Data Protection for OpenShift Virtualization

NetApp Solutions

NetApp
April 24, 2024

Inhalt

Data Protection for OpenShift Virtualization

Datensicherung für VMs in OpenShift-Virtualisierung mit OpenShift-API für Data Protection (OADP)

Autor: Banu Sundhar, NetApp

Dieser Abschnitt des Referenzdokuments enthält Details zum Erstellen von Backups von VMs mithilfe der OpenShift API for Data Protection (OADP) mit Velero unter NetApp ONTAP S3 oder NetApp StorageGRID S3. Die Backups von Persistent Volumes(PVs) der VM-Festplatten werden mit CSI Astra Trident Snapshots erstellt.

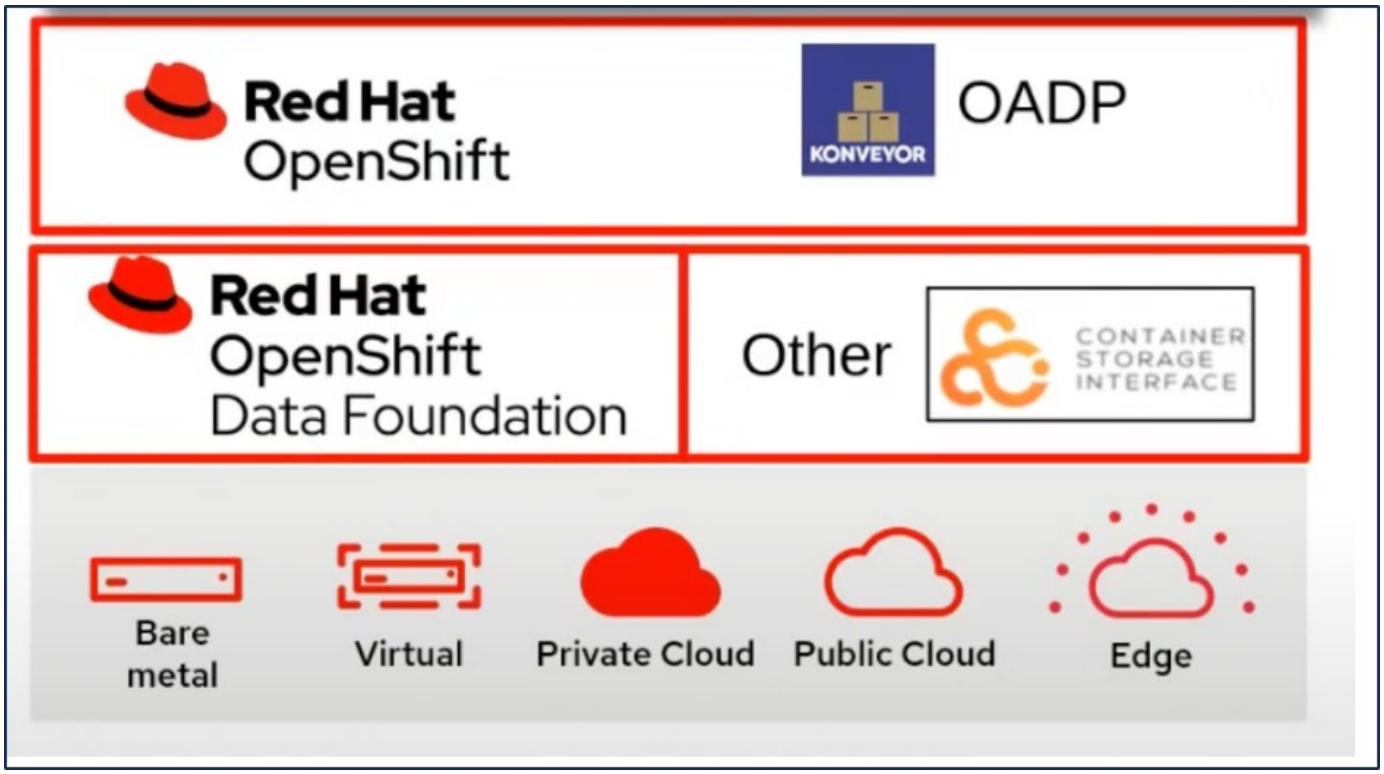
Virtuelle Maschinen in der OpenShift-Virtualisierungsumgebung sind Container-Anwendungen, die in den Workerknoten der OpenShift-Container-Plattform ausgeführt werden. Es ist wichtig, die VM-Metadaten sowie die persistenten Festplatten der VMs zu schützen, damit Sie sie bei Verlust oder Beschädigung wiederherstellen können.

Die persistenten Festplatten der OpenShift-Virtualisierungs-VMs können mithilfe von ONTAP-Speicher gesichert werden, der in den OpenShift-Cluster integriert ist "Astra Trident CSI". In diesem Abschnitt verwenden wir "OpenShift API for Data Protection (OADP)" Um das Backup von VMs einschließlich seiner Daten-Volumes auf durchzuführen

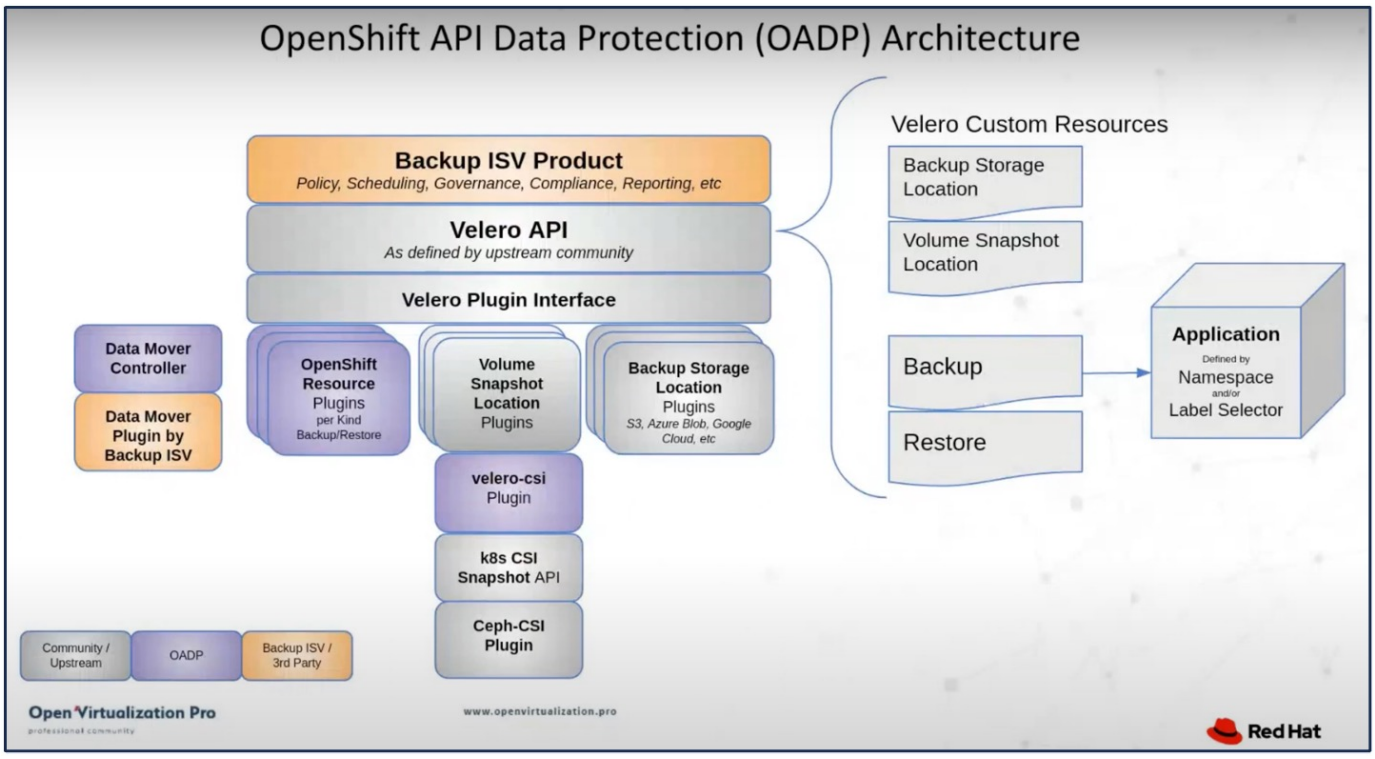
- ONTAP Objekt-Storage
- StorageGRID

Wir führen dann bei Bedarf ein Restore aus dem Backup durch.

OADP ermöglicht Backup, Wiederherstellung und Disaster Recovery von Applikationen auf einem OpenShift-Cluster. Zu den mit OADP gesicherten Daten gehören Kubernetes-Ressourcenobjekte, persistente Volumes und interne Images.



Red hat OpenShift nutzt die von den OpenSource Communities entwickelten Lösungen für den Datenschutz. "Velero" Ist ein Open-Source-Tool für sicheres Backup und Restore, Disaster Recovery und die Migration von Kubernetes-Cluster-Ressourcen und persistenten Volumes. Um Velero einfach nutzen zu können, hat OpenShift den OADP-Operator und das Velero-Plugin für die Integration in die CSI-Speichertreiber entwickelt. Die Kernelemente der OADP-APIs, die offengelegt werden, basieren auf den Velero-APIs. Nach der Installation und Konfiguration des OADP-Bedieners basieren die durchzuführenden Backup-/Wiederherstellungsvorgänge auf den von der Velero-API offengelegten Vorgängen.



OADP 1.3 ist über den Operator Hub von OpenShift Cluster 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 Langlebigkeit, indem Snapshots während des Backups an einen Speicherort für Objekte verschoben werden. Die Snapshots stehen dann für die Wiederherstellung nach Katastrophen zur Verfügung.

