Schützen Sie VMs mit Tools von Drittanbietern

NetApp virtualization solutions

NetApp
January 12, 2026

Inhalt

Schützen Sie VMs mit Tools von Drittanbietern

Erfahren Sie mehr über den Datenschutz für VMs in Red Hat OpenShift Virtualization mithilfe der OpenShift API for Data Protection (OADP).

OpenShift API for Data Protection (OADP) mit Velero bietet Sicherungs-, Wiederherstellungs- und Notfallwiederherstellungsfunktionen für VMs in OpenShift Virtualization. Verwenden Sie Trident CSI-Snapshots, um persistente Volumes und VM-Metadaten auf NetApp ONTAP S3 oder StorageGRID S3 zu sichern. OADP lässt sich in Velero-APIs und CSI-Speichertreiber integrieren, um Datenschutzvorgänge für containerisierte VMs zu verwalten.

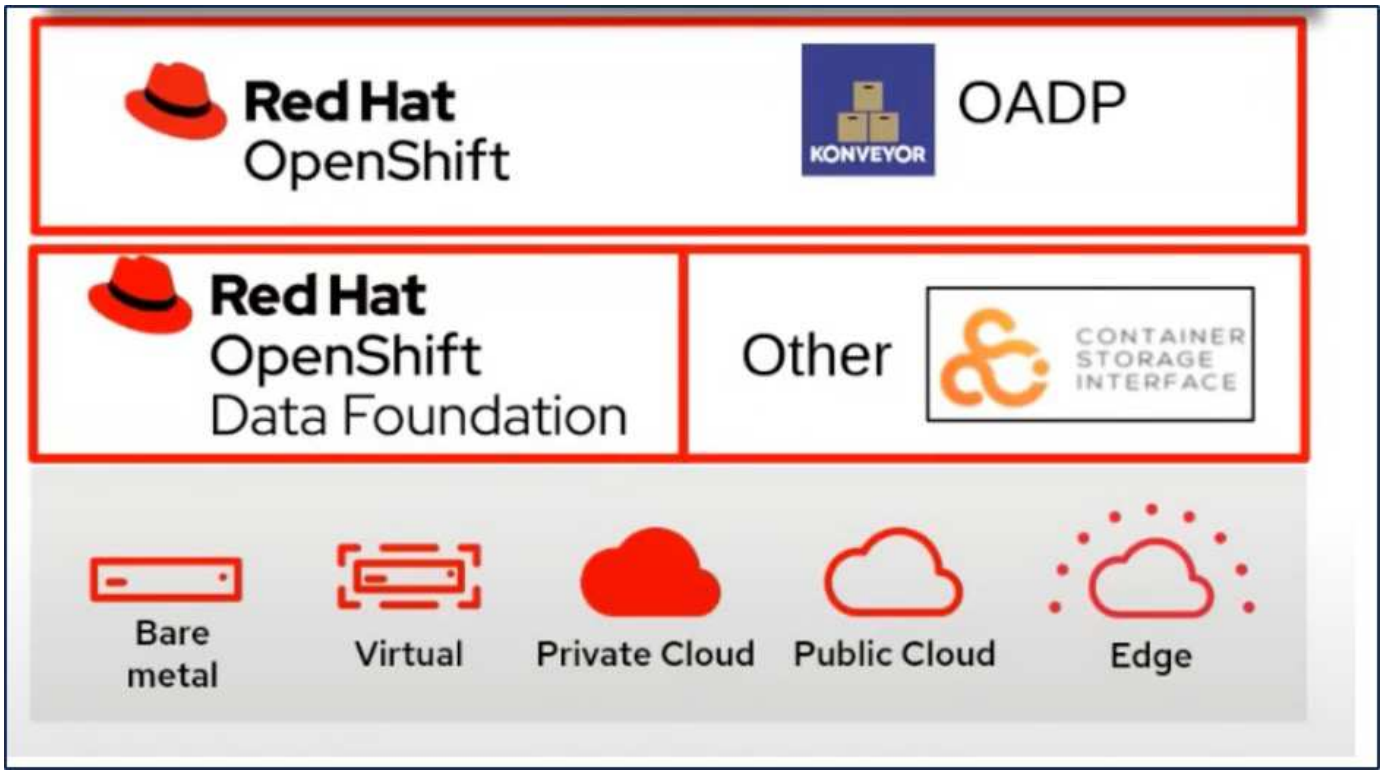
Virtuelle Maschinen in der OpenShift-Virtualisierungsumgebung sind containerisierte Anwendungen, die in den Worker-Knoten Ihrer OpenShift-Containerplattform ausgeführt werden. Es ist wichtig, die VM-Metadaten sowie die persistenten Datenträger der VMs zu schützen, damit Sie sie wiederherstellen können, wenn sie verloren gehen oder beschädigt werden.

Die persistenten Festplatten der OpenShift Virtualization VMs können durch ONTAP Speicher gesichert werden, der in den OpenShift-Cluster integriert ist, indem"Trident CSI" . In diesem Abschnitt verwenden wir"OpenShift-API für Datenschutz (OADP)" zur Durchführung von Backups von VMs inklusive der Datenvolumes auf

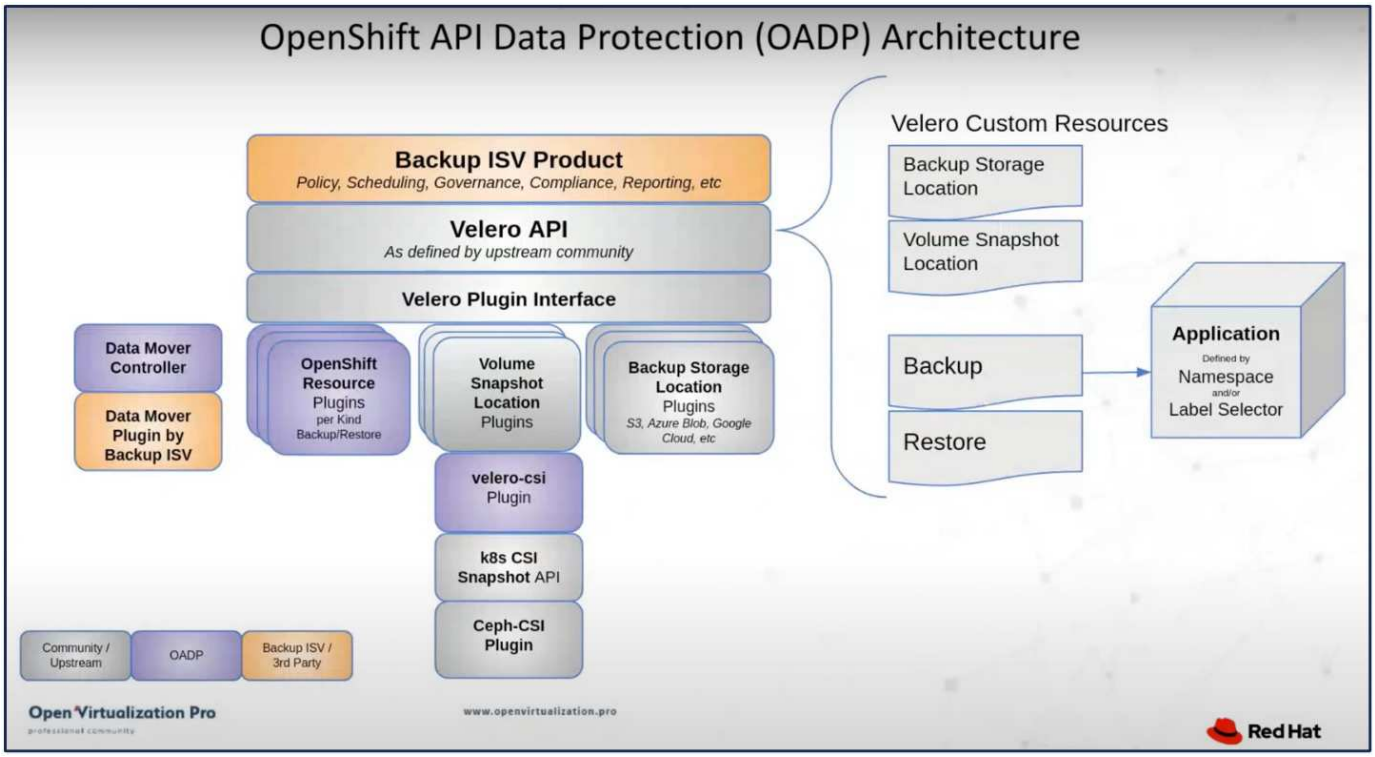
- ONTAP Objektspeicher
- StorageGrid

Bei Bedarf stellen wir dann eine Wiederherstellung aus dem Backup her.

OADP ermöglicht die Sicherung, Wiederherstellung und Notfallwiederherstellung von Anwendungen auf einem OpenShift-Cluster. Zu den Daten, die mit OADP geschützt werden können, gehören Kubernetes-Ressourcenobjekte, persistente Volumes und interne Images.



Red Hat OpenShift nutzt die von den OpenSource-Communitys entwickelten Lösungen zum Datenschutz. "Velero" ist ein Open-Source-Tool zum sicheren Sichern und Wiederherstellen, Durchführen einer Notfallwiederherstellung und Migrieren von Kubernetes-Clusterressourcen und persistenten Volumes. Um Velero einfach verwenden zu können, hat OpenShift den OADP-Operator und das Velero-Plugin zur Integration mit den CSI-Speichertreibern entwickelt. Der Kern der bereitgestellten OADP-APIs basiert auf den Velero-APIs. Nach der Installation und Konfiguration des OADP-Operators basieren die durchführbaren Sicherungs-/Wiederherstellungsvorgänge auf den von der Velero-API bereitgestellten Vorgängen.



OADP 1.3 ist im Operator Hub des OpenShift-Clusters 4.12 und höher verfügbar. Es verfügt über einen integrierten Data Mover, der CSI-Volume-Snapshots in einen Remote-Objektspeicher verschieben kann. Dies sorgt für Portabilität und Haltbarkeit, indem Snapshots während der Sicherung an einen Objektspeicherort verschoben werden. Die Snapshots stehen dann nach Katastrophen zur Wiederherstellung zur Verfügung.

Im Folgenden sind die Versionen der verschiedenen Komponenten aufgeführt, die für die Beispiele in diesem Abschnitt verwendet wurden.

