# Schützen Sie Container-Apps mit Tools von Drittanbietern

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-cloud/openshift/os-dp-velero-solution.html on August 18, 2025. Always check docs.netapp.com for the latest.

# Inhalt


Schützen Sie Container-Apps mit Tools von Drittanbietern . . . 1
- Datenschutz für Container-Apps in der OpenShift Container Platform mithilfe der OpenShift API for Data Protection (OADP) . . . 1
- Installation des OpenShift API for Data Protection (OADP)-Operators . . . 3
  - Voraussetzungen . . . 3
  - Schritte zur Installation des OADP-Operators . . . 3
- Erstellen eines On-Demand-Backups für Apps in OpenShift Container Platform . . . 12
  - Schritte zum Erstellen einer Sicherungskopie einer App . . . 12
  - Erstellen geplanter Backups für Apps . . . 14
- Migrieren einer App von einem Cluster zu einem anderen . . . 15
- Wiederherstellen einer App aus einem Backup . . . 20
  - Voraussetzungen . . . 20
- Löschen von Backups und Wiederherstellungen mit Velero . . . 27
  - Alle Backups auflisten . . . 27
  - Löschen einer Sicherung . . . 27
  - Löschen der Wiederherstellung . . . 28

# Schützen Sie Container-Apps mit Tools von Drittanbietern

## Datenschutz für Container-Apps in der OpenShift Container Platform mithilfe der OpenShift API for Data Protection (OADP)

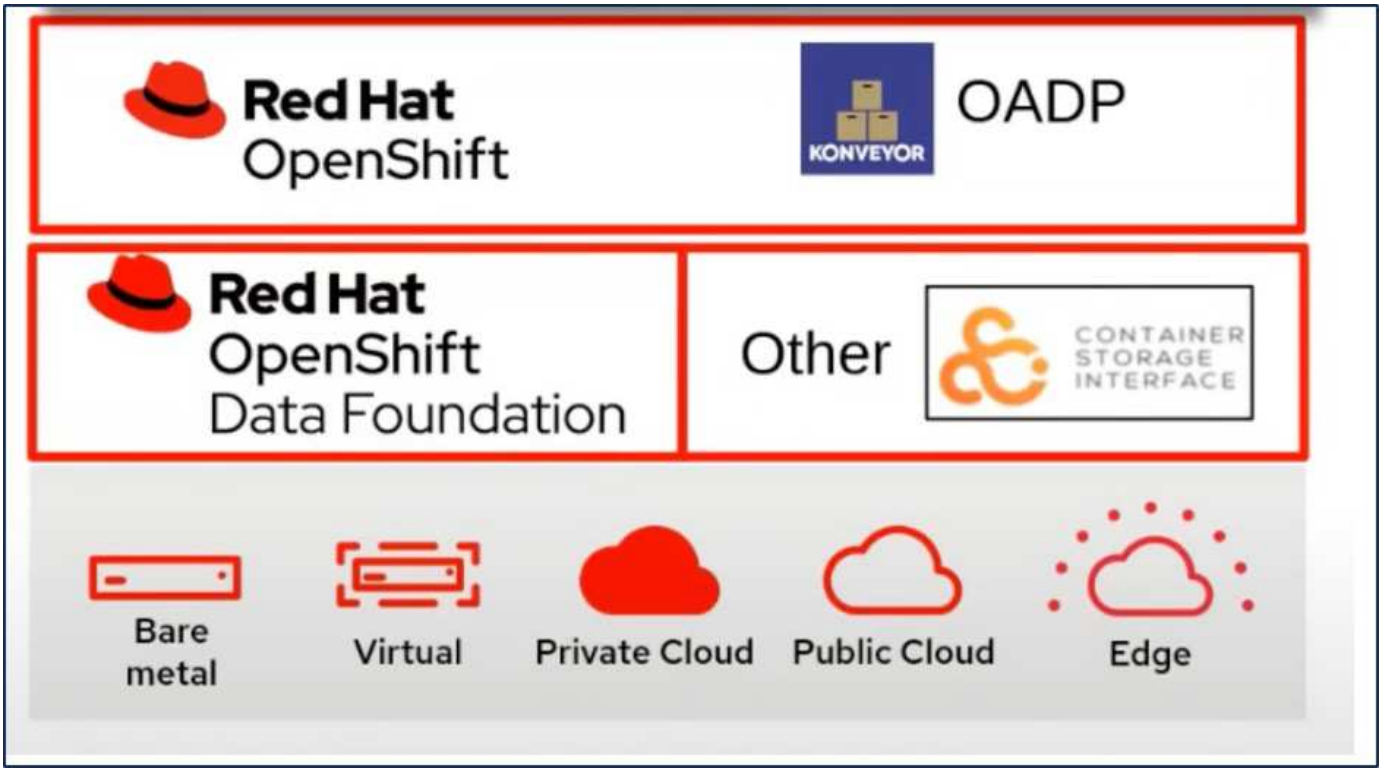
Dieser Abschnitt des Referenzdokuments enthält Details zum Erstellen von Backups von Container-Apps mithilfe der OpenShift API for Data Protection (OADP) mit Velero auf NetApp ONTAP S3 oder NetApp StorageGRID S3. Die Sicherungen der Ressourcen mit Namespace-Bereich, einschließlich der Persistent Volumes (PVs) der App, werden mithilfe von CSI Trident Snapshots erstellt.

Der persistente Speicher für Container-Apps kann durch ONTAP -Speicher unterstützt werden, der in den OpenShift-Cluster integriert ist."Trident CSI" . In diesem Abschnitt verwenden wir"OpenShift-API für Datenschutz (OADP)" um Backups von Apps inklusive der Datenmengen durchzuführen,

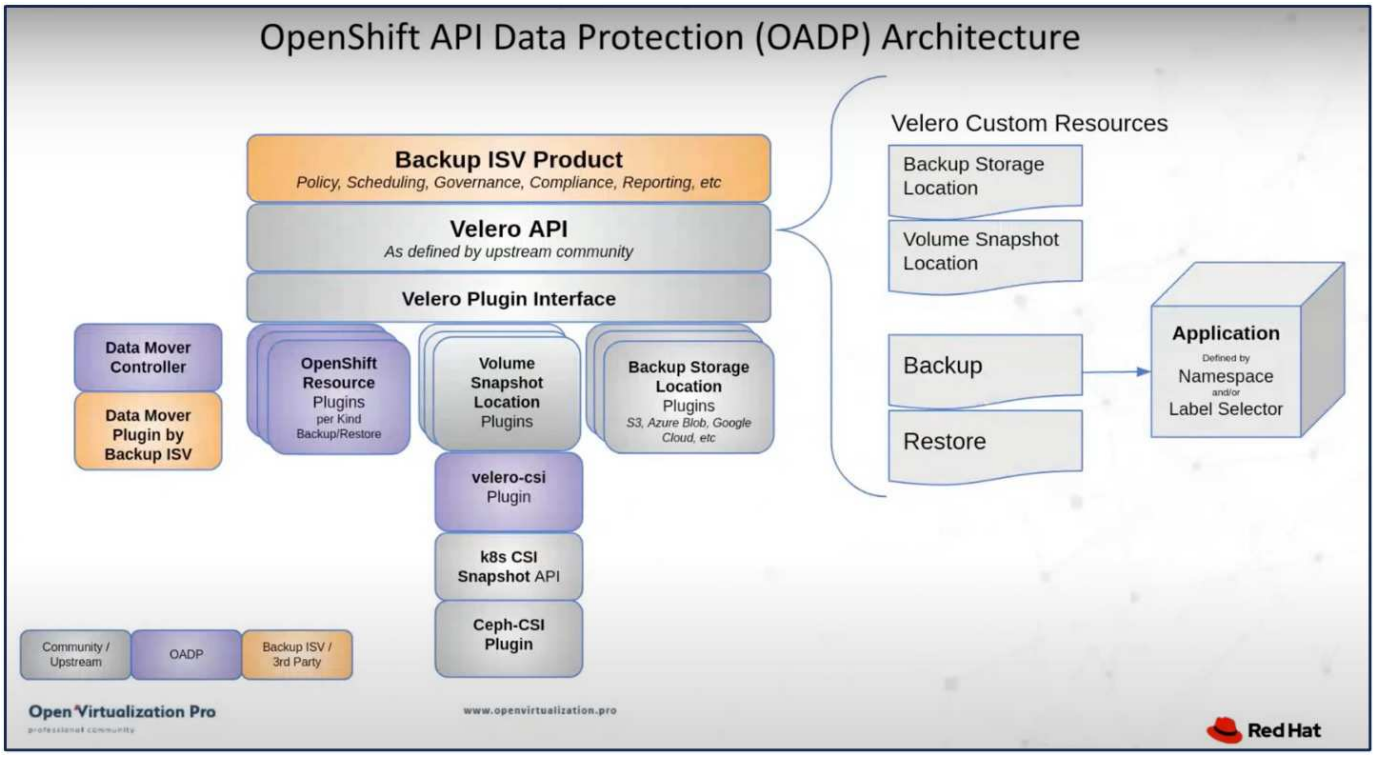
- ONTAP Objektspeicher
- StorageGrid

Bei Bedarf stellen wir dann eine Wiederherstellung aus dem Backup her. Bitte beachten Sie, dass die App nur in dem Cluster wiederhergestellt werden kann, von dem das Backup erstellt wurde.

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
- OADP Operator 1.13 bereitgestellt von Red Hat
- Velero CLI 1.13 für Linux
- Trident 24.02
- ONTAP 9.12
- PostgreSQL mit Helm installiert.