Im Folgenden sind die Versionen der verschiedenen Komponenten, die für die Beispiele in diesem Abschnitt verwendet werden

- OpenShift Cluster 4.14
- OpenShift Virtualization wird über OperatorOpenShift Virtualization Operator von Red hat installiert
- OADP Operator 1.13 von Red hat bereitgestellt
- Velero CLI 1.13 für Linux
- Astra Trident 24.02
- ONTAP 9.12

"Astra Trident CSI"
"OpenShift API for Data Protection (OADP)"
"Velero"

Installation von OpenShift API for Data Protection (OADP) Operator

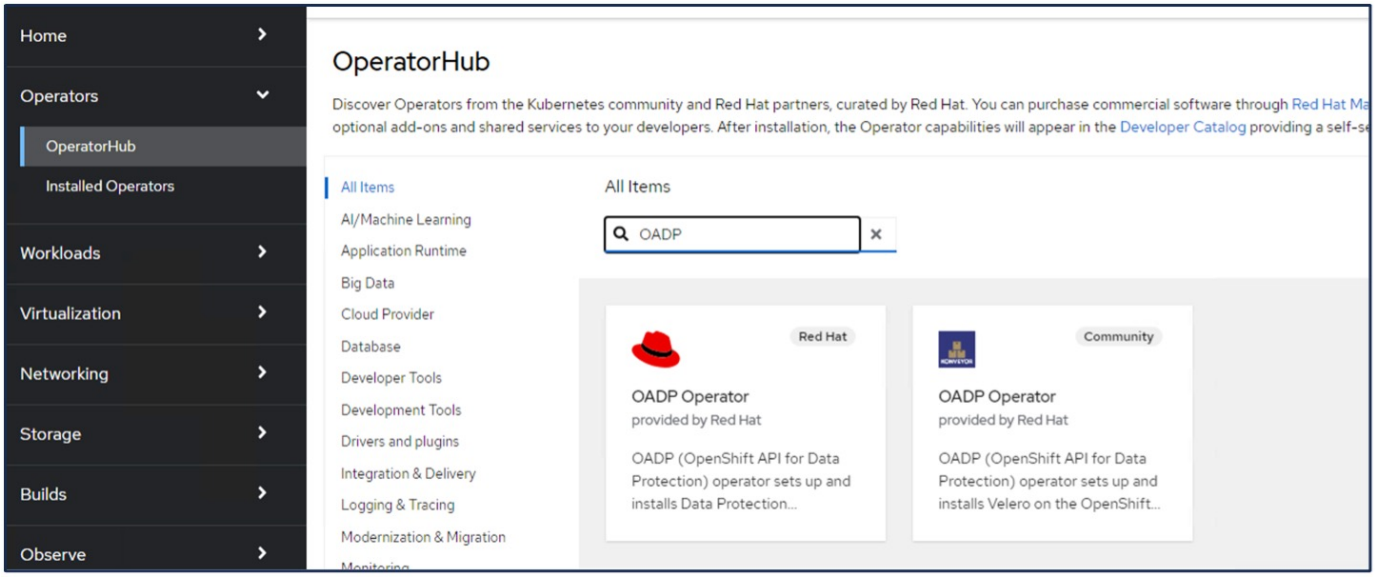
Voraussetzungen

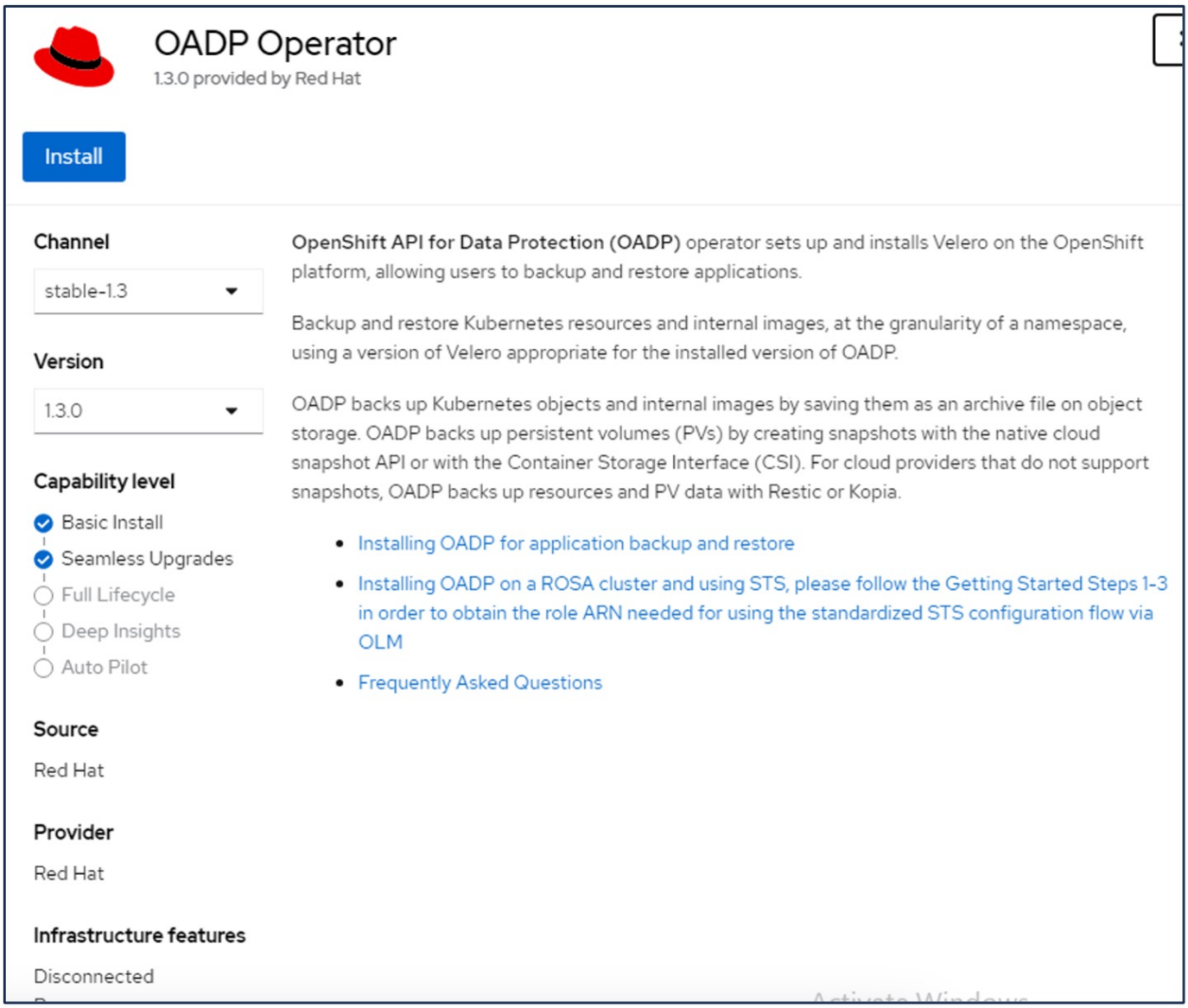
- Ein Red hat OpenShift-Cluster (später als Version 4.12), der auf einer Bare-Metal-Infrastruktur mit RHCOS Worker-Knoten installiert ist
- Ein NetApp ONTAP Cluster ist über Astra Trident in den Cluster integriert
- Ein Trident Back-End, das mit einer SVM auf ONTAP Cluster konfiguriert ist
- StorageClass: Ist auf dem OpenShift-Cluster mit Astra Trident als bereitstellungsunternehmen konfiguriert
- Die Trident Snapshot Klasse wurde auf dem Cluster erstellt
- Cluster-Admin-Zugriff auf Red hat OpenShift-Cluster
- Administratorzugriff auf das NetApp ONTAP-Cluster
- OpenShift Virtualization Operator installiert und konfiguriert
- In einem Namespace auf OpenShift Virtualization implementierte VMs
- Eine Admin-Workstation mit den Tools tridentctl und oc installiert und zur €Pfad hinzugefügt

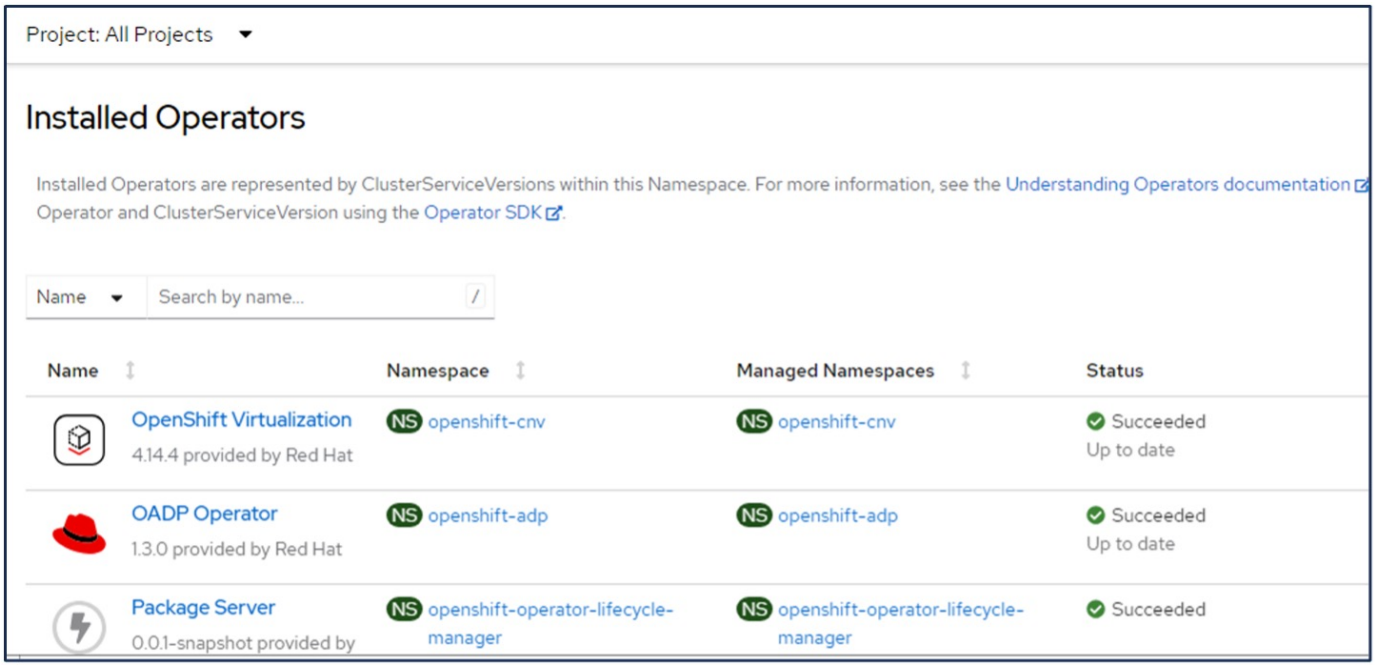
Wenn Sie eine Sicherung einer VM erstellen möchten, wenn sie sich im laufenden Zustand befindet, müssen Sie den QEMU-Gast-Agent auf dieser virtuellen Maschine installieren. Wenn Sie die VM mithilfe einer vorhandenen Vorlage installieren, wird der QEMU-Agent automatisch installiert. QEMU ermöglicht es dem Gast-Agent, während des Snapshot-Prozesses Daten im Gastbetriebssystem stillzulegen und eine mögliche Beschädigung von Daten zu vermeiden. Wenn QEMU nicht installiert ist, können Sie die virtuelle Maschine anhalten, bevor Sie eine Sicherung durchführen.

