



Data Protection für OpenShift Virtualization

NetApp Solutions

NetApp
April 17, 2024

Inhalt

- Data Protection für OpenShift Virtualization 1
 - Datensicherung für VMs in OpenShift-Virtualisierung mit OpenShift-API für Data Protection (OADP) 1
 - Installation von OpenShift API for Data Protection (OADP) Operator 2
 - Erstellen von On-Demand-Backups für VMs in OpenShift-Virtualisierung 11
 - Stellen Sie eine VM aus einem Backup wieder her 14
 - Löschen von Backups und Restores in mit Velero 15

Data Protection für OpenShift Virtualization

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

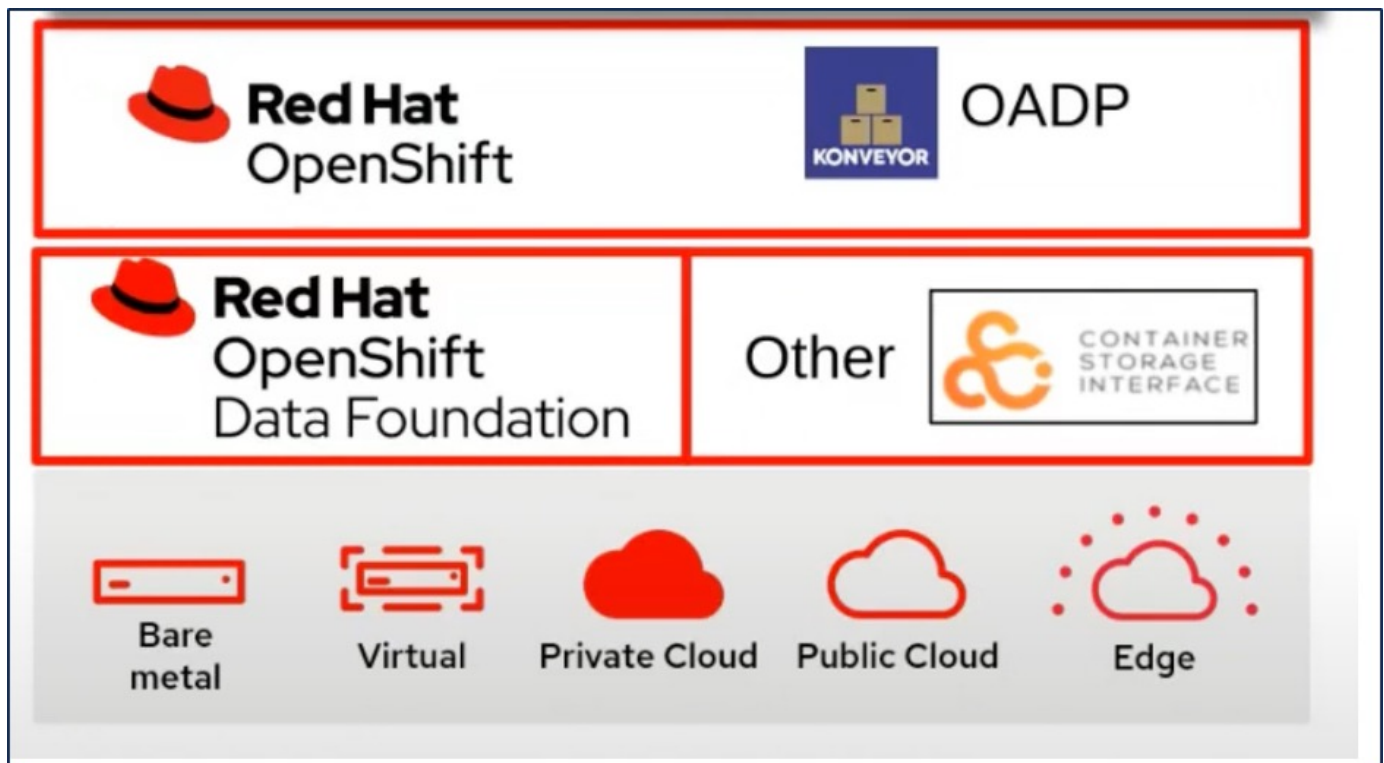
Banu Sundhar, NetApp

Dieses Referenzdokument enthält Details zum Erstellen von Backups von VMs mithilfe der OpenShift API for Data Protection (OADP) mit Velero und zum Verschieben in ONTAP S3. Die Backups der VES der VMs werden mit CSI Astra Trident Snapshots erstellt.

