Red hat OpenShift mit NetApp

NetApp Solutions

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/containers/rh-os-n_openshift_BM.html on April 24, 2024. Always check docs.netapp.com for the latest.

Inhalt

NVA-1160: Red hat OpenShift mit NetApp . . . 1
Anwendungsfälle . . . 1
Geschäftlicher Nutzen . . . 1
Technologieüberblick . . . 1
Erweiterte Konfigurationsoptionen . . . 2
Aktuelle Support-Matrix für validierte Versionen . . . 2
OpenShift Übersicht . . . 3
NetApp Storage-Überblick . . . 18
Überblick über die NetApp Storage-Integration . . . 23
Erweiterte Konfigurationsoptionen . . . 73
Lösungsvalidierung und Anwendungsfälle: Red hat OpenShift mit NetApp . . . 100
Videos und Demos: Red hat OpenShift mit NetApp . . . 199
Weitere Informationen: Red hat OpenShift mit NetApp . . . 199

NVA-1160: Red hat OpenShift mit NetApp

Alan Cowles und Nikhil M Kulkarni, NetApp

Dieses Referenzdokument validiert die Red hat OpenShift-Lösung, die über IPI (Installer Provisioned Infrastructure) in verschiedenen Datacenter-Umgebungen bereitgestellt wird, wie von NetApp validiert. Sie Details zur Storage-Integration in NetApp Storage-Systeme dank des Astra Trident Storage-Orchestrator für das Management von persistentem Storage. Abschließend werden eine Reihe von Validierungen von Lösungen und Anwendungsbeispiele aus der Praxis untersucht und dokumentiert.

Anwendungsfälle

Die Architektur von Red hat OpenShift mit NetApp bietet Kunden folgende Vorteile:

- Einfache Bereitstellung und Verwaltung von Red hat OpenShift, bereitgestellt mit IPI (Installer Provisioned Infrastructure) auf Bare Metal, Red hat OpenStack Platform, Red hat Virtualization und VMware vSphere.
- Kombinierte Leistung von Enterprise-Containern und virtualisierten Workloads mit Red hat OpenShift, die virtuell auf OSP, RHV oder vSphere oder Bare Metal mit OpenShift Virtualization bereitgestellt wird
- Konfigurationsmöglichkeiten in der Praxis und Anwendungsfälle, in denen die Funktionen von Red hat OpenShift im Einsatz mit NetApp Storage und Astra Trident, dem Open-Source-Storage-Orchestrator für Kubernetes, hervorgehoben werden.

Geschäftlicher Nutzen

Unternehmen führen zunehmend DevOps-Praktiken ein, um neue Produkte zu erstellen, Release-Zyklen zu verkürzen und neue Funktionen hinzuzufügen. Dank ihrer angeborenen Agilität spielen Container und Microservices eine entscheidende Rolle bei der Unterstützung von DevOps-Praktiken. Das Praktizieren von DevOps auf Produktionsskala in einer Enterprise-Umgebung stellt jedoch ihre eigenen Herausforderungen und stellt bestimmte Anforderungen an die zugrunde liegende Infrastruktur, wie beispielsweise die folgenden:

- Hochverfügbarkeit auf allen Ebenen im Stack
- Einfache Implementierungsverfahren
- Unterbrechungsfreier Betrieb und Upgrades
- API-gestützte, programmierbare Infrastruktur, um die Flexibilität von Microservices Schritt zu halten
- Mandantenfähigkeit mit garantierter Performance
- Gleichzeitige Ausführung virtualisierter und Container-Workloads
- Unabhängige Skalierung der Infrastruktur je nach Workload-Anforderungen

Red hat OpenShift mit NetApp kennt diese Herausforderungen und präsentiert eine Lösung, mit der sich alle Bedenken lösen lassen. Hierzu wird die vollständig automatisierte Implementierung von RedHat OpenShift IPI in der vom Kunden gewünschten Datacenter-Umgebung implementiert.

Technologieüberblick

Die Lösung Red hat OpenShift mit NetApp umfasst die folgenden Hauptkomponenten:

Red hat OpenShift Container Platform

Die Container-Plattform Red hat OpenShift ist eine vollständig unterstützte Kubernetes-Plattform für Unternehmen. Red hat verbessert Open-Source-Kubernetes und stellt damit eine Applikationsplattform bereit, die vollständig integriert ist, um Container-Applikationen zu erstellen, bereitzustellen und zu managen.

Weitere Informationen finden Sie auf der OpenShift Website "Hier".

NetApp Storage-Systeme

NetApp verfügt über verschiedene Storage-Systeme, die sich perfekt für Enterprise Datacenter und Hybrid-Cloud-Implementierungen eignen. Das NetApp Portfolio umfasst NetApp ONTAP, NetApp Element und NetApp E-Series Storage-Systeme, die persistenten Storage für Container-Applikationen bereitstellen können.

Weitere Informationen finden Sie auf der NetApp Website "Hier".

NetApp Storage-Integrationen

Das NetApp Astra Control Center bietet eine umfassende Auswahl an Storage- und applikationsspezifischen Datenmanagement-Services für zustandsorientierte Kubernetes Workloads, die in einer On-Premises-Umgebung implementiert und mit der bewährten NetApp Datensicherungstechnologie unterstützt werden.

Weitere Informationen finden Sie auf der NetApp Astra Website "Hier".

Astra 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 Astra Trident Website "Hier".

Erweiterte Konfigurationsoptionen

Dieser Abschnitt richtet sich an Anpassungen, die reale Benutzer wahrscheinlich bei der Implementierung dieser Lösung in der Produktion ausführen müssen, wie z. B. die Erstellung einer dedizierten privaten Image-Registrierung oder die Implementierung benutzerdefinierter Load Balancer-Instanzen.

Aktuelle Support-Matrix für validierte Versionen

Technologie	Zweck	Softwareversion
NetApp ONTAP	Storage	9.8, 9.9.1
NetApp Element	Storage	12.3
NetApp Astra Control Center	Applikationsspezifisches Datenmanagement	21.12.60
NetApp Astra Trident	Storage-Orchestrierung	22.01.0
Red hat OpenShift	Container-Orchestrierung	4.6 EUS, 4.7, 4.8
Red hat OpenStack Platform	Private Cloud-Infrastruktur	16.1
Red Hat Virtualization	Datacenter-Virtualisierung	4.4
VMware vSphere	Datacenter-Virtualisierung	6.7U3

OpenShift Übersicht

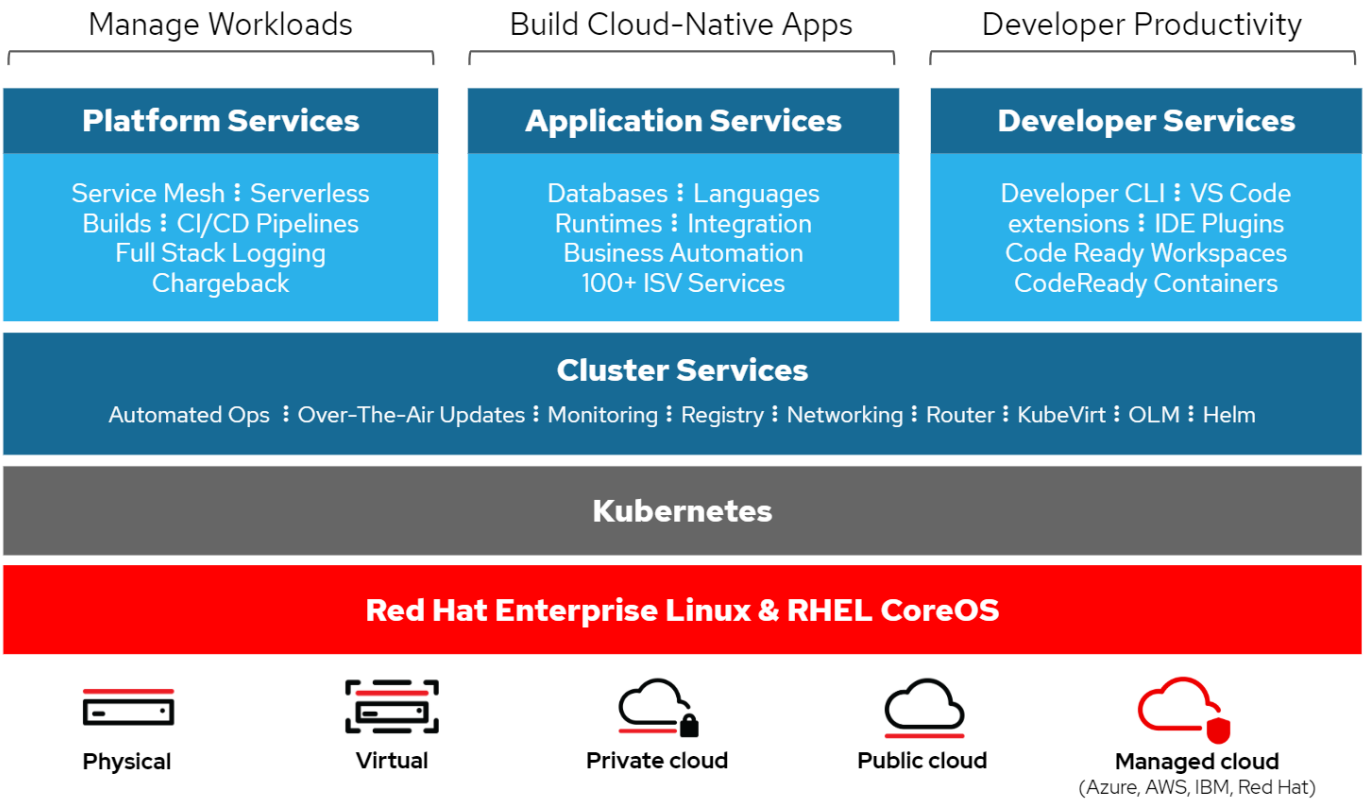
Die Container-Plattform Red hat OpenShift vereint Entwicklungs- und IT-Abläufe auf einer einzigen Plattform, um Anwendungen konsistent in lokalen und Hybrid-Cloud-Infrastrukturen zu erstellen, bereitzustellen und zu managen. Red hat OpenShift basiert auf Open-Source-Innovationen und Branchenstandards, einschließlich Kubernetes und Red hat Enterprise Linux CoreOS, der weltweit führenden Linux-Distribution für Container-basierte Workloads. OpenShift ist Teil des CNCF-zertifizierten Kubernetes-Programms Cloud Native Computing Foundation (Cloud Native Computing Foundation) und bietet Portabilität und Interoperabilität für Container-Workloads.

Red hat OpenShift bietet die folgenden Funktionen:

- **Self-Service-Bereitstellung** Entwickler können mit den Tools, die sie am meisten verwenden, schnell und einfach Anwendungen nach Bedarf erstellen, während der Betrieb die volle Kontrolle über die gesamte Umgebung behält.
- **Persistenter Speicher** durch die Unterstützung für persistenten Speicher ermöglicht Ihnen OpenShift Container Platform sowohl zustandsbehaftete Anwendungen als auch Cloud-native zustandslose Anwendungen.
- **Continuous Integration und Continuous Development (CI/CD)** Diese Quellcode-Plattform verwaltet Build- und Deployment-Images im großen Maßstab.
- **Open-Source-Standards** Diese Standards integrieren die Open Container Initiative (OCI) und Kubernetes für die Container-Orchestrierung zusätzlich zu anderen Open-Source-Technologien. Sie sind nicht auf die Technologie oder die Business-Roadmap eines bestimmten Anbieters beschränkt.
- **CI/CD Pipelines** OpenShift bietet sofort einsetzbare Unterstützung für CI/CD Pipelines, sodass Entwicklungsteams jeden Schritt des Application Delivery Prozesses automatisieren können und sicherstellen, dass es bei jeder Änderung am Code oder an der Konfiguration der Applikation ausgeführt wird.
- **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)** Diese Funktion bietet Team- und Benutzerverfolgung, um eine große Entwicklergruppe zu organisieren.
- **Automatisiertes Erstellen und Bereitstellen** OpenShift bietet Entwicklern die Möglichkeit, ihre Container-Anwendungen zu erstellen oder die Plattform die Container aus dem Anwendungsquellcode oder sogar aus den Binärdateien erstellen zu lassen. Die Plattform automatisiert dann die Implementierung dieser Applikationen in der gesamten Infrastruktur anhand der für die Applikationen definierten Merkmale. Beispiel: Wie viele Ressourcen sollten zugewiesen werden und wo in der Infrastruktur sie implementiert werden sollen, damit sie mit Lizenzen von Drittanbietern konform sind?
- **Konsistente Umgebungen** OpenShift stellt sicher, dass die für Entwickler bereitgestellte Umgebung über den gesamten Lebenszyklus der Anwendung hinweg vom Betriebssystem bis zu Bibliotheken, Laufzeitversion (z. B. Java Runtime) konsistent ist, und sogar die verwendete Anwendungslaufzeit (z. B. Tomcat), um die Risiken aus inkonsistenten Umgebungen zu beseitigen.
- **Konfigurationsmanagement** die Konfiguration und das sensible Datenmanagement sind in die Plattform integriert, um sicherzustellen, dass eine konsistente und umgebungsanunabhängige Anwendungskonfiguration für die Anwendung bereitgestellt wird, unabhängig davon, welche Technologien für die Erstellung der Anwendung verwendet werden oder welche Umgebung sie ist Bereitgestellt.
- **Anwendungsprotokolle und Metrik** schnelles Feedback ist ein wichtiger Aspekt der Anwendungsentwicklung. Die integrierte Überwachungs- und Protokollverwaltung von OpenShift stellt Entwicklern sofort Kennzahlen zur Verfügung, um zu untersuchen, wie sich die Anwendung über

Änderungen hinweg verhält, und Probleme so früh wie möglich im Applikationslebenszyklus beheben zu können.

- **Sicherheits- und Containerkatalog** OpenShift bietet Mandantenfähigkeit und schützt den Benutzer vor schädlicher Codeausführung durch die Verwendung etablierter Sicherheit mit Security-Enhanced Linux (SELinux), CGroups und Secure Computing Mode (seccomp), um Container zu isolieren und zu schützen. Darüber hinaus bietet es Verschlüsselung über TLS-Zertifikate für die verschiedenen Subsysteme sowie Zugriff auf Red hat zertifizierte Container (access.redhat.com/containers), die mit besonderem Schwerpunkt auf Sicherheit gescannt und bewertet werden, um Endbenutzern zertifizierte, vertrauenswürdige und sichere Anwendungs-Container bereitzustellen.



Bereitstellungsmethoden für Red hat OpenShift

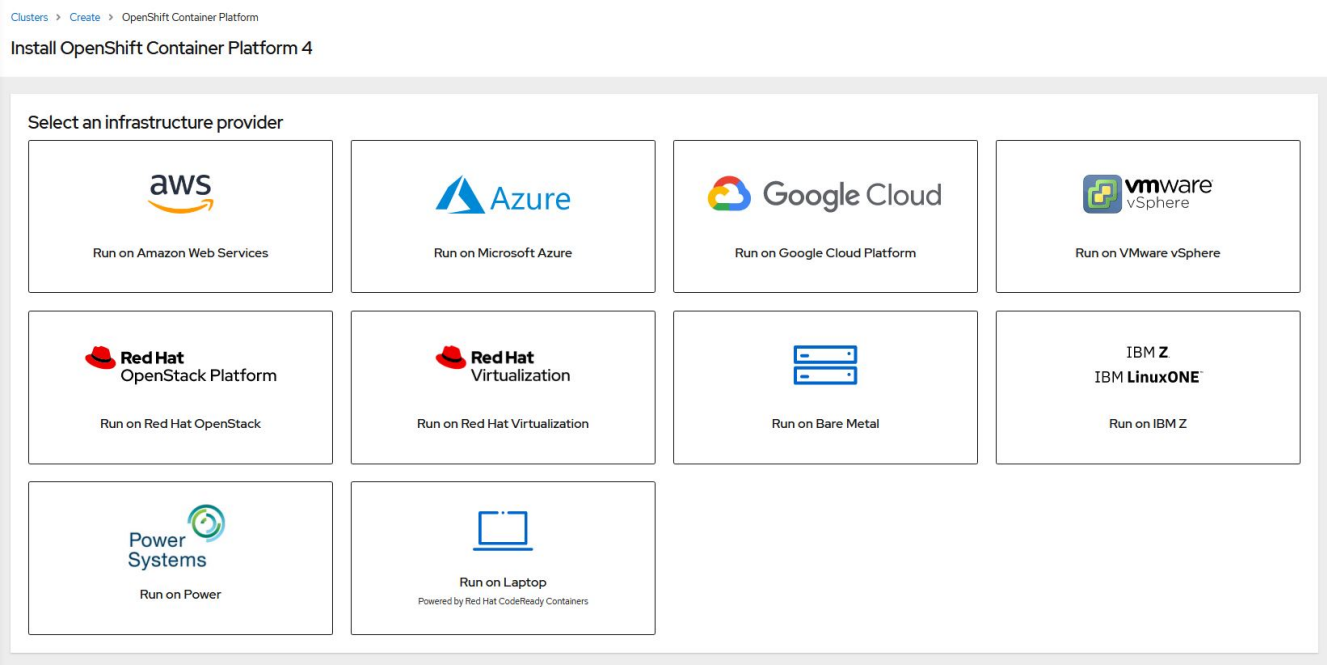
Ab Red hat OpenShift 4 umfassen die Bereitstellungsmethoden für OpenShift manuelle Bereitstellungen mithilfe von User Provisioned Infrastructure (UPI) für stark angepasste Bereitstellungen oder vollständig automatisierte Bereitstellungen mithilfe von Installer Provisioned Infrastructure (IPI).

Die IPI-Installationsmethode ist in den meisten Fällen die bevorzugte Methode, da sie die schnelle Implementierung von OpenShift-Clustern für Entwicklungs-, Test- und Produktionsumgebungen ermöglicht.

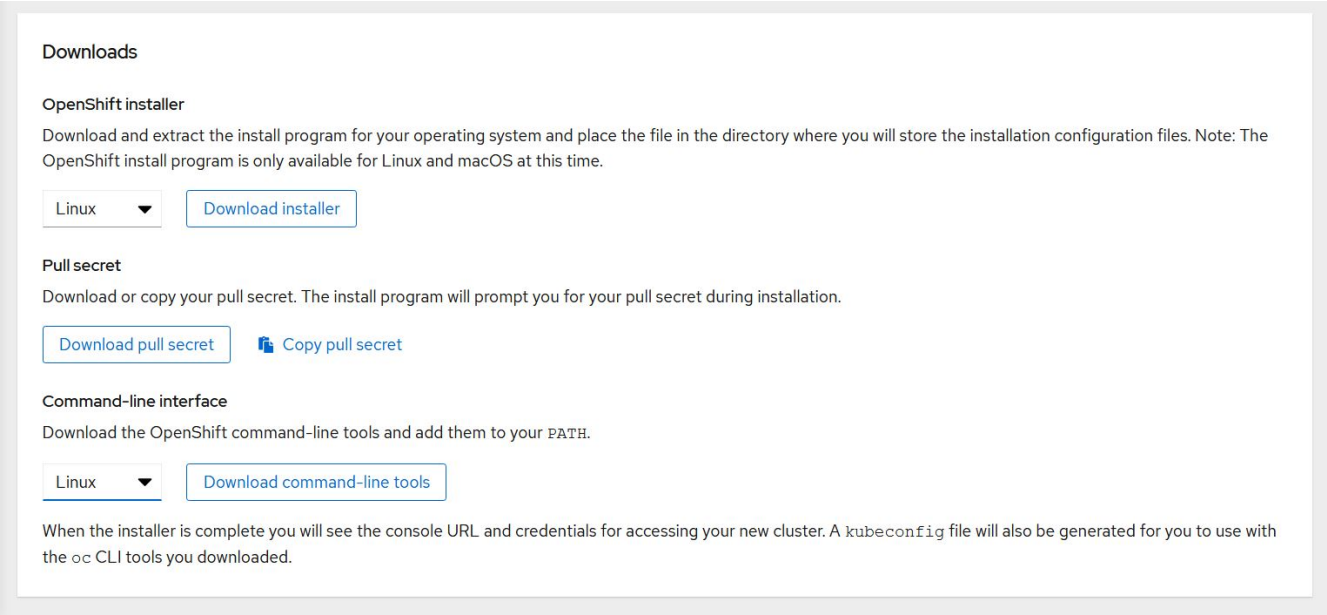
IPI-Installation von Red hat OpenShift

Die Bereitstellung von OpenShift für die installierte Infrastruktur (Installer Provisioned Infrastructure, IPI) umfasst die folgenden grundlegenden Schritte:

1. Besuchen Sie Red hat OpenShift "Website" Und melden Sie sich mit Ihren SSO-Anmeldedaten an.
2. Wählen Sie die Umgebung aus, in der Red hat OpenShift bereitgestellt werden soll.



3. Laden Sie auf dem nächsten Bildschirm das Installationsprogramm, den eindeutigen Pull-Secret und die CLI-Tools zur Verwaltung herunter.



4. Folgen Sie den "Installationsanweisungen" Von Red hat zur Bereitstellung in Ihrer bevorzugten Umgebung bereitgestellt.

Validierte OpenShift-Implementierungen durch NetApp

NetApp hat die Implementierung von Red hat OpenShift in seinen Labs mithilfe der Bereitstellungsmethode IPI (Installer Provisioning Infrastructure) in den folgenden Datacenter-Umgebungen getestet und validiert:

- "OpenShift auf Bare Metal"
- "OpenShift auf der Red hat OpenStack Platform"
- "OpenShift auf Red hat Virtualization"

- "OpenShift auf VMware vSphere"

OpenShift auf Bare Metal

OpenShift auf Bare Metal ermöglicht eine automatisierte Bereitstellung der OpenShift Container Platform auf Standard-Servern.

OpenShift auf Bare Metal ähnelt den virtuellen OpenShift-Implementierungen, die eine einfache Implementierung, schnelle Provisionierung und Skalierung von OpenShift-Clustern ermöglichen. Gleichzeitig werden virtualisierte Workloads für Applikationen unterstützt, die nicht containerisiert werden können. Durch die Implementierung auf Bare Metal-Servern ist neben der OpenShift-Umgebung kein zusätzlicher Overhead für das Management der Host-Hypervisor-Umgebung erforderlich. Durch die direkte Bereitstellung auf Bare Metal-Servern sind zudem weniger physische Overhead-Einschränkungen möglich, wenn Ressourcen zwischen dem Host und der OpenShift-Umgebung gemeinsam genutzt werden müssen.

OpenShift auf Bare Metal bietet folgende Funktionen:

- **IPI oder assistierte Installerbereitstellung** mit einem OpenShift-Cluster, der von Installer Provisioned Infrastructure (IPI) auf Bare-Metal-Servern bereitgestellt wird, können Kunden eine äußerst vielseitige, einfach skalierbare OpenShift-Umgebung direkt auf herkömmlichen Servern bereitstellen, ohne dass eine Hypervisor-Schicht verwaltet werden muss.
- **Kompaktes Clusterdesign** um die Hardwareanforderungen zu minimieren, ermöglicht OpenShift auf Bare Metal Benutzern die Bereitstellung von Clustern mit nur 3 Knoten, indem die OpenShift-Steuerungsebenen-Knoten auch als Workerknoten und Host-Container fungieren können.
- **OpenShift Virtualization** OpenShift kann virtuelle Maschinen innerhalb von Containern mit OpenShift Virtualization ausführen. Bei dieser Container-nativen Virtualisierung wird der KVM-Hypervisor innerhalb eines Containers ausgeführt und persistente Volumes für den VM-Storage angebunden.
- **KI/ML-optimierte Infrastruktur** Bereitstellen von Anwendungen wie Kubeflow für Machine-Learning-Anwendungen durch Einbindung GPU-basierter Workerknoten in Ihre OpenShift-Umgebung und Nutzung von OpenShift Advanced Scheduling.

Netzwerkdesign

Die Red hat OpenShift on NetApp Lösung verwendet zwei Daten-Switches für die primäre Datenkonnektivität mit 25 Gbit/s. Zudem werden zwei Management-Switches mit 1 Gbit/s für in-Band-Management der Storage-Nodes und bandexternen Management für IPMI-Funktionen verwendet.

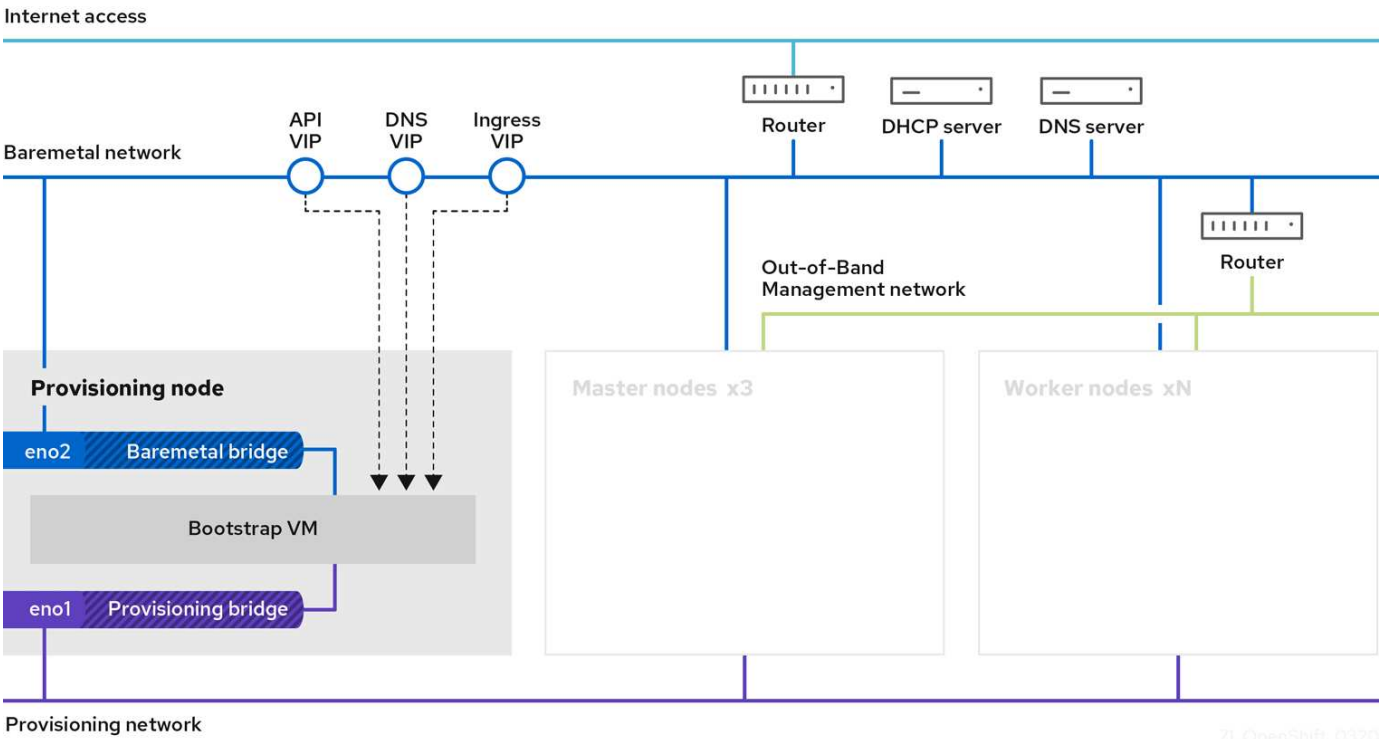
Für eine Bare-Metal-IPI-Bereitstellung mit OpenShift müssen Sie einen bereitstellungsknoten erstellen, einen Red hat Enterprise Linux 8-Rechner, für den Netzwerkschnittstellen mit separaten Netzwerken verbunden sein müssen.