Schritte zum Installieren des OADP-Bedieners

1. Gehen Sie zum Operator Hub des Clusters, und wählen Sie Red hat OADP Operator aus. Verwenden Sie auf der Seite Installieren 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 Bedieners erfolgreich war, konfigurieren Sie die Instanz von Velero.
Velero kann für die Verwendung von S3 Compatible Object Storage konfiguriert werden. Konfigurieren Sie ONTAP S3 mithilfe der in dargestellten Verfahren "Abschnitt „Objekt-Storage-Management“ der ONTAP-Dokumentation". Für die Integration in Velero benötigen Sie die folgenden Informationen aus Ihrer ONTAP S3-Konfiguration.

- Eine logische Schnittstelle (Logical Interface, LIF), die für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldedaten für den Zugriff auf S3, die den Zugriffsschlüssel und den geheimen Zugriffsschlüssel enthalten
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte das TLS-Zertifikat auf dem Object Storage-Server installiert werden.

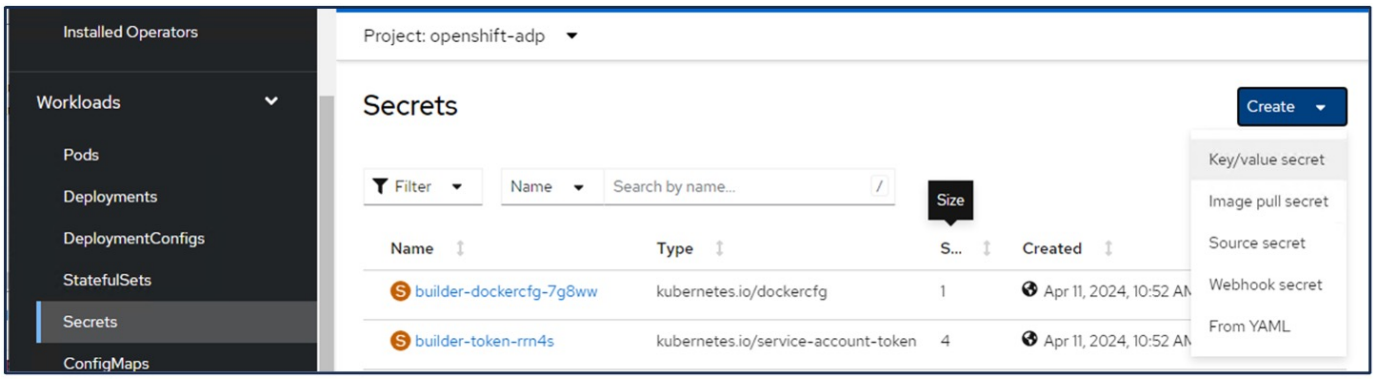
Voraussetzungen für die Velero-Konfiguration mit StorageGRID S3-Details

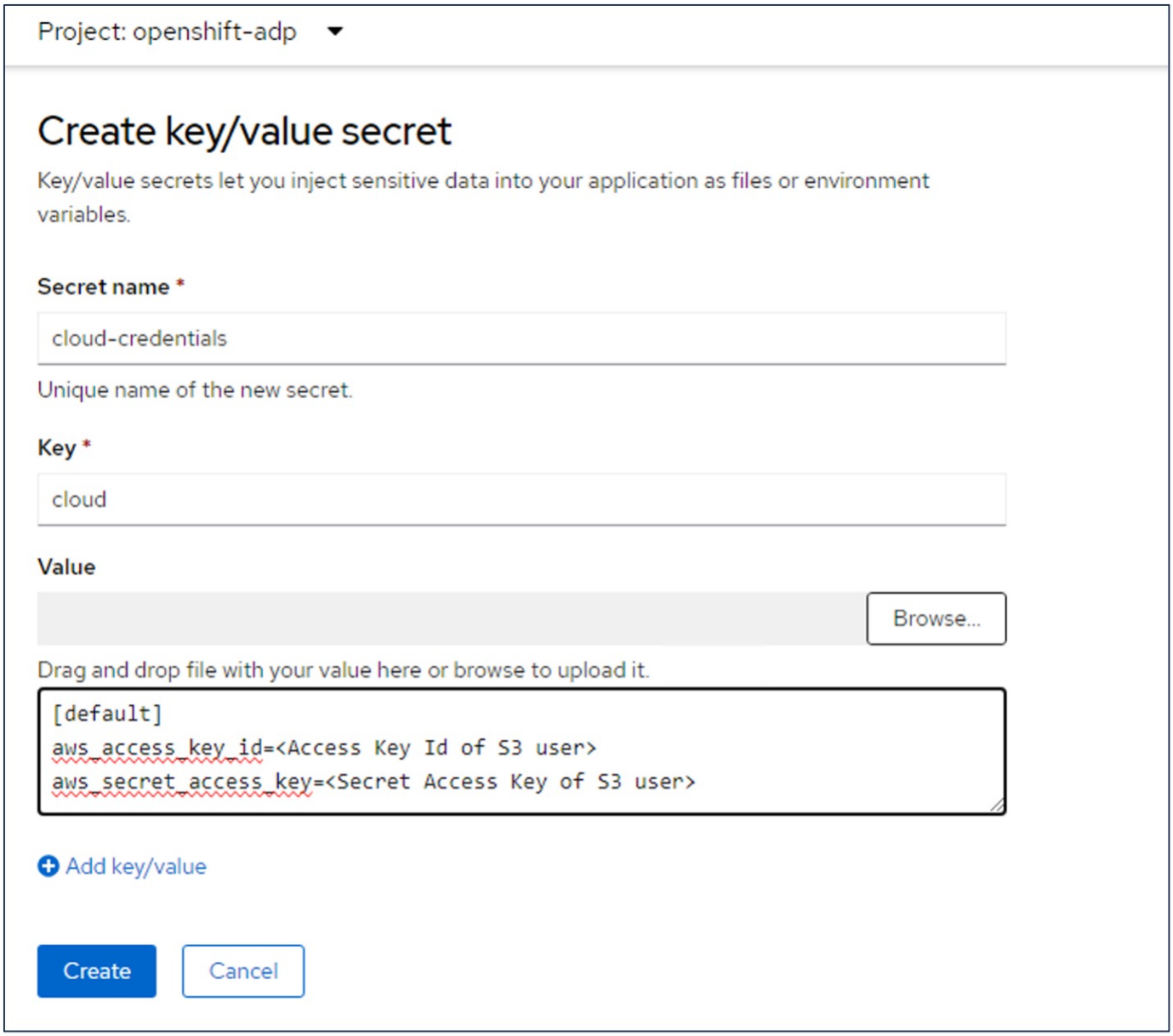
Velero kann für die Verwendung von S3 Compatible Object Storage konfiguriert werden. Sie können StorageGRID S3 mithilfe der in dargestellten Verfahren konfigurieren "StorageGRID Dokumentation". Für die Integration in Velero benötigen Sie die folgenden Informationen aus Ihrer StorageGRID S3-Konfiguration.

- Der Endpunkt, der für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldedaten für den Zugriff auf S3, die den Zugriffsschlüssel und den geheimen Zugriffsschlüssel enthalten
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer
- Für einen sicheren Zugriff auf den Objektspeicher sollte das TLS-Zertifikat auf dem Object Storage-Server installiert werden.

Schritte zum Konfigurieren von Velero

- Erstellen Sie zunächst einen Schlüssel für Anmeldedaten eines ONTAP S3-Benutzers oder eines StorageGRID-Mandanten. Diese wird später zur Konfiguration von Velero verwendet. Sie können einen Schlüssel aus der CLI oder aus der Webkonsole erstellen.
  Um einen Schlüssel von der Webkonsole aus zu erstellen, wählen Sie Geheimnisse aus, und klicken Sie dann auf Schlüssel/Wertgeheimnis. Geben Sie die Werte für den Anmeldeinformationsnamen, den Schlüssel und den angezeigten Wert an. Verwenden Sie unbedingt die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres S3-Benutzers. Nennen Sie das Geheimnis entsprechend. In dem unten stehenden Beispiel wird ein Geheimnis mit den ONTAP S3-Benutzeranmeldeinformationen namens ontap-S3-credentials erstellt.