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

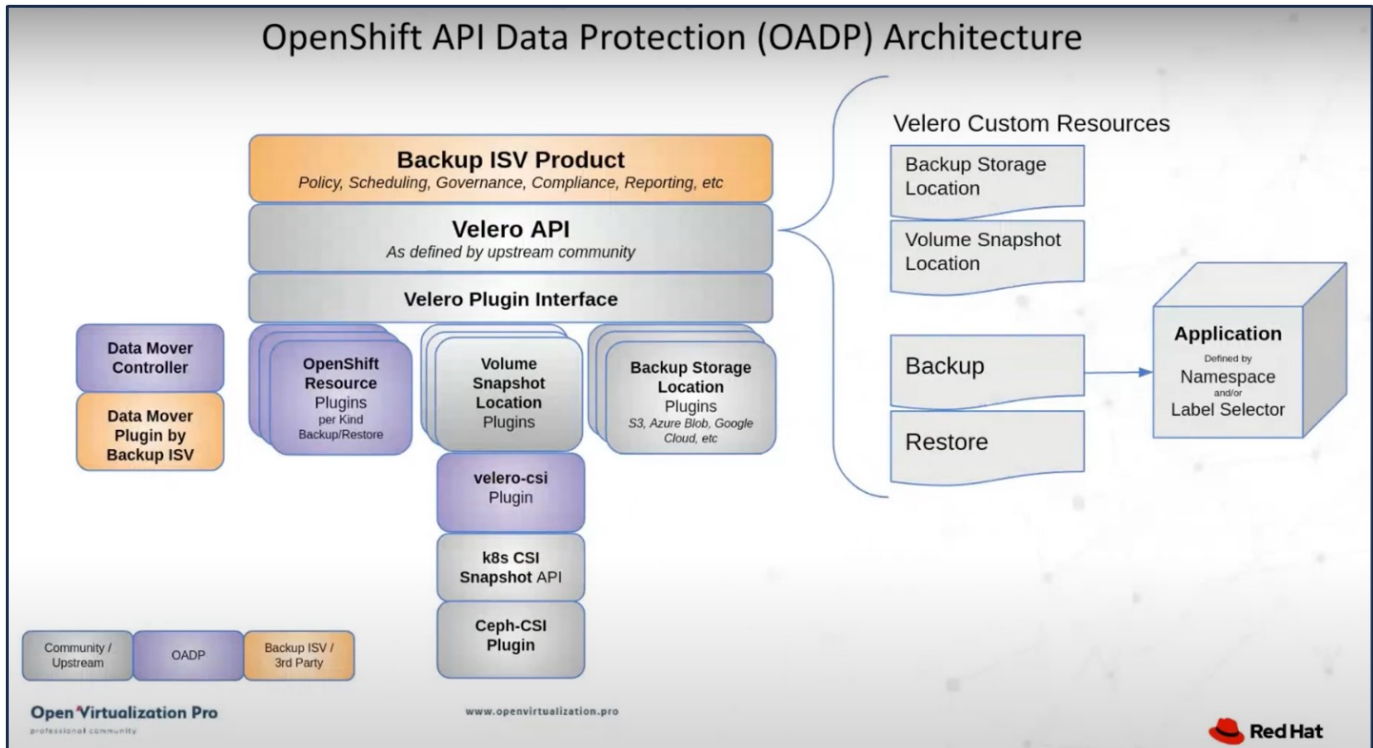
Die persistenten Festplatten der OpenShift-Virtualisierungs-VMs können mithilfe von ONTAP-Speicher gesichert werden, der in den OpenShift-Cluster integriert ist "[Astra Trident CSI](#)". In diesem Abschnitt verwenden wir "[OpenShift API for Data Protection \(OADP\)](#)" Für das Backup von VMs einschließlich seiner Daten-Volumes im ONTAP-Objektspeicher. Wir führen dann bei Bedarf ein Restore aus dem Backup durch.

