



OpenShift Virtualisierung

NetApp Solutions

NetApp
December 19, 2024

Inhalt

- NetApp-Lösungen für die OpenShift-Virtualisierung 1
 - Überblick 1
 - Implementierung vor Ort 5
 - Bereitstellung auf ROSA mit FSxN 31
 - Datensicherung Mit Tools Von Drittanbietern 47
 - Monitoring 69
 - Empfehlung Von Best Practices 76
 - Weitere Informationen: Red hat OpenShift mit NetApp 83

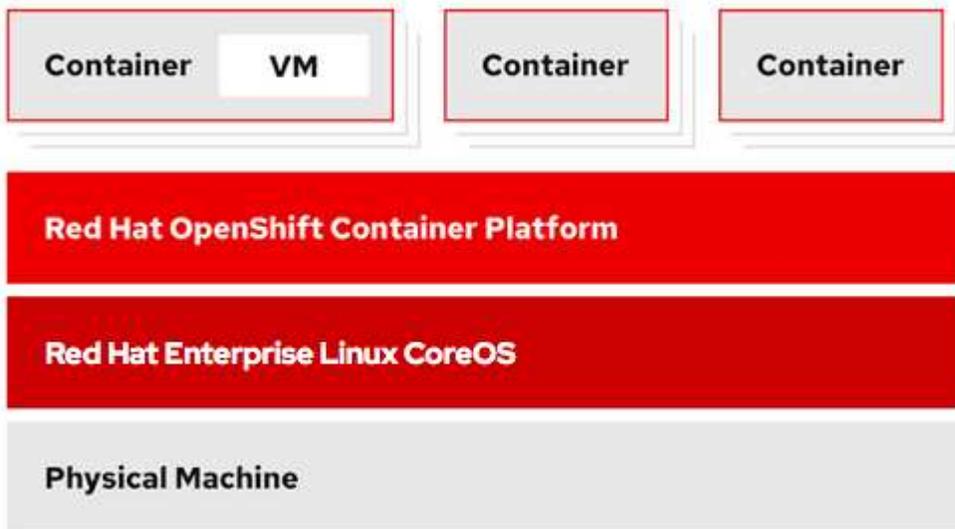
NetApp-Lösungen für die OpenShift-Virtualisierung

Überblick

Red hat OpenShift Virtualisierung mit NetApp ONTAP

Je nach Anwendungsfall können sowohl Container als auch Virtual Machines (VMs) als optimale Plattformen für verschiedene Applikationstypen dienen. Daher führen viele Unternehmen einige ihrer Workloads auf Containern und einige auf VMs aus. Dies führt häufig dazu, dass Unternehmen zusätzliche Herausforderungen meistern müssen, indem sie separate Plattformen managen müssen: Einen Hypervisor für VMs und einen Container-Orchestrator für Applikationen.

Um diese Herausforderung zu bewältigen, hat Red hat die OpenShift Virtualization (früher bekannt als Container Native Virtualization) eingeführt – angefangen bei OpenShift Version 4.6. Mit der OpenShift Virtualization-Funktion können Sie virtuelle Maschinen parallel mit Containern auf derselben OpenShift Container Platform-Installation ausführen und verwalten. Sie bieten Hybrid-Managementfunktionen für die Automatisierung der Bereitstellung und des Managements von VMs durch Betreiber. Neben der Erstellung von VMs in OpenShift unterstützt Red hat mit OpenShift Virtualization auch den Import von VMs aus VMware vSphere, Red hat Virtualization und Red hat OpenStack Platform-Implementierungen.



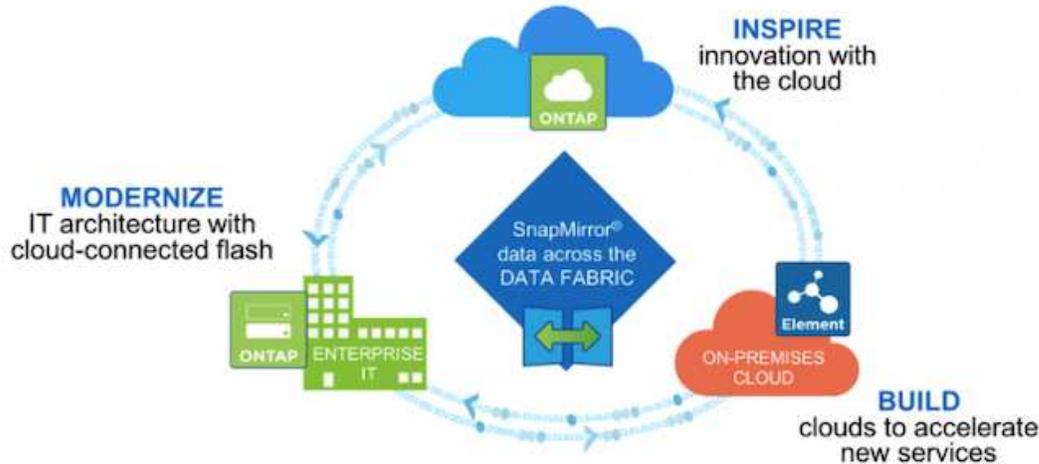
Bestimmte Funktionen wie Live-VM-Migration, Klonen von VM-Festplatten, VM-Snapshots usw. werden auch von OpenShift Virtualization mit Unterstützung von Trident unterstützt, wenn diese durch NetApp ONTAP unterstützt werden. Beispiele für jeden dieser Workflows werden im weiteren Verlauf dieses Dokuments im jeweiligen Abschnitt erläutert.

Weitere Informationen zu Red hat OpenShift Virtualization finden Sie in der Dokumentation "[Hier](#)".

NetApp Storage-Überblick

NetApp verfügt über mehrere Storage-Plattformen, die für Trident Storage Orchestrator geeignet sind, um Storage für auf Red hat OpenShift implementierte Applikationen

bereitzustellen.



- AFF und FAS Systeme führen NetApp ONTAP aus und liefern Storage sowohl für File-basierte (NFS) als auch für blockbasierte Anwendungsfälle (iSCSI).
- Cloud Volumes ONTAP und ONTAP Select bieten die gleichen Vorteile in der Cloud bzw. im virtuellen Bereich.
- Amazon FSX for NetApp ONTAP, Azure NetApp Files und Google Cloud NetApp Volumes bieten dateibasierten Storage in der Cloud.
- NetApp Element Storage-Systeme bieten für blockbasierte (iSCSI-)Anwendungsfälle in hochskalierbarer Umgebung.



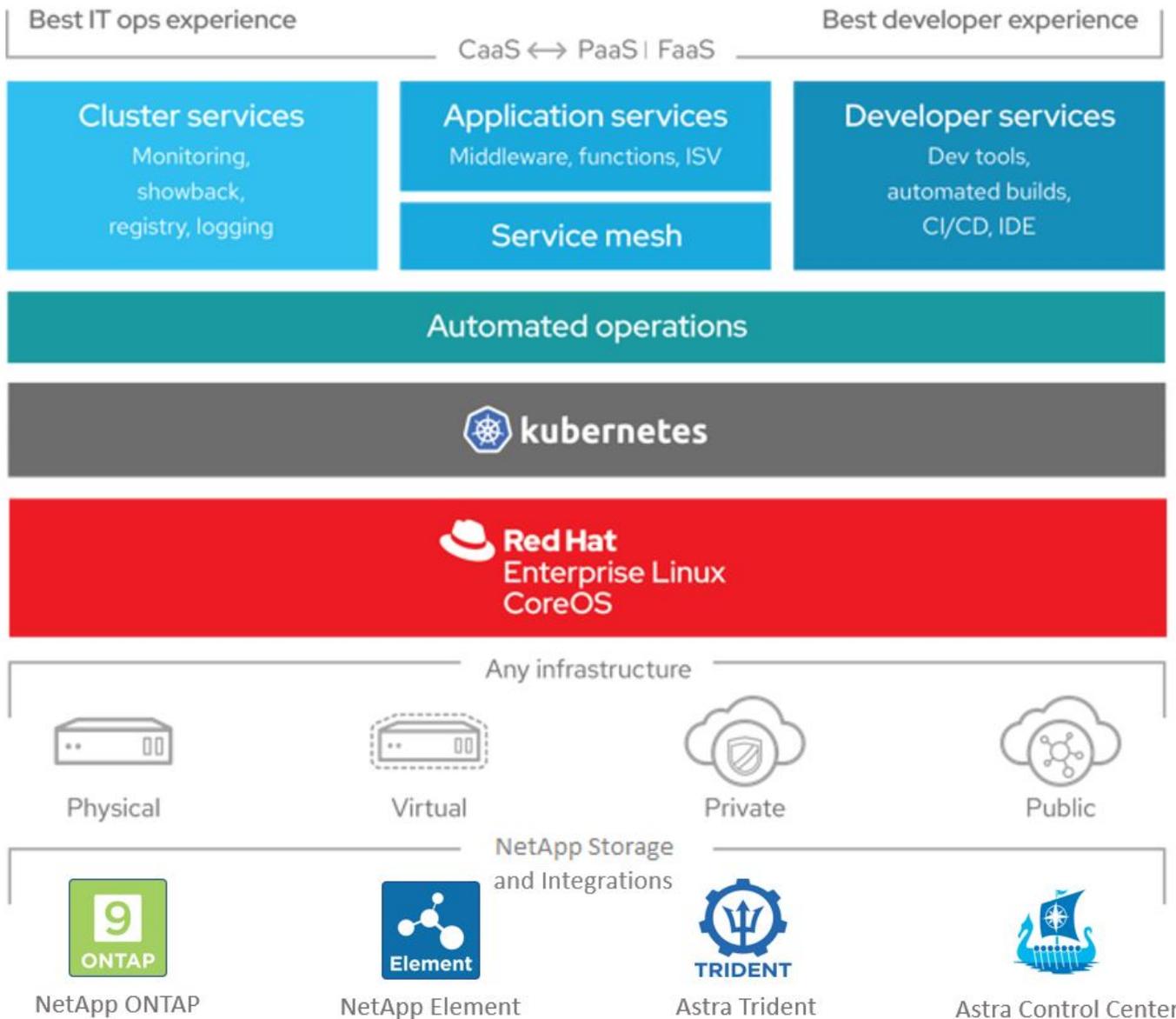
Jedes Storage-System im NetApp Portfolio kann das Datenmanagement und das Verschieben von Daten zwischen lokalen Standorten und der Cloud vereinfachen. Damit befinden sich Ihre Daten genau dort, wo sich Ihre Applikationen befinden.

Auf den folgenden Seiten finden Sie zusätzliche Informationen zu den in Red hat OpenShift mit NetApp validierten NetApp Storage-Systemen:

- ["NetApp ONTAP"](#)
- ["NetApp Element"](#)

Überblick über die NetApp Storage-Integration

NetApp bietet verschiedene Produkte, die Sie bei der Orchestrierung und dem Management persistenter Daten in Container-basierten Umgebungen wie Red hat OpenShift unterstützen.



NetApp Astra Control bietet eine umfassende Auswahl an Storage- und applikationsspezifischen Datenmanagement-Services für zustandsorientierte Kubernetes Workloads auf Basis der NetApp Datensicherungstechnologie. Der Astra Control Service unterstützt statusorientierte Workloads in Cloud-nativen Kubernetes-Implementierungen. Das Astra Control Center unterstützt statusorientierte Workloads in lokalen Implementierungen wie Red hat OpenShift. Weitere Informationen finden Sie auf der NetApp Astra Control Website "[Hier](#)".

NetApp Trident ist ein Open-Source- und vollständig unterstützter Storage-Orchestrator für Container und Kubernetes-Distributionen, einschließlich Red hat OpenShift. Weitere Informationen finden Sie auf der Trident-Website "[Hier](#)".

Auf den folgenden Seiten finden Sie zusätzliche Informationen zu den NetApp Produkten, die für das Management von Applikationen und persistentem Storage in Red hat OpenShift mit NetApp validiert wurden:

- "[NetApp Astra Control Center](#)"
- "[NetApp Trident](#)"

Videos und Demos: Red hat OpenShift mit NetApp

In den folgenden Videos werden einige der in diesem Dokument dokumentierten Funktionen gezeigt

[Amazon FSX for NetApp ONTAP: Red hat OpenShift Service auf AWS mit gehosteter Kontrollebene](#)

[Live-Migration virtueller Maschinen in OpenShift-Virtualisierung auf ROSA mit Amazon FSX für NetApp ONTAP](#)

[Ansible-Automatisierung für die Implementierung von Trident und die Erstellung von Storage-Klassen im OpenShift-Cluster](#)

["Das Playbook, mit dem NetApp Trident, StorageClasses und Back-End mithilfe von Ansible installiert werden, ist in GitHub zu finden."](#)

[Implementieren Sie eine neue VM in OpenShift-Virtualisierung mit ONTAP-SAN-\(iSCSI-\)Storage-Klasse](#)

[Implementieren Sie eine postgresql Container-App mit ONTAP NAS-Storage Class](#)

[Cloud Insights-Integration in OpenShift-Virtualisierung](#)

[Mit Red hat MTV VMs zu OpenShift-Virtualisierung mit NetApp ONTAP-Speicher migrieren](#)

[Failover/Failback von OpenShift-VMs mithilfe erweiterter Datenmanagement-Funktionen von Trident \(nur Early Access Programm verfügbar\)](#)

[Cloud Insights-Integration in OpenShift-Virtualisierung](#)

[Ansible-Automatisierung für die Implementierung von Trident und die Erstellung von Storage-Klassen im OpenShift-Cluster](#)

Beispiel-Ansible-Code in GitHub ["Das Playbook, mit dem NetApp Trident, StorageClasses und Back-End mithilfe von Ansible installiert werden, ist in GitHub zu finden."](#)

[Implementieren Sie eine postgresql Container-App mit ONTAP NAS-Storage Class](#)

[Beschleunigte Softwareentwicklung mit Astra Control und NetApp FlexClone Technologie – Red hat OpenShift mit NetApp](#)

[Nutzen Sie NetApp Astra Control, um eine Analyse nach der Sterblichen durchzuführen und Ihre Applikation Restores durchzuführen](#)

[Datensicherung in CI/CD-Pipeline mit Astra Control Center](#)

[Workload-Migration mit Astra Control Center – Red hat OpenShift mit NetApp](#)

[Workload-Migration – Red hat OpenShift mit NetApp](#)

[Installation von OpenShift Virtualization – Red hat OpenShift mit NetApp](#)

[Bereitstellen einer virtuellen Maschine mit OpenShift-Virtualisierung – Red hat OpenShift mit NetApp](#)

[NetApp HCI für Red hat OpenShift auf Red hat Virtualization](#)

Implementierung vor Ort

Implementieren Sie eine Virtualisierung mit Red hat OpenShift mit NetApp ONTAP

In diesem Abschnitt wird die Bereitstellung von Red hat OpenShift Virtualization mit NetApp ONTAP beschrieben.

Voraussetzungen

- Ein Red hat OpenShift-Cluster (ab Version 4.6) wird auf Bare-Metal-Infrastrukturen mit RHCOS-Worker-Nodes installiert
- Der OpenShift-Cluster muss über eine vom Installer bereitgestellte Infrastruktur (IPI) installiert werden
- Implementieren Sie Machine Health Checks, um die HA für VMs aufrechtzuerhalten
- Ein NetApp ONTAP Cluster
- Trident auf dem OpenShift-Cluster installiert
- Ein Trident Back-End, das mit einer SVM auf ONTAP Cluster konfiguriert ist
- Eine auf dem OpenShift-Cluster konfigurierte StorageClass mit Trident als bereitstellung
- Cluster-Admin-Zugriff auf Red hat OpenShift-Cluster
- Administratorzugriff auf das NetApp ONTAP-Cluster
- Eine Admin-Workstation mit den Tools tridentctl und oc installiert und zur €Pfad hinzugefügt

Da die OpenShift-Virtualisierung von einem auf dem OpenShift-Cluster installierten Operator gemanagt wird, entsteht zusätzlicher Overhead für Speicher, CPU und Speicher, der bei der Planung der Hardwareanforderungen für den Cluster berücksichtigt werden muss. Siehe Dokumentation ["Hier"](#) Entnehmen.

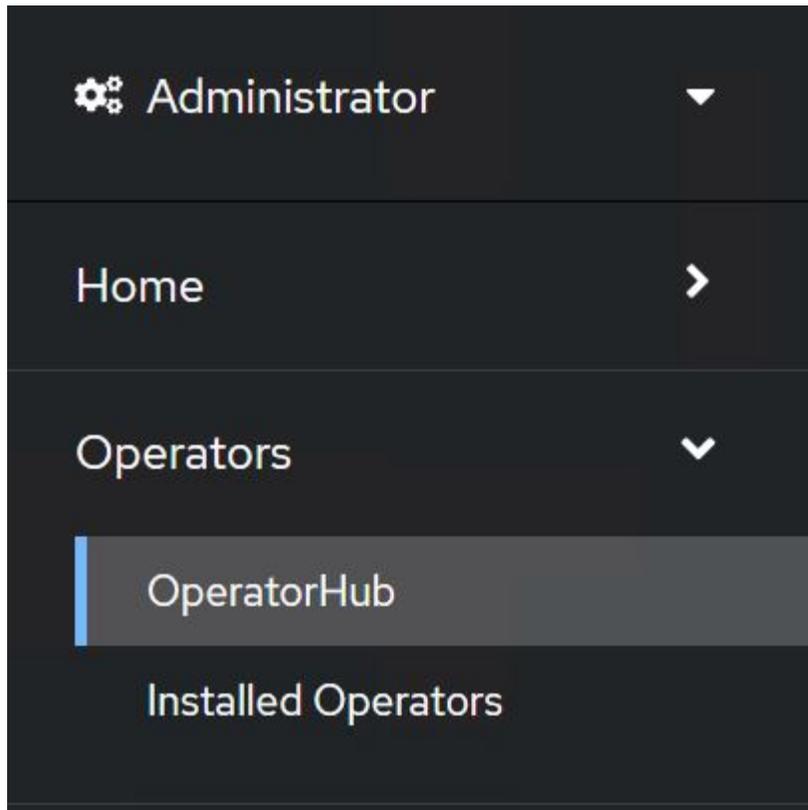
Optional können Sie auch einen Teilbereich der OpenShift-Cluster-Nodes angeben, um die OpenShift-Virtualisierungsbetreiber, -Controller und -VMs zu hosten, indem Sie die Regeln für die Knotenplatzierung konfigurieren. Befolgen Sie die Dokumentation, um die Regeln für die Knotenplatzierung für OpenShift Virtualization zu konfigurieren ["Hier"](#).

Für den von OpenShift Virtualization unterstützten Storage empfiehlt NetApp die Verwendung einer dedizierten StorageClass, die Storage von einem bestimmten Trident-Back-End anfordert. Diese wiederum wird durch eine dedizierte SVM unterstützt. Dies sorgt für eine weiterhin hohe Mandantenfähigkeit im Hinblick auf die Daten, die für VM-basierte Workloads im Cluster OpenShift zur Verfügung gestellt werden.

Implementieren Sie eine Virtualisierung mit Red hat OpenShift mit NetApp ONTAP

Um die OpenShift Virtualization zu installieren, gehen Sie wie folgt vor:

1. Melden Sie sich beim Bare-Metal-Cluster Red hat OpenShift mit Zugriff auf den Cluster-Administrator an.
2. Wählen Sie in der Dropdown-Liste Perspektive den Eintrag Administrator aus.
3. Navigieren Sie zu Operators > OperatorHub, und suchen Sie nach OpenShift Virtualization.



4. Wählen Sie die Kachel OpenShift Virtualization aus, und klicken Sie auf Installieren.

OpenShift Virtualization 2.6.2 provided by Red Hat

Install

Latest version
2.6.2

Capability level

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

Provider type
Red Hat

Provider
Red Hat

Requirements
Your cluster must be installed on bare metal infrastructure with Red Hat Enterprise Linux CoreOS workers.

Details
OpenShift Virtualization extends Red Hat OpenShift Container Platform, allowing you to host and manage virtualized workloads on the same platform as container-based workloads. From the OpenShift Container Platform web console, you can import a VMware virtual machine from vSphere, create new or clone existing VMs, perform live migrations between nodes, and more. You can use OpenShift Virtualization to manage both Linux and Windows VMs.

The technology behind OpenShift Virtualization is developed in the [KubeVirt](#) open source community. The KubeVirt project extends [Kubernetes](#) by adding additional virtualization resource types through [Custom Resource Definitions](#) (CRDs). Administrators can use Custom Resource Definitions to manage [VirtualMachine](#) resources alongside all other resources that Kubernetes provides.

5. Lassen Sie auf dem Bildschirm Install Operator alle Standardparameter stehen, und klicken Sie auf Install.

Update channel *

- 2.1
- 2.2
- 2.3
- 2.4
- stable

Installation mode *

- All namespaces on the cluster (default)
This mode is not supported by this Operator
- A specific namespace on the cluster
Operator will be available in a single Namespace only.

Installed Namespace *

- Operator recommended Namespace: **PR** openshift-cnv

i Namespace creation
Namespace **openshift-cnv** does not exist and will be created.

- Select a Namespace

Approval strategy *

- Automatic
- Manual

Install Cancel

 OpenShift Virtualization
provided by Red Hat

Provided APIs

HC OpenShift Virtualization Deployment **Required**

Represents the deployment of OpenShift Virtualization

6. Warten Sie, bis die Installation des Bedieners abgeschlossen ist.

 OpenShift Virtualization
2.6.2 provided by Red Hat

Installing Operator

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace openshift-cnv](#)

7. Klicken Sie nach der Installation des Operators auf Hyperconverged erstellen.



Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

HC HyperConverged **Required**

Creates and maintains an OpenShift Virtualization Deployment

[Create HyperConverged](#)

[View installed Operators in Namespace openshift-cnv](#)

8. Klicken Sie im Bildschirm Hyperconverged erstellen auf Erstellen, um alle Standardparameter zu akzeptieren. In diesem Schritt wird die Installation von OpenShift Virtualization gestartet.

Name *

Labels

Infra >

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarily directly on each node running VMs/VMIs.

Workloads >

workloads HyperConvergedConfig influences the pod configuration (currently only placement) of components which need to be running on a node where virtualization workloads should be able to run. Changes to Workloads HyperConvergedConfig can be applied only without existing workload.

Bare Metal Platform

true

BareMetalPlatform indicates whether the infrastructure is baremetal.

Feature Gates >

featureGates is a map of feature gate flags. Setting a flag to `true` will enable the feature. Setting `false` or removing the feature gate, disables the feature.

Local Storage Class Name

LocalStorageClassName the name of the local storage class.

- Nachdem alle Pods in den Betriebszustand im Namespace openshift-cnv verschoben wurden und sich der OpenShift Virtualization Operator im Status erfolgreich befindet, ist der Operator betriebsbereit. VMs können jetzt im OpenShift-Cluster erstellt werden.

Project: openshift-cnv ▾

Installed Operators

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

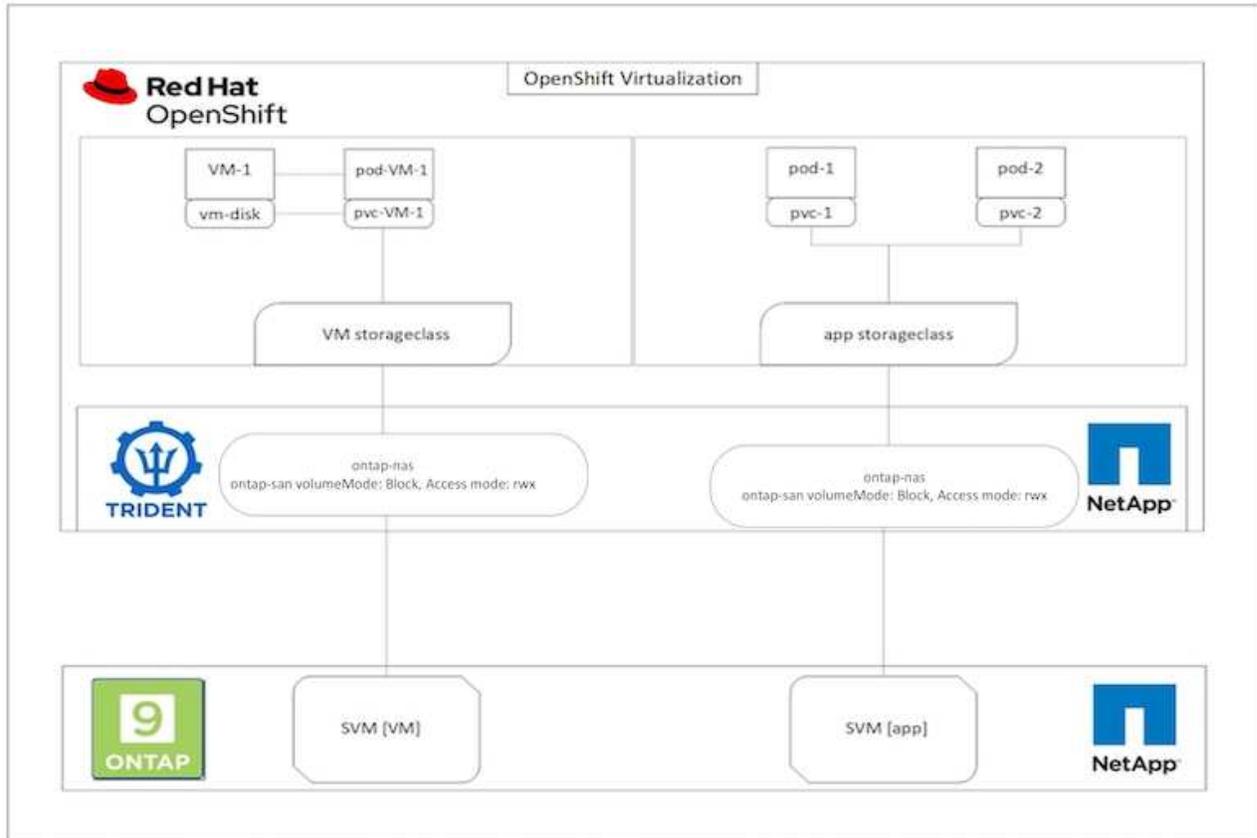
Name ▾	Managed Namespaces	Status	Last updated	Provided APIs
 OpenShift Virtualization 2.6.2 provided by Red Hat	 openshift-cnv	 Succeeded Up to date	 May 18, 8:02 pm	OpenShift Virtualization Deployment HostPathProvisioner deployment

Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

In diesem Abschnitt wird die Erstellung einer virtuellen Maschine mit Red hat OpenShift Virtualization erläutert.

