Convalida della soluzione e casi di utilizzo

NetApp Solutions

NetApp
April 26, 2024

Sommario

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"

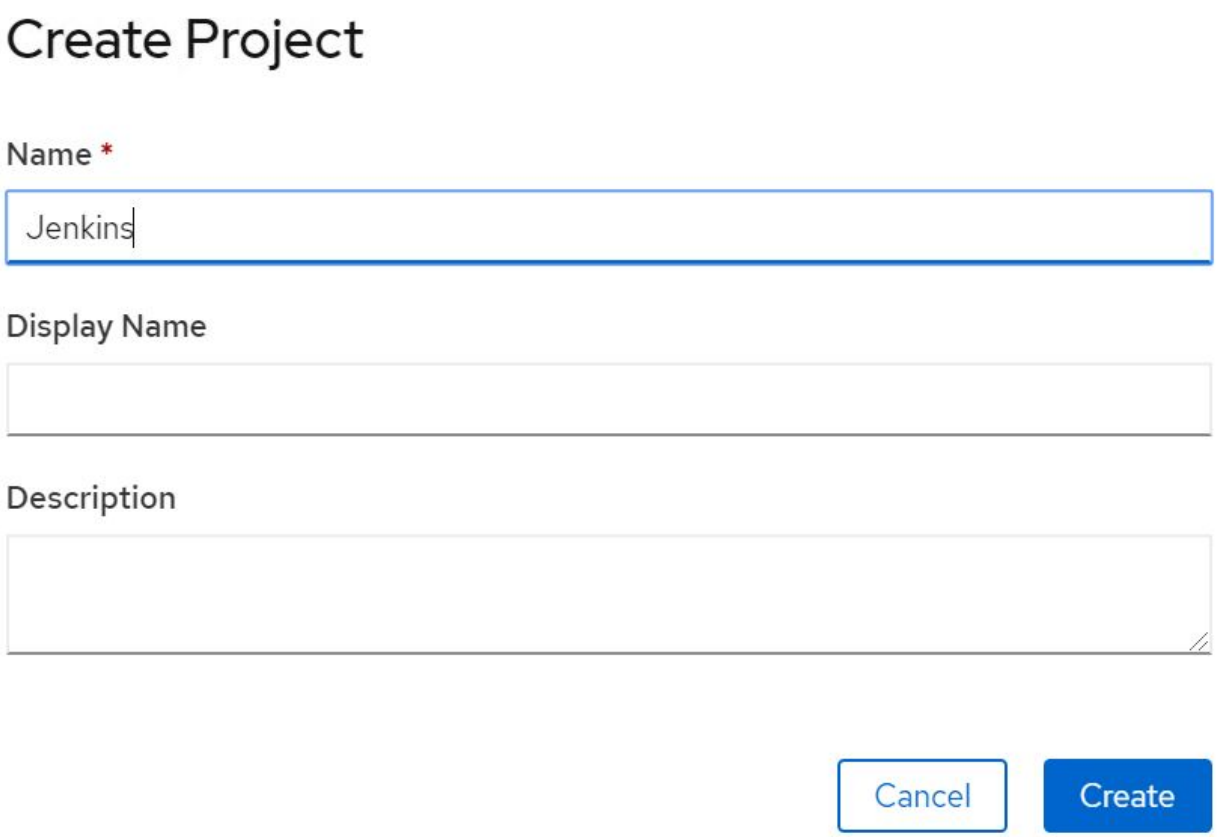
Implementa una pipeline ci/CD Jenkins con storage persistente: Red Hat OpenShift con NetApp

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.



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).

Project: jenkins

Create Persistent Volume Claim

Edit YAML

Storage Class

SC 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

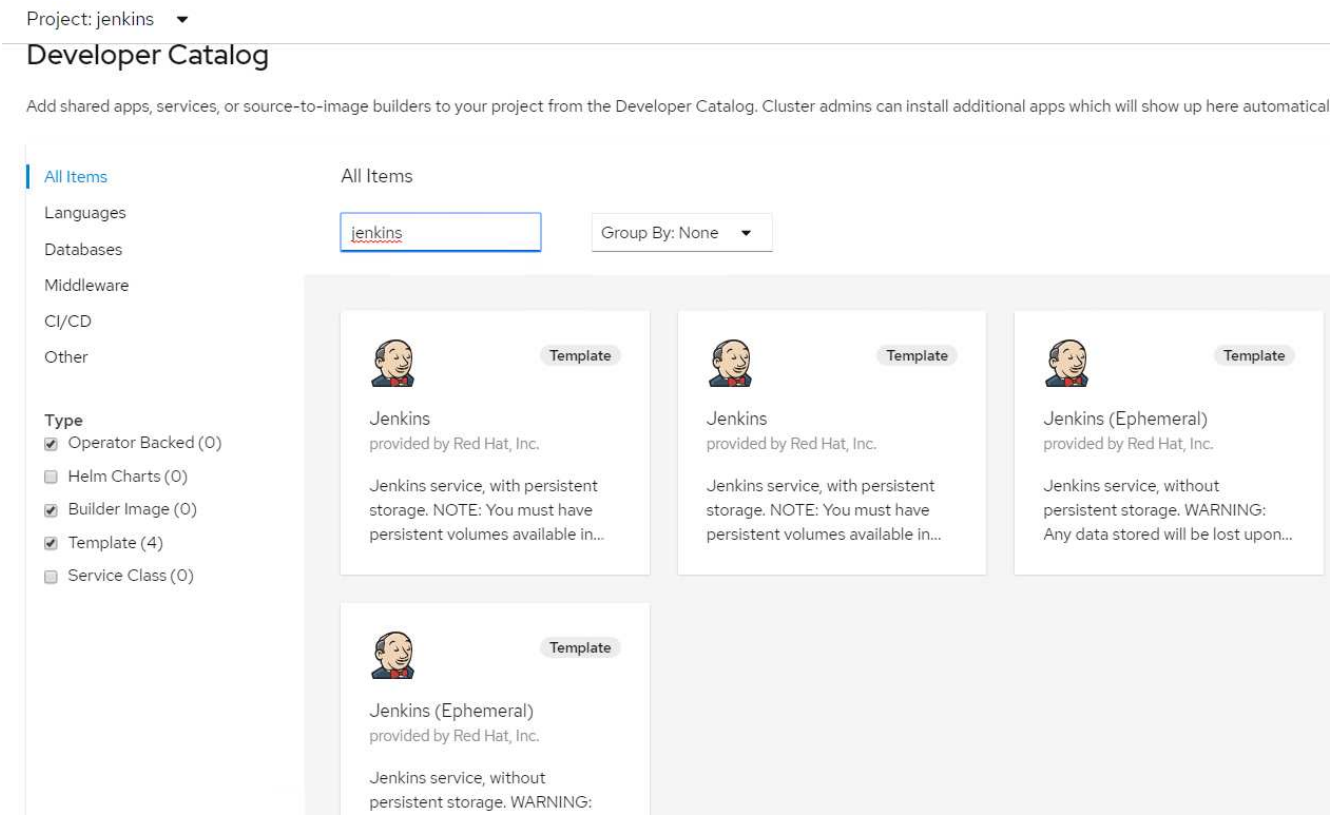
Use label selectors to define how storage is created.

Create Cancel

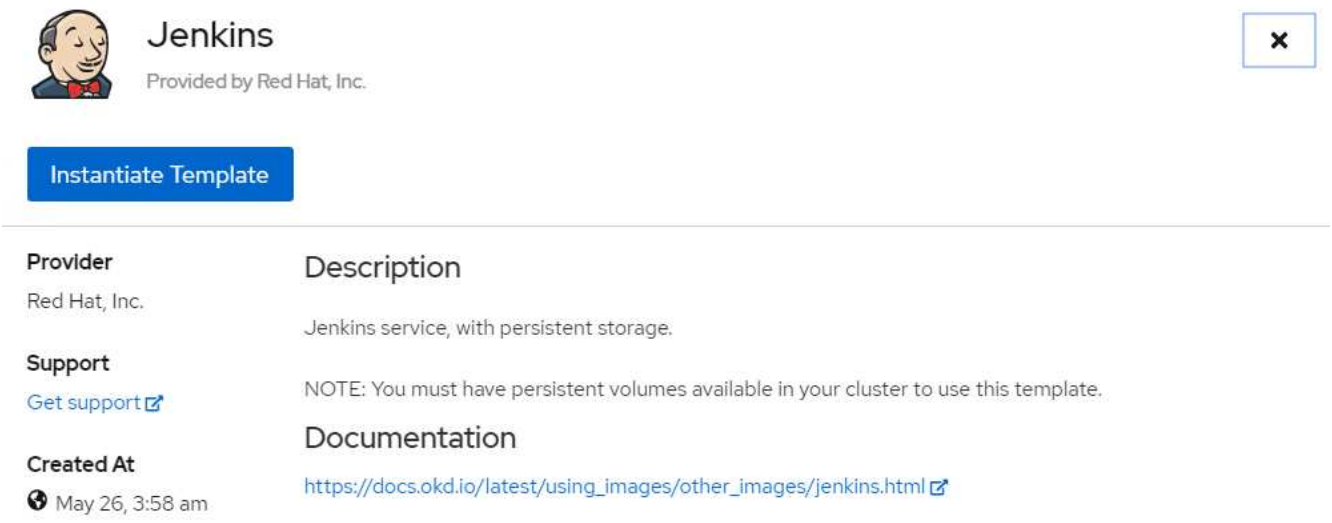
Implementare Jenkins con lo storage persistente

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.

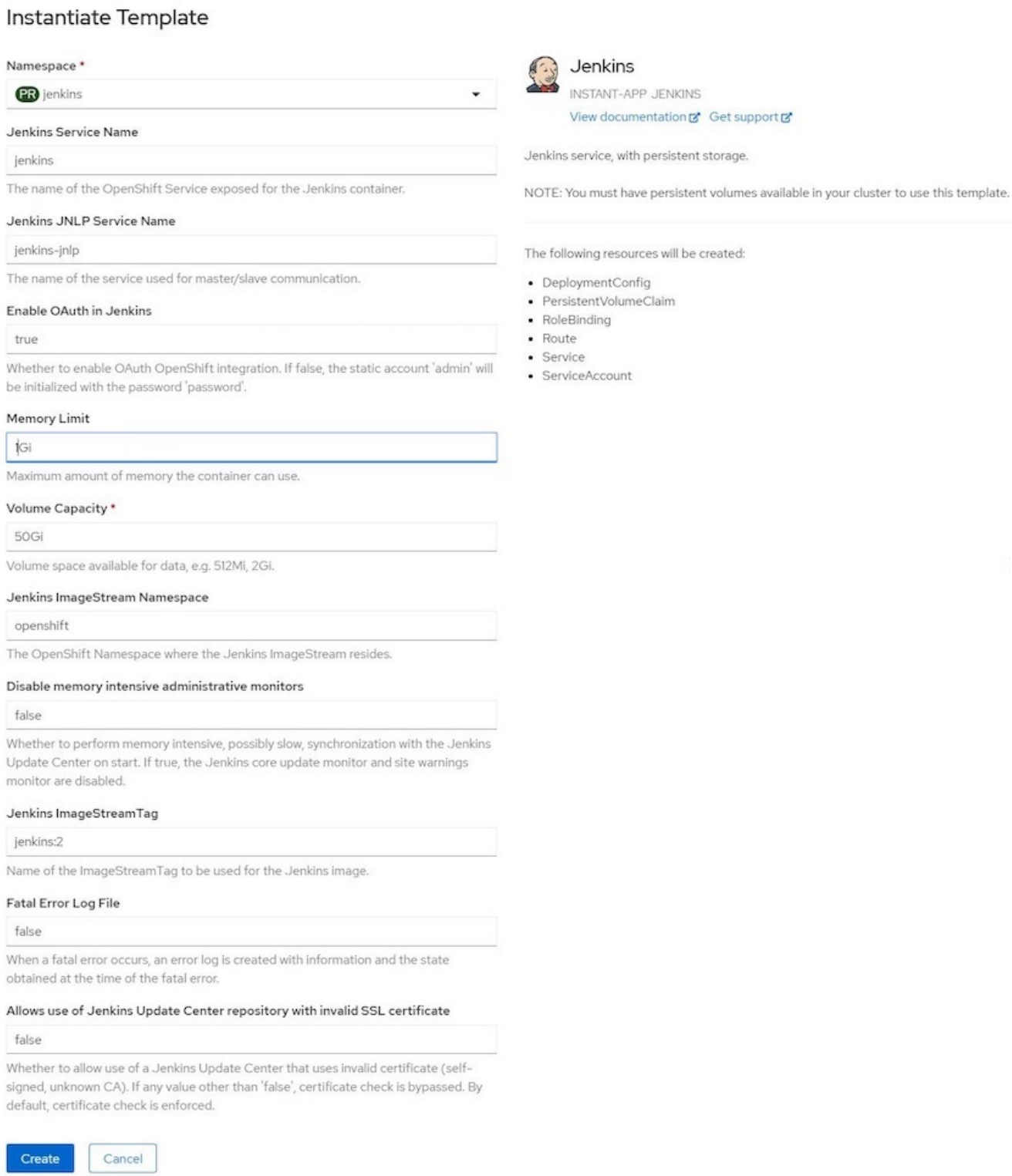


2. Fare clic su `Instantiate Template`.



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.



4. I pod Jenkins impiegano circa 10 - 12 minuti per entrare nello stato Pronta.

Project: jenkins

Pods

Create Pod

Filter by name...

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
P jenkins-1-c77n9	NS jenkins	Running	1/1	RC 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.

Project: jenkins

Routes

Create Route

Filter by name...

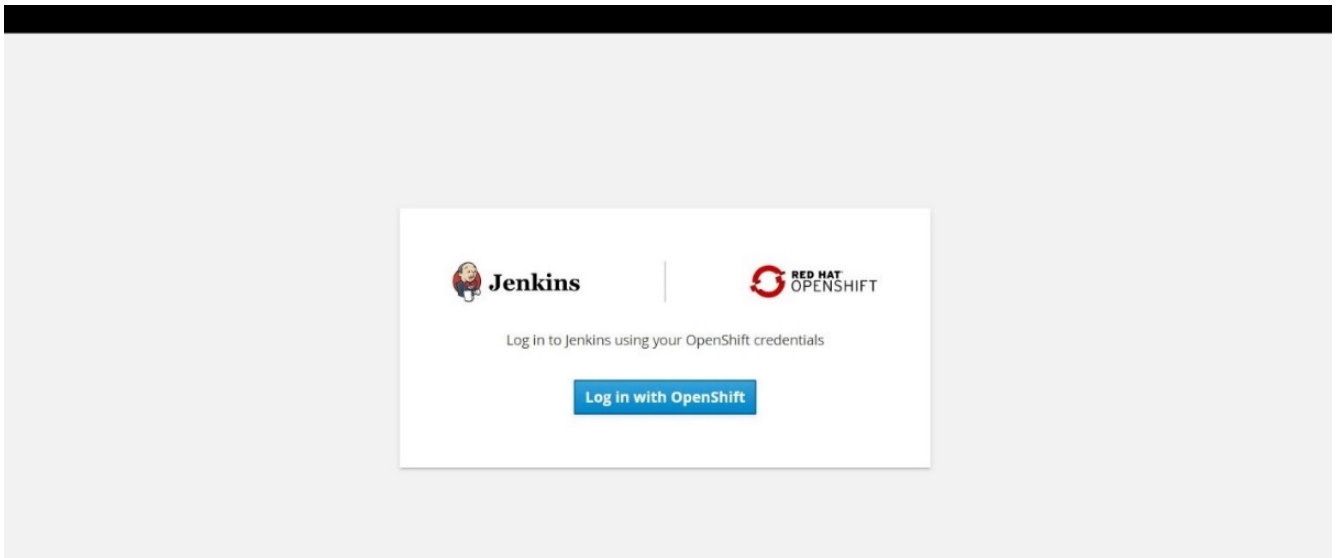
1 Accepted | 0 Rejected | 0 Pending

Select all filters

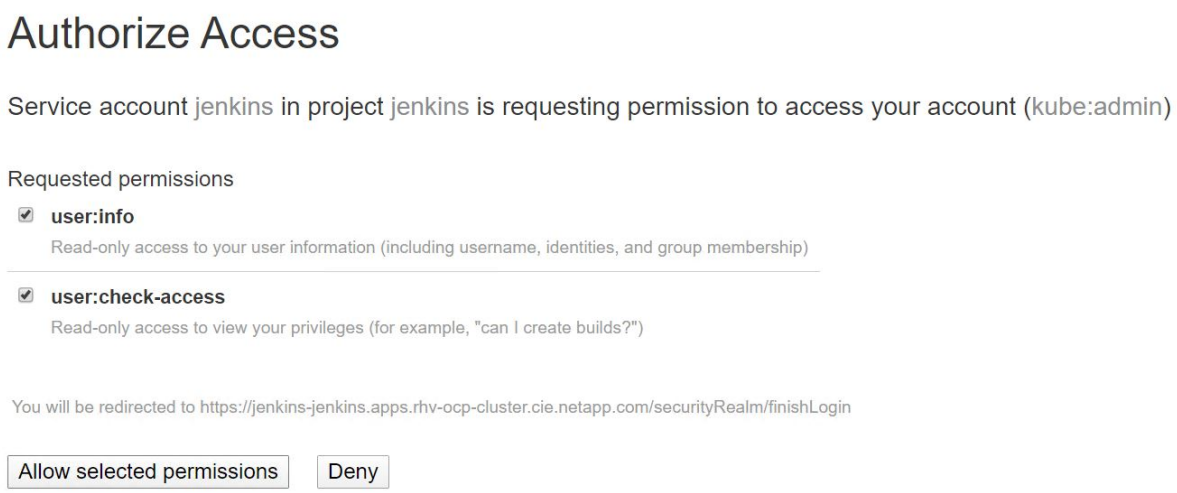
1 Item

Name	Namespace	Status	Location	Service
RT jenkins	NS jenkins	Accepted	https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com	S jenkins

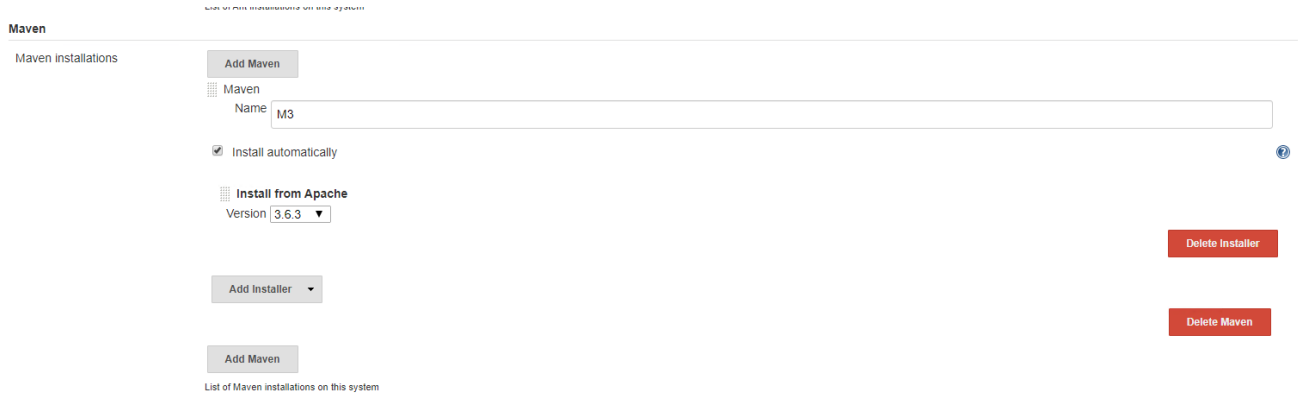
6. Poiché OpenShift OAuth è stato utilizzato durante la creazione dell'applicazione Jenkins, fare clic su Accedi con OpenShift.



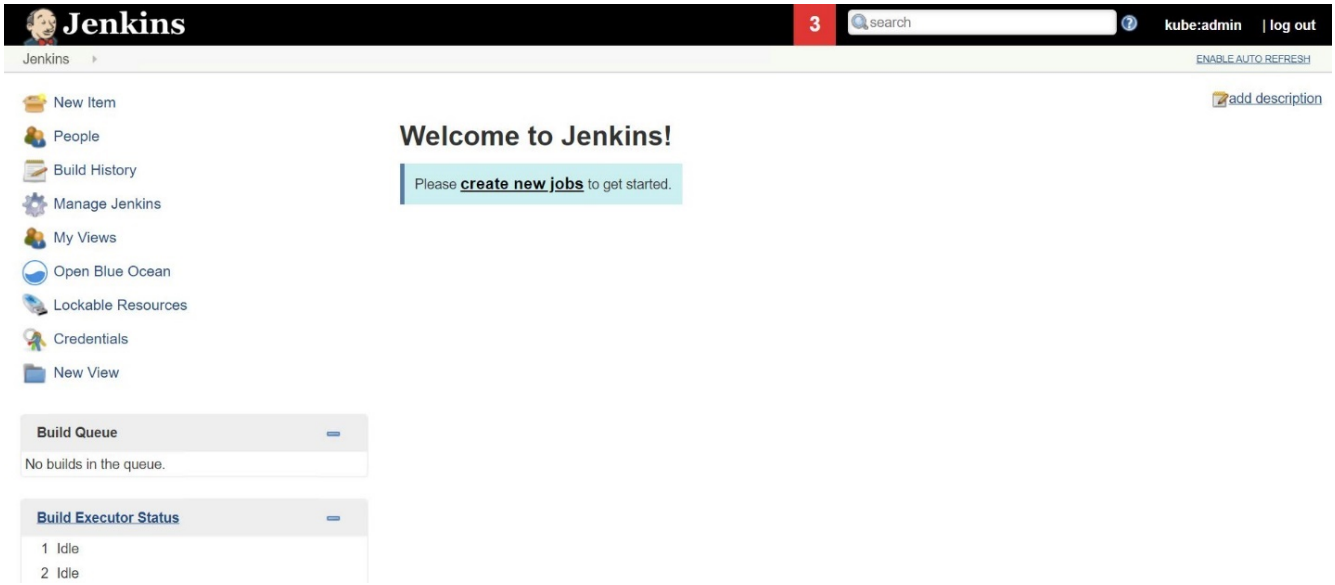
7. Autorizzare l’account del servizio Jenkins ad accedere agli utenti OpenShift.



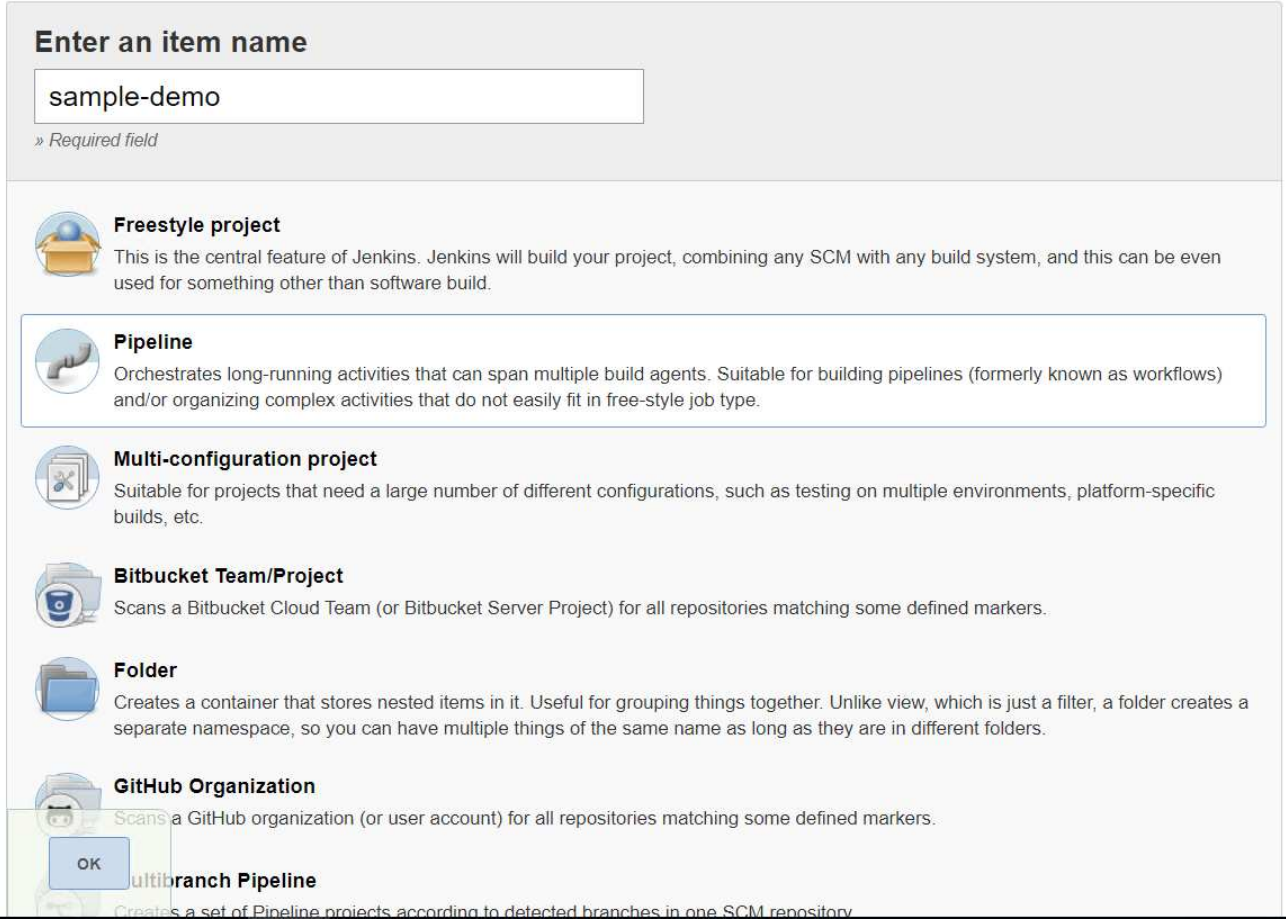
8. Viene visualizzata la pagina di benvenuto di Jenkins. Poiché stiamo utilizzando una build Maven, completare prima l’installazione di Maven. Accedere a Manage Jenkins > Global Tool Configuration (Gestisci Jenkins > Configurazione globale strumenti), quindi fare clic su Add Maven (Aggiungi Maven) nella sottotesta di Maven. Immettere il nome desiderato e assicurarsi che l’opzione Installa automaticamente sia selezionata. Fare clic su Salva.



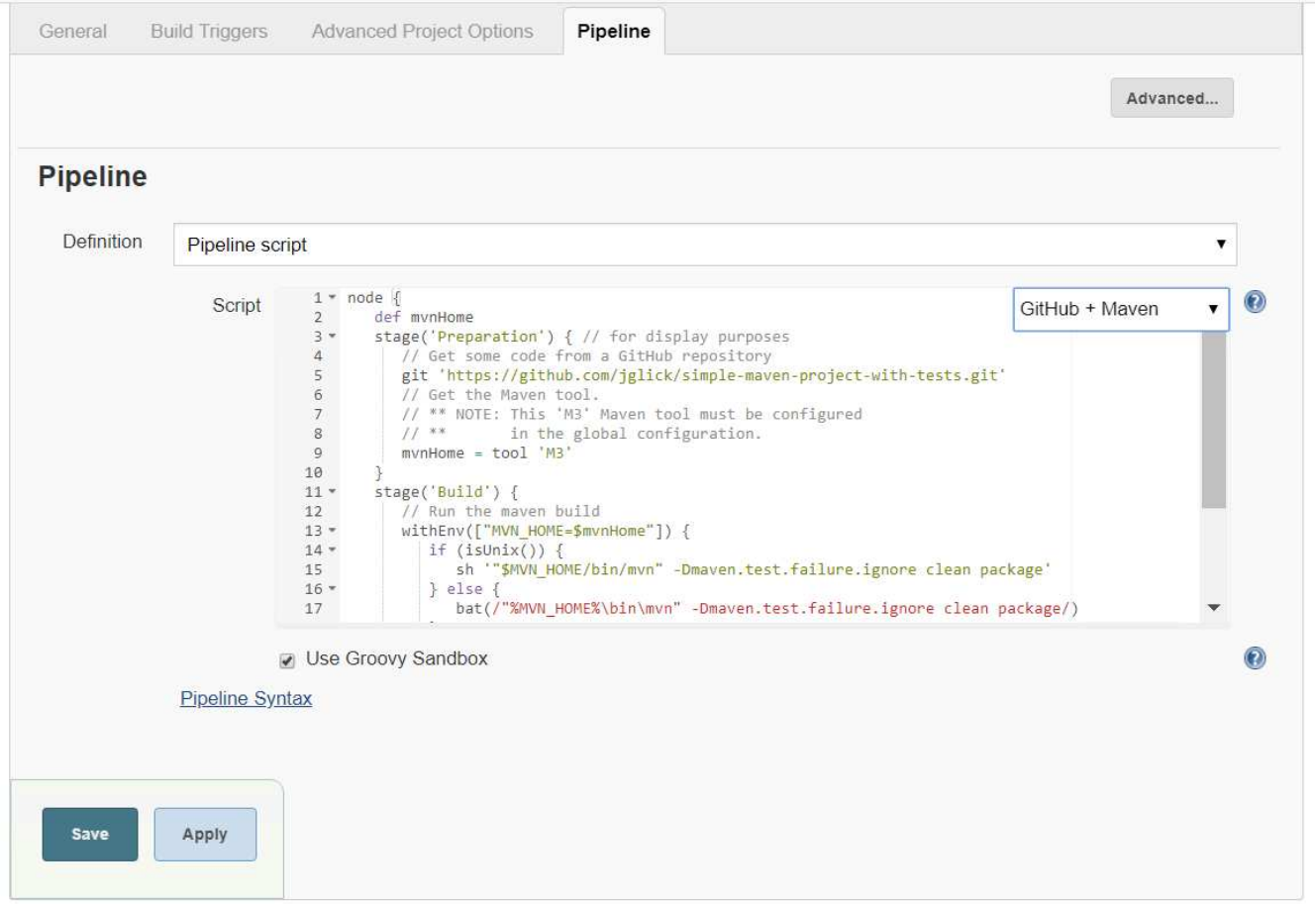
9. È ora possibile creare una pipeline per dimostrare il flusso di lavoro ci/CD. Nella home page, fare clic su Create New Jobs (Crea nuovi lavori) o New Item (nuovo elemento) dal menu a sinistra.



10. Nella pagina Create Item (Crea elemento), immettere il nome desiderato, selezionare Pipeline e fare clic su OK.



11. Selezionare la scheda pipeline. Dal menu a discesa Try Sample Pipeline, selezionare Github + Maven. Il codice viene compilato automaticamente. Fare clic su Salva.



12. 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.

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.

Configura la multi-tenancy su Red Hat OpenShift con NetApp ONTAP

Configurazione della multi-tenancy su Red Hat OpenShift con NetApp

Molte organizzazioni che eseguono più applicazioni o carichi di lavoro su container tendono a implementare un cluster Red Hat OpenShift per applicazione o carico di lavoro. Ciò consente loro di implementare un rigoroso isolamento per l'applicazione o il carico di lavoro, ottimizzare le performance e ridurre le vulnerabilità della sicurezza. Tuttavia, l'implementazione di un cluster Red Hat OpenShift separato per ciascuna applicazione pone un proprio insieme di problemi. Aumenta l'overhead operativo dovendo monitorare e gestire ciascun cluster da solo, aumenta i costi grazie alle risorse dedicate per le diverse applicazioni e ostacola l'efficienza della scalabilità.

Per risolvere questi problemi, si può prendere in considerazione l'esecuzione di tutte le applicazioni o i carichi di lavoro in un singolo cluster Red Hat OpenShift. Tuttavia, in un'architettura di questo tipo, le vulnerabilità legate all'isolamento delle risorse e alla sicurezza delle applicazioni sono una delle sfide principali. Qualsiasi vulnerabilità di sicurezza in un workload potrebbe naturalmente ricadersi in un altro workload, aumentando così la zona di impatto. Inoltre, qualsiasi utilizzo improvviso e non controllato delle risorse da parte di un'applicazione può influire sulle prestazioni di un'altra applicazione, poiché non esiste un criterio di allocazione delle risorse per impostazione predefinita.

