



# **Virtualizzazione Red Hat OpenShift con NetApp ONTAP**

NetApp Solutions

NetApp  
April 26, 2024

This PDF was generated from [https://docs.netapp.com/it-it/netapp-solutions/containers/rh-os-n\\_use\\_case\\_openshift\\_virtualization\\_overview.html](https://docs.netapp.com/it-it/netapp-solutions/containers/rh-os-n_use_case_openshift_virtualization_overview.html) on April 26, 2024. Always check docs.netapp.com for the latest.

# Sommario

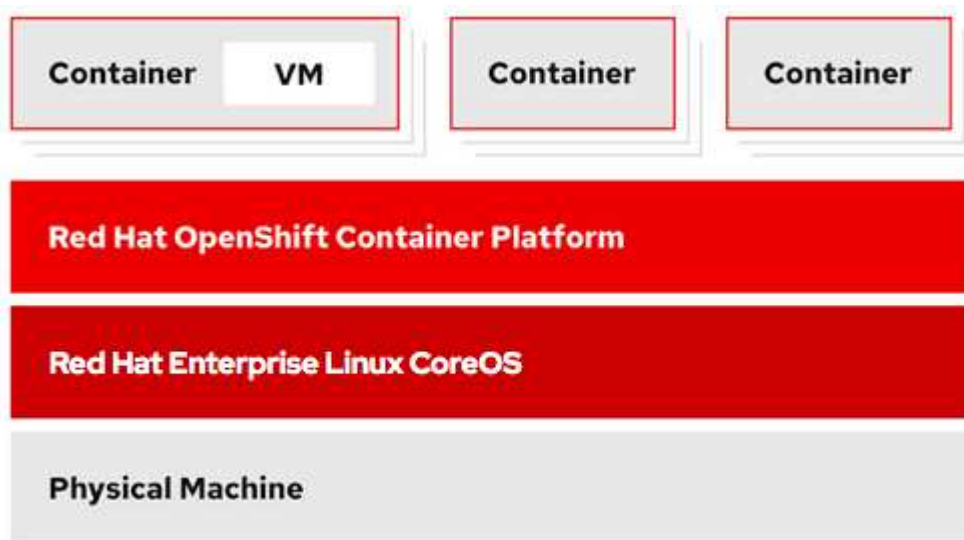
- Virtualizzazione Red Hat OpenShift con NetApp ONTAP ..... 1
  - Virtualizzazione Red Hat OpenShift con NetApp ONTAP ..... 1
  - Implementazione per la virtualizzazione OpenShift ..... 1
  - Protezione dei dati per la virtualizzazione OpenShift ..... 26
  - Monitoraggio tramite Cloud Insights ..... 48

# 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)



## OpenShift Virtualization

2.6.2 provided by Red Hat

[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

**i** 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

**HC** OpenShift  
Virtualization  
Deployment

**i** 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).



## Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.



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 ▾	Search by name...	
Name ↑	Managed Namespaces ↑	Status
 <b>OpenShift Virtualization</b> 2.6.2 provided by Red Hat	 openshift-cnv	 Succeeded Up to date
		Last updated: May 18, 8:02 pm Provided APIs: OpenShift Virtualization Deployment, HostPathProvisioner deployment

## Flussi di lavoro

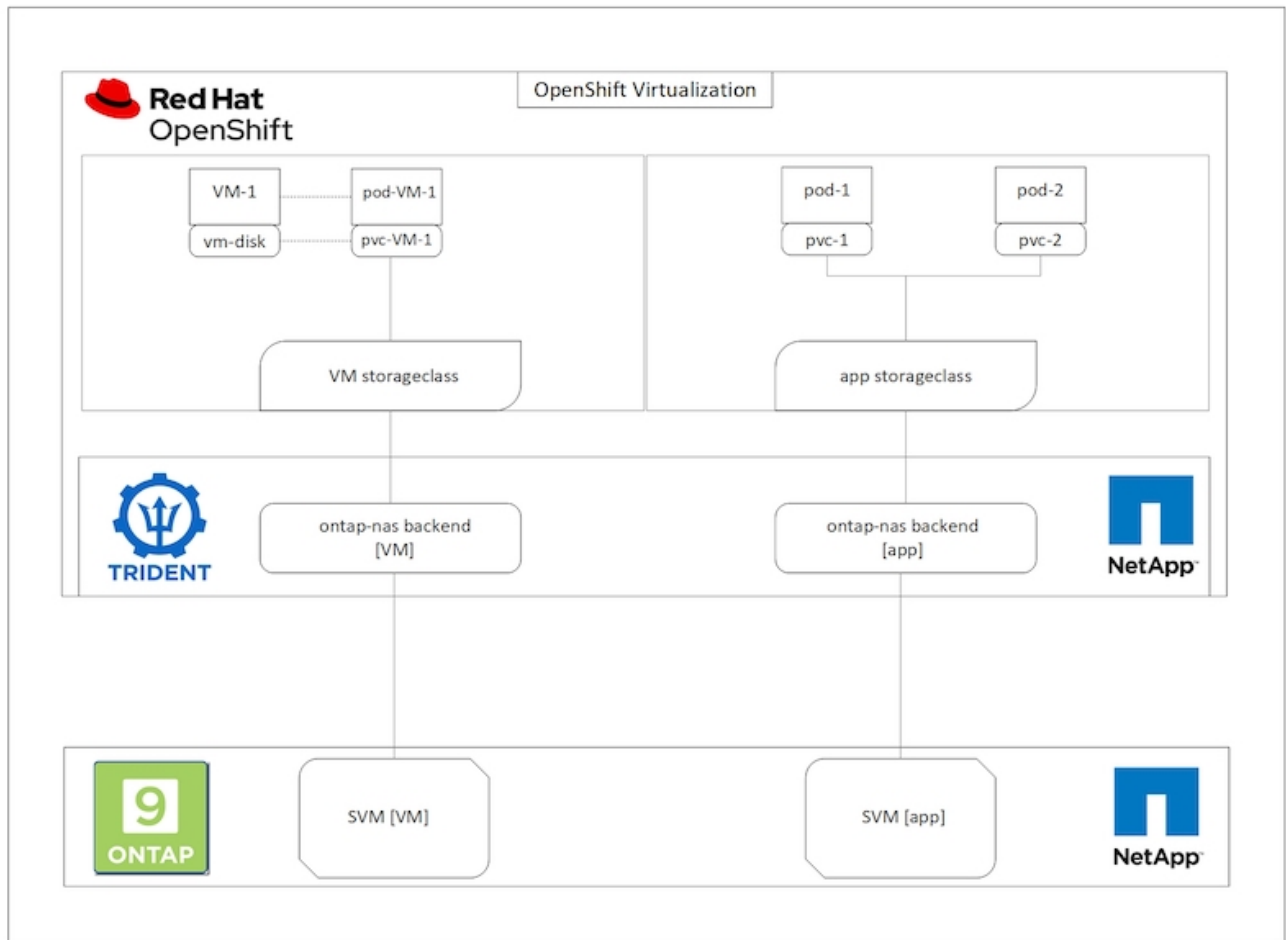
### Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

