Protégez vos données à l'aide d'outils tiers

NetApp virtualization solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions-virtualization/openshift/osv-vm-dp-using-velero-overview.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommaire

Protégez vos données à l'aide d'outils tiers . . . 1
En savoir plus sur la protection des données pour les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide d'OpenShift API for Data Protection (OADP) . . . 1
Installer l'opérateur Red Hat OpenShift API for Data Protection (OADP) . . . 3
Prérequis . . . 3
Étapes d'installation de l'opérateur OADP . . . 4
Créer une sauvegarde à la demande pour les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide de Velero . . . 13
Étapes pour créer une sauvegarde d'une machine virtuelle . . . 13
Création de sauvegardes planifiées pour les machines virtuelles dans OpenShift Virtualization . . . 15
Restaurer une machine virtuelle à partir d'une sauvegarde dans Red Hat OpenShift Virtualization à l'aide de Velero . . . 16
Prérequis . . . 17
Supprimer un CR de sauvegarde ou restaurer un CR dans Red Hat OpenShift Virtualization à l'aide de Velero . . . 23
Supprimer une sauvegarde . . . 23
Suppression d'une restauration . . . 23

Protégez vos données à l'aide d'outils tiers

En savoir plus sur la protection des données pour les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide d'OpenShift API for Data Protection (OADP)

OpenShift API for Data Protection (OADP) avec Velero fournit des fonctionnalités de sauvegarde, de restauration et de reprise après sinistre pour les machines virtuelles dans OpenShift Virtualization. Utilisez les snapshots Trident CSI pour sauvegarder les volumes persistants et les métadonnées de machine virtuelle sur NetApp ONTAP S3 ou StorageGRID S3. OADP s'intègre aux API Velero et aux pilotes de stockage CSI pour gérer les opérations de protection des données pour les machines virtuelles conteneurisées.

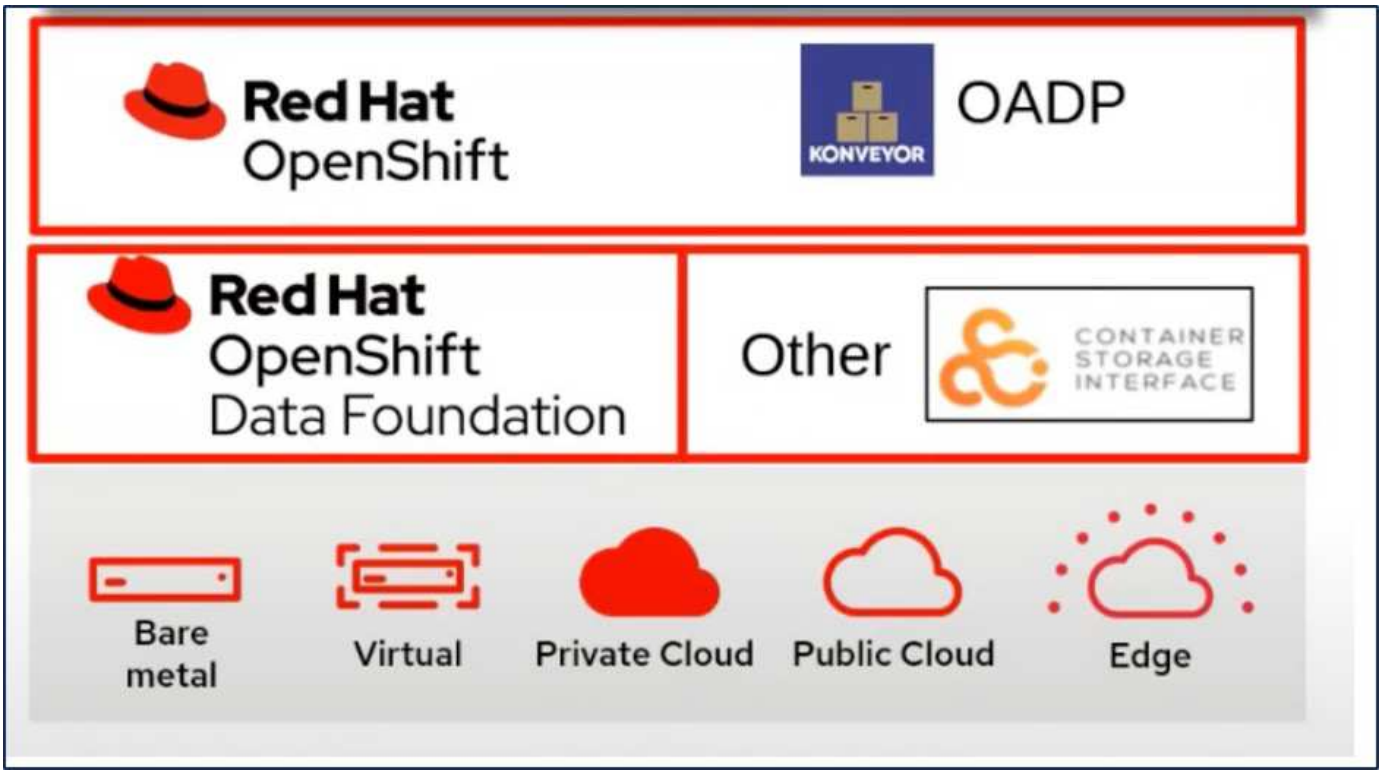
Les machines virtuelles dans l'environnement de virtualisation OpenShift sont des applications conteneurisées qui s'exécutent dans les nœuds de travail de votre plateforme OpenShift Container. Il est important de protéger les métadonnées des machines virtuelles ainsi que les disques persistants des machines virtuelles, afin que lorsqu'elles sont perdues ou corrompues, vous puissiez les récupérer.

Les disques persistants des machines virtuelles de virtualisation OpenShift peuvent être sauvegardés par le stockage ONTAP intégré au cluster OpenShift à l'aide de"Trident CSI" . Dans cette section, nous utilisons"API OpenShift pour la protection des données (OADP)" pour effectuer la sauvegarde des machines virtuelles, y compris leurs volumes de données,

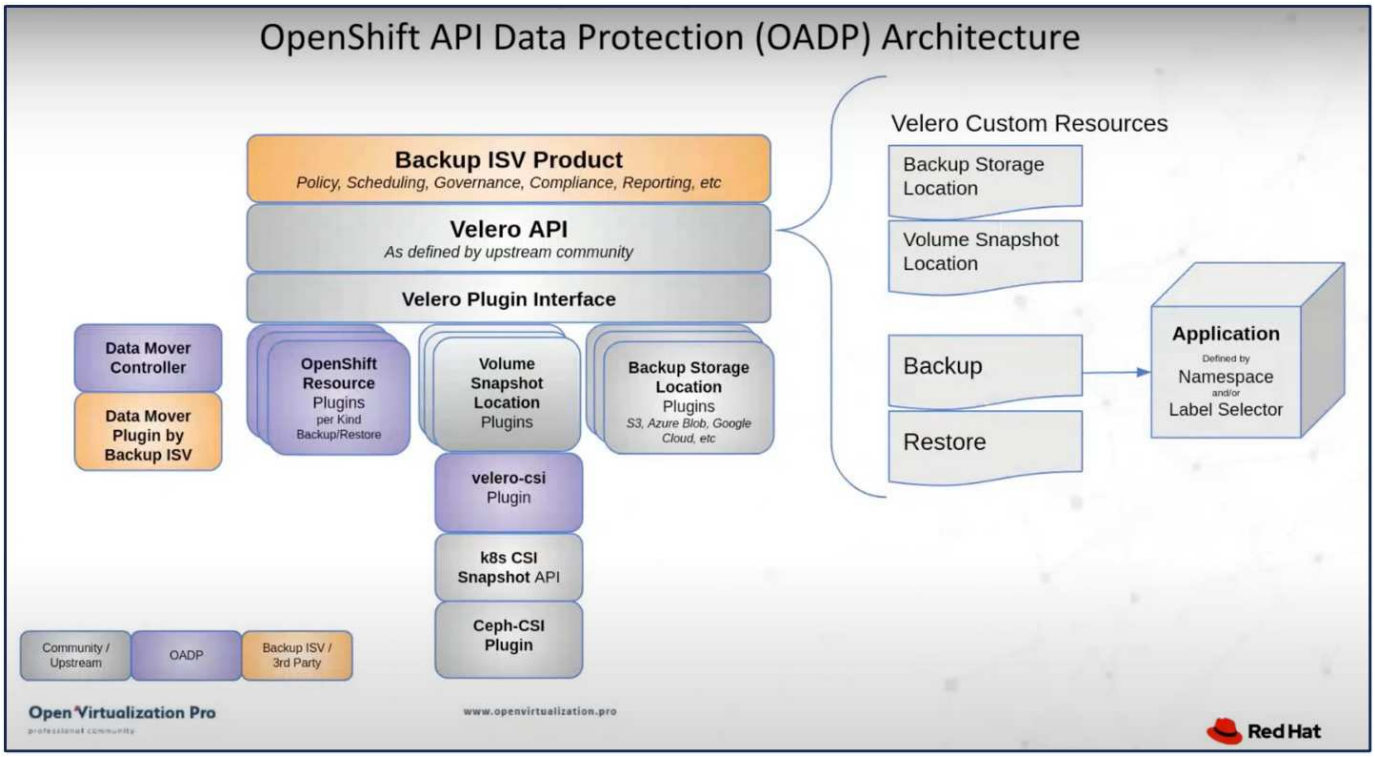
- Stockage d'objets ONTAP
- Grille de stockage

Nous restaurons ensuite à partir de la sauvegarde lorsque cela est nécessaire.