- OpenShift Cluster 4.14
- OpenShift-Virtualisierung über Operator installiertOpenShift Virtualization Operator bereitgestellt von Red Hat
- OADP Operator 1.13 bereitgestellt von Red Hat
- Velero CLI 1.13 für Linux
- Trident 24.02
- ONTAP 9.12

"Trident CSI" "OpenShift-API für Datenschutz (OADP)" "Velero"

Installieren Sie den Red Hat OpenShift API for Data Protection (OADP)-Operator

Installieren Sie den OpenShift API for Data Protection (OADP) Operator, um Sicherungs- und Wiederherstellungsfunktionen für VMs in OpenShift Virtualization zu aktivieren. Dieses Verfahren umfasst die Bereitstellung des OADP-Operators vom OpenShift Operator Hub, die Konfiguration von Velero zur Verwendung von NetApp ONTAP S3 oder StorageGRID als Sicherungsziel und das Einrichten der erforderlichen Geheimnisse und Sicherungsspeicherorte.

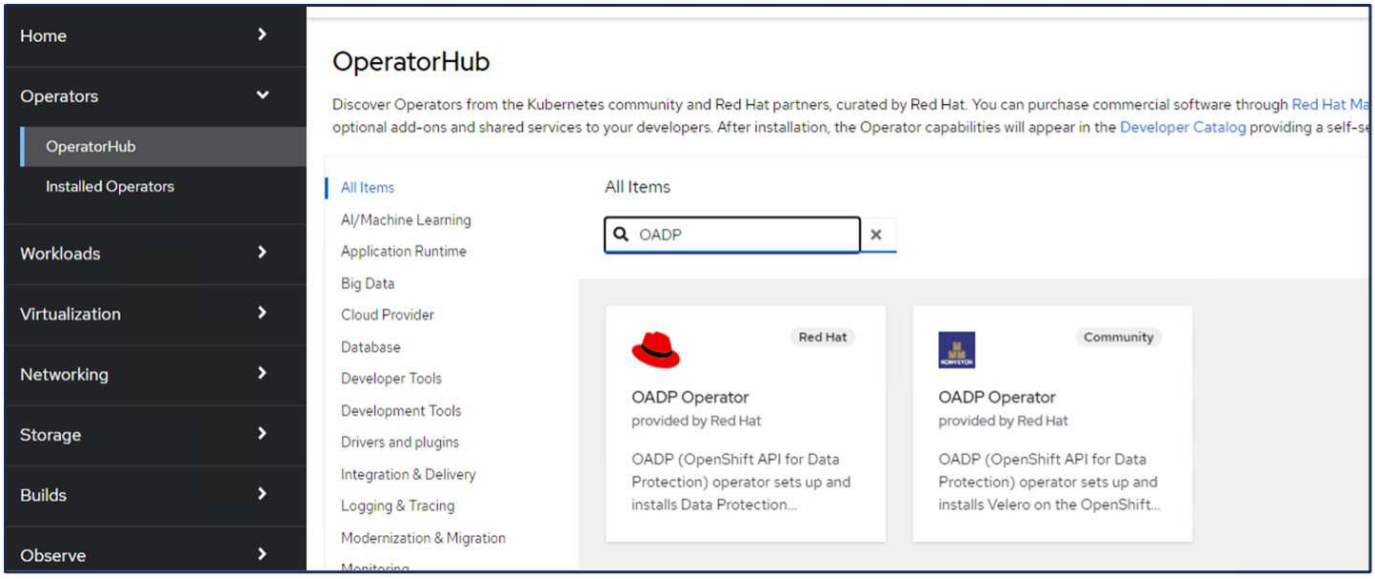
Voraussetzungen

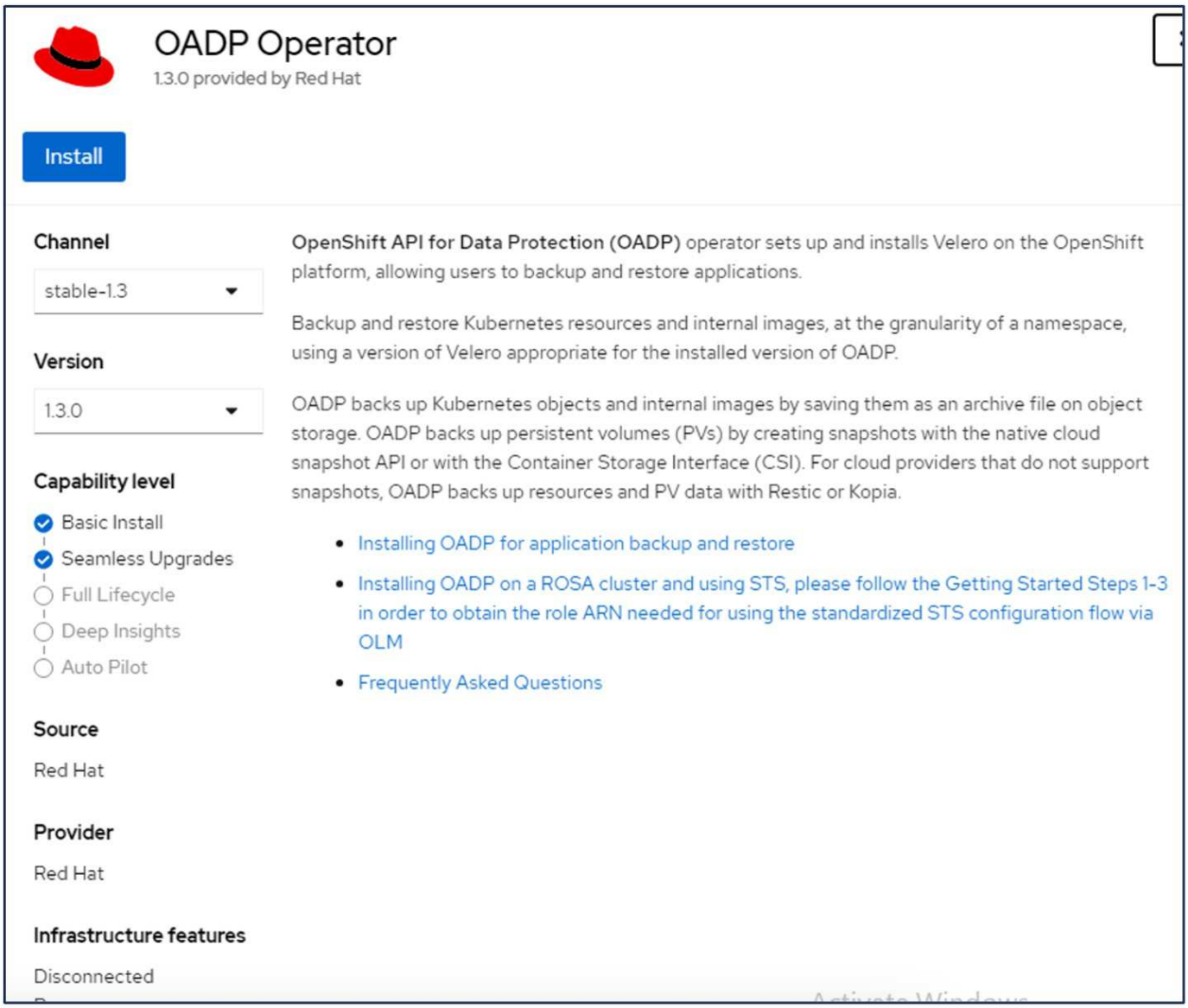
- Ein Red Hat OpenShift-Cluster (neuer als Version 4.12), installiert auf einer Bare-Metal-Infrastruktur mit RHCOS-Worker-Knoten
- Ein NetApp ONTAP -Cluster, der über Trident in den Cluster integriert ist
- Ein Trident -Backend, das mit einem SVM auf einem ONTAP -Cluster konfiguriert ist
- Eine auf dem OpenShift-Cluster konfigurierte StorageClass mit Trident als Provisioner
- Auf dem Cluster erstellte Trident Snapshot-Klasse
- Cluster-Admin-Zugriff auf den Red Hat OpenShift-Cluster
- Administratorzugriff auf NetApp ONTAP -Cluster
- OpenShift-Virtualisierungsoperator installiert und konfiguriert
- In einem Namespace auf OpenShift Virtualization bereitgestellte VMs
- Eine Admin-Workstation mit installierten und zu $PATH hinzugefügten Tridentctl- und OC-Tools

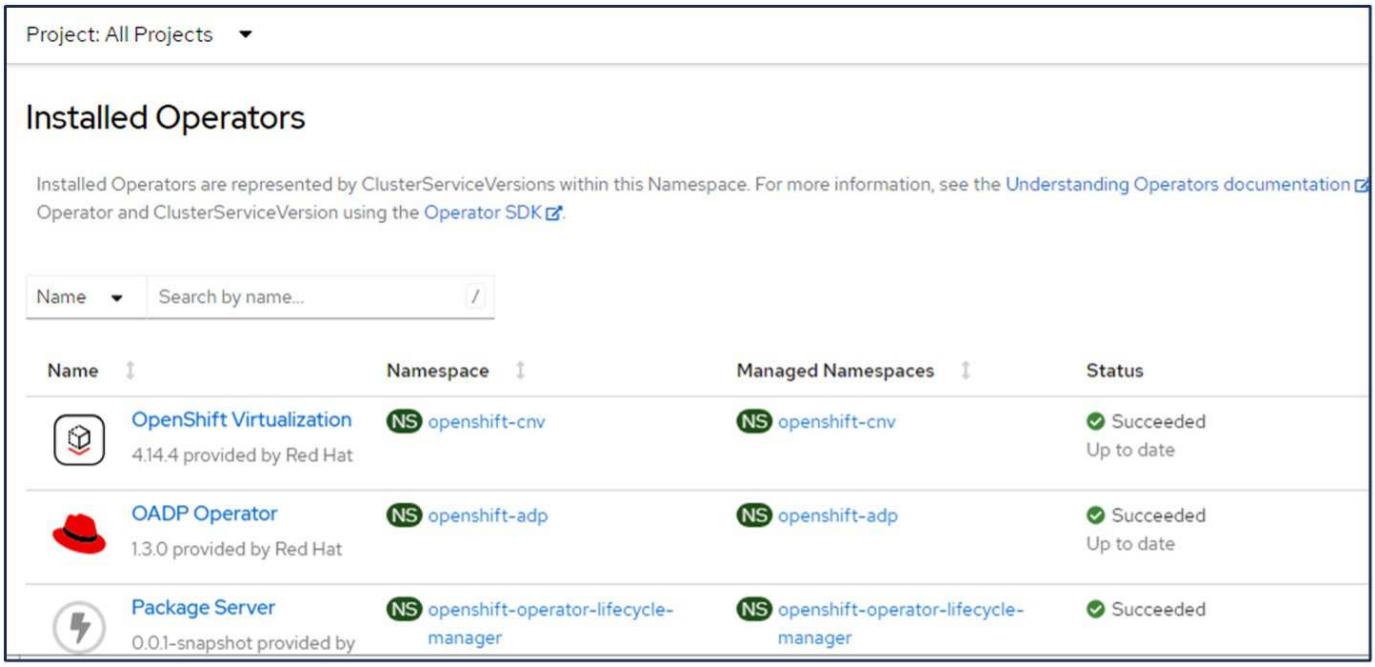
Wenn Sie eine Sicherung einer VM im Status „Ausgeführt“ erstellen möchten, müssen Sie den QEMU-Gast-Agent auf dieser virtuellen Maschine installieren. Wenn Sie die VM mithilfe einer vorhandenen Vorlage installieren, wird der QEMU-Agent automatisch installiert. QEMU ermöglicht es dem Gastagenten, während des Snapshot-Prozesses laufende Daten im Gastbetriebssystem stillzulegen und so eine mögliche Datenbeschädigung zu vermeiden. Wenn Sie QEMU nicht installiert haben, können Sie die virtuelle Maschine stoppen, bevor Sie eine Sicherung durchführen.