Erstellen Sie eine VM

VMs sind statusorientierte Implementierungen, bei denen Volumes das Betriebssystem und die Daten hosten müssen. Da die VMs als Pods ausgeführt werden, werden die VMs mit PVS unterstützt, die über Trident auf NetApp ONTAP gehostet werden. Diese Volumes sind als Festplatten verbunden und speichern das gesamte Dateisystem einschließlich der Boot-Quelle der VM.



Führen Sie die folgenden Schritte aus, um schnell eine virtuelle Maschine auf dem OpenShift-Cluster zu erstellen:

1. Navigieren Sie zu Virtualisierung > Virtuelle Maschinen, und klicken Sie auf Erstellen.
2. Aus Vorlage auswählen.
3. Wählen Sie das gewünschte Betriebssystem aus, für das die Startquelle verfügbar ist.
4. Aktivieren Sie das Kontrollkästchen VirtualMachine nach der Erstellung starten.
5. Klicken Sie auf Quick Create VirtualMachine.

Die virtuelle Maschine wird erstellt und gestartet und kommt in den Status **running**. Es erstellt automatisch eine PVC und ein entsprechendes PV für die Boot-Disk unter Verwendung der Standard-Storage-Klasse. Um die VM in Zukunft live migrieren zu können, müssen Sie sicherstellen, dass die für die Festplatten verwendete Speicherklasse RWX-Volumes unterstützen kann. Dies ist eine Voraussetzung für die Live-Migration. ontap-nas und ontap-san (Volume-Mode Block für iSCSI- und NVMe/TCP-Protokolle) unterstützen RWX Zugriffsmodi für die Volumes, die mithilfe der entsprechenden Storage-Klassen erstellt wurden.

Informationen zum Konfigurieren der ONTAP-san-Storage-Klasse auf dem Cluster finden Sie unter ["Abschnitt zur Migration einer VM von VMware auf OpenShift Virtualization"](#).



Sie können ONTAP NAS oder iSCSI als Standardspeicherklasse für das Cluster einrichten. Wenn Sie auf Quick Create VirtualMachine klicken, wird die Standard-Speicherklasse verwendet, um die PVC und das PV für die bootfähige Root-Festplatte für die VM zu erstellen. Wenn Ihre Standard-Storage-Klasse nicht ontap-nas oder ontap-san ist, können Sie die Storage-Klasse für die Festplatte auswählen, indem Sie VirtualMachine anpassen > VirtualMachine Parameter anpassen > Disks auswählen und dann die Festplatte bearbeiten, um die erforderliche Storage-Klasse zu verwenden.

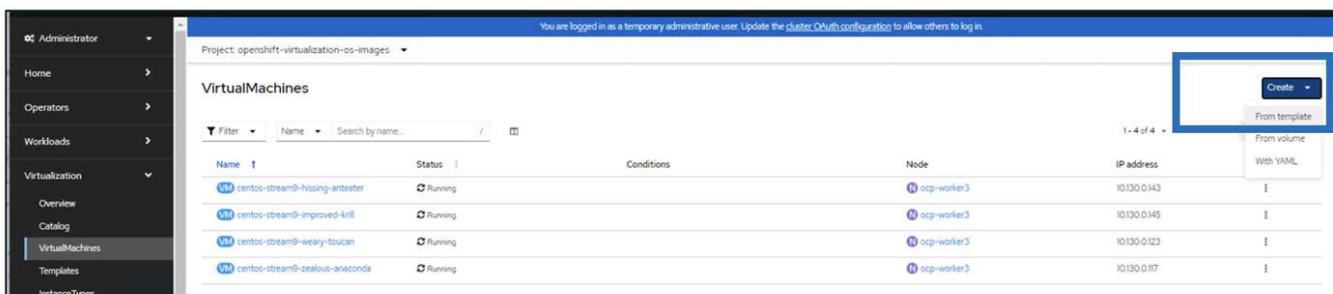
Normalerweise ist der Block-Zugriffsmodus im Vergleich zu Dateisystemen bei der Bereitstellung der VM-Festplatten vorzuziehen.

Um die Erstellung der virtuellen Maschine anzupassen, nachdem Sie die Betriebssystemvorlage ausgewählt haben, klicken Sie auf VirtualMachine anpassen anstatt auf schnelles Erstellen.

1. Wenn das ausgewählte Betriebssystem eine Bootquelle konfiguriert hat, können Sie auf **VirtualMachine Parameter anpassen** klicken.
2. Wenn für das ausgewählte Betriebssystem keine Startquelle konfiguriert ist, müssen Sie es konfigurieren. Details zu den Verfahren finden Sie im "[Dokumentation](#)".
3. Nach der Konfiguration der Startdiskette können Sie auf **VirtualMachine Parameter anpassen** klicken.
4. Sie können die VM über die Registerkarten auf dieser Seite individuell anpassen. Für z. B. Klicken Sie auf die Registerkarte **Disks** und dann auf **Add Disk**, um der VM einen weiteren Datenträger hinzuzufügen.
5. Klicken Sie auf Virtual Machine erstellen, um die virtuelle Maschine zu erstellen. Dadurch wird ein entsprechender Pod im Hintergrund bereitgestellt.



Wenn eine Startquelle für eine Vorlage oder ein Betriebssystem aus einer URL oder aus einer Registrierung konfiguriert ist, wird in der ein PVC erstellt `openshift-virtualization-os-images` Projizieren und Herunterladen des KVM-Gastabbilds auf das PVC. Sie müssen sicherstellen, dass Vorlagen-PVCs über genügend bereitgestellten Speicherplatz verfügen, um das KVM-Gast-Image für das entsprechende Betriebssystem unterzubringen. Diese PVCs werden dann geklont und als Rootdisk an virtuelle Maschinen angehängt, wenn sie mithilfe der entsprechenden Vorlagen in einem Projekt erstellt werden.



Create new VirtualMachine

Select an option to create a VirtualMachine from.

Template catalog InstanceTypes

Template project All projects

Default templates

All items Filter by keyword...

13 items

- Boot source available
- Operating system
 - CentOS
 - Fedora
 - Other
 - RHEL
 - Windows
- Workload
 - Desktop
 - High performance
 - Server

 <p>Source available</p> <p>CentOS Stream 8 VM centos-stream8-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>CentOS Stream 9 VM centos-stream9-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>CentOS 7 VM centos7-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>Fedora VM fedora-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>Red Hat Enterprise Linux 7 VM rhel7-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>
 <p>Source available</p> <p>Red Hat Enterprise Linux 8 VM rhel8-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>Red Hat Enterprise Linux 9 VM rhel9-server-small</p> <p>Project openshift Boot source PVC (auto import) Workload Server CPU 1 Memory 2 GiB</p>	 <p>Source available</p> <p>Microsoft Windows 10 VM windows10-desktop-medium</p> <p>Project openshift Boot source PVC Workload Desktop CPU 1 Memory 4 GiB</p>	 <p>Source available</p> <p>Microsoft Windows 11 VM windows11-desktop-medium</p> <p>Project openshift Boot source PVC Workload Desktop CPU 2 Memory 4 GiB</p>	 <p>Source available</p> <p>Microsoft Windows Server 2012 R2 VM windows2k12r2-server-medium</p> <p>Project openshift Boot source PVC Workload Server CPU 1 Memory 4 GiB</p>



CentOS Stream 9 VM

centos-stream9-server-small



Template info

Operating system

CentOS Stream 9 VM

Workload type

Server (default)

Description

Template for CentOS Stream 9 VM or newer. A PVC with the CentOS Stream disk image must be available.

Documentation

[Refer to documentation](#)

CPU | Memory

1 CPU | 2 GiB Memory

Network interfaces (1)

Name	Network	Type
default	Pod networking	Masquerade

Disks (2)

Name	Drive	Size
rootdisk	Disk	30 GiB
cloudinitdisk	Disk	-

Hardware devices (0)

GPU devices

Not available

Host devices

Not available

Quick create VirtualMachine

VirtualMachine name *

centos-stream9-pleased-ham...

Project

openshift-visualization-os-images

Start this VirtualMachine after creation

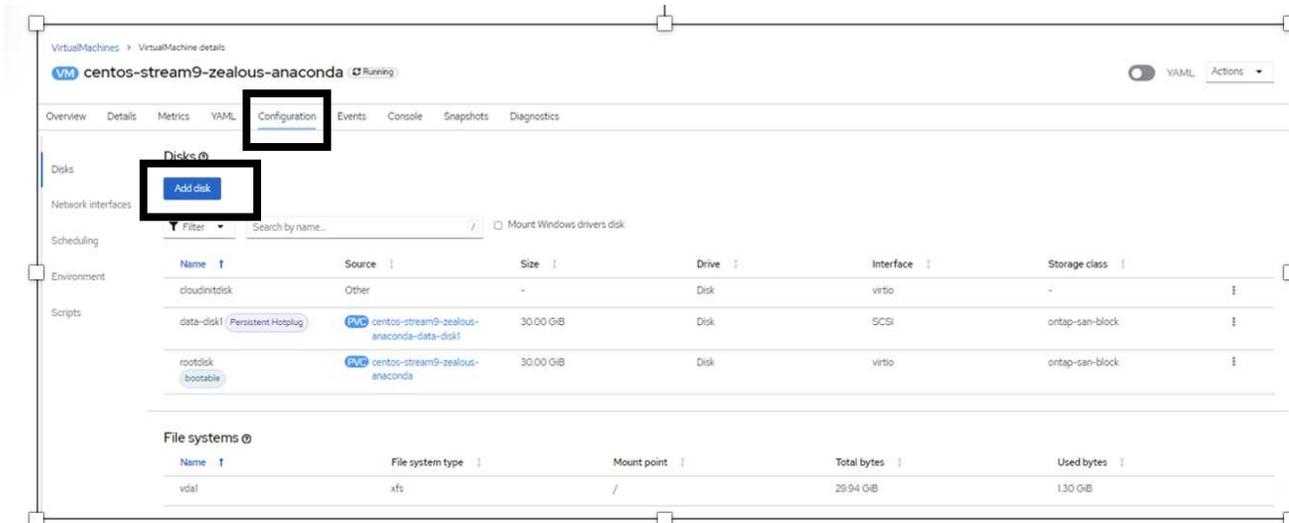
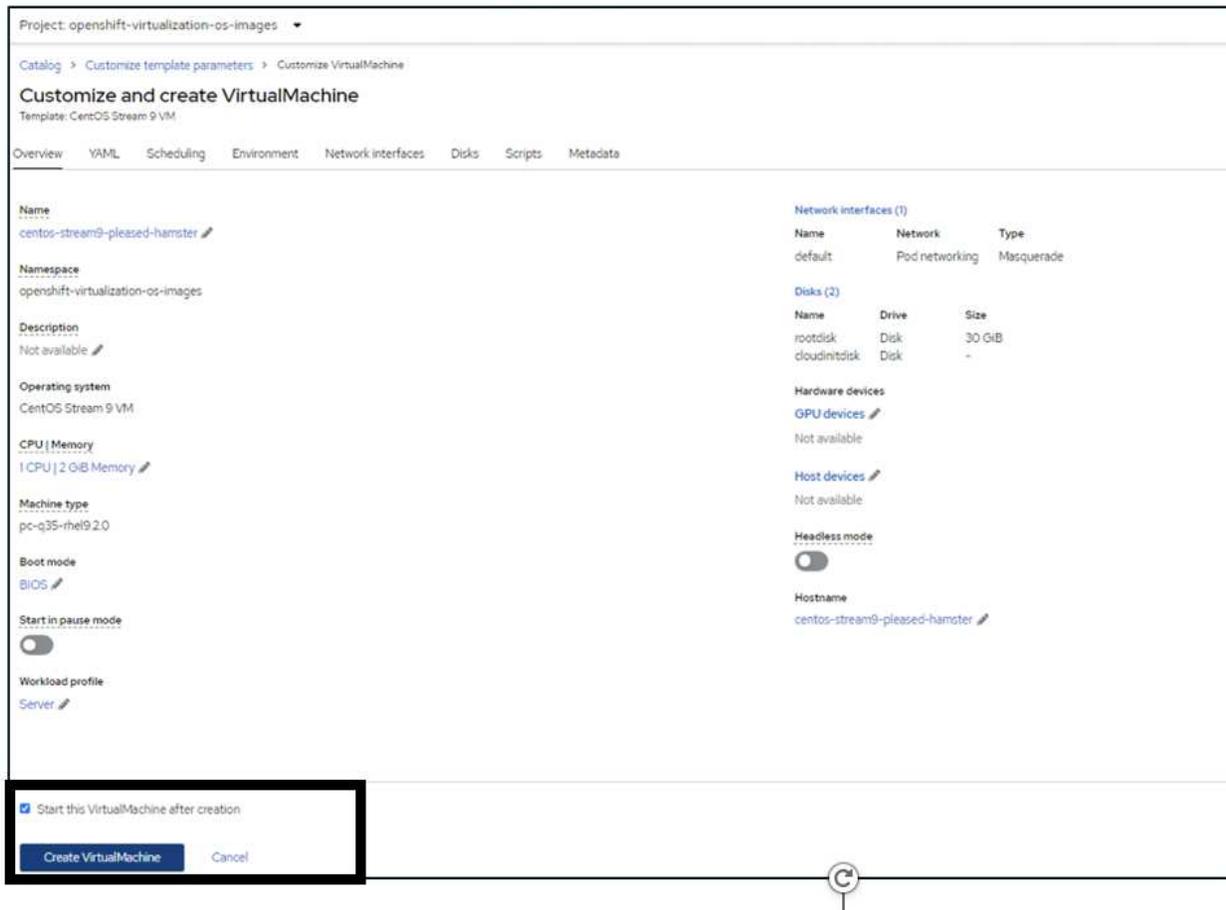
Quick create VirtualMachine

Customize VirtualMachine

Cancel

Activate Windows

Go to Settings to activate Windows.



Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

In diesem Abschnitt wird die Migration einer virtuellen Maschine zwischen VMware und einem OpenShift-Cluster mithilfe des Red hat OpenShift Virtualization Migrations-Toolkits beschrieben.

Migration der VM von VMware zu OpenShift-Virtualisierung mithilfe des Migration Toolkit für Virtualisierung

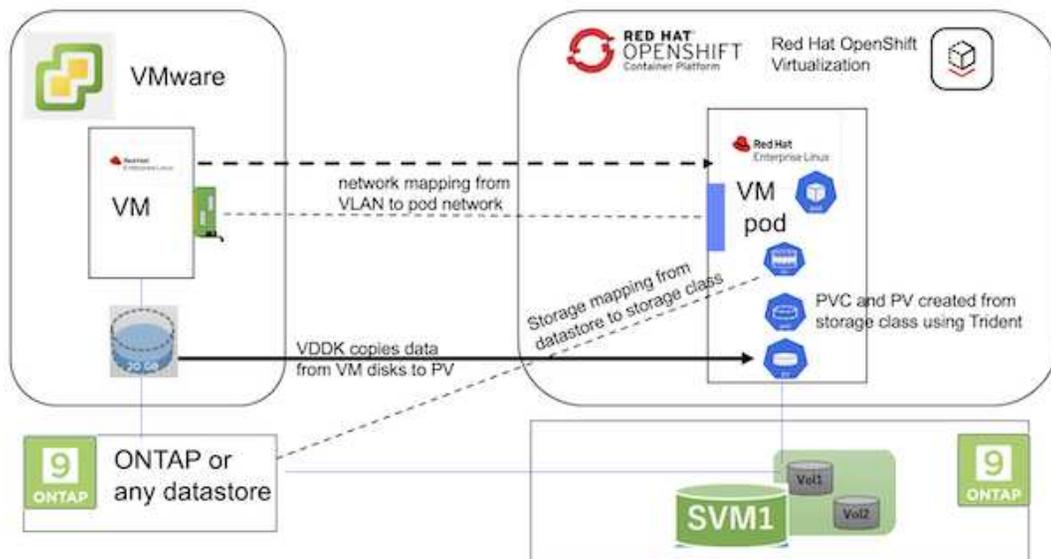
In diesem Abschnitt erfahren Sie, wie Sie mithilfe des Migrations-Toolkits für die Virtualisierung (MTV) virtuelle Maschinen von VMware auf OpenShift-Virtualisierung migrieren, die auf der OpenShift-Container-Plattform ausgeführt und mithilfe von Trident in NetApp ONTAP-Storage integriert wird.

Das folgende Video zeigt eine Demonstration der Migration einer RHEL VM von VMware zur OpenShift-Virtualisierung mit ontap-san Storage Class für persistenten Storage.

[Mit Red hat MTV VMs zu OpenShift-Virtualisierung mit NetApp ONTAP-Speicher migrieren](#)

Das folgende Diagramm zeigt eine allgemeine Ansicht der Migration einer VM von VMware zu Red hat OpenShift Virtualization.

Migration of VM from VMware to OpenShift Virtualization



Voraussetzungen für die Beispielmigration

Auf VMware

- Eine RHEL 9-VM mit RHEL 9.3 mit den folgenden Konfigurationen wurde installiert:
 - CPU: 2, Arbeitsspeicher: 20 GB, Festplatte: 20 GB
 - Benutzeranmeldeinformationen: Root-Benutzer und Anmeldedaten des Admin-Benutzers
- Nachdem die VM bereit war, wurde der postgresql-Server installiert.
 - postgresql-Server wurde gestartet und aktiviert, um beim Booten zu starten

```
systemctl start postgresql.service`  
systemctl enable postgresql.service  
The above command ensures that the server can start in the VM in  
OpenShift Virtualization after migration
```

- Es wurden 2 Datenbanken, 1 Tabelle und 1 Zeile in der Tabelle hinzugefügt. Siehe "[Hier](#)" Anweisungen zum Installieren von postgresql-Servern auf RHEL und zum Erstellen von Datenbank- und Tabelleneinträgen.



Stellen Sie sicher, dass Sie den postgresql-Server starten und den Dienst beim Booten starten.

Auf OpenShift Cluster

Die folgenden Installationen wurden vor der Installation von MTV abgeschlossen:

- OpenShift Cluster 4.13.34
- "[Trident 23.10](#)"
- Multipath auf den Cluster-Knoten mit aktivierter iSCSI-Funktion (für ontap-san Storage-Klasse). Informationen zum Erstellen eines Daemon-Satzes, der iSCSI auf jedem Knoten im Cluster aktiviert, finden Sie im bereitgestellten yamL.
- Trident Back-End- und Storage-Klasse für ONTAP SAN mit iSCSI Siehe die bereitgestellten yamL-Dateien für das dreigesichtige Backend und die Speicherklasse.
- "[OpenShift Virtualisierung](#)"

Um iscsi und Multipath auf den OpenShift-Cluster-Knoten zu installieren, verwenden Sie die unten angegebene yamL-Datei

Cluster-Knoten für iSCSI vorbereiten

```
apiVersion: apps/v1
kind: DaemonSet
metadata:
  namespace: trident
  name: trident-iscsi-init
  labels:
    name: trident-iscsi-init
spec:
  selector:
    matchLabels:
      name: trident-iscsi-init
  template:
    metadata:
      labels:
        name: trident-iscsi-init
    spec:
      hostNetwork: true
      serviceAccount: trident-node-linux
      initContainers:
        - name: init-node
          command:
            - nsenter
            - --mount=/proc/1/ns/mnt
            - --
```

```

- sh
- -c
args: ["$(STARTUP_SCRIPT)"]
image: alpine:3.7
env:
- name: STARTUP_SCRIPT
  value: |
    #!/bin/bash
    sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils
device-mapper-multipath
    rpm -q iscsi-initiator-utils
    sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'
/etc/iscsi/iscsid.conf
    cat /etc/iscsi/initiatorname.iscsi
    sudo mpathconf --enable --with_multipathd y --find_multipaths
n
    sudo systemctl enable --now iscsid multipathd
    sudo systemctl enable --now iscsi
securityContext:
  privileged: true
hostPID: true
containers:
- name: wait
  image: k8s.gcr.io/pause:3.1
hostPID: true
hostNetwork: true
tolerations:
- effect: NoSchedule
  key: node-role.kubernetes.io/master
updateStrategy:
  type: RollingUpdate

```

Verwenden Sie die folgende yaml-Datei, um die dreigesichtige Backend-Konfiguration für die Verwendung von ONTAP-san-Speicher zu erstellen

Trident Backend für iSCSI

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: <username>
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-san
spec:
  version: 1
  storageDriverName: ontap-san
  managementLIF: <management LIF>
  backendName: ontap-san
  svm: <SVM name>
  credentials:
    name: backend-tbc-ontap-san-secret

```

Verwenden Sie die folgende yaml-Datei, um eine dreilagige Konfiguration für die Verwendung von ONTAP-san-Speicher zu erstellen

Trident Storage-Klasse für iSCSI

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true

```

Installieren Sie MTV

Jetzt können Sie das Migration Toolkit for Virtualization (MTV) installieren. Beachten Sie die mitgelieferten Anweisungen ["Hier"](#) Für Hilfe bei der Installation.

Die Benutzeroberfläche des Migration Toolkit for Virtualization (MTV) ist in die OpenShift-Webkonsole integriert.

Sie können sich darauf beziehen ["Hier"](#) So verwenden Sie die Benutzeroberfläche für verschiedene Aufgaben.

Quellanbieter Erstellen

Um die RHEL VM von VMware auf OpenShift Virtualization zu migrieren, müssen Sie zunächst den Quellanbieter für VMware erstellen. Beachten Sie die Anweisungen ["Hier"](#) Um den Quellanbieter zu erstellen.

Um Ihren VMware-Quellanbieter zu erstellen, benötigen Sie Folgendes:

- VCenter-url
- VCenter-Anmeldedaten
- Fingerabdruck des vCenter-Servers
- VDDK-Bild in einem Repository

Beispiel für die Erstellung eines Quellanbieters:

Select provider type *

vm vSphere

Provider resource name *

vmware-source ✓

Unique Kubernetes resource name identifier

URL *

URL of the vCenter SDK endpoint. Ensure the URL includes the "/sdk" path. For example: https://vCenter-host-example.com/sdk ✓

VDDK init image:

docker.repo.eng.netapp.com/banum/vddk:801 ✓

VDDK container image of the provider, when left empty some functionality will not be available

Username *

administrator@vsphere.local ✓

vSphere REST API user name.

Password *

..... ✓

vSphere REST API password credentials.

SSHA-1 fingerprint *

The provider currently requires the SHA-1 fingerprint of the vCenter Server's TLS certificate in all circumstances. vSphere calls this the server's thumbprint. ✓

Skip certificate validation



Das Migration Toolkit for Virtualization (MTV) verwendet das VMware Virtual Disk Development Kit (VDDK) SDK zur Beschleunigung der Übertragung virtueller Laufwerke von VMware vSphere. Daher wird dringend empfohlen, ein VDDK-Bild zu erstellen, obwohl dies optional ist. Um diese Funktion zu nutzen, laden Sie das VMware Virtual Disk Development Kit (VDDK) herunter, erstellen ein VDDK-Image und schieben das VDDK-Image in Ihre Bildregistrierung.

Befolgen Sie die Anweisungen ["Hier"](#) So erstellen und verschieben Sie das VDDK-Image in eine Registrierung, auf die über den OpenShift-Cluster zugegriffen werden kann.

Zielanbieter erstellen

Der Host-Cluster wird automatisch hinzugefügt, da der OpenShift-Virtualisierungsanbieter der Quellanbieter ist.

Migrationsplan Erstellen

Befolgen Sie die Anweisungen ["Hier"](#) Um einen Migrationsplan zu erstellen.

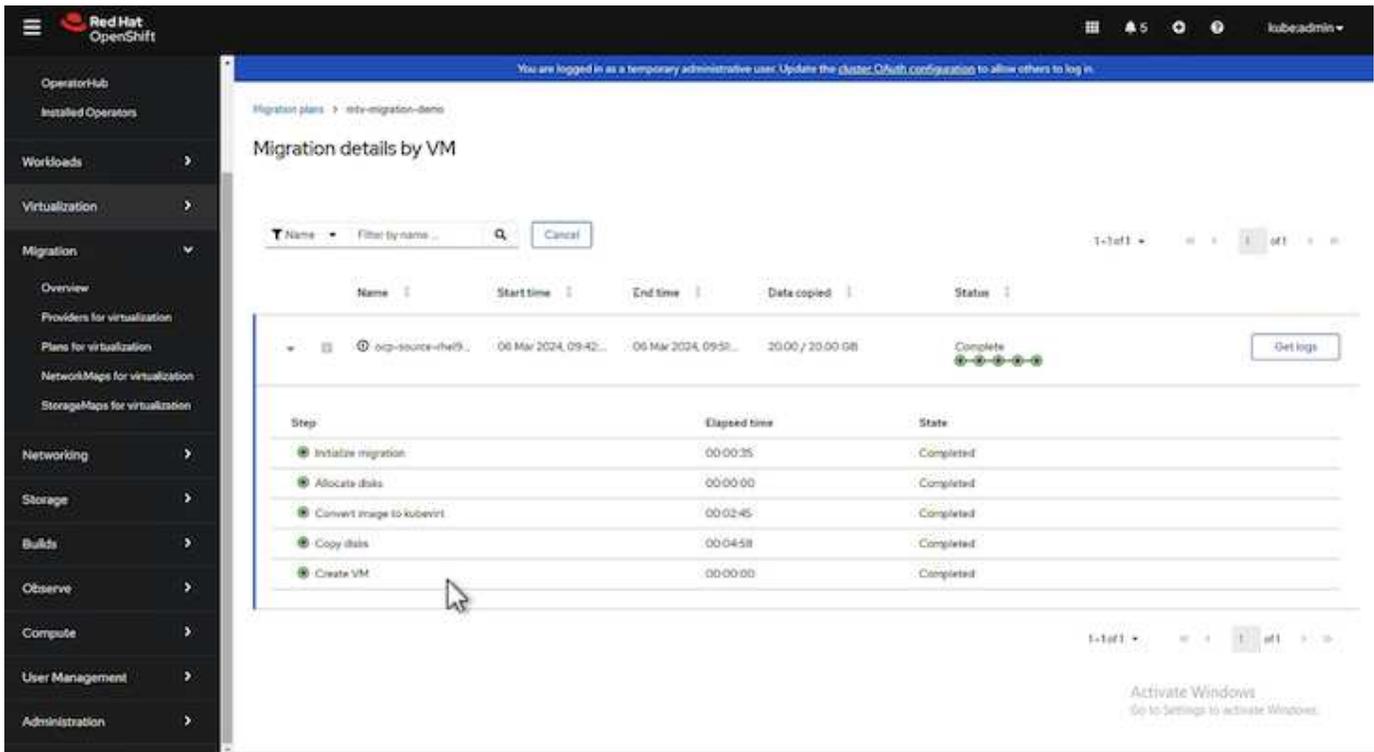
Wenn Sie einen Plan erstellen, müssen Sie Folgendes erstellen, falls noch nicht erstellt:

- Eine Netzwerkzuordnung, um das Quellnetzwerk dem Zielnetzwerk zuzuordnen.
 - Eine Speicherzuordnung, um den Quell-Datastore der Ziel-Storage-Klasse zuzuordnen. Hierfür können Sie sich für eine ontap-san-Storage-Klasse entscheiden.
- Sobald der Migrationsplan erstellt ist, sollte der Status des Plans **Ready** anzeigen und Sie sollten nun **Start** des Plans haben.