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

# Installation des OpenShift API for Data Protection (OADP)-Operators

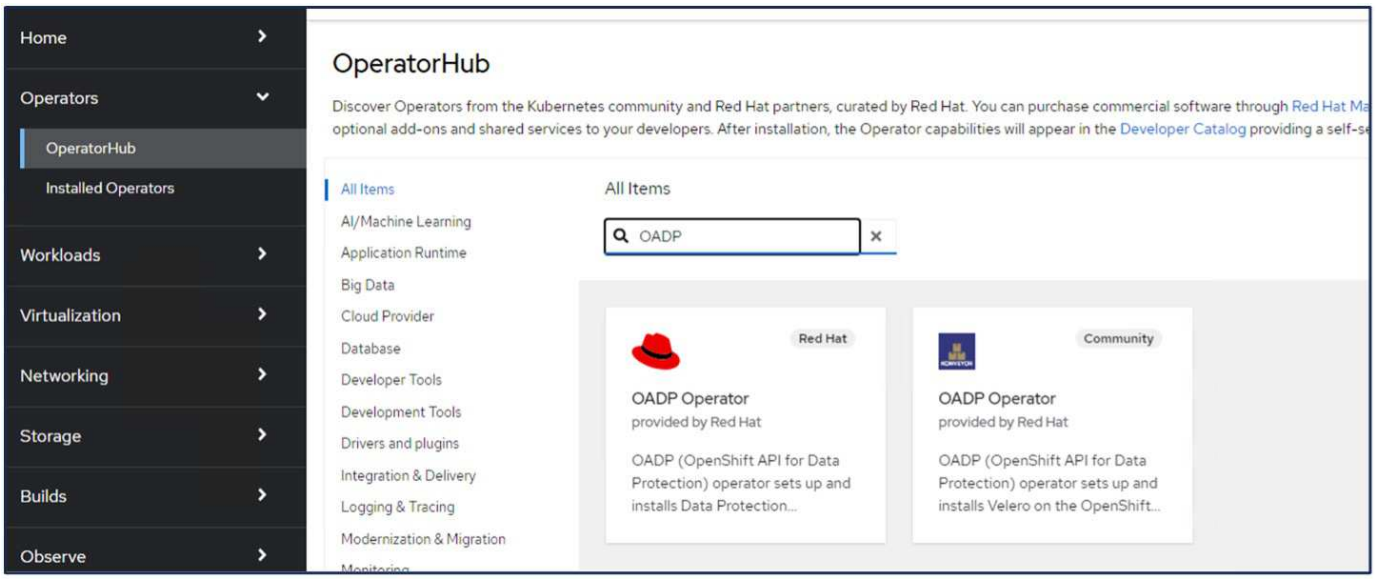
In diesem Abschnitt wird die Installation des OpenShift API for Data Protection (OADP) Operator beschrieben.

## 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
- Eine Anwendung, zB PostgreSQL, die auf dem Cluster bereitgestellt wird
- Eine Admin-Workstation mit installierten und zu $PATH hinzugefügten Tridentctl- und OC-Tools

## 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<br>4.14.4 provided by Red Hat | NS openshift-cnv | NS openshift-cnv | Succeeded<br>Up to date |
| OADP Operator<br>1.3.0 provided by Red Hat | NS openshift-adp | NS openshift-adp | Succeeded<br>Up to date |
| Package Server<br>0.0.1-snapshot provided by | NS openshift-operator-lifecycle-manager | NS 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.

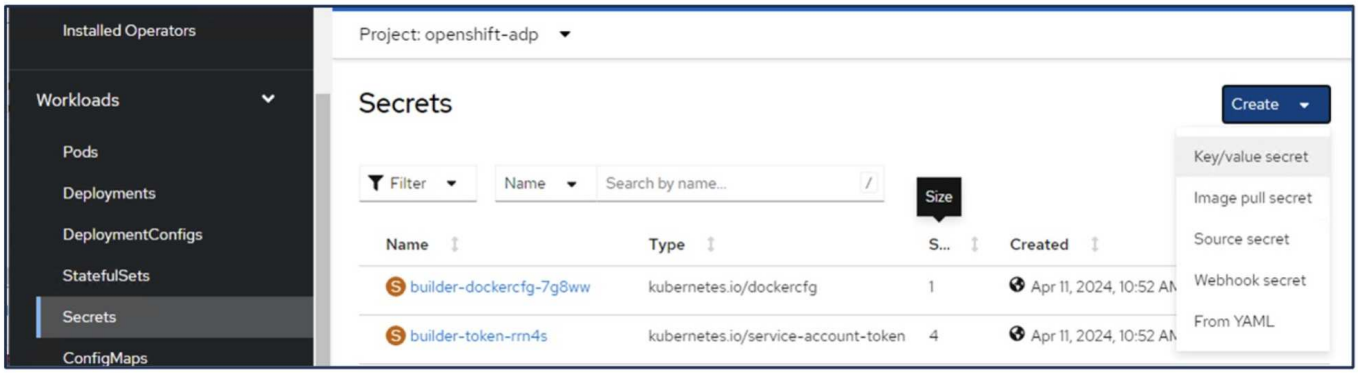
### Voraussetzungen für die Velero-Konfiguration mit StorageGrid S3-Details

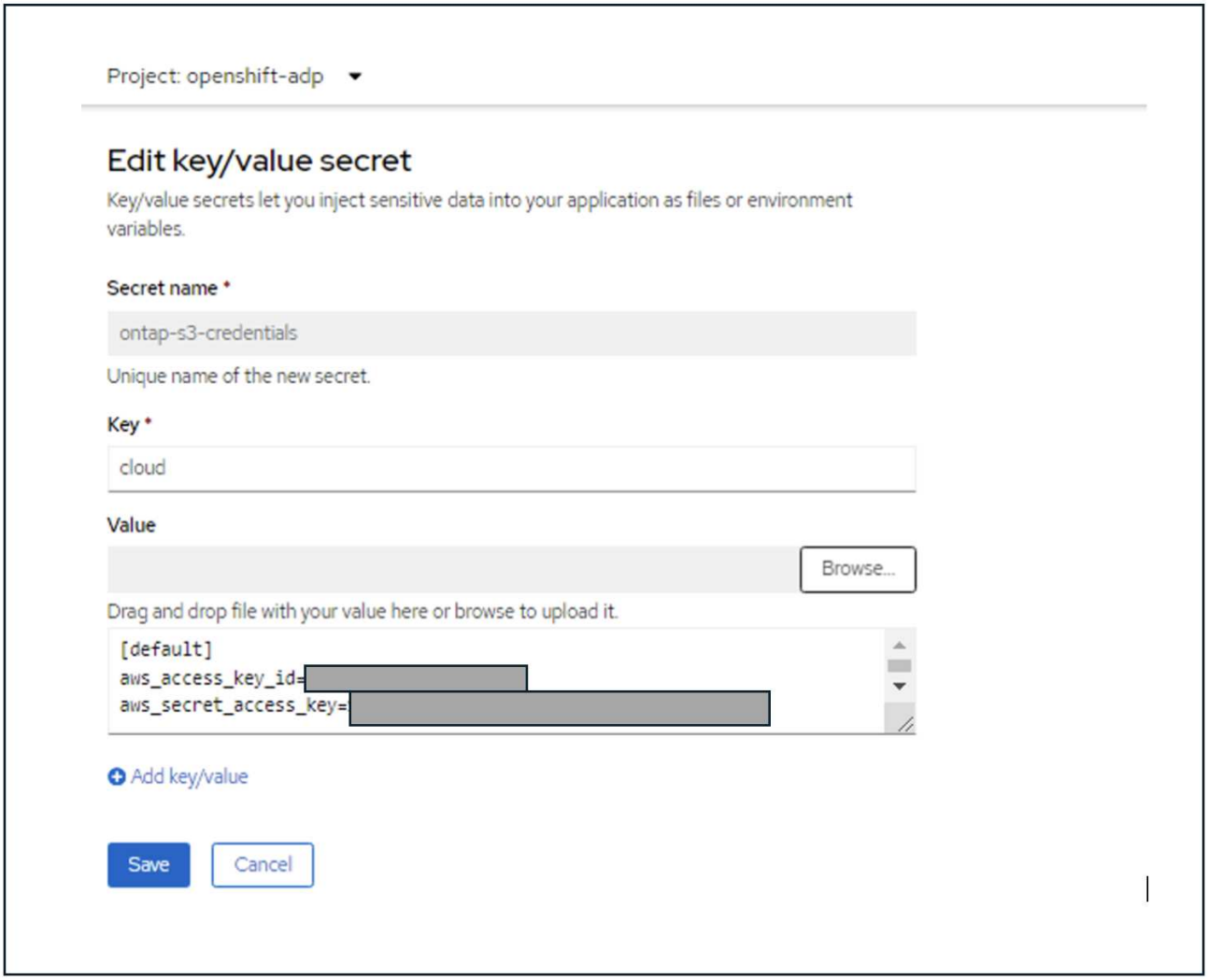
Velero kann für die Verwendung von S3-kompatiblem Object Storage konfiguriert werden. Sie können StorageGrid S3 mit den im folgenden Abschnitt beschriebenen Verfahren konfigurieren."StorageGrid-Dokumentation" . Für die Integration mit Velero benötigen Sie die folgenden Informationen aus Ihrer StorageGrid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