Schritte zur Installation des OADP-Operators

1. Gehen Sie zum Operator Hub des Clusters und wählen Sie den Red Hat OADP-Operator aus. Verwenden Sie auf der Installationsseite alle Standardauswahlen und klicken Sie auf „Installieren“. Verwenden Sie auf der nächsten Seite erneut alle Standardeinstellungen und klicken Sie auf Installieren. Der OADP-Operator wird im Namespace openshift-adp installiert.




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
openshift-cnv
openshift-cnv
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

Voraussetzungen für die Velero-Konfiguration mit Ontap S3-Details

Nachdem die Installation des Operators erfolgreich war, konfigurieren Sie die Velero-Instanz. Velero kann für die Verwendung von S3-kompatiblem Object Storage konfiguriert werden. Konfigurieren Sie ONTAP S3 mit den Verfahren, die im"Abschnitt „Object Storage Management“ der ONTAP Dokumentation" . Für die Integration mit Velero benötigen Sie die folgenden Informationen aus Ihrer ONTAP S3-Konfiguration.

- Eine logische Schnittstelle (LIF), die für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldeinformationen für den Zugriff auf S3, einschließlich des Zugriffsschlüssels und des geheimen Zugriffsschlüssels
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte auf dem Objektspeicherserver ein TLS-Zertifikat installiert werden.

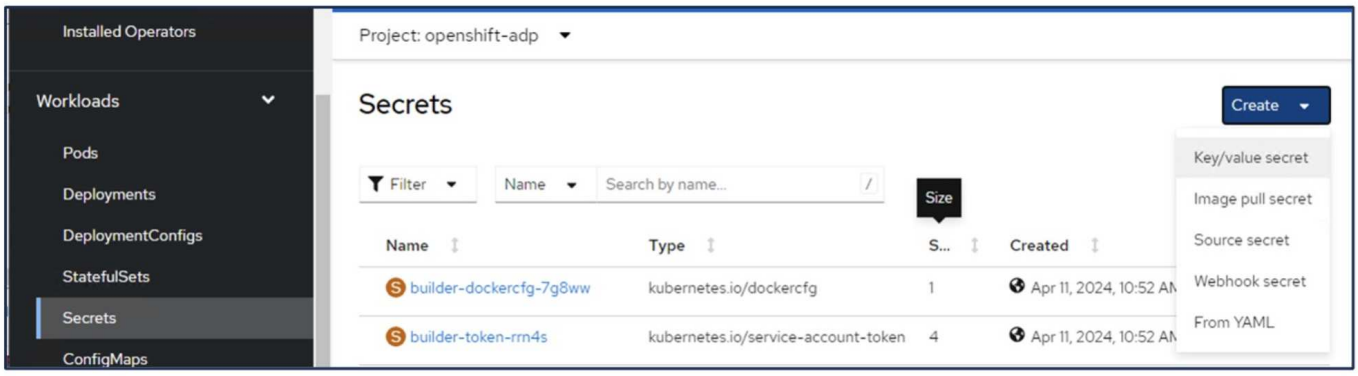
Voraussetzungen für die Velero-Konfiguration mit StorageGrid S3-Details

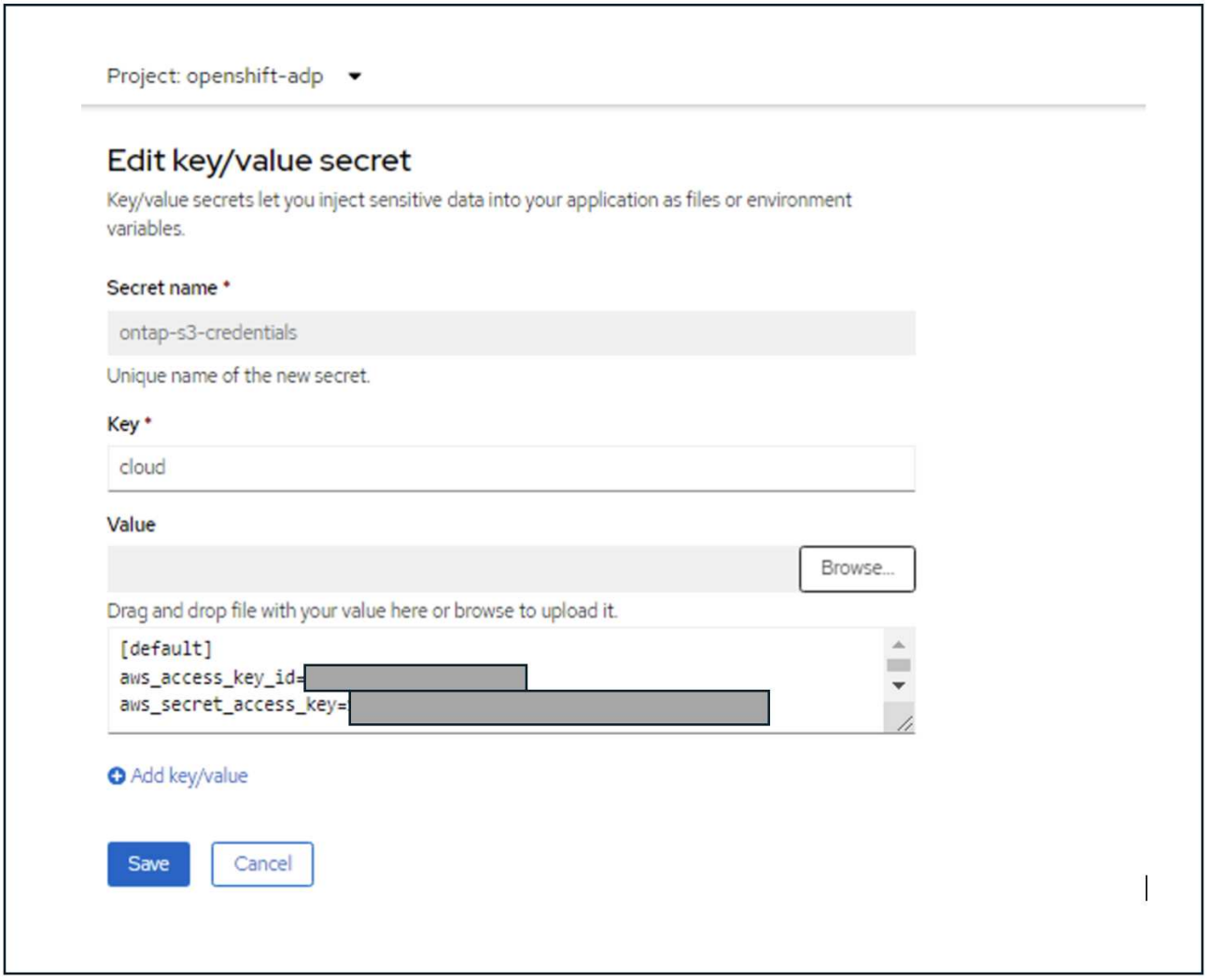
Velero kann für die Verwendung von S3-kompatiblem Object Storage konfiguriert werden. Sie können StorageGrid S3 mit den im folgenden Abschnitt beschriebenen Verfahren konfigurieren."StorageGrid-Dokumentation" . Für die Integration mit Velero benötigen Sie die folgenden Informationen aus Ihrer StorageGrid S3-Konfiguration.

- Der Endpunkt, der für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldeinformationen für den Zugriff auf S3, einschließlich des Zugriffsschlüssels und des geheimen Zugriffsschlüssels
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte auf dem Objektspeicherserver ein TLS-Zertifikat installiert werden.

Schritte zum Konfigurieren von Velero

- Erstellen Sie zunächst ein Geheimnis für die Benutzeranmeldeinformationen eines ONTAP S3 oder eines StorageGrid Tenant. Dies wird später zur Konfiguration von Velero verwendet. Sie können ein Geheimnis über die CLI oder die Webkonsole erstellen. Um ein Geheimnis über die Webkonsole zu erstellen, wählen Sie „Geheimnisse“ aus und klicken Sie dann auf „Schlüssel/Wert-Geheimnis“. Geben Sie die Werte für den Anmeldeinformationsnamen, den Schlüssel und den Wert wie angezeigt ein. Stellen Sie sicher, dass Sie die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres S3-Benutzers verwenden. Geben Sie dem Geheimnis einen passenden Namen. Im folgenden Beispiel wird ein Geheimnis mit ONTAP S3-Benutzeranmeldeinformationen namens ontap-s3-credentials erstellt.

