



Protection des données à l'aide d'outils tiers

NetApp Solutions

NetApp
September 26, 2024

Sommaire

- Protection des données à l'aide d'outils tiers 1
 - Protection des données pour les VM dans OpenShift Virtualization à l'aide d'OpenShift API for Data protection (OADP) 1
 - Installation de l'opérateur OpenShift API for Data protection (OADP) 3
 - Création d'une sauvegarde à la demande pour les machines virtuelles dans OpenShift Virtualization 13
 - Restaurer une machine virtuelle à partir d'une sauvegarde 16
 - Suppression des sauvegardes et des restaurations dans à l'aide de Velero 22

Protection des données à l'aide d'outils tiers

Protection des données pour les VM dans OpenShift Virtualization à l'aide d'OpenShift API for Data protection (OADP)

Auteur: Banu Sundhar, NetApp

Cette section du document de référence fournit des informations détaillées sur la création de sauvegardes de machines virtuelles à l'aide d'OpenShift API for Data protection (OADP) avec Velero sur NetApp ONTAP S3 ou NetApp StorageGRID S3. Les sauvegardes des volumes persistants (persistent volumes) des disques de la machine virtuelle sont créées à l'aide des snapshots CSI Astra Trident.

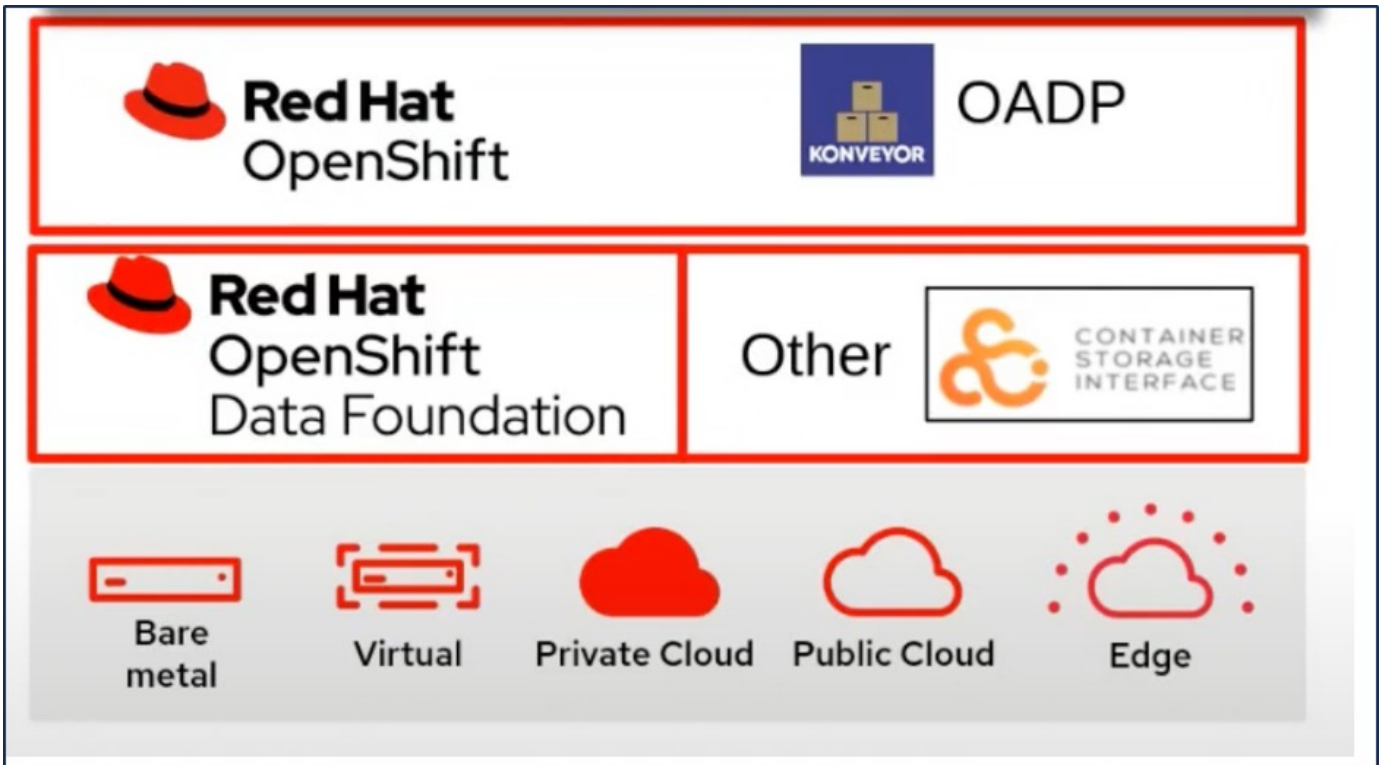
Les machines virtuelles de l'environnement OpenShift Virtualization sont des applications conteneurisées qui s'exécutent dans les nœuds workers de votre plateforme OpenShift Container. Il est important de protéger les métadonnées des machines virtuelles ainsi que les disques persistants des machines virtuelles, afin que vous puissiez les restaurer en cas de perte ou de corruption.

Les disques persistants des VM de virtualisation OpenShift peuvent être pris en charge par le stockage ONTAP intégré au cluster OpenShift à l'aide de ["ASTRA Trident CSI"](#). Dans cette section, nous utilisons ["OpenShift API pour la protection des données \(OADP\)"](#) Pour effectuer la sauvegarde des machines virtuelles, y compris leurs volumes de données vers