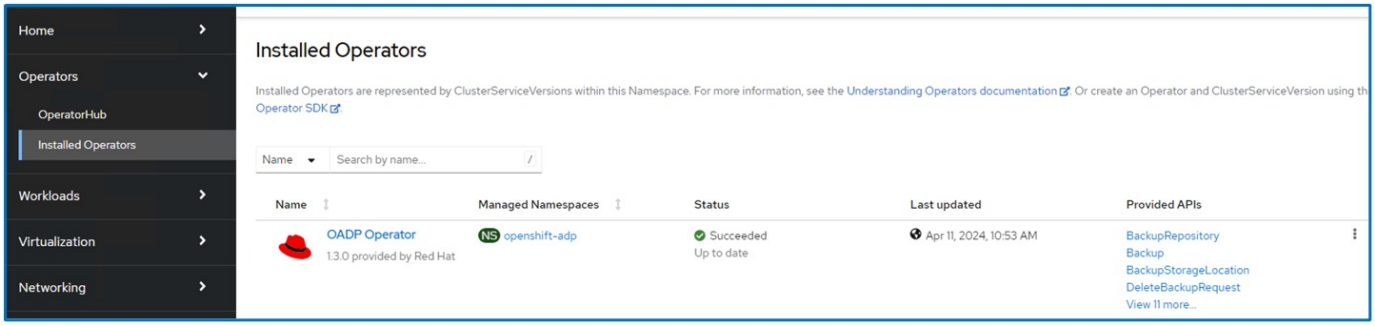




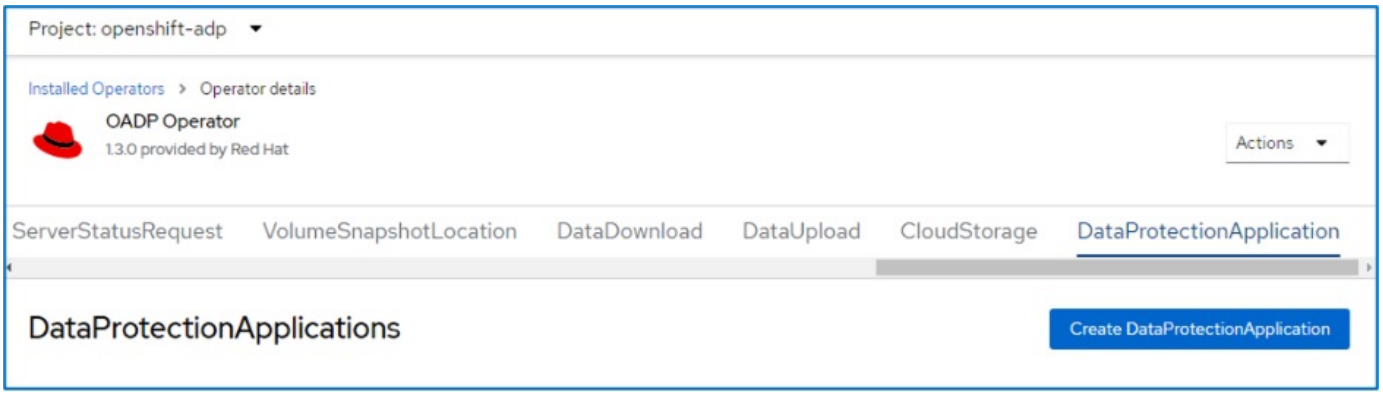
Um einen Schlüssel mit dem Namen sg-s3-credentials aus der CLI zu erstellen, können Sie den folgenden Befehl verwenden.

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

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

[default]
aws_access_key_id=<Access Key Id of S3 user>
aws_secret_access_key=<Secret Access Key of S3 user>
```

- Um Velero zu konfigurieren, wählen Sie im Menüpunkt unter Operatoren die Option Installed Operators aus, klicken Sie auf OADP Operator und wählen Sie dann die Registerkarte DataProtectionApplication aus.



Klicken Sie auf Create DataProtectionApplication. Geben Sie in der Formularansicht einen Namen für die Datenschutzanwendung ein, oder verwenden Sie den Standardnamen.



Wechseln Sie nun zur YAML-Ansicht, und ersetzen Sie die Spezifikationsinformationen, wie in den nachfolgenden Beispielen für yaml-Dateien gezeigt.

Beispiel-yaml-Datei zur Konfiguration von Velero mit ONTAP S3 als Backup-Speicherort

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true' ->use this for https communication
with ONTAP S3
          profile: default
          region: us-east
          s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' ->Ensure TLS certificate for S3 is
configured
        credential:
          key: cloud
          name: ontap-s3-credentials ->previously created secret
        default: true
        objectStorage:
          bucket: velero ->Your bucket name previously created in S3 for
backups
          prefix: demobackup ->The folder that will be created in the
bucket
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->Add this plugin
        - openshift
        - aws
        - kubevirt ->Add this plugin
```