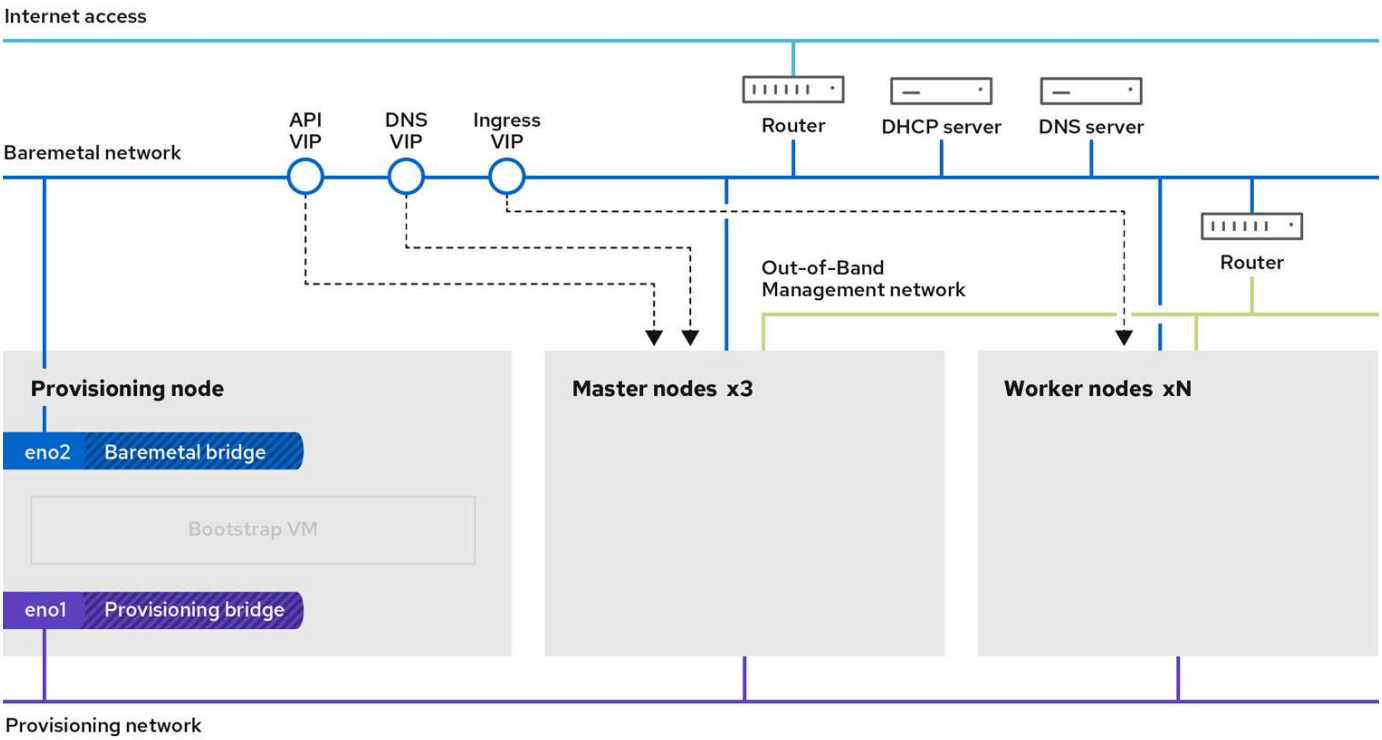
- **Provisioning-Netzwerk** Dieses Netzwerk wird verwendet, um die Bare-Metal-Knoten zu starten und die notwendigen Images und Pakete zu installieren, um den OpenShift-Cluster bereitzustellen.
- **Bare-Metal-Netzwerk** Dieses Netzwerk wird nach der Bereitstellung für die öffentliche Kommunikation des Clusters verwendet.

Für das Setup des bereitstellungsknoten erstellt der Kunde Bridge-Schnittstellen, die es dem Traffic ermöglichen, auf dem Node selbst und auf der Bootstrap-VM, die für Bereitstellungszwecke bereitgestellt wird, ordnungsgemäß zu leiten. Nach der Bereitstellung des Clusters werden die API- und Ingress-VIP-Adressen vom Bootstrap-Node zum neu implementierten Cluster migriert.

Die folgenden Bilder zeigen die Umgebung sowohl während der IPI-Bereitstellung als auch nach Abschluss

der Bereitstellung.





VLAN-Anforderungen

Die Lösung Red hat OpenShift mit NetApp wurde speziell zur logischen Trennung des Netzwerk-Traffic für unterschiedliche Zwecke mithilfe von Virtual Local Area Networks (VLANs) entwickelt.

VLANs	Zweck	VLAN-ID
Out-of-Band-Managementnetzwerk	Management für Bare-Metal-Nodes und IPMI	16
Bare-Metal-Netzwerk	Netzwerk für OpenShift-Services, sobald Cluster verfügbar ist	181
Bereitstellung von Netzwerken	Netzwerk für PXE-Boot und Installation von Bare Metal-Knoten über IPI	3485

Obwohl jedes dieser Netzwerke virtuell durch VLANs getrennt ist, muss jeder physische Port im Zugriffsmodus mit dem zugewiesenen primären VLAN eingerichtet werden, da es während einer PXE-Startsequenz keine Möglichkeit gibt, ein VLAN-Tag zu übergeben.

Support-Ressourcen für die Netzwerkinfrastruktur

Vor der Bereitstellung der OpenShift-Container-Plattform sollte die folgende Infrastruktur vorhanden sein:

- Mindestens ein DNS-Server, der eine vollständige Host-Name-Auflösung bietet, auf die über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.
- Mindestens ein NTP-Server, auf den über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.
- (Optional) ausgehende Internetverbindung sowohl für das bandinterne Managementnetzwerk als auch für das VM-Netzwerk.

OpenShift auf der Red hat OpenStack Platform

Die Red hat OpenStack Platform bietet eine integrierte Grundlage zur Erstellung, Implementierung und Skalierung einer sicheren und zuverlässigen OpenStack Private Cloud.

OSP ist eine IaaS-Cloud (Infrastruktur als Service), die durch eine Sammlung von Kontroll-Services implementiert wird und Computing-, Storage- und Netzwerkressourcen managt. Die Umgebung wird über eine webbasierte Schnittstelle gemanagt, die es Administratoren und Benutzern ermöglicht, OpenStack Ressourcen zu kontrollieren, bereitzustellen und zu automatisieren. Darüber hinaus wird die OpenStack Infrastruktur durch eine umfangreiche Befehlszeilenschnittstelle und API erleichtert, die umfassende Automatisierungsfunktionen für Administratoren und Endbenutzer ermöglichen.

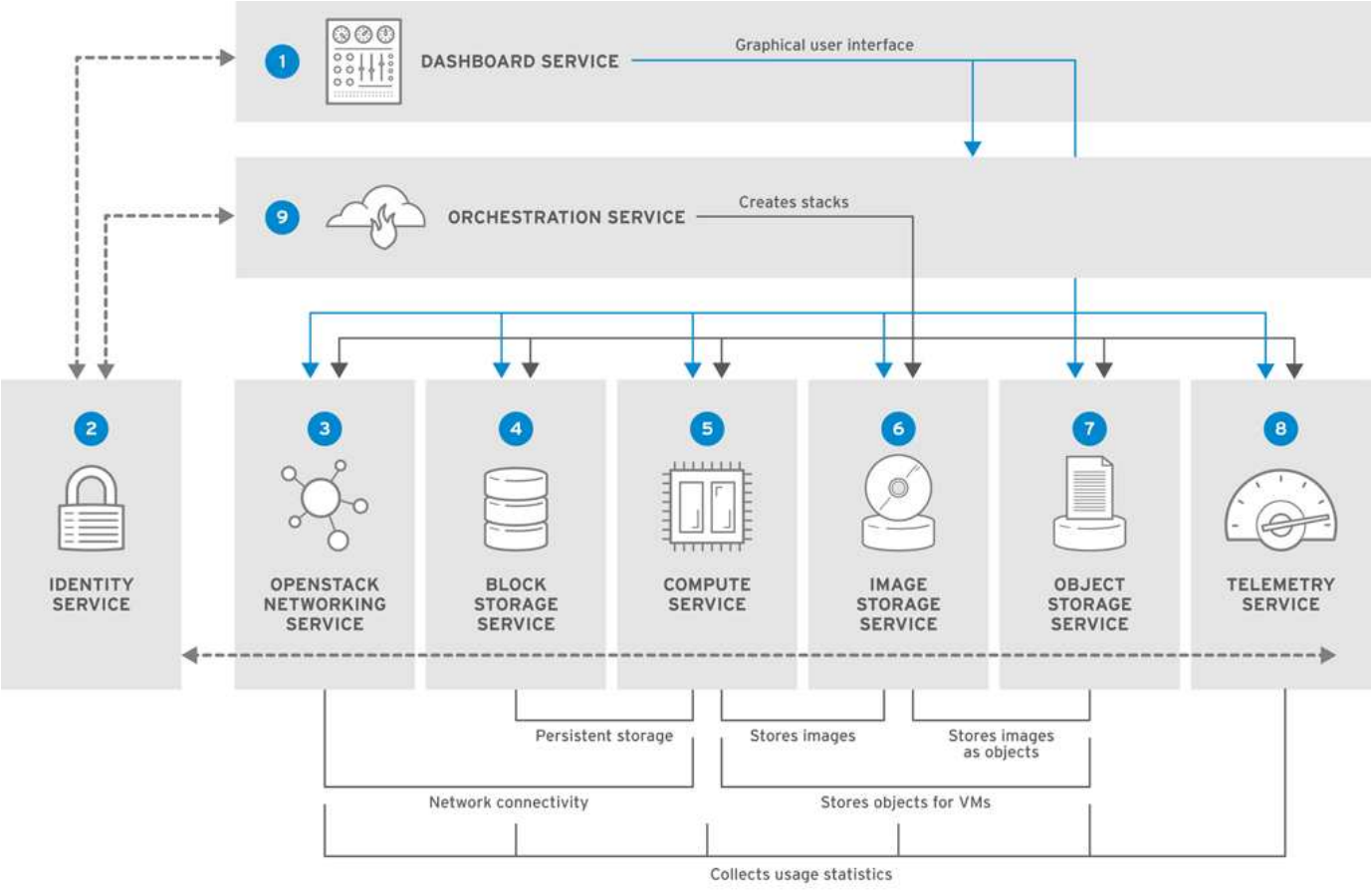
Das OpenStack Projekt ist ein schnell entwickeltes Community-Projekt, das alle sechs Monate aktualisierte Versionen bereitstellt. Zunächst hat Red hat OpenStack Platform mit diesem Release-Zyklus Schritt gehalten, indem es eine neue Version zusammen mit jeder Upstream-Version veröffentlichte und für jede dritte Version langfristige Unterstützung bietet. In jüngster Zeit hat Red hat mit der OSP 16.0-Version (auf OpenStack Train) entschieden, nicht mit den Versionsnummern Schritt zu halten, sondern neue Funktionen in Unterversionen zu portieren. Die neueste Version ist Red hat OpenStack Platform 16.1, die erweiterte Funktionalitäten der Upstream-Versionen Ussuri und Victoria unterstützt.

Weitere Informationen zu OSP finden Sie im "Red hat OpenStack Platform Website".

OpenStack Services

OpenStack Platform Services werden als Container implementiert. Dadurch werden Services voneinander isoliert, einfache Upgrades ermöglicht. Die OpenStack Plattform nutzt eine Reihe von Containern, die mit einer

Kolla erstellt und gemanagt werden. Die Bereitstellung von Services erfolgt durch Ziehen von Container-Images aus dem Red hat Custom Portal. Diese Service-Container werden über den Podman-Befehl gemanagt und mit Red hat OpenStack Director implementiert, konfiguriert und gewartet.



Service	Projektname	Beschreibung
Dashboard	Horizont	Webbrowser-basiertes Dashboard für das Management von OpenStack Services.
Identität	Keystone	Zentraler Service zur Authentifizierung und Autorisierung von OpenStack Services sowie zur Verwaltung von Benutzern, Projekten und Rollen.
OpenStack Networking	Neutron	Bietet Konnektivität zwischen den Schnittstellen von OpenStack Services.
Block-Storage	Cinder	Managt persistente Block-Storage-Volumes für Virtual Machines (VMs)
Computing	Nova	Management und Bereitstellung von VMs, die auf Computing-Nodes ausgeführt werden
Bild	Überblick	Registry-Service zur Speicherung von Ressourcen wie VM Images und Volume Snapshots
Objekt-Storage	Swift	Benutzer können Storage-Ressourcen speichern und Dateien sowie beliebige Daten abrufen.
Telemetrie	Decken	Erlaubt Messungen der Nutzung von Cloud-Ressourcen

Service	Projektname	Beschreibung
Orchestrierung	Wärme	Vorlagenbasierte Orchestrierungs-Engine zur automatischen Erstellung von Ressourcen-Stacks.

Netzwerkdesign

Die Red hat OpenShift mit NetApp Lösung verwendet zwei Daten-Switches für die primäre Datenkonnektivität mit 25 Gbit/s. Zudem werden zwei zusätzliche Management-Switches verwendet, die mit 1 Gbit/s Konnektivität für in-Band-Management der Storage-Nodes und Out-of-Band-Management-Funktionen für IPMI-Funktionalität bieten.

Die IPMI-Funktionalität ist von Red hat OpenStack Director für die Implementierung der Red hat OpenStack Plattform unter Verwendung des ironischen Bare-Metal-Bereitstellungsservice erforderlich.

VLAN-Anforderungen

Red hat OpenShift mit NetApp wurde entwickelt, um den Netzwerk-Traffic für verschiedene Zwecke durch die Verwendung von Virtual Local Area Networks (VLANs) logisch voneinander zu trennen. Diese Konfiguration kann entsprechend den Kundenanforderungen skaliert werden oder um eine weitere Isolierung für spezifische Netzwerkservices zu bieten. In der folgenden Tabelle werden die für die Implementierung der Lösung erforderlichen VLANs bei der Validierung der Lösung bei NetApp aufgeführt.

VLANs	Zweck	VLAN-ID
Out-of-Band-Managementnetzwerk	Das Netzwerk, das für das Management physischer Nodes und den IPMI-Service verwendet wird, dient zur ironischen Ironie.	16
Storage-Infrastrukturbereit	Netzwerk, das für Controller Nodes verwendet wird, um Volumes direkt zuzuweisen, um Infrastrukturservices wie Swift zu unterstützen.	201
Storage Cinder	Netzwerk, das verwendet wird, um Block-Volumes direkt an virtuelle Instanzen in der Umgebung zuzuordnen und anzubinden.	202
Interne API	Ein Netzwerk, das für die Kommunikation zwischen den OpenStack-Diensten unter Verwendung von API-Kommunikation, RPC-Meldungen und Datenbankkommunikation verwendet wird.	301
Mandant	Neutron stellt jedem Mieter über VXLAN sein eigenes Netzwerk zur Verfügung. Der Netzwerkverkehr wird innerhalb jedes Mandantennetzwerks isoliert. Jedem Mandantennetzwerk ist ein IP-Subnetz zugewiesen. Netzwerknamenpaces bedeuten, dass mehrere Mandantennetzwerke denselben Adressbereich verwenden können, ohne dass Konflikte verursacht werden.	302
Storage-Management	OpenStack Object Storage (Swift) verwendet dieses Netzwerk zur Synchronisierung von Datenobjekten zwischen den teilnehmenden Replikationsknoten. Der Proxy-Dienst fungiert als Schnittstelle zwischen Benutzeranfragen und der zugrunde liegenden Speicherebene. Der Proxy empfängt eingehende Anforderungen und lokalisiert das erforderliche Replikat, um die angeforderten Daten abzurufen.	303
PXE	Der OpenStack Director bietet PXE-Boot als Bestandteil des ironischen Bare Metal-Bereitstellungsservice und ermöglicht so die Orchestrierung der Installation von OSP OverCloud.	3484

VLANs	Zweck	VLAN-ID
Extern	Ein öffentlich verfügbares Netzwerk, das das OpenStack Dashboard (Horizon) für das grafische Management hostet und öffentliche API-Aufrufe zur Verwaltung von OpenStack Services ermöglicht.	3485
In-Band-Managementnetzwerk	Bietet Zugriff auf Systemverwaltungsfunktionen wie SSH-Zugriff, DNS-Traffic und NTP-Datenverkehr (Network Time Protocol). Dieses Netzwerk fungiert auch als Gateway für Nodes ohne Controller.	3486

Support-Ressourcen für die Netzwerkinfrastruktur

Die folgende Infrastruktur sollte vor der Bereitstellung der OpenShift Container Platform vorhanden sein:

- Mindestens ein DNS-Server, der eine vollständige Namensauflösung bietet.
- Mindestens drei NTP-Server, die die Zeit für die Server in der Lösung synchronisiert halten können.
- (Optional) ausgehende Internetverbindung für die OpenShift-Umgebung.

Best Practices für Produktionsimplementierungen

In diesem Abschnitt werden verschiedene Best Practices aufgeführt, die ein Unternehmen vor der Implementierung dieser Lösung in der Produktion berücksichtigen sollte.

OpenShift in eine Private Cloud mit mindestens drei Computing-Nodes auf einem OSP-System implementieren

Die in diesem Dokument beschriebene Architektur enthält die minimale Hardwareimplementierung, die durch Implementierung von drei OSP-Controller-Nodes und zwei OSP-Computing-Nodes für HA-Vorgänge geeignet ist. Diese Architektur sorgt für eine fehlertolerante Konfiguration, bei der beide Computing-Nodes virtuelle Instanzen starten und implementierte VMs zwischen den beiden Hypervisoren migrieren können.

Da Red hat OpenShift zunächst mit drei Master-Nodes implementiert wird, kann es vorkommen, dass mindestens zwei Master-Konfigurationen denselben Node belegen, was zu einem möglichen Ausfall für OpenShift führen kann, wenn dieser bestimmte Node nicht mehr verfügbar ist. Daher ist es eine Best Practice von Red hat, mindestens drei OSP-Computing-Nodes bereitzustellen, damit die OpenShift-Master gleichmäßig verteilt werden können und die Lösung eine zusätzliche Fehlertoleranz erhält.

Konfiguration der virtuellen Maschine/Host-Affinität

OpenShift-Master kann durch Unterstützung der VM-/Host-Affinität auf mehrere Hypervisor-Nodes verteilt werden.

Affinity ermöglicht die Definition von Regeln für eine Gruppe von VMs und/oder Hosts, anhand derer bestimmt wird, ob die VMs auf demselben Host oder denselben Hosts in der Gruppe oder auf verschiedenen Hosts ausgeführt werden. Wird auf die VMs angewendet, indem Gruppen von Affinitätsgruppen erstellt werden, die aus VMs und/oder Hosts mit einer Reihe identischer Parameter und Bedingungen bestehen. Je nachdem, ob die VMs einer Affinitätsgruppe auf demselben Host oder Hosts der Gruppe oder separat auf verschiedenen Hosts ausgeführt werden, können die Parameter der Affinitätsgruppe entweder eine positive oder eine negative Affinität definieren. In der Red hat OpenStack Platform können Host-Affinität und Anti-Affinität-Regeln erstellt und durchgesetzt werden, indem Servergruppen erstellt und Filter konfiguriert werden, damit Instanzen von Nova in einer Servergruppe auf unterschiedlichen Computing-Nodes bereitgestellt werden.

Eine Servergruppe verfügt standardmäßig über maximal 10 virtuelle Instanzen, für die sie die Platzierung managen kann. Dies kann durch Aktualisierung der Standardkontingente für Nova geändert werden.

> Es gibt ein bestimmtes Limit für die Hardinität/Antiaffinität für OSP-Servergruppen. Wenn nicht genügend Ressourcen für die Bereitstellung auf separaten Nodes vorhanden sind oder nicht genügend Ressourcen zur gemeinsamen Nutzung von Nodes vorhanden sind, wird die VM nicht gestartet.

Informationen zum Konfigurieren von Affinitätsgruppen finden Sie unter "Wie konfiguriere ich Affinität und Antiaffinität für OpenStack Instanzen?".

Verwenden Sie eine benutzerdefinierte Installationsdatei für die OpenShift-Bereitstellung

IPI vereinfacht die Bereitstellung von OpenShift-Clustern durch den interaktiven Assistenten, den bereits in diesem Dokument erläutert wurde. Es ist jedoch möglich, dass Sie einige Standardwerte im Rahmen einer Cluster-Bereitstellung ändern müssen.

In diesen Fällen können Sie die Anwendung erst ausführen und ausführen, ohne gleich einen Cluster implementieren zu müssen. Stattdessen erstellt es eine Konfigurationsdatei, aus der das Cluster später implementiert werden kann. Dies ist sehr nützlich, wenn Sie IPI-Standards ändern müssen oder mehrere identische Cluster in Ihrer Umgebung für andere Zwecke wie Mandantenfähigkeit implementieren möchten. Weitere Informationen zum Erstellen einer benutzerdefinierten Installationskonfiguration für OpenShift finden Sie unter "Red hat OpenShift – Installation eines Clusters auf OpenStack mit Anpassungen".

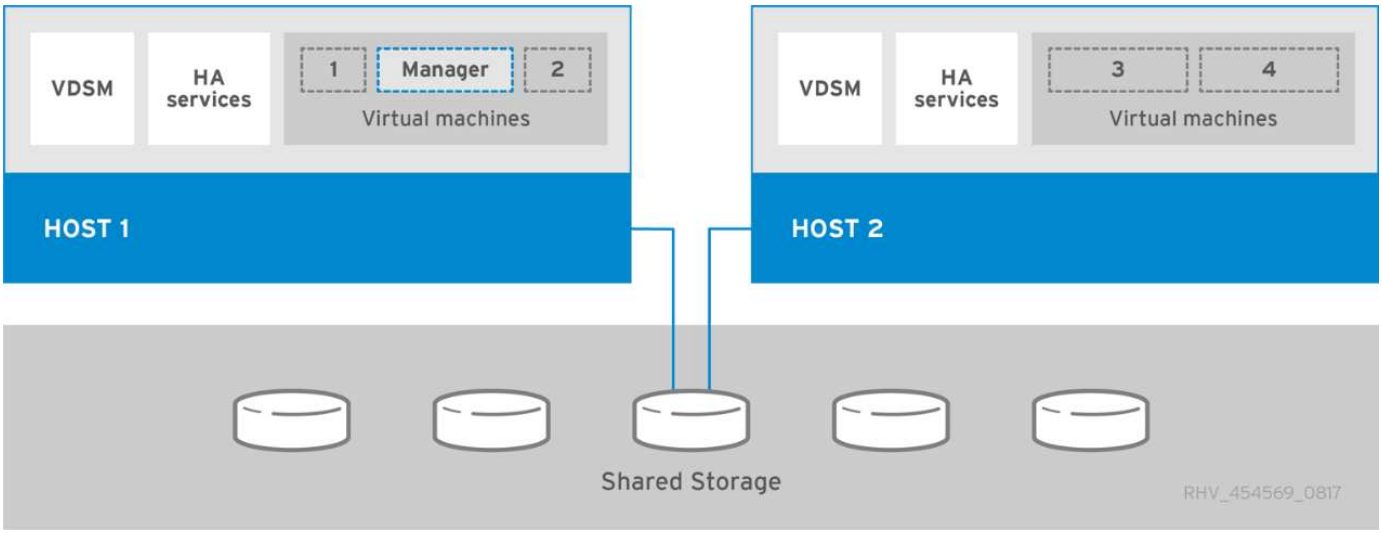
OpenShift auf Red hat Virtualization

Red hat Virtualization (RHV) ist eine virtuelle Rechenzentrumsplattform für Unternehmen, die auf Red hat Enterprise Linux (RHEL) ausgeführt wird und den KVM-Hypervisor verwendet.

Weitere Informationen zu RHV finden Sie im "Red hat Virtualization Website".