The screenshot shows the OpenShift MTV interface. The left sidebar contains navigation options: OperatorHub, Installed Operators, Workloads, Virtualization, Migration (selected), Overview, Providers for virtualization, Plans for virtualization (selected), NetworkMaps for virtualization, StorageMaps for virtualization, and Networking. The main content area displays a table of migration plans under the heading 'Plans'. The table has columns for Name, Source, Target, VMs, Status, and Description. The first plan, 'mtv-migration-demo', is in a 'Ready' state and has a 'Start' button next to it. The other plans are in 'Succeeded' or 'Failed' states.

Name	Source	Target	VMs	Status	Description
mtv-migration-demo	vmware	host	1	Ready	Plan for migrating VM to OpenShift Virt...
vmware-ovs-migration	vmware2	host	1	Succeeded	Migrating RHEL 9 vm to OpenShift Virtu...
vmware-ovs-migration-plan1	vmware2	host	1	Succeeded	1 of 1 VMs migrated
vmware-ovs-migration-plan2	vmware2	host	1	Succeeded	migrating RHEL 9 vm using ONTAP NFS...

Durch Klicken auf **Start** wird eine Reihe von Schritten durchlaufen, um die Migration der VM abzuschließen.



Wenn alle Schritte abgeschlossen sind, können Sie die migrierten VMs sehen, indem Sie im Navigationsmenü auf der linken Seite unter **Virtualisierung** auf **virtuelle Maschinen** klicken. Anweisungen für den Zugriff auf die virtuellen Maschinen werden bereitgestellt ["Hier"](#).

Sie können sich bei der virtuellen Maschine anmelden und den Inhalt der postgresql-Datenbanken überprüfen. Die Datenbanken, Tabellen und die Einträge in der Tabelle sollten identisch sein mit denen, die auf der Quell-VM erstellt wurden.

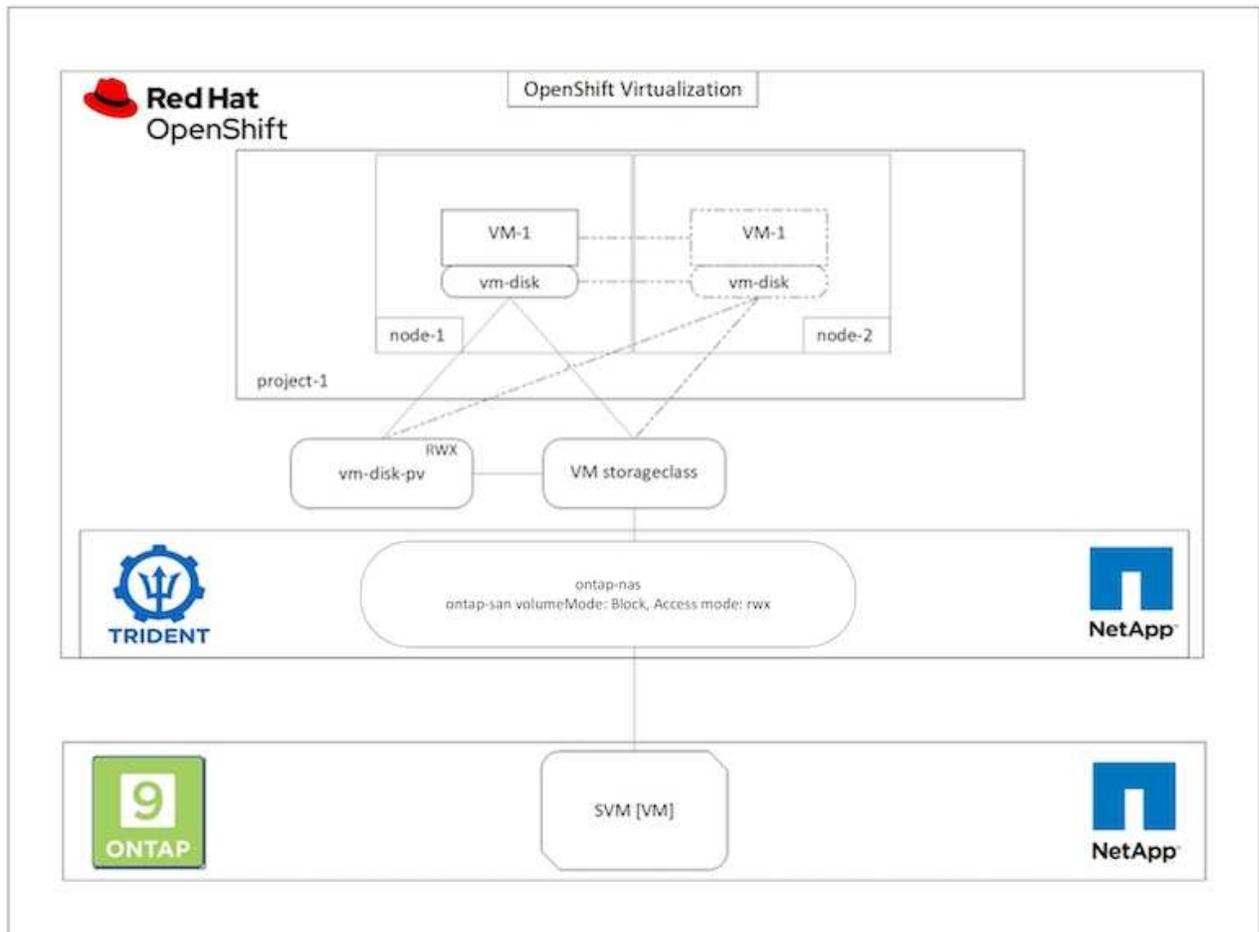
Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

Dieser Abschnitt zeigt, wie eine virtuelle Maschine in OpenShift Virtualization zwischen Knoten im Cluster migriert wird.

VM-Live-Migration

Live Migration ist ein Prozess, bei dem eine VM-Instanz in einem OpenShift-Cluster ohne Ausfallzeit von einem Node zu einem anderen migriert wird. Damit die Live-Migration in einem OpenShift-Cluster funktioniert, müssen VMs mit Shared ReadWriteManche-Zugriffsmodus an PVCs gebunden sein. Trident-Back-Ends, die mit ONTAP-nas-Treibern konfiguriert sind, unterstützen den RWX-Zugriffsmodus für die Dateisystemprotokolle nfs und smb. Siehe Dokumentation ["Hier"](#). Trident-Back-Ends, die mit ONTAP-san-Treibern konfiguriert sind, unterstützen den RWX Zugriffsmodus für Block-Volume-Modus für iSCSI- und NVMe/TCP-Protokolle. Siehe Dokumentation ["Hier"](#).

Damit die Live-Migration erfolgreich sein kann, müssen die VMs mithilfe von ontap-nas oder Storage-Klassen von ontap-san (VolumeMode: Block) mit PVCs mit Festplatten (Boot-Disks und zusätzliche Hot-Plug-Disks) bereitgestellt werden. Bei der Erstellung der PVCs erstellt Trident ONTAP Volumes in einer SVM, die NFS-aktiviert oder iSCSI aktiviert ist.



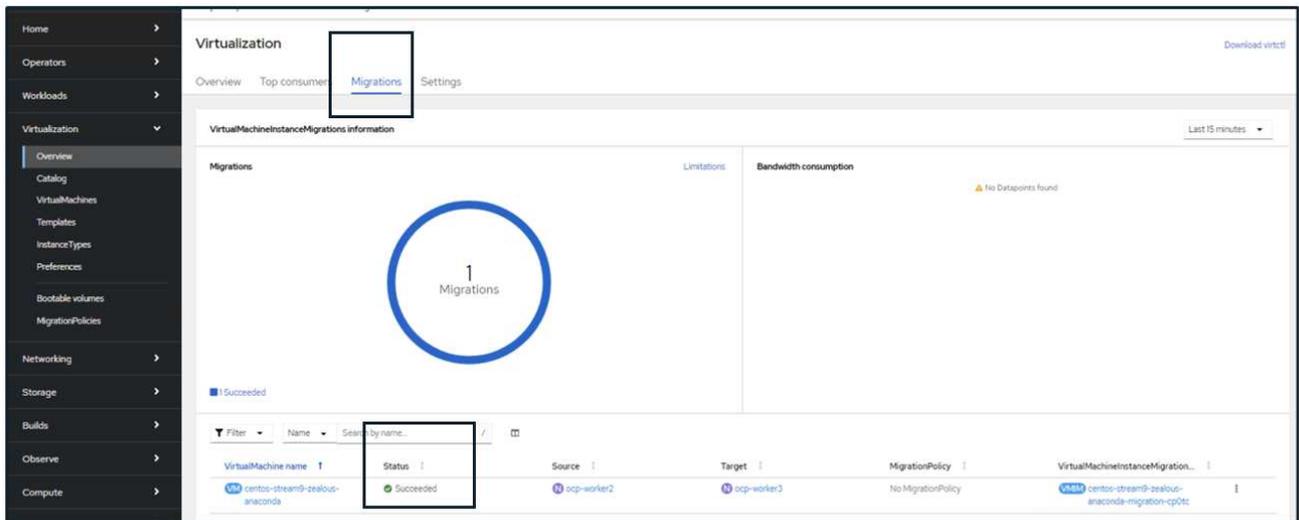
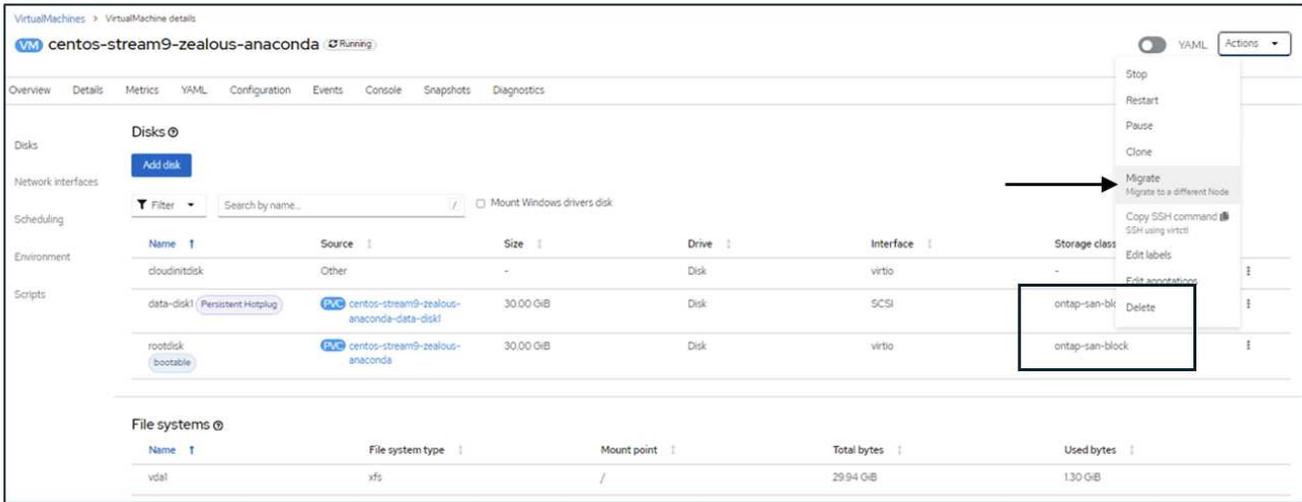
So führen Sie eine Live-Migration einer zuvor erstellten VM durch, die sich in einem laufenden Zustand befindet:

1. Wählen Sie die VM aus, die Sie live migrieren möchten.
2. Klicken Sie auf die Registerkarte **Konfiguration**.
3. Stellen Sie sicher, dass alle Festplatten der VM mithilfe von Speicherklassen erstellt werden, die den RWX-Zugriffsmodus unterstützen.
4. Klicken Sie auf **actions** in der rechten Ecke und wählen Sie dann **Migrate**.
5. Um sich den Verlauf der Migration anzusehen, gehen Sie auf der linken Seite zu Virtualisierung > Übersicht und klicken Sie dann auf die Registerkarte **Migrationen**.

Die Migration der VM wird von **Pending** zu **Scheduling** zu **succeed** übergehen



Eine VM-Instanz in einem OpenShift-Cluster wird automatisch auf einen anderen Node migriert, wenn der ursprüngliche Node in den Wartungsmodus versetzt wird, wenn die „vertreiben“-Strategie auf „LiveMigrate“ gesetzt ist.

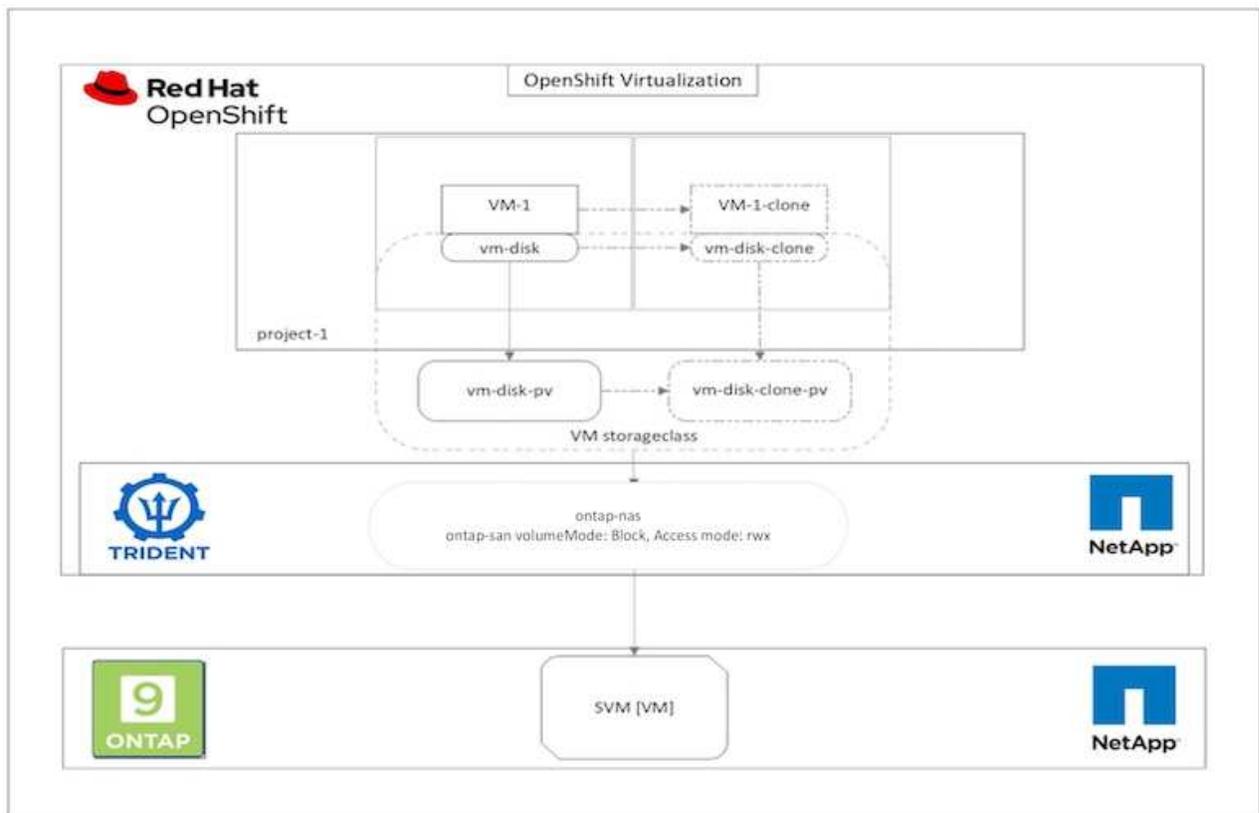


Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

In diesem Abschnitt wird das Klonen einer virtuellen Maschine mit Red hat OpenShift Virtualization beschrieben.

Klonen von VMs

Das Klonen einer vorhandenen VM in OpenShift wird durch die Volume-CSI-Klonfunktion von Trident erreicht. Das Klonen von CSI-Volumes ermöglicht die Erstellung eines neuen PVC mithilfe einer vorhandenen PVC als Datenquelle durch die Duplizierung des PV. Nach der Erstellung des neuen PVC funktioniert es als separate Einheit und ohne Verbindung zur PVC-Quelle oder Abhängigkeit.



Das Klonen von CSI-Volumes unterliegt bestimmten Einschränkungen:

1. Die PVC-Quelle und das Ziel-PVC müssen sich im selben Projekt befinden.
2. Klonen wird in derselben Storage-Klasse unterstützt.
3. Das Klonen kann nur dann durchgeführt werden, wenn Quell- und Ziel-Volumes dieselbe VolumeMode-Einstellung verwenden. Ein Block-Volume kann beispielsweise nur auf einem anderen Block-Volume geklont werden.

VMs in einem OpenShift-Cluster können auf zwei Arten geklont werden:

1. Durch Herunterfahren der Quell-VM
2. Indem die Quell-VM verfügbar bleibt

Durch Herunterfahren der Quell-VM

Das Klonen einer vorhandenen VM durch Herunterfahren der VM ist eine native OpenShift-Funktion, die mit Unterstützung von Trident implementiert wird. Führen Sie folgende Schritte durch, um eine VM zu klonen.

1. Navigieren Sie zu Workloads > Virtualisierung > Virtual Machines und klicken Sie neben der zu klonenden virtuellen Maschine auf die Auslassungspunkte.
2. Klicken Sie auf Virtual Machine klonen, und geben Sie die Details für die neue VM ein.

Clone Virtual Machine

Name *

rhel8-short-frog-clone

Description

Namespace *

default

Start virtual machine on clone

Configuration

Operating System

Red Hat Enterprise Linux 8.0 or higher

Flavor

Small: 1 CPU | 2 GiB Memory

Workload Profile

server

NICs

default - virtio

Disks

cloudinitdisk - cloud-init disk

rootdisk - 20Gi - basic



The VM rhel8-short-frog is still running. It will be powered off while cloning.

Cancel

Clone Virtual Machine

3. Klicken Sie auf Virtual Machine klonen. Dadurch wird die Quell-VM heruntergefahren und die Erstellung der Klon-VM initiiert.
4. Nach Abschluss dieses Schritts können Sie auf den Inhalt der geklonten VM zugreifen und diesen überprüfen.

Indem die Quell-VM verfügbar bleibt

Eine vorhandene VM kann auch geklont werden, indem das vorhandene PVC der Quell-VM geklont und dann mithilfe des geklonten PVC eine neue VM erstellt wird. Bei dieser Methode müssen Sie die Quell-VM nicht herunterfahren. Führen Sie die folgenden Schritte aus, um eine VM zu klonen, ohne sie herunterzufahren.

1. Navigieren Sie zu Storage > PersistenzVolumeClaims und klicken Sie auf die Ellipse neben dem PVC, das an die Quell-VM angehängt ist.
2. Klicken Sie auf PVC klonen und geben Sie die Details für das neue PVC an.

Clone

Name *

Access Mode *

Single User (RWO) Shared Access (RWX) Read Only (ROX)

Size *

GiB ▼

PVC details

Namespace

NS default

Storage Class

SC basic

Requested capacity

20 GiB

Used capacity

2.2 GiB

Access mode

Shared Access (RWX)

Volume mode

Filesystem

Cancel

Clone

3. Klicken Sie dann auf Klonen. Dadurch wird ein PVC für die neue VM erstellt.
4. Navigieren Sie zu Workloads > Virtualisierung > Virtuelle Maschinen, und klicken Sie auf Erstellen > mit YAML.
5. Hängen Sie im Abschnitt Spec > Template > Spec > Volumes die geklonte PVC an anstatt der Container-Disk. Geben Sie alle anderen Details für die neue VM nach Ihren Anforderungen an.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvv-clone
```

6. Klicken Sie auf Erstellen, um die neue VM zu erstellen.
7. Nachdem die VM erfolgreich erstellt wurde, zugreifen und überprüfen Sie, ob die neue VM ein Klon der Quell-VM ist.

Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

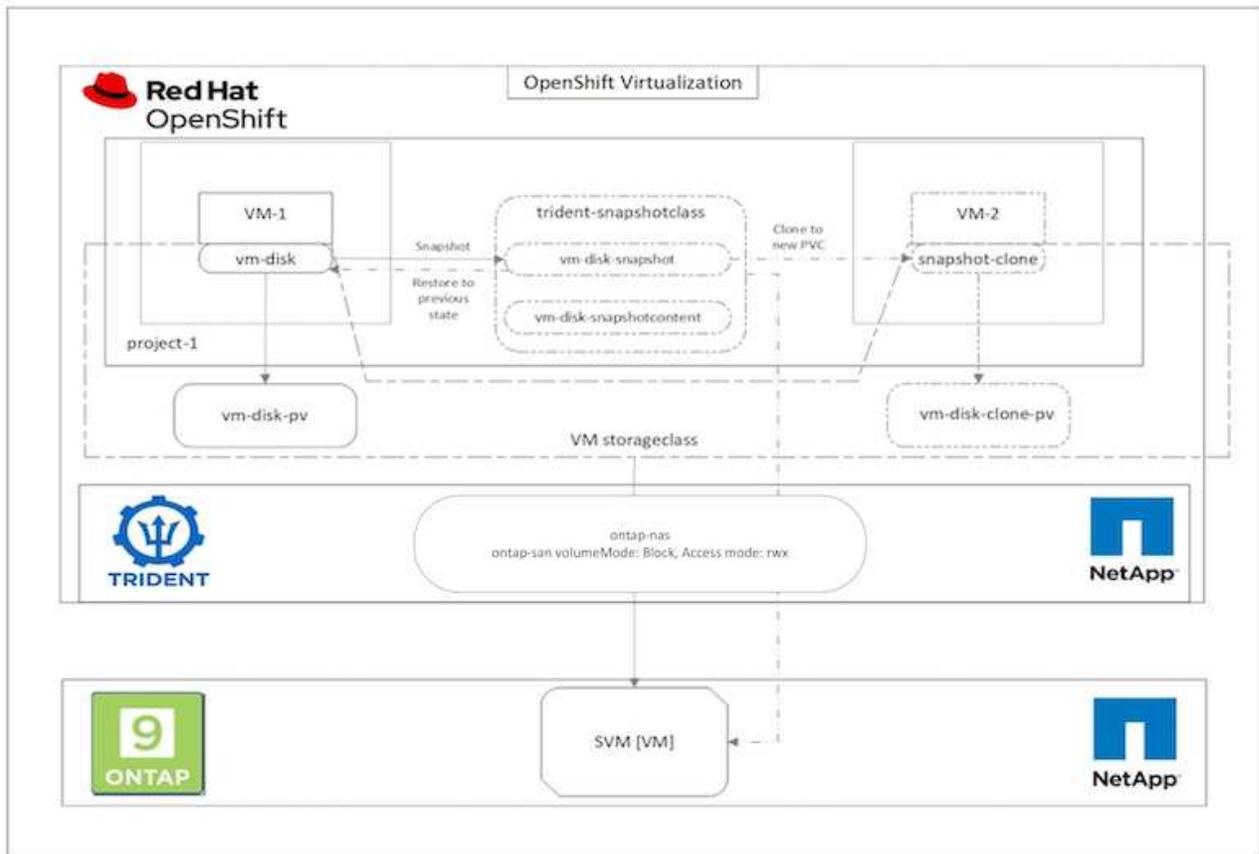
In diesem Abschnitt wird erläutert, wie Sie eine virtuelle Maschine aus einem Snapshot mit Red hat OpenShift Virtualization erstellen.

Erstellen Sie eine VM aus einem Snapshot

Mit Trident und Red hat OpenShift können Benutzer einen Snapshot eines persistenten Volumes in von der IT bereitgestellten Storage-Klassen erstellen. Mit dieser Funktion können Benutzer eine zeitpunktgenaue Kopie eines Volumes erstellen oder dasselbe Volume in einen vorherigen Zustand zurückversetzen. Ob Rollback, Klonen oder Datenwiederherstellung – lassen sich in unterschiedlichen Anwendungsfällen einsetzen.

Für Snapshot-Vorgänge in OpenShift müssen die Ressourcen VolumeSnapshotClass, VolumeSnapshot und VolumeSnapshotContent definiert werden.

- Ein VolumeSnapshotContent ist der tatsächliche Snapshot, der von einem Volume im Cluster erstellt wurde. Es handelt sich um eine Cluster-weite Ressource, die dem PersistentVolume für Storage gleicht.
- Ein VolumeSnapshot ist eine Anforderung zum Erstellen des Snapshots eines Volumes. Es ist analog zu einem PersistentVolumeClaim.
- Mit VolumeSnapshotClass kann der Administrator verschiedene Attribute für einen VolumeSnapshot festlegen. Damit können Sie unterschiedliche Attribute für verschiedene Snapshots haben, die vom selben Volume erstellt wurden.



Um einen Snapshot einer VM zu erstellen, führen Sie die folgenden Schritte aus:

1. Erstellen Sie eine VolumeSnapshotKlasse, die dann zum Erstellen eines VolumeSnapshots verwendet werden kann. Navigieren Sie zu Storage > VolumeSnapshotClasses und klicken Sie auf Create VolumeSnapshotClass.
2. Geben Sie den Namen der Snapshot-Klasse ein, geben Sie `csi.trident.netapp.io` für den Treiber ein, und klicken Sie auf Erstellen.