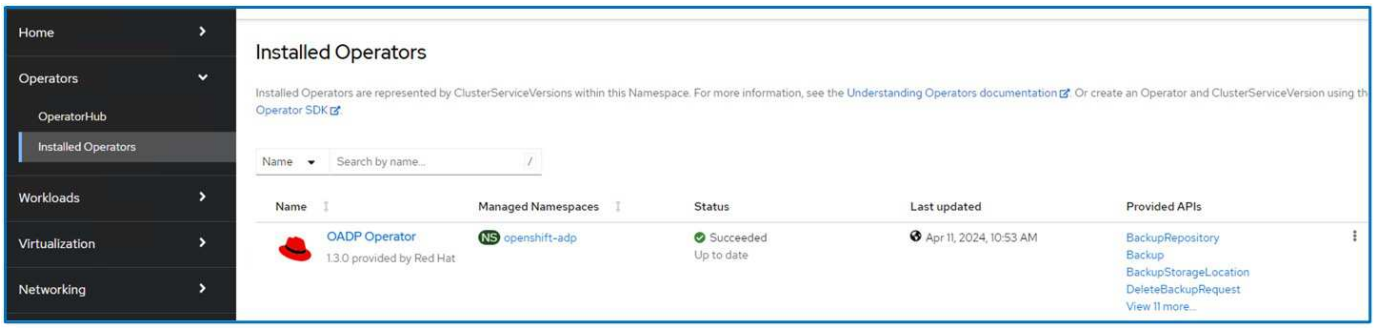




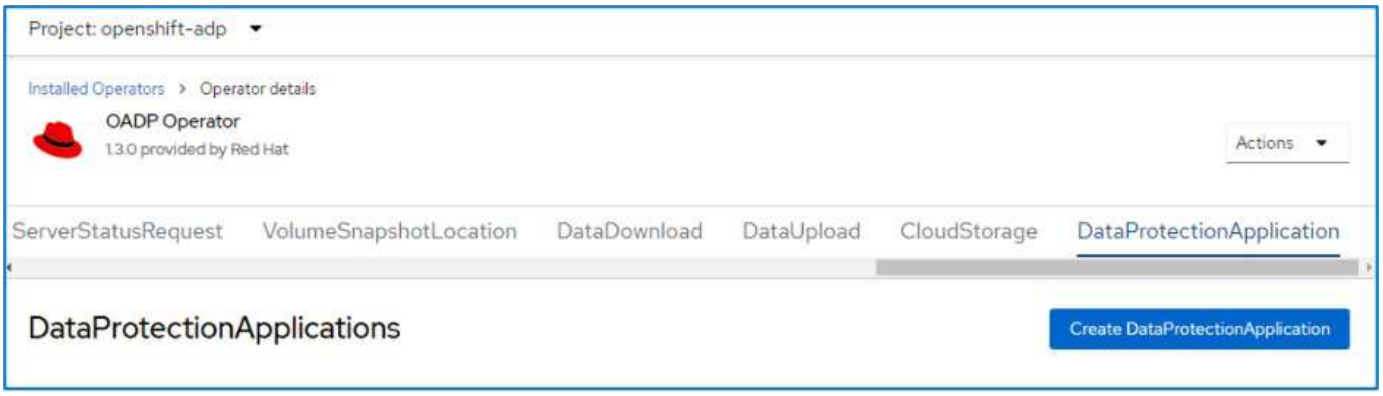
Um ein Geheimnis mit dem Namen sg-s3-credentials über die CLI zu erstellen, können Sie den folgenden Befehl verwenden.

```
# 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>
```

- Um Velero zu konfigurieren, wählen Sie als Nächstes im Menüpunkt „Operatoren“ die Option „Installierte Operatoren“ aus, klicken Sie auf den OADP-Operator und wählen Sie dann die Registerkarte „DataProtectionApplication“ aus.



Klicken Sie auf „DataProtectionApplication erstellen“. Geben Sie in der Formularansicht einen Namen für die DataProtection-Anwendung ein oder verwenden Sie den Standardnamen.



Gehen Sie nun zur YAML-Ansicht und ersetzen Sie die Spezifikationsinformationen wie in den folgenden YAML-Dateibeispielen gezeigt.

Beispiel-YAML-Datei zum Konfigurieren von Velero mit ONTAP S3 als Backup-Speicherort

```
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
```

Beispiel-YAML-Datei zum Konfigurieren von Velero mit StorageGrid S3 als Backup- und Snapshot-Speicherort

```
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
```

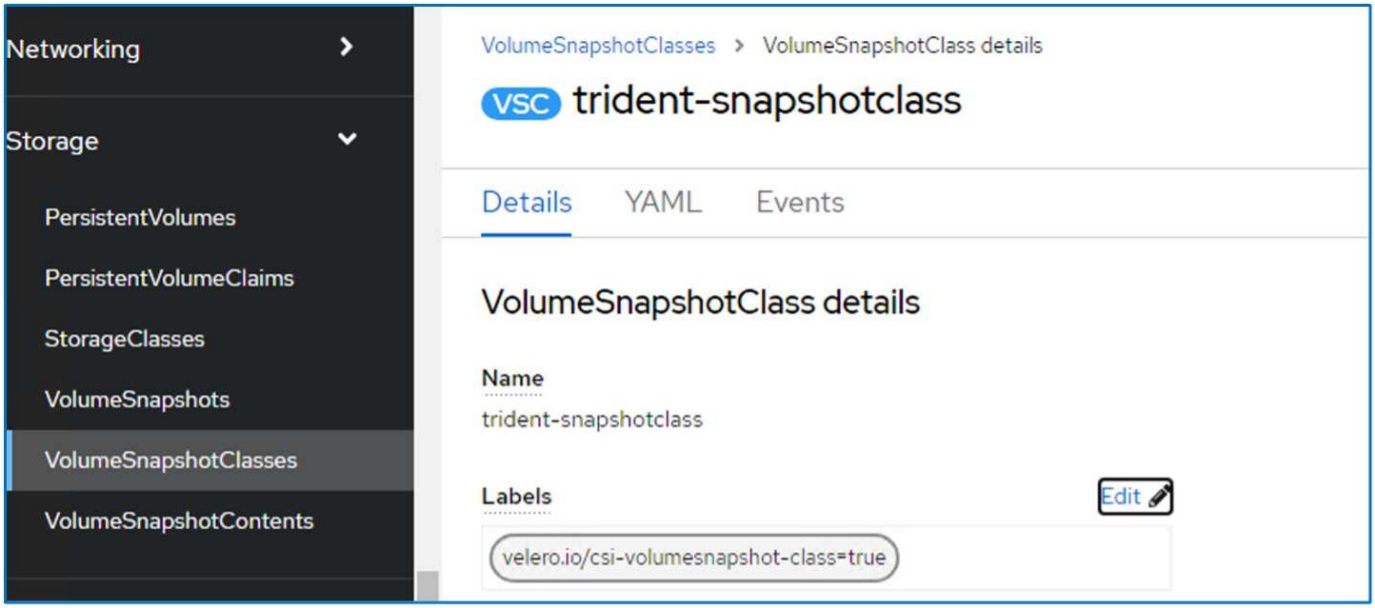
Der Abschnitt „Spec“ in der YAML-Datei sollte für die folgenden Parameter entsprechend dem obigen Beispiel konfiguriert werden.

backupLocations ONTAP S3 oder StorageGrid S3 (mit seinen Anmeldeinformationen und anderen Informationen, wie im YAML angezeigt) ist als Standard-BackupLocation für Velero konfiguriert.

snapshotLocations Wenn Sie Container Storage Interface (CSI)-Snapshots verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie ein VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Trident CSI und haben zuvor VolumeSnapShotClass CR mit dem Trident CSI-Treiber erstellt.

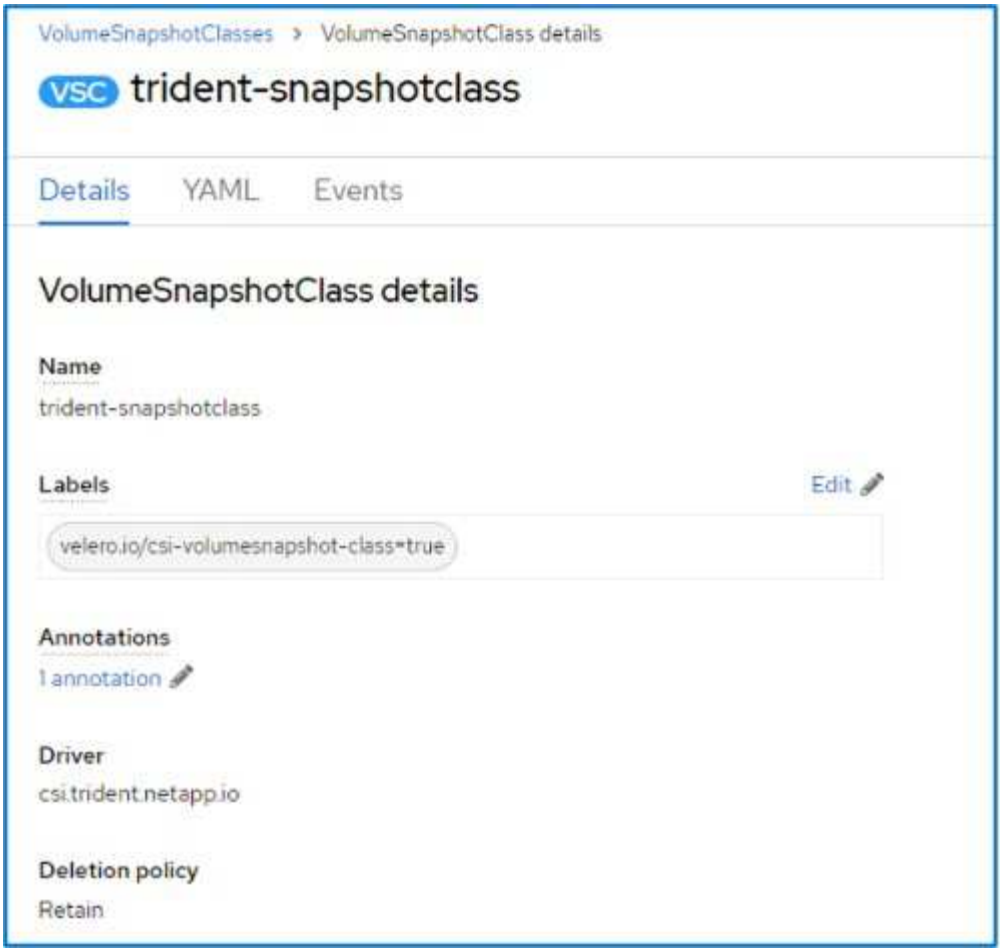
CSI-Plugin aktivieren Fügen Sie csi zu den Standard-Plugins für Velero hinzu, um persistente Volumes mit CSI-Snapshots zu sichern. Die Velero CSI-Plugins wählen zum Sichern von CSI-gestützten PVCs die VolumeSnapshotClass im Cluster aus, auf die das Label **velero.io/csi-volumesnapshot-class** gesetzt ist. Dafür

- Sie müssen die Trident VolumeSnapshotClass erstellt haben.
- Bearbeiten Sie die Bezeichnung der Trident-Snapshot-Klasse und setzen Sie sie wie unten gezeigt auf **velero.io/csi-volumesnapshot-class=true**.

