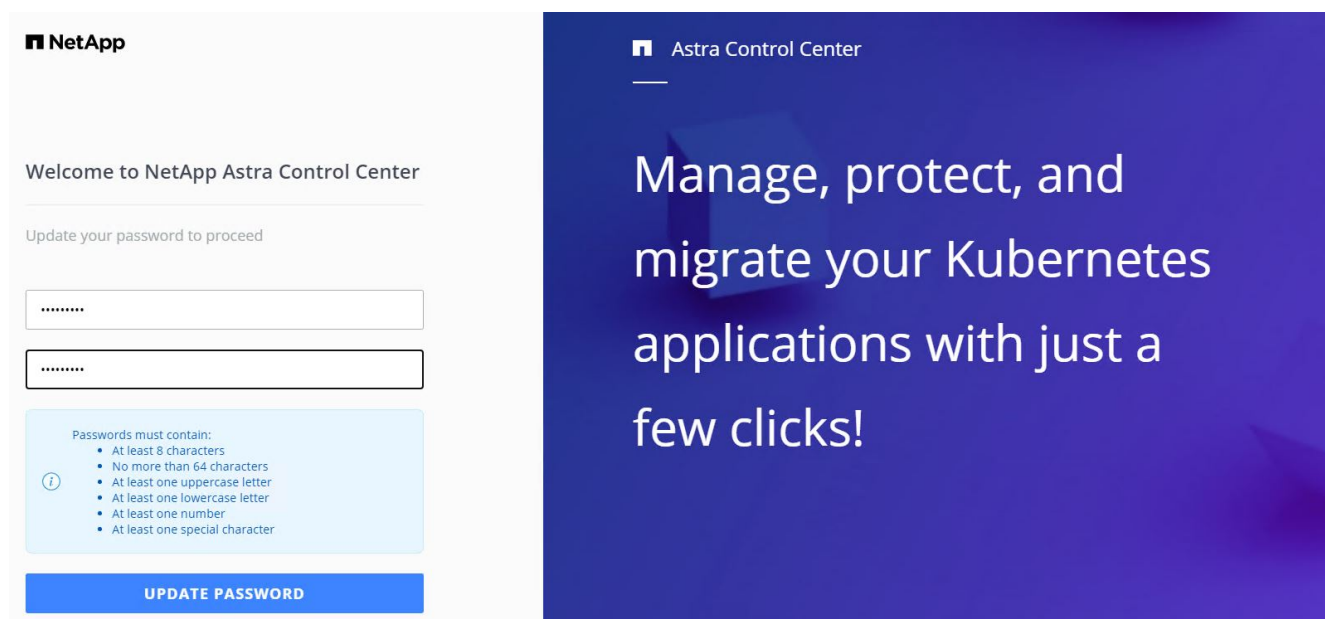
☐ Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

6. Accedere alla GUI di Astra Control Center esplorando il relativo FQDN.



7. Quando si accede all'interfaccia grafica di Astra Control Center per la prima volta utilizzando l'indirizzo email admin fornito in CRD, è necessario modificare la password.



8. Se si desidera aggiungere un utente ad Astra Control Center, accedere a account > Users (account > utenti), fare clic su Add (Aggiungi), inserire i dettagli dell'utente e fare clic su Add (Aggiungi).

**Add user**
✕

USER DETAILS

First name

Nikhil

Last name

Kulkarni

Email address

tme\_nik@netapp.com

PASSWORD

Temporary password

\*\*\*\*\*

Confirm temporary password

\*\*\*\*\*

ⓘ

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE ⓘ

Role

Owner

▼

Cancel

Add ✓

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

- Astra Control Center richiede una licenza per il funzionamento di tutte le funzionalità IT. Per aggiungere una licenza, accedere a account > License (account > licenza), fare clic su Add License (Aggiungi licenza) e caricare il file di licenza.

Account

Users
Credentials
Notifications
**License**
Connections

ASTRA CONTROL CENTER LICENSE 0

To get started with Astra Control Center, select Add license to manually upload the file.

License file

EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

⬆

✕

Cancel

Add

In caso di problemi con l'installazione o la configurazione di NetApp Astra Control Center, è disponibile la knowledge base dei problemi noti ["qui"](#).

## Registra i tuoi Red Hat OpenShift Clusters con Astra Control Center

Per consentire ad Astra Control Center di gestire i carichi di lavoro, devi prima registrare il cluster Red Hat OpenShift.

103

## Registra i cluster Red Hat OpenShift

1. Il primo passo consiste nell'aggiungere i cluster OpenShift all'Astra Control Center e gestirli. Accedere a Clusters e fare clic su Add a Cluster (Aggiungi cluster), caricare il file kubeconfig per il cluster OpenShift e fare clic su Select Storage (Seleziona storage).

The screenshot shows the 'Add cluster' dialog box in Astra Control Center, specifically the 'STEP 1/3: CREDENTIALS' tab. The dialog has a title bar with a close button (X) and a progress indicator. Below the title bar, there's a section titled 'CREDENTIALS' with instructions: 'Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential. Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.' There are two options: 'Upload file' (selected) and 'Paste from clipboard'. Under 'Upload file', there's a text input field containing 'ocp-vmw kubeconfig.txt' and a file selection icon. To the right, there's a 'Credential name' input field containing 'ocp-vmw'. On the right side of the dialog, there's a sidebar titled 'ADDING A CLUSTER' with text: 'Adding a cluster is needed for Astra Control to discover your Kubernetes applications. Select a cloud provider and input credentials to get started. Read more in [Clusters](#).' At the bottom of the dialog, there are two buttons: 'Cancel' and 'Configure storage →'.



Il file kubeconfig può essere generato per l'autenticazione con un nome utente e una password o un token. I token scadono dopo un periodo di tempo limitato e potrebbero non essere raggiungibili dal cluster registrato. NetApp consiglia di utilizzare un file kubeconfig con nome utente e password per registrare i cluster OpenShift su Astra Control Center.

2. Astra Control Center rileva le classi di storage idonee. Selezionare ora il modo in cui lo storageclass effettua il provisioning dei volumi utilizzando Trident supportato da una SVM su NetApp ONTAP e fare clic su Review (esamina). Nel riquadro successivo, verificare i dettagli e fare clic su Add Cluster (Aggiungi cluster).

## STORAGE

Existing storage classes are discovered and verified as eligible for use with Astra Control. You can use your existing default, or choose to set a new default at this time.  
Applications with persistent volumes on eligible storage classes are validated for use with Astra Control.

| Set default                      | Storage class                      | Storage provisioner          | Reclaim policy | Binding mode | Eligible |
|----------------------------------|------------------------------------|------------------------------|----------------|--------------|----------|
| <input checked="" type="radio"/> | ocp-trident <small>Default</small> | csi.trident.netapp.io        | Delete         | Immediate    |          |
| <input type="radio"/>            | ocp-trident-iscsi                  | csi.trident.netapp.io        | Delete         | Immediate    |          |
| <input type="radio"/>            | project-1-sc                       | csi.trident.netapp.io        | Delete         | Immediate    |          |
| <input type="radio"/>            | thin                               | kubernetes.io/vsphere-volume | Delete         | Immediate    |          |

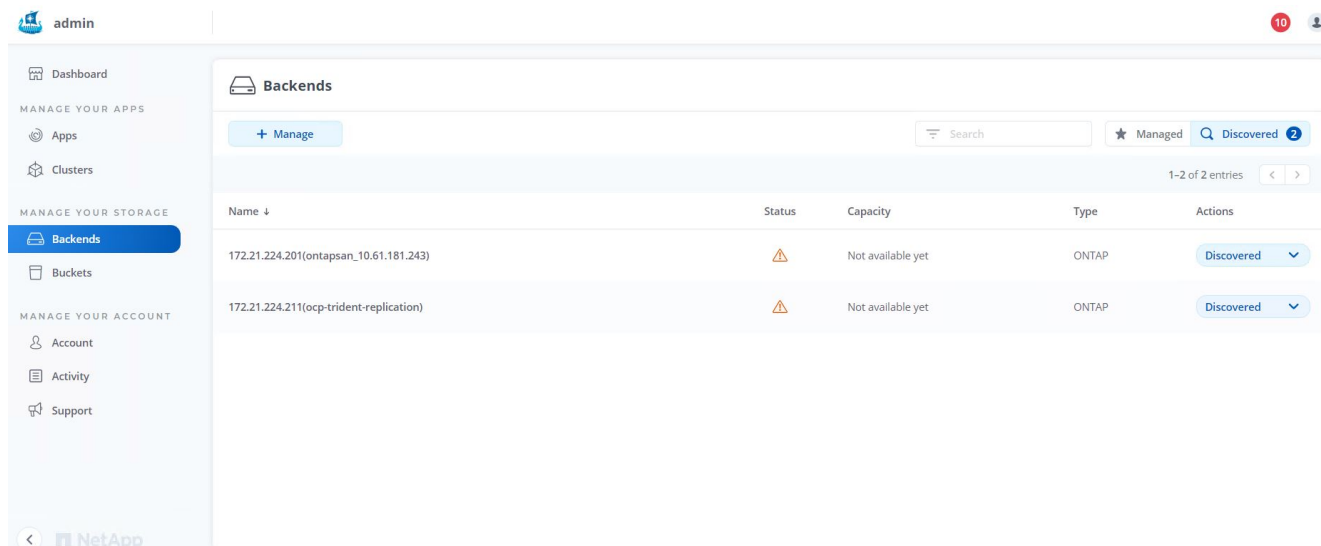
[← Select credentials](#)
[Review →](#)

3. Registrare entrambi i cluster OpenShift come descritto al punto 1. Una volta aggiunti, i cluster passano allo stato di rilevamento mentre Astra Control Center li ispeziona e installa gli agenti necessari. Lo stato del cluster diventa in esecuzione dopo che sono stati registrati correttamente.



Tutti i cluster Red Hat OpenShift che devono essere gestiti da Astra Control Center devono avere accesso al registro delle immagini utilizzato per l'installazione, poiché gli agenti installati sui cluster gestiti estraggono le immagini da tale registro.

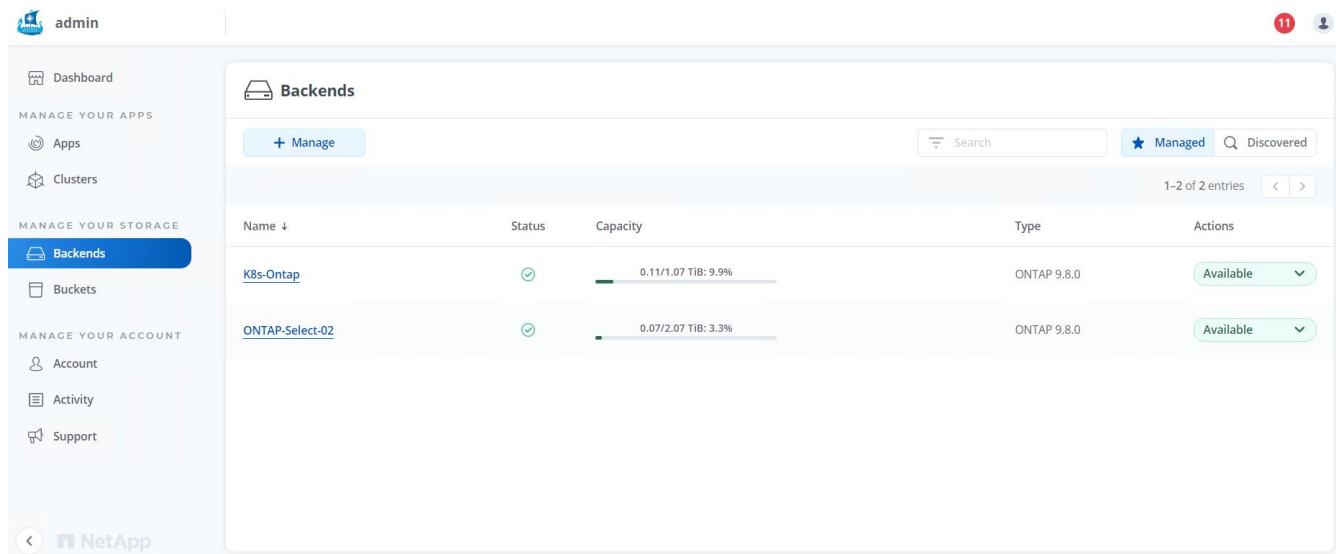
4. Importa i cluster ONTAP come risorse storage da gestire come back-end dal centro di controllo Astra. Quando i cluster OpenShift vengono aggiunti ad Astra e viene configurato uno storageclass, il cluster ONTAP viene automaticamente ispezionato e ispezionato per il backup dello storageclass, ma non viene importato nel centro di controllo Astra da gestire.



5. Per importare i cluster ONTAP, accedere a Backend, fare clic sul menu a discesa e selezionare Manage (Gestisci) accanto al cluster ONTAP da gestire. Immettere le credenziali del cluster ONTAP, fare clic su informazioni di revisione, quindi fare clic su Importa backend storage.

6. Una volta aggiunti i backend, lo stato diventa disponibile. Questi backend ora dispongono delle informazioni sui volumi persistenti nel cluster OpenShift e sui volumi corrispondenti nel sistema ONTAP.





- Per il backup e il ripristino tra cluster OpenShift utilizzando Astra Control Center, è necessario eseguire il provisioning di un bucket di storage a oggetti che supporti il protocollo S3. Le opzioni attualmente supportate sono ONTAP S3, StorageGRID e AWS S3. Ai fini di questa installazione, configureremo un bucket AWS S3. Accedere a Bucket, fare clic su Add bucket (Aggiungi bucket) e selezionare Generic S3. Inserisci i dettagli sul bucket S3 e le credenziali per accedervi, fai clic sulla casella di controllo "Rendi questo bucket il bucket predefinito per il cloud", quindi fai clic su Aggiungi.

**Add bucket**
×

**STORAGE BUCKET**

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type

Generic S3

Existing bucket name

ocp-vmware2-astra-cc

Description (optional)

S3 server name or IP address

s3.us-east-1.amazonaws.com

☒ Make this bucket the default bucket for this cloud

**SELECT CREDENTIALS**

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.

Add

Use existing

Access ID

AMWSI7CFKDSU6HWSZXABD

Secret key

.....

Credential name

AWS-S3

Cancel

Add ✓

**ADDING STORAGE BUCKETS**

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

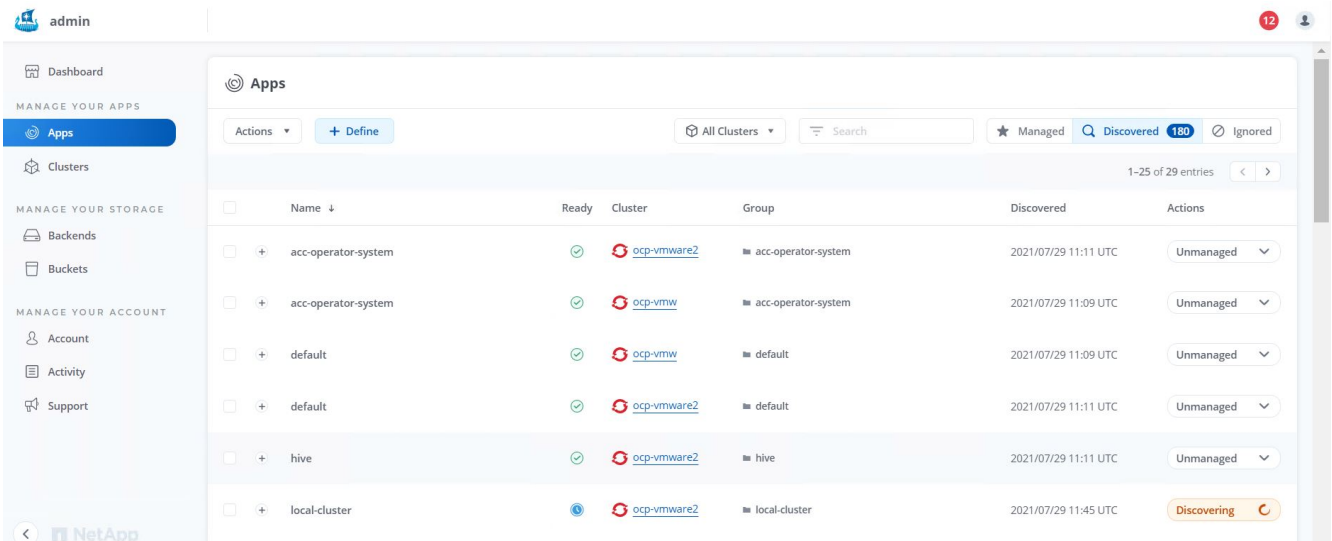
Read more in [storage buckets](#).

## Scegliere le applicazioni da proteggere

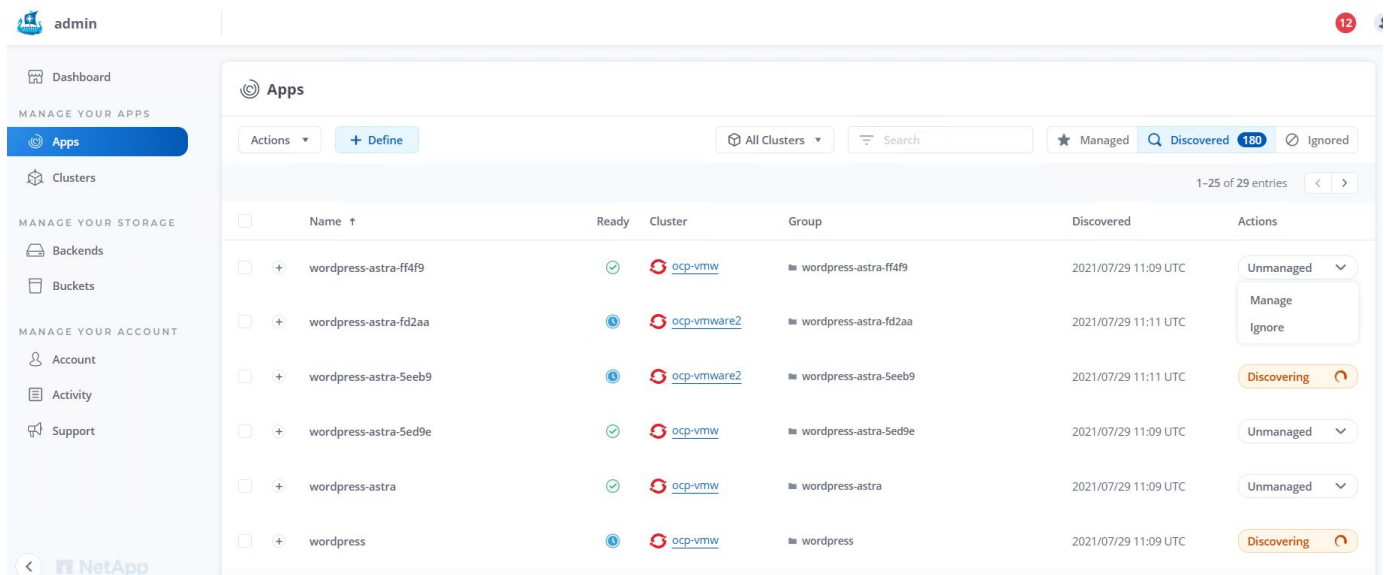
Dopo aver registrato i cluster Red Hat OpenShift, è possibile individuare le applicazioni implementate e gestirle tramite Astra Control Center.

## Gestire le applicazioni

1. Una volta registrati i cluster OpenShift e i backend ONTAP con il centro di controllo Astra, il centro di controllo inizia automaticamente a rilevare le applicazioni in tutti gli spazi dei nomi che utilizzano lo storageclass configurato con il backend ONTAP specificato.



2. Accedere a Apps > Discovered (applicazioni > rilevate) e fare clic sul menu a discesa accanto all'applicazione che si desidera gestire utilizzando Astra. Quindi fare clic su Manage (Gestisci)



1. L'applicazione entra nello stato Available (disponibile) e può essere visualizzata nella scheda Managed (gestito) nella sezione Apps (applicazioni).

Apps

Actions

+ Define

All Clusters

Search

★ Managed

Discovered

175

Ignored

1-1 of 1 entries

| <input type="checkbox"/> | Name                                  | Ready       | Protected   | Cluster             | Group                             | Discovered           | Actions              |
|--------------------------|---------------------------------------|-------------|-------------|---------------------|-----------------------------------|----------------------|----------------------|
| <input type="checkbox"/> | <a href="#">wordpress-astra-ff4f9</a> | <div></div> | <div></div> | <div></div> ocp-vmw | <div></div> wordpress-astra-ff4f9 | 2021/07/29 11:09 UTC | <div>Available</div> |

## Proteggi le tue applicazioni

Una volta gestiti i carichi di lavoro delle applicazioni da Astra Control Center, è possibile configurare le impostazioni di protezione per tali carichi di lavoro.

## Creazione di un'istantanea dell'applicazione

Un'istantanea di un'applicazione crea una copia Snapshot di ONTAP che può essere utilizzata per ripristinare o clonare l'applicazione in un momento specifico in base a tale copia Snapshot.

1. Per creare un'istantanea dell'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione di cui si desidera creare una copia Snapshot. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Snapshot.

APPLICATION STATUS
 

Healthy

APPLICATION PROTECTION STATUS
 

Unprotected

Images

docker.io/bitnami/mariadb:10.5.13-debian-10-r58  
 docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule

Disabled

Group

■ wp

Cluster

Running ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. Inserire i dettagli dell'istantanea, fare clic su Next (Avanti), quindi su Snapshot (istantanea). La creazione dello snapshot richiede circa un minuto e lo stato diventa disponibile dopo la creazione dello snapshot.

109

## SNAPSHOT DETAILS

Name  
wp-snapshot-20220228185949

## CREATING APPLICATION SNAPSHOTS

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#).

Application  
wp

Namespace  
wp

Cluster  
ocp-vmw

Cancel

Next →

## Creazione di un backup dell'applicazione

Un backup di un'applicazione acquisisce lo stato attivo dell'applicazione e la configurazione delle risorse IT, le taglia in file e le memorizza in un bucket di storage a oggetti remoto.

Per il backup e il ripristino delle applicazioni gestite nel centro di controllo Astra, è necessario configurare le impostazioni del superutente per i sistemi ONTAP di backup come prerequisito. A tale scopo, immettere i seguenti comandi.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname  
default -ruleindex 1 -superuser sys  
ONTAP::> export-policy rule modify -policyname default -ruleindex 1 -anon  
65534 -vserver ocp-trident
```

1. Per creare un backup dell'applicazione gestita in Astra Control Center, accedere alla scheda Apps (applicazioni) > Managed (gestite) e fare clic sull'applicazione di cui si desidera eseguire il backup. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Backup.



APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Running

- Snapshot
- Backup
- Clone
- Restore
- Unmanage

Images  
docker.io/bitnami/mariadb:10.5.13-debian-10-r58  
docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule  
Disabled

Group  
wp

Cluster  
ocp-vmw

2. Inserire i dettagli del backup, selezionare il bucket di storage a oggetti in cui memorizzare i file di backup, fare clic su Next (Avanti) e, dopo aver esaminato i dettagli, fare clic su Backup (Backup). A seconda delle dimensioni dell'applicazione e dei dati, il backup può richiedere alcuni minuti e lo stato del backup diventa disponibile una volta completato correttamente il backup.

Backup application

STEP 1/2: DETAILS

X

BACKUP DETAILS

Name

wp-backup

☐ Backup from an existing snapshot

BACKUP DESTINATION

Bucket

na-ocp-astra/na-ocp-acc Available

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#).

Application

wp

Namespace

wp

Cluster

ocp-vmw

Cancel

Next →

## Ripristino di un'applicazione

Con la semplice pressione di un pulsante, è possibile ripristinare un'applicazione nello spazio dei nomi di origine nello stesso cluster o in un cluster remoto per la protezione delle applicazioni e il disaster recovery.

1. Per ripristinare un'applicazione, selezionare Apps (applicazioni) > Managed Tab (scheda gestita) e fare clic sull'applicazione in questione. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Restore.

wp

Running

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Partially protected

Images

docker.io/bitnami/mariadb:10.5.13-debian-10-r58

docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule

Disabled

Group

wp

Cluster

ocp-vmw

Snapshot

Backup

Clone

Restore

Unmanage

2. Immettere il nome dello spazio dei nomi di ripristino, selezionare il cluster in cui si desidera ripristinarlo e scegliere se si desidera ripristinarlo da uno snapshot esistente o da un backup dell'applicazione. Fare clic su Avanti.

Restore application

STEP 1/2: DETAILS

RESTORE DETAILS

Destination cluster

ocp-vmw

Destination namespace

wp

RESTORE SOURCE

Filter

Snapshots

Backups

| Application backup | Ready | On-Schedule/On-Demand | Created ↑            |
|--------------------|-------|-----------------------|----------------------|
| wp-backup          | ✓     | On-Demand             | 2022/02/28 18:54 UTC |

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

- Application wp
- Namespace wp
- Cluster ocp-vmw

Cancel

Next →

- Nel riquadro di revisione, immettere `restore` E fare clic su Restore (Ripristina) dopo aver esaminato i dettagli.

Restore application

STEP 2/2: SUMMARY

REVIEW RESTORE INFORMATION

⚠

All existing resources associated with this application will be deleted and replaced with the source backup "wp-backup" taken on 2022/02/28 18:54 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this application may be impacted.

We recommend taking a snapshot or a backup of your application before proceeding.

BACKUP

wp-backup

ORIGINAL GROUP

wp

ORIGINAL CLUSTER

ocp-vmw

RESOURCE LABELS

ClusterRole

kubernetes.io/bootstrapping: rbac-defaults +1

ClusterRoleBinding

RESTORE

wp

DESTINATION GROUP

wp

DESTINATION CLUSTER

ocp-vmw

RESOURCE LABELS

ClusterRole

kubernetes.io/bootstrapping: rbac-defaults +1

ClusterRoleBinding

Are you sure you want to restore the application "wp"?

Type **restore** below to confirm.

Confirm to restore

restore

← Back

Restore ✓

- La nuova applicazione passa allo stato di ripristino mentre Astra Control Center ripristina l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).

Actions ▾

+ Define

▾

Search

★

🔍

110

🗑

🔄

1-1 of 1 entries

<


>


| <input type="checkbox"/> | Name ↓             | Ready | Protected                          | Cluster                                  | Group                               | Discovered           | Actions                           |
|--------------------------|--------------------|-------|------------------------------------|--|-------------------------------------|----------------------|-----------------------------------|
| <input type="checkbox"/> | <a href="#">wp</a> | ✔     | <div><div></div><div>i</div></div> | <div><div></div><div>ocp-vmw</div></div> | <div><div></div><div>wp</div></div> | 2022/02/28 18:34 UTC | <div>Available</div> <div>▾</div> |


## Clonare un'applicazione


È possibile clonare un'applicazione nel cluster di origine o in un cluster remoto per scopi di sviluppo/test o protezione dell'applicazione e disaster recovery. La clonazione di un'applicazione all'interno dello stesso cluster sullo stesso backend di storage utilizza la tecnologia NetApp FlexClone, che clona i PVC all'istante e consente di risparmiare spazio di storage.


1. Per clonare un'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione in questione. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Clone (Clona).

 wp

 APPLICATION STATUS


 Healthy


 APPLICATION PROTECTION STATUS


 Partially protected

Images  
 docker.io/bitnami/mariadb:10.5.13-debian-10-r58  
 docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule  
 Disabled


Group  
 wp

Cluster  



Running 

Snapshot  
 Backup  
**Clone**  
 Restore  
 Unmanage

2. Immettere i dettagli del nuovo spazio dei nomi, selezionare il cluster in cui si desidera clonarlo e scegliere se clonarlo da uno snapshot esistente o da un backup o dallo stato corrente dell'applicazione. Quindi, fare clic su Next (Avanti) e su Clone on review pane (Clona sul pannello di revisione) dopo aver esaminato i dettagli.

 Clone application


STEP 1/2: DETAILS



CLONE DETAILS

Clone name  
 wp-clone

Clone namespace  
 wp-clone


Destination cluster  
 ocp-vmw


☐ Clone from an existing snapshot or backup


CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Read more in [Clone applications](#)

 Application  
wp

 Namespace  
wp


 Cluster  
ocp-vmw

Cancel

Next →





3. La nuova applicazione passa allo stato di rilevamento mentre Astra Control Center crea l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).

 **Applications**

Actions ▾ + Define 📦 ▾ 🔍 Search ★ 🔍 110 🔗

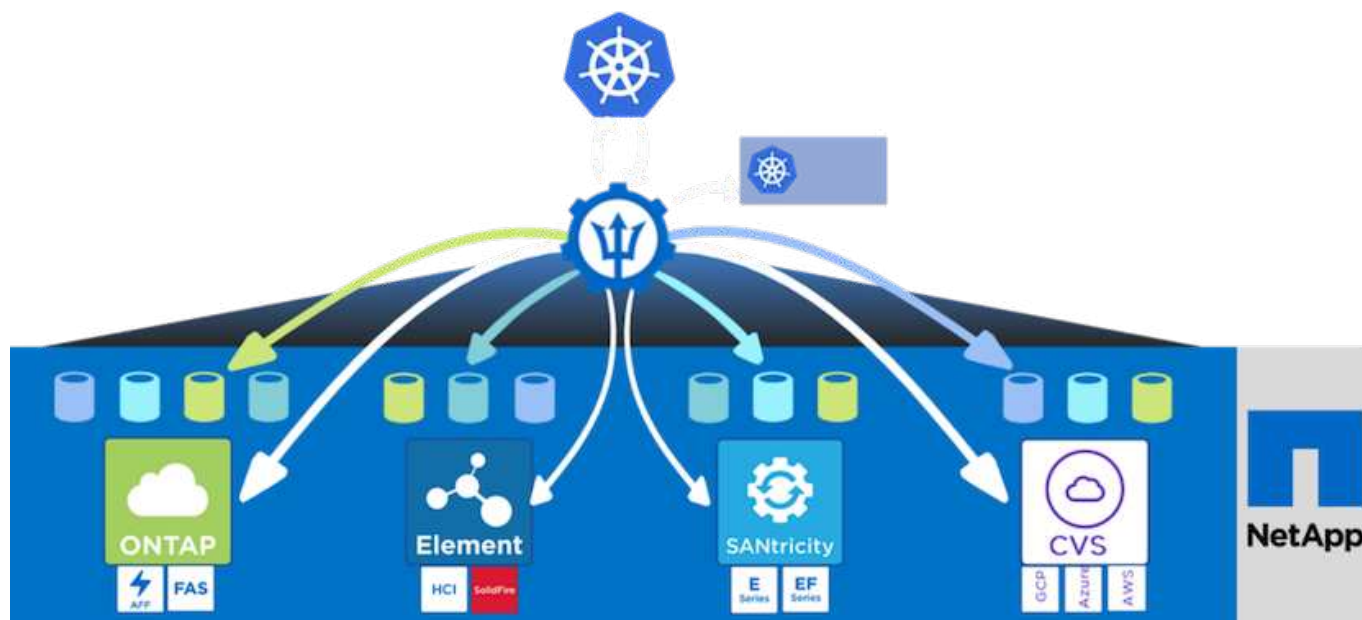
🔄 1-2 of 2 entries < >

| <input type="checkbox"/> | Name ↓                   | Ready | Protected      | Cluster   | Group    | Discovered           | Actions     |
|--------------------------|--------------------------|-------|----------------|---|----------|----------------------|-------------|
| <input type="checkbox"/> | <a href="#">wp</a>       | ✓     | <span>i</span> |  <a href="#">ocp-vmw</a> | wp       | 2022/02/28 18:34 UTC | Available ▾ |
| <input type="checkbox"/> | <a href="#">wp-clone</a> | ✓     | <span>⚠</span> |  <a href="#">ocp-vmw</a> | wp-clone | 2022/02/28 19:21 UTC | Available ▾ |

## Panoramica di Astra Trident

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, incluso Red Hat OpenShift. Trident lavora con l'intero portfolio di storage NetApp, inclusi i sistemi storage NetApp ONTAP ed Element, e supporta anche connessioni NFS e iSCSI. Trident accelera il workflow DevOps consentendo agli utenti finali di eseguire il provisioning e gestire lo storage dai sistemi storage NetApp senza richiedere l'intervento di un amministratore dello storage.

Un amministratore può configurare una serie di backend di storage in base alle esigenze di progetto e ai modelli di sistemi di storage che consentono funzionalità di storage avanzate, tra cui compressione, tipi di dischi specifici o livelli di QoS che garantiscono un certo livello di performance. Una volta definiti, questi backend possono essere utilizzati dagli sviluppatori nei loro progetti per creare dichiarazioni di volume persistenti (PVC) e per collegare storage persistente ai propri container on-demand.



Astra Trident ha un rapido ciclo di sviluppo e, proprio come Kubernetes, viene rilasciato quattro volte all'anno.

L'ultima versione di Astra Trident è la 22.01 rilasciata a gennaio 2022. Matrice di supporto per quale versione



di Trident è stata testata con la quale è possibile trovare la distribuzione Kubernetes "qui".

A partire dalla versione 20.04, l'impostazione di Trident viene eseguita dall'operatore Trident. L'operatore semplifica le implementazioni su larga scala e fornisce supporto aggiuntivo, inclusa la riparazione automatica dei pod implementati nell'installazione di Trident.

Con la versione 21.01, è stato reso disponibile un grafico Helm per facilitare l'installazione dell'operatore Trident.

### Scarica Astra Trident

Per installare Trident sul cluster di utenti implementato ed eseguire il provisioning di un volume persistente, attenersi alla seguente procedura:

1. Scaricare l'archivio di installazione sulla workstation di amministrazione ed estrarre il contenuto. La versione corrente di Trident è la 22.01, che può essere scaricata "qui".

```
[netapp-user@rhel7 ~]$ wget
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
--2021-05-06 15:17:30--
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
[following]
--2021-05-06 15:17:30-- https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
```

```

22.01.0.tar.gz&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com (github-
releases.githubusercontent.com)... 185.199.108.154, 185.199.109.154,
185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-
releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38349341 (37M) [application/octet-stream]
Saving to: 'trident-installer-22.01.0.tar.gz'

100%[=====
=====>] 38,349,341  88.5MB/s
in 0.4s

2021-05-06 15:17:30 (88.5 MB/s) - 'trident-installer-22.01.0.tar.gz'
saved [38349341/38349341]

```

## 2. Estrarre l'installazione di Trident dal bundle scaricato.

```

[netapp-user@rhel7 ~]$ tar -xzf trident-installer-22.01.0.tar.gz
[netapp-user@rhel7 ~]$ cd trident-installer/
[netapp-user@rhel7 trident-installer]$

```

### Installare l'operatore Trident con Helm

1. Innanzitutto, impostare la posizione del cluster utente `kubeconfig` File come variabile di ambiente in modo da non doverla fare riferimento, perché Trident non ha alcuna opzione per passare questo file.

```

[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/.ocp-
install/auth/kubeconfig

```

2. Eseguire il comando Helm per installare l'operatore Trident dal tarball nella directory `helm` durante la creazione dello spazio dei nomi Trident nel cluster di utenti.

```
[netapp-user@rhel7 trident-installer]$ helm install trident
helm/trident-operator-22.01.0.tgz --create-namespace --namespace trident
NAME: trident
LAST DEPLOYED: Fri May  7 12:54:25 2021
NAMESPACE: trident
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Thank you for installing trident-operator, which will deploy and manage
NetApp's Trident CSI
storage provisioner for Kubernetes.

Your release is named 'trident' and is installed into the 'trident'
namespace.
Please note that there must be only one instance of Trident (and
trident-operator) in a Kubernetes cluster.

To configure Trident to manage storage resources, you will need a copy
of tridentctl, which is
available in pre-packaged Trident releases. You may find all Trident
releases and source code
online at https://github.com/NetApp/trident.

To learn more about the release, try:

$ helm status trident
$ helm get all trident
```

3. È possibile verificare che Trident sia installato correttamente controllando i pod in esecuzione nello spazio dei nomi o utilizzando il binario tridentctl per controllare la versione installata.

```
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
```

| NAME                             | READY | STATUS  | RESTARTS | AGE |
|----------------------------------|-------|---------|----------|-----|
| trident-csi-5z45l                | 1/2   | Running | 2        | 30s |
| trident-csi-696b685cf8-htdb2     | 6/6   | Running | 0        | 30s |
| trident-csi-b74p2                | 2/2   | Running | 0        | 30s |
| trident-csi-lrw4n                | 2/2   | Running | 0        | 30s |
| trident-operator-7c748d957-gr2gw | 1/1   | Running | 0        | 36s |

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
```

```
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0       | 22.01.0       |
+-----+-----+
```



In alcuni casi, gli ambienti dei clienti potrebbero richiedere la personalizzazione dell'implementazione di Trident. In questi casi, è anche possibile installare manualmente l'operatore Trident e aggiornare i manifesti inclusi per personalizzare l'implementazione.

### Installare manualmente l'operatore Trident

1. Innanzitutto, impostare la posizione del cluster utente `kubeconfig` File come variabile di ambiente in modo da non doverla fare riferimento, perché Trident non ha alcuna opzione per passare questo file.

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/.ocp-
install/auth/kubeconfig
```

2. Il `trident-installer` la `directory` contiene i manifesti per la definizione di tutte le risorse richieste. Utilizzando i manifesti appropriati, creare `TridentOrchestrator` definizione personalizzata delle risorse.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
customresourcedefinition.apiextensions.k8s.io/tridentorchestrators.tride
nt.netapp.io created
```

3. Se non ne esiste uno, creare uno spazio dei nomi Trident nel cluster utilizzando il manifesto fornito.

```
[netapp-user@rhel7 trident-installer]$ oc apply -f deploy/namespace.yaml
namespace/trident created
```

4. Creare le risorse necessarie per l'implementazione dell'operatore Trident, ad esempio un `ServiceAccount` per l'operatore, un `ClusterRole` e `ClusterRoleBinding` al `ServiceAccount`, un

dedicato `PodSecurityPolicy` o l'operatore stesso.

```
[netapp-user@rhel7 trident-installer]$ oc create -f deploy/bundle.yaml
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

5. È possibile controllare lo stato dell'operatore dopo l'implementazione con i seguenti comandi:

```
[netapp-user@rhel7 trident-installer]$ oc get deployment -n trident
NAME                READY   UP-TO-DATE   AVAILABLE   AGE
trident-operator    1/1     1             1           23s
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-operator-66f48895cc-lzczk  1/1     Running   0           41s
```

6. Con l'implementazione dell'operatore, ora possiamo utilizzarlo per installare Trident. Per eseguire questa operazione, è necessario creare un `TridentOrchestrator`.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created
[netapp-user@rhel7 trident-installer]$ oc describe torc trident
Name:                trident
Namespace:
Labels:               <none>
Annotations:          <none>
API Version:          trident.netapp.io/v1
Kind:                 TridentOrchestrator
Metadata:
  Creation Timestamp:  2021-05-07T17:00:28Z
  Generation:          1
  Managed Fields:
    API Version:        trident.netapp.io/v1
    Fields Type:        FieldsV1
    fieldsV1:
      f:spec:
        ..
        f:debug:
        f:namespace:
  Manager:             kubectl-create
  Operation:            Update
```

```

Time:          2021-05-07T17:00:28Z
API Version:   trident.netapp.io/v1
Fields Type:   FieldsV1
fieldsV1:
  f:status:
    .:
    f:currentInstallationParams:
      .:
      f:IPv6:
      f:autosupportHostname:
      f:autosupportImage:
      f:autosupportProxy:
      f:autosupportSerialNumber:
      f:debug:
      f:enableNodePrep:
      f:imagePullSecrets:
      f:imageRegistry:
      f:k8sTimeout:
      f:kubeletDir:
      f:logFormat:
      f:silenceAutosupport:
      f:tridentImage:
    f:message:
    f:namespace:
    f:status:
    f:version:
  Manager:      trident-operator
  Operation:    Update
  Time:         2021-05-07T17:00:28Z
  Resource Version: 931421
  Self Link:
/apis/trident.netapp.io/v1/tridentorchestrators/trident
  UID:          8a26a7a6-dde8-4d55-9b66-a7126754d81f
Spec:
  Debug:        true
  Namespace:    trident
Status:
  Current Installation Params:
    IPv6:          false
    Autosupport Hostname:
    Autosupport Image:      netapp/trident-autosupport:21.01
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:              true
    Enable Node Prep:    false
    Image Pull Secrets:

```

```

Image Registry:
k8sTimeout:      30
Kubelet Dir:     /var/lib/kubelet
Log Format:      text
Silence Autosupport: false
Trident Image:   netapp/trident:22.01.0
Message:         Trident installed
Namespace:       trident
Status:          Installed
Version:         v22.01.0

Events:
  Type    Reason          Age   From                      Message
  ----    -
Normal    Installing      80s   trident-operator.netapp.io Installing
Trident
Normal    Installed       68s   trident-operator.netapp.io Trident
installed

```

7. È possibile verificare che Trident sia installato correttamente controllando i pod in esecuzione nello spazio dei nomi o utilizzando il binario `tridentctl` per controllare la versione installata.

```

[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-csi-bb64c6cb4-lmd6h        6/6     Running   0           82s
trident-csi-gn59q                   2/2     Running   0           82s
trident-csi-m4szj                   2/2     Running   0           82s
trident-csi-sb9k9                   2/2     Running   0           82s
trident-operator-66f48895cc-lzczk   1/1     Running   0           2m39s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0       | 22.01.0       |
+-----+-----+

```

## Preparare i nodi di lavoro per lo storage

### NFS

La maggior parte delle distribuzioni Kubernetes viene fornita con i pacchetti e le utility per montare i backend NFS installati di default, incluso Red Hat OpenShift.

Tuttavia, per NFSv3, non esiste alcun meccanismo per negoziare la concorrenza tra il client e il server. Pertanto, il numero massimo di voci della tabella degli slot `sunrpc` lato client deve essere sincronizzato manualmente con il valore supportato sul server per garantire le migliori prestazioni per la connessione NFS

senza che il server debba ridurre le dimensioni della finestra della connessione.

Per ONTAP, il numero massimo supportato di voci della tabella degli slot sunrpc è 128, ovvero ONTAP può gestire 128 richieste NFS simultanee alla volta. Tuttavia, per impostazione predefinita, Red Hat CoreOS/Red Hat Enterprise Linux ha un massimo di 65,536 voci della tabella degli slot sunrpc per connessione. È necessario impostare questo valore su 128 e questo può essere fatto usando Machine Config Operator (MCO) in OpenShift.

Per modificare il numero massimo di voci della tabella degli slot sunrpc nei nodi di lavoro OpenShift, attenersi alla seguente procedura:

1. Accedere alla console Web di OCP e selezionare Compute > Machine Configs (calcolo > configurazioni macchina). Fare clic su Create Machine Config. Copiare e incollare il file YAML e fare clic su Create (Crea).

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 98-worker-nfs-rpc-slot-tables
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=utf-8;base64,b3B0aW9ucyBzdW5ycGMgdGNwX21heF9zbG90X3RhYmxlX2VudHJpZXM9MTI4Cg==
            filesystem: root
            mode: 420
            path: /etc/modprobe.d/sunrpc.conf
```

2. Dopo aver creato l'MCO, la configurazione deve essere applicata a tutti i nodi di lavoro e riavviata uno alla volta. L'intero processo richiede da 20 a 30 minuti circa. Verificare se la configurazione del computer viene applicata utilizzando `oc get mcp` e assicurarsi che il pool di configurazione del computer per i lavoratori sia aggiornato.

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
```

| NAME     | CONFIG                                   | UPDATED | UPDATING |
|----------|--|---------|----------|
| DEGRADED |  |         |          |
| master   | rendered-master-a520ae930e1d135e0dee7168 | True    | False    |
| False    |  |         |          |
| worker   | rendered-worker-de321b36eeba62df41feb7bc | True    | False    |
| False    |  |         |          |



## ISCSI

Per preparare i nodi di lavoro per consentire la mappatura dei volumi di storage a blocchi tramite il protocollo iSCSI, è necessario installare i pacchetti necessari per supportare tale funzionalità.

In Red Hat OpenShift, questo viene gestito applicando un MCO (Machine Config Operator) al cluster dopo averlo implementato.

Per configurare i nodi di lavoro per l'esecuzione dei servizi iSCSI, attenersi alla seguente procedura:

1. Accedere alla console Web di OCP e selezionare Compute > Machine Configs (calcolo > configurazioni macchina). Fare clic su Create Machine Config. Copiare e incollare il file YAML e fare clic su Create (Crea).

Quando non si utilizza il multipathing:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-worker-element-iscsi
spec:
  config:
    ignition:
      version: 3.2.0
    systemd:
      units:
        - name: iscsid.service
          enabled: true
          state: started
  osImageURL: ""
```

Quando si utilizza il multipathing:

```

apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 99-worker-ontap-iscsi
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
      - contents:
          source: data:text/plain;charset=utf-8;base64,ZGVmYXVsdHMgewogICAgICAgIHVzZXJfZnJpZW5kbHlfbmFtZXMgYm8KICAgICAgICBmaW5kX211bHRpcGF0aHMgYm8KfQoKYmxhY2tsaXN0X2V4Y2VwdGlvbnMgewogICAgICAgIHByb3BlcnR5ICIoU0NTSV9JREV0VF98SURfV1dOKSikfQoKYmxhY2tsaXN0IHsKfQoK
          verification: {}
        filesystem: root
        mode: 400
        path: /etc/multipath.conf
    systemd:
      units:
      - name: iscsid.service
        enabled: true
        state: started
      - name: multipathd.service
        enabled: true
        state: started
  osImageURL: ""

```

2. Una volta creata la configurazione, sono necessari circa 20 - 30 minuti per applicarla ai nodi di lavoro e ricaricarla. Verificare se la configurazione del computer viene applicata utilizzando `oc get mcp` e assicurarsi che il pool di configurazione del computer per i lavoratori sia aggiornato. È inoltre possibile accedere ai nodi di lavoro per confermare che il servizio `iscsid` è in esecuzione (e il servizio `multipath` è in esecuzione se si utilizza il `multipathing`).

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME          CONFIG                                UPDATED    UPDATING
DEGRADED
master        rendered-master-a520ae930e1d135e0dee7168    True       False
False
worker        rendered-worker-de321b36eeba62df41feb7bc    True       False
False

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status iscsid
● iscsid.service - Open-iSCSI
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; enabled;
   vendor preset: disabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
     Docs: man:iscsid(8)
           man:iscsiadm(8)
  Main PID: 1242 (iscsid)
    Status: "Ready to process requests"
     Tasks: 1
   Memory: 4.9M
      CPU: 9ms
   CGroup: /system.slice/iscsid.service
           └─1242 /usr/sbin/iscsid -f

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status multipathd
● multipathd.service - Device-Mapper Multipath Device Controller
   Loaded: loaded (/usr/lib/systemd/system/multipathd.service; enabled;
   vendor preset: enabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
  Main PID: 918 (multipathd)
    Status: "up"
     Tasks: 7
   Memory: 13.7M
      CPU: 57ms
   CGroup: /system.slice/multipathd.service
           └─918 /sbin/multipathd -d -s
```



È inoltre possibile confermare che MachineConfig sia stato applicato correttamente e che i servizi siano stati avviati come previsto eseguendo il `oc debug` con i flag appropriati.

### Creazione di backend per il sistema storage

Dopo aver completato l'installazione di Astra Trident Operator, è necessario configurare il backend per la piattaforma di storage NetApp specifica in uso. Seguire i collegamenti riportati di seguito per continuare

l'installazione e la configurazione di Astra Trident.

- ["NetApp ONTAP NFS"](#)
- ["ISCSI NetApp ONTAP"](#)
- ["ISCSI NetApp Element"](#)

### Configurazione NFS di NetApp ONTAP

Per consentire l'integrazione di Trident con il sistema storage NetApp ONTAP, è necessario creare un backend che consenta la comunicazione con il sistema storage.

1. Nell'archivio di installazione scaricato in sono disponibili file backend di esempio `sample-input` gerarchia di cartelle. Per i sistemi NetApp ONTAP che servono NFS, copiare il `backend-ontap-nas.json` nella directory di lavoro e modificare il file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-samples/ontap-nas/backend-ontap-nas.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-nas.json
```

2. Modificare il `backendName`, `managementLIF`, `dataLIF`, `svm`, nome utente, e password in questo file.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "password"
}
```



È consigliabile definire il valore `backendName` personalizzato come combinazione di `storageDriverName` e `dataLIF` che fornisce NFS per una facile identificazione.

3. Una volta creato questo file di back-end, eseguire il comando seguente per creare il primo backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-nas.json
```

| NAME                    | STATE  | VOLUMES | STORAGE DRIVER | UUID                                 |
|-------------------------|--------|---------|----------------|--------------------------------------|
| ontap-nas+10.61.181.221 | online | 0       | ontap-nas      | be7a619d-c81d-445c-b80c-5c87a73c5b1e |

- Una volta creato il backend, è necessario creare una classe di storage. Come per il backend, esiste un file di esempio della classe di storage che può essere modificato per l'ambiente disponibile nella cartella di input di esempio. Copiarlo nella directory di lavoro e apportare le modifiche necessarie per riflettere il backend creato.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.template ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

- L'unica modifica che deve essere apportata a questo file è definire `backendType` valore al nome del driver di storage dal backend appena creato. Annotare anche il valore del campo `nome`, a cui si deve fare riferimento in un passaggio successivo.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```



Esiste un campo opzionale chiamato `fsType` definito in questo file. Questa riga può essere eliminata nei backend NFS.

- Eseguire `oc` per creare la classe di storage.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

- Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). C'è un esempio `pvc-basic.yaml` file che può essere utilizzato per eseguire questa azione, disponibile anche in input di esempio.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

- L'unica modifica che deve essere apportata a questo file è garantire che il `storageClassName` il campo corrisponde a quello appena creato. La definizione PVC può essere ulteriormente personalizzata in base alle esigenze del carico di lavoro da fornire.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

- Creare il PVC emettendo il `oc` comando. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
basic      Bound       pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d  1Gi
RWO                                     basic-csi      7s
```

## Configurazione iSCSI di NetApp ONTAP

Per consentire l'integrazione di Trident con il sistema storage NetApp ONTAP, è necessario creare un backend che consenta la comunicazione con il sistema storage.