```
1  apiVersion: snapshot.storage.k8s.io/v1
2  kind: VolumeSnapshotClass
3  metadata:
4    name: trident-snapshot-class
5  driver: csi.trident.netapp.io
6  deletionPolicy: Delete
7
```

[Create](#)[Cancel](#)[Download](#)

- Identifizieren Sie die PVC, die an die Quell-VM angeschlossen ist, und erstellen Sie dann einen Snapshot dieser PVC. Navigieren Sie zu `Storage > VolumeSnapshots` und klicken Sie auf `VolumeSnapshots erstellen`.
- Wählen Sie das PVC aus, für das Sie den Snapshot erstellen möchten, geben Sie den Namen des Snapshots ein oder übernehmen Sie den Standardwert, und wählen Sie die entsprechende `VolumeSnapshotClass` aus. Klicken Sie dann auf `Erstellen`.

Create VolumeSnapshot

[Edit YAML](#)

PersistentVolumeClaim *

PVC rhel8-short-frog-rootdisk-28dvv

Name *

rhel8-short-frog-rootdisk-28dvv-snapshot

Snapshot Class *

VSC trident-snapshot-class

[Create](#)[Cancel](#)

- Dadurch wird die Momentaufnahme des PVC zu diesem Zeitpunkt erstellt.

Erstellen Sie aus dem Snapshot eine neue VM

1. Stellen Sie zuerst den Snapshot in einer neuen PVC wieder her. Navigieren Sie zu „Storage“ > „VolumeSnapshots“, klicken Sie auf die Ellipsen neben dem Snapshot, den Sie wiederherstellen möchten, und klicken Sie auf „als neues PVC wiederherstellen“.
2. Geben Sie die Details des neuen PVC ein, und klicken Sie auf Wiederherstellen. Dadurch wird ein neues PVC erzeugt.

Restore as new PVC

When restore action for snapshot **rhel8-short-frog-rootdisk-28dvb-snapshot** is finished a new crash-consistent PVC copy will be created.

Name *

rhel8-short-frog-rootdisk-28dvb-snapshot-restore

Storage Class *

SC basic

Access Mode *

Single User (RWO) Shared Access (RWX) Read Only (ROX)

Size *

20

GiB

VolumeSnapshot details

Created at

 May 21, 12:46 am

Namespace

 default

Status

 Ready

API version

snapshot.storage.k8s.io/v1

Size

20 GiB

3. Erstellen Sie dann eine neue VM aus diesem PVC. Navigieren Sie zu Virtualisierung > Virtuelle Maschinen,

und klicken Sie auf Erstellen > mit YAML.

4. Geben Sie im Abschnitt Spec > Template > spec > Volumes das neue PVC an, das aus Snapshot erstellt wurde, anstatt von der Container-Festplatte aus. Geben Sie alle anderen Details für die neue VM nach Ihren Anforderungen an.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvh-snapshot-restore
```

5. Klicken Sie auf Erstellen, um die neue VM zu erstellen.
6. Nachdem die VM erfolgreich erstellt wurde, können Sie auf die neue VM zugreifen und diese überprüfen, ob sie denselben Status hat wie die VM, deren PVC zum Zeitpunkt der Snapshot-Erstellung verwendet wurde.

Bereitstellung auf ROSA mit FSxN

Bereitstellung von Red hat OpenShift Virtualization mit FSxN auf ROSA

Überblick

Dieser Abschnitt enthält Details zum Einrichten von FSX für NetApp ONTAP als Standard-Speicherklasse für den ROSA-Cluster und Erstellen einer virtuellen Maschine, die FSX ONTAP-Speicher für seine Volumes nutzt. Wir werden auch prüfen, wie eine Verbindung zur Virtual Machine mit den Gastmeldeinformationen hergestellt wird, und die VM neu starten. Und schließlich führen wir eine Live-Migration der virtuellen Maschine vom aktuellen Knoten zu einem neuen Knoten durch. Nach einem VM-Neustart und der Live-Migration werden wir den Inhalt des Plattenspeichers untersuchen.

Voraussetzungen

- ["AWS Konto"](#)
- ["Ein Red hat Konto"](#)
- IAM-Benutzer ["Mit entsprechenden Berechtigungen"](#) zum Erstellen und Zugreifen auf ROSA-Cluster
- ["AWS CLI"](#)
- ["ROSA CLI"](#)
- ["OpenShift -Befehlszeilenschnittstelle"](#) (oc)
- ["Helm 3-Dokumentation"](#)
- ["EIN HCP-ROSA-CLUSTER"](#) (Mit mindestens 3 Bare-Metal-Worker-Nodes)
- ["OpenShift Virtualization ist auf ROSA Cluster installiert"](#)
- ["Zugriff auf die Red hat OpenShift -Webkonsole"](#)

Ersteinrichtung

Dieser Abschnitt zeigt, wie die Standard-Speicherklasse als Trident-csi und die Standard-VolumeSnapshotKlasse als FSX Volumes-Snapshot-Klasse eingerichtet wird. Anschließend wird gezeigt, wie Sie eine VM aus einer Vorlage erstellen und dann mit den Gast-Zugangsdaten verbinden und sich anmelden.

Stellen Sie sicher, dass die Standardspeicherklasse auf Trident-csi gesetzt ist



Name	Provisioner	Reclaim policy
SC gp2-csi	ebs.csi.aws.com	Delete
SC gp3-csi	ebs.csi.aws.com	Delete
SC trident-csi - Default	csi.trident.netapp.io	Retain

Stellen Sie sicher, dass die StandardvolumeSnapShotClasses wie gezeigt eingestellt sind



Name	Driver	Deletion policy
VSC csi-aws-vsc	ebs.csi.aws.com	Delete
VSC fsx-snapclass - Default	csi.trident.netapp.io	Delete

Wenn die Standardeinstellungen nicht festgelegt sind, können Sie sie entweder über die Konsole oder über die Befehlszeile einrichten

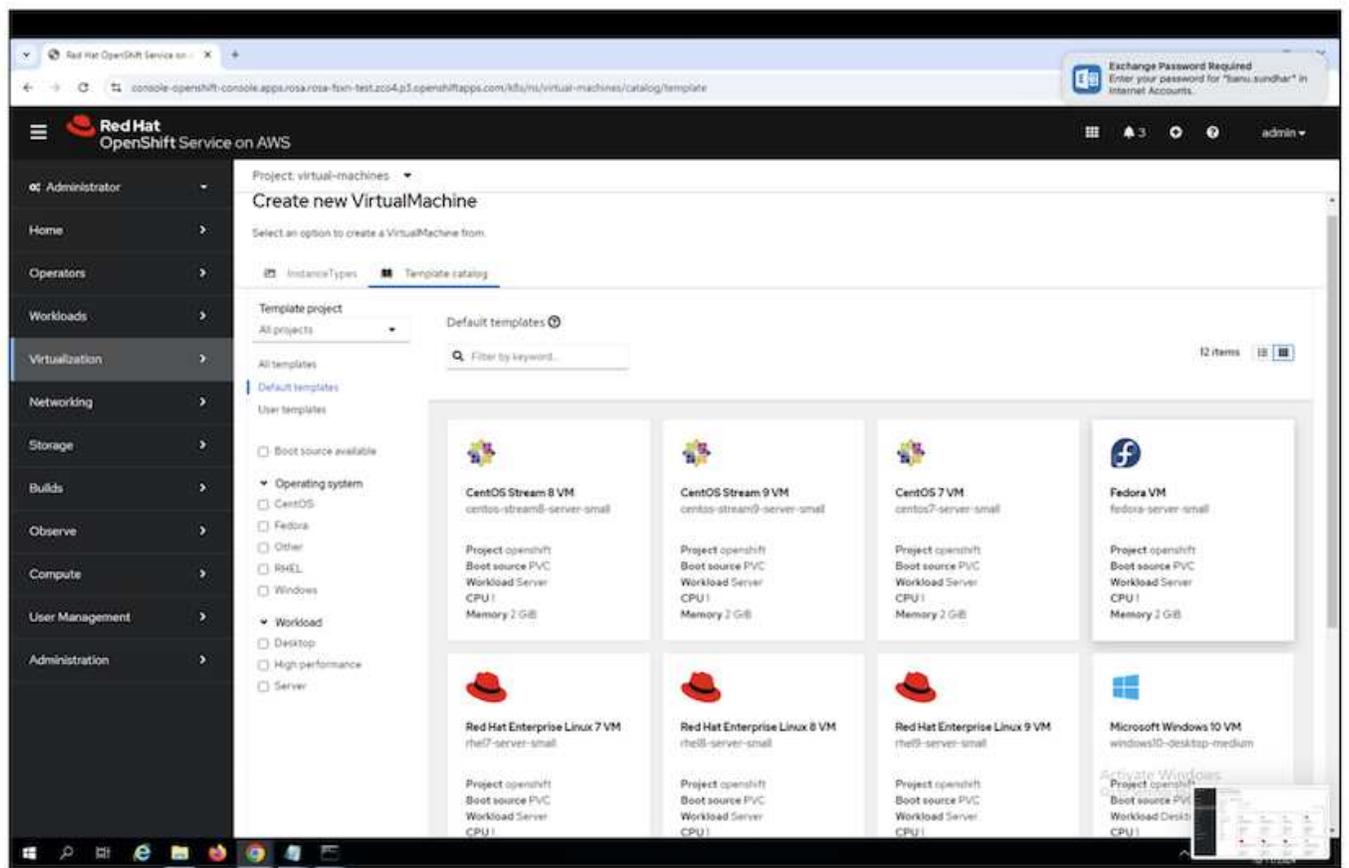
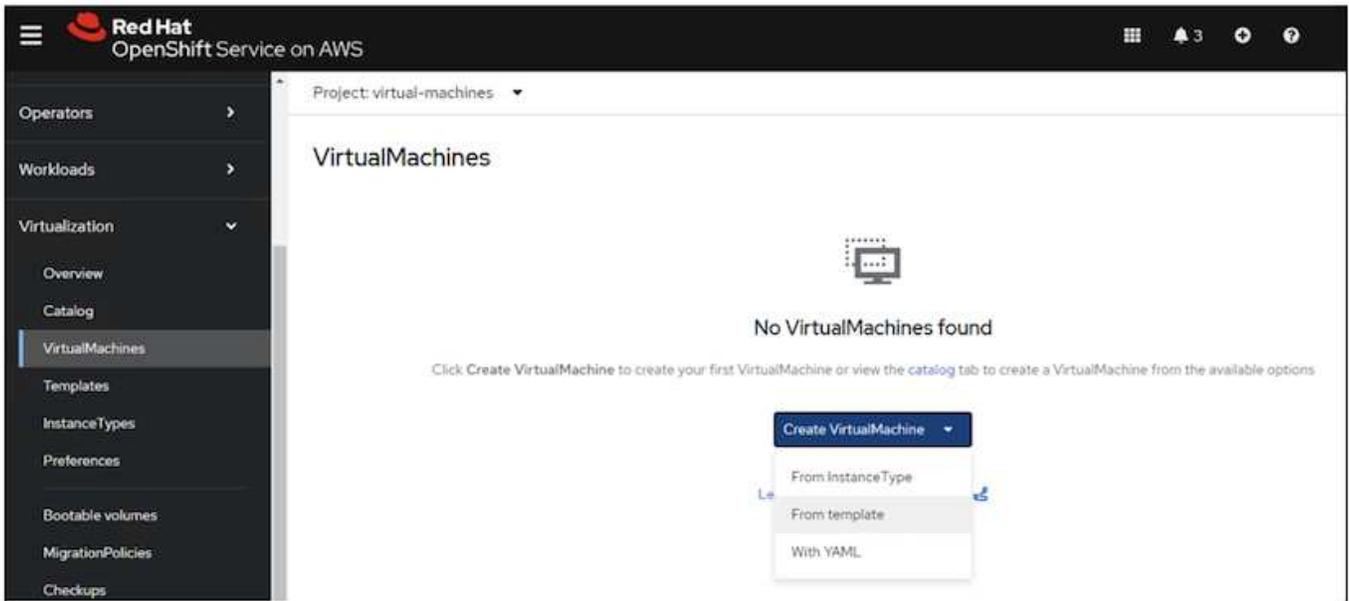
```
$ oc patch storageclass trident-csi -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "true"}}}'
```

```
$ oc patch VolumeSnapshotClasses fsx-snapclass -p '{"metadata": {"annotations": {"snapshot.storage.kubernetes.io/is-default-class": "true"}}}'
```

Erstellen Sie eine VM aus der Vorlage

Erstellen Sie eine VM aus einer Vorlage mithilfe der Webkonsole. Erstellen Sie über den RedHat OpenShiftService auf der AWS-Konsole eine virtuelle Maschine. Im Cluster sind Vorlagen verfügbar, die zum Erstellen der VM verwendet werden können. In der Abbildung unten wählen wir Fedora VM aus dieser Liste aus. Geben Sie der VM einen Namen, und klicken Sie dann auf **Anpassung der virtuellen Maschine**. Wählen Sie die Registerkarte **Disks** und klicken Sie auf **Add Disks**. Ändern Sie den Namen der Festplatte vorzugsweise in etwas aussagekräftiges, stellen Sie sicher, dass **Trident-csi** für die Speicherklasse ausgewählt ist. Klicken Sie auf **Speichern**. Klicken Sie auf **Create VirtualMachine**

Nach einigen Minuten befindet sich die VM im laufenden Zustand





Template info

Operating system

Fedora VM

Workload type

Server (default)

Description

Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be available.

Documentation

[Refer to documentation](#)

CPU | Memory

1 CPU | 2 GiB Memory

Network interfaces (1)

Name	Network	Type
default	Pod networking	Masquerade

Disks (2)

Name	Drive	Size
rootdisk	Disk	30 GiB
cloudinitdisk	Disk	-

Storage

Boot from CD

Disk source *

Template default

Disk size *

- 30 + GiB

Drivers

Mount Windows drivers disk

[Optional parameters](#)

Quick create VirtualMachine

VirtualMachine name *

fedora-vm1

Project Public SSH key

default Not configured

Start this VirtualMachine after creation

Quick create VirtualMachine

Customize VirtualMachine

Activate Windows

Go to Settings to activate Windows.

Cancel

Customize and create VirtualMachine YAML

Template: Fedora VM

- Overview
- YAML
- Scheduling
- Environment
- Network interfaces
- Disks**
- Scripts
- Metadata

Add disk

Filter Search by name... Mount Windows drivers disk

Name ↑	Source ↓	Size ↓	Drive ↓	Interface ↓	Storage class ↓	
cloudinitdisk	Other	-	Disk	virtio	-	⋮
rootdisk bootable	Other	30 GiB	Disk	virtio	-	⋮

Add disk



Use this disk as a boot source

Name *

fedora-vm1-disk1

Source *

Empty disk (blank)

PersistentVolumeClaim size *

-

30

+

GiB

▼

Type

Disk

Hot plug is enabled only for "Disk" type

Interface *

VirtIO

Hot plug is enabled only for "SCSI" interface

StorageClass

trident-csi

Save

Cancel

Project: virtual-machines

VirtualMachines > VirtualMachine details

VM fedora-vm1 Running

Overview Metrics YAML Configuration Events Console Snapshots Diagnostics

Details

Name: fedora-vm1

Status: Running

Created: Oct 11, 2024, 1:46 PM (4 minutes ago)

Operating system: Fedora Linux 40 (Cloud Edition)

CPU | Memory: 1 CPU | 2 GiB Memory

Time zone: UTC

Template: [fedora-server-small](#)

Hostname: fedora-vm1

Machine type: pc-q35-rhel9.4.0

VNC console

Alerts (0)

General

Namespace: [virtual-machi...](#)

Node: [ip-10-10-3-191...](#)

VirtualMachineInstance: [fedora-vm1](#)

Pod: [virt-launcher-f...](#)

Owner: No owner

Snapshots (0) [Take snapshot](#)

Activate Windows
No snapshots found
Go to Settings to activate Windows.

Alle für die VM erstellten Objekte überprüfen

Die Speicherlaufwerke.

Storage (3)

Name	Drive	Size	Interface
rootdisk	Disk	31.75 GiB	virtio
cloudinitdisk	Disk	-	virtio
fedora-vm1-disk1	Disk	31.75 GiB	virtio

Die Dateisysteme der VM zeigen die Partitionen, den Typ des Dateisystems und die Mount-Punkte an.

File systems ⓘ

Name ↑	File system type ⓘ	Mount point ⓘ	Total bytes ⓘ	Used bytes ⓘ
vda2	vfat	/boot/efi	99.76 MiB	16.01 MiB
vda3	ext4	/boot	899.85 MiB	73.12 MiB
vda4	btrfs	/var	28.47 GiB	406.83 MiB
vda4	btrfs	/home	28.47 GiB	406.83 MiB
vda4	btrfs	/	28.47 GiB	406.83 MiB

2 PVCs werden für die VM erstellt, eines von der Boot-Festplatte und eines von der Hot-Plug-Festplatte.

Project: virtual-machines ▾

PersistentVolumeClaims

[Create PersistentVolumeClaim ▾](#)

Filter ▾ Name ▾ Search by name... /

Name ⓘ	Status ⓘ	PersistentVolumes ⓘ	Capacity ⓘ
 fedora-vm1	 Bound	 pvc-7d60a3cf-d4cc-47d5-8053-efbb6ae1135f	31.75 GiB
 fedora-vm1-fedora-vm1-disk1	 Bound	 pvc-a769e022-2ae5-43fb-b8a1-a40f4447c6c2	31.75 GiB

Die PVC für die Startdiskette zeigt an, dass der Zugriffsmodus ReadWriteMany und die Speicherklasse Trident-csi sind.

Project: virtual-machines

PersistentVolumeClaims > PersistentVolumeClaim details

PVC fedora-vm1 Bound

Details | YAML | Events | VolumeSnapshots

PersistentVolumeClaim details



Name
fedora-vm1

Namespace
virtual-machines

Labels Edit

- app=containerized-data-importer
- app.kubernetes.io/part-of=hyperconverged-cluster
- instancetype.kubevirt.io/default-preference=fedora
- app.kubernetes.io/version=4.15.3
- app.kubernetes.io/component=storage
- alerts.k8s.io/KubePersistentVolumeFillingUp=disabled
- app.kubernetes.io/managed-by=ncd-controller
- instancetype.kubevirt.io/default-instancetype=ul.medium
- kubevirt.io/created-by=90537934-9ba5-47b5-8caa-63c0c9e5b7f

Annotations
20 annotations

Label selector
No selector

Created at
Oct 11, 2024, 1:46 PM

Status
Bound

Requested capacity
31.75 GiB

Capacity
31.75 GiB

Used
25.09 GiB

Access modes
ReadWriteMany

Volume mode
Filesystem

StorageClasses
trident-csi

PersistentVolumes
pvc-70b0a3cf-d4cc-4765-8053-efbb6ae1035f

Activate Windows
Go to Settings to activate Windows

Ebenso zeigt die PVC für die Hot-Plug-Festplatte an, dass der Zugriffsmodus ReadWriteViele ist und die Speicherklasse Trident-csi ist.

Project: virtual-machines

PersistentVolumeClaims > PersistentVolumeClaim details

PVC fedora-vm1-fedora-vm1-disk1 Bound

Details | YAML | Events | VolumeSnapshots

PersistentVolumeClaim details

31.8 GiB
Available

Name
fedora-vm1-fedora-vm1-disk1

Namespace
virtual-machines

Labels

- alerts.k8s.io/KubePersistentVolumeFillingUp=disabled
- app=containerized-data-importer
- app.kubernetes.io/component=storage
- app.kubernetes.io/managed-by=cdi-controller
- app.kubernetes.io/part-of=hyperconverged-cluster
- app.kubernetes.io/version=4.10.3
- kubevirt.io/created-by=89537594-9ba5-47bb-8caa-03c0c90e5b7f

Annotations
15 annotations

Label selector
No selector

Created at
Oct 11, 2024, 1:46 PM

Status
Bound

Requested capacity
31.75 GiB

Capacity
31.75 GiB

Used
320 KiB

Access modes
ReadWriteMany

Volume mode
Filesystem

StorageClasses
trident-csi

PersistentVolumes
pvc-a769e022-2ae5-43fb-b8a1-a40f4447c6c2

In dem Screenshot unten sehen wir, dass der Pod für die VM den Status „running“ hat.

Pods Create Pod

Filter Name Search by name

Name	Status	Ready	Restarts	Owner	Memory	CPU	Created
virt-launcher-fedora-vm1-8fp2k	Running	1/1	0	VM fedora-vm1	595.5 MB	0.010 cores	Oct 11, 2024, 2:27 PM
virt-launcher-fedora-vm1-ko8k9	Completed	0/1	0	VM fedora-vm1	-	-	Oct 11, 2024, 2:21 PM

Hier können wir die beiden Volumes sehen, die dem VM-Pod zugeordnet sind, und die 2 damit verbundenen PVCs.

Name	Mount path	SubPath	Type	Permissions	Utilized by
private	/var/run/kubevirt-private	No subpath		Read/Write	compute
public	/var/run/kubevirt	No subpath		Read/Write	compute
ephemeral-disks	/var/run/kubevirt-ephemeral-disks	No subpath		Read/Write	compute
container-disks	/var/run/kubevirt/container-disks	No subpath		Read/Write	compute
libvirt-runtime	/var/run/libvirt	No subpath		Read/Write	compute
sockets	/var/run/kubevirt/sockets	No subpath		Read/Write	compute
rootdisk	/var/run/kubevirt-private/vmi-disks/rootdisk	No subpath	PVC fedora-vm1	Read/Write	compute
fedora-vm1-disk1	/var/run/kubevirt-private/vmi-disks/fedora-vm1-disk1	No subpath	PVC fedora-vm1-fedora-vm1-disk1	Read/Write	compute
hotplug-disks	/var/run/kubevirt/hotplug-disks	No subpath		Read/Write	compute

Verbindung zur VM herstellen

Klicken Sie auf die Schaltfläche 'Webkonsole öffnen' und melden Sie sich mit den Gast-Anmeldedaten an

The screenshot shows the OpenShift console interface for a virtual machine named 'fedora-vm1'. The VM is in a 'Running' state. The left sidebar lists various details: Name (fedora-vm1), Status (Running), Created (Oct 11, 2024, 1:46 PM), Operating system (Fedora Linux 40), CPU/Memory (1 CPU | 2 GiB Memory), Time zone (UTC), Template (fedora-server-small), Hostname (fedora-vm1), and Machine type (pc-q35-rhel9.4.0). The main area displays a 'VNC console' window which is currently blank with a play button in the center. At the bottom of the console area, there is a button labeled 'Open web console' with an external link icon, which is highlighted with a blue box.



Geben Sie die folgenden Befehle ein

```
$ df (to display information about the disk space usage on a file system).
```

```
$ dd if=/dev/urandom of=random.dat bs=1M count=10240 (to create a file called random.dat in the home dir and fill it with random data).
```

Die Festplatte ist mit 11 GB Daten gefüllt.

```
[fedora@fedora-vm1 ~]$  
[fedora@fedora-vm1 ~]$ df .  
Filesystem      1K-blocks    Used Available Use% Mounted on  
/dev/uda4        30327788 10939828 18943548 37% /home  
[fedora@fedora-vm1 ~]$ dd if=/dev/urandom of=random.dat bs=1M count=10240  
10240+0 records in  
10240+0 records out  
10737418240 bytes (11 GB, 10 GiB) copied, 35.8159 s, 300 MB/s  
[fedora@fedora-vm1 ~]$ df  
Filesystem      1K-blocks    Used Available Use% Mounted on  
/dev/uda4        30327788 9699188 20190780 33% /home  
[fedora@fedora-vm1 ~]$ ls  
random.dat  
[fedora@fedora-vm1 ~]$
```

Verwenden Sie vi, um eine Beispieltextdatei zu erstellen, die wir zum Testen verwenden werden.

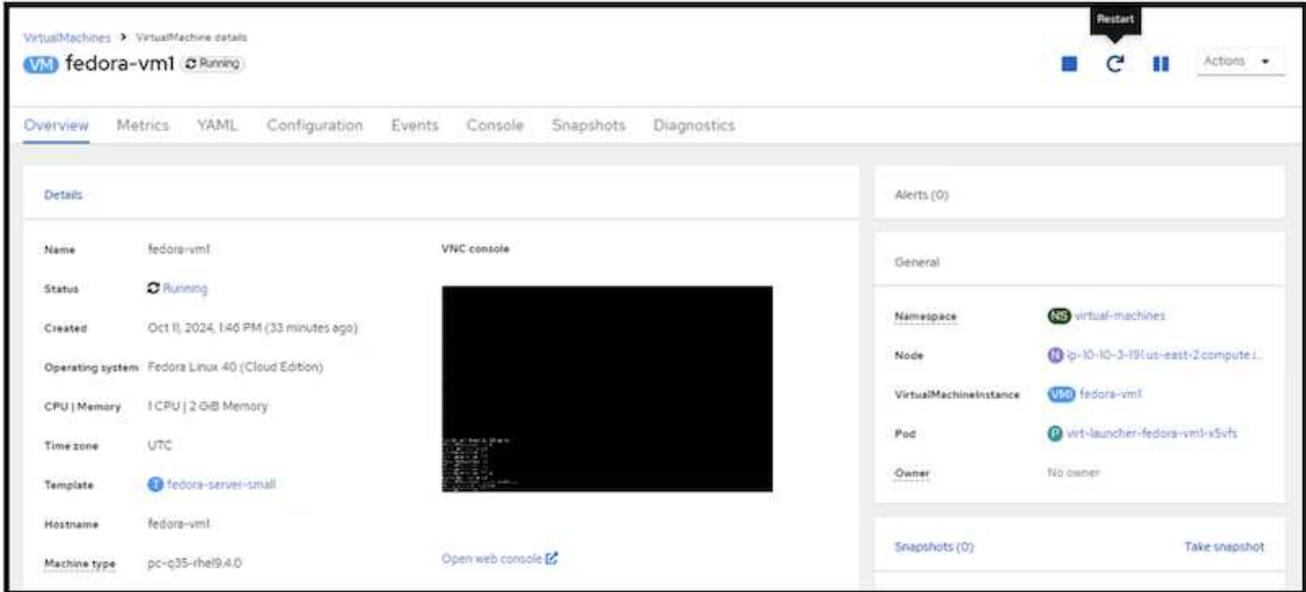
```
[fedora@fedora-vm1 ~]$ ls  
random.dat sample.txt  
[fedora@fedora-vm1 ~]$ cat sample.txt  
This is a sample text file.  
[fedora@fedora-vm1 ~]$
```

Workflows

VM neu starten

In diesen Abschnitten werden wir einen VM-Neustart durchführen und dann den Inhalt der Platten untersuchen.