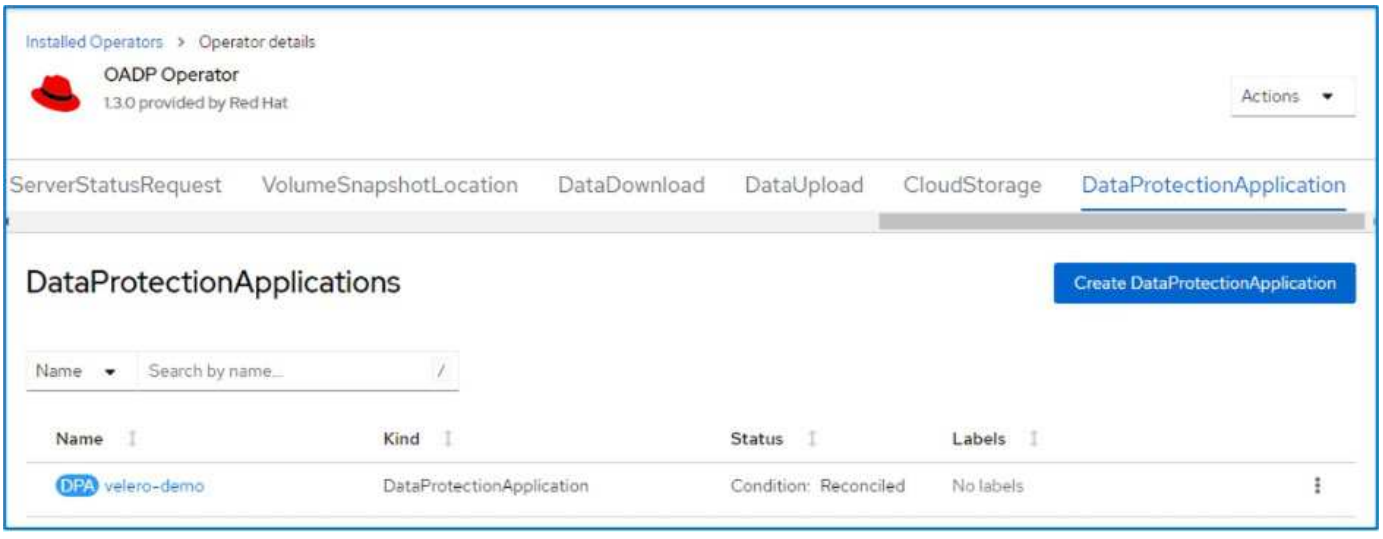


Stellen Sie sicher, dass die Snapshots auch dann bestehen bleiben, wenn die VolumeSnapshot-Objekte gelöscht werden. Dies kann durch Festlegen der **deletionPolicy** auf „Beibehalten“ erfolgen. Andernfalls gehen beim Löschen eines Namespace alle darin jemals gesicherten PVCs vollständig verloren.

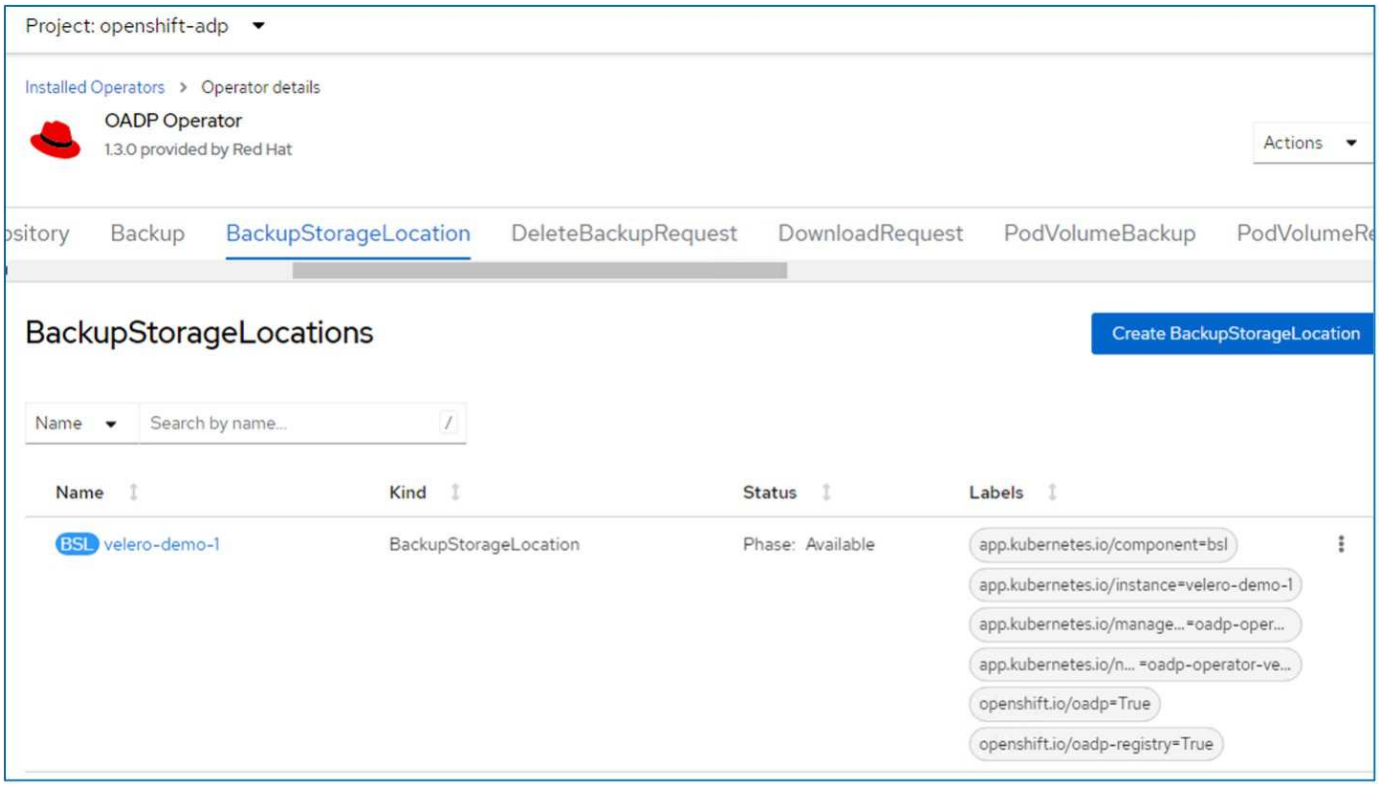
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Stellen Sie sicher, dass die DataProtectionApplication erstellt wurde und sich im Zustand „Abgestimmt“ befindet.



Der OADP-Operator erstellt einen entsprechenden BackupStorageLocation. Dieser wird beim Erstellen eines Backups verwendet.



Erstellen Sie On-Demand-Backups für VMs in Red Hat OpenShift Virtualization mit Velero

Sichern Sie VMs in OpenShift Virtualization mit Velero und NetApp ONTAP S3 oder StorageGRID. Dieses Verfahren umfasst das Erstellen von benutzerdefinierten Backup-Ressourcen (CRs) für On-Demand-Backups und von geplanten CRs für geplante Backups. Bei jeder Sicherung werden VM-Metadaten und persistente Volumes erfasst und zu Wiederherstellungs- oder Compliance-Zwecken am angegebenen Objektspeicherort gespeichert.

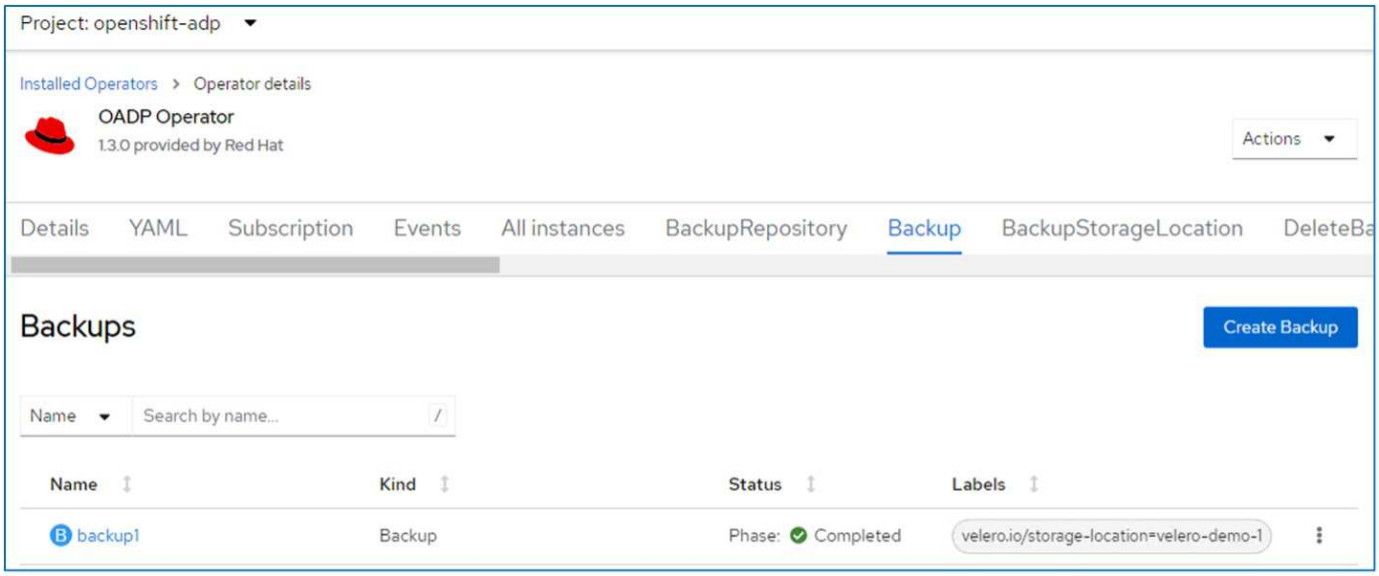
Schritte zum Erstellen einer Sicherung einer VM

Um ein On-Demand-Backup der gesamten VM (VM-Metadaten und VM-Datenträger) zu erstellen, klicken Sie auf die Registerkarte **Backup**. Dadurch wird eine benutzerdefinierte Backup-Ressource (CR) erstellt. Zum Erstellen des Backup-CR wird ein YAML-Beispiel bereitgestellt. Mit diesem YAML werden die VM und ihre Festplatten im angegebenen Namespace gesichert. Weitere Parameter können wie in der Abbildung gezeigt eingestellt werden."Dokumentation" .