- Nell'archivio di installazione scaricato in sono disponibili file backend di esempio `sample-input` gerarchia di cartelle. Per i sistemi NetApp ONTAP che utilizzano iSCSI, copiare il `backend-ontap-san.json` nella directory di lavoro e modificare il file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/ontap-san/backend-ontap-san.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-san.json
```

2. Modificare i valori di gestione LIF, dataLIF, svm, nome utente e password in questo file.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.240",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```

3. Una volta creato questo file di back-end, eseguire il comando seguente per creare il primo backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES | |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontapsan_10.61.181.241 | ontap-san      | 6788533c-7fea-4a35-b797-
fb9bb3322b91 | online |          0 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

4. Una volta creato il backend, è necessario creare una classe di storage. Come per il backend, esiste un file di esempio della classe di storage che può essere modificato per l'ambiente disponibile nella cartella di input di esempio. Copiarlo nella directory di lavoro e apportare le modifiche necessarie per riflettere il backend creato.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. L'unica modifica che deve essere apportata a questo file è definire `backendType` valore al nome del driver di storage dal backend appena creato. Annotare anche il valore del campo `nome`, a cui si deve fare riferimento in un passaggio successivo.

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"

```



Esiste un campo opzionale chiamato `fsType` definito in questo file. Nei backend iSCSI, questo valore può essere impostato su un tipo di filesystem Linux specifico (XFS, ext4, ecc.) o può essere cancellato per consentire a OpenShift di decidere quale filesystem usare.

## 6. Eseguire `oc` per creare la classe di storage.

```

[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created

```

## 7. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). C'è un esempio `pvc-basic.yaml` file che può essere utilizzato per eseguire questa azione, disponibile anche in input di esempio.

```

[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-
basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml

```

## 8. L'unica modifica che deve essere apportata a questo file è garantire che il `storageClassName` il campo corrisponde a quello appena creato. La definizione PVC può essere ulteriormente personalizzata in base alle esigenze del carico di lavoro da fornire.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi

```

## 9. Creare il PVC emettendo il `oc` comando. La creazione può richiedere del tempo a seconda delle



dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS  AGE
basic       Bound       pvc-7ceac1ba-0189-43c7-8f98-094719f7956c  1Gi
RWO           basic-csi     3s
```

### Configurazione iSCSI NetApp Element

Per abilitare l'integrazione di Trident con il sistema storage NetApp Element, è necessario creare un backend che consenta la comunicazione con il sistema storage utilizzando il protocollo iSCSI.

1. Nell'archivio di installazione scaricato in sono disponibili file backend di esempio `sample-input` gerarchia di cartelle. Per i sistemi NetApp Element che utilizzano iSCSI, copiare `backend-solidfire.json` nella directory di lavoro e modificare il file.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/solidfire/backend-solidfire.json ./
[netapp-user@rhel7 trident-installer]$ vi ./backend-solidfire.json
```

- a. Modificare i valori di utente, password e MVIP su `EndPoint` linea.
- b. Modificare il `SVIP` valore.

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://trident:password@172.21.224.150/json-
rpc/8.0",
  "SVIP": "10.61.180.200:3260",
  "TenantName": "trident",
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS":
2000, "burstIOPS": 4000}},
            {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS":
6000, "burstIOPS": 8000}},
            {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS":
8000, "burstIOPS": 10000}}}
}
```

2. Una volta creato questo file back-end, eseguire il seguente comando per creare il primo backend.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-solidfire.json
```

| NAME                    | STATE  | VOLUMES | STORAGE DRIVER | UUID                                 |
|-------------------------|--------|---------|----------------|--------------------------------------|
| solidfire_10.61.180.200 | online | 0       | solidfire-san  | b90783ee-e0c9-49af-8d26-3ea87ce2efdf |

- Una volta creato il backend, è necessario creare una classe di storage. Come per il backend, esiste un file di esempio della classe di storage che può essere modificato per l'ambiente disponibile nella cartella di input di esempio. Copiarlo nella directory di lavoro e apportare le modifiche necessarie per riflettere il backend creato.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.tmpl ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

- L'unica modifica che deve essere apportata a questo file è definire `backendType` valore al nome del driver di storage dal backend appena creato. Annotare anche il valore del campo `nome`, a cui si deve fare riferimento in un passaggio successivo.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "solidfire-san"
```



Esiste un campo opzionale chiamato `fsType` definito in questo file. Nei backend iSCSI, questo valore può essere impostato su un tipo di filesystem Linux specifico (XFS, ext4 e così via), oppure può essere cancellato per consentire a OpenShift di decidere quale filesystem usare.

- Eseguire `oc` per creare la classe di storage.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

6. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). C'è un esempio `pvc-basic.yaml` file che può essere utilizzato per eseguire questa azione, disponibile anche in input di esempio.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

7. L'unica modifica che deve essere apportata a questo file è garantire che il `storageClassName` il campo corrisponde a quello appena creato. La definizione PVC può essere ulteriormente personalizzata in base alle esigenze del carico di lavoro da fornire.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

8. Creare il PVC emettendo il `oc` comando. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
basic      Bound       pvc-3445b5cc-df24-453d-a1e6-b484e874349d  1Gi
RWO                basic-csi      5s
```

## Opzioni di configurazione avanzate

### Analisi delle opzioni di bilanciamento del carico: Red Hat OpenShift con NetApp

Nella maggior parte dei casi, Red Hat OpenShift rende le applicazioni disponibili al mondo esterno attraverso i percorsi. Un servizio viene esposto assegnandogli un nome host raggiungibile esternamente. Il percorso definito e gli endpoint identificati dal servizio possono essere utilizzati da un router OpenShift per fornire questa connettività denominata ai client esterni.

Tuttavia, in alcuni casi, le applicazioni richiedono l'implementazione e la configurazione di bilanciatori di carico personalizzati per esporre i servizi appropriati. Un esempio è NetApp Astra Control Center. Per soddisfare questa esigenza, abbiamo valutato diverse opzioni di bilanciamento del carico personalizzate. L'installazione e la configurazione sono descritte in questa sezione.

Le seguenti pagine contengono informazioni aggiuntive sulle opzioni di bilanciamento del carico validate nella soluzione Red Hat OpenShift con NetApp:

- ["MetalLB"](#)
- ["F5 BIG-IP"](#)

### Installazione di bilanciatori di carico MetalLB: Red Hat OpenShift con NetApp

Questa pagina elenca le istruzioni di installazione e configurazione per il bilanciamento del carico MetalLB.

MetalLB è un bilanciamento del carico di rete self-hosting installato sul cluster OpenShift che consente la creazione di servizi OpenShift di bilanciamento del carico di tipo in cluster che non vengono eseguiti su un provider cloud. Le due funzionalità principali di MetalLB che lavorano insieme per supportare i servizi LoadBalancer sono l'allocazione degli indirizzi e l'annuncio esterno.

### Opzioni di configurazione di MetalLB

In base al modo in cui MetalLB annuncia l'indirizzo IP assegnato ai servizi LoadBalancer all'esterno del cluster OpenShift, opera in due modalità:

- **Layer 2 mode.** in questa modalità, un nodo del cluster OpenShift assume la proprietà del servizio e risponde alle richieste ARP per quell'IP per renderlo raggiungibile all'esterno del cluster OpenShift. Poiché solo il nodo annuncia l'IP, presenta un collo di bottiglia nella larghezza di banda e limitazioni di failover lente. Per ulteriori informazioni, consultare la documentazione ["qui"](#).
- **Modalità BGP.** in questa modalità, tutti i nodi del cluster OpenShift stabiliscono sessioni di peering BGP con un router e pubblicizzano i route per inoltrare il traffico agli IP del servizio. Il prerequisito per questa operazione è l'integrazione di MetalLB con un router in tale rete. A causa del meccanismo di hashing in BGP, il mapping IP-to-Node per un servizio presenta una certa limitazione. Per ulteriori informazioni, consultare la documentazione ["qui"](#).



Ai fini di questo documento, stiamo configurando MetalLB in modalità Layer-2.

### Installazione del bilanciamento del carico MetalLB

1. Scarica le risorse di MetalLB.

```
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/namespace.yaml
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/metallb.yaml
```

2. Modificare il file `metallb.yaml` e rimuovere `spec.template.spec.securityContext` Da Controller Deployment e dal DemonSet dell'oratore.

**Righe da eliminare:**

```
securityContext:
  runAsNonRoot: true
  runAsUser: 65534
```

3. Creare il `metallb-system` namespace.

```
[netapp-user@rhel7 ~]$ oc create -f namespace.yaml
namespace/metallb-system created
```

4. Creare il CR MetalLB.

```
[netapp-user@rhel7 ~]$ oc create -f metallb.yaml
podsecuritypolicy.policy/controller created
podsecuritypolicy.policy/speaker created
serviceaccount/controller created
serviceaccount/speaker created
clusterrole.rbac.authorization.k8s.io/metallb-system:controller created
clusterrole.rbac.authorization.k8s.io/metallb-system:speaker created
role.rbac.authorization.k8s.io/config-watcher created
role.rbac.authorization.k8s.io/pod-lister created
role.rbac.authorization.k8s.io/controller created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:controller
created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:speaker
created
rolebinding.rbac.authorization.k8s.io/config-watcher created
rolebinding.rbac.authorization.k8s.io/pod-lister created
rolebinding.rbac.authorization.k8s.io/controller created
daemonset.apps/speaker created
deployment.apps/controller created
```

5. Prima di configurare l'altoparlante MetalLB, concedere al relatore i privilegi elevati DemonSet in modo che possa eseguire la configurazione di rete richiesta per far funzionare i bilanciatori di carico.

```
[netapp-user@rhel7 ~]$ oc adm policy add-scc-to-user privileged -n metallb-system -z speaker
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:privileged
added: "speaker"
```

6. Configurare MetalLB creando un ConfigMap in metallb-system namespace.

```
[netapp-user@rhel7 ~]$ vim metallb-config.yaml

apiVersion: v1
kind: ConfigMap
metadata:
  namespace: metallb-system
  name: config
data:
  config: |
    address-pools:
    - name: default
      protocol: layer2
      addresses:
      - 10.63.17.10-10.63.17.200

[netapp-user@rhel7 ~]$ oc create -f metallb-config.yaml
configmap/config created
```

7. Ora, quando vengono creati i servizi loadbalancer, MetalLB assegna un IP esterno ai servizi e annuncia l'indirizzo IP rispondendo alle richieste ARP.



Se si desidera configurare MetalLB in modalità BGP, saltare il punto 6 e seguire la procedura nella documentazione di MetalLB "[qui](#)".

### Installazione di F5 BIG-IP Load Balancer

F5 BIG-IP è un Application Delivery Controller (ADC) che offre un'ampia gamma di servizi avanzati di gestione del traffico e sicurezza di livello produttivo come il bilanciamento del carico L4-L7, l'offload SSL/TLS, DNS, firewall e molto altro ancora. Questi servizi aumentano drasticamente la disponibilità, la sicurezza e le performance delle tue applicazioni.

F5 BIG-IP può essere implementato e utilizzato in vari modi, su hardware dedicato, nel cloud o come appliance virtuale on-premise. Fare riferimento alla documentazione qui per esplorare e implementare F5 BIG-IP in base ai requisiti.

Per un'integrazione efficiente dei servizi Big-IP di F5 con Red Hat OpenShift, F5 offre IL BIG-IP Container Ingress Service (CIS). CIS viene installato come controller pod che controlla l'API OpenShift per alcune

definizioni di risorse personalizzate (CRD) e gestisce la configurazione del sistema F5 BIG-IP. F5 BIG-IP CIS può essere configurato per controllare i tipi di servizio LoadBalancer e route in OpenShift.

Inoltre, per l'allocazione automatica dell'indirizzo IP al servizio del tipo LoadBalancer, è possibile utilizzare il controller F5 IPAM. Il controller F5 IPAM viene installato come controller pod che controlla i servizi di OpenShift API per LoadBalancer con un'annotazione ipamLabel per allocare l'indirizzo IP da un pool preconfigurato.

Questa pagina elenca le istruzioni di installazione e configurazione per i controller F5 BIG-IP CIS e IPAM. Come prerequisito, è necessario disporre di un sistema F5 BIG-IP distribuito e concesso in licenza. Deve inoltre essere concesso in licenza per i servizi SDN, inclusi per impostazione predefinita con LA licenza base BIG-IP VE.



F5 BIG-IP può essere implementato in modalità standalone o cluster. Ai fini di questa convalida, F5 BIG-IP è stato implementato in modalità standalone, ma per scopi di produzione, è preferibile disporre di un cluster di big-IP per evitare un singolo punto di errore.



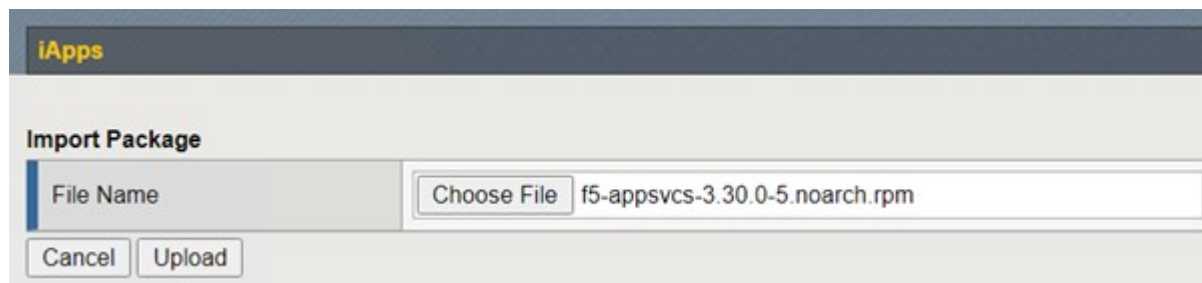
Un sistema F5 BIG-IP può essere implementato su hardware dedicato, nel cloud o come appliance virtuale on-premise con versioni superiori alla 12.x per l'integrazione con F5 CIS. Ai fini di questo documento, il sistema F5 BIG-IP è stato validato come appliance virtuale, ad esempio utilizzando L'edizione BIG-IP VE.

## Release validate

| Tecnologia                   | Versione del software |
|------------------------------|-----------------------|
| Red Hat OpenShift            | 4.6 EUS, 4.7          |
| F5 BIG-IP VE EDITION         | 16.1.0                |
| F5 Container Ingress Service | 2.5.1                 |
| F5 Controller IPAM           | 0.1.4                 |
| F5 AS3                       | 3.30.0                |

## Installazione

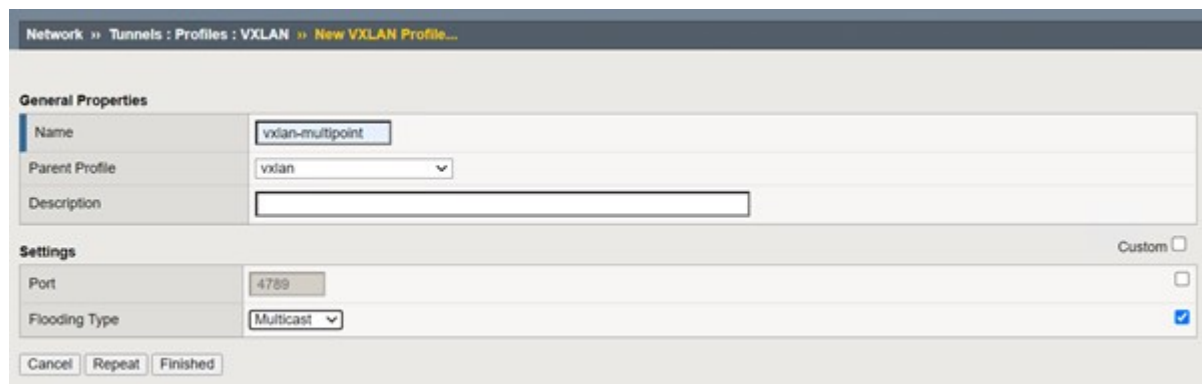
1. Installare l'estensione F5 Application Services 3 per consentire ai sistemi BIG-IP di accettare configurazioni in JSON invece di comandi imperativi. Passare a ["F5 repository AS3 GitHub"](#) e scaricare il file RPM più recente.
2. Accedere al sistema F5 BIG-IP, accedere a iApps > Package Management LX e fare clic su Import (Importa).
3. Fare clic su Choose file (Scegli file) e selezionare il file RPM AS3 scaricato, fare clic su OK, quindi su Upload (carica).



4. Verificare che l'estensione AS3 sia installata correttamente.



5. Quindi, configurare le risorse necessarie per la comunicazione tra OpenShift e I sistemi BIG-IP. Creare innanzitutto un tunnel tra OpenShift e IL SERVER BIG-IP creando un'interfaccia di tunnel VXLAN sul sistema BIG-IP per OpenShift SDN. Accedere a Network > Tunnels > Profiles (rete > tunnel > profili), fare clic su Create (Crea) e impostare il profilo principale su vxlan e il tipo di flooding su Multicast. Inserire un nome per il profilo e fare clic su fine.



6. Accedere a Network (rete) > Tunnels (tunnel) > Tunnel List (elenco tunnel), fare clic su Create (Crea) e immettere il nome e l'indirizzo IP locale per il tunnel. Selezionare il profilo di tunnel creato nel passaggio precedente e fare clic su fine.



Network » Tunnels : Tunnel List » New Tunnel...

**Configuration**

|                   |   |
|-------------------|---|
| Name              | openshift_vxlan                             |
| Description       |   |
| Key               | 0   |
| Profile           | vxlan-multipoint                            |
| Local Address     | 10.63.172.239                               |
| Secondary Address | Any   |
| Remote Address    | Any   |
| Mode              | Bidirectional                               |
| MTU               | 0   |
| Use PMTU          | <input checked="" type="checkbox"/> Enabled |
| TOS               | Preserve                                    |
| Auto-Last Hop     | Default                                     |
| Traffic Group     | None  |

Cancel Repeat Finished

- Accedi al cluster Red Hat OpenShift con privilegi di amministratore del cluster.
- Creare una subnet host su OpenShift per il server F5 BIG-IP, che estende la subnet dal cluster OpenShift al server F5 BIG-IP. Scaricare la definizione YAML della subnet host.

```
wget https://github.com/F5Networks/k8s-bigip-ctlr/blob/master/docs/config_examples/openshift/f5-kctlr-openshift-hostsubnet.yaml
```

- Modificare il file di sottorete host e aggiungere l'IP BIG-IP VTEP (tunnel VXLAN) per OpenShift SDN.

```

apiVersion: v1
kind: HostSubnet
metadata:
  name: f5-server
  annotations:
    pod.network.openshift.io/fixed-vnid-host: "0"
    pod.network.openshift.io/assign-subnet: "true"
# provide a name for the node that will serve as BIG-IP's entry into the
cluster
host: f5-server
# The hostIP address will be the BIG-IP interface address routable to
the
# OpenShift Origin nodes.
# This address is the BIG-IP VTEP in the SDN's VXLAN.
hostIP: 10.63.172.239

```



Modificare l'indirizzo e altri dettagli in base all'ambiente in uso.

#### 10. Creare la risorsa HostSubnet.

```

[admin@rhel-7 ~]$ oc create -f f5-kctlr-openshift-hostsubnet.yaml

hostsubnet.network.openshift.io/f5-server created

```

#### 11. Ottenere l'intervallo di subnet IP del cluster per la subnet host creata per il server Big-IP F5.

```
[admin@rhel-7 ~]$ oc get hostssubnet
```

| NAME                       | HOST                       | HOST IP       |
|----------------------------|----------------------------|---------------|
| SUBNET                     | EGRESS CIDRS               | EGRESS IPS    |
| f5-server                  | f5-server                  | 10.63.172.239 |
| 10.131.0.0/23              |                            |               |
| ocp-vmw-nszws-master-0     | ocp-vmw-nszws-master-0     | 10.63.172.44  |
| 10.128.0.0/23              |                            |               |
| ocp-vmw-nszws-master-1     | ocp-vmw-nszws-master-1     | 10.63.172.47  |
| 10.130.0.0/23              |                            |               |
| ocp-vmw-nszws-master-2     | ocp-vmw-nszws-master-2     | 10.63.172.48  |
| 10.129.0.0/23              |                            |               |
| ocp-vmw-nszws-worker-r8fh4 | ocp-vmw-nszws-worker-r8fh4 | 10.63.172.7   |
| 10.130.2.0/23              |                            |               |
| ocp-vmw-nszws-worker-tvr46 | ocp-vmw-nszws-worker-tvr46 | 10.63.172.11  |
| 10.129.2.0/23              |                            |               |
| ocp-vmw-nszws-worker-wdxhg | ocp-vmw-nszws-worker-wdxhg | 10.63.172.24  |
| 10.128.2.0/23              |                            |               |
| ocp-vmw-nszws-worker-wg8r4 | ocp-vmw-nszws-worker-wg8r4 | 10.63.172.15  |
| 10.131.2.0/23              |                            |               |
| ocp-vmw-nszws-worker-wtgfw | ocp-vmw-nszws-worker-wtgfw | 10.63.172.17  |
| 10.128.4.0/23              |                            |               |

12. Creare un IP self su OpenShift VXLAN con un IP nell'intervallo di subnet host di OpenShift corrispondente al server F5 BIG-IP. Accedere al sistema F5 BIG-IP, selezionare Network > Self IPs (rete > IP automatici) e fare clic su Create (Crea). Inserire un IP dalla subnet IP del cluster creata per la subnet host F5 BIG-IP, selezionare il tunnel VXLAN e immettere gli altri dettagli. Quindi fare clic su fine.

**Network » Self IPs » New Self IP...**

**Configuration**

|                |   |
|----------------|---|
| Name           | 10.131.0.60   |
| IP Address     | 10.131.0.60   |
| Netmask        | 255.252.0.0   |
| VLAN / Tunnel  | openshift_vxla ▾  |
| Port Lockdown  | Allow All ▾   |
| Traffic Group  | <input type="checkbox"/> Inherit traffic group from current partition / path<br>traffic-group-local-only (non-floating) ▾ |
| Service Policy | None ▾  |

Cancel Repeat Finished

13. Creare una partizione nel sistema F5 BIG-IP da configurare e utilizzare con CIS. Accedere a sistema > utenti > elenco partizioni, fare clic su Crea e immettere i dettagli. Quindi fare clic su fine.

**System » Users : Partition List » New Partition...**

**Properties**

|                                |   |
|--------------------------------|---|
| Partition Name                 | <input type="text" value="ocp-vmw"/>  |
| Partition Default Route Domain | <input type="text" value="0"/>  |
| Description                    | <div><div></div><div><input type="checkbox"/> Extend Text Area<br/><input type="checkbox"/> Wrap Text</div></div> |

**Redundant Device Configuration**

|               |   |
|---------------|---|
| Device Group  | <input checked="" type="checkbox"/> Inherit device group from root folder<br><input type="text" value="None"/>                        |
| Traffic Group | <input checked="" type="checkbox"/> Inherit traffic group from root folder<br><input type="text" value="traffic-group-1 (floating)"/> |



F5 consiglia di non eseguire alcuna configurazione manuale sulla partizione gestita da CIS.

14. Installare F5 BIG-IP CIS utilizzando l'operatore di OperatorHub. Accedi al cluster Red Hat OpenShift con privilegi di amministrazione del cluster e crea un segreto con le credenziali di accesso del sistema F5 BIG-IP, un prerequisito per l'operatore.

```
[admin@rhel-7 ~]$ oc create secret generic bigip-login -n kube-system
--from-literal=username=admin --from-literal=password=admin

secret/bigip-login created
```

## 15. Installare F5 CIS CRD.

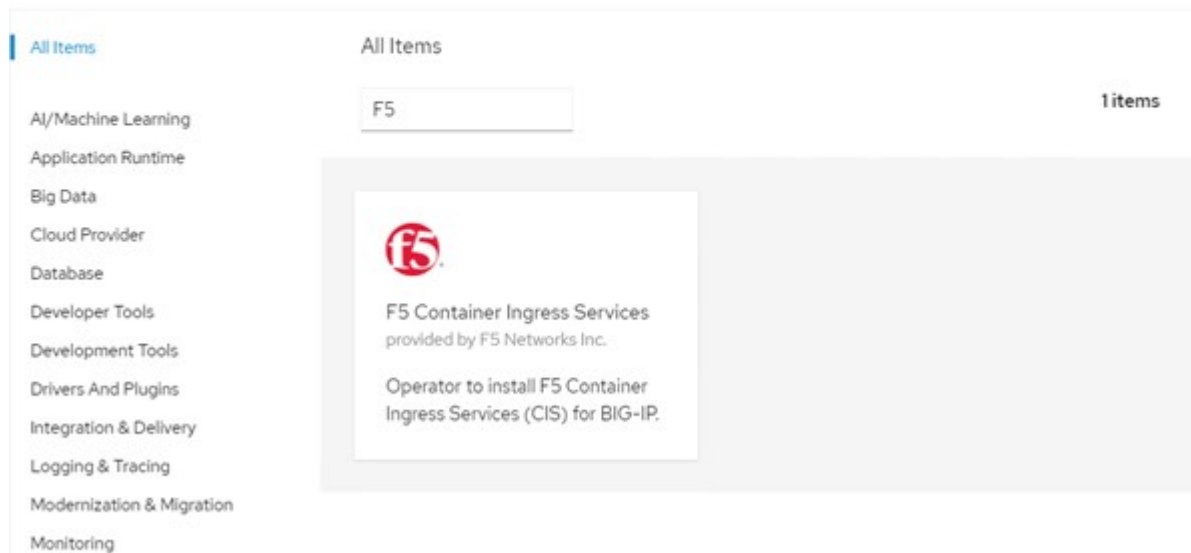
```
[admin@rhel-7 ~]$ oc apply -f
https://raw.githubusercontent.com/F5Networks/k8s-bigip-
ctlr/master/docs/config_examples/crd/Install/customresourcedefinitions.y
ml

customresourcedefinition.apiextensions.k8s.io/virtualservers.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/tlsprofiles.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/transportservers.cis.f5.co
m created
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com
created
```


## 16. Accedere a Operator > OperatorHub, cercare la parola chiave F5 e fare clic sul riquadro F5 Container Ingress Service.

### OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through [Red Hat Marketplace](#). You can install Operators on your clusters to provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the [Developer Catalog](#) providing a self-service experience.



17. Leggere le informazioni dell'operatore e fare clic su Install (Installa).

**F5 Container Ingress Services**1.8.0 provided by F5 Networks Inc.×

Install

**Latest version**  
1.8.0

**Capability level**  
☒ Basic Install  
☐ Seamless Upgrades  
☐ Full Lifecycle  
☐ Deep Insights  
☐ Auto Pilot

**Provider type**  
Certified

**Provider**  
F5 Networks Inc.

**Repository**  
<https://github.com/F5Networks/k8s-bigip-ctlr>

**Container image**  
[registry.connect.redhat.com/f5networks/k8s-bigip-ctlr](https://registry.connect.redhat.com/f5networks/k8s-bigip-ctlr)

### Introduction

This Operator installs F5 Container Ingress Services (CIS) for BIG-IP in your Cluster. This enables to configure and deploy CIS using Helm Charts.

### F5 Container Ingress Services for BIG-IP

F5 Container Ingress Services (CIS) integrates with container orchestration environments to dynamically create L4/L7 services on F5 BIG-IP systems, and load balance network traffic across the services. Monitoring the orchestration API server, CIS is able to modify the BIG-IP system configuration based on changes made to containerized applications.

### Documentation

Refer to F5 documentation

- CIS on OpenShift (<https://clouddocs.f5.com/containers/latest/userguide/openshift/>) - OpenShift Routes (<https://clouddocs.f5.com/containers/latest/userguide/routes.html>)

### Prerequisites

Create BIG-IP login credentials for use with Operator Helm charts. A basic way be,

```
oc create secret generic <SECRET-NAME> -n kube-system --from-literal=username=<USERNAME> --from-literal=password=<PASSWORD>
```

18. Nella schermata Install operator (Installa operatore), lasciare tutti i parametri predefiniti e fare clic su Install (Installa).

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

### Update channel \*

☒ beta

### Installation mode \*

- ☒ All namespaces on the cluster (default)  
Operator will be available in all Namespaces.
- ☐ A specific namespace on the cluster  
Operator will be available in a single Namespace only.

### Installed Namespace \*

**PR** openshift-operators

### Approval strategy \*

- ☒ Automatic
- ☐ Manual

Install

Cancel



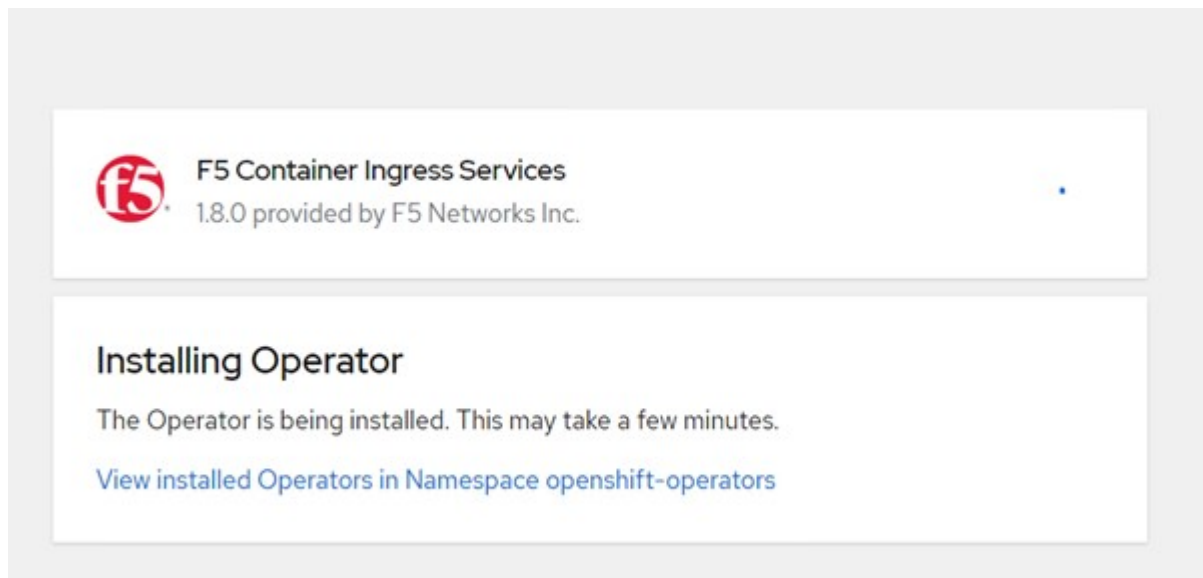
**F5 Container Ingress Services**  
provided by F5 Networks Inc.

### Provided APIs

**FBIC** F5BigIpCtrlr

This CRD provides kind **F5BigIpCtrlr** to configure and deploy F5 BIG-IP Controller.

19. L'installazione dell'operatore richiede un po' di tempo.



20. Una volta installato l'operatore, viene visualizzato il messaggio Installazione completata.

21. Accedere a Operators > Installed Operators (operatori > operatori installati), fare clic su F5 Container Ingress Service (F5 Container Ingress Service), quindi fare clic su Create Instance (Crea istanza) nella sezione F5BigIpCtrlr.

[Installed Operators](#) > Operator details



**F5 Container Ingress Services**  
1.8.0 provided by F5 Networks Inc.

[Details](#)

[YAML](#)

[Subscription](#)

[Events](#)

[F5BigIpCtrlr](#)

## Provided APIs

**FBIC** F5BigIpCtrlr

This CRD provides kind `F5BigIpCtrlr` to configure and deploy F5 BIG-IP Controller.

[+ Create instance](#)

22. Fare clic su [YAML View](#) (Visualizza YAML) e incollare il seguente contenuto dopo aver aggiornato i parametri necessari.



Aggiornare i parametri `bigip_partition`, `openshift_sdn_name`, `bigip_url` e `bigip_login_secret` di seguito per riflettere i valori per la configurazione prima di copiare il contenuto.



```




apiVersion: cis.f5.com/v1
kind: F5BigIpCtlr
metadata:
  name: f5-server
  namespace: openshift-operators
spec:
  args:
    log_as3_response: true
    agent: as3
    log_level: DEBUG
    bigip_partition: ocp-vmw
    openshift_sdn_name: /Common/openshift_vxlan
    bigip_url: 10.61.181.19
    insecure: true
    pool-member-type: cluster
    custom_resource_mode: true
    as3_validation: true
    ipam: true
    manage_configmaps: true
  bigip_login_secret: bigip-login
  image:
    pullPolicy: Always
    repo: f5networks/cntr-ingress-svcs
    user: registry.connect.redhat.com
  namespace: kube-system
  rbac:
    create: true
  resources: {}
  serviceAccount:
    create: true
  version: latest

```

23. Dopo aver incollato questo contenuto, fare clic su Create (Crea). In questo modo vengono installati i pod CIS nello spazio dei nomi del sistema kube.

**Pods** Create Pod

Filter Name Search by name...

| Name ↑   | Status ↓  | Ready ↓ | Restarts ↓ | Owner ↓  | Memory ↓ | CPU ↓       |
|--|---|---------|------------|--|----------|-------------|
|  f5-server-f5-bigip-ctlr-5d7578667d-qxdgj |  Running | 1/1     | 0          |  f5-server-f5-bigip-ctlr-5d7578667d | 611 MiB  | 0.003 cores |



Red Hat OpenShift, per impostazione predefinita, fornisce un modo per esporre i servizi tramite route per il bilanciamento del carico L7. Un router OpenShift integrato è responsabile della pubblicità e della gestione del traffico per questi percorsi. Tuttavia, è anche possibile configurare F5 CIS per supportare i percorsi attraverso un sistema esterno F5 BIG-IP, che può essere eseguito come router ausiliario o come sostituto del router OpenShift self-hosting. CIS crea un server virtuale nel sistema BIG-IP che funge da router per i route OpenShift, mentre BIG-IP gestisce il routing degli annunci pubblicitari e del traffico. Fare riferimento alla documentazione qui per informazioni sui parametri per attivare questa funzione. Si noti che questi parametri sono definiti per la risorsa di implementazione OpenShift nell'API apps/v1. Pertanto, quando si utilizzano questi dati con l'API cis.f5.com/v1 della risorsa F5BigIpCtrlr, sostituire i trattini (-) con i trattini (\_) per i nomi dei parametri.

24. Gli argomenti passati alla creazione delle risorse CIS includono `ipam: true` e `custom_resource_mode: true`. Questi parametri sono necessari per abilitare l'integrazione CIS con un controller IPAM. Verificare che il CIS abbia attivato l'integrazione IPAM creando la risorsa F5 IPAM.

```
[admin@rhel-7 ~]$ oc get f5ipam -n kube-system
```

| NAMESPACE   | NAME                      | AGE |
|-------------|---------------------------|-----|
| kube-system | ipam.10.61.181.19.ocp-vmw | 43s |

25. Creare l'account del servizio, il ruolo e il rolebinding richiesti per il controller F5 IPAM. Creare un file YAML e incollare il seguente contenuto.

```
[admin@rhel-7 ~]$ vi f5-ipam-rbac.yaml

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole
rules:
  - apiGroups: ["fic.f5.com"]
    resources: ["ipams","ipams/status"]
    verbs: ["get", "list", "watch", "update", "patch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole-binding
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ipam-ctrl-clusterrole
subjects:
  - apiGroup: ""
    kind: ServiceAccount
    name: ipam-ctrl
    namespace: kube-system
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: ipam-ctrl
  namespace: kube-system
```

## 26. Creare le risorse.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-rbac.yaml

clusterrole.rbac.authorization.k8s.io/ipam-ctrl-clusterrole created
clusterrolebinding.rbac.authorization.k8s.io/ipam-ctrl-clusterrole-
binding created
serviceaccount/ipam-ctrl created
```

## 27. Creare un file YAML e incollare la definizione di implementazione F5 IPAM fornita di seguito.



Aggiornare il parametro `ip-range` in `spec.template.spec.containers[0].args` di seguito per riflettere gli intervalli di indirizzi IP e `ipamLabels` corrispondenti alla configurazione.



`ipamLabels` [`range1` e `range2` Nell'esempio seguente] devono essere annotati per i servizi di tipo `LoadBalancer` affinché il controller IPAM rilevi e assegni un indirizzo IP dall'intervallo definito.

```
[admin@rhel-7 ~]$ vi f5-ipam-deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    name: f5-ipam-controller
    name: f5-ipam-controller
    namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: f5-ipam-controller
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: f5-ipam-controller
    spec:
      containers:
      - args:
        - --orchestration=openshift
        - --ip-range='{"range1":"10.63.172.242-10.63.172.249",
"range2":"10.63.170.111-10.63.170.129"}'
        - --log-level=DEBUG
        command:
        - /app/bin/f5-ipam-controller
        image: registry.connect.redhat.com/f5networks/f5-ipam-
controller:latest
        imagePullPolicy: IfNotPresent
        name: f5-ipam-controller
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      serviceAccount: ipam-ctrlr
      serviceAccountName: ipam-ctrlr
```

## 28. Creare l'implementazione del controller F5 IPAM.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-deployment.yaml  
  
deployment/f5-ipam-controller created
```

## 29. Verificare che i controller pod F5 IPAM siano in esecuzione.

```
[admin@rhel-7 ~]$ oc get pods -n kube-system
```

| NAME                                     | READY | STATUS  | RESTARTS |
|--|-------|---------|----------|
| AGE                                      |       |         |          |
| f5-ipam-controller-5986cff5bd-2bvn6      | 1/1   | Running | 0        |
| 30s                                      |       |         |          |
| f5-server-f5-bigip-ctlr-5d7578667d-qxdgj | 1/1   | Running | 0        |
| 14m                                      |       |         |          |

## 30. Creare lo schema F5 IPAM.

```
[admin@rhel-7 ~]$ oc create -f  
https://raw.githubusercontent.com/F5Networks/f5-ipam-  
controller/main/docs/_static/schemas/ipam_schema.yaml  
  
customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

## Verifica

1. Creare un servizio di tipo LoadBalancer

```
[admin@rhel-7 ~]$ vi example_svc.yaml
```

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    cis.f5.com/ipamLabel: range1
  labels:
    app: f5-demo-test
  name: f5-demo-test
  namespace: default
spec:
  ports:
  - name: f5-demo-test
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: f5-demo-test
  sessionAffinity: None
  type: LoadBalancer
```

```
[admin@rhel-7 ~]$ oc create -f example_svc.yaml
```

```
service/f5-demo-test created
```

## 2. Controllare se il controller IPAM assegna un indirizzo IP esterno.

```
[admin@rhel-7 ~]$ oc get svc
```

| NAME         | TYPE         | CLUSTER-IP     | EXTERNAL-IP   |
|--------------|--------------|----------------|---------------|
| f5-demo-test | LoadBalancer | 172.30.210.108 | 10.63.172.242 |
| 80:32605/TCP | 27s          |                |               |

## 3. Creare un'implementazione e utilizzare il servizio LoadBalancer creato.

```
[admin@rhel-7 ~]$ vi example_deployment.yaml
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: f5-demo-test
  name: f5-demo-test
spec:
  replicas: 2
  selector:
    matchLabels:
      app: f5-demo-test
  template:
    metadata:
      labels:
        app: f5-demo-test
    spec:
      containers:
      - env:
        - name: service_name
          value: f5-demo-test
        image: nginx
        imagePullPolicy: Always
        name: f5-demo-test
        ports:
        - containerPort: 80
          protocol: TCP
```

```
[admin@rhel-7 ~]$ oc create -f example_deployment.yaml
```

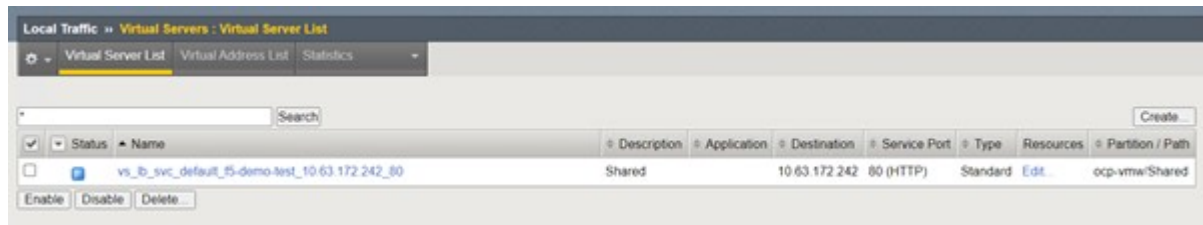
```
deployment/f5-demo-test created
```

#### 4. Verificare che i pod siano in funzione.

```
[admin@rhel-7 ~]$ oc get pods
```

| NAME                          | READY | STATUS  | RESTARTS | AGE |
|-------------------------------|-------|---------|----------|-----|
| f5-demo-test-57c46f6f98-47wwp | 1/1   | Running | 0        | 27s |
| f5-demo-test-57c46f6f98-cl2m8 | 1/1   | Running | 0        | 27s |

#### 5. Controllare se il server virtuale corrispondente viene creato nel sistema BIG-IP per il servizio di tipo LoadBalancer in OpenShift. Accedere a traffico locale > Server virtuali > elenco server virtuali.



## Creazione di registri immagine privati

Per la maggior parte delle implementazioni di Red Hat OpenShift, utilizzando un registro pubblico come "Quay.io" oppure "DockerHub" soddisfa la maggior parte delle esigenze dei clienti. Tuttavia, in alcuni casi un cliente potrebbe voler ospitare le proprie immagini private o personalizzate.

Questa procedura documenta la creazione di un registro di immagini privato supportato da un volume persistente fornito da Astra Trident e NetApp ONTAP.



Astra Control Center richiede un registro per ospitare le immagini richieste dai container Astra. La sezione seguente descrive i passaggi per configurare un registro privato sul cluster Red Hat OpenShift e per inviare le immagini necessarie per supportare l'installazione di Astra Control Center.

### Creazione Di un registro di immagine privato

1. Rimuovere l'annotazione predefinita dalla classe di storage predefinita corrente e annotare la classe di storage supportata da Trident come predefinita per il cluster OpenShift.

```
[netapp-user@rhel7 ~]$ oc patch storageclass thin -p '{"metadata":
{"annotations": {"storageclass.kubernetes.io/is-default-class":
"false"}}}'
storageclass.storage.k8s.io/thin patched

[netapp-user@rhel7 ~]$ oc patch storageclass ocp-trident -p
'{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-
class": "true"}}}'
storageclass.storage.k8s.io/ocp-trident patched
```

2. Modificare l'operatore di imageregistry immettendo i seguenti parametri di storage in spec sezione.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

3. Inserire i seguenti parametri in spec Sezione per la creazione di un percorso OpenShift con un nome host personalizzato. Salvare e uscire.



```
routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
```



La suddetta configurazione del percorso viene utilizzata quando si desidera un nome host personalizzato per il percorso. Se si desidera che OpenShift crei un percorso con un nome host predefinito, è possibile aggiungere i seguenti parametri a `spec` sezione:

```
defaultRoute: true.
```

## Certificati TLS personalizzati

Quando si utilizza un nome host personalizzato per il percorso, per impostazione predefinita, utilizza la configurazione TLS predefinita dell'operatore OpenShift Ingress. Tuttavia, è possibile aggiungere una configurazione TLS personalizzata al percorso. A tale scopo, attenersi alla seguente procedura.

- a. Creare un segreto con i certificati TLS e la chiave del percorso.

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n
openshift-image-registry -cert/home/admin/netapp-astra/tls.crt
--key=/home/admin/netapp-astra/tls.key
```

- b. Modificare l'operatore di imageregistry e aggiungere i seguenti parametri a `spec` sezione.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
  secretName: astra-route-tls
```

4. Modificare nuovamente l'operatore di imageregistry e modificare lo stato di gestione dell'operatore in `Managed` stato. Salvare e uscire.

```
oc edit configs.imageregistry/cluster

managementState: Managed
```

5. Se tutti i prerequisiti sono soddisfatti, PVC, POD e servizi vengono creati per il registro delle immagini private. In pochi minuti, il registro dovrebbe essere attivo.

```
[netapp-user@rhel7 ~]$oc get all -n openshift-image-registry
```

| NAME   | READY | STATUS    |
|--|-------|-----------|
| pod/cluster-image-registry-operator-74f6d954b6-rb7zr | 1/1   | Running   |
| 3  |       | 90d       |
| pod/image-pruner-1627257600-f5cpj                    | 0/1   | Completed |
| 0  |       | 2d9h      |
| pod/image-pruner-1627344000-swqx9                    | 0/1   | Completed |
| 0  |       | 33h       |
| pod/image-pruner-1627430400-rv5nt                    | 0/1   | Completed |
| 0  |       | 9h        |
| pod/image-registry-6758b547f-6pnj8                   | 1/1   | Running   |
| 0  |       | 76m       |
| pod/node-ca-bwb5r                                    | 1/1   | Running   |
| 0  |       | 90d       |
| pod/node-ca-f8w54                                    | 1/1   | Running   |
| 0  |       | 90d       |
| pod/node-ca-gjx7h                                    | 1/1   | Running   |
| 0  |       | 90d       |
| pod/node-ca-lcx4k                                    | 1/1   | Running   |
| 0  |       | 33d       |
| pod/node-ca-v7zmx                                    | 1/1   | Running   |
| 0  |       | 7d21h     |
| pod/node-ca-xpppp                                    | 1/1   | Running   |
| 0  |       | 89d       |

| NAME                            | TYPE      | CLUSTER-IP     | EXTERNAL-IP |
|---------------------------------|-----------|----------------|-------------|
| service/image-registry          | ClusterIP | 172.30.196.167 | <none>      |
| 5000/TCP                        |           |                | 15h         |
| service/image-registry-operator | ClusterIP | None           | <none>      |
| 60000/TCP                       |           |                | 90d         |

| NAME                   | DESIRED | CURRENT | READY | UP-TO-DATE |
|------------------------|---------|---------|-------|------------|
| daemonset.apps/node-ca | 6       | 6       | 6     | 6          |
| kubernetes.io/os=linux | 90d     |         |       |            |

| NAME  | READY | UP-TO-DATE |
|---|-------|------------|
| deployment.apps/cluster-image-registry-operator | 1/1   | 1          |
| 90d   |       |            |
| deployment.apps/image-registry                  | 1/1   | 1          |
| 15h   |       |            |

| NAME   | DESIRED |
|--|---------|
| CURRENT READY AGE  |         |
| replicaset.apps/cluster-image-registry-operator-74f6d954b6 | 1 1     |
| 1 90d  |         |
| replicaset.apps/image-registry-6758b547f                   | 1 1     |
| 1 76m  |         |
| replicaset.apps/image-registry-78bfbd7f59                  | 0 0     |
| 0 15h  |         |
| replicaset.apps/image-registry-7fcc8d6cc8                  | 0 0     |
| 0 80m  |         |
| replicaset.apps/image-registry-864f88f5b                   | 0 0     |
| 0 15h  |         |
| replicaset.apps/image-registry-cb47fffb                    | 0 0     |
| 0 10h  |         |

| NAME                              | COMPLETIONS | DURATION | AGE  |
|-----------------------------------|-------------|----------|------|
| job.batch/image-pruner-1627257600 | 1/1         | 10s      | 2d9h |
| job.batch/image-pruner-1627344000 | 1/1         | 6s       | 33h  |
| job.batch/image-pruner-1627430400 | 1/1         | 5s       | 9h   |

| NAME                       | SCHEDULE  | SUSPEND | ACTIVE | LAST |
|----------------------------|-----------|---------|--------|------|
| SCHEDULE AGE               |           |         |        |      |
| cronjob.batch/image-pruner | 0 0 * * * | False   | 0      | 9h   |
| 90d                        |           |         |        |      |

| NAME                                    | HOST/PORT                           |
|---|-------------------------------------|
| PATH SERVICES PORT TERMINATION WILDCARD |                                     |
| route.route.openshift.io/public-routes  | astra-registry.apps.ocp-            |
| vmw.cie.netapp.com                      | image-registry <all> reencrypt None |

6. Se si utilizzano i certificati TLS predefiniti per il percorso del Registro di sistema OpenShift dell'operatore di ingresso, è possibile recuperare i certificati TLS utilizzando il seguente comando.

```
[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n
openshift-ingress-operator
```

7. Per consentire ai nodi OpenShift di accedere e estrarre le immagini dal Registro di sistema, aggiungere i certificati al client del docker sui nodi OpenShift. Creare una mappa di configurazione in `openshift-config` Namespace che utilizza i certificati TLS e lo patch alla configurazione dell'immagine del cluster per rendere attendibile il certificato.

```
[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config
--from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}'
--type=merge
```

8. Il registro interno di OpenShift è controllato dall'autenticazione. Tutti gli utenti di OpenShift possono accedere al registro di OpenShift, ma le operazioni che l'utente connesso può eseguire dipendono dalle autorizzazioni dell'utente.

- a. Per consentire a un utente o a un gruppo di utenti di estrarre immagini dal registro, agli utenti deve essere assegnato il ruolo di visualizzatore del registro.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer
ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer
ocp-user-group
```

- b. Per consentire a un utente o a un gruppo di utenti di scrivere o inviare immagini, agli utenti deve essere assegnato il ruolo di editor del Registro di sistema.

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor
ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor
ocp-user-group
```

9. Per consentire ai nodi OpenShift di accedere al Registro di sistema e di eseguire il push o il pull delle immagini, è necessario configurare un pull secret.

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-
credentials --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com
--docker-username=ocp-user --docker-password=password
```

10. Questo segreto pull può quindi essere patchato agli account di servizio o può essere referenziato nella definizione del pod corrispondente.