RHV bietet die folgenden Funktionen:

- **Zentrales Management von VMs und Hosts** der RHV-Manager wird als physische oder virtuelle Maschine (VM) in der Bereitstellung ausgeführt und stellt eine webbasierte GUI für die Verwaltung der Lösung von einer zentralen Schnittstelle aus zur Verfügung.
- **Self-Hosted Engine** um die Hardwareanforderungen zu minimieren, ermöglicht RHV es RHV Manager (RHV-M) als VM auf denselben Hosts bereitzustellen, auf denen Gast-VMs ausgeführt werden.
- **Hohe Verfügbarkeit** um Störungen im Falle eines Host-Ausfalls zu vermeiden, erlaubt RHV die Konfiguration von VMs für hohe Verfügbarkeit. Die hochverfügbaren VMs werden auf Cluster-Ebene mithilfe von Resiliency-Richtlinien gesteuert.
- * Hohe Skalierbarkeit* Ein einzelner RHV-Cluster kann bis zu 200 Hypervisor-Hosts haben, wodurch er die Anforderungen massiver VMs unterstützt, um ressourcenhungrige Workloads der Enterprise-Klasse zu hosten.
- **Verbesserte Sicherheit**, die von den Technologien RHV, Secure Virtualization (sVirt) und Security Enhanced Linux (SELinux) übernommen wurde, wird von RHV für erhöhte Sicherheit und Hardening für Hosts und VMs eingesetzt. Der wichtigste Vorteil dieser Funktionen ist die logische Isolierung einer VM und der damit verbundenen Ressourcen.



Netzwerkdesign

Die Red hat OpenShift on NetApp Lösung verwendet zwei Daten-Switches für die primäre Datenkonnektivität mit 25 Gbit/s. Zudem werden zwei zusätzliche Management-Switches eingesetzt, die mit 1 Gbit/s Konnektivität für das in-Band-Management der Storage-Nodes und das Out-of-Band-Management für IPMI-Funktionen bereitstellen. OCP verwendet das logische Netzwerk der virtuellen Maschine auf RHV für die Clusterverwaltung. Dieser Abschnitt beschreibt die Anordnung und der Zweck jedes in der Lösung verwendeten virtuellen Netzwerksegments und beschreibt die Voraussetzungen für die Implementierung der Lösung.

VLAN-Anforderungen

Red hat OpenShift auf RHV wurde entwickelt, um den Netzwerkverkehr für verschiedene Zwecke durch die Verwendung von Virtual Local Area Networks (VLANs) logisch zu trennen. Diese Konfiguration kann entsprechend den Kundenanforderungen skaliert werden oder um eine weitere Isolierung für spezifische Netzwerkservices zu bieten. In der folgenden Tabelle werden die für die Implementierung der Lösung erforderlichen VLANs bei der Validierung der Lösung bei NetApp aufgeführt.

VLANs	Zweck	VLAN-ID
Out-of-Band-Managementnetzwerk	Management für physische Knoten und IPMI	16
VM Network	Zugriff auf das virtuelle Gastnetzwerk	1172
In-Band-Managementnetzwerk	Management für RHV-H-Knoten, RHV-Manager und ovirtmgmt-Netzwerk	3343
Datennetzwerk Storage-Netzwerk	Storage-Netzwerk für NetApp Element iSCSI	3344
Migrationsnetzwerk	Netzwerk für die Migration von virtuellen Gastnetzvorgängen	3345

Support-Ressourcen für die Netzwerkinfrastruktur

Die folgende Infrastruktur sollte vor der Bereitstellung der OpenShift Container Platform vorhanden sein:

- Mindestens ein DNS-Server bietet vollständige Host-Name-Auflösung, auf die über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.

- Mindestens ein NTP-Server, auf den über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.
- (Optional) ausgehende Internetverbindung sowohl für das bandinterne Managementnetzwerk als auch für das VM-Netzwerk.

Best Practices für Produktionsimplementierungen

In diesem Abschnitt werden verschiedene Best Practices aufgeführt, die ein Unternehmen vor der Implementierung dieser Lösung in der Produktion berücksichtigen sollte.

OpenShift wird in einem RHV-Cluster mit mindestens drei Nodes bereitgestellt

Die in diesem Dokument beschriebene verifizierte Architektur stellt die minimale Hardwareimplementierung dar, die für HA-Vorgänge geeignet ist. Sie stellt zwei RHV-H-Hypervisor-Knoten bereit und sorgt für eine fehlertolerante Konfiguration, bei der beide Hosts die gehostete Engine und implementierte VMs zwischen den beiden Hypervisoren migrieren können.

Da Red hat OpenShift zunächst mit drei Master-Nodes implementiert wird, wird in einer Konfiguration mit zwei Nodes sichergestellt, dass mindestens zwei Master denselben Node belegen. Dies kann zu einem möglichen Ausfall von OpenShift führen, wenn dieser bestimmte Node nicht mehr verfügbar ist. Daher ist es eine Best Practice von Red hat, dass mindestens drei RHV-H-Hypervisor-Nodes als Teil der Lösung eingesetzt werden, damit die OpenShift-Master gleichmäßig verteilt werden können und die Lösung eine zusätzliche Fehlertoleranz erhält.

Konfiguration der virtuellen Maschine/Host-Affinität

Sie können die OpenShift-Master durch Unterstützung der VM-/Host-Affinität auf mehrere Hypervisor-Nodes verteilen.

Affinity ermöglicht die Definition von Regeln für eine Gruppe von VMs und/oder Hosts, anhand derer bestimmt wird, ob die VMs auf demselben Host oder denselben Hosts in der Gruppe oder auf verschiedenen Hosts ausgeführt werden. Wird auf die VMs angewendet, indem Gruppen von Affinitätsgruppen erstellt werden, die aus VMs und/oder Hosts mit einer Reihe identischer Parameter und Bedingungen bestehen. Je nachdem, ob die VMs einer Affinitätsgruppe auf demselben Host oder Hosts der Gruppe oder separat auf verschiedenen Hosts ausgeführt werden, können die Parameter der Affinitätsgruppe entweder eine positive oder eine negative Affinität definieren.

Die für die Parameter definierten Bedingungen können eine harte Durchsetzung oder eine weiche Durchsetzung sein. Harte Durchsetzung stellt sicher, dass die VMs in einer Affinitätsgruppe immer die positive oder negative Affinität streng ohne Berücksichtigung von externen Bedingungen folgen. Die weiche Durchsetzung sorgt dafür, dass die VMs in einer Affinitätsgruppe, sofern dies möglich ist, eine höhere Vorliebe für die VMs festgelegt werden, um nach Möglichkeit eine positive oder negative Affinität zu verfolgen. In der in diesem Dokument beschriebenen zwei- oder drei-Hypervisor-Konfiguration ist die weiche Affinität die empfohlene Einstellung. In größeren Clustern kann die Verteilung von OpenShift-Nodes durch Hard-Affinität korrekt erfolgen.

Informationen zum Konfigurieren von Affinitätsgruppen finden Sie im "Red Hat 6.11 Dokumentation von Affinitätsgruppen".

Verwenden Sie eine benutzerdefinierte Installationsdatei für die OpenShift-Bereitstellung

IPI vereinfacht die Bereitstellung von OpenShift-Clustern durch den interaktiven Assistenten, den bereits in diesem Dokument erläutert wurde. Es ist jedoch möglich, dass es einige Standardwerte gibt, die im Rahmen der Cluster-Implementierung geändert werden müssen.

In diesen Fällen können Sie den Assistenten ausführen und ausführen, ohne sofort ein Cluster bereitzustellen. Stattdessen wird eine Konfigurationsdatei erstellt, aus der der Cluster später bereitgestellt werden kann. Dies ist sehr nützlich, wenn Sie IPI-Standards ändern möchten oder mehrere identische Cluster in Ihrer Umgebung für andere Zwecke wie Mandantenfähigkeit implementieren möchten. Weitere Informationen zum Erstellen einer benutzerdefinierten Installationskonfiguration für OpenShift finden Sie unter "Red hat OpenShift Installieren eines Clusters auf RHV mit Anpassungen".

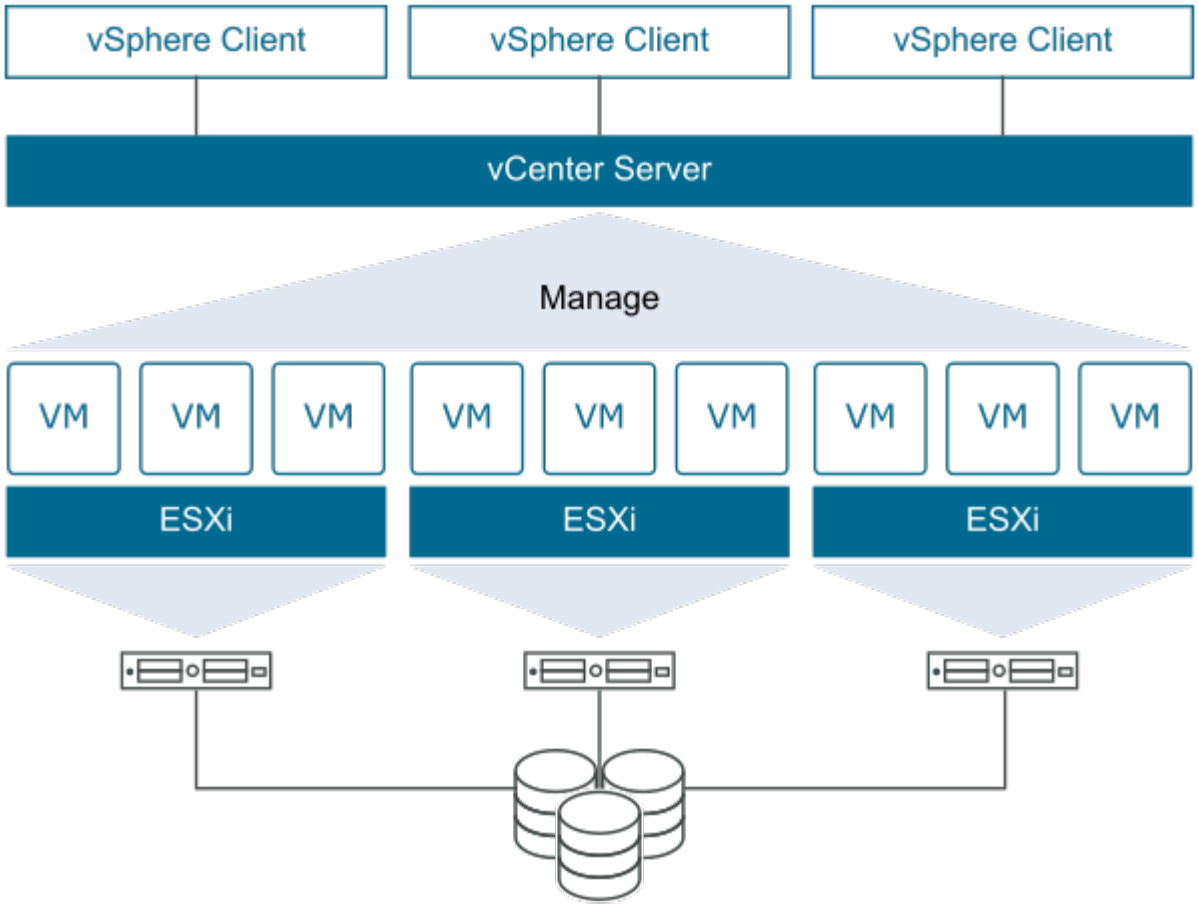
OpenShift auf VMware vSphere

VMware vSphere ist eine Virtualisierungsplattform zur zentralen Verwaltung einer großen Anzahl virtualisierter Server und Netzwerke, die auf dem ESXi Hypervisor ausgeführt werden.

Weitere Informationen zu VMware vSphere finden Sie im "VMware vSphere Website".

VMware vSphere bietet folgende Funktionen:

- **VMware vCenter Server** VMware vCenter Server bietet einheitliches Management aller Hosts und VMs von einer einzigen Konsole aus und aggregiert die Performance-Überwachung von Clustern, Hosts und VMs.
- **VMware vSphere vMotion** VMware vCenter ermöglicht die unterbrechungsfreie Migration von VMs zwischen Knoten im Cluster auf Anfrage.
- **VSphere High Availability** um Unterbrechungen im Falle eines Host-Ausfalls zu vermeiden, erlaubt VMware vSphere die Cluster-Konfiguration von Hosts für High Availability. VMs, die durch einen Host-Ausfall unterbrochen werden, werden in Kürze auf anderen Hosts im Cluster neu gestartet, wodurch die Services wiederhergestellt werden.
- **Distributed Resource Scheduler (DRS)** Ein VMware vSphere Cluster kann so konfiguriert werden, dass die Ressourcenanforderungen der VMs, die es hostet, ausgeglichen werden. VMs mit Ressourceninhaltungen können Hot-to-andere Nodes im Cluster migriert werden, um sicherzustellen, dass genügend Ressourcen verfügbar sind.



Netzwerkdesign

Die Red hat OpenShift on NetApp Lösung verwendet zwei Daten-Switches für die primäre Datenkonnektivität mit 25 Gbit/s. Zudem werden zwei zusätzliche Management-Switches verwendet, die mit 1 Gbit/s Konnektivität für in-Band-Management der Storage-Nodes und Out-of-Band-Management-Funktionen für IPMI-Funktionalität bieten. OCP verwendet für das Cluster-Management das logische VM-Netzwerk auf VMware vSphere. Dieser Abschnitt beschreibt die Anordnung und der Zweck jedes in der Lösung verwendeten virtuellen Netzwerksegments und beschreibt die Voraussetzungen für die Implementierung der Lösung.

VLAN-Anforderungen

Red hat OpenShift auf VMware vSphere wurde entwickelt, um den Netzwerkverkehr für verschiedene Zwecke durch die Verwendung von Virtual Local Area Networks (VLANs) logisch zu trennen. Diese Konfiguration kann entsprechend den Kundenanforderungen skaliert werden oder um eine weitere Isolierung für spezifische Netzwerkservices zu bieten. In der folgenden Tabelle werden die für die Implementierung der Lösung erforderlichen VLANs bei der Validierung der Lösung bei NetApp aufgeführt.

VLANs	Zweck	VLAN-ID
Out-of-Band-Managementnetzwerk	Management für physische Knoten und IPMI	16
VM Network	Zugriff auf das virtuelle Gastnetzwerk	181
Datennetzwerk Storage-Netzwerk	Storage-Netzwerk für ONTAP NFS	184
Datennetzwerk Storage-Netzwerk	Storage-Netzwerk für ONTAP iSCSI	185

VLANs	Zweck	VLAN-ID
In-Band-Managementnetzwerk	Management für ESXi Knoten, vCenter Server, ONTAP Select	3480
Datennetzwerk Storage-Netzwerk	Storage-Netzwerk für NetApp Element iSCSI	3481
Migrationsnetzwerk	Netzwerk für die Migration von virtuellen Gastnetzvorgängen	3482

Support-Ressourcen für die Netzwerkinfrastruktur

Die folgende Infrastruktur sollte vor der Bereitstellung der OpenShift Container Platform vorhanden sein:

- Mindestens ein DNS-Server bietet vollständige Host-Name-Auflösung, auf die über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.
- Mindestens ein NTP-Server, auf den über das bandinterne Managementnetzwerk und das VM-Netzwerk zugegriffen werden kann.
- (Optional) ausgehende Internetverbindung sowohl für das bandinterne Managementnetzwerk als auch für das VM-Netzwerk.

Best Practices für Produktionsimplementierungen

In diesem Abschnitt werden verschiedene Best Practices aufgeführt, die ein Unternehmen vor der Implementierung dieser Lösung in der Produktion berücksichtigen sollte.

OpenShift in ein ESXi-Cluster mit mindestens drei Nodes implementieren

Die in diesem Dokument beschriebene Architektur behandelt die minimale Hardwarebereitstellung für HA-Vorgänge durch Implementierung von zwei ESXi Hypervisor-Nodes und die Gewährleistung einer fehlertoleranten Konfiguration durch die Unterstützung von VMware vSphere HA und VMware vMotion. Mit dieser Konfiguration können implementierte VMs zwischen den beiden Hypervisoren migriert und neu gestartet werden, sollte ein Host nicht mehr verfügbar sein.

Da Red hat OpenShift zunächst mit drei Master-Nodes implementiert wird, können unter bestimmten Umständen mindestens zwei Master-Master-Konfigurationen mit zwei Nodes denselben Node belegen. Dies kann zu einem möglichen Ausfall von OpenShift führen, wenn dieser bestimmte Node nicht mehr verfügbar ist. Daher ist es eine Best Practice von Red hat, dass mindestens drei ESXi-Hypervisor-Nodes bereitgestellt werden müssen, damit die OpenShift-Master gleichmäßig verteilt werden können, was eine zusätzliche Fehlertoleranz bietet.

Konfiguration der virtuellen Maschine und der Host-Affinität

Durch die Unterstützung der VM- und Host-Affinität kann sichergestellt werden, dass die OpenShift-Master-Verteilung über mehrere Hypervisor-Nodes hinweg erreicht werden kann.

Affinität oder Antiaffinität ist eine Möglichkeit, Regeln für eine Gruppe von VMs und/oder Hosts zu definieren, die festlegen, ob die VMs auf demselben Host oder denselben Hosts in der Gruppe oder auf verschiedenen Hosts ausgeführt werden. Wird auf die VMs angewendet, indem Gruppen von Affinitätsgruppen erstellt werden, die aus VMs und/oder Hosts mit einer Reihe identischer Parameter und Bedingungen bestehen. Je nachdem, ob die VMs einer Affinitätsgruppe auf demselben Host oder Hosts der Gruppe oder separat auf verschiedenen Hosts ausgeführt werden, können die Parameter der Affinitätsgruppe entweder eine positive oder eine negative Affinität definieren.

Informationen zum Konfigurieren von Affinitätsgruppen finden Sie im "VSphere 6.7 Dokumentation: Nutzung von DRS Affinity Rules".

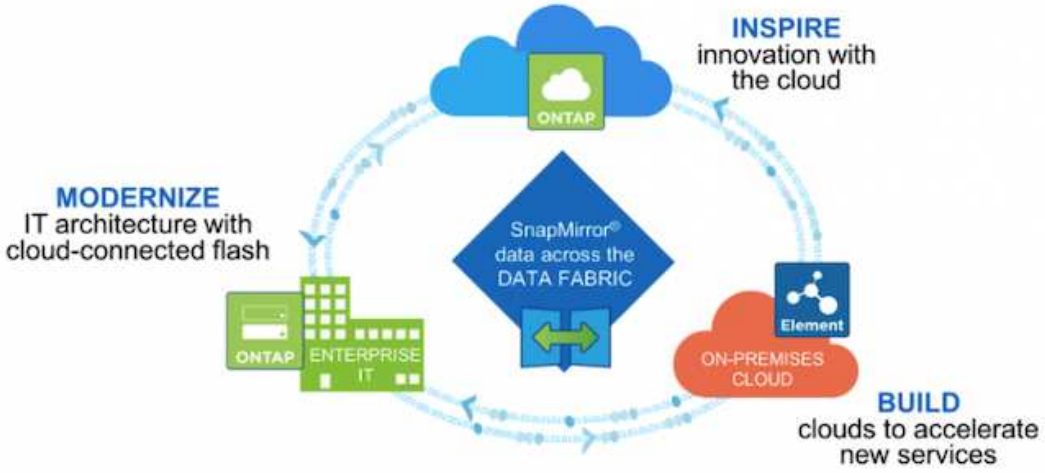
Verwenden Sie eine benutzerdefinierte Installationsdatei für die OpenShift-Bereitstellung

IPI vereinfacht die Bereitstellung von OpenShift-Clustern durch den interaktiven Assistenten, den bereits in diesem Dokument erläutert wurde. Es ist jedoch möglich, dass Sie einige Standardwerte im Rahmen einer Cluster-Bereitstellung ändern müssen.

In diesen Fällen können Sie den Assistenten ausführen und ausführen, ohne sofort einen Cluster bereitzustellen. Stattdessen erstellt der Assistent eine Konfigurationsdatei, aus der das Cluster später bereitgestellt werden kann. Dies ist sehr nützlich, wenn Sie IPI-Standards ändern müssen oder wenn Sie mehrere identische Cluster in Ihrer Umgebung für andere Zwecke wie Mandantenfähigkeit implementieren möchten. Weitere Informationen zum Erstellen einer benutzerdefinierten Installationskonfiguration für OpenShift finden Sie unter "Red hat OpenShift Installieren eines Clusters auf vSphere mit Anpassungen".

NetApp Storage-Überblick

NetApp verfügt über verschiedene Storage-Plattformen, die sich für unseren Astra Trident Storage Orchestrator für die Bereitstellung von Storage für Applikationen eignen, die auf Red hat OpenShift implementiert sind.



- 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.
- NetApp Cloud Volumes Service (AWS/GCP) und Azure NetApp Files 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"

NetApp ONTAP

NetApp ONTAP ist ein leistungsstarkes Storage-Software-Tool mit Funktionen wie einer intuitiven GUI, REST-APIs mit Automatisierungsintegration, KI-informierte prädiktive Analysen und Korrekturmaßnahmen, unterbrechungsfreien Hardware-Upgrades und Storage-übergreifenden Import.

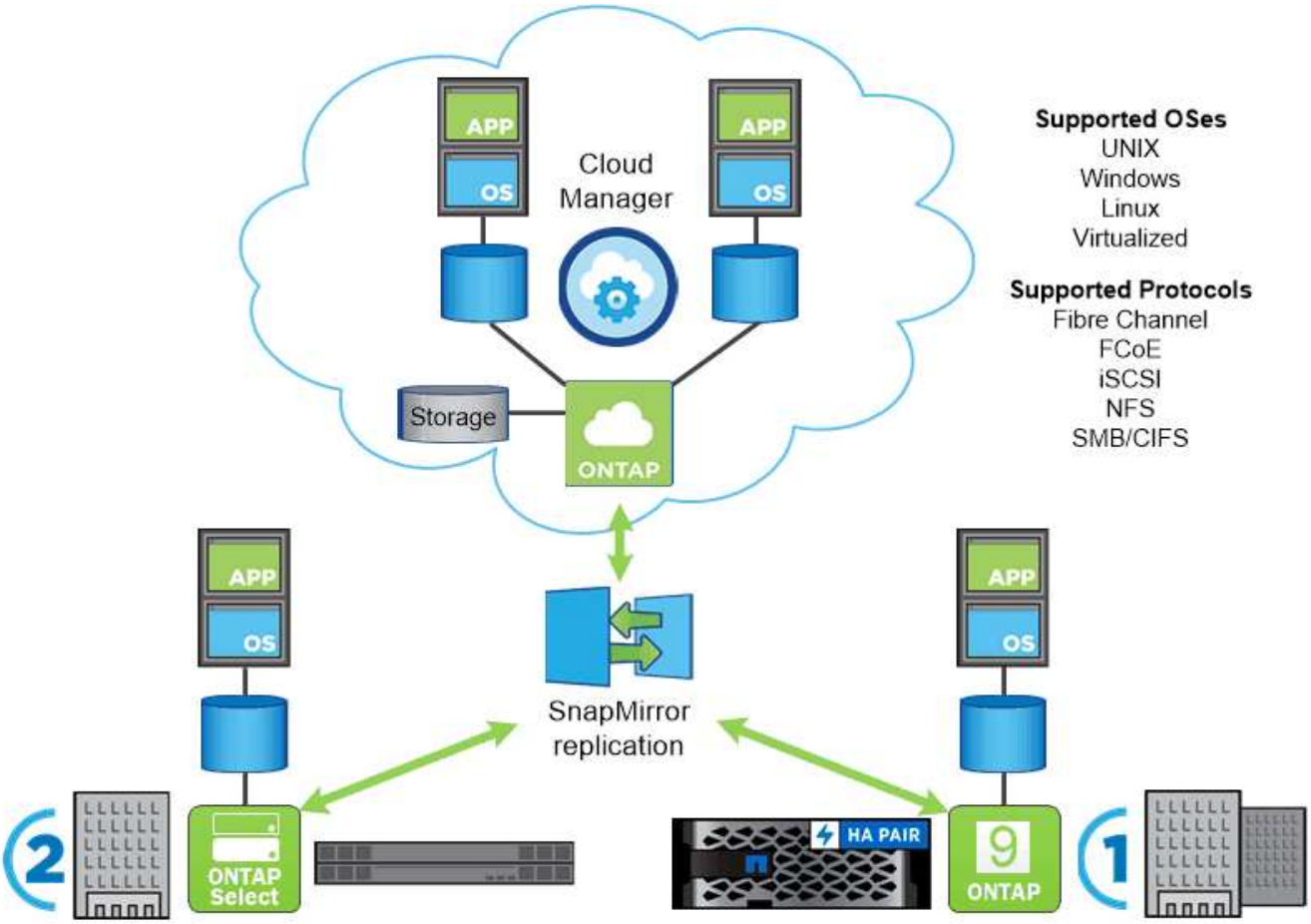
Weitere Informationen zum NetApp ONTAP Storage-System finden Sie unter "NetApp ONTAP Website".

ONTAP bietet folgende Funktionen:

- Ein Unified Storage-System mit gleichzeitigem Datenzugriff und Management von NFS, CIFS, iSCSI, FC, FCoE Und FC-NVMe-Protokolle unterstützt.
- Verschiedene Implementierungsmodelle umfassen lokale Konfigurationen auf All-Flash-, Hybrid- und rein HDD-basierten Hardware, VM-basierte Storage-Plattformen auf einem unterstützten Hypervisor wie ONTAP Select und in der Cloud als Cloud Volumes ONTAP.
- Erhöhte Storage-Effizienz auf ONTAP Systemen mit Unterstützung für automatisches Daten-Tiering, Inline-Datenkomprimierung, Deduplizierung und Data-Compaction
- Workload-basierter QoS-gesteuerter Storage
- Nahtlose Integration in eine Public Cloud für Tiering und Datensicherung ONTAP bietet zudem robuste Datensicherungsfunktionen, die die Technologie in jeder Umgebung auszeichnet:
    - **NetApp Snapshot Kopien.** Ein schnelles, zeitpunktgenaues Backup von Daten mit minimalem Festplattenspeicher ohne zusätzlichen Performance Overhead.
    - **NetApp SnapMirror.** spiegelt die Snapshot Kopien von Daten von einem Storage-System auf ein anderes. ONTAP unterstützt die Spiegelung von Daten auch auf andere physische Plattformen und Cloud-native Services.
    - **NetApp SnapLock.** effiziente Verwaltung nicht wiederbeschreibbarer Daten durch Schreiben auf spezielle Volumes, die für einen vorgegebenen Zeitraum nicht überschrieben oder gelöscht werden können.
    - **NetApp SnapVault.** sichert Daten von mehreren Speichersystemen auf eine zentrale Snapshot Kopie, die als Backup auf allen designierten Systemen dient.
    - **NetApp SyncMirror.** bietet Echtzeit-Spiegelung auf RAID-Ebene von Daten auf zwei verschiedenen Plexen von Festplatten, die physisch mit demselben Controller verbunden sind.
    - **NetApp SnapRestore.** ermöglicht eine schnelle Wiederherstellung von gesicherten Daten bei Bedarf aus Snapshot-Kopien.
    - **NetApp FlexClone.** ermöglicht die sofortige Bereitstellung einer vollständig lesbaren und schreibbaren Kopie eines NetApp Volumes auf Basis einer Snapshot Kopie.