Ein Snapshot der persistenten Volumes, die die Festplatten unterstützen, wird vom CSI erstellt. Es wird eine Sicherung der VM zusammen mit dem Snapshot ihrer Festplatten erstellt und am im YAML angegebenen Sicherungsspeicherort gespeichert. Das Backup bleibt gemäß TTL 30 Tage lang im System.

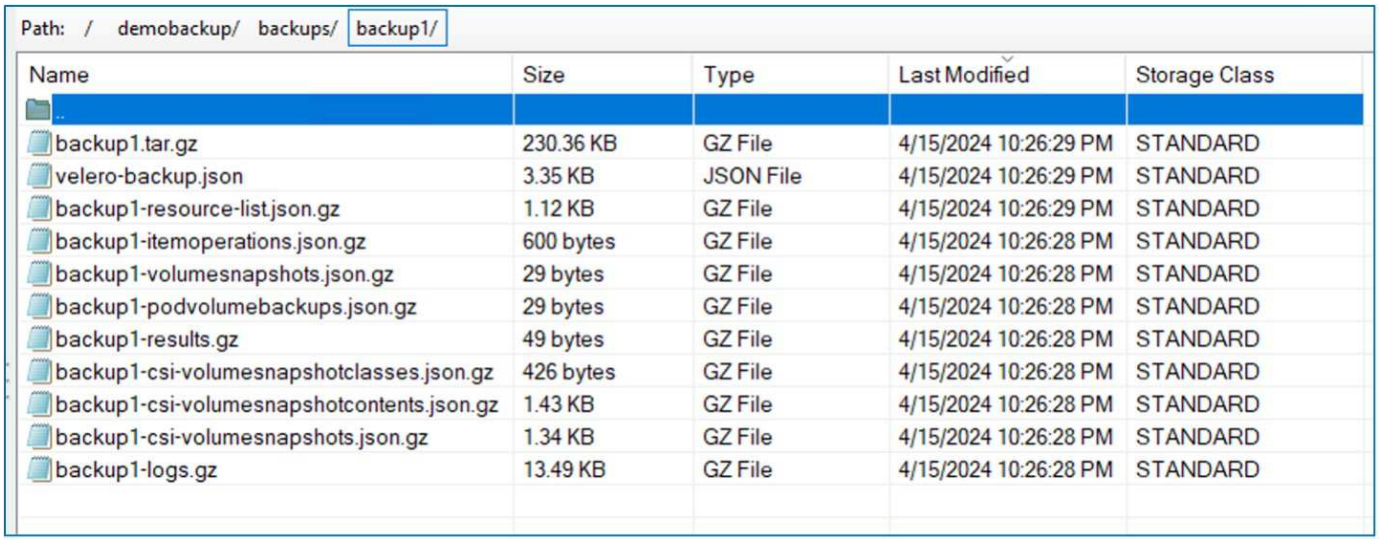
```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when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

Sobald die Sicherung abgeschlossen ist, wird ihre Phase als abgeschlossen angezeigt.



Sie können das Backup im Objektspeicher mithilfe einer S3-Browseranwendung überprüfen. Der Pfad des Backups wird im konfigurierten Bucket mit dem Präfixnamen (velero/demobackup) angezeigt. Sie können sehen, dass der Inhalt der Sicherung die Volume-Snapshots, Protokolle und andere Metadaten der virtuellen Maschine umfasst.

In StorageGrid können Sie zum Anzeigen der Sicherungsobjekte auch die S3-Konsole verwenden, die über den Tenant Manager verfügbar ist.



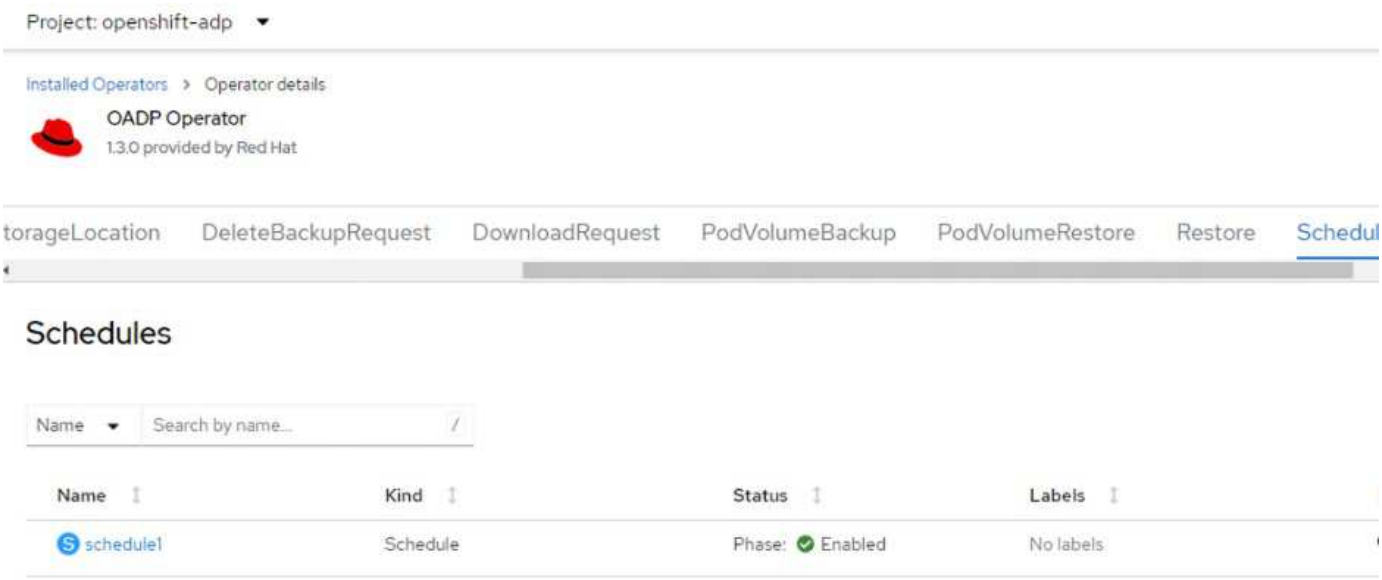
Erstellen geplanter Sicherungen für VMs in OpenShift Virtualization

Um Backups nach einem Zeitplan zu erstellen, müssen Sie einen Zeitplan-CR erstellen. Der Zeitplan ist einfach ein Cron-Ausdruck, mit dem Sie den Zeitpunkt angeben können, zu dem Sie das Backup erstellen möchten. Ein YAML-Beispiel zum Erstellen eines Schedule CR.

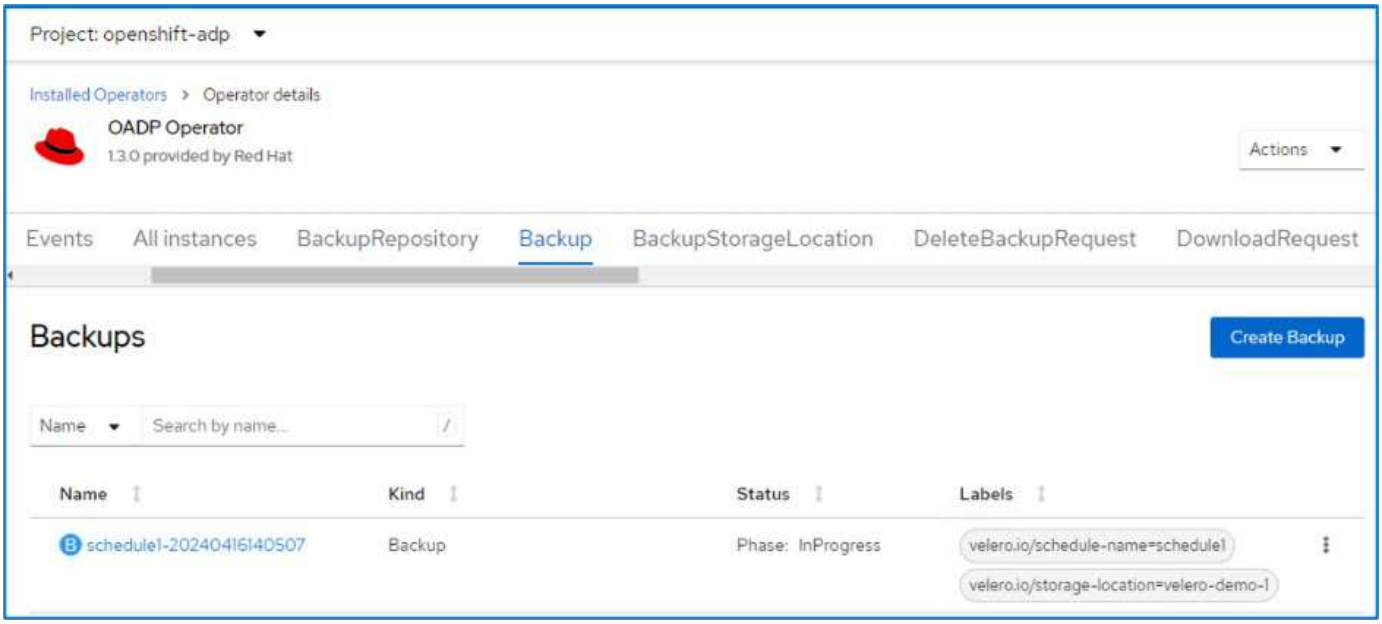
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

Der Cron-Ausdruck 0 7 * * * bedeutet, dass jeden Tag um 7:00 Uhr ein Backup erstellt wird. Außerdem werden die in die Sicherung einzubeziehenden Namespaces und der Speicherort für die Sicherung angegeben. Anstelle einer Backup-CR wird also eine geplante CR verwendet, um zum angegebenen Zeitpunkt und in der angegebenen Häufigkeit eine Sicherung zu erstellen.

Sobald der Zeitplan erstellt ist, wird er aktiviert.



Backups werden gemäß diesem Zeitplan erstellt und können auf der Registerkarte „Backup“ angezeigt werden.



Wiederherstellen einer VM aus einem Backup in Red Hat OpenShift Virtualization mit Velero

Stellen Sie VMs in OpenShift Virtualization mit Velero und der OpenShift API for Data Protection (OADP) wieder her. Dieses Verfahren umfasst das Erstellen einer benutzerdefinierten Wiederherstellungsressource (CR) zum Wiederherstellen von VMs und ihren persistenten Volumes aus Sicherungen mit Optionen zum Wiederherstellen im ursprünglichen Namespace, einem anderen Namespace oder unter Verwendung einer alternativen Speicherklasse.

Voraussetzungen

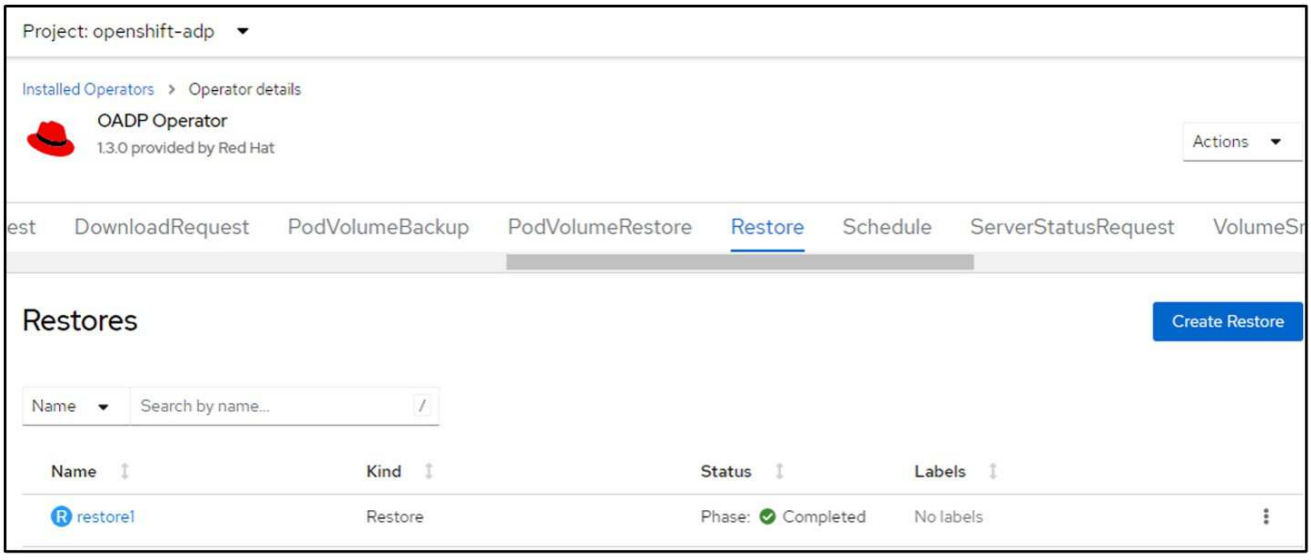
Um eine Wiederherstellung aus einer Sicherung durchzuführen, gehen wir davon aus, dass der Namespace, in dem sich die virtuelle Maschine befand, versehentlich gelöscht wurde.

Wiederherstellen im selben Namespace

Um die Wiederherstellung aus der gerade erstellten Sicherung durchzuführen, müssen wir eine benutzerdefinierte Wiederherstellungsressource (CR) erstellen. Wir müssen ihm einen Namen geben, den Namen des Backups angeben, aus dem wir wiederherstellen möchten, und die RestorePVs auf „true“ setzen. Weitere Parameter können wie in der Abbildung gezeigt eingestellt werden."Dokumentation" . Klicken Sie auf die Schaltfläche „Erstellen“.


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

Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die virtuellen Maschinen in den Zustand zurückversetzt wurden, in dem sie sich zum Zeitpunkt der Snapshot-Erstellung befanden. (Wenn die Sicherung erstellt wurde, als die VM ausgeführt wurde, wird durch die Wiederherstellung der VM aus der Sicherung die wiederhergestellte VM gestartet und in einen laufenden Zustand versetzt.) Die VM wird im selben Namespace wiederhergestellt.



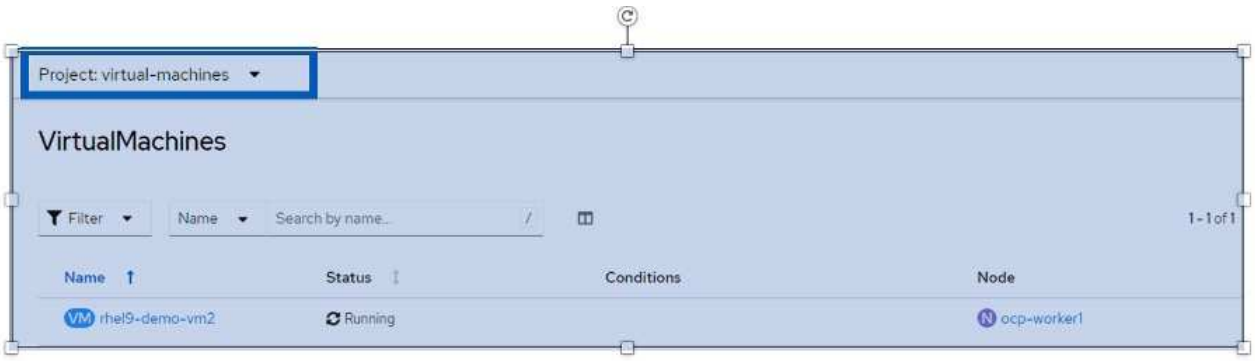
Wiederherstellen in einem anderen Namespace

Um die VM in einem anderen Namespace wiederherzustellen, können Sie in der YAML-Definition der Wiederherstellungs-CR ein NamespaceMapping angeben.

Die folgende YAML-Beispieldatei erstellt eine Wiederherstellungs-CR, um eine VM und ihre Datenträger im Namespace „virtual-machines-demo“ wiederherzustellen, wenn die Sicherung in den Namespace „virtual-machines“ übernommen wurde.