OADP permet la sauvegarde, la restauration et la reprise après sinistre des applications sur un cluster OpenShift. Les données qui peuvent être protégées avec OADP incluent les objets de ressources Kubernetes, les volumes persistants et les images internes.



Red Hat OpenShift a exploité les solutions développées par les communautés OpenSource pour la protection des données. "Velero" est un outil open source permettant de sauvegarder et de restaurer en toute sécurité, d'effectuer une reprise après sinistre et de migrer les ressources de cluster Kubernetes et les volumes persistants. Pour utiliser Velero facilement, OpenShift a développé l'opérateur OADP et le plugin Velero pour s'intégrer aux pilotes de stockage CSI. Le cœur des API OADP exposées est basé sur les API Velero. Après avoir installé l'opérateur OADP et l'avoir configuré, les opérations de sauvegarde/restauration qui peuvent être effectuées sont basées sur les opérations exposées par l'API Velero.



OADP 1.3 est disponible à partir du hub opérateur du cluster OpenShift 4.12 et versions ultérieures. Il dispose d'un Data Mover intégré qui peut déplacer des instantanés de volume CSI vers un magasin d'objets distant. Cela offre portabilité et durabilité en déplaçant les instantanés vers un emplacement de stockage d'objets pendant la sauvegarde. Les instantanés sont ensuite disponibles pour restauration après sinistre.

Voici les versions des différents composants utilisés pour les exemples de cette section

- OpenShift Cluster 4.14
- OpenShift Virtualization installé via OperatorOpenShift Virtualization Operator fourni par Red Hat
- Opérateur OADP 1.13 fourni par Red Hat
- Velero CLI 1.13 pour Linux
- Trident 24.02
- ONTAP 9.12

"Trident CSI" "API OpenShift pour la protection des données (OADP)" "Velero"

Installer l'opérateur Red Hat OpenShift API for Data Protection (OADP)

Installez l'opérateur OpenShift API for Data Protection (OADP) pour activer les fonctionnalités de sauvegarde et de restauration des machines virtuelles dans OpenShift Virtualization. Cette procédure comprend le déploiement de l'opérateur OADP à partir d'OpenShift Operator Hub, la configuration de Velero pour utiliser NetApp ONTAP S3 ou StorageGRID comme cible de sauvegarde et la configuration des secrets et des emplacements de sauvegarde nécessaires.

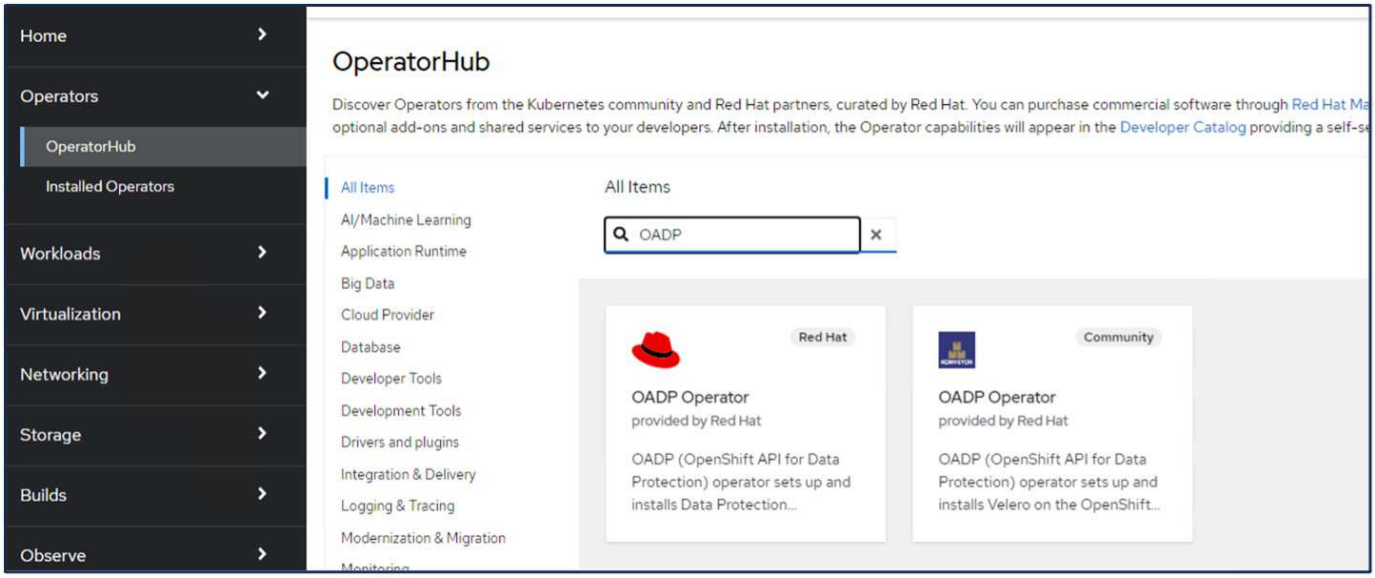
Prérequis

- Un cluster Red Hat OpenShift (version ultérieure à la version 4.12) installé sur une infrastructure bare-metal avec des nœuds de travail RHCOS
- Un cluster NetApp ONTAP intégré au cluster à l'aide de Trident
- Un backend Trident configuré avec un SVM sur un cluster ONTAP
- Une StorageClass configurée sur le cluster OpenShift avec Trident comme provisionneur
- Classe Trident Snapshot créée sur le cluster
- Accès administrateur du cluster au cluster Red Hat OpenShift
- Accès administrateur au cluster NetApp ONTAP
- Opérateur de virtualisation OpenShift installé et configuré
- Machines virtuelles déployées dans un espace de noms sur OpenShift Virtualization
- Un poste de travail administrateur avec les outils tridentctl et oc installés et ajoutés à $PATH

Si vous souhaitez effectuer une sauvegarde d'une machine virtuelle lorsqu'elle est en cours d'exécution, vous devez installer l'agent invité QEMU sur cette machine virtuelle. Si vous installez la machine virtuelle à l'aide d'un modèle existant, l'agent QEMU est installé automatiquement. QEMU permet à l'agent invité de suspendre les données en vol dans le système d'exploitation invité pendant le processus de capture instantanée et d'éviter une éventuelle corruption des données. Si vous n'avez pas installé QEMU, vous pouvez arrêter la machine virtuelle avant d'effectuer une sauvegarde.

Étapes d'installation de l'opérateur OADP

1. Accédez au hub opérateur du cluster et sélectionnez l'opérateur Red Hat OADP. Dans la page Installer, utilisez toutes les sélections par défaut et cliquez sur Installer. Sur la page suivante, utilisez à nouveau tous les paramètres par défaut et cliquez sur Installer. L'opérateur OADP sera installé dans l'espace de noms 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

Prérequis pour la configuration de Velero avec Ontap S3

Une fois l'installation de l'opérateur réussie, configurez l'instance de Velero. Velero peut être configuré pour utiliser le stockage d'objets compatible S3. Configurez ONTAP S3 à l'aide des procédures indiquées dans le"Section Gestion du stockage d'objets de la documentation ONTAP" . Vous aurez besoin des informations suivantes de votre configuration ONTAP S3 pour l'intégration avec Velero.

- Une interface logique (LIF) qui peut être utilisée pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3 qui incluent la clé d'accès et la clé d'accès secrète
- Un nom de bucket dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage d'objets, le certificat TLS doit être installé sur le serveur de stockage d'objets.

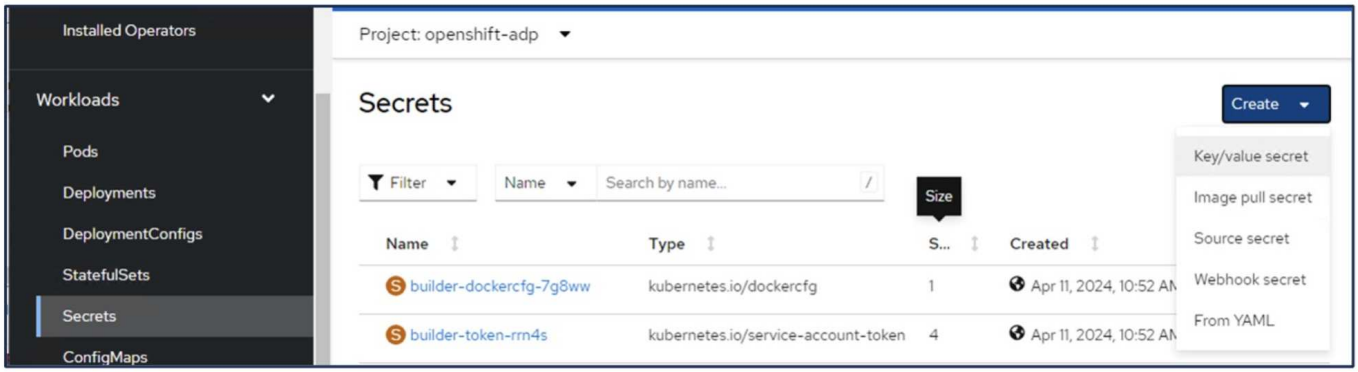
Prérequis pour la configuration de Velero avec StorageGrid S3