- a. Per applicare la patch agli account di servizio, eseguire il seguente comando.

```
[netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-
registry-credentials --for=pull
```

- b. Per fare riferimento al segreto pull nella definizione del pod, aggiungere il seguente parametro a spec sezione.

```
imagePullSecrets:
- name: astra-registry-credentials
```

11. Per trasferire o estrarre un'immagine dalle workstation a parte il nodo OpenShift, attenersi alla seguente procedura.

- a. Aggiungere i certificati TLS al client docker.

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com

[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

- b. Accedere a OpenShift usando il comando oc login.

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO
-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

- c. Accedere al registro utilizzando le credenziali utente di OpenShift con il comando podman/docker.

#### podman

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t) --tls
-verify=false
```

+ NOTA: Se si utilizza kubeadmin per accedere al registro di sistema privato, quindi utilizzare il token invece della password.

#### docker

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

+ NOTA: Se si utilizza kubeadmin per accedere al registro di sistema privato, quindi utilizzare il token invece della password.

- d. Premere o tirare le immagini.

### podman

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

### docker

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

## Convalida della soluzione e casi d'utilizzo: Red Hat OpenShift con NetApp

Gli esempi forniti in questa pagina sono validazioni di soluzioni e casi di utilizzo per Red Hat OpenShift con NetApp.

- ["Implementare una pipeline ci/CD Jenkins con storage persistente"](#)
- ["Configura la multitenancy su Red Hat OpenShift con NetApp"](#)
- ["Virtualizzazione Red Hat OpenShift con NetApp ONTAP"](#)
- ["Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp"](#)

### Implementa una pipeline ci/CD Jenkins con storage persistente: Red Hat OpenShift con NetApp

In questa sezione vengono fornite le fasi necessarie per implementare una pipeline ci/CD (Continuous Integration/Continuous Delivery or Deployment) con Jenkins per convalidare il funzionamento della soluzione.

#### Creare le risorse necessarie per l'implementazione di Jenkins

Per creare le risorse necessarie per l'implementazione dell'applicazione Jenkins, attenersi alla seguente procedura:

1. Crea un nuovo progetto chiamato Jenkins.

# Create Project

Name \*

Display Name

Description

Cancel

Create

2. In questo esempio, abbiamo implementato Jenkins con storage persistente. Per supportare la build Jenkins, creare il PVC. Selezionare Storage > Persistent Volume Claims (Storage > Reclami volumi persistenti) e fare clic su Create Persistent. Selezionare la classe di storage creata, assicurarsi che il nome della richiesta di rimborso del volume persistente sia jenkins, selezionare la dimensione e la modalità di accesso appropriate, quindi fare clic su Create (Crea).

## Create Persistent Volume Claim

[Edit YAML](#)

### Storage Class

 basic ▼

Storage class for the new claim.

### Persistent Volume Claim Name \*

jenkins

A unique name for the storage claim within the project.

### Access Mode \*

☒ Single User (RWO) ☐ Shared Access (RWX) ☐ Read Only (ROX)

Permissions to the mounted drive.

### Size \*

100 GiB ▼

Desired storage capacity.

☐ Use label selectors to request storage

Use label selectors to define how storage is created.

[Create](#) [Cancel](#)

### Implementare Jenkins con lo storage persistente

Per implementare Jenkins con lo storage persistente, attenersi alla seguente procedura:

1. Nell'angolo in alto a sinistra, modificare il ruolo da Amministratore a sviluppatore. Fare clic su +Add (Aggiungi) e selezionare From Catalog (dal catalogo) Nella barra Filtra per parola chiave, cercare jenkins. Selezionare Servizio Jenkins con storage persistente.



## Developer Catalog

Add shared apps, services, or source-to-image builders to your project from the Developer Catalog. Cluster admins can install additional apps which will show up here automatically.

All Items

Languages

Databases

Middleware

CI/CD

Other

Type

☒ Operator Backed (0)

☐ Helm Charts (0)

☒ Builder Image (0)


☒ Template (4)

☐ Service Class (0)

All Items


jenkins

Group By: None ▾

Template


Jenkins  
provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...

Template


Jenkins  
provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...

Template

Jenkins (Ephemeral)  
provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING: Any data stored will be lost upon...

Template

Jenkins (Ephemeral)  
provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING:

2. Fare clic su **Instantiate Template**.



### Jenkins

Provided by Red Hat, Inc.



**Instantiate Template**

#### Provider

Red Hat, Inc.

#### Support

[Get support](#)

#### Created At

 May 26, 3:58 am

#### Description

Jenkins service, with persistent storage.

NOTE: You must have persistent volumes available in your cluster to use this template.

#### Documentation

[https://docs.okd.io/latest/using\\_images/other\\_images/jenkins.html](https://docs.okd.io/latest/using_images/other_images/jenkins.html)

3. Per impostazione predefinita, i dettagli dell'applicazione Jenkins vengono popolati. In base alle proprie esigenze, modificare i parametri e fare clic su **Create** (Crea). Questo processo crea tutte le risorse

necessarie per supportare Jenkins su OpenShift.

## Instantiate Template

**Namespace \***  

PR jenkins

**Jenkins Service Name**  

jenkins

The name of the OpenShift Service exposed for the Jenkins container.

**Jenkins JNLP Service Name**  

jenkins-jnlp

The name of the service used for master/slave communication.

**Enable OAuth in Jenkins**  

true

Whether to enable OAuth OpenShift integration. If false, the static account 'admin' will be initialized with the password 'password'.

**Memory Limit**  

1Gi

Maximum amount of memory the container can use.

**Volume Capacity \***  

50Gi

Volume space available for data, e.g. 512Mi, 2Gi.

**Jenkins ImageStream Namespace**  

openshift

The OpenShift Namespace where the Jenkins ImageStream resides.

**Disable memory intensive administrative monitors**  

false

Whether to perform memory intensive, possibly slow, synchronization with the Jenkins Update Center on start. If true, the Jenkins core update monitor and site warnings monitor are disabled.

**Jenkins ImageStreamTag**  

jenkins:2

Name of the ImageStreamTag to be used for the Jenkins image.

**Fatal Error Log File**  

false

When a fatal error occurs, an error log is created with information and the state obtained at the time of the fatal error.


**Allows use of Jenkins Update Center repository with invalid SSL certificate**  

false

Whether to allow use of a Jenkins Update Center that uses invalid certificate (self-signed, unknown CA). If any value other than 'false', certificate check is bypassed. By default, certificate check is enforced.

Create

Cancel



**Jenkins**  
INSTANT-APP JENKINS  
[View documentation](#) [Get support](#)

Jenkins service, with persistent storage.

NOTE: You must have persistent volumes available in your cluster to use this template.

The following resources will be created:





- DeploymentConfig
- PersistentVolumeClaim
- RoleBinding
- Route
- Service
- ServiceAccount

4. I pod Jenkins impiegano circa 10 - 12 minuti per entrare nello stato Pronto.

## Pods

[Create Pod](#)

|                    |           |               |                    |             |          |              |
|--------------------|-----------|---------------|--------------------|-------------|----------|--------------|
| 1 Running          | 0 Pending | 0 Terminating | 0 CrashLoopBackOff | 1 Completed | 0 Failed | 0 Unknown    |
| Select all filters |           |               |                    |             |          | 1 of 2 Items |





| Name ↑  | Namespace ↓   | Status ↓  | Ready ↓ | Owner ↓   | Memory ↓ | CPU ↓       |   |
|---|---|---|---------|---|----------|-------------|---|
|  jenkins-1-c77n9 |  jenkins |  Running | 1/1     |  jenkins-1 | -        | 0.004 cores | ⋮ |

5. Una volta creata l'istanza dei pod, accedere a Networking > routes (rete > percorsi). Per aprire la pagina Web di Jenkins, fare clic sull'URL fornito per il percorso jenkins.

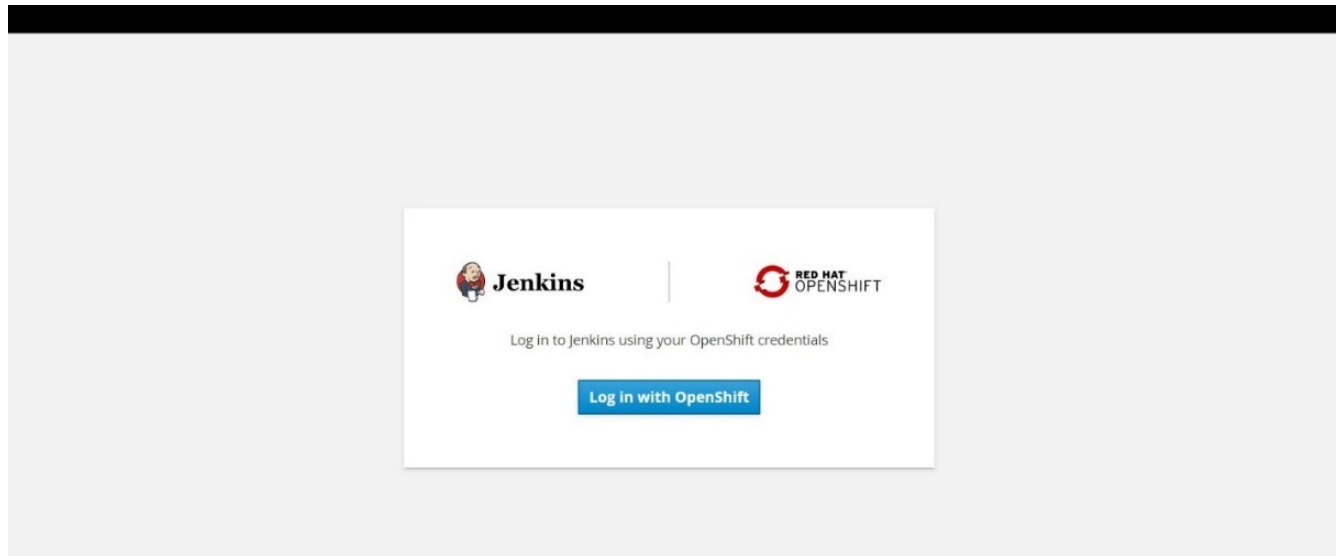
## Routes

[Create Route](#)

|            |            |           |                                    |        |
|------------|------------|-----------|------------------------------------|--------|
| 1 Accepted | 0 Rejected | 0 Pending | <a href="#">Select all filters</a> | 1 Item |
|------------|------------|-----------|------------------------------------|--------|

| Name ↓  | Namespace ↓   | Status   | Location ↓  | Service ↓   |   |
|---|---|--|---|---|---|
|  jenkins |  jenkins |  Accepted | <a href="https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com">https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com</a> |  jenkins | ⋮ |

6. Poiché OpenShift OAuth è stato utilizzato durante la creazione dell'applicazione Jenkins, fare clic su Accedi con OpenShift.



7. Autorizzare l'account del servizio Jenkins ad accedere agli utenti OpenShift.

## Authorize Access

Service account `jenkins` in project `jenkins` is requesting permission to access your account (`kube:admin`)

Requested permissions

☒ **user:info**

Read-only access to your user information (including username, identities, and group membership)

☒ **user:check-access**

Read-only access to view your privileges (for example, "can I create builds?")

You will be redirected to <https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com/securityRealm/finishLogin>

Allow selected permissions

Deny

8. Viene visualizzata la pagina di benvenuto di Jenkins. Poiché stiamo utilizzando una build Maven, completare prima l'installazione di Maven. Accedere a Manage Jenkins > Global Tool Configuration (Gestisci Jenkins > Configurazione globale strumenti), quindi fare clic su Add Maven (Aggiungi Maven) nella sottotesta di Maven. Immettere il nome desiderato e assicurarsi che l'opzione Installa automaticamente sia selezionata. Fare clic su Salva.

**Maven**

Maven installations

**Add Maven**

Maven

Name

☒ Install automatically

**Install from Apache**

Version

**Add Installer**

**Add Maven**

List of Maven installations on this system

**Delete Installer**

**Delete Maven**

9. È ora possibile creare una pipeline per dimostrare il flusso di lavoro ci/CD. Nella home page, fare clic su Create New Jobs (Crea nuovi lavori) o New Item (nuovo elemento) dal menu a sinistra.

**Jenkins** 3 search kube:admin | log out

Jenkins

ENABLE AUTO REFRESH

add description

New Item

People

Build History

Manage Jenkins

My Views

Open Blue Ocean

Lockable Resources

Credentials

New View

**Welcome to Jenkins!**

Please [create new jobs](#) to get started.

**Build Queue**

No builds in the queue.

**Build Executor Status**

1 Idle

2 Idle

10. Nella pagina Create Item (Crea elemento), immettere il nome desiderato, selezionare Pipeline e fare clic su OK.

## Enter an item name

» Required field



### Freestyle project

This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.



### Pipeline

Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.



### Multi-configuration project

Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.



### Bitbucket Team/Project

Scans a Bitbucket Cloud Team (or Bitbucket Server Project) for all repositories matching some defined markers.



### Folder

Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.



### GitHub Organization

Scans a GitHub organization (or user account) for all repositories matching some defined markers.



### Multibranch Pipeline

Creates a set of Pipeline projects according to detected branches in one SCM repository.

11. Selezionare la scheda pipeline. Dal menu a discesa Try Sample Pipeline, selezionare Github + Maven. Il codice viene compilato automaticamente. Fare clic su Salva.

General
Build Triggers
Advanced Project Options
**Pipeline**

Advanced...

## Pipeline

Definition
Pipeline script

Script

```

1 node {
2   def mvnHome
3   stage('Preparation') { // for display purposes
4     // Get some code from a GitHub repository
5     git 'https://github.com/jglick/simple-maven-project-with-tests.git'
6     // Get the Maven tool.
7     // ** NOTE: This 'M3' Maven tool must be configured
8     // **       in the global configuration.
9     mvnHome = tool 'M3'
10  }
11  stage('Build') {
12    // Run the maven build
13    withEnv(["MVN_HOME=$mvnHome"]) {
14      if (isUnix()) {
15        sh "$MVN_HOME/bin/mvn" -Dmaven.test.failure.ignore clean package
16      } else {
17        bat ("%MVN_HOME%\bin\mvn" -Dmaven.test.failure.ignore clean package/)

```

GitHub + Maven


☒ Use Groovy Sandbox

[Pipeline Syntax](#)


Save


Apply


- Fare clic su Build Now (Crea ora) per avviare lo sviluppo attraverso la fase di preparazione, creazione e test. Il completamento dell'intero processo di creazione e la visualizzazione dei risultati della creazione possono richiedere alcuni minuti.


Jenkins


Jenkins > sample-demo >


Back to Dashboard


Status


Changes


Build Now


Delete Pipeline

Configure

Full Stage View

Open Blue Ocean

Rename

Pipeline Syntax

Build History


trend


find X

#1 May 27, 2020 3:53 PM

Atom feed for all Atom feed for failures

# Pipeline sample-demo


Last Successful Artifacts

Recent Changes

Average stage times:  
(Average full run time: ~7s)

#1 May 27 08:53 No Changes

| Preparation | Build | Results |
|-------------|-------|---------|
| 2s          | 4s    | 69ms    |

Latest Test Result (no failures)

Permalinks

- Last build (#1), 1 min 23 sec ago
- Last stable build (#1), 1 min 23 sec ago
- Last successful build (#1), 1 min 23 sec ago
- Last completed build (#1), 1 min 23 sec ago

13. Ogni volta che si verifica una modifica del codice, la pipeline può essere ricostruita per applicare patch alla nuova versione del software, consentendo un'integrazione continua e un'erogazione continua. Fare clic su Recent Changes (modifiche recenti) per tenere traccia delle modifiche rispetto alla versione precedente.

170





Una di queste soluzioni efficaci consiste nel configurare la multi-tenancy su Red Hat OpenShift. La multi-tenancy è un'architettura che consente a più tenant di coesistere sullo stesso cluster con un corretto isolamento delle risorse, della sicurezza e così via. In questo contesto, un tenant può essere visualizzato come un sottoinsieme delle risorse del cluster configurate per essere utilizzate da un particolare gruppo di utenti a scopo esclusivo. La configurazione della multi-tenancy su un cluster Red Hat OpenShift offre i seguenti vantaggi:

- Riduzione di CapEx e OpEx grazie alla condivisione delle risorse del cluster
- Riduzione dell'overhead operativo e di gestione
- Proteggere i carichi di lavoro dalla contaminazione incrociata delle violazioni della sicurezza
- Protezione dei carichi di lavoro da un peggioramento inatteso delle performance dovuto a conflitti di risorse

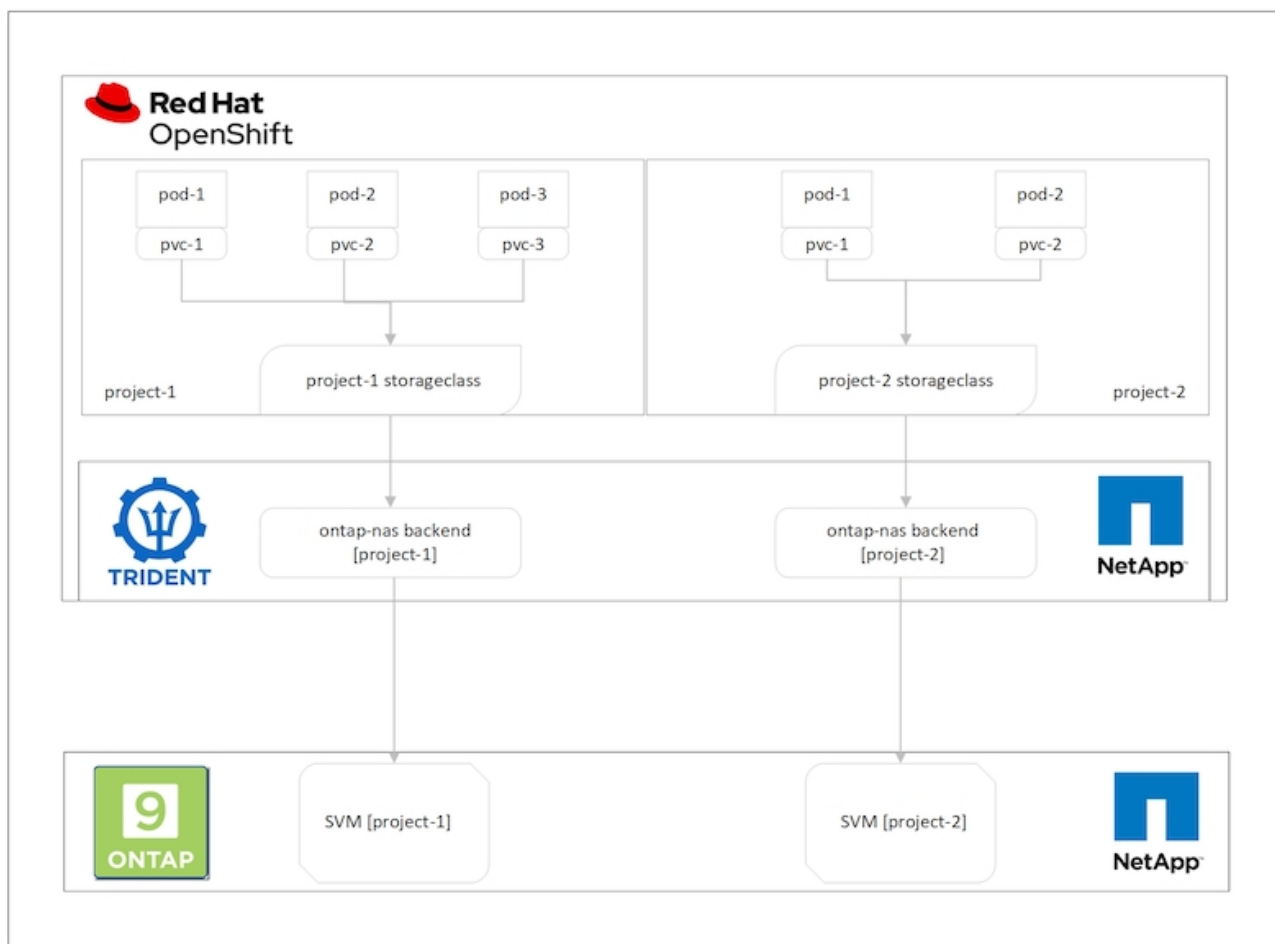
Per un cluster OpenShift multitenant completamente realizzato, è necessario configurare le quote e le restrizioni per le risorse cluster appartenenti a diversi bucket di risorse: Calcolo, storage, networking, sicurezza e così via. Anche se vengono trattati alcuni aspetti di tutti i bucket di risorse di questa soluzione, Ci concentriamo sulle Best practice per isolare e proteggere i dati serviti o consumati da più carichi di lavoro sullo stesso cluster Red Hat OpenShift configurando la multi-tenancy sulle risorse storage allocate dinamicamente da Astra Trident con il supporto di NetApp ONTAP.

### **Architettura**

Sebbene Red Hat OpenShift e Astra Trident supportati da NetApp ONTAP non forniscano l'isolamento tra i carichi di lavoro per impostazione predefinita, offrono un'ampia gamma di funzionalità che possono essere utilizzate per configurare la multi-tenancy. Per comprendere meglio la progettazione di una soluzione multi-tenant su un cluster Red Hat OpenShift con Astra Trident supportato da NetApp ONTAP, prendiamo in considerazione un esempio con una serie di requisiti e descriviamo la configurazione che lo circonda.

Supponiamo che un'organizzazione esegue due dei propri workload su un cluster Red Hat OpenShift nell'ambito di due progetti su cui lavorano due team diversi. I dati per questi carichi di lavoro risiedono su PVC che vengono forniti dinamicamente da Astra Trident su un backend NAS NetApp ONTAP. L'organizzazione deve progettare una soluzione multi-tenant per questi due carichi di lavoro e isolare le risorse utilizzate per questi progetti per garantire il mantenimento della sicurezza e delle performance, concentrandosi principalmente sui dati che servono tali applicazioni.

La seguente figura illustra la soluzione multi-tenant su un cluster Red Hat OpenShift con Astra Trident supportato da NetApp ONTAP.



## Requisiti tecnologici

1. Cluster di storage NetApp ONTAP
2. Cluster Red Hat OpenShift
3. Astra Trident

## Red Hat OpenShift – risorse cluster

Dal punto di vista del cluster Red Hat OpenShift, la risorsa di primo livello da iniziare è il progetto. Un progetto OpenShift può essere visto come una risorsa di cluster che divide l'intero cluster OpenShift in più cluster virtuali. Pertanto, l'isolamento a livello di progetto fornisce una base per la configurazione della multi-tenancy.

Successivamente, configurare RBAC nel cluster. La Best practice consiste nell'avere tutti gli sviluppatori che lavorano su un singolo progetto o workload configurati in un singolo gruppo di utenti nel provider di identità (IdP). Red Hat OpenShift consente l'integrazione di IdP e la sincronizzazione dei gruppi di utenti, consentendo così l'importazione di utenti e gruppi da IdP nel cluster. Ciò consente agli amministratori del cluster di separare l'accesso delle risorse del cluster dedicate a un progetto a un gruppo di utenti o a gruppi che lavorano su tale progetto, limitando in tal modo l'accesso non autorizzato a qualsiasi risorsa del cluster. Per ulteriori informazioni sull'integrazione di IdP con Red Hat OpenShift, consulta la documentazione ["qui"](#).

## NetApp ONTAP

È importante isolare lo storage condiviso che funge da provider di storage persistente per un cluster Red Hat

OpenShift per assicurarsi che i volumi creati sullo storage per ogni progetto appaiano agli host come se fossero creati su storage separato. A tale scopo, è possibile creare un numero di SVM (macchine virtuali di storage) su NetApp ONTAP pari al numero di progetti o carichi di lavoro e dedicare ogni SVM a un carico di lavoro.

## Astra Trident

Dopo aver creato diverse SVM per diversi progetti su NetApp ONTAP, è necessario mappare ciascuna SVM su un backend Trident diverso. La configurazione di back-end su Trident determina l'allocazione dello storage persistente alle risorse del cluster OpenShift e richiede il mapping dei dettagli della SVM. Questo dovrebbe essere il driver del protocollo per il backend al minimo. Facoltativamente, consente di definire il provisioning dei volumi sullo storage e di impostare limiti per la dimensione dei volumi o l'utilizzo degli aggregati e così via. È possibile trovare i dettagli relativi alla definizione dei backend Trident ["qui"](#).

## Red Hat OpenShift – risorse di storage

Dopo aver configurato i backend Trident, il passaggio successivo consiste nella configurazione di StorageClasses. Configura quante sono le classi di storage in cui sono presenti i backend, fornendo a ciascuna classe di storage l'accesso per eseguire lo spin up dei volumi su un solo backend. È possibile mappare StorageClass a un particolare backend Trident utilizzando il parametro storagePools durante la definizione della classe di storage. È possibile trovare i dettagli per definire una classe di storage ["qui"](#). Pertanto, esiste una mappatura uno a uno da StorageClass a Trident backend che punta a una SVM. In questo modo, tutte le attestazioni di storage tramite la StorageClass assegnata a quel progetto vengono gestite solo dalla SVM dedicata a quel progetto.

Poiché le classi di storage non sono risorse con spazio dei nomi, come possiamo garantire che le attestazioni di storage alla classe di storage di un progetto per pod in un altro namespace o progetto vengano rifiutate? La risposta è utilizzare ResourceQuotas. ResourceQuotas sono oggetti che controllano l'utilizzo totale delle risorse per progetto. Può limitare il numero e la quantità totale di risorse che possono essere utilizzate dagli oggetti nel progetto. Quasi tutte le risorse di un progetto possono essere limitate utilizzando ResourceQuotas e questo può aiutare le organizzazioni a ridurre i costi e le interruzioni dovute all'overprovisioning o all'eccessivo consumo di risorse. Consultare la documentazione ["qui"](#) per ulteriori informazioni.

In questo caso di utilizzo, dobbiamo limitare i pod di un progetto specifico al fine di richiedere storage da classi di storage non dedicate al loro progetto. A tale scopo, è necessario limitare le richieste di rimborso persistenti per volumi per altre classi di storage mediante l'impostazione `<storage-class-name>.storageclass.storage.k8s.io/persistentvolumeclaims` a 0. Inoltre, un amministratore del cluster deve garantire che gli sviluppatori di un progetto non abbiano accesso per modificare le ResourceQuotas.

## Configurazione

Per qualsiasi soluzione multi-tenant, nessun utente può avere accesso a più risorse di cluster di quelle richieste. Pertanto, l'intero insieme di risorse da configurare come parte della configurazione multi-tenancy è diviso tra cluster-admin, storage-admin e sviluppatori che lavorano su ciascun progetto.

La seguente tabella descrive le diverse attività che devono essere eseguite da diversi utenti:

| Ruolo                | Attività  |
|----------------------|---|
| <b>Cluster-admin</b> | Crea progetti per applicazioni o carichi di lavoro diversi  |
|                      | Creare ClusterRoles e RoleBinding per l'amministrazione dello storage                               |
|                      | Creazione di ruoli e associazioni per gli sviluppatori che assegnano l'accesso a progetti specifici |
|                      | [Facoltativo] configurare i progetti per pianificare i pod su nodi specifici                        |
| <b>Storage-admin</b> | Creare SVM su NetApp ONTAP  |
|                      | Creare backend Trident  |
|                      | Creare StorageClasses   |
|                      | Creare ResourceQuotas di storage  |
| <b>Sviluppatori</b>  | Convalidare l'accesso per creare o applicare patch a PVC o pod nel progetto assegnato               |
|                      | Convalida l'accesso per creare o applicare patch a PVC o pod in un altro progetto                   |
|                      | Convalida l'accesso per visualizzare o modificare progetti, ResourceQuotas e StorageClasses         |

## Configurazione

### Prerequisiti

- Cluster NetApp ONTAP
- Cluster Red Hat OpenShift
- Trident installato sul cluster
- Workstation di amministrazione con tool tridentctl e oc installati e aggiunti al percorso dei dollari
- Accesso amministratore a ONTAP
- Accesso cluster-admin al cluster OpenShift
- Il cluster è integrato con il provider di identità
- Il provider di identità è configurato in modo da distinguere in modo efficiente tra gli utenti di diversi team

### Configurazione: Attività di amministrazione del cluster

Le seguenti attività vengono eseguite dall'amministratore del cluster Red Hat OpenShift:

1. Accedere al cluster Red Hat OpenShift come amministratore del cluster.
2. Creare due progetti corrispondenti a progetti diversi.

```
oc create namespace project-1
oc create namespace project-2
```

### 3. Creare il ruolo di sviluppatore per il progetto-1.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
      - replicationcontrollers
```

```

- services
- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- trident.snapshots
EOF

```



La definizione del ruolo fornita in questa sezione è solo un esempio. I ruoli dello sviluppatore devono essere definiti in base ai requisiti dell'utente finale.

1. Allo stesso modo, creare ruoli di sviluppatore per il progetto 2.
2. Tutte le risorse storage di OpenShift e NetApp sono generalmente gestite da un amministratore dello storage. L'accesso per gli amministratori dello storage è controllato dal ruolo di operatore trident creato al momento dell'installazione di Trident. Inoltre, l'amministratore dello storage richiede l'accesso a ResourceQuotas per controllare il modo in cui lo storage viene utilizzato.
3. Creare un ruolo per la gestione di ResourceQuotas in tutti i progetti del cluster per associarlo all'amministratore dello storage.

```

cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
- verbs:
  - '*'
  apiGroups:
  - ''
  resources:
  - resourcequotas
- verbs:
  - '*'
  apiGroups:
  - quota.openshift.io
  resources:
  - '*'
EOF

```

4. Assicurarsi che il cluster sia integrato con il provider di identità dell'organizzazione e che i gruppi di utenti siano sincronizzati con i gruppi di cluster. L'esempio seguente mostra che il provider di identità è stato integrato con il cluster e sincronizzato con i gruppi di utenti.

```
$ oc get groups
NAME                                USERS
ocp-netapp-storage-admins          ocp-netapp-storage-admin
ocp-project-1                      ocp-project-1-user
ocp-project-2                      ocp-project-2-user
```

1. Configurare ClusterRoleBinding per gli amministratori dello storage.

```
cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF
```



Per gli amministratori dello storage, devono essere associati due ruoli: trident-operator e Resource-quote.

1. Creare i RoleBinding per gli sviluppatori che associano il ruolo Developer-project-1 al gruppo corrispondente (ocp-project-1) nel progetto-1.



```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF
```

2. Allo stesso modo, creare RoleBinding per gli sviluppatori che associano i ruoli di sviluppatore al gruppo di utenti corrispondente nel progetto-2.

### **Configurazione: Attività di amministrazione dello storage**

Le seguenti risorse devono essere configurate da un amministratore dello storage:

1. Accedere al cluster NetApp ONTAP come amministratore.
2. Accedere a Storage > Storage VM (Storage > Storage VM) e fare clic su Add (Aggiungi). Creare due SVM, una per il progetto 1 e l'altra per il progetto 2, fornendo i dettagli richiesti. Inoltre, creare un account vsadmin per gestire SVM e le relative risorse.

# Add Storage VM



STORAGE VM NAME

project-1-svm

## Access Protocol



SMB/CIFS, NFS

iSCSI



Enable SMB/CIFS



Enable NFS



Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

| Rule Index | Clients        | Access Protocols | Read-Only R... | Read/Wr |
|------------|----------------|------------------|----------------|---------|
|            | 10.61.181.0/24 | Any              | Any            | Any     |

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf\_8



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.224

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4



1. Accedere al cluster Red Hat OpenShift come amministratore dello storage.
2. Creare il backend per il progetto 1 e mapparla sulla SVM dedicata al progetto. NetApp consiglia di utilizzare l'account vsadmin di SVM per connettere il backend a SVM invece di utilizzare l'amministratore del cluster ONTAP.

```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_1",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.224",
  "svm": "project-1-svm",
  "username": "vsadmin",
  "password": "NetApp123"
}
EOF
```



Per questo esempio, viene utilizzato il driver ontap-nas. Utilizzare il driver appropriato per creare il backend in base al caso d'utilizzo.



Supponiamo che Trident sia installato nel progetto Trident.

1. Analogamente, creare il backend Trident per il progetto 2 e mapparla sulla SVM dedicata al progetto 2.
2. Quindi, creare le classi di storage. Creare la classe di storage per il project-1 e configurarla per utilizzare i pool di storage dal backend dedicato al project-1 impostando il parametro storagePools.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF
```

3. Allo stesso modo, creare una classe di storage per il progetto 2 e configurarla per utilizzare i pool di storage dal back-end dedicato al progetto 2.
4. Creare un ResourceQuota per limitare le risorse nel progetto 1, richiedendo storage da storageclasses dedicati ad altri progetti.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

5. Allo stesso modo, creare un ResourceQuota per limitare le risorse nel progetto 2, richiedendo lo storage da storageclasses dedicati ad altri progetti.

## Convalida

Per convalidare l'architettura multi-tenant configurata nei passaggi precedenti, attenersi alla seguente procedura:

### Convalidare l'accesso per creare PVC o pod nel progetto assegnato

1. Accedi come ocp-project-1-user, Developer in project-1.
2. Controllare l'accesso per creare un nuovo progetto.

```
oc create ns sub-project-1
```

3. Creare un PVC nel progetto 1 utilizzando lo storageclass assegnato al progetto 1.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Controllare il PV associato al PVC.

```
oc get pv
```

5. Convalida che il PV e il suo volume siano creati in una SVM dedicata al progetto 1 su NetApp ONTAP.

```
volume show -vserver project-1-svm
```

6. Creare un pod nel progetto 1 e montare il PVC creato nel passaggio precedente.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
        claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: test-pvc-project-1
EOF
```

7. Verificare che il pod sia in funzione e che il volume sia stato montato.

```
oc describe pods test-pvc-pod -n project-1
```

**Convalidare l'accesso per creare PVC o pod in un altro progetto o utilizzare risorse dedicate a un altro progetto**

1. Accedi come ocp-project-1-user, Developer in project-1.
2. Creare un PVC nel progetto 1 utilizzando lo storageclass assegnato al progetto 2.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF
```

### 3. Creare un PVC nel progetto 2.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

### 4. Assicurarsi che i PVC test-pvc-project-1-sc-2 e test-pvc-project-2-sc-1 non sono stati creati.

```
oc get pvc -n project-1
oc get pvc -n project-2
```

### 5. Creare un pod nel progetto 2.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
  - name: test-container
    image: nginx
    ports:
    - containerPort: 80
      name: "http-server"
EOF
```

### Convalida l'accesso per visualizzare e modificare progetti, ResourceQuotas e StorageClasses

1. Accedi come ocp-project-1-user, Developer in project-1.
2. Controllare l'accesso per creare nuovi progetti.

```
oc create ns sub-project-1
```

3. Convalidare l'accesso per visualizzare i progetti.

```
oc get ns
```

4. Verificare se l'utente può visualizzare o modificare ResourceQuotas nel progetto-1.

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. Verificare che l'utente abbia accesso per visualizzare gli storageclasses.

```
oc get sc
```

6. Controllare l'accesso per descrivere i magazzini.
7. Convalidare l'accesso dell'utente per modificare gli storageclasses.

```
oc edit sc project-1-sc
```

## Scalabilità: Aggiunta di più progetti

In una configurazione multi-tenant, l'aggiunta di nuovi progetti con risorse di storage richiede una configurazione aggiuntiva per garantire che la multi-tenancy non venga violata. Per aggiungere altri progetti in un cluster multi-tenant, attenersi alla seguente procedura:

1. Accedere al cluster NetApp ONTAP come amministratore dello storage.
2. Selezionare `Storage` → `Storage VMs` e fare clic su `Add`. Creare una nuova SVM dedicata al progetto
3. Inoltre, creare un account `vsadmin` per gestire SVM e le relative risorse.



# Add Storage VM



STORAGE VM NAME

project-3-svm

## Access Protocol

☒ SMB/CIFS, NFS

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

| Rule Index | Clients        | Access Protocols | Read-Only R... | Read/Wr |
|------------|----------------|------------------|----------------|---------|
|            | 10.61.181.0/24 | Any              | Any            | Any     |

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf\_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.228

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4

1. Accedere al cluster Red Hat OpenShift come amministratore del cluster.
2. Creare un nuovo progetto.

```
oc create ns project-3
```

3. Assicurarsi che il gruppo di utenti per il project-3 sia creato su IdP e sincronizzato con il cluster OpenShift.

```
oc get groups
```

#### 4. Creare il ruolo di sviluppatore per il progetto 3.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
  - verbs:
    - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
    - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
      - replicationcontrollers
      - services
```

```

- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- trident.snapshots
EOF

```



La definizione del ruolo fornita in questa sezione è solo un esempio. Il ruolo dello sviluppatore deve essere definito in base ai requisiti dell'utente finale.

1. Creare il RoleBinding per gli sviluppatori nel progetto-3 che legano il ruolo di sviluppatore-progetto-3 al gruppo corrispondente (ocp-progetto-3) nel progetto-3.

```

cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF

```

2. Accedere al cluster Red Hat OpenShift come amministratore dello storage
3. Creare un backend Trident e mapparlo sulla SVM dedicata al progetto 3. NetApp consiglia di utilizzare l'account vsadmin della SVM per connettere il backend alla SVM invece di utilizzare l'amministratore del cluster ONTAP.

```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_3",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.228",
  "svm": "project-3-svm",
  "username": "vsadmin",
  "password": "NetApp!23"
}
EOF
```



Per questo esempio, viene utilizzato il driver ontap-nas. Utilizzare il driver appropriato per creare il backend in base al caso d'utilizzo.



Supponiamo che Trident sia installato nel progetto Trident.

1. Creare la classe di storage per il progetto 3 e configurarla per utilizzare i pool di storage dal back-end dedicato al progetto 3.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF
```

2. Creare un ResourceQuota per limitare le risorse nel progetto 3, richiedendo storage da storageclasses dedicati ad altri progetti.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

3. Applicare patch alle ResourceQuotas in altri progetti per limitare l'accesso alle risorse in tali progetti dallo storage dallo storageclass dedicato al progetto-3.

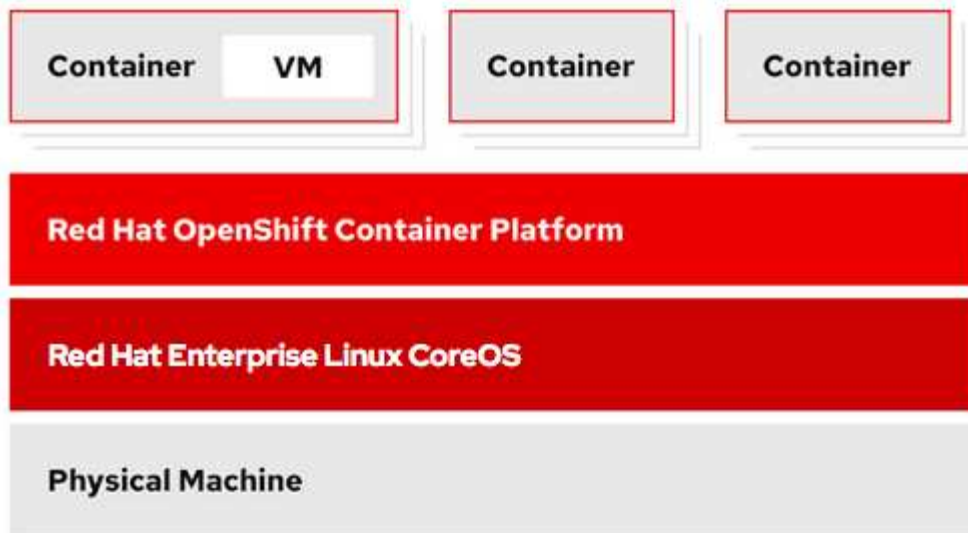
```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
```

## Virtualizzazione Red Hat OpenShift con NetApp ONTAP

### Virtualizzazione Red Hat OpenShift con NetApp ONTAP

A seconda del caso di utilizzo specifico, sia i container che le macchine virtuali (VM) possono fungere da piattaforme ottimali per diversi tipi di applicazioni. Pertanto, molte organizzazioni eseguono alcuni dei propri carichi di lavoro su container e alcune su macchine virtuali. Spesso, questo porta le organizzazioni ad affrontare ulteriori sfide dovendo gestire piattaforme separate: Un hypervisor per le macchine virtuali e un container orchestrator per le applicazioni.

Per affrontare questa sfida, Red Hat ha introdotto la virtualizzazione OpenShift (precedentemente nota come virtualizzazione nativa container) a partire dalla versione 4.6 di OpenShift. La funzionalità di virtualizzazione di OpenShift consente di eseguire e gestire macchine virtuali insieme ai container nella stessa installazione di OpenShift Container Platform, offrendo una funzionalità di gestione ibrida per automatizzare l'implementazione e la gestione delle macchine virtuali attraverso gli operatori. Oltre a creare macchine virtuali in OpenShift, con la virtualizzazione OpenShift, Red Hat supporta anche l'importazione di macchine virtuali da VMware vSphere, Red Hat Virtualization e Red Hat OpenStack Platform.



Alcune funzionalità come la migrazione live delle macchine virtuali, la clonazione dei dischi delle macchine virtuali, le snapshot delle macchine virtuali e così via sono supportate dalla virtualizzazione OpenShift con l'assistenza di Astra Trident, se supportata da NetApp ONTAP. Esempi di ciascuno di questi flussi di lavoro sono discussi più avanti in questo documento nelle rispettive sezioni.

Per ulteriori informazioni sulla virtualizzazione di Red Hat OpenShift, consulta la documentazione ["qui"](#).

#### Implementazione per la virtualizzazione OpenShift

### Implementa la virtualizzazione di Red Hat OpenShift con NetApp ONTAP

#### Prerequisiti

- Un cluster Red Hat OpenShift (successivo alla versione 4.6) installato su un'infrastruttura bare-metal con nodi di lavoro RHCOS
- Il cluster OpenShift deve essere installato tramite l'infrastruttura di provisioning del programma di installazione (IPI)
- Implementare i controlli dello stato delle macchine per mantenere l'ha per le macchine virtuali
- Un cluster NetApp ONTAP
- Astra Trident installato sul cluster OpenShift
- Un backend Trident configurato con una SVM sul cluster ONTAP
- StorageClass configurato sul cluster OpenShift con Astra Trident come provisioner
- Accesso cluster-admin al cluster Red Hat OpenShift
- Accesso amministrativo al cluster NetApp ONTAP
- Una workstation di amministrazione con tridentctl e oc tools installati e aggiunti al percorso dei dollari

Poiché la virtualizzazione OpenShift è gestita da un operatore installato sul cluster OpenShift, impone un overhead aggiuntivo su memoria, CPU e storage, che deve essere tenuto in considerazione durante la pianificazione dei requisiti hardware per il cluster. Consultare la documentazione ["qui"](#) per ulteriori dettagli.

In alternativa, è possibile specificare un sottoinsieme dei nodi del cluster OpenShift per ospitare gli operatori, i controller e le macchine virtuali della virtualizzazione OpenShift configurando le regole di posizionamento dei nodi. Per configurare le regole di posizionamento dei nodi per la virtualizzazione OpenShift, seguire la

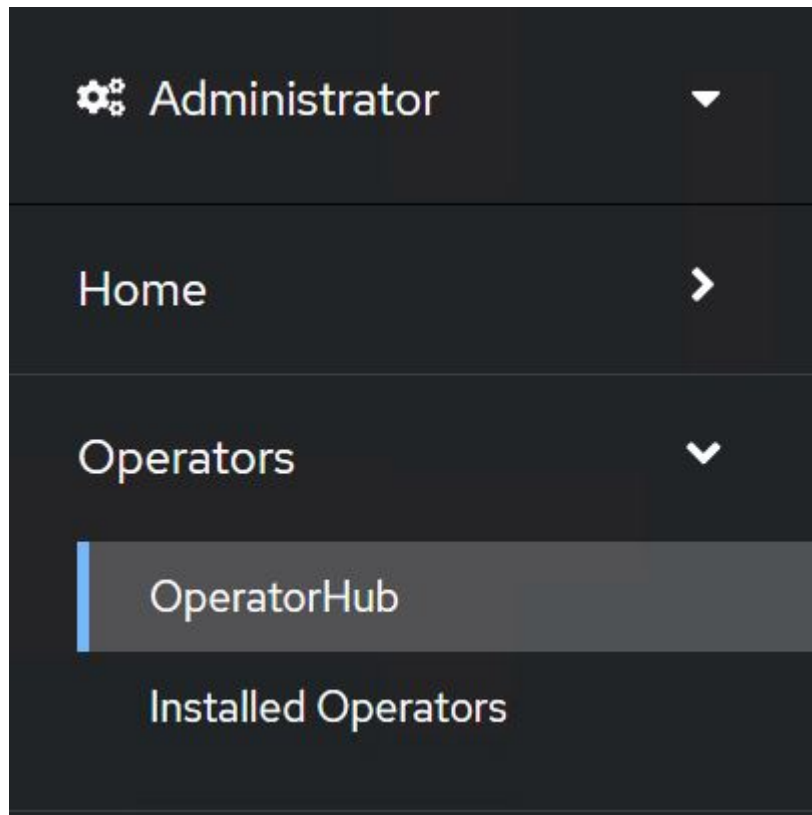
documentazione ["qui"](#).

Per il supporto dello storage OpenShift Virtualization, NetApp consiglia di disporre di un StorageClass dedicato che richieda storage da un particolare backend Trident, a sua volta supportato da una SVM dedicata. In questo modo si mantiene un livello di multi-tenancy in relazione ai dati serviti per i carichi di lavoro basati su macchine virtuali sul cluster OpenShift.

### Implementa la virtualizzazione di Red Hat OpenShift con NetApp ONTAP

Per installare OpenShift Virtualization, attenersi alla seguente procedura:

1. Accedi al cluster bare-metal Red Hat OpenShift con accesso cluster-admin.
2. Selezionare Administrator (Amministratore) dal menu a discesa Perspective (prospettiva).
3. Accedere a Operator > OperatorHub e cercare OpenShift Virtualization.



4. Selezionare il riquadro OpenShift Virtualization (virtualizzazione OpenShift) e fare clic su Install (Installa)



Install

## Latest version

2.6.2

## Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☒ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

## Provider type

Red Hat

## Provider

Red Hat

## Requirements

Your cluster must be installed on bare metal infrastructure with Red Hat Enterprise Linux CoreOS workers.

## Details

**OpenShift Virtualization** extends Red Hat OpenShift Container Platform, allowing you to host and manage virtualized workloads on the same platform as container-based workloads. From the OpenShift Container Platform web console, you can import a VMware virtual machine from vSphere, create new or clone existing VMs, perform live migrations between nodes, and more. You can use OpenShift Virtualization to manage both Linux and Windows VMs.

The technology behind OpenShift Virtualization is developed in the [KubeVirt](#) open source community. The KubeVirt project extends [Kubernetes](#) by adding additional virtualization resource types through [Custom Resource Definitions](#) (CRDs). Administrators can use Custom Resource Definitions to manage [VirtualMachine](#) resources alongside all other resources that Kubernetes provides.

5. Nella schermata Install Operator (Installa operatore), lasciare tutti i parametri predefiniti e fare clic su Install (Installa).

### Update channel \*

- ☐ 2.1
- ☐ 2.2
- ☐ 2.3
- ☐ 2.4
- ☒ stable

### Installation mode \*

- ☐ All namespaces on the cluster (default)  
This mode is not supported by this Operator
- ☒ A specific namespace on the cluster  
Operator will be available in a single Namespace only.

### Installed Namespace \*

- ☒ Operator recommended Namespace: **PR** openshift-cnv



#### Namespace creation

Namespace **openshift-cnv** does not exist and will be created.

- ☐ Select a Namespace

### Approval strategy \*

- ☒ Automatic
- ☐ Manual

Install

Cancel



OpenShift Virtualization  
provided by Red Hat

### Provided APIs



OpenShift  
Virtualization  
Deployment

**Required**

Represents the deployment of  
OpenShift Virtualization



6. Attendere il completamento dell'installazione da parte dell'operatore.



OpenShift Virtualization  
2.6.2 provided by Red Hat



## Installing Operator

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace openshift-cnv](#)

7. Una volta installato l'operatore, fare clic su Create HyperConverged (Crea HyperConverged).



OpenShift Virtualization  
2.6.2 provided by Red Hat



## Installed operator – operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

**HC** HyperConverged **Required**

Creates and maintains an OpenShift Virtualization Deployment

Create HyperConverged

[View installed Operators in Namespace openshift-cnv](#)

8. Nella schermata Create HyperConverged (Crea HyperConverged), fare clic su Create (Crea), accettando tutti i parametri predefiniti. Questa fase avvia l'installazione di OpenShift Virtualization.

**Name \***

kubevirt-hyperconverged

**Labels**

app=frontend

**Infra** >

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarily directly on each node running VMs/VMLs.

**Workloads** >

workloads HyperConvergedConfig influences the pod configuration (currently only placement) of components which need to be running on a node where virtualization workloads should be able to run. Changes to Workloads HyperConvergedConfig can be applied only without existing workload.

**Bare Metal Platform**

☒ true

BareMetalPlatform indicates whether the infrastructure is baremetal.

**Feature Gates** >

featureGates is a map of feature gate flags. Setting a flag to `true` will enable the feature. Setting `false` or removing the feature gate, disables the feature.

**Local Storage Class Name**

LocalStorageClassName the name of the local storage class.





[Create](#) [Cancel](#)

9. Dopo che tutti i pod sono stati spostati nello stato di esecuzione nello spazio dei nomi openshift-cnv e l'operatore di virtualizzazione OpenShift è in stato di successo, l'operatore è pronto per l'uso. È ora possibile creare macchine virtuali sul cluster OpenShift.