Beispiel-yaml-Datei zur Konfiguration von Velero mit StorageGRID S3 als Backup Location und 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
```

Der Abschnitt „Spec“ in der yaml-Datei sollte für die folgenden Parameter, ähnlich wie im obigen Beispiel, entsprechend konfiguriert werden

Backup-Standorte
ONTAP S3 oder StorageGRID S3 (mit seinen Zugangsdaten und anderen in der yaml angezeigten Informationen) ist als Standardspeicherort für velero konfiguriert.

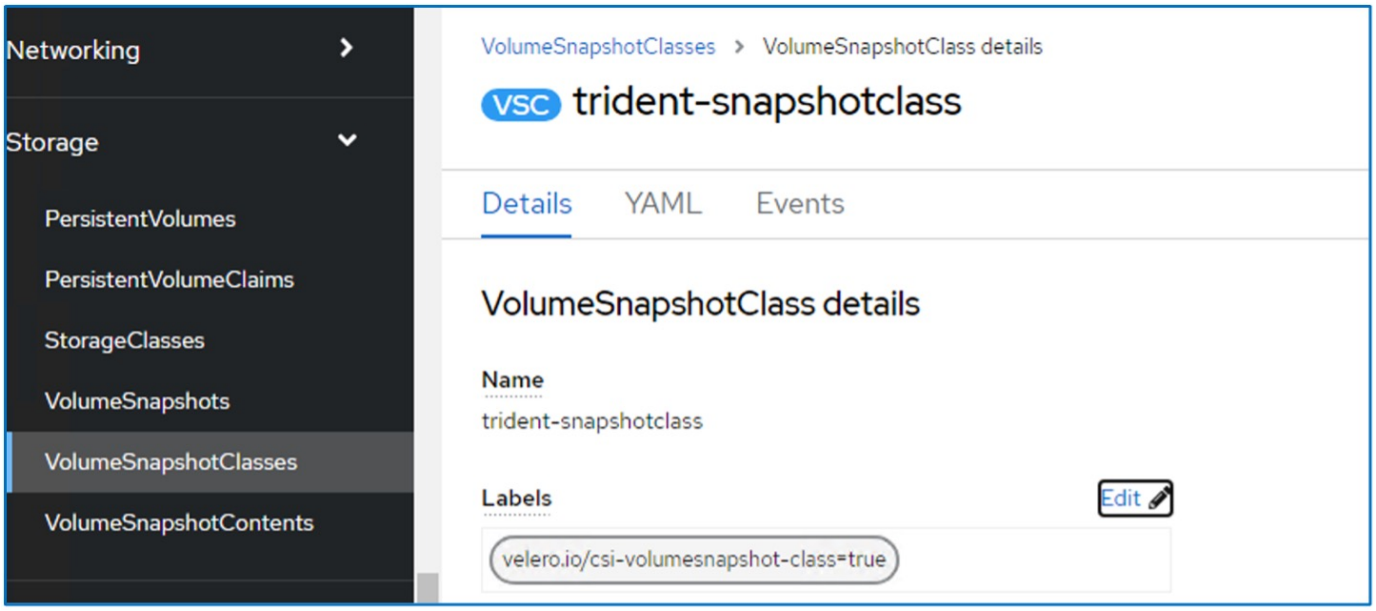
Schnappschusspositionen
Wenn Sie CSI-Snapshots (Container Storage Interface) verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie einen VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Astra Trident CSI und Sie haben bereits VolumeSnapShotClass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

CSI-Plugin aktivieren

Fügen Sie csi zu den defaultPlugins für Velero hinzu, um persistente Volumes mit CSI-Snapshots zu sichern. Die Velero CSI Plugins, um CSI-gestützte VES zu sichern, wählen die VolumeSnapshotClass im Cluster, die **velero.io/csi-Volumesnapshot-class** Label darauf gesetzt hat. Für diese

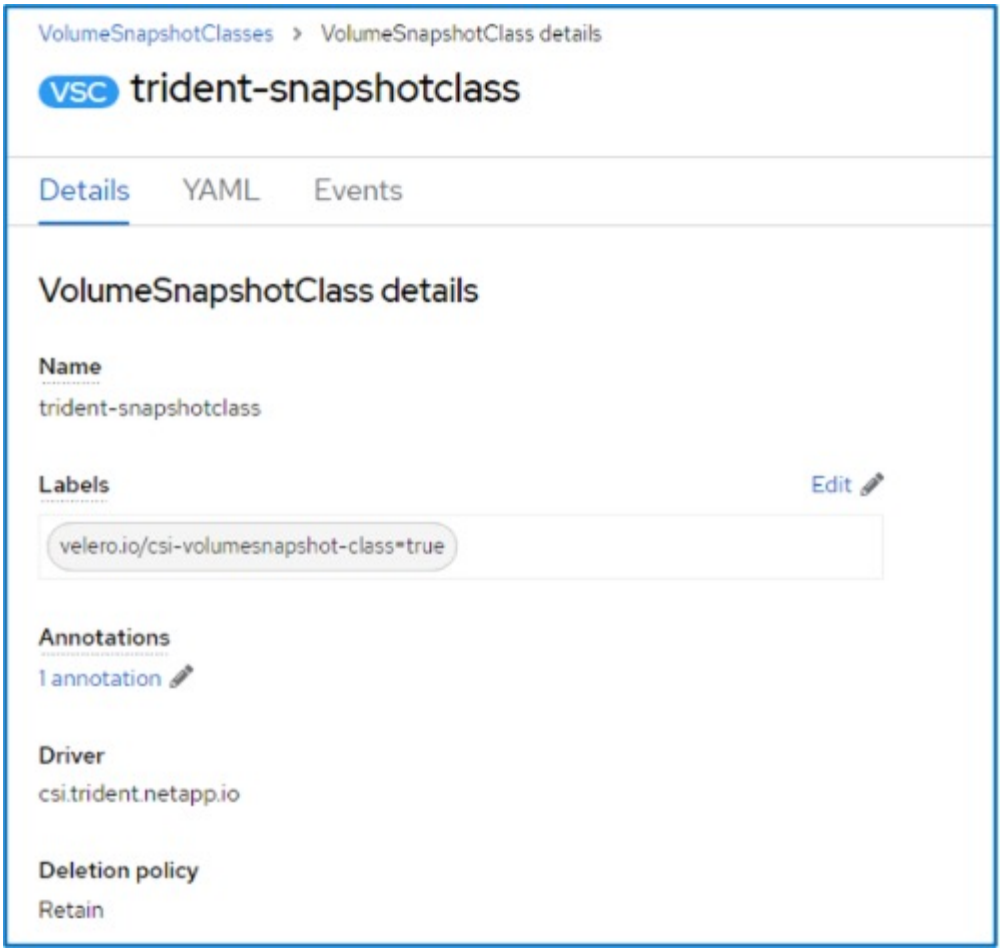
- Sie müssen die Dreizack-VolumeSnapshotClass erstellen lassen.

- Bearbeiten Sie die Beschriftung der Dreizack-snapshotklasse, und setzen Sie sie auf **velero.io/csi-Volumesnapshot-class=true** wie unten gezeigt.

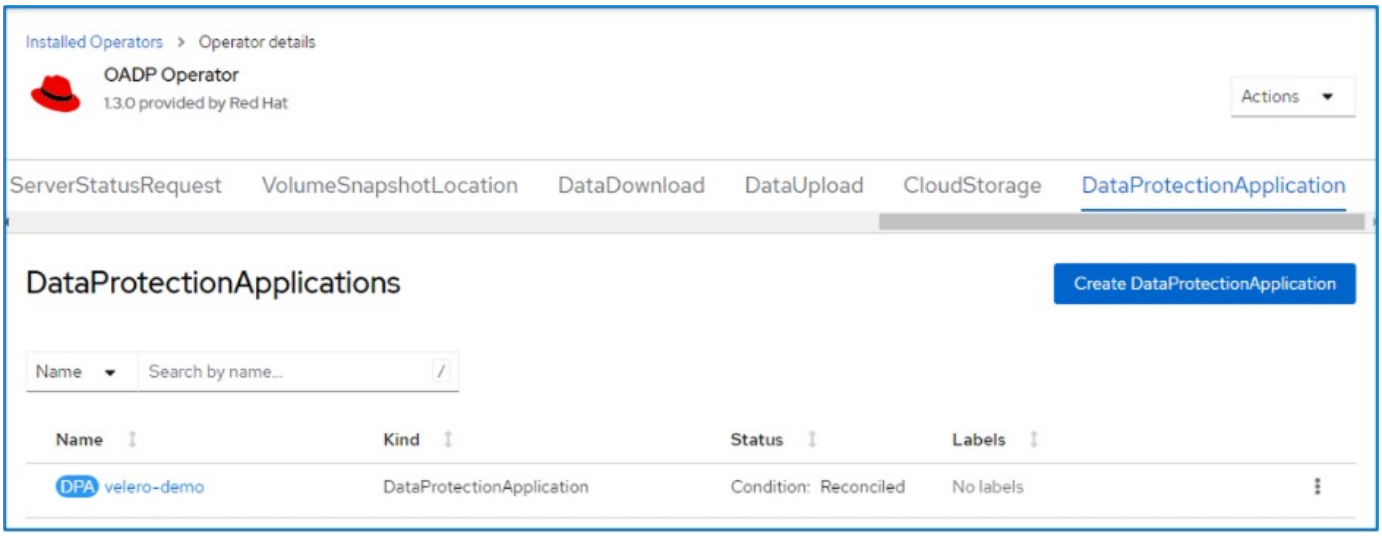


Stellen Sie sicher, dass die Snapshots auch dann bestehen können, wenn die VolumeSnapshot-Objekte gelöscht werden. Dies kann durch Setzen der **deletionPolicy** auf behalten erfolgen. Wenn nicht, geht durch das Löschen eines Namespace sämtliche darin gesicherten PVCs verloren.

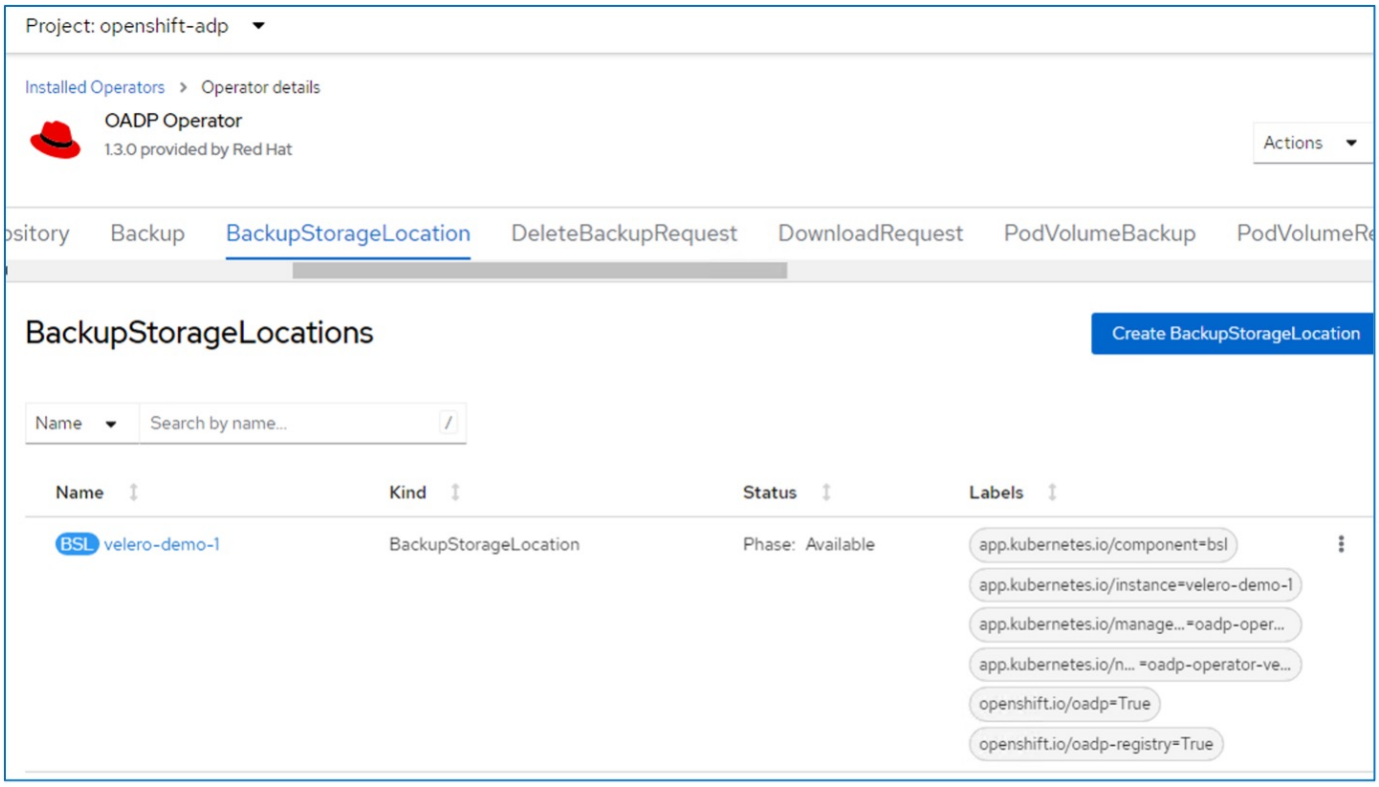
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Stellen Sie sicher, dass die DataProtectionApplication erstellt wurde und sich in der Bedingung:abgestimmt befindet.



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



Erstellen von On-Demand-Backups für VMs in OpenShift Virtualization

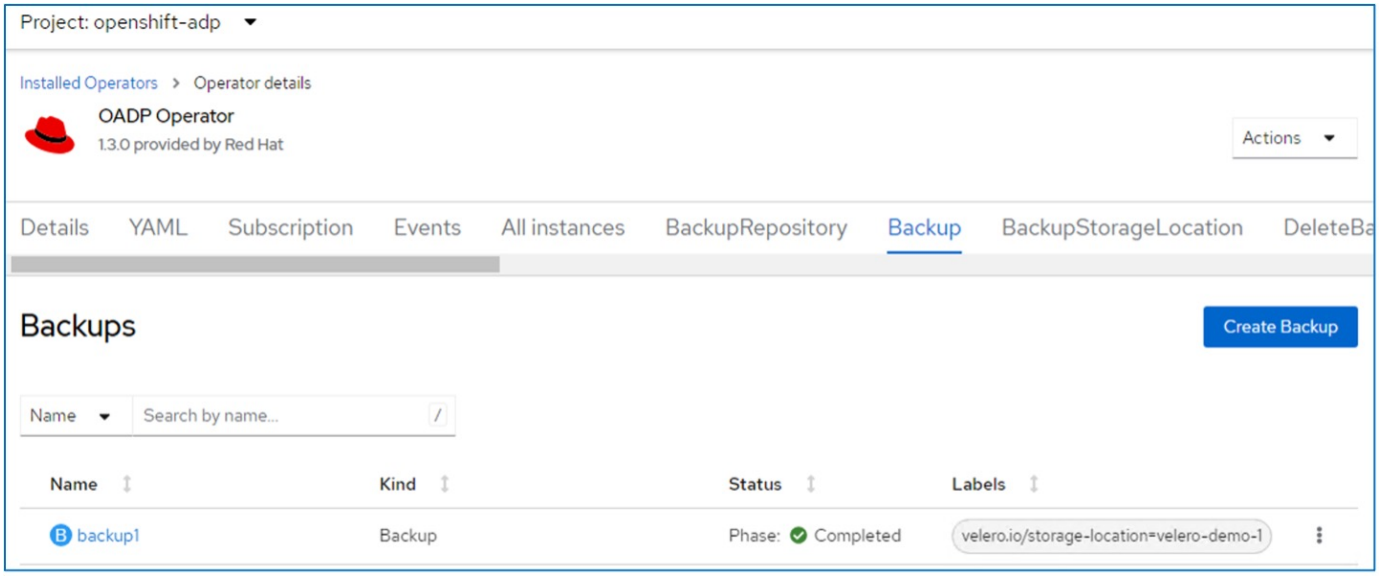
Schritte zum Erstellen einer Sicherung einer VM

Um eine On-Demand-Sicherung der gesamten VM (VM-Metadaten und VM-Festplatten) zu erstellen, klicken Sie auf die Registerkarte **Backup**. Dadurch wird eine benutzerdefinierte Backup-Ressource (CR) erstellt. Ein Beispiel für yaml wird zur Erstellung des Backup CR bereitgestellt. Mit diesem yaml werden die VM und ihre Laufwerke im angegebenen Namespace gesichert. Weitere Parameter können wie in dargestellt eingestellt werden "Dokumentation".

Ein Snapshot der persistenten Volumes, die die Festplatten sichern, wird vom CSI erstellt. Ein Backup der VM zusammen mit dem Snapshot ihrer Festplatten wird erstellt und im Backup-Speicherort gespeichert, der in der yaml angegeben ist. Das Backup bleibt gemäß ttl 30 Tage im System.

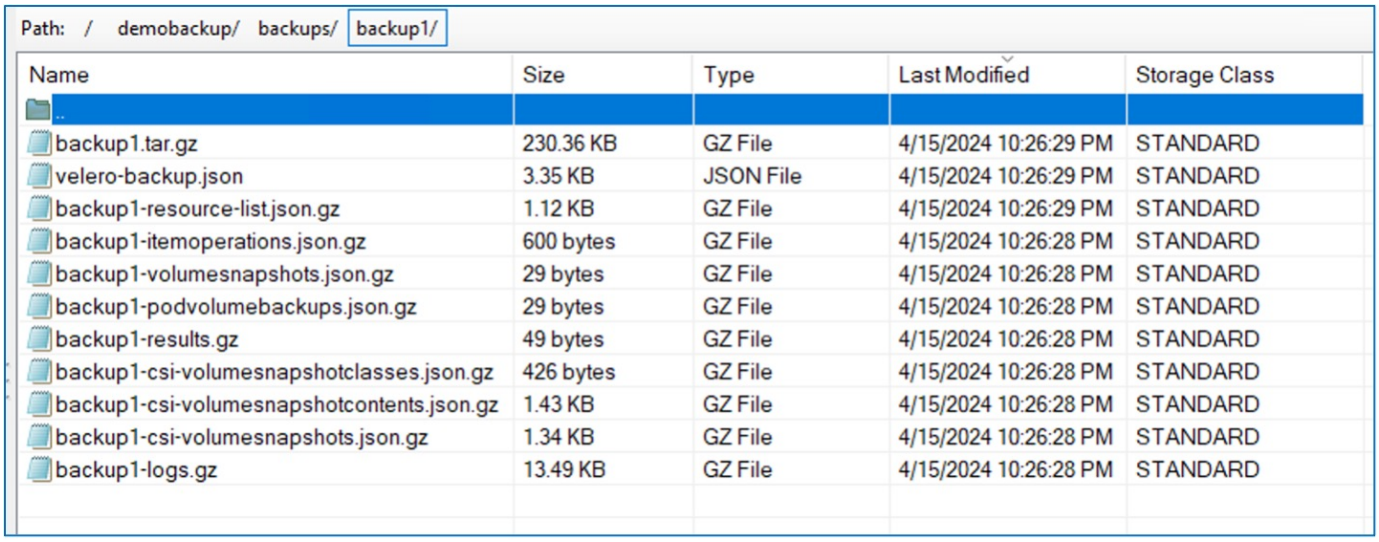
```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when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