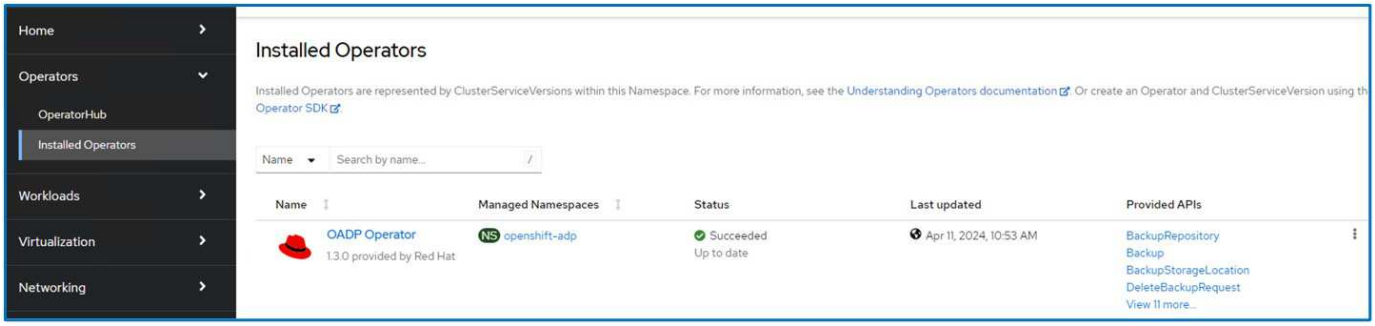




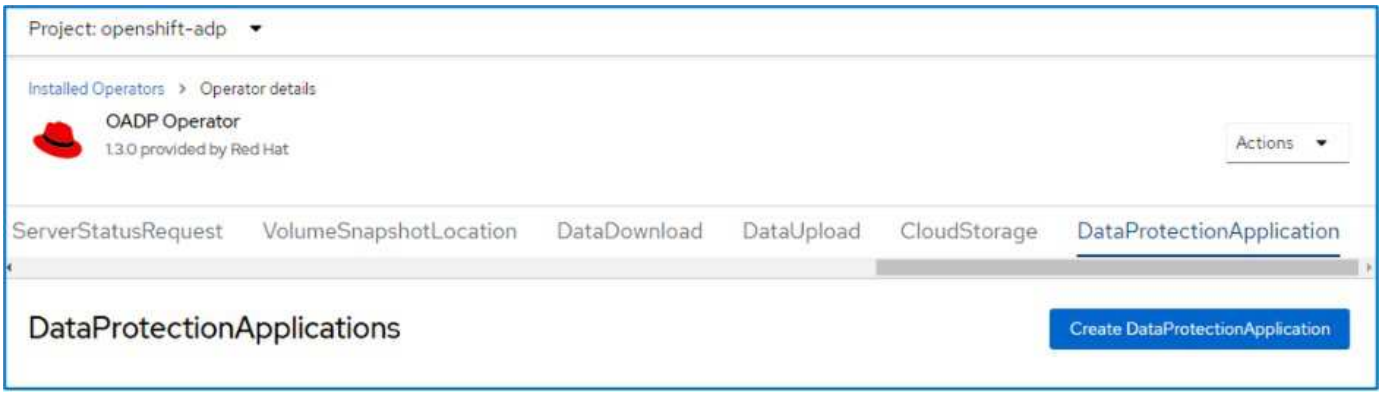

Um ein Geheimnis mit dem Namen sg-s3-credentials über die CLI zu erstellen, können Sie den folgenden Befehl verwenden.

```
# 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://10.61.181.161' ->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: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

**Beispiel-YAML-Datei zum Konfigurieren von Velero mit StorageGrid S3 als Backup-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
```

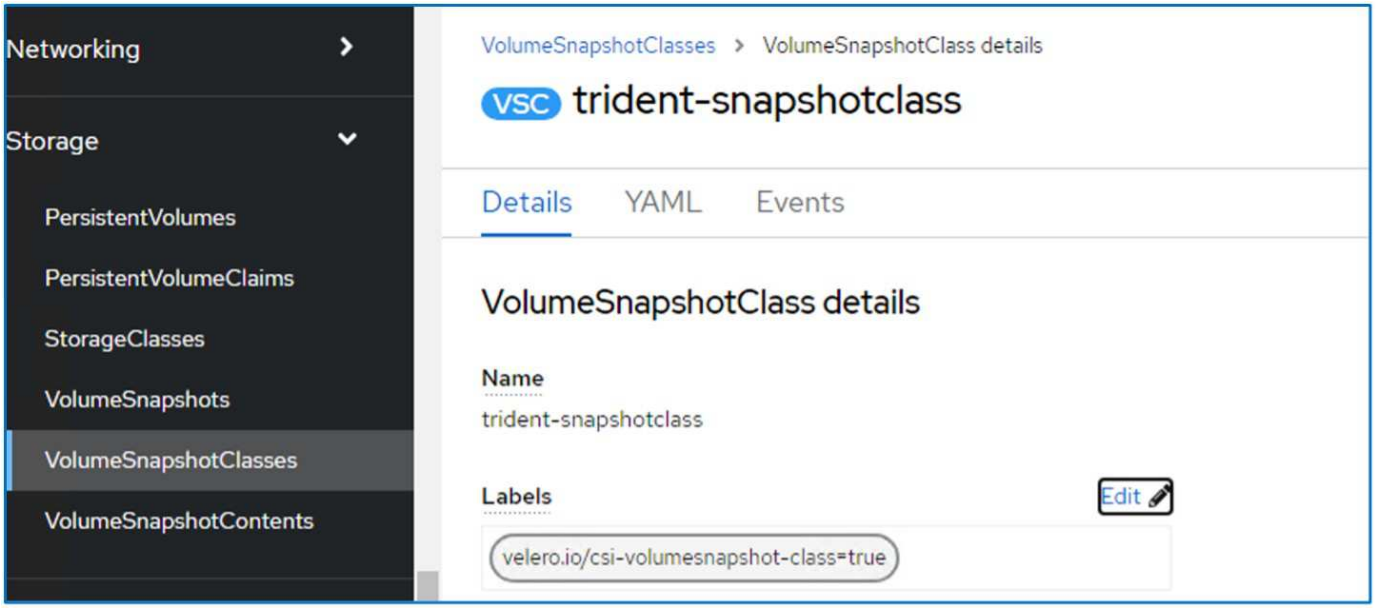
Der Abschnitt „Spec“ in der YAML-Datei sollte für die folgenden Parameter entsprechend dem obigen Beispiel konfiguriert werden.

**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.

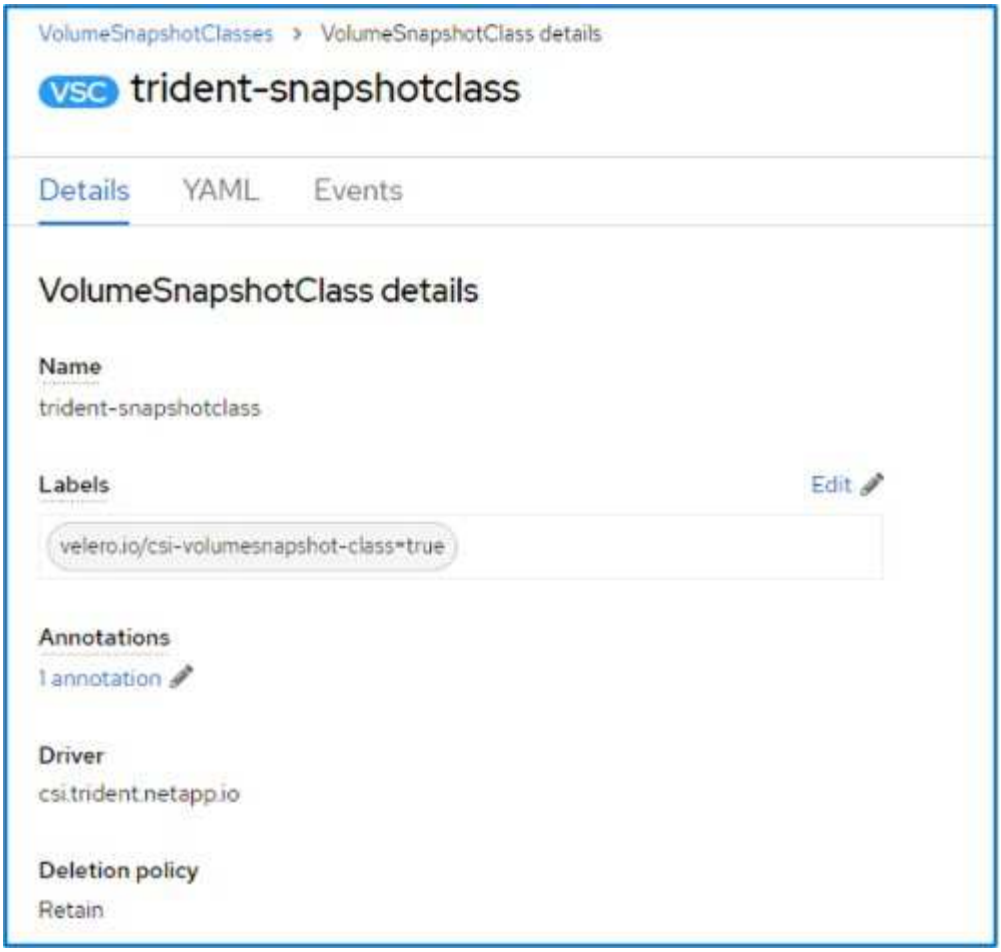
**CSI-Plugin aktivieren** Fügen Sie csi zu den Standard-Plugins für Velero hinzu, um persistente Volumes mit CSI-Snapshots zu sichern. Die Velero CSI-Plugins wählen zum Sichern von CSI-gestützten PVCs die VolumeSnapshotClass im Cluster aus, auf die das Label **velero.io/csi-volumesnapshot-class** gesetzt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