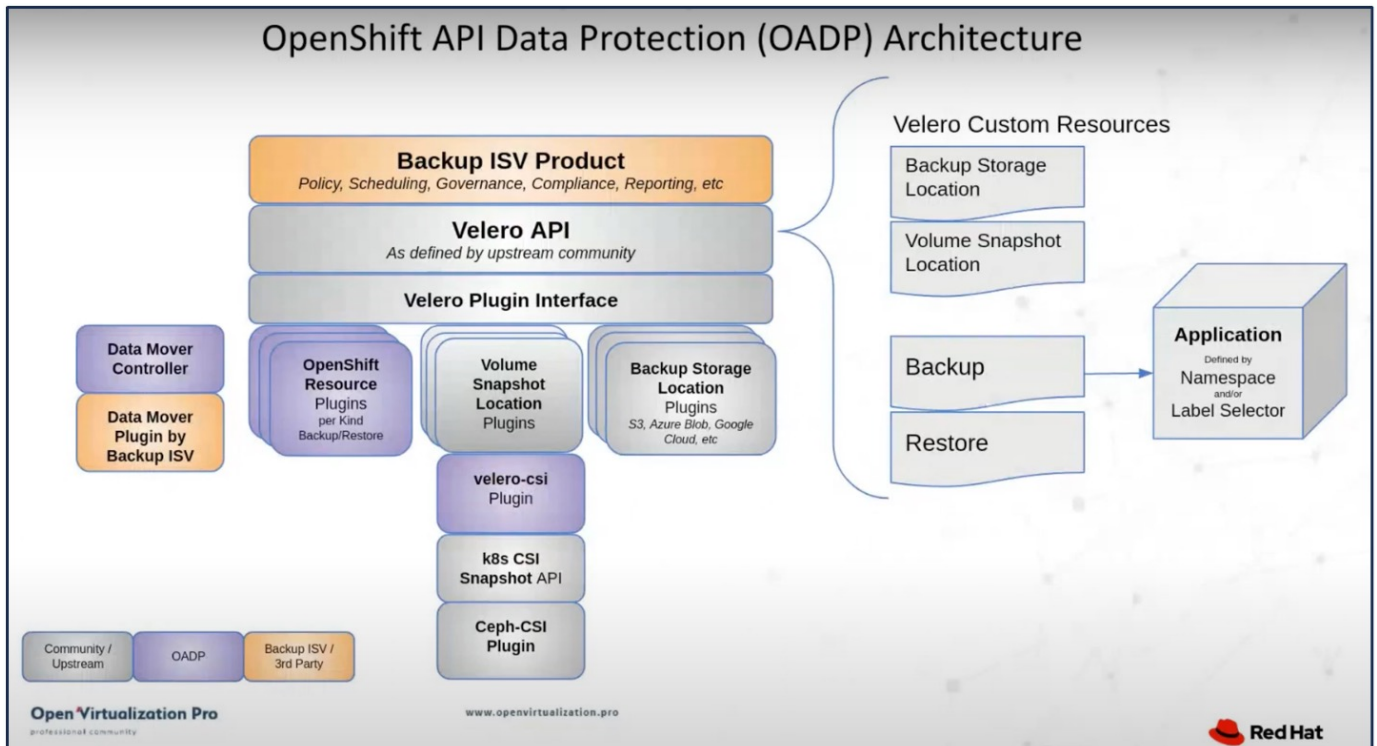
- Stockage objet ONTAP
- StorageGRID

Nous restaurons ensuite les données à partir de la sauvegarde si nécessaire.

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



Red Hat OpenShift a mis à profit les solutions développées par les communautés OpenSource pour la protection des données. "Velero" Est un outil open source qui permet de sauvegarder et de restaurer en toute sécurité, d'effectuer une reprise d'activité et de migrer les ressources de cluster Kubernetes et les volumes persistants. Pour utiliser Velero facilement, OpenShift a développé l'opérateur OADP et le plug-in Velero pour s'intégrer aux pilotes de stockage CSI. Les principales API OADP exposées sont basées sur les API Velero. Après l'installation de l'opérateur OADP et sa configuration, les opérations de sauvegarde/restauration qui peuvent être effectuées sont basées sur les opérations exposées par l'API Velero.



OADP 1.3 est disponible sur le hub opérateur d'OpenShift cluster 4.12 et versions ultérieures. Il est doté d'un Data Mover intégré qui peut déplacer les instantanés de volume CSI vers un magasin d'objets distant. Ces fonctionnalités assurent la portabilité et la durabilité en déplaçant les snapshots vers un emplacement de stockage objet pendant la sauvegarde. Les snapshots sont ensuite disponibles pour la restauration après un incident.

Les versions suivantes des différents composants utilisés dans 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
- ASTRA Trident 24.02
- ONTAP 9.12

"ASTRA Trident CSI"

"OpenShift API pour la protection des données (OADP)"

"Velero"

Installation de l'opérateur OpenShift API for Data protection (OADP)

Cette section décrit l'installation de l'opérateur OADP (OpenShift API for Data protection).

Prérequis

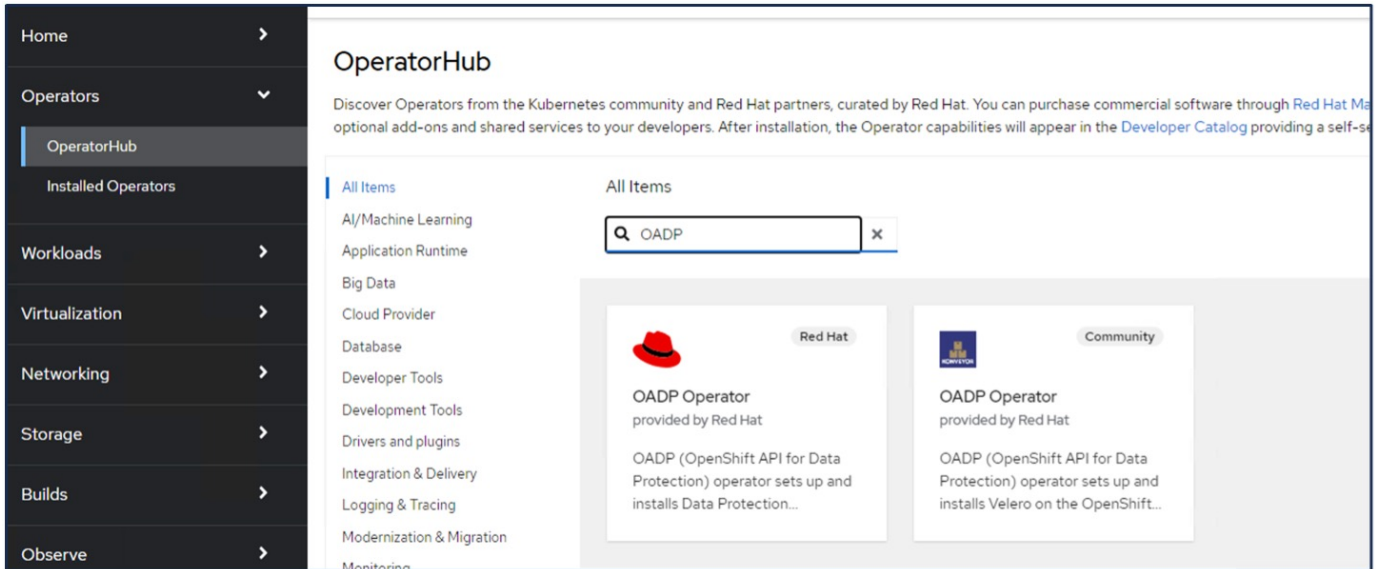
- Cluster Red Hat OpenShift (version ultérieure à la version 4.12) installé sur une infrastructure sans système d'exploitation avec des nœuds worker RHCOS
- Un cluster NetApp ONTAP intégré au cluster via Astra Trident
- Un système back-end Trident configuré avec un SVM sur le cluster ONTAP
- Classe de stockage configurée sur le cluster OpenShift avec Astra Trident en tant que mécanisme de provisionnement
- Classe Snapshot Trident créée sur le cluster
- L'accès cluster-admin au cluster Red Hat OpenShift
- Accès au cluster NetApp ONTAP par administrateur
- L'opérateur OpenShift Virtualization est installé et configuré
- VM déployées dans un espace de noms sur OpenShift Virtualization
- Une station de travail d'administration avec des outils tridentctl et oc installés et ajoutés à \$PATH