Project: openshift-cnv ▾

## Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

| Name ▾   | Managed Namespaces  | Status  | Last updated  | Provided APIs   |
|--|---|---|---|---|
|  <b>OpenShift Virtualization</b><br>2.6.2 provided by Red Hat |  openshift-cnv |  Succeeded<br>Up to date |  May 18, 8:02 pm | <a href="#">OpenShift Virtualization Deployment</a><br><a href="#">HostPathProvisioner deployment</a> |

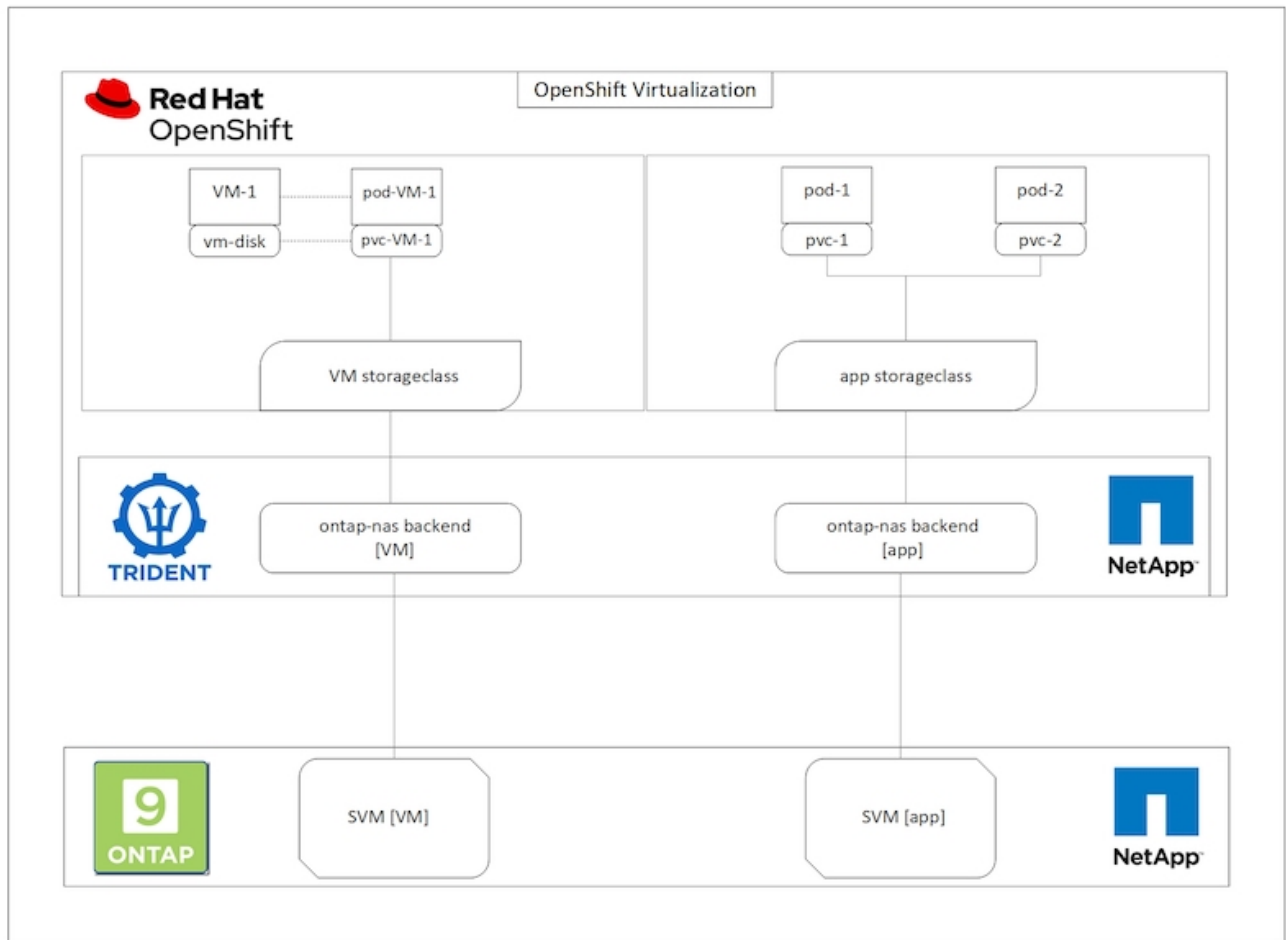
## Flussi di lavoro

### Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

#### Creare una macchina virtuale

Le VM sono implementazioni stateful che richiedono volumi per ospitare il sistema operativo e i dati. Con CNV,

poiché le macchine virtuali vengono eseguite come pod, le macchine virtuali vengono supportate da PVS ospitati su NetApp ONTAP tramite Trident. Questi volumi sono collegati come dischi e memorizzano l'intero file system, inclusa l'origine di boot della macchina virtuale.



Per creare una macchina virtuale sul cluster OpenShift, attenersi alla seguente procedura:

1. Accedere a workload > virtualizzazione > macchine virtuali e fare clic su Crea > con Wizard.
2. Selezionare il sistema operativo desiderato e fare clic su Next (Avanti).
3. Se nel sistema operativo selezionato non è configurata alcuna origine di avvio, è necessario configurarla. Per Boot Source (origine di avvio), selezionare se si desidera importare l'immagine del sistema operativo da un URL o da un registro e fornire i dettagli corrispondenti. Espandere Advanced (Avanzate) e selezionare Trident-Backed StorageClass (StorageClass supportato da Trident). Quindi fare clic su Next (Avanti).

## Boot source

This template does not have a boot source. Provide a custom boot source for this **CentOS 8.0+ VM** virtual machine.

### Boot source type \*

Import via URL (creates PVC) ▼

### Import URL \*

<https://access.cdn.redhat.com/content/origin/files/sha256/58/588167f828001e57688ec4b9b31c11a59d532489f527488ebc89ac5e952...>

Example: For RHEL, visit the [RHEL download page](#) (requires login) and copy the download link URL of the KVM guest image

☒ Mount this as a CD-ROM boot source ?

### Persistent Volume Claim size \*

5 GiB ▼

Ensure your PVC size covers the requirements of the uncompressed image and any other space requirements. More storage can be added later.

### ▼ Advanced

#### Storage class \*

basic (default) ▼

#### Access mode \*

Single User (RWO) ▼

#### Volume mode \*

Filesystem ▼

4. Se il sistema operativo selezionato ha già una sorgente di avvio configurata, il passaggio precedente può essere ignorato.
5. Nel riquadro Review and Create (Revisione e creazione), selezionare il progetto in cui si desidera creare la macchina virtuale e fornire i dettagli della macchina virtuale. Assicurarsi che l'origine di boot sia selezionata come Clone (Clona) e boot from CD-ROM (Avvio da CD-ROM) con il PVC appropriato assegnato per il sistema operativo selezionato.

- 1 Select template
- 2 Review and create

## Review and create

You are creating a virtual machine from the **Red Hat Enterprise Linux 8.0+ VM** template.

Project \*

PR default

Virtual Machine Name \* ⓘ

rhel8-light-bat

Flavor \*

Small: 1 CPU | 2 GiB Memory

Storage

40 GiB

Workload profile ⓘ

server

Boot source

Clone and boot from CD-ROM

PVC rhel8

ⓘ A new disk has been added to support the CD-ROM boot source. Edit this disk by customizing the virtual machine.

▼ Disk details

rootdisk-install - Blank - 20GiB - virtio - default Storage class

☒ Start this virtual machine after creation

Create virtual machine

Customize virtual machine

Back

Cancel

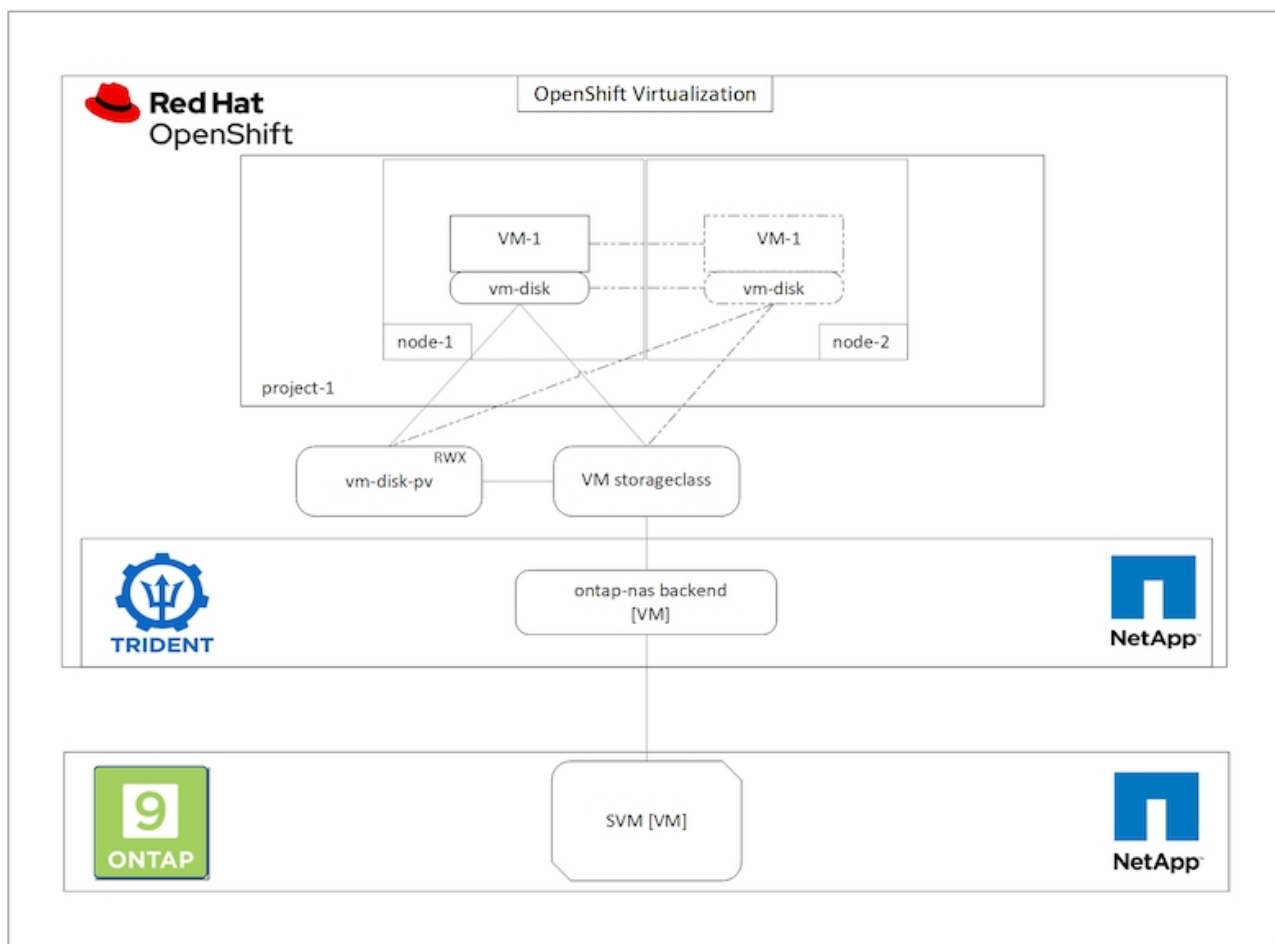
6. Se si desidera personalizzare la macchina virtuale, fare clic su **Customize Virtual Machine** (Personalizza macchina virtuale) e modificare i parametri richiesti.
7. Fare clic su **Create Virtual Machine** (Crea macchina virtuale) per creare la macchina virtuale; in questo modo viene fatto rotare in background un pod corrispondente.

Quando un'origine di avvio viene configurata per un modello o un sistema operativo da un URL o da un registro, crea un PVC in `openshift-virtualization-os-images` Proiettare e scaricare l'immagine guest KVM sul PVC. È necessario assicurarsi che i PVC modello dispongano di spazio di provisioning sufficiente per ospitare l'immagine guest KVM per il sistema operativo corrispondente. Questi PVC vengono quindi clonati e collegati come rootdisk alle macchine virtuali quando vengono creati utilizzando i rispettivi modelli in qualsiasi progetto.

## Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

### Migrazione VM Live

Live Migration è un processo di migrazione di un'istanza di macchina virtuale da un nodo all'altro in un cluster OpenShift senza downtime. Affinché la migrazione live funzioni in un cluster OpenShift, le macchine virtuali devono essere associate a PVC con modalità di accesso condivisa `ReadWriteMany`. Il backend Astra Trident configurato con una SVM su un cluster NetApp ONTAP abilitato per il protocollo NFS supporta l'accesso `ReadWriteMany` condiviso per i PVC. Pertanto, le macchine virtuali con PVC richieste da `StorageClasses` fornite da Trident da SVM abilitato NFS possono essere migrate senza downtime.



Per creare una macchina virtuale associata a PVC con accesso condiviso ReadWriteMany:

1. Accedere a workload > virtualizzazione > macchine virtuali e fare clic su Crea > con Wizard.
2. Selezionare il sistema operativo desiderato e fare clic su Next (Avanti). Supponiamo che il sistema operativo selezionato abbia già configurato una fonte di avvio.
3. Nel riquadro Review and Create (Revisione e creazione), selezionare il progetto in cui si desidera creare la macchina virtuale e fornire i dettagli della macchina virtuale. Assicurarsi che l'origine di boot sia selezionata come Clone (Clona) e boot from CD-ROM (Avvio da CD-ROM) con il PVC appropriato assegnato per il sistema operativo selezionato.
4. Fare clic su Customize Virtual Machine (Personalizza macchina virtuale), quindi su Storage (Storage).
5. Fare clic sui puntini di sospensione accanto a rootdisk e assicurarsi che sia selezionato lo storageclass con provisioning mediante Trident. Espandere Advanced (Avanzate) e selezionare Shared Access (RWX) (accesso condiviso) per Access Mode (modalità di accesso). Quindi fare clic su Save (Salva).

## Edit Disk

Type

Disk

Interface \*

virtio

Storage Class

basic (default)

▼ Advanced



Volume Mode

Filesystem

Volume Mode is set by Source PVC

Access Mode

Shared Access (RWX) - Not recommended for basic storage class

 **Access and Volume modes should follow storage feature matrix**  
[Learn more](#) 

Cancel

Save

6. Fare clic su Revisiona e conferma, quindi su Crea macchina virtuale.

Per migrare manualmente una macchina virtuale in un altro nodo del cluster OpenShift, attenersi alla seguente procedura.

1. Accedere a workload > virtualizzazione > macchine virtuali.

2. Per la macchina virtuale che si desidera migrare, fare clic sui puntini di sospensione, quindi fare clic su Migrate the Virtual Machine (Migra macchina virtuale).
3. Fare clic su Migrate (Migra) quando viene visualizzato il messaggio per confermare.

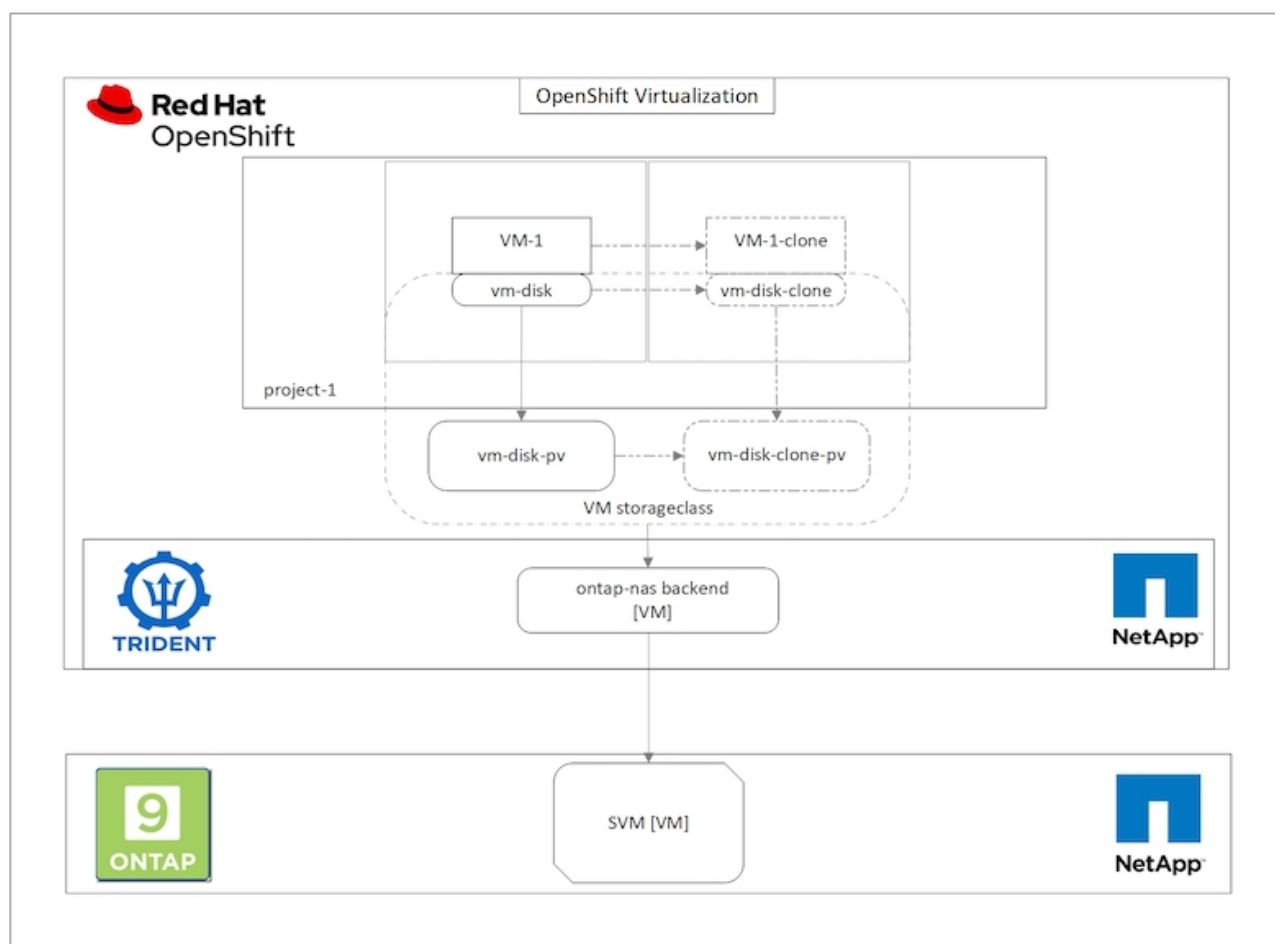


Un'istanza della macchina virtuale in un cluster OpenShift esegue automaticamente la migrazione a un altro nodo quando il nodo originale viene messo in modalità di manutenzione se evictionStrategy è impostato su LiveMigrate.

## Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

### Cloning delle macchine virtuali

Il cloning di una macchina virtuale esistente in OpenShift viene ottenuto con il supporto della funzionalità di cloning di Volume CSI di Astra Trident. Il cloning del volume CSI consente la creazione di un nuovo PVC utilizzando un PVC esistente come origine dati duplicando il suo PV. Dopo la creazione del nuovo PVC, funziona come entità separata e senza alcun collegamento o dipendenza dal PVC di origine.



La clonazione dei volumi CSI è soggetta a determinate restrizioni:

1. Il PVC di origine e il PVC di destinazione devono trovarsi nello stesso progetto.
2. La clonazione è supportata all'interno della stessa classe di storage.
3. La clonazione può essere eseguita solo quando i volumi di origine e di destinazione utilizzano la stessa



impostazione VolumeMode; ad esempio, un volume di blocco può essere clonato solo su un altro volume di blocco.

Le VM in un cluster OpenShift possono essere clonate in due modi:

1. Spegnendo la VM di origine
2. Mantenendo attiva la VM di origine

### **Spegnendo la VM di origine**

Clonare una macchina virtuale esistente spegnendo la macchina virtuale è una funzionalità OpenShift nativa implementata con il supporto di Astra Trident. Per clonare una macchina virtuale, attenersi alla seguente procedura.

1. Accedere a workload > Virtualization > Virtual Machines (carichi di lavoro > virtualizzazione > macchine virtuali) e fare clic sui puntini di sospensione accanto alla macchina virtuale che si desidera clonare.
2. Fare clic su Clone Virtual Machine (Clona macchina virtuale) e fornire i dettagli della nuova macchina virtuale.

# Clone Virtual Machine

|               |  |
|---------------|--|
| Name *        | <input type="text" value="rhel8-short-frog-clone"/>  |
| Description   | <div></div>  |
| Namespace *   | <div>default ▼</div>   |
|               | <input checked="" type="checkbox"/> Start virtual machine on clone   |
| Configuration | <div><div>Operating System</div><div>Red Hat Enterprise Linux 8.0 or higher</div><div>Flavor</div><div>Small: 1 CPU   2 GiB Memory</div><div>Workload Profile</div><div>server</div><div>NICs</div><div>default - virtio</div><div>Disks</div><div>cloudinitdisk - cloud-init disk</div><div>rootdisk - 20Gi - basic</div></div> |



The VM rhel8-short-frog is still running. It will be powered off while cloning.

Cancel

Clone Virtual Machine

3. Fare clic su Clone Virtual Machine (Clona macchina virtuale) per chiudere la macchina virtuale di origine e avviare la creazione della macchina virtuale clone.
4. Al termine di questa fase, è possibile accedere e verificare il contenuto della VM clonata.

## Mantenendo attiva la VM di origine

Una macchina virtuale esistente può anche essere clonata clonando il PVC esistente della macchina virtuale di origine e quindi creando una nuova macchina virtuale utilizzando il PVC clonato. Questo metodo non richiede l'arresto della VM di origine. Per clonare una macchina virtuale senza spegnerla, attenersi alla procedura riportata di seguito.

1. Accedere a Storage > PersistentVolumeClaims (Storage > PersistentVolumeClaims) e fare clic sui puntini di sospensione accanto al PVC collegato alla VM di origine.
2. Fare clic su Clone PVC e fornire i dettagli del nuovo PVC.

### Clone

Name \*

rhel8-short-frog-rootdisk-28dvv-clone



Access Mode \*

☐ Single User (RWO) ☒ Shared Access (RWX) ☐ Read Only (ROX)

Size \*

20 GiB ▼

PVC details

| Namespace   | Requested capacity | Access mode         |
|---|--------------------|---------------------|
|  default | 20 GiB             | Shared Access (RWX) |
| Storage Class   | Used capacity      | Volume mode         |
|  basic   | 2.2 GiB            | Filesystem          |

Cancel

Clone

3. Quindi fare clic su Clone (Clona). In questo modo si crea un PVC per la nuova macchina virtuale.
4. Accedere a workload > virtualizzazione > macchine virtuali e fare clic su Create > with YAML (Crea > con YAML).
5. Nella sezione spec > template > spec > Volumes (specifiche > modello > specifiche > volumi), collegare il PVC clonato invece del disco container. Fornire tutti gli altri dettagli della nuova macchina virtuale in base alle proprie esigenze.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvv-clone
```

6. Fare clic su Create (Crea) per creare la nuova macchina virtuale.
7. Una volta creata correttamente la macchina virtuale, accedere e verificare che la nuova macchina sia un clone della macchina virtuale di origine.

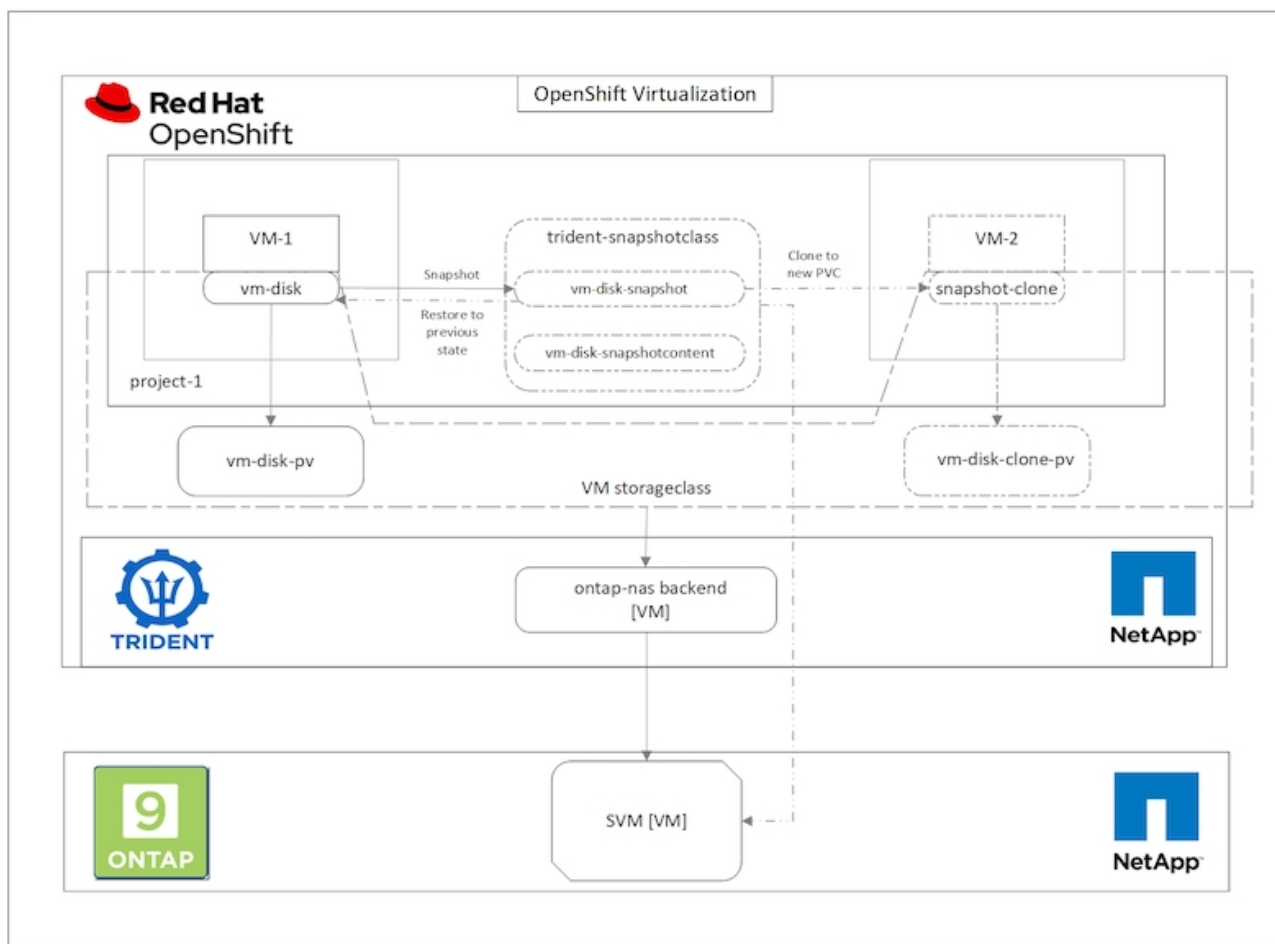
## **Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP**

### **Creare una macchina virtuale da un'istantanea**

Con Astra Trident e Red Hat OpenShift, gli utenti possono creare un'istantanea di un volume persistente su classi di storage fornite dall'IT. Con questa funzione, gli utenti possono eseguire una copia point-in-time di un volume e utilizzarlo per creare un nuovo volume o ripristinare lo stato precedente dello stesso volume. Ciò consente o supporta una varietà di casi di utilizzo, dal rollback ai cloni al ripristino dei dati.

Per le operazioni Snapshot in OpenShift, è necessario definire le risorse VolumeSnapshotClass, VolumeSnapshot e VolumeSnapshotContent.

- Un VolumeSnapshotContent è lo snapshot effettivo preso da un volume nel cluster. Si tratta di una risorsa a livello di cluster analoga a PersistentVolume per lo storage.
- VolumeSnapshot è una richiesta per la creazione dello snapshot di un volume. È analogo a un PersistentVolumeClaim.
- VolumeSnapshotClass consente all'amministratore di specificare attributi diversi per un'istantanea VolumeSnapshot. Consente di avere attributi diversi per diversi snapshot acquisiti dallo stesso volume.



Per creare un'istantanea di una macchina virtuale, attenersi alla seguente procedura:

1. Creare una classe `VolumeSnapshotClass` da utilizzare per creare un'istantanea `VolumeSnapshot`. Accedere a `Storage > VolumeSnapshotClasses` e fare clic su `Create VolumeSnapshotClass` (Crea `VolumeSnapshotClass`).
2. Immettere il nome della classe `Snapshot`, immettere `csi.trident.netapp.io` per il driver e fare clic su `Create` (Crea).

```
1 apiVersion: snapshot.storage.k8s.io/v1
2 kind: VolumeSnapshotClass
3 metadata:
4   name: trident-snapshot-class
5 driver: csi.trident.netapp.io
6 deletionPolicy: Delete
7
```

[Create](#)[Cancel](#)[Download](#)

3. Identificare il PVC collegato alla VM di origine e creare un'istanza del PVC. Selezionare Storage > VolumeSnapshots E fare clic su Create VolumeSnapshots (Crea snapshot Volume).
4. Selezionare il PVC per il quale si desidera creare l'istanza, immettere il nome dell'istanza o accettare il valore predefinito, quindi selezionare la VolumeSnapshotClass appropriata. Quindi fare clic su Create (Crea).

## Create VolumeSnapshot

[Edit YAML](#)

PersistentVolumeClaim \*

**PVC** rhel8-short-frog-rootdisk-28dvv

Name \*

rhel8-short-frog-rootdisk-28dvv-snapshot

Snapshot Class \*

**VSC** trident-snapshot-class

[Create](#)[Cancel](#)

5. In questo modo viene creata l'istanza del PVC in quel momento.

## Creare una nuova macchina virtuale dall'istantanea

1. Innanzitutto, ripristinare l'istantanea in un nuovo PVC. Accedere a Storage > VolumeSnapshots (Storage > VolumeSnapshots), fare clic sui puntini di sospensione accanto all'istantanea che si desidera ripristinare e fare clic su Restore as new PVC (Ripristina come nuovo PVC).
2. Inserire i dettagli del nuovo PVC e fare clic su Restore (Ripristina). In questo modo si crea un nuovo PVC.

## Restore as new PVC

When restore action for snapshot **rhel8-short-frog-rootdisk-28dvb-snapshot** is finished a new crash-consistent PVC copy will be created.

Name \*

rhel8-short-frog-rootdisk-28dvb-snapshot-restore

Storage Class \*

SC basic

Access Mode \*

☐ Single User (RWO) ☒ Shared Access (RWX) ☐ Read Only (ROX)

Size \*

20

GiB

### VolumeSnapshot details

Created at

 May 21, 12:46 am

Namespace

 default

Status

 Ready

API version

snapshot.storage.k8s.io/v1

Size

20 GiB

3. Quindi, creare una nuova macchina virtuale da questo PVC. Accedere a workload > virtualizzazione > macchine virtuali e fare clic su Create > with YAML (Crea > con YAML).

4. Nella sezione spec > template > spec > Volumes (specifiche > modello > specifiche > volumi), specificare il nuovo PVC creato da Snapshot anziché dal disco container. Fornire tutti gli altri dettagli della nuova macchina virtuale in base alle proprie esigenze.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvh-snapshot-restore
```

5. Fare clic su Create (Crea) per creare la nuova macchina virtuale.
6. Una volta creata correttamente la macchina virtuale, accedere e verificare che la nuova macchina virtuale abbia lo stesso stato della macchina virtuale il cui PVC è stato utilizzato per creare lo snapshot al momento della creazione dello snapshot.

## Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

### Migrazione di VM da VMware alla virtualizzazione OpenShift mediante Migration Toolkit for Virtualization

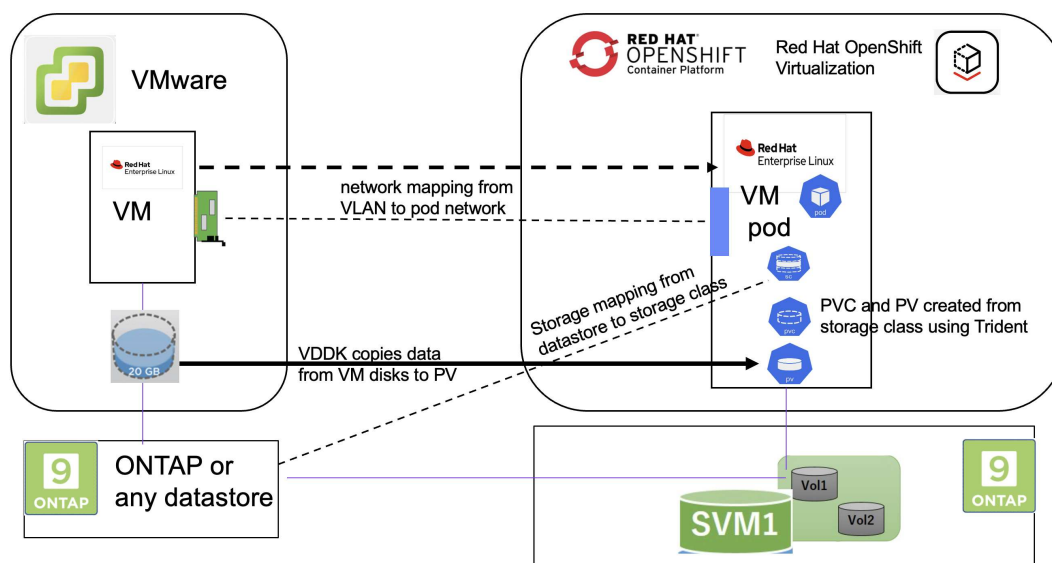
In questa sezione, vedremo come utilizzare l'Toolkit di migrazione per la virtualizzazione (MTV) per migrare le macchine virtuali da VMware alla virtualizzazione OpenShift eseguita sulla piattaforma contenitore OpenShift e integrata con lo storage NetApp ONTAP utilizzando Astra Trident.

Il seguente video mostra una dimostrazione della migrazione di una macchina virtuale RHEL da VMware alla virtualizzazione OpenShift utilizzando ontap-san per lo storage persistente.

### Utilizzo di Red Hat MTV per migrare le VM alla virtualizzazione OpenShift con lo storage NetApp ONTAP

Il diagramma seguente mostra una vista di alto livello della migrazione di una VM da VMware a Red Hat OpenShift Virtualization.

## Migration of VM from VMware to OpenShift Virtualization





## Prerequisiti per la migrazione dei campioni

### Su VMware

- È stata installata una macchina virtuale rhel 9 che utilizza rhel 9,3 con le seguenti configurazioni:
  - CPU: 2, memoria: 20 GB, disco rigido: 20 GB
  - credenziali utente: credenziali utente root e amministratore
- Dopo che la VM era pronta, il server postgresql è stato installato.
  - postgresql server è stato avviato e abilitato all'avvio

```
systemctl start postgresql.service`  
systemctl enable postgresql.service  
The above command ensures that the server can start in the VM in  
OpenShift Virtualization after migration
```

- Sono stati aggiunti 2 database, 1 tabella e 1 riga nella tabella. Fare riferimento a. ["qui"](#) Per le istruzioni per l'installazione del server postgresql su RHEL e per la creazione di database e voci di tabella.



Assicurarsi di avviare il server postgresql e abilitare il servizio all'avvio.

### Sul quadro strumenti OpenShift

Le seguenti installazioni sono state completate prima di installare MTV:

- Gruppo OpenShift 4.13.34
- ["Astra Trident 23,10"](#)
- Multipath sui nodi del cluster abilitato per iSCSI (per storage ontap-san). Consultare il codice yaml fornito per creare un set di daemon che abiliti iSCSI su ciascun nodo del cluster.
- Backend Trident e classe di storage per SAN ONTAP utilizzando iSCSI. Vedere i file yaml forniti per il backend tridente e la classe di archiviazione.
- ["Virtualizzazione OpenShift"](#)

Per installare iscsi e multipath sui nodi del cluster OpenShift, utilizzare il file yaml riportato di seguito

#### Preparazione dei nodi cluster per iSCSI

```
apiVersion: apps/v1  
kind: DaemonSet  
metadata:  
  namespace: trident  
  name: trident-iscsi-init  
  labels:  
    name: trident-iscsi-init  
spec:  
  selector:  
    matchLabels:
```

```

    name: trident-iscsi-init
template:
  metadata:
    labels:
      name: trident-iscsi-init
  spec:
    hostNetwork: true
    serviceAccount: trident-node-linux
    initContainers:
      - name: init-node
        command:
          - nsenter
          - --mount=/proc/1/ns/mnt
          - --
          - sh
          - -c
        args: ["$(STARTUP_SCRIPT)"]
        image: alpine:3.7
        env:
          - name: STARTUP_SCRIPT
            value: |
              #! /bin/bash
              sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils
device-mapper-multipath
      rpm -q iscsi-initiator-utils
      sudo sed -i 's/^\(node.session.scan\) .*/\1 = manual/'
/etc/iscsi/iscsid.conf
      cat /etc/iscsi/initiatorname.iscsi
      sudo mpathconf --enable --with_multipathd y --find_multipaths
n
      sudo systemctl enable --now iscsid multipathd
      sudo systemctl enable --now iscsi
    securityContext:
      privileged: true
    hostPID: true
    containers:
      - name: wait
        image: k8s.gcr.io/pause:3.1
    hostPID: true
    hostNetwork: true
    tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/master
    updateStrategy:
      type: RollingUpdate

```

Utilizzare il seguente file yaml per creare una configurazione back-end tridente per l'utilizzo dello storage san ONTAP

### Backend Trident per iSCSI

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

Utilizzare il seguente file yaml per creare la configurazione della classe di archiviazione tridente per l'utilizzo dello storage san ONTAP

### Classe di storage Trident per iSCSI

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

### Installare MTV

A questo punto è possibile installare il Migration Toolkit for Virtualization (MTV). Fare riferimento alle istruzioni fornite ["qui"](#) per informazioni sull'installazione.

L'interfaccia utente di Migration Toolkit for Virtualization (MTV) è integrata nella console Web OpenShift. È possibile fare riferimento ["qui"](#) per iniziare a utilizzare l'interfaccia utente per varie attività.

## Creare il fornitore di origine

Per migrare RHEL VM da VMware a OpenShift Virtualization, è necessario innanzitutto creare il provider di origine per VMware. Fare riferimento alle istruzioni ["qui"](#) per creare il provider di origine.

Per creare il provider di origine VMware sono necessari i seguenti elementi:

- URL vCenter
- Credenziali vCenter
- Identificazione utente del server vCenter
- Immagine VDDK in un repository

Creazione del provider di origine campione:

Select provider type \*

vm vSphere

Provider resource name \*

vmware-source

Unique Kubernetes resource name identifier

URL \*

URL of the vCenter SDK endpoint. Ensure the URL includes the "/sdk" path. For example: https://vCenter-host-example.com/sdk

VDDK init image

docker.repo.eng.netapp.com/banum/vddk:801

VDDK container image of the provider, when left empty some functionality will not be available

Username \*

administrator@vsphere.local

vSphere REST API user name.

Password \*

.....

vSphere REST API password credentials.

SSHA-1 fingerprint \*

The provider currently requires the SHA-1 fingerprint of the vCenter Server's TLS certificate in all circumstances. vSphere calls this the server's thumbprint.

Skip certificate validation

☒



MTV (Migration Toolkit for Virtualization) utilizza VMware Virtual Disk Development Kit (VDDK) SDK per accelerare il trasferimento dei dischi virtuali da VMware vSphere. Pertanto, si consiglia vivamente di creare un'immagine VDDK, anche se facoltativa. Per utilizzare questa funzione, è necessario scaricare VMware Virtual Disk Development Kit (VDDK), creare un'immagine VDDK e inviare l'immagine VDDK al registro delle immagini.

Seguire le istruzioni fornite ["qui"](#) Per creare e inviare l'immagine VDDK a un registro accessibile dal cluster OpenShift.

## Crea fornitore di destinazione

Il cluster host viene aggiunto automaticamente in quanto il provider di virtualizzazione OpenShift è il provider di origine.

## Creare un piano di migrazione

Seguire le istruzioni fornite ["qui"](#) per creare un piano di migrazione.

Durante la creazione di un piano, è necessario creare quanto segue se non è già stato creato:

- Mappatura di rete per mappare la rete di origine alla rete di destinazione.
- Mappatura dello storage per mappare il datastore di origine alla classe dello storage di destinazione. Per questo puoi scegliere la classe dello storage ontap-san.  
Una volta creato il piano di migrazione, lo stato del piano dovrebbe mostrare **Ready** e si dovrebbe ora essere in grado di **Start** il piano.

The screenshot shows the Red Hat OpenShift Migration console interface. The left sidebar contains navigation links: OperatorHub, Installed Operators, Workloads, Virtualization, Migration (selected), Overview, Providers for virtualization, Plans for virtualization (highlighted), NetworkMaps for virtualization, StorageMaps for virtualization, and Networking. The main panel displays a table of migration plans under the heading 'Plans'. The table has columns for Name, Source, Target, VMs, Status, and Description. A 'Create plan' button is in the top right. A 'Start' button is visible next to the first plan, which is in 'Ready' status. A hand cursor is pointing at the 'Ready' status of the first plan.

| Name                               | Source     | Target  | VMs | Status                        | Description                                |
|------------------------------------|------------|---------|-----|-------------------------------|--|
| PL mtv-migration-demo cold         | PR vmware  | PR host | 1   | Ready                         | Plan for migrating VM to OpenShift Virt... |
| PL vmware-osv-migration cold       | PR vmware2 | PR host | 1   | Succeeded 1 of 1 VMs migrated | Migrating RHEL 9 vm to OpenShift Virt...   |
| PL vmware-osv-migration-plan1 cold | PR vmware2 | PR host | 1   | Succeeded 1 of 1 VMs migrated |  |
| PL vmware-osv-migration-plan2 cold | PR vmware2 | PR host | 1   | Succeeded 1 of 1 VMs migrated | migrating RHEL 9 vm using ONTAP NFS...     |

Facendo clic su **Start** verrà eseguita una sequenza di passaggi per completare la migrazione della VM.

The screenshot displays the Red Hat OpenShift console interface. On the left, a dark sidebar contains a navigation menu with categories like OperatorHub, Workloads, Virtualization, Migration, Networking, Storage, Builds, Observe, Compute, User Management, and Administration. The 'Migration' section is expanded, showing sub-items like Overview, Providers for virtualization, Plans for virtualization, NetworkMaps for virtualization, and StorageMaps for virtualization. The main content area is titled 'Migration details by VM' and shows details for a migration plan named 'mtv-migration-demo'. It includes a search bar, a table of migration steps, and a 'Get logs' button. The migration steps are: Initialize migration (00:00:35), Allocate disks (00:00:00), Convert image to kubevirt (00:02:45), Copy disks (00:04:58), and Create VM (00:00:00). All steps are marked as 'Completed'. The overall status of the migration is 'Complete'.

Al termine di tutte le fasi, è possibile visualizzare le VM migrate facendo clic su **macchine virtuali** in **virtualizzazione** nel menu di navigazione a sinistra.

Vengono fornite le istruzioni per accedere alle macchine virtuali "qui".

È possibile accedere alla macchina virtuale e verificare il contenuto dei database postgresql. I database, le tabelle e le voci nella tabella devono essere uguali a quelli creati sulla macchina virtuale di origine.

## Protezione dei dati per la virtualizzazione OpenShift

### Protezione dei dati delle VM in OpenShift Virtualization con OpenShift API for Data Protection (OADP)

Autore: Banu Sundhar, NetApp

Questa sezione del documento di riferimento fornisce dettagli per la creazione di backup di macchine virtuali utilizzando l'API OpenShift per la protezione dei dati (OADP) con Velero su NetApp ONTAP S3 o NetApp StorageGRID S3. I backup dei volumi persistenti (PVS) dei dischi della macchina virtuale vengono creati utilizzando gli Snapshot CSI Astra Trident.

Le macchine virtuali nell'ambiente di virtualizzazione OpenShift sono applicazioni containerizzate che vengono eseguite nei nodi di lavoro della piattaforma container OpenShift. È importante proteggere i metadati delle macchine virtuali e i dischi persistenti delle macchine virtuali, in modo che in caso di perdita o danneggiamento possano essere ripristinati.

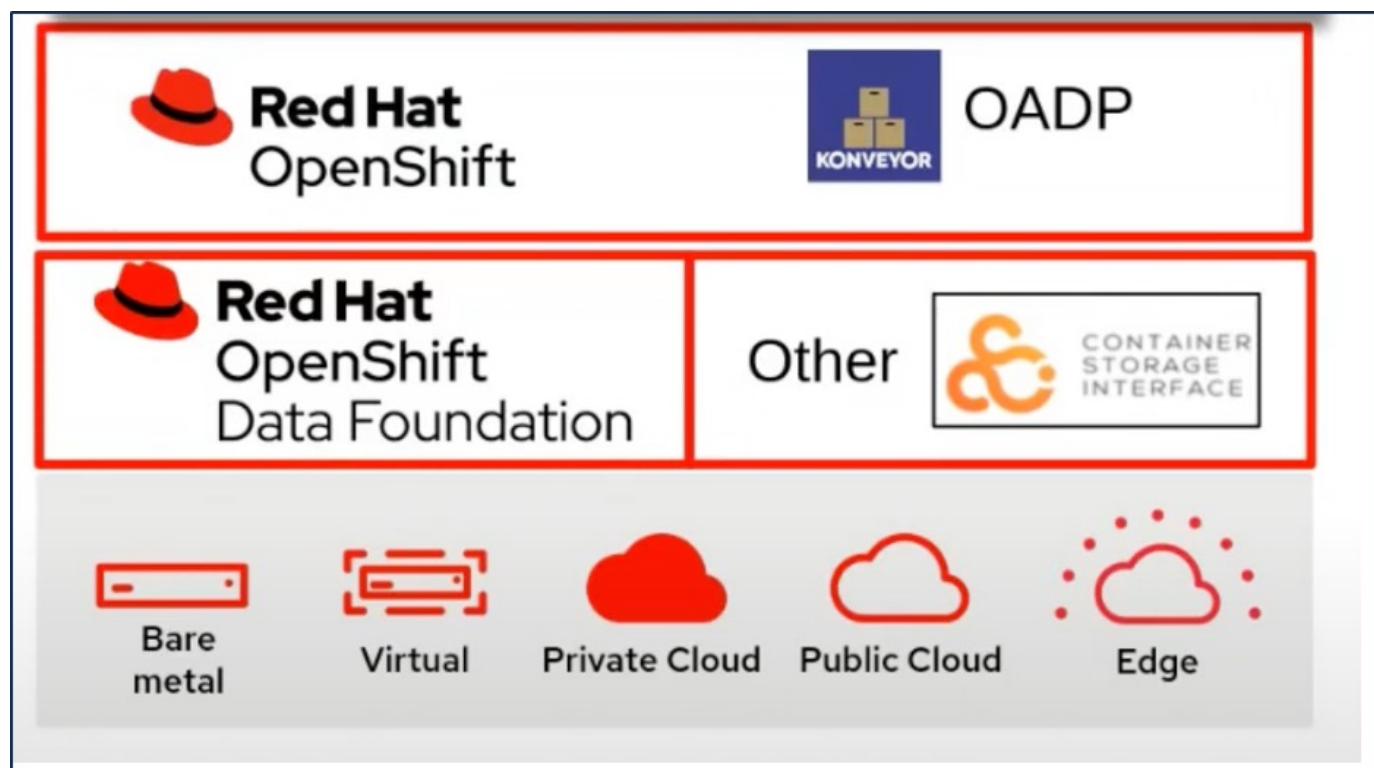
I dischi persistenti delle macchine virtuali di virtualizzazione OpenShift possono essere sottoposti a backup dallo storage ONTAP integrato nel cluster OpenShift utilizzando "CSI Astra Trident". In questa sezione usiamo "OpenShift API per la protezione dei dati (OADP)" Per eseguire il backup delle VM, inclusi i relativi volumi di dati su

- Storage a oggetti ONTAP

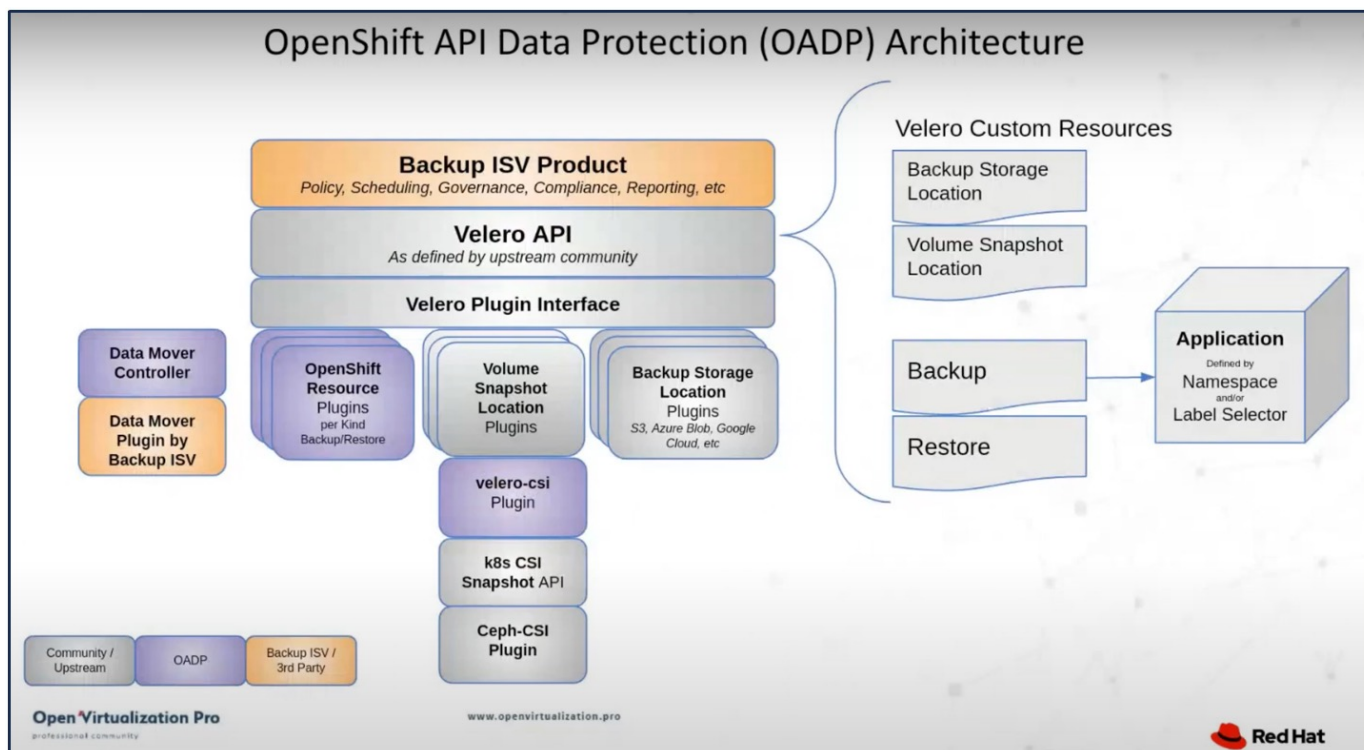
- StorageGRID

Quindi, eseguiamo il ripristino dal backup quando necessario.