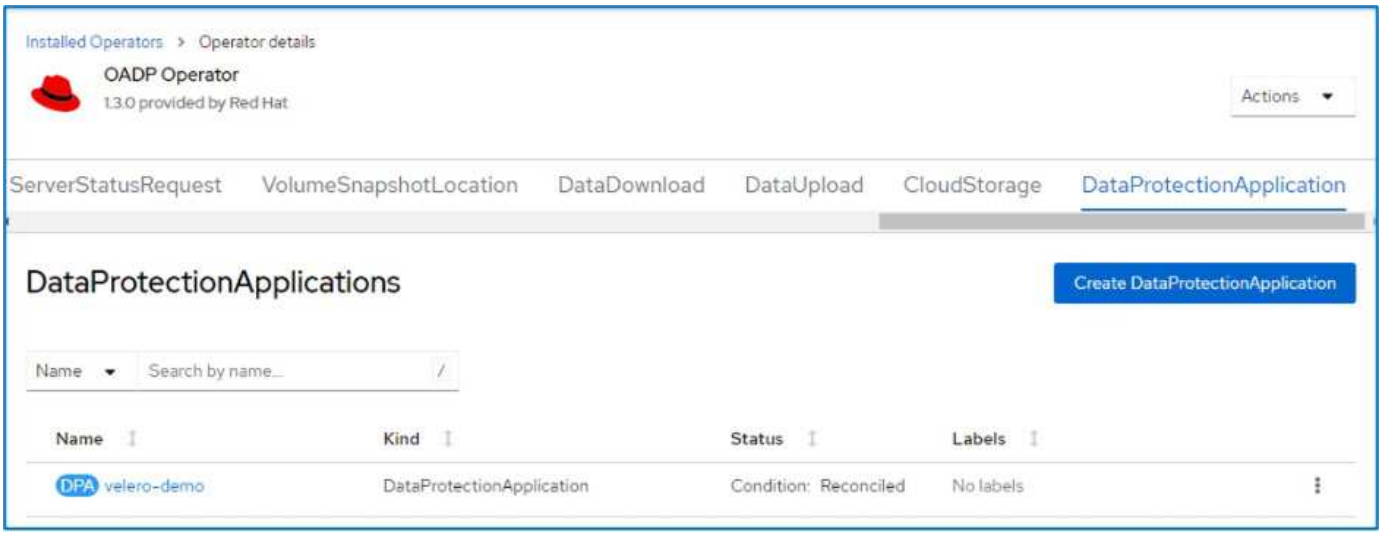



Stellen Sie sicher, dass die Snapshots auch dann bestehen bleiben, wenn die VolumeSnapshot-Objekte gelöscht werden. Dies kann durch Festlegen der **deletionPolicy** auf „Beibehalten“ erfolgen. Andernfalls gehen beim Löschen eines Namespace alle darin jemals gesicherten PVCs vollständig verloren.

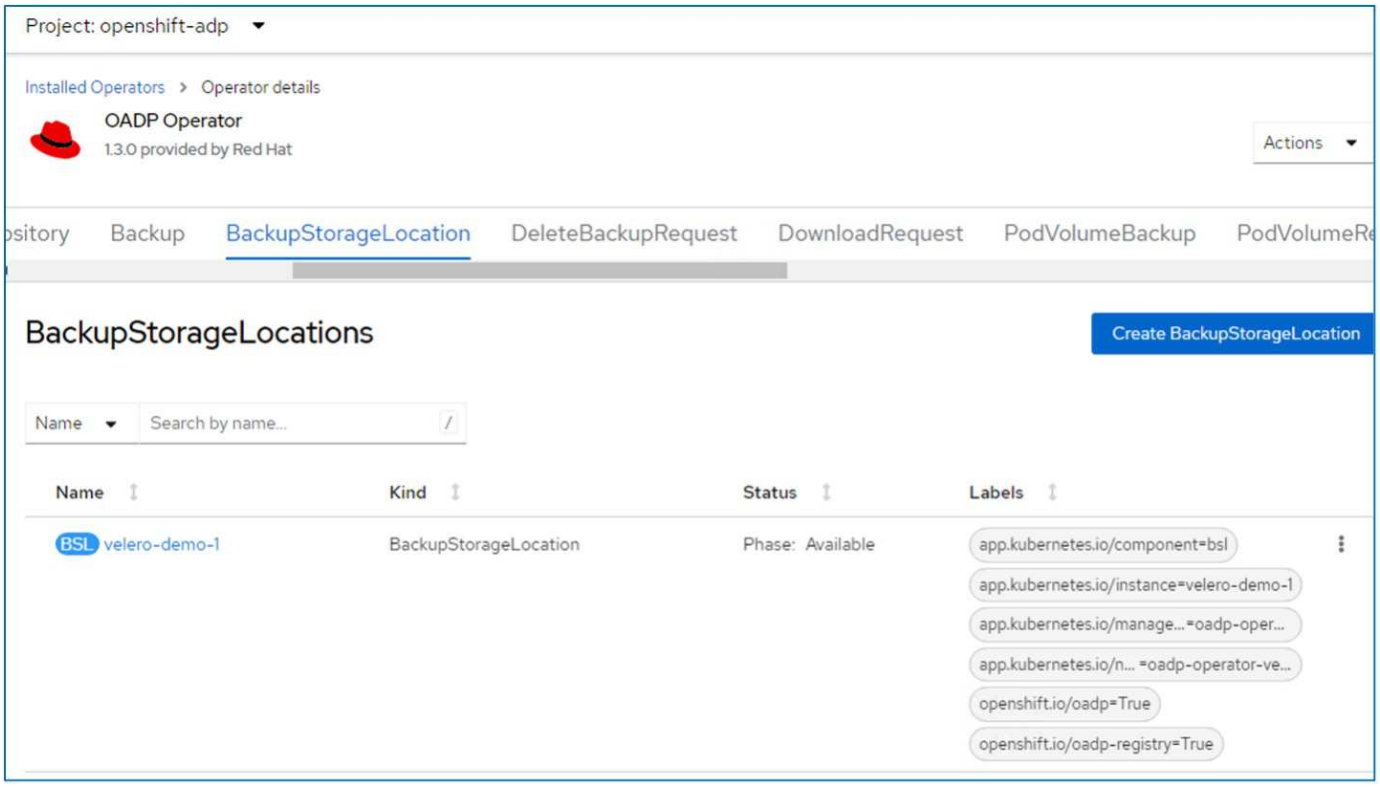
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```




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 eines On-Demand-Backups für Apps in OpenShift Container Platform

In diesem Abschnitt wird beschrieben, wie Sie On-Demand-Backups für VMs in OpenShift Virtualization erstellen.

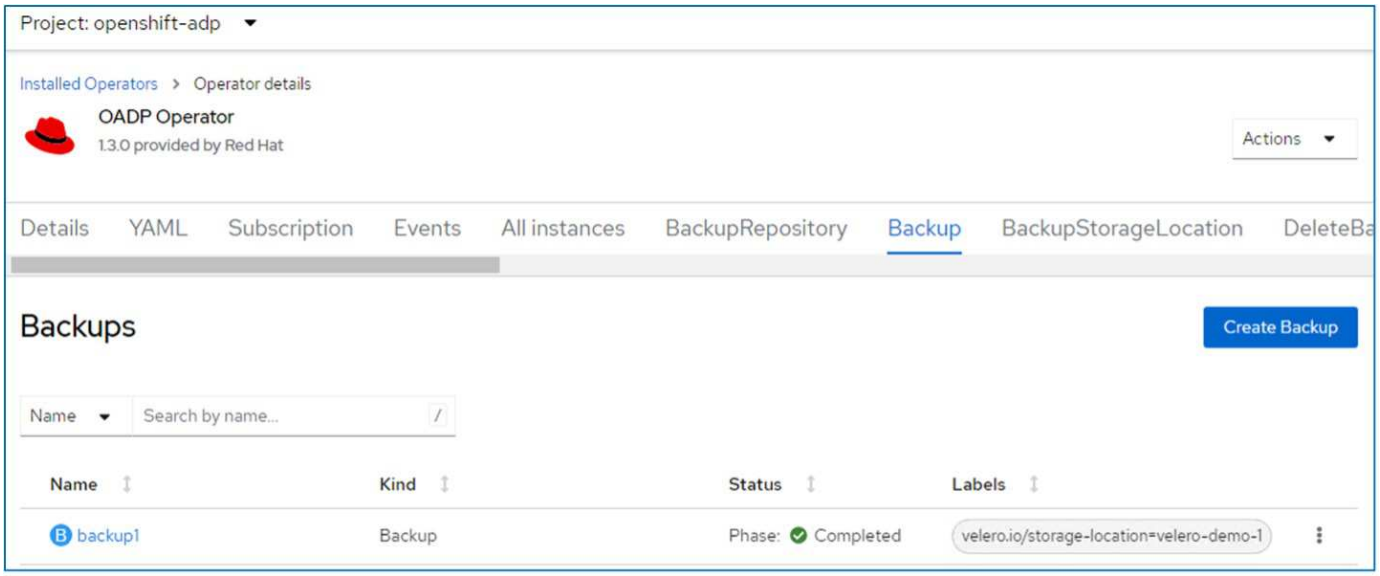
## Schritte zum Erstellen einer Sicherungskopie einer App

Um ein On-Demand-Backup einer App (App-Metadaten und persistente Volumes der App) zu erstellen, klicken Sie auf die Registerkarte **Backup**, um eine benutzerdefinierte Backup-Ressource (CR) zu erstellen. Zum Erstellen des Backup-CR wird ein YAML-Beispiel bereitgestellt. Mithilfe dieses YAML werden die App und ihr dauerhafter Speicher im angegebenen Namespace gesichert. Weitere Parameter können wie in der Abbildung gezeigt eingestellt werden."Dokumentation" .

Ein Snapshot der persistenten Volumes und der App-Ressourcen im angegebenen Namespace wird vom CSI erstellt. Dieser Snapshot wird am im YAML angegebenen Sicherungsspeicherort gespeichert. Das Backup bleibt gemäß TTL 30 Tage lang im System.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-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/container-demo-backup) angezeigt. Sie können sehen, dass der Inhalt der Sicherung die Volume-Snapshots, Protokolle und andere Metadaten der Anwendung umfasst.