Klicken Sie auf die Schaltfläche Neustart.



Die VM kehrt mit exakt den gleichen Dateisystemen, PVCs und Dateien in den Dateisystemen in den Ausführungszustand zurück

Name	File system type	Mount point	Total bytes	Used bytes
vda2	vfat	/boot/efi	99.76 MiB	16.01 MiB
vda3	ext4	/boot	899.85 MiB	73.12 MiB
vda4	btrfs	/var	28.50 GiB	10.43 GiB
vda4	btrfs	/home	28.50 GiB	10.43 GiB
vda4	btrfs	/	28.50 GiB	10.43 GiB

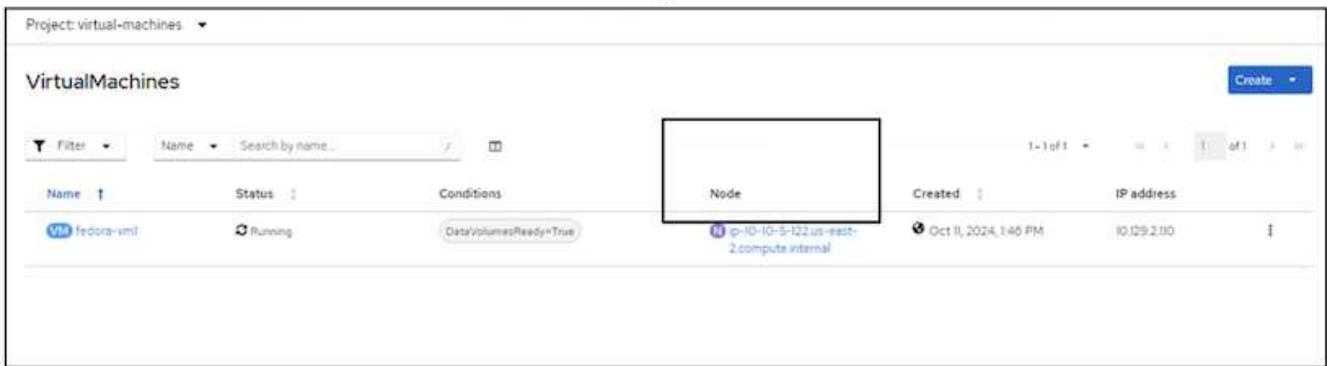
```
[fedora@fedora-vm1 ~]# ls
random.dat  sample.txt
[fedora@fedora-vm1 ~]# df .
Filesystem      1K-blocks      Used Available Use% Mounted on
/dev/vda4      30327788 10948176 18935632  37% /home
[fedora@fedora-vm1 ~]# _
```

```
[fedora@fedora-vm1 ~]$ ls
random.dat  sample.txt
[fedora@fedora-vm1 ~]$ cat sample.txt
This is a sample text file.
[fedora@fedora-vm1 ~]$
```

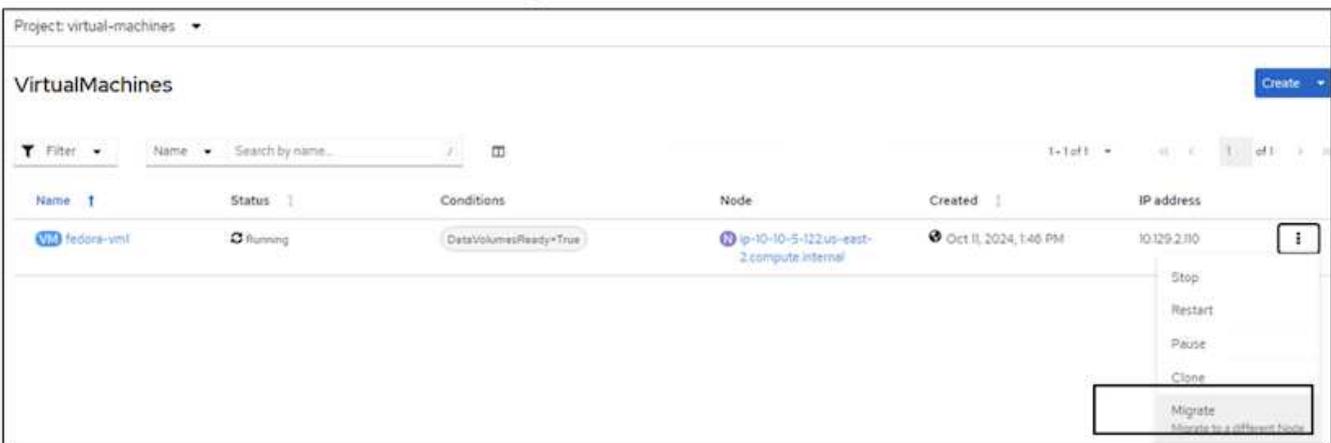
VM-Live-Migration

In diesen Abschnitten führen wir eine VM-Live-Migration durch und untersuchen dann den Inhalt der Festplatten. Live-Migration bezieht sich auf das Verschieben einer laufenden Virtual Machine (VM) von einem physischen Host auf einen anderen, ohne den normalen Betrieb zu unterbrechen oder Ausfallzeiten oder andere negative Auswirkungen für den Endbenutzer zu verursachen. Live-Migration ist ein wichtiger Schritt in der Virtualisierung. Damit kann eine gesamte VM mit einem laufenden Betriebssystem (OS), Arbeitsspeicher, Storage und Netzwerk-Konnektivität von ihrem aktuellen Node zum Ziel verschoben werden. Nachfolgend sehen Sie, wie eine Live Migration der VM vom aktuellen Knoten zu einem neuen Knoten durchgeführt wird.

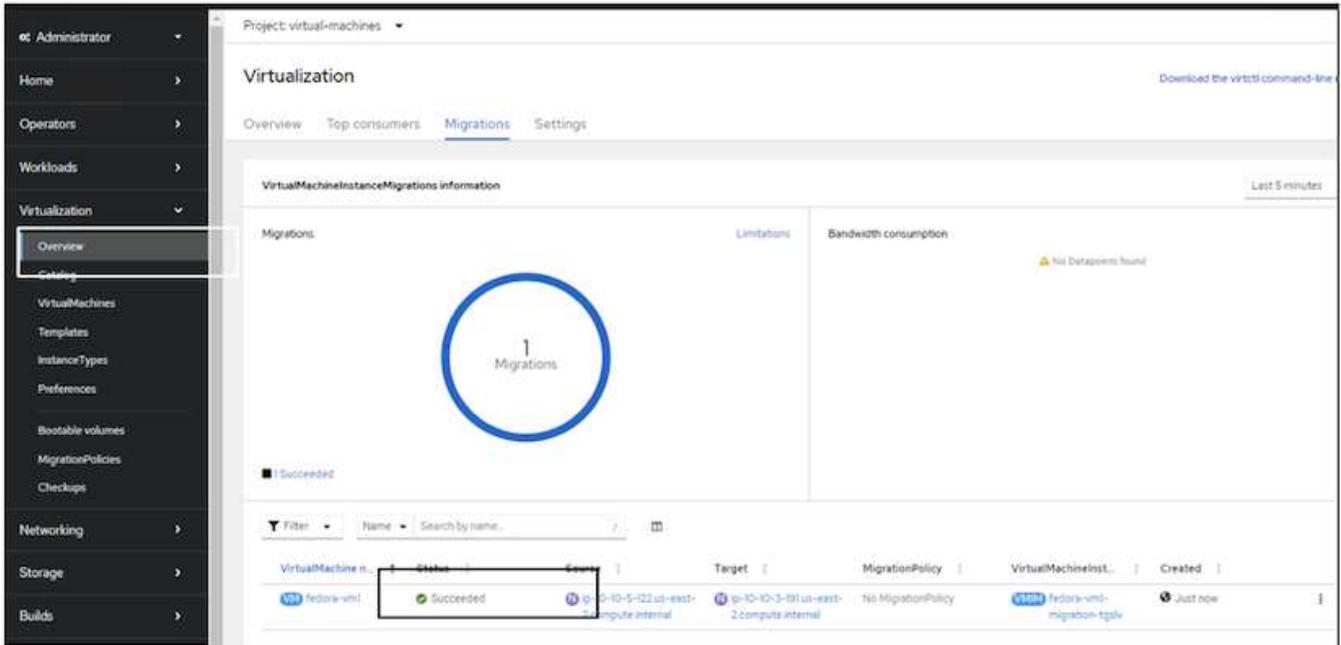
Notieren Sie den Node, auf dem die VM ausgeführt wird



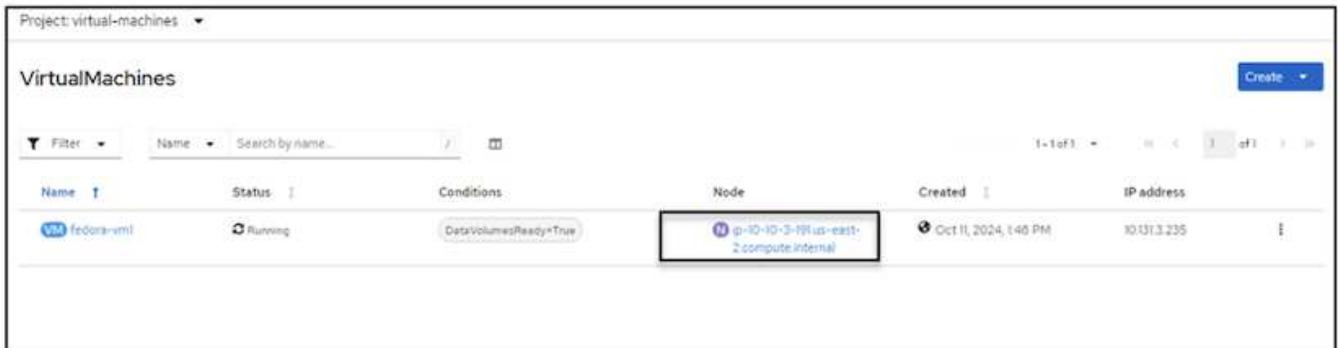
Klicken Sie auf die 3 Punkte und wählen Sie Migrate



Auf der Seite Übersicht sehen Sie, dass die Migration erfolgreich war und der Status in erfolgreich geändert wurde.



Nach Abschluss der Live-Migration befindet sich die VM nun auf einem anderen Node.



Öffnen Sie die Webkonsole, und zeigen Sie den Inhalt der Festplatten an. Es enthält immer noch die gleichen 2 Dateien, die wir vor der Live-Migration erstellt haben.

```
[fedora@fedora-vm1 ~]$ df .
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/vda1       30327788 10956768  18927040  37% /home
[fedora@fedora-vm1 ~]$
[fedora@fedora-vm1 ~]$
[fedora@fedora-vm1 ~]$ ls
random.dat  sample.txt
[fedora@fedora-vm1 ~]$
```

```
[fedora@fedora-vm1 ~]$ ls
random.dat  sample.txt
[fedora@fedora-vm1 ~]$ cat sample.txt
This is a sample text file.
[fedora@fedora-vm1 ~]$
```

Der Speicher für die VM auf dem neuen Knoten zeigt noch immer die gleichen Festplatten

Storage (3)

Name	Drive	Size	Interface
rootdisk	Disk	31.75 GiB	virtio
cloudinitdisk	Disk	-	virtio
fedora-vm1-disk1	Disk	31.75 GiB	virtio

Außerdem sind die VES die gleichen.

Project: virtual-machines

PersistentVolumeClaims Create PersistentVolumeClaim

Filter Name Search by name...

Name	Status	PersistentVolumes	Capacity	Used	StorageClass
fedora-vm1	Bound	pvc-7d00a3cf-d4cc-47d5-8053-efbb0ser135f	31.75 GiB	28.12 GiB	trident-csi
fedora-vm1-fedora-vm1-disk1	Bound	pvc-a709e022-2ae5-43fb-b8a1-a40f4447c6c2	31.75 GiB	320 KiB	trident-csi

Die Volumes, die dem VM-Pod zugeordnet sind, sind ebenfalls die gleichen (2 PVCs) wie zuvor.

Name	Mount path	SubPath	Type	Permissions	Utilized by
private	/var/run/kubevirt-private	No subpath		Read/Write	compute
public	/var/run/kubevirt	No subpath		Read/Write	compute
ephemeral-disks	/var/run/kubevirt-ephemeral-disks	No subpath		Read/Write	compute
container-disks	/var/run/kubevirt/container-disks	No subpath		Read/Write	compute
libvirt-runtime	/var/run/libvirt	No subpath		Read/Write	compute
sockets	/var/run/kubevirt/sockets	No subpath		Read/Write	compute
rootdisk	/var/run/kubevirt-private/vmi-disks/rootdisk	No subpath	PV feora-vmi	Read/Write	compute
fedora-vmi-disk1	/var/run/kubevirt-private/vmi-disks/fedora-vmi-disk1	No subpath	PVC feora-vmi-fedora-vmi-disk1	Read/Write	compute
hotplug-disks	/var/run/kubevirt/hotplug-disks	No subpath		Read/Write	compute

Demovideo

[Live-Migration virtueller Maschinen in OpenShift-Virtualisierung auf ROSA mit Amazon FSX für NetApp ONTAP](#)

Weitere Videos zu Red hat OpenShift- und OpenShift-Virtualisierungslösungen finden Sie ["Hier"](#).

Datensicherung Mit Tools Von Drittanbietern

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

Autor: Banu Sundhar, NetApp

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

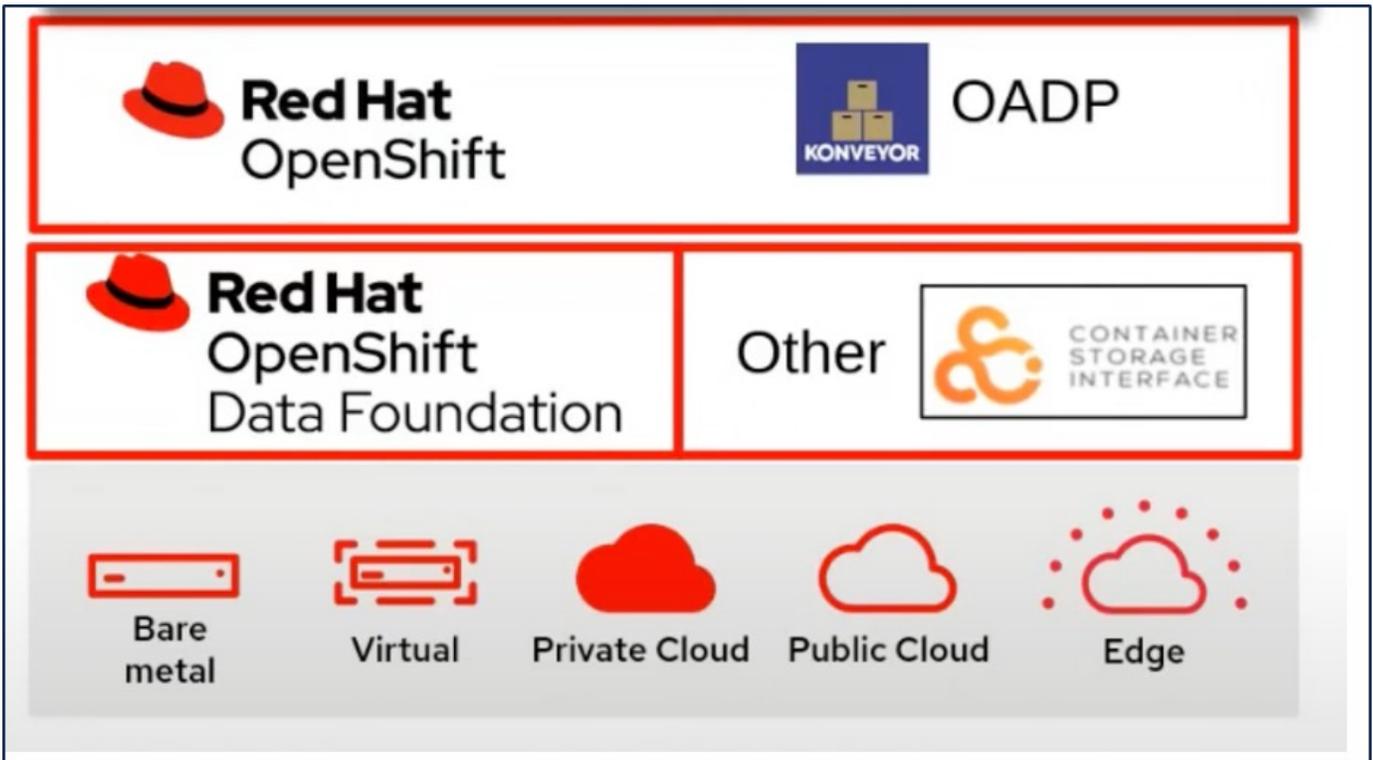
Virtuelle Maschinen in der OpenShift-Virtualisierungsumgebung sind Container-Anwendungen, die in den Workerknoten der OpenShift-Container-Plattform ausgeführt werden. Es ist wichtig, die VM-Metadaten sowie die persistenten Festplatten der VMs zu schützen, damit Sie sie bei Verlust oder Beschädigung wiederherstellen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

Die persistenten Festplatten der OpenShift-Virtualisierungs-VMs können mithilfe von ONTAP-Speicher gesichert werden, der in den OpenShift-Cluster integriert ["Trident-CSI"](#) ist. In diesem Abschnitt führen wir ["OpenShift API for Data Protection \(OADP\)"](#) ein Backup von VMs durch, einschließlich der Daten-Volumes in

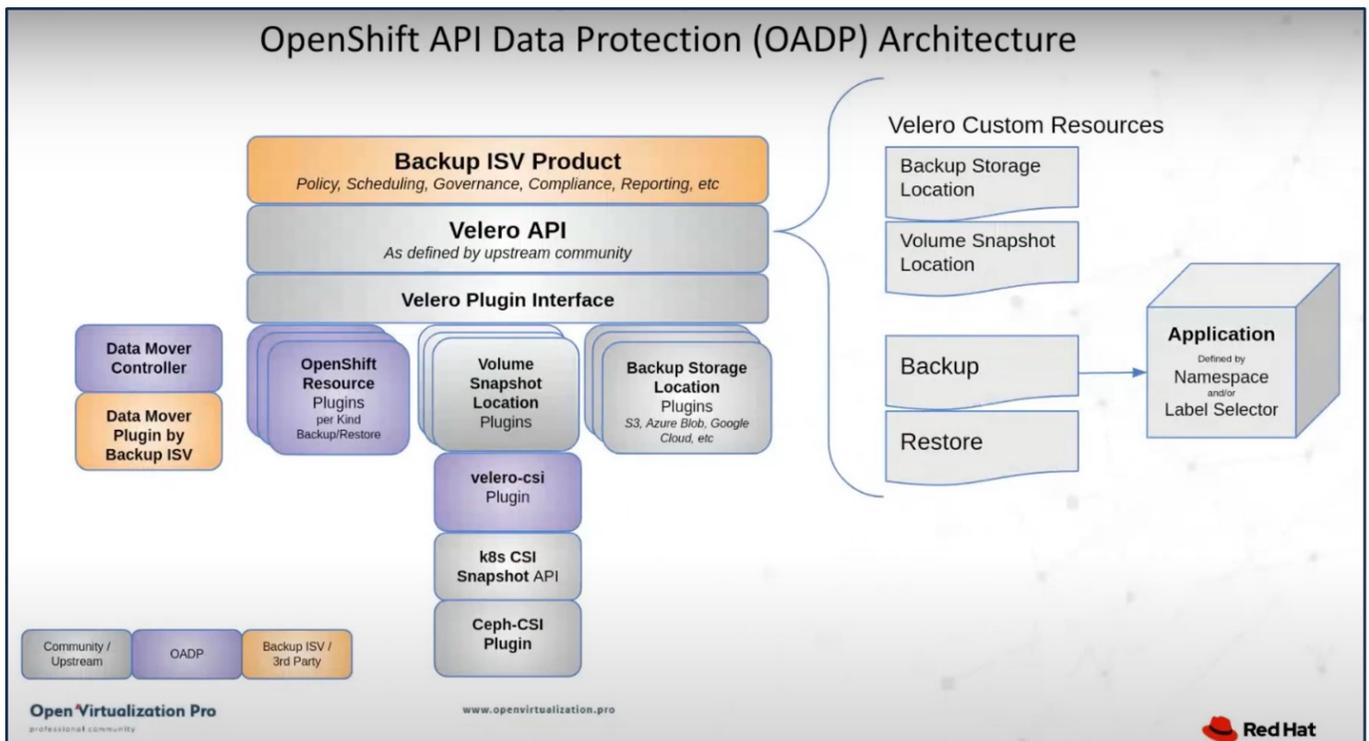
- ONTAP Objekt-Storage
- StorageGRID

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

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



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



OADP 1.3 ist über den Operator Hub von OpenShift Cluster 4.12 und höher verfügbar. Es verfügt über einen integrierten Data Mover, der CSI-Volume-Snapshots in einen Remote-Objektspeicher verschieben kann. Dies sorgt für Portabilität und Langlebigkeit, indem Snapshots während des Backups an einen Speicherort für Objekte verschoben werden. Die Snapshots stehen dann für die Wiederherstellung nach Katastrophen zur Verfügung.

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

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

["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

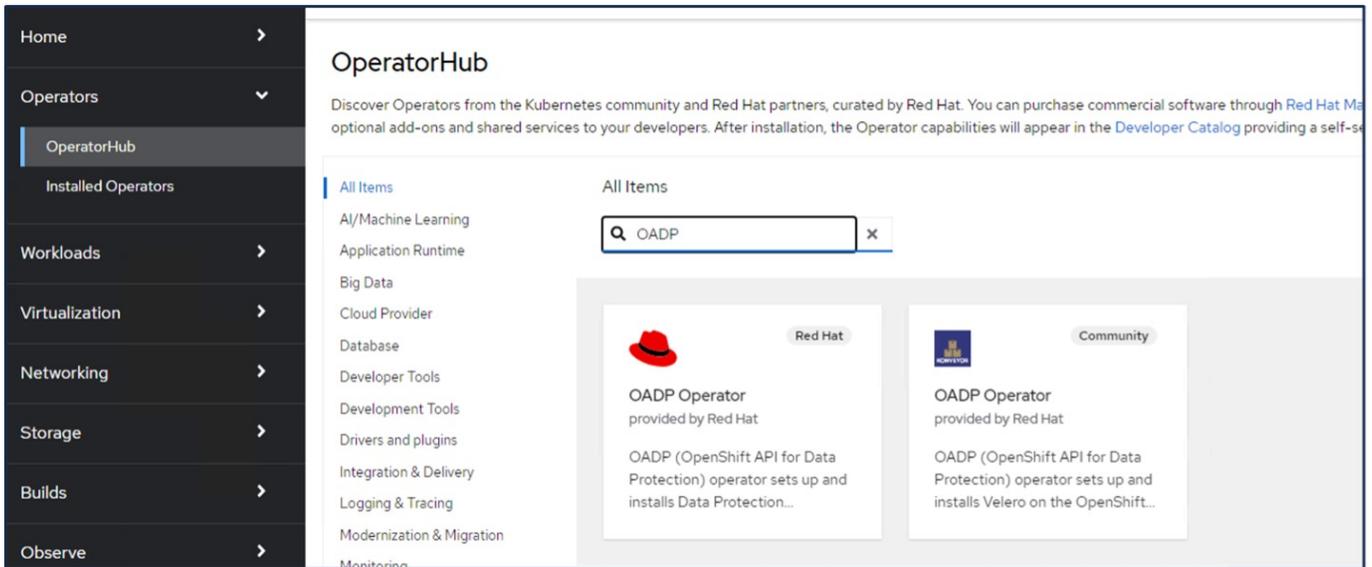
- Ein Red hat OpenShift-Cluster (später als Version 4.12), der auf einer Bare-Metal-Infrastruktur mit RHCOS Worker-Knoten installiert ist
- Ein NetApp ONTAP Cluster, der mithilfe von Trident in den Cluster integriert ist
- Ein Trident Back-End, das mit einer SVM auf ONTAP Cluster konfiguriert ist
- Eine 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
- OpenShift Virtualization Operator installiert und konfiguriert
- In einem Namespace auf OpenShift Virtualization implementierte VMs
- Eine Admin-Workstation mit den Tools tridentctl und oc installiert und zur €Pfad hinzugefügt



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

Schritte zum Installieren des OADP-Bedieners

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



The screenshot displays the OperatorHub interface. On the left 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 includes a search bar with "OADP" entered. Below the search bar, two operator cards are visible: one from Red Hat and one from the Community. Both cards describe the "OADP Operator" and its function in setting up and installing Data Protection and Velero on 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](#)

Project: All Projects

Installed Operators

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

Name Search by name... /

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

Voraussetzungen für die Velero-Konfiguration mit ONTAP S3-Details

Nachdem die Installation des Bedieners erfolgreich war, konfigurieren Sie die Instanz von Velero. Velero kann für die Verwendung von S3 Compatible Object Storage konfiguriert werden. Konfigurieren Sie ONTAP S3 mithilfe der in dargestellten Verfahren "[Abschnitt „Objekt-Storage-Management“ der ONTAP-Dokumentation](#)". Für die Integration in Velero benötigen Sie die folgenden Informationen aus Ihrer ONTAP S3-Konfiguration.