OADP consente il backup, il ripristino e il disaster recovery delle applicazioni su un cluster OpenShift. I dati che possono essere protetti con OADP includono oggetti risorsa Kubernetes, volumi persistenti e immagini interne.



Red Hat OpenShift ha sfruttato le soluzioni sviluppate dalla comunità OpenSource per la protezione dei dati. ["Velero"](#) È uno strumento open-source per eseguire backup e ripristino in tutta sicurezza, eseguire disaster recovery e migrare risorse del cluster e volumi persistenti di Kubernetes. Per utilizzare Velero facilmente, OpenShift ha sviluppato l'operatore OADP e il plugin Velero per integrarsi con i driver di storage CSI. Il nucleo delle API OADP esposte si basa sulle API di Velero. Dopo aver installato e configurato l'operatore OADP, le operazioni di backup/ripristino che possono essere eseguite si basano sulle operazioni esposte dall'API Velero.



OADP 1,3 è disponibile dall'hub operatore del gruppo OpenShift 4,12 e versioni successive. Dispone di un Data Mover integrato che può spostare gli snapshot di volume CSI in un archivio di oggetti remoto. In questo modo è possibile ottenere portabilità e durata spostando le snapshot in una posizione di storage a oggetti durante il backup. Le snapshot sono quindi disponibili per il ripristino dopo un disastro.

**Di seguito sono riportate le versioni dei vari componenti utilizzati per gli esempi di questa sezione**

- Gruppo OpenShift 4,14
- OpenShift Virtualization installato tramite OperatorOpenShift Virtualization Operator fornito da Red Hat
- OADP Operator 1,13 fornito da Red Hat
- Velero CLI 1,13 per Linux
- Astra Trident 24,02
- ONTAP 9,12

"CSI Astra Trident"

"OpenShift API per la protezione dei dati (OADP)"

"Velero"

## Installazione dell'operatore OpenShift API for Data Protection (OADP)

### Prerequisiti

- Un cluster Red Hat OpenShift (versione successiva alla 4,12) installato in un'infrastruttura bare-metal con nodi di lavoro RHCOS
- Un cluster NetApp ONTAP integrato con il cluster utilizzando Astra Trident
- Un backend Trident configurato con una SVM sul cluster ONTAP
- StorageClass configurato sul cluster OpenShift con Astra Trident come provisioner



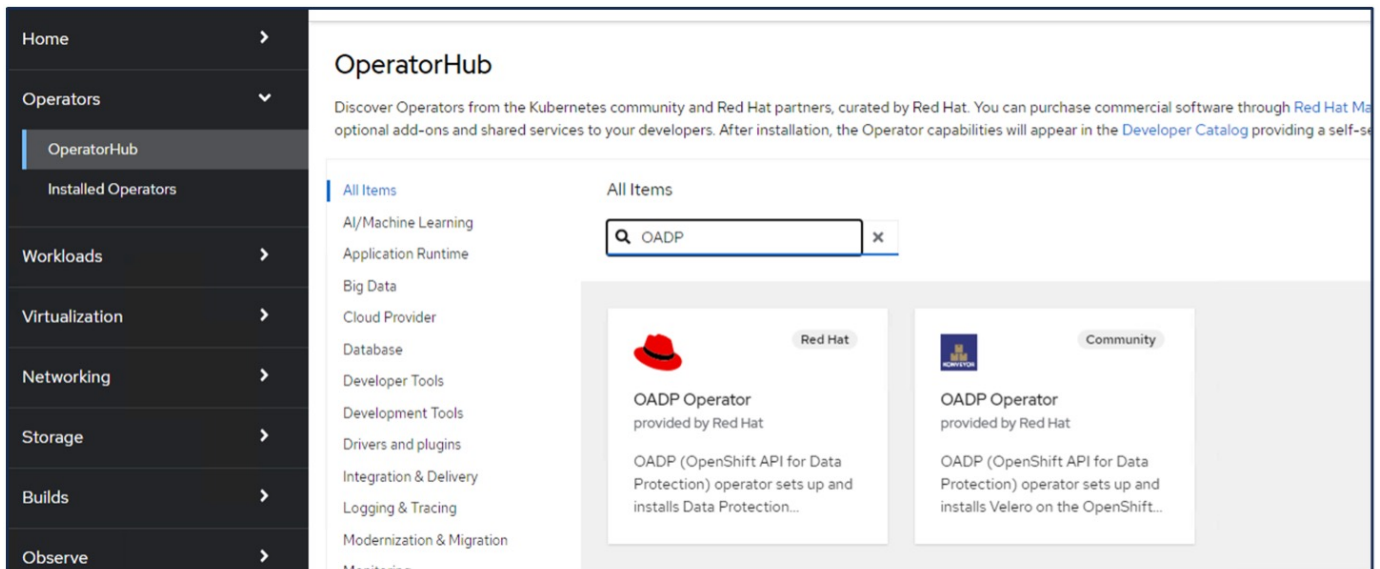
- Classe Snapshot Trident creata nel cluster
- Accesso cluster-admin al cluster Red Hat OpenShift
- Accesso amministrativo al cluster NetApp ONTAP
- Operatore di virtualizzazione OpenShift installato e configurato
- VM implementate in uno spazio dei nomi su OpenShift Virtualization
- Una workstation di amministrazione con tridentctl e oc tools installati e aggiunti al percorso dei dollari



Se si desidera eseguire un backup di una macchina virtuale quando è in esecuzione, è necessario installare l'agente guest QEMU su tale macchina virtuale. Se si installa la macchina virtuale utilizzando un modello esistente, l'agente QEMU viene installato automaticamente. QEMU consente all'agente ospite di disattivare i dati in-flight nel sistema operativo guest durante il processo di snapshot ed evitare possibili danneggiamenti dei dati. Se QEMU non è installato, è possibile arrestare la macchina virtuale prima di eseguire un backup.

## Procedura per l'installazione dell'operatore OADP

1. Andare all'Operator Hub del cluster e selezionare Red Hat OADP operator. Nella pagina Installa, utilizzare tutte le selezioni predefinite e fare clic su Installa. Nella pagina successiva, utilizzare nuovamente tutte le impostazioni predefinite e fare clic su Installa. L'operatore OADP sarà installato nello spazio dei nomi openshift-adp.





# OADP Operator

1.3.0 provided by Red Hat

Install

## Channel

stable-1.3

## Version

1.3.0

## Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

## Source

Red Hat

## Provider

Red Hat

## Infrastructure features

Disconnected

OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.








- [Installing OADP for application backup and restore](#)
- [Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM](#)
- [Frequently Asked Questions](#)

Project: All Projects

## Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#) Operator and ClusterServiceVersion using the [Operator SDK](#).

Name Search by name...

| Name  | Namespace  | Managed Namespaces   | Status  |
|---|--|--|---|
|  <b>OpenShift Virtualization</b><br>4.14.4 provided by Red Hat |  openshift-cnv                            |  openshift-cnv                            |  Succeeded<br>Up to date |
|  <b>OADP Operator</b><br>1.3.0 provided by Red Hat             |  openshift-adp                            |  openshift-adp                            |  Succeeded<br>Up to date |
|  <b>Package Server</b><br>0.0.1-snapshot provided by           |  openshift-operator-lifecycle-<br>manager |  openshift-operator-lifecycle-<br>manager |  Succeeded               |

Prerequisiti per la configurazione di Velero con i dettagli di ONTAP S3

Una volta completata l'installazione dell'operatore, configurare l'istanza di Velero. Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. Configurare ONTAP S3 utilizzando le procedure illustrate nella ["Sezione Gestione dello storage a oggetti della documentazione di ONTAP"](#). Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di ONTAP S3.

- Un'interfaccia logica (LIF) che può essere usata per accedere a S3
- Credenziali utente per accedere a S3 che include la chiave di accesso e la chiave di accesso segreta
- Un nome bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'archiviazione a oggetti, è necessario installare il certificato TLS sul server di archiviazione a oggetti.

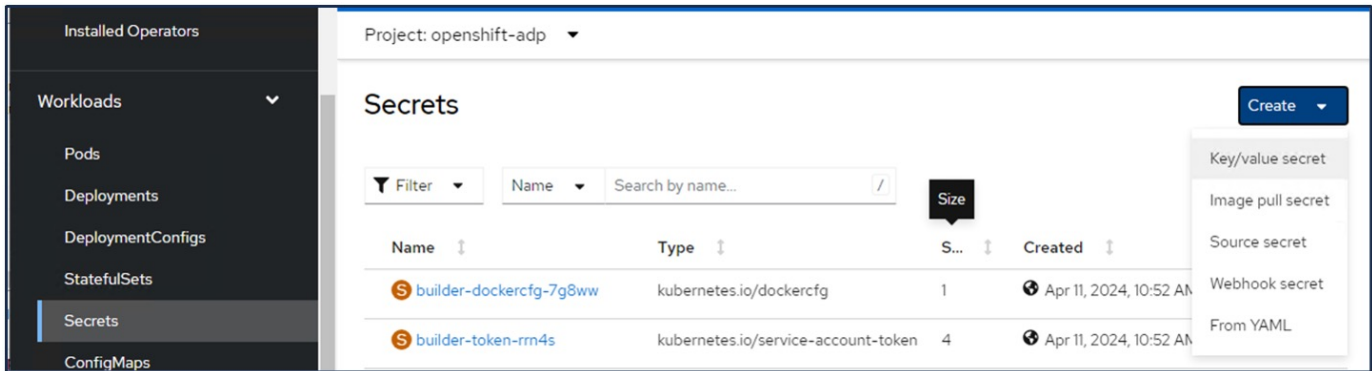
Prerequisiti per la configurazione di Velero con i dettagli di StorageGRID S3

Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. È possibile configurare StorageGRID S3 utilizzando le procedure illustrate nella ["Documentazione StorageGRID"](#). Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di StorageGRID S3.

- L'endpoint che può essere utilizzato per accedere a S3
- Credenziali utente per accedere a S3 che include la chiave di accesso e la chiave di accesso segreta
- Un nome bucket in S3 per i backup con autorizzazioni di accesso per l'utente
- Per un accesso sicuro all'archiviazione a oggetti, è necessario installare il certificato TLS sul server di archiviazione a oggetti.

Procedura di configurazione di Velero

- Innanzitutto, creare un segreto per una credenziale utente ONTAP S3 o per le credenziali utente StorageGRID tenant. Verrà utilizzato per configurare Velero in un secondo momento. È possibile creare un segreto dall'interfaccia CLI o dalla console Web. Per creare un segreto dalla console Web, selezionare segreti, quindi fare clic su chiave/valore segreto. Fornire i valori per il nome della credenziale, la chiave e il valore come mostrato. Assicurarsi di utilizzare l'ID chiave di accesso e la chiave di accesso segreta dell'utente S3. Assegnare un nome appropriato al segreto. Nell'esempio seguente, viene creato un segreto con credenziali utente di ONTAP S3 denominato credenziali ontap-S3.



Project: openshift-adp ▼

## Create key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

**Secret name \***

Unique name of the new secret.

**Key \***

**Value**

Drag and drop file with your value here or browse to upload it.

```
[default]
aws_access_key_id=<Access Key Id of S3 user>
aws_secret_access_key=<Secret Access Key of S3 user>
```

+ Add key/value





Per creare un segreto denominato sg-S3-credenziali dall'interfaccia CLI, è possibile utilizzare il seguente comando.

```
# oc create secret generic cloud-credentials --namespace openshift-adp --
from-file cloud=cloud-credentials.txt
```

credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

```
[default]
aws_access_key_id=<Access Key Id of S3 user>
aws_secret_access_key=<Secret Access Key of S3 user>
```


- Quindi, per configurare Velero, selezionare Installed Operators dalla voce di menu in Operators, fare clic sull'operatore OADP, quindi selezionare la scheda DataProtectionApplication.

|                     |   |  |   |  |   |
|---------------------|---|--|---|--|---|
| Home                | Installed Operators   |  |   |  |   |
| Operators           | Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the <a href="#">Understanding Operators documentation</a> or create an Operator and ClusterServiceVersion using the <a href="#">Operator SDK</a> . |  |   |  |   |
| OperatorHub         | <div> <div>Name</div> <div>Search by name...</div> </div>   |  |   |  |   |
| Installed Operators |   |  |   |  |   |
| Workloads           |   |  |   |  |   |
| Virtualization      |   |  |   |  |   |
| Networking          |   |  |   |  |   |
|                     | Name  | Managed Namespaces   | Status  | Last updated   | Provided APIs   |
|                     |  <b>OADP Operator</b><br>1.3.0 provided by Red Hat   |  <b>openshift-adp</b> |  Succeeded<br>Up to date |  Apr 11, 2024, 10:53 AM | <a href="#">BackupRepository</a><br><a href="#">Backup</a><br><a href="#">BackupStorageLocation</a><br><a href="#">DeleteBackupRequest</a><br><a href="#">View 11 more...</a> |

Fare clic su Create DataProtectionApplication. Nella vista modulo, specificare un nome per l'applicazione DataProtection o utilizzare il nome predefinito.

Project: openshift-adp

Installed Operators > Operator details


**OADP Operator**  
 1.3.0 provided by Red Hat

Actions

ServerStatusRequest
VolumeSnapshotLocation
DataDownload
DataUpload
CloudStorage
DataProtectionApplication

DataProtectionApplications

Create DataProtectionApplication

Passare ora alla visualizzazione YAML e sostituire le informazioni sulle specifiche come mostrato negli esempi di file yaml riportati di seguito.

### Esempio di file yaml per la configurazione di Velero con ONTAP S3 come backupLocation

```

spec:
  backupLocations:
    - velero:
        config:
            insecureSkipTLSVerify: 'true' ->use this for https communication
with ONTAP S3
            profile: default
            region: us-east
            s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
            s3Url: 'https://10.xx.xx.xx' ->Ensure TLS certificate for S3 is
configured
            credential:
                key: cloud
                name: ontap-s3-credentials ->previously created secret
            default: true
            objectStorage:
                bucket: velero ->Your bucket name previously created in S3 for
backups
                prefix: demobackup ->The folder that will be created in the
bucket
            provider: aws
        configuration:
            nodeAgent:
                enable: true
                uploaderType: kopia
                #default Data Mover uses Kopia to move snapshots to Object Storage
            velero:
                defaultPlugins:
                    - csi ->Add this plugin
                    - openshift
                    - aws
                    - kubevirt ->Add this plugin

```

**File yaml di esempio per la configurazione di Velero con StorageGRID S3 come backupLocation e snapshotLocation**

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

La sezione delle specifiche nel file yaml deve essere configurata in modo appropriato per i seguenti parametri, come nell'esempio precedente

### BackupLocations

ONTAP S3 o StorageGRID S3 (con le relative credenziali e altre informazioni come mostrato in yaml) è configurato come BackupLocation predefinito per velero.

### SnapshotLocations

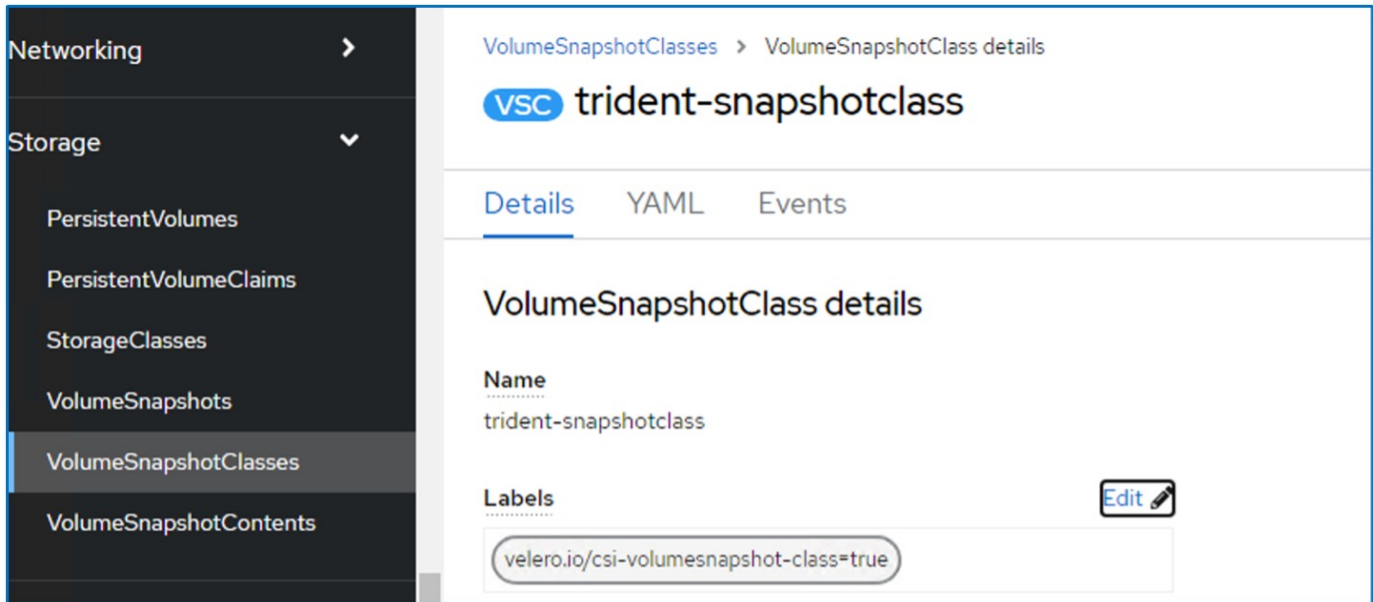
Se si utilizzano gli snapshot Container Storage Interface (CSI), non è necessario specificare una posizione dello snapshot perché si creerà un VolumeSnapshotClass CR per registrare il driver CSI. Nel nostro esempio, si utilizza Astra Trident CSI e in precedenza si è creato VolumeSnapshotClass CR utilizzando il driver Trident CSI.

### Attiva plugin CSI

Aggiungere csi ai prefaultPlugin per Velero per eseguire il backup dei volumi persistenti con gli snapshot CSI. I plug-in di Velero CSI, per eseguire il backup dei PVC supportati da CSI, sceglieranno VolumeSnapshotClass nel cluster su cui è impostata l'etichetta **velero.io/csi-volumesnapshot-class**. Per questo

- È necessario creare il tridente VolumeSnapshotClass.

- Modificare l'etichetta della classe trident-snapshotclass e impostarla su **velero.io/csi-volumesnapshot-class=true** come mostrato di seguito.



Verificare che gli snapshot possano persistere anche se gli oggetti VolumeSnapshot vengono eliminati. A tale scopo, impostare **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi perderà completamente tutti i PVC di cui è stato eseguito il backup.

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



VolumeSnapshotClasses > VolumeSnapshotClass details

**vsc trident-snapshotclass**

Details | YAML | Events

### VolumeSnapshotClass details

**Name**  
trident-snapshotclass

**Labels** [Edit](#)

velero.io/csi-volumesnapshot-class=true


**Annotations**  
[1 annotation](#)

**Driver**  
csi.trident.netapp.io

**Deletion policy**  
Retain

Verificare che DataProtectionApplication sia stato creato e che sia in condizioni: riconciliato.

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat


Actions

ServerStatusRequest | VolumeSnapshotLocation | DataDownload | DataUpload | CloudStorage | **DataProtectionApplication**

### DataProtectionApplications

[Create DataProtectionApplication](#)


Name Search by name... /

| Name   | Kind                      | Status                | Labels    |
|--|---------------------------|-----------------------|-----------|
|  <b>velero-demo</b> | DataProtectionApplication | Condition: Reconciled | No labels |

L'operatore OADP creerà un BackupStorageLocation corrispondente. Questo verrà utilizzato durante la creazione di un backup.

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat


Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRecovery

## BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

| Name ▴ ▾   | Kind ▴ ▾              | Status ▴ ▾       | Labels ▴ ▾   |
|--|-----------------------|------------------|--|
|  <b>velero-demo-1</b> | BackupStorageLocation | Phase: Available | <div>app.kubernetes.io/component=bsl</div> <div>app.kubernetes.io/instance=velero-demo-1</div> <div>app.kubernetes.io/managed-by=oadp-operator</div> <div>app.kubernetes.io/name=oadp-operator-velero</div> <div>openshift.io/oadp=True</div> <div>openshift.io/oadp-registry=True</div> |

## Creazione di backup su richiesta per le VM in OpenShift Virtualization

### Procedura per creare un backup di una VM

Per creare un backup su richiesta dell'intera VM (metadati VM e dischi VM), fare clic sulla scheda **Backup**. In questo modo viene creata una risorsa personalizzata di backup (CR). Viene fornito un yaml di esempio per creare la CR di backup. Utilizzando questo yaml, verrà eseguito il backup della VM e dei relativi dischi nello spazio dei nomi specificato. È possibile impostare parametri aggiuntivi come illustrato nella ["documentazione"](#).


Uno snapshot dei volumi persistenti che eseguono il backup dei dischi verrà creato dal CSI. Viene creato un backup della macchina virtuale insieme all'istantanea dei relativi dischi e memorizzato nella posizione di backup specificata nel codice yaml. Il backup rimarrà nel sistema per 30 giorni come specificato nel ttl.

```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
  previously created
                                when Velero is configured.
  ttl: 720h0m0s
```

Una volta completato il backup, la sua fase viene visualizzata come completata.

Project: openshift-adp

Installed Operators > Operator details

 OADP Operator

1.3.0 provided by Red Hat

Actions

Details

YAML

Subscription

Events

All instances

BackupRepository

Backup

BackupStorageLocation

DeleteBa

Backups


Create Backup

Name

Search by name...

| Name    | Kind   | Status                        | Labels                                   |
|---------|--------|-------------------------------|--|
| backup1 | Backup | Phase: <span>Completed</span> | velero.io/storage-location=velero-demo-1 |

È possibile esaminare il backup nell'archiviazione a oggetti con l'aiuto di un'applicazione browser S3. Il percorso del backup viene visualizzato nel bucket configurato con il nome del prefisso (velero/demobackup). Il contenuto del backup include gli snapshot del volume, i log e altri metadati della macchina virtuale.



In StorageGRID, è anche possibile utilizzare la console S3 disponibile in Gestione tenant per visualizzare gli oggetti di backup.

Path: / demobackup/ backups/ backup1/

| Name                                       | Size      | Type      | Last Modified         | Storage Class |
|--|-----------|-----------|-----------------------|---------------|
| ..   |           |           |                       |               |
| backup1.tar.gz                             | 230.36 KB | GZ File   | 4/15/2024 10:26:29 PM | STANDARD      |
| velero-backup.json                         | 3.35 KB   | JSON File | 4/15/2024 10:26:29 PM | STANDARD      |
| backup1-resource-list.json.gz              | 1.12 KB   | GZ File   | 4/15/2024 10:26:29 PM | STANDARD      |
| backup1-itemoperations.json.gz             | 600 bytes | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-volumesnapshots.json.gz            | 29 bytes  | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-podvolumebackups.json.gz           | 29 bytes  | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-results.gz                         | 49 bytes  | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-csi-volumesnapshotclasses.json.gz  | 426 bytes | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-csi-volumesnapshotcontents.json.gz | 1.43 KB   | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-csi-volumesnapshots.json.gz        | 1.34 KB   | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |
| backup1-logs.gz                            | 13.49 KB  | GZ File   | 4/15/2024 10:26:28 PM | STANDARD      |

Creazione di backup pianificati per le VM in OpenShift Virtualization

Per creare backup in base a una pianificazione, è necessario creare una pianificazione CR. La pianificazione è semplicemente un'espressione Cron che consente di specificare l'ora in cui si desidera creare il backup. Un esempio di yaml per creare una pianificazione CR.

```

apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s

```


Cron Expression 0 7 \* \* \* significa che ogni giorno verrà creato un backup alle 7:00:00. Vengono inoltre specificati gli spazi dei nomi da includere nel backup e la posizione di archiviazione per il backup. Quindi, invece di un CR di backup, il CR di pianificazione viene utilizzato per creare un backup all'ora e alla frequenza specificate.

Una volta creata, la pianificazione viene attivata.

Project: openshift-adp ▼

---

[Installed Operators](#) > [Operator details](#)

 **OADP Operator**  
1.3.0 provided by Red Hat



---

[storageLocation](#) [DeleteBackupRequest](#) [DownloadRequest](#) [PodVolumeBackup](#) [PodVolumeRestore](#) [Restore](#) [Schedule](#)

---

## Schedules


Name ▼ Search by name... /

| Name ↕  | Kind ↕   | Status ↕   | Labels ↕  |
|---|----------|--|-----------|
|  schedule1 | Schedule | Phase:  Enabled | No labels |

I backup verranno creati in base a questa pianificazione e possono essere visualizzati dalla scheda Backup.

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat


Actions ▾

Events All instances BackupRepository **Backup** BackupStorageLocation DeleteBackupRequest DownloadRequest

## Backups

Create Backup

Name ▾ Search by name... /

| Name ▴ ▾   | Kind ▴ ▾ | Status ▴ ▾        | Labels ▴ ▾  |
|--|----------|-------------------|---|
|  schedule1-20240416140507 | Backup   | Phase: InProgress | velero.io/schedule-name=schedule1<br>velero.io/storage-location=velero-demo-1 |

## Ripristinare una VM da un backup

### Prerequisiti


Per eseguire il ripristino da un backup, supponiamo che lo spazio dei nomi in cui esisteva la macchina virtuale sia stato eliminato accidentalmente.

## Ripristinare nello stesso namespace

Per eseguire il ripristino dal backup appena creato, è necessario creare una risorsa personalizzata di ripristino (CR). Dobbiamo fornirgli un nome, fornire il nome del backup da cui eseguire il ripristino e impostare su true. È possibile impostare parametri aggiuntivi come illustrato nella ["documentazione"](#). Fare clic sul pulsante Crea.

Project: openshift-adp

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat

Actions

est

DownloadRequest

PodVolumeBackup

PodVolumeRestore

**Restore**

Schedule

ServerStatusRequest

VolumeSnap

Restores


Create Restore

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true
```

Quando la fase è completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui è stato acquisito lo snapshot. (Se il backup è stato creato quando la VM era in esecuzione, ripristinando la VM dal backup si avvia la VM ripristinata e la si porta in esecuzione). La VM viene ripristinata nello stesso namespace.

Project: openshift-adp

Installed Operators > Operator details

 **OADP Operator**  
1.3.0 provided by Red Hat

Actions

est

DownloadRequest

PodVolumeBackup

PodVolumeRestore

**Restore**

Schedule

ServerStatusRequest



VolumeSr

Restores

Create Restore

Name

Search by name...

| Name   | Kind    | Status   | Labels    |
|--|---------|--|-----------|
|  restore1 | Restore | Phase:  Completed | No labels |

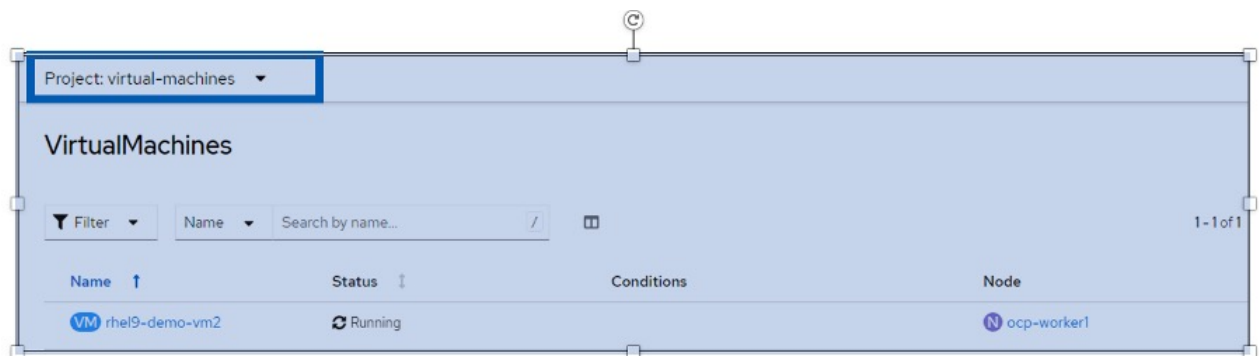
## Ripristinare in un namespace diverso

Per ripristinare la macchina virtuale in uno spazio dei nomi diverso, è possibile fornire un `namespaceMapping` nella definizione yaml di Restore CR.

Il seguente file yaml di esempio crea un Restore CR per ripristinare una VM e i relativi dischi nello spazio dei nomi `virtual-machine-demo` quando il backup è stato eseguito nello spazio dei nomi `virtual-machines`.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

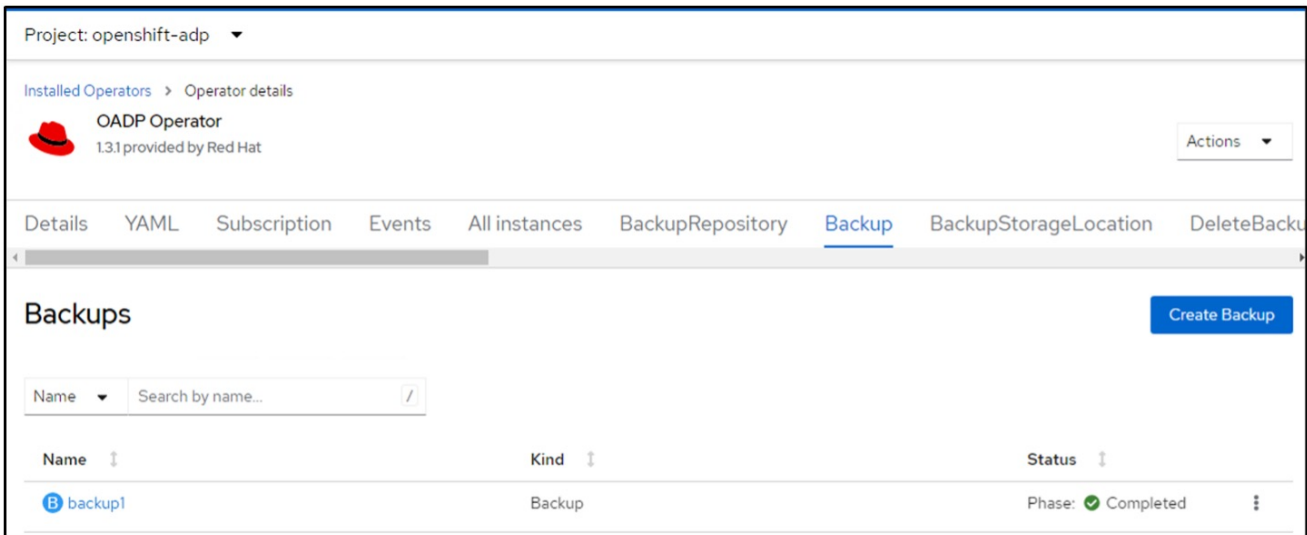
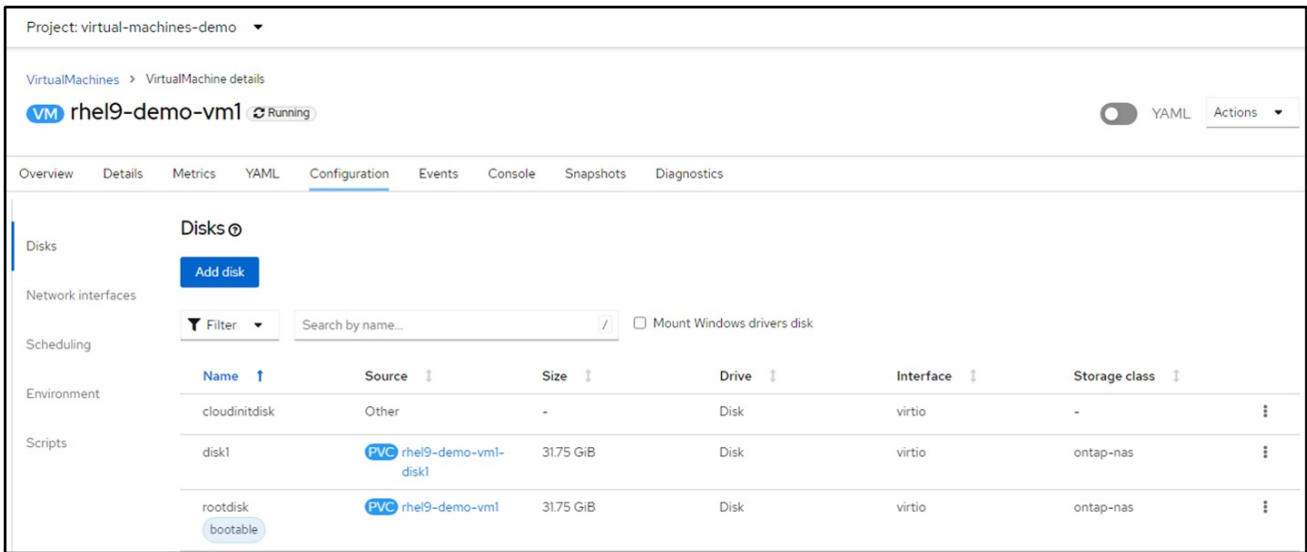
Quando la fase è completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui è stato acquisito lo snapshot. (Se il backup è stato creato quando la VM era in esecuzione, ripristinando la VM dal backup si avvia la VM ripristinata e la si porta in esecuzione). La VM viene ripristinata in uno spazio dei nomi diverso, come specificato in yaml.



Ripristinare in una classe di archiviazione diversa

Velero fornisce una capacità generica di modificare le risorse durante il ripristino specificando le patch json. Le patch json vengono applicate alle risorse prima di essere ripristinate. Le patch json sono specificate in una configmap e la configmap è referenziata nel comando restore. Questa funzione consente di eseguire il ripristino utilizzando una classe di archiviazione diversa.

Nell'esempio seguente, la macchina virtuale, in fase di creazione, utilizza ontap-nas come classe di storage per i dischi. Viene creato un backup della macchina virtuale denominata Backup1.



Simula la perdita della macchina virtuale eliminando la macchina virtuale.

Per ripristinare la macchina virtuale utilizzando una classe di storage diversa, ad esempio ontap-nas-eco storage, devi effettuare i due seguenti passaggi:

Passo 1

Creare una mappa di configurazione (console) nello spazio dei nomi openshift-adp come segue:  
Inserisci i dettagli come mostrato nella schermata:  
Selezionare spazio dei nomi : openshift-adp  
Nome: Change-storage-class-config (può essere qualsiasi nome)



Chiave: Change-storage-class-config.yaml:

Valore:

```
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"
```

Project: openshift-adp

### Edit ConfigMap

Config maps hold key-value pairs that can be used in pods to read application configuration.

Configure via: ☒ Form view ☐ YAML view

**Name \***

change-storage-class-config

A unique name for the ConfigMap within the project

☐ Immutable  
Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated

**Data**

Data contains the configuration data that is in UTF-8 range

**Key \***

change-storage-class-config.yaml

**Value**

Browse...

Drag and drop file with your value here or browse to upload it.

```
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
```

[Remove key/value](#)

[Add key/value](#)

L'oggetto della mappa di configurazione risultante dovrebbe essere simile al seguente (CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:          change-storage-class-config
Namespace:     openshift-adp
Labels:        velero.io/change-storage-class=RestoreItemAction
               velero.io/plugin-config=
Annotations:   <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"

BinaryData
====

Events:   <none>
```

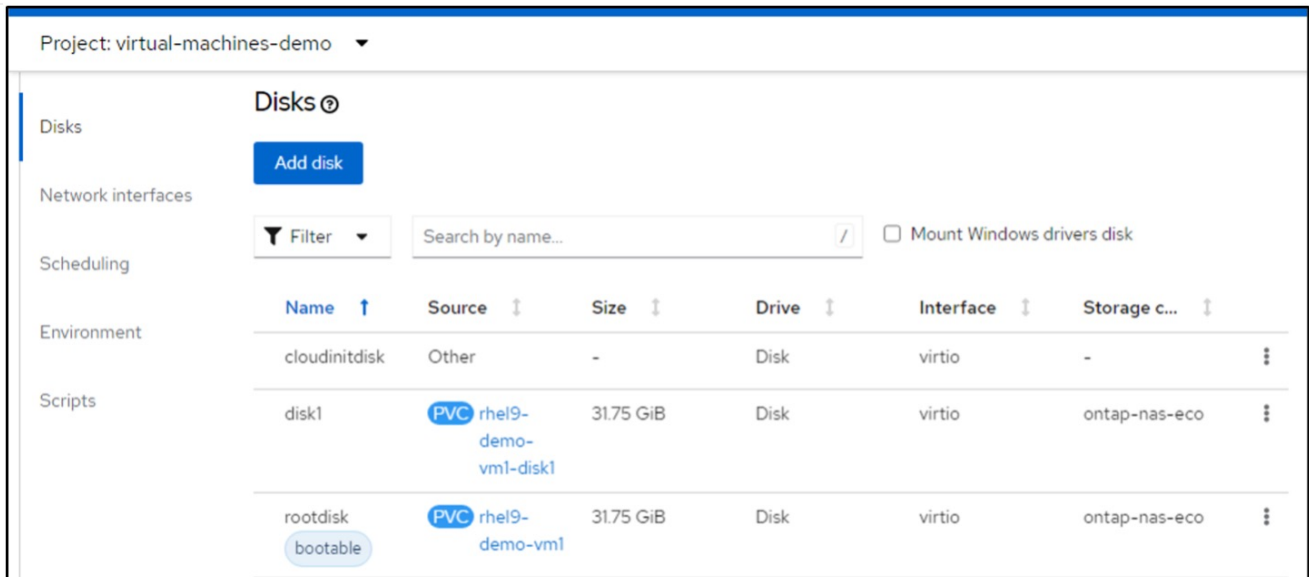
Questa mappa di configurazione applicherà la regola del modificatore di risorse quando viene creato il ripristino. Verrà applicata una patch per sostituire il nome della classe storage in ontap-nas-eco per tutte le richieste di volume persistenti a partire da rhel.

## Passo 2

Per ripristinare la macchina virtuale, utilizzare il seguente comando dall'interfaccia CLI di Velero:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

La macchina virtuale viene ripristinata con lo stesso namespace con i dischi creati utilizzando la classe storage ontap-nas-eco.



## Eliminazione di backup e ripristini mediante Velero

### Eliminazione di un backup

È possibile eliminare una CR di backup senza eliminare i dati di archiviazione oggetti utilizzando lo strumento CLI OC.

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Se si desidera eliminare la CR di backup ed eliminare i dati di archiviazione degli oggetti associati, è possibile farlo utilizzando lo strumento CLI Velero.

Scaricare l'interfaccia CLI come indicato nelle istruzioni nella ["Documentazione Velero"](#).

Eseguire il seguente comando delete utilizzando l'interfaccia CLI di Velero

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

È inoltre possibile eliminare il ripristino CR utilizzando l'interfaccia CLI Velero

```
velero restore delete restore --namespace openshift-adp
```

È possibile utilizzare il comando oc e l'interfaccia utente per eliminare la CR di ripristino

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

### Monitoraggio utilizzando Cloud Insights per le VM nella virtualizzazione Red Hat OpenShift

Autore: Banu Sundhar, NetApp

Questa sezione del documento di riferimento fornisce dettagli sull'integrazione di NetApp Cloud Insights con un cluster Red Hat OpenShift per il monitoraggio delle VM di virtualizzazione OpenShift.

NetApp Cloud Insights è uno strumento di monitoraggio dell'infrastruttura cloud che offre visibilità sull'intera infrastruttura. Con Cloud Insights, puoi monitorare, risolvere i problemi e ottimizzare tutte le risorse, inclusi i cloud pubblici e i data center privati. Per ulteriori informazioni su NetApp Cloud Insights, consultare la ["Documentazione Cloud Insights"](#).

Per iniziare a utilizzare Cloud Insights, devi iscriverti al portale NetApp BlueXP. Per ulteriori informazioni, fare riferimento a ["Assunzione di Cloud Insights"](#).

Cloud Insights dispone di diverse funzionalità che ti consentono di trovare i dati in modo rapido e semplice, risolvere i problemi e fornire informazioni dettagliate sull'ambiente. È possibile trovare facilmente i dati con potenti query, visualizzare i dati nelle dashboard e inviare avvisi e-mail per le soglie di dati impostate. Fare riferimento a ["tutorial video"](#) per facilitare la comprensione di queste funzioni.

Per avviare la raccolta dei dati da parte di Cloud Insights, è necessario disporre di quanto segue

#### Data Collector

Esistono 3 tipi di Data Collector:

- \* Infrastruttura (dispositivi di storage, switch di rete, infrastruttura di elaborazione)
- \* Sistemi operativi (come VMware o Windows)
- \* Servizi (come Kafka)

I Data Collector rilevano le informazioni provenienti dalle origini dati, ad esempio il dispositivo di archiviazione ONTAP (raccoglitore dati infrastruttura). Le informazioni raccolte vengono utilizzate per l'analisi, la convalida, il monitoraggio e la risoluzione dei problemi.

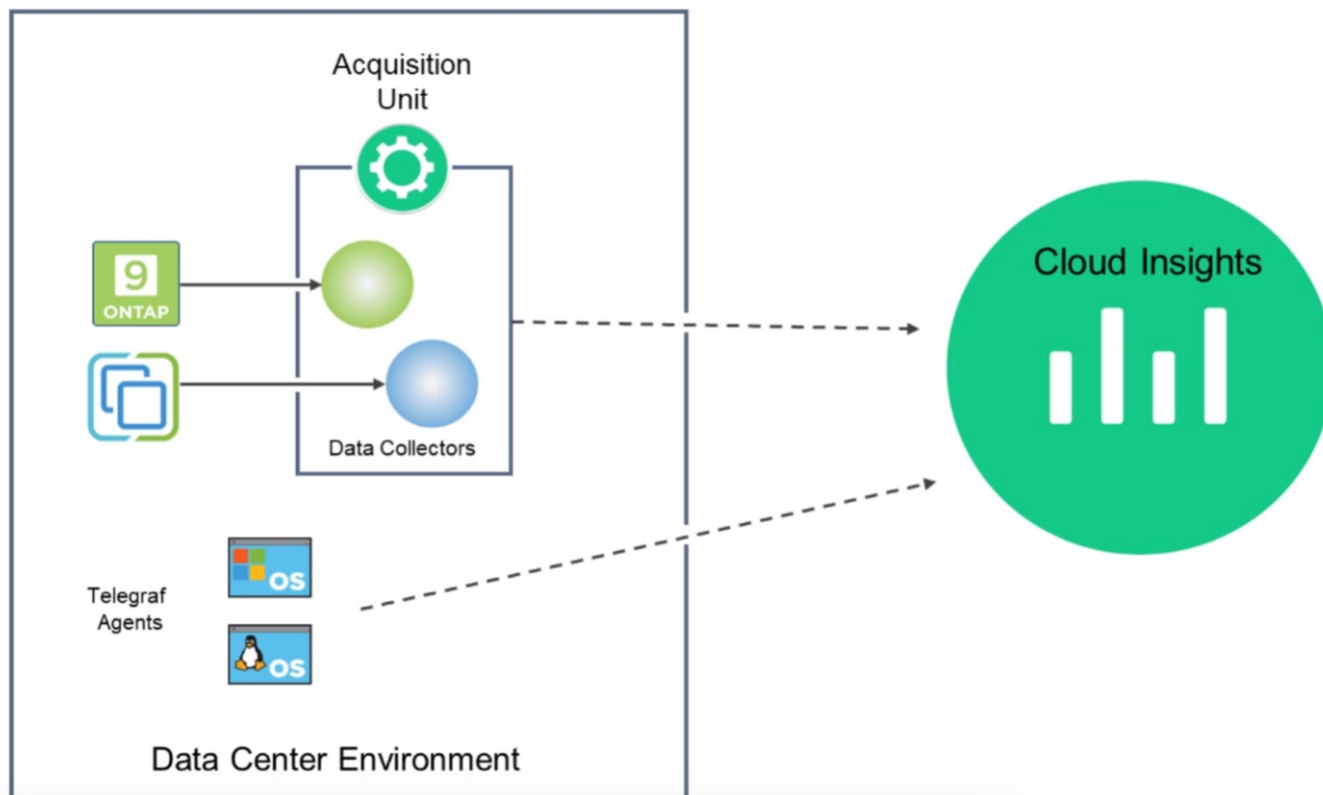
#### Unità di acquisizione

Se si utilizza un servizio Data Collector di infrastruttura, è necessaria anche un'unità di acquisizione per inserire i dati in Cloud Insights. Un'unità di acquisizione è un computer dedicato all'hosting di raccoglitori di dati, in genere una macchina virtuale. In genere, questo computer si trova nello stesso centro dati/VPC degli elementi monitorati.

#### Agenti Telegraf

Cloud Insights supporta anche Telegraf come agente per la raccolta dei dati di integrazione. Telegraf è un agente server basato su plug-in che può essere utilizzato per raccogliere e generare report su metriche, eventi e registri.

Architettura Cloud Insights



## Integrazione con Cloud Insights per VM nella virtualizzazione Red Hat OpenShift

Per iniziare a raccogliere dati per le VM in OpenShift Virtualization è necessario installare:

1. Un operatore di monitoring e un data collector Kubernetes per raccogliere i dati Kubernetes  
Per istruzioni complete, fare riferimento a. "[documentazione](#)".
2. Un'unità di acquisizione per raccogliere dati dallo storage ONTAP che fornisce storage persistente per i dischi delle macchine virtuali  
Per istruzioni complete, fare riferimento a. "[documentazione](#)".
3. Un data collector per ONTAP  
Per istruzioni complete, fare riferimento a. "[documentazione](#)".

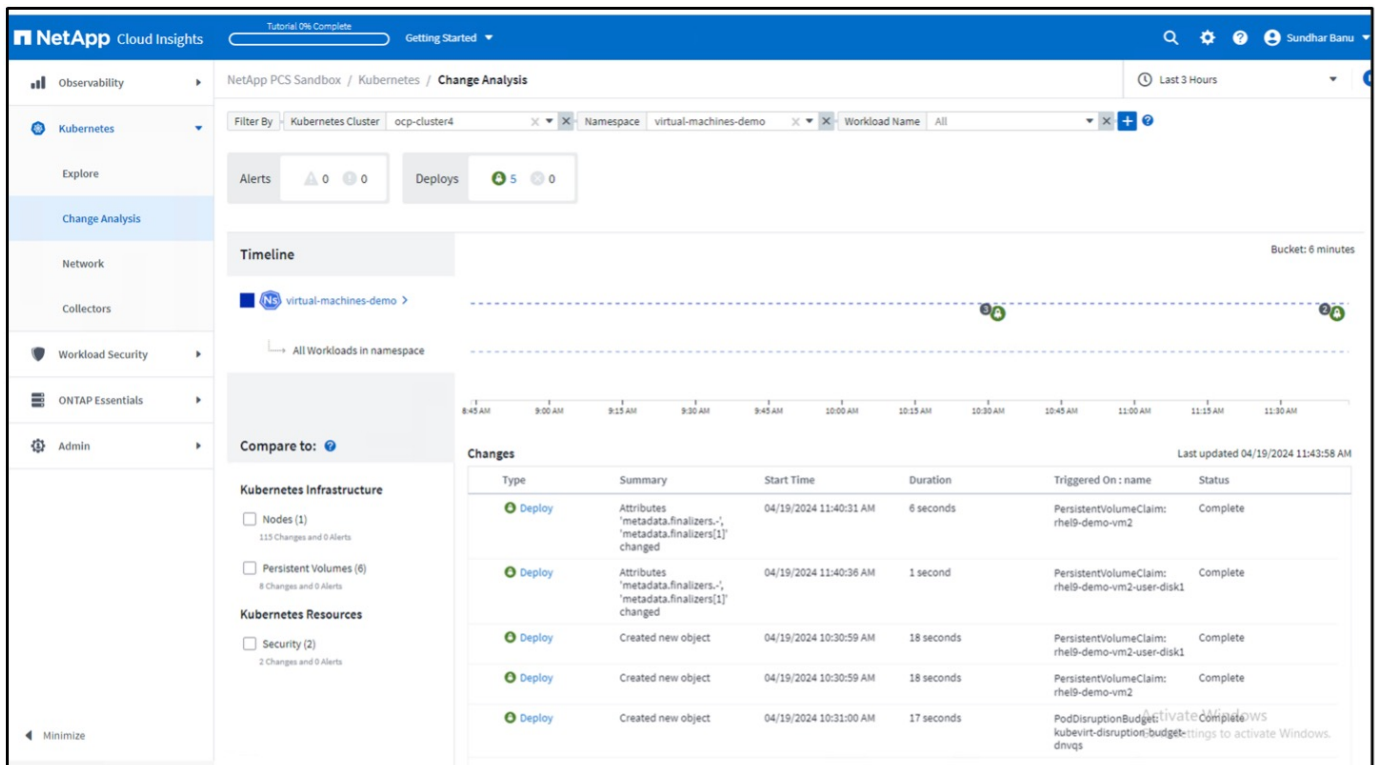
Inoltre, se si utilizza StorageGRID per i backup delle VM, è necessario disporre di un data collector anche per StorageGRID.