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

Path: / demobackup/ backups/ backup1/

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

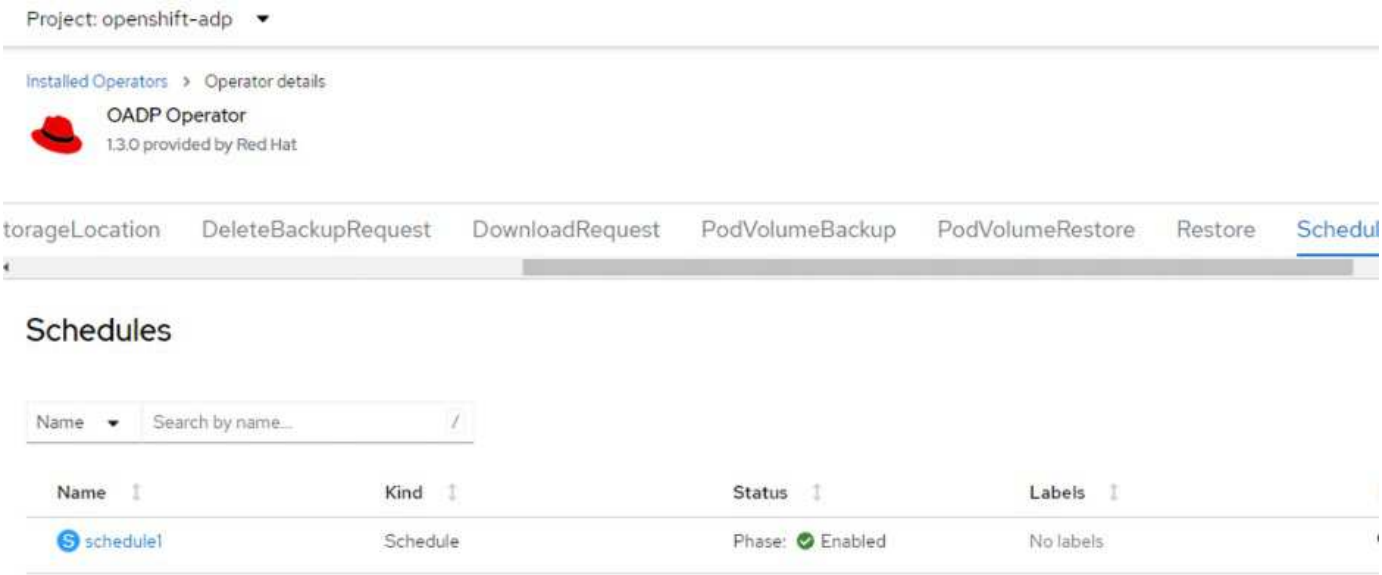
## Erstellen geplanter Backups für Apps

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. Unten sehen Sie ein YAML-Beispiel zum Erstellen eines Schedule CR.

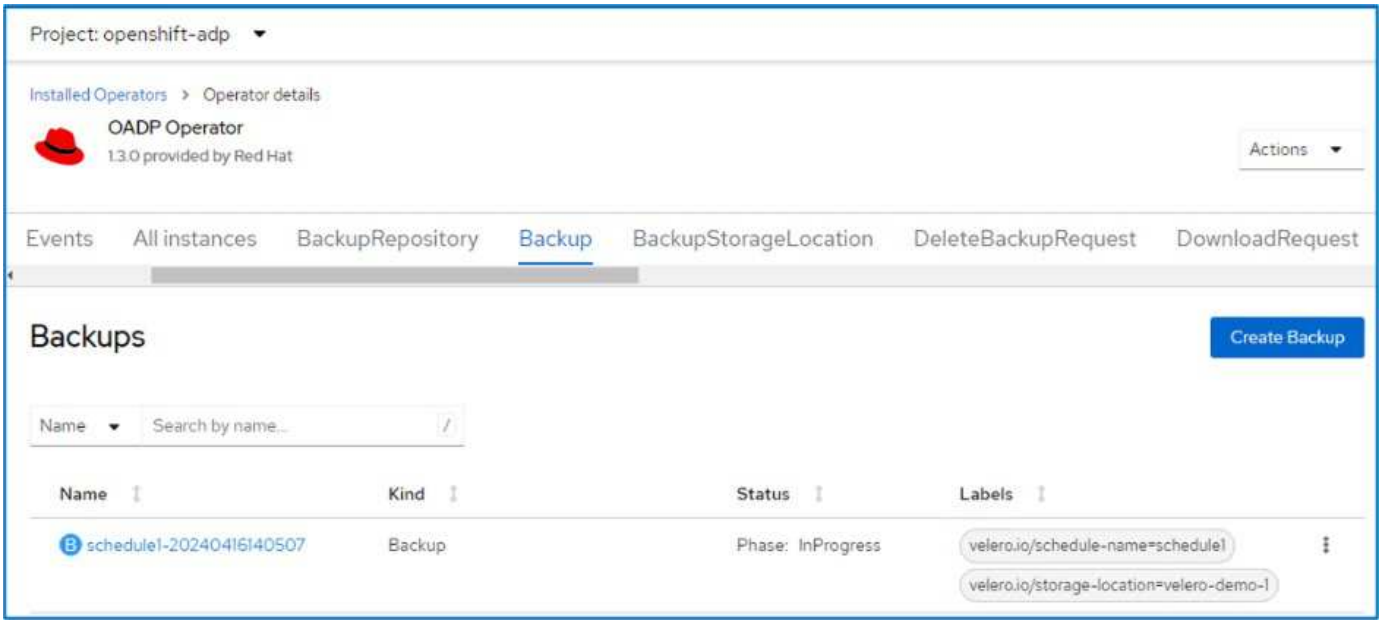
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

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.




# Migrieren einer App von einem Cluster zu einem anderen

Die Sicherungs- und Wiederherstellungsfunktionen von Velero machen es zu einem wertvollen Tool für die Migration Ihrer Daten zwischen Clustern. In diesem Abschnitt wird beschrieben, wie Sie Apps von einem Cluster zu einem anderen migrieren, indem Sie eine Sicherungskopie der App im Objektspeicher eines Clusters erstellen und die App dann aus demselben Objektspeicher in einem anderen Cluster wiederherstellen. .

**Sicherung vom ersten Cluster**

**Voraussetzungen für Cluster 1**

- Trident muss auf dem Cluster installiert sein.
- Es müssen ein Trident-Backend und eine Speicherklasse erstellt werden.
- Der OADP-Operator muss auf dem Cluster installiert sein.
- Die DataProtectionApplication sollte konfiguriert werden.

Verwenden Sie die folgende Spezifikation, um das DataProtectionApplication-Objekt zu konfigurieren.

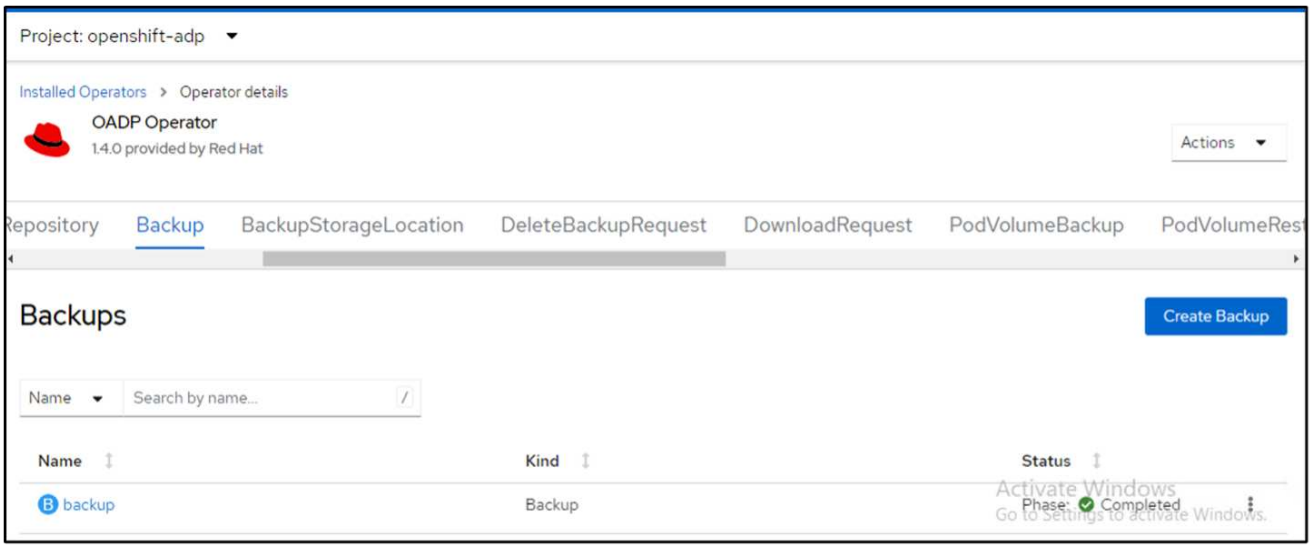
```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Erstellen Sie eine Anwendung auf dem Cluster und erstellen Sie eine Sicherungskopie dieser Anwendung. Installieren Sie beispielsweise eine Postgres-Anwendung.