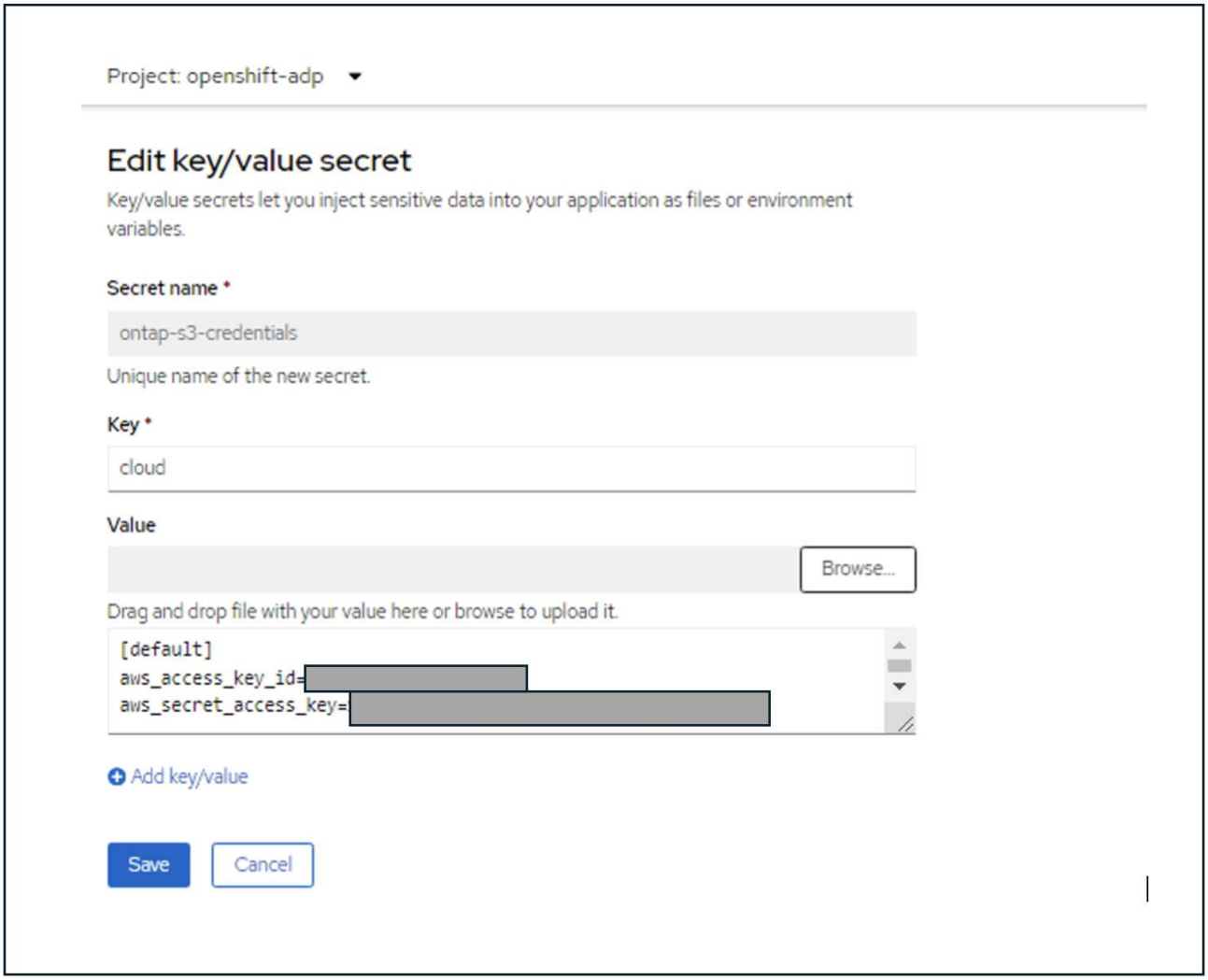
Velero peut être configuré pour utiliser le stockage d'objets compatible S3. Vous pouvez configurer StorageGrid S3 en utilisant les procédures indiquées dans le"Documentation de StorageGrid" . Vous aurez besoin des informations suivantes de votre configuration StorageGrid S3 pour l'intégrer à Velero.

- Le point de terminaison qui peut être utilisé pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3 qui incluent la clé d'accès et la clé d'accès secrète
- Un nom de bucket dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage d'objets, le certificat TLS doit être installé sur le serveur de stockage d'objets.

Étapes pour configurer Velero

- Tout d'abord, créez un secret pour les informations d'identification d'un utilisateur ONTAP S3 ou d'un locataire StorageGrid. Cela sera utilisé pour configurer Velero plus tard. Vous pouvez créer un secret à partir de la CLI ou de la console Web. Pour créer un secret à partir de la console Web, sélectionnez Secrets, puis cliquez sur Clé/Valeur secrète. Fournissez les valeurs pour le nom des informations d'identification, la clé et la valeur comme indiqué. Assurez-vous d'utiliser l'ID de clé d'accès et la clé d'accès secrète de votre utilisateur S3. Nommez le secret de manière appropriée. Dans l'exemple ci-dessous, un secret avec les informations d'identification de l'utilisateur ONTAP S3 nommé ontap-s3-credentials est créé.

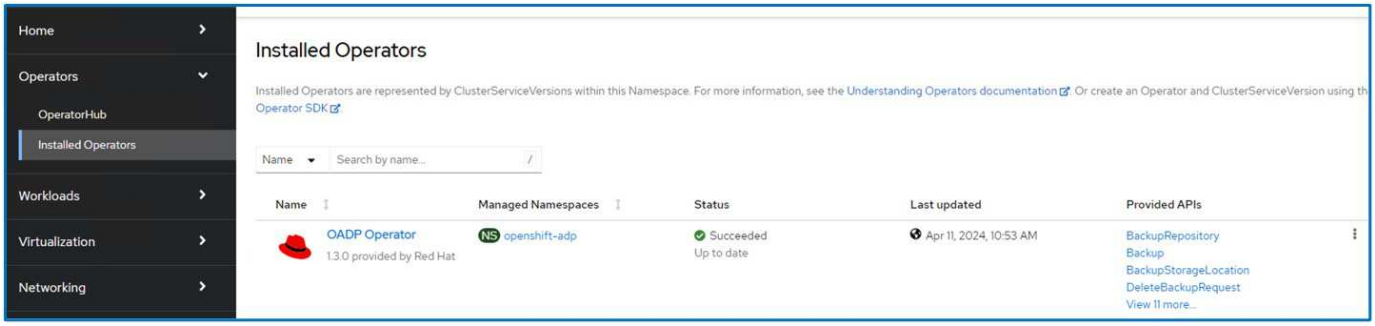




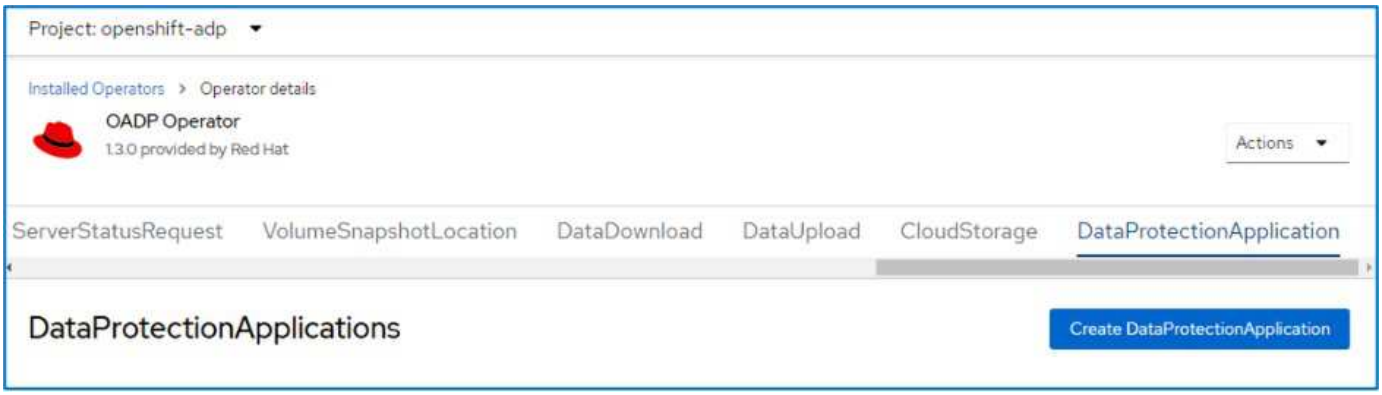
Pour créer un secret nommé sg-s3-credentials à partir de la CLI, vous pouvez utiliser la commande suivante.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

Where 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>
```

- Ensuite, pour configurer Velero, sélectionnez Opérateurs installés dans l'élément de menu sous Opérateurs, cliquez sur Opérateur OADP, puis sélectionnez l'onglet DataProtectionApplication.



Cliquez sur Créer une application de protection des données. Dans la vue formulaire, indiquez un nom pour l'application DataProtection ou utilisez le nom par défaut.



Accédez maintenant à la vue YAML et remplacez les informations de spécification comme indiqué dans les exemples de fichiers yaml ci-dessous.

Exemple de fichier YAML pour la configuration de Velero avec ONTAP S3 comme emplacement de sauvegarde

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' ->LIF to access S3. 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
```

