



Datensicherung von Container- Applikationen mit Tools von Drittanbietern

NetApp Solutions

NetApp
December 19, 2024

Inhalt

- Datensicherung von Container-Applikationen mit Tools von Drittanbietern 1
 - Datensicherung für Container-Applikationen in der OpenShift-Container-Plattform mit OpenShift-API für Data Protection (OADP) 1
 - Installation von OpenShift API for Data Protection (OADP) Operator 3
 - Erstellen von On-Demand-Backups für Applikationen in der OpenShift Container Plattform 12
 - Migrieren einer App von einem Cluster zu einem anderen 15
 - Wiederherstellen einer App aus einem Backup 20
 - Löschen von Backups und Restores in mit Velero 27

Datensicherung von Container-Applikationen mit Tools von Drittanbietern

Datensicherung für Container-Applikationen in der OpenShift-Container-Plattform mit OpenShift-API für Data Protection (OADP)

Autor: Banu Sundhar, NetApp

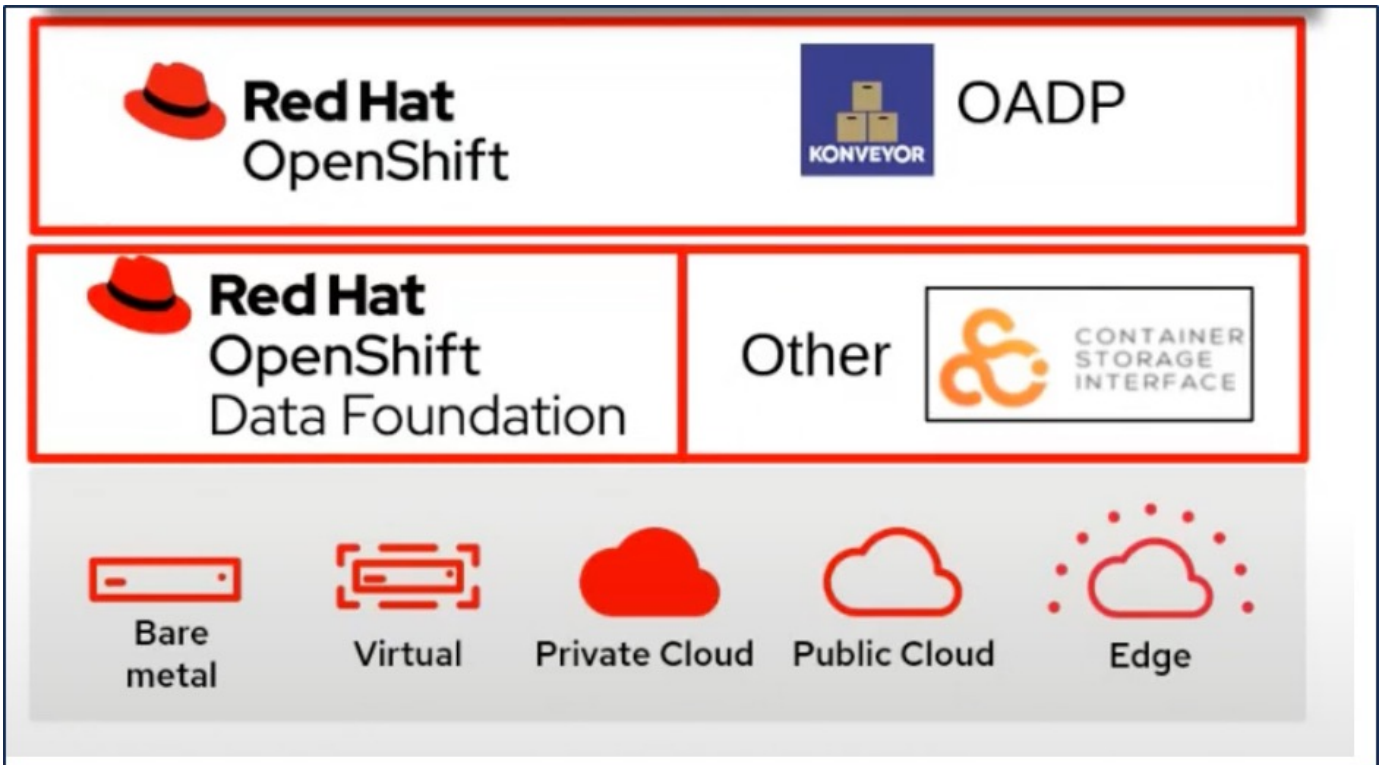
Dieser Abschnitt des Referenzdokuments enthält Details zum Erstellen von Backups von Container-Apps mithilfe der OpenShift-API für die Datensicherung (OADP) mit Velero auf NetApp ONTAP S3 oder NetApp StorageGRID S3. Die Backups von im Namespace enthaltenen Ressourcen einschließlich persistenter Volumes (PVs) der App werden mithilfe von CSI-Trident-Snapshots erstellt.

Der persistente Speicher für Container-Apps kann über ONTAP-Speicher gesichert werden, der in den OpenShift-Cluster integriert ["Trident-CSI"](#) ist. In diesem Abschnitt führen wir ["OpenShift API for Data Protection \(OADP\)"](#) Backups von Applikationen durch, einschließlich der Daten-Volumes auf