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



Red hat OpenShift nutzt die von den OpenSource Communities entwickelten Lösungen für den Datenschutz. "[Velero](#)" Ist ein Open-Source-Tool für sicheres Backup und Restore, Disaster Recovery und die Migration von Kubernetes-Cluster-Ressourcen und persistenten Volumes. Um Velero einfach nutzen zu können, hat

OpenShift den OADP-Operator und das Velero-Plugin für die Integration in die CSI-Speichertreiber entwickelt. Die Kernelemente der OADP-APIs, die offengelegt werden, basieren auf den Velero-APIs. Nach der Installation und Konfiguration des OADP-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 Komponentenversionen für die Beispiele in diesem Abschnitt aufgeführt

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

Installation von OpenShift API for Data Protection (OADP) Operator

Voraussetzungen

- Ein Red hat OpenShift-Cluster (später als Version 4.12), der auf einer Bare-Metal-Infrastruktur mit RHCOS Worker-Knoten installiert ist

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



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

Schritte zum Installieren des OADP-Bediensers

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 namens openshift-adp installiert.

The screenshot shows the OperatorHub interface. On the left, there is a dark sidebar with navigation options: Home, Operators (expanded), OperatorHub (selected), Installed Operators, Workloads, Virtualization, Networking, Storage, Builds, and Observe. The main content area is titled 'OperatorHub' and contains a search bar with 'OADP' entered. Below the search bar, there are two operator cards. The first card is for 'OADP Operator provided by Red Hat' and the second is for 'OADP Operator provided by Red Hat' (Community). Both cards describe the operator's function: 'OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...'.



OADP Operator

1.3.0 provided by Red Hat

Install

Channel

stable-1.3

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

Version

1.3.0

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

Capability level

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

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.

- [Installing OADP for application backup and restore](#)
- [Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM](#)
- [Frequently Asked Questions](#)

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

Activate Windows

Project: All Projects

Installed Operators

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

Name Search by name... /

| Name | Namespace | Managed Namespaces | Status |
|---|---|---|---------------------------|
| OpenShift Virtualization 4.14.4 provided by Red Hat | 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.

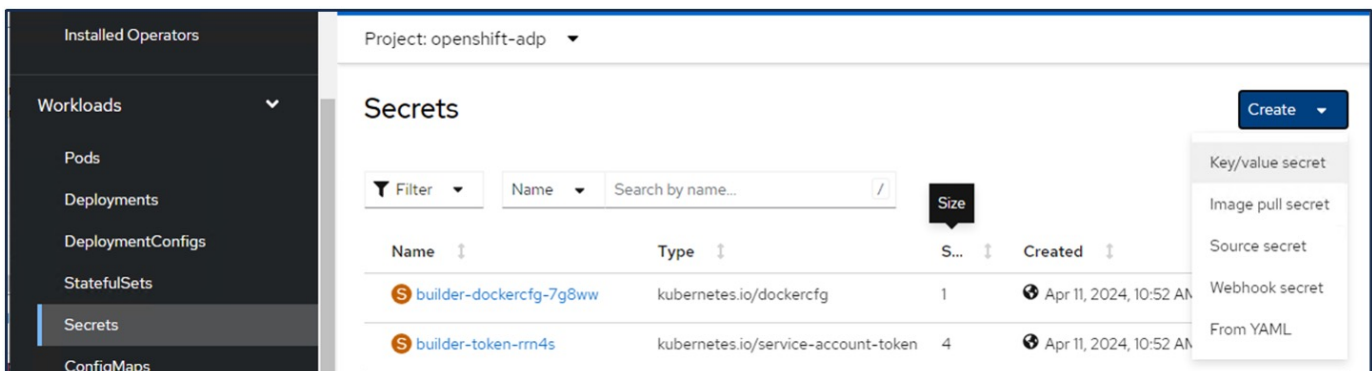
- Eine logische Schnittstellen-IP (Logical Interface, LIF), die für den Zugriff auf S3 verwendet werden kann
- Benutzeranmeldedaten für den Zugriff auf S3, die den Zugriffsschlüssel und den geheimen Zugriffsschlüssel enthalten
- Ein Bucket-Name in S3 für Backups mit Zugriffsberechtigungen für den Benutzer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

Schritte zum Konfigurieren von Velero

- Erstellen Sie zunächst einen Schlüssel für die ONTAP S3-Benutzeranmeldeinformationen. 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.