#### 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

Workload profile ⓘ

40 GiB

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

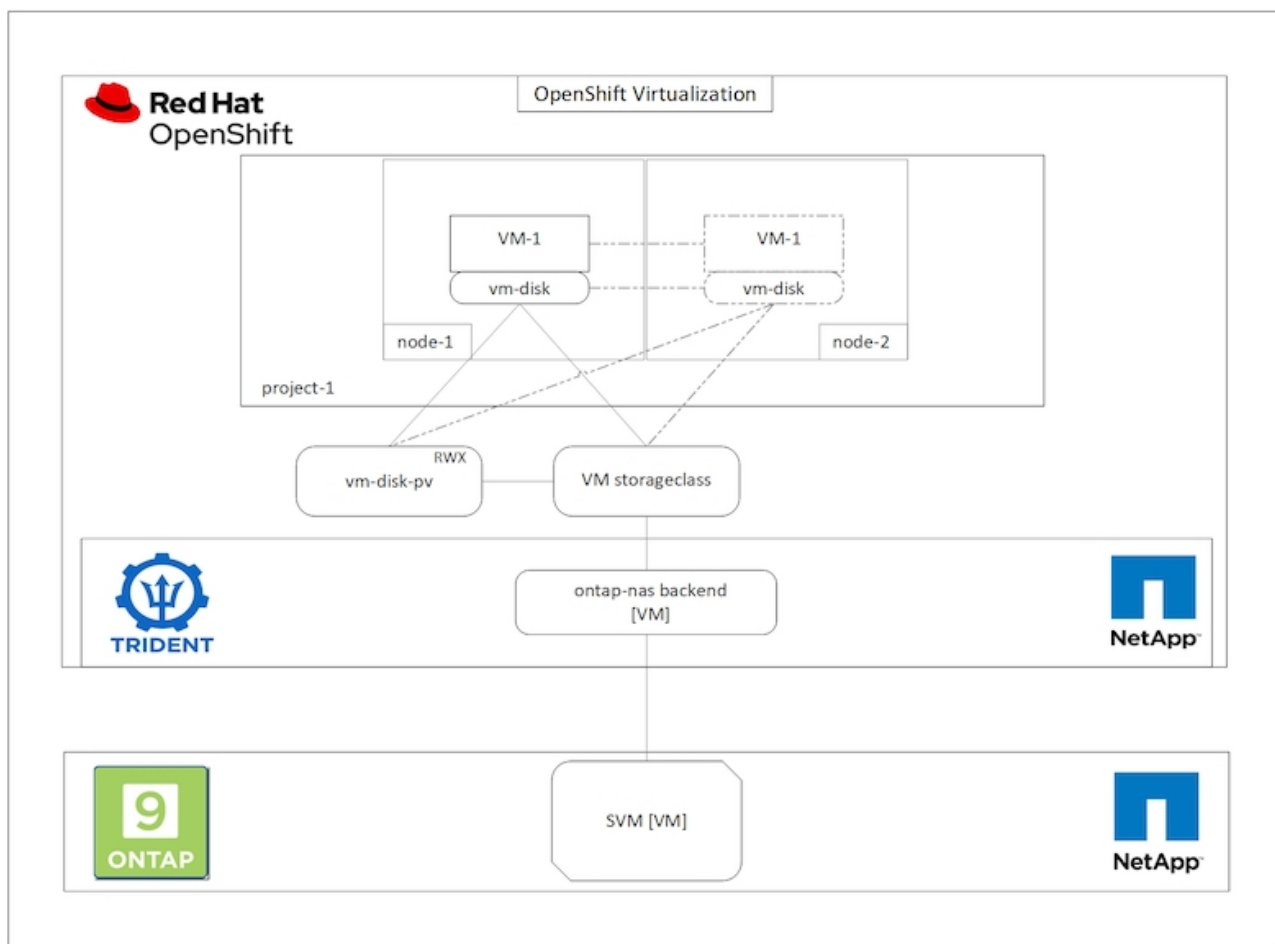
6. Se si desidera personalizzare la macchina virtuale, fare clic su **Customize Virtual Machine** (Personalizza macchina virtuale) e modificare i parametri richiesti.
7. Fare clic su **Create Virtual Machine** (Crea macchina virtuale) per creare la macchina virtuale; in questo modo viene fatto rotare 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.

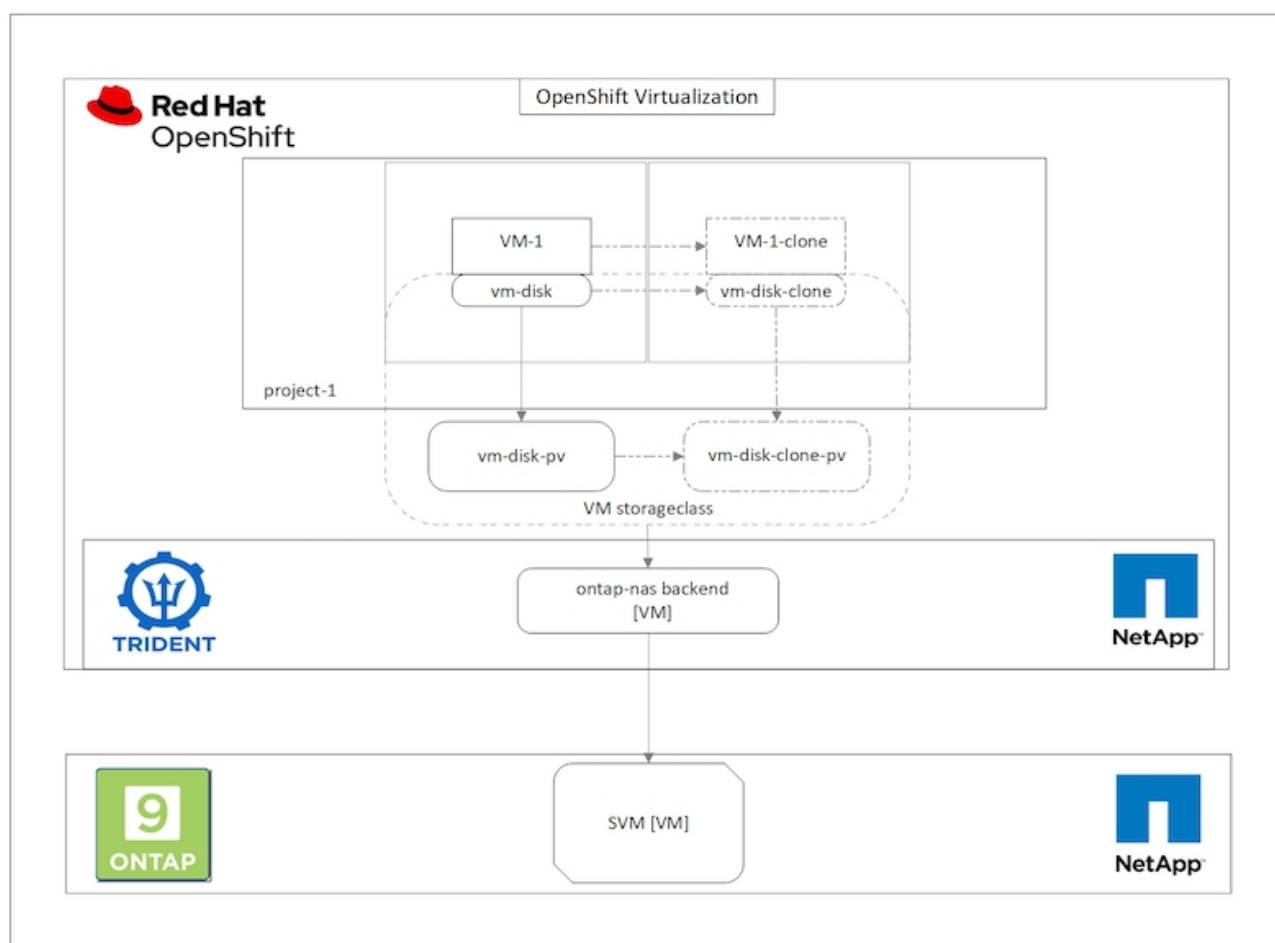


Un'istanza della macchina virtuale in un cluster OpenShift esegue automaticamente la migrazione a un altro nodo quando il nodo originale viene messo in modalità di manutenzione se evictionStrategy è impostato su LiveMigrate.

## 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

 default

Requested capacity

20 GiB

Access mode

Shared Access (RWX)

Storage Class

 basic

Used capacity

2.2 GiB

Volume mode

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-28dvvb-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.

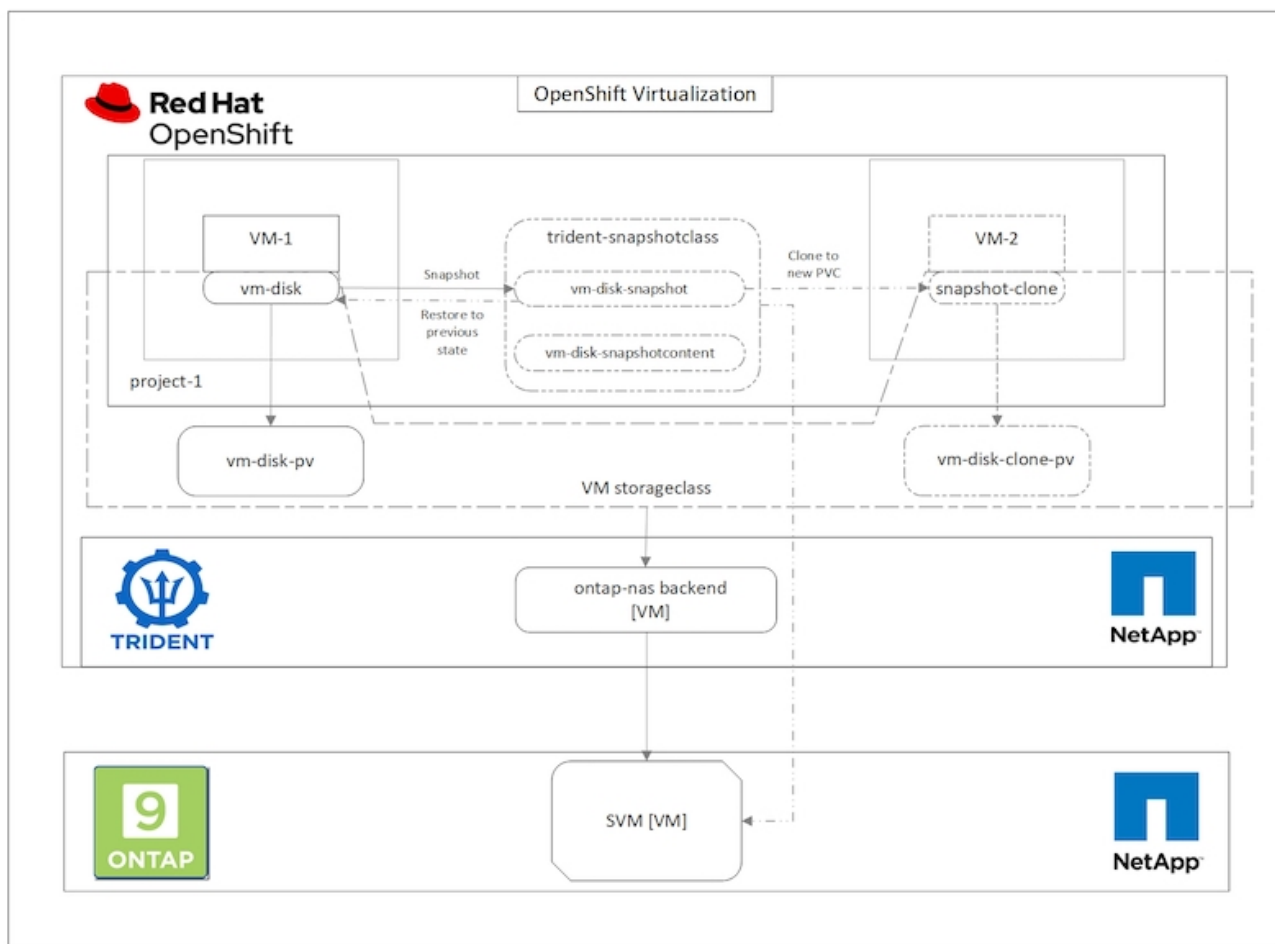
## Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