Weitere Informationen zu ONTAP finden Sie im "ONTAP 9 Dokumentationszentrum".

NetApp ONTAP ist vor Ort, virtualisiert oder in der Cloud verfügbar.



Plattformen von NetApp

NetApp All Flash FAS/FAS

NetApp bietet robuste All-Flash (AFF) und horizontal skalierbare Hybrid (FAS) Storage-Plattformen, die auf latenzarme Performance, integrierte Datensicherung und Multiprotokoll-Unterstützung abgestimmt sind.

Beide Systeme werden durch die Datenmanagement-Software NetApp ONTAP unterstützt. Sie ist eine der fortschrittlichsten Datenmanagement-Software der Branche für das hochverfügbare, Cloud-integrierte und vereinfachte Storage-Management. So erhalten Sie die Geschwindigkeit, Effizienz und Sicherheit Ihrer Data-Fabric-Infrastruktur der Enterprise-Klasse.

Weitere Informationen zu NETAPP All Flash FAS/FAS Plattformen finden Sie unter "Hier".

ONTAP Select

ONTAP Select ist eine softwaredefinierte Implementierung von NetApp ONTAP, die in einer Hypervisor-Umgebung implementiert werden kann. Es kann auf VMware vSphere oder KVM installiert werden und bietet den vollen Funktionsumfang und die Erfahrung eines hardwarebasierten ONTAP Systems.

Weitere Informationen zu ONTAP Select finden Sie auf "Hier".

Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP ist eine Cloud-implementierte Version von NetApp ONTAP, die in einer Reihe von Public Clouds implementiert werden kann, darunter Amazon AWS, Microsoft Azure und Google Cloud.

Weitere Informationen zu Cloud Volumes ONTAP finden Sie auf "Hier".

NetApp Element: Red hat OpenShift mit NetApp

Die NetApp Element Software bietet eine modulare, skalierbare Performance, bei der jeder Storage-Node garantierte Kapazität und Durchsatz für die Umgebung bietet. NetApp Element Systeme lassen sich von 4 bis 100 Nodes in einem einzigen Cluster skalieren und bieten zahlreiche erweiterte Storage-Management-Funktionen.

Weitere Informationen über NetApp Element Storage-Systeme finden Sie unter "NetApp SolidFire Website".

ISCSI-Anmeldeumleitung und Funktionen zur Selbstreparatur

Die NetApp Element Software nutzt das iSCSI Storage-Protokoll. Hierbei handelt es sich um eine Standardart zur Einkapselung von SCSI-Befehlen in einem herkömmlichen TCP/IP-Netzwerk. Wenn sich die SCSI-Standards ändern oder die Performance von Ethernet-Netzwerken verbessert wird, profitiert das iSCSI-Storage-Protokoll von Vorteilen, ohne dass Änderungen erforderlich sind.

Obwohl alle Storage-Nodes über eine Management-IP und eine Storage-IP verfügen, stellt die NetApp Element Software eine einzelne Storage-virtuelle IP-Adresse (SVIP-Adresse) für den gesamten Storage-Datenverkehr im Cluster bereit. Im Rahmen des iSCSI-Anmeldeprozesses kann Storage darauf reagieren, dass das Ziel-Volume auf eine andere Adresse verschoben wurde, und kann so den Verhandlungsprozess nicht fortsetzen. Der Host gibt die Anmeldeanforderung dann in einem Prozess, der keine Neukonfiguration auf Host-Seite erfordert, an die neue Adresse erneut aus. Dieser Prozess wird als iSCSI-Anmeldeumleitung bezeichnet.

Die iSCSI-Login-Umleitung ist ein wichtiger Bestandteil des NetApp Element Software-Clusters. Wenn eine Host-Login-Anfrage eingeht, entscheidet der Node, welches Mitglied des Clusters den Datenverkehr auf Basis der IOPS und der Kapazitätsanforderungen für das Volume verarbeitet. Volumes werden über das NetApp Element Software-Cluster verteilt und neu verteilt, wenn ein einzelner Node zu viel Datenverkehr für seine Volumes verarbeitet oder ein neuer Node hinzugefügt wird. Dem gesamten Array werden mehrere Kopien eines bestimmten Volumes zugewiesen.

Auf diese Weise wird beim Ausfall eines Node nach der Umverteilung des Volumes keine Auswirkung auf die Host-Konnektivität über die Abmeldung hinaus und die Anmeldung mit Umleitung zum neuen Speicherort verursacht. Dank iSCSI-Login-Umleitung ist ein NetApp Element Software-Cluster eine selbstheilende und horizontal skalierbare Architektur, die unterbrechungsfreie Upgrades und den Betrieb ermöglicht.

NetApp Element Software Cluster-QoS

Über ein NetApp Element Software-Cluster kann QoS dynamisch für einzelne Volumes konfiguriert werden. Mithilfe der QoS-Einstellungen pro Volume lässt sich die Storage Performance anhand von in Ihnen definierten SLAs steuern. Die QoS wird durch die folgenden drei konfigurierbaren Parameter definiert:

- **Minimum IOPS.** die Mindestanzahl kontinuierlicher IOPS, die der NetApp Element Software Cluster einem Volume zur Verfügung stellt. Das für ein Volume konfigurierte Minimum an IOPS ist das garantierte Performance-Level für ein Volume. Die Performance pro Volume fällt nicht unter diese Ebene.
- **Maximale IOPS.** die maximale Anzahl kontinuierlicher IOPS, die der NetApp Element Software Cluster einem bestimmten Volume zur Verfügung stellt.
- **Burst IOPS.** die maximale Anzahl von IOPS in einem kurzen Burst Szenario erlaubt. Die Einstellung für die Burst-Dauer ist konfigurierbar, standardmäßig 1 Minute. Wenn ein Volume unter dem maximalen IOPS-Wert läuft, werden Burst Credits gesammelt. Wenn die Performance sehr hoch ist und viele gesteigert werden, sind auf dem Volume kurze IOPS-Spitzenlasten über die maximalen IOPS hinaus zulässig.

Mandantenfähigkeit

Die sichere Mandantenfähigkeit wird durch folgende Funktionen erreicht:

- **Sichere Authentifizierung.** das Challenge-Handshake Authentication Protocol (CHAP) wird für den sicheren Volumenzugriff verwendet. Das Lightweight Directory Access Protocol (LDAP) wird für den sicheren Zugriff auf das Cluster für Management und Reporting verwendet.
- **Volume Access Groups (Vags).** optional kann Vags anstelle der Authentifizierung verwendet werden, wobei eine beliebige Anzahl iSCSI Initiator-spezifischer iSCSI-qualifizierter Namen (IQNs) einem oder mehreren Volumes zugeordnet wird. Um auf ein Volume in einem VAG zuzugreifen, muss sich der IQN des Initiators in der Liste erlaubte IQN für die Gruppe von Volumes befinden.
- **Tenant Virtual LANs (VLANs).** auf Netzwerkebene wird die End-to-End-Netzwerksicherheit zwischen iSCSI-Initiatoren und dem NetApp Element-Software-Cluster durch VLANs erleichtert. Für jedes zur Isolierung eines Workloads oder Mandanten erstellte VLAN erstellt die NetApp Element Software eine separate iSCSI-Ziel-SVIP-Adresse, auf die nur über das spezifische VLAN zugegriffen werden kann.
- **VRF-fähige VLANs.** um die Sicherheit und Skalierbarkeit im Rechenzentrum weiter zu unterstützen, ermöglicht Ihnen die NetApp Element-Software, jedes Mandanten-VLAN für VRF-ähnliche Funktionen zu aktivieren. Diese Funktion erweitert die beiden wichtigsten Funktionen:
  - **L3 Routing zu einem Mieter SVIP-Adresse.** mit dieser Funktion können Sie iSCSI-Initiatoren in einem separaten Netzwerk oder VLAN aus dem des NetApp Element Software-Clusters platzieren.
  - **Überlappende oder doppelte IP-Subnetze.** mit dieser Funktion können Sie eine Vorlage zu Mandantenumgebungen hinzufügen, sodass jedem jeweiligen Mandanten-VLAN IP-Adressen aus demselben IP-Subnetz zugewiesen werden können. Dies kann für in-Service-Provider-Umgebungen nützlich sein, in denen Skalierbarkeit und Erhaltung von IPspace wichtig sind.

Enterprise Storage-Effizienzfunktionen

Der NetApp Element Software-Cluster steigert die allgemeine Storage-Effizienz und -Performance. Die folgenden Funktionen werden inline ausgeführt, sind immer aktiviert und erfordern keine manuelle Konfiguration durch den Benutzer:

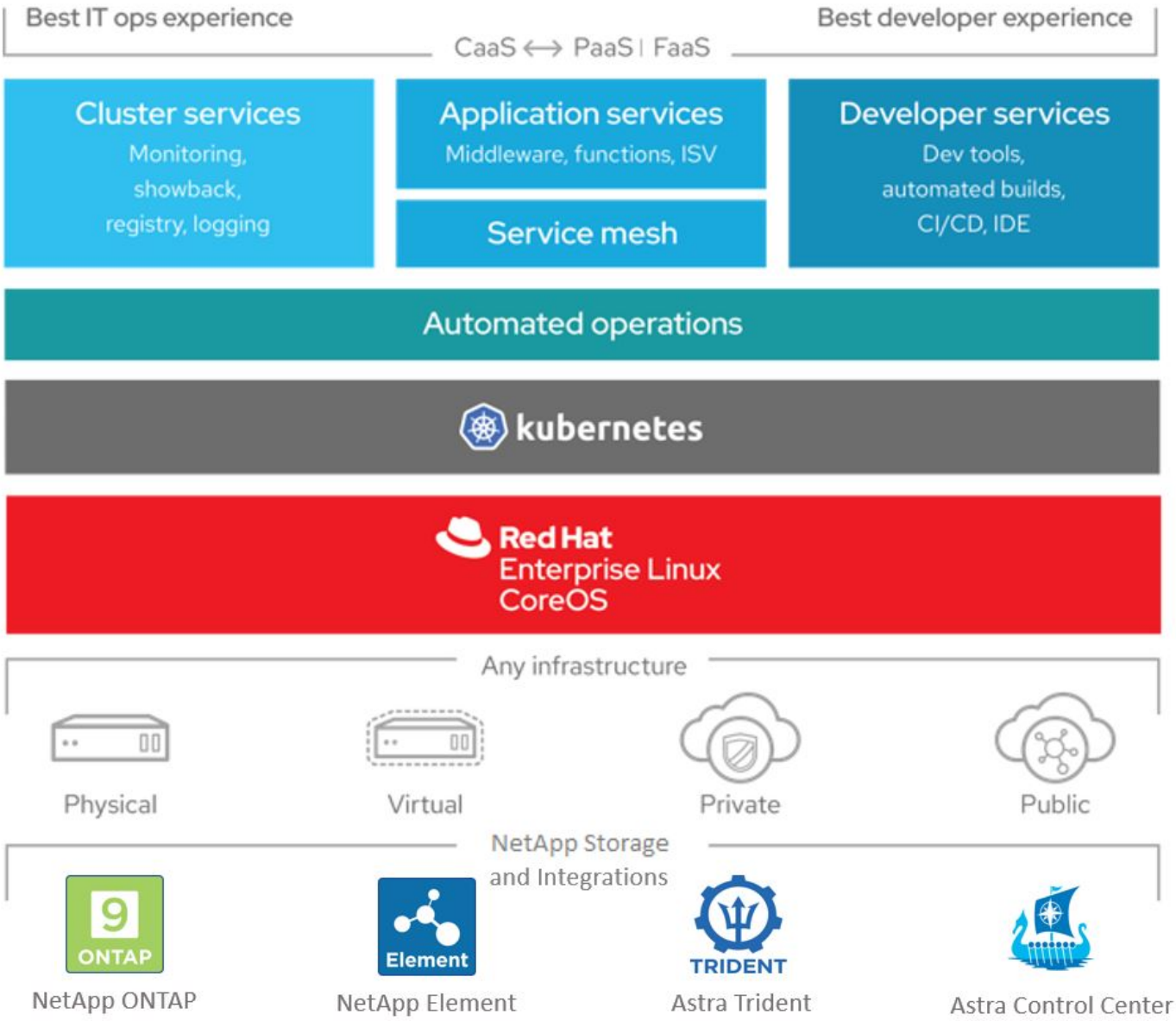
- **Deduplizierung.** das System speichert nur einzigartige 4K Blöcke. Doppelte 4-KB-Blöcke werden automatisch einer bereits gespeicherten Version der Daten zugeordnet. Die Daten befinden sich auf Blockebene und werden mithilfe der NetApp Element Software Helix Datensicherung gespiegelt. Dieses System reduziert den Kapazitätsverbrauch und die Schreibzugriffe innerhalb des Systems deutlich.

- **Komprimierung.** die Komprimierung wird inline ausgeführt, bevor Daten in den NVRAM geschrieben werden. Daten werden komprimiert, in 4-KB-Blöcken gespeichert und im System weiterhin komprimiert. Diese Komprimierung reduziert den Kapazitätsverbrauch, Schreibvorgänge und den Bandbreitenbedarf im gesamten Cluster deutlich.
- **Thin Provisioning.** Diese Funktion bietet zur richtigen Zeit den richtigen Storage und vermeidet den Kapazitätsverbrauch durch überprovisioniertes Volume oder nicht ausgelastete Volumes.
- **Helix.** die Metadaten für ein einzelnes Volume werden auf einem Metadatenlaufwerk gespeichert und aus Redundanzgründen auf ein sekundäres Metadatenlaufwerk repliziert.

> Element wurde für die Automatisierung entwickelt. Alle Storage-Funktionen sind über APIs verfügbar. Diese APIs sind die einzige Methode, die die Benutzeroberfläche zur Steuerung des Systems verwendet.

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".

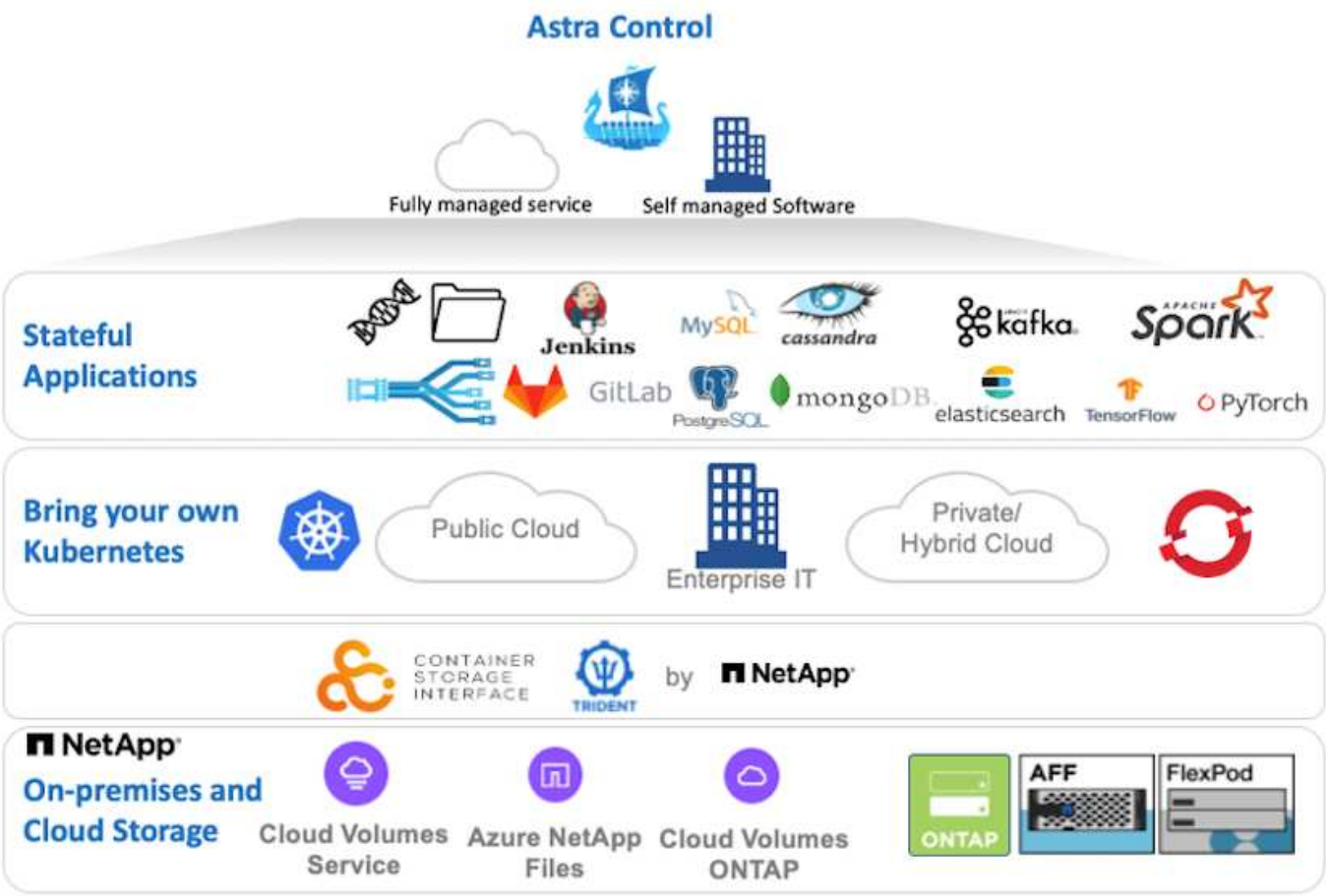
NetApp Astra Trident ist ein Open-Source- und vollständig unterstützter Storage-Orchestrator für Container und Kubernetes-Distributionen, einschließlich Red hat OpenShift. Weitere Informationen finden Sie auf der Astra Trident Website "Hier".

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 Astra Trident"

Übersicht über das NetApp Astra Control Center

Das NetApp Astra Control Center bietet umfassende Storage- und applikationsorientierte Datenmanagement-Services für statusorientierte Kubernetes Workloads in einer On-Premises-Umgebung mit NetApp Datensicherungstechnologie.



Das NetApp Astra Control Center kann auf einem Red hat OpenShift-Cluster installiert werden. Über den Astra Trident Storage-Orchestrator mit Storage-Klassen und Storage-Back-Ends für NetApp ONTAP Storage-Systeme implementiert und konfiguriert werden.

Informationen zur Installation und Konfiguration von Astra Trident zur Unterstützung des Astra Control Center finden Sie unter "Dieses Dokument hier einfügen".

In einer Umgebung mit Cloud-Anbindung sorgt Astra Control Center mithilfe von Cloud Insights für erweitertes Monitoring und Telemetrie. Liegt keine Cloud Insights-Verbindung vor, ist eingeschränktes Monitoring und Telemetrie (7 Tage mit Kennzahlen) verfügbar und über offene metrische Endpunkte in native Kubernetes-Monitoring-Tools (Prometheus und Grafana) exportiert.

Astra Control Center ist vollständig in das AutoSupport- und Active IQ-Ecosystem von NetApp integriert und bietet damit Support für Benutzer, Hilfestellung bei der Fehlerbehebung und Statistiken zur Anzeige der Nutzungsstatistik.

Zusätzlich zur kostenpflichtigen Version des Astra Control Center ist eine 90-Tage-Evaluierungslizenz verfügbar. Die Evaluierungsversion wird durch die E-Mail und die Community (Slack-Kanal) unterstützt. Kunden haben Zugriff auf diese und andere Knowledge-Base-Artikel sowie auf die Dokumentation, die über das Produkt-Support-Dashboard verfügbar sind.

Besuchen Sie das NetApp Astra Control Center "Astra-Website".

Installationsvoraussetzungen für Astra Control Center

1. Ein oder mehrere Red hat OpenShift-Cluster. Die Versionen 4.6 EUS und 4.7 werden derzeit unterstützt.
2. Astra Trident muss bereits auf jedem Red hat OpenShift-Cluster installiert und konfiguriert sein.
3. Mindestens ein NetApp ONTAP Storage-System mit ONTAP 9.5 oder höher

> Es ist Best Practice für jede OpenShift-Installation an einem Standort, die über eine dedizierte SVM für persistenten Storage verfügt. Implementierungen an mehreren Standorten erfordern zusätzliche Storage-Systeme.

4. Auf jedem OpenShift-Cluster muss ein Trident-Storage-Back-End mit einer durch einen ONTAP-Cluster gesicherten SVM konfiguriert werden.
5. Eine Standard-StorageClass-Konfiguration auf jedem OpenShift-Cluster mit Astra Trident als Storage-provisionierung
6. Auf jedem OpenShift-Cluster muss ein Load Balancer installiert und konfiguriert werden, um den Lastausgleich zu ermöglichen und OpenShift Services offenzulegen.

> Siehe den Link "Hier" Weitere Informationen zu Load Balancer, die zu diesem Zweck validiert wurden.

7. Eine private Image-Registrierung muss konfiguriert sein, um die NetApp Astra Control Center Images zu hosten.

> Siehe den Link "Hier" So installieren und konfigurieren Sie eine private OpenShift-Registrierung zu diesem Zweck.

8. Sie benötigen Cluster-Admin-Zugriff auf das Red hat OpenShift-Cluster.
9. Sie müssen Administratorzugriff auf NetApp ONTAP Cluster haben.
10. Sie erhalten eine Admin-Workstation mit den Tools Docker oder Podman, tridentctl und oc oder kubectl, die Sie installiert und Ihrem €Pfad hinzugefügt haben.

> Bei Docker-Installationen muss die Docker-Version größer als 20.10 sein, und Podman-Installationen müssen über eine Podman-Version von mehr als 3.0 verfügen.

Installieren Sie Astra Control Center

OperatorHub wird verwendet

1. Melden Sie sich bei der NetApp Support-Website an und laden Sie die neueste Version des NetApp Astra Control Center herunter. Dazu ist eine Lizenz erforderlich, die an Ihr NetApp Konto angehängt ist. Nach dem Download des Tarballs, übertragen Sie es auf die Admin-Workstation.

   Um mit einer Testlizenz für Astra Control zu beginnen, besuchen Sie die "Astra: Anmelde-Website".

2. Entpacken Sie den tar-Ball und ändern Sie das Arbeitsverzeichnis in den resultierenden Ordner.

```
[netapp-user@rhel7 ~]$ tar -vxzf astra-control-center-
21.12.60.tar.gz
[netapp-user@rhel7 ~]$ cd astra-control-center-21.12.60
```

3. Bevor Sie mit der Installation beginnen, schieben Sie die Astra Control Center-Bilder in eine Bildregistrierung. Hierfür wählen Sie entweder Docker oder Podman. In diesem Schritt werden Anweisungen für beide angegeben.

Podman

a. Exportieren Sie den FQDN der Registrierung mit dem Namen der Organisation/des Namespace/Projekts als Umgebungsvariable ‘registry’.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-
registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

b. Melden Sie sich bei der Registrierung an.

```
[netapp-user@rhel7 ~]$ podman login -u ocp-user -p password
--tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```

> Wenn Sie verwenden `kubeadmin` Benutzer, um sich bei der privaten Registrierung anzumelden, dann Token statt Passwort verwenden - `podman login -u ocp-user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com`.

> Alternativ können Sie ein Service-Konto erstellen, dem Registry-Editor und/oder der Registry-Viewer-Rolle zuweisen (ob Sie Push/Pull-Zugriff benötigen) und sich mithilfe des Token des Service-Kontos bei der Registrierung anmelden.

c. Erstellen Sie eine Shell-Skriptdatei, und fügen Sie den folgenden Inhalt darin ein.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded
image trimming the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

> Wenn Sie nicht vertrauenswürdige Zertifikate für Ihre Registrierung verwenden, bearbeiten Sie das Shell-Skript und verwenden Sie es `--tls-verify=false` Für den Podman-Push-Befehl `podman push $REGISTRY/$(echo $astraImage | sed 's/[\/]\+\///') --tls-verify=false`.

d. Machen Sie die Datei ausführbar.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. Das Shell-Skript ausführen.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

Docker

a. Exportieren Sie den FQDN der Registrierung mit dem Namen der Organisation/des Namespace/Projekts als Umgebungsvariable ‘registry’.

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-
registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

b. Melden Sie sich bei der Registrierung an.

```
[netapp-user@rhel7 ~]$ docker login -u ocp-user -p password
astra-registry.apps.ocp-vmw.cie.netapp.com
```

> Wenn Sie verwenden `kubeadmin` Benutzer, um sich bei der privaten Registrierung anzumelden, dann Token statt Passwort verwenden - `docker login -u ocp-user -p token astra-registry.apps.ocp-vmw.cie.netapp.com`.

> Alternativ können Sie ein Service-Konto erstellen, dem Registry-Editor und/oder der Registry-Viewer-Rolle zuweisen (ob Sie Push/Pull-Zugriff benötigen) und sich mithilfe des Token des Service-Kontos bei der Registrierung anmelden.

c. Erstellen Sie eine Shell-Skriptdatei, und fügen Sie den folgenden Inhalt darin ein.

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded
image trimming the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

d. Machen Sie die Datei ausführbar.

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. Das Shell-Skript ausführen.

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

4. Wenn Sie private Bildregistries verwenden, die nicht öffentlich vertrauenswürdig sind, laden Sie die TLS-Zertifikate der Bildregistrierung auf die OpenShift-Knoten hoch. Erstellen Sie dazu im Namespace openshift-config eine configmap mit den TLS-Zertifikaten und patchen Sie sie auf die Cluster-Image-Konfiguration, damit das Zertifikat vertrauenswürdig ist.