The screenshot shows the 'Secrets' page in the Kubernetes dashboard. The page title is 'Secrets' and the project is 'openshift-adp'. There are two secrets listed in the table:

| 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 |

The 'Create' button is located in the top right corner, and a dropdown menu is open showing options: Key/value secret, Image pull secret, Source secret, Webhook secret, and From YAML.

Project: openshift-adp ▾

Create key/value secret

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

Secret name *

Unique name of the new secret.

Key *

Value

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

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

+ Add key/value

Create

Cancel



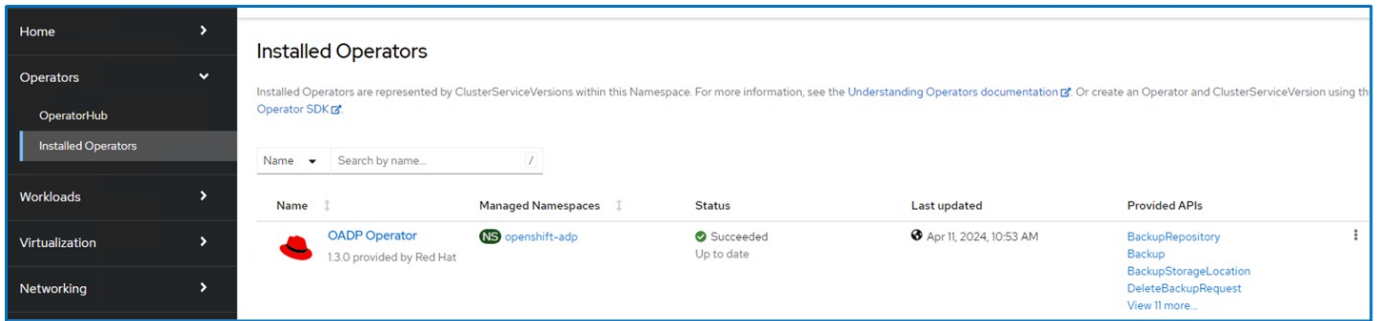
Um den Standardschlüssel mit dem Namen „Cloud-Anmeldedaten“ aus der CLI zu erstellen, können Sie den folgenden Befehl verwenden. Wenn die Backup- und Snapshot-Speicherorte die gleichen Anmeldeinformationen verwenden, müssen Sie nur das Standardgeheimnis wie oben gezeigt erstellen. Weitere Szenarien finden Sie in der OADP-Dokumentation.

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

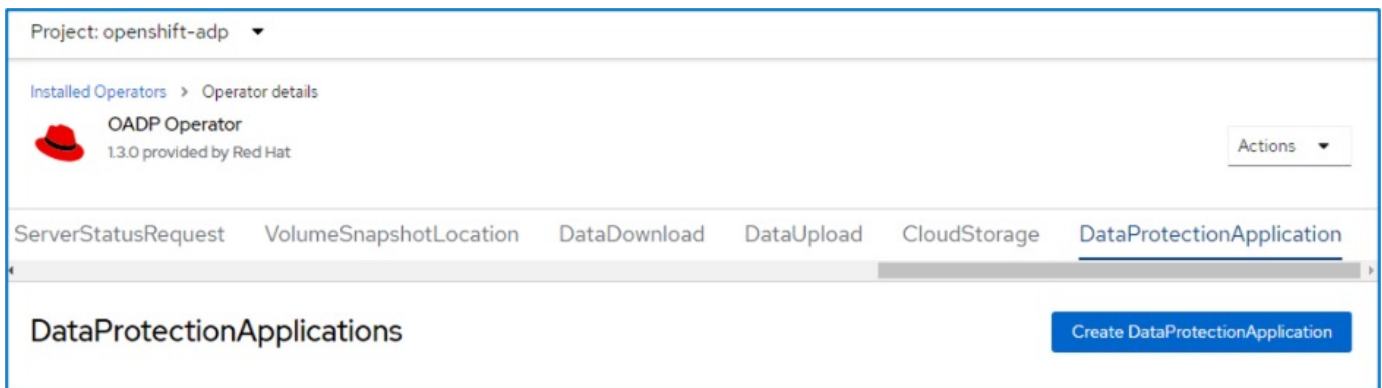
credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