Exemple de fichier YAML pour la configuration de Velero avec StorageGrid S3 comme backupLocation et 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
```

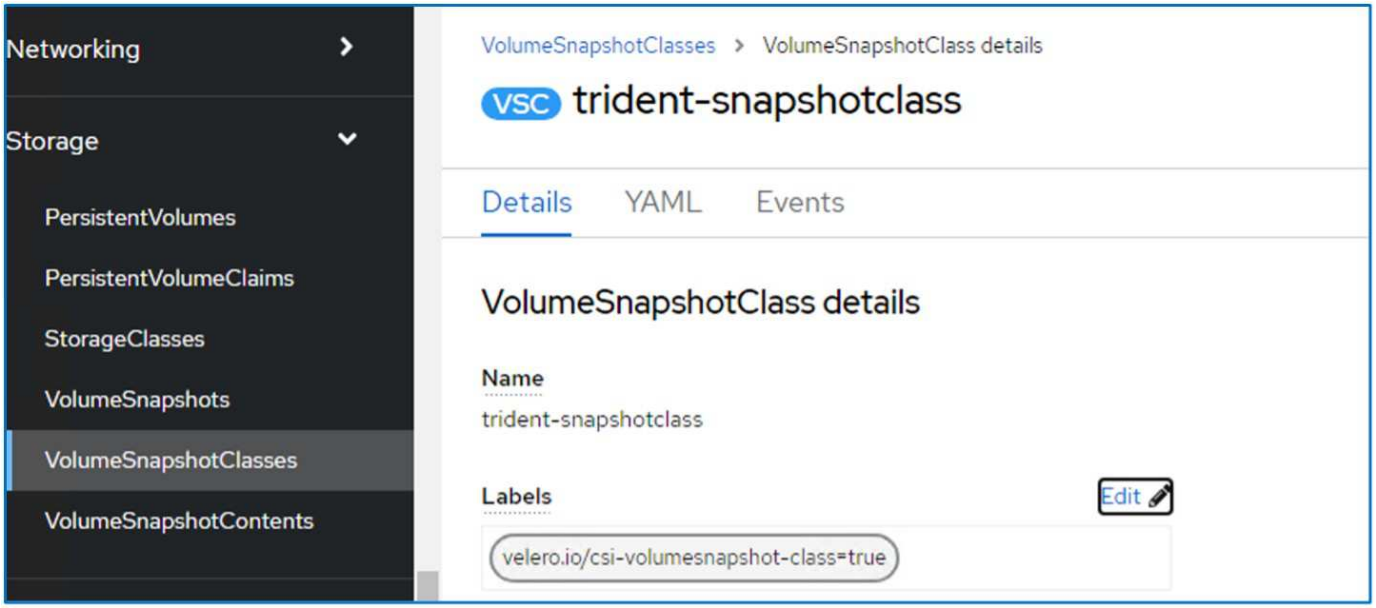
La section spec dans le fichier yaml doit être configurée de manière appropriée pour les paramètres suivants, similaires à l'exemple ci-dessus

backupLocations ONTAP S3 ou StorageGrid S3 (avec ses informations d'identification et autres informations telles qu'indiquées dans le fichier yaml) est configuré comme BackupLocation par défaut pour velero.

snapshotLocations Si vous utilisez des snapshots Container Storage Interface (CSI), vous n'avez pas besoin de spécifier un emplacement de snapshot, car vous créerez un CR VolumeSnapshotClass pour enregistrer le pilote CSI. Dans notre exemple, vous utilisez Trident CSI et vous avez précédemment créé VolumeSnapShotClass CR à l'aide du pilote Trident CSI.

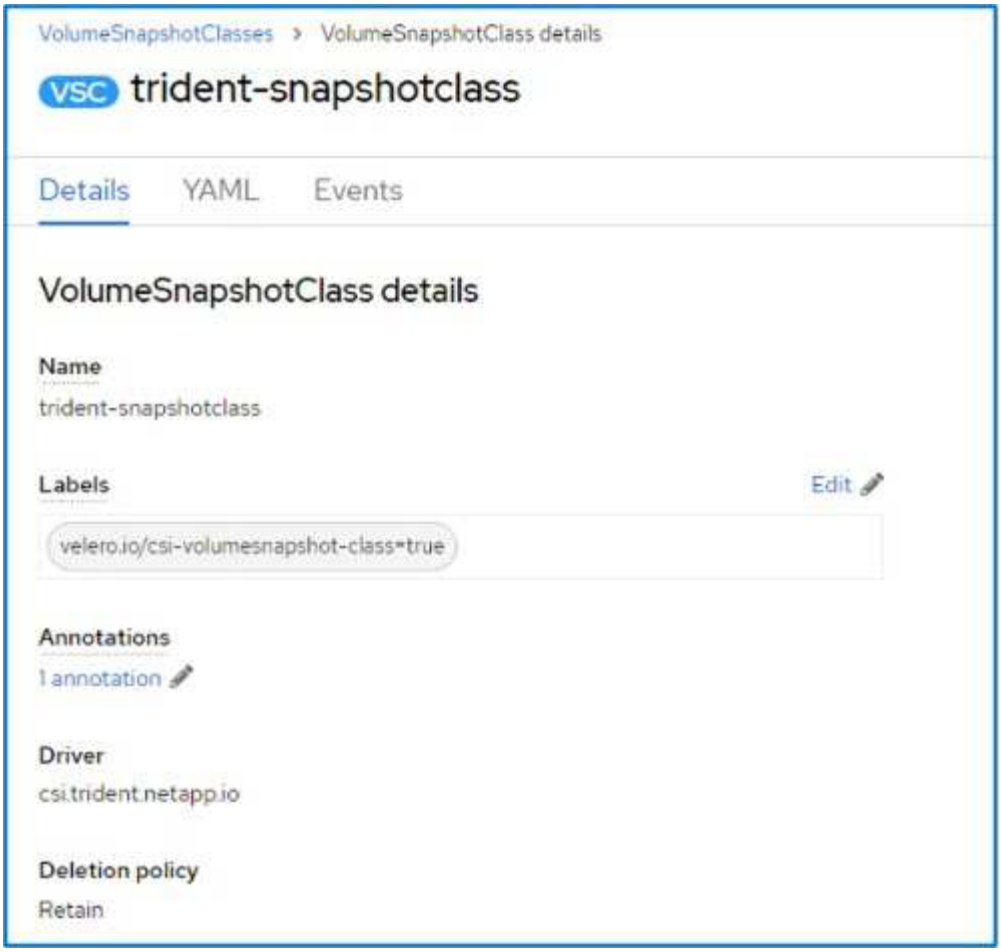
Activer le plugin CSI Ajoutez csi aux plugins par défaut pour Velero pour sauvegarder les volumes persistants avec des instantanés CSI. Les plugins Velero CSI, pour sauvegarder les PVC sauvegardés par CSI, choisiront le VolumeSnapshotClass dans le cluster sur lequel l'étiquette **velero.io/csi-volumesnapshot-class** est définie. Pour ça

- Vous devez avoir créé le trident VolumeSnapshotClass.
- Modifiez l'étiquette de trident-snapshotclass et définissez-la sur **velero.io/csi-volumesnapshot-class=true** comme indiqué ci-dessous.

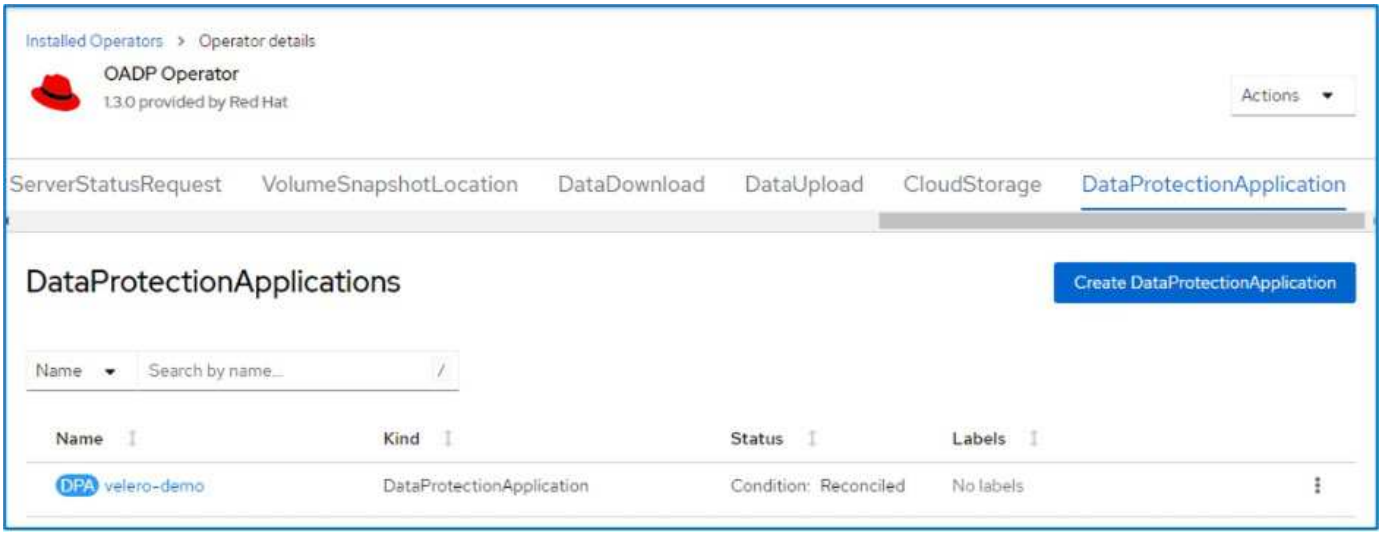


Assurez-vous que les instantanés peuvent persister même si les objets VolumeSnapshot sont supprimés. Cela peut être fait en définissant **deletionPolicy** sur Retain. Dans le cas contraire, la suppression d'un espace de noms entraînera la perte complète de tous les PVC sauvegardés dans celui-ci.

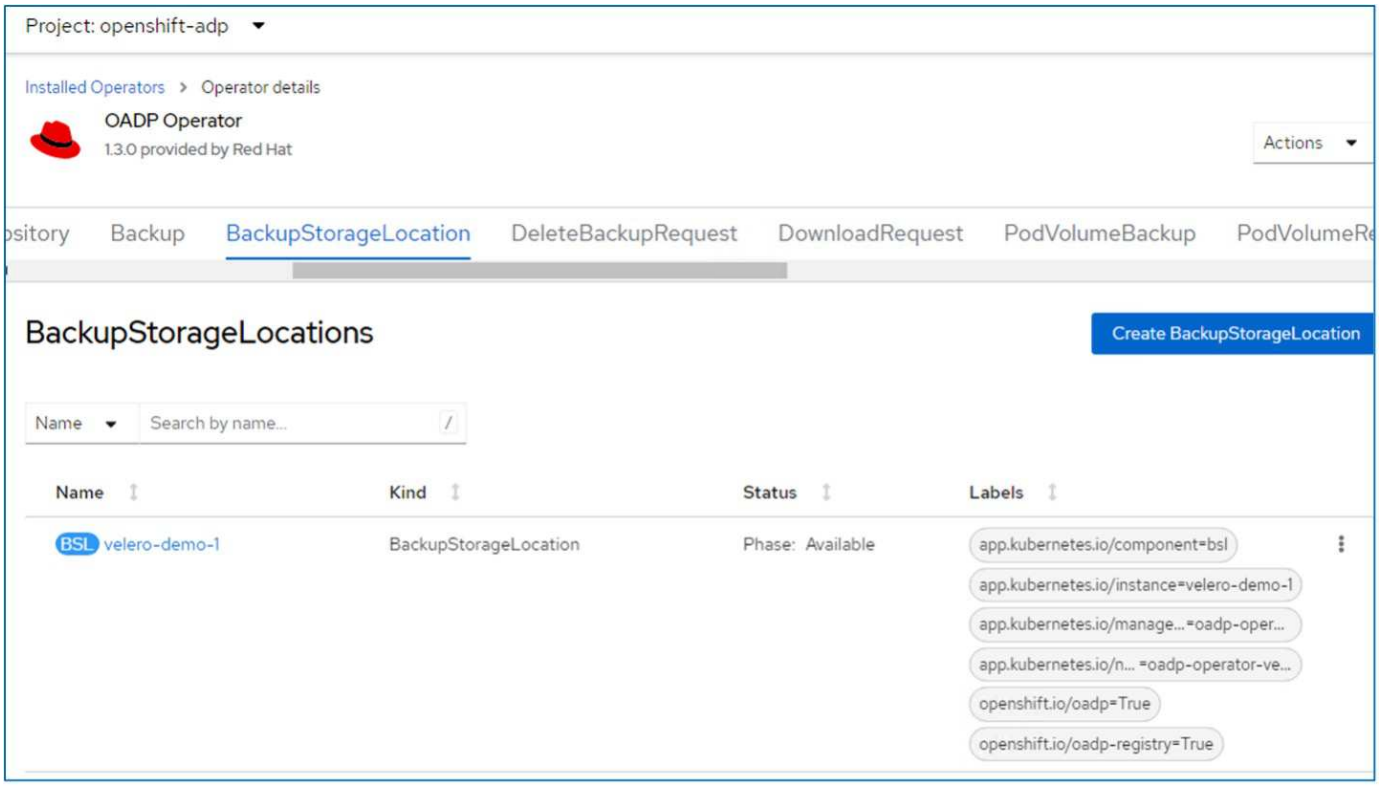