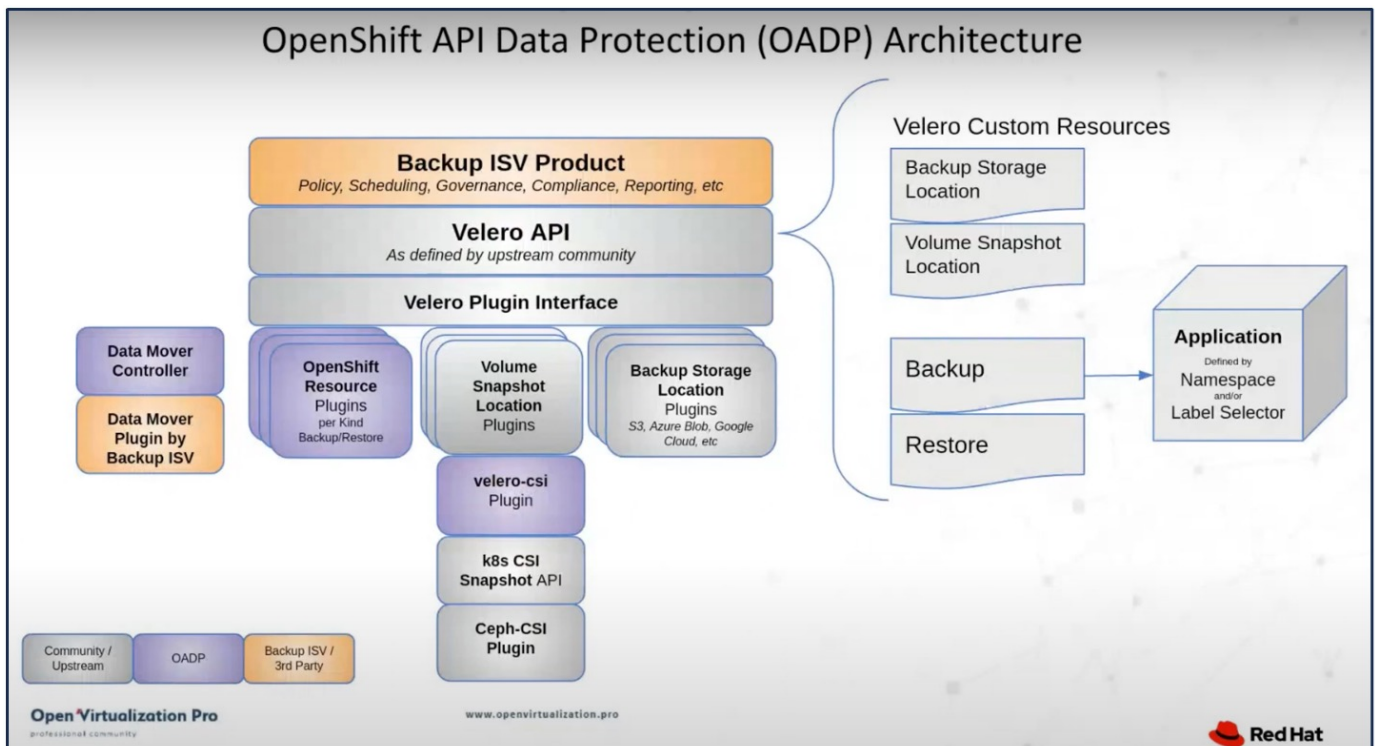
- ONTAP Objekt-Storage
- StorageGRID

Wir führen dann bei Bedarf ein Restore aus dem Backup durch. Bitte beachten Sie, dass die App nur auf dem Cluster wiederhergestellt werden kann, von dem aus das Backup erstellt wurde.

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-Bediensers 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
- OADP Operator 1.13 von Red hat bereitgestellt
- Velero CLI 1.13 für Linux
- Trident 24.02
- ONTAP 9.12
- postgresql mit Helm installiert.

["Trident-CSI" "OpenShift API for Data Protection \(OADP\)" "Velero"](#)

Installation von OpenShift API for Data Protection (OADP) Operator

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

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, der mithilfe von Trident in den Cluster integriert ist
- Ein Trident Back-End, das mit einer SVM auf ONTAP Cluster konfiguriert ist
- Eine auf dem OpenShift-Cluster konfigurierte StorageClass mit Trident als bereitstellung
- Die Trident Snapshot Klasse wurde auf dem Cluster erstellt
- Cluster-Admin-Zugriff auf Red hat OpenShift-Cluster
- Administratorzugriff auf das NetApp ONTAP-Cluster
- Eine auf dem Cluster implementierte Applikation, z. B. postgresql
- Eine Admin-Workstation mit den Tools tridentctl und oc installiert und zur €Pfad hinzugefügt

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.

Home >

Operators >

OperatorHub

Installed Operators

Workloads >

Virtualization >

Networking >

Storage >

Builds >

Observe >

OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Marketplace optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-service experience.

All Items

AI/Machine Learning

Application Runtime

Big Data

Cloud Provider

Database

Developer Tools

Development Tools

Drivers and plugins

Integration & Delivery

Logging & Tracing


Modernization & Migration

Monitoring

All Items

Q OADP x


Red Hat



OADP Operator
provided by Red Hat


OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...

Community



OADP Operator
provided by Red Hat

OADP (OpenShift API for Data Protection) operator sets up and installs Velero on the OpenShift...



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](#)







Activate Windows

Project: All Projects ▾

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#) Operator and ClusterServiceVersion using the [Operator SDK](#).

Name ▾ Search by name... /

Name	Namespace	Managed Namespaces	Status
 OpenShift Virtualization 4.14.4 provided by Red Hat	NS openshift-cnv	NS openshift-cnv	 Succeeded Up to date
 OADP Operator 1.3.0 provided by Red Hat	NS openshift-adp	NS openshift-adp	 Succeeded Up to date
 Package Server 0.0.1-snapshot provided by	NS openshift-operator-lifecycle-manager	NS openshift-operator-lifecycle-manager	 Succeeded

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.

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

Project: openshift-adp

Edit key/value secret

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

Secret name *
ontap-s3-credentials
Unique name of the new secret.

Key *
cloud

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

```
[default]
aws_access_key_id=
aws_secret_access_key=
```

+ Add key/value

Save Cancel





Um einen Schlüssel mit dem Namen sg-s3-credentials aus der 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 im Menüpunkt unter Operatoren die Option Installed Operators aus, klicken Sie auf OADP Operator und wählen Sie dann die Registerkarte **DataProtectionApplication**.

Name	Managed Namespaces	Status	Last updated	Provided APIs
 OADP Operator 1.3.0 provided by Red Hat	 openshift-adp	 Succeeded Up to date	 Apr 11, 2024, 10:53 AM	BackupRepository Backup BackupStorageLocation DeleteBackupRequest View 11 more...

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

Project: openshift-adp

Installed Operators > Operator details

 OADP Operator
1.3.0 provided by Red Hat

Actions

ServerStatusRequest VolumeSnapshotLocation DataDownload DataUpload CloudStorage **DataProtectionApplication**

DataProtectionApplications [Create DataProtectionApplication](#)

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: '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 zur Konfiguration 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, 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.