Pertanto, le organizzazioni cercano soluzioni in grado di ottenere il meglio in entrambi i mondi, ad esempio, consentendo loro di eseguire tutti i propri carichi di lavoro in un singolo cluster e offrendo al contempo i vantaggi di un cluster dedicato per ogni carico di lavoro.

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

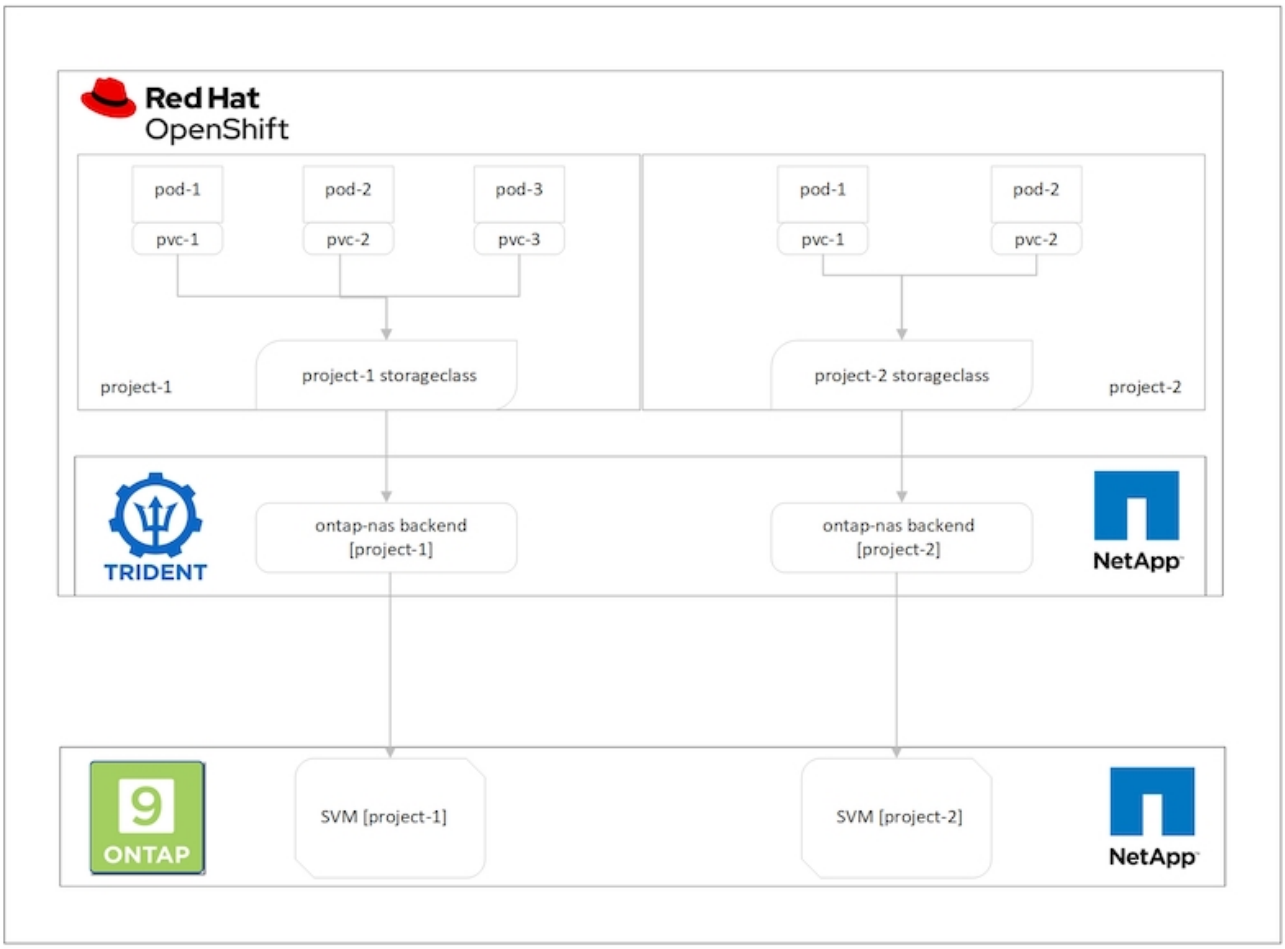
Per un cluster OpenShift multitenant completamente realizzato, è necessario configurare le quote e le restrizioni per le risorse cluster appartenenti a diversi bucket di risorse: Calcolo, storage, networking, sicurezza e così via. Anche se vengono trattati alcuni aspetti di tutti i bucket di risorse 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
Cluster-admin	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
Storage-admin	Creare SVM su NetApp ONTAP
	Creare backend Trident
	Creare StorageClasses
	Creare ResourceQuotas di storage
Sviluppatori	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:
      - tridentsnapshots
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.

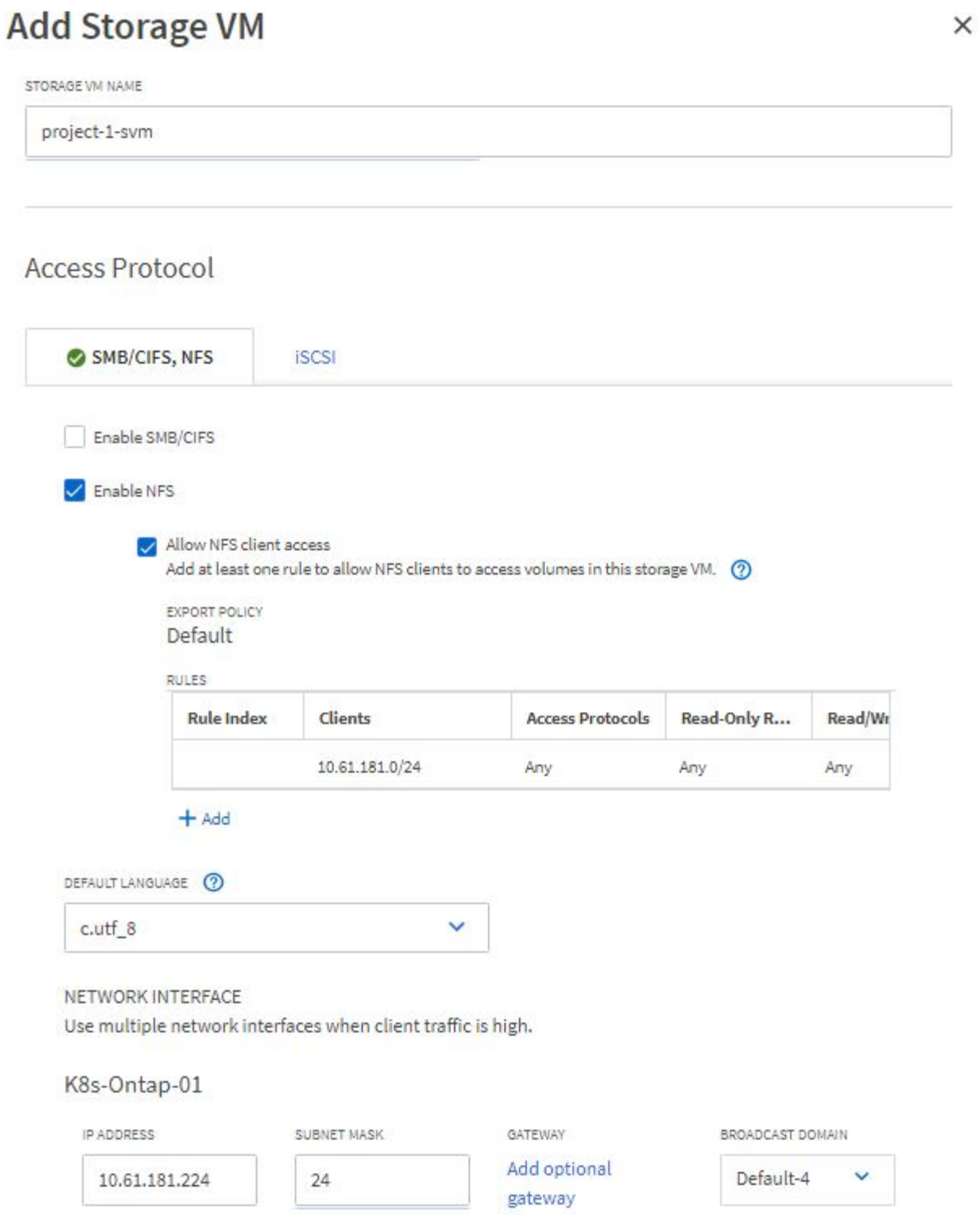
```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  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.



1. Accedere al cluster Red Hat OpenShift come amministratore dello storage.
2. Creare il backend per il progetto 1 e mapparlo 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 mapparlo 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
```

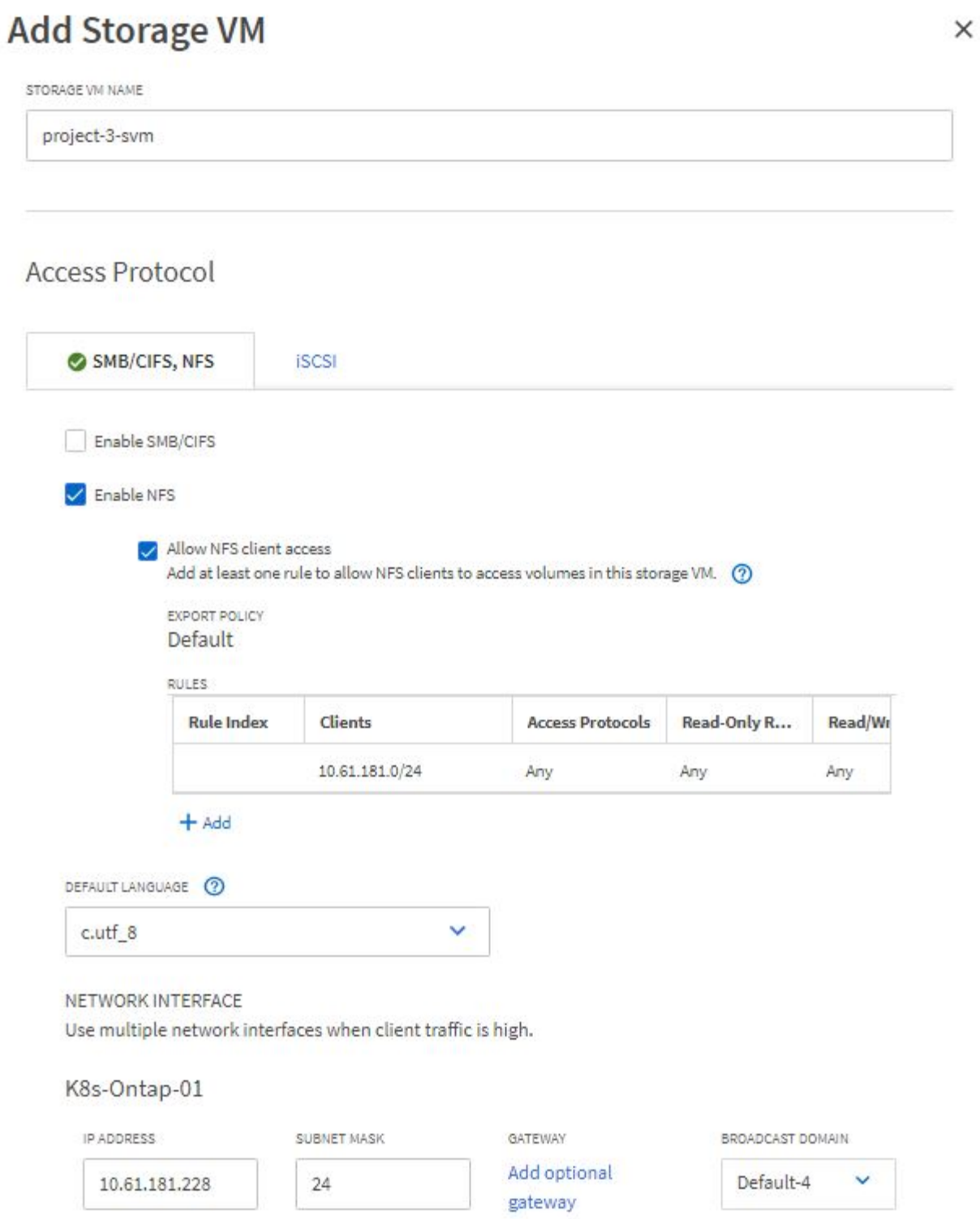
6. Controllare l'accesso per descrivere i magazzini.
7. Convalidare l'accesso dell'utente per modificare gli storageclasses.

```
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.



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:
      - tridentsnapshots
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.

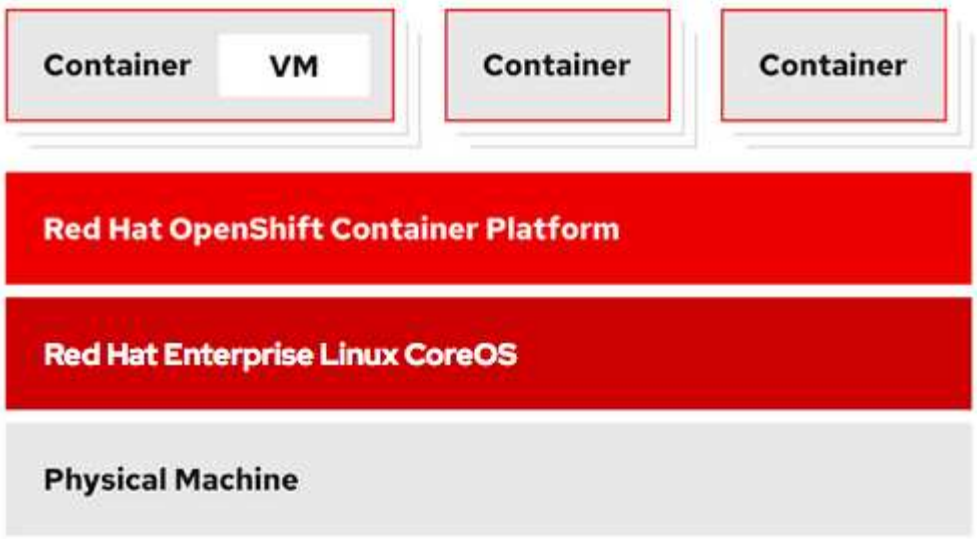
```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 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

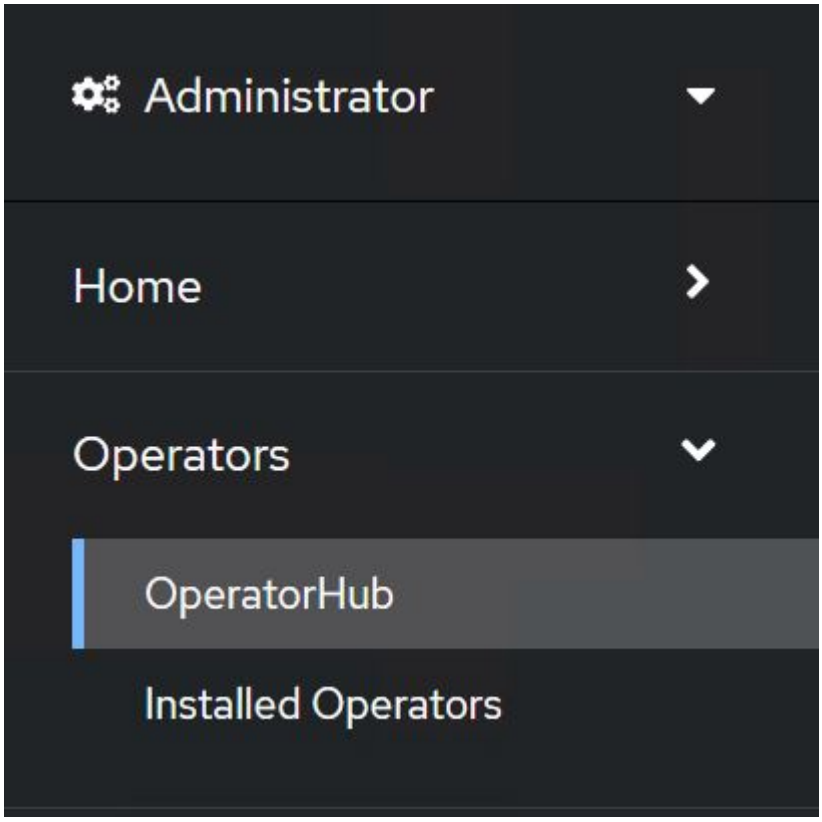
documentazione "qui".

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.

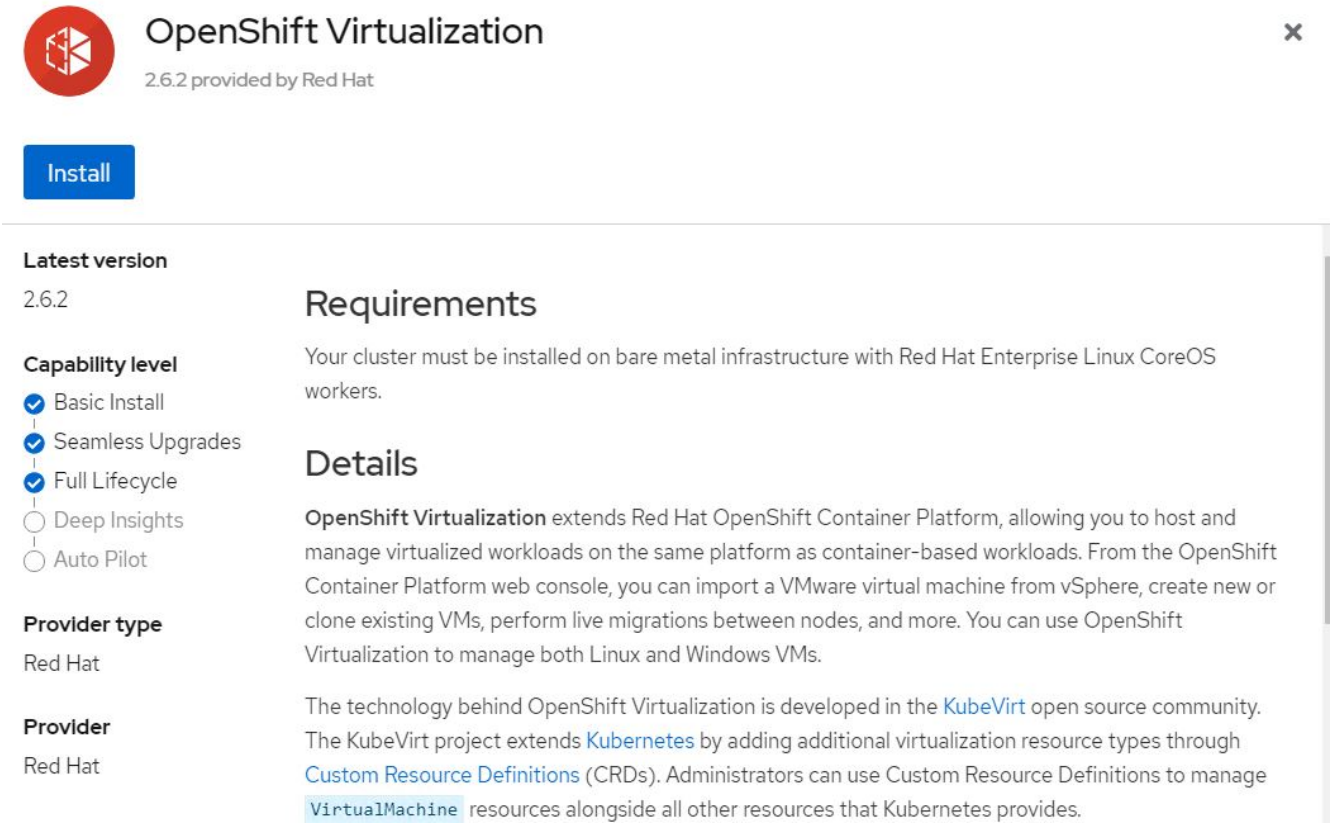
Implementa la virtualizzazione di Red Hat OpenShift con NetApp ONTAP

Per installare OpenShift Virtualization, attenersi alla seguente procedura:

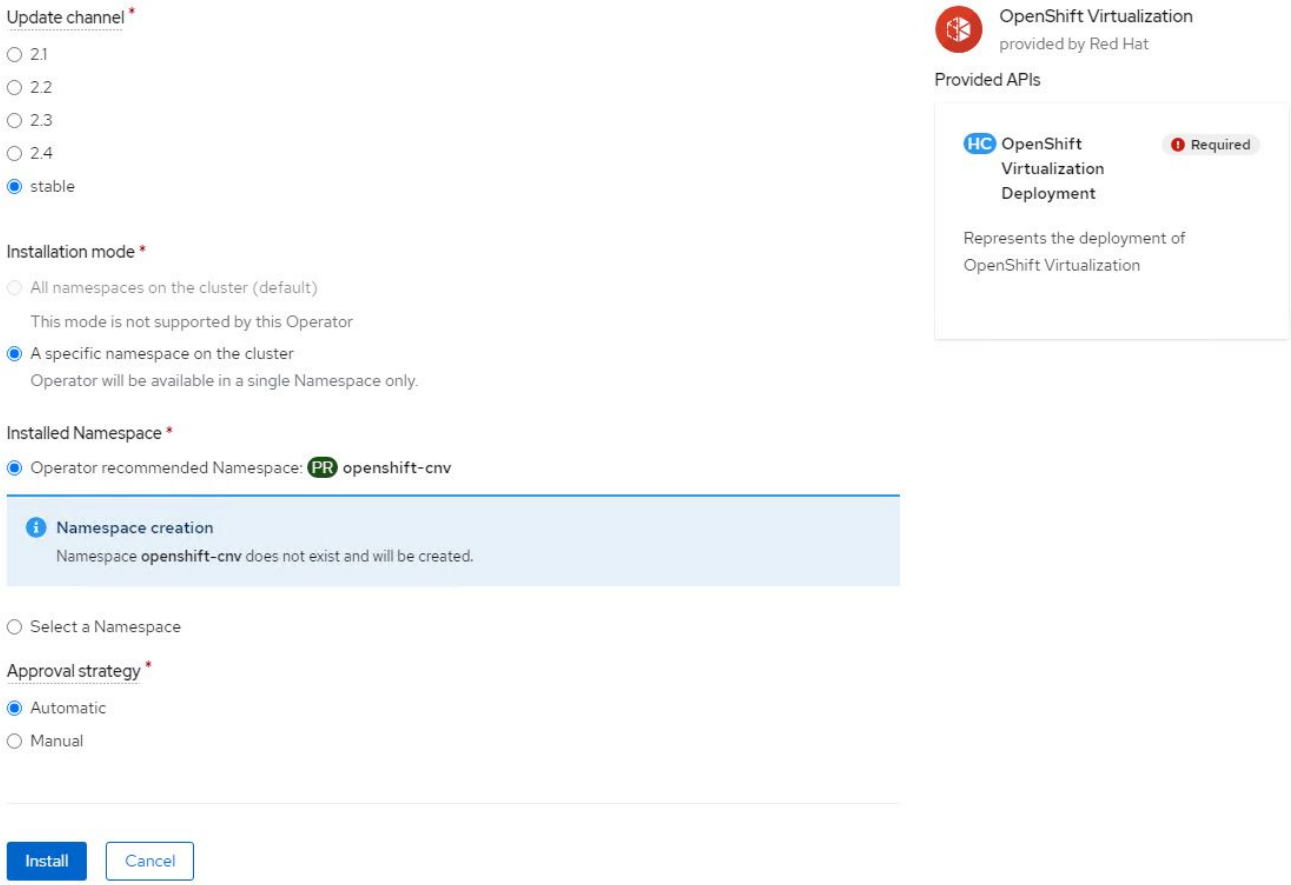
1. Accedi al cluster bare-metal Red Hat OpenShift con accesso cluster-admin.
2. Selezionare Administrator (Amministratore) dal menu a discesa Perspective (prospettiva).
3. Accedere a Operator > OperatorHub e cercare OpenShift Virtualization.



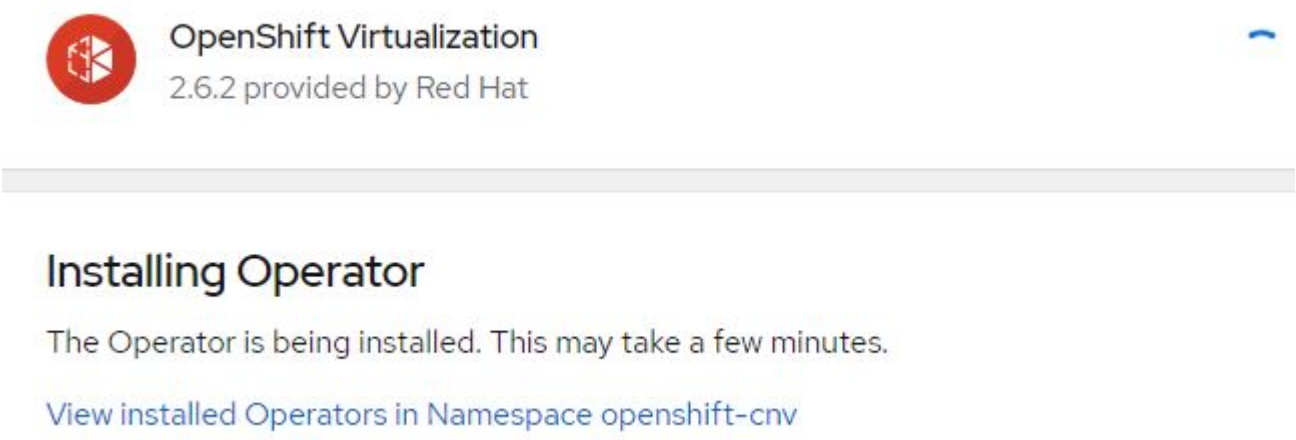
4. Selezionare il riquadro OpenShift Virtualization (virtualizzazione OpenShift) e fare clic su Install (Installa)



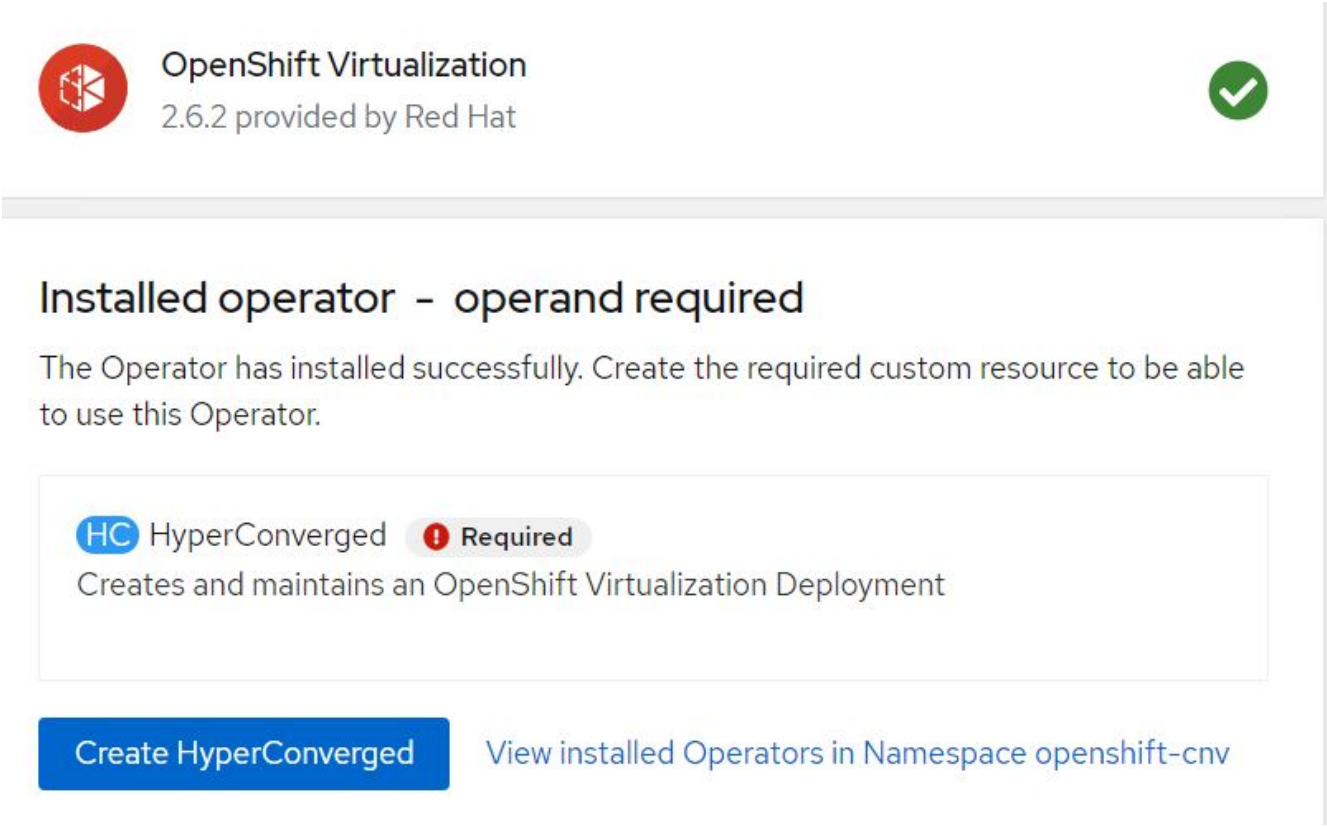
5. Nella schermata Install Operator (Installa operatore), lasciare tutti i parametri predefiniti e fare clic su Install (Installa).



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



7. Una volta installato l'operatore, fare clic su Create HyperConverged (Crea HyperConverged).



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 necessarely directly on each node running VMs/VMIs.