```
[netapp-user@rhel7 ~]$ oc create configmap default-ingress-ca -n
openshift-config --from-file=astra-registry.apps.ocp
-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"default-ingress-
ca"}}}' --type=merge
```

> Wenn Sie eine interne OpenShift-Registrierung mit Standard-TLS-Zertifikaten vom Ingress Operator mit einer Route verwenden, müssen Sie den vorherigen Schritt dennoch befolgen, um die Zertifikate auf den Routing-Hostnamen zu patchen. Um die Zertifikate aus dem Ingress Operator zu extrahieren, können Sie den Befehl verwenden `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`.

5. Erstellen Sie einen Namespace `netapp-acc-operator` Für Astra Control Center.

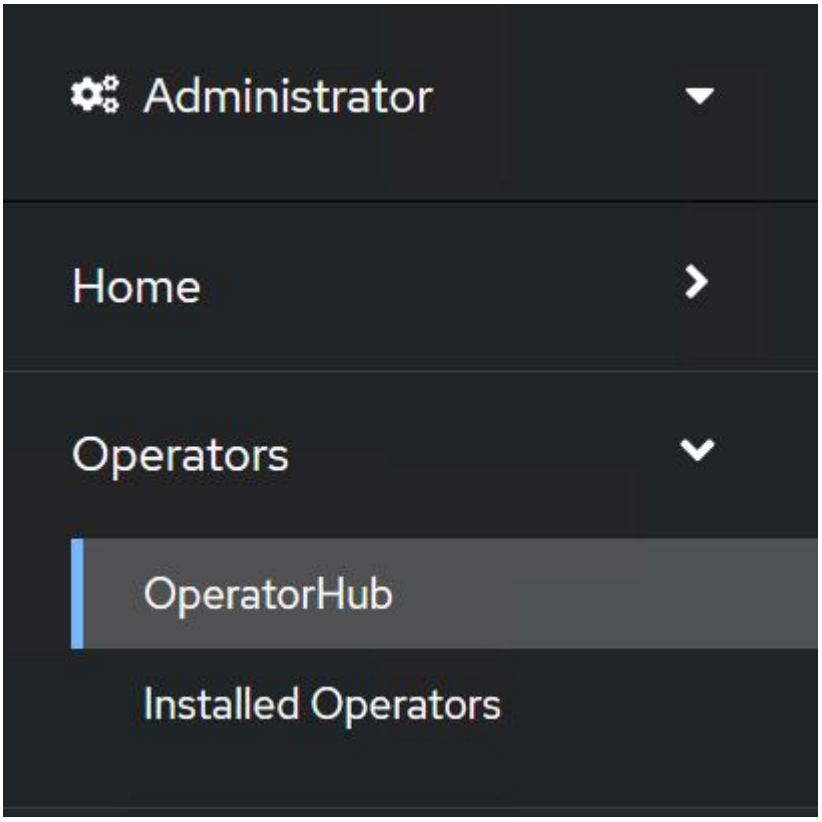
```
[netapp-user@rhel7 ~]$ oc create ns netapp-acc-operator

namespace/netapp-acc-operator created
```

6. Erstellen Sie ein Geheimnis mit Anmeldeinformationen, um sich in der Bildregistrierung anzumelden `netapp-acc-operator` Namespace.

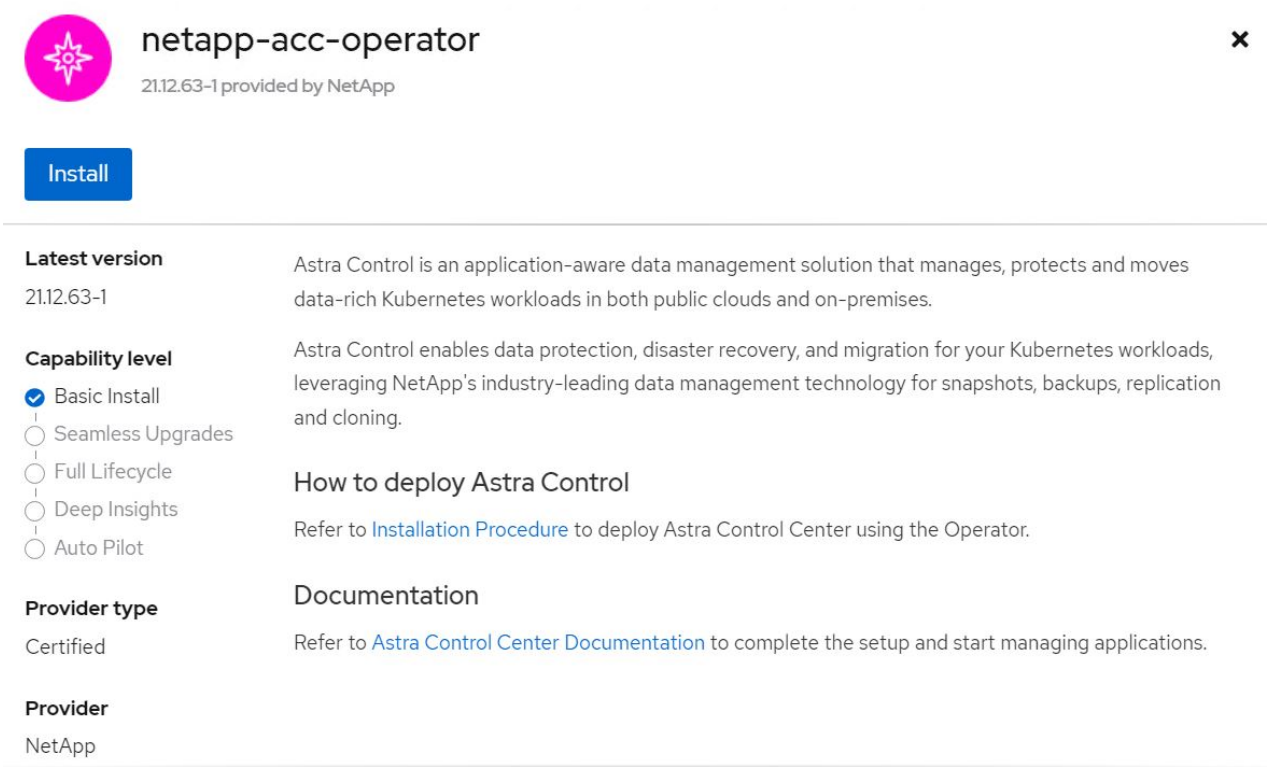
```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-
registry-cred --docker-server=astra-registry.apps.ocp
-vmw.cie.netapp.com --docker-username=ocp-user --docker
-password=password -n netapp-acc-operator

secret/astra-registry-cred created
```

7. Melden Sie sich bei der Red hat OpenShift GUI-Konsole mit Zugriff auf Cluster-Administratoren an.
8. Wählen Sie in der Dropdown-Liste Perspektive den Eintrag Administrator aus.

9. Navigieren Sie zu Operators > OperatorHub, und suchen Sie nach Astra.



10. Wählen Sie `netapp-acc-operator` kachel und klicken Sie auf `Install`.



11. Übernehmen Sie im Bildschirm Operator installieren alle Standardparameter, und klicken Sie auf `Install`.

OperatorHub > Operator Installation

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

- alpha
- stable

Installation mode *

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

Installed Namespace *

PR netapp-acc-operator (Operator recommended)

Namespace already exists
Namespace **netapp-acc-operator** already exists and will be used. Other users can already have access to this namespace.

Approval strategy *

- Automatic
- Manual

Install Cancel

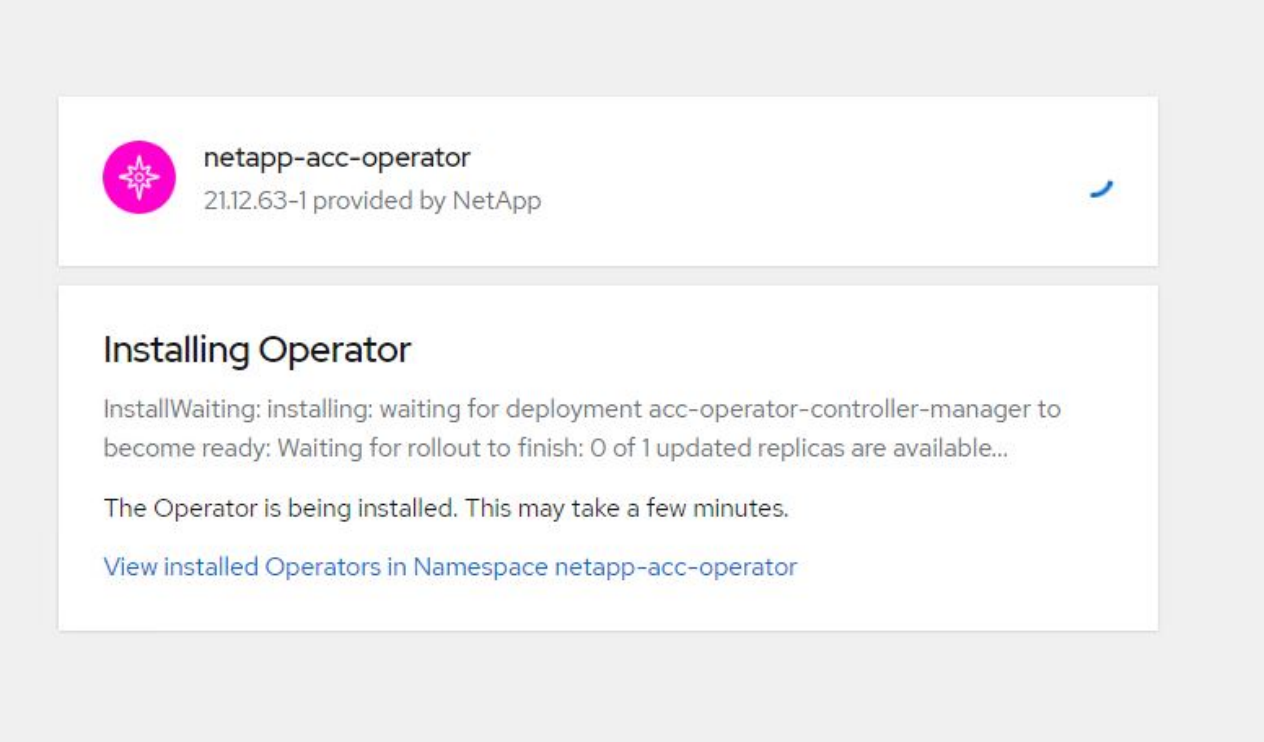
netapp-acc-operator
provided by NetApp

Provided APIs

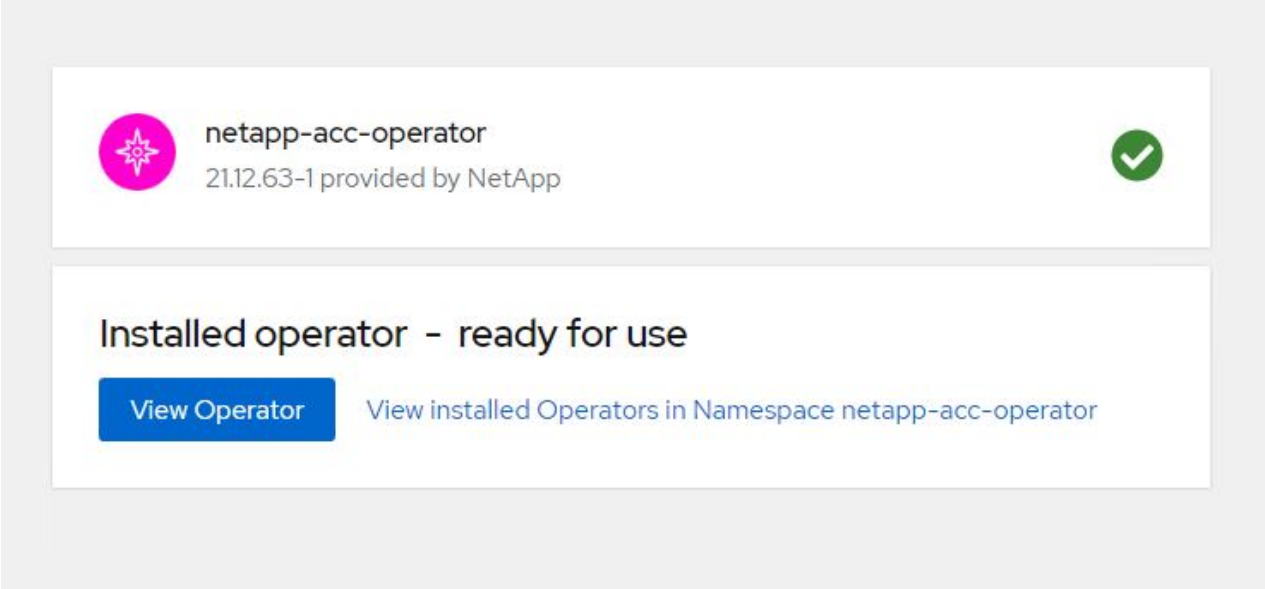
ACC Astra Control Center

AstraControlCenter is the Schema for the astracontrolcenters API

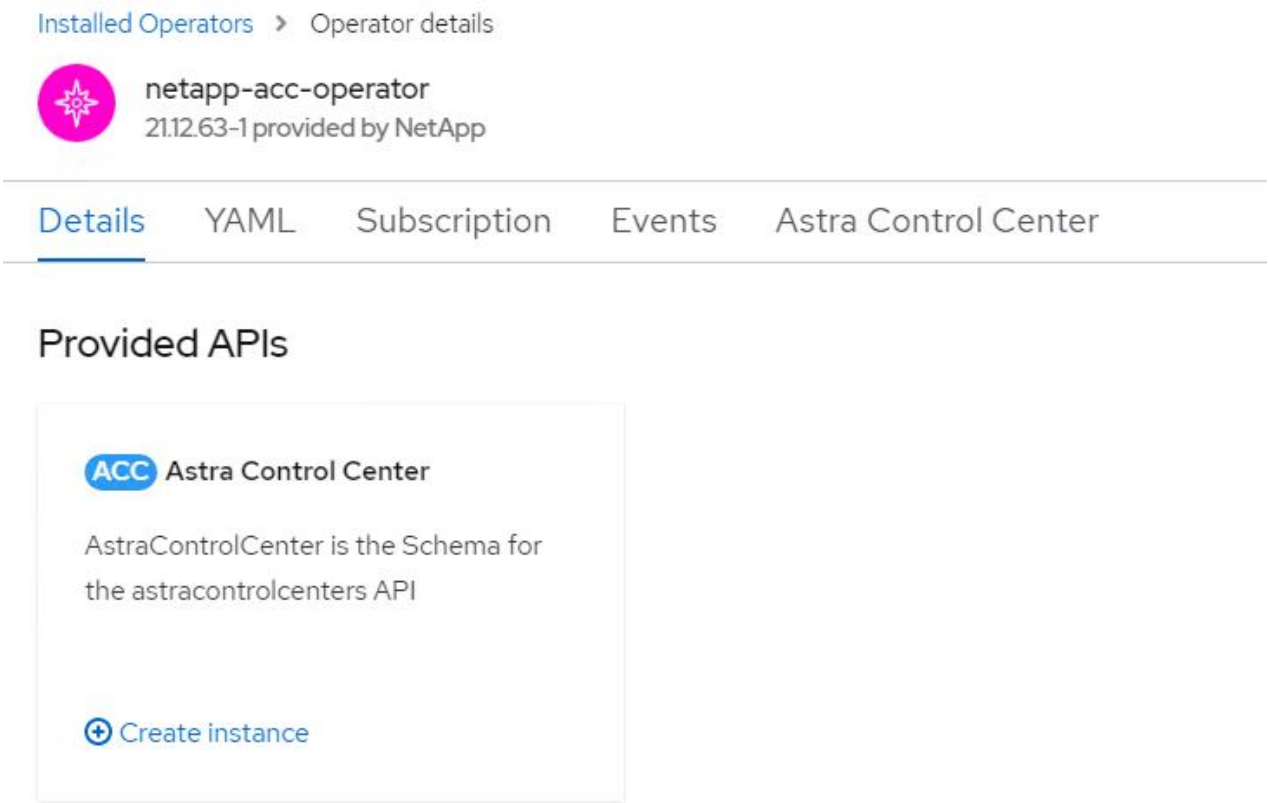
12. Warten Sie, bis die Installation des Bedieners abgeschlossen ist.



13. Sobald die Installation des Bedieners erfolgreich abgeschlossen ist, navigieren Sie zu, um auf zu klicken `View Operator`.



14. Klicken Sie dann auf `Create Instance` Im Astra Control Center Kachel im Operator.



15. Füllen Sie die aus `Create AstraControlCenter` Formularfelder und klicken Sie auf `Create`.

    a. Bearbeiten Sie optional den Instanznamen des Astra Control Center.
    b. Aktivieren oder deaktivieren Sie optional Auto Support. Es wird empfohlen, die Auto Support-Funktion beizubehalten.
    c. Geben Sie den FQDN für Astra Control Center ein.
    d. Geben Sie die Astra Control Center-Version ein. Die neueste wird standardmäßig angezeigt.

e. Geben Sie einen Kontonamen für das Astra Control Center und die Administratordetails wie Vorname, Nachname und E-Mail-Adresse ein.

f. Geben Sie die Richtlinie zur Rückgewinnung von Volumes ein. Die Standardeinstellung wird beibehalten.

g. Geben Sie in der Bildregistrierung den FQDN für Ihre Registrierung zusammen mit dem Namen der Organisation ein, den Sie erhalten haben, während Sie die Bilder in die Registrierung schieben (in diesem Beispiel `astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra`)

h. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, geben Sie den geheimen Namen im Abschnitt Image Registry ein.

i. Konfigurieren Sie Skalierungsoptionen für Astra Control Center Ressourceneinschränkungen.

j. Geben Sie den Namen der Speicherklasse ein, wenn PVCs in eine nicht-Standardspeicherklasse platziert werden sollen.

k. Definieren Sie die Einstellungen für die Verarbeitung von CRD.

Project: netapp-acc-operator

Name *

astra

Labels

app=frontend

Account Name *

HCG Solutions Engineering

Astra Control Center account name

Astra Address *

astra-control-center.cie.netapp.com

AstraAddress defines how Astra will be found in the data center. This IP address and/or DNS A record must be created prior to provisioning Astra Control Center. Example - "astra.example.com" The A record and its IP address must be allocated prior to provisioning Astra Control Center

Astra Version *

21.12.60

Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch

Email *

solutions_tme@netapp.com

EmailAddress will be notified by Astra as events warrant.

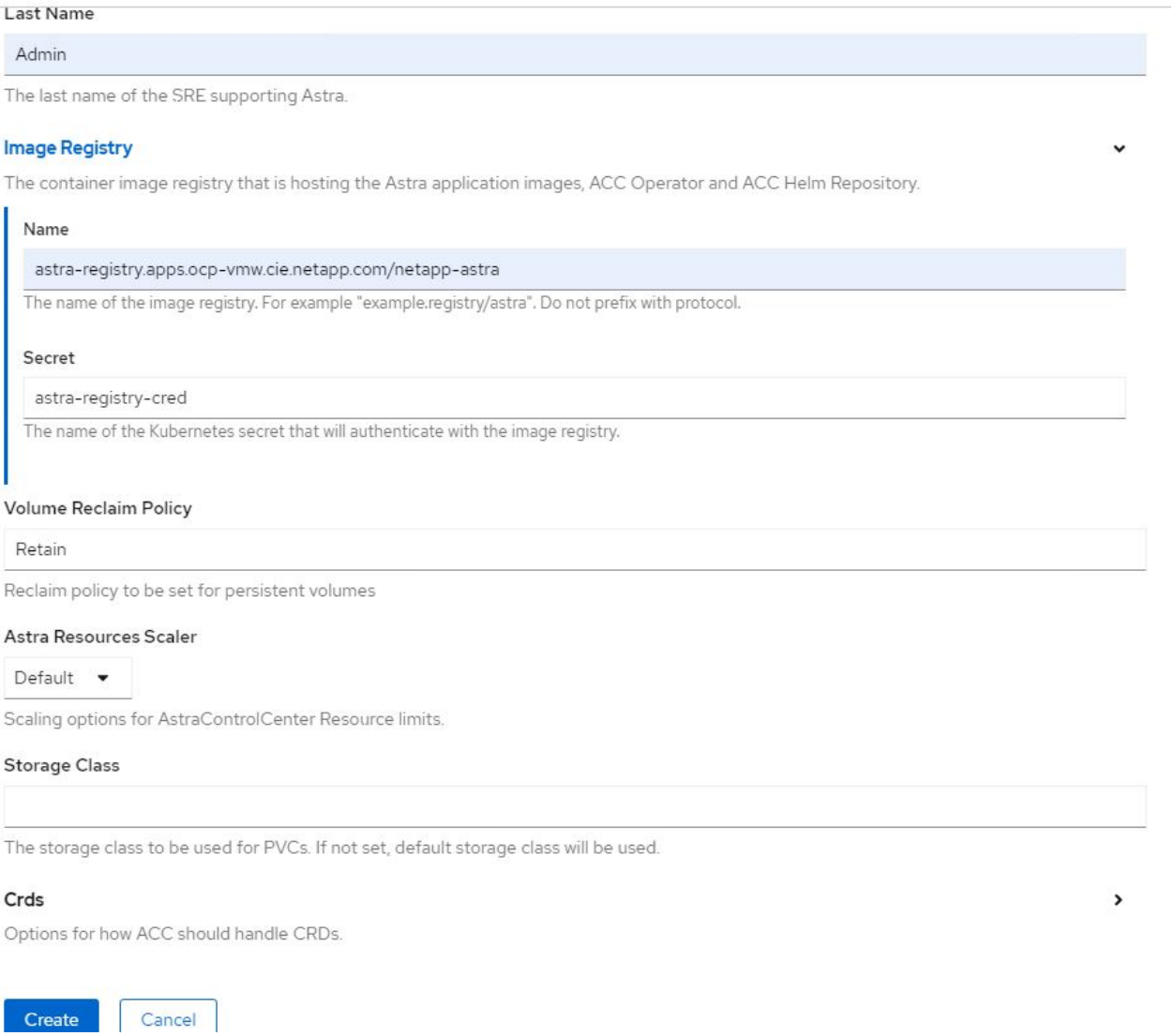
Auto Support *

AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. The default election is true and indicates support data will be sent to NetApp. An empty or blank election is the same as a default election. Air gapped installations should enter false.

First Name

HCG

The first name of the SRE supporting Astra.



Automatisiert [Ansible]

1. Um Astra Control Center mit Ansible-Playbooks zu implementieren, benötigen Sie eine Ubuntu/RHEL-Maschine mit installiertem Ansible. Befolgen Sie die Anweisungen "Hier" Für Ubuntu und RHEL.
2. Klonen Sie das GitHub Repository, das Ansible-Inhalte hostet.

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. Melden Sie sich bei der NetApp Support-Website an und laden Sie die neueste Version des NetApp Astra Control Center herunter. Dazu ist eine Lizenz erforderlich, die an Ihr NetApp Konto angehängt ist. Nach dem Download des Tarballs, übertragen Sie es auf die Workstation.

> Um mit einer Testlizenz für Astra Control zu beginnen, besuchen Sie die "Astra: Anmelde-Website".

4. Erstellen oder beziehen Sie die kubeconfig-Datei mit Administratorzugriff auf das OpenShift-Cluster, auf dem Astra Control Center installiert werden soll.

5. Ändern Sie das Verzeichnis in die na_astra_control_Suite.

```
cd na_astra_control_suite
```

6. Bearbeiten Sie das `vars/vars.yml` Datei, und füllen Sie die Variablen mit den erforderlichen Informationen.

```
#Define whether or not to push the Astra Control Center images to
your private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or
"Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer
type service to access ACC, requires MetalLB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the
kubernetes/openshift cluster Astra Control Center needs to be
installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-
kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want
to accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the
PVCs to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
```

```
values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values:
yes, no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image
registry credentials
#Usually, the registry namespace and usernames are same for
individual users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the
playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin
```

7. Nutzen Sie das Playbook zur Implementierung des Astra Control Center. Für bestimmte Konfigurationen sind Root-Berechtigungen erforderlich.

   Wenn der Benutzer, der das Playbook ausführt, root ist oder eine passwortlose sudo-Konfiguration hat, führen Sie den folgenden Befehl aus, um das Playbook auszuführen.

   ```
   ansible-playbook install_acc_playbook.yml
   ```

   Wenn der Benutzer passwortbasierten sudo-Zugriff konfiguriert hat, führen Sie den folgenden Befehl aus, um das Playbook auszuführen, und geben Sie dann das sudo-Passwort ein.

```
ansible-playbook install_acc_playbook.yml -K
```

Schritte Nach Der Installation

1. Die Installation kann einige Minuten dauern. Überprüfen Sie, ob alle Pods und Services im enthalten sind `netapp-astra-cc` Der Namespace ist betriebsbereit.

```
[netapp-user@rhel7 ~]$ oc get all -n netapp-astra-cc
```

2. Prüfen Sie die `acc-operator-controller-manager` Protokolle, um sicherzustellen, dass die Installation abgeschlossen ist.