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


- Wählen Sie dann zum Konfigurieren von Velero im Menüpunkt unter Operatoren die Option installierte Operatoren aus, klicken Sie auf OADP-Operator und wählen Sie dann die Registerkarte DataProtectionApplication aus.



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



Gehen Sie nun zur YAML-Ansicht und ersetzen Sie die Standardinformationen oder fügen Sie die Informationen wie in der yaml-Datei unten gezeigt hinzu.

```

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

```

Die oben genannte YAML enthält die folgenden Abschnitte in der Spezifikation, die entsprechend dem Beispiel konfiguriert werden müssen:

Backup-Standorte

ONTAP S3 (mit seinen Zugangsdaten und anderen in der yaml angezeigten Informationen) ist als

Standardspeicherort für velero konfiguriert.

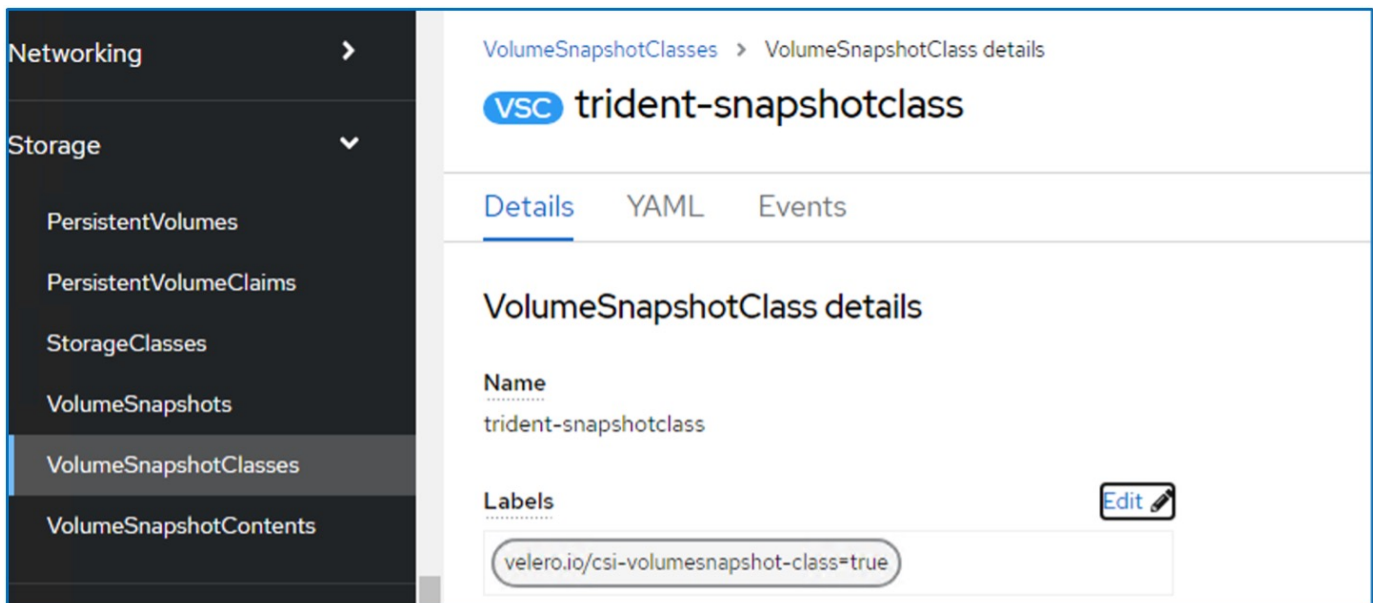
Schnappschusspositionen

ONTAP S3 ist als Standardspeicherort für PVC-Snapshots für Velero konfiguriert.