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	Last updated	Provided APIs
OpenShift Virtualization 2.6.2 provided by Red Hat	NS openshift-cnv	Succeeded Up to date	May 18, 8:02 pm	OpenShift Virtualization Deployment HostPathProvisioner deployment

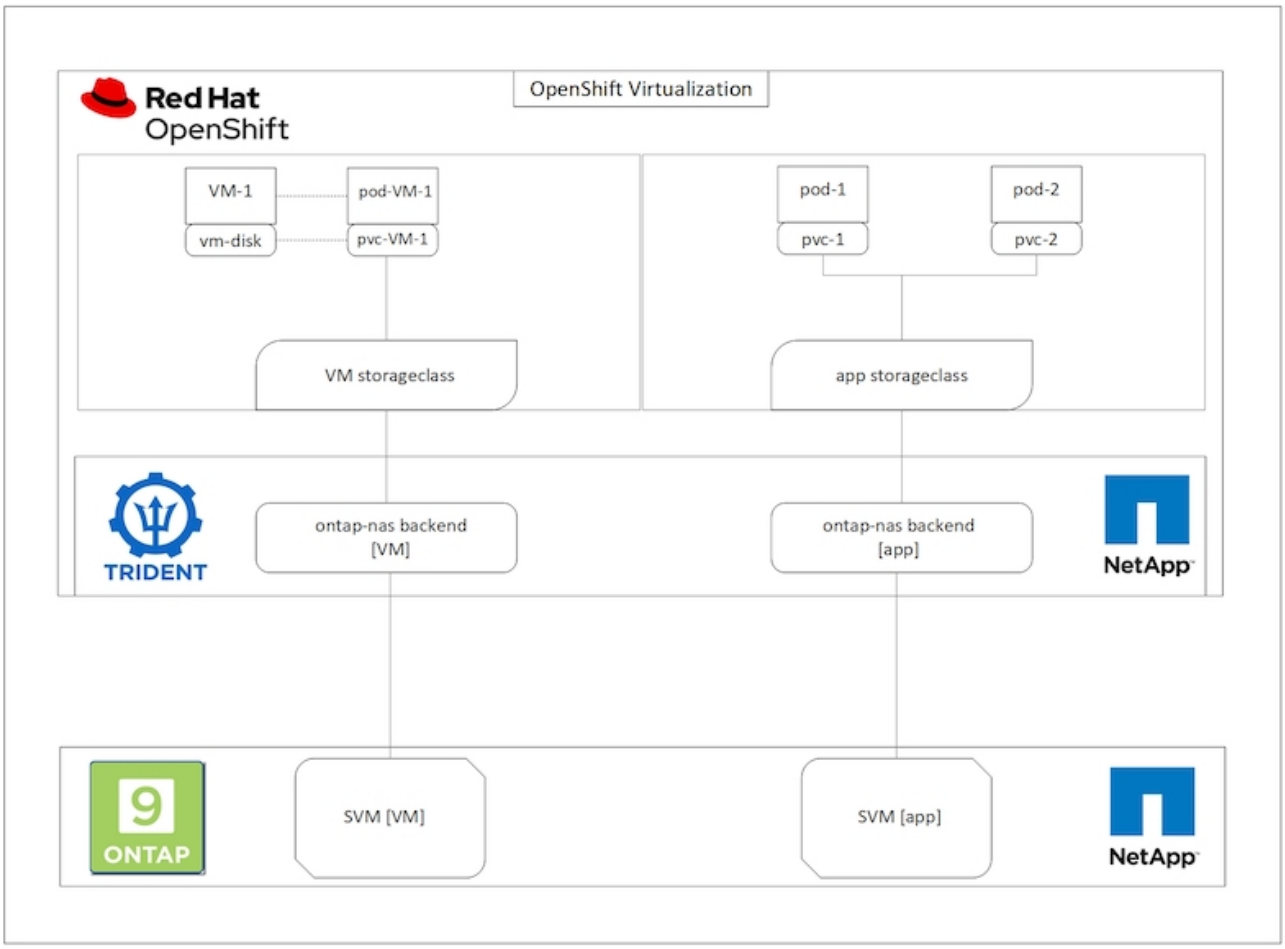
Flussi di lavoro

Workflow: Virtualizzazione Red Hat OpenShift con NetApp ONTAP

Creare una macchina virtuale

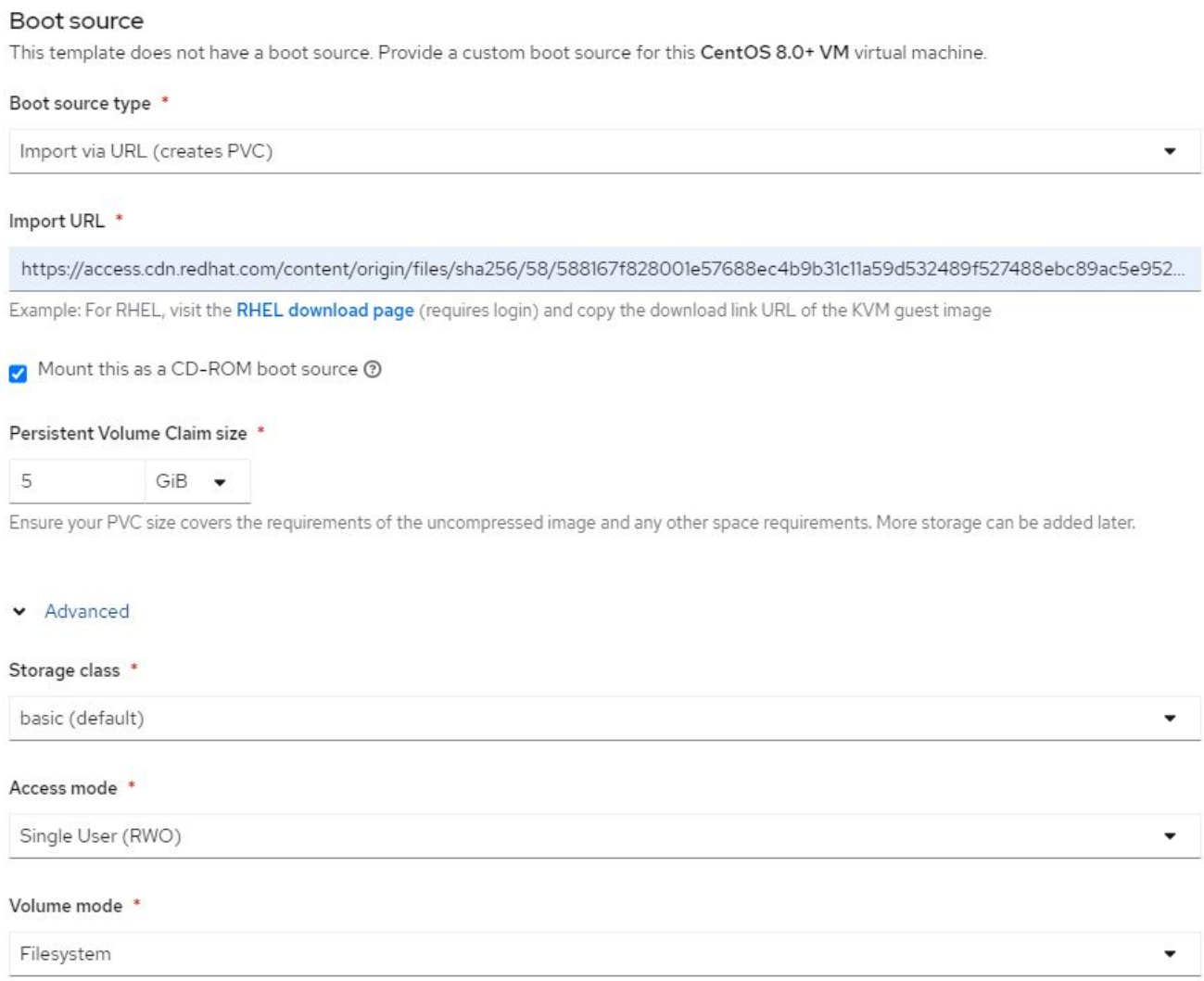
Le VM sono implementazioni stateful che richiedono volumi per ospitare il sistema operativo e i dati. Con CNV, poiché le macchine virtuali vengono eseguite come pod, le macchine virtuali vengono supportate da PVS

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.

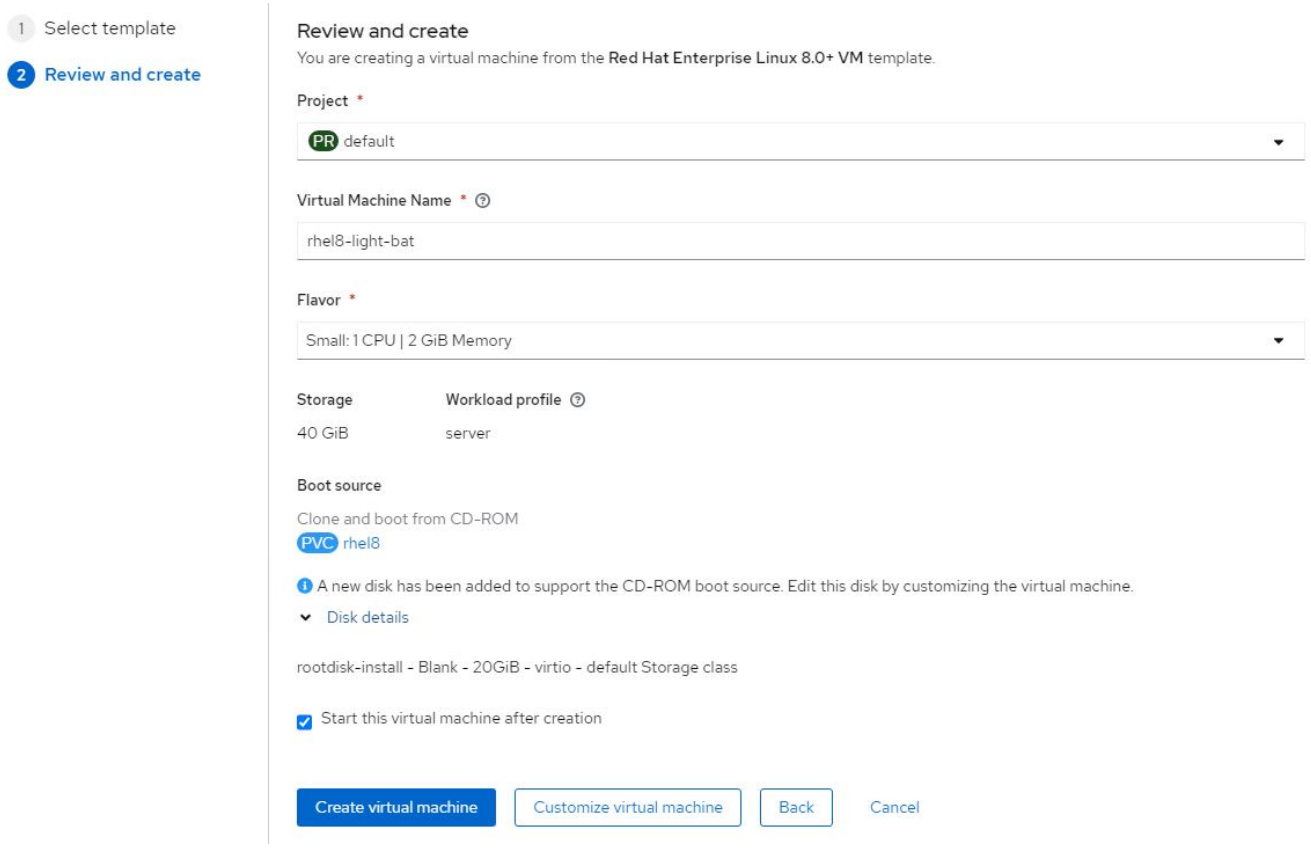


Per creare una macchina virtuale sul cluster OpenShift, attenersi alla seguente procedura:

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).



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.



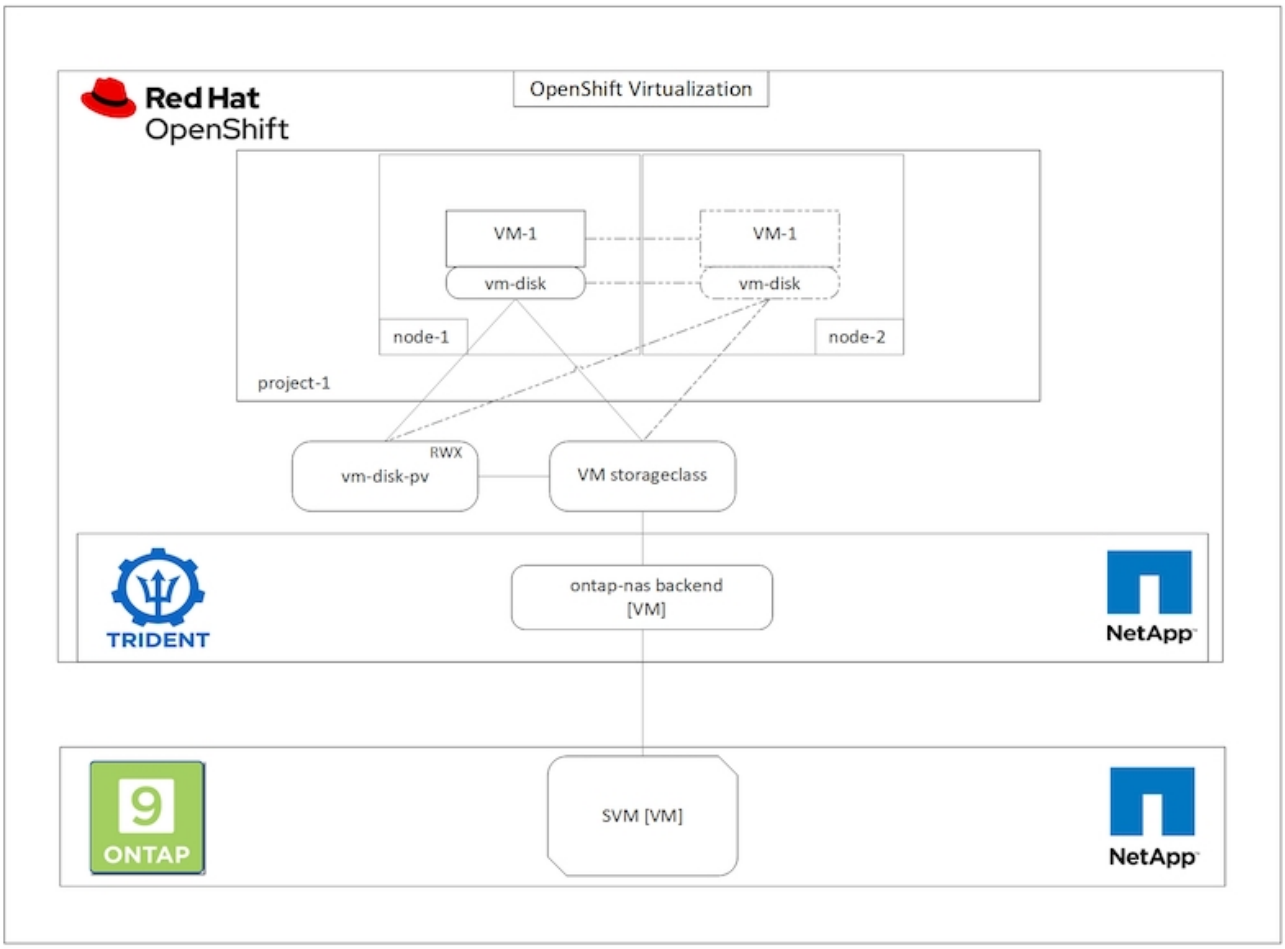
6. Se si desidera personalizzare la macchina virtuale, fare clic su Customize Virtual Machine (Personalizza macchina virtuale) e modificare i parametri richiesti.
7. Fare clic su Create Virtual Machine (Crea macchina virtuale) per creare la macchina virtuale; in questo modo viene fatto rotare in background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

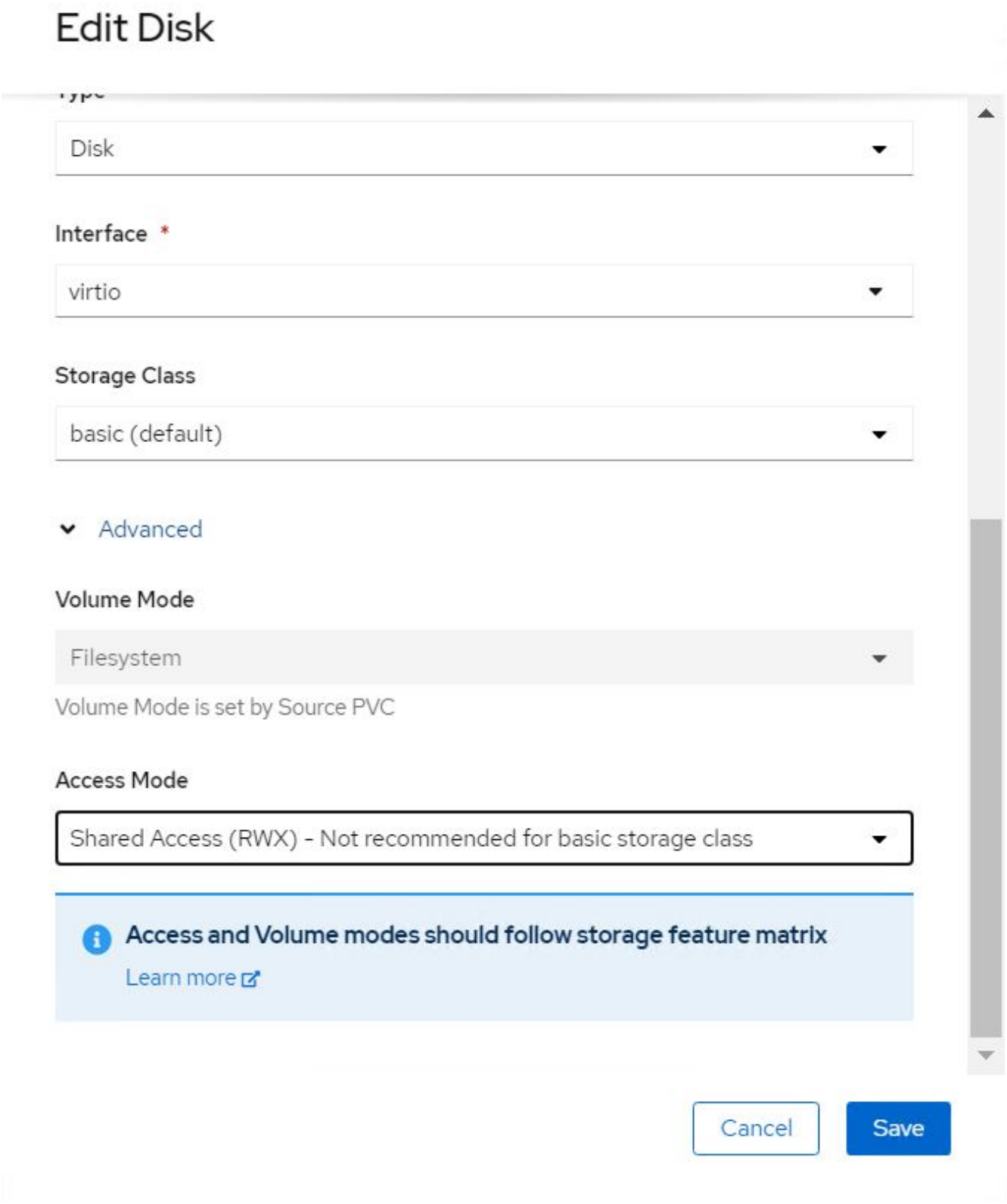
Migrazione VM Live

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).



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.

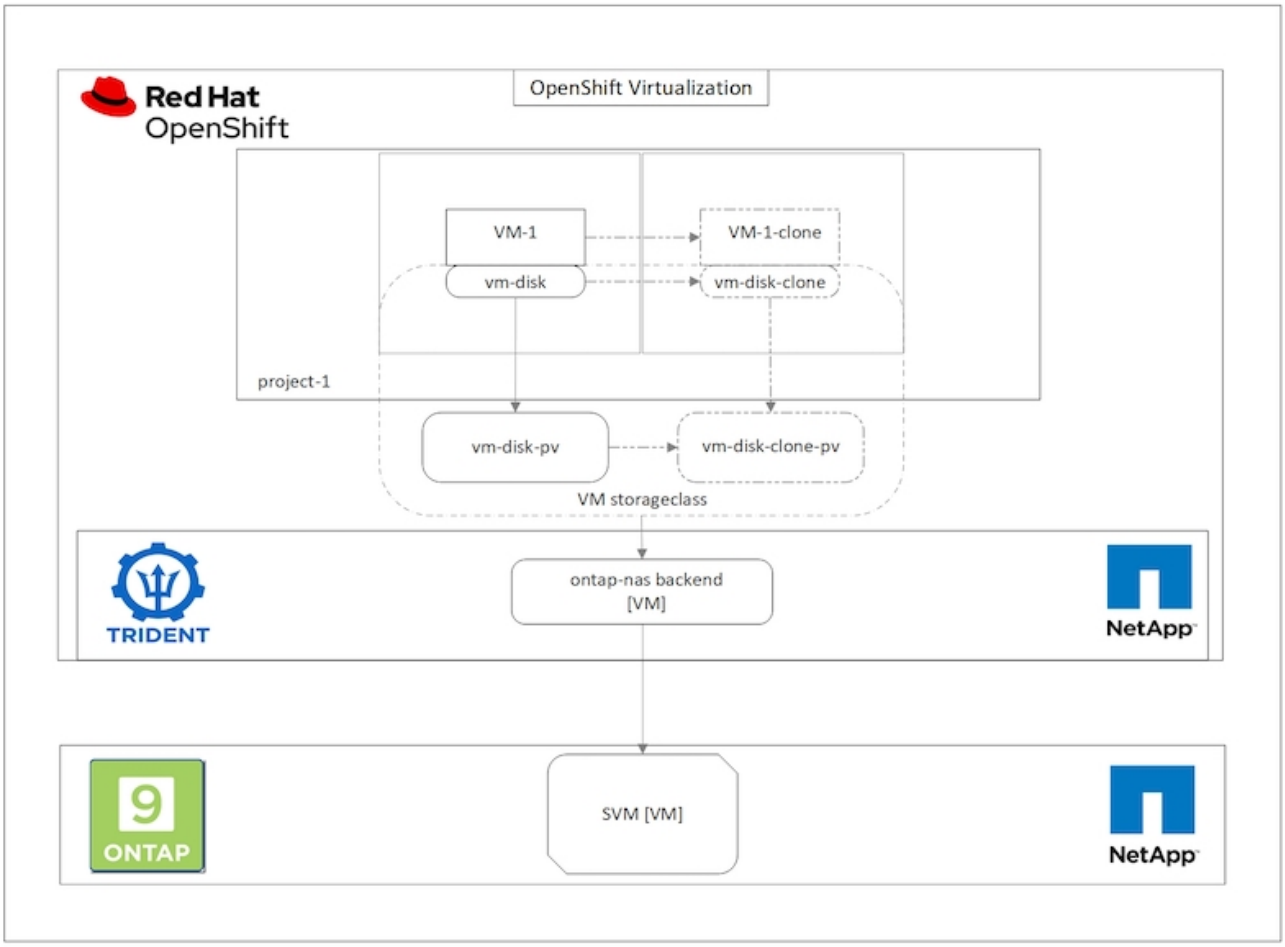
2. Per la macchina virtuale che si desidera migrare, fare clic sui puntini di sospensione, quindi fare clic su Migrate the Virtual Machine (Migra macchina virtuale).
3. Fare clic su Migrate (Migra) quando viene visualizzato il messaggio per confermare.

> 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.

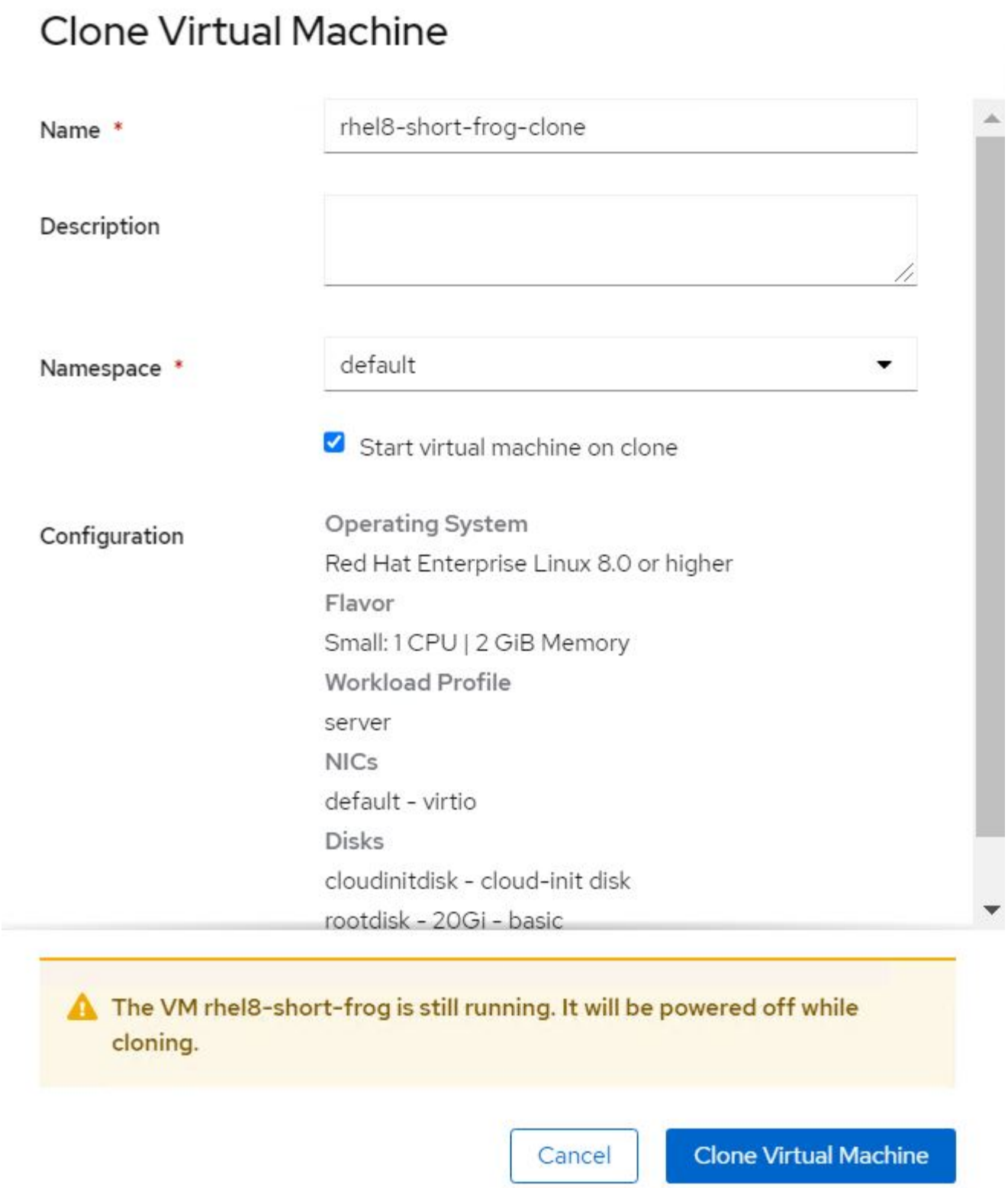
Le VM in un cluster OpenShift possono essere clonate in due modi:

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.

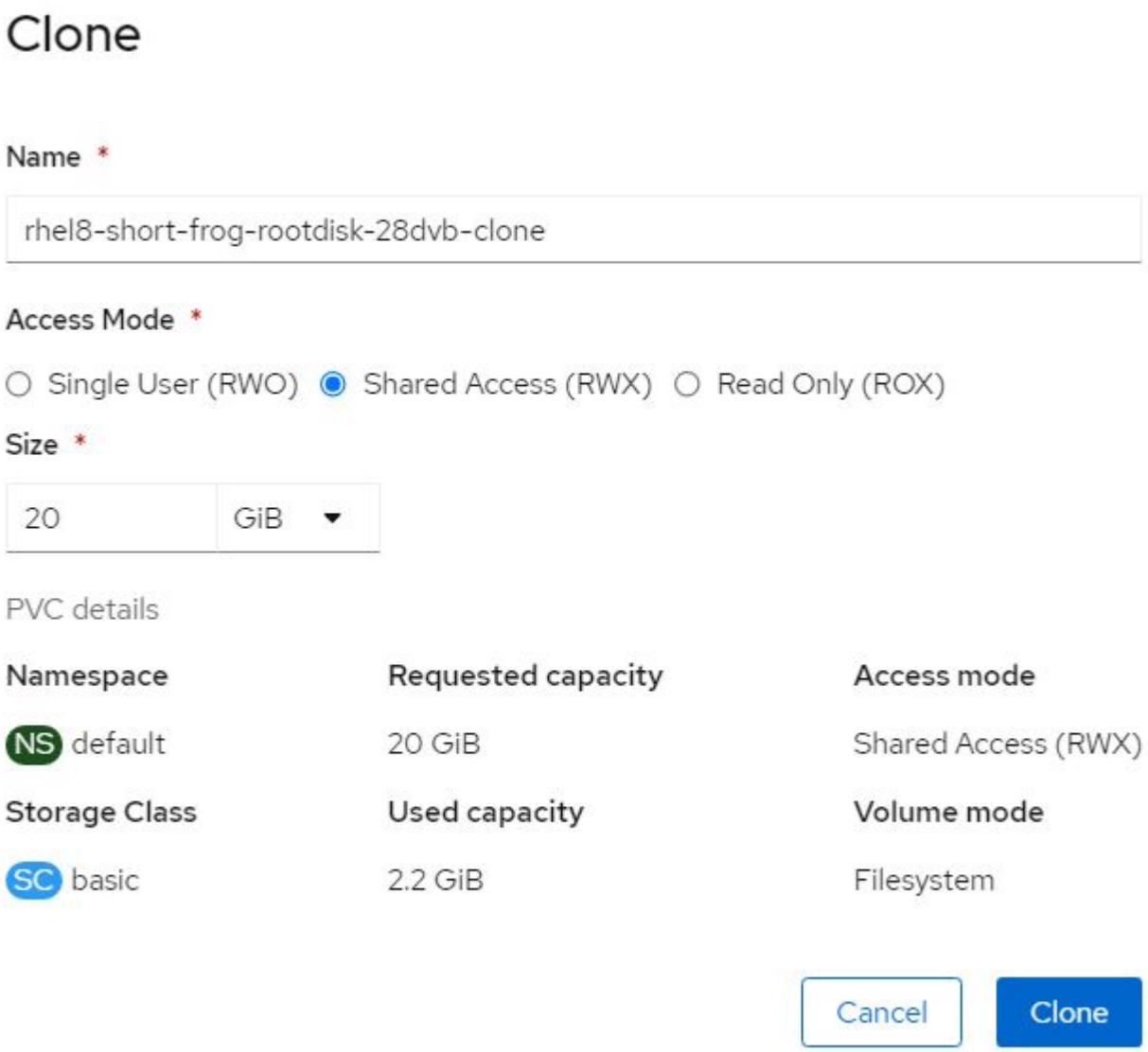


3. Fare clic su Clone Virtual Machine (Clona macchina virtuale) per chiudere la macchina virtuale di origine e avviare la creazione della macchina virtuale clone.
4. Al termine di questa fase, è possibile accedere e verificare il contenuto della VM clonata.

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.