Sobald das Backup abgeschlossen ist, wird seine Phase als abgeschlossen angezeigt.



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

In StorageGRID können Sie die S3-Konsole, die im Tenant Manager verfügbar ist, auch zum Anzeigen der Backup-Objekte verwenden.



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

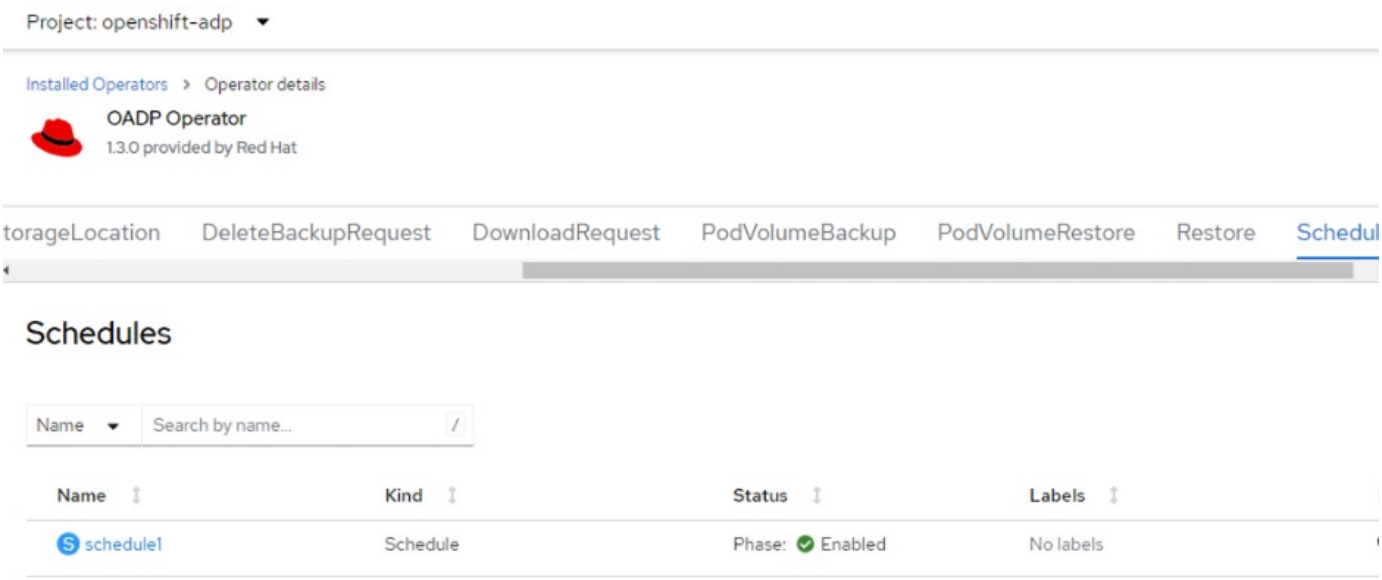
Erstellen geplanter Backups für VMs in OpenShift Virtualization

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

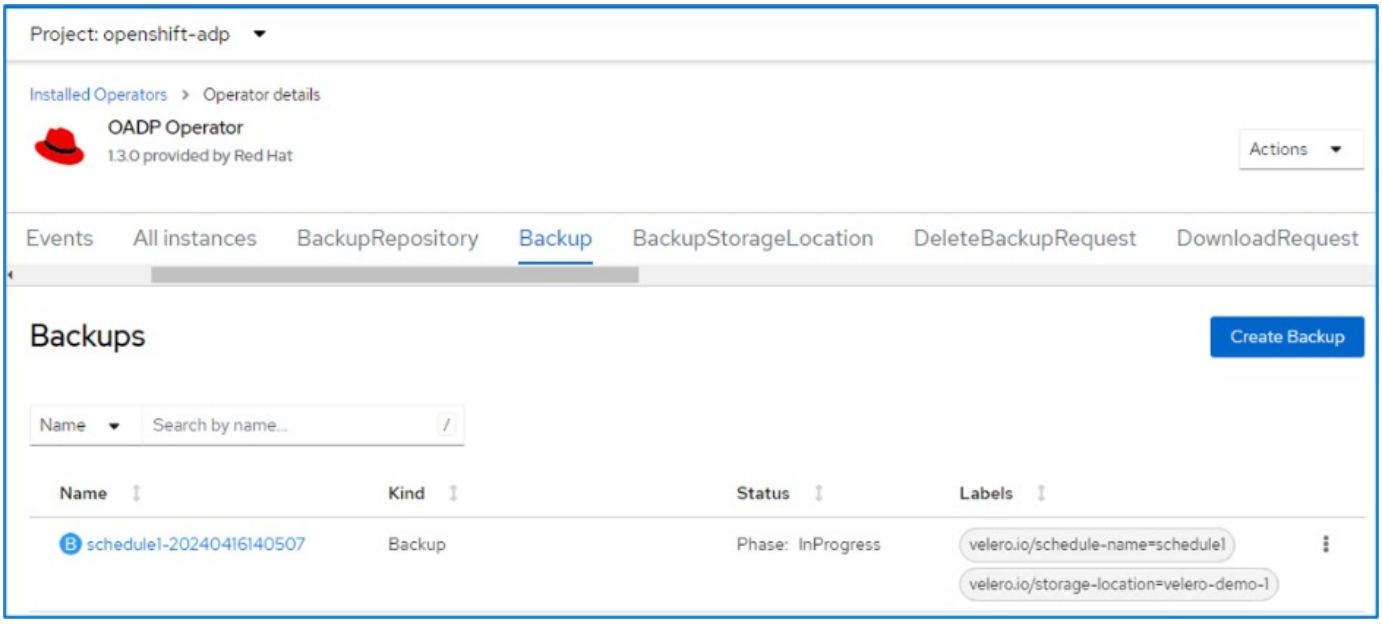
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

Der Cron-Ausdruck 0 7 * * * bedeutet, dass täglich um 7:00 Uhr ein Backup erstellt wird.
Die Namespaces, die in das Backup aufgenommen werden sollen, und der Speicherort für das Backup werden ebenfalls angegeben. Anstelle eines Backup CR wird Schedule CR verwendet, um ein Backup zu der angegebenen Zeit und Häufigkeit zu erstellen.

Sobald der Zeitplan erstellt wurde, wird er aktiviert.