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

Stellen Sie sicher, dass die Snapshots auch dann bestehen können, wenn die VolumeSnapshot-Objekte gelöscht werden. Dazu kann die Delegationsrichtlinie auf „Beibehalten“ gesetzt werden. 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
```


VolumeSnapshotClasses > VolumeSnapshotClass details

VSC trident-snapshotclass


Details | YAML | Events

VolumeSnapshotClass details

Name
trident-snapshotclass

Labels Edit 

velero.io/csi-volumesnapshot-class=true



Annotations
1 annotation 

Driver
csi.trident.netapp.io

Deletion policy
Retain

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


Installed Operators > Operator details







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

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

DataProtectionApplications

Create DataProtectionApplication


Name  Search by name...

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

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

Project: openshift-adp

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat


Actions

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRe

BackupStorageLocations

Create BackupStorageLocation

Name Search by name...

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

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

Schritte zum Erstellen einer Sicherung einer VM

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

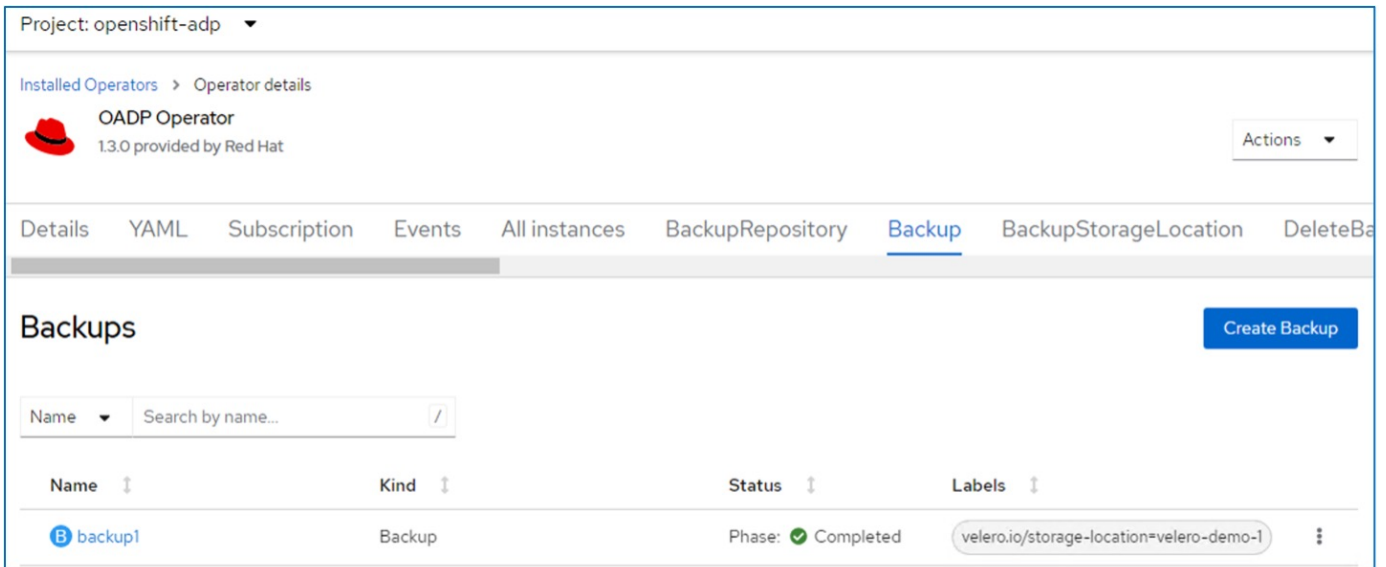
Ein Snapshot der persistenten Volumes, auf denen die Festplatten gesichert werden, wird vom CSI erstellt und an den im yaml bereitgestellten Objektspeicherort verschoben. Das Backup bleibt gemäß ttl 30 Tage im System.