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-28dvb-clone
```

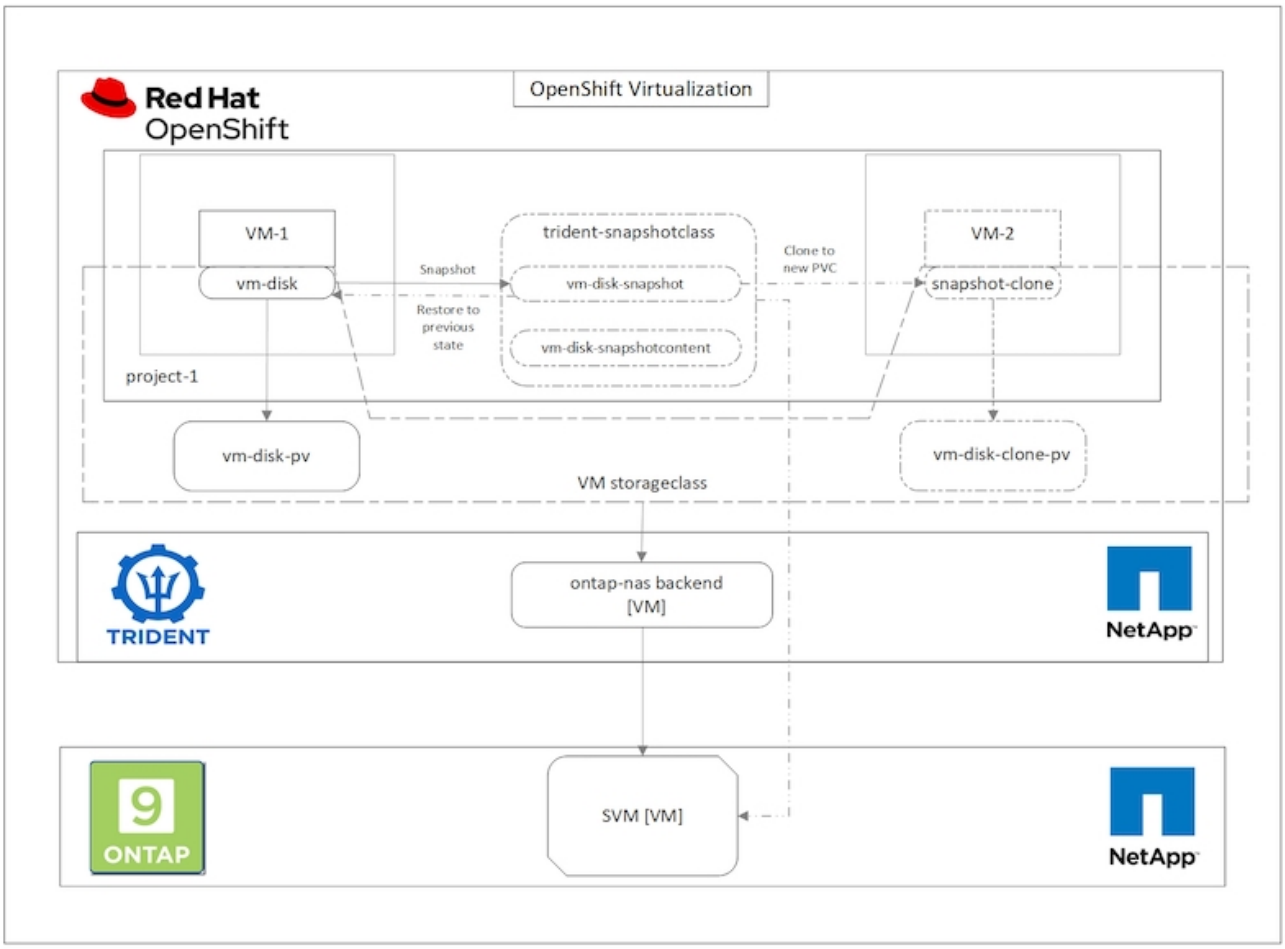
6. Fare clic su Create (Crea) per creare la nuova macchina virtuale.
7. Una volta creata correttamente la macchina virtuale, accedere e verificare che la nuova macchina sia un clone della macchina virtuale di origine.

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.

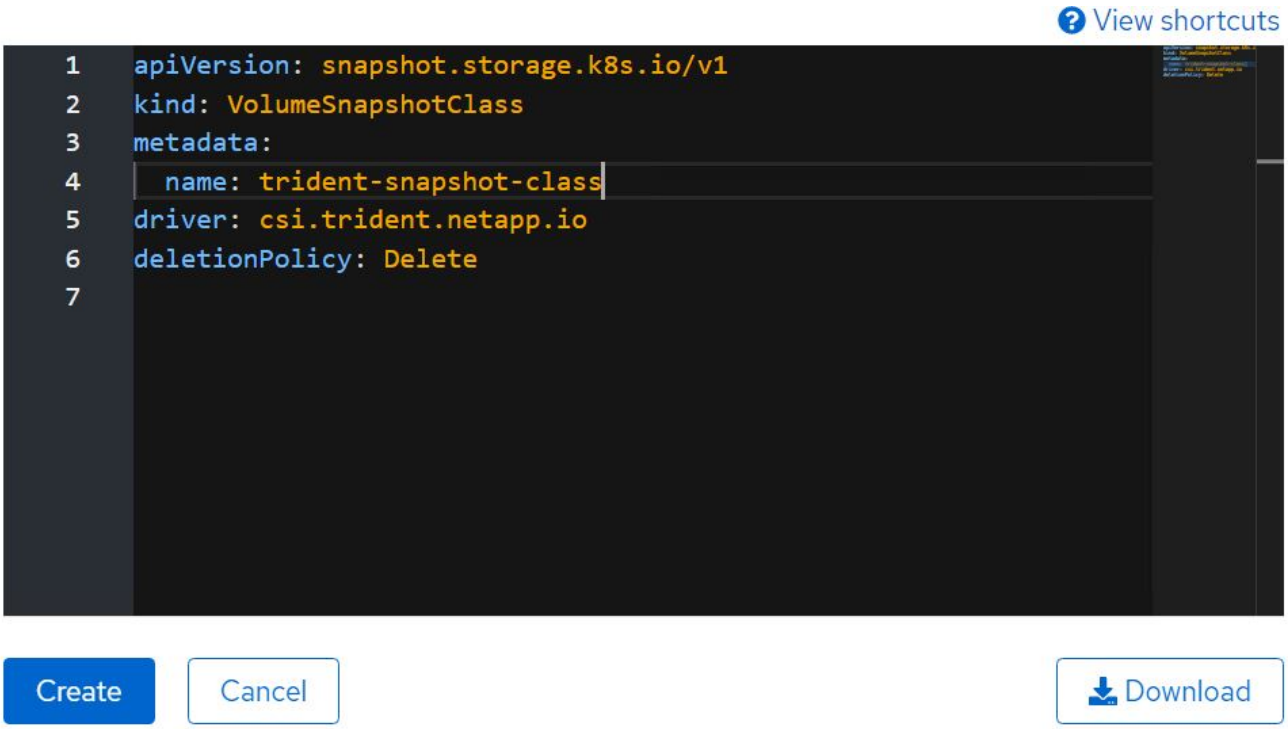
Per le operazioni Snapshot in OpenShift, è necessario definire le risorse VolumeSnapshotClass, VolumeSnapshot e VolumeSnapshotContent.

- 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.

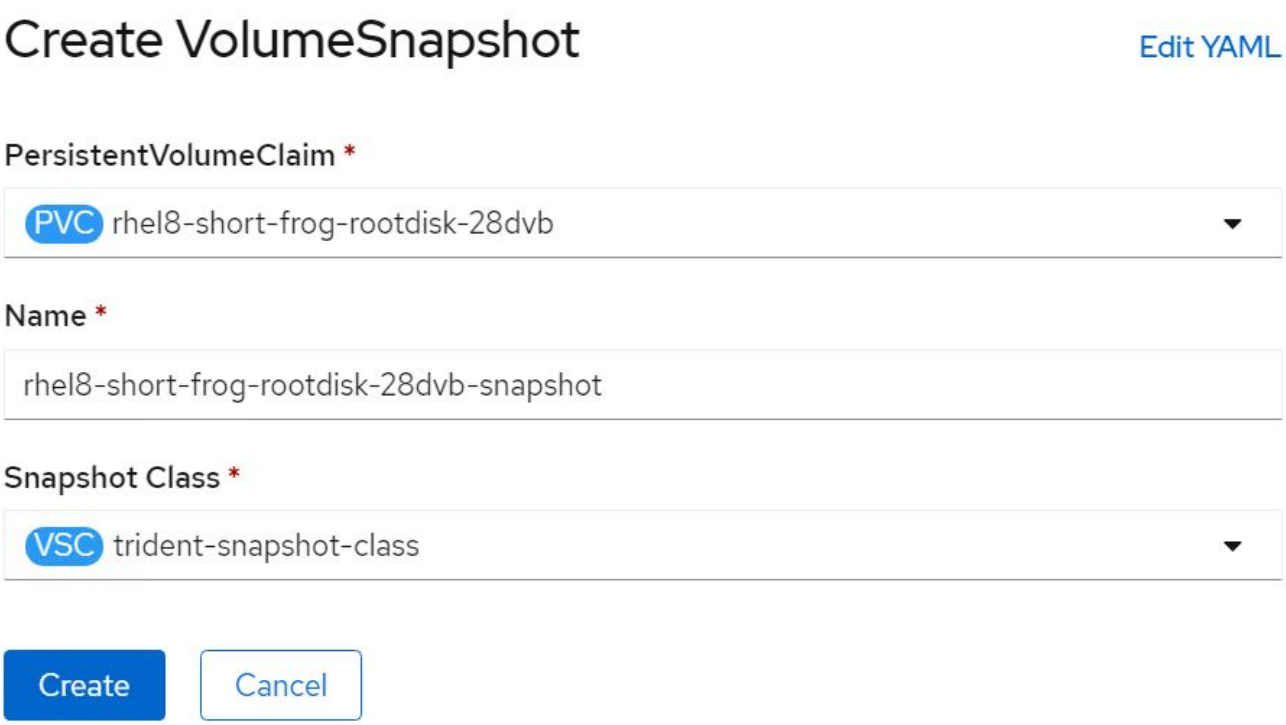


Per creare un'istantanea di una macchina virtuale, attenersi alla seguente procedura:

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).



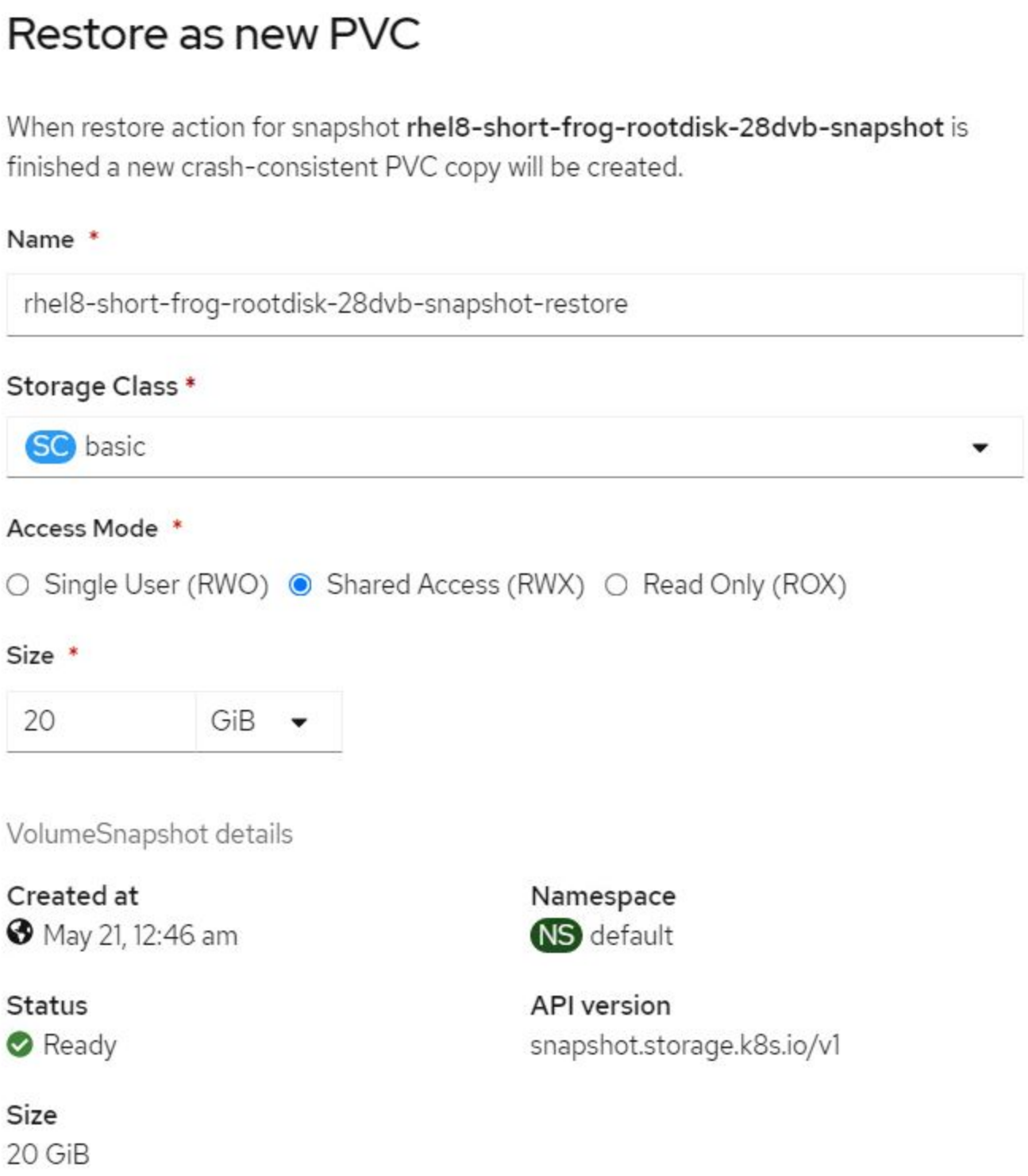
3. Identificare il PVC collegato alla VM di origine e creare un'istantanea del PVC. Selezionare `Storage > VolumeSnapshots` E fare clic su Create VolumeSnapshots (Crea snapshot Volume).
4. Selezionare il PVC per il quale si desidera creare l'istantanea, immettere il nome dell'istantanea o accettare il valore predefinito, quindi selezionare la VolumeSnapshotClass appropriata. Quindi fare clic su Create (Crea).



5. In questo modo viene creata l'istantanea 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.



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-28dvb-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

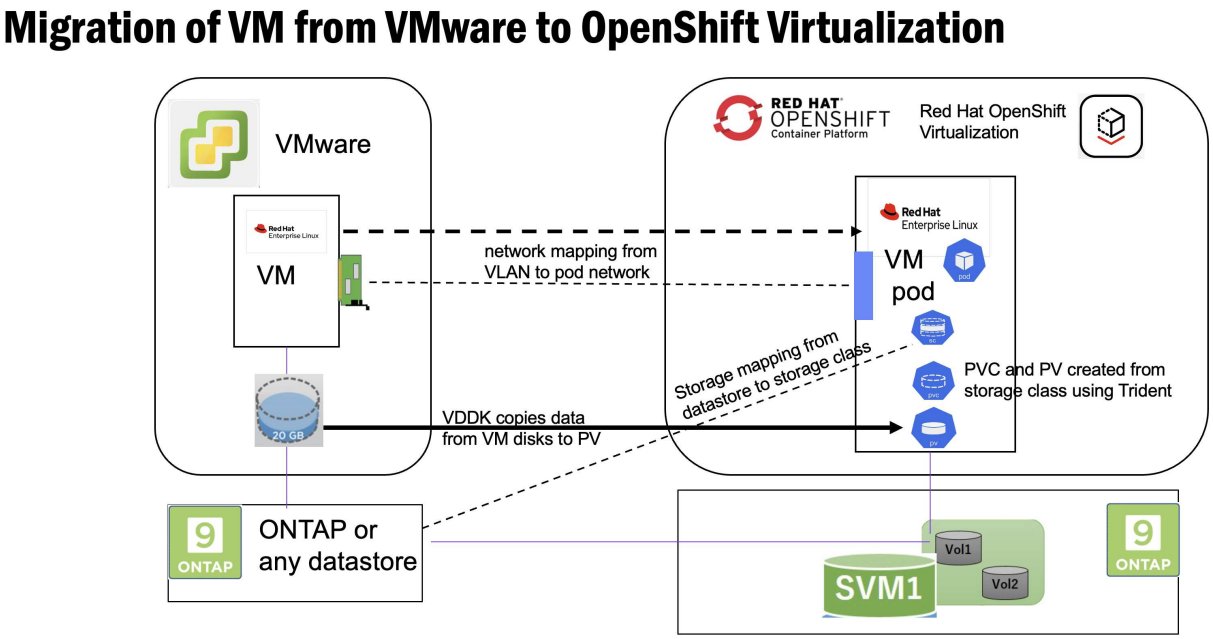
Migrazione di VM da VMware alla virtualizzazione OpenShift mediante Migration Toolkit for Virtualization

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.



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

```yaml
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

```yaml
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

```yaml
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.

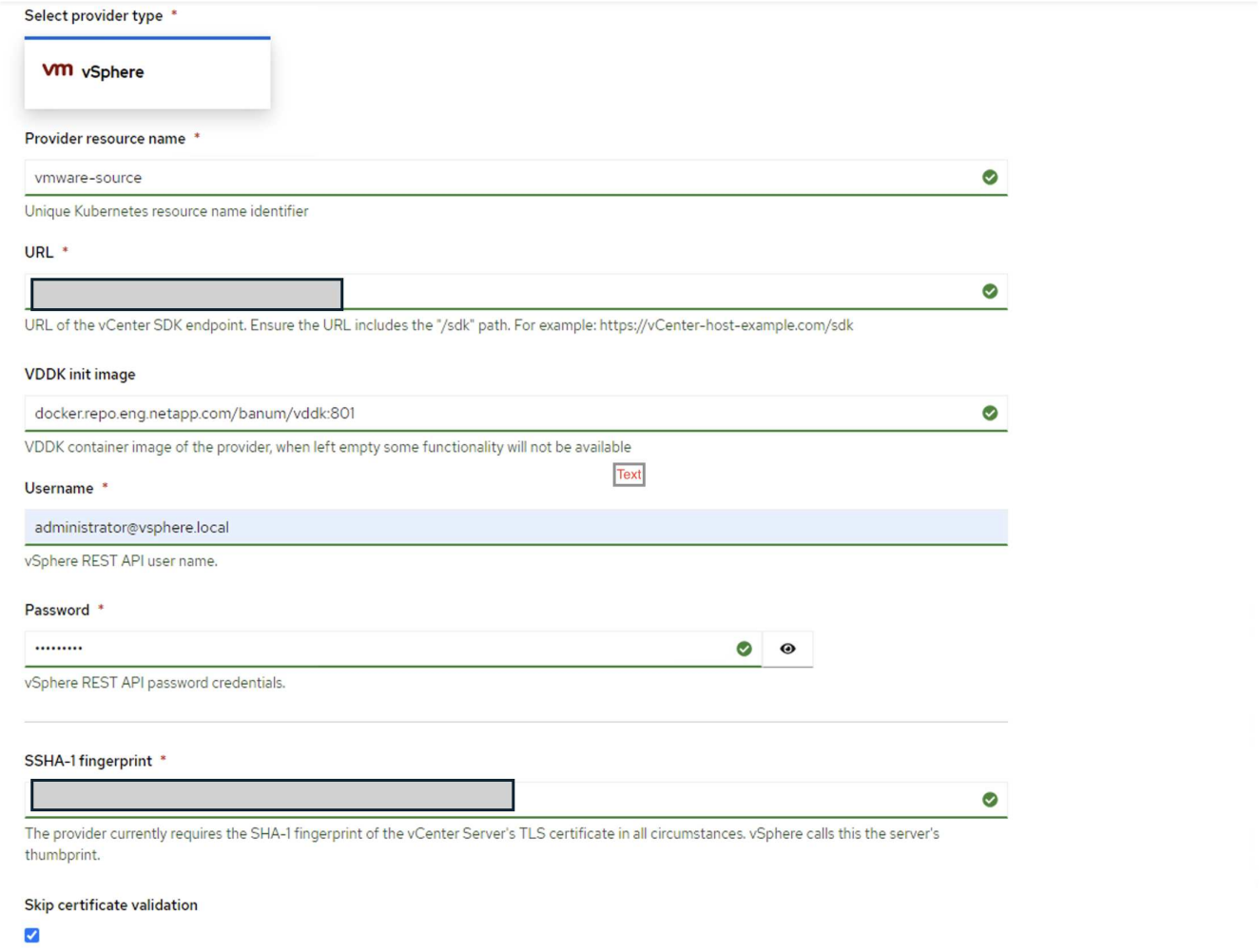
Creare il fornitore di origine

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:



> 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

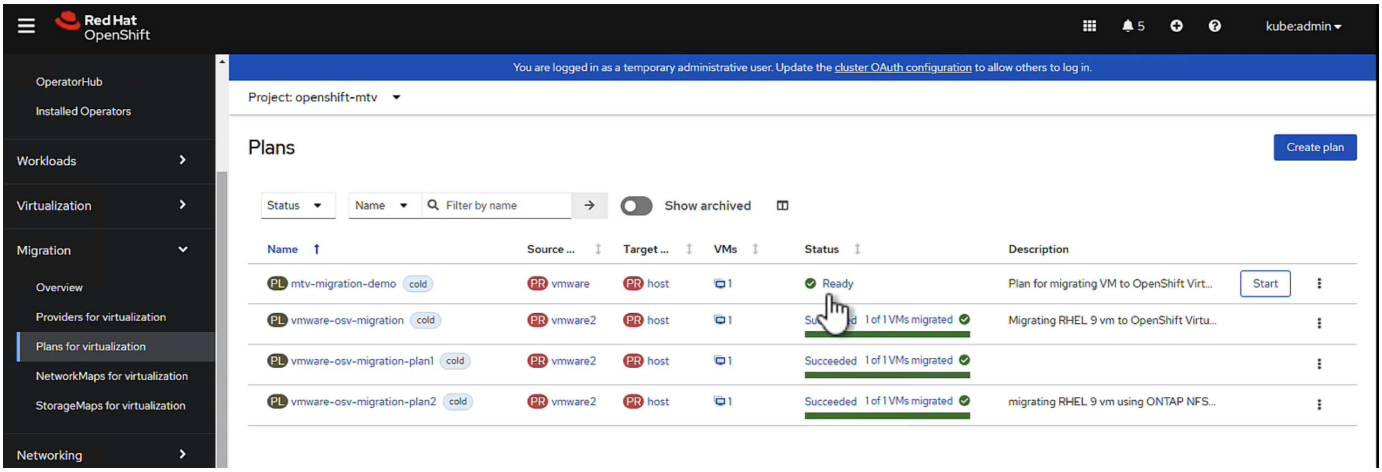
Il cluster host viene aggiunto automaticamente in quanto il provider di virtualizzazione OpenShift è il provider di origine.

Creare un piano di migrazione

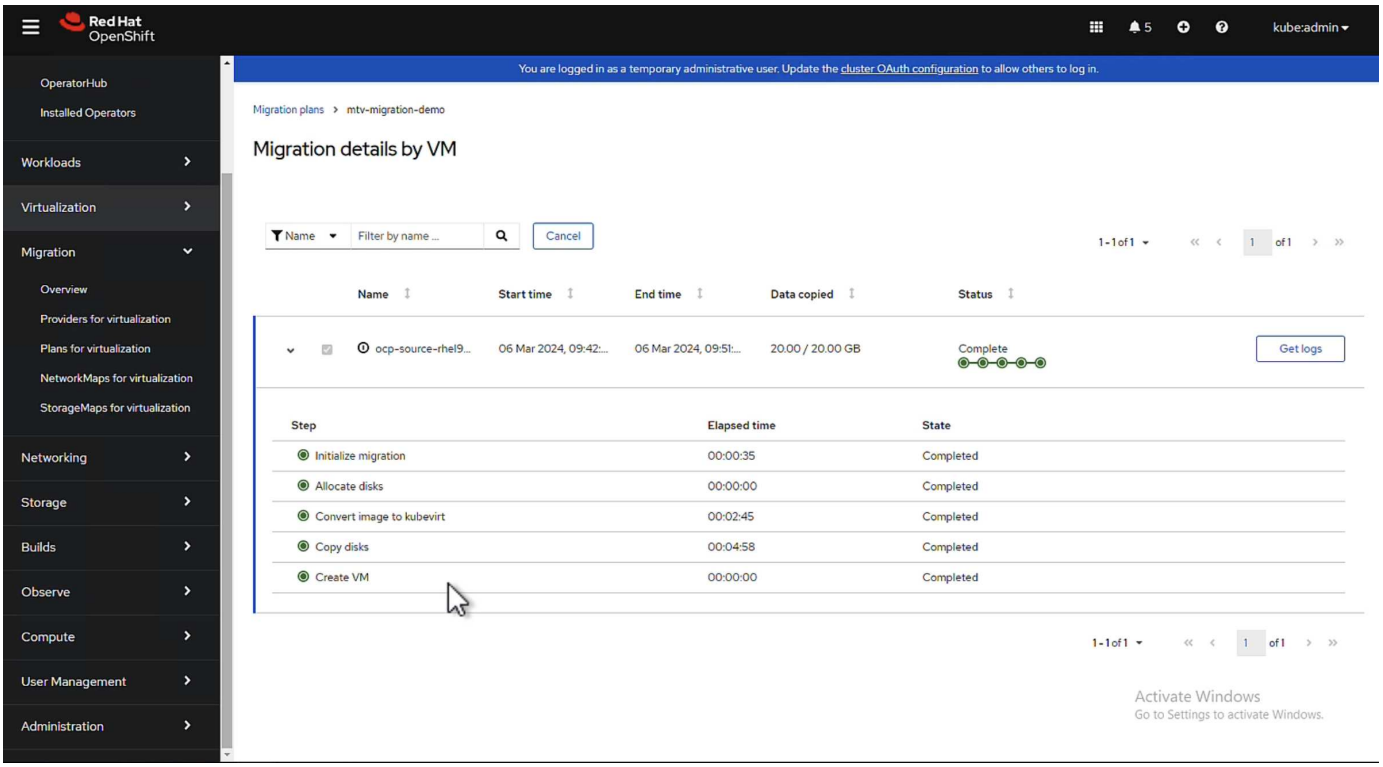
Seguire le istruzioni fornite "qui" per creare un piano di migrazione.

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.



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 posgresql. 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.

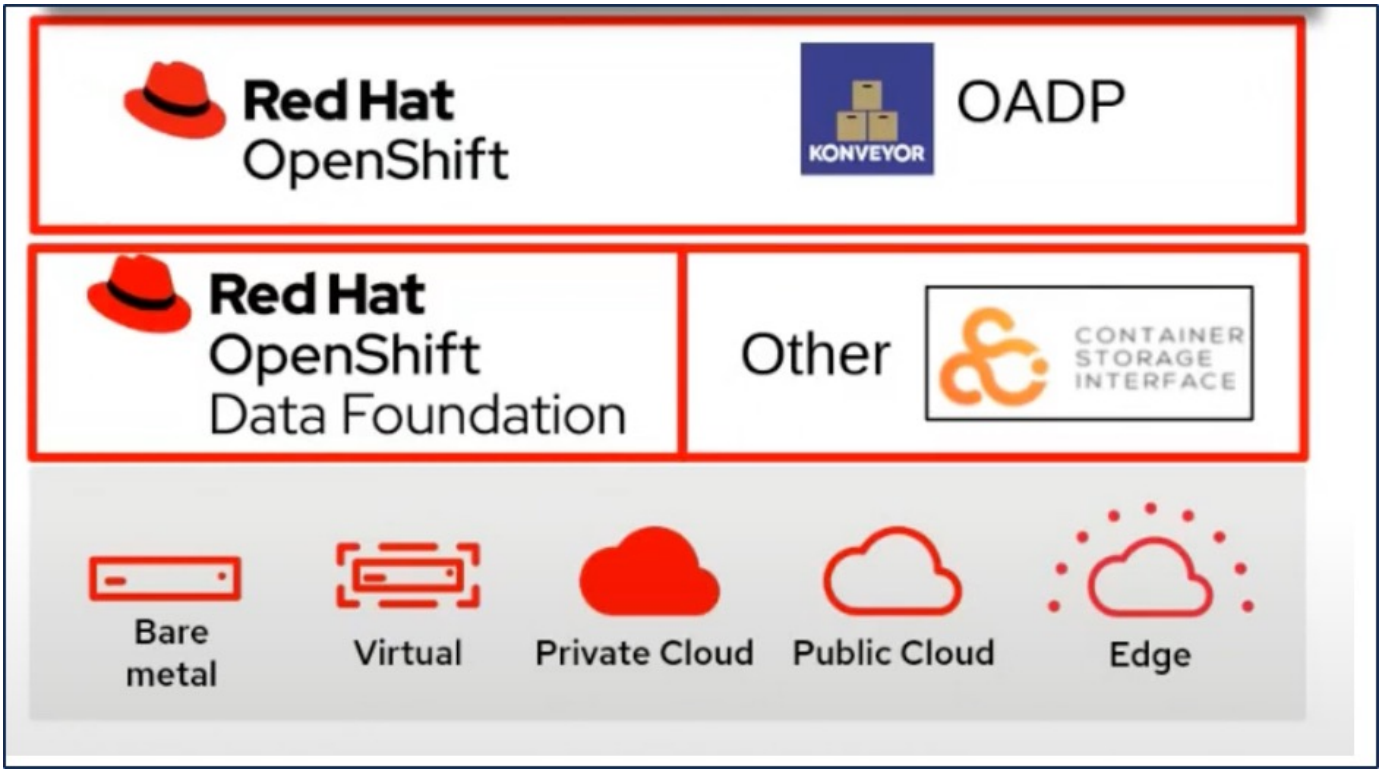
I dischi persistenti delle macchine virtuali di virtualizzazione OpenShift possono essere sottoposti a backup dallo storage ONTAP integrato nel cluster OpenShift utilizzando "CSI Astra Trident". In questa sezione usiamo "OpenShift API per la protezione dei dati (OADP)" Per eseguire il backup delle VM, inclusi i relativi volumi di dati su

- Storage a oggetti ONTAP

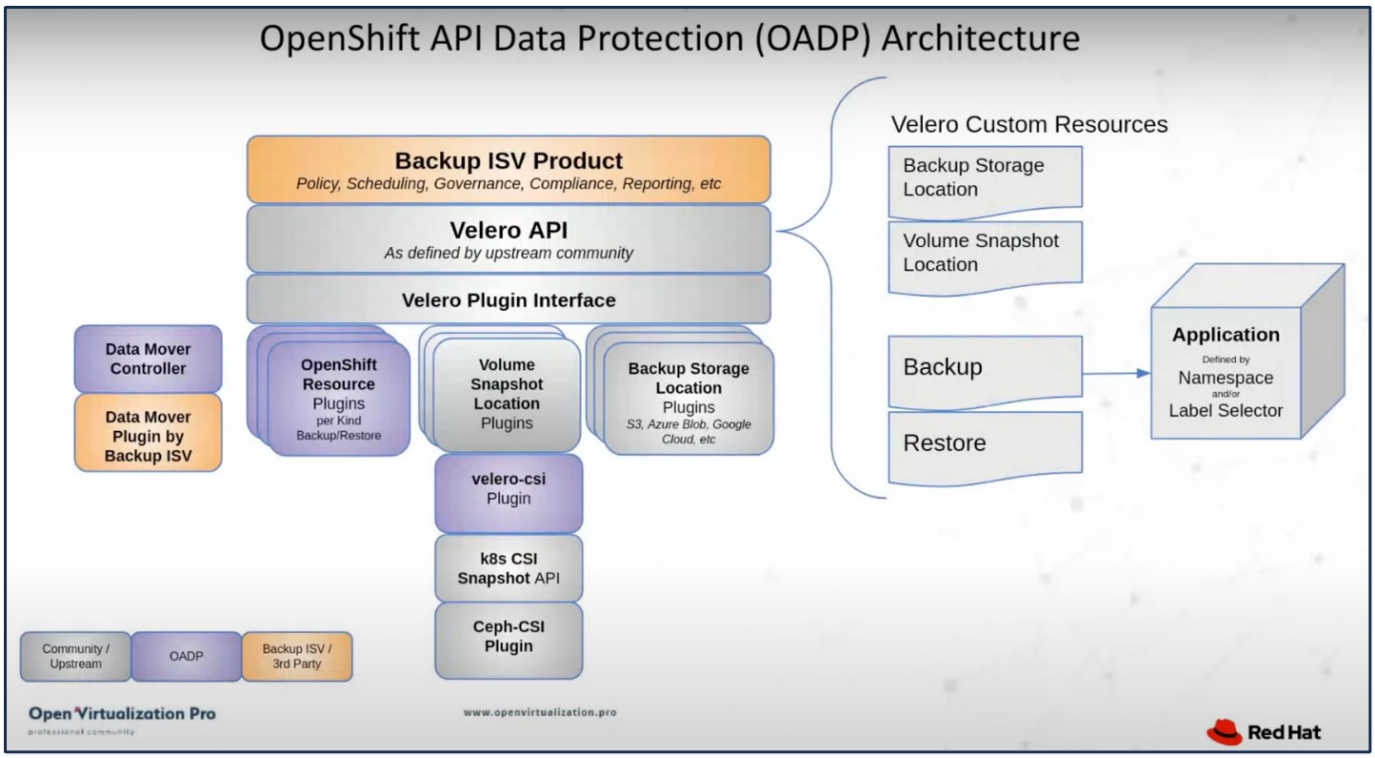
- StorageGRID

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

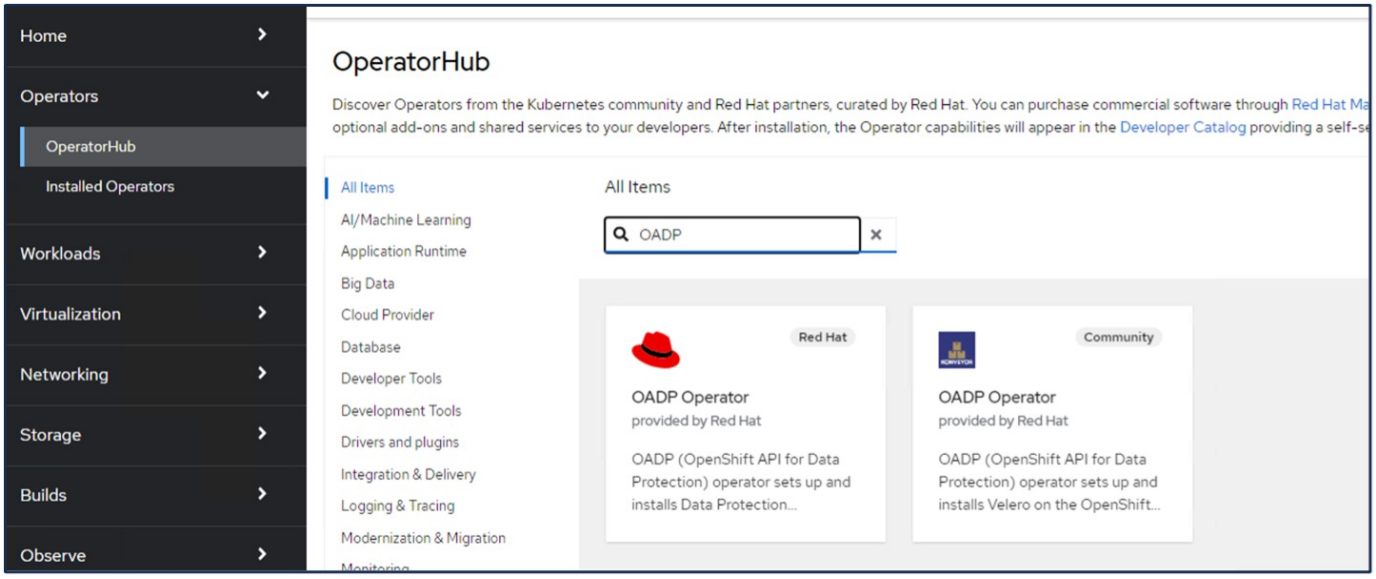
- Un cluster Red Hat OpenShift (versione successiva alla 4,12) installato in un'infrastruttura bare-metal con nodi di lavoro RHCOS
- Un cluster NetApp ONTAP integrato con il cluster utilizzando Astra Trident
- Un backend Trident configurato con una SVM sul cluster ONTAP
- StorageClass configurato sul 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
OpenShift Virtualization 4.14.4 provided by Red Hat	NS openshift-cnv	NS openshift-cnv	Succeeded Up to date
OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	NS openshift-adp	Succeeded Up to date
Package Server 0.0.1-snapshot provided by	NS openshift-operator-lifecycle-manager	NS 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.