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

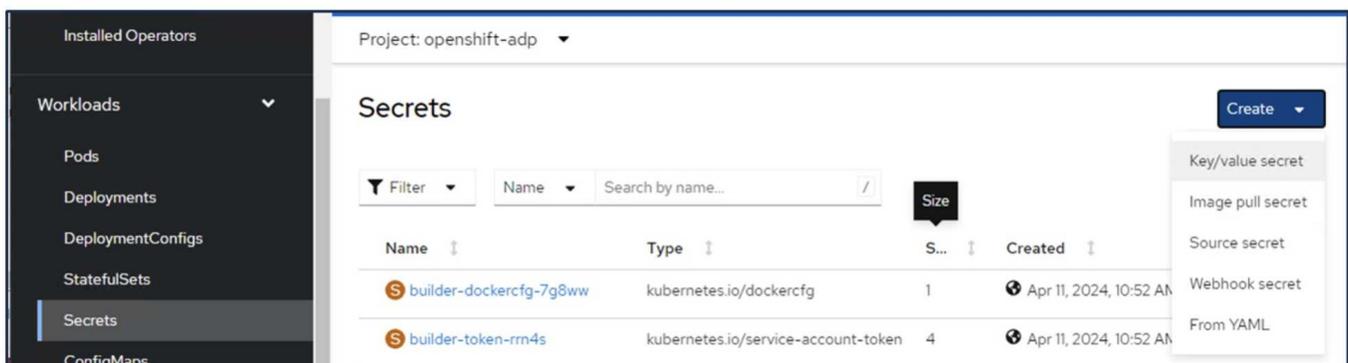
Voraussetzungen für die Velero-Konfiguration mit StorageGRID S3-Details

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

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

Schritte zum Konfigurieren von Velero

- Erstellen Sie zunächst einen Schlüssel für Anmeldedaten eines ONTAP S3-Benutzers oder eines StorageGRID-Mandanten. Diese wird später zur Konfiguration von Velero verwendet. Sie können einen Schlüssel aus der CLI oder aus der Webkonsole erstellen.
Um einen Schlüssel von der Webkonsole aus zu erstellen, wählen Sie Geheimnisse aus, und klicken Sie dann auf Schlüssel/Wertgeheimnis. Geben Sie die Werte für den Anmeldeinformationsnamen, den Schlüssel und den angezeigten Wert an. Verwenden Sie unbedingt die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres S3-Benutzers. Nennen Sie das Geheimnis entsprechend. In dem unten stehenden Beispiel wird ein Geheimnis mit den ONTAP S3-Benutzeranmeldeinformationen namens `ontap-s3-credentials` erstellt.



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 *

 Unique name of the new secret.

Key *

Value

 Browse...

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

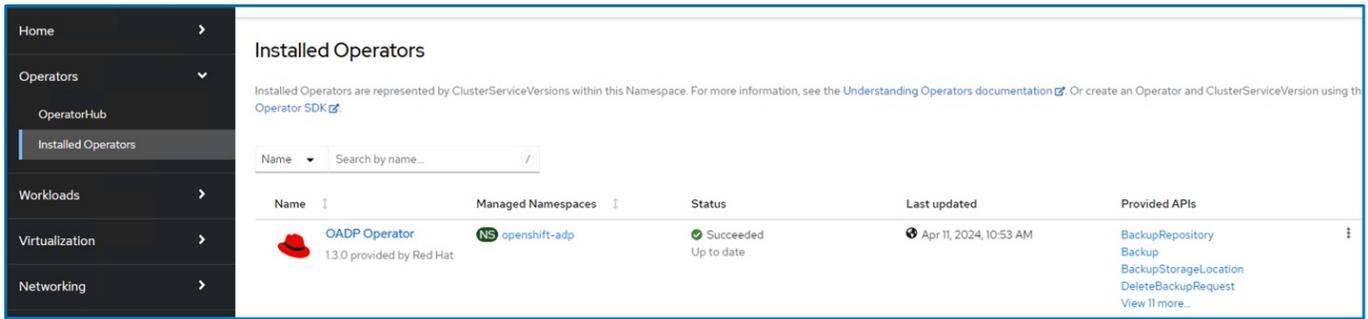
Um einen Schlüssel mit dem Namen sg-s3-credentials aus der CLI zu erstellen, können Sie den folgenden Befehl verwenden.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt
```

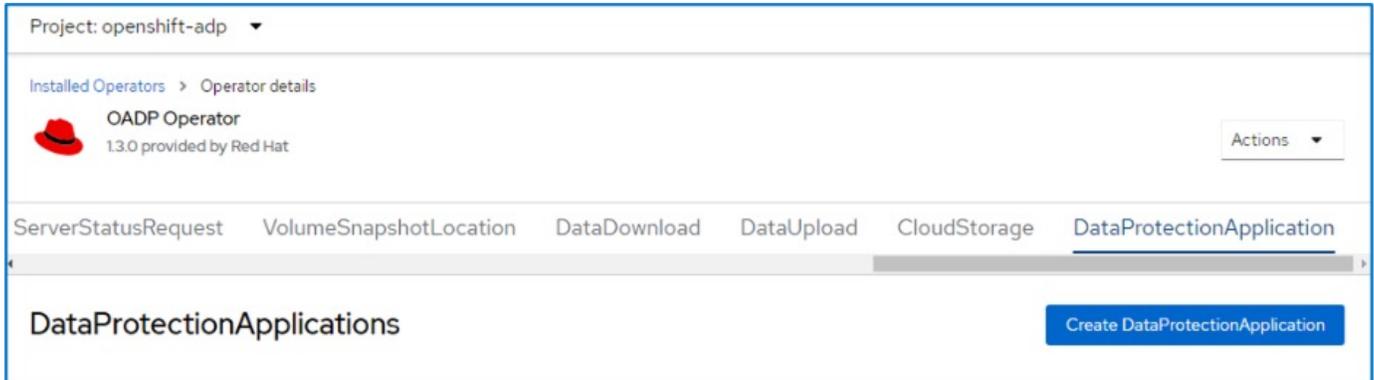
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

```
[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 aus.



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



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

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

```

spec:
  backupLocations:
    - velero:
      config:
        insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
        profile: default
        region: us-east-1
        s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
        s3Url: 'https://10.xx.xx.xx' ->LIF to access S3. Ensure TLS
certificate for S3 is configured
        credential:
          key: cloud
          name: ontap-s3-credentials ->previously created secret
        default: true
        objectStorage:
          bucket: velero ->Your bucket name previously created in S3 for
backups
          prefix: demobackup ->The folder that will be created in the
bucket
          provider: aws
        configuration:
          nodeAgent:
            enable: true
            uploaderType: kopia
            #default Data Mover uses Kopia to move snapshots to Object Storage
          velero:
            defaultPlugins:
              - csi ->Add this plugin
              - openshift
              - aws
              - kubevirt ->Add this plugin

```

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

```

spec:
  backupLocations:
    - velero:
      config:
        insecureSkipTLSVerify: 'true'
        profile: default
        region: us-east-1 ->region of your StorageGrid system
        s3ForcePathStyle: 'True'
        s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
      credential:
        key: cloud
        name: sg-s3-credentials ->secret created earlier
      default: true
      objectStorage:
        bucket: velero
        prefix: demobackup
      provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt

```

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

Backup-Standorte

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

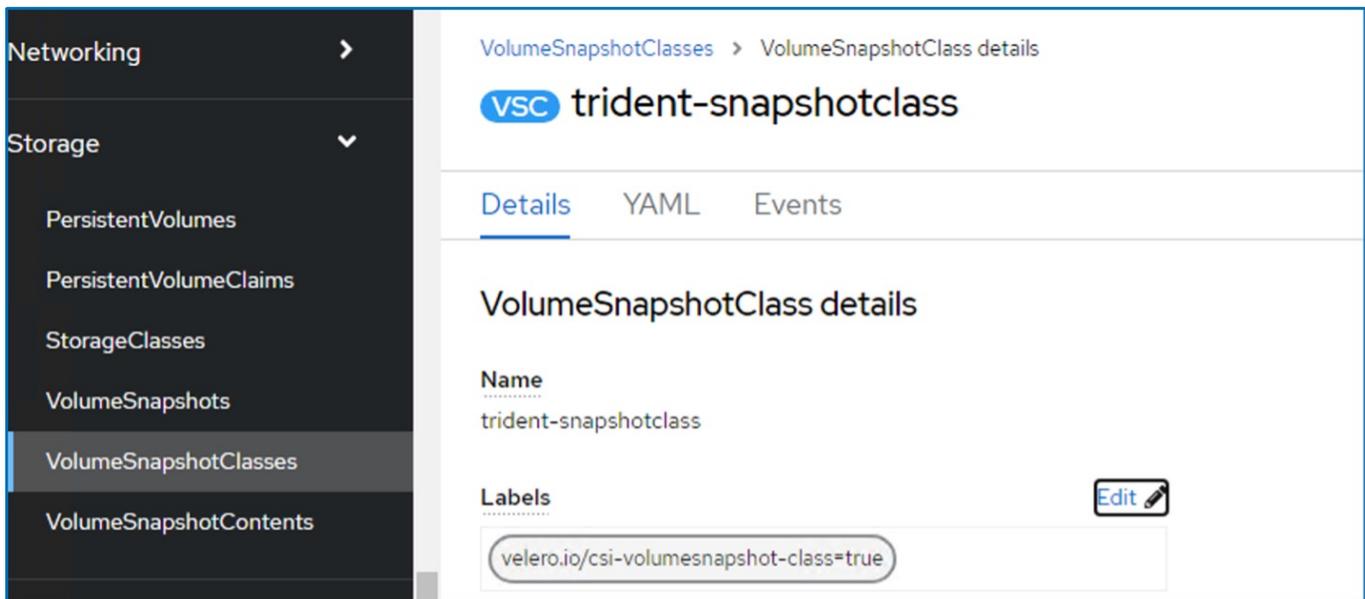
SnapshotLocations Wenn Sie CSI-Snapshots (Container Storage Interface) verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie einen VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Trident CSI und Sie haben bereits VolumeSnapShotClass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

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/manager=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 Virtualization

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

Schritte zum Erstellen einer Sicherung einer VM

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

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

```

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

```

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

The screenshot shows the OpenShift console interface for the 'openshift-adp' project. It displays the 'OADP Operator' details, with the 'Backup' tab selected. A table lists the backup 'backup1' with a status of 'Completed' and a label 'velero.io/storage-location=velero-demo-1'. A 'Create Backup' button is visible in the top right corner.

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.



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

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 Virtualization

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

```

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

```

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

Sobald der Zeitplan erstellt wurde, wird er aktiviert.

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.

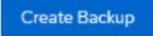
Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

Events All instances BackupRepository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups



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

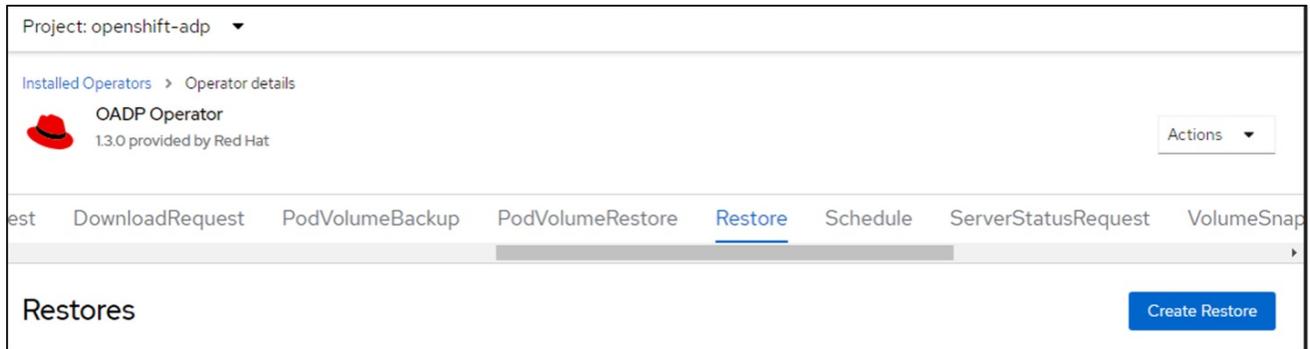
In diesem Abschnitt wird beschrieben, wie virtuelle Maschinen aus einem Backup wiederhergestellt werden.

Voraussetzungen

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

Restore auf denselben Namespace

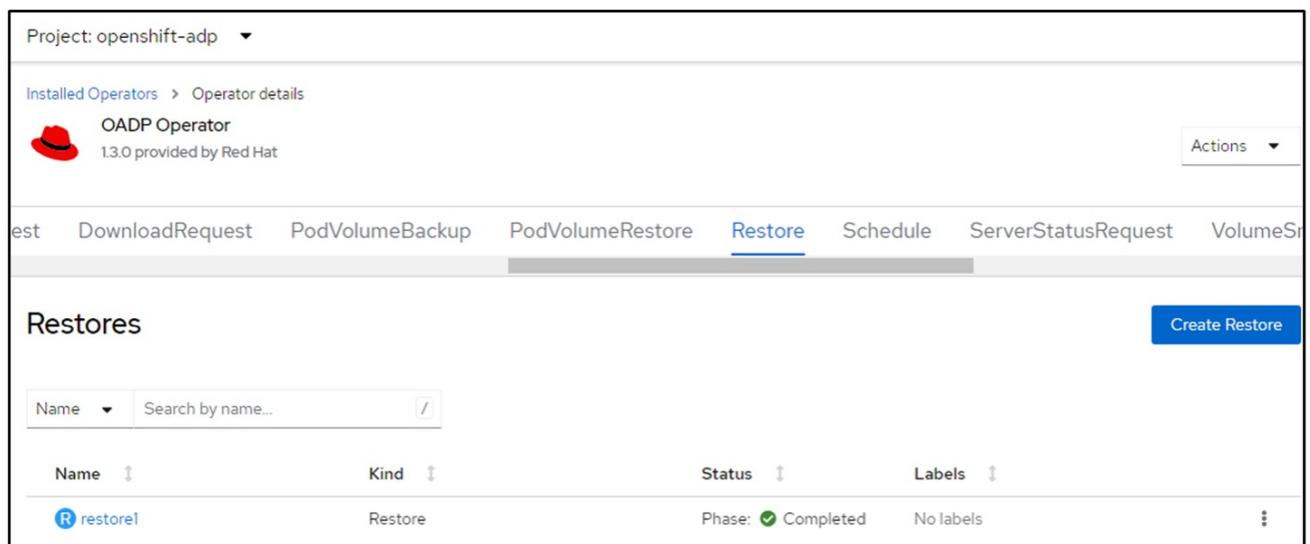
Um das Backup wiederherzustellen, das wir gerade erstellt haben, müssen wir eine Restore Custom Resource (CR) erstellen. Geben Sie ihm einen Namen, geben Sie den Namen des Backups an, von dem aus wir die Wiederherstellungs-PVs wiederherstellen möchten, und setzen Sie sie auf „True“. Weitere Parameter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



The screenshot shows the OADP Operator interface. At the top, it says 'Project: openshift-adp'. Below that, there's a breadcrumb 'Installed Operators > Operator details'. The operator is identified as 'OADP Operator' with version '1.3.0 provided by Red Hat'. A navigation bar contains several tabs: 'DownloadRequest', 'PodVolumeBackup', 'PodVolumeRestore', 'Restore' (which is highlighted), 'Schedule', 'ServerStatusRequest', and 'VolumeSnap'. Below the navigation bar, the 'Restores' section is visible, featuring a 'Create Restore' button.

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

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



This screenshot shows the OADP Operator interface after a restore operation. The 'Restore' tab is still selected. In the 'Restores' section, there is a search bar and a table listing the restore. The table has columns for 'Name', 'Kind', 'Status', and 'Labels'. One restore is listed with the name 'restore1', kind 'Restore', and status 'Phase: Completed'. There are also 'Create Restore' and 'Actions' buttons.

Name	Kind	Status	Labels
restore1	Restore	Phase: Completed	No labels

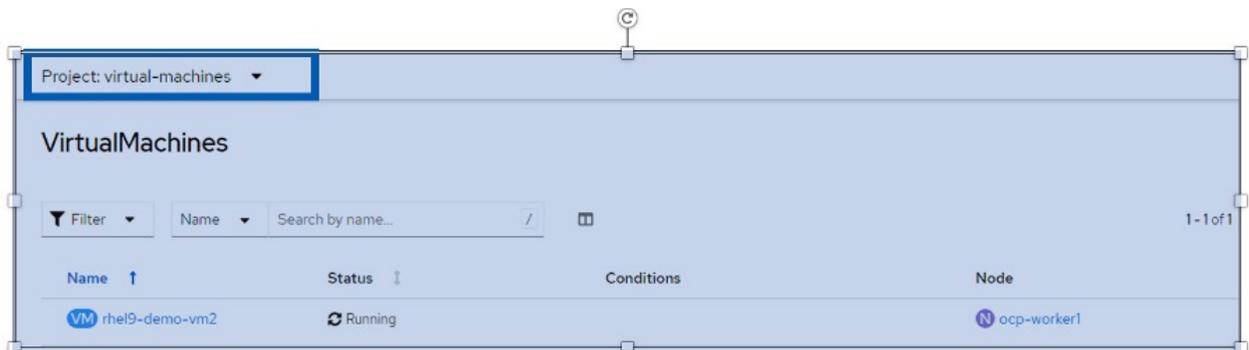
Wiederherstellung in einem anderen Namespace

Um die VM 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 VM und ihre Laufwerke im Namespace „Virtual-Machines-Demo“ wiederherzustellen, als das Backup in den Namespace „Virtual Machines“ aufgenommen wurde.

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

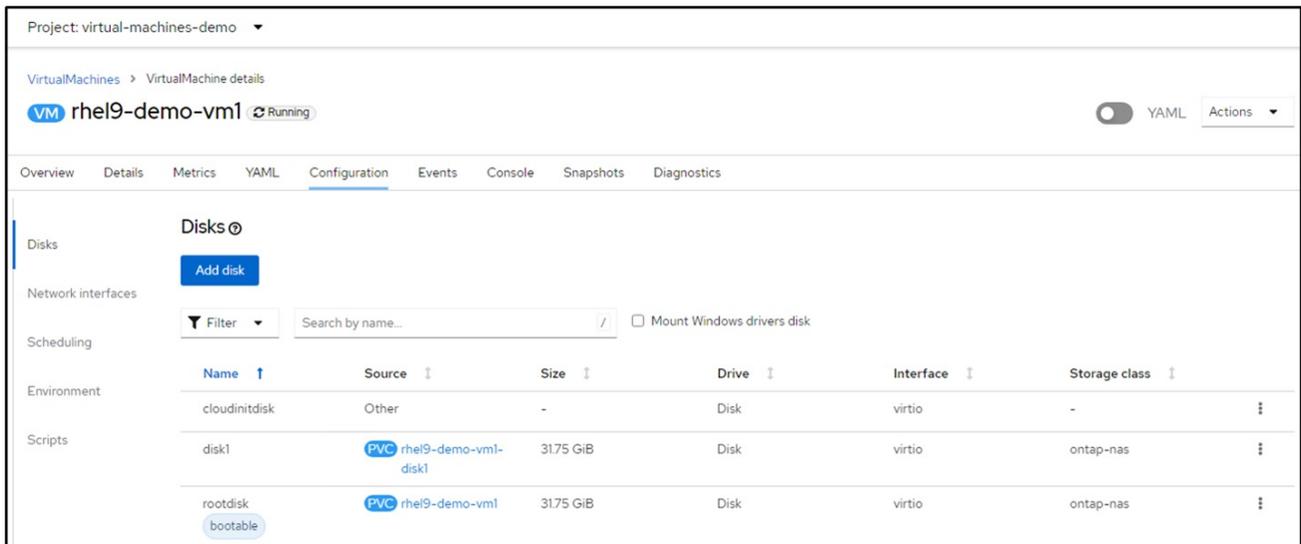
Wenn in der Phase „Abgeschlossen“ angezeigt wird, sehen Sie, dass die virtuellen Maschinen zum Zeitpunkt der Snapshot-Erstellung wieder in den Status versetzt wurden. (Wenn das Backup bei der Ausführung der VM erstellt wurde, wird durch die Wiederherstellung der VM aus dem Backup die wiederhergestellte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



Wiederherstellung auf eine andere Storage-Klasse

Velero bietet eine allgemeine Möglichkeit, die Ressourcen während der Wiederherstellung durch Angabe von json Patches zu ändern. Die json-Patches werden auf die Ressourcen angewendet, bevor sie wiederhergestellt werden. Die json-Patches werden in einer configmap angegeben und im Wiederherstellungsbefehl auf die configmap verwiesen. Diese Funktion ermöglicht Ihnen die Wiederherstellung mit einer anderen Storage-Klasse.

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



Project: virtual-machines-demo

VirtualMachines > VirtualMachine details

VM rhel9-demo-vm1 Running

Overview Details Metrics YAML Configuration Events Console Snapshots Diagnostics

Disks

Add disk

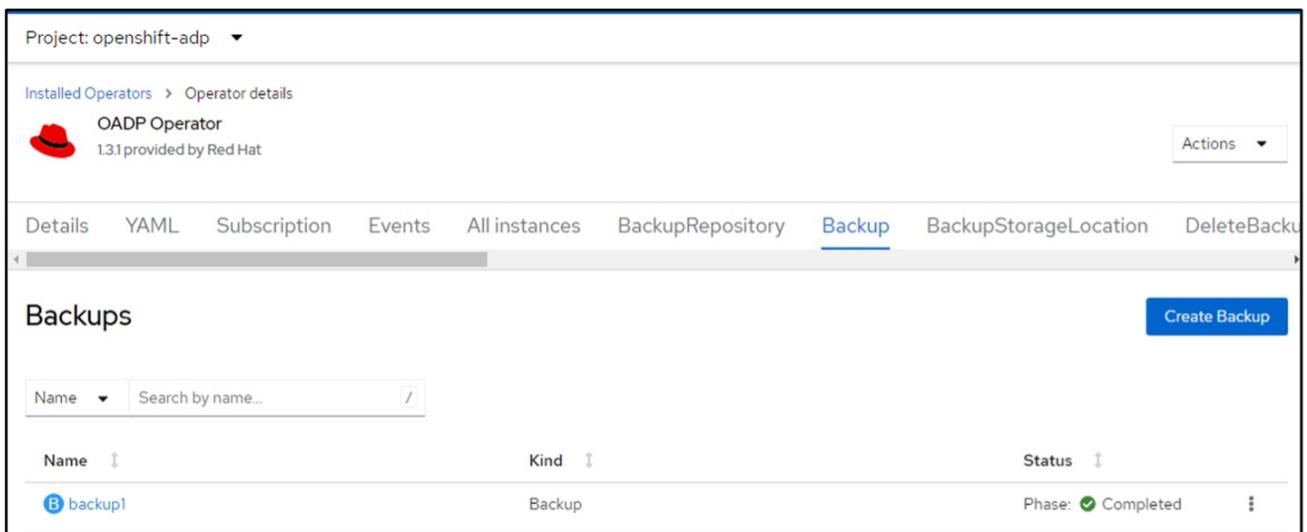
Network interfaces

Scheduling

Environment

Scripts

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	31.75 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	31.75 GiB	Disk	virtio	ontap-nas



Project: openshift-adp

Installed Operators > Operator details

OADP Operator
1.3.1 provided by Red Hat

Details YAML Subscription Events All instances BackupRepository Backup BackupStorageLocation DeleteBackup

Backups

Create Backup

Name Search by name...

Name	Kind	Status
backup1	Backup	Phase: Completed

Simulieren Sie einen Verlust der VM durch Löschen der VM.

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

Schritt 1

Erstellen Sie eine Konfigurationszuordnung (Konsole) im openshift-adp-Namespace wie folgt: Geben Sie die Details wie im Screenshot gezeigt ein:

Wählen Sie Namespace : openshift-adp
Name: Change-Storage-class-config (kann ein beliebiger Name sein)
Schlüssel: Change-Storage-class-config.yaml:
Wert:

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

The screenshot displays the OpenShift web console interface for editing a ConfigMap. The left sidebar shows a navigation menu with 'ConfigMaps' highlighted. The main content area is titled 'Edit ConfigMap' and includes a description: 'Config maps hold key-value pairs that can be used in pods to read application configuration.' Below this, there are radio buttons for 'Form view' (selected) and 'YAML view'. The form contains several sections: 'Name' with the value 'change-storage-class-config', 'Data' with a 'Remove key/value' button, and 'Key' with the value 'change-storage-class-config.yaml'. The 'Value' field is a large text area containing the YAML configuration, with a 'Browse...' button to its right. At the bottom of the form, there is an 'Add key/value' button.