```

apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1
  ttl: 720h0m0s


```

Sobald das Backup abgeschlossen ist, sollte seine Phase als abgeschlossen angezeigt werden.



Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat



Actions ▾

Details | YAML | Subscription | Events | All instances | BackupRepository | **Backup** | BackupStorageLocation | DeleteBa

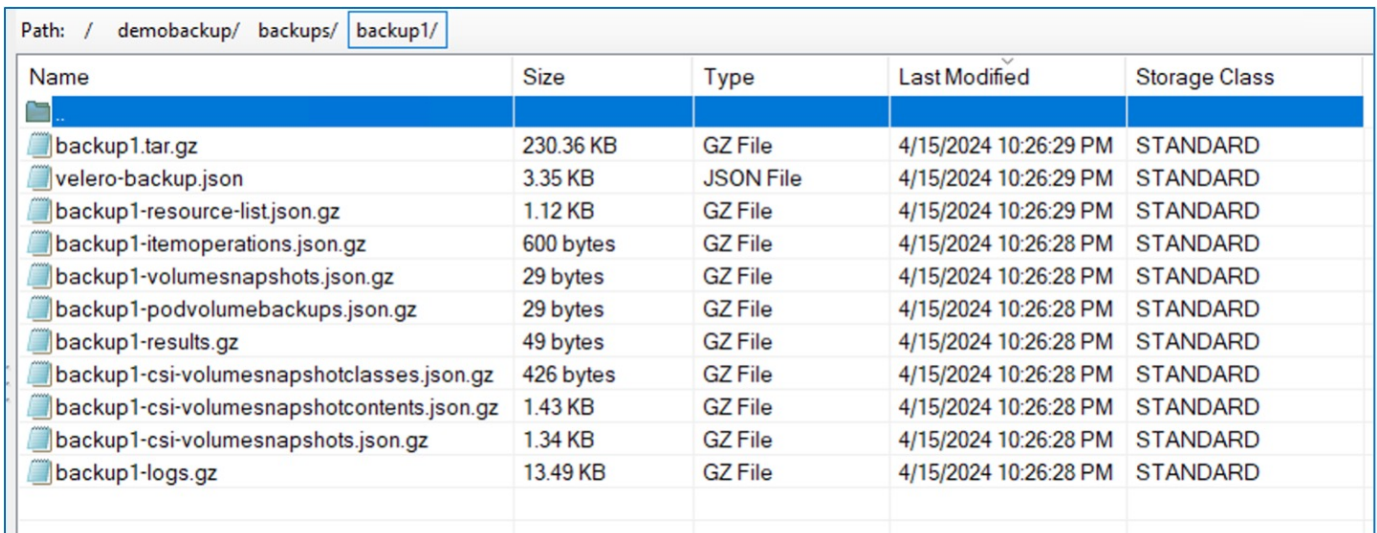
Backups

Create Backup

Name ▾ Search by name... /

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

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



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 VMs in OpenShift-Virtualisierung

Um Backups nach einem Zeitplan zu erstellen, müssen Sie eine benutzerdefinierte Ressource für den Zeitplan erstellen.

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


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

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

Sobald der Zeitplan erstellt wurde, wird er aktiviert.

Project: openshift-adp ▾



[Installed Operators](#) > [Operator details](#)

 **OADP Operator**
1.3.0 provided by Red Hat

[storageLocation](#) [DeleteBackupRequest](#) [DownloadRequest](#) [PodVolumeBackup](#) [PodVolumeRestore](#) [Restore](#) [Schedule](#)

Schedules


Name ▾ Search by name... /

| Name | Kind | Status | Labels |
|---|----------|--|-----------|
|  schedule1 | Schedule | Phase:  Enabled | No labels |

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

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat


Actions ▾

Events All instances BackupRepository **Backup** BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups

Create Backup

Name ▾ Search by name... /

| Name | Kind | Status | Labels |
|--|--------|-------------------|---|
|  schedule1-20240416140507 | Backup | Phase: InProgress | velero.io/schedule-name=schedule1 velero.io/storage-location=velero-demo-1 |

Stellen Sie eine VM aus einem Backup wieder her