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Assurez-vous que DataProtectionApplication est créée et qu'elle est dans l'état : Réconcilié.



L'opérateur OADP créera un BackupStorageLocation correspondant. Celui-ci sera utilisé lors de la création d'une sauvegarde.



Créer une sauvegarde à la demande pour les machines virtuelles dans Red Hat OpenShift Virtualization à l'aide de Velero

Sauvegardez les machines virtuelles dans OpenShift Virtualization à l'aide de Velero et NetApp ONTAP S3 ou StorageGRID. Cette procédure inclut la création de ressources personnalisées de sauvegarde (CR) pour les sauvegardes à la demande et de CR planifiées pour les sauvegardes planifiées. Chaque sauvegarde capture les métadonnées de la machine virtuelle et les volumes persistants, en les stockant dans l'emplacement de stockage d'objets spécifié à des fins de récupération ou de conformité.

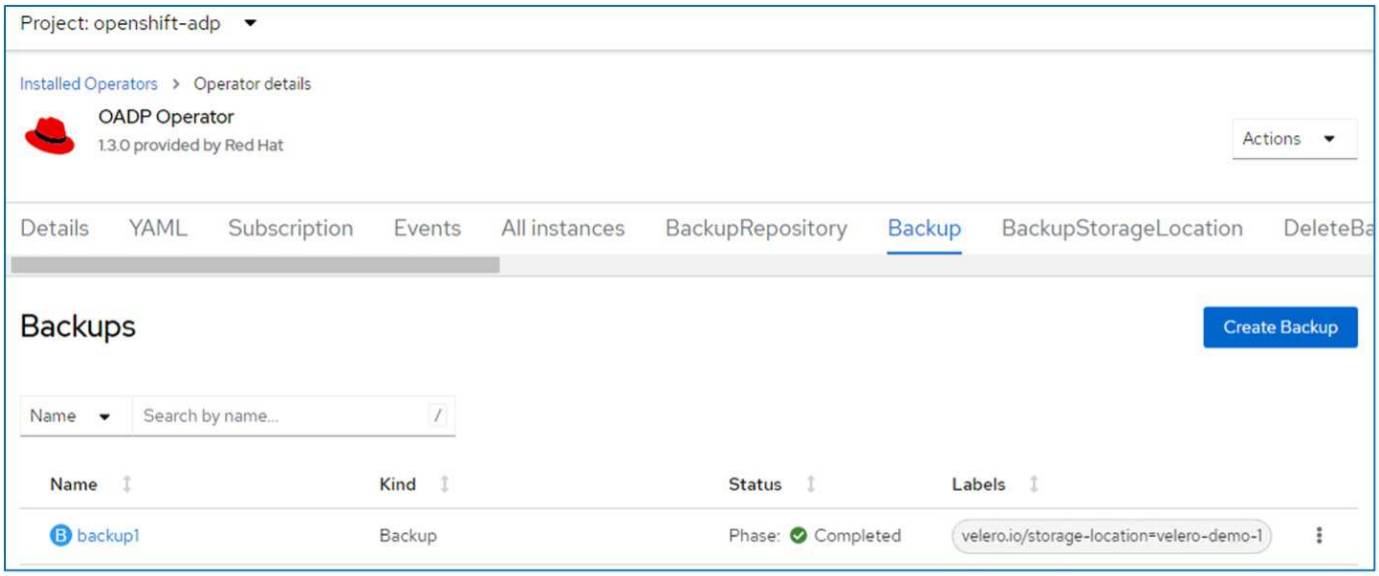
Étapes pour créer une sauvegarde d'une machine virtuelle

Pour créer une sauvegarde à la demande de l'intégralité de la VM (métadonnées de la VM et disques de la VM), cliquez sur l'onglet **Sauvegarde**. Cela crée une ressource personnalisée de sauvegarde (CR). Un exemple de fichier yaml est fourni pour créer le CR de sauvegarde. À l'aide de ce fichier yaml, la machine virtuelle et ses disques dans l'espace de noms spécifié seront sauvegardés. Des paramètres supplémentaires peuvent être définis comme indiqué dans le"documentation" .

Un instantané des volumes persistants soutenant les disques sera créé par le CSI. Une sauvegarde de la machine virtuelle ainsi que l'instantané de ses disques sont créés et stockés dans l'emplacement de sauvegarde spécifié dans le fichier yaml. La sauvegarde restera dans le système pendant 30 jours comme spécifié dans le 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
```