Si vous souhaitez effectuer une sauvegarde d'une machine virtuelle alors qu'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 automatiquement installé. QEMU permet à l'agent invité de suspendre les données en vol dans le système d'exploitation invité pendant le processus de snapshot et d'éviter toute corruption potentielle des données. Si QEMU n'est pas installé, vous pouvez arrêter la machine virtuelle avant d'effectuer une sauvegarde.

Procédure d'installation de l'opérateur OADP

1. Accédez au hub opérateur du cluster et sélectionnez opérateur OADP Red Hat. Dans la page installer, utilisez toutes les sélections par défaut et cliquez sur installer. Sur la page suivante, utilisez à nouveau toutes les valeurs 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

OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Version

1.3.0

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.

Capability level

- Basic Install
- Seamless Upgrades
- Full Lifecycle
- Deep Insights
- Auto Pilot

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](#)

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

Activate Windows

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	openshift-cnrv	openshift-cnrv	Succeeded Up to date
OADP Operator 1.3.0 provided by Red Hat	openshift-adp	openshift-adp	Succeeded Up to date
Package Server 0.0.1-snapshot provided by	openshift-operator-lifecycle-manager	openshift-operator-lifecycle-manager	Succeeded

Conditions préalables pour la configuration Velero avec les détails de ONTAP S3

Une fois l'installation de l'opérateur réussie, configurez l'instance de Velero.

Velero peut être configuré pour utiliser le stockage objet compatible S3. Configurez ONTAP S3 à l'aide des procédures indiquées dans le "[Section gestion du stockage objet de la documentation ONTAP](#)". Pour l'intégration à Velero, vous aurez besoin des informations suivantes de votre configuration ONTAP S3.

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

Conditions préalables pour la configuration Velero avec les détails de StorageGRID S3

Velero peut être configuré pour utiliser le stockage objet compatible S3. Vous pouvez configurer StorageGRID S3 à l'aide des procédures indiquées dans le "[Documentation StorageGRID](#)". Pour l'intégration à Velero, vous aurez besoin des informations suivantes de votre configuration StorageGRID S3.

- Terminal pouvant être utilisé pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3, y compris la clé d'accès et la clé d'accès secrète
- Nom de compartiment dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage objet, le certificat TLS doit être installé sur le serveur de stockage objet.

Procédure de configuration de Velero

- Commencez par créer un secret pour les informations d'identification d'un utilisateur ONTAP S3 ou pour les informations d'identification d'un utilisateur de locataire StorageGRID. Ceci sera utilisé pour configurer Velero ultérieurement. Vous pouvez créer un secret à partir de l'interface de ligne de commande ou de la console Web.

Pour créer un secret à partir de la console Web, sélectionnez secrets, puis cliquez sur clé/valeur Secret. Indiquez les valeurs pour le nom, la clé et la valeur des informations d'identification, 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 code secret associé aux informations d'identification d'utilisateur ONTAP S3 nommées identifiants ontap-s3 est créé.

The screenshot shows the OpenShift console interface for the 'Project: openshift-adp'. The 'Secrets' page is active, displaying a table of secrets. The table has columns for Name, Type, Size, and Created. Two secrets are listed:

Name	Type	Size	Created
builder-dockercfg-7g8ww	kubernetes.io/dockercfg	1	Apr 11, 2024, 10:52 AM
builder-token-rm4s	kubernetes.io/service-account-token	4	Apr 11, 2024, 10:52 AM

A 'Create' dropdown menu is open, showing options for creating a secret: Key/value secret, Image pull secret, Source secret, Webhook secret, and From YAML.

Project: openshift-adp ▾

Edit key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

Secret name *

 Unique name of the new secret.

Key *

Value

 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

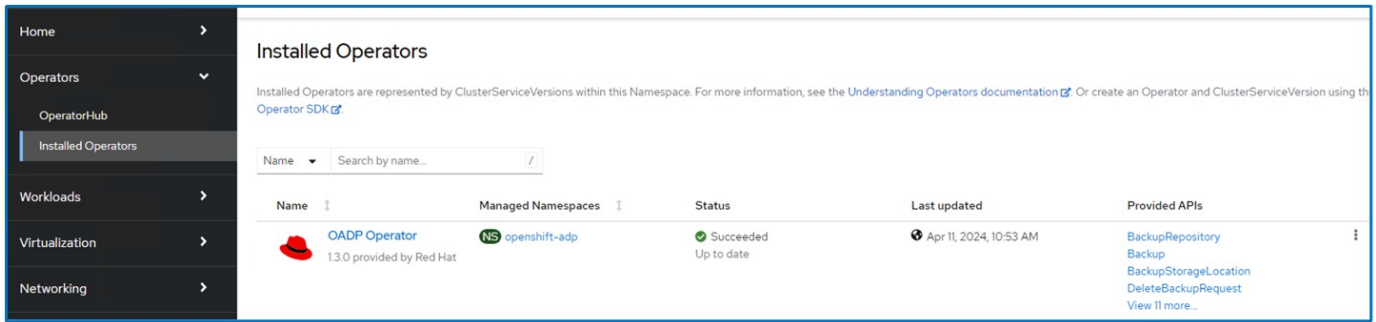
Pour créer un secret nommé sg-s3-credentials à partir de l'interface de ligne de commande, vous pouvez utiliser la commande suivante.