```
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
```

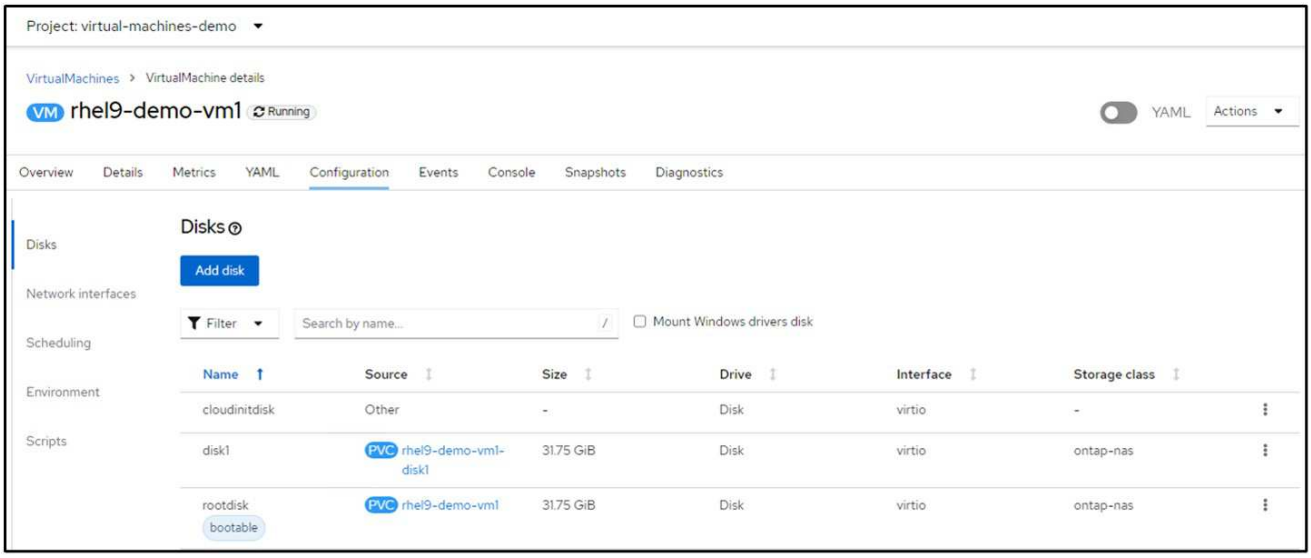
Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die virtuellen Maschinen in den Zustand zurückversetzt wurden, in dem sie sich zum Zeitpunkt der Snapshot-Erstellung befanden. (Wenn die Sicherung erstellt wurde, als die VM ausgeführt wurde, wird durch die Wiederherstellung der VM aus der Sicherung die wiederhergestellte VM gestartet und in einen laufenden Zustand versetzt.) Die VM wird in einem anderen Namespace wiederhergestellt, wie im YAML angegeben.

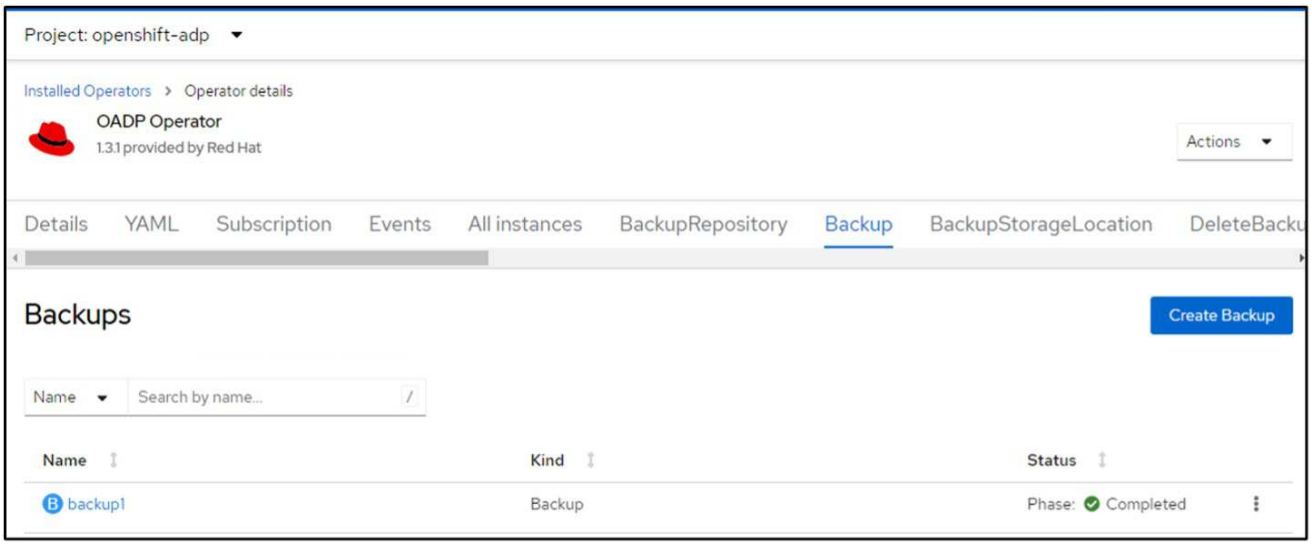


Wiederherstellen in einer anderen Speicherklasse

Velero bietet eine allgemeine Möglichkeit, die Ressourcen während der Wiederherstellung durch Angabe von JSON-Patches zu ändern. Die JSON-Patches werden auf die Ressourcen angewendet, bevor sie wiederhergestellt werden. Die JSON-Patches werden in einer Konfigurationszuordnung angegeben und auf die Konfigurationszuordnung wird im Wiederherstellungsbefehl verwiesen. Mit dieser Funktion können Sie die Wiederherstellung mithilfe einer anderen Speicherklasse durchführen.

Im folgenden Beispiel verwendet die virtuelle Maschine während der Erstellung ontap-nas als Speicherklasse für ihre Festplatten. Es wird eine Sicherung der virtuellen Maschine mit dem Namen „backup1“ erstellt.





Simulieren Sie einen Verlust der VM, indem Sie die VM löschen.

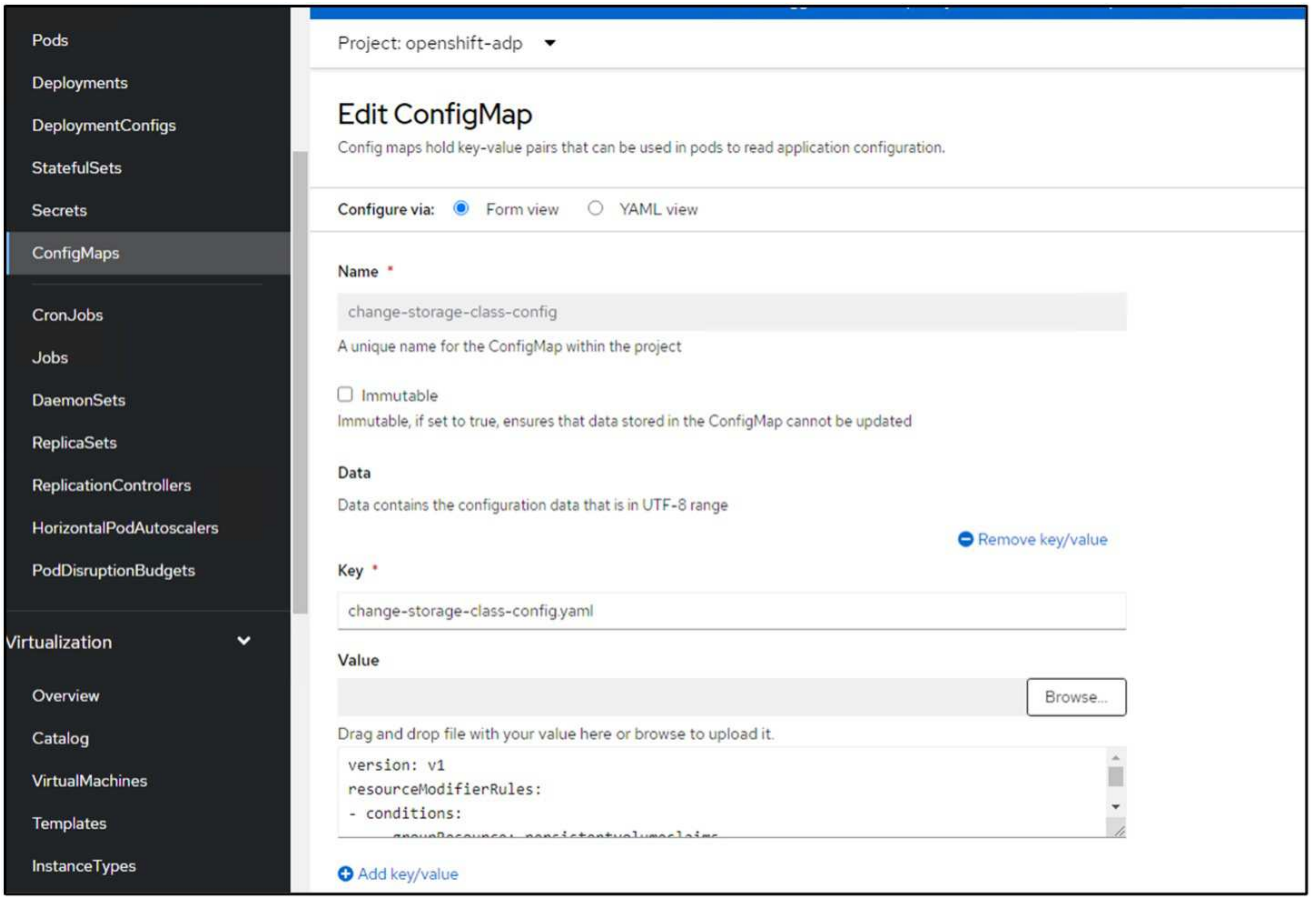
Um die VM mit einer anderen Speicherklasse wiederherzustellen, beispielsweise der Speicherklasse ontap-nas-eco, müssen Sie die folgenden zwei Schritte ausführen:

Schritt 1

Erstellen Sie wie folgt eine Konfigurationszuordnung (Konsole) im OpenShift-ADP-Namespace: Füllen Sie

die Details wie im Screenshot gezeigt aus: Namespace auswählen: OpenShift-ADP Name: Change-Storage-Class-Config (kann ein beliebiger Name sein) Schlüssel: Change-Storage-Class-Config.yaml: Wert:

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



Das resultierende Konfigurationszuordnungsobjekt sollte folgendermaßen aussehen (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>
```