Une fois la sauvegarde terminée, sa phase s'affichera comme terminée.



Vous pouvez inspecter la sauvegarde dans le stockage d'objets à l'aide d'une application de navigateur S3. Le chemin de la sauvegarde s'affiche dans le bucket configuré avec le nom de préfixe (velero/demobackup). Vous pouvez voir que le contenu de la sauvegarde comprend les instantanés de volume, les journaux et d'autres métadonnées de la machine virtuelle.

> Dans StorageGrid, vous pouvez également utiliser la console S3 disponible à partir du gestionnaire de locataires pour afficher les objets de sauvegarde.

Path: / demobackup/ backups/ backup1/

Name	Size	Type	Last Modified	Storage Class
..				
backup1.tar.gz	230.36 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
velero-backup.json	3.35 KB	JSON File	4/15/2024 10:26:29 PM	STANDARD
backup1-resource-list.json.gz	1.12 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
backup1-itemoperations.json.gz	600 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-volumesnapshots.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-podvolumebackups.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-results.gz	49 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotclasses.json.gz	426 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotcontents.json.gz	1.43 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshots.json.gz	1.34 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-logs.gz	13.49 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD

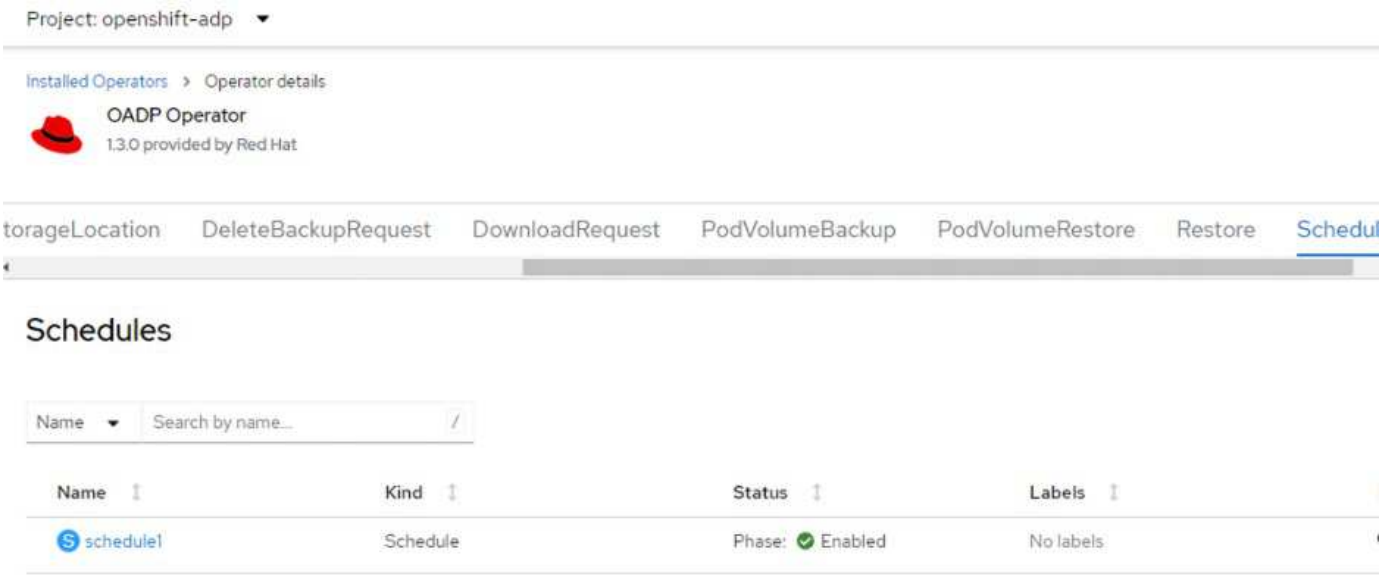
Création de sauvegardes planifiées pour les machines virtuelles dans OpenShift Virtualization

Pour créer des sauvegardes selon une planification, vous devez créer une CR de planification. La planification est simplement une expression Cron vous permettant de spécifier l'heure à laquelle vous souhaitez créer la sauvegarde. Un exemple de fichier yaml pour créer un CR de planification.

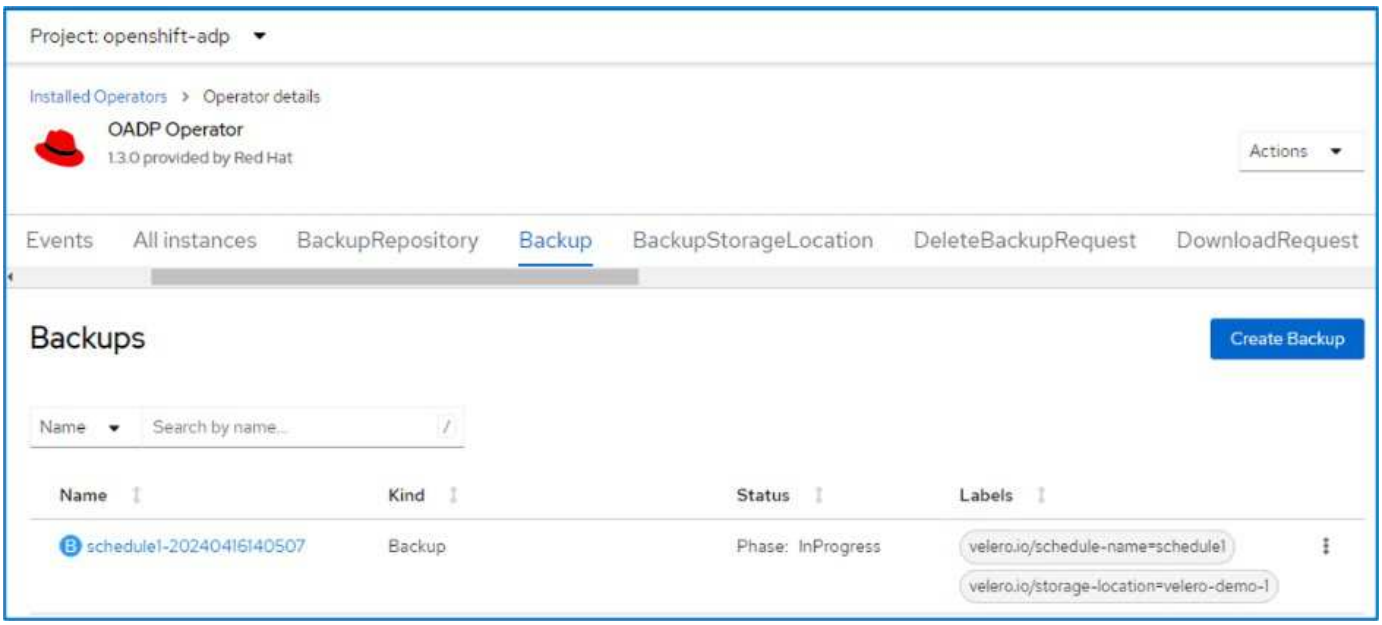
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

L'expression Cron 0 7 * * * signifie qu'une sauvegarde sera créée à 7h00 tous les jours. Les espaces de noms à inclure dans la sauvegarde et l'emplacement de stockage de la sauvegarde sont également spécifiés. Ainsi, au lieu d'un CR de sauvegarde, le CR planifié est utilisé pour créer une sauvegarde à l'heure et à la fréquence spécifiées.

Une fois le calendrier créé, il sera activé.



Les sauvegardes seront créées selon ce calendrier et pourront être consultées à partir de l'onglet Sauvegarde.



Restaurer une machine virtuelle à partir d'une sauvegarde dans Red Hat OpenShift Virtualization à l'aide de Velero

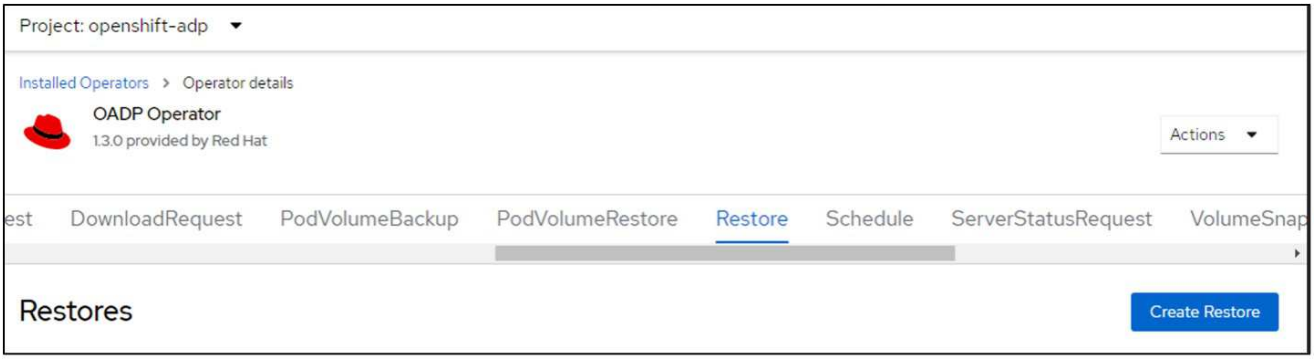
Restaurez les machines virtuelles dans OpenShift Virtualization à l'aide de Velero et de l'API OpenShift pour la protection des données (OADP). Cette procédure inclut la création d'une ressource personnalisée de restauration (CR) pour récupérer les machines virtuelles et leurs volumes persistants à partir de sauvegardes, avec des options de restauration vers l'espace de noms d'origine, un espace de noms différent ou l'utilisation d'une classe de stockage alternative.

Prérequis

Pour restaurer à partir d’une sauvegarde, supposons que l’espace de noms où la machine virtuelle existait a été supprimé accidentellement.