### 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-28dvv-snapshot** is finished a new crash-consistent PVC copy will be created.

Name \*

rhel8-short-frog-rootdisk-28dvv-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

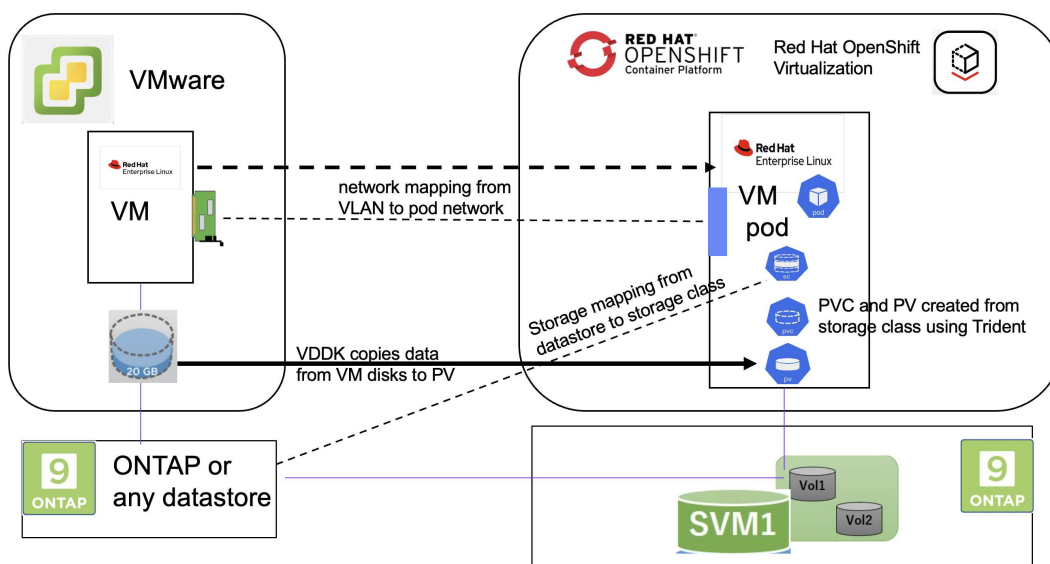
In questa sezione, vedremo come utilizzare l'Toolkit di migrazione per la virtualizzazione (MTV) per migrare le macchine virtuali da VMware alla virtualizzazione OpenShift eseguita sulla piattaforma contenitore OpenShift e integrata con lo storage NetApp ONTAP utilizzando Astra Trident.

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.

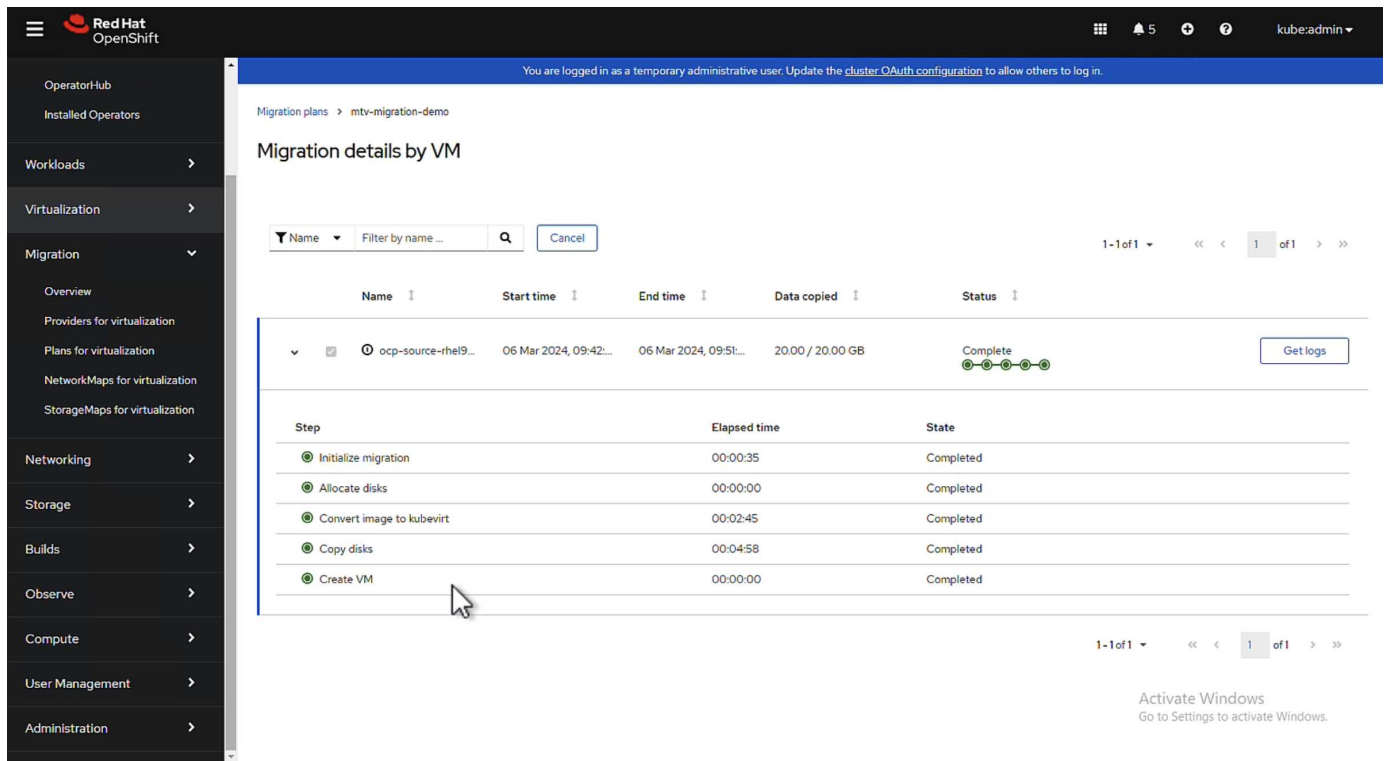
Durante la creazione di un piano, è necessario creare quanto segue se non è già stato creato:

- 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. 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 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... <a href="#">Start</a>
PL vmware-osv-migration cold	PR vmware2	PR host	1	Succeeded 1 of 1 VMs migrated	Migrating RHEL 9 vm to OpenShift Virtu...
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.



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.