Voraussetzungen

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


Schritte zum Durchführen einer Wiederherstellung

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.

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

Actions ▾

est DownloadRequest PodVolumeBackup PodVolumeRestore **Restore** Schedule ServerStatusRequest VolumeSnap

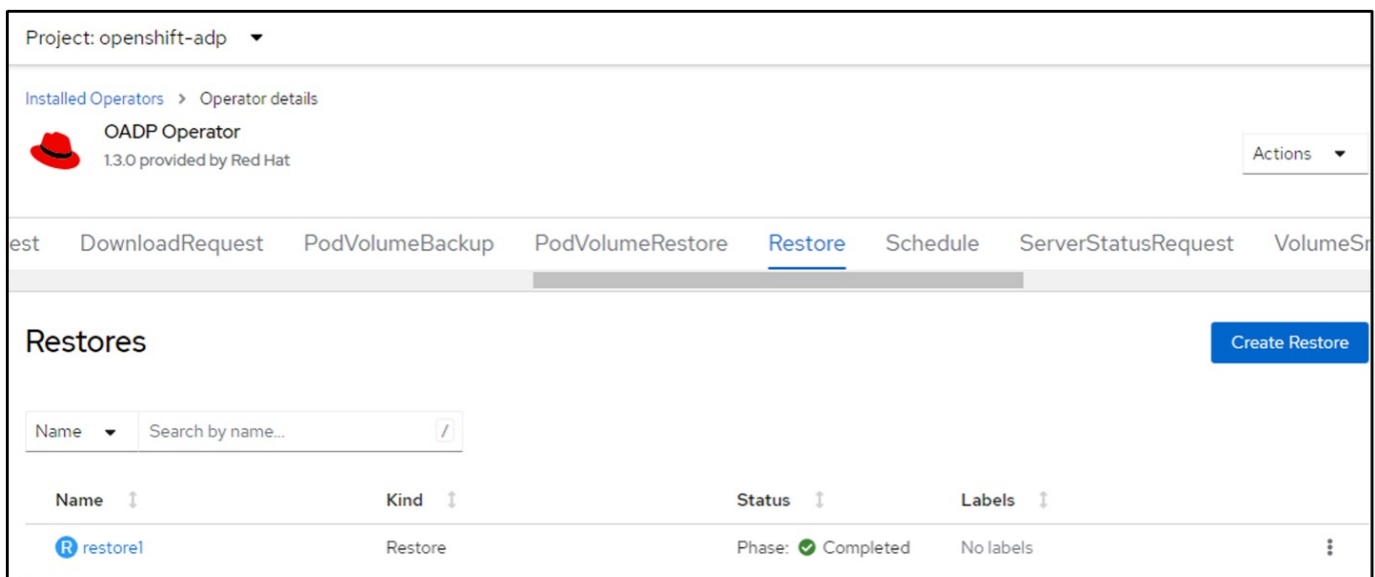
Restores

Create Restore

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


Wenn die Phase abgeschlossen angezeigt wird, sehen Sie, dass die virtuellen Maschinen wiederhergestellt wurden

In den Status, in dem der Snapshot erstellt wurde. (Wenn die Sicherung erstellt wurde, als die VM lief, wird die Wiederherstellung der VM aus dem Backup die wiederhergestellte VM starten und ihren Betrieb wieder herstellen)



Project: openshift-adp

Installed Operators > Operator details

 OADP Operator
1.3.0 provided by Red Hat



Actions

est DownloadRequest PodVolumeBackup PodVolumeRestore **Restore** Schedule ServerStatusRequest VolumeS

Restores

Create Restore

Name Search by name...

| Name | Kind | Status | Labels |
|--|---------|--|-----------|
|  restore1 | Restore | Phase:  Completed | No labels |

Löschen von Backups und Restores in mit Velero

Löschen eines Backups

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

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

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

Laden Sie die CLI gemäß den Anweisungen in der herunter ["Velero-Dokumentation"](#).

Führen Sie den folgenden Löschbefehl über die Velero CLI aus

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

Sie können den Restore CR auch über die Velero CLI löschen

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

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

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

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.