```
[netapp-user@rhel7 ~]$ oc logs deploy/acc-operator-controller-manager -n
netapp-acc-operator -c manager -f
```

Die folgende Meldung zeigt die erfolgreiche Installation des Astra Control Centers an.

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraContro
lCenter","msg":"Successfully Reconciled AstraControlCenter in
[seconds]s","AstraControlCenter":"netapp-astra-
cc/astra","ae.Version":"[21.12.60]"}
```

3. Der Benutzername für die Anmeldung beim Astra Control Center ist die E-Mail-Adresse des Administrators in der CRD-Datei und das Passwort ist eine Zeichenfolge `ACC-` An die Astra Control Center UUID angehängt. Führen Sie den folgenden Befehl aus:

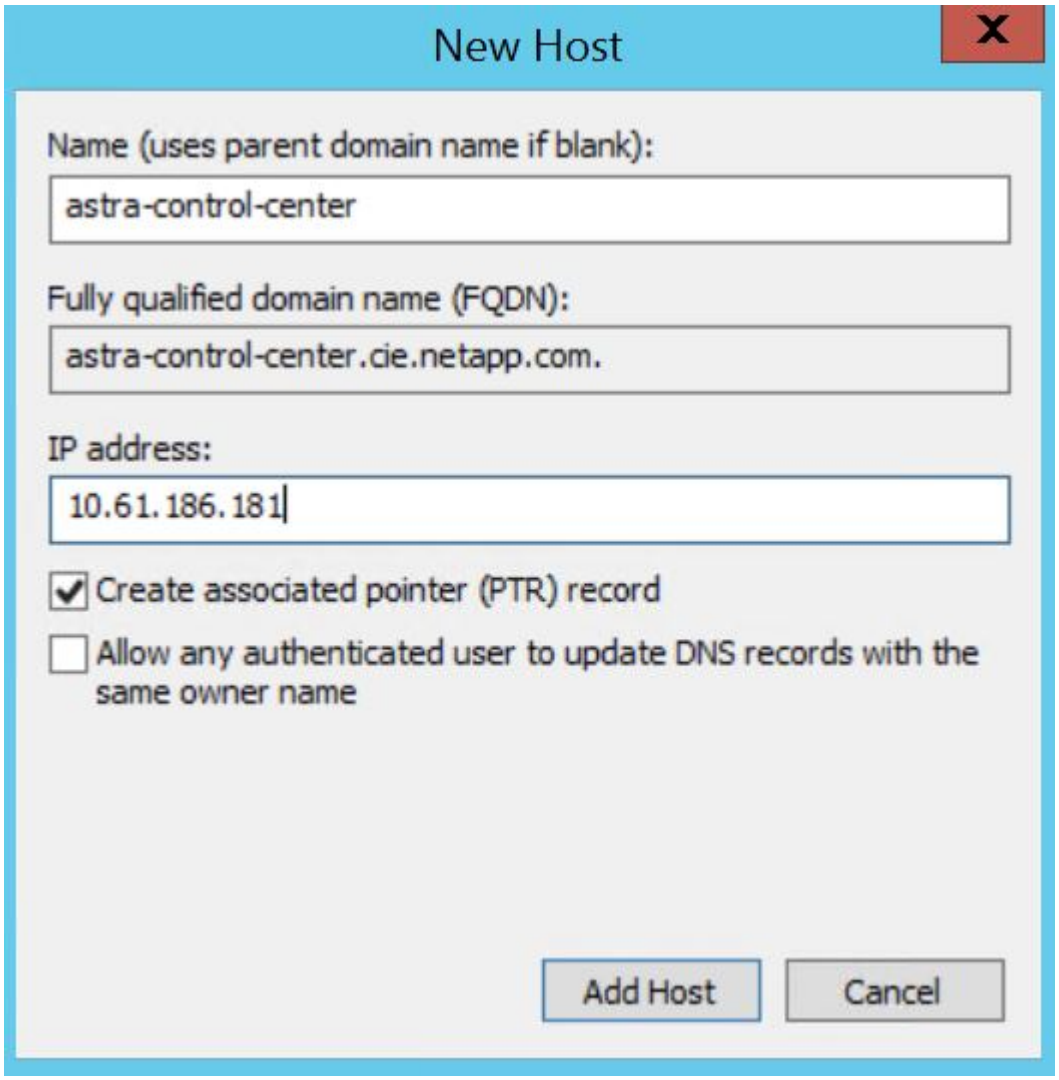
```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME    UUID
astra   345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```

In diesem Beispiel lautet das Passwort `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

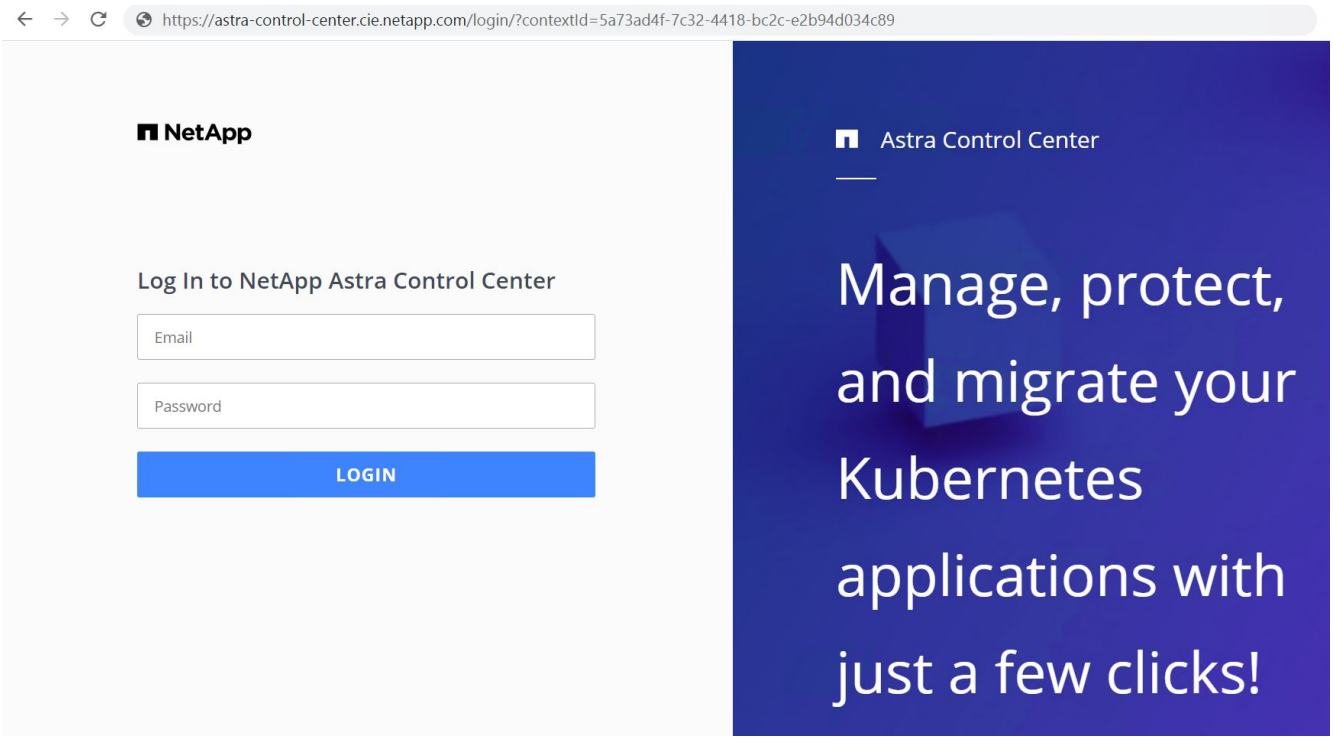
4. Holen Sie die LastausgleichsIP für den Traefik-Dienst ab.

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep
'EXTERNAL|traefik'

NAME                                        TYPE           CLUSTER-IP
EXTERNAL-IP     PORT(S)
AGE
traefik                                     LoadBalancer   172.30.99.142
10.61.186.181   80:30343/TCP,443:30060/TCP
16m
```

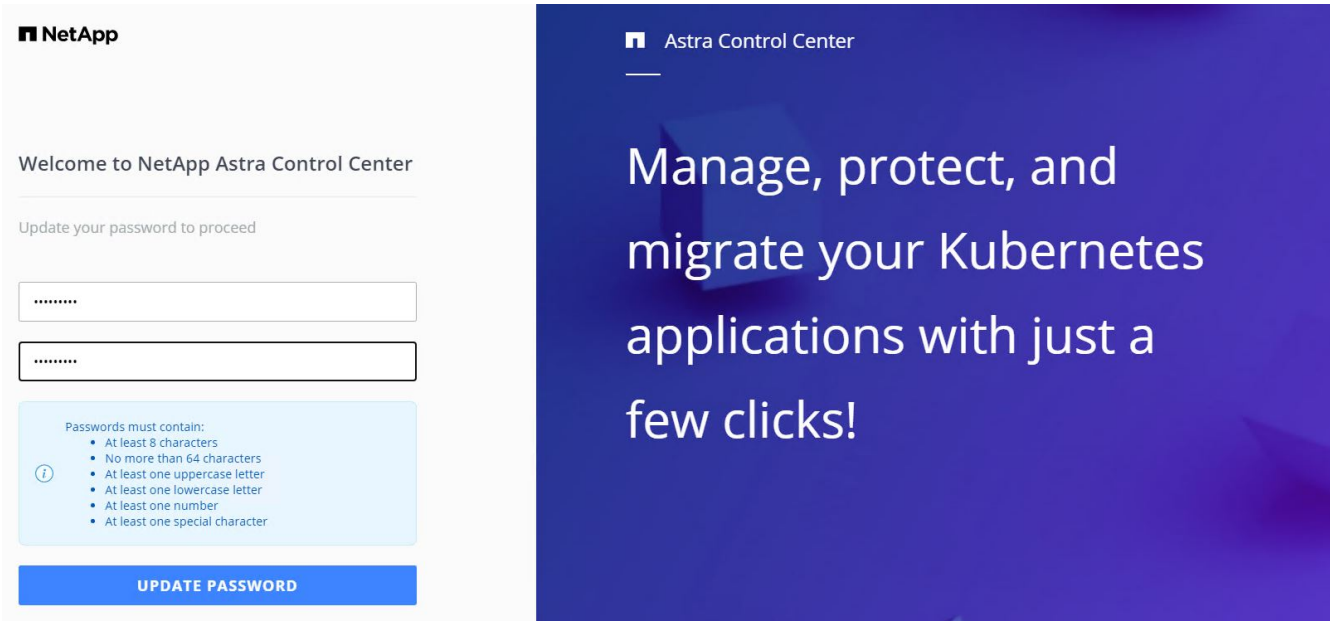
5. Fügen Sie einen Eintrag im DNS-Server hinzu, der auf den in der Astra Control Center CRD-Datei angegebenen FQDN verweist `EXTERNAL-IP` Des Schleppdienstes.



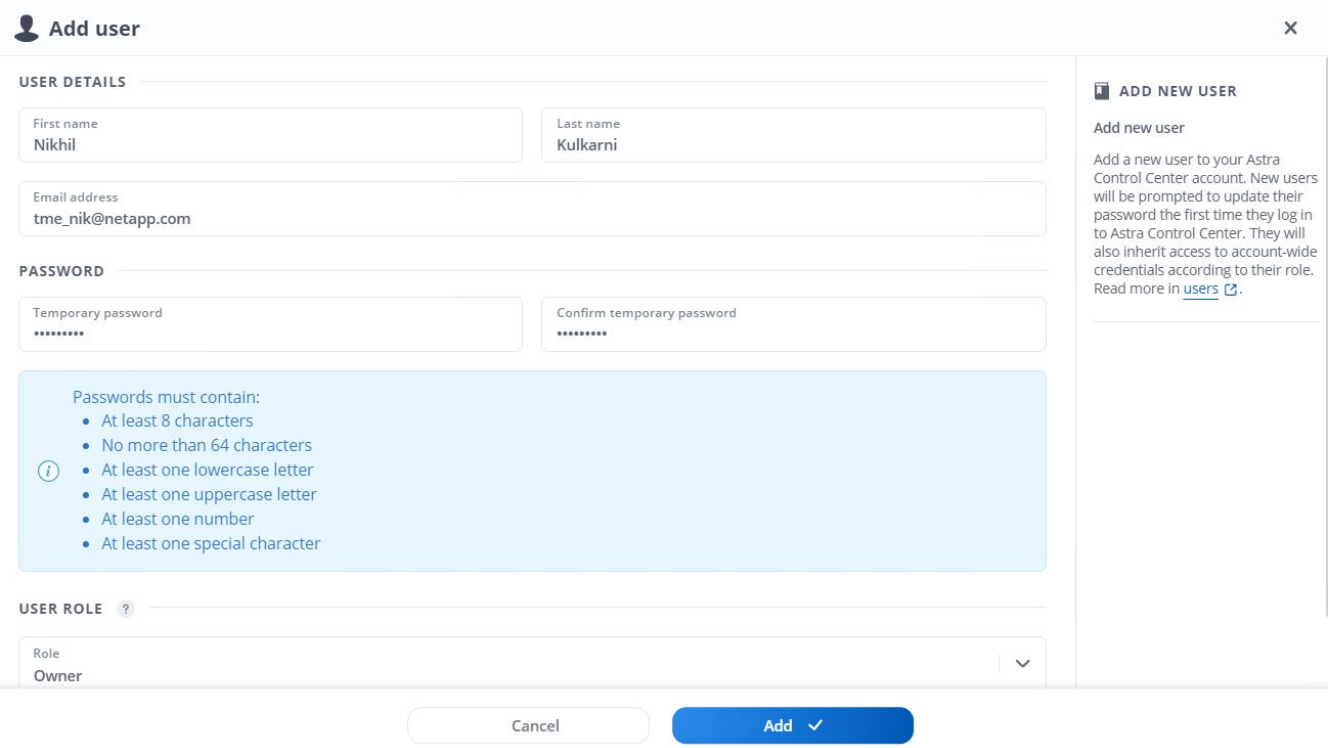
6. Melden Sie sich bei der Astra Control Center-GUI an, indem Sie den FQDN durchsuchen.



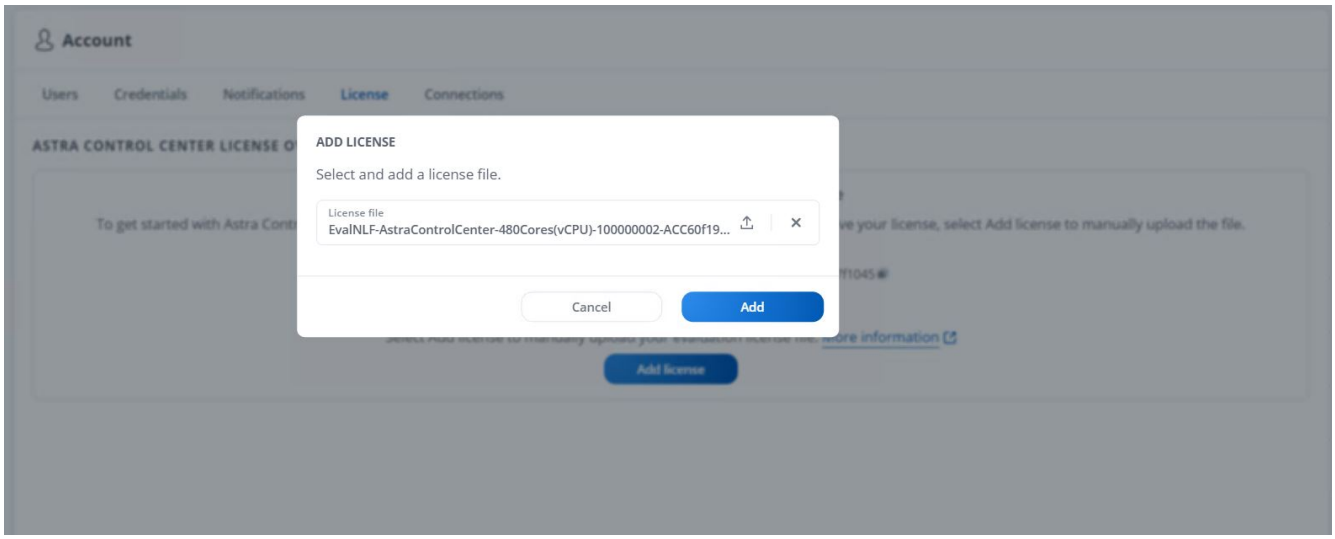
7. Wenn Sie sich zum ersten Mal über die in CRD angegebene Admin-E-Mail-Adresse bei der Benutzeroberfläche des Astra Control Center anmelden, müssen Sie das Passwort ändern.



8. Wenn Sie dem Astra Control Center einen Benutzer hinzufügen möchten, navigieren Sie zu Konto > Benutzer, klicken Sie auf Hinzufügen, geben Sie die Details des Benutzers ein und klicken Sie auf Hinzufügen.



9. Astra Control Center erfordert eine Lizenz, damit alle Funktionalitäten der IT funktionieren können. Um eine Lizenz hinzuzufügen, navigieren Sie zu Konto > Lizenz, klicken Sie auf Lizenz hinzufügen und laden Sie die Lizenzdatei hoch.



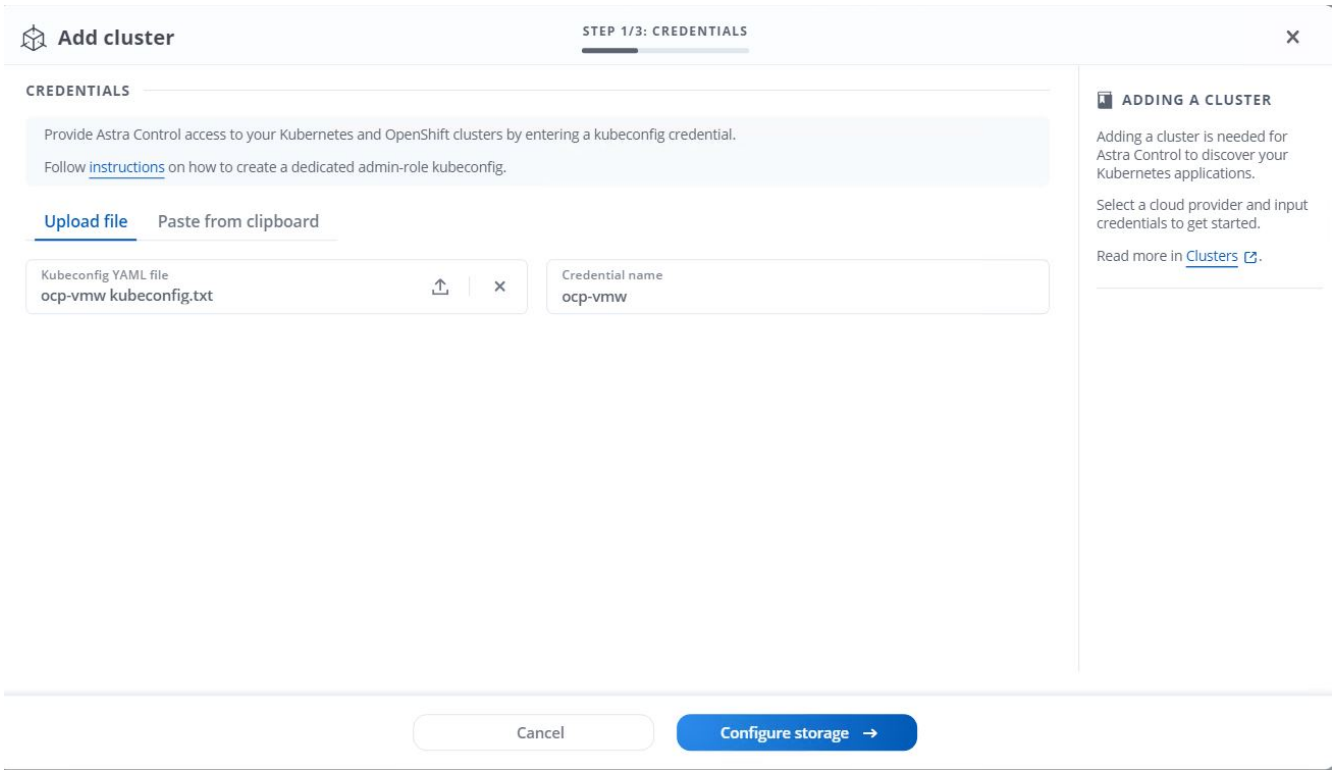
> Bei Problemen mit der Installation oder Konfiguration von NetApp Astra Control Center steht die Wissensdatenbank mit bekannten Problemen zur Verfügung "Hier".

Registrieren Sie Ihre Red hat OpenShift-Cluster mit dem Astra Control Center

Damit das Astra Control Center Ihre Workloads managen kann, müssen Sie zunächst Ihren Red hat OpenShift-Cluster registrieren.

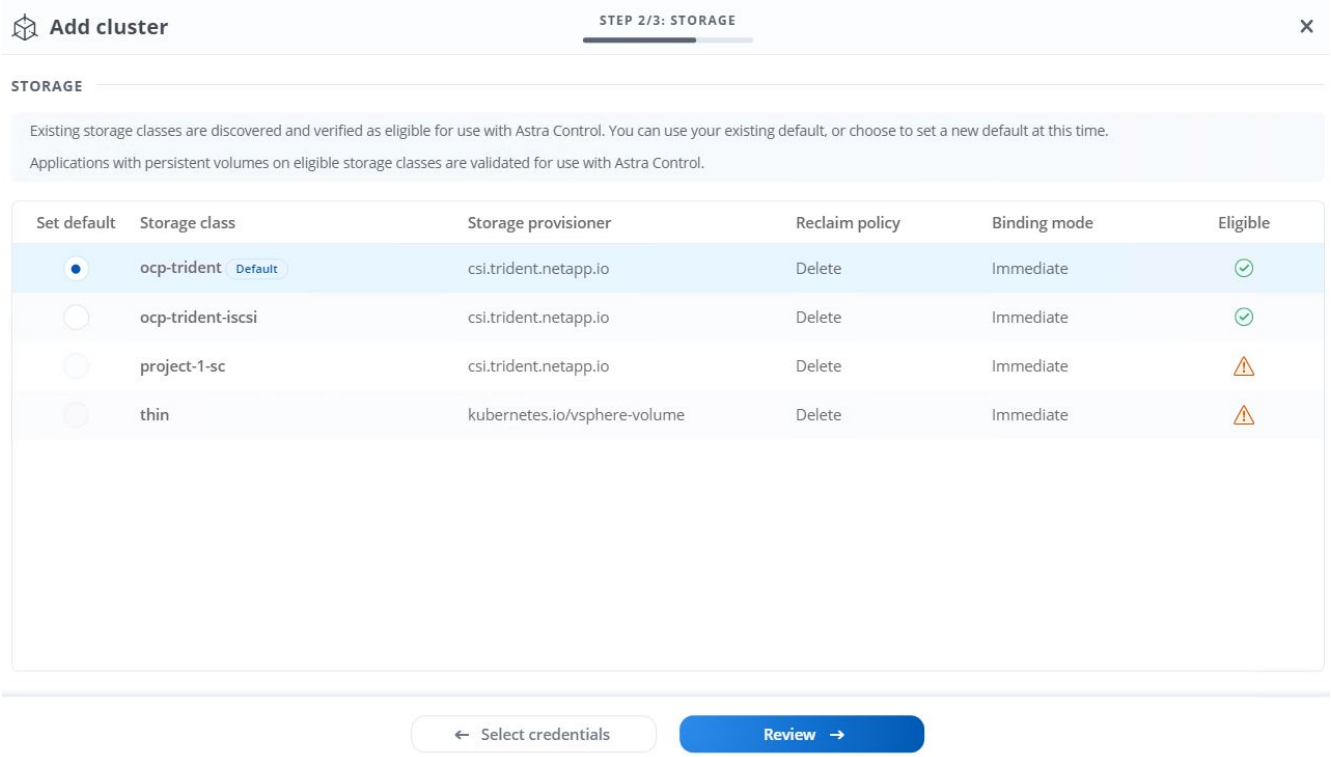
Red hat OpenShift-Cluster registrieren

1. Der erste Schritt besteht darin, die OpenShift Cluster zum Astra Control Center hinzuzufügen und zu verwalten. Wechseln Sie zu Cluster und klicken Sie auf Cluster hinzufügen, laden Sie die kubeconffig-Datei für den OpenShift-Cluster hoch, und klicken Sie auf Storage auswählen.

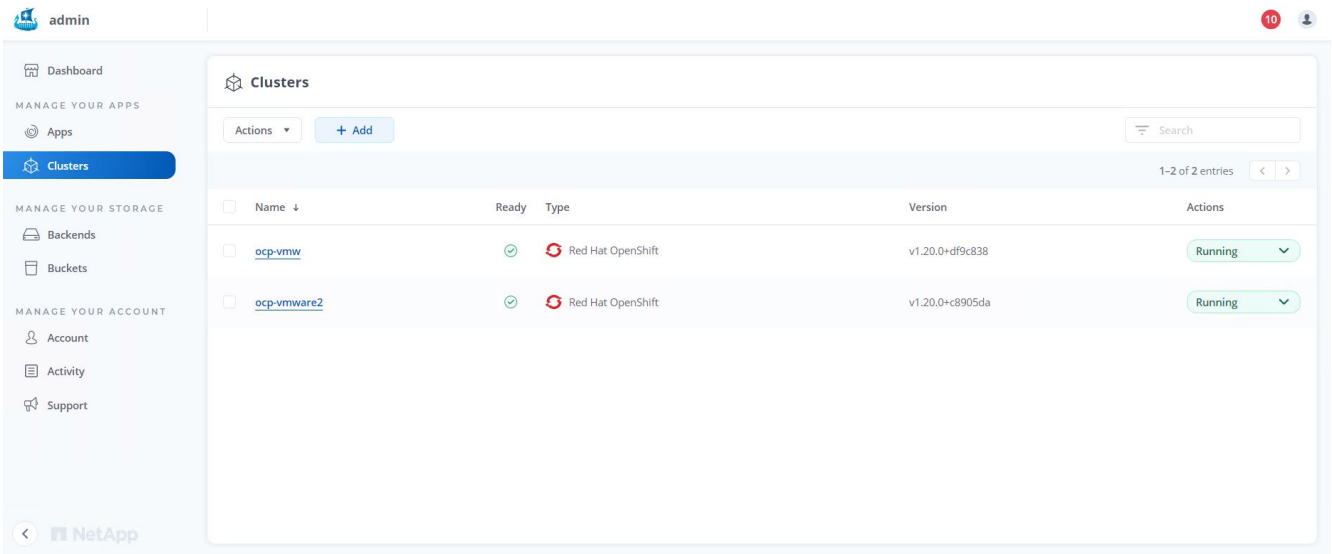


> Die kubeconfig-Datei kann zur Authentifizierung mit einem Benutzernamen und Passwort oder einem Token erzeugt werden. Token laufen nach begrenzter Zeit ab und lassen das registrierte Cluster möglicherweise nicht mehr erreichbar. NetApp empfiehlt, eine kubeconfig-Datei mit einem Benutzernamen und einem Passwort zu verwenden, um Ihre OpenShift-Cluster beim Astra Control Center zu registrieren.