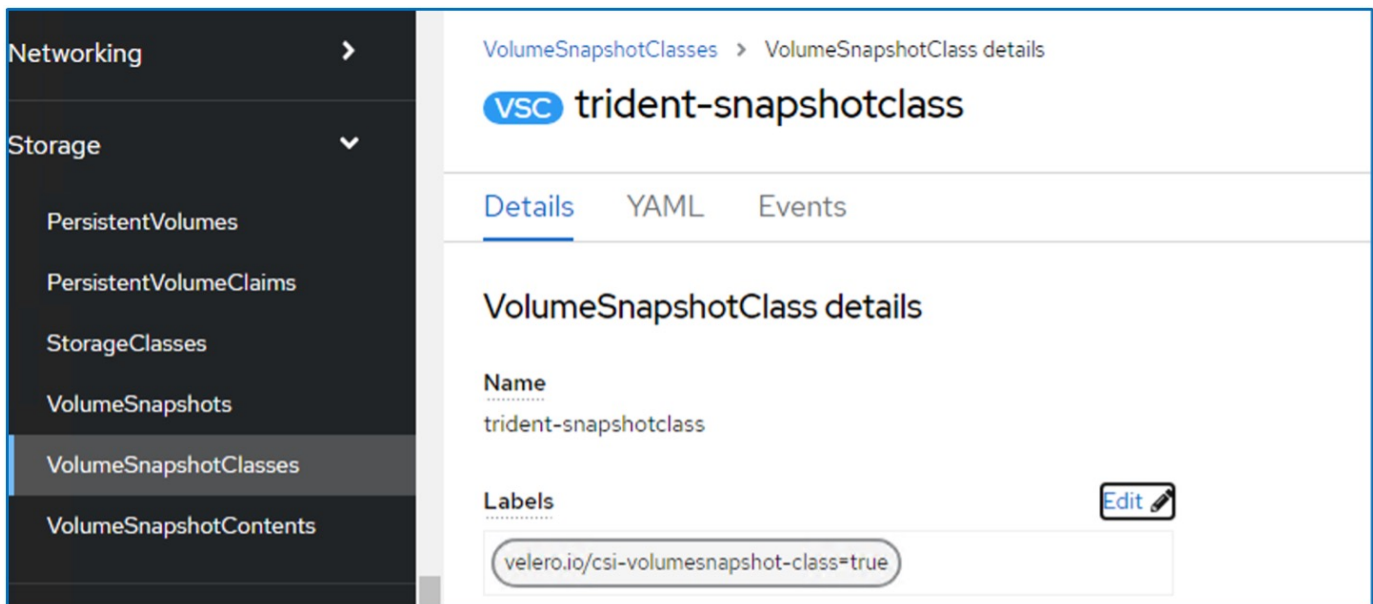
SnapshotLocations Wenn Sie CSI-Snapshots (Container Storage Interface) verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie einen VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Trident CSI und Sie haben bereits VolumeSnapShotClass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

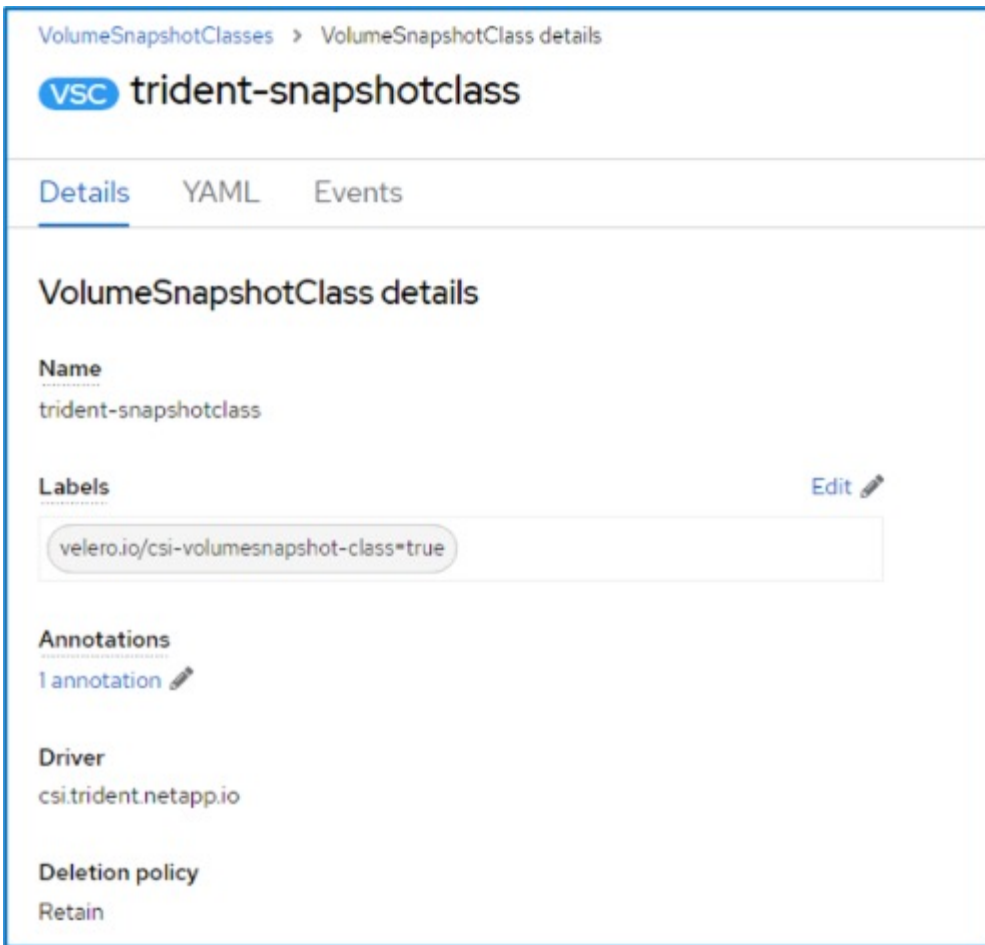
`velero.io/csi-Volumesnapshot-class=true` wie unten gezeigt.