## Esempio di funzionalità di monitoraggio per le VM in Red Hat OpenShift Virtualization

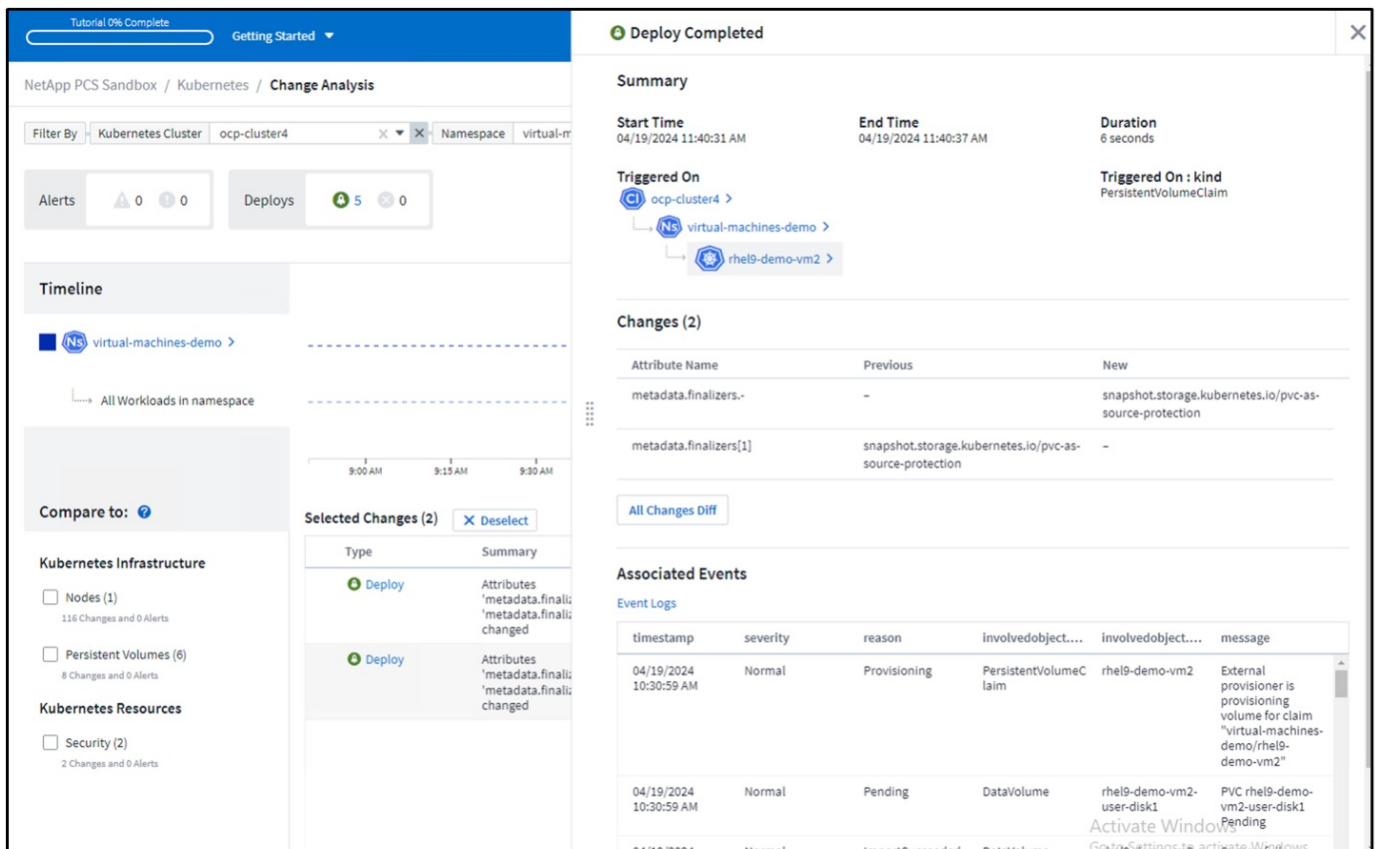
### Monitoraggio basato su eventi e creazione di avvisi

Di seguito viene riportato un esempio in cui lo spazio dei nomi che contiene una VM in OpenShift Virtualization viene monitorato in base agli eventi. In questo esempio, viene creato un monitor in base all'evento **logs.kuPand** per lo spazio dei nomi specificato nel cluster.





Nell'esempio precedente, Change Analysis è configurato sul cluster OpenShift per lo spazio dei nomi che contiene una VM di virtualizzazione OpenShift. Il dashboard mostra le modifiche rispetto alla timeline. Si può drill-down per vedere cosa è cambiato e fare clic su tutte le modifiche Diff per vedere la diff dei manifesti. Dal manifesto, è possibile vedere che è stato creato un nuovo backup dei dischi permanenti.

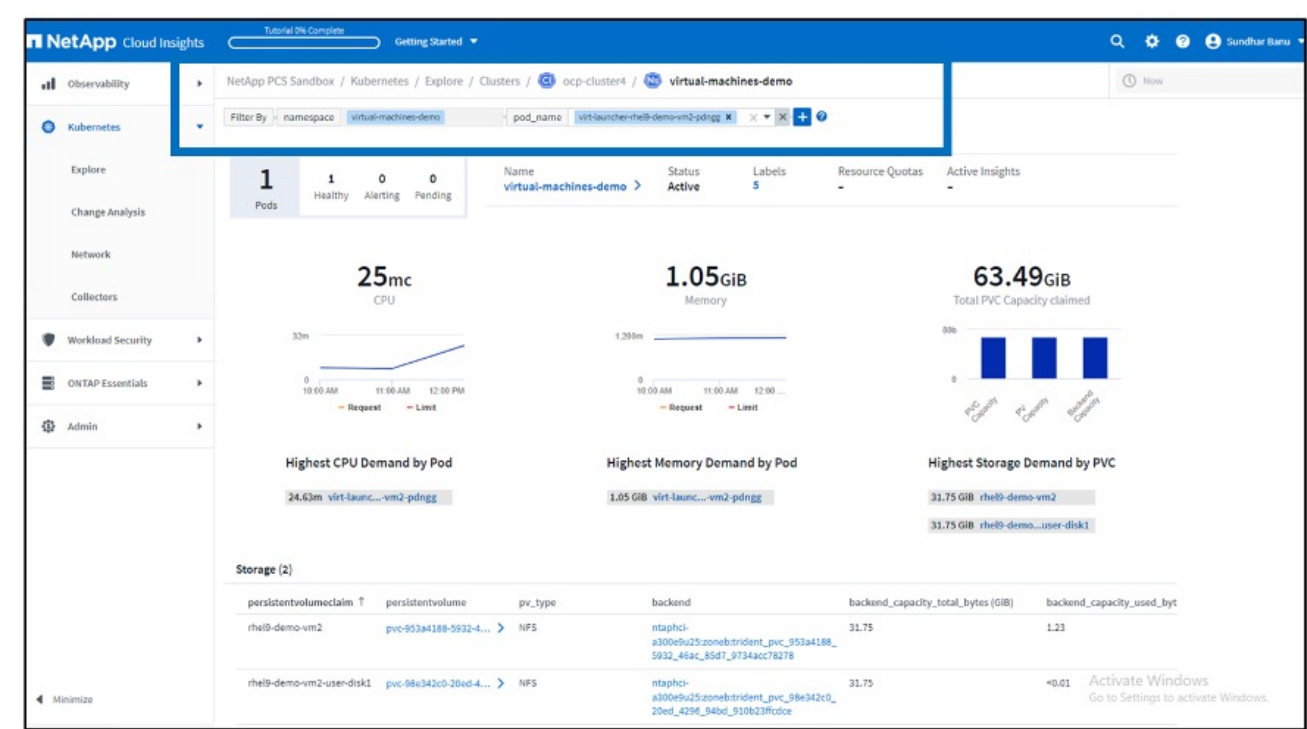




| All Changes Diff |   |     |   | X |
|------------------|---|-----|---|---|
| Previous         |   | New |   |   |
|                  | Expand 45 lines ...                       |     |   |   |
| 46               | kind: DataVolume                          | 46  | kind: DataVolume                          |   |
| 47               | name: rhel9-demo-vm2                      | 47  | name: rhel9-demo-vm2                      |   |
| 48               | uid: dcf93b7a-71bc-409b-ad12-4916d05e0980 | 48  | uid: dcf93b7a-71bc-409b-ad12-4916d05e0980 |   |
| 49               | - resourceVersion: "8569671"              | 49  | + resourceVersion: "8619670"              |   |
| 50               | uid: 953a4188-5932-46ac-85d7-9734acc78278 | 50  | uid: 953a4188-5932-46ac-85d7-9734acc78278 |   |
| 51               | spec:                                     | 51  | spec:                                     |   |
| 52               | accessModes:                              | 52  | accessModes:                              |   |
|                  | Expand 15 lines ...                       |     |   |   |

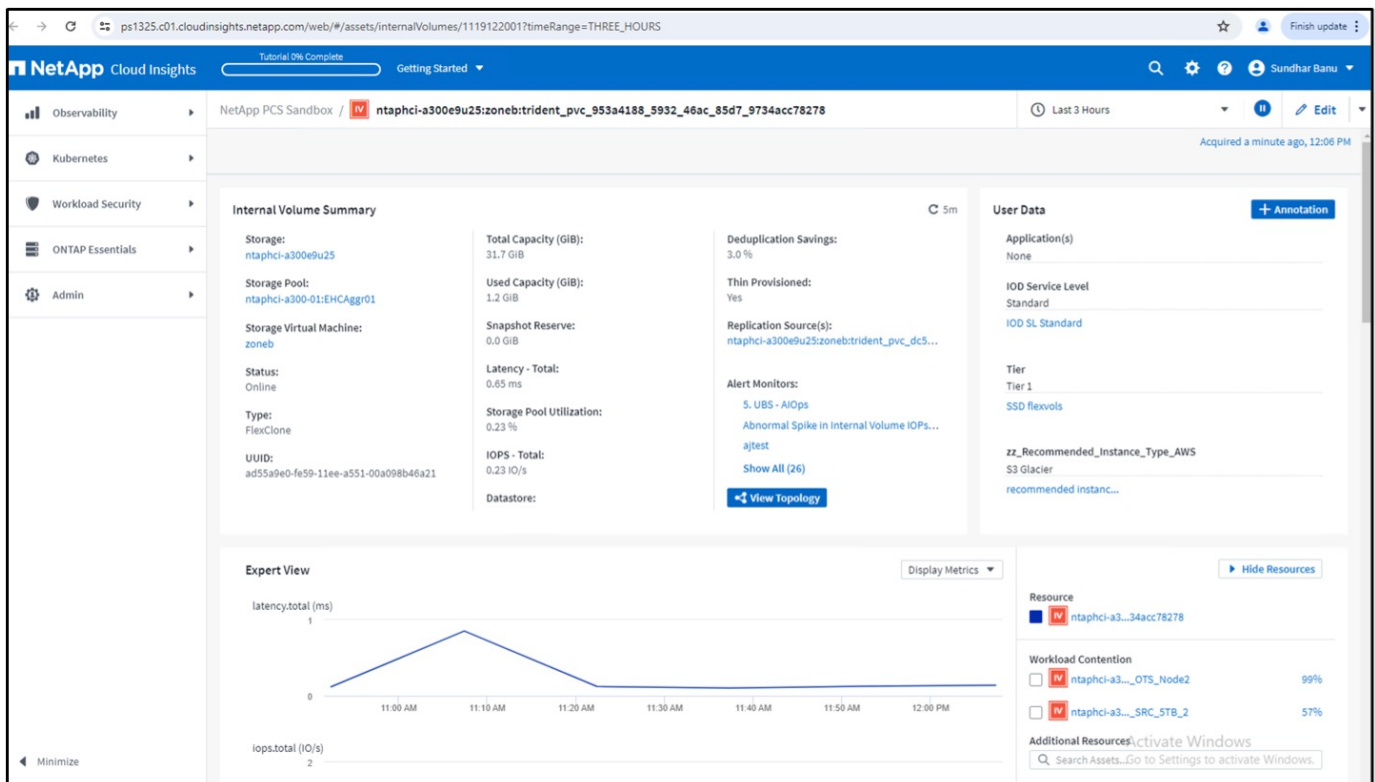
## Mappatura archiviazione backend

Con Cloud Insights, è possibile vedere facilmente lo storage backend dei dischi della macchina virtuale e le diverse statistiche sui PVC.

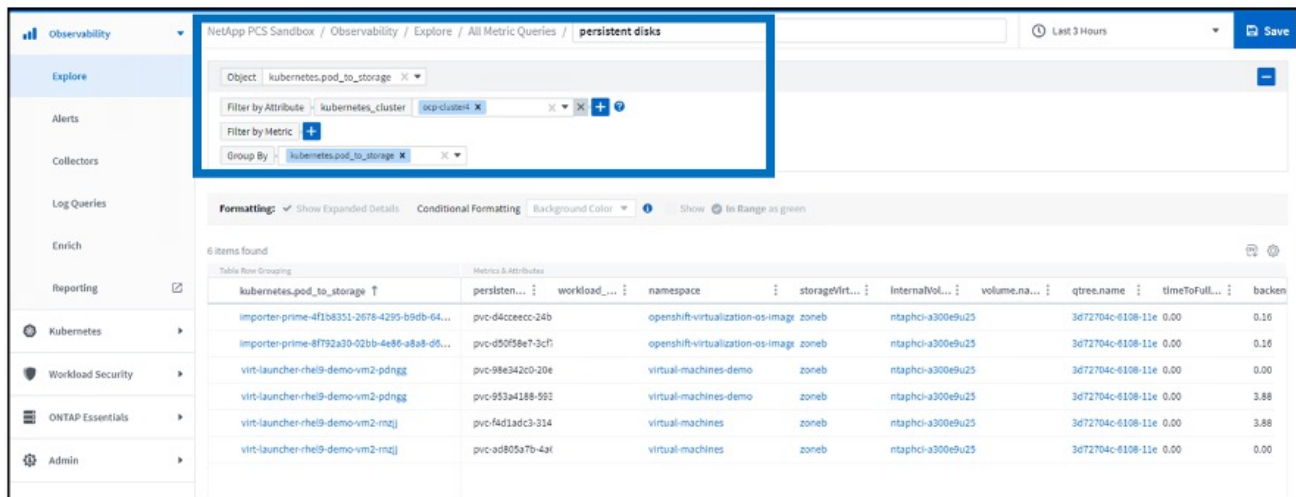


È possibile fare clic sui link presenti nella colonna backend per estrarre i dati direttamente dallo storage ONTAP back-end.



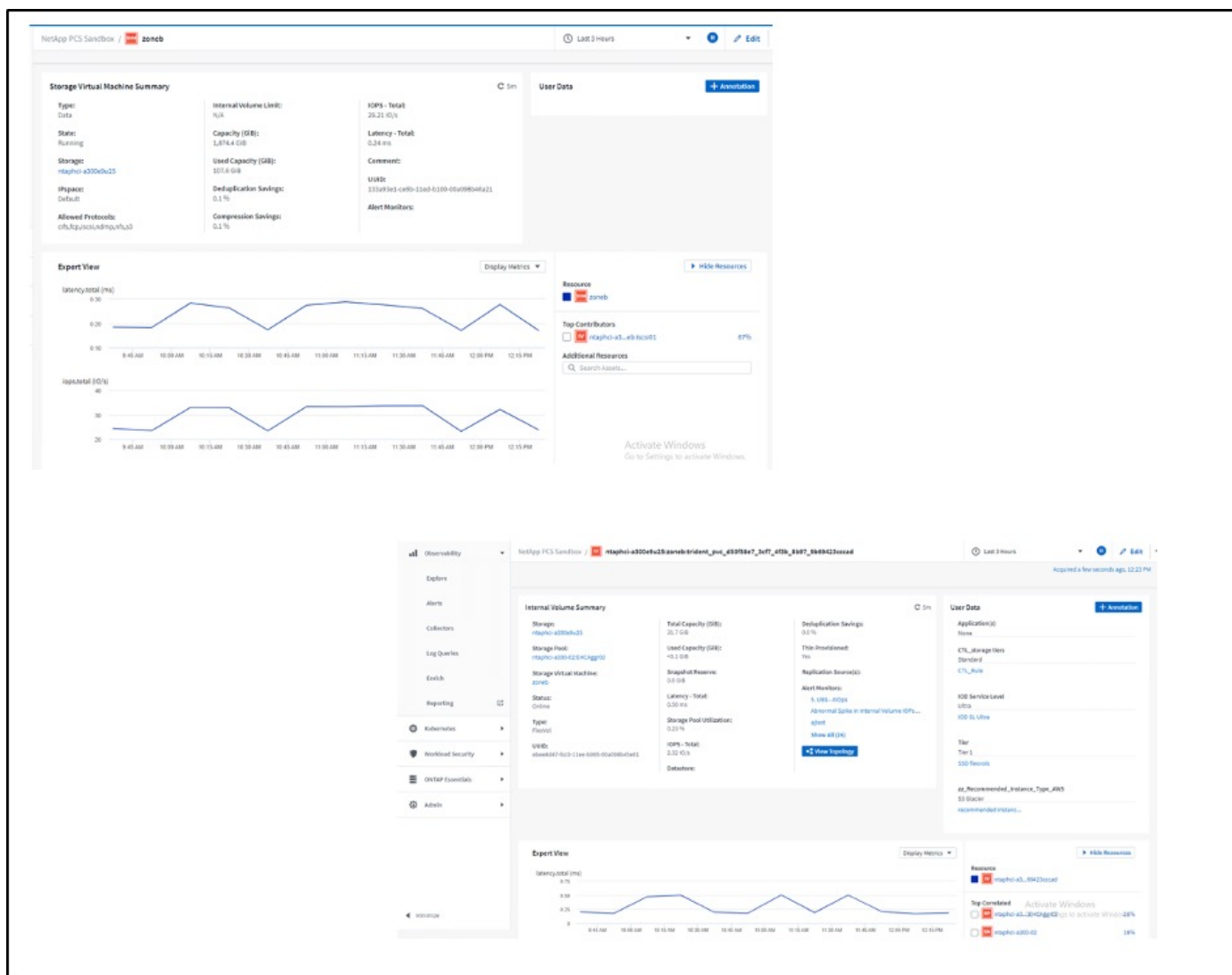


Un altro modo per esaminare tutte le mappature pod-storage è creare una query All Metrics dal menu Observability (osservabilità) in Explore (Esplora).



Facendo clic su uno dei collegamenti si otterranno i dettagli corrispondenti dall'archivio ONTP. Ad esempio, facendo clic sul nome di una SVM nella colonna storageVirtualMachine verranno estratti i dettagli relativi alla SVM da ONTAP. Facendo clic sul nome di un volume interno vengono visualizzati i dettagli relativi al volume in ONTAP.

|                 |                         |                     |                                   |
|-----------------|-------------------------|---------------------|-----------------------------------|
|                 | storageVirtualMachin... | internalVolume.name | volume.na..                       |
| zation-os-image | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |
| zation-os-image | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |
| demo            | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |
| demo            | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |
|                 | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |
|                 | zoneb                   |                     | ntaphci-a300e9u25:zoneb:trident_p |



## Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

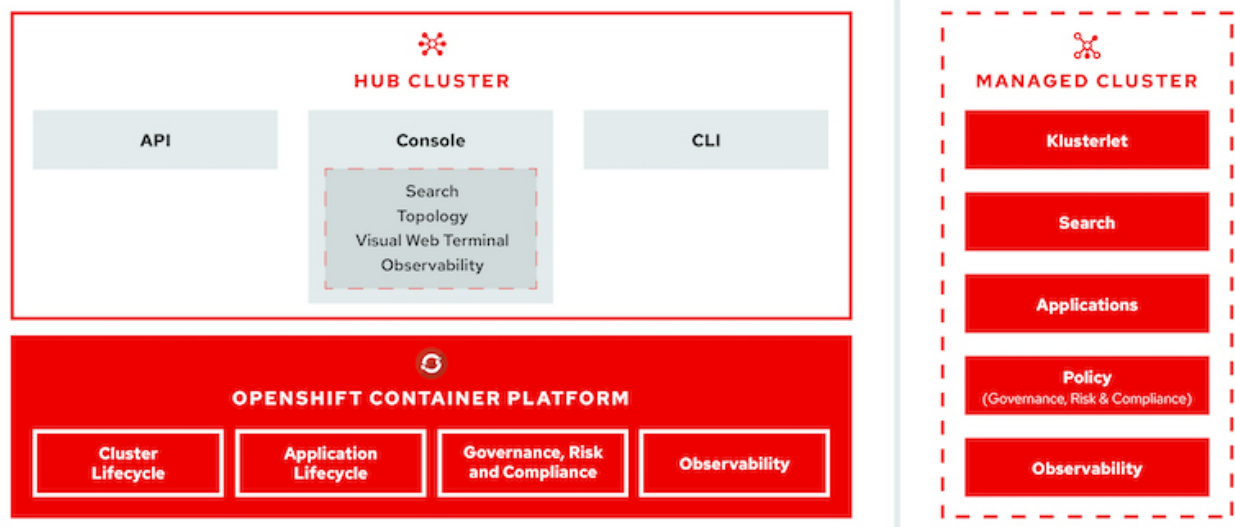
### Gestione avanzata dei cluster per Kubernetes: Red Hat OpenShift con NetApp

Poiché un'applicazione containerizzata passa dallo sviluppo alla produzione, molte organizzazioni richiedono più cluster Red Hat OpenShift per supportare il test e l'implementazione di tale applicazione. In combinazione con questo, le organizzazioni generalmente ospitano più applicazioni o carichi di lavoro su cluster OpenShift. Pertanto, ogni organizzazione finisce per gestire un insieme di cluster e gli amministratori di OpenShift devono quindi affrontare la sfida aggiunta di gestire e mantenere più cluster in una gamma di ambienti che si estendono a più data center on-premise e cloud pubblici. Per affrontare queste sfide, Red Hat ha introdotto la gestione avanzata dei cluster per Kubernetes.

Red Hat Advanced Cluster Management per Kubernetes consente di eseguire le seguenti operazioni:

1. Crea, importa e gestisci più cluster tra data center e cloud pubblici
2. Implementa e gestisci applicazioni o carichi di lavoro su più cluster da una singola console
3. Monitorare e analizzare lo stato e lo stato delle diverse risorse del cluster
4. Monitorare e applicare la conformità alla sicurezza in più cluster

Red Hat Advanced Cluster Management per Kubernetes viene installato come add-on in un cluster Red Hat OpenShift e utilizza questo cluster come controller centrale per tutte le operazioni. Questo cluster è noto come cluster di hub ed espone un piano di gestione per consentire agli utenti di connettersi a Advanced Cluster Management. Tutti gli altri cluster OpenShift importati o creati tramite la console Advanced Cluster Management sono gestiti dal cluster hub e sono denominati cluster gestiti. Installa un agente chiamato Klusterlet sui cluster gestiti per connetterli al cluster hub e soddisfare le richieste di attività diverse correlate alla gestione del ciclo di vita del cluster, alla gestione del ciclo di vita delle applicazioni, all'osservabilità e alla conformità alla sicurezza.



Per ulteriori informazioni, consultare la documentazione ["qui"](#).

### Implementazione

## Implementare Advanced Cluster Management per Kubernetes

### Prerequisiti

1. Un cluster Red Hat OpenShift (superiore alla versione 4.5) per il cluster hub
2. Cluster Red Hat OpenShift (superiori alla versione 4.4.3) per cluster gestiti
3. Accesso cluster-admin al cluster Red Hat OpenShift
4. Un abbonamento Red Hat per Advanced Cluster Management per Kubernetes

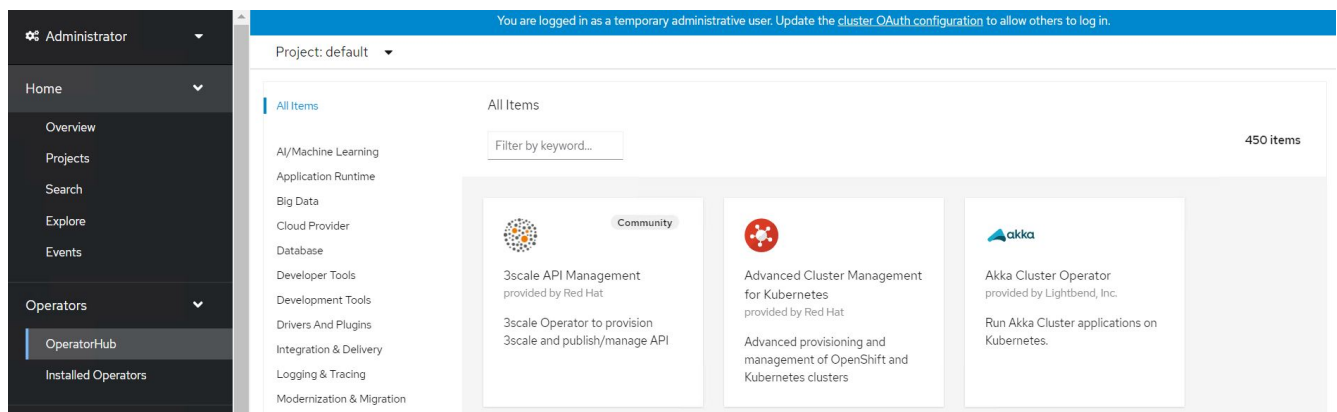
Advanced Cluster Management è un add-on per il cluster OpenShift, pertanto esistono determinati requisiti e restrizioni sulle risorse hardware in base alle funzionalità utilizzate nell'hub e nei cluster gestiti. È necessario tenere conto di questi problemi durante il dimensionamento dei cluster. Consultare la documentazione ["qui"](#) per ulteriori dettagli.

Se il cluster hub dispone di nodi dedicati per l'hosting dei componenti dell'infrastruttura e si desidera installare risorse di Advanced Cluster Management solo su tali nodi, è necessario aggiungere di conseguenza tolleranze e selettori a tali nodi. Per ulteriori informazioni, consultare la documentazione ["qui"](#).

## Implementare Advanced Cluster Management per Kubernetes

Per installare Advanced Cluster Management per Kubernetes su un cluster OpenShift, attenersi alla seguente procedura:

1. Scegliere un cluster OpenShift come cluster hub e accedervi con privilegi di amministratore del cluster.
2. Accedere a Operators > Operators Hub e cercare Advanced Cluster Management for Kubernetes.



3. Selezionare Advanced Cluster Management for Kubernetes (Gestione avanzata cluster per Kubernetes) e fare clic su Install (Installa).



# Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat



Install

## Latest version

2.2.3

## Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

## Provider type

Red Hat

## Provider

Red Hat

## Infrastructure features

Disconnected

Red Hat Advanced Cluster Management for Kubernetes provides the multicluster hub, a central management console for managing multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the hub to create Red Hat OpenShift Container Platform clusters on selected providers, or import existing Kubernetes-based clusters. After the clusters are managed, you can set compliance requirements to ensure that the clusters maintain the specified security requirements. You can also deploy business applications across your clusters.

Red Hat Advanced Cluster Management for Kubernetes also provides the following operators:

- Multicluster subscriptions: An operator that provides application management capabilities including subscribing to resources from a channel and deploying those resources on MCH-managed Kubernetes clusters based on placement rules.
- Hive for Red Hat OpenShift: An operator that provides APIs for provisioning and performing initial configuration of OpenShift clusters. These operators are used by the multicluster hub to provide its provisioning and application-management capabilities.

## How to Install

Use of this Red Hat product requires a licensing and subscription agreement.

4. Nella schermata Install Operator (operatore di installazione), fornire i dettagli necessari (NetApp consiglia di conservare i parametri predefiniti) e fare clic su Install (Installa).

## Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

### Update channel \*

- ☐ release-2.0
- ☐ release-2.1
- ☒ release-2.2

### Installation mode \*

- ☐ All namespaces on the cluster (default)  
This mode is not supported by this Operator
- ☒ A specific namespace on the cluster  
Operator will be available in a single Namespace only.

### Installed Namespace \*

- ☒ Operator recommended Namespace: **PR** open-cluster-management

#### Namespace creation

Namespace **open-cluster-management** does not exist and will be created.

- ☐ Select a Namespace

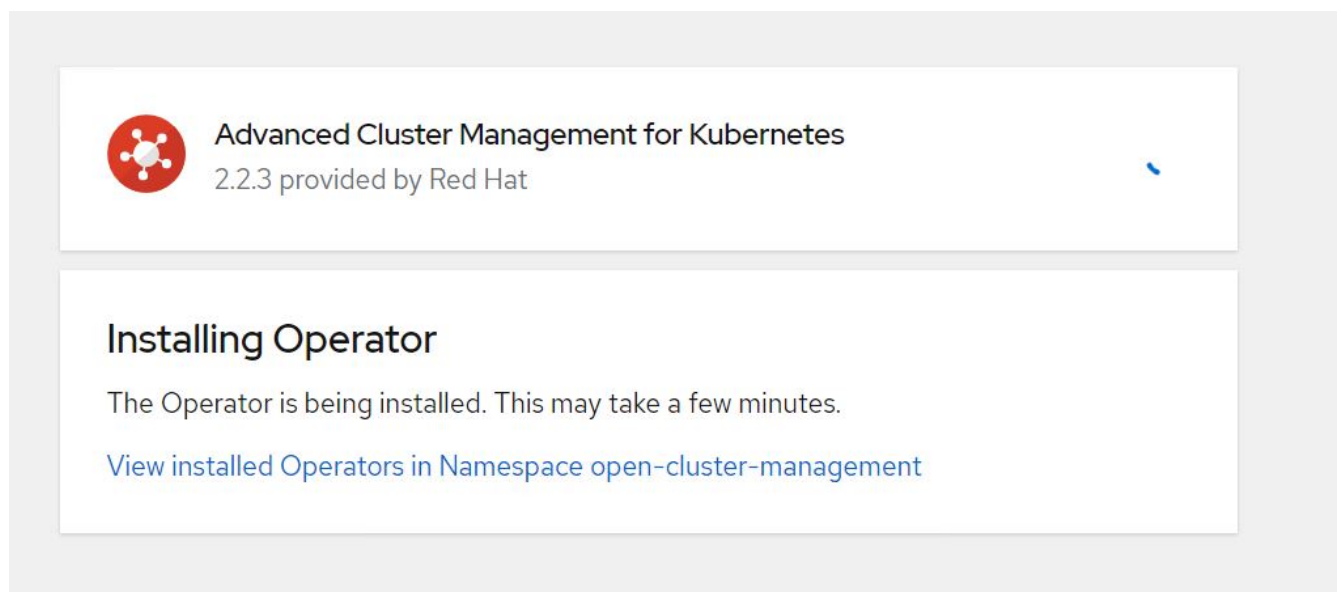
### Approval strategy \*

- ☒ Automatic
- ☐ Manual

**Install**

Cancel

5. Attendere il completamento dell'installazione da parte dell'operatore.



6. Una volta installato l'operatore, fare clic su Create MultiClusterHub (Crea MultiClusterHub).





## Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat



### Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.



**MultiClusterHub** Required

Advanced provisioning and management of OpenShift and Kubernetes clusters

Create MultiClusterHub

[View installed Operators in Namespace open-cluster-management](#)

7. Nella schermata Create MultiClusterHub (Crea MultiClusterHub), fare clic su Create (Crea) dopo aver inserito i dettagli. In questo modo viene avviata l'installazione di un hub multi-cluster.

Project: open-cluster-management

Advanced Cluster Management for Kubernetes > Create MultiClusterHub

#### Create MultiClusterHub

Create by completing the form. Default values may be provided by the Operator authors.

Configure via: ☒ Form view ☐ YAML view

**Note:** Some fields may not be represented in this form view. Please select "YAML view" for full control.



**MultiClusterHub**

provided by Red Hat

MultiClusterHub defines the configuration for an instance of the MultiCluster Hub

Name \*

multiclusterhub

Labels

app=frontend

> [Advanced configuration](#)

Create

Cancel

8. Dopo che tutti i pod sono stati spostati nello stato in esecuzione nello spazio dei nomi di gestione del cluster aperto e l'operatore passa allo stato riuscito, viene installata la funzione Advanced Cluster Management per Kubernetes.


## Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

Name ▾


Search by name...

/

| Name ↑  | Managed Namespaces ↓                                       | Status   | Provided APIs   |
|---|--|--|---|
| <div><div></div><div><div>Advanced Cluster Management for Kubernetes</div><div>2.2.3 provided by Red Hat</div></div></div> | <div><div>NS</div><div>open-cluster-management</div></div> | <div><div>✓ Succeeded</div><div>Up to date</div></div> | <div><div>MultiClusterHub</div><div>ClusterManager</div><div>ClusterDeployment</div><div>ClusterState</div><div>View 25 more...</div></div> |

9. Il completamento dell'installazione dell'hub richiede un po' di tempo e, una volta completata, l'hub MultiCluster passa allo stato di esecuzione.

Installed Operators > Operator details

 **Advanced Cluster Management for Kubernetes**  
2.2.3 provided by Red Hat

Actions ▾

Details | **YAML** | Subscription | Events | All instances | **MultiClusterHub** | ClusterManager | ClusterDeployment | ClusterSt...

**MultiClusterHubs** [Create MultiClusterHub](#)

Name ▾

Search by name...

| Name ↑                   | Kind ↓          | Status ↓         | Labels ↓  |
|--------------------------|-----------------|------------------|-----------|
| <b>MCH</b> multicloudhub | MultiClusterHub | Phase: ✓ Running | No labels |

10. Crea un percorso nello spazio dei nomi di gestione del cluster aperto. Connettersi all'URL nel percorso per accedere alla console Advanced Cluster Management.

## Routes

[Create Route](#)

Filter ▾

Name ▾ mul

Name mul ✕

[Clear all filters](#)

| Name ↑                       | Status     | Location ↓  | Service ↓                   |
|------------------------------|------------|---|-----------------------------|
| <b>RT</b> multicloud-console | ✓ Accepted | <a href="https://multicloud-console.apps.ocp-vmware2.cie.netapp.com">https://multicloud-console.apps.ocp-vmware2.cie.netapp.com</a> | <b>S</b> management-ingress |





^ Configuration

Cluster name \* ⓘ

rh-aws

^ Distribution

Select the type of Kubernetes distribution to use for your cluster.

 Red Hat OpenShift

Select an infrastructure provider to host your Red Hat OpenShift cluster.

 Amazon Web Services

 Google Cloud

 Microsoft Azure

 VMware vSphere

 Bare Metal

Release image \* ⓘ

quay.io/openshift-release-dev/ocp-release:4.7.12-x86\_64

Provider connection \* ⓘ

nik-hcl-aws

[Add a connection](#)

- c. Una volta creato, il cluster viene visualizzato nell'elenco dei cluster con lo stato Ready (Pronto).
3. Per importare un cluster esistente, attenersi alla seguente procedura:
- a. Accedere a Clusters e fare clic su Add a Cluster (Aggiungi cluster) > Import an Existing Cluster (Importa cluster esistente).
  - b. Inserire il nome del cluster e fare clic su Save Import and generate Code (Salva importazione e genera codice). Viene visualizzato un comando per aggiungere il cluster esistente.
  - c. Fare clic su Copy Command (Copia comando) ed eseguire il comando sul cluster da aggiungere al cluster hub. In questo modo viene avviata l'installazione degli agenti necessari sul cluster e, al termine di questo processo, il cluster viene visualizzato nell'elenco dei cluster con lo stato Ready.

**Name \***

ocp-vmw1

**Additional labels**

Once you click on "Save import and generate code", the information you entered will be used to generate the code and cannot be modified anymore. If you wish to change any information, you will have to delete and re-import this cluster.

Code generated successfully Import saved

**Run a command**

**1. Copy this command**

Click the button to have the command automatically copied to your clipboard.

Copy command

**2. Run this command with kubectl configured for your targeted cluster to start the import**

Log in to the existing cluster in your terminal and run the command.

View cluster Import another

4. Dopo aver creato e importato più cluster, è possibile monitorarli e gestirli da una singola console.

## Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

### Gestione del ciclo di vita dell'applicazione

Per creare un'applicazione e gestirla in un insieme di cluster,

1. Accedere a Manage Applications (Gestisci applicazioni) dalla barra laterale e fare clic su Create Application (Crea applicazione). Fornire i dettagli dell'applicazione che si desidera creare e fare clic su Save (Salva).

Create an application YAML: Off

Cancel

Save

Name\* ⓘ

demo-app

Namespace\* ⓘ

default

X

▼

## ^ Repository location for resources

## ^ Repository types

Select the type of repository where resources that you want to deploy are located



Git



URL\* ⓘ

https://github.com/open-cluster-management/acm-hive-openshift-releases.git

X

▼

Branch ⓘ

main

X

▼

Path ⓘ

clusterImageSets/fast/4.7

X

▼

2. Una volta installati i componenti dell'applicazione, l'applicazione viene visualizzata nell'elenco.

## Applications

Refresh every 15s ▼

Last update: 7:36:23 PM

Overview

Advanced configuration

Create application

Q Search

Name ↑

Namespace ↑

Clusters ↑ ⓘ

Resource ↑ ⓘ

Time window ↑ ⓘ

Created ↑

demo-app

default

Local

Git

8 days ago



1 - 1 of 1 ▼

&lt;&lt;

&lt;

1

of 1

&gt;

&gt;&gt;

3. L'applicazione può ora essere monitorata e gestita dalla console.

### Governance e rischi


Questa funzionalità consente di definire le policy di conformità per diversi cluster e di assicurarsi che i cluster aderiscano ad esso. È possibile configurare le policy per informare o correggere eventuali deviazioni o violazioni delle regole.

1. Accedere a Governance and Risk (Governance e rischi) dalla barra laterale.
2. Per creare policy di compliance, fare clic su Create Policy (Crea policy), inserire i dettagli degli standard dei policy e selezionare i cluster che devono aderire a tali policy. Se si desidera correggere automaticamente le violazioni di questa policy, selezionare la casella di controllo Applica se supportato e fare clic su Crea.





# Create policy YAML: Off

**Name \***

policy-complianceoperator

**Namespace \*** 

default

**Specifications \***  ComplianceOperator**Cluster selector**  local-cluster: "true"**Standards**  NIST-CSF**Categories**  PR.IP Information Protection Processes and Procedures**Controls**  PR.IP-1 Baseline Configuration☐ **Enforce if supported** ☐ **Disable policy** 

3. Dopo aver configurato tutti i criteri richiesti, è possibile monitorare e correggere eventuali violazioni di policy o cluster da Advanced Cluster Management.

Summary 1

Standards ▼

## NIST-CSF



No violations found

Based on the industry standards, there are no cluster or policy violations.

Policies

Cluster violations

Find policies

| Policy name ↑             | Namespace ↑ | Remediation ↑ | Cluster violations ↑ | Standards ↑ | Categories ↑  | Controls ↑                     | Created ↓        |
|---------------------------|-------------|---------------|----------------------|-------------|---|--------------------------------|------------------|
| policy-complianceoperator | default     | inform        | ✓ 0/1                | NIST-CSF    | PR.IP Information Protection Processes and Procedures | PR.IP-1 Baseline Configuration | 32 minutes ago ⋮ |

1 - 1 of 1 ▼ << < 1 of 1 > >>

**Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp****Osservabilità**

La gestione avanzata dei cluster per Kubernetes consente di monitorare nodi, pod, applicazioni e carichi di lavoro in tutti i cluster.

1. Accedere a osservare gli ambienti > Panoramica.



2. Tutti i pod e i carichi di lavoro di tutti i cluster vengono monitorati e ordinati in base a una varietà di filtri. Fare clic su Pod per visualizzare i dati corrispondenti.



3. Tutti i nodi dei cluster vengono monitorati e analizzati in base a una varietà di punti dati. Fare clic su Nodes (nodi) per ulteriori informazioni sui dettagli corrispondenti.



## Search

Saved searches [Open new search tab](#)

3 Related cluster

1k Related pod

12 Related service

Show all (3)

### Node (20)

| Name                                       | Cluster        | Role              | Architecture | OS image   | CPU | Created     | Labels   |
|--|----------------|-------------------|--------------|--|-----|-------------|--|
| ocp-master-1.ocp-bare-metal.cie.netapp.com | ocp-bare-metal | master;<br>worker | amd64        | Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa) | 48  | a month ago | beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux<br>kubernetes.io/arch=amd64 5 more |
| ocp-master-2.ocp-bare-metal.cie.netapp.com | ocp-bare-metal | master;<br>worker | amd64        | Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa) | 48  | a month ago | beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux<br>kubernetes.io/arch=amd64 5 more |
| ocp-master-3.ocp-bare-metal.cie.netapp.com | ocp-bare-metal | master;<br>worker | amd64        | Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa) | 48  | a month ago | beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux<br>kubernetes.io/arch=amd64 5 more |

4. Tutti i cluster vengono monitorati e organizzati in base a diverse risorse e parametri del cluster. Fare clic su Clusters (Clusters) per visualizzare i dettagli del cluster.

## Search

Saved searches [Open new search tab](#)

3k Related secret

787 Related pod

15 Related persistentvolumeclaim

17 Related node

1 Related application

15 Related persistentvolume

1 Related searchcollector

8 Related clusterclaim

3 Related resourcequota

5 Related identity

Show all (159)

### Cluster (2)

| Name          | Available | Hub accepted | Joined | Nodes | Kubernetes version | CPU | Memory   | Console URL            | Labels   |
|---------------|-----------|--------------|--------|-------|--------------------|-----|----------|------------------------|--|
| local-cluster | True      | True         | True   | 8     | v1.20.0+c8905da    | 84  | 418501Mi | <a href="#">Launch</a> | cloud=VSphere clusterID=148632d9-69d5-4ae4-98ee-8df886463c3<br>installer.name=multiclusterhub 4 more |
| ocp-vmw       | True      | True         | True   | 9     | v1.20.0+df9c838    | 28  | 111981Mi | <a href="#">Launch</a> | cloud=VSphere clusterID=9d76ac4e-4aae-4d45-a2e8-11b6b54282fe name=ocp-vmw 1 more                     |

## Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

### Creare risorse su più cluster

Advanced Cluster Management per Kubernetes consente agli utenti di creare risorse su uno o più cluster gestiti contemporaneamente dalla console. Ad esempio, se si dispone di cluster OpenShift in siti diversi supportati da diversi cluster NetApp ONTAP e si desidera eseguire il provisioning dei PVC in entrambi i siti, è possibile fare clic sul segno (+) nella barra superiore. Quindi selezionare i cluster in cui si desidera creare il PVC, incollare la risorsa YAML e fare clic su Create (Crea).

## Create resource

[Cancel](#)[Create](#)

Clusters | Select the clusters where the resource(s) will be deployed.

2 x local-cluster,  
ocp-vmw

Resource configuration | Enter the configuration manifest for the resource(s).

YAML

```
1 kind: PersistentVolumeClaim
2 apiVersion: v1
3 metadata:
4   name: demo-pvc
5 spec:
6   accessModes:
7     - ReadWriteOnce
8   resources:
9     requests:
10      storage: 1Gi
11   storageClassName: ocp-trident
```

## Video e demo: Red Hat OpenShift con NetApp

I seguenti video mostrano alcune delle funzionalità documentate in questo documento:

[Utilizzo di Red Hat MTV per migrare le VM alla virtualizzazione OpenShift con lo storage NetApp ONTAP](#)

[Accelera lo sviluppo del software con Astra Control e la tecnologia NetApp FlexClone - Red Hat OpenShift con NetApp](#)

[Sfrutta NetApp Astra Control per eseguire l'analisi post-mortem e ripristinare l'applicazione](#)

[Data Protection in pipeline ci/CD con Astra Control Center](#)

[Migrazione dei workload con Centro di controllo Astra - Red Hat OpenShift con NetApp](#)

[Migrazione dei workload - Red Hat OpenShift con NetApp](#)

[Installazione della virtualizzazione OpenShift - Red Hat OpenShift con NetApp](#)

[Implementazione di una macchina virtuale con virtualizzazione OpenShift - Red Hat OpenShift con NetApp](#)

[NetApp HCI per Red Hat OpenShift sulla virtualizzazione Red Hat](#)

## Ulteriori informazioni: Red Hat OpenShift con NetApp

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione NetApp

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Documentazione di Astra Trident

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- Documentazione di NetApp Astra Control Center

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Documentazione di Red Hat OpenShift

["https://access.redhat.com/documentation/en-us/openshift\\_container\\_platform/4.7/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/)

- Documentazione sulla piattaforma Red Hat OpenStack

["https://access.redhat.com/documentation/en-us/red\\_hat\\_openshift\\_container\\_platform/4.7/"](https://access.redhat.com/documentation/en-us/red_hat_openshift_container_platform/4.7/)

- Documentazione sulla virtualizzazione Red Hat

["https://access.redhat.com/documentation/en-us/red\\_hat\\_virtualization/4.4/"](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/)

- Documentazione VMware vSphere

["https://docs.vmware.com/"](https://docs.vmware.com/)

## NVA-1166: VMware Tanzu con NetApp

Alan Cowles e Nikhil M Kulkarni, NetApp

Questo documento di riferimento fornisce la convalida dell'implementazione di diversi tipi di soluzioni VMware Tanzu Kubernetes, implementate come tanzu Kubernetes Grid (TKG), tanzu Kubernetes Grid Service (TKGS) o tanzu Kubernetes Grid Integrated (TKGI) in diversi ambienti di data center validati da NetApp. Descrive inoltre l'integrazione dello storage con i sistemi di storage NetApp e Astra Trident Storage orchestrator per la gestione dello storage persistente e Astra Control Center per il backup e la clonazione delle applicazioni stateful che utilizzano tale storage persistente. Infine, il documento fornisce dimostrazioni video delle integrazioni e delle validazioni della soluzione.

### Casi di utilizzo

La soluzione VMware Tanzu con NetApp è progettata per offrire un valore eccezionale ai clienti con i seguenti casi di utilizzo:

- Semplice implementazione e gestione delle offerte VMware Tanzu Kubernetes Grid implementate su VMware vSphere e integrate con i sistemi storage NetApp.
- La potenza combinata dei container aziendali e dei carichi di lavoro virtualizzati con le offerte di VMware Tanzu Kubernetes Grid.
- Configurazione e casi di utilizzo reali che evidenziano le funzionalità di VMware Tanzu quando viene utilizzato con lo storage NetApp e la suite di prodotti NetApp Astra.
- Protezione o migrazione coerente con l'applicazione di workload containerizzati implementati su cluster VMware Tanzu Kubernetes Grid i cui dati risiedono su sistemi storage NetApp utilizzando Astra Control Center.

## Valore di business

Le aziende stanno adottando sempre più pratiche DevOps per creare nuovi prodotti, abbreviare i cicli di rilascio e aggiungere rapidamente nuove funzionalità. A causa della loro natura innata e agile, i container e i microservizi svolgono un ruolo cruciale nel supporto delle pratiche DevOps. Tuttavia, la pratica di DevOps su scala di produzione in un ambiente aziendale presenta le proprie sfide e impone determinati requisiti all'infrastruttura sottostante, come ad esempio:

- Alta disponibilità a tutti i livelli dello stack
- Procedure di implementazione semplici
- Operazioni e aggiornamenti senza interruzioni
- Infrastruttura programmabile e basata su API per restare al passo con l'agilità dei microservizi
- Multi-tenancy con garanzie di performance
- Possibilità di eseguire contemporaneamente carichi di lavoro virtualizzati e containerizzati
- Possibilità di scalare l'infrastruttura in modo indipendente in base alle esigenze dei carichi di lavoro
- Possibilità di implementazione in un modello di cloud ibrido con container in esecuzione sia nei data center on-premise che nel cloud.

VMware Tanzu con NetApp riconosce queste sfide e presenta una soluzione che aiuta a risolvere ogni problema implementando le offerte VMware Tanzu Kubernetes nell'ambiente di cloud ibrido scelto dal cliente.

## Panoramica della tecnologia

La soluzione VMware Tanzu con NetApp comprende i seguenti componenti principali:

### Piattaforme VMware Tanzu Kubernetes

VMware Tanzu è disponibile in una serie di varianti che il team di progettazione delle soluzioni di NetApp ha validato nei nostri laboratori. Ogni release di Tanzu si integra con successo con il portfolio di storage NetApp e ciascuna di esse può aiutare a soddisfare determinate esigenze infrastrutturali. I seguenti punti chiave puntati descrivono le funzionalità e le offerte di ciascuna versione di Tanzu descritte in questo documento.

### VMware Tanzu Kubernetes Grid (TKG)

- Ambiente Kubernetes upstream standard implementato in un ambiente VMware vSphere.
- Precedentemente noto come Essential PKS (da Heptio Acquisition, febbraio 2019).
- TKG viene implementato con un'istanza di cluster di gestione separata per il supporto su vSphere 6.7U3 in poi.
- Le implementazioni di TKG possono essere implementate nel cloud e con AWS o Azure.
- Consente l'utilizzo di nodi di lavoro Windows o Linux (Ubuntu/Photon).
- NSX-T, ha Proxy, rete AVI o bilanciamento del carico possono essere utilizzati per il piano di controllo.
- TKG supporta MetalLB per il piano dati/applicazioni.
- Può utilizzare vSphere CSI e CSI di terze parti come NetApp Astra Trident.

### VMware Tanzu Kubernetes Grid Service (TKGS)

- Ambiente Kubernetes upstream standard implementato in un ambiente VMware vSphere.