2. Astra Control Center erkennt geeignete Storage-Klassen. Wählen Sie jetzt aus, wie Storage Volumes mithilfe von Trident durch eine SVM auf NetApp ONTAP bereitgestellt werden, und klicken Sie auf „Review“ (prüfen). Überprüfen Sie im nächsten Teilfenster die Details, und klicken Sie auf Cluster hinzufügen.

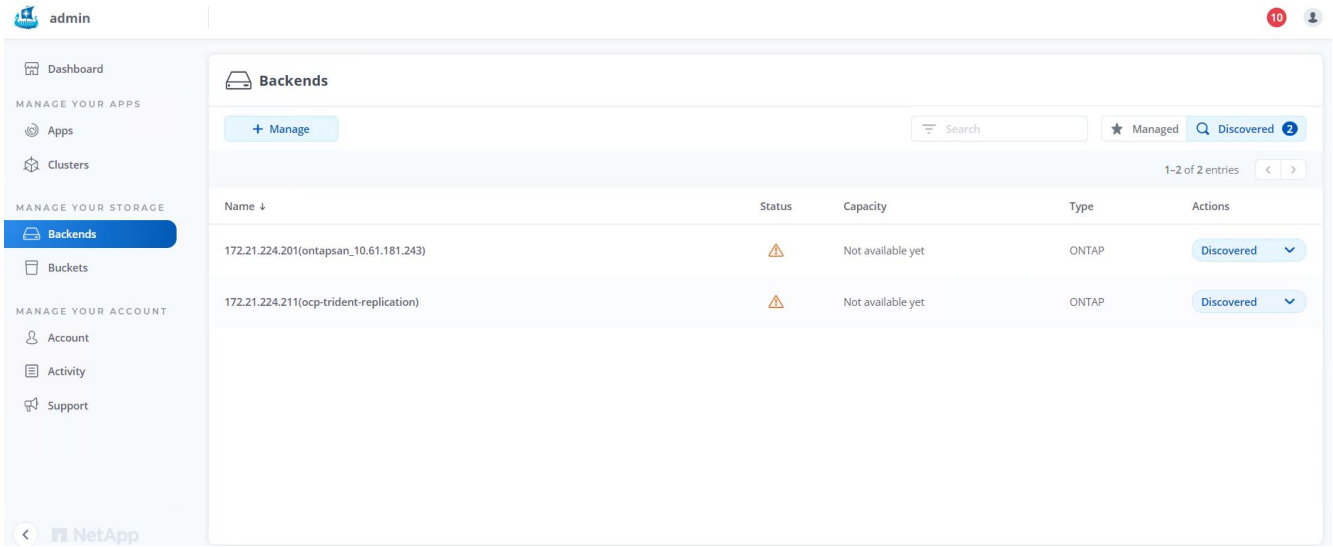


3. Registrieren Sie beide OpenShift-Cluster wie in Schritt 1 beschrieben. Wenn sie hinzugefügt werden, wechseln die Cluster zum Status Erkennung, während das Astra Control Center sie überprüft und die erforderlichen Agenten installiert. Der Cluster-Status ändert sich auf „ausgeführt“, nachdem sie erfolgreich registriert wurden.

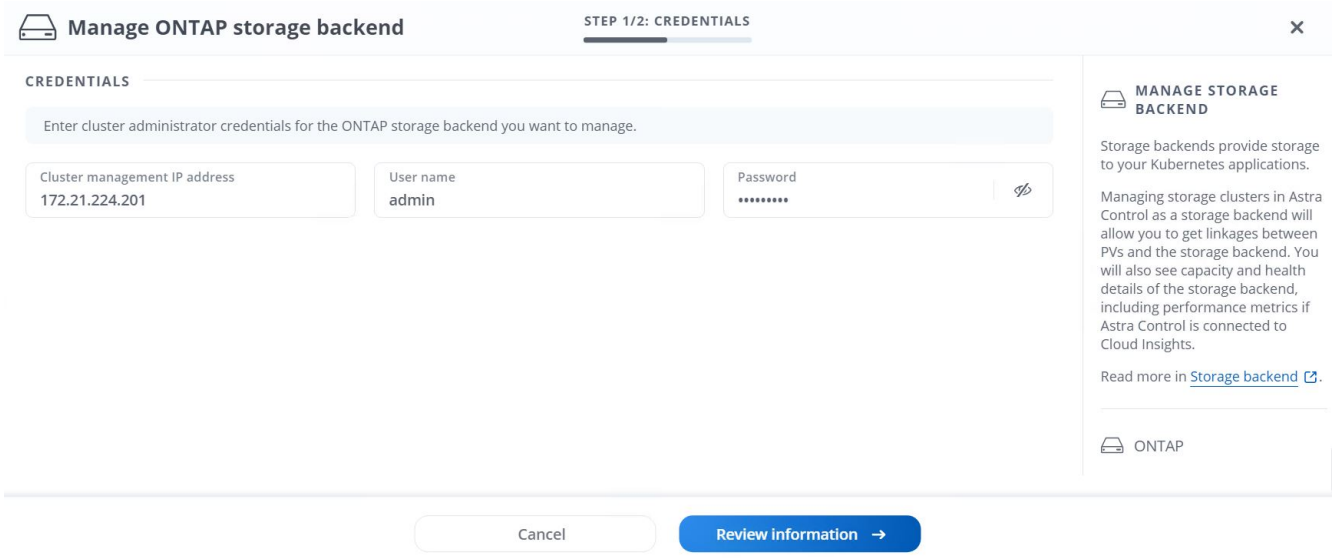


> Alle von Astra Control Center zu verwaltenden Red hat OpenShift-Cluster sollten Zugriff auf die Bildregistrierung haben, die für die Installation verwendet wurde, da die auf den verwalteten Clustern installierten Agenten die Bilder aus dieser Registrierung ziehen.

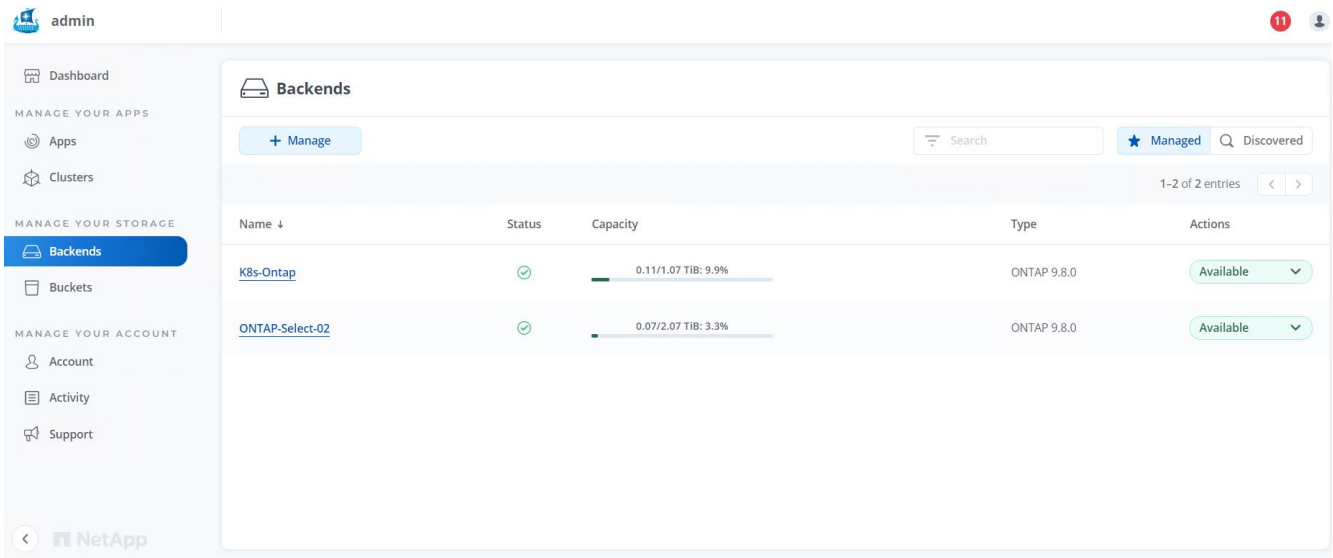
4. Importieren Sie ONTAP-Cluster als Storage-Ressourcen, die vom Astra Control Center als Back-Ends gemanagt werden sollen. Wenn dem Astra OpenShift-Cluster hinzugefügt und ein Storage-glass konfiguriert ist, erkennt und inspiziert er den ONTAP-Cluster automatisch auf der Basis der Storage-glass, importiert ihn aber nicht in das zu verwaltende Astra-Control-Center.



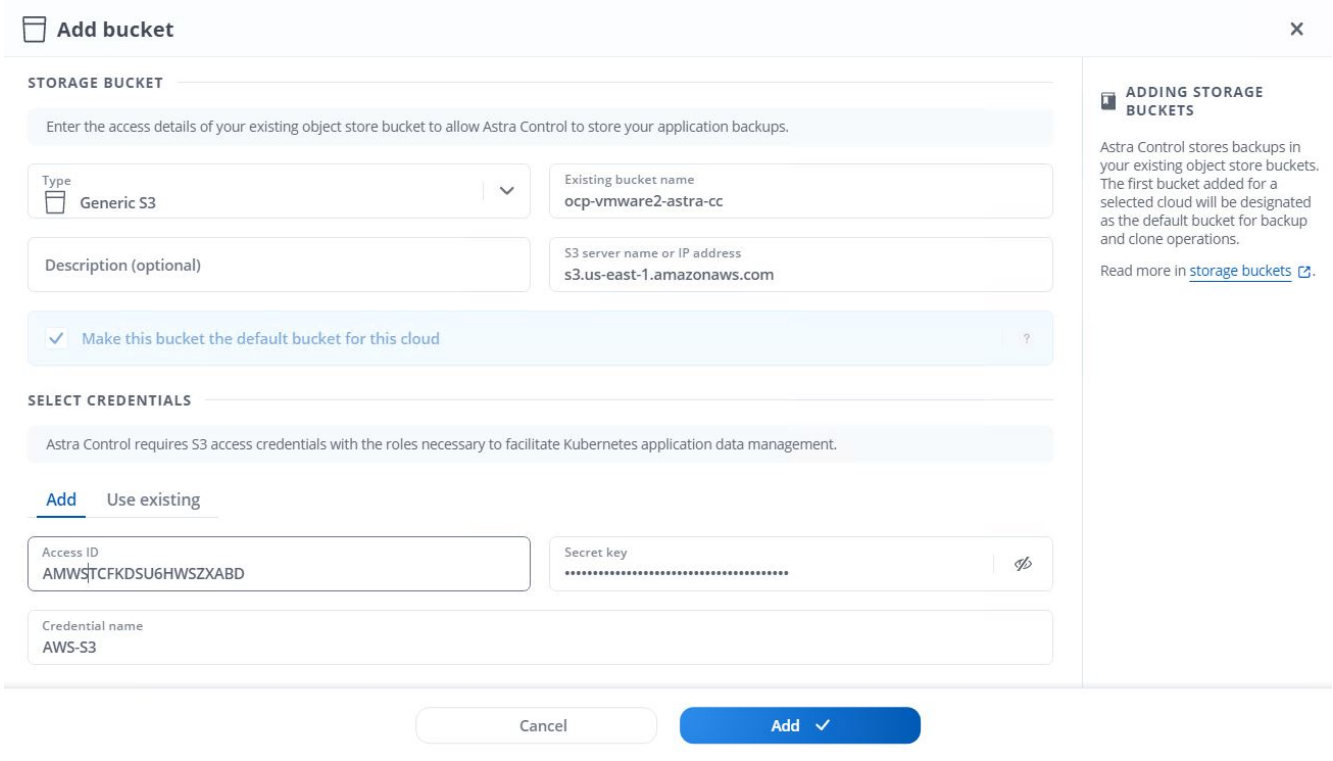
5. Um die ONTAP-Cluster zu importieren, gehen Sie zu Backend, klicken Sie auf das Dropdown-Menü und wählen Sie Verwalten neben dem zu verwaltenden ONTAP-Cluster aus. Geben Sie die ONTAP-Cluster-Anmeldeinformationen ein, klicken Sie auf Informationen überprüfen und klicken Sie dann auf Speicher-Backend importieren.



6. Nach dem Hinzufügen der Back-Ends ändert sich der Status in „verfügbar“. Diese Back-Ends enthalten jetzt Informationen über die persistenten Volumes im OpenShift-Cluster und die entsprechenden Volumes im ONTAP-System.



7. Für Backups und Restores in OpenShift-Clustern mit Astra Control Center müssen Sie einen Objekt-Storage-Bucket bereitstellen, der das S3-Protokoll unterstützt. Aktuell werden ONTAP S3, StorageGRID und AWS S3 unterstützt. Im Rahmen dieser Installation wird ein AWS S3-Bucket konfiguriert. Wechseln Sie zu Buckets, klicken Sie auf „Bucket hinzufügen“ und wählen Sie „Allgemeines S3“ aus. Geben Sie die Details zum S3-Bucket ein und erhalten Sie Zugangsdaten, um darauf zuzugreifen. Aktivieren Sie das Kontrollkästchen „Machen Sie diesen Bucket zum Standard-Bucket für die Cloud“ und klicken Sie dann auf Hinzufügen.

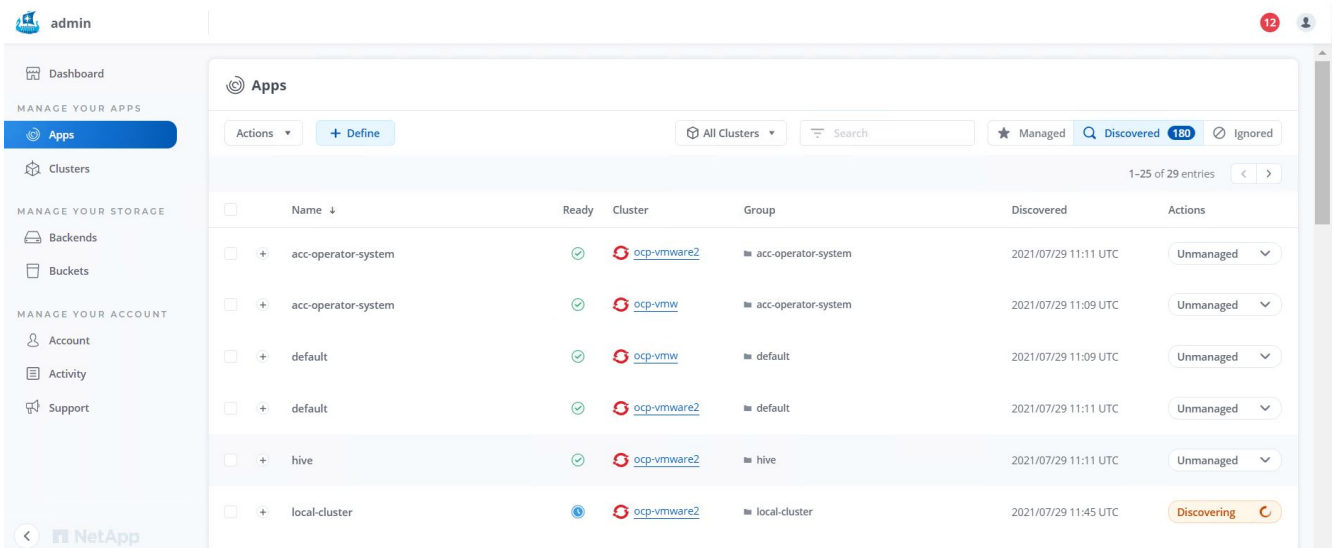


Wählen Sie die zu schützenden Applikationen aus

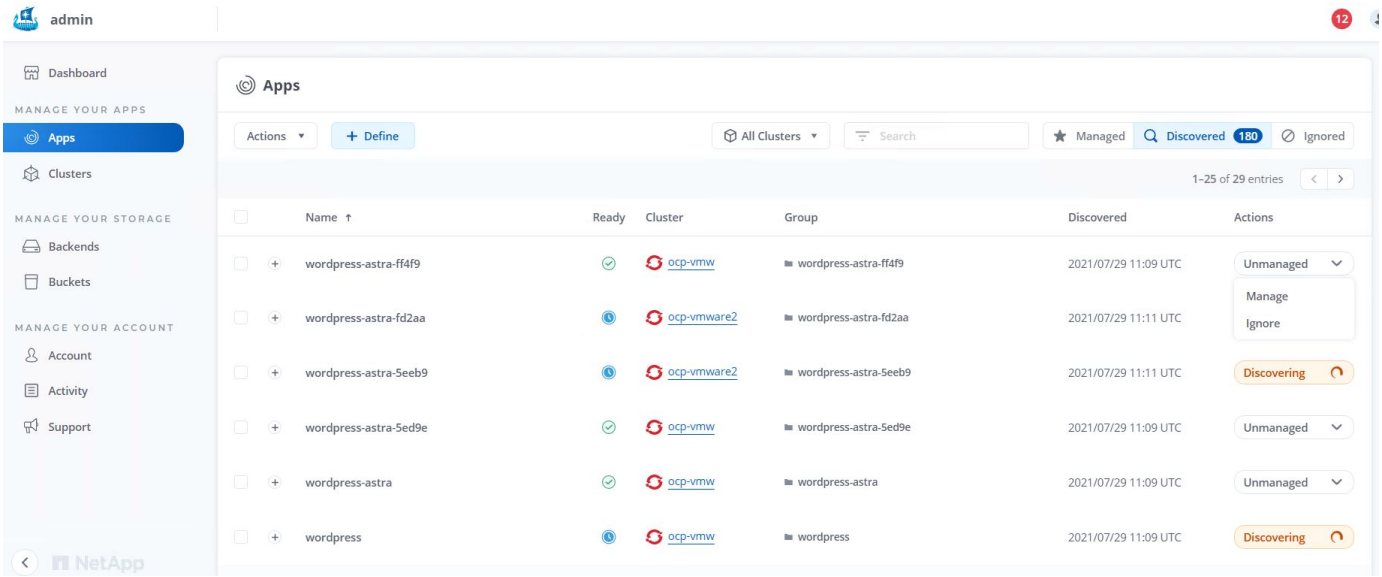
Nachdem Sie Ihre Red hat OpenShift-Cluster registriert haben, können Sie über das Astra Control Center die Anwendungen ermitteln, die bereitgestellt und verwaltet werden.

Management von Applikationen

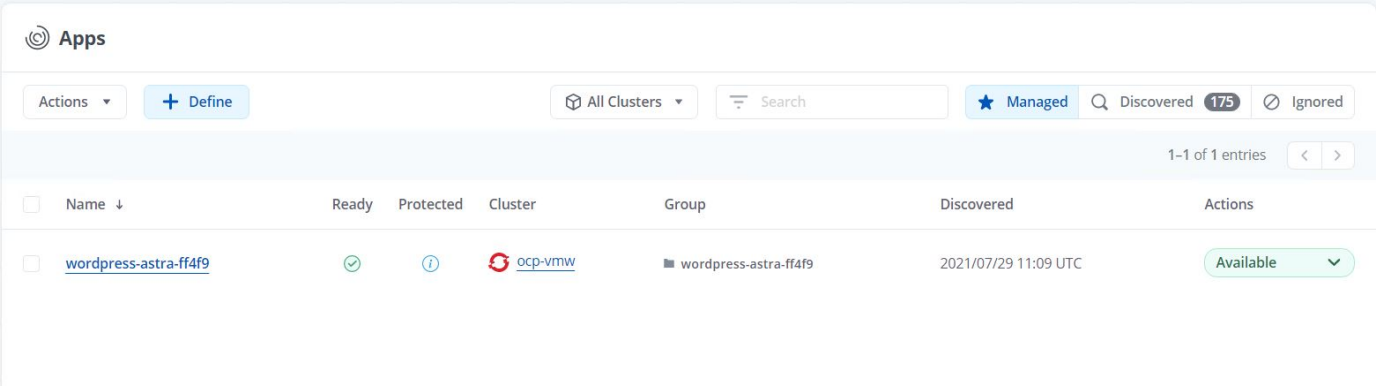
1. Nachdem die OpenShift-Cluster und ONTAP-Back-Ends beim Astra Control Center registriert wurden, beginnt das Kontrollzentrum automatisch die Anwendungen in allen Namespaces zu erkennen, die die mit dem angegebenen ONTAP-Backend konfigurierte Speicherageclass verwenden.



2. Navigieren Sie zu Apps > entdeckt, und klicken Sie auf das Dropdown-Menü neben der Anwendung, die Sie mit Astra verwalten möchten. Klicken Sie dann auf Verwalten.



1. Die Anwendung wechselt in den Status „verfügbar“ und kann im Abschnitt „Apps“ unter der Registerkarte „verwaltet“ angezeigt werden.



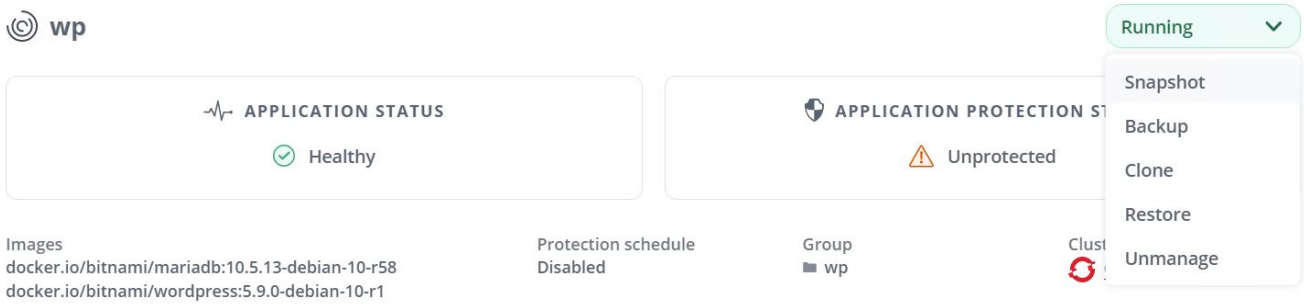
Sichern Sie Ihre Applikationen

Nachdem die Applikations-Workloads vom Astra Control Center gemanagt wurden, können Sie die Sicherungseinstellungen für diese Workloads konfigurieren.

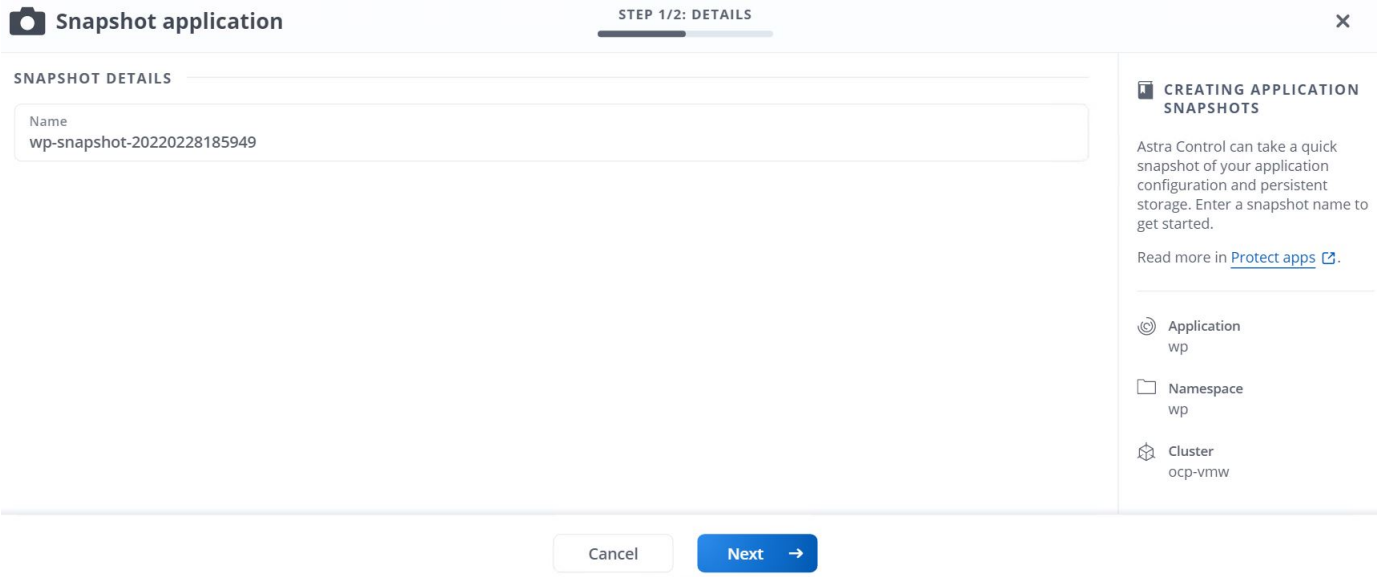
Erstellen eines Anwendungs-Snapshots

Ein Snapshot einer Applikation erstellt eine ONTAP Snapshot Kopie, mit der die Applikation auf Basis dieser Snapshot Kopie einem bestimmten Zeitpunkt wiederhergestellt oder geklont werden kann.

1. Um einen Snapshot der Anwendung zu erstellen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die Anwendung, von der Sie eine Snapshot Kopie erstellen möchten. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf Snapshot.



2. Geben Sie die Snapshot-Details ein, klicken Sie auf Weiter und klicken Sie dann auf Snapshot. Es dauert etwa eine Minute, um den Snapshot zu erstellen, und der Status wird verfügbar, nachdem der Snapshot erfolgreich erstellt wurde.