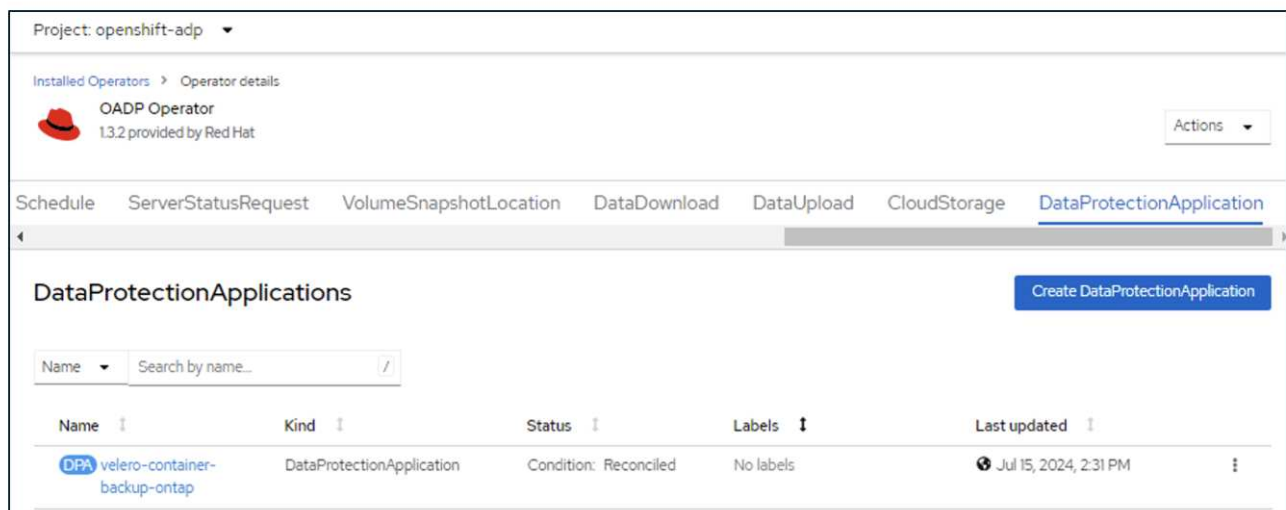
The screenshot displays the Kubernetes dashboard interface for a VolumeSnapshotClass. On the left, a dark sidebar contains a navigation menu with 'Storage' expanded and 'VolumeSnapshotClasses' selected. The main panel shows the 'trident-snapshotclass' details, including its name and a label 'velero.io/csi-volumesnapshot-class=true'.

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.

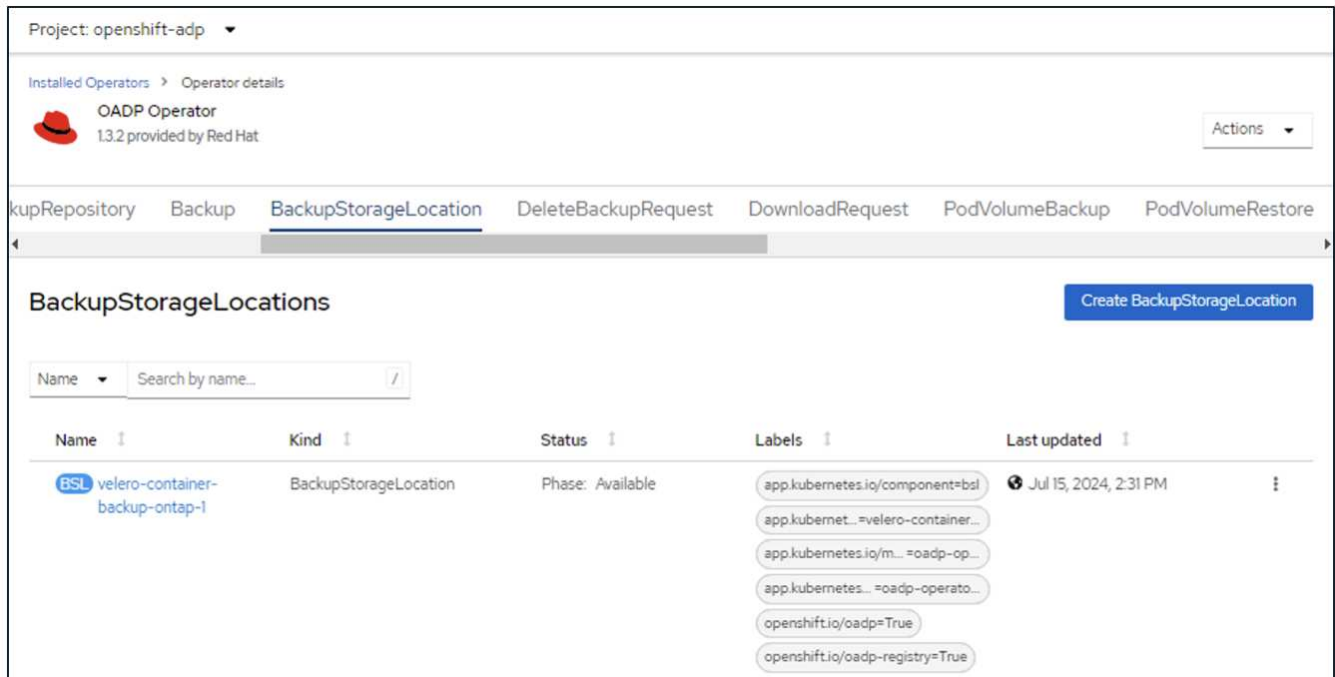
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



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 Applikationen in der OpenShift Container Platform

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

Schritte zum Erstellen einer Sicherung 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 Backup Custom Resource (CR) zu erstellen. Ein Beispiel für yml wird zur Erstellung des Backup CR bereitgestellt. Mit diesem yml wird die App und ihr persistenter Speicher im angegebenen Namespace gesichert. Weitere Parameter können wie in dargestellt eingestellt werden "[Dokumentation](#)".