- Precedentemente noto come Essential PKS (da Heptio Acquisition, febbraio 2019).
- TKGS implementato con cluster di supervisore e cluster di workload solo su vSphere 7.0U1 e versioni successive.
- Consente l'utilizzo di nodi di lavoro Windows o Linux (Ubuntu/Photon).
- NSX-T, ha Proxy, rete AVI o bilanciamento del carico possono essere utilizzati per il piano di controllo.
- TKGS supporta MetalLB per il piano dati/applicazioni.
- Può utilizzare vSphere CSI e CSI di terze parti come NetApp Astra Trident.
- Fornisce supporto per vSphere Pod con Tanzu, consentendo l'esecuzione diretta dei pod su host ESXi abilitati nell'ambiente.

### **VMware Tanzu Kubernetes Grid Integrated (TKGI)**

- Precedentemente noto come Enterprise PKS (da Heptio Acquisition, febbraio 2019).
- Può utilizzare NSX-T, ha Proxy o avi. È anche possibile fornire il proprio bilanciamento del carico.
- Supportato da vSphere 6.7U3 in poi, oltre a AWS, Azure e GCP.
- Installazione tramite procedura guidata per semplificare l'implementazione.
- Esegue tanzu in macchine virtuali controllate immutabili gestite da BOSH.
- Può utilizzare vSphere CSI e CSI di terze parti come NetApp Astra Trident (sono applicabili alcune condizioni).

### **vSphere con Tanzu (vSphere Pod)**

- I pod nativi di vSphere vengono eseguiti in un layer sottile e basato su fotoni con hardware virtuale prescritto per un isolamento completo.
- Richiede NSX-T, ma che consente il supporto di funzionalità aggiuntive come un registro di immagine Harbour.
- Implementato e gestito in vSphere 7.0U1 in poi utilizzando un cluster di Supervisor virtuale come TKGS. Esegue i pod direttamente sui nodi ESXi.
- Completamente integrato con vSphere, massima visibilità e controllo grazie all'amministrazione di vSphere.
- Pod isolati basati su CRX per il massimo livello di sicurezza.
- Supporta solo vSphere CSI per lo storage persistente. Nessun orchestratore di storage di terze parti supportato.

### **Sistemi storage NetApp**

NetApp dispone di diversi sistemi storage perfetti per data center aziendali e implementazioni di cloud ibrido. Il portfolio NetApp include i sistemi storage NetApp ONTAP, NetApp Element e NetApp e-Series, tutti in grado di fornire storage persistente per le applicazioni containerizzate.

Per ulteriori informazioni, visitare il sito Web di NetApp ["qui"](#).

### **Integrazioni di storage NetApp**

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful, implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati NetApp.

Per ulteriori informazioni, visitare il sito Web di NetApp Astra ["qui"](#).

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, tra cui VMware Tanzu.

Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

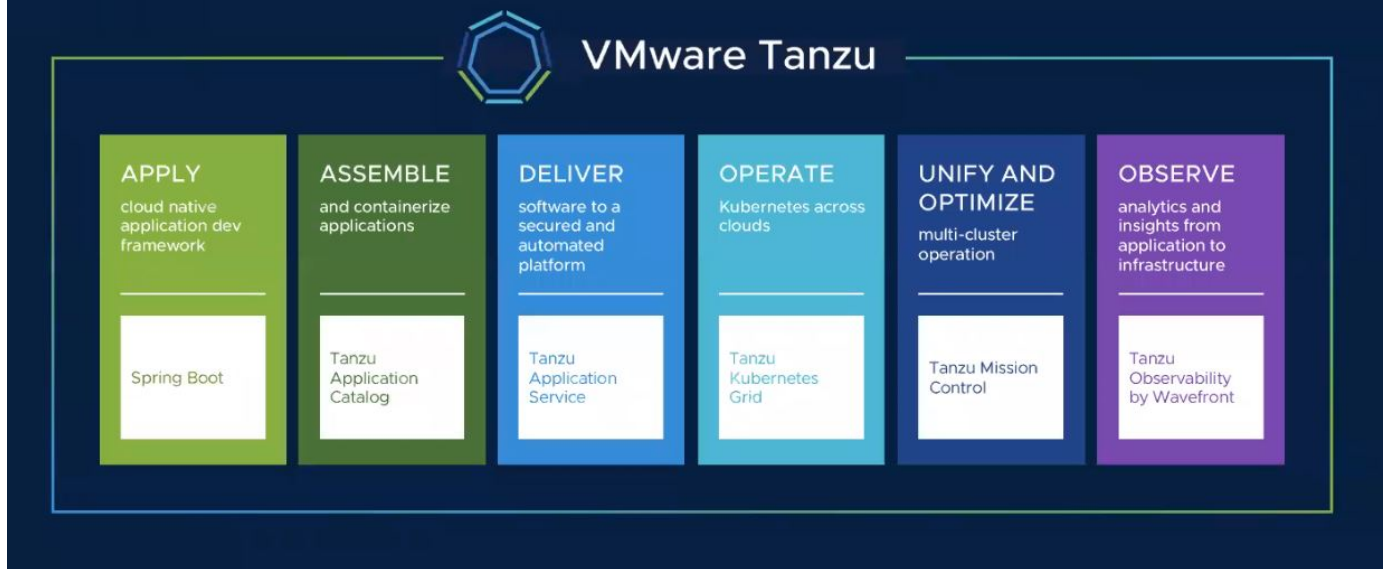
## Matrice di supporto corrente per le release validate

| Tecnologia                               | Scopo   | Versione del software                  |
|--|---|--|
| NetApp ONTAP                             | Storage   | 9.9.1                                  |
| NetApp Astra Control Center              | Gestione dei dati consapevole dell'applicazione | 22.04                                  |
| NetApp Astra Trident                     | Orchestrizzazione dello storage                 | 22.04.0                                |
| Griglia VMware Tanzu Kubernetes          | Orchestrizzazione di container                  | 1.4+                                   |
| Servizio griglia VMware Tanzu Kubernetes | Orchestrizzazione di container                  | 0.0.15 [vSphere Namespaces]            |
|  |   | 1.22.6 [Supervisor Cluster Kubernetes] |
| VMware Tanzu Kubernetes Grid integrato   | Orchestrizzazione di container                  | 1.13.3                                 |
| VMware vSphere                           | Virtualizzazione del data center                | 7.0U3                                  |
| Data center VMware NSX-T.                | Networking e sicurezza                          | 3.1.3                                  |
| VMware NSX Advanced Load Balancer        | Bilanciamento del carico                        | 20.1.3                                 |

## Panoramica di VMware Tanzu

VMware Tanzu è un portfolio di prodotti che consente alle aziende di modernizzare le proprie applicazioni e l'infrastruttura su cui vengono eseguite. Lo stack completo di funzionalità di VMware Tanzu unisce i team di sviluppo e delle operazioni IT su un'unica piattaforma per adottare la modernizzazione sia nelle applicazioni che nella loro infrastruttura in modo coerente in ambienti di cloud ibrido e on-premise per offrire continuamente software migliori alla produzione.

# VMware Tanzu Portfolio



Per ulteriori informazioni sulle diverse offerte e sulle relative funzionalità del portfolio Tanzu, consulta la documentazione ["qui"](#).

Per quanto riguarda il catalogo delle operazioni di Tanzu Kubernetes, VMware dispone di una vasta gamma di implementazioni per Tanzu Kubernetes Grid, che forniscono e gestiscono il ciclo di vita dei cluster di Tanzu Kubernetes su una vasta gamma di piattaforme. Un cluster Tanzu Kubernetes è una distribuzione Kubernetes completa creata e supportata da VMware.

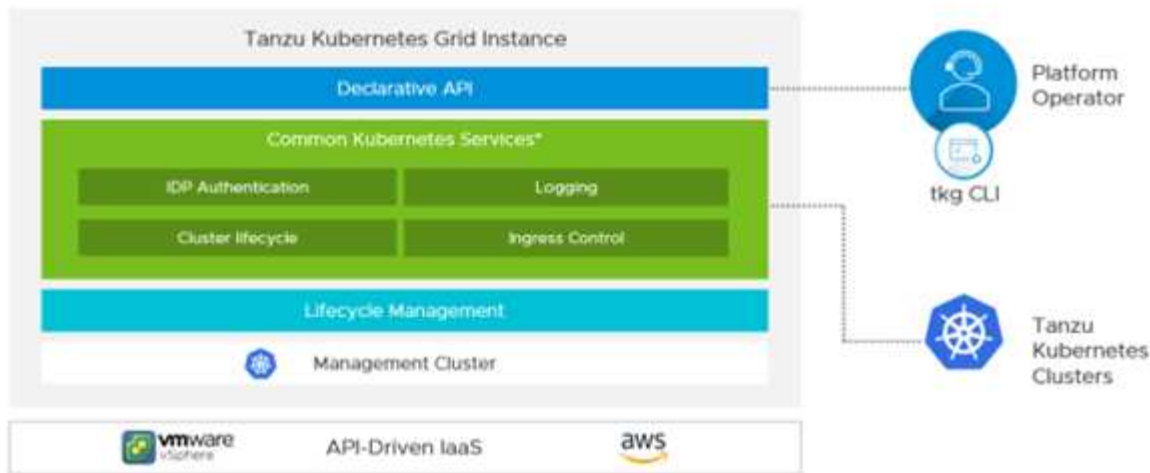
NetApp ha testato e validato l'implementazione e l'interoperabilità dei seguenti prodotti del portfolio VMware Tanzu nei propri laboratori:

- ["Griglia VMware Tanzu Kubernetes \(TKG\)"](#)
- ["VMware Tanzu Kubernetes Grid Service \(TKGS\)"](#)
- ["VMware Tanzu Kubernetes Grid Integrated \(TKGI\)"](#)
- ["VMware vSphere con Tanzu \(vSphere Pod\)"](#)

## Panoramica di VMware Tanzu Kubernetes Grid (TKG)

VMware Tanzu Kubernetes Grid, noto anche come TKG, consente di implementare cluster Tanzu Kubernetes in ambienti cloud ibridi o cloud pubblici. TKG viene installato come cluster di gestione, che è un cluster Kubernetes stesso, che implementa e gestisce i cluster Tanzu Kubernetes. Questi cluster Tanzu Kubernetes sono i cluster Kubernetes per il carico di lavoro su cui viene implementato il carico di lavoro effettivo.

Tanzu Kubernetes Grid si basa su alcuni dei promettenti progetti della community upstream e offre una piattaforma Kubernetes sviluppata, commercializzata e supportata da VMware. Oltre alla distribuzione Kubernetes, Tanzu Kubernetes Grid fornisce add-on aggiuntivi che sono servizi essenziali per la produzione come Registro di sistema, bilanciamento del carico, autenticazione e così via. VMware TKG con cluster di gestione è ampiamente utilizzato negli ambienti vSphere 6.7 e, anche se supportato, non è un'implementazione consigliata per gli ambienti vSphere 7 perché TKGS dispone di funzionalità di integrazione nativa con vSphere 7.



Per ulteriori informazioni su Tanzu Kubernetes Grid, consultare la documentazione ["qui"](#).

A seconda che il sistema Tanzu Kubernetes Grid venga installato on-premise sul cluster vSphere o in ambienti cloud, preparare e implementare il sistema Tanzu Kubernetes Grid seguendo la guida all'installazione ["qui"](#).

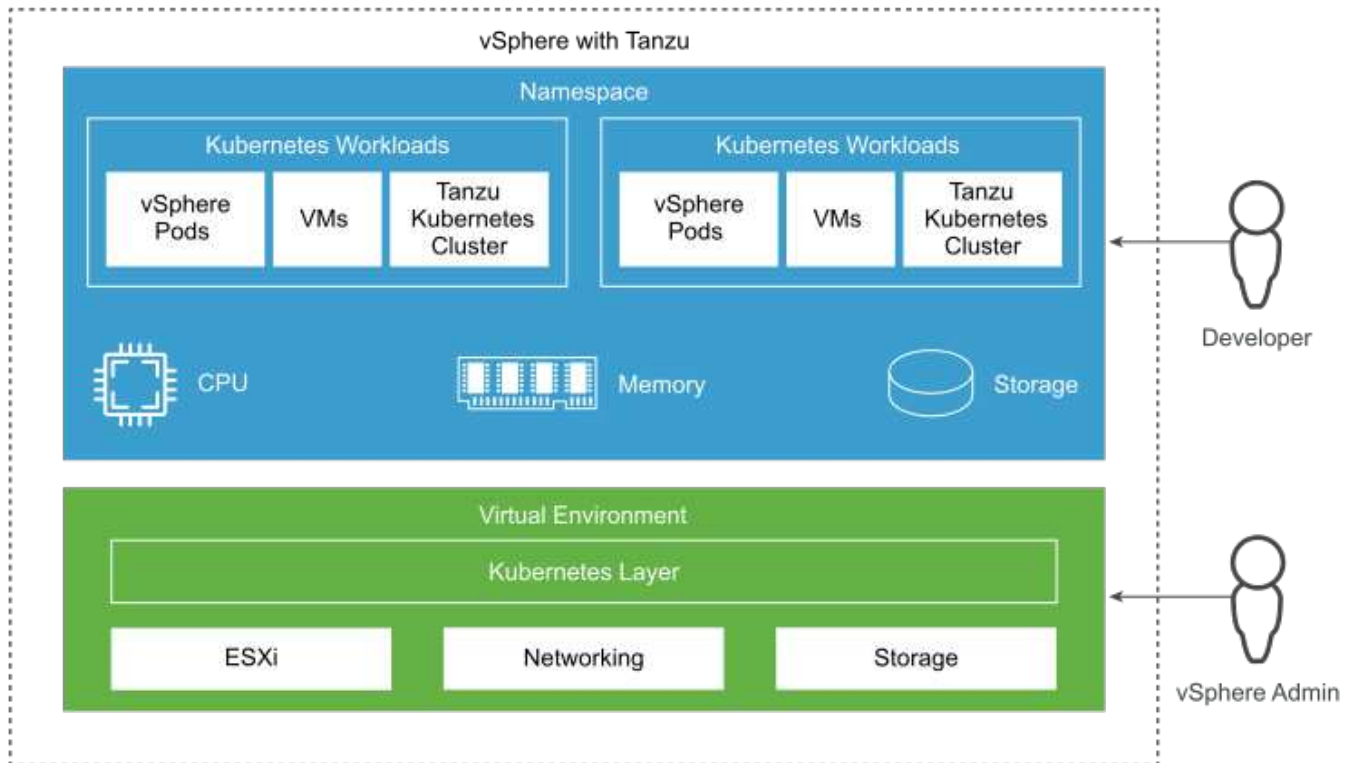
Dopo aver installato il cluster di gestione per Tanzu Kubernetes Grid, implementare i cluster di utenti o i cluster di workload in base alle esigenze seguendo la documentazione ["qui"](#). Il cluster di gestione VMware TKG richiede la fornitura di una chiave SSH per l'installazione e il funzionamento dei cluster Tanzu Kubernetes. Questa chiave può essere utilizzata per accedere ai nodi del cluster utilizzando `capv` utente.

### Panoramica di VMware Tanzu Kubernetes Grid Service (TKGS)

VMware Tanzu Kubernetes Grid Service (noto anche come vSphere con Tanzu) consente di creare e utilizzare i cluster Tanzu Kubernetes in modo nativo in vSphere e consente inoltre di eseguire alcuni carichi di lavoro più piccoli direttamente sugli host ESXi. Consente di trasformare vSphere in una piattaforma per l'esecuzione di workload containerizzati in modo nativo sul layer dell'hypervisor. Tanzu Kubernetes Grid Service implementa su vSphere un cluster di supervisore, se abilitato, che implementa e gestisce i cluster richiesti per i carichi di lavoro. È integrato in modo nativo con vSphere 7 e sfrutta molte funzionalità vSphere affidabili come vCenter SSO, Content Library, rete vSphere, storage vSphere, vSphere ha e DRS e sicurezza vSphere per un'esperienza più perfetta con Kubernetes.

VSphere con Tanzu offre una singola piattaforma per ambienti applicativi ibridi, in cui è possibile eseguire i componenti delle applicazioni in container o in macchine virtuali, garantendo una migliore visibilità e facilità di gestione per sviluppatori, ingegneri DevOps e amministratori vSphere. VMware TKGS è supportato solo con gli ambienti vSphere 7 ed è l'unica offerta del portfolio di operazioni di Tanzu Kubernetes che consente di eseguire i pod direttamente sugli host ESXi.





Per ulteriori informazioni su Tanzu Kubernetes Grid Service, seguire la documentazione ["qui"](#).

Esistono molte considerazioni architetturali relative a set di funzionalità, networking e così via. A seconda dell'architettura scelta, i prerequisiti e il processo di implementazione di Tanzu Kubernetes Grid Service differiscono. Per implementare e configurare il servizio Grid di Tanzu Kubernetes nel tuo ambiente, segui la guida ["qui"](#). Inoltre, per accedere ai nodi del cluster Tanzu Kubernetes implementati tramite TKGS, seguire la procedura descritta in questo documento ["collegamento"](#).

NetApp consiglia di implementare tutti gli ambienti di produzione in implementazioni master multiple per la fault tolerance, scegliendo la configurazione dei nodi di lavoro per soddisfare i requisiti dei carichi di lavoro previsti. Pertanto, una classe di macchine virtuali consigliata per un carico di lavoro altamente intensivo avrebbe almeno quattro vCPU e 12 GB di RAM.

Quando i cluster Tanzu Kubernetes vengono creati in uno spazio dei nomi, gli utenti con `owner` oppure `edit` l'autorizzazione può creare pod direttamente in qualsiasi namespace utilizzando l'account utente. Questo perché gli utenti con `owner` oppure `edit` l'autorizzazione viene assegnata al ruolo di amministratore del cluster. Tuttavia, quando si creano implementazioni, daemon set, stateful set o altri in qualsiasi namespace, è necessario assegnare un ruolo con le autorizzazioni richieste agli account di servizio corrispondenti. Ciò è necessario perché le implementazioni o i set di daemon utilizzano account di servizio per implementare i pod.

Vedere il seguente esempio di ClusterRoleBinding per assegnare il ruolo di amministratore del cluster a tutti gli account di servizio nel cluster:

```

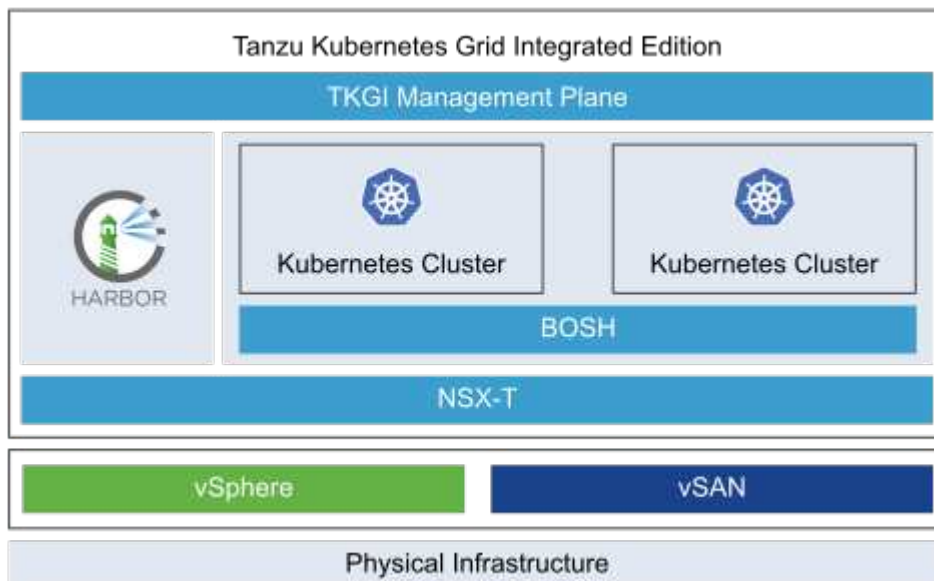
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: all_sa_ca
subjects:
- kind: Group
  name: system:serviceaccounts
  namespace: default
roleRef:
  kind: ClusterRole
  name: psp:vmware-system-privileged
  apiGroup: rbac.authorization.k8s.io

```

## Panoramica di VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

VMware Tanzu Kubernetes Grid Integrated (TKGI) Edition, precedentemente noto come VMware Enterprise PKS, è una piattaforma standalone per l'orchestrazione di container basata su Kubernetes con funzionalità come gestione del ciclo di vita, monitoraggio dello stato dei cluster, networking avanzato, un registro dei container e così via. TKGI fornisce e gestisce i cluster Kubernetes con il piano di controllo TKGI, che consiste in BOSH e Ops Manager.

TKGI può essere installato e utilizzato in ambienti vSphere o OpenStack on-premise o in uno dei principali cloud pubblici delle rispettive offerte IaaS. Inoltre, l'integrazione di TKGI con NSX-T e Harbor consente casi di utilizzo più ampi per i carichi di lavoro aziendali. Per ulteriori informazioni su TKGI e sulle sue funzionalità, consulta la documentazione ["qui"](#).



TKGI viene installato in una varietà di configurazioni su una varietà di piattaforme basate su diversi casi di utilizzo e design. Seguire la guida ["qui"](#) Per installare e configurare TKGI e i relativi prerequisiti. TKGI utilizza le macchine virtuali Bosh come nodi per i cluster Tanzu Kubernetes che eseguono immagini di configurazione immutabili e qualsiasi modifica manuale sulle macchine virtuali Bosh non rimane persistente durante i riavvii.

Note importanti:

- NetApp Trident richiede un accesso privilegiato ai container. Quindi, durante l'installazione di TKGI, assicurarsi di selezionare la casella di controllo Enable Privileged Containers (Abilita container privilegiati) nella fase per configurare i piani dei nodi del cluster Tanzu Kubernetes.

The screenshot displays the configuration interface for a Tanzu Kubernetes cluster. It includes several sections with adjustable settings:

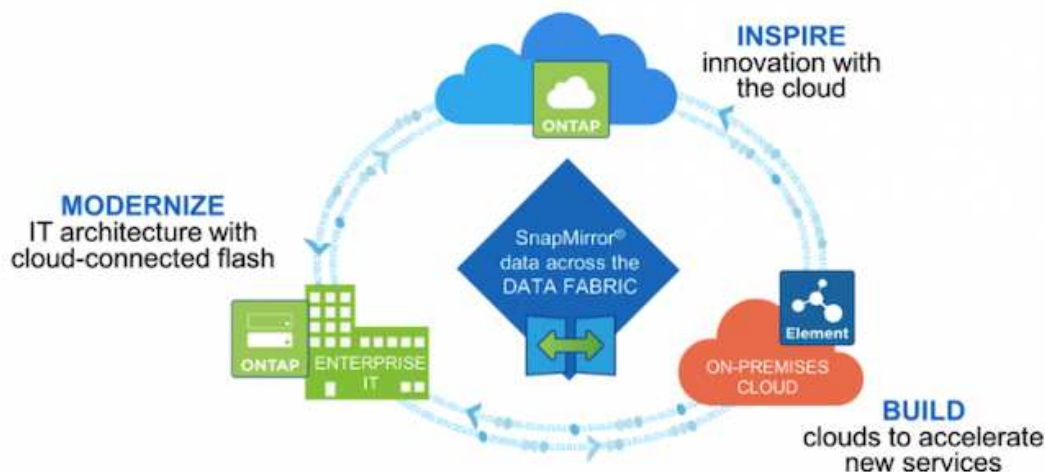
- Worker Node Instances:** Set to 3.
- Worker Persistent Disk Size:** Set to 50 GB.
- Worker Availability Zones:** Enabled (toggle on), set to 'az'.
- Worker VM Type:** Set to 'medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)'.
- Max Worker Node Instances:** Set to 50.
- Errand VM Type:** Set to 'medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)'.
- Enable Privileged Containers (Use with caution):** Checked (blue square icon).
- Admission Plugins:**
  - PodSecurityPolicy:** Disabled (toggle off).
  - SecurityContextDeny:** Disabled (toggle off).
- Cluster Services:**
  - Force node to drain even if it has running pods not managed by a ReplicationController, ReplicaSet, Job, DaemonSet or Stateful Set:** Enabled (toggle on).
  - Force node to drain even if it has running DaemonSet managed pods:** Enabled (toggle on).
  - Force node to drain even if it has running pods using emptyDir:** Enabled (toggle on).
  - Force node to drain even if pods are still running after timeout:** Disabled (toggle off).
- Node Drain Timeout (minutes, min: 0, max: 1440):** Set to 0.
- Pod Shutdown Grace Period (seconds, min: -1, max: 86400):** Set to 10.

At the bottom left, there are two buttons: **SAVE PLAN** (in a blue box) and **DELETE** (in a light blue box).

- NetApp consiglia di implementare tutti gli ambienti di produzione in implementazioni master multiple per la tolleranza agli errori, scegliendo la configurazione dei nodi di lavoro per soddisfare i requisiti dei carichi di lavoro previsti. Pertanto, un piano cluster TKGI consigliato consiste di almeno tre master e tre lavoratori con almeno quattro vCPU e 12 GB di RAM per un carico di lavoro altamente intensivo.

## Panoramica dei sistemi storage NetApp

NetApp dispone di diverse piattaforme storage qualificate con Astra Trident e Astra Control per il provisioning, la protezione e la gestione dei dati per le applicazioni containerizzate.



- I sistemi AFF e FAS eseguono NetApp ONTAP e forniscono storage per i casi di utilizzo basati su file (NFS) e basati su blocchi (iSCSI).
- Cloud Volumes ONTAP e ONTAP Select offrono gli stessi vantaggi rispettivamente nel cloud e nello spazio virtuale.
- NetApp Cloud Volumes Service (AWS/GCP) e Azure NetApp Files offrono storage basato su file nel cloud.



Ogni sistema storage del portfolio NetApp può semplificare la gestione dei dati e lo spostamento tra i siti on-premise e il cloud, in modo che i dati si trovino dove si trovano le applicazioni.

Le pagine seguenti contengono informazioni aggiuntive sui sistemi di storage NetApp validati nella soluzione VMware Tanzu with NetApp:

- ["NetApp ONTAP"](#)

## NetApp ONTAP

NetApp ONTAP è un potente tool software per lo storage con funzionalità come GUI intuitiva, API REST con integrazione dell'automazione, analisi predittive e azioni correttive informate dell'AI, aggiornamenti hardware senza interruzioni e importazione di storage incrociato.

Per ulteriori informazioni sul sistema di storage NetApp ONTAP, visitare il sito ["Sito Web di NetApp ONTAP"](#).

ONTAP offre le seguenti funzionalità:

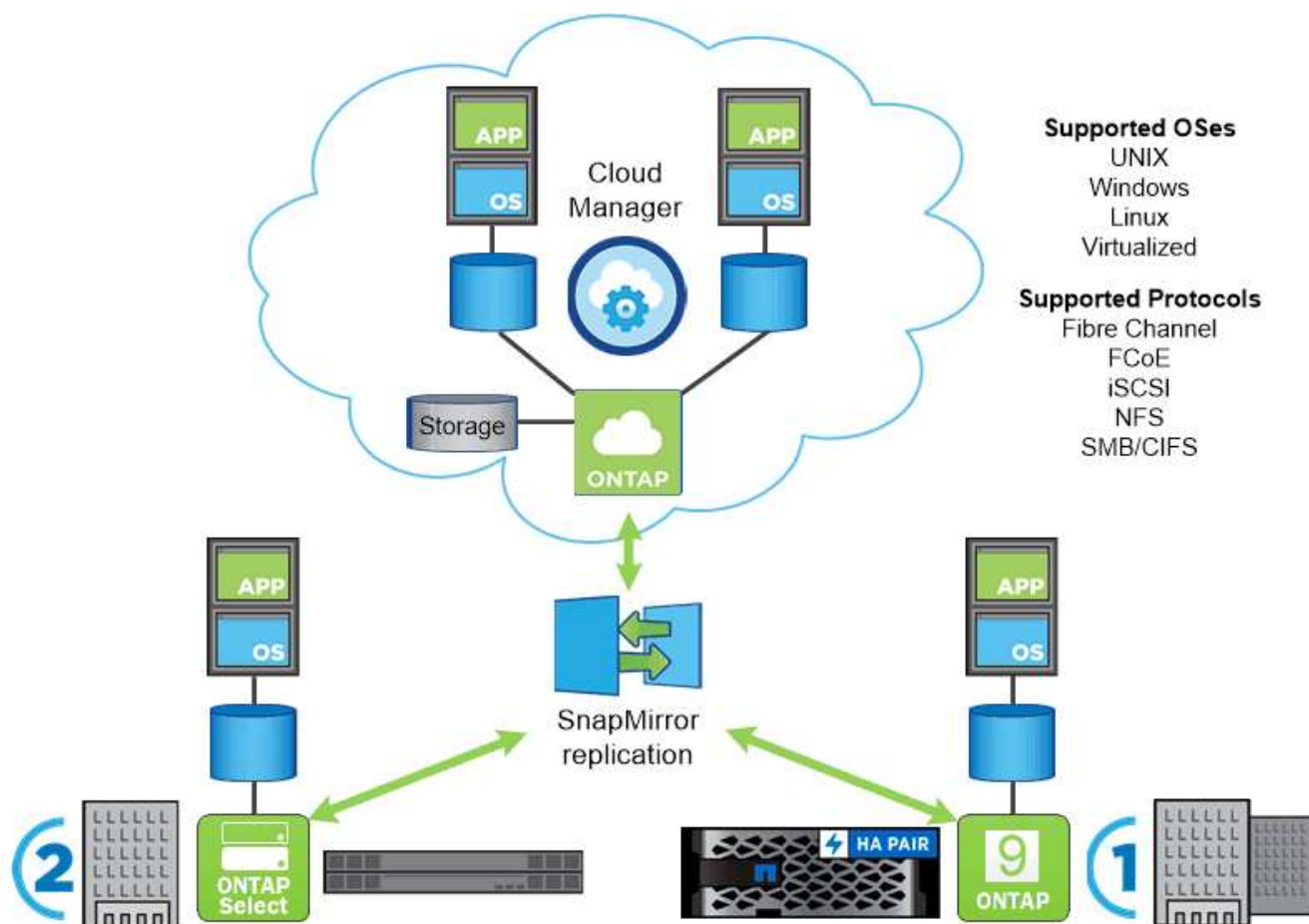
- Un sistema storage unificato con accesso e gestione simultanei dei dati di NFS, CIFS, iSCSI, FC, FCoE, E protocolli FC-NVMe.
- Diversi modelli di implementazione includono configurazioni hardware on-premise su all-flash, ibride e all-HDD, piattaforme di storage basate su VM su un hypervisor supportato come ONTAP Select e nel cloud come Cloud Volumes ONTAP.
- Maggiore efficienza dello storage dei dati sui sistemi ONTAP con supporto per tiering automatico dei dati, compressione dei dati inline, deduplica e compaction.

- Storage basato su workload e controllato dalla QoS.
- Integrazione perfetta con un cloud pubblico per tiering e protezione dei dati. ONTAP offre inoltre solide funzionalità di protezione dei dati che lo differenziano in qualsiasi ambiente:
  - **NetApp Snapshot Copies.** Backup rapido e point-in-time dei dati utilizzando una quantità minima di spazio su disco senza alcun overhead delle performance aggiuntivo.
  - **NetApp SnapMirror.** Mirror le copie Snapshot dei dati da un sistema storage a un altro. ONTAP supporta il mirroring dei dati su altre piattaforme fisiche e servizi nativi del cloud.
  - **NetApp SnapLock.** Amministrazione efficiente dei dati non riscrivibili, scrivendo su volumi speciali che non possono essere sovrascritti o cancellati per un determinato periodo.
  - **NetApp SnapVault.** esegue il backup dei dati da più sistemi storage in una copia Snapshot centrale che funge da backup su tutti i sistemi designati.
  - **NetApp SyncMirror.** offre mirroring dei dati in tempo reale a livello RAID su due diversi plessi di dischi collegati fisicamente allo stesso controller.
  - **NetApp SnapRestore.** offre un rapido ripristino dei dati di backup on-demand dalle copie Snapshot.
  - **NetApp FlexClone.** fornisce il provisioning istantaneo di una copia leggibile e scrivibile di un volume NetApp basata su una copia Snapshot.

Per ulteriori informazioni su ONTAP, consultare ["Centro documentazione di ONTAP 9"](#).



NetApp ONTAP è disponibile on-premise, virtualizzato o nel cloud.



### NetApp AFF/FAS

NetApp offre solide piattaforme di storage all-flash (AFF) e ibride scale-out (FAS), realizzate su misura con performance a bassa latenza, protezione integrata dei dati e supporto multiprotocollo.

Entrambi i sistemi sono basati sul software per la gestione dei dati NetApp ONTAP, il software per la gestione dei dati più avanzato del settore per una gestione dello storage semplificata, altamente disponibile e integrata nel cloud, per offrire velocità, efficienza e sicurezza di livello Enterprise per le tue esigenze di data fabric.

Per ulteriori informazioni sulle piattaforme NETAPP AFF/FAS, fare clic su ["qui"](#).

### ONTAP Select

ONTAP Select è un'implementazione software-defined di NetApp ONTAP che può essere implementata su un hypervisor nel tuo ambiente. Può essere installato su VMware vSphere o su KVM e offre tutte le funzionalità e l'esperienza di un sistema ONTAP basato su hardware.

Per ulteriori informazioni su ONTAP Select, fare clic su ["qui"](#).

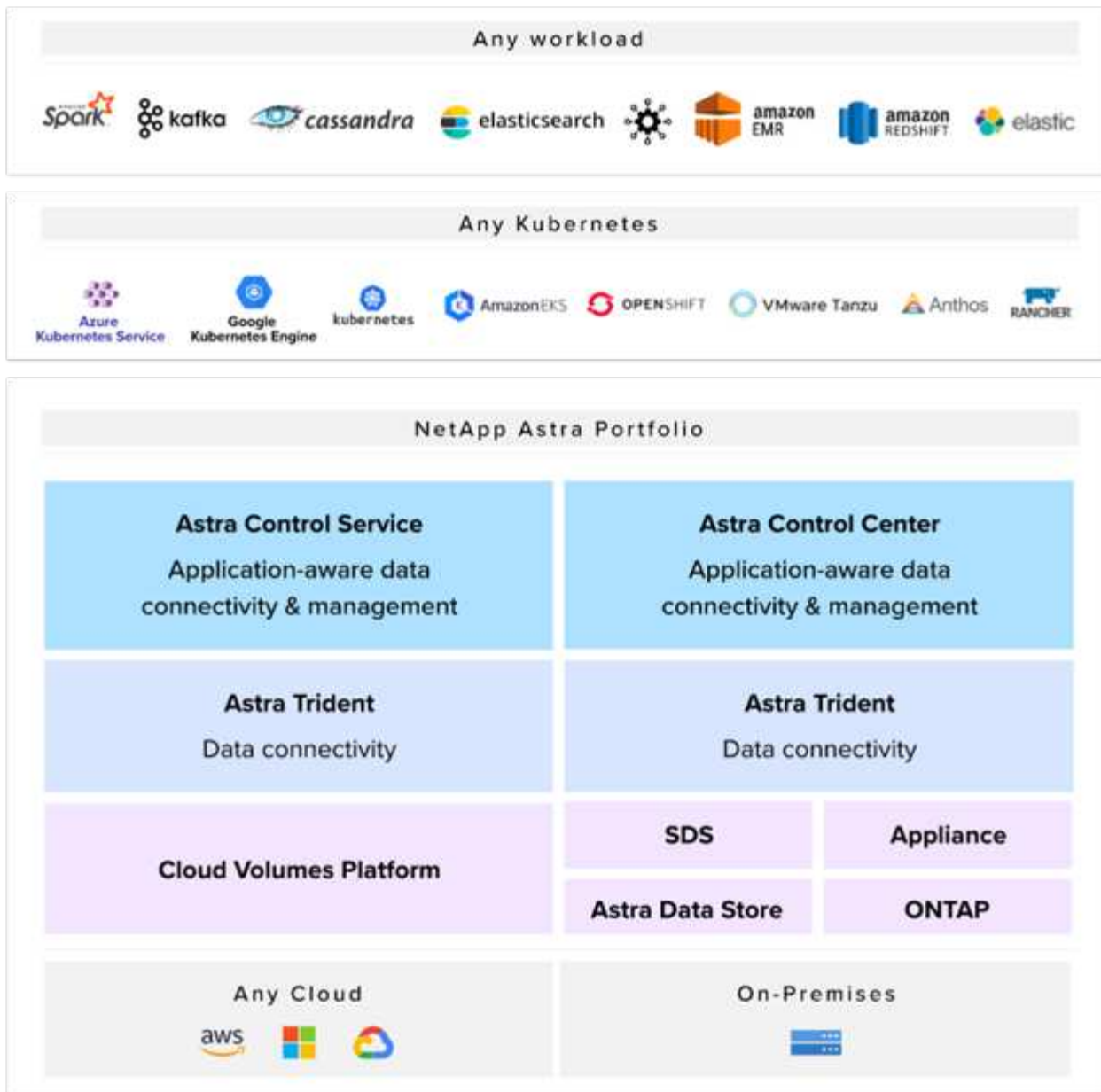
### Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP è una versione di NetApp ONTAP implementata nel cloud che può essere implementata in diversi cloud pubblici, tra cui Amazon AWS, Microsoft Azure e Google Cloud.

Per ulteriori informazioni su Cloud Volumes ONTAP, fare clic su ["qui"](#).

### Panoramica sull'integrazione dello storage NetApp

NetApp offre una serie di prodotti che consentono di orchestrare, gestire, proteggere e migrare le applicazioni stateful containerizzate e i relativi dati.



NetApp Astra Control offre un set completo di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful basati sulla tecnologia di protezione dei dati di NetApp. Astra Control Service è disponibile per supportare carichi di lavoro stateful nelle implementazioni Kubernetes native nel cloud. Astra Control Center è disponibile per supportare carichi di lavoro stateful in implementazioni on-premise di piattaforme Enterprise Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito Web di NetApp Astra Control ["qui"](#).

NetApp Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito web di Astra Trident ["qui"](#).

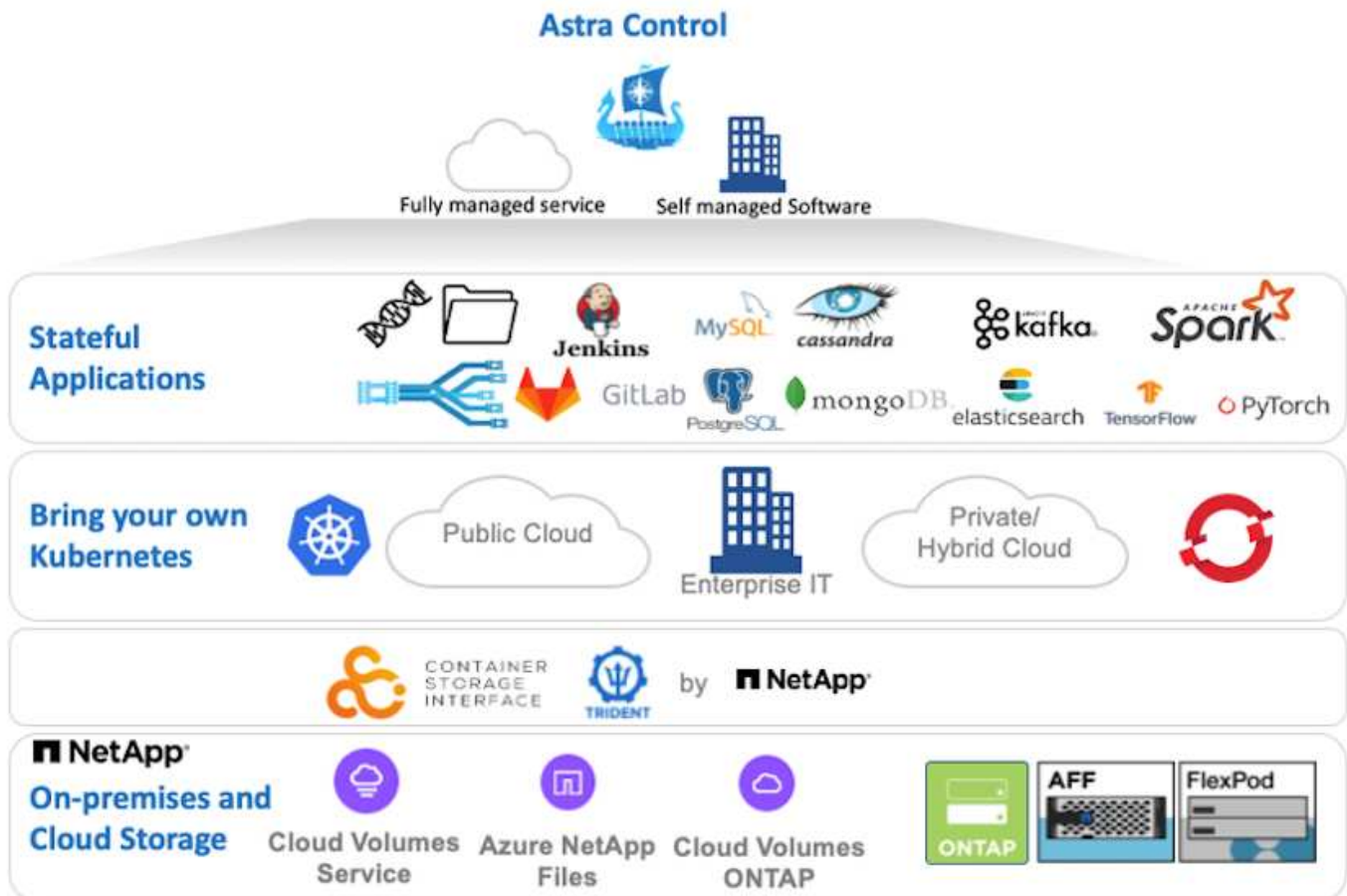
Le pagine seguenti contengono informazioni aggiuntive sui prodotti NetApp validati per la gestione delle applicazioni e dello storage persistente nella soluzione VMware Tanzu with NetApp:

- ["NetApp Astra Control Center"](#)
- ["NetApp Astra Trident"](#)



## Panoramica di NetApp Astra Control

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati basati su applicazioni e storage per carichi di lavoro Kubernetes stateful implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati di NetApp.



NetApp Astra Control Center può essere installato su un cluster VMware Tanzu che ha installato e configurato Astra Trident Storage orchestrator con classi di storage e backend di storage per i sistemi storage NetApp ONTAP.

Per ulteriori informazioni su Astra Trident, vedere ["questo documento qui"](#).

In un ambiente connesso al cloud, il centro di controllo Astra utilizza Cloud Insights per fornire monitoraggio avanzato e telemetria. In assenza di una connessione Cloud Insights, sono disponibili funzioni limitate di monitoraggio e telemetria (per un valore di sette giorni di metriche) ed esportate negli strumenti di monitoraggio nativi di Kubernetes (Prometheus e Grafana) attraverso endpoint di metriche aperte.

Il centro di controllo Astra è completamente integrato nell'ecosistema NetApp AutoSupport e Active IQ per fornire supporto agli utenti, fornire assistenza per la risoluzione dei problemi e visualizzare le statistiche di utilizzo.

Oltre alla versione a pagamento di Astra Control Center, è disponibile anche una licenza di valutazione di 90 giorni. La versione di valutazione è supportata tramite e-mail e il canale slack della community. I clienti hanno accesso a queste risorse, ad altri articoli della Knowledge base e alla documentazione disponibile nella dashboard di supporto dei prodotti.

Per ulteriori informazioni sul portfolio Astra, visitare il ["Sito web Astra"](#).



## Automazione di Astra Control Center

Astra Control Center dispone di un'API REST completamente funzionale per l'accesso programmatico. Gli utenti possono utilizzare qualsiasi linguaggio di programmazione o utility per interagire con gli endpoint API REST di Astra Control. Per ulteriori informazioni su questa API, consultare la documentazione ["qui"](#).

Se stai cercando un toolkit di sviluppo software pronto per interagire con le API REST di Astra Control, NetApp fornisce un toolkit con l'SDK di Astra Control Python che puoi scaricare ["qui"](#).

Se la programmazione non è adatta alla situazione e si desidera utilizzare uno strumento di gestione della configurazione, è possibile clonare ed eseguire i playbook Ansible pubblicati da NetApp ["qui"](#).

## Prerequisiti per l'installazione di Astra Control Center

L'installazione di Astra Control Center richiede i seguenti prerequisiti:

- Uno o più cluster Tanzu Kubernetes, gestiti da un cluster di gestione o da TKGS o TKGI. Sono supportati i cluster di workload TKG 1.4+ e i cluster di utenti TKGI 1.12.2+.
- Astra Trident deve essere già installato e configurato su ciascuno dei cluster Tanzu Kubernetes.
- Uno o più sistemi storage NetApp ONTAP con ONTAP 9.5 o superiore.



È consigliabile che ogni Tanzu Kubernetes installato in un sito disponga di una SVM dedicata per lo storage persistente. Le implementazioni multi-sito richiedono sistemi storage aggiuntivi.

- È necessario configurare un backend di storage Trident su ogni cluster Tanzu Kubernetes con una SVM supportata da un cluster ONTAP.
- Un StorageClass predefinito configurato su ciascun cluster Tanzu Kubernetes con Astra Trident come provisioning dello storage.
- È necessario installare e configurare un bilanciamento del carico su ciascun cluster Tanzu Kubernetes per il bilanciamento del carico e l'esposizione di Astra Control Center se si utilizza ingressType `AccTraefik`.
- È necessario installare e configurare un controller di ingresso su ciascun cluster Tanzu Kubernetes per esporre Astra Control Center se si utilizza ingressType `Generic`.
- È necessario configurare un registro di immagini privato per ospitare le immagini di NetApp Astra Control Center.
- È necessario disporre dell'accesso Cluster Admin al cluster Tanzu Kubernetes in cui viene installato Astra Control Center.
- È necessario disporre dell'accesso come amministratore ai cluster NetApp ONTAP.
- Una workstation di amministrazione RHEL o Ubuntu.

## Installare Astra Control Center

Questa soluzione descrive una procedura automatica per l'installazione di Astra Control Center utilizzando i playbook Ansible. Se si sta cercando una procedura manuale per installare Astra Control Center, seguire la guida dettagliata all'installazione e alle operazioni ["qui"](#).

1. Per utilizzare i playbook Ansible che implementano Astra Control Center, è necessario disporre di una macchina Ubuntu/RHEL con Ansible installato. Seguire le procedure ["qui"](#) Per Ubuntu e RHEL.
2. Clonare il repository GitHub che ospita il contenuto Ansible.

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. Accedere al NetApp Support Site e scaricare l'ultima versione di NetApp Astra Control Center. Per farlo, è necessaria una licenza allegata al tuo account NetApp. Dopo aver scaricato il tarball, trasferirlo sulla workstation.



Per iniziare a utilizzare una licenza di prova per Astra Control, visitare il sito ["Sito di registrazione Astra"](#).

4. Creare o ottenere il file kubeconfig con accesso amministratore all'utente o al cluster del carico di lavoro Tanzu Kubernetes su cui deve essere installato Astra Control Center.
5. Modificare la directory in `na_astra_control_suite`.

```
cd na_astra_control_suite
```

6. Modificare il `vars/vars.yml` archiviare e compilare le variabili con le informazioni richieste.

```
#Define whether or not to push the Astra Control Center images to your
private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or "Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer type
service to access ACC, requires MetalLB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the kubernetes/openshift
cluster Astra Control Center needs to be installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want to
```

```

accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the PVCs
to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values: yes,
no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image registry
credentials
#Usually, the registry namespace and usernames are same for individual
users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

7. Esegui il manuale per implementare Astra Control Center. Il playbook richiede privilegi root per alcune configurazioni.

Eseguire il seguente comando per eseguire il playbook se l'utente che esegue il playbook è root o ha configurato sudo senza password.

```
ansible-playbook install_acc_playbook.yml
```

Se l'utente ha configurato l'accesso sudo basato su password, eseguire il seguente comando per eseguire il manuale e inserire la password sudo.

```
ansible-playbook install_acc_playbook.yml -K
```

### Fasi successive all'installazione

1. Il completamento dell'installazione potrebbe richiedere alcuni minuti. Verificare che tutti i pod e i servizi in `netapp-astra-cc` namespace in esecuzione.

```
[netapp-user@rhel7 ~]$ kubectl get all -n netapp-astra-cc
```

2. Controllare `acc-operator-controller-manager` registri per garantire che l'installazione sia completata.