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

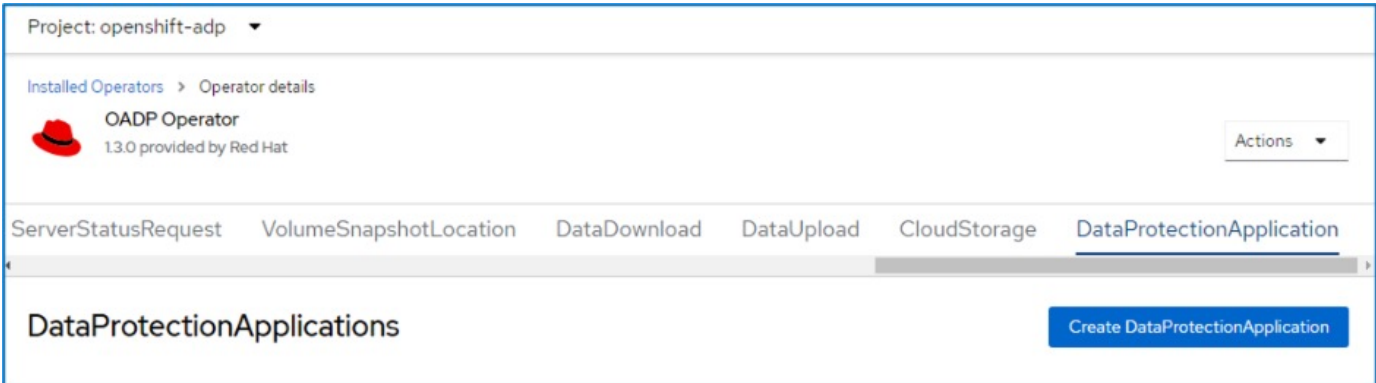
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

```
[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 **Create DataProtectionApplication**. Dans la vue formulaire, indiquez un nom pour l'application Dataprotection ou utilisez le nom par défaut.



Allez maintenant à la vue YAML et remplacez les informations de spécification comme indiqué dans les exemples de fichier 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 des spécifications du fichier yaml doit être configurée de manière appropriée pour les paramètres suivants, comme dans l'exemple ci-dessus

BackupLocation

ONTAP S3 ou StorageGRID S3 (avec ses informations d'identification et d'autres informations comme indiqué dans le yaml) est configuré comme emplacement de sauvegarde par défaut pour velero.

SnapshotLocation

Si vous utilisez des instantanés Container Storage interface (CSI), vous n'avez pas besoin de spécifier un emplacement de snapshot car vous allez créer un VolumeSnapshotClass CR pour enregistrer le pilote CSI. Dans cet exemple, vous utilisez Astra Trident CSI et vous avez déjà créé VolumeSnapShotClass CR à l'aide du pilote Trident CSI.

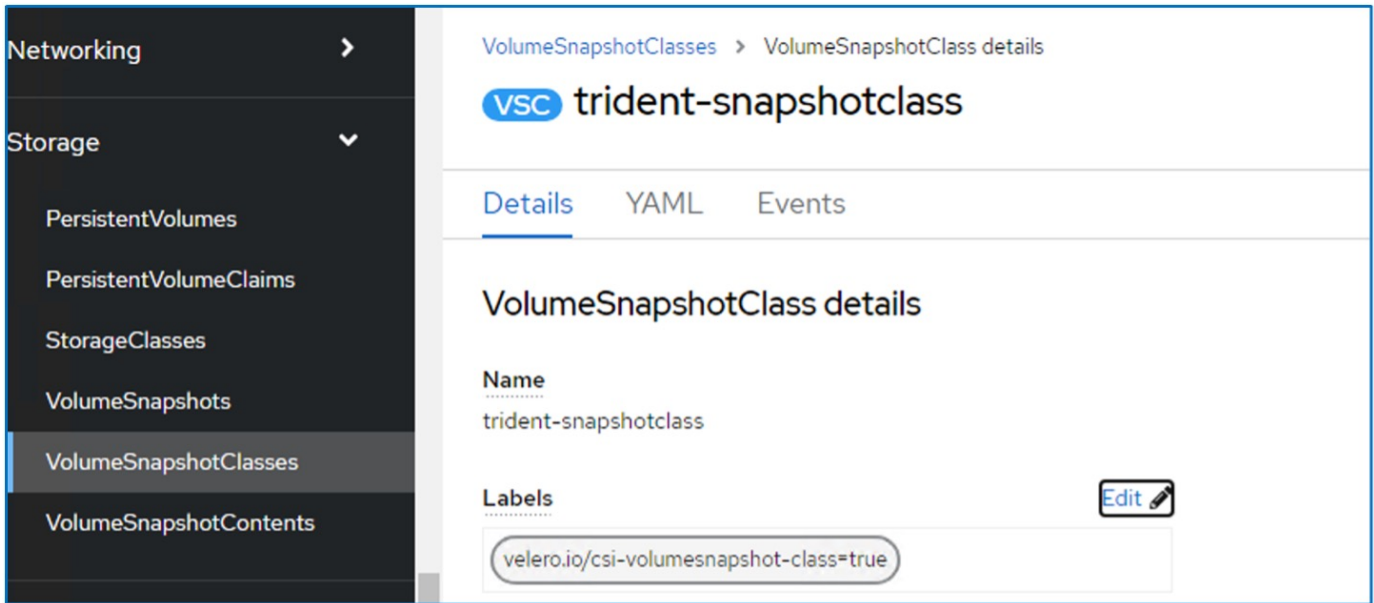
Activer le plug-in CSI

Ajoutez csi aux plug-ins par défaut de Velero pour sauvegarder les volumes persistants avec des snapshots CSI.

Les plug-ins Velero CSI, pour sauvegarder les PVC CSI, choisiront le VolumeSnapshotClass dans le cluster qui a le label **velero.io/csi-volumesnapshot-class** sur celui-ci. Pour cela

- Vous devez avoir créé la classe VolumeSnapshotClass.

- Modifiez le libellé de la classe trident-snapshotclass et définissez-le sur **velero.io/csi-volumesnapshot-class=true** comme indiqué ci-dessous.



The screenshot shows the Kubernetes dashboard interface. On the left, a sidebar menu is visible with 'Storage' expanded and 'VolumeSnapshotClasses' selected. The main content area displays the details for the 'trident-snapshotclass' VolumeSnapshotClass. The 'Name' field is 'trident-snapshotclass'. The 'Labels' field is highlighted with a rounded rectangle and contains the label 'velero.io/csi-volumesnapshot-class=true'. An 'Edit' button is visible next to the labels field.

Assurez-vous que les snapshots peuvent persister même si les objets VolumeSnapshot sont supprimés. Pour ce faire, définissez la **deletionPolicy** à conserver. Si ce n'est pas le cas, la suppression d'un namespace perd complètement toutes les demandes de volume virtuels sauvegardées.

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

VolumeSnapshotClasses > VolumeSnapshotClass details

VSC trident-snapshotclass

Details | YAML | Events

VolumeSnapshotClass details

Name
trident-snapshotclass

Labels Edit

velero.io/csi-volumesnapshot-class=true


Annotations
1 annotation

Driver
csi.trident.netapp.io

Deletion policy
Retain

Assurez-vous que l'application DataProtectionApplication est créée et qu'elle est en condition:réconciliée.

Installed Operators > Operator details


 **OADP Operator**
1.3.0 provided by Red Hat Actions