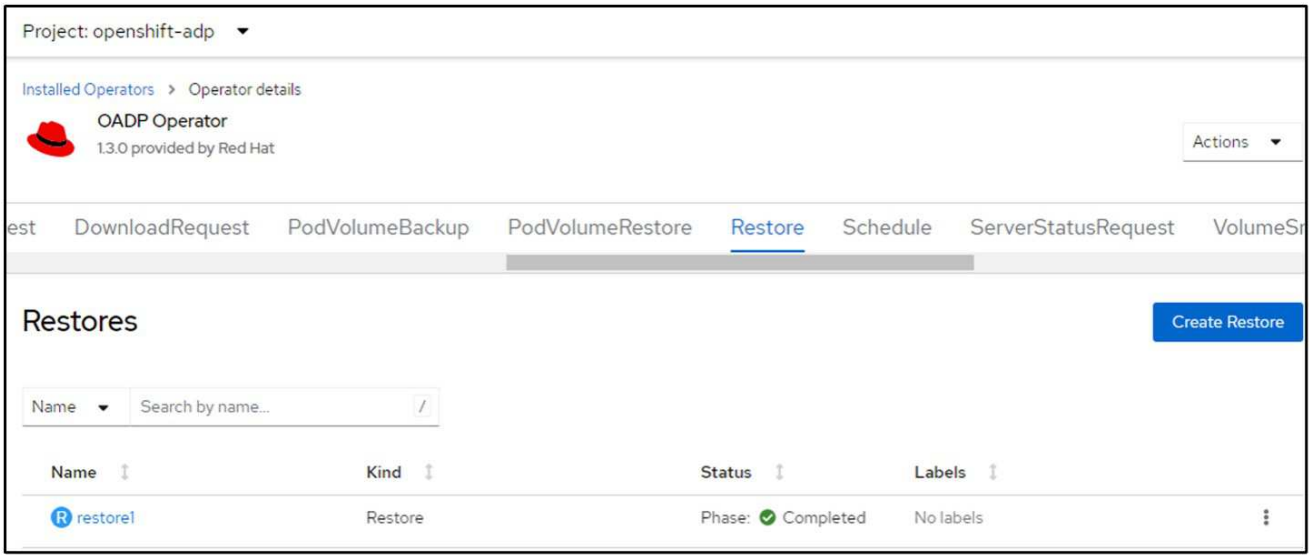
Restaurer vers le même espace de noms

Pour restaurer à partir de la sauvegarde que nous venons de créer, nous devons créer une ressource personnalisée de restauration (CR). Nous devons lui donner un nom, fournir le nom de la sauvegarde à partir de laquelle nous voulons restaurer et définir restorePVs sur true. Des paramètres supplémentaires peuvent être définis comme indiqué dans le"documentation" . Cliquez sur le bouton Créer.




```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true
```

Lorsque la phase est terminée, vous pouvez voir que les machines virtuelles ont été restaurées à l'état dans lequel l'instantané a été pris. (Si la sauvegarde a été créée lorsque la machine virtuelle était en cours d'exécution, la restauration de la machine virtuelle à partir de la sauvegarde démarrera la machine virtuelle restaurée et la ramènera à un état d'exécution). La machine virtuelle est restaurée dans le même espace de noms.



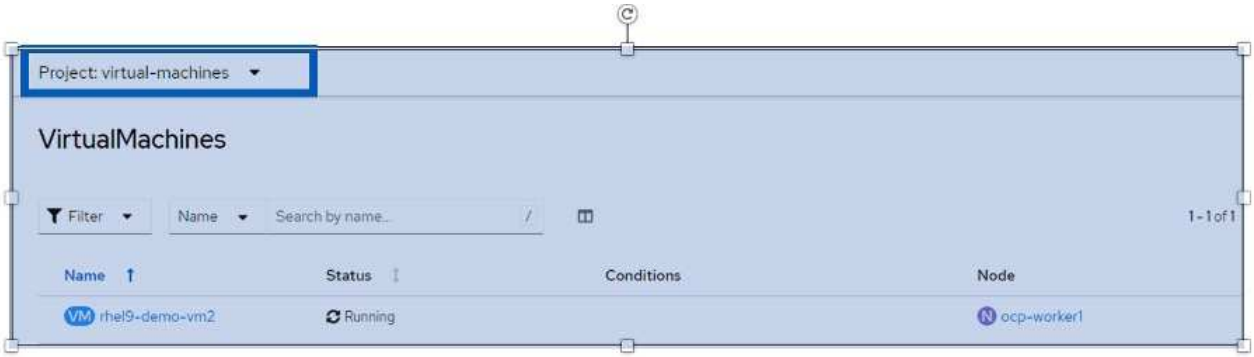
Restaurer vers un espace de noms différent

Pour restaurer la machine virtuelle dans un espace de noms différent, vous pouvez fournir un namespaceMapping dans la définition yaml du CR de restauration.

L'exemple de fichier yaml suivant crée un CR de restauration pour restaurer une machine virtuelle et ses disques dans l'espace de noms virtual-machines-demo lorsque la sauvegarde a été effectuée dans l'espace de noms virtual-machines.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

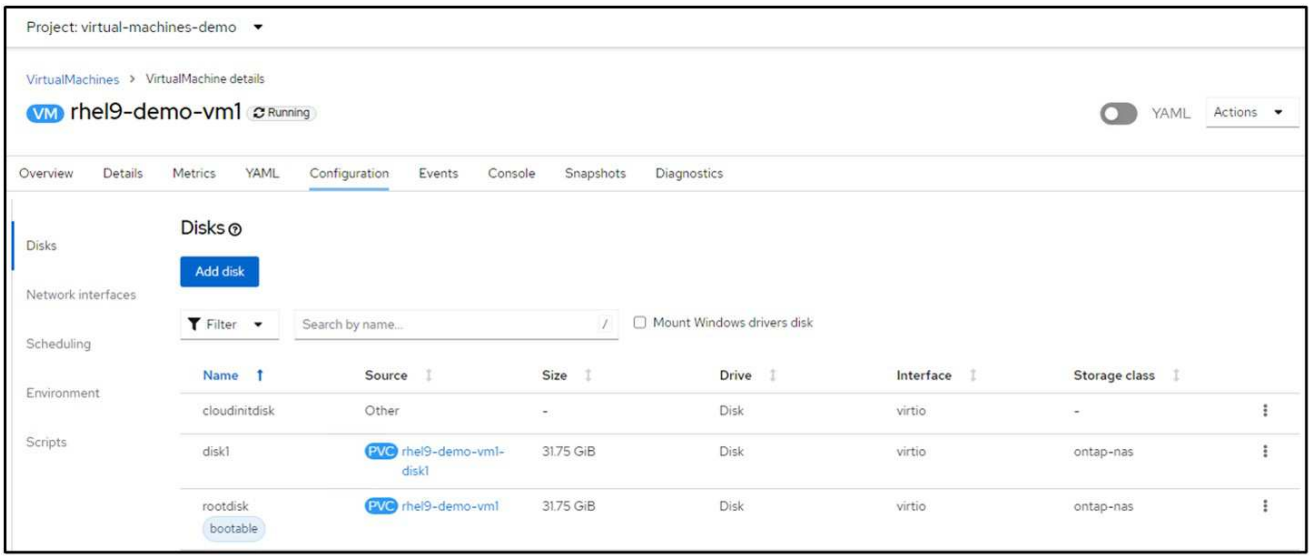
Lorsque la phase est terminée, vous pouvez voir que les machines virtuelles ont été restaurées à l'état dans lequel l'instantané a été pris. (Si la sauvegarde a été créée lorsque la machine virtuelle était en cours d'exécution, la restauration de la machine virtuelle à partir de la sauvegarde démarrera la machine virtuelle restaurée et la ramènera à un état d'exécution). La machine virtuelle est restaurée dans un espace de noms différent comme spécifié dans le fichier yaml.

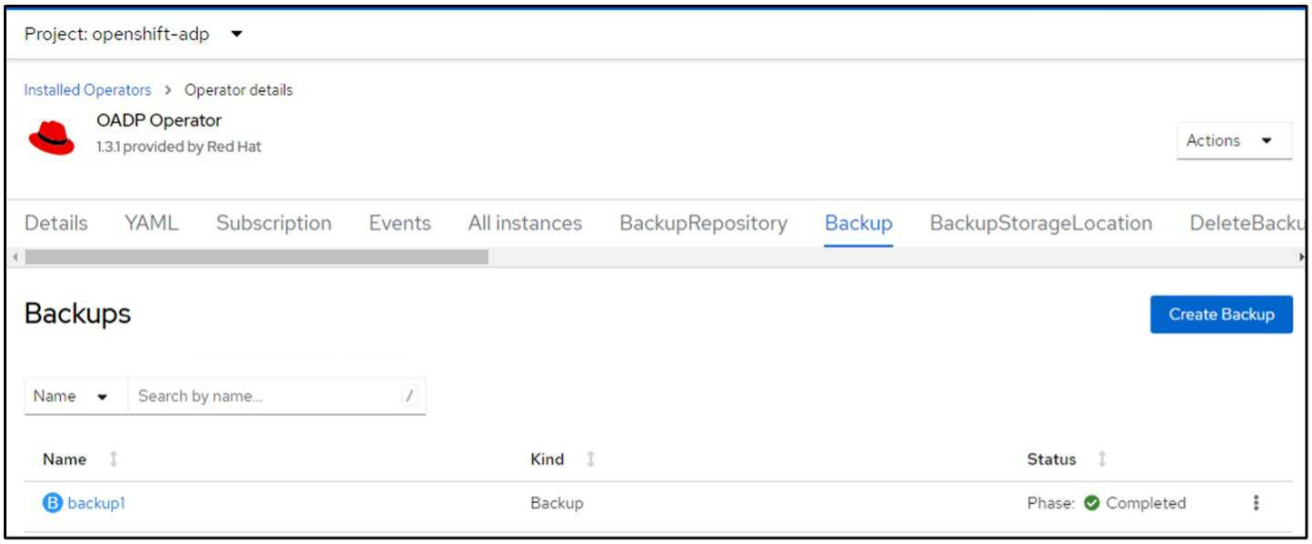


Restaurer vers une classe de stockage différente

Velero fournit une capacité générique pour modifier les ressources pendant la restauration en spécifiant des correctifs json. Les correctifs JSON sont appliqués aux ressources avant leur restauration. Les correctifs json sont spécifiés dans une configmap et la configmap est référencée dans la commande de restauration. Cette fonctionnalité vous permet de restaurer à l'aide de différentes classes de stockage.

Dans l'exemple ci-dessous, la machine virtuelle, lors de sa création, utilise ontap-nas comme classe de stockage pour ses disques. Une sauvegarde de la machine virtuelle nommée backup1 est créée.