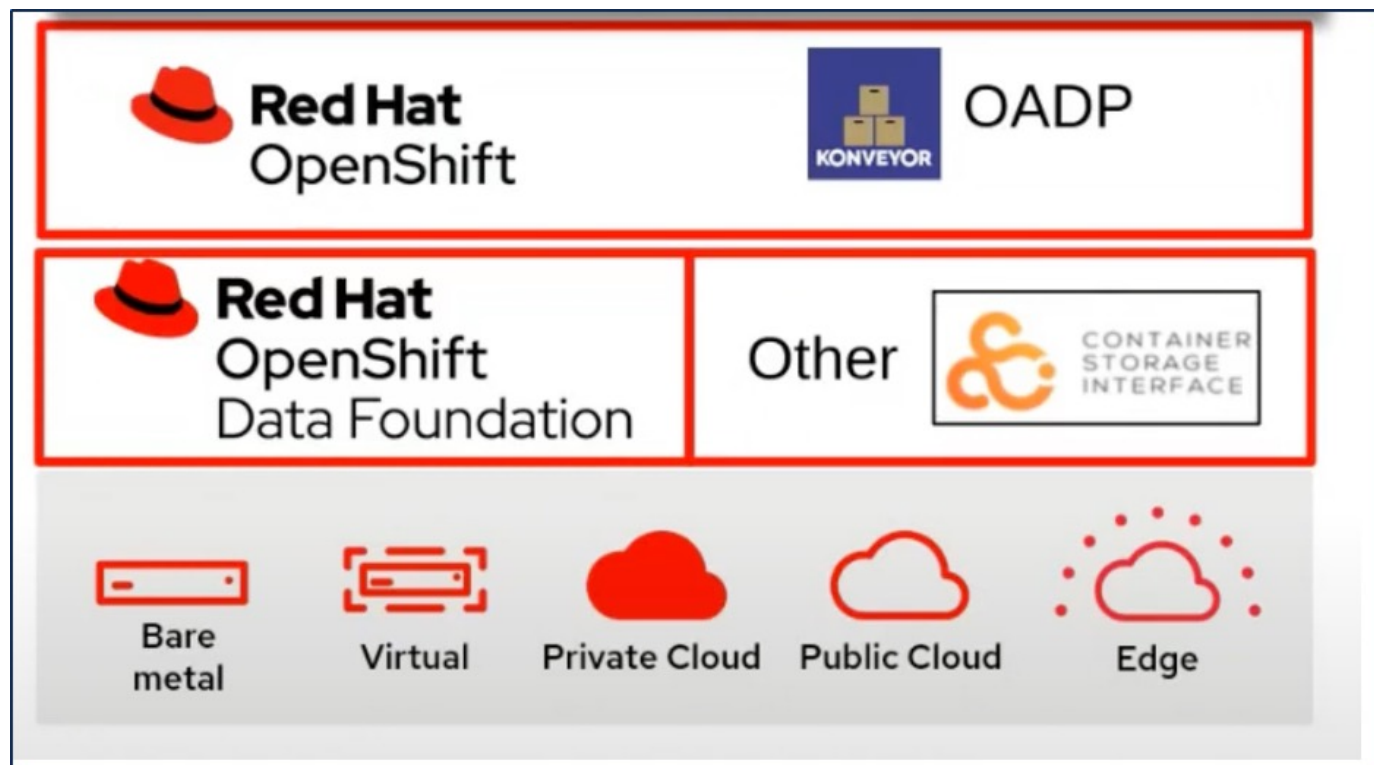
Le macchine virtuali nell'ambiente di virtualizzazione OpenShift sono applicazioni containerizzate che vengono eseguite nei nodi di lavoro della piattaforma container OpenShift. È importante proteggere i metadati delle macchine virtuali e i dischi persistenti delle macchine virtuali, in modo che in caso 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

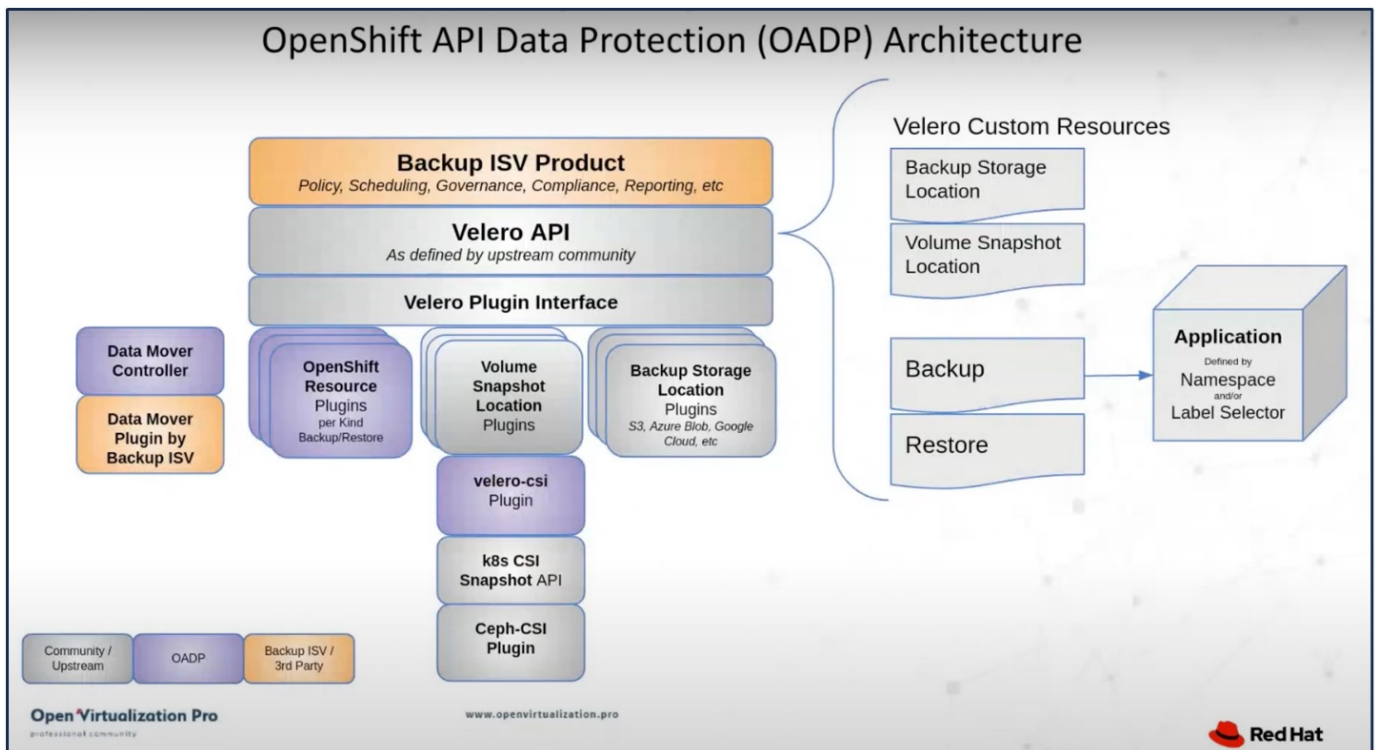
- Storage a oggetti ONTAP
- StorageGRID

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

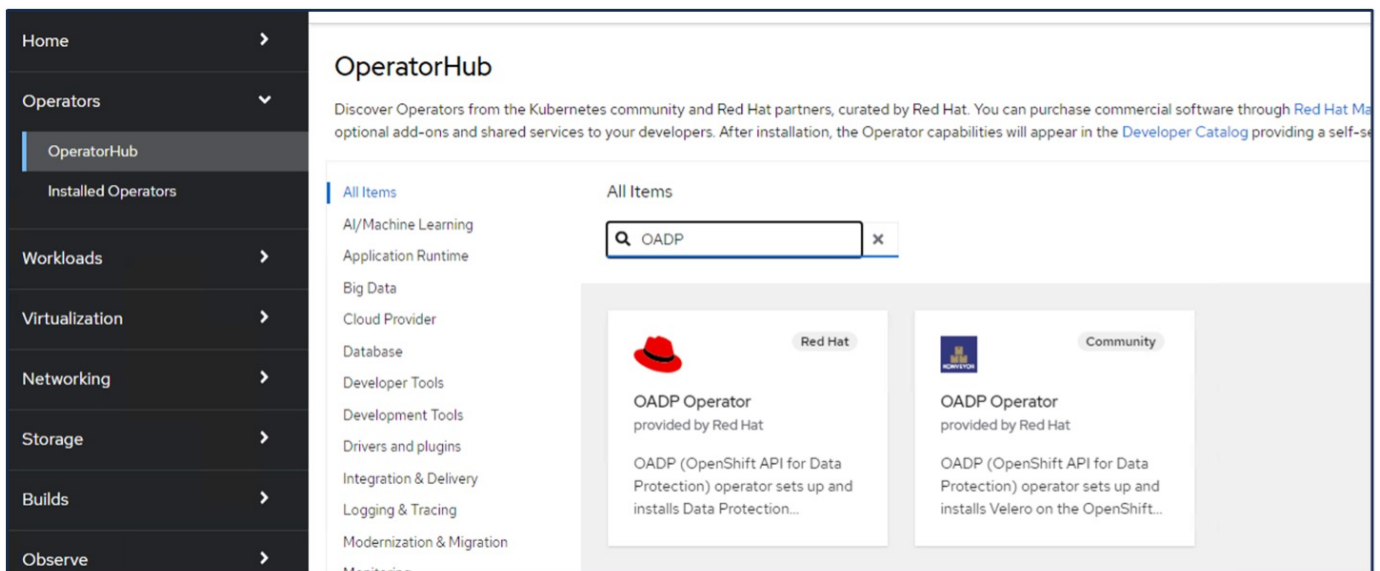
- Classe Snapshot Trident creata nel cluster
- Accesso cluster-admin al cluster Red Hat OpenShift
- Accesso amministrativo al cluster NetApp ONTAP
- Operatore di virtualizzazione OpenShift installato e configurato
- VM implementate in uno spazio dei nomi su OpenShift Virtualization
- Una workstation 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> 4.14.4 provided by Red Hat	 openshift-cnv	 openshift-cnv	 Succeeded Up to date
 <b>OADP Operator</b> 1.3.0 provided by Red Hat	 openshift-adp	 openshift-adp	 Succeeded Up to date
 <b>Package Server</b> 0.0.1-snapshot provided by	 openshift-operator-lifecycle- manager	 openshift-operator-lifecycle- 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