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



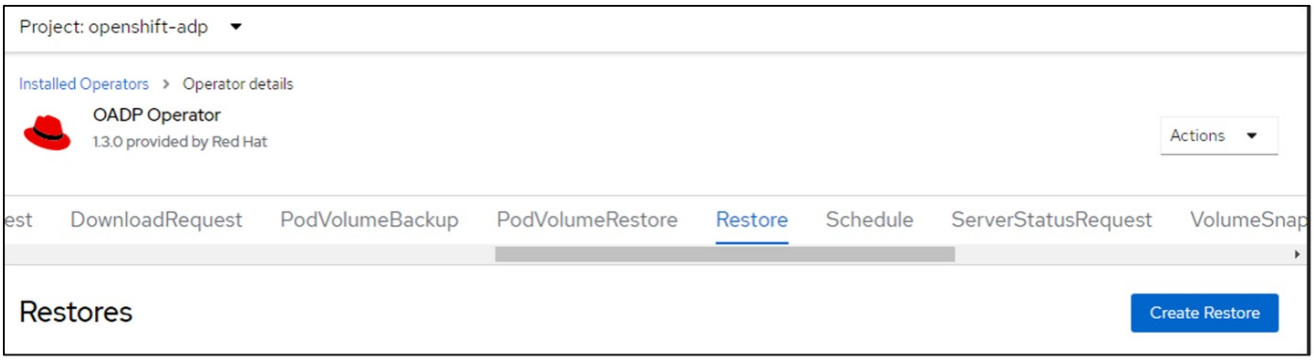
Stellen Sie eine VM aus einem Backup wieder her

Voraussetzungen

Um aus einem Backup wiederherzustellen, nehmen wir an, dass der Namespace, in dem die virtuelle Maschine existierte, versehentlich gelöscht wurde.

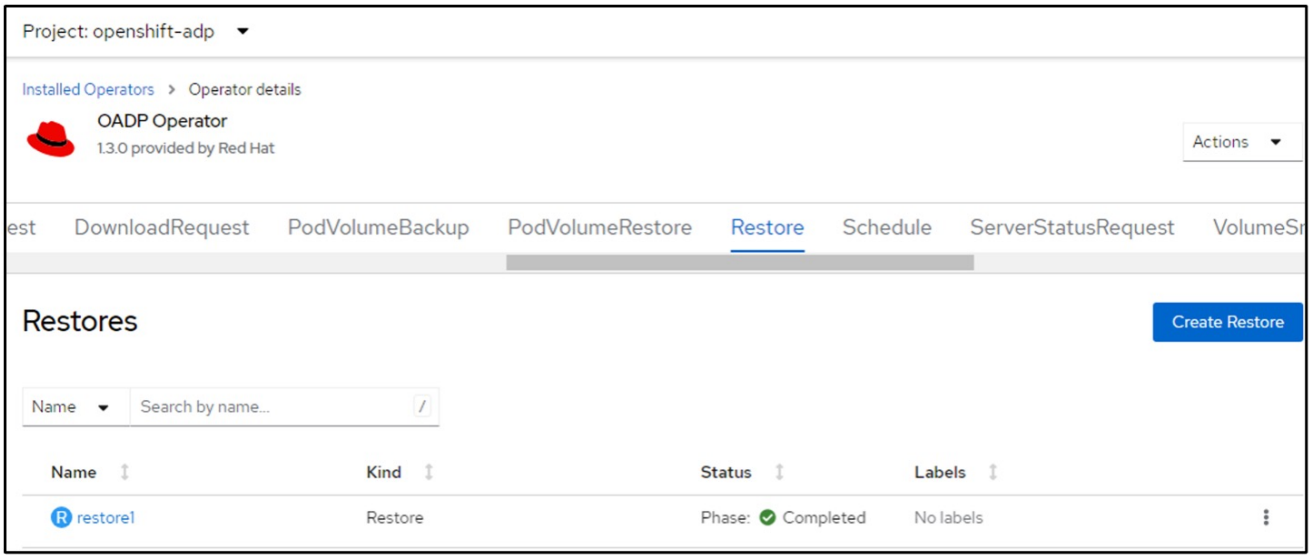
Restore auf denselben Namespace

Um das Backup wiederherzustellen, das wir gerade erstellt haben, müssen wir eine Restore Custom Resource (CR) erstellen. Geben Sie ihm einen Namen, geben Sie den Namen des Backups an, von dem aus wir die Wiederherstellungs-PVs wiederherstellen möchten, und setzen Sie sie auf „True“. Weitere Parameter können wie in dargestellt 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 in der Phase „Abgeschlossen“ angezeigt wird, sehen Sie, dass die virtuellen Maschinen zum Zeitpunkt der Snapshot-Erstellung wieder in den Status versetzt wurden. (Wenn das Backup bei der Ausführung der VM erstellt wurde, wird durch die Wiederherstellung der VM aus dem Backup die wiederhergestellte VM gestartet und in den Betriebszustand versetzt). Die VM wird im gleichen Namespace wiederhergestellt.



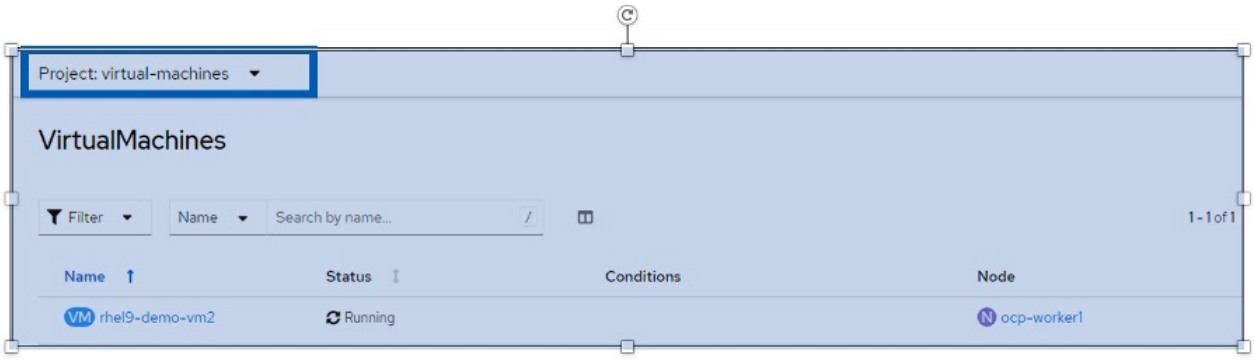
Wiederherstellung in einem anderen Namespace

Um die VM in einem anderen Namespace wiederherzustellen, können Sie in der yaml-Definition des Restore CR ein NamepaceMapping bereitstellen.