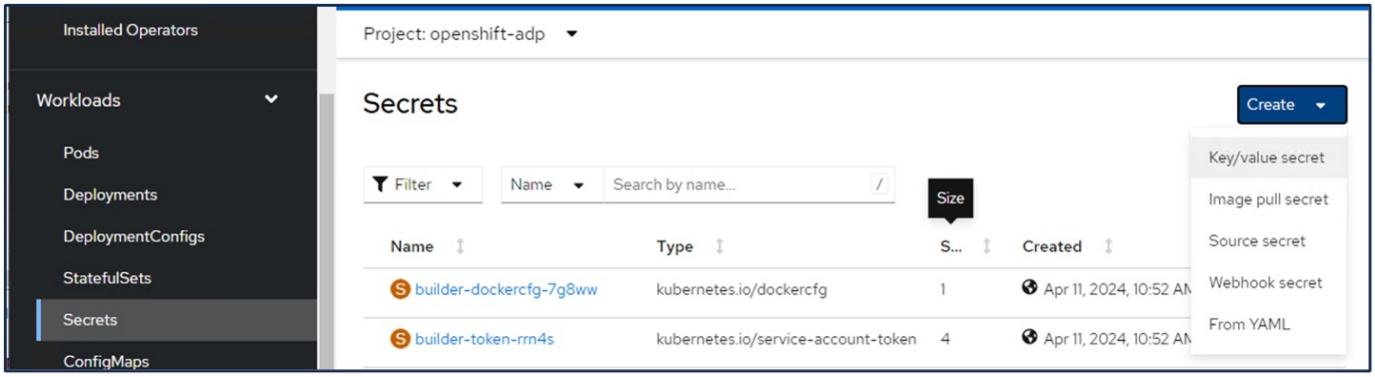
Prerequisiti per la configurazione di Velero con i dettagli di StorageGRID S3

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 *

cloud-credentials

Unique name of the new secret.

Key *

cloud

Value

Browse...

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>
```

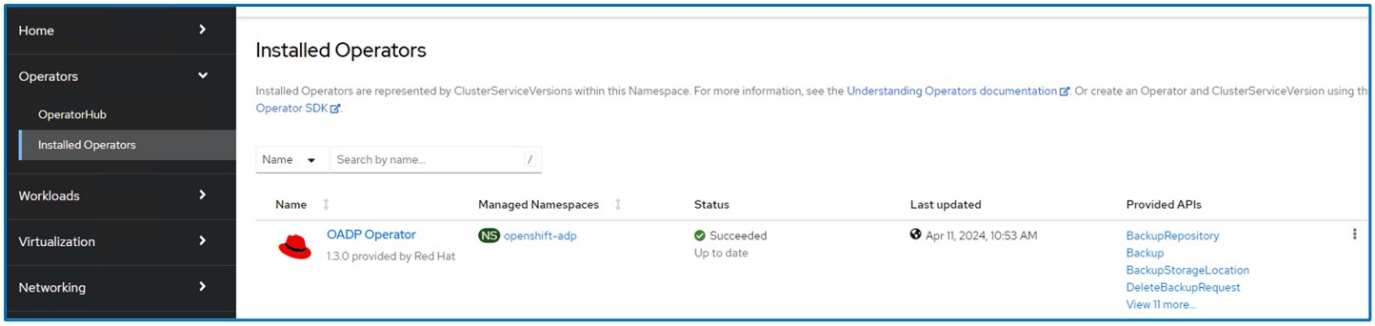
Add key/value

Create Cancel

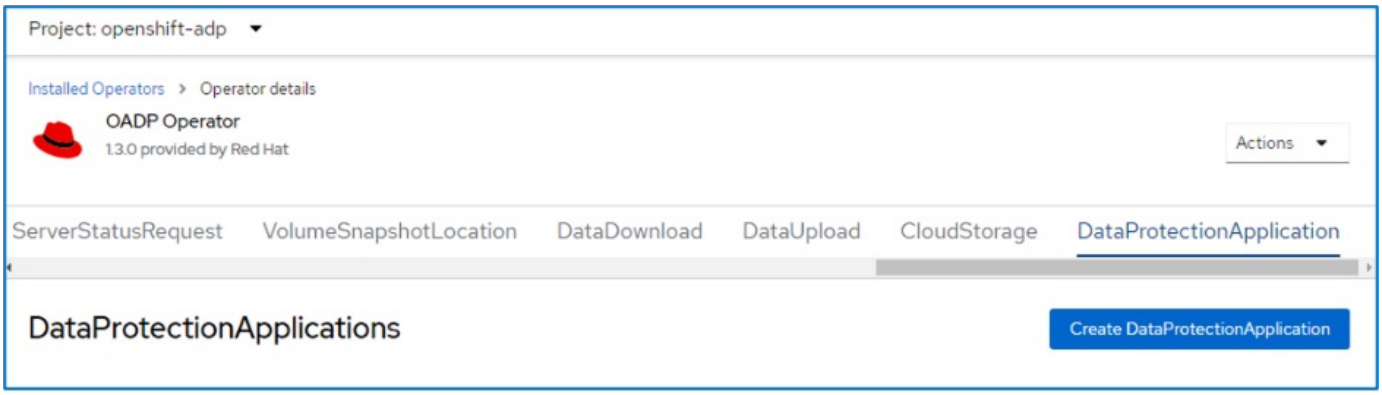
Per creare un segreto denominato sg-S3-credenziali dall'interfaccia CLI, è possibile utilizzare il seguente comando.

```
# 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.



Fare clic su Create DataProtectionApplication. Nella vista modulo, specificare un nome per l'applicazione DataProtection o utilizzare il nome predefinito.



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.

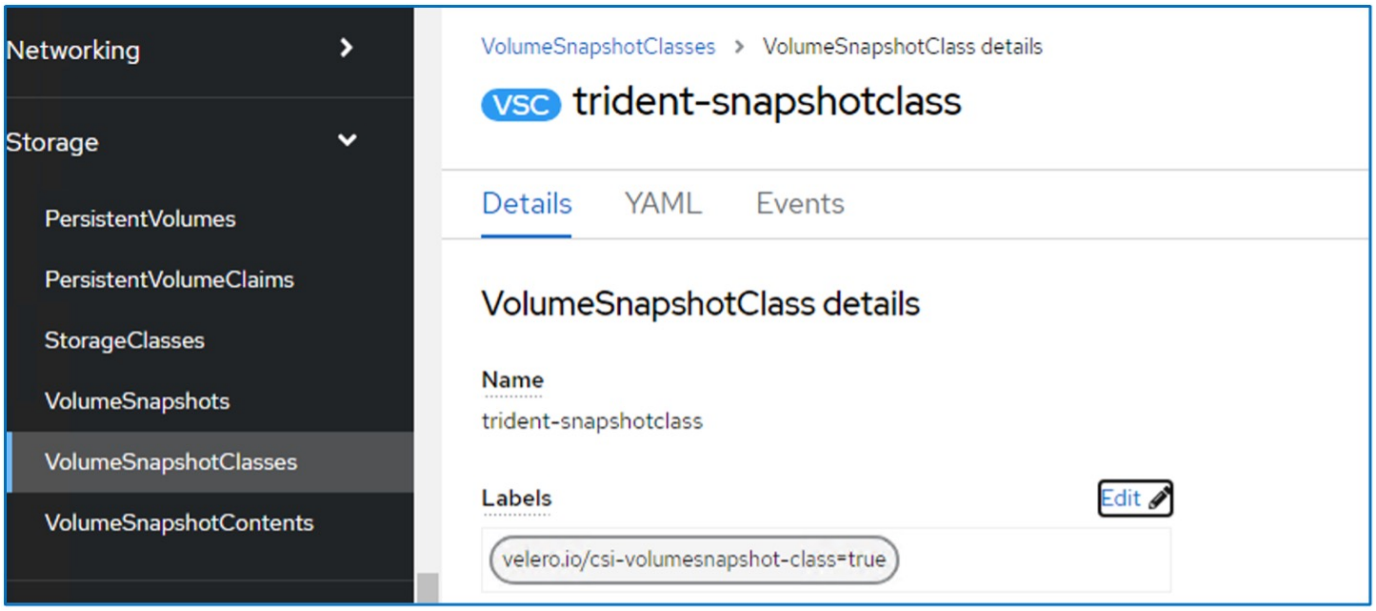
SnapshotLocations
Se si utilizzano gli snapshot Container Storage Interface (CSI), non è necessario specificare una posizione dello snapshot perché si creerà un VolumeSnapshotClass CR per registrare il driver CSI. Nel nostro esempio, si utilizza Astra Trident CSI e in precedenza si è creato VolumeSnapShotClass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

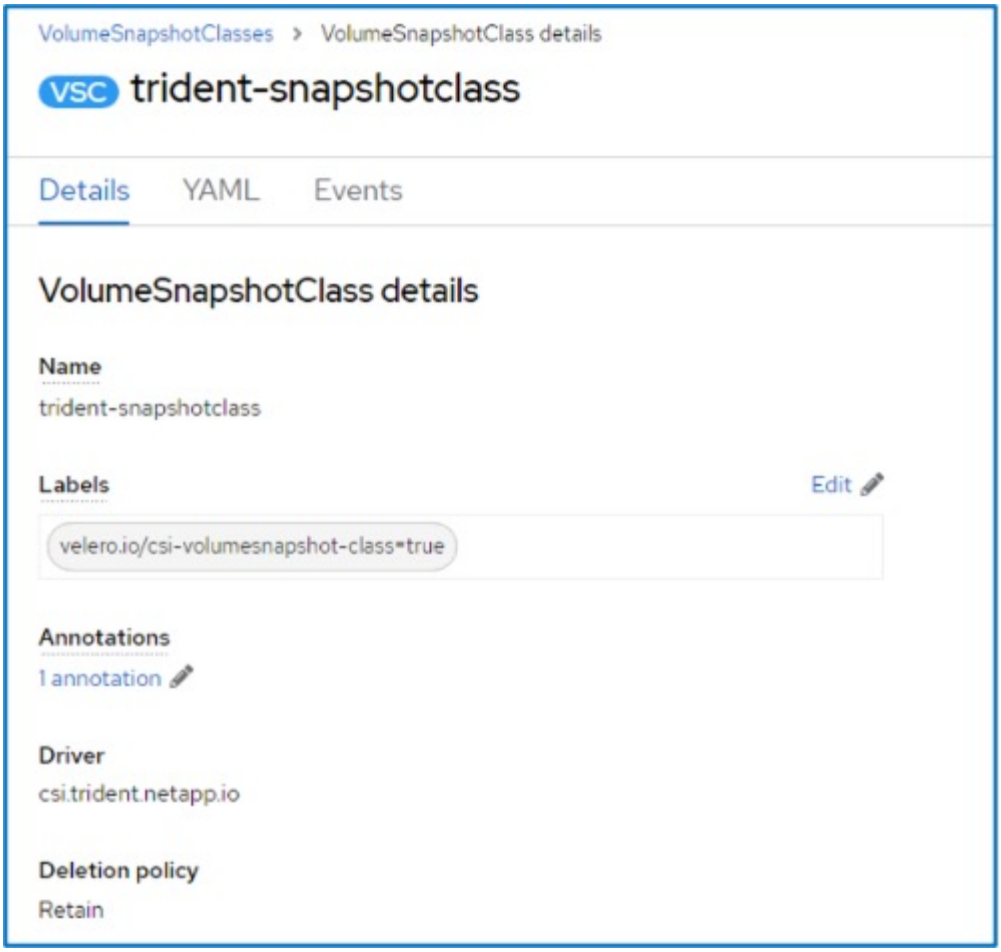
- È necessario creare il tridente VolumeSnapshotClass.

- Modificare l'etichetta della classe trident-snapshotclass e impostarla su **velero.io/csi-volumesnapshot-class=true** come mostrato di seguito.

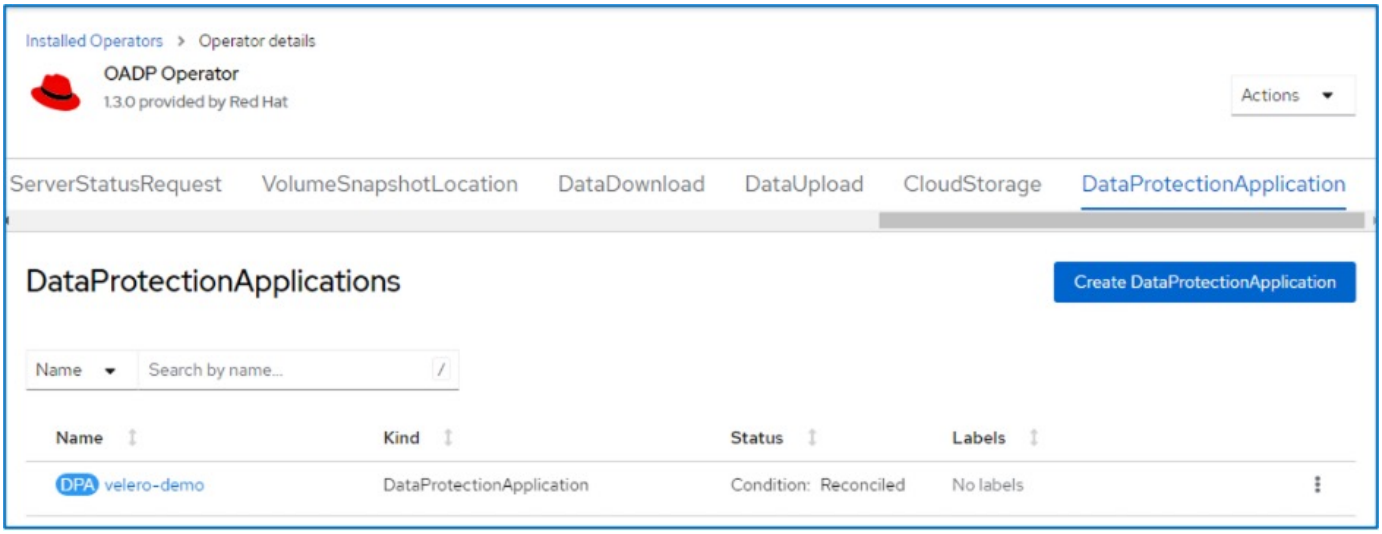


Verificare che gli snapshot possano persistere anche se gli oggetti VolumeSnapshot vengono eliminati. A tale scopo, impostare **deletionPolicy** su Retain. In caso contrario, l'eliminazione di uno spazio dei nomi perderà completamente tutti i PVC di cui è stato eseguito il backup.

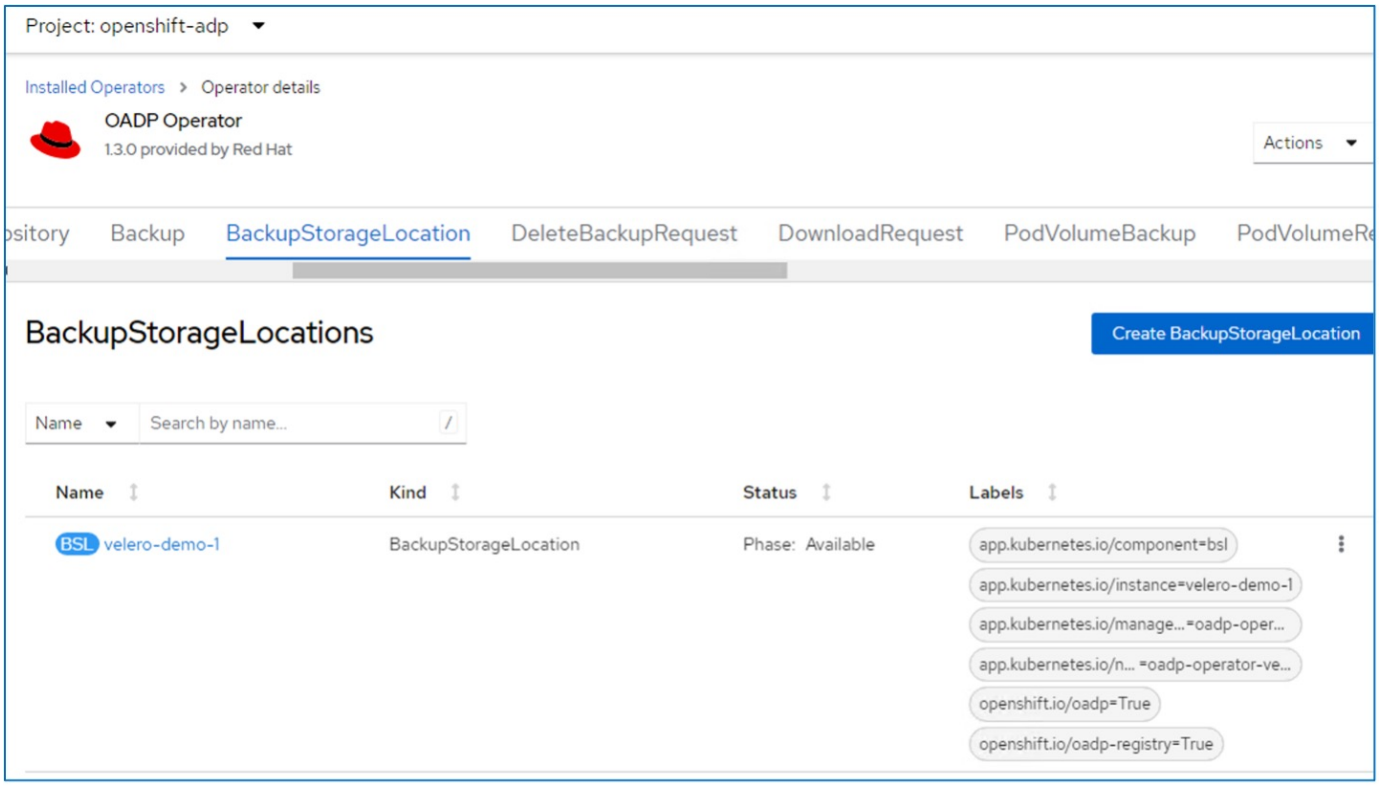
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Verificare che DataProtectionApplication sia stato creato e che sia in condizioni:riconciliato.



L'operatore OADP creerà un BackupStorageLocation corrispondente. Questo verrà utilizzato durante la creazione di un backup.



Creazione di backup su richiesta per le VM in OpenShift Virtualization

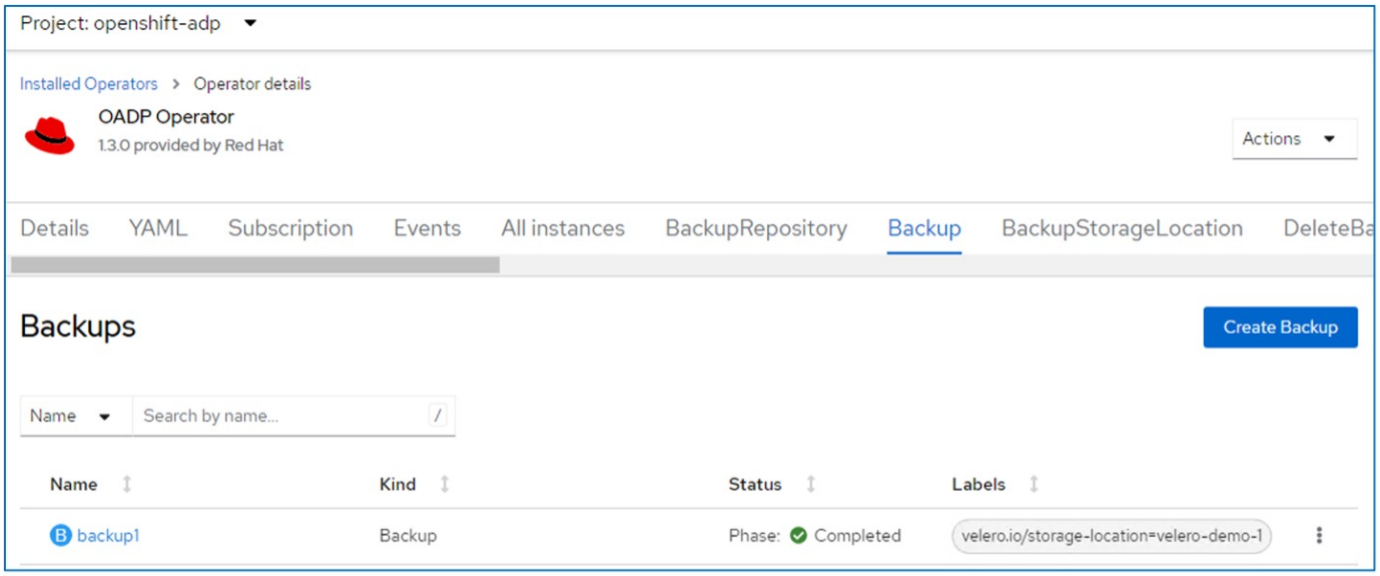
Procedura per creare un backup di una VM

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.

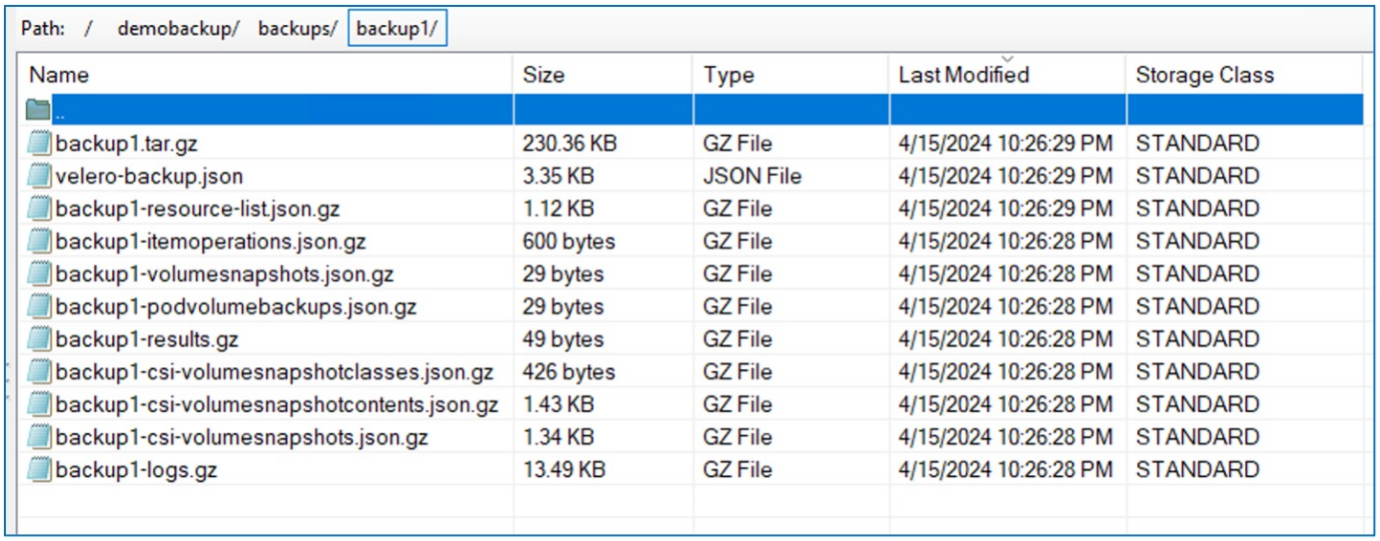
```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when Velero is configured.
  ttl: 720h0m0s
```

Una volta completato il backup, la sua fase viene visualizzata come completata.



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.



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

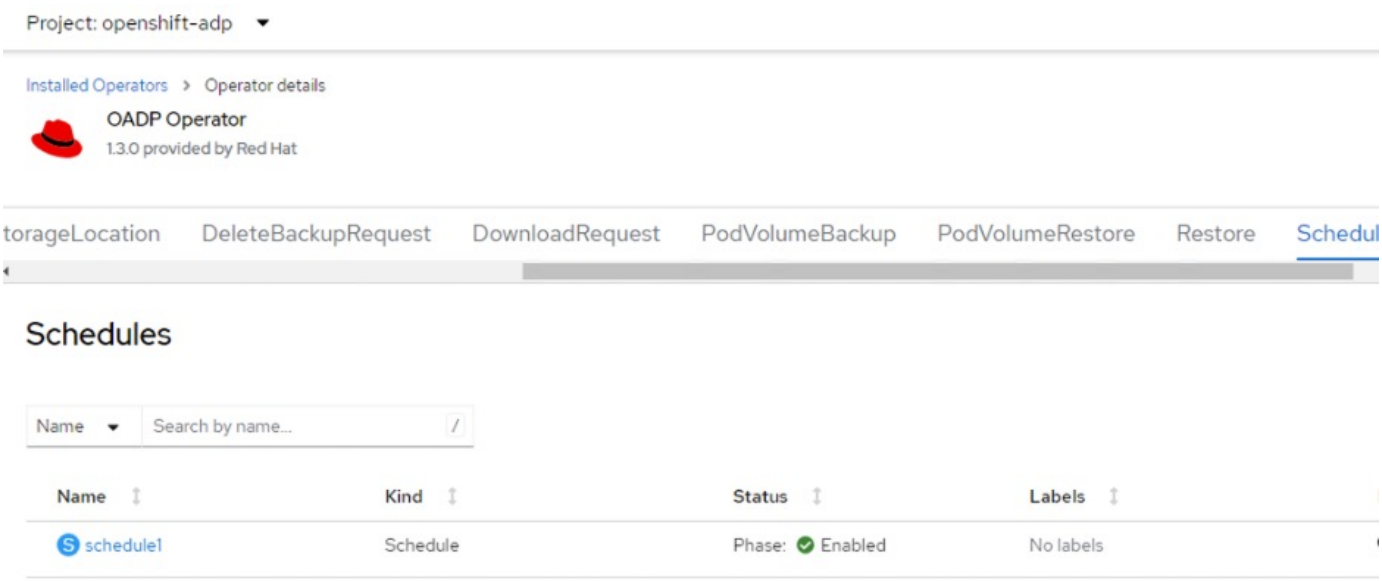
Creazione di backup pianificati per le VM in OpenShift Virtualization

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.

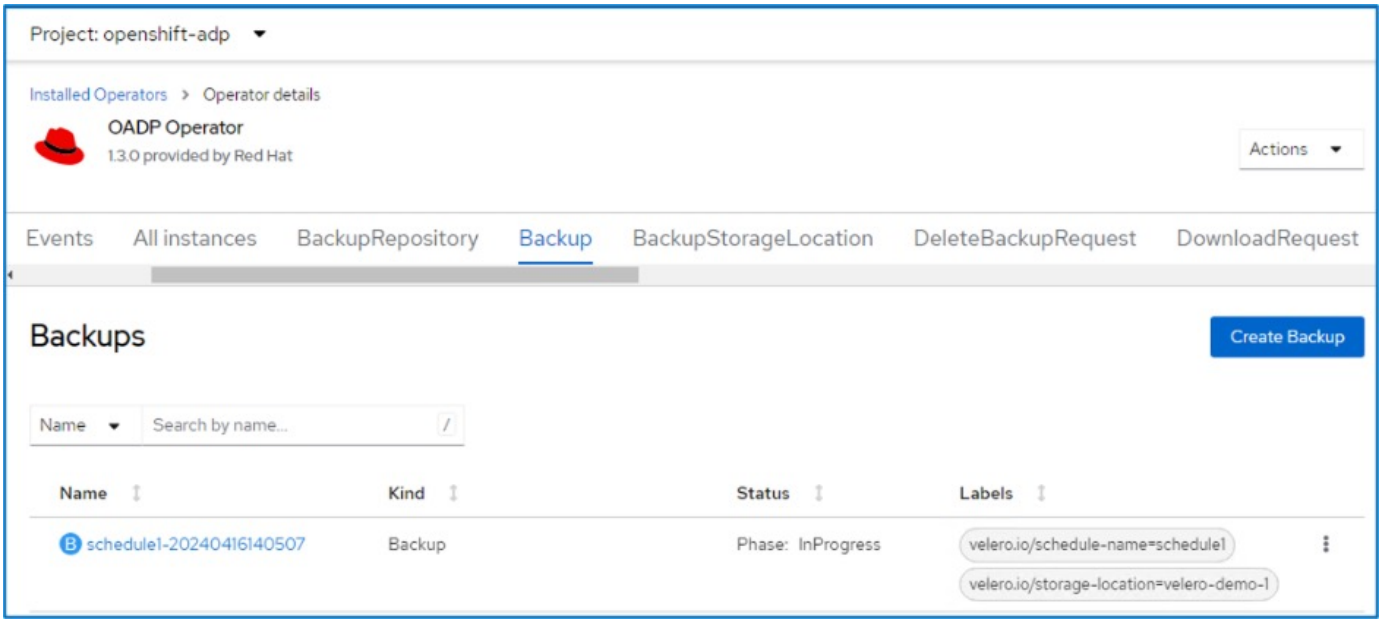
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

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.



I backup verranno creati in base a questa pianificazione e possono essere visualizzati dalla scheda Backup.



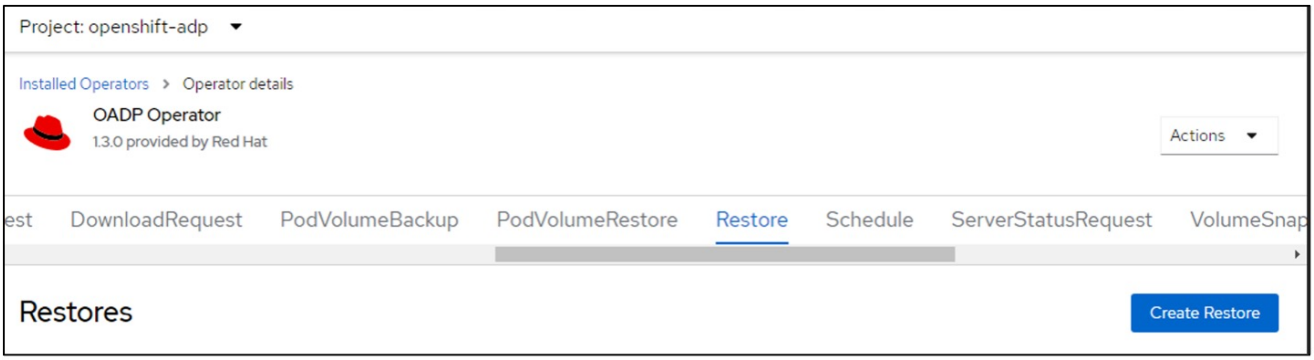
Ripristinare una VM da un backup

Prerequisiti

Per eseguire il ripristino da un backup, supponiamo che lo spazio dei nomi in cui esisteva la macchina virtuale sia stato eliminato accidentalmente.