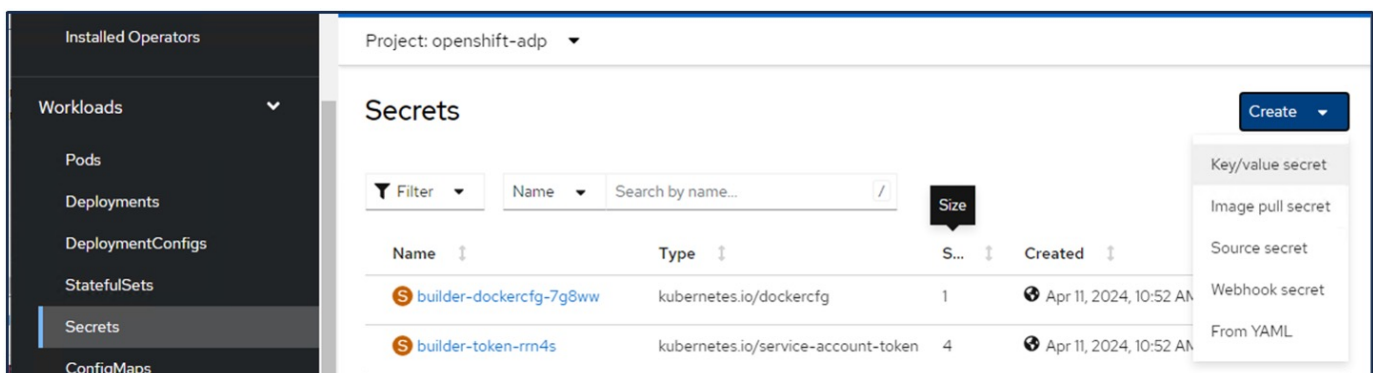
Velero può essere configurato per utilizzare l'archiviazione oggetti compatibile con S3. È possibile configurare StorageGRID S3 utilizzando le procedure illustrate nella ["Documentazione StorageGRID"](#). Per l'integrazione con Velero, sono necessarie le seguenti informazioni della configurazione di 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					
	<div>Name</div> <div></div>	<div>Managed Namespaces</div> <div></div>	<div>Status</div> <div></div>	<div>Last updated</div> <div></div>	<div>Provided APIs</div> <div></div>
	<div></div> <div>OADP Operator</div> <div>1.3.0 provided by Red Hat</div>	<div></div> <div>openshift-adp</div>	<div></div> <div>Succeeded</div> <div>Up to date</div>	<div></div> <div>Apr 11, 2024, 10:53 AM</div>	<div><a href="#">BackupRepository</a></div> <div><a href="#">Backup</a></div> <div><a href="#">BackupStorageLocation</a></div> <div><a href="#">DeleteBackupRequest</a></div> <div><a href="#">View 11 more...</a></div>

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

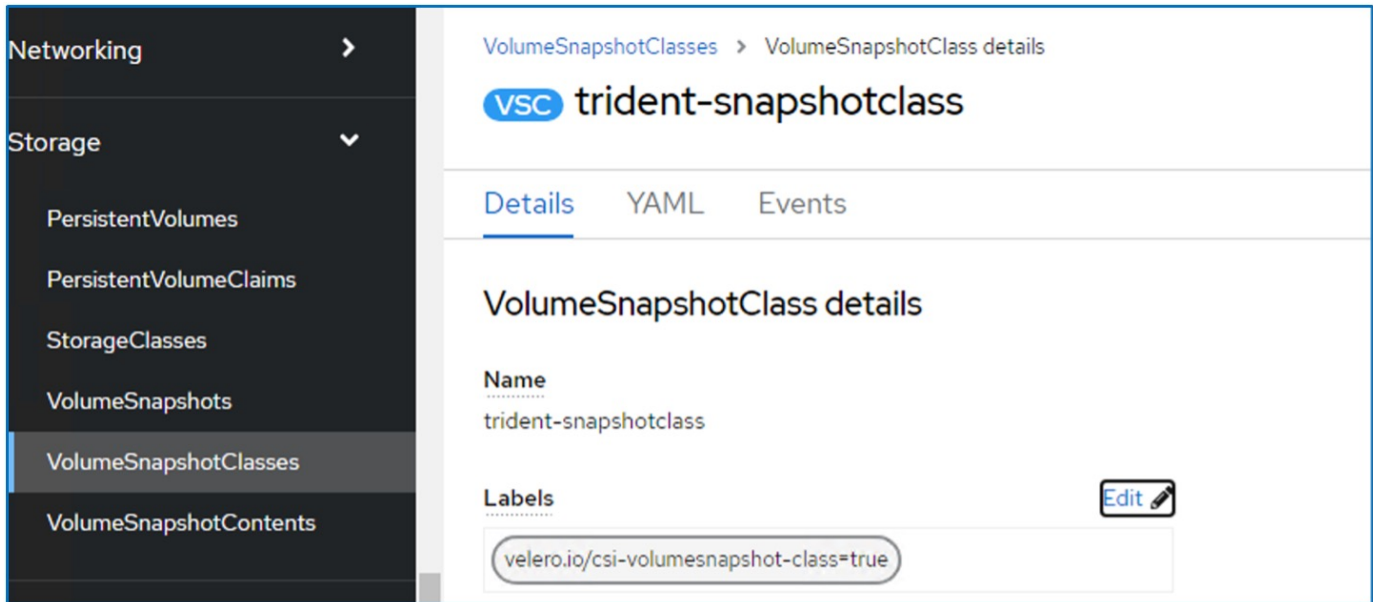
Se si utilizzano gli snapshot Container Storage Interface (CSI), non è necessario specificare una posizione dello snapshot perché si creerà un VolumeSnapshotClass CR per registrare il driver CSI. Nel nostro esempio, si utilizza Astra Trident CSI e in precedenza si è creato VolumeSnapshotClass CR utilizzando 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 PodVolumeRe

## 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-oper...</div> <div>app.kubernetes.io/name=oadp-operator-ve...</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
  ttl: 720h0m0s
```


when Velero is configured.



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](#) [Schedules](#)

---

## 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 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

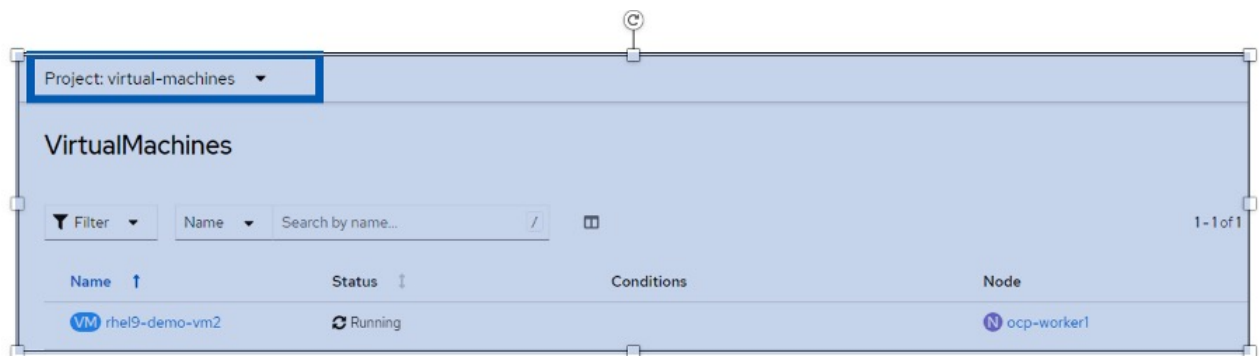
## Ripristinare in un namespace diverso

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.

The screenshot shows the 'VirtualMachine details' page for 'rhel9-demo-vm1' in the 'virtual-machines-demo' project. The 'Configuration' tab is selected, displaying a table of disks. The table has columns: Name, Source, Size, Drive, Interface, and Storage class. There are three disks listed: 'cloudinitdisk' (Source: Other, Size: -, Interface: virtio, Storage class: -), 'disk1' (Source: PVC rhel9-demo-vm1-disk1, Size: 31.75 GiB, Interface: virtio, Storage class: ontap-nas), and 'rootdisk' (Source: PVC rhel9-demo-vm1, Size: 31.75 GiB, Interface: virtio, Storage class: ontap-nas). The 'rootdisk' is marked as 'bootable'.

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	31.75 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	31.75 GiB	Disk	virtio	ontap-nas

The screenshot shows the 'Operator details' page for 'OADP Operator' in the 'openshift-adp' project. The 'Backup' tab is selected, displaying a table of backups. The table has columns: Name, Kind, and Status. There is one backup listed: 'backup1' (Kind: Backup, Status: Phase: Completed). A 'Create Backup' button is visible in the top right corner.

Name	Kind	Status
backup1	Backup	Phase: Completed

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
```

[+ Add key/value](#) [- Remove 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.