ServerStatusRequest | VolumeSnapshotLocation | DataDownload | DataUpload | CloudStorage | **DataProtectionApplication**

DataProtectionApplications

Create DataProtectionApplication


Name Search by name...

Name	Kind	Status	Labels
 velero-demo	DataProtectionApplication	Condition: Reconciled	No labels

L'opérateur OADP va créer un BackupStorageLocation correspondant. Il sera utilisé lors de la création d'une sauvegarde.

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat


Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRe

BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

Name ↕	Kind ↕	Status ↕	Labels ↕
 velero-demo-1	BackupStorageLocation	Phase: Available	<ul style="list-style-type: none"> app.kubernetes.io/component=bsl app.kubernetes.io/instance=velero-demo-1 app.kubernetes.io/manager=oadp-oper... app.kubernetes.io/n...=oadp-operator-ve... openshift.io/oadp=True openshift.io/oadp-registry=True

Création d'une sauvegarde à la demande pour les machines virtuelles dans OpenShift Virtualization

Cette section décrit comment créer une sauvegarde à la demande pour les machines virtuelles dans OpenShift Virtualization.

Étapes de création d'une sauvegarde d'une machine virtuelle

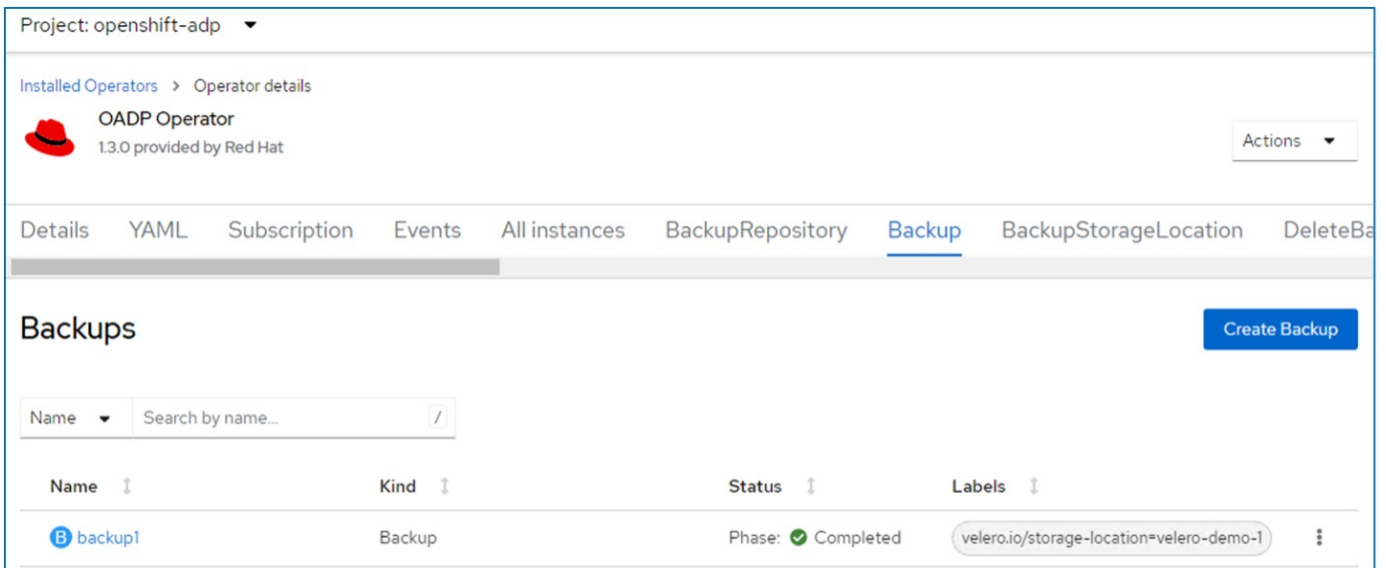
Pour créer une sauvegarde à la demande de l'ensemble de la machine virtuelle (métadonnées de la machine virtuelle et disques de la machine virtuelle), cliquez sur l'onglet **sauvegarde**. Cela crée une ressource personnalisée de sauvegarde (CR). Un exemple de yaml est fourni pour créer la CR de sauvegarde. En utilisant ce 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 qui soutiennent 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 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'affiche comme terminée.



The screenshot shows the OpenShift console interface for the 'openshift-adp' project. It displays the 'OADP Operator' details, version 1.3.0, provided by Red Hat. The 'Backup' tab is selected, showing a list of backups. A single backup named 'backup1' is listed with a status of 'Completed' and a label 'velero.io/storage-location=velero-demo-1'. A 'Create Backup' button is visible in the top right corner.

Name	Kind	Status	Labels
backup1	Backup	Phase: ✔ Completed	velero.io/storage-location=velero-demo-1

Vous pouvez inspecter la sauvegarde dans le stockage objet à l'aide d'une application de navigateur S3. Le chemin de la sauvegarde s'affiche dans le compartiment configuré avec le préfixe nom (velero/démobilackup). Vous pouvez voir le contenu de la sauvegarde inclut les snapshots de volume, les journaux et d'autres métadonnées de la machine virtuelle.



Dans StorageGRID, vous pouvez également utiliser la console S3 disponible dans le gestionnaire de locataires pour afficher les objets de sauvegarde.

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 sur un planning, vous devez créer une demande de modification d'horaires. Le planning est simplement une expression cron qui vous permet de spécifier l'heure à laquelle vous souhaitez créer la sauvegarde. Un exemple de yaml pour créer une demande de modification d'horaire.