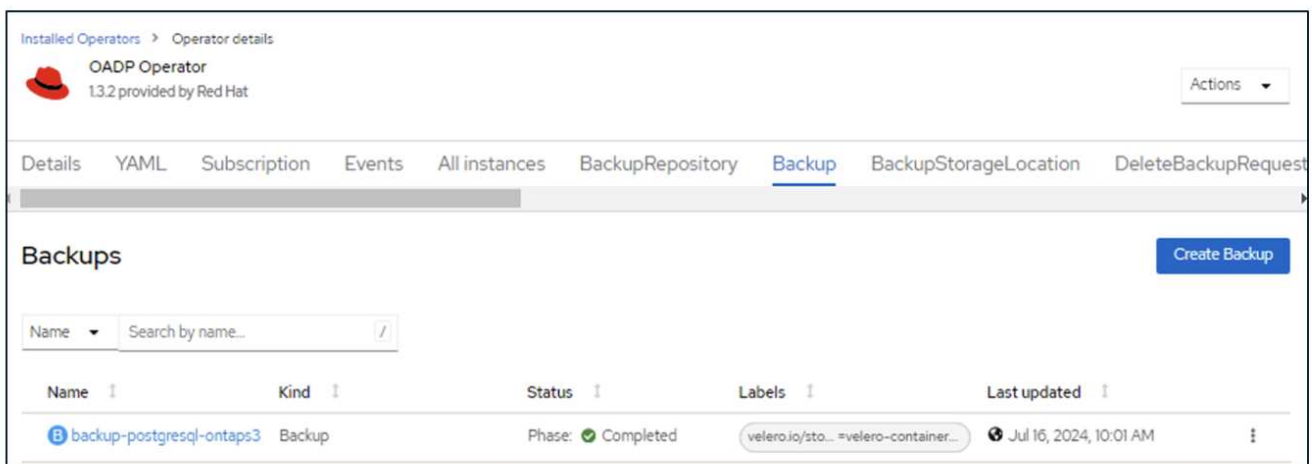
Ein Snapshot der persistenten Volumes und der App-Ressourcen im angegebenen Namespace wird vom CSI erstellt. Dieser Snapshot wird im Backup-Speicherort gespeichert, der in yml angegeben ist. Das Backup bleibt gemäß ttl 30 Tage im System.

```

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 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/Container-Demo-Backup) angezeigt. Sie können den Inhalt des Backups sehen, der die Volume-Snapshots, Protokolle und andere Metadaten der Anwendung umfasst.



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

Path: / container-demo-backup/ backups/ backup-postgresql-ontaps3/

Name	Size	Type	Last Modified	Storage Class
backup-postgresql-ontaps3.tar.gz	384.66 KB	GZ File	7/16/2024 10:01:20 AM	STANDARD
velero-backup.json	3.30 KB	JSON File	7/16/2024 10:01:20 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap...	731 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap...	760 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-resource-list.jso...	823 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-itemoperations.j...	378 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-volumesnapshot...	29 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-podvolumeback...	29 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-results.gz	49 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-csi-volumesnap...	429 bytes	GZ File	7/16/2024 10:01:19 AM	STANDARD
backup-postgresql-ontaps3-logs.gz	12.01 KB	GZ File	7/16/2024 10:01:19 AM	STANDARD

Upload Download Delete New Folder Refresh

Erstellen geplanter Backups für Apps

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. Im Folgenden wird ein Beispiel für yaml zum Erstellen eines Schedule CR angezeigt.

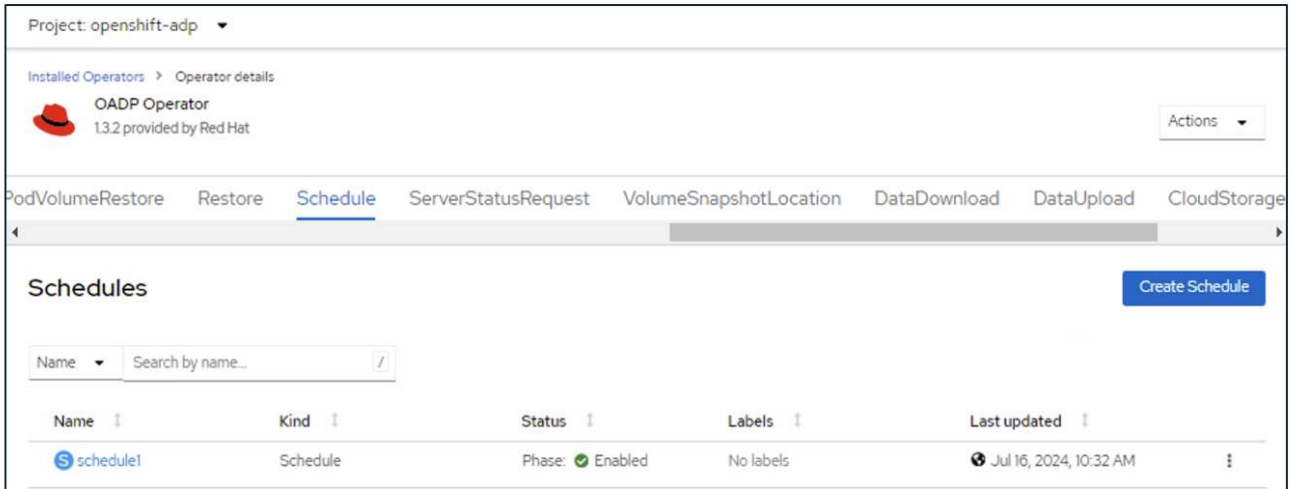
```