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

```

# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:          change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
  groupResource: persistentvolumeclaims
  resourceNameRegex: "^rhel*"
  namespaces:
  - virtual-machines-demo
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"

BinaryData
====

Events:  <none>

```

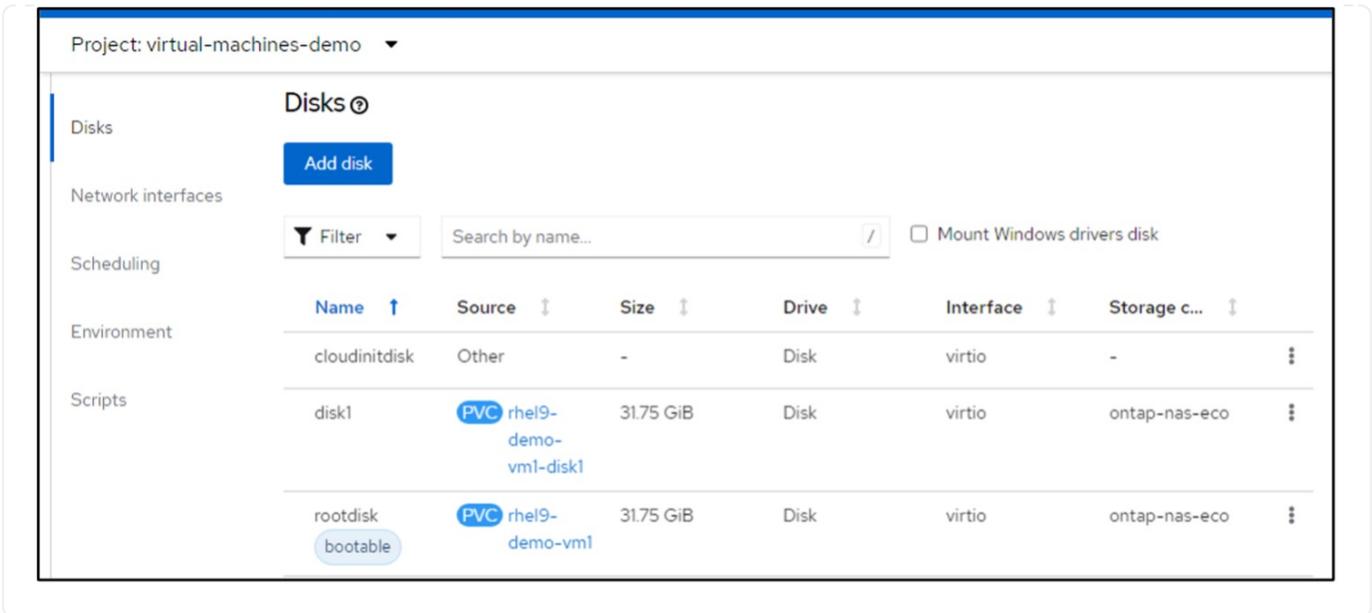
Diese Konfigurationszuordnung wendet die Ressourcenänderungsregel an, wenn die Wiederherstellung erstellt wird. Für alle Ansprüche auf persistente Volumes, die mit RHEL beginnen, wird ein Patch eingesetzt, der den Namen der Storage-Klasse auf ontap-nas-Eco ersetzt.

Schritt 2

Verwenden Sie zum Wiederherstellen der VM den folgenden Befehl aus der Velero CLI:

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

Die VM wird im gleichen Namespace mit den Festplatten wiederhergestellt, die mit der Storage-Klasse ontap-nas-eco erstellt wurden.



Löschen von Backups und Restores in mit Velero

In diesem Abschnitt wird erläutert, wie Backups und Restores für VMs in OpenShift Virtualization mithilfe von Velero gelöscht werden.

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>
```

Löschen einer Wiederherstellung

Sie können den Restore CR mit der 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>
```

Monitoring

Überwachung mit Cloud Insights für VMs in Red hat OpenShift Virtualization

Autor: Banu Sundhar, NetApp

Dieser Abschnitt des Referenzdokuments enthält Details zur Integration von NetApp Cloud Insights in einen Red hat OpenShift-Cluster zur Überwachung von OpenShift-Virtualisierungs-VMs.

NetApp Cloud Insights ist ein Tool für das Monitoring der Cloud-Infrastruktur, mit dem Sie Ihre gesamte Infrastruktur im Blick haben. Es überwacht nicht nur alle Ressourcen, die in Public Clouds und privaten Datacentern liegen, sondern hilft auch dabei, Fehler aufzuspüren und den Ressourceneinsatz zu optimieren. Cloud Insights Weitere Informationen zu NetApp Cloud Insights finden Sie im "[Cloud Insights-Dokumentation](#)".

Um Cloud Insights nutzen zu können, müssen Sie sich im NetApp BlueXP Portal anmelden. Weitere Informationen finden Sie im "[Cloud Insights-Onboarding](#)".

Cloud Insights bietet verschiedene Funktionen, mit denen Sie Daten schnell und einfach finden, Probleme beheben und Einblicke in Ihre Umgebung erhalten. Mit leistungsstarken Abfragen können Sie Daten einfach auffinden, Daten in Dashboards visualisieren und E-Mail-Warnungen für von Ihnen festgelegte Datenschwellenwerte senden. Siehe "[Video-Tutorials](#)" Um Ihnen das Verständnis dieser Funktionen zu erleichtern.

Damit Cloud Insights mit der Datenerfassung beginnen kann, benötigen Sie Folgendes

Datensammler

Es gibt 3 Arten von Datensammlern:

- * Infrastruktur (Speichergeräte, Netzwerk-Switches, Rechnerinfrastruktur)
- * Betriebssysteme (wie VMware oder Windows)
- * Dienste (wie Kafka)

Data Collectors erfassen Informationen aus Datenquellen, wie z. B. ONTAP-Speichergeräten (Infrastructure Data Collector). Die gesammelten Informationen dienen Analyse-, Validierungs-, Monitoring- und Fehlerbehebungszwecken.

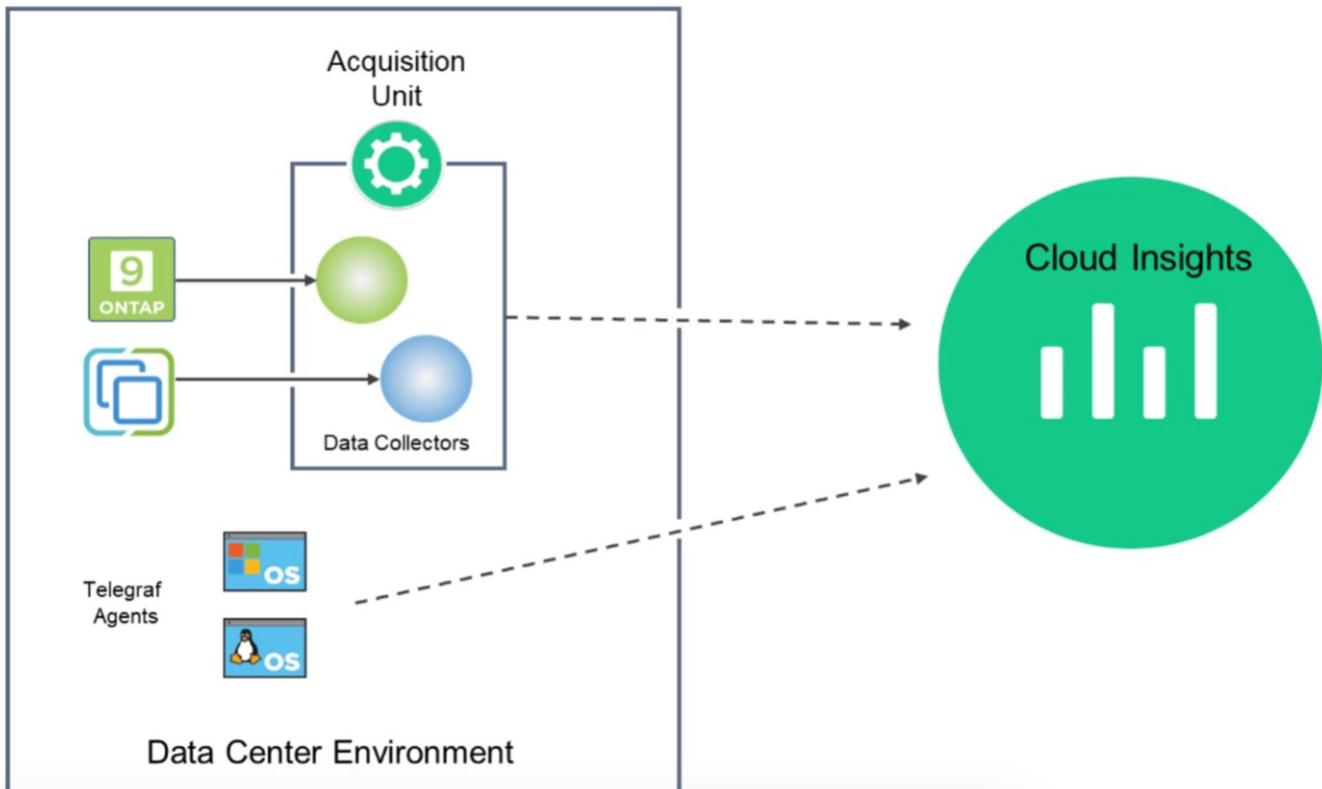
Erfassungseinheit

Wenn Sie einen Infrastruktur-Data Collector verwenden, benötigen Sie auch eine Erfassungseinheit, um Daten in Cloud Insights zu injizieren. Eine Erfassungseinheit ist ein Computer, der speziell für das Hosten von Datensammlern verwendet wird, in der Regel eine virtuelle Maschine. Dieser Computer befindet sich in der Regel im gleichen Rechenzentrum/VPC wie die überwachten Elemente.

Telegraf Agenten

Cloud Insights unterstützt außerdem Telegraf als Agent für die Erfassung von Integrationsdaten. Telegraf ist ein Plug-in-gestützter Server-Agent, mit dem Kennzahlen, Ereignisse und Protokolle erfasst und protokolliert werden können.

Cloud Insights-Architektur



Integration mit Cloud Insights für VMs in Red hat OpenShift Virtualization

Um Daten für VMs in OpenShift Virtualization zu sammeln, müssen Sie Folgendes installieren:

1. Ein Kubernetes Monitoring Operator und Datensammler zum Erfassen von Kubernetes-Daten
Vollständige Anweisungen finden Sie im "[Dokumentation](#)".
2. Eine Einheit zur Erfassung von Daten aus ONTAP Storage, die persistenten Storage für VM-Festplatten bereitstellt
Vollständige Anweisungen finden Sie im "[Dokumentation](#)".
3. Ein Datensammler für ONTAP
Vollständige Anweisungen finden Sie im "[Dokumentation](#)".

Wenn Sie StorageGRID außerdem für VM-Backups verwenden, benötigen Sie auch einen Datensammler für die StorageGRID.

Beispielfunktionen für die Überwachung von VMs in Red hat OpenShift Virtualization

In diesem Abschnitt wird die Überwachung mit Cloud Insights für VMs in Red hat OpenShift Virtualization erläutert.

Überwachung auf Basis von Ereignissen und Erstellung von Warnungen

Hier ist ein Beispiel, bei dem der Namespace, der eine VM in OpenShift Virtualization enthält, anhand von Ereignissen überwacht wird. In diesem Beispiel wird ein Monitor basierend auf `logs.kubernetes.Event` für den

angegebenen Namespace im Cluster erstellt.

NetApp PCS Sandbox / Observability / Alerts / Manage Monitors / Monitor virtual-machines-demo-ns

Edit log monitor

Filter/Advanced Query and Group by in section 1 must not be empty. If alert resolution is based on log entry, section 3 filter/advanced query also must not be empty.

1 Select the log to monitor

Log Source: logs.kubernetes.event

Filter By: kubernetes_cluster: ocp-cluster4, involvedobject.namespace: virtual-machines-demo-ns

Group By: reason

27 items found

timestamp	type	source	message
04/19/2024 10:31:18 AM	logs.kubernetes.event	kubernetes_cluster:ocp-cluster4;namespace:cloudi nsights-monitoring;pod_name:net app-ci-event-exporter-7f7c8d84c4-sk7t9;	VirtualMachineInstance started.
04/19/2024 10:31:18 AM	logs.kubernetes.event	kubernetes_cluster:ocp-cluster4;namespace:cloudi nsights-monitoring;pod_name:net app-ci-event-exporter-7f7c8d84c4-sk7t9;	VirtualMachineInstance defined.

2 Define alert behavior

Create an alert at severity: Warning when the conditions above occur: 1 time

Diese Abfrage enthält alle Ereignisse für die virtuelle Maschine im Namespace. (Im Namespace befindet sich nur eine virtuelle Maschine). Eine erweiterte Abfrage kann auch so konstruiert werden, dass sie auf der Grundlage des Ereignisses gefiltert wird, bei dem der Grund „Fehlgeschlagen“ oder „FailedMount“ lautet. Diese Ereignisse werden normalerweise erstellt, wenn beim Erstellen eines PV ein Problem auftritt oder das PV in einen Pod gemountet wird, der Probleme im dynamischen provisionierer anzeigt, um persistente Daten zu erstellen Volumes für die VM.

Beim Erstellen des Alarmmonitors wie oben gezeigt können Sie auch Benachrichtigungen an Empfänger konfigurieren. Sie können auch Korrekturmaßnahmen oder zusätzliche Informationen bereitstellen, die zur Behebung des Fehlers hilfreich sein können. Im obigen Beispiel könnten Sie weitere Informationen darüber finden, wie die Trident Back-End-Konfiguration und die Storage-Klassendefinitionen zur Behebung des Problems aussehen könnten.

Änderungsanalyse

Mit Change Analytics erhalten Sie einen Überblick darüber, was sich im Zustand Ihres Clusters geändert hat, einschließlich der Person, die diese Änderung vorgenommen hat, um Probleme zu beheben.

NetApp Cloud Insights Tutorial 0% Complete Getting Started

NetApp PCS Sandbox / Kubernetes / **Change Analysis** Last 3 Hours

Filter By: Kubernetes Cluster: ocp-cluster4 Namespace: virtual-machines-demo Workload Name: All

Alerts: 0 Deploys: 5

Timeline Bucket: 6 minutes

virtual-machines-demo

All Workloads in namespace

Compare to:

- Kubernetes Infrastructure
 - Nodes (1) 115 Changes and 0 Alerts
 - Persistent Volumes (6) 8 Changes and 0 Alerts
- Kubernetes Resources
 - Security (2) 2 Changes and 0 Alerts

Changes Last updated 04/19/2024 11:43:58 AM

Type	Summary	Start Time	Duration	Triggered On: name	Status
Deploy	Attributes 'metadata.finalizers-', 'metadata.finalizers[1]' changed	04/19/2024 11:40:31 AM	6 seconds	PersistentVolumeClaim: rhel9-demo-vm2	Complete
Deploy	Attributes 'metadata.finalizers-', 'metadata.finalizers[1]' changed	04/19/2024 11:40:36 AM	1 second	PersistentVolumeClaim: rhel9-demo-vm2-user-disk1	Complete
Deploy	Created new object	04/19/2024 10:30:59 AM	18 seconds	PersistentVolumeClaim: rhel9-demo-vm2-user-disk1	Complete
Deploy	Created new object	04/19/2024 10:30:59 AM	18 seconds	PersistentVolumeClaim: rhel9-demo-vm2	Complete
Deploy	Created new object	04/19/2024 10:31:00 AM	17 seconds	PodDisruptionBudget: kubevirt-disruption-budget-dnvs	Complete

Im obigen Beispiel wird die Änderungsanalyse auf dem OpenShift-Cluster für den Namespace konfiguriert, der eine OpenShift-Virtualisierungs-VM enthält. Das Dashboard zeigt Änderungen gegenüber der Zeitachse an. Sie können nach unten gehen, um zu sehen, was sich geändert hat, und klicken Sie auf Alle Änderungen Diff, um den Unterschied der Manifeste zu sehen. Aus dem Manifest können Sie sehen, dass eine neue Sicherung der persistenten Laufwerke erstellt wurde.

Deploy Completed

Summary

Start Time: 04/19/2024 11:40:31 AM End Time: 04/19/2024 11:40:37 AM Duration: 6 seconds

Triggered On: ocp-cluster4 > virtual-machines-demo > rhel9-demo-vm2 >

Triggered On: kind PersistentVolumeClaim

Changes (2)

Attribute Name	Previous	New
metadata.finalizers-	-	snapshot.storage.kubernetes.io/pvc-as-source-protection
metadata.finalizers[1]	snapshot.storage.kubernetes.io/pvc-as-source-protection	-

All Changes Diff

Associated Events

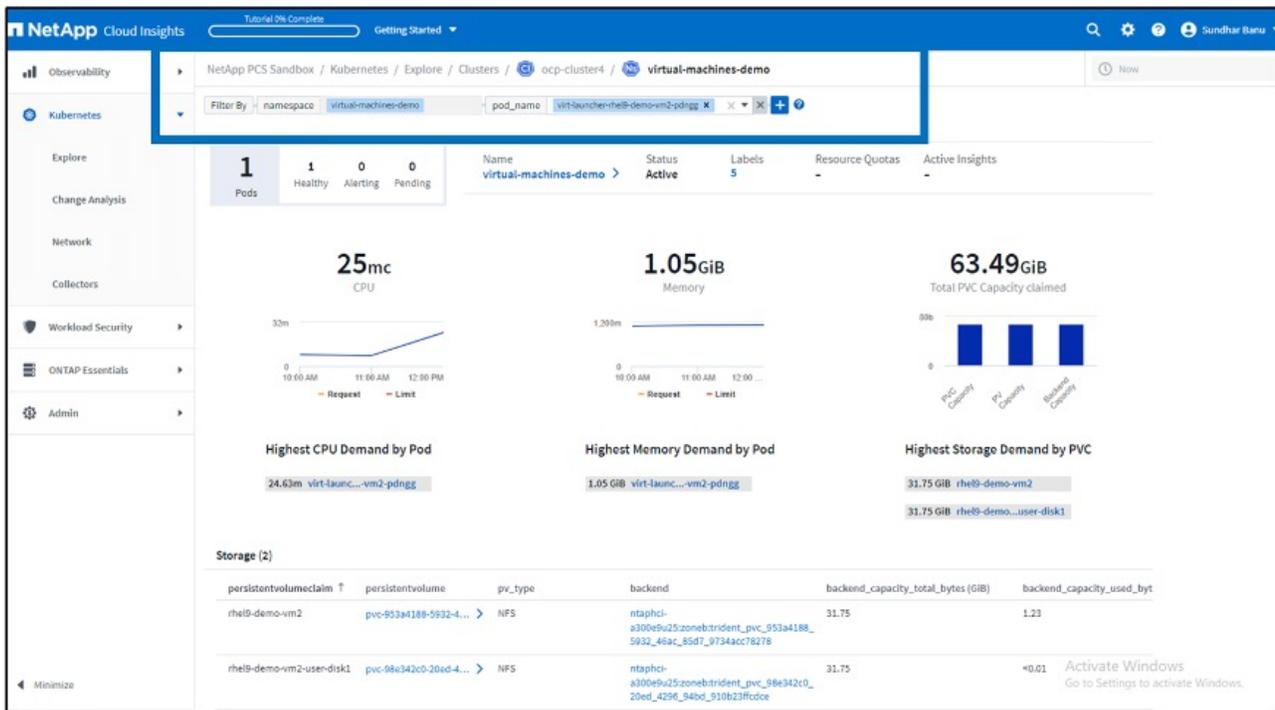
Event Logs

timestamp	severity	reason	involvedObject...	involvedObject...	message
04/19/2024 10:30:59 AM	Normal	Provisioning	PersistentVolumeClaim	rhel9-demo-vm2	External provisioner is provisioning volume for claim "virtual-machines-demo/rhel9-demo-vm2"
04/19/2024 10:30:59 AM	Normal	Pending	DataVolume	rhel9-demo-vm2-user-disk1	PVC rhel9-demo-vm2-user-disk1 Pending
04/19/2024	Normal	ImportSucceeded	DataVolume	rhel9-demo-vm2	Successfully

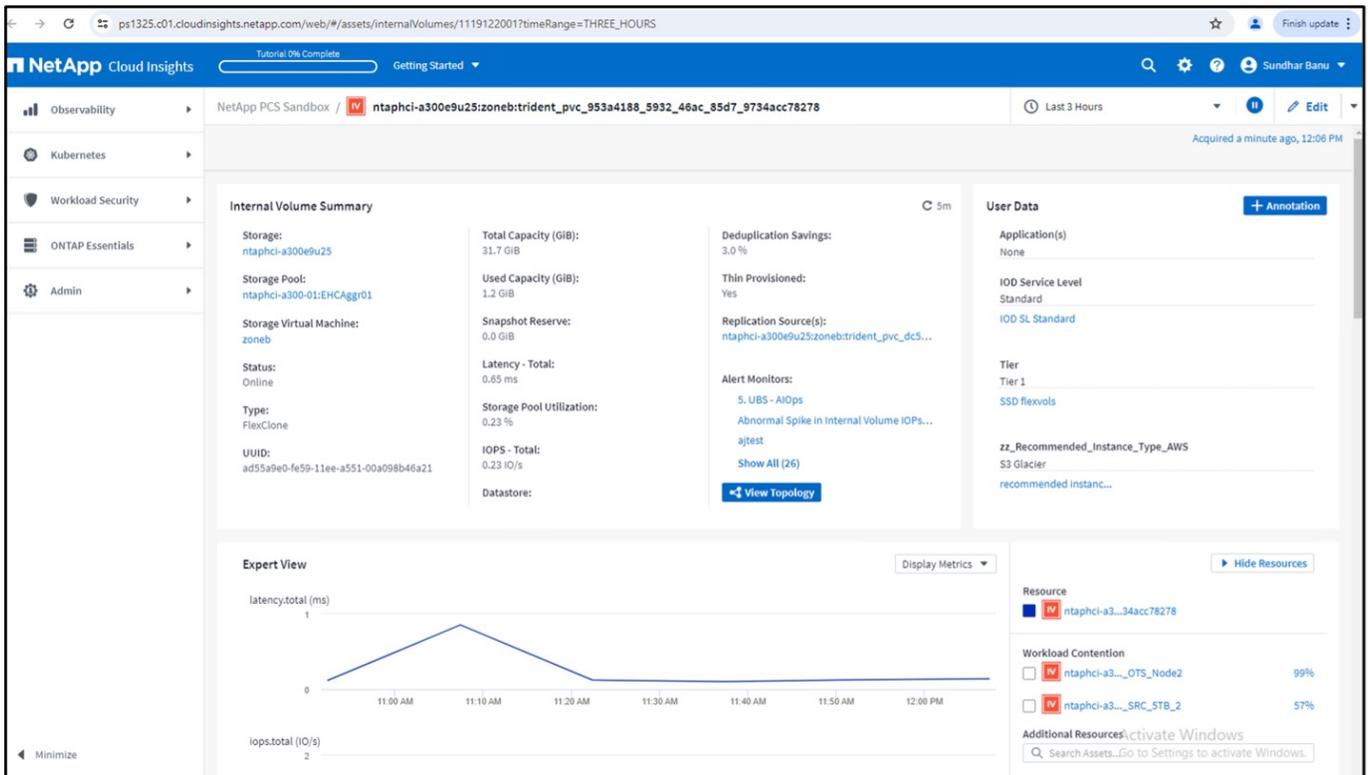
All Changes Diff			
Previous		New	
Expand 45 lines ...			
46	kind: DataVolume	46	kind: DataVolume
47	name: rhel9-demo-vm2	47	name: rhel9-demo-vm2
48	uid: dcf93b7a-71bc-409b-ad12-4916d05e0980	48	uid: dcf93b7a-71bc-409b-ad12-4916d05e0980
49	- resourceVersion: "8569671"	49	+ resourceVersion: "8619670"
50	uid: 953a4188-5932-46ac-85d7-9734acc78278	50	uid: 953a4188-5932-46ac-85d7-9734acc78278
51	spec:	51	spec:
52	accessModes:	52	accessModes:
Expand 15 lines ...			

Back-End-Speicherzuordnung

Mit Cloud Insights können Sie den Back-End Storage der VM-Festplatten und verschiedene Statistiken zu den VES problemlos einsehen.



Sie können auf die Links unter der Backend-Spalte klicken, die Daten direkt aus dem Back-End-ONTAP-Speicher ziehen.



Eine weitere Möglichkeit, sich das gesamte Pod-zu-Storage-Mapping anzusehen, ist das Erstellen einer Abfrage „Alle Metriken“ aus dem Observability Menü unter Explore.

The screenshot shows the "Explore" view in NetApp Cloud Insights. A query is defined for "persistent disks" with filters for "kubernetes_cluster" and "kubernetes_pod_to_storage". The results table is as follows:

Object	Filter by Attribute	Filter by Metric	Group By
kubernetes_pod_to_storage	kubernetes_cluster		kubernetes_pod_to_storage

Table Row Grouping	Metrics & Attributes
kubernetes_pod_to_storage ↑	persisten... workload... namespace storageVirt... InternalVol... volume.na... qtree.name timeToFull... backen
importer-prime-4f1b8351-2678-4295-b9db-64...	pvc-d4c2cecc-24b opershif-virtualization-os-image zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.16
importer-prime-8f792a39-02bb-4e86-a8a8-d5...	pvc-d50f56e7-3cf7 opershif-virtualization-os-image zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.16
virt-launcher-rhel9-demo-vm2-pdngg	pvc-98e342c0-20e virtual-machines-demo zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.00
virt-launcher-rhel9-demo-vm2-pdngg	pvc-953a188-99f virtual-machines-demo zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 3.88
virt-launcher-rhel9-demo-vm2-rnzj	pvc-f4d1adc3-314 virtual-machines zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 3.88
virt-launcher-rhel9-demo-vm2-rnzj	pvc-ad805a7b-4af virtual-machines zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.00

Wenn Sie auf einen der Links klicken, erhalten Sie die entsprechenden Informationen zum ONTP Storage. Wenn Sie beispielsweise in der Spalte storageVirtualMachine auf einen SVM-Namen klicken, werden Details zur SVM von ONTAP übertragen. Wenn Sie auf einen Namen für ein internes Volume klicken, werden Details zum Volume in ONTAP angezeigt.

storageVirtualMachin...	internalVolume.name	volume.na..
zation-os-image zoneb		ntaphci-a300e9u25:zoneb:trident_p
zation-os-image zoneb		ntaphci-a300e9u25:zoneb:trident_p
demo zoneb		ntaphci-a300e9u25:zoneb:trident_p
demo zoneb		ntaphci-a300e9u25:zoneb:trident_p
	zoneb	ntaphci-a300e9u25:zoneb:trident_p
	zoneb	ntaphci-a300e9u25:zoneb:trident_p

The screenshot displays the NetApp PCS Sandbox interface for a resource named 'zoneb'. It is divided into several sections:

- Storage Virtual Machine Summary:**
 - Type: Data
 - Status: Running
 - Storage: ntaphci-a300e9u25
 - Wpagent: Default
 - Allowed Protocols: cifs, nfs, smb, iqn, vifs, vvol
 - Internal Volume LVM: %s
 - Capacity (GB): 1,074.0 GB
 - Used Capacity (GB): 103.4 GB
 - Defragmentation Savings: 0.1 %
 - Compression Savings: 0.1 %
 - IOPS - Total: 26.21 IOPS
 - Latency - Total: 0.28 ms
 - Comment:
 - UUID: 335a91c1-c9f0-11e0-0100-000000000001
 - Alert Monitors:
- User Data:** Includes an 'Annotations' button.
- Expert View:** Contains two line graphs:
 - Latency (ms):** Shows latency fluctuating between approximately 0.10 and 0.30 ms over time.
 - IopsTotal (IOPS):** Shows total IOPS fluctuating between approximately 20 and 40 over time.
- Resource:** 'zoneb' is selected.
- Top Contributor:** 'ntaphci-a3...-eh-nc001' with 87% contribution.
- Additional Resources:** A search bar for assets.
- Alerts:** A section for alerts, currently showing 'Abnormal Spikes in Internal Volume IOPS...' with a 'View Topology' button.
- User Data (Detailed):**
 - Application(s): None
 - CTS_Monitoring: Disabled
 - CTS_Bulk: Disabled
 - K00 Service Level: VRTS
 - K00 % Util: 0%
 - Tier: Tier 1
 - SSD Reads: 0
 - Recommended_Instance_Type: VRTS
 - SS Stack: recommended instance...