```

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 7:00 chaque jour. Les espaces de noms à inclure dans la sauvegarde et l'emplacement de stockage de la sauvegarde sont également spécifiés. Par conséquent, au lieu d'une CR de sauvegarde, la CR de planification est utilisée pour créer une sauvegarde à l'heure et à la fréquence spécifiées.

Une fois le planning créé, il est activé.

Project: openshift-adp ▾



Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore Schedule

Schedules


Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1	Schedule	Phase:  Enabled	No labels

Les sauvegardes seront créées en fonction de ce planning et peuvent être affichées à partir de l'onglet sauvegarde.

Project: openshift-adp ▾

Installed Operators > Operator details


 **OADP Operator**
1.3.0 provided by Red Hat

Events All instances BackupRepository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups

[Create Backup](#)

Name ▾ Search by name... /

Name	Kind	Status	Labels
 schedule1-20240416140507	Backup	Phase: InProgress	<ul style="list-style-type: none"> velero.io/schedule-name=schedule1 velero.io/storage-location=velero-demo-1

Restaurer une machine virtuelle à partir d'une sauvegarde

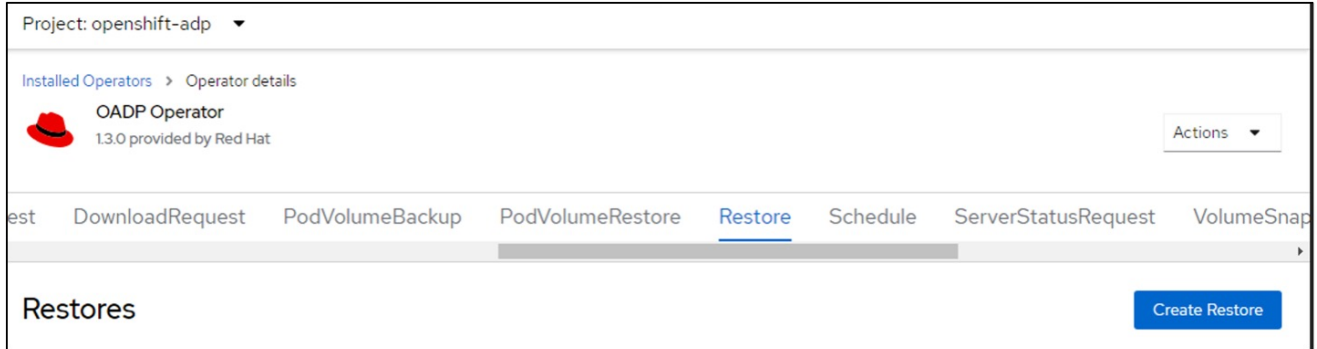
Cette section décrit comment restaurer une ou plusieurs machines virtuelles à partir d'une sauvegarde.

Prérequis

Pour effectuer une restauration à partir d'une sauvegarde, supposons que l'espace de noms dans lequel existait la machine virtuelle a été accidentellement supprimé.

Restaurer dans le même espace de noms

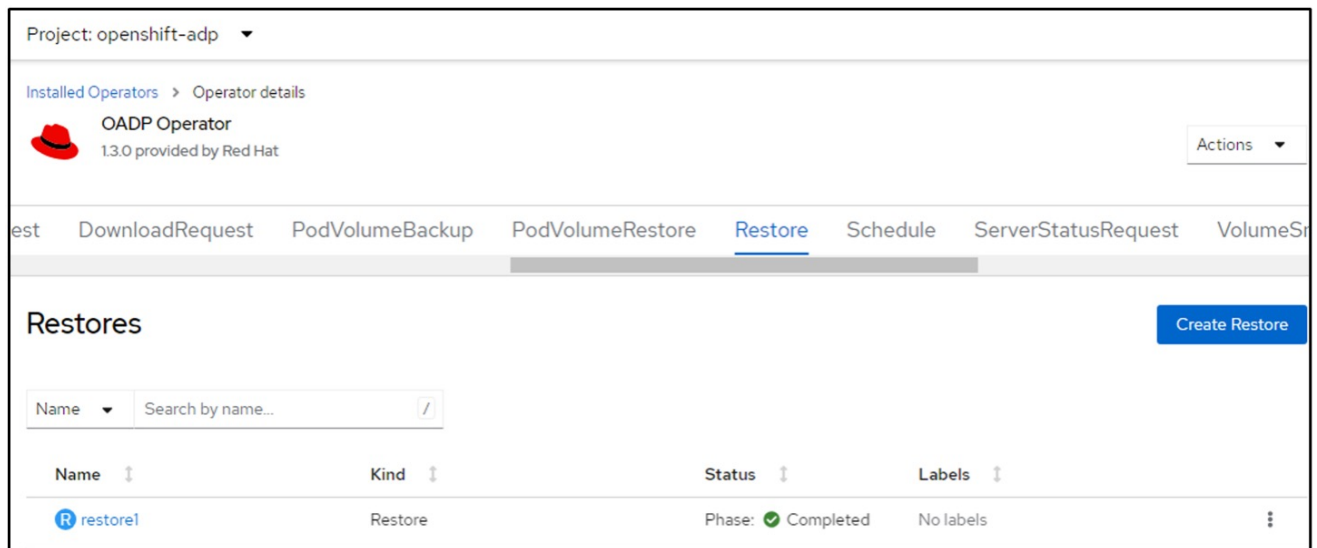
Pour restaurer à partir de la sauvegarde que nous venons de créer, nous devons créer une ressource personnalisée de restauration (CR). Nous devons lui fournir un nom, fournir le nom de la sauvegarde à partir de laquelle nous voulons restaurer et définir les PV de restauration sur true. Des paramètres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



The screenshot shows the OADP Operator interface. At the top, it says 'Project: openshift-adp'. Below that, there's a breadcrumb 'Installed Operators > Operator details'. The operator is identified as 'OADP Operator' with version '1.3.0 provided by Red Hat'. A navigation bar includes 'DownloadRequest', 'PodVolumeBackup', 'PodVolumeRestore', 'Restore' (selected), 'Schedule', 'ServerStatusRequest', and 'VolumeSnap'. Below the navigation bar, the 'Restores' section is visible with a 'Create Restore' button.

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

Lorsque la phase affiche terminé, vous pouvez voir que les machines virtuelles ont été restaurées à l'état au moment où l'instantané a été pris. (Si la sauvegarde a été créée lors de l'exécution de la machine virtuelle, la restauration de la machine virtuelle à partir de la sauvegarde démarre la machine virtuelle restaurée et la met en état d'exécution). La machine virtuelle est restaurée dans le même espace de noms.