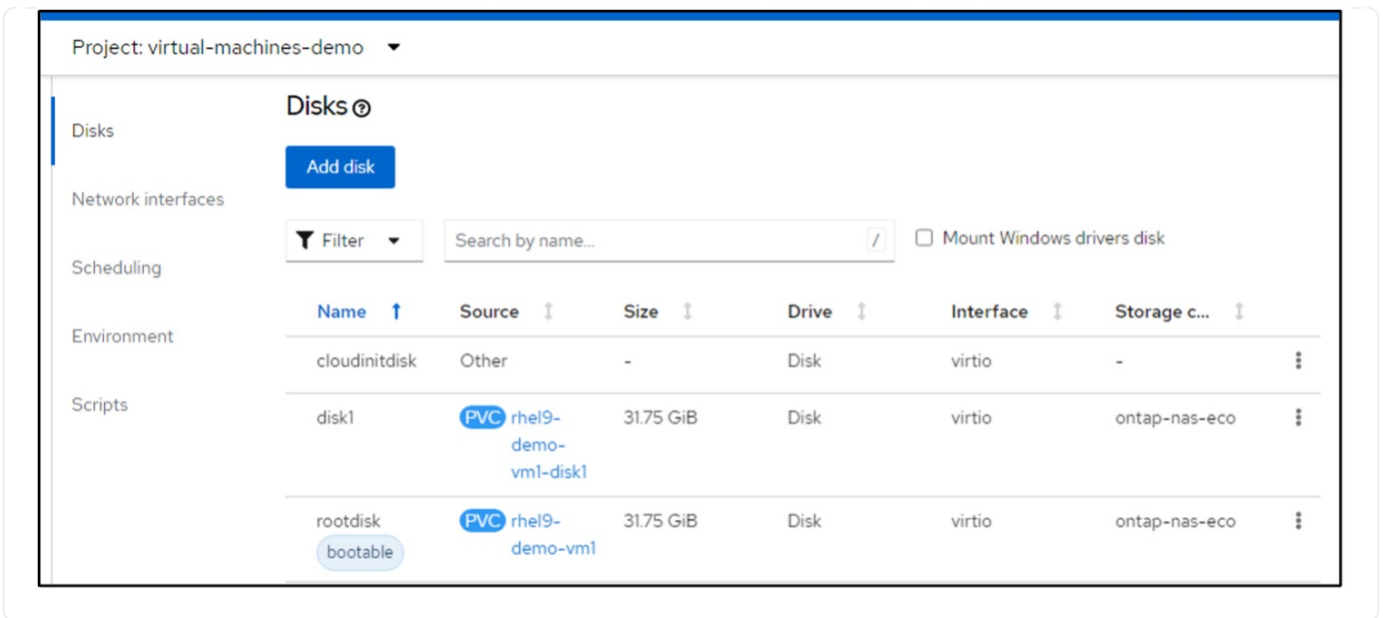
## Passo 2

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 tramite Cloud Insights

## 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 (raccogliatore dati infrastruttura). Le informazioni raccolte vengono utilizzate per l'analisi, la convalida, il monitoraggio e la risoluzione dei problemi.

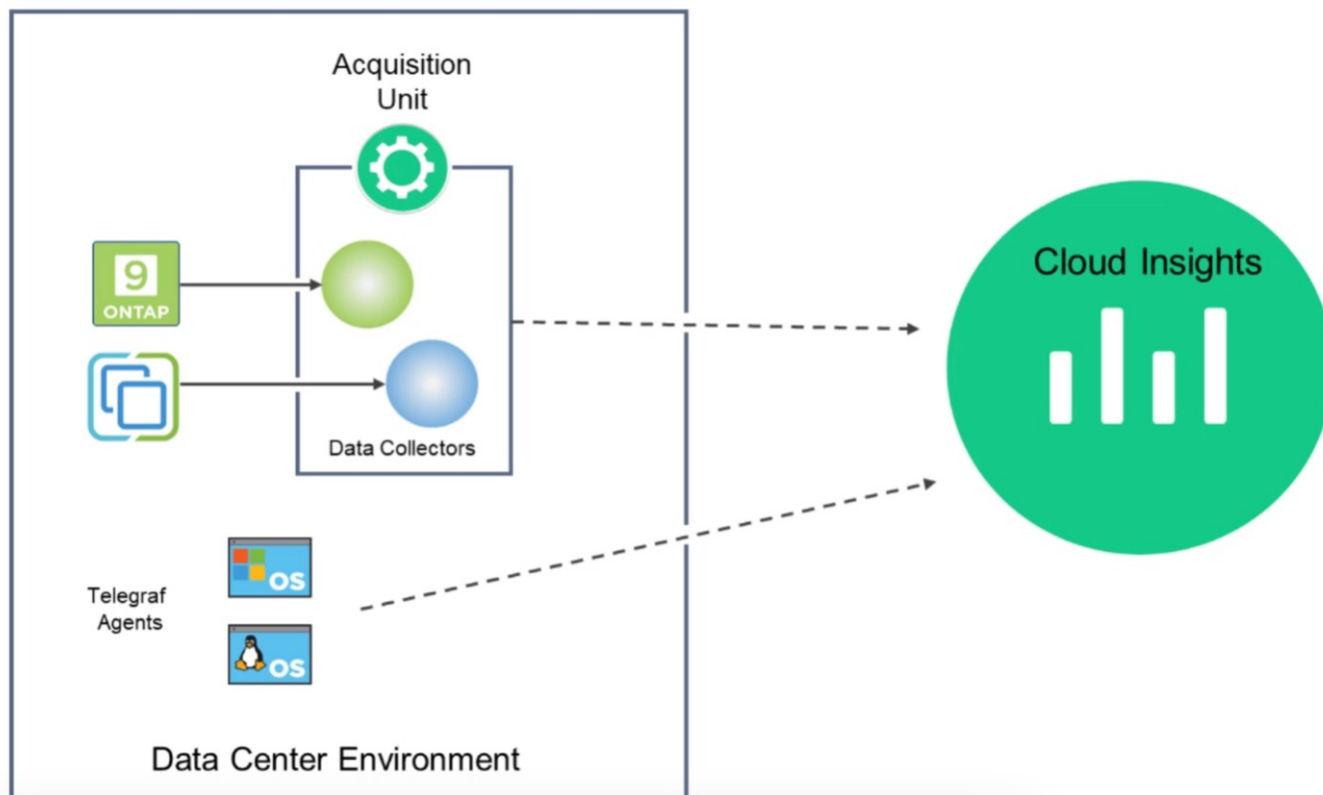
### Unità di acquisizione

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"](#)

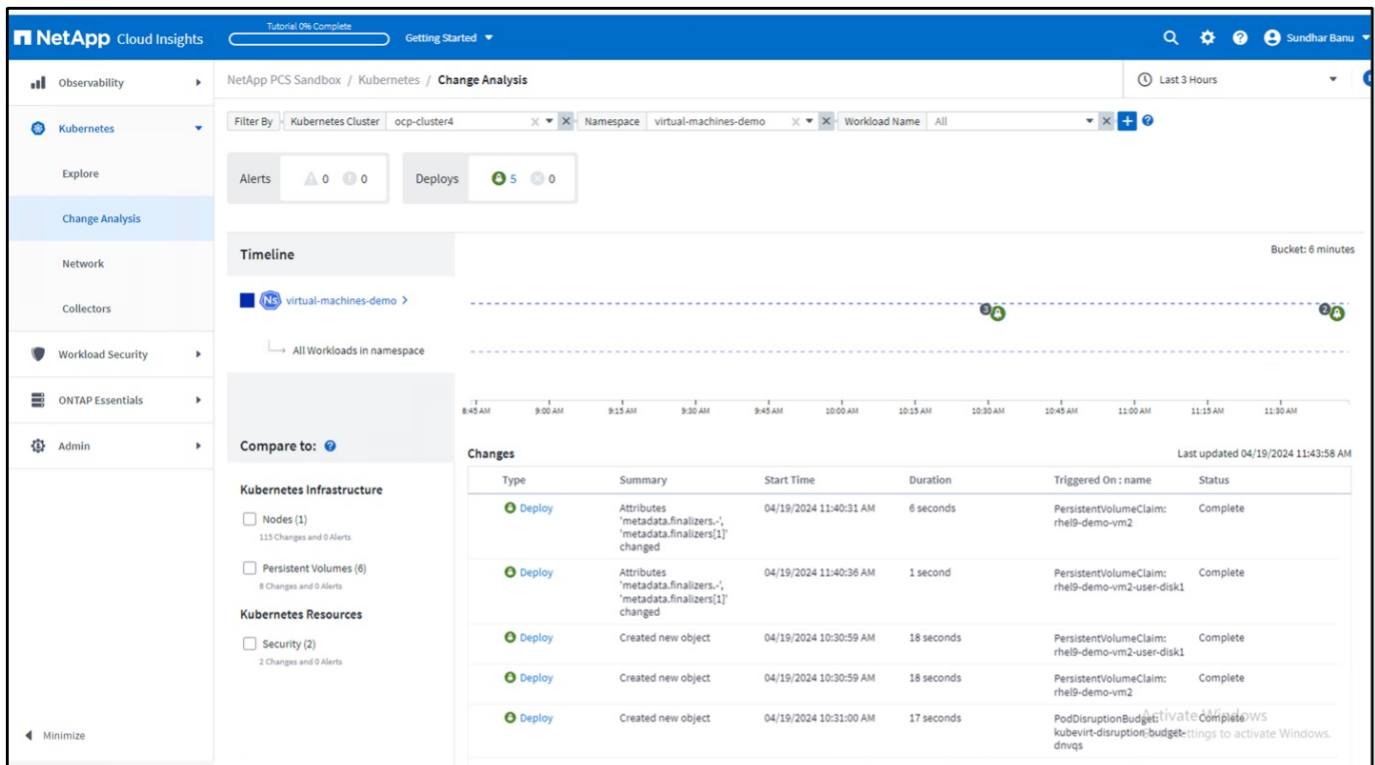
Inoltre, se si utilizza StorageGRID per i backup delle VM, è necessario disporre di un data collector anche per StorageGRID.