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

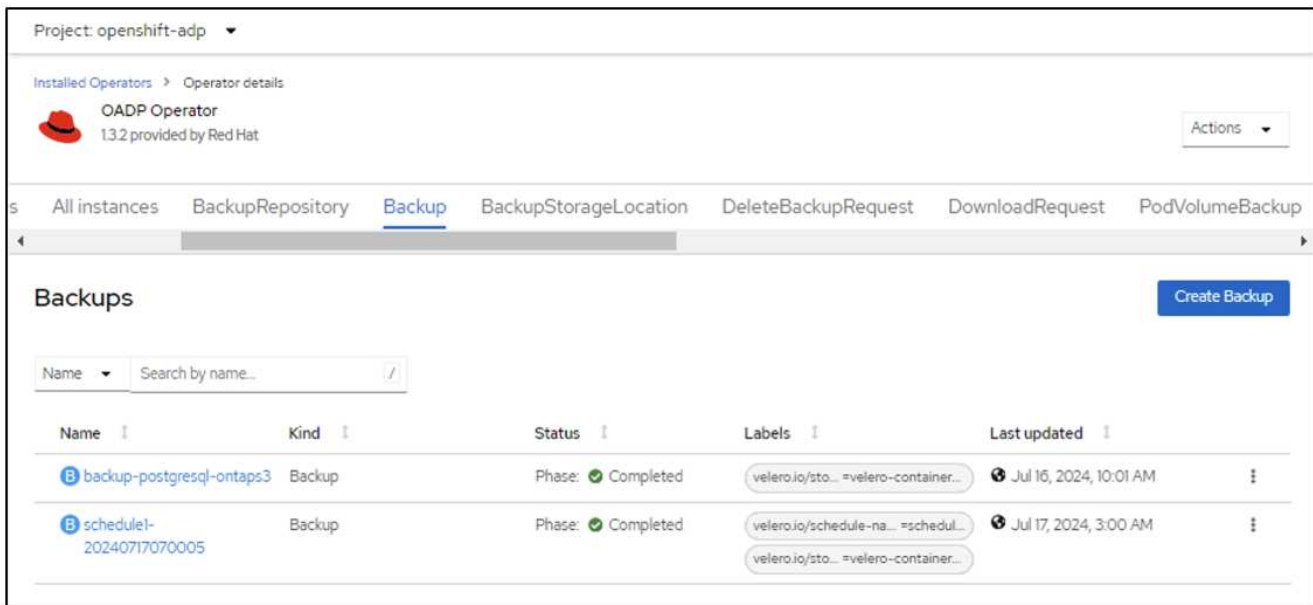
```

Der Cron-Ausdruck `0 7 * * *` bedeutet, dass 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.



Migrieren einer App von einem Cluster zu einem anderen

Die Backup- und Restore-Funktionen von Velero machen es zu einem wertvollen Tool für die Migration von Daten zwischen Clustern. In diesem Abschnitt wird beschrieben, wie Sie Apps von einem Cluster zu einem anderen migrieren, indem Sie ein Backup der App im Objektspeicher von einem Cluster erstellen und dann die App aus demselben Objektspeicher in einen anderen Cluster wiederherstellen. .

Backup vom ersten Cluster

Voraussetzungen für Cluster 1

- Trident muss auf dem Cluster installiert sein.
- Es müssen ein dreigestelltes Backend und eine Storage-Klasse 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.

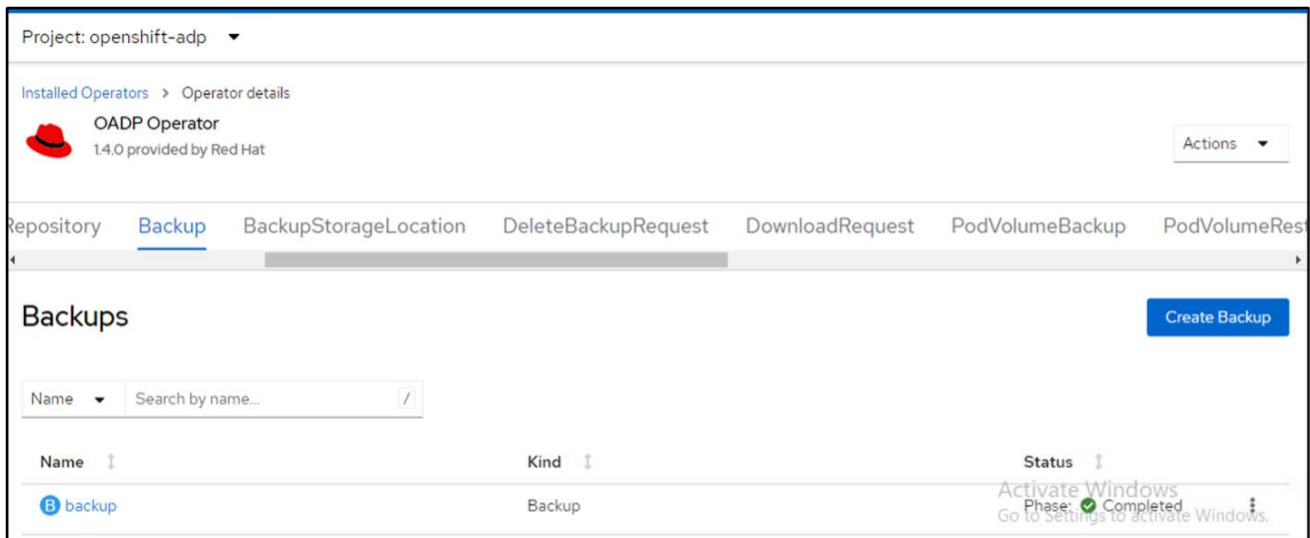
```
spec:
  backupLocations:
    - velero:
      config:
        insecureSkipTLSVerify: 'false'
        profile: default
        region: us-east-1
        s3ForcePathStyle: 'true'
        s3Url: 'https://10.61.181.161'
      credential:
        key: cloud
        name: ontap-s3-credentials
      default: 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 ein Backup 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 folgenden Spezifikationen für die Backup-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 zu sehen, die erstellt werden und durch verschiedene Phasen zu bewegen, um schließlich zur Backup **abgeschlossen** Phase zu kommen.

Eine Sicherung der Ressourcen im Namespace postgresql wird im Objektspeicherort (ONTAP S3) gespeichert, der im Backup-Speicherort in der OADP-Spezifikation angegeben ist.

Wiederherstellung 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 das Backup vom ersten Cluster aus gespeichert wurde.
- Die 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        OnTerminated 11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d 10Gi       RWO            Delete           Bound   default/test-pvc     vsphere-sc    2d7h
[root@localhost ~]#
```

The screenshot shows the OpenShift console interface. At the top, the project is set to 'openshift-adp'. Under 'Installed Operators', the 'OADP Operator' (version 1.4.0) is listed. Below this, a navigation bar contains several tabs: 'Backup', 'BackupStorageLocation' (which is selected), 'DeleteBackupRequest', 'DownloadRequest', 'PodVolumeBackup', 'PodVolumeRestore', and 'Res'. The main content area is titled 'BackupStorageLocations' and includes a search bar and a table. The table has columns for 'Name', 'Kind', and 'Status'. One entry is visible: 'BSL velero-container-demo-1' with Kind 'BackupStorageLocation' and Status 'Phase: Available'. A 'Create BackupStorageLocation' button is located in the top right of the table area.

Installed Operators > Operator details

 **OADP Operator**
1.4.0 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | BackupRepository | **Backup** | BackupStorageLocation | DeleteBackupRequest | DownloadRequest

Backups

Create Backup

Name Search by name...

Name	Kind	Status	Labels	Last updated
backup	Backup	Phase: ✔ Completed	velero.io/storage-locati...=velero-sampl...	Jul 25, 2024, 8:39 PM

Stellen Sie die App auf diesem Cluster aus dem Backup wieder her. Verwenden Sie die folgende yaml-Datei, um die CR-Wiederherstellung 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 der pvc und einem entsprechenden pv verknüpft ist. Der Status der App ist der gleiche wie beim Backup.

Project: openshift-adp

Installed Operators > Operator details

 **OADP Operator**
1.4.0 provided by Red Hat

Actions

eLocation | DeleteBackupRequest | DownloadRequest | PodVolumeBackup | PodVolumeRestore | **Restore** | Schedule | Server

Restores

Create Restore

Name Search by name...

Name	Kind	Status
restore	Restore	Phase: ✔ Completed

Activate Windows
Go to Settings to activate Windows.