This screenshot shows the OADP Operator interface after a restore operation. The 'Restore' tab is selected. Below the navigation bar, the 'Restores' section shows a table with one entry:

Name	Kind	Status	Labels
restore1	Restore	Phase: ✔ Completed	No labels

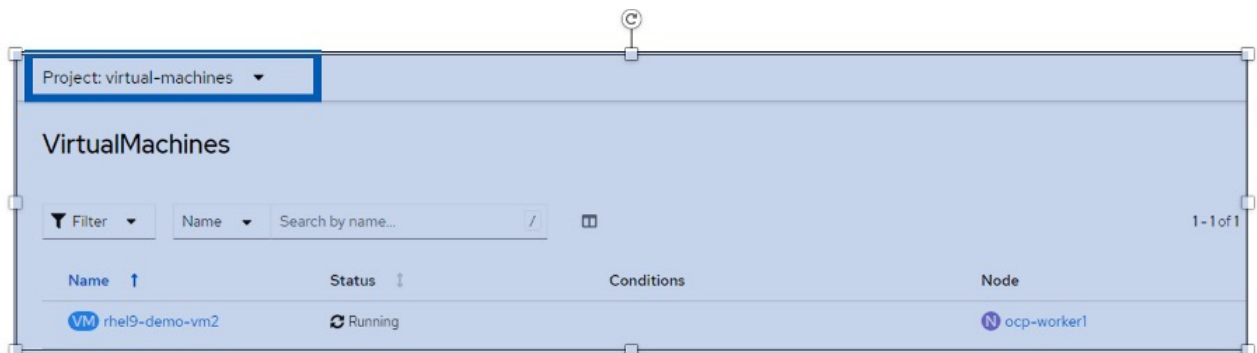
Restauration dans un autre espace de noms

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

L'exemple de fichier yaml suivant crée une CR de restauration pour restaurer une machine virtuelle et ses disques dans l'espace de nom de démonstration des machines virtuelles lorsque la sauvegarde a été effectuée dans l'espace de noms des machines virtuelles.

```
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
```

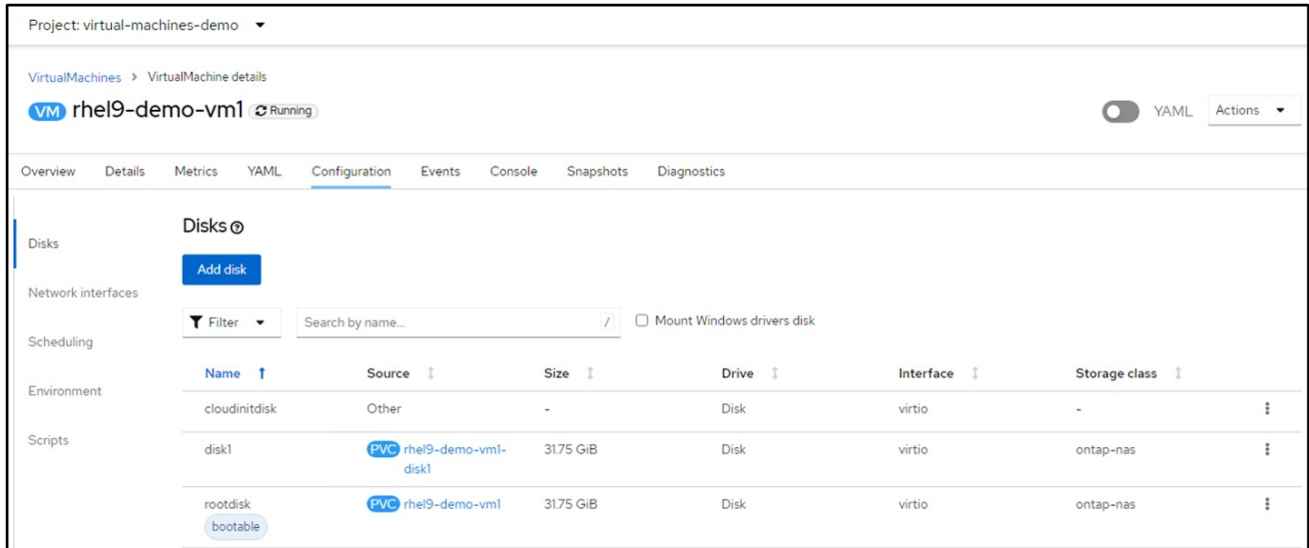
Lorsque la phase affiche terminé, vous pouvez voir que les machines virtuelles ont été restaurées à l'état au moment où l'instantané a été pris. (Si la sauvegarde a été créée lors de l'exécution de la machine virtuelle, la restauration de la machine virtuelle à partir de la sauvegarde démarre la machine virtuelle restaurée et la met en état d'exécution). La machine virtuelle est restaurée dans un espace de noms différent, comme spécifié dans le yaml.



Restauration vers une autre classe de stockage

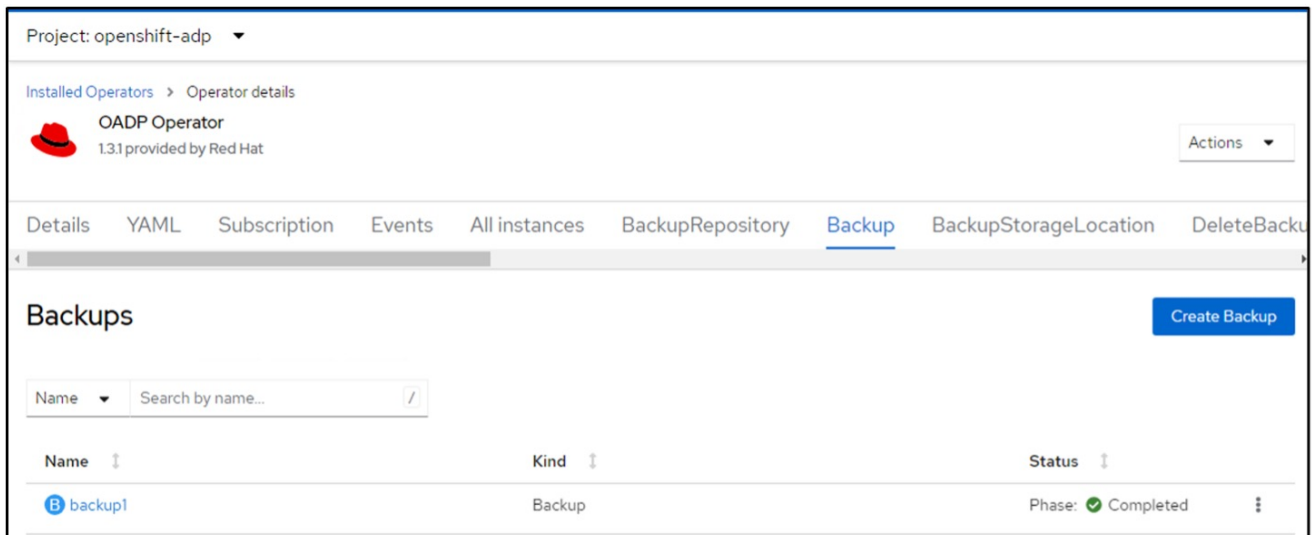
Velero fournit une capacité générique de modifier les ressources pendant la restauration en spécifiant des correctifs json. Les correctifs json sont appliqués aux ressources avant leur restauration. Les patches json sont spécifiés dans un configmap et le configmap est référencé dans la commande restore. Cette fonctionnalité vous permet de restaurer à l'aide d'une classe de stockage différente.