Simulez une perte de la VM en supprimant la VM.

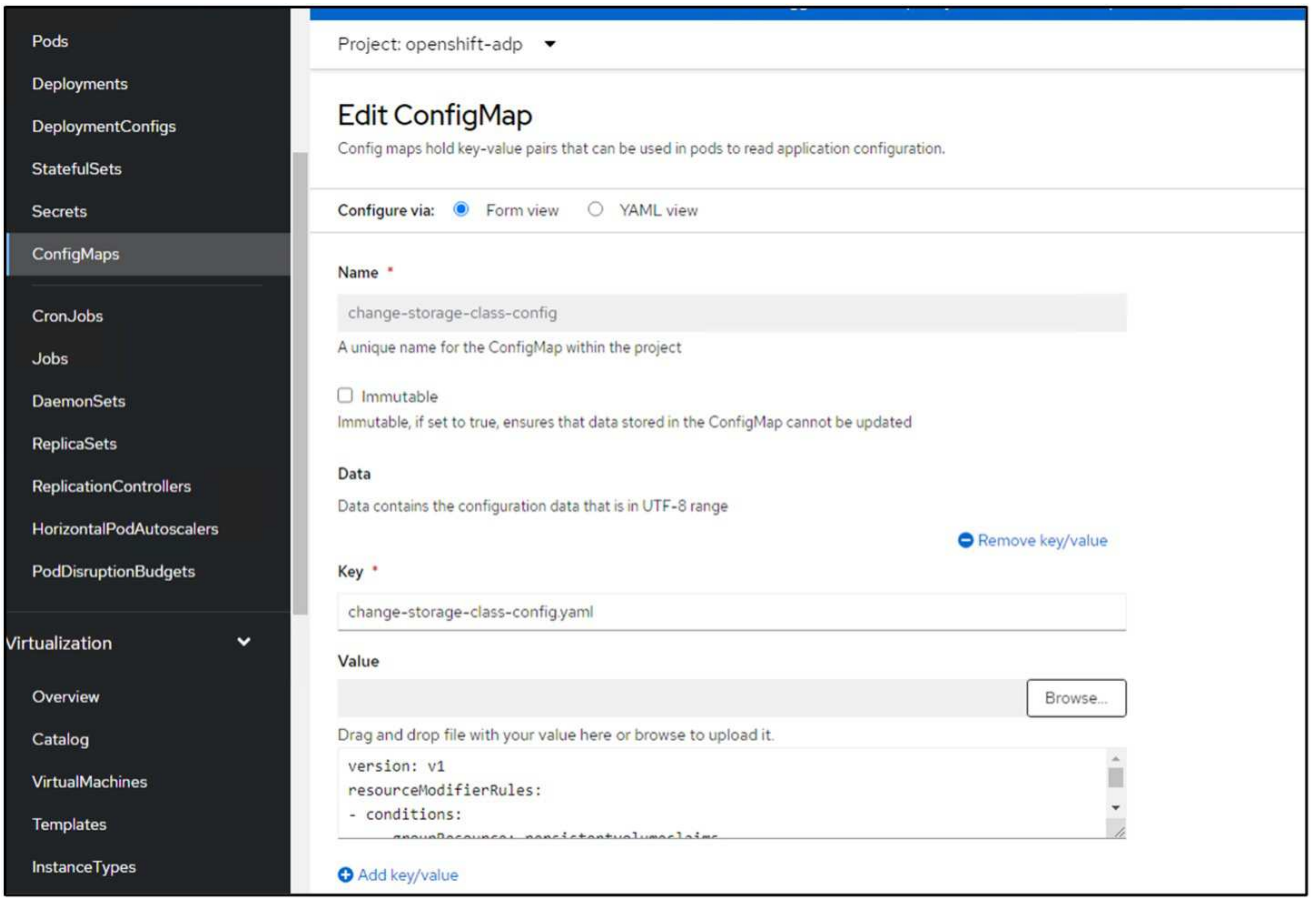
Pour restaurer la machine virtuelle à l'aide d'une classe de stockage différente, par exemple, la classe de stockage ontap-nas-eco, vous devez effectuer les deux étapes suivantes :

Étape 1

Créez une carte de configuration (console) dans l'espace de noms openshift-adp comme suit : Remplissez les détails comme indiqué dans la capture d'écran : Sélectionnez l'espace de noms : openshift-adp Nom : change-storage-class-config (peut être n'importe quel nom) Clé : change-storage-

class-config.yaml : Valeur :

```
version: v1
    resourceModifierRules:
    - conditions:
        groupResource: persistentvolumeclaims
        resourceNameRegex: "^rhel*"
        namespaces:
        - virtual-machines-demo
      patches:
      - operation: replace
        path: "/spec/storageClassName"
        value: "ontap-nas-eco"
```



L'objet de carte de configuration résultant devrait ressembler à ceci (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>
```

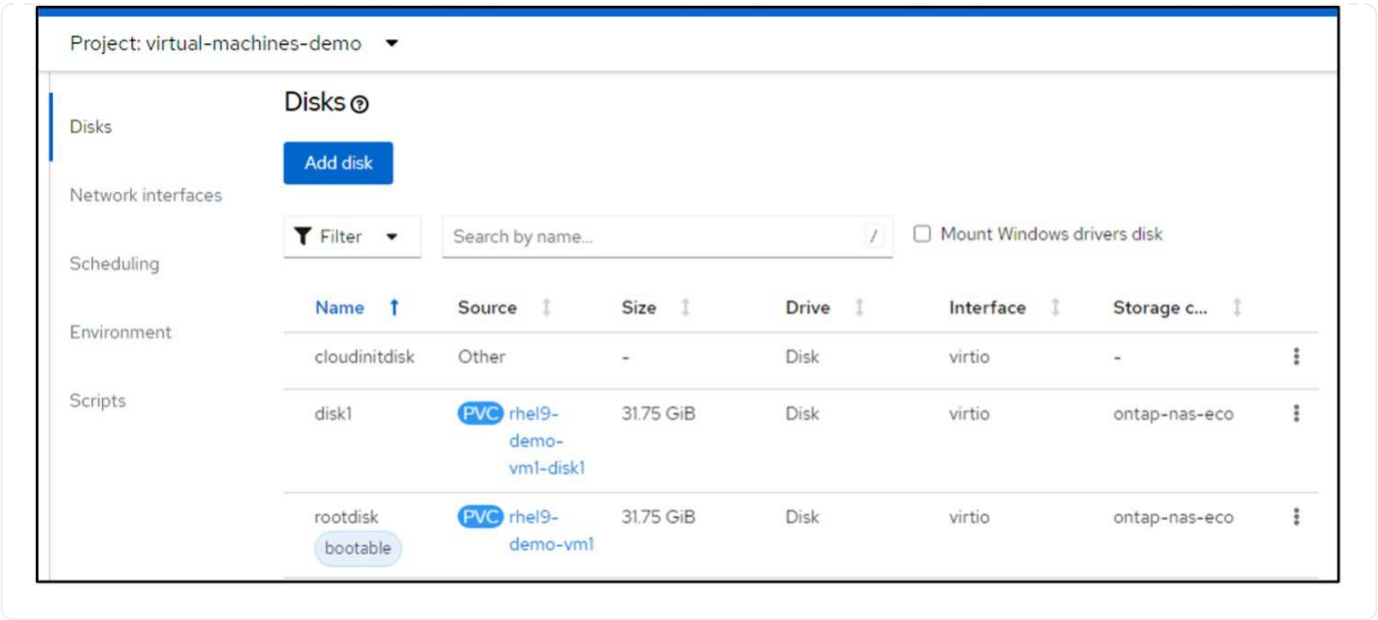
Cette carte de configuration appliquera la règle de modification des ressources lors de la création de la restauration. Un correctif sera appliqué pour remplacer le nom de la classe de stockage par ontap-nas-eco pour toutes les revendications de volume persistant commençant par rhel.

Étape 2

Pour restaurer la machine virtuelle, utilisez la commande suivante depuis la CLI Velero :

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

La machine virtuelle est restaurée dans le même espace de noms avec les disques créés à l'aide de la classe de stockage ontap-nas-eco.



Supprimer un CR de sauvegarde ou restaurer un CR dans Red Hat OpenShift Virtualization à l'aide de Velero

Supprimez les ressources de sauvegarde et de restauration pour les machines virtuelles dans OpenShift Virtualization à l'aide de Velero. Utilisez l'interface de ligne de commande OpenShift pour supprimer les sauvegardes tout en conservant les données de stockage d'objets, ou l'interface de ligne de commande Velero pour supprimer à la fois la ressource personnalisée de sauvegarde (CR) et les données de stockage associées.

Supprimer une sauvegarde

Vous pouvez supprimer un CR de sauvegarde sans supprimer les données de stockage d'objets à l'aide de l'outil OC CLI.

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Si vous souhaitez supprimer le CR de sauvegarde et supprimer les données de stockage d'objets associées, vous pouvez le faire à l'aide de l'outil Velero CLI.

Téléchargez la CLI comme indiqué dans les instructions du"Documentation Velero" .

Exécutez la commande de suppression suivante à l'aide de la CLI Velero

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

Suppression d'une restauration

Vous pouvez supprimer le CR de restauration à l'aide de la CLI Velero

```
velero restore delete restore --namespace openshift-adp
```

Vous pouvez utiliser la commande oc ainsi que l’interface utilisateur pour supprimer le CR de restauration

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.