```
[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-sphere-sc      ontap-nas
2d10h
[root@localhost ~]#
```

Wiederherstellen einer App aus einem Backup

In diesem Abschnitt wird beschrieben, wie Apps aus einem Backup wiederhergestellt werden.

Voraussetzungen

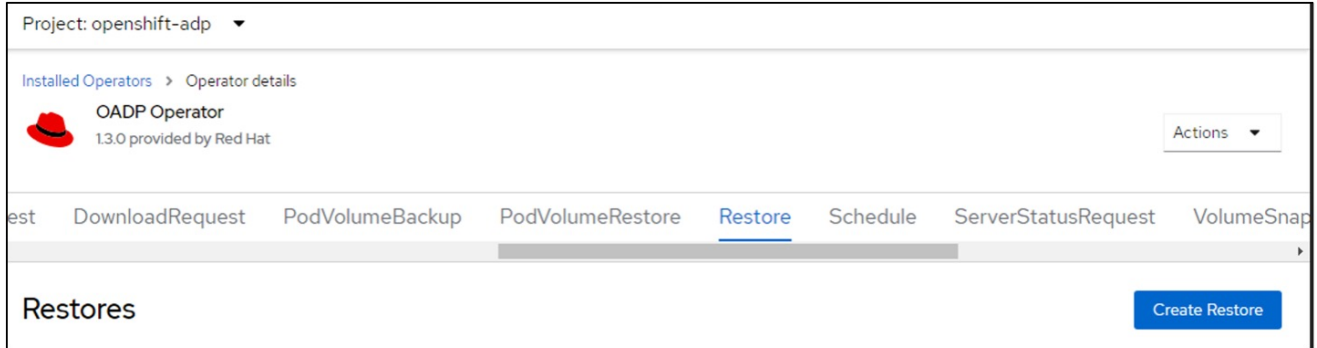
Um aus einem Backup wiederherzustellen, nehmen wir an, dass der Namespace, in dem die App existierte, versehentlich gelöscht wurde.

```
[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 ~]#
```

Restore auf denselben Namespace

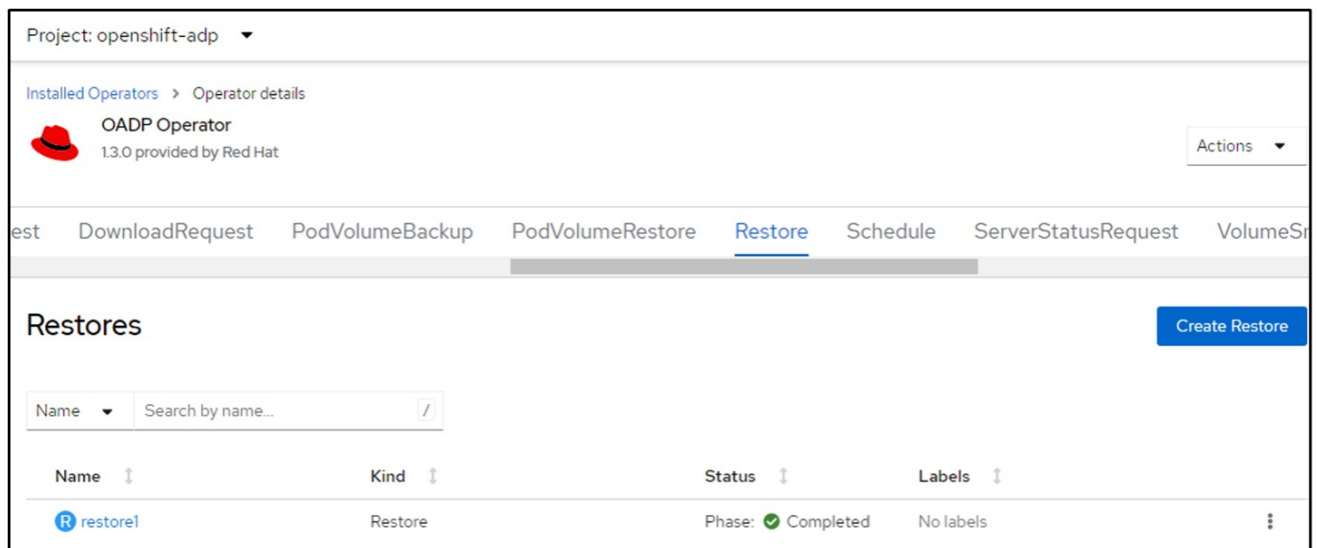
Um das Backup wiederherzustellen, das wir gerade erstellt haben, müssen wir eine Restore Custom Resource (CR) erstellen. Geben Sie ihm einen Namen, geben Sie den Namen des Backups an, von dem aus wir die Wiederherstellungs-PVs wiederherstellen möchten, und setzen Sie sie auf „True“. Weitere Parameter können wie in dargestellt eingestellt werden ["Dokumentation"](#). Klicken Sie auf die Schaltfläche Erstellen.



The screenshot shows the OADP Operator interface for the 'openshift-adp' project. The 'Restore' tab is selected, and a 'Create Restore' button is visible in the top right corner.

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

Wenn in der Phase Abgeschlossen angezeigt wird, wird angezeigt, dass die App zum Zeitpunkt der Snapshot-Erstellung wieder in den Status zurückgesetzt wurde. Die App wird im selben Namespace wiederhergestellt.



The screenshot shows the OADP Operator interface with the 'Restore' tab selected. A table lists the restore operation, showing it is completed.

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

```
[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 ~]#
```


Wiederherstellung in einem anderen Namespace

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

Mit der folgenden yaml-Beispieldatei wird ein Restore CR erstellt, um eine App und ihren persistenten Speicher aus dem postgresql-Namespace auf den neuen Namespace postgresql-wiederhergestellt 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
```