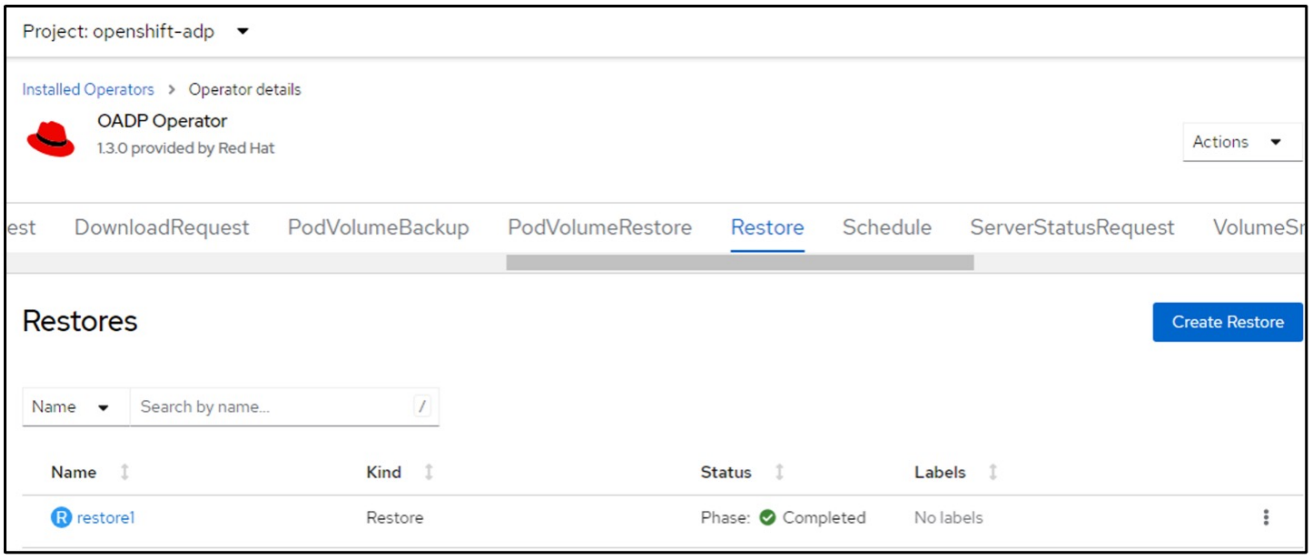
Ripristinare nello stesso namespace

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.




```
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.



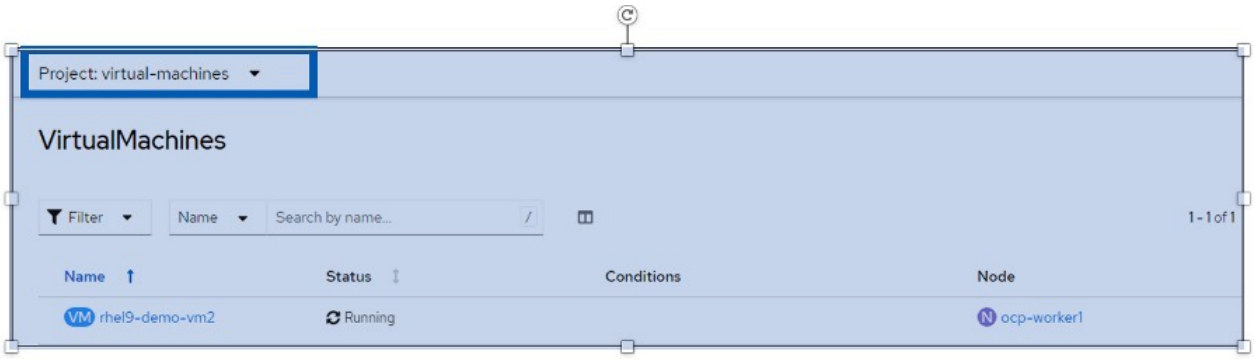
Ripristinare in un namespace diverso

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-machine.

```
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
```

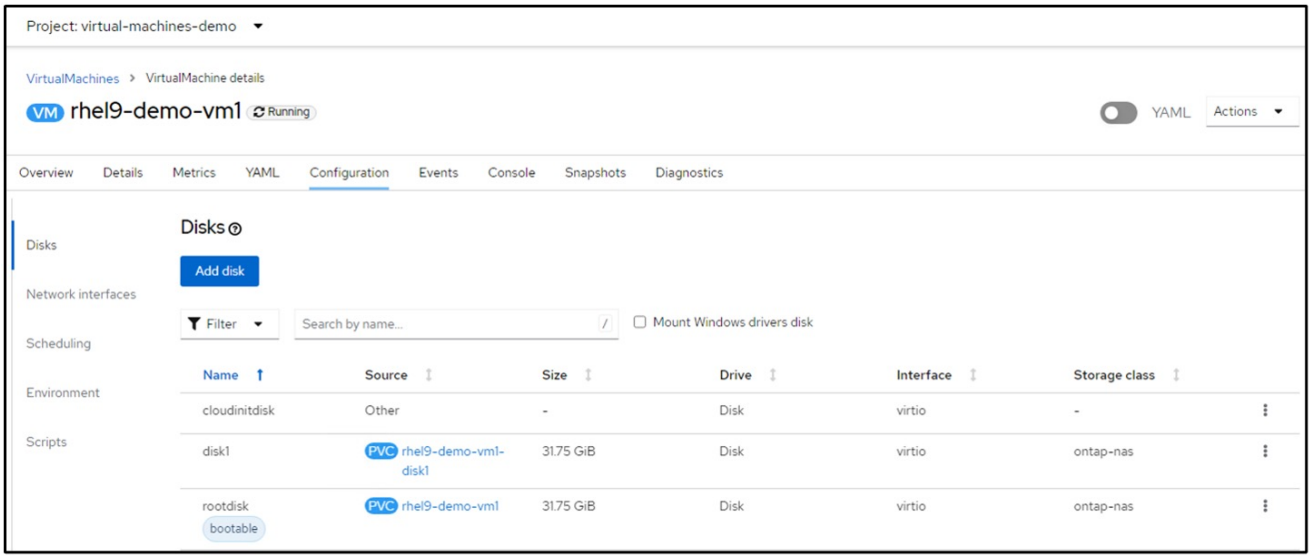
Quando la fase è completata, è possibile vedere che le macchine virtuali sono state ripristinate allo stato in cui è stato acquisito lo snapshot. (Se il backup è stato creato quando la VM era in esecuzione, ripristinando la VM dal backup si avvia la VM ripristinata e la si porta in esecuzione). La VM viene ripristinata in uno spazio dei nomi diverso, come specificato in yaml.

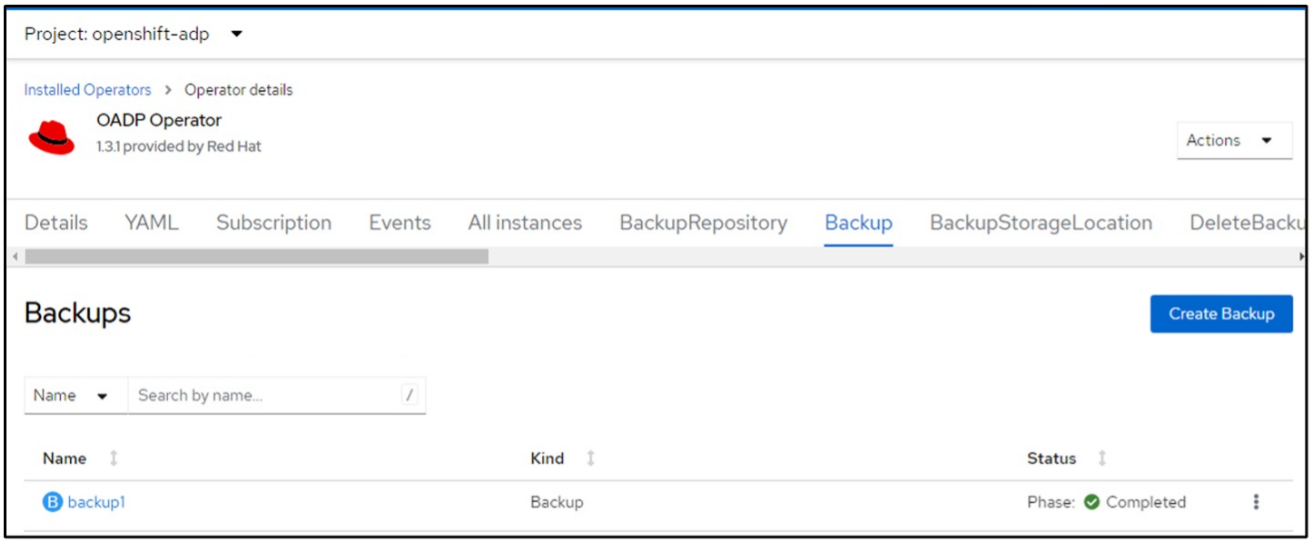


Ripristinare in una classe di archiviazione diversa

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.

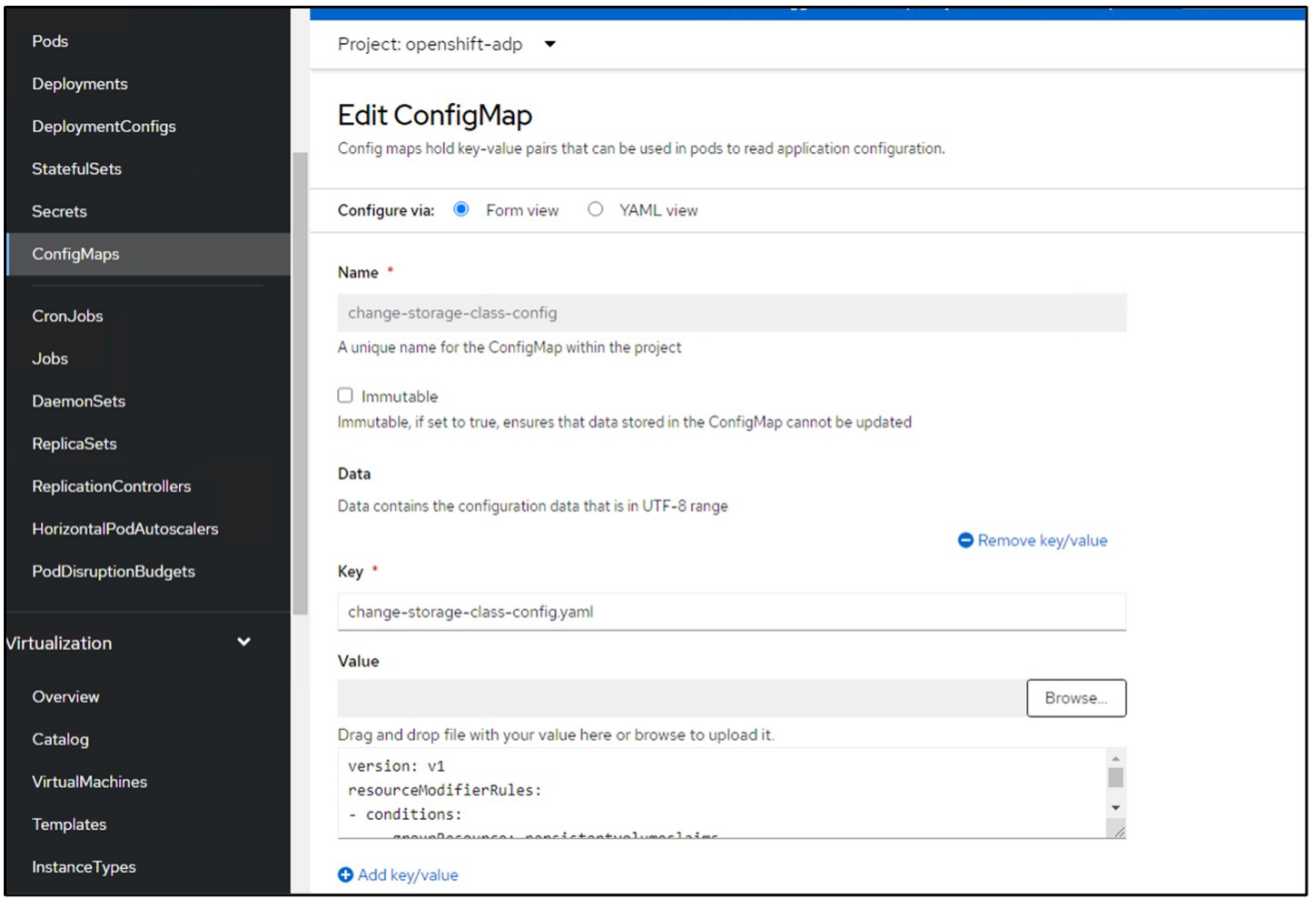
Per ripristinare la macchina virtuale utilizzando una classe di storage diversa, ad esempio ontap-nas-eco storage, devi effettuare i due seguenti passaggi:

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"
```