```
[netapp-user@rhel7 ~]$ kubectl logs deploy/acc-operator-controller-  
manager -n netapp-acc-operator -c manager -f
```



Il seguente messaggio indica la corretta installazione di Astra Control Center.

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[22.04.0]"}
```

3. Il nome utente per l'accesso ad Astra Control Center è l'indirizzo e-mail dell'amministratore fornito nel file CRD e la password è una stringa `ACC-` Aggiunto all'UUID di Astra Control Center. Eseguire il seguente comando:

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc  
NAME      UUID  
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



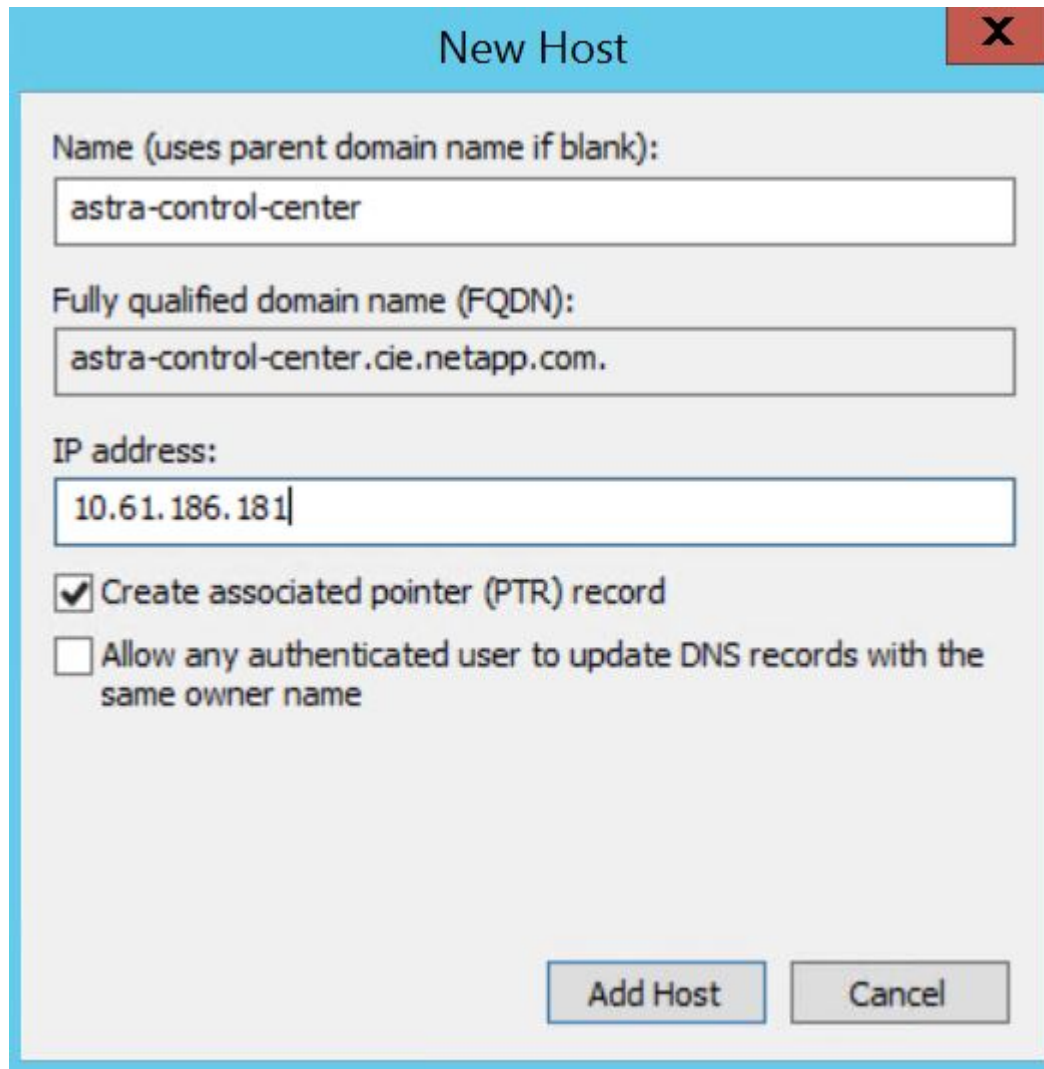
In questo esempio, la password è `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

4. Ottenere l'IP del bilanciamento del carico del servizio `traefik` se il tipo di `entressType` è `AccTraefik`.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep  
'EXTERNAL|traefik'
```

| NAME       | EXTERNAL-IP   | PORT(S)                     | TYPE         | CLUSTER-IP    |
|------------|---------------|-----------------------------|--------------|---------------|
| traefik    | 10.61.186.181 | 80:30343/TCP, 443:30060/TCP | LoadBalancer | 172.30.99.142 |
| AGE<br>16m |               |                             |              |               |

5. Aggiungere una voce nel server DNS che punta all'FQDN fornito nel file CRD di Astra Control Center  
EXTERNAL-IP del servizio traefik.



New Host

Name (uses parent domain name if blank):  
astra-control-center

Fully qualified domain name (FQDN):  
astra-control-center.cie.netapp.com.

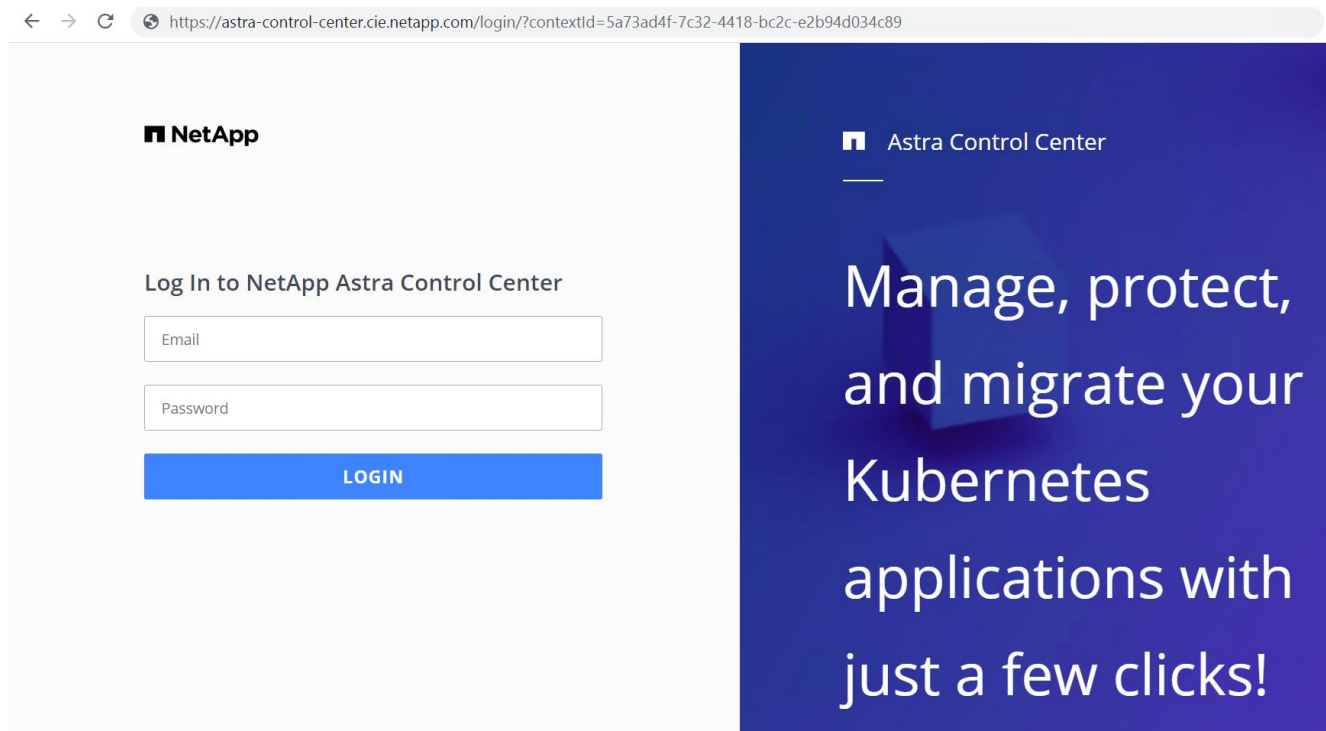
IP address:  
10.61.186.181

☒ Create associated pointer (PTR) record

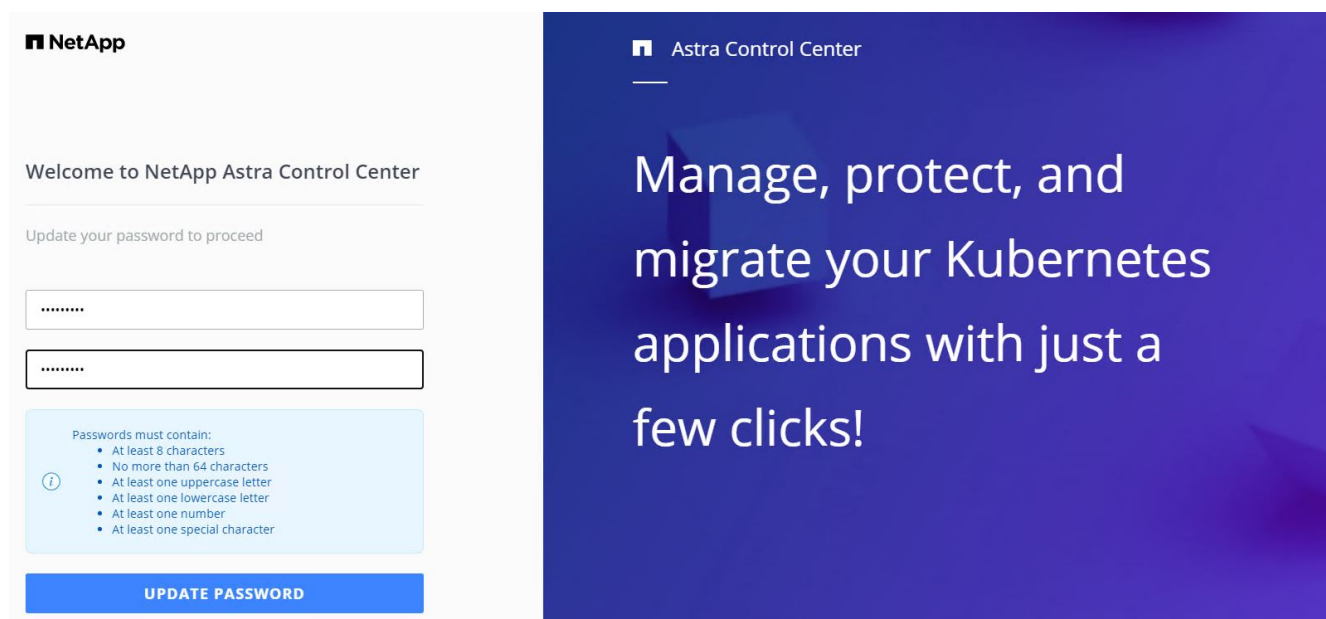
☐ Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

6. Accedere alla GUI di Astra Control Center esplorando il relativo FQDN.



7. Quando si accede all'interfaccia grafica di Astra Control Center per la prima volta utilizzando l'indirizzo email admin fornito in CRD, è necessario modificare la password.



8. Se si desidera aggiungere un utente ad Astra Control Center, accedere a account > Users (account > utenti), fare clic su Add (Aggiungi), inserire i dettagli dell'utente e fare clic su Add (Aggiungi).

**Add user**
✕

USER DETAILS

First name

Nikhil

Last name

Kulkarni

Email address

tme\_nik@netapp.com

PASSWORD

Temporary password

\*\*\*\*\*

Confirm temporary password

\*\*\*\*\*

ⓘ

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE ?

Role

Owner

▼

Cancel

Add ✓

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

9. Astra Control Center richiede una licenza per il funzionamento di tutte le sue funzionalità. Per aggiungere una licenza, accedere a account > License (account > licenza), fare clic su Add License (Aggiungi licenza) e caricare il file di licenza.

Account

Users

Credentials

Notifications

License

Connections

ASTRA CONTROL CENTER LICENSE 0

To get started with Astra Control Center, select Add license to manually upload the file.

Add license

ADD LICENSE

Select and add a license file.

License file

EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

⬆

✕

Cancel

Add




In caso di problemi con l'installazione o la configurazione di NetApp Astra Control Center, è disponibile la knowledge base dei problemi noti ["qui"](#).

## Registra i tuoi cluster VMware Tanzu Kubernetes con Astra Control Center


Per consentire ad Astra Control Center di gestire i carichi di lavoro, devi prima registrare i cluster Tanzu Kubernetes.

## Registrare i cluster VMware Tanzu Kubernetes

1. Il primo passo consiste nell'aggiungere i cluster Tanzu Kubernetes all'Astra Control Center e gestirli. Accedere a Clusters e fare clic su Add a Cluster (Aggiungi cluster), caricare il file kubeconfig per il cluster Tanzu Kubernetes e fare clic su Select Storage (Seleziona storage).

 **Add Kubernetes cluster**

STEP 1/3: CREDENTIALS



CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.


[Upload file](#) [Paste from clipboard](#)

Kubeconfig YAML file  
tkgi-kubeconfig.txt

Credential name  
tkgi-acc

Cancel

Next →


 **ADDING CLUSTERS**

Adding a cluster allows Astra Control to install its storage services, and enable data management operations on your containerized applications.

For more details on required versions or cloud specific setup refer to the documentation.

Read more in [Adding clusters](#).

2. Astra Control Center rileva le classi di storage idonee. Selezionare ora il modo in cui lo storageclass effettua il provisioning dei volumi utilizzando Trident supportato da una SVM su NetApp ONTAP e fare clic su Review (esamina). Nel riquadro successivo, verificare i dettagli e fare clic su Add Cluster (Aggiungi cluster).
3. Una volta aggiunto, il cluster passa allo stato di rilevamento mentre Astra Control Center lo ispeziona e installa gli agenti necessari. Lo stato del cluster diventa **Healthy** una volta completata la registrazione.

 **Clusters**




Actions ▾

[+ Add Kubernetes cluster](#)

Search

1-1 of 1 entries

< >

| <input type="checkbox"/> | Name ↓                   | State   | Type   | Version          | Actions   |
|--------------------------|--------------------------|---|--|------------------|---|
| <input type="checkbox"/> | <a href="#">tkgi-acc</a> |  Healthy |  Kubernetes | v1.22.6+vmware.1 |  |



Tutti i cluster di Tanzu Kubernetes gestiti da Astra Control Center devono avere accesso al registro delle immagini utilizzato per l'installazione, poiché gli agenti installati sui cluster gestiti estraggono le immagini da tale registro.

4. Importa i cluster ONTAP come risorse storage da gestire come back-end dal centro di controllo Astra. Quando i cluster Tanzu Kubernetes vengono aggiunti ad Astra e viene configurato uno storageclass, il cluster ONTAP viene automaticamente scoperto e ispezionato a supporto dello storageclass, ma non viene



importato nel centro di controllo Astra da gestire.

Backends

+ Add

Search

★

1

1-1 of 1 entries

<

>

| Name ↓                  | State                                       | Capacity          | Throughput        | Type  | Cluster        | Cloud          | Actions                |
|-------------------------|---|-------------------|-------------------|-------|----------------|----------------|------------------------|
| 172.21.224.201(trident) | <div><div></div><div>Discovered</div></div> | Not available yet | Not available yet | ONTAP | Not applicable | Not applicable | <div><div></div></div> |

5. Per importare i cluster ONTAP, accedere a backend, fare clic sul menu a discesa e selezionare Manage (Gestisci) accanto al cluster ONTAP da gestire. Immettere le credenziali del cluster ONTAP, fare clic su informazioni di revisione, quindi fare clic su Importa backend storage.

Manage ONTAP storage backend

STEP 1/2: CREDENTIALS

CREDENTIALS

Enter cluster administrator credentials for the ONTAP storage backend you want to manage.

Cluster management IP address

172.21.224.201

User name

admin

Password

\*\*\*\*\*

MANAGING STORAGE BACKENDS

Storage backends provide storage to your Kubernetes applications.

Managing storage clusters in Astra Control as a storage backend will allow you to get linkages between PVs and the storage backend. You will also see capacity and health details of the storage backend, including performance metrics if Astra Control is connected to Cloud Insights.

Read more in [Storage type](#) .

ONTAP

Cancel



Next →

6. Una volta aggiunti i backend, lo stato diventa disponibile. Questi backend ora dispongono delle informazioni sui volumi persistenti nel cluster Tanzu Kubernetes e sui volumi corrispondenti nel sistema ONTAP.

283


## Backends

7. Per il backup e il ripristino nei cluster Tanzu Kubernetes utilizzando Astra Control Center, è necessario eseguire il provisioning di un bucket di storage a oggetti che supporti il protocollo S3. Le opzioni attualmente supportate sono ONTAP S3, StorageGRID, AWS S3 e lo storage Microsoft Azure Blob. Ai fini di questa installazione, configureremo un bucket AWS S3. Accedere a Bucket, fare clic su Add bucket (Aggiungi bucket) e selezionare Generic S3. Inserisci i dettagli sul bucket S3 e le credenziali per accedervi, fai clic sulla casella di controllo Rendi questo bucket il bucket predefinito per il cloud, quindi fai clic su Aggiungi.

 **Add bucket** 

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type

 Generic S3


Existing bucket name

na-tanzu-astra/na-astra-tkgi

Description (optional)

S3 server name or IP address

s3.us-east-1.amazonaws.com

☒ Make this bucket the default bucket for this cloud 

SELECT CREDENTIALS


Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.

Add [Use existing](#)

Select credential


AWS Creds

Cancel

Add 

**BUCKETS**

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

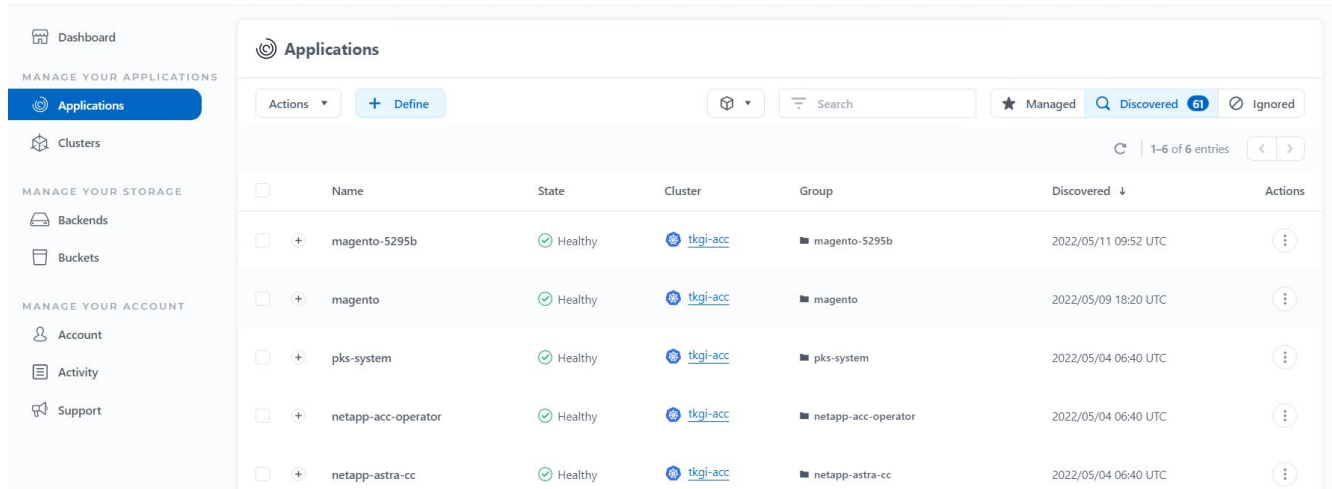
Read more in [Storage buckets](#) .

## Scegliere le applicazioni da proteggere

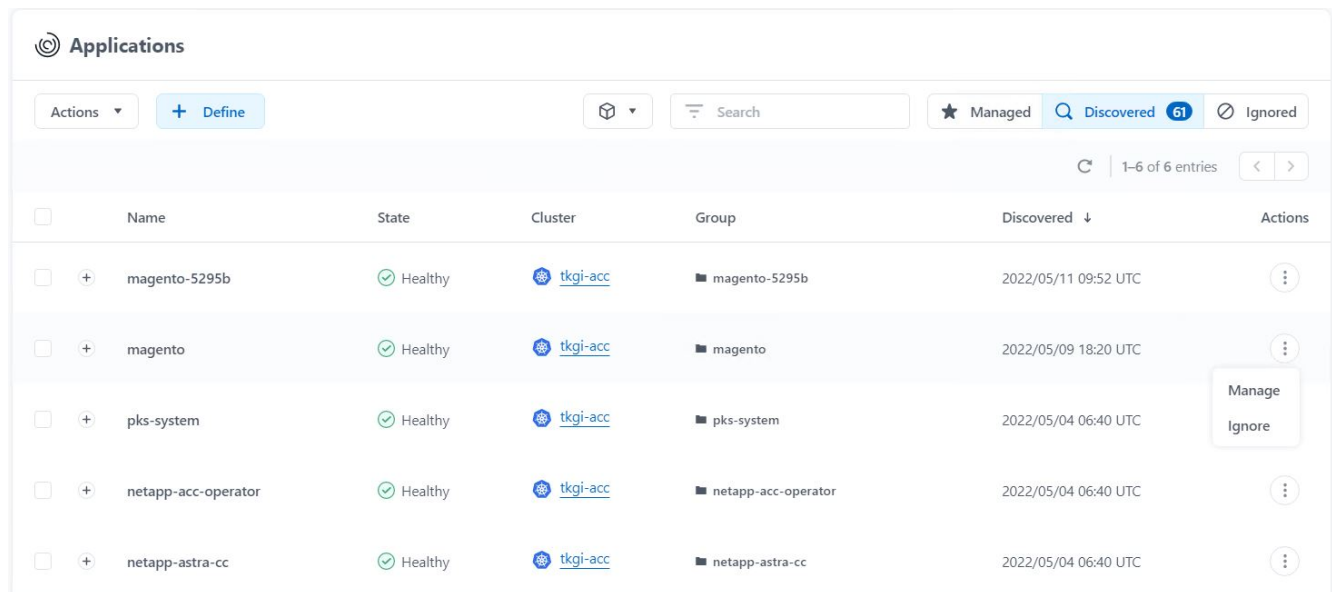
Dopo aver registrato i cluster Tanzu Kubernetes, è possibile individuare le applicazioni implementate e gestirle tramite Astra Control Center.

## Gestire le applicazioni

1. Una volta registrati i cluster e i backend ONTAP di Tanzu Kubernetes con il centro di controllo Astra, il centro di controllo inizia automaticamente a rilevare le applicazioni in tutti gli spazi dei nomi che utilizzano lo storageclass configurato con il backend ONTAP specificato.



2. Accedere a Apps > Discovered (applicazioni > rilevate) e fare clic sul menu a discesa accanto all'applicazione che si desidera gestire utilizzando Astra. Quindi fare clic su Manage (Gestisci)



3. L'applicazione entra nello stato Available (disponibile) e può essere visualizzata nella scheda Managed (gestito) nella sezione Apps (applicazioni).

Applications

Actions ▾

+ Define

All clusters ▾

⌵

Search

★ Managed

🔍

Discovered 

60

🚫

Ignored

↻

1-1 of 1 entries

<

>

| <input type="checkbox"/> | Name                    | State                | Protection                | Cluster                               | Group                | Discovered ↓         | Actions      |
|--------------------------|-------------------------|----------------------|---------------------------|---------------------------------------|----------------------|----------------------|--------------|
| <input type="checkbox"/> | <a href="#">magento</a> | <div>✓</div> Healthy | <div>⚠️</div> Unprotected | <div>🌐</div> <a href="#">tkgi-acc</a> | <div>📁</div> magento | 2022/05/09 18:20 UTC | <div>⋮</div> |

Proteggi le tue applicazioni

Una volta gestiti i carichi di lavoro delle applicazioni da Astra Control Center, è possibile configurare le impostazioni di protezione per tali carichi di lavoro.

Creare un’istantanea dell’applicazione

Un’istantanea di un’applicazione crea una copia Snapshot di ONTAP e una copia dei metadati dell’applicazione che possono essere utilizzati per ripristinare o clonare l’applicazione in un momento specifico in base a tale copia Snapshot.

1. Per creare un’istantanea dell’applicazione, accedere alla scheda applicazioni > gestite e fare clic sull’applicazione di cui si desidera creare una copia Snapshot. Fare clic sul menu a discesa accanto al nome dell’applicazione e fare clic su Snapshot.

Actions ▾

APPLICATION STATUS

✓ Healthy

APPLICATION PROTECTION STATUS

⚠️ Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61

docker.io/bitnami/magento:2.4.1-debian-10-r14

docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Snapshot

Backup

Clone

Restore

Unmanage

2. Inserire i dettagli dell’istantanea, fare clic su Next (Avanti), quindi su Snapshot (istantanea). La creazione dello snapshot richiede circa un minuto e lo stato diventa disponibile dopo la creazione dello snapshot.

**Snapshot namespace application**

STEP 1/2: DETAILS

✕

**SNAPSHOT DETAILS**

Name  
magento-snapshot-20220516212403

**CREATING APPLICATION SNAPSHOTS**

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#).

- Namespace application  
magento
- Namespace  
magento
- Cluster  
tkgi-acc

Cancel

Next →

## Creare un backup dell'applicazione

Un backup di un'applicazione acquisisce lo stato attivo dell'applicazione e la configurazione delle risorse IT, le taglia in file e le memorizza in un bucket di storage a oggetti remoto.

- Per il backup e il ripristino delle applicazioni gestite nel centro di controllo Astra, è necessario configurare le impostazioni del superutente per i sistemi ONTAP di backup come prerequisito. A tale scopo, immettere i seguenti comandi.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

- Per creare un backup dell'applicazione gestita in Astra Control Center, accedere alla scheda Apps (applicazioni) > Managed (gestite) e fare clic sull'applicazione di cui si desidera eseguire il backup. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Backup.

**APPLICATION STATUS**

**APPLICATION PROTECTION STATUS**

Images  
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/magento:2.4.1-debian-10-r14  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule  
Disabled

Group  
magento

Cluster  
tkgi-acc

Actions

Snapshot

Backup


Clone

Restore

Unmanage

- Inserire i dettagli del backup, selezionare il bucket di storage a oggetti in cui memorizzare i file di backup, fare clic su Next (Avanti) e, dopo aver esaminato i dettagli, fare clic su Backup (Backup). A seconda delle dimensioni dell'applicazione e dei dati, il backup può richiedere alcuni minuti e lo stato del backup diventa

disponibile una volta completato correttamente il backup.

 **Back up namespace application**

STEP 1/2: DETAILS

X

BACKUP DETAILS

Name  
magento-backup-20220516212622

☐ Back up from an existing snapshot ?

BACKUP DESTINATION

Bucket  
na-tanzu-astra/na-astra-tkgi Available Default

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#).

Namespace application  
magento

Namespace  
magento

Cluster  
tkgi-acc


Cancel

Next →

## Ripristino di un'applicazione

Con la semplice pressione di un pulsante, è possibile ripristinare un'applicazione nello spazio dei nomi di origine nello stesso cluster o in un cluster remoto per la protezione delle applicazioni e il disaster recovery.

1. Per ripristinare un'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione in questione. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Restore (Ripristina).

 **magento**

↻

Actions ▼

APPLICATION STATUS  
Healthy

APPLICATION PROTECTION STATUS  
Unprotected

Images  
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/magento:2.4.1-debian-10-r14  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule  
Disabled

Group  
magento

Cluster  
tkgi-acc

2. Immettere il nome dello spazio dei nomi di ripristino, selezionare il cluster in cui si desidera ripristinarlo e scegliere se si desidera ripristinarlo da uno snapshot esistente o da un backup dell'applicazione. Fare clic su Avanti.

Restore namespace application

STEP 1/2: DETAILS

X

RESTORE DETAILS

Destination cluster

tkgi-acc

Destination namespace

magento

RESTORE SOURCE

Filter

Snapshots

Backups

| Application backup   | State              | On-Schedule/On-Demand | Created ↑                       |
|--|--------------------|-----------------------|---------------------------------|
| <input type="radio"/> <div>magento-backup-20220516212730</div> | <div>Healthy</div> | <div>On-Demand</div>  | <div>2022/05/16 21:27 UTC</div> |

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

Namespace application

magento

Namespace

magento

Cluster

tkgi-acc

Cancel

Next →

- Nel riquadro di revisione, immettere `restore` E fare clic su Restore (Ripristina) dopo aver esaminato i dettagli.

Restore namespace application

STEP 2/2: SUMMARY

X

REVIEW RESTORE INFORMATION

All existing resources associated with this namespace application will be deleted and replaced with the source backup "magento-backup-20220516212730" taken on 2022/05/16 21:27 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this namespace application might be impacted.

We recommend taking a snapshot or a backup of your namespace application before proceeding.

BACKUP

magento-backup-20220516212730

ORIGINAL GROUP

magento

ORIGINAL CLUSTER

tkgi-acc

RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

RESTORE

magento

DESTINATION GROUP

magento

DESTINATION CLUSTER

tkgi-acc

RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

Are you sure you want to restore the namespace application "magento"?

Type restore below to confirm.

Confirm to restore

restore

Back

Restore ✓

- La nuova applicazione passa allo stato di ripristino mentre Astra Control Center ripristina l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).

289

Applications

Actions ▾

+ Define

All clusters ▾

Search

★ Managed

Discovered

60

Ignored

1-1 of 1 entries

| <input type="checkbox"/> | Name                    | State                         | Protection                        | Cluster  | Group                         | Discovered ↓         | Actions                |
|--------------------------|-------------------------|-------------------------------|-----------------------------------|--|-------------------------------|----------------------|------------------------|
| <input type="checkbox"/> | <a href="#">magento</a> | <div><div></div>Healthy</div> | <div><div></div>Unprotected</div> | <div><div></div><a href="#">tkgi-acc</a></div> | <div><div></div>magento</div> | 2022/05/09 18:20 UTC | <div><div></div></div> |

## Clonare un'applicazione

È possibile clonare un'applicazione nel cluster di origine o in un cluster remoto per scopi di sviluppo/test o protezione dell'applicazione e disaster recovery. La clonazione di un'applicazione all'interno dello stesso cluster sullo stesso backend di storage utilizza la tecnologia NetApp FlexClone, che clona i PVC all'istante e consente di risparmiare spazio di storage.

1. Per clonare un'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione in questione. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Clone (Clona).

magento

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61  
docker.io/bitnami/magento:2.4.1-debian-10-r14  
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Actions

Snapshot  
Backup  
Clone  
Restore  
Unmanage

2. Immettere i dettagli del nuovo spazio dei nomi, selezionare il cluster in cui si desidera clonarlo e scegliere se clonarlo da uno snapshot esistente, da un backup o dallo stato corrente dell'applicazione. Fare clic su Next (Avanti), quindi su Clone (Clona) nel riquadro di revisione dopo aver esaminato i dettagli.



Clone namespace application

STEP 1/2: DETAILS

✕

CLONE DETAILS

Clone namespace  
magento-bef7f

Destination cluster  
tkgi-acc

☐ Clone from an existing snapshot or backup

CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Not all applications may support cloning.

Read more in [Clone applications](#)

- Namespace application  
magento
- Namespace  
magento
- Cluster  
tkgi-acc

Cancel

Next →

3. La nuova applicazione passa allo stato di rilevamento mentre Astra Control Center crea l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).

Applications

Actions ▾

+ Define

All clusters ▾

Search

★ Managed

🔍 Discovered 60

🚫 Ignored

1-2 of 2 entries

< >

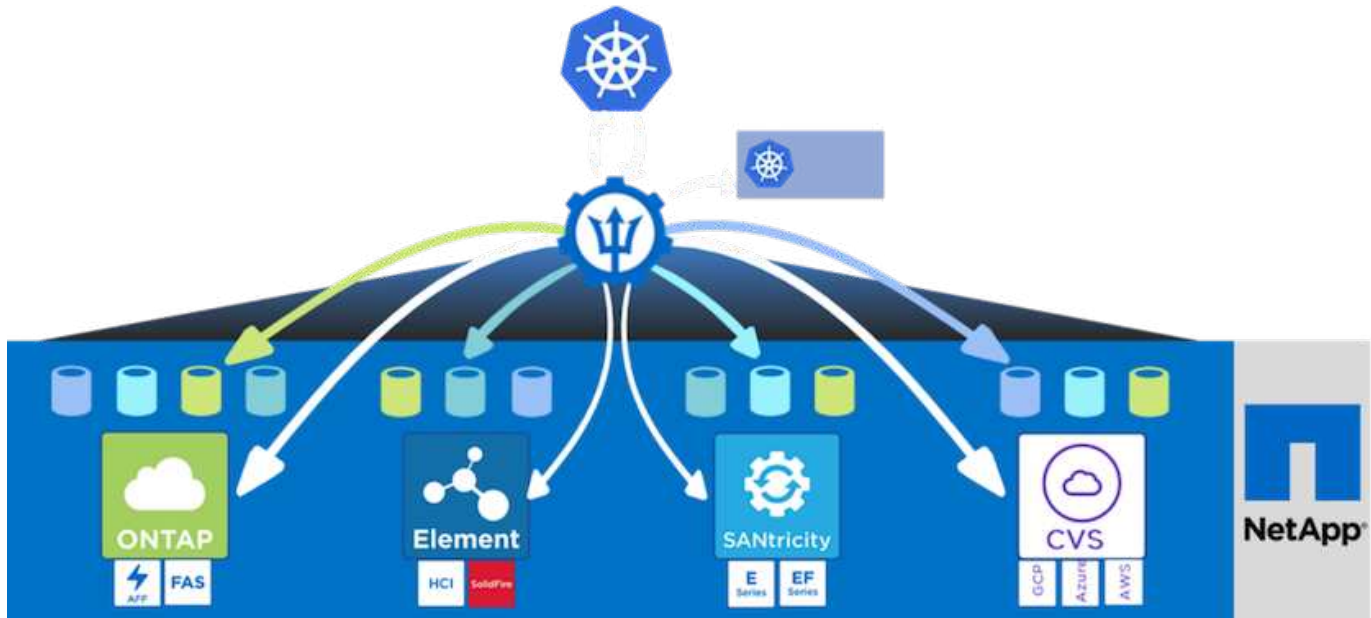
| <input type="checkbox"/> | Name                          | State     | Protection             | Cluster  | Group         | Discovered ↓         | Actions |
|--------------------------|-------------------------------|-----------|------------------------|----------|---------------|----------------------|---------|
| <input type="checkbox"/> | <a href="#">magento-bef7f</a> | ✓ Healthy | ⚠️ Unprotected         | tkgi-acc | magento-bef7f | 2022/05/16 21:31 UTC | ⋮       |
| <input type="checkbox"/> | <a href="#">magento</a>       | ✓ Healthy | ℹ️ Partially protected | tkgi-acc | magento       | 2022/05/09 18:20 UTC | ⋮       |

## Panoramica di Astra Trident

Astra Trident è uno storage orchestrator open-source completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident lavora con l'intero portfolio di storage NetApp, inclusi i sistemi storage NetApp ONTAP ed Element, e supporta anche connessioni NFS e iSCSI. Trident accelera il workflow DevOps consentendo agli utenti finali di eseguire il provisioning e gestire lo storage dai sistemi storage NetApp senza richiedere l'intervento di un amministratore dello storage.

Un amministratore può configurare una serie di backend di storage in base alle esigenze di progetto e ai modelli di sistemi di storage che consentono funzionalità di storage avanzate, tra cui compressione, tipi di dischi specifici o livelli di QoS che garantiscono un certo livello di performance. Una volta definiti, questi backend possono essere utilizzati dagli sviluppatori nei loro progetti per creare dichiarazioni di volume

persistenti (PVC) e per collegare storage persistente ai propri container on-demand.



Astra Trident ha un rapido ciclo di sviluppo e, come Kubernetes, viene rilasciato quattro volte all'anno.

L'ultima versione di Astra Trident è la 22.04 rilasciata ad aprile 2022. Matrice di supporto per quale versione di Trident è stata testata con la quale è possibile trovare la distribuzione Kubernetes "qui".

A partire dalla versione 20.04, l'impostazione di Trident viene eseguita dall'operatore Trident. L'operatore semplifica le implementazioni su larga scala e fornisce supporto aggiuntivo, inclusa la riparazione automatica dei pod implementati nell'installazione di Trident.

Con la versione 21.01, è stato reso disponibile un grafico Helm per facilitare l'installazione dell'operatore Trident.

### Implementare l'operatore Trident utilizzando Helm

1. Innanzitutto, impostare la posizione del cluster utente `kubeconfig` File come variabile di ambiente in modo da non doverla fare riferimento, perché Trident non ha alcuna opzione per passare questo file.

```
<<<<<<< HEAD
[netapp-user@rhel7]$ export KUBECONFIG=~/.tanzu-install/auth/kubeconfig
=====
[netapp-user@rhel7]$ export KUBECONFIG=~/.Tanzu-install/auth/kubeconfig
>>>>>>> eba1007b77b1ef6011dadd158f1df991acc5299f
```

2. Aggiungi il repository NetApp Astra Trident Helm.

```
[netapp-user@rhel7]$ helm repo add netapp-trident
https://netapp.github.io/trident-helm-chart
"netapp-trident" has been added to your repositories
```

### 3. Aggiornare i repository Helm.

```
[netapp-user@rhel7]$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart repository
...Successfully got an update from the "bitnami" chart repository
Update Complete. ☐Happy Helming!☐
```

### 4. Creare un nuovo namespace per l'installazione di Trident.

```
[netapp-user@rhel7]$ kubectl create ns trident
```

### 5. Crea un segreto con le credenziali DockerHub per scaricare le immagini di Astra Trident.

```
[netapp-user@rhel7]$ kubectl create secret docker-registry docker-registry-cred --docker-server=docker.io --docker-username=netapp-solutions-tme --docker-password=xxxxxxx -n trident
```

### 6. Per i cluster di utenti o carichi di lavoro gestiti da TKGS (vSphere con Tanzu) o TKG con implementazioni di cluster di gestione, completare la seguente procedura per installare Astra Trident:

- a. Assicurarsi che l'utente che ha effettuato l'accesso disponga delle autorizzazioni necessarie per creare account di servizio nello spazio dei nomi Trident e che gli account di servizio nello spazio dei nomi Trident dispongano delle autorizzazioni necessarie per creare pod.
- b. Eseguire il seguente comando helm per installare l'operatore Trident nello spazio dei nomi creato.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-operator -n trident --set imagePullSecrets[0]=docker-registry-cred
```

### 7. Per un cluster di utenti o workload gestito dalle implementazioni TKGI, eseguire il seguente comando helm per installare l'operatore Trident nello spazio dei nomi creato.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-operator -n trident --set imagePullSecrets[0]=docker-registry-cred,kubeletDir="/var/vcap/data/kubelet"
```

### 8. Verificare che i pod Trident siano in funzione.

| NAME                              | READY | STATUS  | RESTARTS |
|-----------------------------------|-------|---------|----------|
| AGE                               |       |         |          |
| trident-csi-6vv62                 | 2/2   | Running | 0        |
| 14m                               |       |         |          |
| trident-csi-cfd844bcc-sqhcg       | 6/6   | Running | 0        |
| 12m                               |       |         |          |
| trident-csi-dfcmz                 | 2/2   | Running | 0        |
| 14m                               |       |         |          |
| trident-csi-pb2n7                 | 2/2   | Running | 0        |
| 14m                               |       |         |          |
| trident-csi-qsw6z                 | 2/2   | Running | 0        |
| 14m                               |       |         |          |
| trident-operator-67c94c4768-xw978 | 1/1   | Running | 0        |
| 14m                               |       |         |          |

```
[netapp-user@rhel7]$ ./tridentctl -n trident version
+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+
| 22.04.0        | 22.04.0        |
+-----+
```

### Creazione di backend per il sistema storage

Dopo aver completato l'installazione di Astra Trident Operator, è necessario configurare il backend per la piattaforma di storage NetApp specifica in uso. Seguire i collegamenti riportati di seguito per continuare l'installazione e la configurazione di Astra Trident.

- ["NetApp ONTAP NFS"](#)
- ["ISCSI NetApp ONTAP"](#)

### Configurazione NFS di NetApp ONTAP

Per consentire l'integrazione di Trident con il sistema storage NetApp ONTAP tramite NFS, è necessario creare un backend che consenta la comunicazione con il sistema storage. In questa soluzione viene configurato un backend di base, ma se si cercano opzioni più personalizzate, consultare la documentazione ["qui"](#).

### Creare una SVM in ONTAP

1. Accedere a Gestore di sistema di ONTAP, selezionare Storage > Storage VM e fare clic su Aggiungi.
2. Immettere un nome per SVM, attivare il protocollo NFS, selezionare la casella di controllo Allow NFS Client Access (Consenti accesso client NFS) e aggiungere le subnet su cui si trovano i nodi di lavoro nelle regole dei criteri di esportazione per consentire il montaggio dei volumi come PVS nei cluster di workload.

# Add Storage VM



STORAGE VM NAME

trident\_svm

## Access Protocol

☒ SMB/CIFS, NFS, S3

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

| Rule Index | Clients   | Access Protocols | Read-Only Rule | Read/Wr |
|------------|-----------|------------------|----------------|---------|
|            | 0.0.0.0/0 | Any              | Any            | Any     |



Se si utilizza l'implementazione NAT dei cluster di utenti o dei cluster di workload con NSX-T, è necessario aggiungere la subnet Egress (nel caso di TKGS0 o la subnet IP mobile (nel caso di TKGI) alle regole dei criteri di esportazione.

3. Fornire i dettagli relativi ai file LIF dei dati e all'account di amministrazione SVM, quindi fare clic su Save (Salva).

## NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

### K8s-Ontap-01

IP ADDRESS

172.21.252.180

SUBNET MASK

24

GATEWAY

172.21.252.1



BROADCAST DOMAIN

Default



## Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

4. Assegnare gli aggregati a una SVM. Accedere a Storage > Storage VM (Storage VM), fare clic sui puntini di sospensione accanto alla SVM appena creata, quindi fare clic su Edit (Modifica). Selezionare la casella di controllo Limit Volume Creation to Preferred Local Tier (limita creazione volume a livelli locali preferiti) e allegarvi gli aggregati richiesti.

## Edit Storage VM



STORAGE VM NAME

trident\_svm

DEFAULT LANGUAGE

c.utf\_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

## Resource Allocation



Limit volume creation to preferred local tiers

LOCAL TIERS

K8s\_Ontap\_01\_SSD\_1 

Cancel

Save

5. In caso di implementazioni NAT di cluster di utenti o workload su cui deve essere installato Trident, la richiesta di montaggio dello storage potrebbe provenire da una porta non standard a causa di SNAT. Per impostazione predefinita, ONTAP consente le richieste di montaggio del volume solo quando originate

dalla porta root. Quindi, accedere all'interfaccia utente di ONTAP e modificare l'impostazione per consentire le richieste di montaggio da porte non standard.

```
ontap-01> vserver nfs modify -vserver tanzu_svm -mount-rootonly disabled
```

## Creare backend e StorageClasses

1. Per i sistemi NetApp ONTAP che utilizzano NFS, creare un file di configurazione back-end sul jumphost con backendName, managementLIF, dataLIF, svm, nome utente, password e altri dettagli.

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```



È consigliabile definire il valore backendName personalizzato come combinazione di storageDriverName e dataLIF che fornisce NFS per una facile identificazione.

2. Creare il backend Trident eseguendo il seguente comando.

```
[netapp-user@rhel7]$ ./tridentctl -n trident create backend -f backend-ontap-nas.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-5c87a73c5b1e |
| online |         | 0 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. Una volta creato il backend, è necessario creare una classe di storage. La seguente definizione di classe di storage di esempio evidenzia i campi obbligatori e di base. Il parametro backendType Dovrebbe riflettere il driver di storage del backend Trident appena creato.



```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"

```

4. Creare la classe di storage eseguendo il comando `kubectl`.

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-nfs.yaml
storageclass.storage.k8s.io/ontap-nfs created

```

5. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). Di seguito viene fornita una definizione di PVC di esempio. Assicurarsi che il `storageClassName` il campo corrisponde al nome della classe di storage appena creata. La definizione del PVC può essere ulteriormente personalizzata in base alle esigenze, a seconda del carico di lavoro da fornire.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-nfs

```

6. Creare il PVC emettendo il comando `kubectl`. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc

```

| NAME         | STATUS       | VOLUME                                   | CAPACITY |
|--------------|--------------|--|----------|
| ACCESS MODES | STORAGECLASS | AGE                                      |          |
| basic        | Bound        | pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d | 1Gi      |
| RWO          |              | ontap-nfs                                | 7s       |

## Configurazione iSCSI di NetApp ONTAP

Per integrare il sistema di storage NetApp ONTAP con i cluster VMware Tanzu Kubernetes per volumi persistenti tramite iSCSI, il primo passo è preparare i nodi accedendo a ciascun nodo e configurando le utility o i pacchetti iSCSI per il montaggio dei volumi iSCSI. A tale scopo, seguire la procedura descritta in questo documento ["collegamento"](#).



NetApp sconsiglia questa procedura per le implementazioni NAT dei cluster VMware Tanzu Kubernetes.



TKGI utilizza le macchine virtuali Bosh come nodi per i cluster Tanzu Kubernetes che eseguono immagini di configurazione immutabili e qualsiasi modifica manuale dei pacchetti iSCSI sulle macchine virtuali Bosh non rimane persistente durante i riavvii. Pertanto, NetApp consiglia di utilizzare volumi NFS per lo storage persistente per i cluster Tanzu Kubernetes implementati e gestiti da TKGI.

Una volta preparati i nodi del cluster per i volumi iSCSI, è necessario creare un backend che consenta la comunicazione con il sistema storage. In questa soluzione è stato configurato un backend di base, ma per ulteriori opzioni personalizzate, consultare la documentazione ["qui"](#).

## Creare una SVM in ONTAP

Per creare una SVM in ONTAP, attenersi alla seguente procedura:

1. Accedere a Gestore di sistema di ONTAP, selezionare Storage > Storage VM e fare clic su Aggiungi.
2. Inserire un nome per la SVM, attivare il protocollo iSCSI, quindi fornire i dettagli per la LIF dei dati.

# Add Storage VM



STORAGE VM NAME

trident\_svm\_iscsi

## Access Protocol

SMB/CIFS, NFS, S3

iSCSI

☒ Enable iSCSI

NETWORK INTERFACE

### K8s-Ontap-01

IP ADDRESS

10.61.181.231

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

☐ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

10.61.181.232

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

3. Inserire i dettagli dell'account di amministrazione SVM, quindi fare clic su Save (Salva).

## Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

Save

Cancel

4. Per assegnare gli aggregati alla SVM, selezionare Storage > Storage VM (Storage > Storage VM), fare clic sui puntini di sospensione accanto alla SVM appena creata, quindi fare clic su Edit (Modifica). Selezionare la casella di controllo Limit Volume Creation to Preferred Local Tier (limita creazione volume a livelli locali preferiti) e allegarvi gli aggregati richiesti.

## Edit Storage VM



STORAGE VM NAME

trident\_svm\_iscsi

DEFAULT LANGUAGE

c.utf\_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

## Resource Allocation

☒ Limit volume creation to preferred local tiers

LOCAL TIERS

K8s\_Ontap\_01\_SSD\_1 

Cancel

Save

### Creare backend e StorageClasses

1. Per i sistemi NetApp ONTAP che utilizzano NFS, creare un file di configurazione back-end sul jumphost con backendName, managementLIF, dataLIF, svm, nome utente, password e altri dettagli.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap-san+10.61.181.231",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.231",
  "svm": "trident_svm_iscsi",
  "username": "admin",
  "password": "password"
}
```

2. Creare il backend Trident eseguendo il seguente comando.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |                      UUID                      |
| STATE | VOLUMES | |                      |                      |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san+10.61.181.231 | ontap-san      | 6788533c-7fea-4a35-b797- |
| fb9bb3322b91 | online |      0 | |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. Dopo aver creato un backend, è necessario creare una classe di storage. La seguente definizione di classe di storage di esempio evidenzia i campi obbligatori e di base. Il parametro `backendType` Dovrebbe riflettere il driver di storage del backend Trident appena creato. Annotare anche il valore del campo `nome`, a cui si deve fare riferimento in un passaggio successivo.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-iscsi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```



Esiste un campo opzionale chiamato `fsType` definito in questo file. Nei backend iSCSI, questo valore può essere impostato su un tipo di file system Linux specifico (XFS, ext4 e così via) o può essere cancellato per consentire ai cluster Tanzu Kubernetes di decidere quale filesystem utilizzare.

4. Creare la classe di storage eseguendo il comando kubectl.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-iscsi.yaml
storageclass.storage.k8s.io/ontap-iscsi created
```

5. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). Di seguito viene fornita una definizione di PVC di esempio. Assicurarsi che il `storageClassName` il campo corrisponde al nome della classe di storage appena creata. La definizione del PVC può essere ulteriormente personalizzata in base alle esigenze, a seconda del carico di lavoro da fornire.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-iscsi
```

6. Creare il PVC emettendo il comando kubectl. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
basic      Bound      pvc-7ceac1ba-0189-43c7-8f98-094719f7956c  1Gi
RWO                ontap-iscsi      3s
```

## Video e demo: VMware Tanzu con NetApp

I seguenti video mostrano alcune delle funzionalità descritte in questo documento:

[Utilizza Astra Trident per eseguire il provisioning dello storage persistente in VMware Tanzu - VMware Tanzu con NetApp](#)

[Utilizza il centro di controllo Astra per clonare le applicazioni in VMware Tanzu - VMware Tanzu con NetApp](#)



Queste demo sono state registrate come anteprima tecnica utilizzando la versione 1.3.1 di TKG e la versione 21,12 di Astra Control Center. Consulta la matrice di supporto per le versioni ufficiali supportate.

## Ulteriori informazioni: VMware Tanzu con NetApp

Per ulteriori informazioni sulle informazioni descritte in questo documento, visitare i seguenti siti Web:

- Documentazione NetApp

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Documentazione di Astra Trident

["https://docs.netapp.com/us-en/trident/"](https://docs.netapp.com/us-en/trident/)

- Documentazione di NetApp Astra Control Center

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Documentazione Ansible

["https://docs.ansible.com/"](https://docs.ansible.com/)

- Documentazione VMware Tanzu

["https://docs.vmware.com/en/VMware-Tanzu/index.html"](https://docs.vmware.com/en/VMware-Tanzu/index.html)

- Documentazione di VMware Tanzu Kubernetes Grid

["https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-index.html"](https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-index.html)

- Documentazione del servizio Grid VMware Tanzu Kubernetes

["https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-152BE7D2-E227-4DAA-B527-557B564D9718.html"](https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-152BE7D2-E227-4DAA-B527-557B564D9718.html)

- Documentazione di VMware Tanzu Kubernetes Grid Integrated Edition

["https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid-Integrated-Edition/index.html"](https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid-Integrated-Edition/index.html)

## Soluzioni archiviate

### Anthos su bare metal

=  
:allow-uri-read:



## Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.