```
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE     VERSION
ocp6-master1  Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-master2  Ready    worker                 3d12h   v1.27.15+6147456
ocp6-master3  Ready    control-plane,master   3d13h   v1.27.15+6147456
ocp6-worker1  Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker2  Ready    worker                 3d12h   v1.27.15+6147456
ocp6-worker3  Ready    control-plane,master   3d12h   v1.27.15+6147456
[root@localhost ~]# helm install postgresql bitnami/postgresql -n postgresql --create namespace^C
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          4h53m
[root@localhost ~]# oc get pvc -n postgresql
NAME                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0    Bound    pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            ontap-nas      4h53m
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-2e9e982f-54a4-4e7b-8eae-a589e0d9d819   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         4h55m
pvc-f7a3c772-0e61-49cb-a3d0-7c7b2ec87dc6   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         4h53m
[root@localhost ~]#
```

- Verwenden Sie die folgende Spezifikation für die Sicherungs-CR:

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```




Sie können auf die Registerkarte **Alle Instanzen** klicken, um die verschiedenen Objekte anzuzeigen, die erstellt werden und verschiedene Phasen durchlaufen, bis sie schließlich zur Phase **abgeschlossen** der Sicherung gelangen.

Eine Sicherung der Ressourcen im Namespace „postgresql“ wird am Object Storage-Speicherort (ONTAP S3) gespeichert, der im „backupLocation“ in der OADP-Spezifikation angegeben ist.

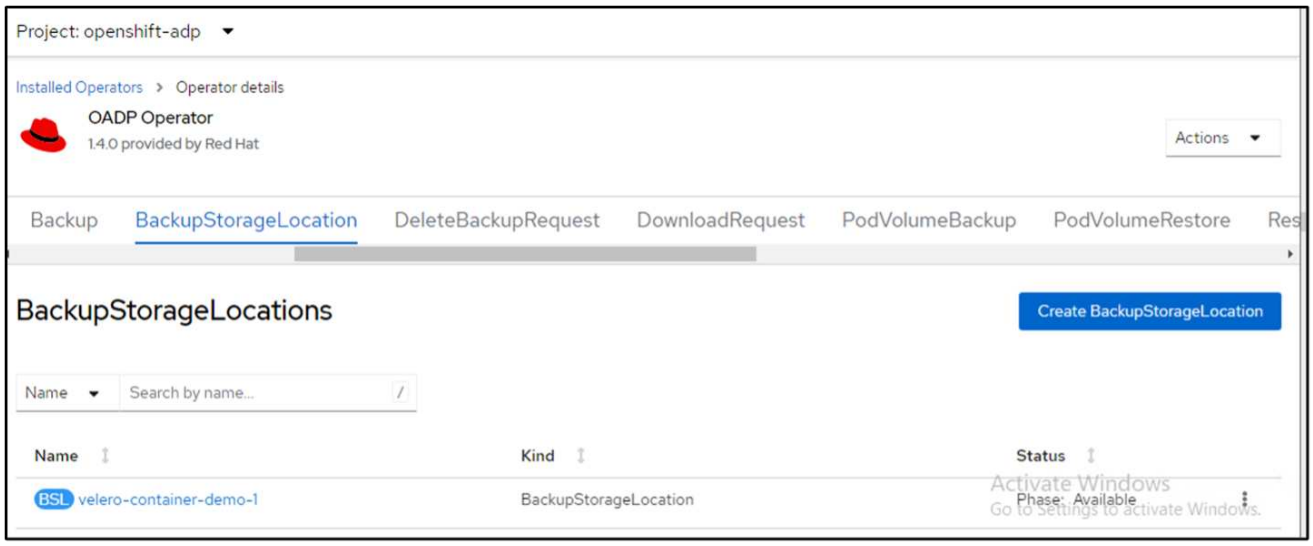
### Wiederherstellen auf einem zweiten Cluster

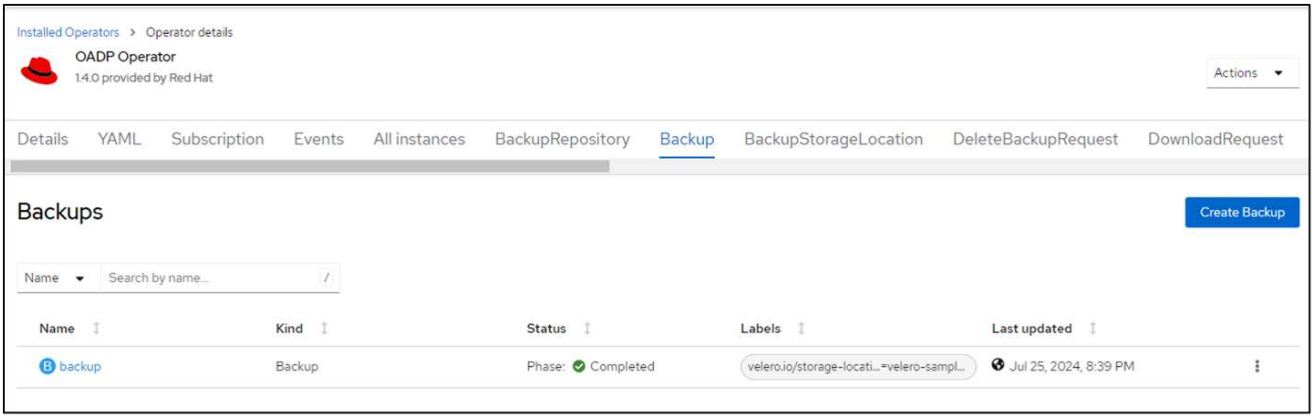
#### Voraussetzungen für Cluster 2

- Trident muss auf Cluster 2 installiert sein.
- Die PostgreSQL-App darf NICHT bereits im PostgreSQL-Namespace installiert sein.
- Der OADP-Operator muss auf Cluster 2 installiert sein und der BackupStorage-Speicherort muss auf denselben Objektspeicherort verweisen, an dem die Sicherung vom ersten Cluster gespeichert wurde.
- Der Backup-CR muss vom zweiten Cluster aus sichtbar sein.

```
[root@localhost ~]# oc get pods -n trident
NAME                                  READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz              2/2     Running   2          2d7h
trident-node-linux-8vvm2              2/2     Running   0          2d7h
trident-node-linux-bgs6f              2/2     Running   2          2d7h
trident-node-linux-njwb8              2/2     Running   0          2d7h
trident-node-linux-scqjl              2/2     Running   0          2d7h
trident-node-linux-swr69              2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68      1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM              STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic      ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc   vsphere-sc              2d7
h
[root@localhost ~]#
```

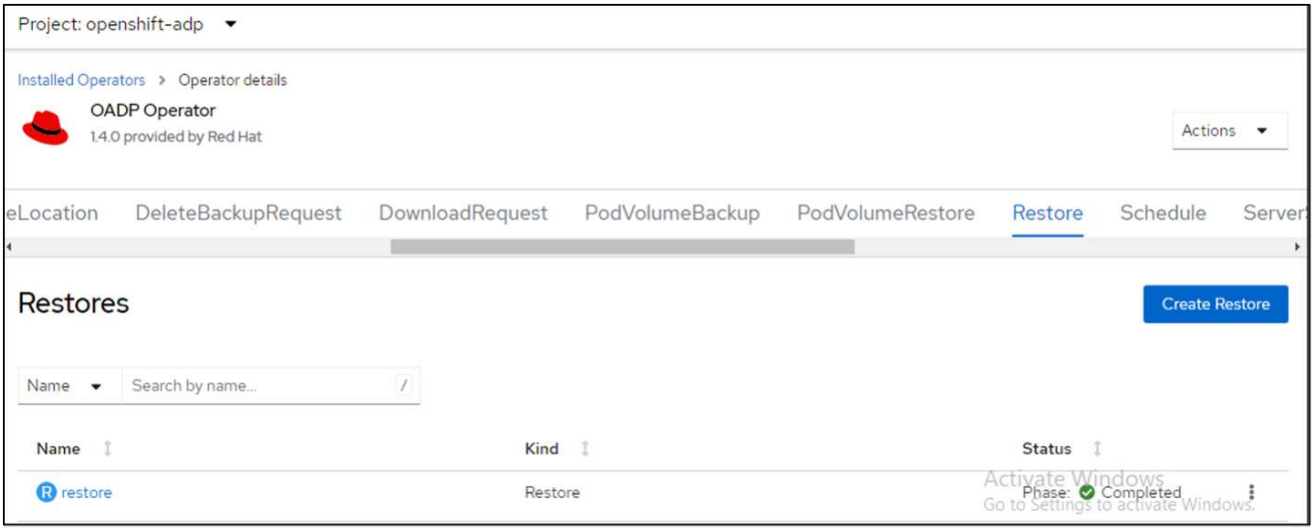





Stellen Sie die App auf diesem Cluster aus der Sicherung wieder her. Verwenden Sie das folgende YAML, um die Wiederherstellungs-CR zu erstellen.

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

Wenn die Wiederherstellung abgeschlossen ist, sehen Sie, dass die PostgreSQL-App auf diesem Cluster ausgeführt wird und mit dem PVC und einem entsprechenden PV verknüpft ist. Der Zustand der App ist derselbe wie zum Zeitpunkt der Sicherung.