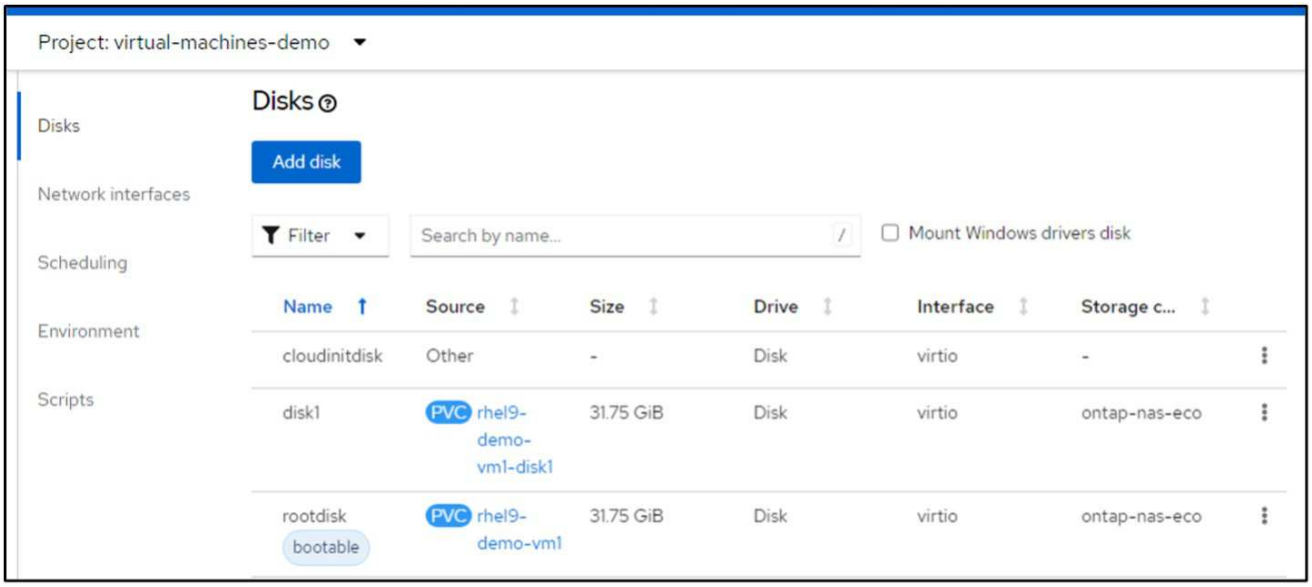
Diese Konfigurationszuordnung wendet die Ressourcenmodifikatorregel an, wenn die Wiederherstellung erstellt wird. Es wird ein Patch angewendet, um den Speicherklassennamen für alle persistenten Volume-Ansprüche, die mit rhel beginnen, durch ontap-nas-eco zu ersetzen.

Schritt 2

Um die VM wiederherzustellen, verwenden Sie den folgenden Befehl aus der Velero-CLI:

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

Die VM wird im selben Namespace wie die mit der Speicherklasse ontap-nas-eco erstellten Datenträger wiederhergestellt.



Löschen Sie eine Sicherungs-CR oder stellen Sie eine CR in Red Hat OpenShift Virtualization mit Velero wieder her

Löschen Sie Sicherungs- und Wiederherstellungsressourcen für VMs in OpenShift Virtualization mit Velero. Verwenden Sie die OpenShift-CLI, um Sicherungen zu löschen und gleichzeitig die Objektspeicherdaten beizubehalten, oder die Velero-CLI, um sowohl die Backup Custom Resource (CR) als auch die zugehörigen Speicherdaten zu löschen.

Löschen einer Sicherung

Sie können ein Backup-CR löschen, ohne die Object Storage-Daten zu löschen, indem Sie das OC CLI-Tool verwenden.

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

Wenn Sie das Backup CR und die zugehörigen Objektspeicherdaten löschen möchten, können Sie dies mit dem Velero CLI-Tool tun.

Laden Sie die CLI gemäß den Anweisungen im"Velero-Dokumentation" .

Führen Sie den folgenden Löschbefehl mit der Velero-CLI aus

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

Löschen einer Wiederherstellung

Sie können die Wiederherstellungs-CR mit der Velero-CLI löschen

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

Sie können den oc-Befehl sowie die Benutzeroberfläche verwenden, um die Wiederherstellungs-CR zu löschen

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