Mit der folgenden yaml-Beispieldatei wird ein Restore CR erstellt, um eine VM und ihre Laufwerke im Namespace „Virtual-Machines-Demo“ wiederherzustellen, als das Backup in den Namespace „Virtual Machines“ aufgenommen 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
```

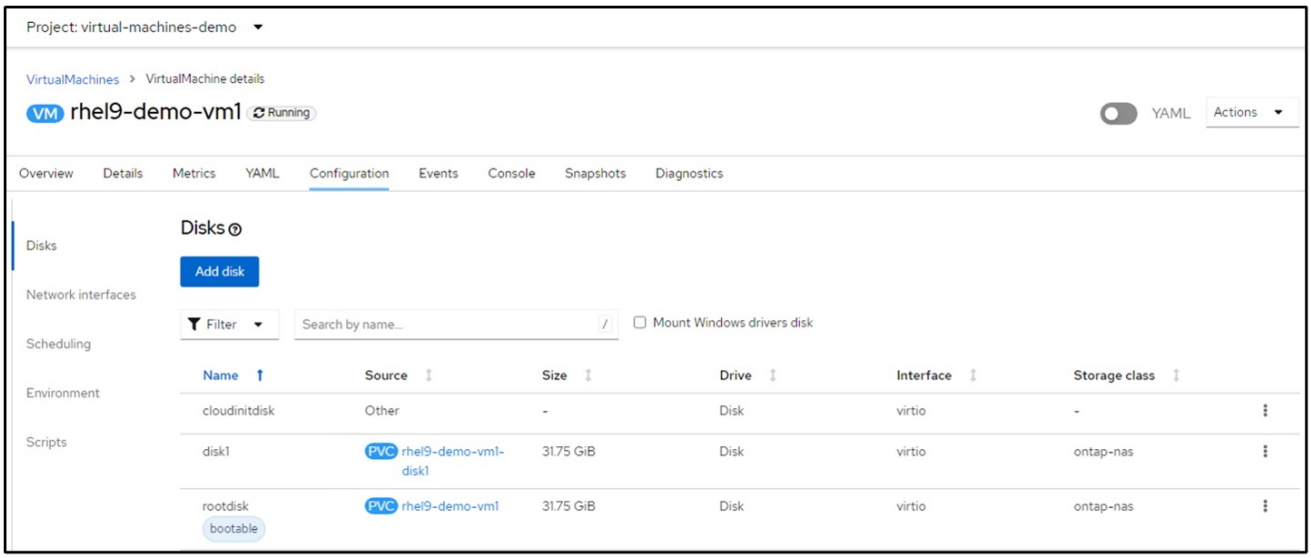
Wenn in der Phase „Abgeschlossen“ angezeigt wird, sehen Sie, dass die virtuellen Maschinen zum Zeitpunkt der Snapshot-Erstellung wieder in den Status versetzt wurden. (Wenn das Backup bei der Ausführung der VM erstellt wurde, wird durch die Wiederherstellung der VM aus dem Backup die wiederhergestellte VM gestartet und in den Betriebszustand versetzt). Die VM wird in einem anderen Namespace wiederhergestellt, wie im yaml angegeben.

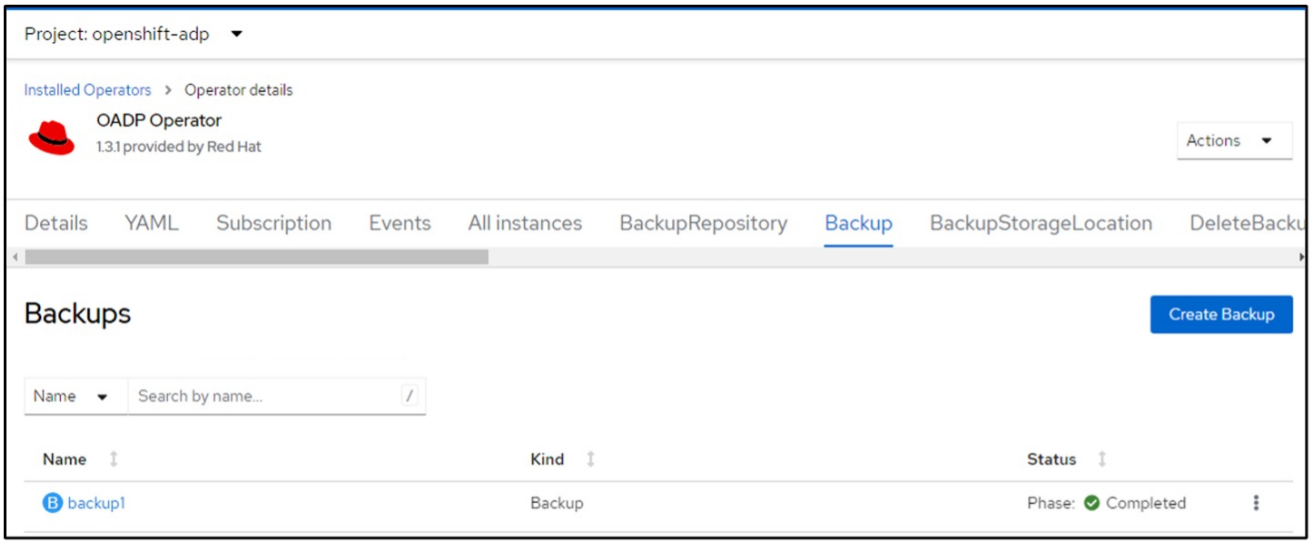


Wiederherstellung auf eine andere Storage-Klasse

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 configmap angegeben und im Wiederherstellungsbefehl auf die configmap verwiesen. Diese Funktion ermöglicht Ihnen die Wiederherstellung mit einer anderen Storage-Klasse.

Im folgenden Beispiel verwendet die virtuelle Maschine während der Erstellung ontap-nas als Storage-Klasse für ihre Festplatten. Es wird ein Backup der virtuellen Maschine namens backup1 erstellt.





Simulieren Sie einen Verlust der VM durch Löschen der VM.

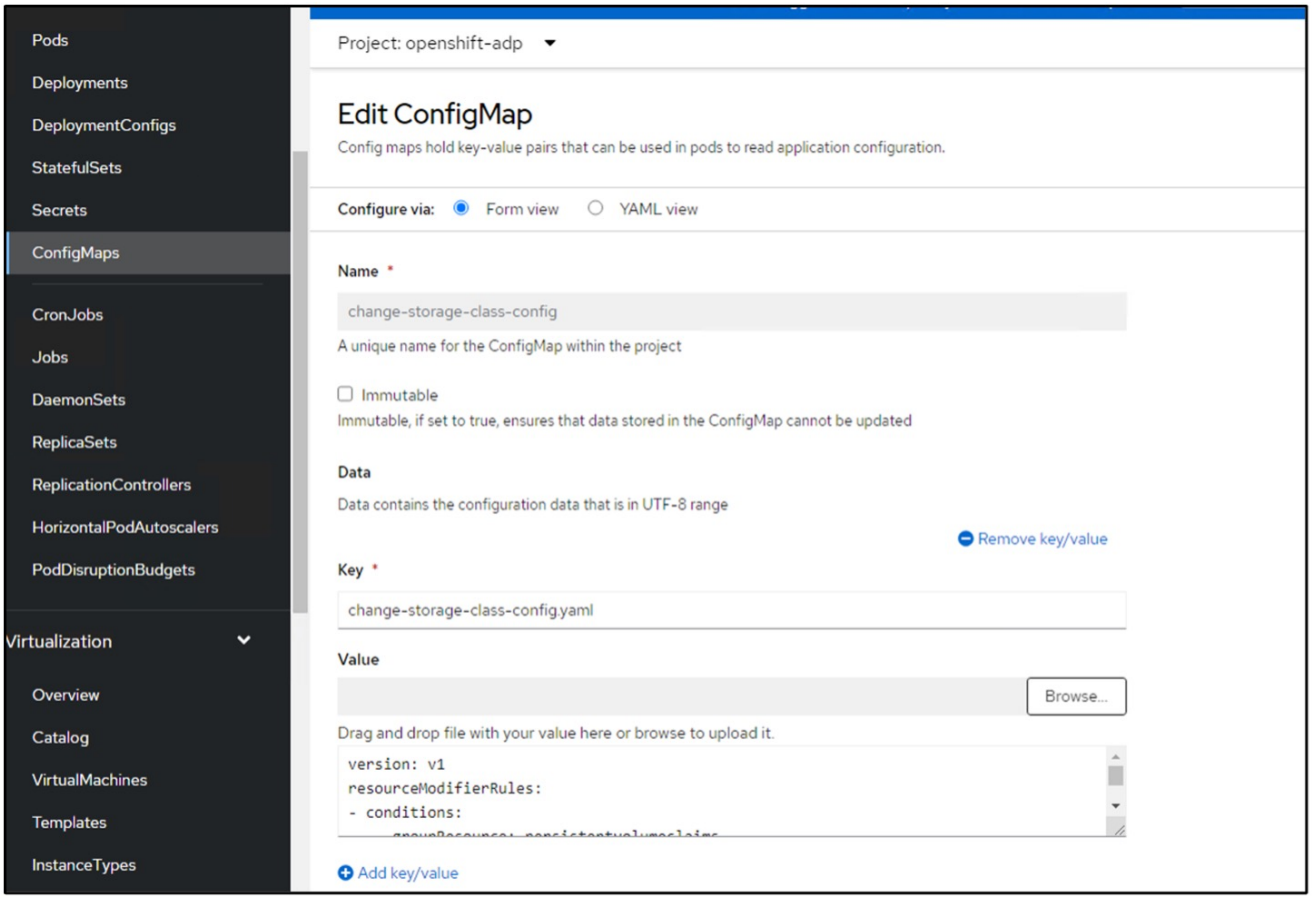
Um die VM mithilfe einer anderen Storage-Klasse, z. B. der Storage-Klasse ontap-nas-eco, wiederherzustellen, müssen Sie die folgenden zwei Schritte durchführen:

Schritt 1

Erstellen Sie eine Konfigurationszuordnung (Konsole) im openshift-adp-Namespace wie folgt:
Geben Sie die Details wie im Screenshot gezeigt ein:
Wählen Sie Namespace : 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 config map-Objekt sollte wie folgt 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>
```

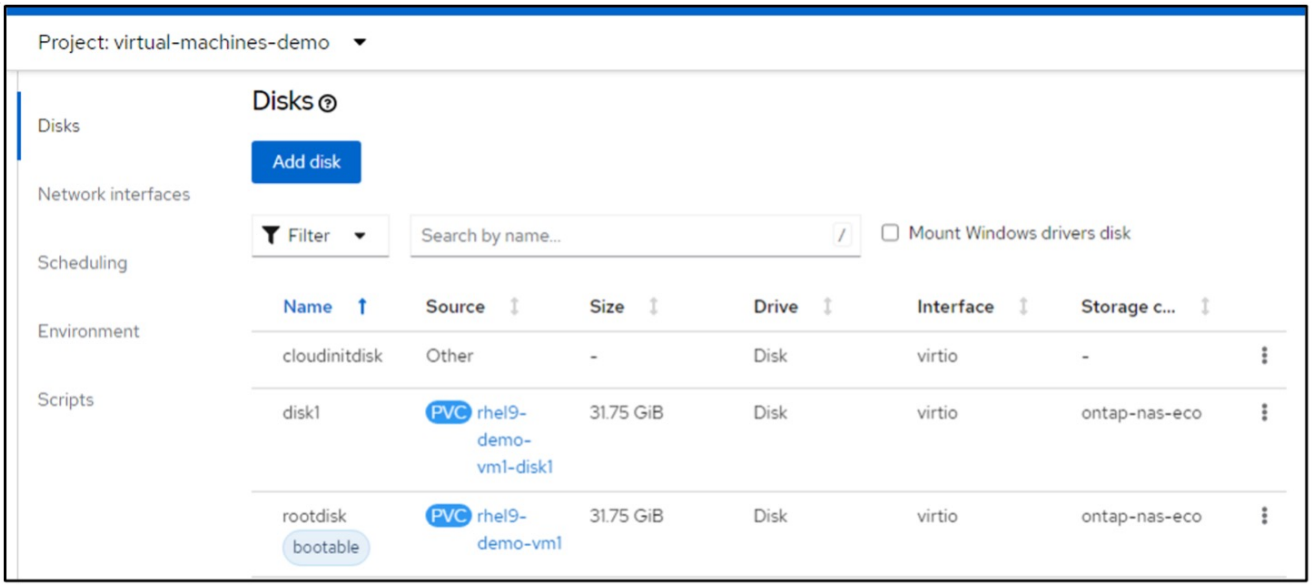
Diese Konfigurationszuordnung wendet die Ressourcenänderungsregel an, wenn die Wiederherstellung erstellt wird. Für alle Ansprüche auf persistente Volumes, die mit RHEL beginnen, wird ein Patch eingesetzt, der den Namen der Storage-Klasse auf ontap-nas-Eco ersetzt.

Schritt 2

Verwenden Sie zum Wiederherstellen der VM 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 gleichen Namespace mit den Festplatten wiederhergestellt, die mit der Storage-Klasse ontap-nas-eco erstellt wurden.



Löschen von Backups und Restores in mit Velero

Löschen eines Backups

Sie können einen Backup CR löschen, ohne die Objektspeicherdaten mit dem OC CLI-Tool zu löschen.

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

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

Laden Sie die CLI gemäß den Anweisungen in der herunter "Velero-Dokumentation".

Führen Sie den folgenden Löschbefehl über die Velero CLI aus

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

Sie können den Restore CR auch über die Velero CLI löschen

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

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

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