```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE    VERSION
ocp7-master1   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0   Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc               vsphere-sc
         2d10h
[root@localhost ~]#
```

# Wiederherstellen einer App aus einem Backup

In diesem Abschnitt wird beschrieben, wie Sie Apps aus einer Sicherung wiederherstellen.

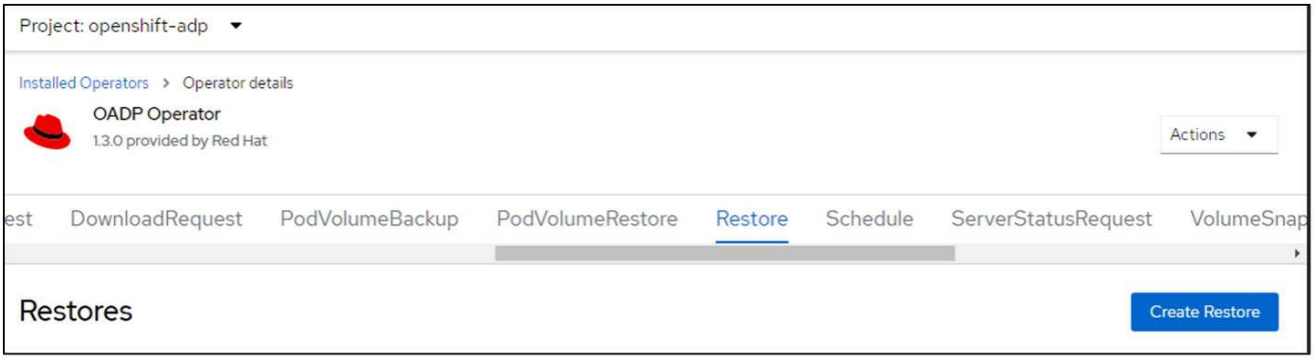
## Voraussetzungen

Um eine Wiederherstellung aus einer Sicherung durchzuführen, gehen wir davon aus, dass der Namespace, in dem die App vorhanden war, versehentlich gelöscht wurde.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

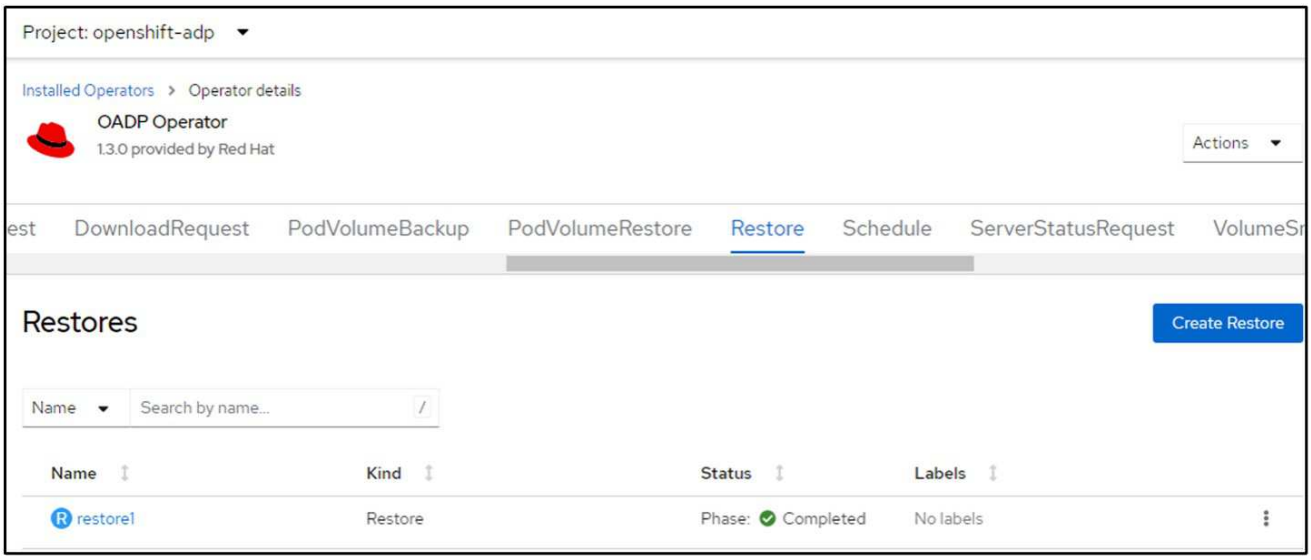
### Wiederherstellen im selben Namespace

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
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die App in den Zustand zurückversetzt wurde, in dem sie sich zum Zeitpunkt der Erstellung des Snapshots befand. Die App wird im selben Namespace wiederhergestellt.



```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

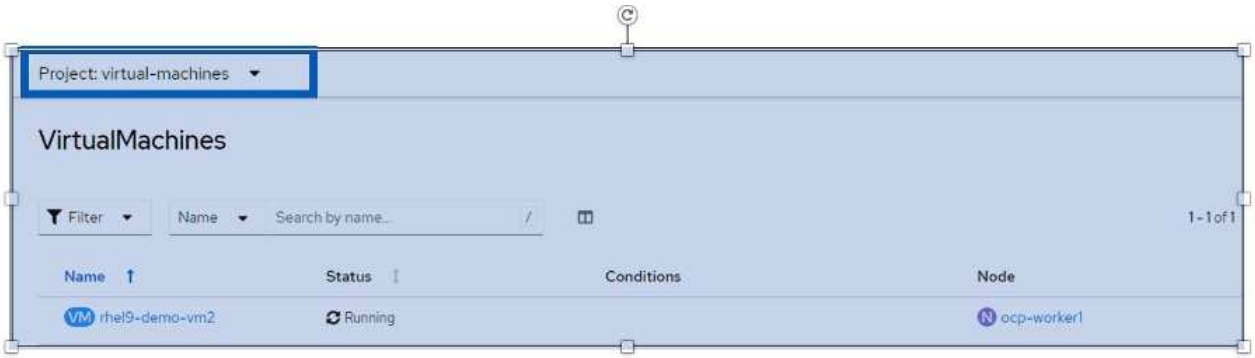
**Wiederherstellen in einem anderen Namespace**

Um die App in einem anderen Namespace wiederherzustellen, können Sie in der YAML-Definition des Restore CR ein NamespaceMapping angeben.

Die folgende YAML-Beispieldatei erstellt eine Wiederherstellungs-CR, um eine App und ihren persistenten Speicher aus dem PostgreSQL-Namespace in den neuen Namespace „postgresql-restored“ wiederherzustellen.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

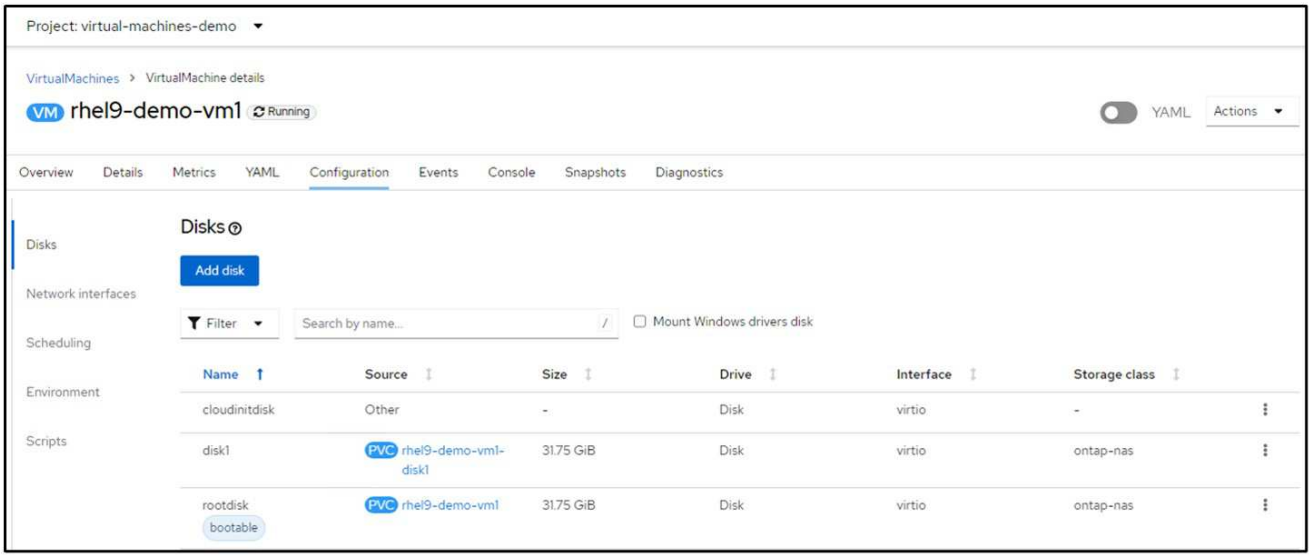
Wenn die Phase als abgeschlossen angezeigt wird, können Sie sehen, dass die App in den Zustand zurückversetzt wurde, in dem sie sich zum Zeitpunkt der Erstellung des Snapshots befand. Die App wird in einem anderen Namespace wiederhergestellt, wie im YAML angegeben.

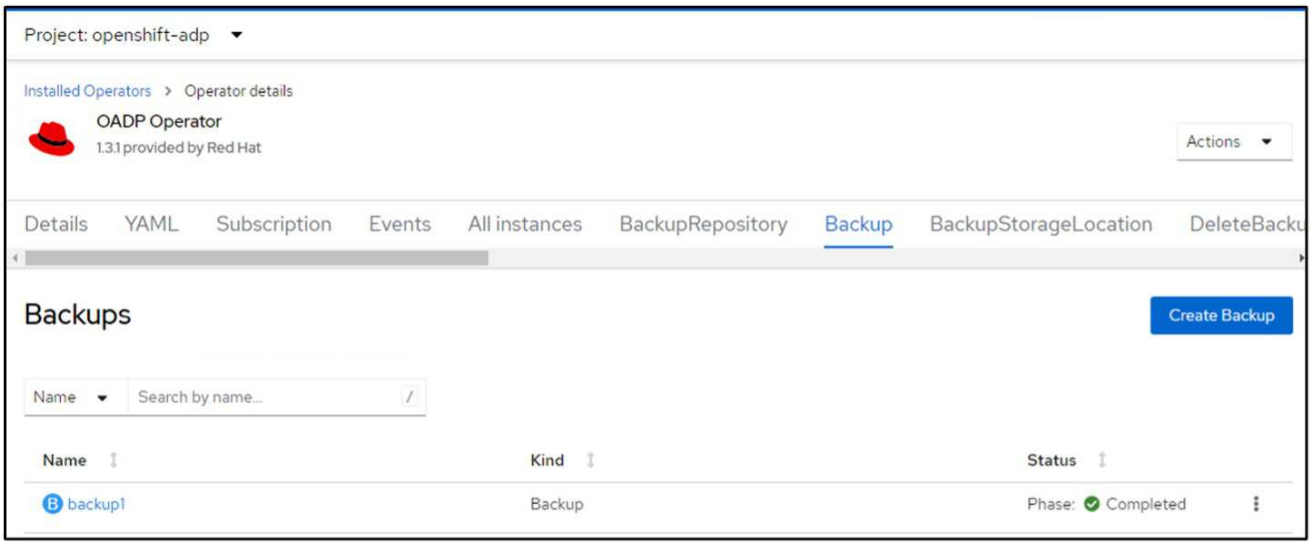


### Wiederherstellen in einer anderen Speicherklasse

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 App während der Bereitstellung ontap-nas als Speicherklasse für ihre persistenten Volumes. Es wird ein Backup der App mit dem Namen backup-postgresql-ontaps3 erstellt.