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>
```

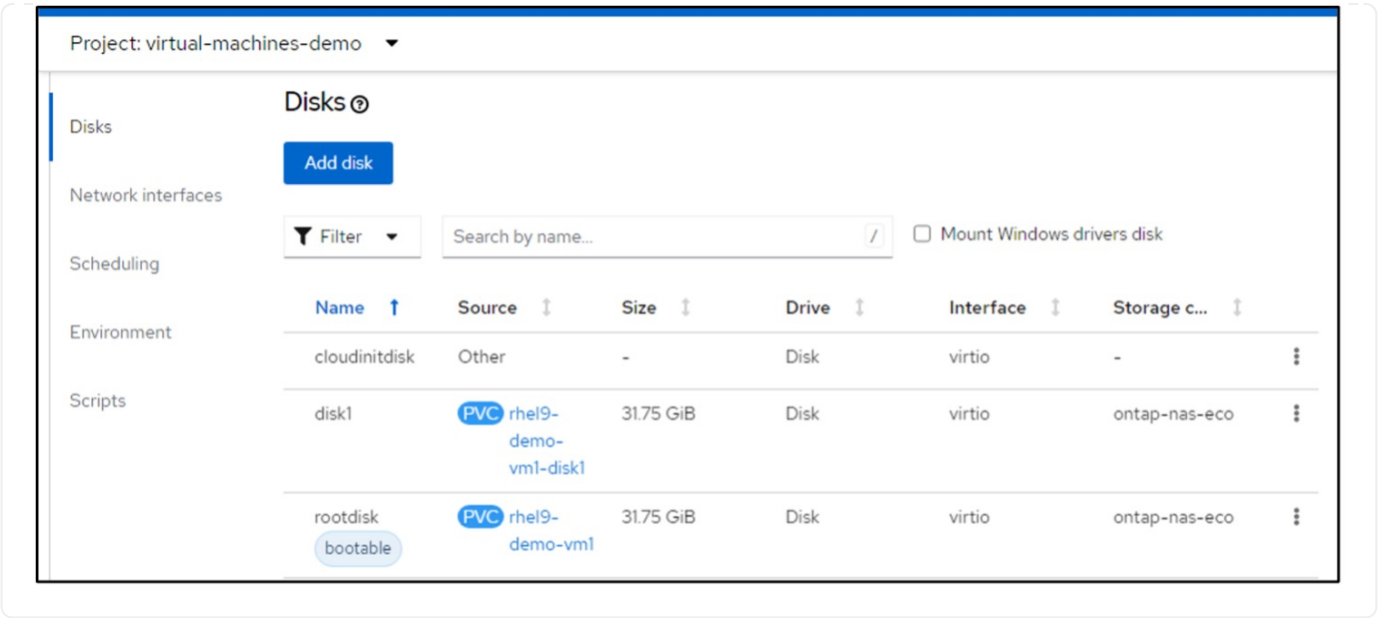
Questa mappa di configurazione applicherà la regola del modificatore di risorse quando viene creato il ripristino. Verrà applicata una patch per sostituire il nome della classe storage in ontap-nas-eco per tutte le richieste di volume persistenti a partire da rhel.

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

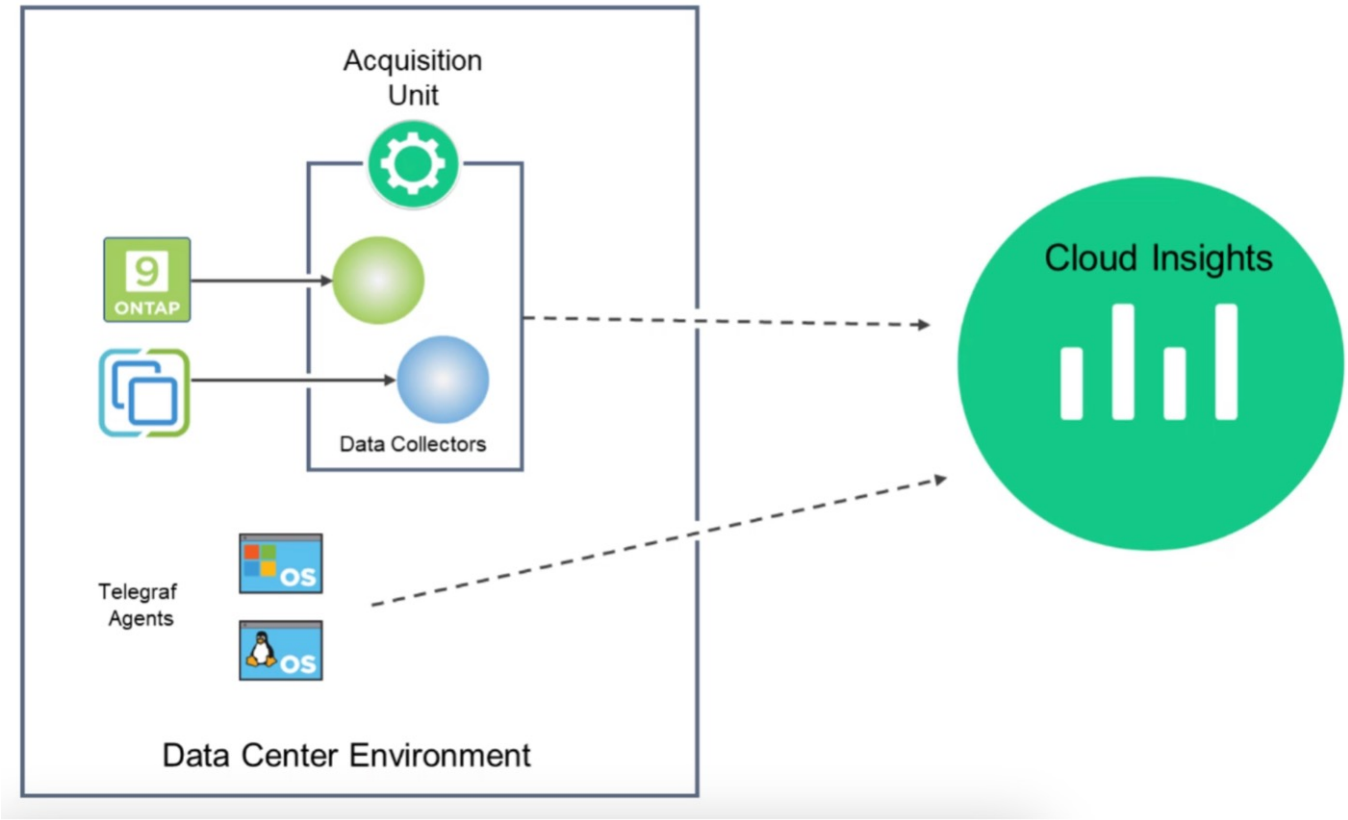
Data Collector
Esistono 3 tipi di Data Collector:
* Infrastruttura (dispositivi di storage, switch di rete, infrastruttura di elaborazione)
* Sistemi operativi (come VMware o Windows)
* Servizi (come Kafka)

I Data Collector rilevano le informazioni provenienti dalle origini dati, ad esempio il dispositivo di archiviazione ONTAP (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:

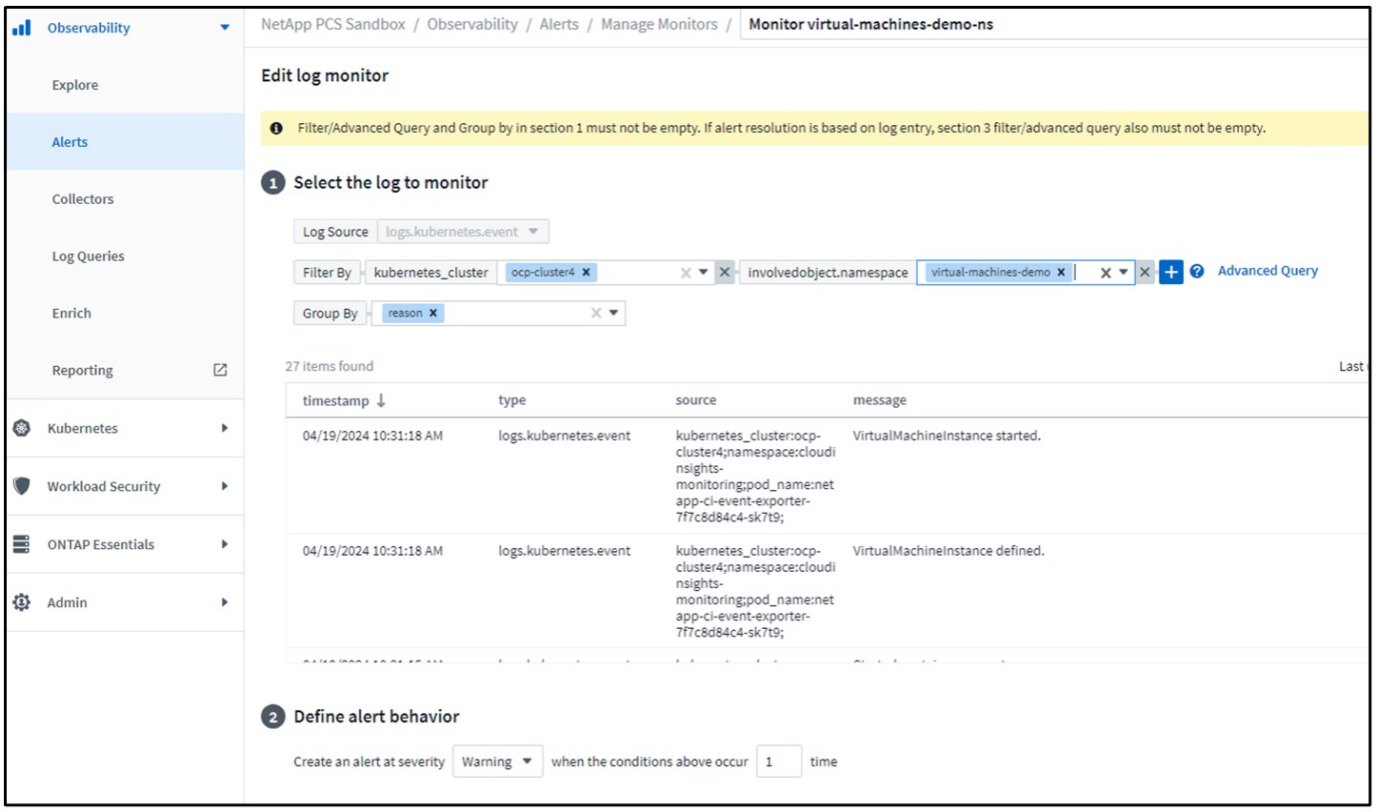
1. Un operatore di monitoring e un data collector Kubernetes per raccogliere i dati Kubernetes
   Per istruzioni complete, fare riferimento a. "documentazione".
2. Un'unità di acquisizione per raccogliere dati dallo storage ONTAP che fornisce storage persistente per i dischi delle macchine virtuali
   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

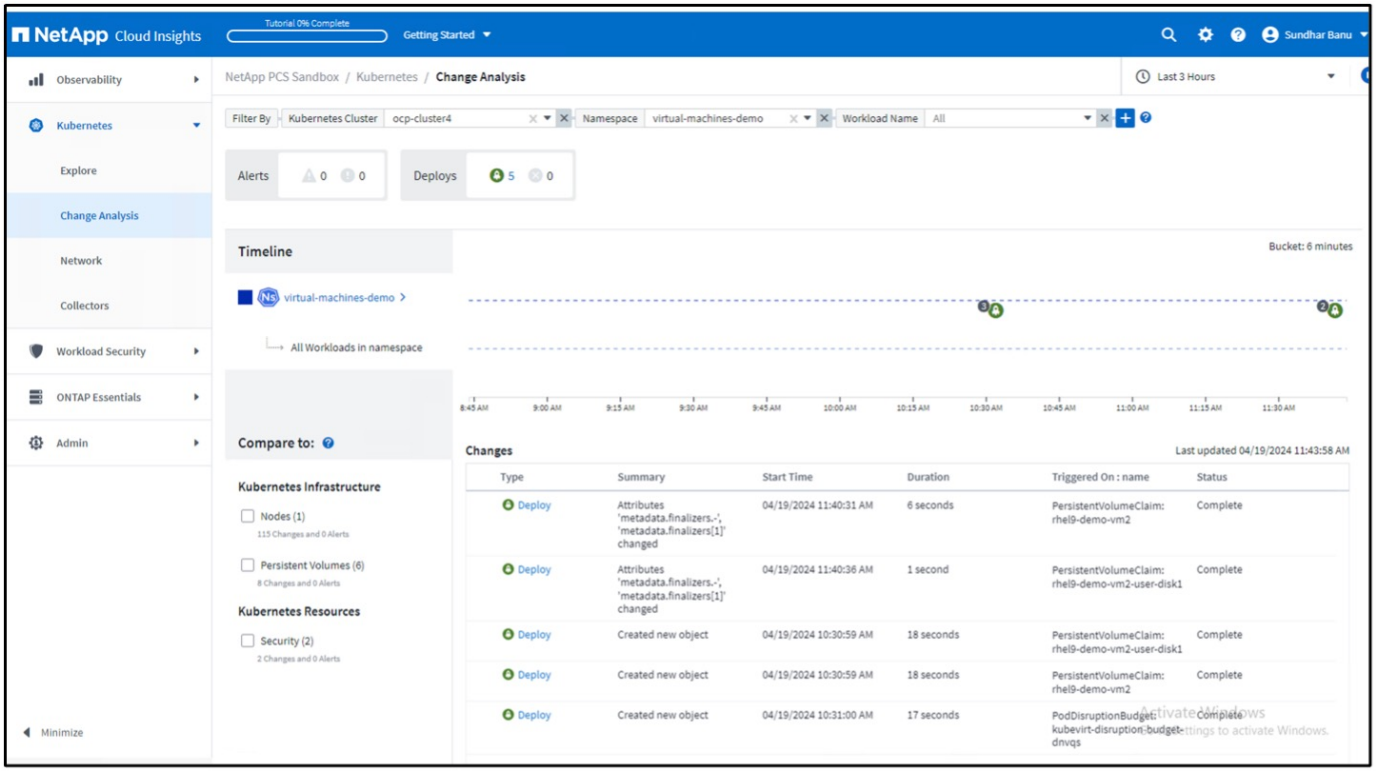
Di seguito viene riportato un esempio in cui lo spazio dei nomi che contiene una VM in OpenShift Virtualization viene monitorato in base agli eventi. In questo esempio, viene creato un monitor in base all'evento **logs.kuPand** per lo spazio dei nomi specificato nel cluster.



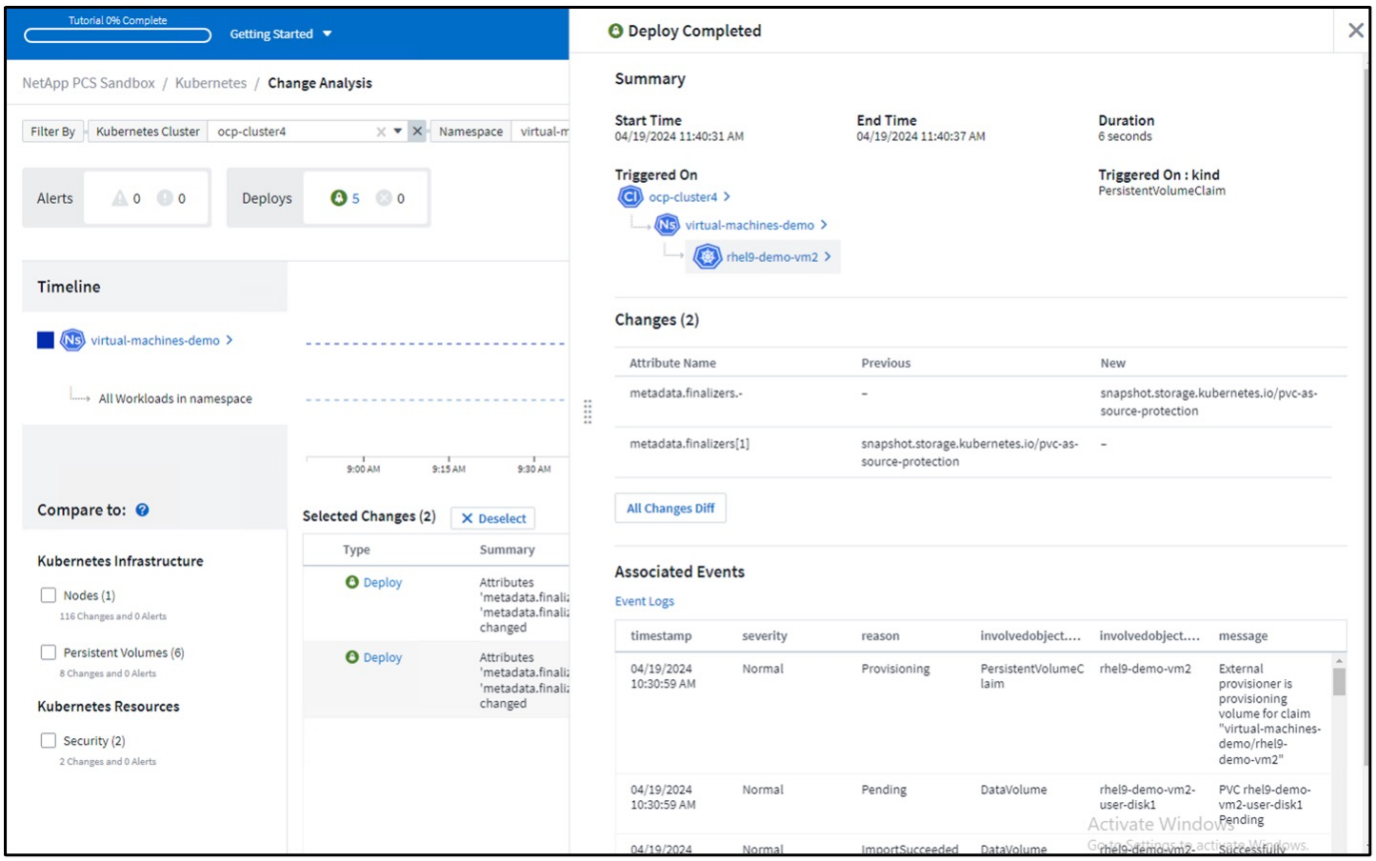
Questa query fornisce tutti gli eventi per la macchina virtuale nello spazio dei nomi. (Esiste una sola macchina virtuale nello spazio dei nomi). Una query avanzata può anche essere costruita per filtrare in base all'evento in cui il motivo è "fallito" o "non riuscito". Questi eventi vengono in genere creati quando si verifica un problema nella creazione di un PV o nel montaggio del PV su un pod che indica problemi nel provisioner dinamico per la creazione di dati persistenti dei volumi per la macchina virtuale.
Durante la creazione del monitoraggio degli avvisi, come illustrato sopra, è anche possibile configurare la notifica ai destinatari. È inoltre possibile fornire azioni correttive o informazioni aggiuntive utili per risolvere l'errore. Nell'esempio precedente, informazioni aggiuntive potrebbero essere la ricerca della configurazione di back-end Trident e delle definizioni delle classi di storage per la risoluzione del problema.

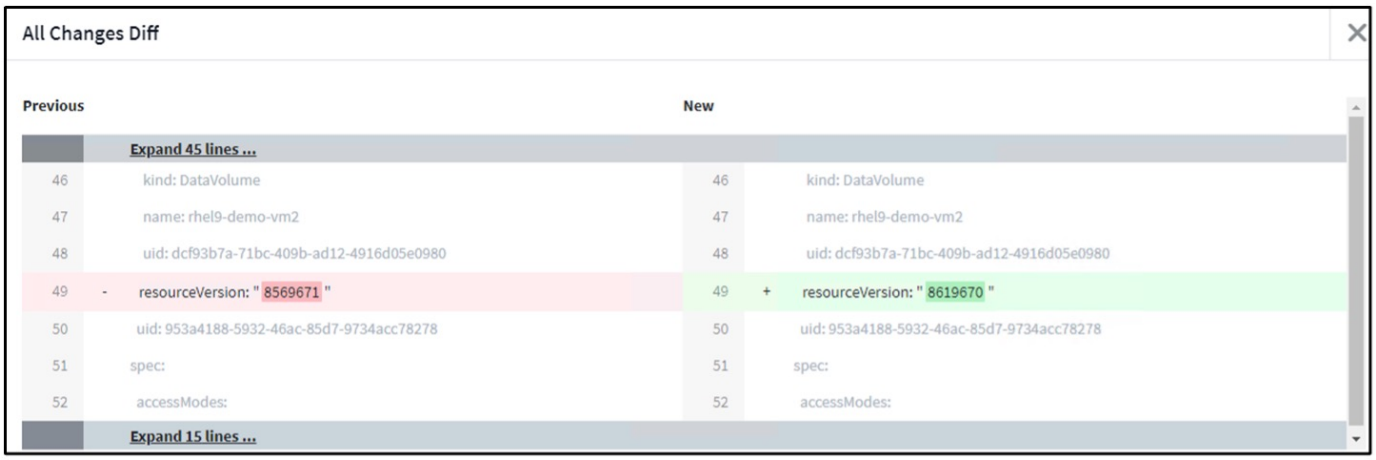
Cambia analisi

Con Change Analytics, è possibile ottenere una panoramica delle modifiche apportate allo stato del cluster, incluse le persone che hanno apportato tale modifica, che possono contribuire alla risoluzione dei problemi.



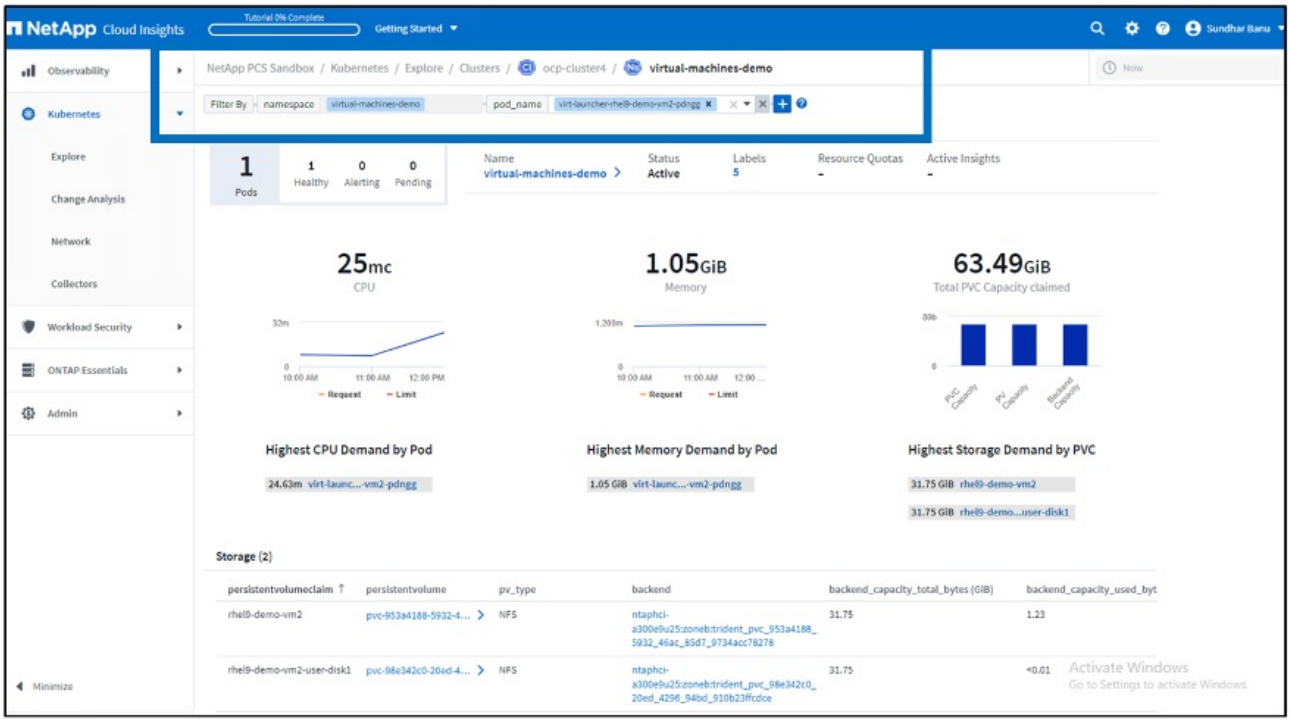
Nell'esempio precedente, Change Analysis è configurato sul cluster OpenShift per lo spazio dei nomi che contiene una VM di virtualizzazione OpenShift. Il dashboard mostra le modifiche rispetto alla timeline. Si può drill-down per vedere cosa è cambiato e fare clic su tutte le modifiche Diff per vedere la diff dei manifesti. Dal manifesto, è possibile vedere che è stato creato un nuovo backup dei dischi permanenti.



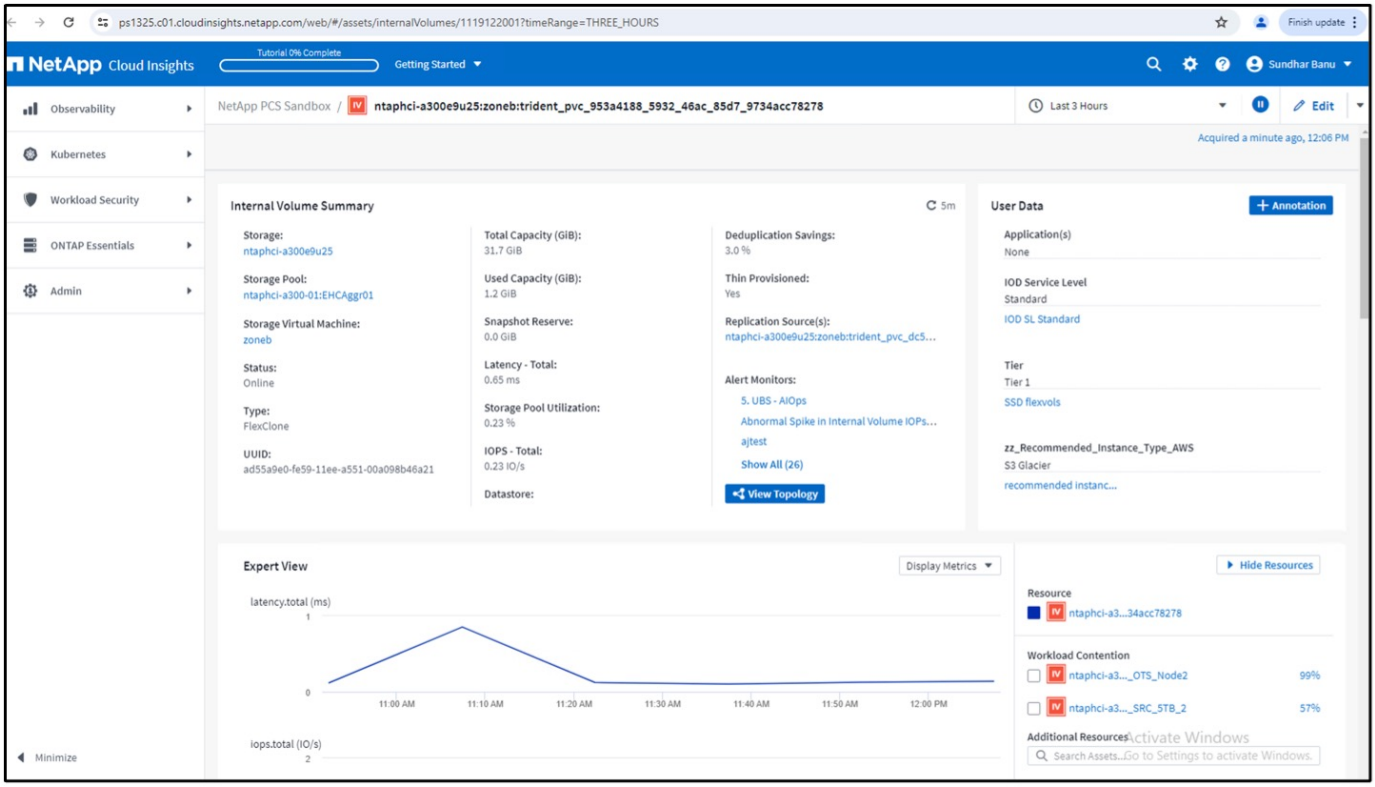


Mappatura archiviazione backend

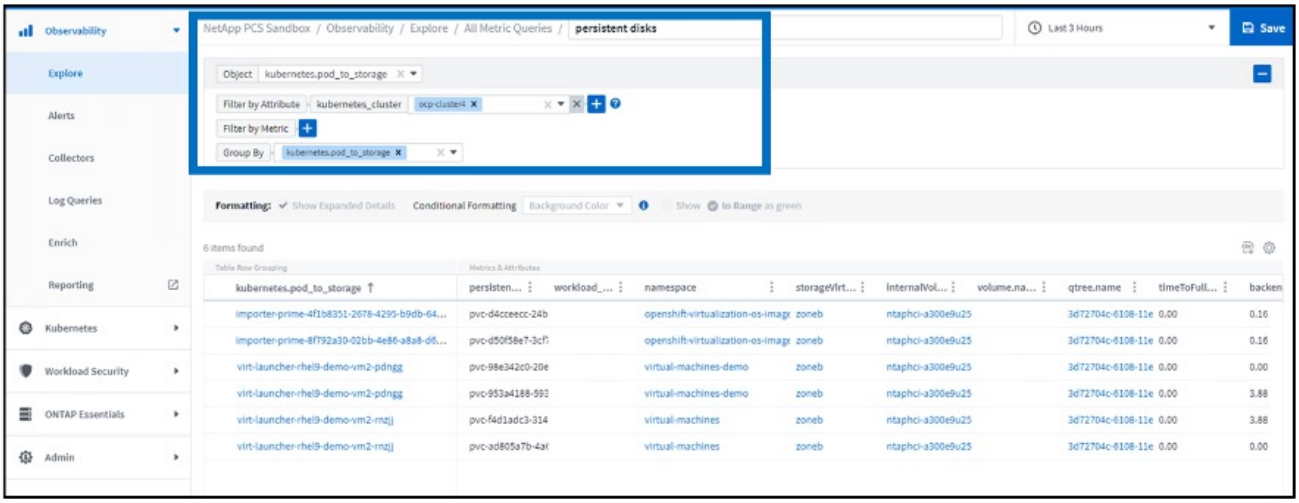
Con Cloud Insights, è possibile vedere facilmente lo storage backend dei dischi della macchina virtuale e le diverse statistiche sui PVC.



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

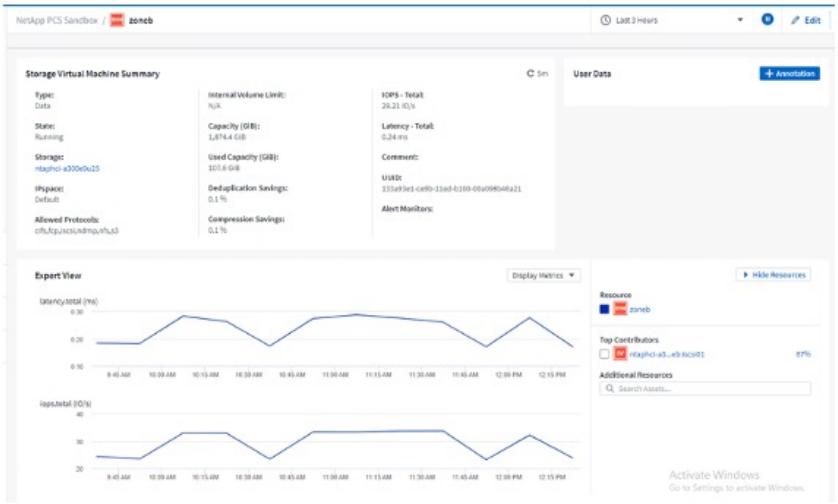


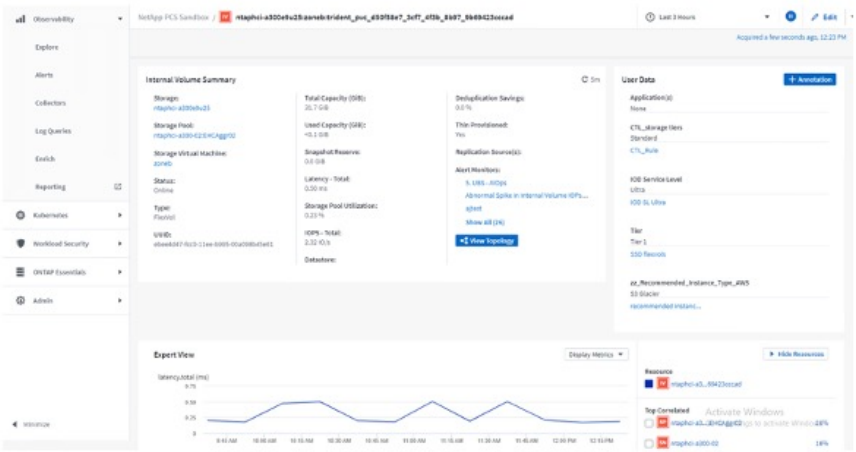
Un altro modo per esaminare tutte le mappature pod-storage è creare una query All Metrics dal menu Observability (osservabilità) in Explore (Esplora).



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

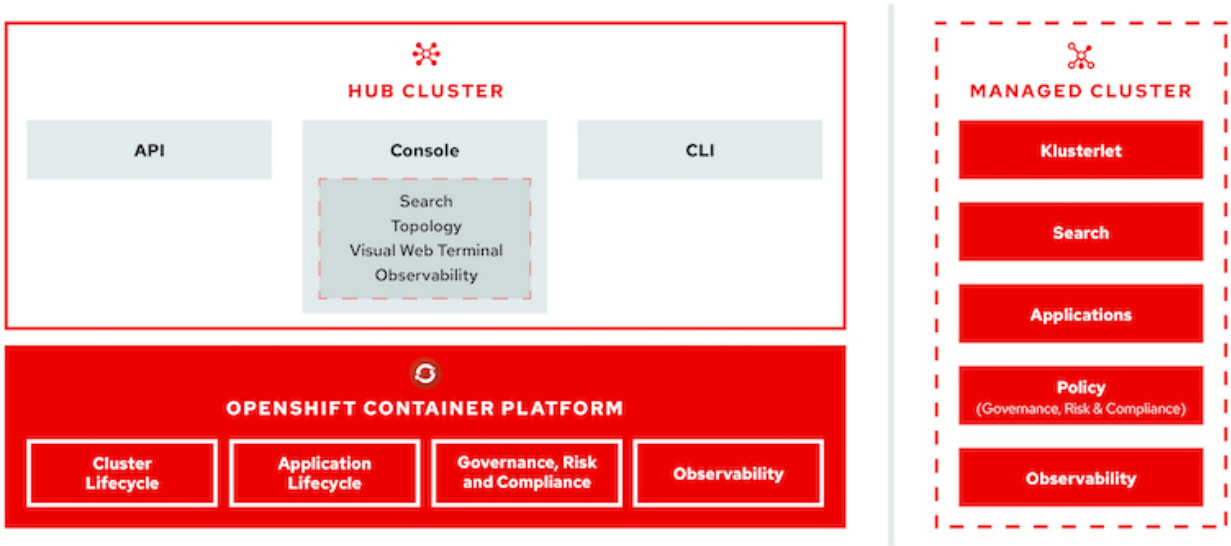
Gestione avanzata dei cluster per Kubernetes: Red Hat OpenShift con NetApp

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

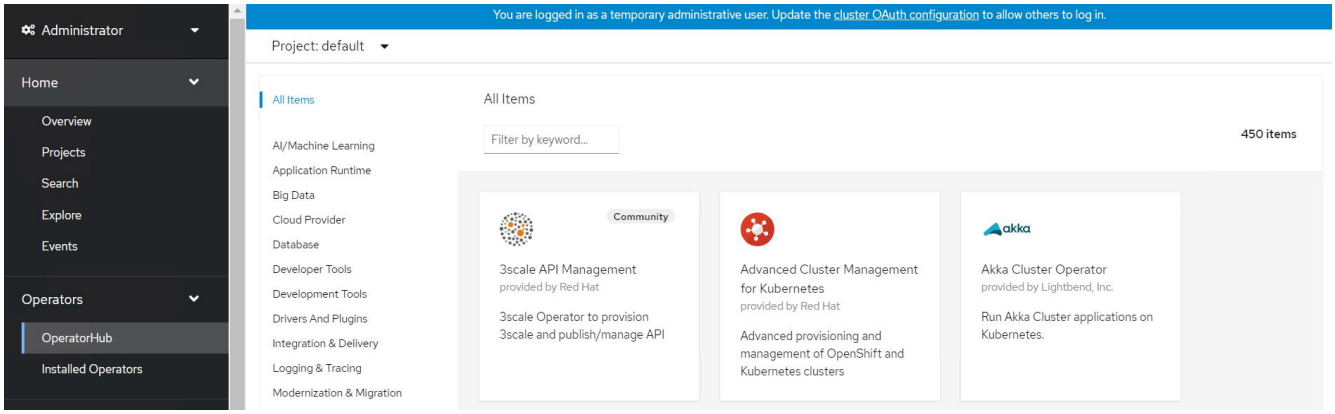
Advanced Cluster Management è un add-on per il cluster OpenShift, pertanto esistono determinati requisiti e restrizioni sulle risorse hardware in base alle funzionalità utilizzate nell'hub e nei cluster gestiti. È necessario tenere conto di questi problemi durante il dimensionamento dei cluster. Consultare 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).