Empfehlung Von Best Practices

Best Practices-Empfehlungen für VMs in Red hat OpenShift Virtualization

Autor: Banu Sundhar, NetApp

In diesem Abschnitt werden die verschiedenen Faktoren beschrieben, die Sie beim Bereitstellen neuer VMs oder beim Importieren vorhandener VMs aus VMware vSphere in OpenShift Virtualization auf der OpenShift Container Platform berücksichtigen sollten.

VM-Performance

Beim Erstellen einer neuen VM in OpenShift Virtualization müssen Sie das Zugriffsmuster sowie die Performance-Anforderungen (IOPS und Durchsatz) des Workloads berücksichtigen, der auf der VM ausgeführt wird. Dies beeinflusst die Anzahl der VMs, die Sie auf der OpenShift Virtualization in einer OpenShift-Container-Plattform ausführen müssen, sowie den Speichertyp, den Sie für die VM-Festplatten verwenden müssen.

Der Storage-Typ, den Sie für Ihre VM-Festplatten auswählen möchten, wird von folgenden Faktoren beeinflusst:

- Das Protokoll, das Sie für den Datenzugriff Ihrer Workloads benötigen
- Die benötigten Zugriffsmodi (RWO vs RWX)
- Performance-Merkmale, die Sie für Ihre Workloads benötigen

Weitere Informationen finden Sie im Abschnitt Speicherkonfiguration weiter unten.

Hochverfügbarkeit von VM-Workloads

OpenShift Virtualization unterstützt Live-Migrationen einer VM. Bei der Live-Migration kann eine laufende VM-Instanz (VMI) auf einen anderen Node verschoben werden, ohne den Workload zu unterbrechen. Die Migration kann besonders hilfreich sein für einen reibungslosen Übergang während eines Upgrades eines Clusters oder jedes Mal, wenn ein Node aufgrund von Wartungs- oder Konfigurationsänderungen nicht mehr benötigt wird. Für die Live-Migration ist die Verwendung einer gemeinsamen Speicherlösung erforderlich, die den Zugriffsmodus ReadWriteMany (RWX) bietet. Die VM-Festplatten sollten über eine Speicheroption gesichert werden, die den RWX-Zugriffsmodus bietet. OpenShift Virtualization überprüft, ob eine VMI **live migrierbar ist** und wenn ja, wird die **evictionStrategy** auf **LiveMigrate** gesetzt. Weitere Informationen finden Sie unter ["Informationen zum Abschnitt Live Migration in der Red hat Dokumentation"](#) .

Es ist wichtig, dass Sie einen Treiber verwenden, der **RWX**-Zugriffsmodus unterstützt. Im Abschnitt Speicherkonfiguration unten finden Sie weitere Informationen darüber, welche ONTAP-Treiber den RWX-Zugriffsmodus unterstützen.

Storage-Konfiguration

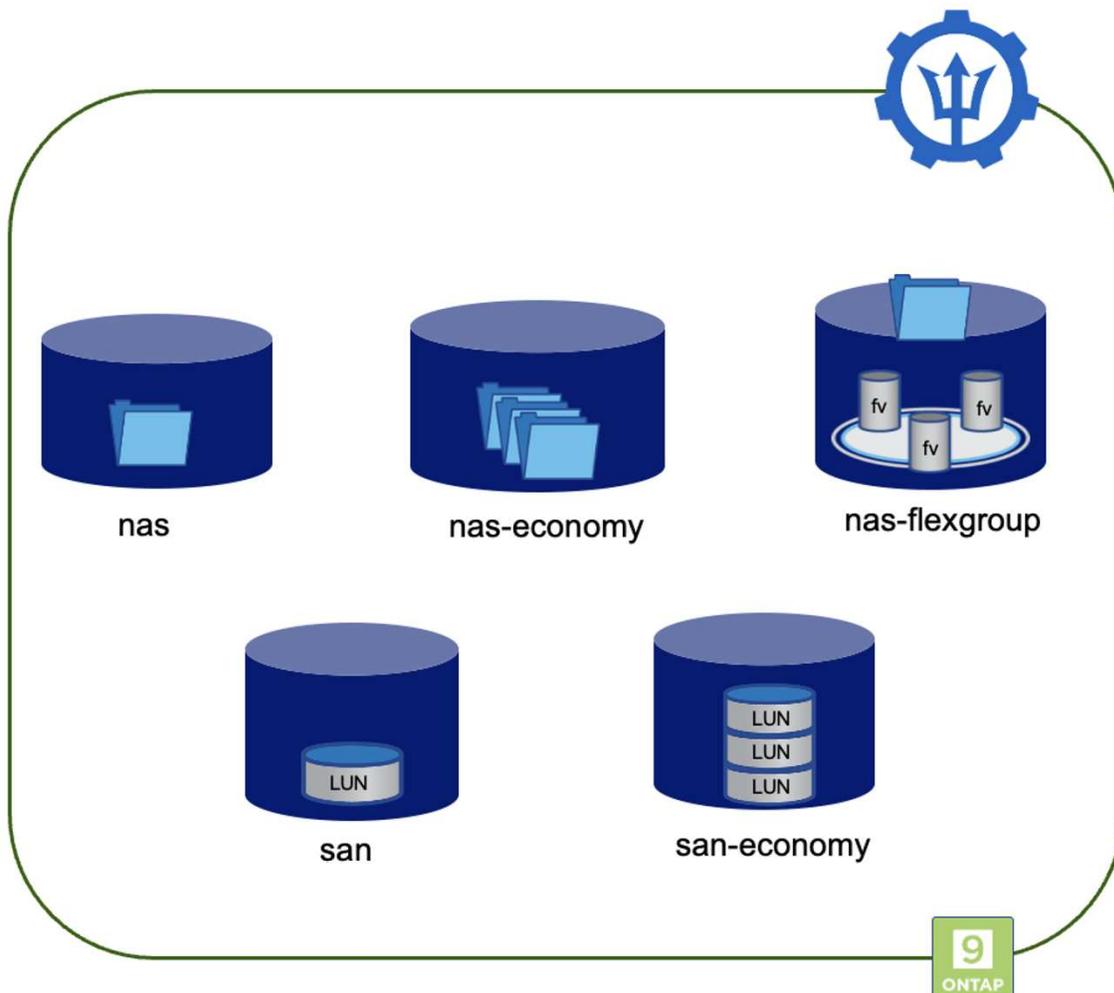
die CSI-bereitstellung von Trident bietet verschiedene Treiber (nas, nas-Economy, nas-FlexGroup, san und san-Economy) für die Provisionierung von Storage mit NetApp Storage-Optionen.

Verwendete Protokolle: * nas-Treiber verwenden NAS-Protokolle (NFS und SMB) * san-Treiber verwenden das iSCSI- oder NVMe/TCP-Protokoll

Die folgende Seite hilft Ihnen bei der Entscheidung, wie die Storage-Konfiguration auf der Basis der Workload-Anforderungen und der Storage-Auslastung konfiguriert werden soll.

- **nas**-Treiber erstellt ein persistentes Volume (PV) auf einem FlexVolume.
- **nas-Economy** Treiber erstellt ein PV auf einem qtree auf einem gemeinsamen FlexVolume. (Ein FlexVolume für je 200 PVS, konfigurierbar zwischen 50 und 300)
- **nas-FlexGroup** Treiber erstellt auf einem PV auf einem FlexGroup
- **san** Driver erstellt ein PV auf einer LUN auf einem dedizierten FlexVolume
- **san-Economy** Treiber erstellt ein PV auf LUN auf Shared FlexVolume (ein FlexVolume für alle 100 PVs, konfigurierbar zwischen 50 und 200)

Das folgende Diagramm veranschaulicht dies.



Außerdem unterscheiden sich die von den Treibern unterstützten Zugriffsmodi.

Unterstützung von ONTAP nas-Treibern

- Zugriff auf das Dateisystem und Zugriffsmodi RWO, ROX, RWX, RWOP.

ONTAP san-Treiber unterstützen sowohl RAW-Block- als auch Dateisystemmodi

- Im RAW-Block-Modus unterstützt er die Zugriffsmodi RWO, ROX, RWX, RWOP.
- Im Dateisystem-Modus sind nur RWO-, RWOP-Zugriffsmodi erlaubt.

Bei der Live-Migration von OpenShift Virtualization-VMs müssen die Festplatten über RWX-Zugriffsmodi verfügen. Daher ist es wichtig, dass Sie im reinen Block-Volume-Modus nas-Treiber oder san-Treiber auswählen, um VES und VES zu erstellen, die von ONTAP unterstützt werden.

Best Practices Für Die Speicherkonfiguration

Dedicated Storage Virtual Machines (SVMs)

Storage Virtual Machines (SVMs) sorgen für die Trennung von Mandanten auf einem ONTAP System. Die Zuweisung einer SVM für OpenShift-Container und OpenShift-Virtualisierungs-VMs ermöglicht die Delegation von Privileges und die Anwendung von Best Practices zur Begrenzung des Ressourcenverbrauchs.

Begrenzung der maximalen Volumenanzahl auf der SVM

Damit Trident nicht alle verfügbaren Volumes im Storage-System verbraucht, sollten Sie ein Limit für die SVM festlegen. Dies können Sie über die Befehlszeile ausführen:

```
vserver modify -vserver <svm_name> -max-volumes <num_of_volumes>
```

Der Wert für max-Volumes ist die Gesamtzahl der Volumes, die über alle Nodes im ONTAP Cluster bereitgestellt werden, nicht aber über einen einzelnen ONTAP Node. Aus diesem Grund treten möglicherweise einige Bedingungen auf, bei denen auf einem ONTAP Cluster-Node mehr oder weniger mit Trident bereitgestellte Volumes als ein anderer Node vorhanden sind. Um dies zu vermeiden, stellen Sie sicher, dass der von Trident verwendeten SVM dieselbe Anzahl von Aggregaten von jedem Node im Cluster zugewiesen wird.

Begrenzung der maximalen Größe der von Trident erstellten Volumes

Eine maximale Volume-Größe pro SVM kann in ONTAP festgelegt werden:

1. SVM mit dem Befehl `vserver create` erstellen und Storage-Grenze festlegen:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume root_volume_name -rootvolume-security-style {unix|ntfs|mixed} -storage -limit value
```

1. So ändern Sie die Speichergrenze für eine vorhandene SVM:

```
vserver modify -vserver vserver_name -storage-limit value -storage-limit -threshold-alert percentage
```



Storage-Limits können nicht für SVMs konfiguriert werden, die Datensicherungs-Volumes, Volumes in einer SnapMirror Beziehung oder in einer MetroCluster Konfiguration enthalten.

Neben der Kontrolle der Volume-Größe im Storage-Array sollten auch Kubernetes-Funktionen genutzt werden.

1. Um die maximale Größe für Volumes zu konfigurieren, die von Trident erstellt werden können, verwenden Sie den Parameter **limitVolumeSize** in Ihrer Backend.json-Definition.
2. Um die maximale Größe für FlexVols zu konfigurieren, die als Pools für ONTAP-san-Economy und ONTAP-nas-Economy-Treiber verwendet werden, verwenden Sie den Parameter **limitVolumePoolSize** in Ihrer Backend.json-Definition.

SVM QOS Policy verwenden

Wenden Sie die QoS-Richtlinie (Quality of Service) auf die SVM an, um die Anzahl der von den Trident bereitgestellten Volumes verbrauchbaren IOPS zu begrenzen. Dadurch wird verhindert, dass Workloads, die über Trident bereitgestellten Storage verwenden, Workloads außerhalb der Trident SVM beeinträchtigen.

ONTAP QoS-Richtliniengruppen bieten QoS-Optionen für Volumes und ermöglichen es Benutzern, die Durchsatzobergrenze für eine oder mehrere Workloads zu definieren. Weitere Informationen zu QoS-Richtliniengruppen finden Sie unter "[ONTAP 9.15 QoS-Befehle](#)"

Zugriff auf Storage-Ressourcen auf Kubernetes-Cluster-Mitglieder einschränken

Namespaces verwenden die Beschränkung des Zugriffs auf die von Trident erstellten NFS Volumes und iSCSI LUNs ist eine wichtige Komponente bei der Sicherheit Ihrer Kubernetes-Implementierung. Auf diese Weise wird verhindert, dass Hosts, die nicht zum Kubernetes Cluster gehören, auf die Volumes zugreifen und Daten unerwartet ändern können.

Außerdem kann ein Prozess in einem Container auf Speicher zugreifen, der auf den Host gemountet ist, aber nicht für den Container vorgesehen ist. Dieses Problem kann durch die Verwendung von Namespaces als logische Grenze für Ressourcen vermieden werden. Jedoch

Es ist wichtig zu wissen, dass Namespaces die logische Grenze für Ressourcen in Kubernetes sind. Daher ist es wichtig, sicherzustellen, dass Namespaces bei Bedarf zur Trennung verwendet werden. Privilegierte Container werden jedoch mit wesentlich mehr Berechtigungen auf Hostebene ausgeführt als normal. Deaktivieren Sie diese Funktion mit "[Pod-Sicherheitsrichtlinien](#)".

Verwenden Sie eine dedizierte Exportrichtlinie für OpenShift-Bereitstellungen mit dedizierten Infrastrukturlisten oder anderen Knoten, die keine Benutzeranwendungen planen können, sollten separate Exportrichtlinien verwendet werden, um den Zugriff auf Speicherressourcen weiter zu beschränken. Dies umfasst die Erstellung einer Exportrichtlinie für Services, die auf diesen Infrastruktur-Nodes bereitgestellt werden (z. B. OpenShift Metrics and Logging Services), sowie Standardanwendungen, die auf nicht-Infrastruktur-Nodes bereitgestellt werden.

Trident kann Richtlinien für den Export automatisch erstellen und managen. So beschränkt Trident den Zugriff auf die Volumes, die ihm im Kubernetes Cluster zur Verfügung stehen, und vereinfacht das Hinzufügen/Löschen von Nodes.

Wenn Sie jedoch eine Exportrichtlinie manuell erstellen, füllen Sie sie mit einer oder mehreren Exportrichtlinien aus, die jede Knotenzugriffsanforderung verarbeiten.

Disable showmount for the Application SVM Ein auf den Kubernetes-Cluster bereitgestellter Pod kann den showmount -e-Befehl gegen die Daten-LIF ausgeben und eine Liste der verfügbaren Mounts erhalten, einschließlich derjenigen, auf die er keinen Zugriff hat. Um dies zu verhindern, deaktivieren Sie die showmount-Funktion mithilfe der folgenden CLI:

```
vserver nfs modify -vserver <svm_name> -showmount disabled
```



Weitere Informationen zu Best Practices für die Storage-Konfiguration und die Trident-Verwendung finden Sie im Artikel "[Trident Dokumentation](#)".

OpenShift Virtualization - Tuning & Scaling Guide

Red hat dokumentiert "[OpenShift Cluster Scaling – Empfehlungen und Einschränkungen](#)".

Darüber hinaus haben sie auch dokumentiert "[OpenShift Virtualization Tuning Guide](#)" und "[Unterstützte Grenzwerte für OpenShift Virtualization 4.x](#)".



Für den Zugriff auf die oben genannten Inhalte ist eine aktive Red hat Subskription erforderlich.

Der Tuning-Leitfaden enthält Informationen zu vielen Tuning-Parametern, darunter:

- Tuning-Parameter zur Erstellung mehrerer VMs auf einmal oder in großen Stapeln
- Live-Migration von VMs
- "[Konfigurieren eines dedizierten Netzwerks für die Live-Migration](#)"
- Anpassung einer VM-Vorlage unter Berücksichtigung eines Workload-Typs

Die unterstützten Grenzwerte dokumentieren die Höchstwerte der getesteten Objekte, wenn VMs auf OpenShift ausgeführt werden

Höchstwerte für virtuelle Maschinen einschließlich

- Max. Virtuelle CPUs pro VM
- Max. Und Min. Des Arbeitsspeichers pro VM
- Max. Größe einer einzelnen Festplatte pro VM
- Maximale Anzahl der Hot-Plug-fähigen Festplatten pro VM

Host-Maximalwerte einschließlich * gleichzeitige Live-Migrationen (pro Node und Cluster)

Cluster-Maximalwerte einschließlich * maximale Anzahl definierter VMs

VMs von VMware Umgebung migrieren

Migration Toolkit for OpenShift Virtualization ist ein von Red hat bereitgestellter Betreiber, der über den OperatorHub der OpenShift Container Platform verfügbar ist. Dieses Tool kann zur Migration von VMs von vSphere, Red hat Virtualization, OpenStack und OpenShift Virtualization verwendet werden.

Weitere Informationen zur Migration von VMs von vSphere finden Sie unter [Workflows](#) > [Red hat OpenShift Virtualization with NetApp ONTAP](#)

Sie können Grenzwerte für verschiedene Parameter entweder über die CLI oder über die Migrationswebkonsole konfigurieren. Einige Beispiele sind unten angegeben

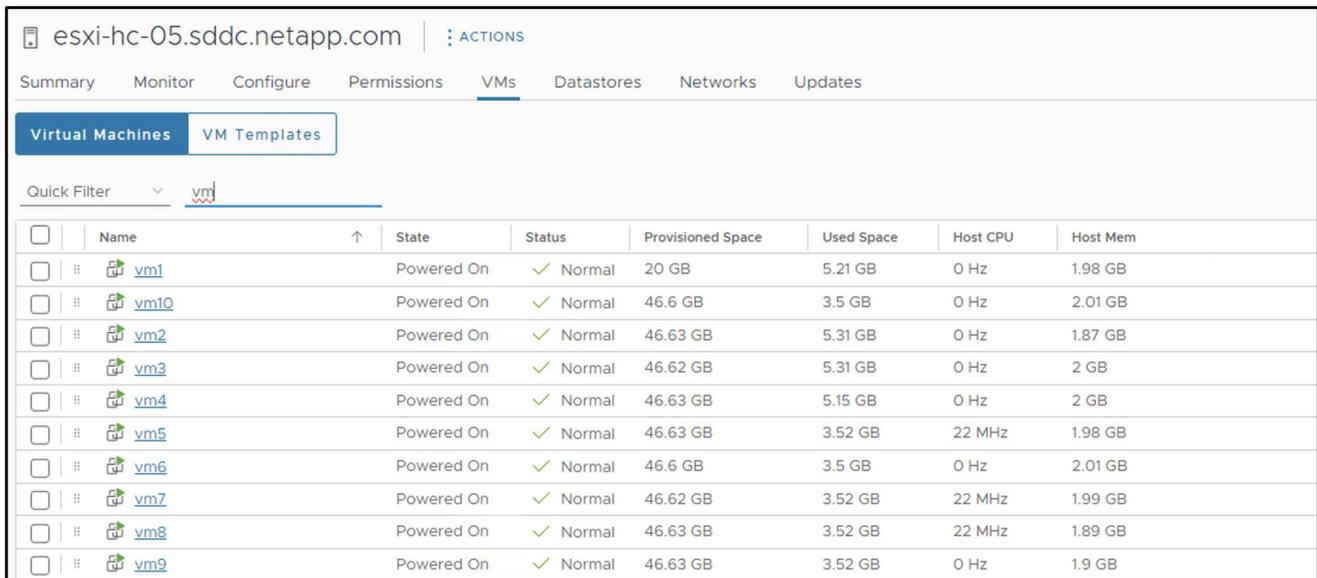
1. Durch die maximale Anzahl gleichzeitiger Migrationen virtueller Maschinen wird die maximale Anzahl gleichzeitig migrierter VMs festgelegt. Der Standardwert ist 20 virtuelle Maschinen.
2. PreCopy-Intervall (Minuten) steuert das Intervall, in dem ein neuer Snapshot angefordert wird, bevor eine warme Migration gestartet wird. Der Standardwert ist 60 Minuten.
3. Das Snapshot-Polling-Intervall (Sekunden) bestimmt, mit welcher Häufigkeit das System den Status der

Snapshot-Erstellung bzw. -Entfernung während der oVirt Warmmigration überprüft. Der Standardwert ist 10 Sekunden.

Wenn Sie mehr als 10 VMs von einem ESXi-Host im selben Migrationsplan migrieren, müssen Sie den NFC-Dienstspeicher des Hosts erhöhen. Andernfalls schlägt die Migration fehl, da der Speicher des NFC-Dienstes auf 10 parallele Verbindungen beschränkt ist. Weitere Informationen finden Sie in der Red hat Dokumentation: ["Erhöhen des NFC-Dienstspeichers eines ESXi-Hosts"](#)

Hier finden Sie eine erfolgreiche parallele Migration von 10 VMs vom selben Host in vSphere zu OpenShift Virtualization mit dem Migration Toolkit für Virtualisierung.

VMs auf demselben ESXi-Host



The screenshot shows the vSphere Web Client interface for an ESXi host named 'esxi-hc-05.sddc.netapp.com'. The 'VMs' tab is selected, displaying a list of 10 virtual machines. The table includes columns for Name, State, Status, Provisioned Space, Used Space, Host CPU, and Host Mem. All VMs are in a 'Powered On' state with a 'Normal' status.

	Name	↑	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
<input type="checkbox"/>	vm1		Powered On	✓ Normal	20 GB	5.21 GB	0 Hz	1.98 GB
<input type="checkbox"/>	vm10		Powered On	✓ Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
<input type="checkbox"/>	vm2		Powered On	✓ Normal	46.63 GB	5.31 GB	0 Hz	1.87 GB
<input type="checkbox"/>	vm3		Powered On	✓ Normal	46.62 GB	5.31 GB	0 Hz	2 GB
<input type="checkbox"/>	vm4		Powered On	✓ Normal	46.63 GB	5.15 GB	0 Hz	2 GB
<input type="checkbox"/>	vm5		Powered On	✓ Normal	46.63 GB	3.52 GB	22 MHz	1.98 GB
<input type="checkbox"/>	vm6		Powered On	✓ Normal	46.6 GB	3.5 GB	0 Hz	2.01 GB
<input type="checkbox"/>	vm7		Powered On	✓ Normal	46.62 GB	3.52 GB	22 MHz	1.99 GB
<input type="checkbox"/>	vm8		Powered On	✓ Normal	46.63 GB	3.52 GB	22 MHz	1.89 GB
<input type="checkbox"/>	vm9		Powered On	✓ Normal	46.63 GB	3.52 GB	0 Hz	1.9 GB

Zunächst wird Ein Plan für die Migration von 10 VMs von VMware erstellt

Project: openshift-ntv

Plans > Plan Details

ten-vms-from-same-host Succeeded Actions

Details YAML **Virtual Machines** Resources Mappings Hooks

Virtual Machines

Pipeline status Name Filter by name Remove virtual machines

Name	Started at	Completed at	Disk transfer	Disk counter	Pipeline status
vm1	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:41 AM	20480 / 20480 MB	- / 1 Disks	●
vm2	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:41 AM	20480 / 20480 MB	- / 1 Disks	●
vm3	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	●
vm4	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:42 AM	20480 / 20480 MB	- / 1 Disks	●
vm5	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:42 AM	20480 / 20480 MB	- / 1 Disks	●
vm6	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	●
vm7	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	●
vm8	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	●
vm9	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:38 AM	20480 / 20480 MB	- / 1 Disks	●
vm10	Sep 16, 2024, 10:23 AM	Sep 16, 2024, 10:37 AM	20480 / 20480 MB	- / 1 Disks	●

Alle 10 VMs befinden sich in einem laufenden Zustand in OpenShift Virtualization

Project: ten-vms-from-same-host

VirtualMachines Create

Filter Name Search by name... 1-10 of 10 1 of 1

Name	Status	Conditions	Node	IP address
vm1	Running		ocp7-worker3	-
vm2	Running		ocp7-worker1	-
vm3	Running		ocp7-worker2	-
vm4	Running		ocp7-worker1	-
vm5	Running		ocp7-worker2	-
vm6	Running		ocp7-worker2	-
vm7	Running		ocp7-worker1	-
vm8	Running		ocp7-worker3	-
vm9	Running		ocp7-worker2	-
vm10	Running		ocp7-worker1	-

Weitere Informationen: Red hat OpenShift mit NetApp

Sehen Sie sich die folgenden Websites an, um mehr über die in diesem Dokument beschriebenen Daten zu erfahren:

- NetApp Dokumentation

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Trident-Dokumentation

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- NetApp Astra Control Center - Dokumentation

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Red hat OpenShift-Dokumentation

["https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/)

- Dokumentation der Red hat OpenStack Platform

["https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/16.1/"](https://access.redhat.com/documentation/en-us/red_hat_openstack_platform/16.1/)

- Red Hat Virtualization Documentation

["https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/"](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/)

- Dokumentation zu VMware vSphere

["https://docs.vmware.com/"](https://docs.vmware.com/)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.