## Esempio di funzionalità di monitoraggio per le VM in Red Hat OpenShift Virtualization

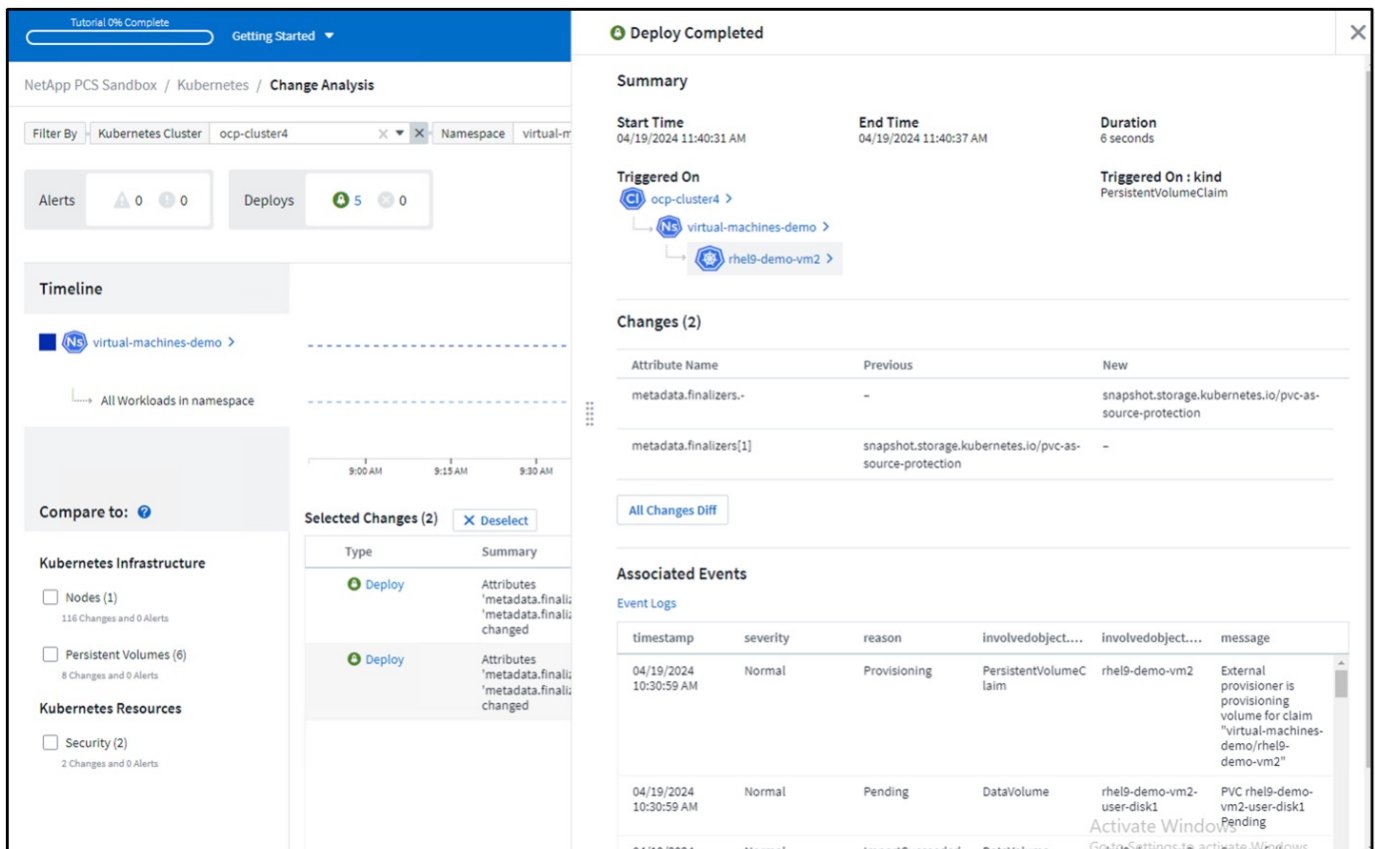
### Monitoraggio basato su eventi e creazione di avvisi

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

Previous

Expand 45 lines ...

46

kind: DataVolume

47

name: rhel9-demo-vm2

48

uid: dcf93b7a-71bc-409b-ad12-4916d05e0980

49

- resourceVersion: "8569671"

50

uid: 953a4188-5932-46ac-85d7-9734acc78278

51

spec:

52

accessModes:

Expand 15 lines ...

New

46

kind: DataVolume

47

name: rhel9-demo-vm2

48

uid: dcf93b7a-71bc-409b-ad12-4916d05e0980

49

+ resourceVersion: "8619670"

50

uid: 953a4188-5932-46ac-85d7-9734acc78278

51

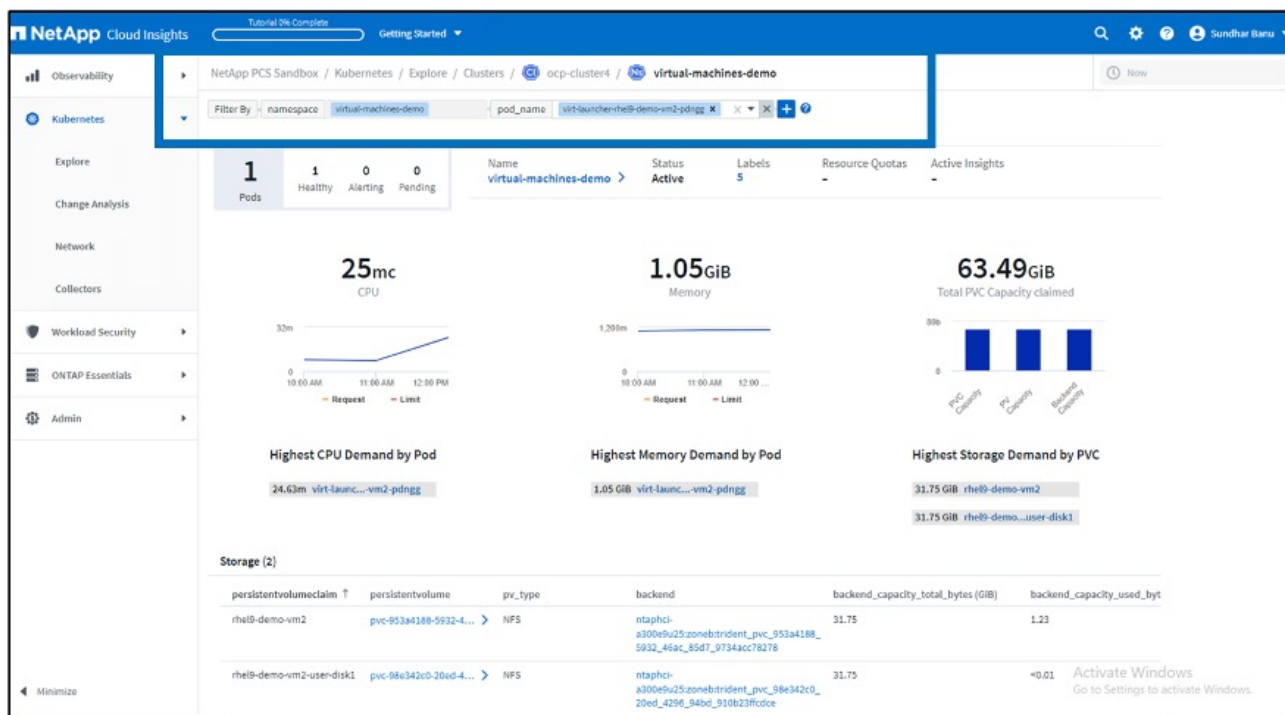
spec:

52

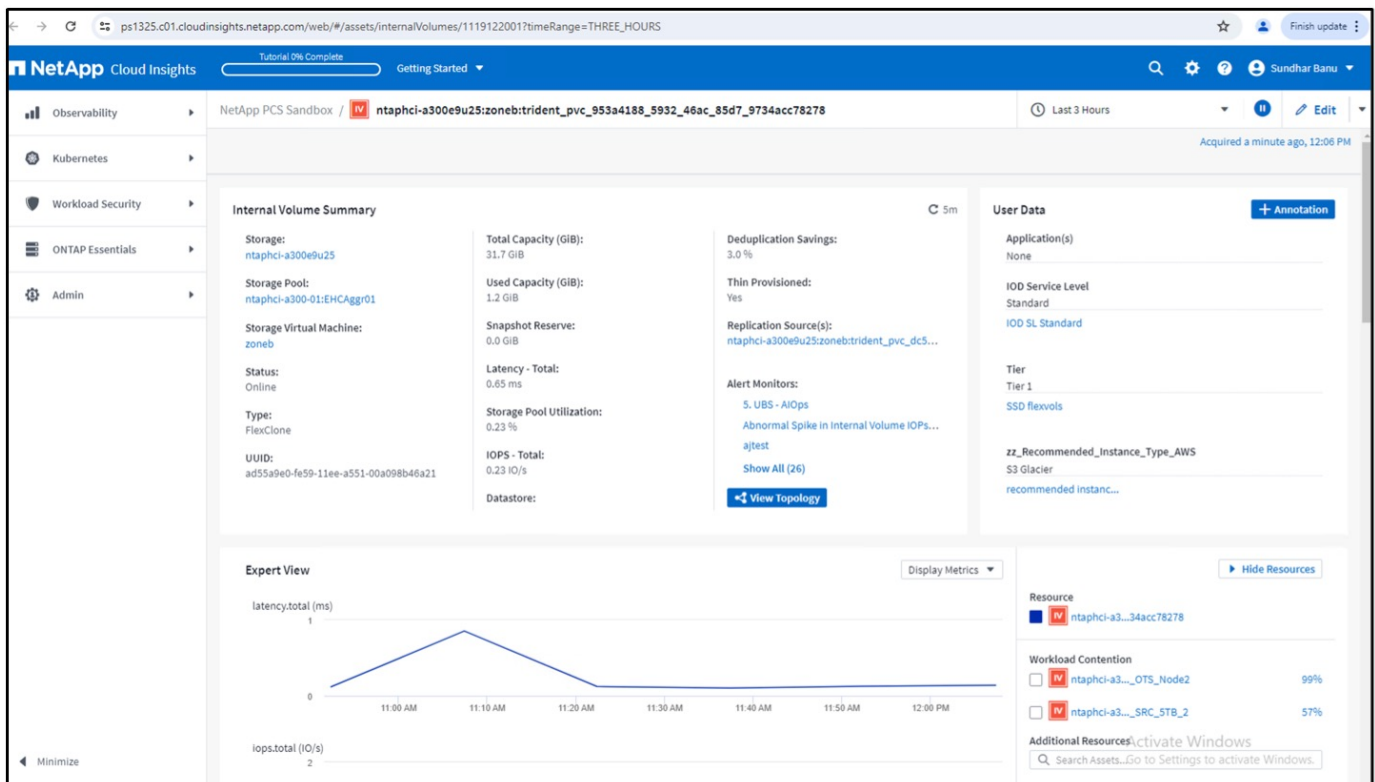
accessModes:

## Mappatura archiviazione backend

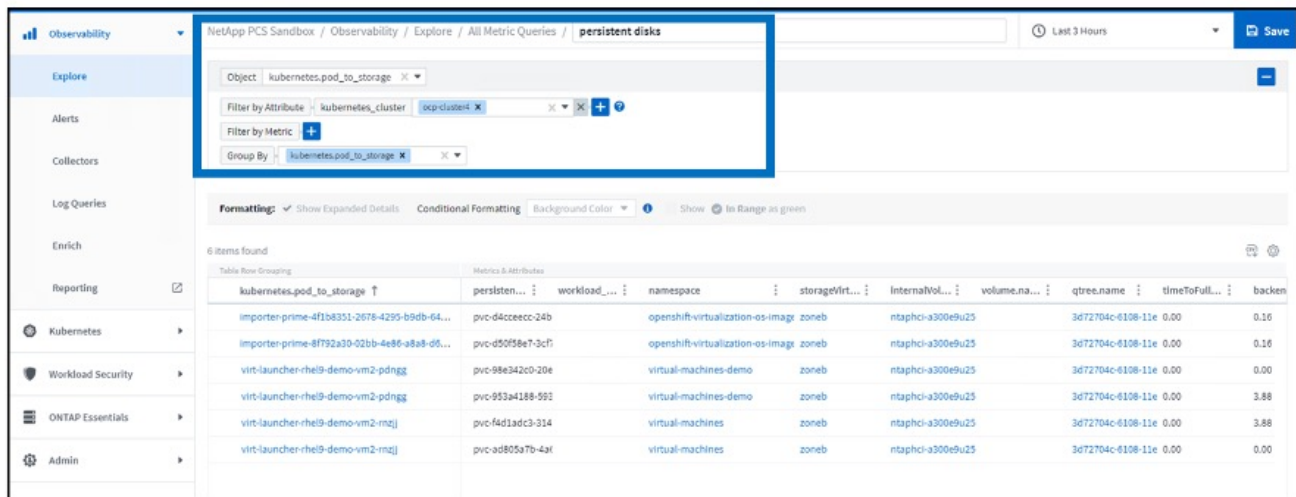
Con Cloud Insights, è possibile vedere facilmente lo storage backend dei dischi della macchina virtuale e le diverse statistiche sui PVC.



È possibile fare clic sui link presenti nella colonna backend per estrarre i dati direttamente dallo storage ONTAP back-end.



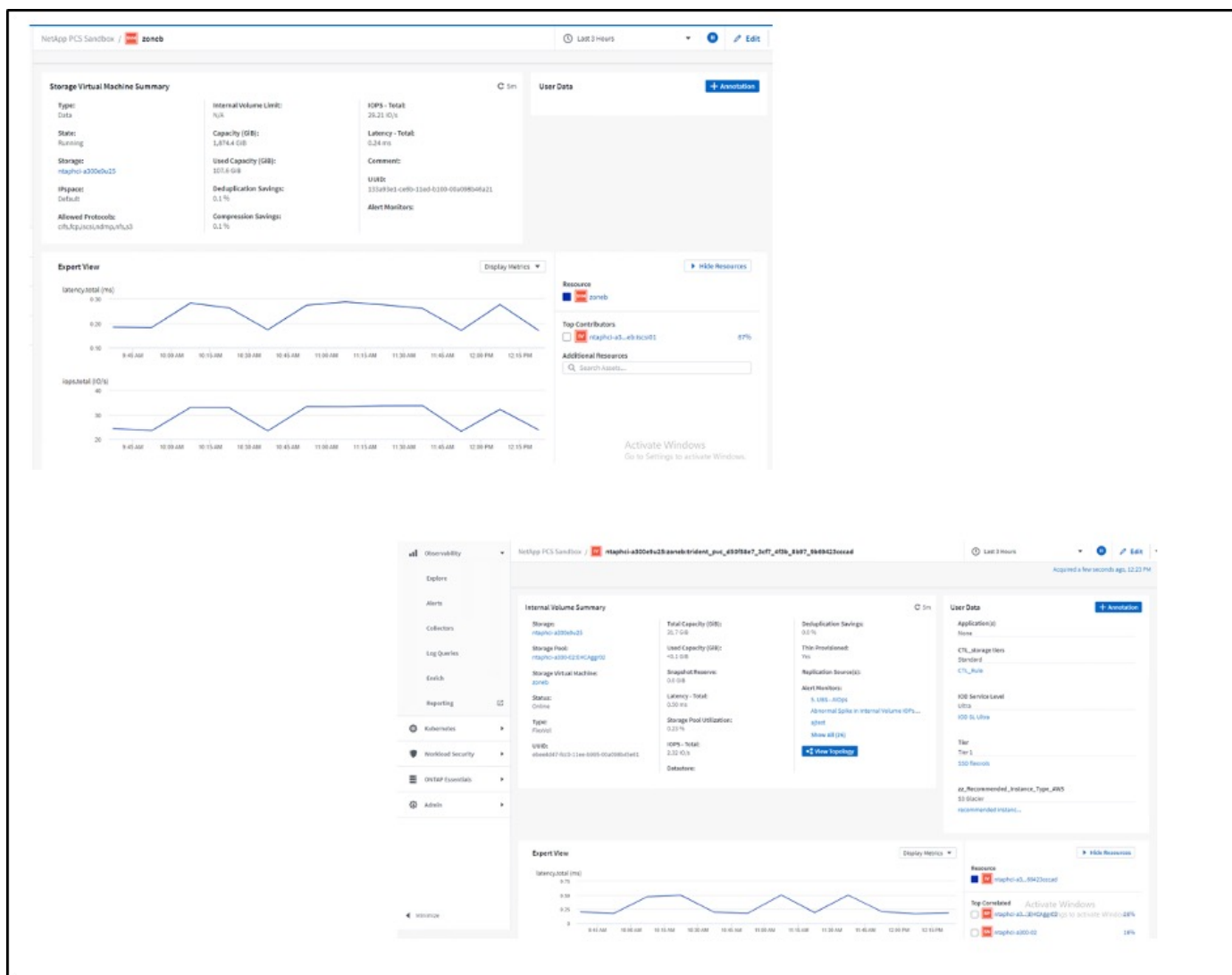
Un altro modo per esaminare tutte le mappature pod-storage è creare una query All Metrics dal menu Observability (osservabilità) in Explore (Esplora).



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





## 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.