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



The screenshot shows the configuration page for a virtual machine named 'rhel9-demo-vm1' in the 'virtual-machines-demo' project. The 'Configuration' tab is active, displaying a table of disks. The table has columns for Name, Source, Size, Drive, Interface, and Storage class. Two disks are listed: 'disk1' and 'rootdisk', both using the 'ontap-nas' storage class.

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	3175 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	3175 GiB	Disk	virtio	ontap-nas



The screenshot shows the 'Backup' page for the 'OADP Operator' in the 'openshift-adp' project. The 'Backup' tab is active, displaying a table of backups. One backup named 'backup1' is listed with a status of 'Completed'.

Name	Kind	Status
backup1	Backup	Phase: Completed

Simulez une perte de la machine virtuelle en supprimant cette dernière.

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 un mappage de configuration (console) dans l'espace de noms openshift-adp comme suit :
Renseignez les détails comme indiqué dans la capture d'écran :
Sélectionnez namespace : openshift-adp

Name : 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"
```

Project: openshift-adp

Edit ConfigMap

Config maps hold key-value pairs that can be used in pods to read application configuration.

Configure via: Form view YAML view

Name *

change-storage-class-config

A unique name for the ConfigMap within the project

Immutable
Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated

Data

Data contains the configuration data that is in UTF-8 range

[Remove key/value](#)

Key *

change-storage-class-config.yaml

Value

[Browse...](#)

Drag and drop file with your value here or browse to upload it.

```
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
```

[Add key/value](#)

L'objet de mappage de configuration résultant doit 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>

```

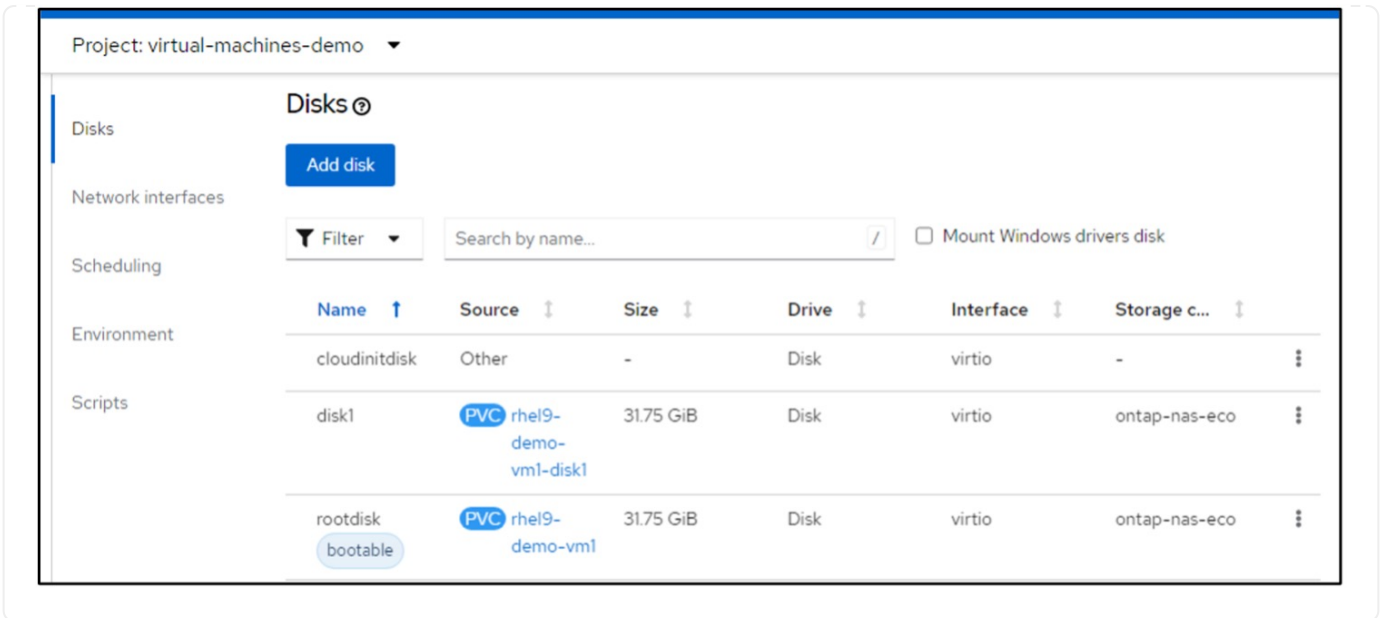
Cette carte de configuration applique la règle de modificateur de ressource lors de la création de la restauration. Un correctif sera appliqué pour remplacer le nom de classe de stockage par ontap-nas-eco pour toutes les demandes de volume persistant commençant par rhel.

Étape 2

Pour restaurer la machine virtuelle, utilisez la commande suivante depuis l'interface de ligne de commande 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 namespace avec les disques créés à l'aide de la classe de stockage ontap-nas-eco.



Suppression des sauvegardes et des restaurations dans à l'aide de Velero

Cette section décrit comment supprimer les sauvegardes et les restaurations des machines virtuelles dans OpenShift Virtualization à l'aide de Velero.

Suppression d'une sauvegarde

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

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

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

Téléchargez l'interface de ligne de commande comme indiqué dans les instructions du "[Documentation Velero](#)".

Exécutez la commande DELETE suivante à l'aide de l'interface de ligne de commande Velero

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

Suppression d'une restauration

Vous pouvez supprimer la CR de restauration à l'aide de l'interface de ligne de commande Velero

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


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

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

Informations sur le copyright

Copyright © 2024 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 DÉLICTELLE (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.