Simulieren Sie einen Verlust der App, indem Sie die App deinstallieren.

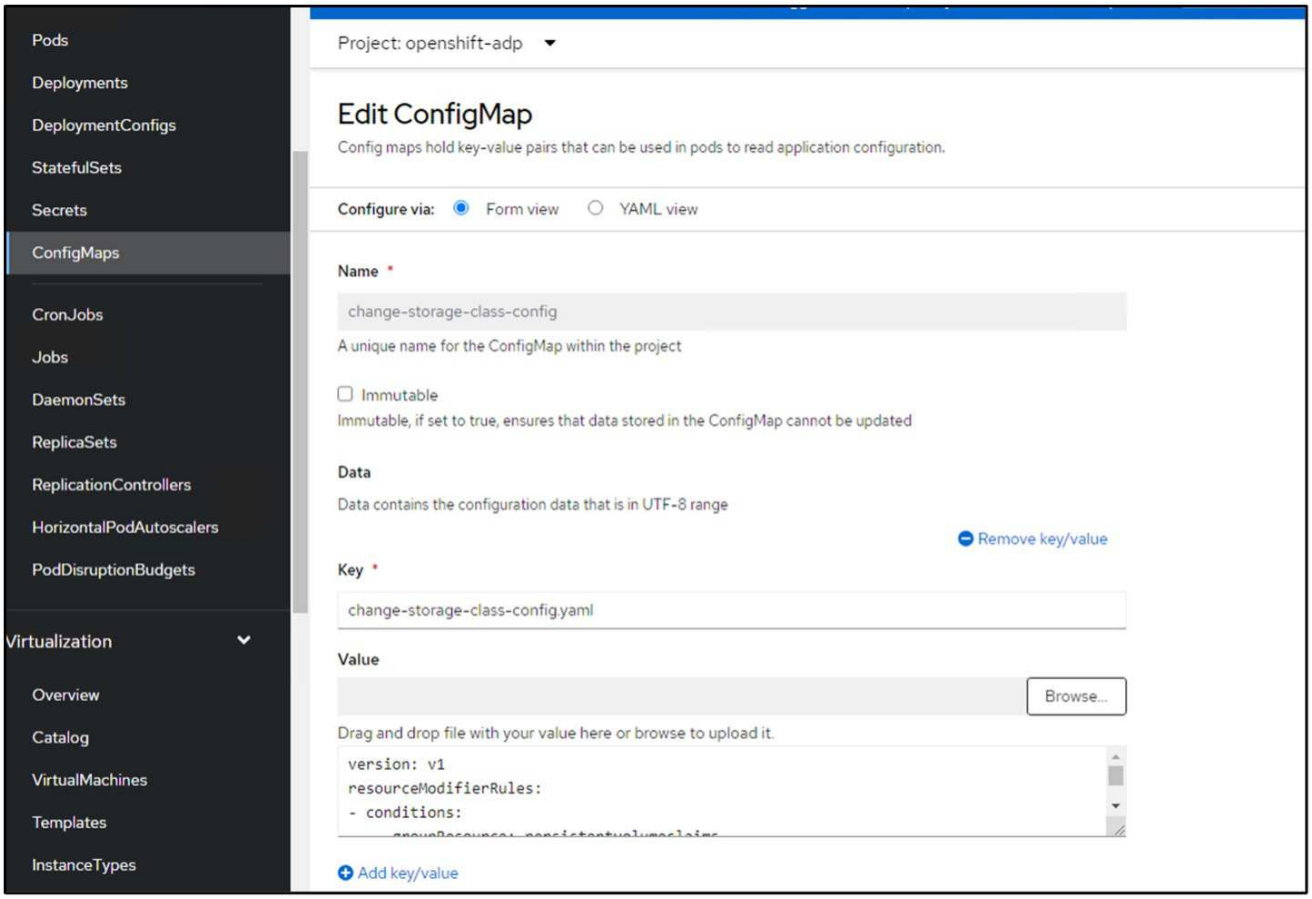
Um die VM mit einer anderen Speicherklasse wiederherzustellen, beispielsweise der Speicherklasse ontap-nas-eco, müssen Sie die folgenden zwei Schritte ausführen:

**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-Ontap-SC (kann ein beliebiger Name sein) Schlüssel: Change-Ontap-SC-Config.yaml: Wert:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  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>
```

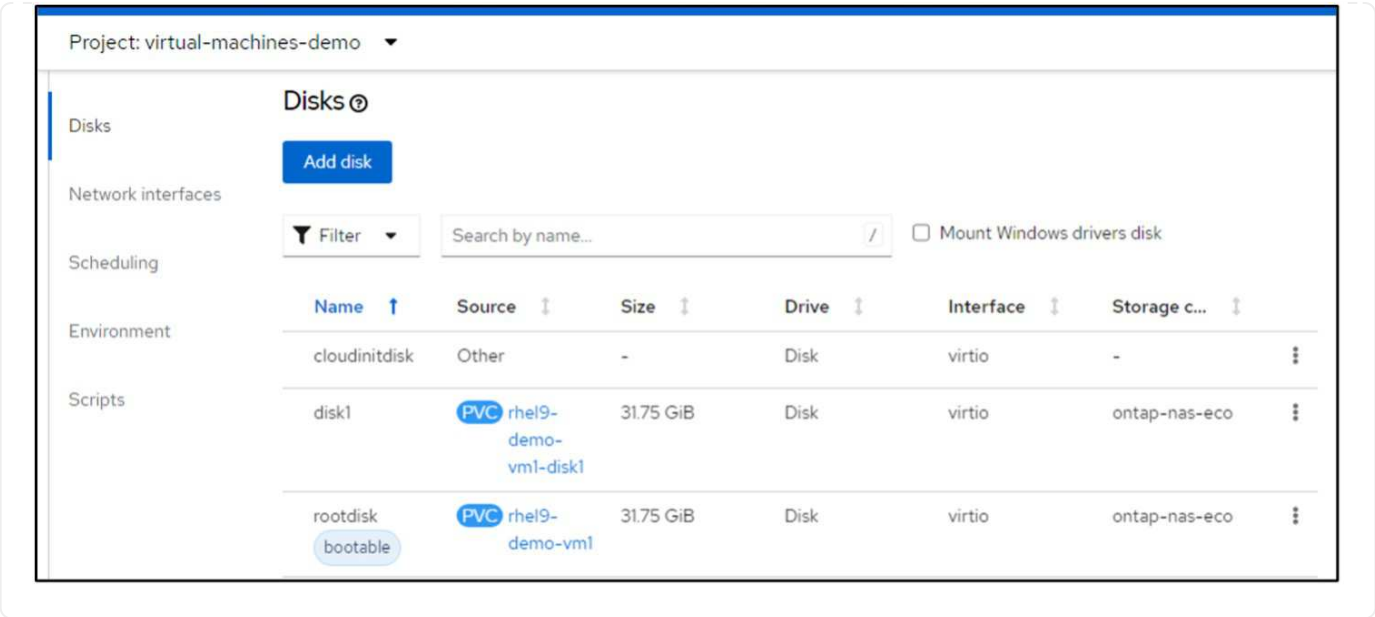
Diese Konfigurationszuordnung wendet die Ressourcenmodifikatorregel an, wenn die Wiederherstellung erstellt wird. Es wird ein Patch angewendet, um den Speicherklassennamen für alle persistenten Volume-Ansprüche, die mit rhel beginnen, durch ontap-nas-eco zu ersetzen.

**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 App wird im selben Namespace wiederhergestellt, in dem die persistenten Volume-Ansprüche mit der Speicherklasse ontap-nas-eco erstellt wurden.




# Löschen von Backups und Wiederherstellungen mit Velero

In diesem Abschnitt wird beschrieben, wie Sie mithilfe von Velero Backups und Wiederherstellungen von Apps auf der OpenShift-Containerplattform löschen.

## Alle Backups auflisten

Sie können alle Backup-CRs auflisten, indem Sie das OC CLI-Tool oder das Velero CLI-Tool verwenden. Laden Sie die Velero CLI gemäß den Anweisungen im"Velero-Dokumentation" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

## Löschen einer Sicherung

Sie können ein Backup-CR löschen, ohne die Object Storage-Daten zu löschen, indem Sie das OC CLI-Tool verwenden. Die Sicherung wird aus der CLI-/Konsolenausgabe entfernt. Da das entsprechende Backup jedoch nicht aus dem Objektspeicher entfernt wird, wird es erneut in der CLI-/Konsolenausgabe angezeigt.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

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

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                      STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3 Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
backup2                   Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
schedule1-20240717070005  Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                      STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3 Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
schedule1-20240717070005  Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1  <none>
[root@localhost ~]#
```

## Löschen der Wiederherstellung

Sie können das Restore CR-Objekt entweder mit der OC CLI oder der Velero CLI löschen.

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME      BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore   backup-postgresql-ontaps3 Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1  backup-postgresql-ontaps3 Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME      BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore   backup-postgresql-ontaps3 Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

**Copyright-Informationen**

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.