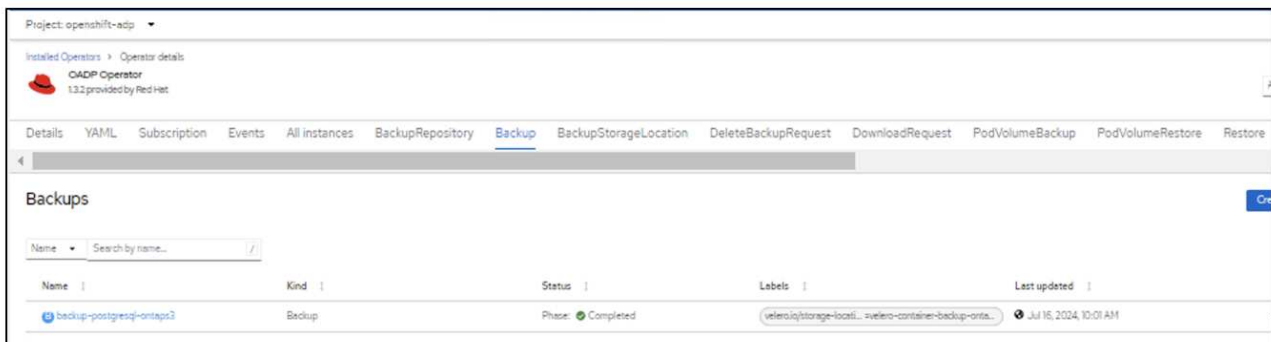
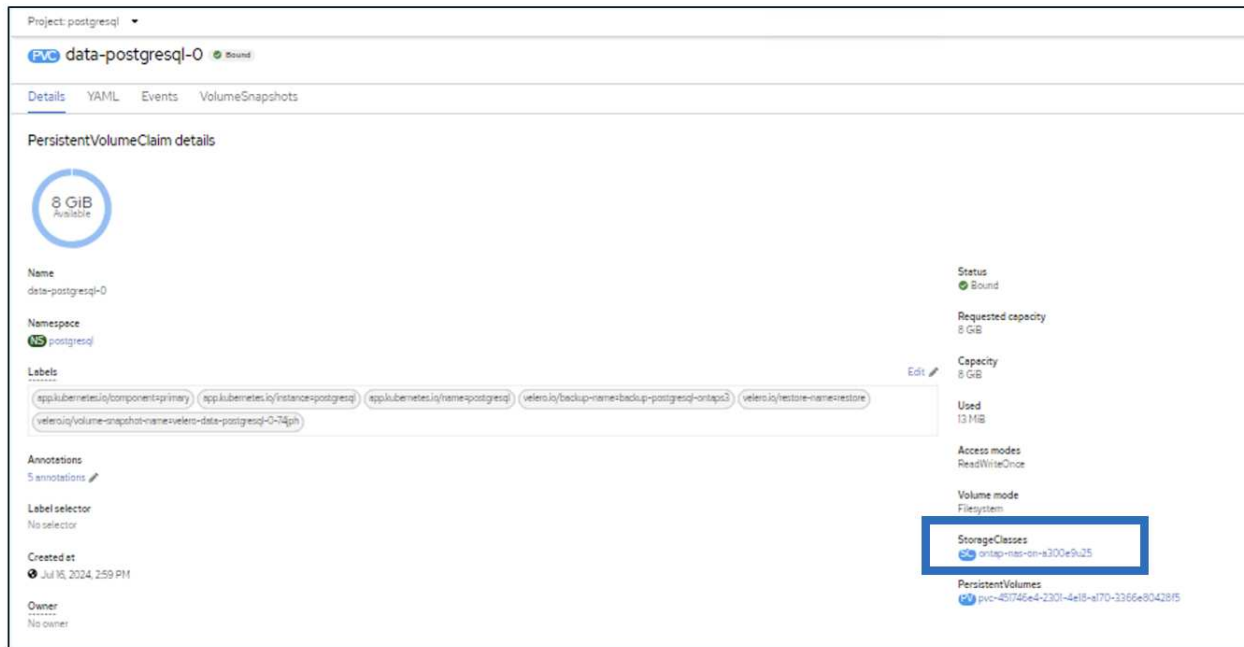
Wenn in der Phase Abgeschlossen angezeigt wird, wird angezeigt, dass die App zum Zeitpunkt der Snapshot-Erstellung wieder in den Status zurückgesetzt wurde. Die App wird in einem anderen Namespace wiederhergestellt, wie im yaml angegeben.

```
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql-restored
NAME          READY   STATUS    RESTARTS   AGE
postgresql-0  0/1     Running   0           19s
[root@localhost ~]# oc get pods -n postgresql-restored
NAME          READY   STATUS    RESTARTS   AGE
postgresql-0  0/1     Running   0           22s
[root@localhost ~]# oc get pods -n postgresql-restored
NAME          READY   STATUS    RESTARTS   AGE
postgresql-0  1/1     Running   0           36s
[root@localhost ~]#
```

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 nachfolgenden Beispiel verwendet die Applikation während der Implementierung ontap-nas als Storage-Klasse für ihre persistenten Volumes. Es wird ein Backup der App Backup-postgresql-ontaps3 erstellt.



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

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 config map (Console) im openshift-adp Namespace wie folgt: Geben Sie die Details wie im Screenshot gezeigt ein: Select Namespace : openshift-adp Name: Change-ontap-sc (kann jeder

beliebige Name sein) Key: Change-ontap-sc-config.yaml: Value:

```
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
  resourceNameRegex: "data-postgresql*"
  namespaces:
  - postgresql
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"
```

Project: openshift-adp ▾

Edit ConfigMap

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

Configure via: Form view YAML view

Name *

A unique name for the ConfigMap within the project

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

Data

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

Key *

Value

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

```
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
  resourceNameRegex: "data-postgresql*"
  namespaces:
  - postgresql
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"
```

Das resultierende config map-Objekt sollte wie folgt aussehen (CLI):

```
[root@localhost ~]# kubectl describe cm/change-ontap-sc -n openshift-adp
Name:          change-ontap-sc
Namespace:     openshift-adp
Labels:        <none>
Annotations:   <none>

Data
====
change-ontap-sc.yaml:
----
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
  resourceNameRegex: "data-postgresql*"
  namespaces:
  - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"

BinaryData
====

Events: <none>
[root@localhost ~]#
```

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 App wird im selben Namespace mit den Angaben zu persistenten Volumes wiederhergestellt, die über die Storage-Klasse ontap-nas-eco erstellt wurden.

```
[root@localhost ~]# oc get pods -n postgresql
NAME          READY   STATUS    RESTARTS   AGE
postgresql-0  1/1    Running   0           11m
[root@localhost ~]# oc get pvc -n postgresql
NAME          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0  Bound   pvc-33526ea4-37c2-4180-a9f6-fb47aea3b4e2  8Gi        RWO             ontap-nas-eco  11m
[root@localhost ~]#
```

Löschen von Backups und Restores in mit Velero

In diesem Abschnitt wird beschrieben, wie Backups und Restores von Apps in der OpenShift Container-Plattform mithilfe von Velero gelöscht werden.

Listen Sie alle Backups auf

Sie können alle Backup CRS mit dem OC CLI-Tool oder dem Velero CLI-Tool auflisten. Laden Sie die Velero CLI wie in den Anweisungen im beschrieben herunter "[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 eines Backups

Sie können einen Backup CR löschen, ohne die Objektspeicherdaten mit dem OC CLI-Tool zu löschen. Das Backup wird aus der CLI/Console-Ausgabe entfernt. Da das entsprechende Backup jedoch nicht aus dem Objektspeicher entfernt wird, wird es erneut in der CLI/Console-Ausgabe 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 den 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 über die OC-CLI oder die 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 © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.