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).

OperatorHub > Operator Installation

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.

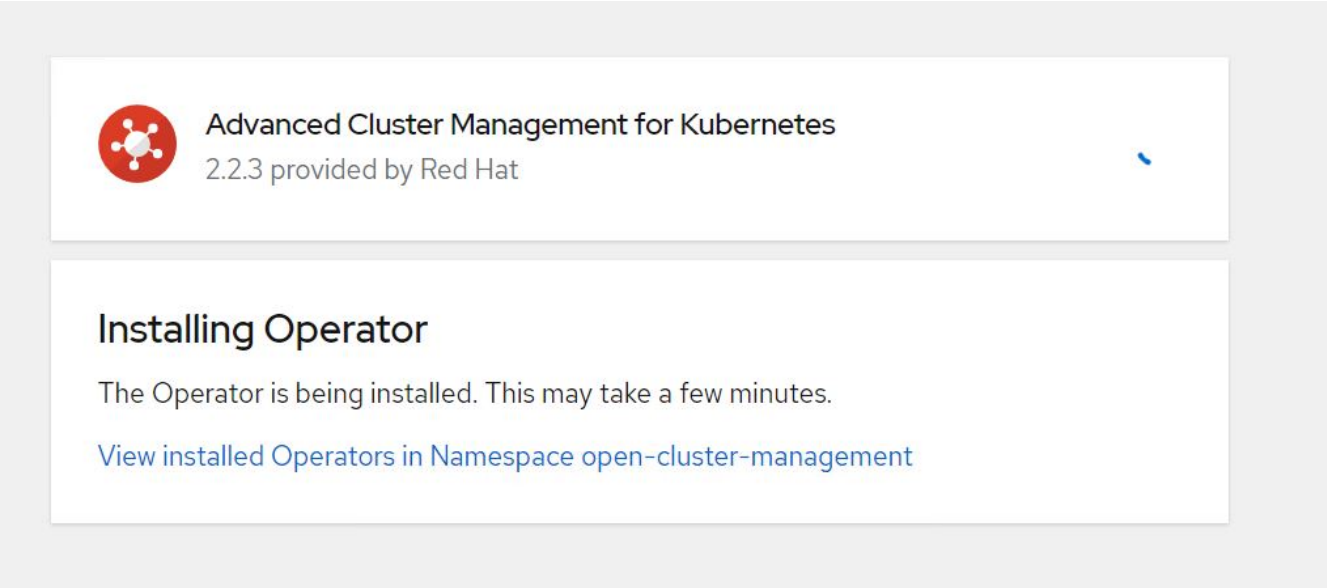
- ○ Select a Namespace

Approval strategy *

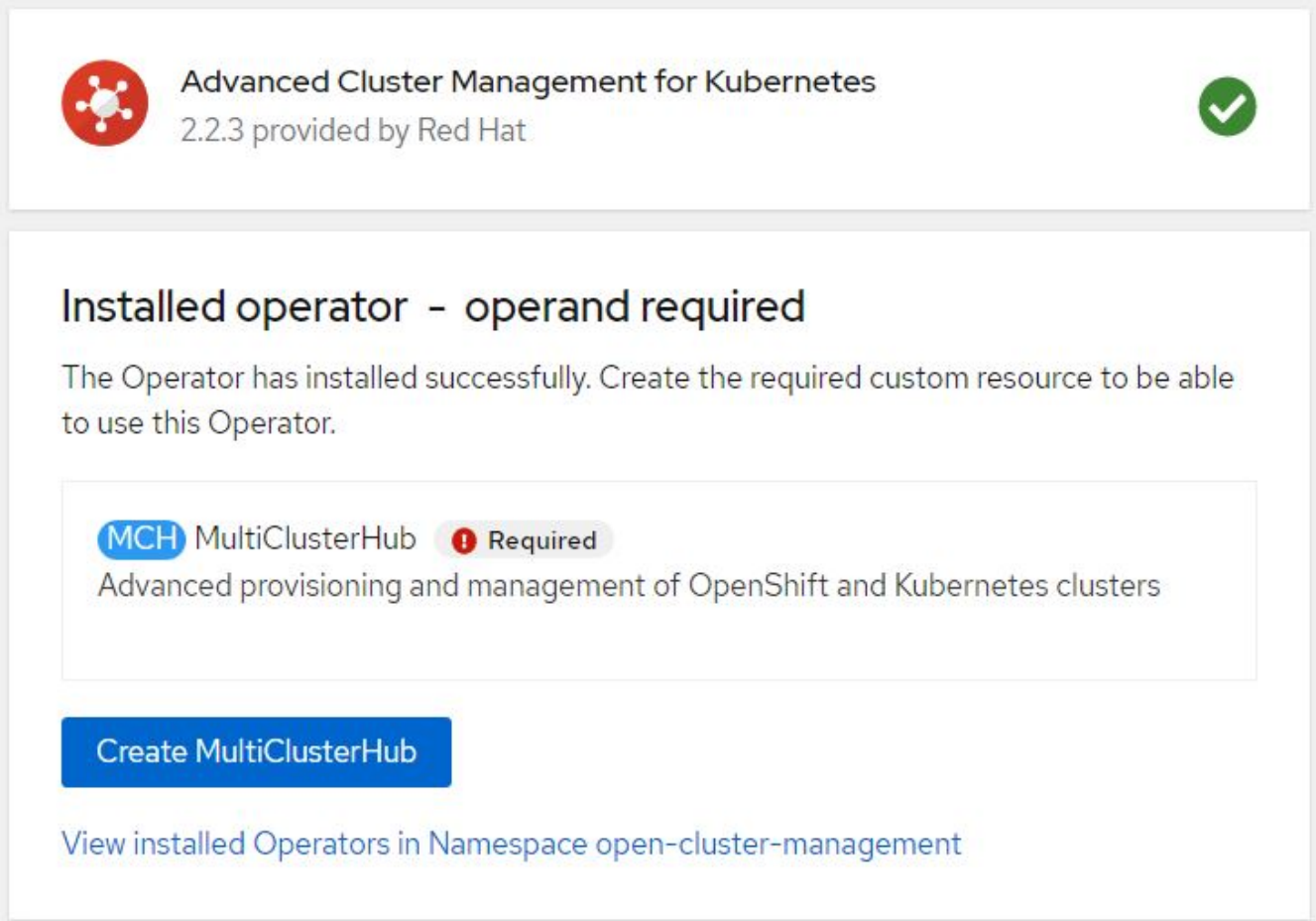
- ◉ Automatic
- ○ Manual

Install Cancel

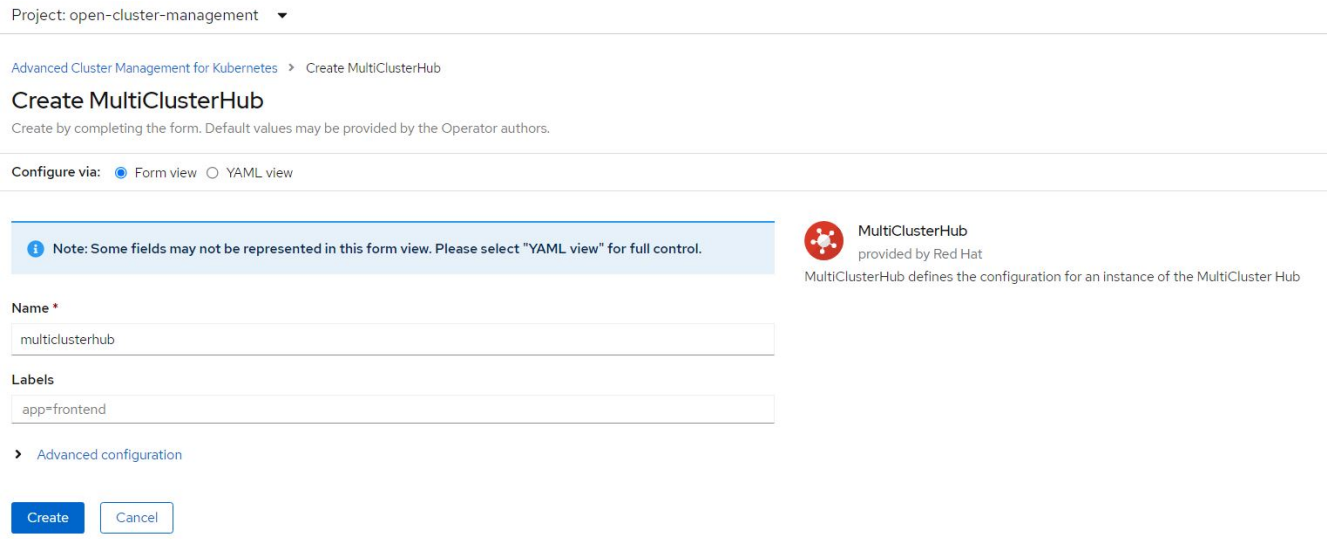
5. Attendere il completamento dell'installazione da parte dell'operatore.



6. Una volta installato l'operatore, fare clic su Create MultiClusterHub (Crea MultiClusterHub).



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.



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.

Project: open-cluster-management

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
Advanced Cluster Management for Kubernetes 2.2.3 provided by Red Hat	NS open-cluster-management	Succeeded Up to date	MultiClusterHub ClusterManager ClusterDeployment ClusterState View 25 more...

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
MCH multiclusterhub	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.

Project: open-cluster-management

Routes

Create Route

Filter | Name | mul

Name mul ✕ | Clear all filters

Name	Status	Location	Service
RT multicloud-console	Accepted	https://multicloud-console.apps.ocp-vmware2.cie.netapp.com	S management-ingress

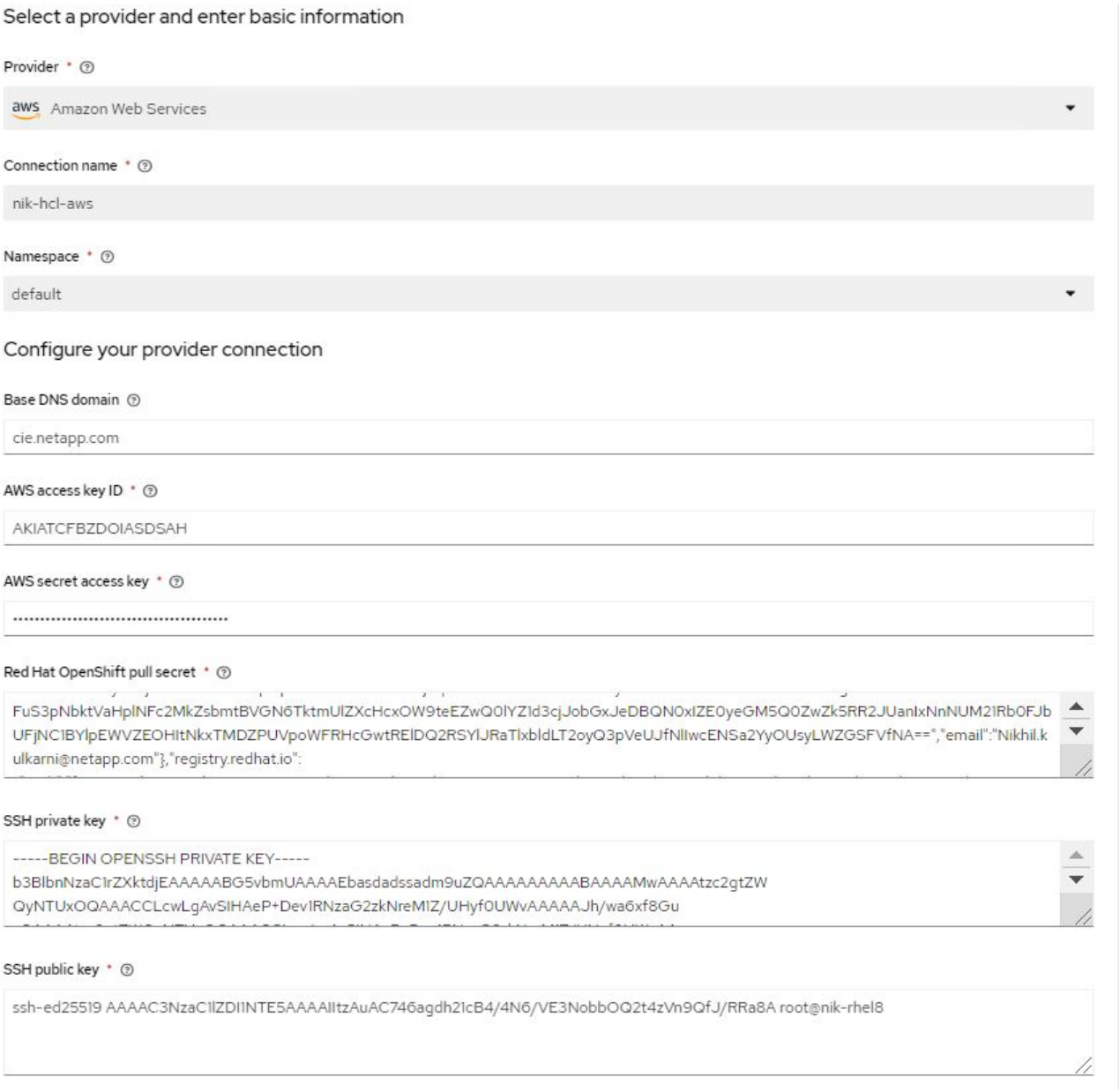
Caratteristiche

Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

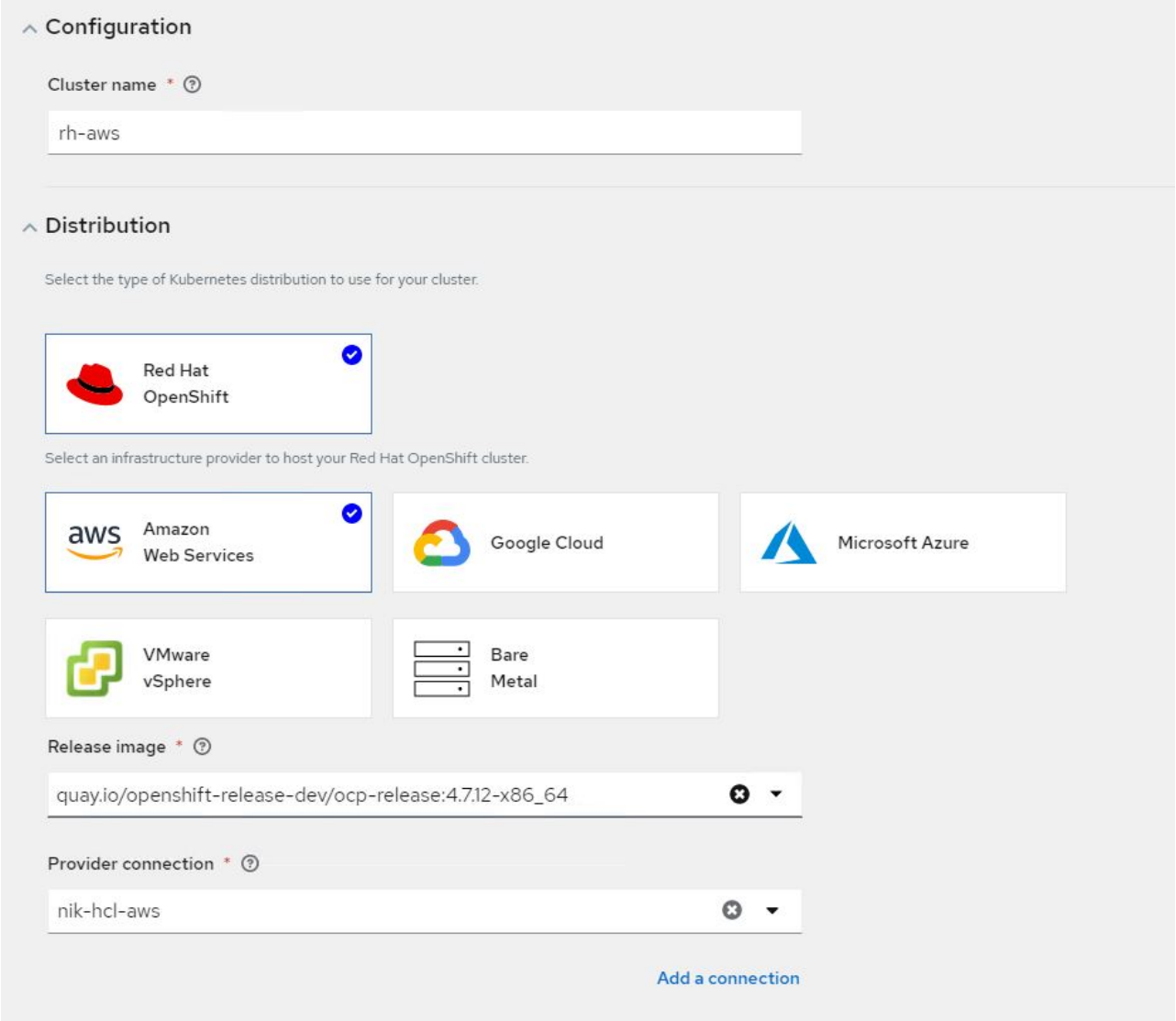
Gestione del ciclo di vita del cluster

Per gestire diversi cluster OpenShift, è possibile crearli o importarli in Advanced Cluster Management.

1. Prima di tutto, automatizza le infrastrutture > Clusters.
2. Per creare un nuovo cluster OpenShift, attenersi alla seguente procedura:
   a. Creare una connessione al provider: Accedere a connessioni provider e fare clic su Aggiungi una connessione, fornire tutti i dettagli corrispondenti al tipo di provider selezionato e fare clic su Aggiungi.

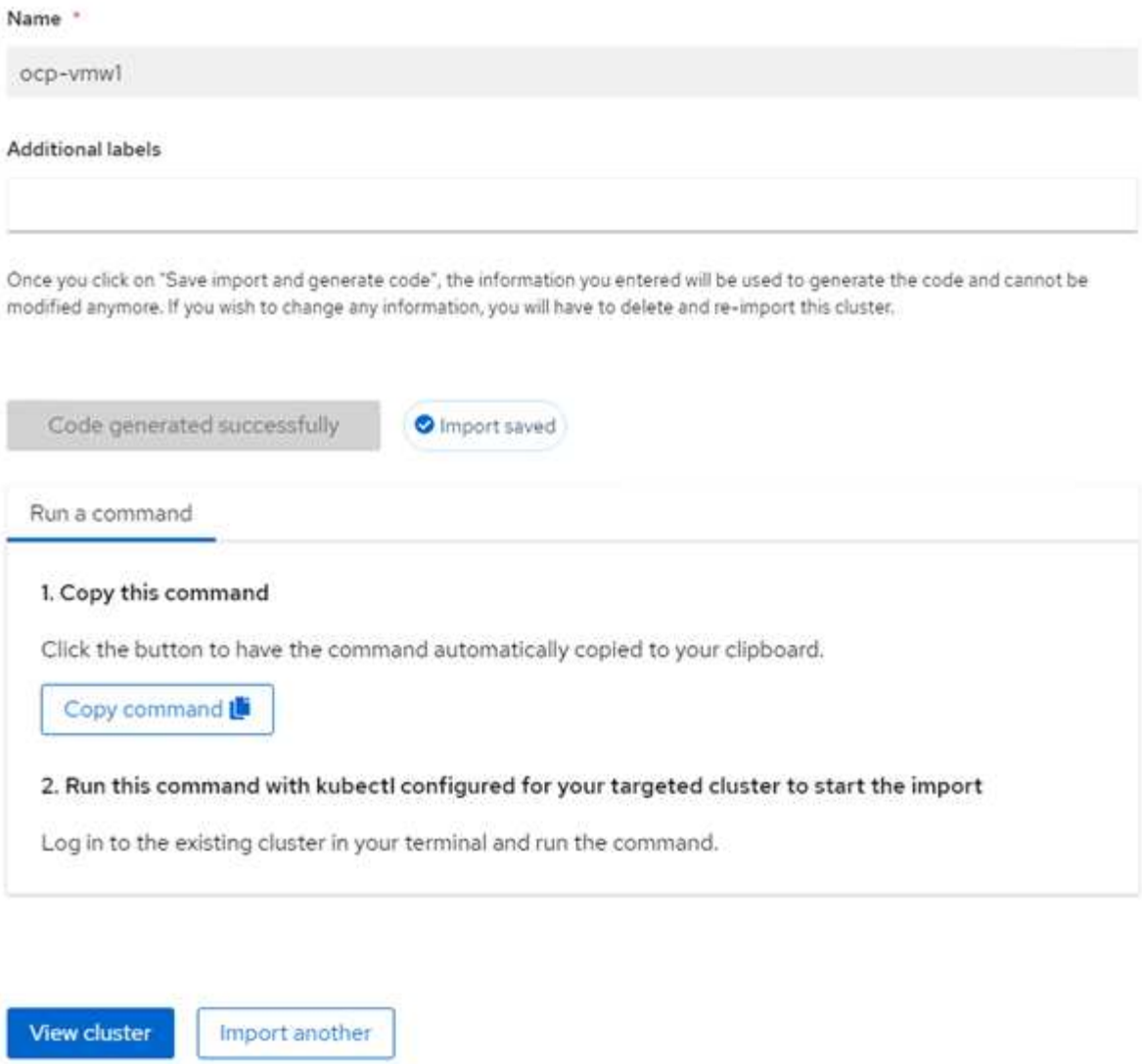


   b. Per creare un nuovo cluster, accedere a Clusters e fare clic su Add a Cluster (Aggiungi cluster) > Create a Cluster (Crea cluster). Fornire i dettagli del cluster e del provider corrispondente, quindi fare clic su Create (Crea).



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.



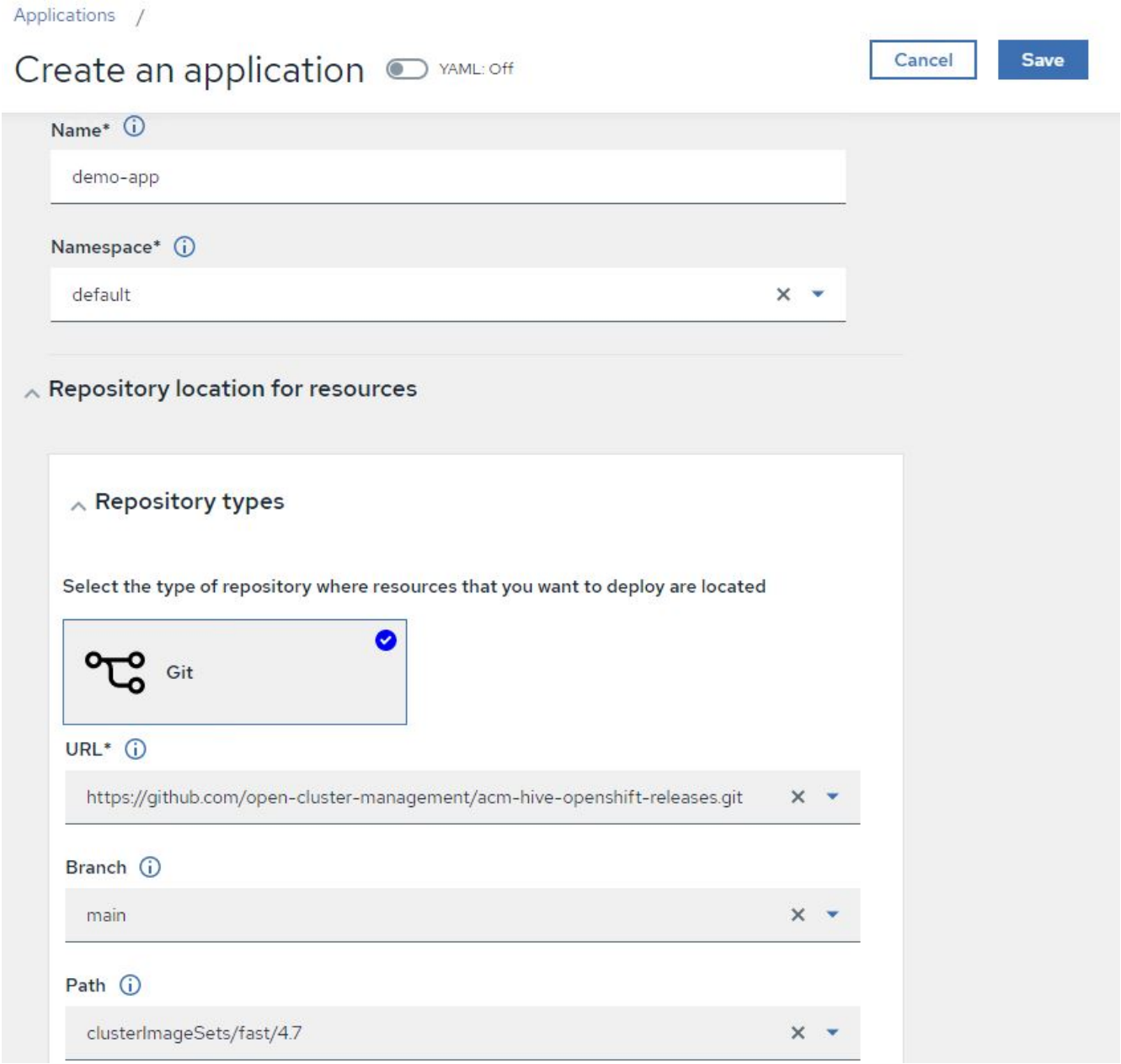
4. Dopo aver creato e importato più cluster, è possibile monitorarli e gestirli da una singola console.

Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

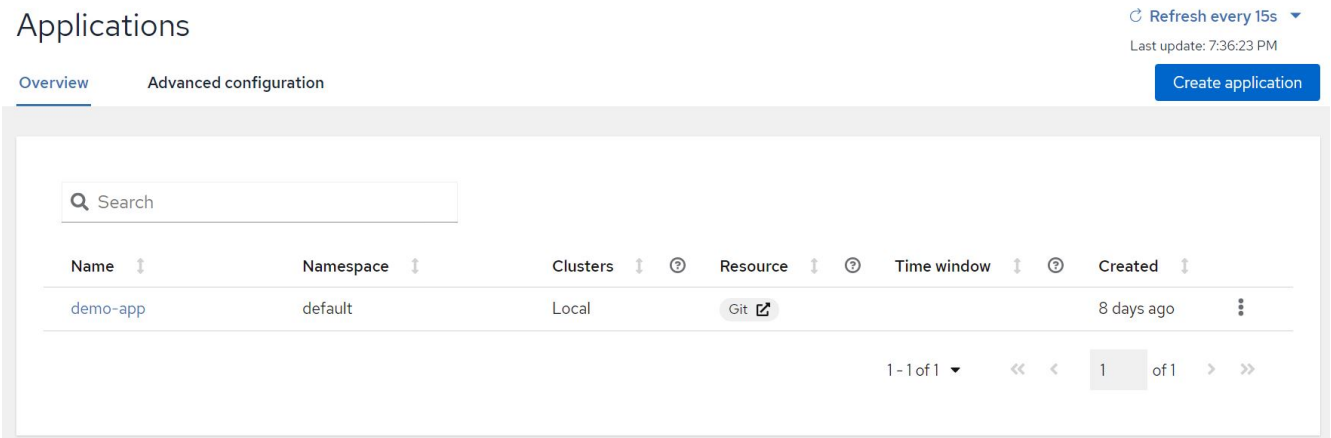
Gestione del ciclo di vita dell’applicazione

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).



2. Una volta installati i componenti dell'applicazione, l'applicazione viene visualizzata nell'elenco.

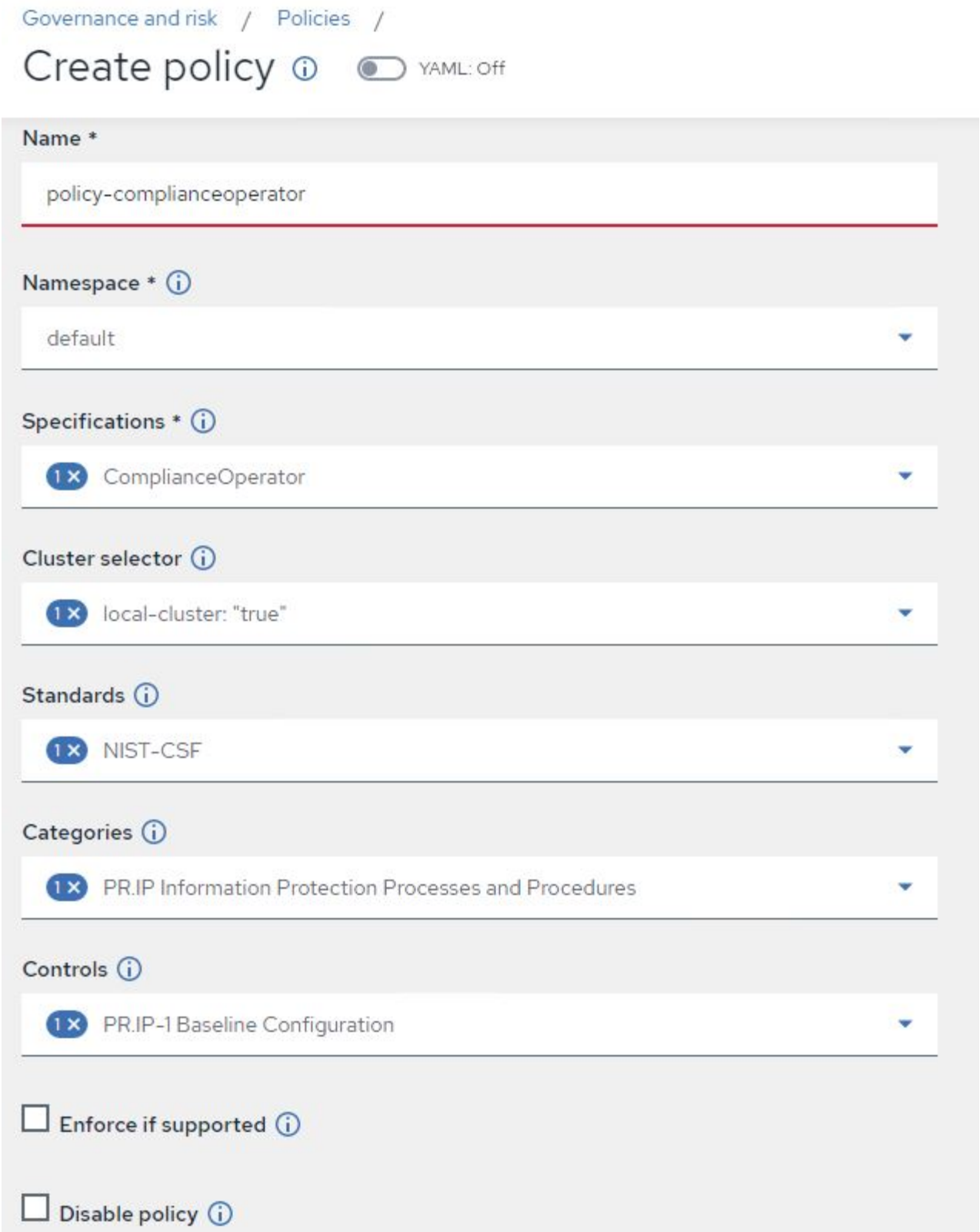


3. L'applicazione può ora essere monitorata e gestita dalla console.

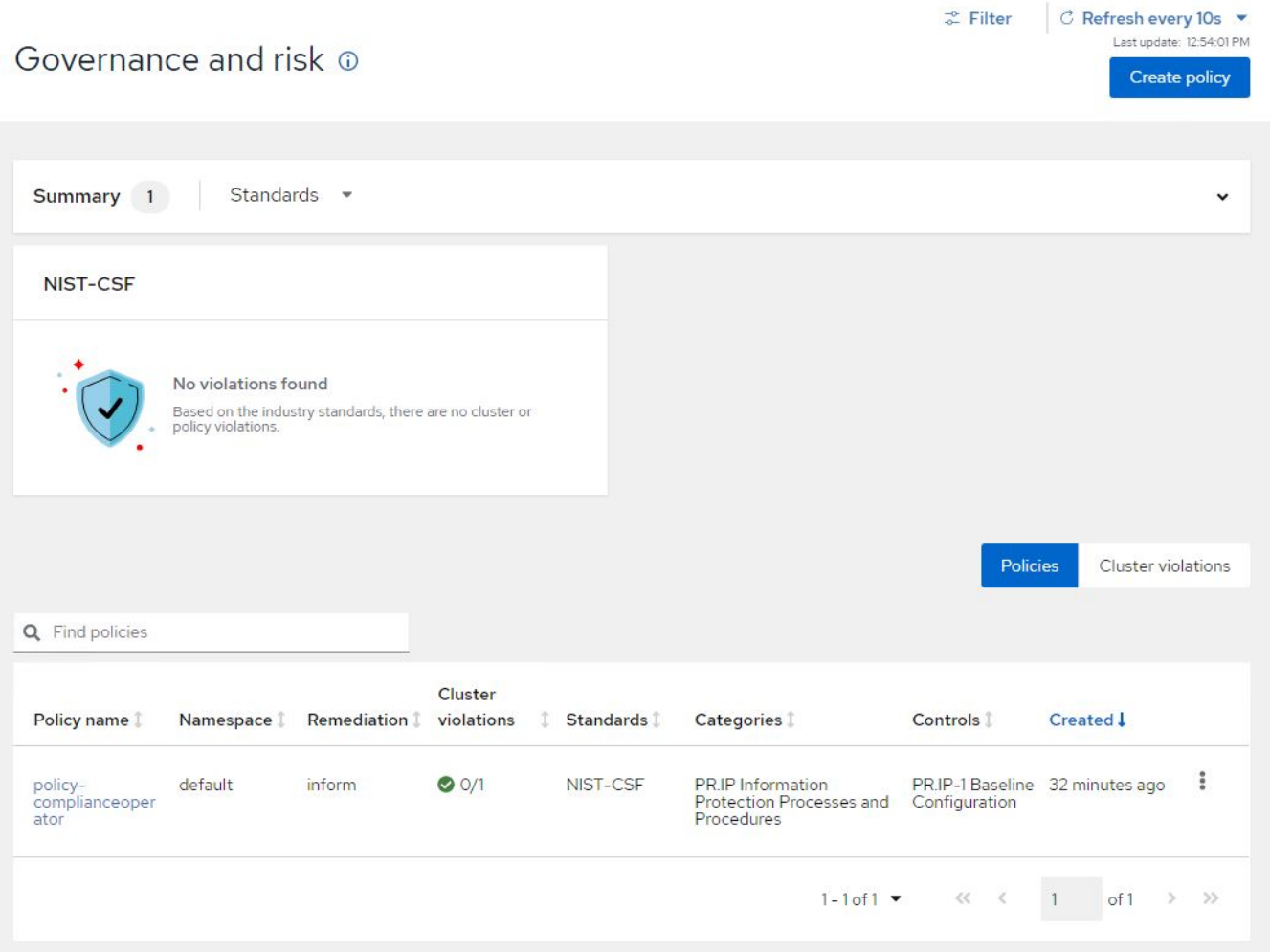
Governance e rischi

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.



3. Dopo aver configurato tutti i criteri richiesti, è possibile monitorare e correggere eventuali violazioni di policy o cluster da Advanced Cluster Management.

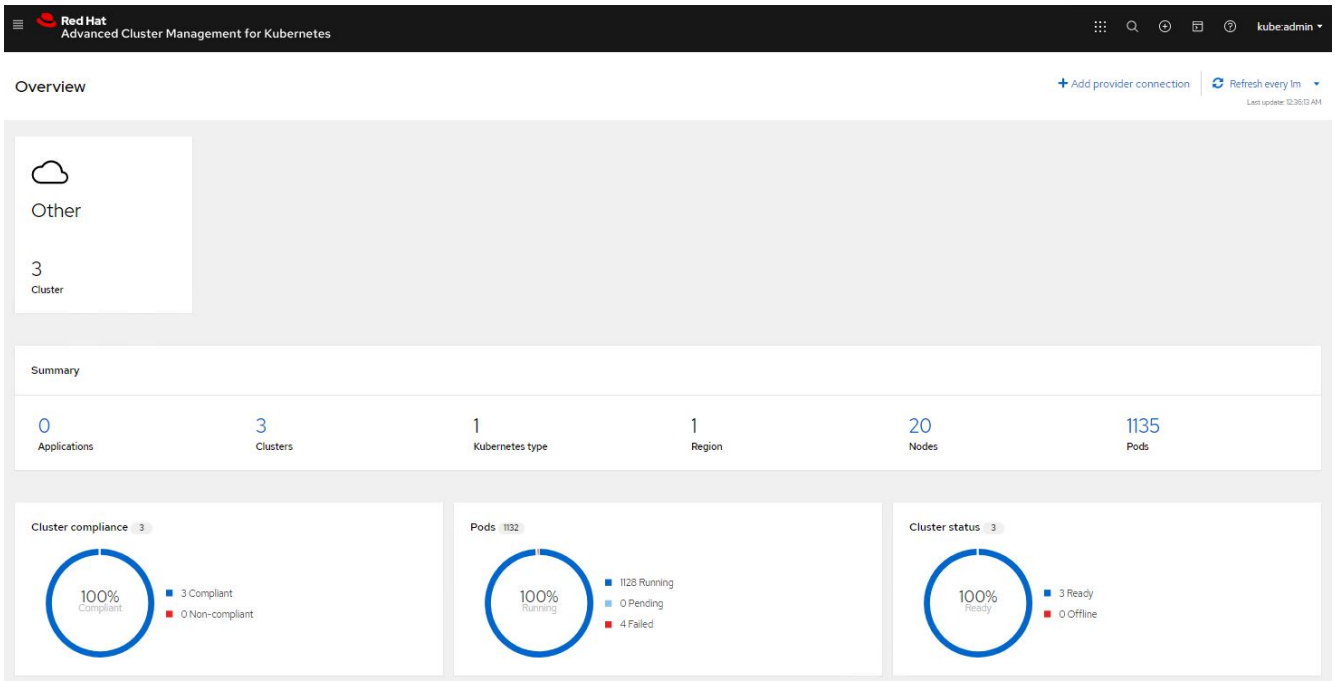


Funzionalità: Gestione avanzata dei cluster per Kubernetes su Red Hat OpenShift con NetApp

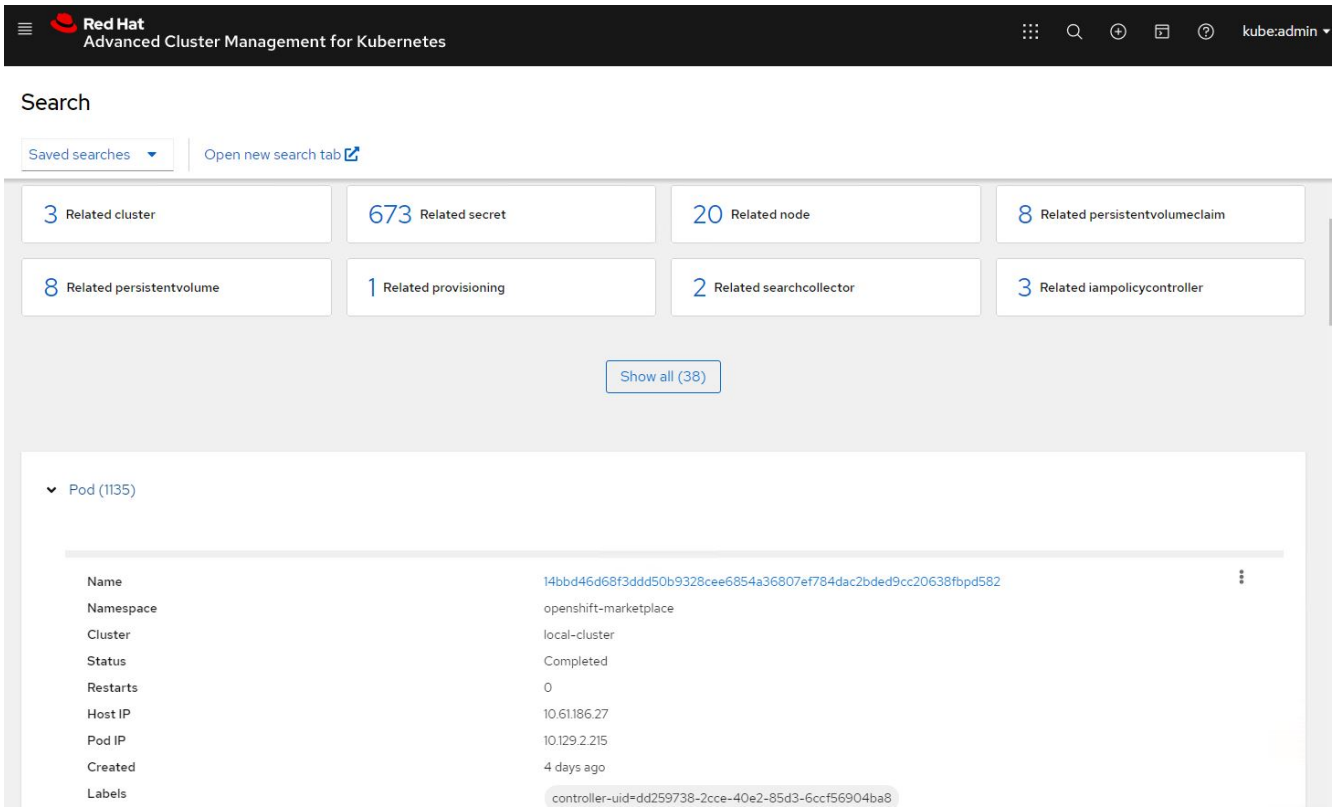
Osservabilità

La gestione avanzata dei cluster per Kubernetes consente di monitorare nodi, pod, applicazioni e carichi di lavoro in tutti i cluster.

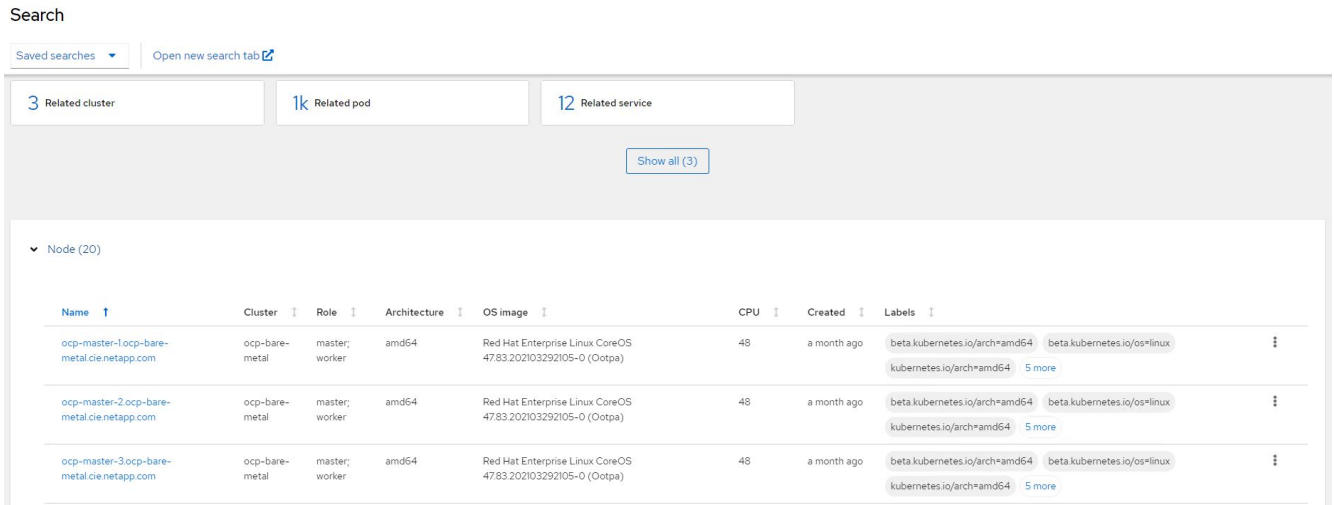
1. Accedere a osservare gli ambienti > Panoramica.



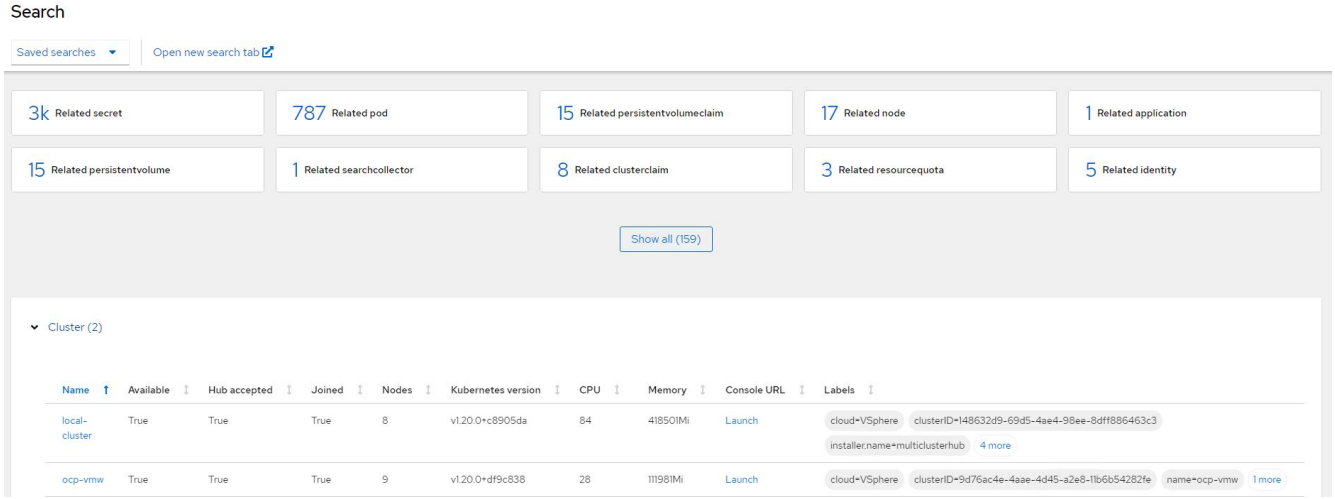
2. Tutti i pod e i carichi di lavoro di tutti i cluster vengono monitorati e ordinati in base a una varietà di filtri. Fare clic su Pod per visualizzare i dati corrispondenti.



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.



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.



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 × local-cluster, ocp-vmw

Resource configuration | Enter the configuration manifest for the resource(s).

YAML

```yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: demo-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ocp-trident
```