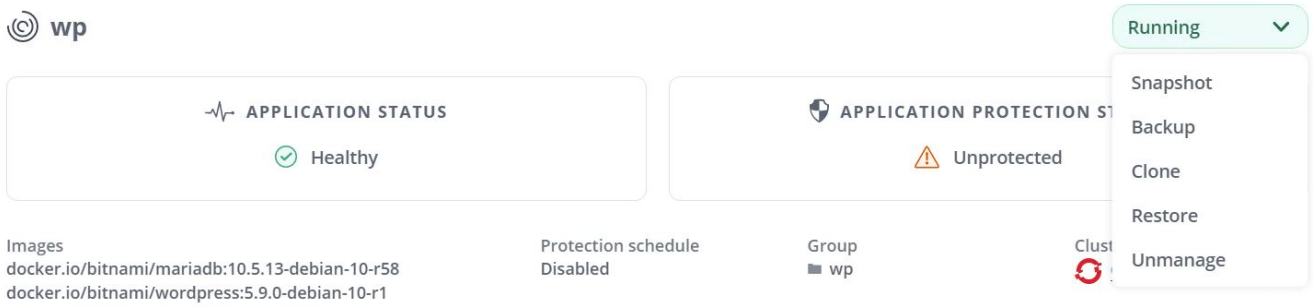
Erstellen eines Applikations-Backups

Ein Backup einer Applikation erfasst den aktiven Status der Applikation und die Konfiguration der Ressourcen des IT-Systems, deckt sie in Dateien ab und speichert sie in einem Remote-Objekt-Storage-Bucket.

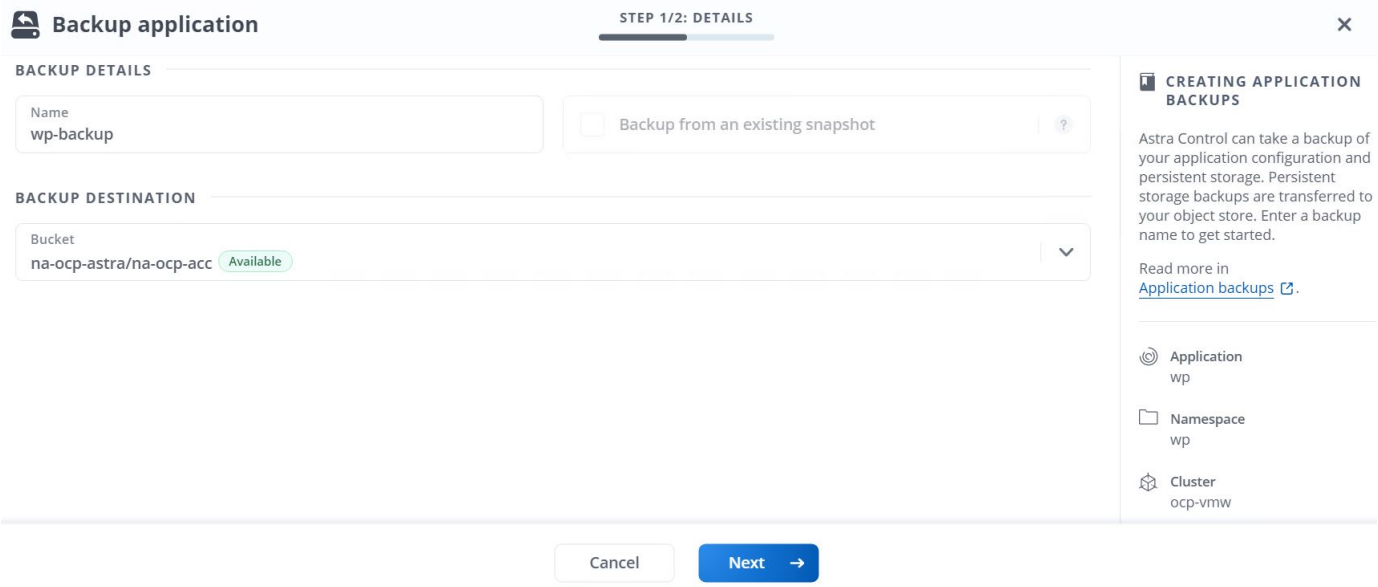
Für die Sicherung und Wiederherstellung von verwalteten Anwendungen im Astra Control Center müssen Sie die Superuser-Einstellungen für die ONTAP-Systeme als Voraussetzung konfigurieren. Geben Sie dazu die folgenden Befehle ein.

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1 -anon
65534 -vserver ocp-trident
```

1. Um ein Backup der verwalteten Anwendung im Astra Control Center zu erstellen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die Anwendung, von der Sie ein Backup durchführen möchten. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf Backup.



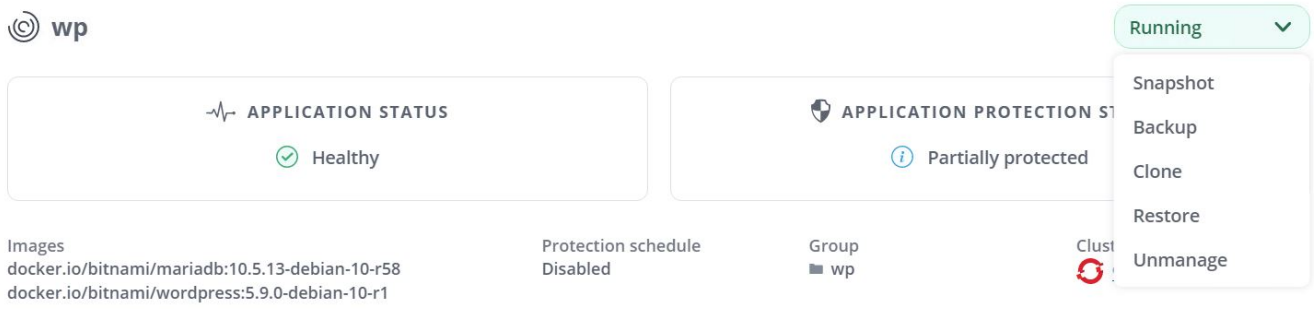
2. Geben Sie die Backup-Details ein, wählen Sie den Objekt-Storage-Bucket aus, der die Backup-Dateien enthält, klicken Sie auf Weiter und klicken Sie nach Überprüfung der Details auf Backup. Abhängig von der Größe der Applikation und den Daten kann das Backup mehrere Minuten dauern und der Status des Backups wird nach erfolgreichem Abschluss des Backups wieder verfügbar.



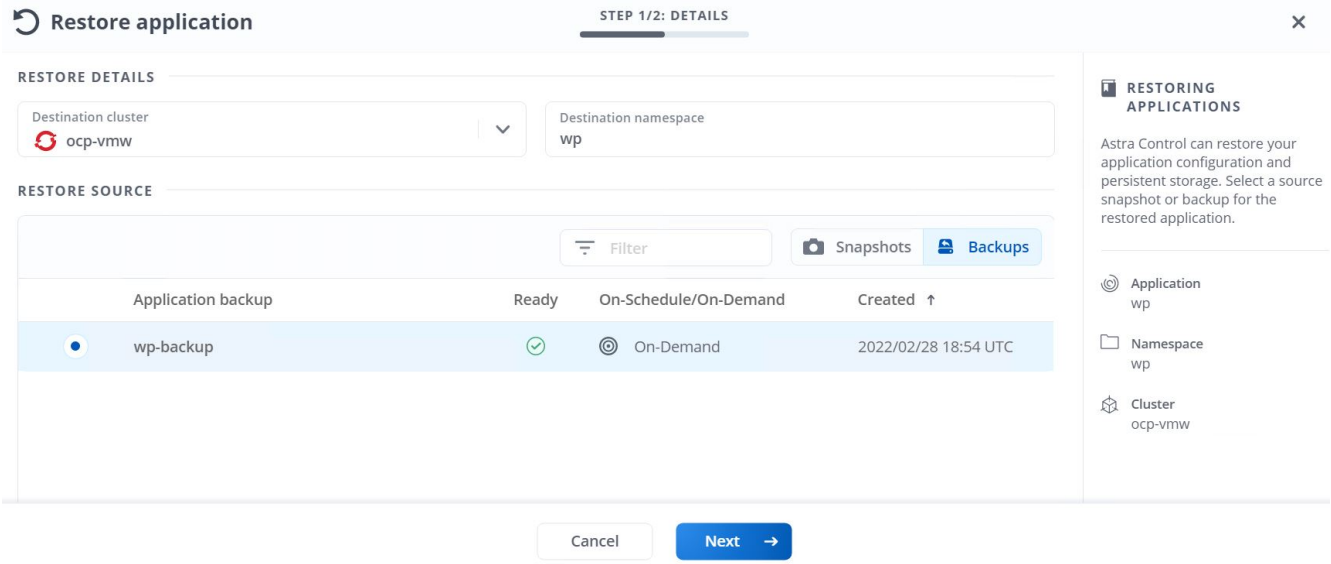
Wiederherstellen einer Anwendung

Auf Knopfdruck können Sie eine Applikation zum Zwecke der Applikationssicherung und Disaster Recovery im selben Cluster oder zu einem Remote-Cluster wiederherstellen, was den Namespace Ursprung im selben Cluster hat.

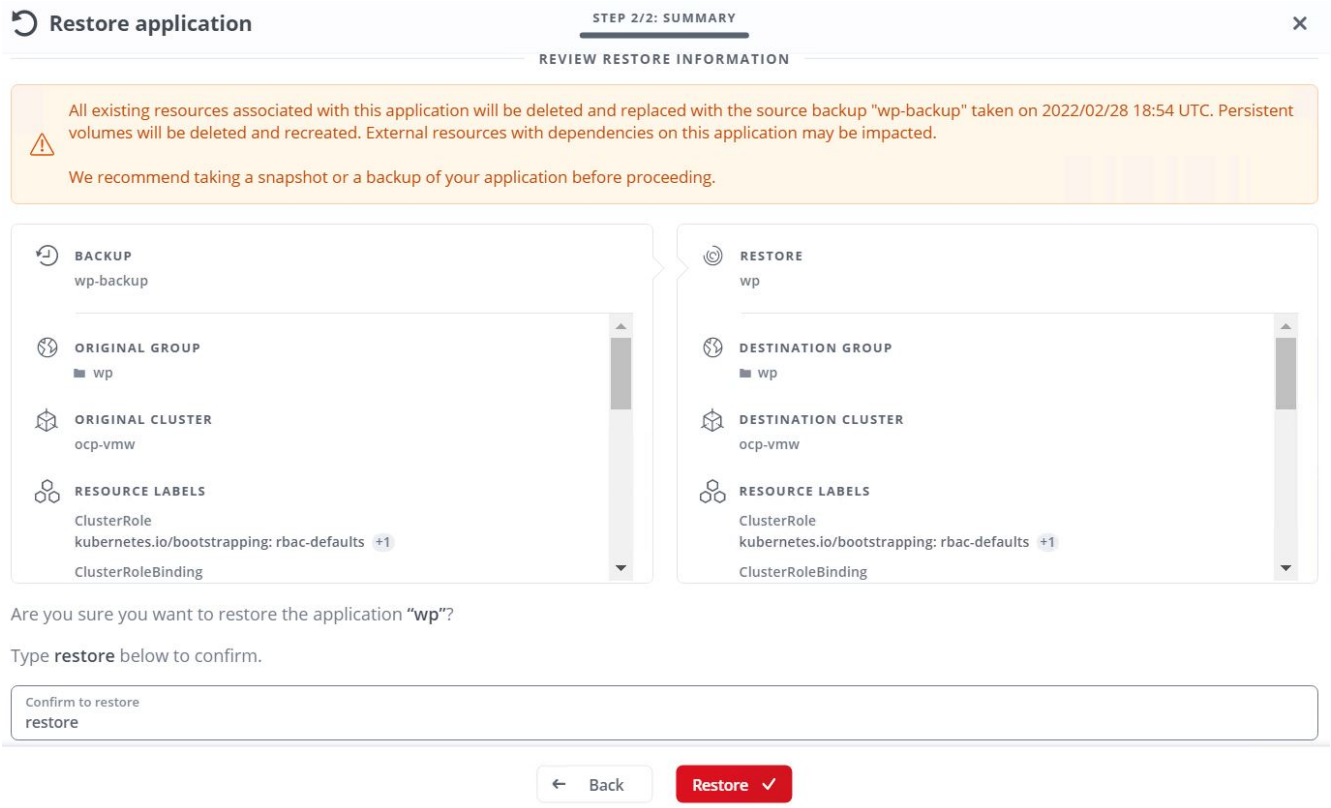
1. Um eine Anwendung wiederherzustellen, navigieren Sie zu „Apps“ > „Managed“, und klicken Sie auf die betreffende Anwendung. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen, und klicken Sie auf `Restore`.



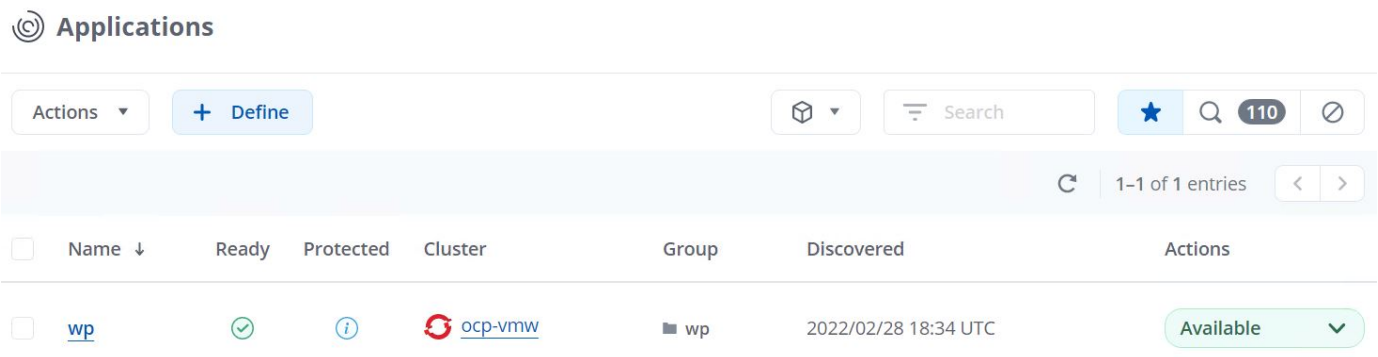
2. Geben Sie den Namen des Restore Namespace ein, wählen Sie den Cluster aus, in dem Sie ihn wiederherstellen möchten, und wählen Sie aus einem vorhandenen Snapshot oder aus einem Backup der Applikation aus, ob Sie ihn wiederherstellen möchten. Klicken Sie Auf Weiter.



3. Geben Sie im Prüfungsfenster ein `restore` Und klicken Sie auf Wiederherstellen, nachdem Sie die Details geprüft haben.



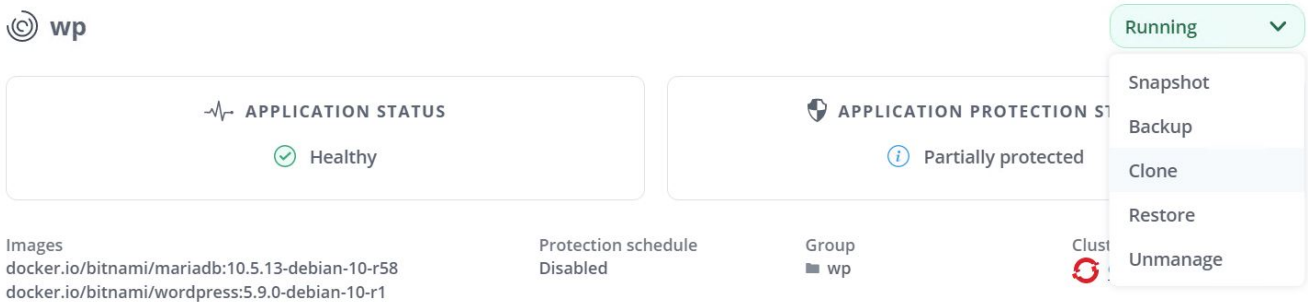
4. Die neue Applikation geht in den Status Wiederherstellen, während Astra Control Center die Anwendung auf dem ausgewählten Cluster wiederherstellt. Nachdem alle Ressourcen der Anwendung installiert und von Astra erkannt wurden, geht die Anwendung in den verfügbaren Zustand.



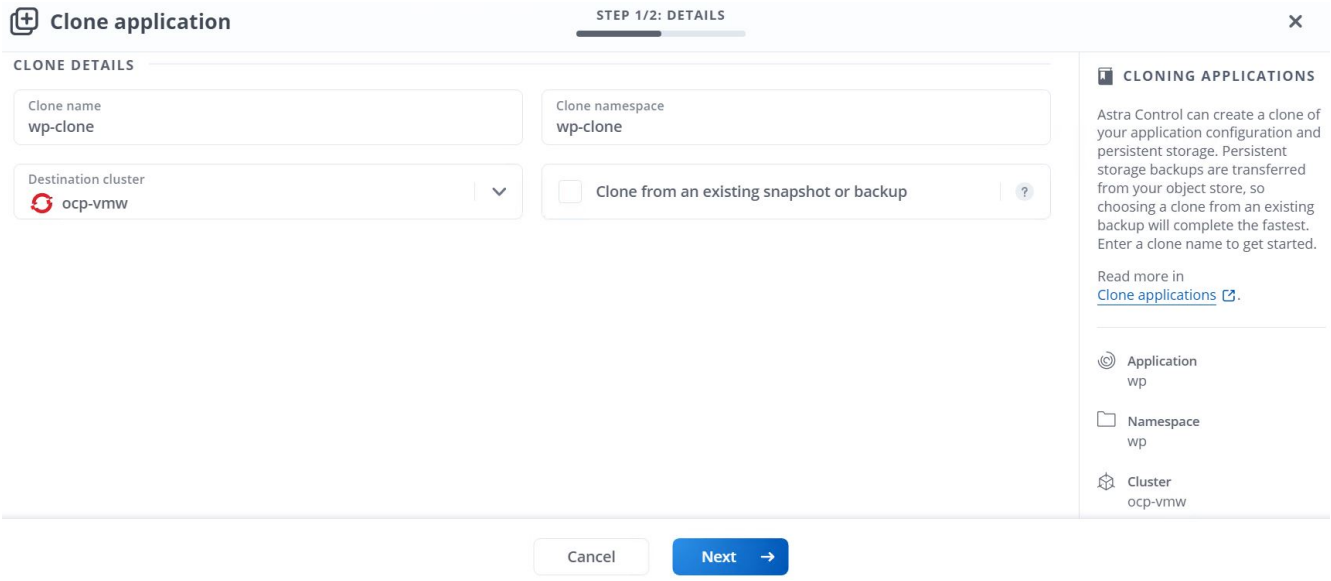
Klonen einer Applikation

Sie können eine Applikation zu Entwicklungs-/Testzwecken oder zur Sicherung von Applikationen und Disaster Recovery in einem entfernten Cluster klonen. Das Klonen einer Applikation im selben Cluster im selben Storage-Back-End nutzt die NetApp FlexClone Technologie, die VES sofort klont und Storage-Platz einspart.

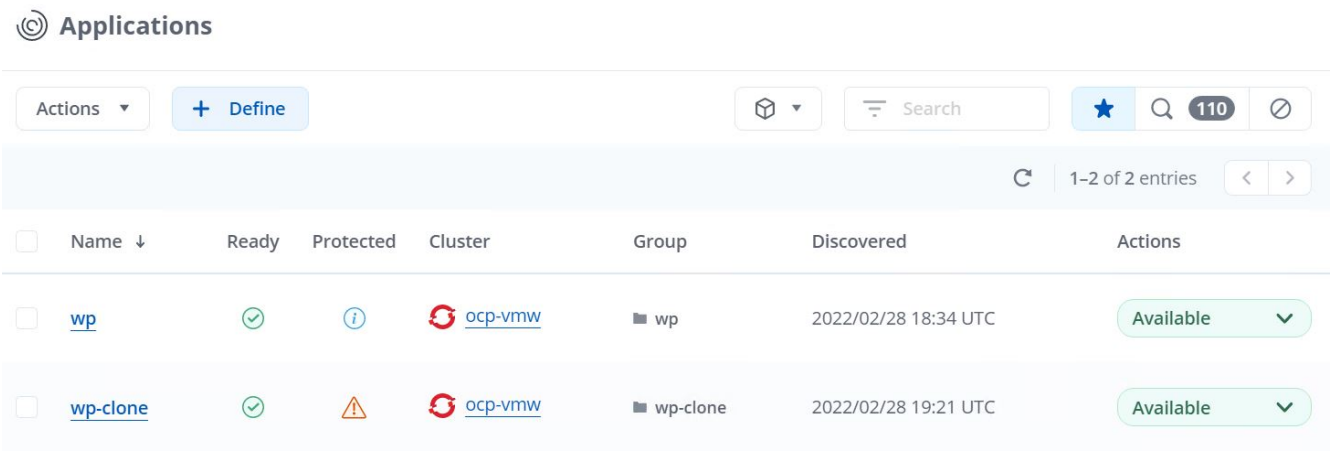
1. Um eine Anwendung zu klonen, navigieren Sie zur Registerkarte Apps > Managed und klicken Sie auf die betreffende Anwendung. Klicken Sie auf das Dropdown-Menü neben dem Anwendungsnamen und klicken Sie auf Klonen.



2. Geben Sie die Details zum neuen Namespace ein, wählen Sie den Cluster aus, in dem Sie ihn klonen möchten, und legen Sie fest, ob er aus einem vorhandenen Snapshot oder einem Backup oder dem aktuellen Status der Applikation geklont werden soll. Klicken Sie dann auf Weiter, und klicken Sie auf den Fensterbereich Klonen im Überprüfungsbereich, sobald Sie die Details geprüft haben.



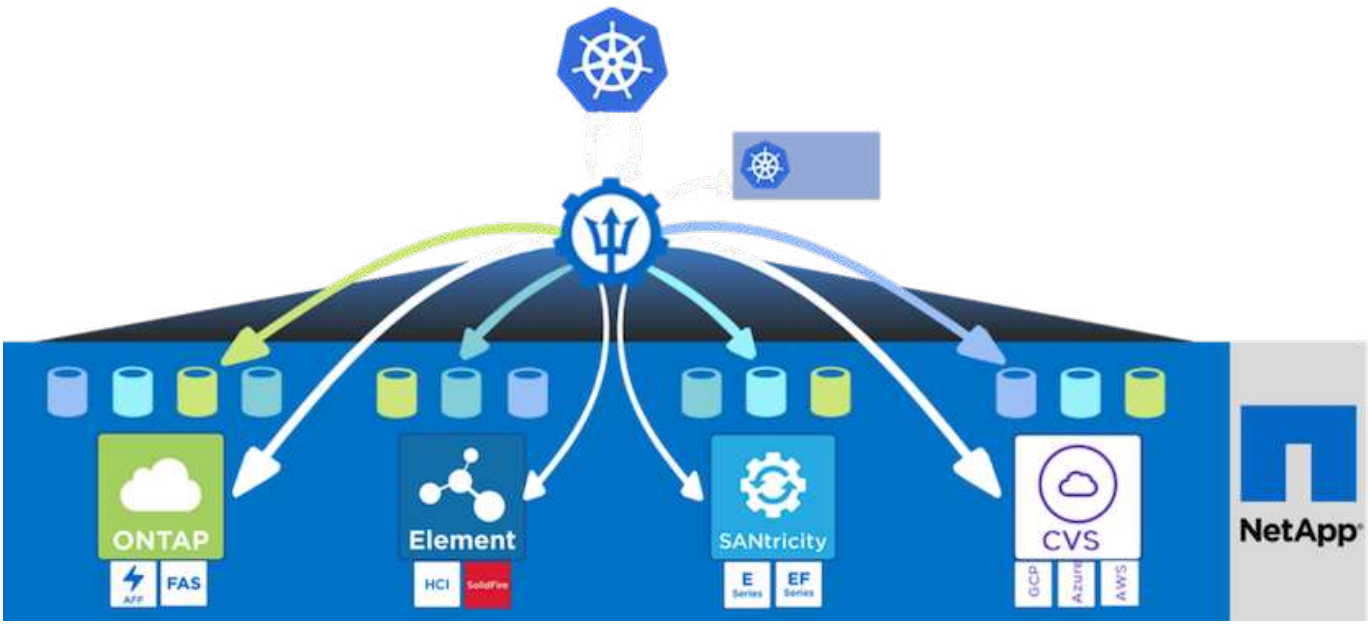
3. Die neue Applikation geht in den Entdeckungszustand, während Astra Control Center die Anwendung im ausgewählten Cluster erstellt. Nachdem alle Ressourcen der Anwendung installiert und von Astra erkannt wurden, geht die Anwendung in den verfügbaren Zustand.



Astra Trident – Überblick

Astra Trident ist ein Open-Source- und vollständig unterstützter Storage-Orchestrator für Container und Kubernetes-Distributionen, einschließlich Red hat OpenShift. Trident kann mit dem gesamten NetApp Storage-Portfolio eingesetzt werden, einschließlich NetApp ONTAP und Element Storage-Systeme. Es unterstützt auch NFS- und iSCSI-Verbindungen. Trident beschleunigt den DevOps-Workflow, da Endbenutzer Storage über ihre NetApp Storage-Systeme bereitstellen und managen können, ohne dass ein Storage-Administrator eingreifen muss.

Ein Administrator kann verschiedene Storage-Back-Ends basierend auf den Projektanforderungen und Storage-Systemmodellen konfigurieren, die erweiterte Storage-Funktionen wie Komprimierung, bestimmte Festplattentypen oder QoS-Level ermöglichen, die eine bestimmte Performance garantieren. Nach ihrer Definition können diese Back-Ends von Entwicklern in ihren Projekten verwendet werden, um persistente Volume Claims (PVCs) zu erstellen und persistenten Storage nach Bedarf an ihre Container anzubinden.



Astra Trident verfügt über einen schnellen Entwicklungszyklus, und genau wie Kubernetes bereits viermal im Jahr veröffentlicht.

Die neueste Version von Astra Trident ist die 22.01 Version von Januar 2022. Eine Support-Matrix, in der die Version von Trident getestet wurde, mit der Kubernetes Distribution zu finden ist "Hier".

Ab Version 20.04 wird die Trident-Einrichtung vom Trident Operator durchgeführt. Der Operator vereinfacht umfangreiche Implementierungen und bietet zusätzlichen Support einschließlich Selbstreparatur für Pods, die im Rahmen der Trident-Installation bereitgestellt werden.

In der Version 21.01 wurde ein Helm Chart zur Erleichterung der Installation des Trident Operators zur Verfügung gestellt.

Laden Sie Astra Trident Herunter

Um Trident auf dem implementierten Benutzer-Cluster zu installieren und ein persistentes Volume bereitzustellen, gehen Sie die folgenden Schritte durch:

1. Laden Sie das Installationsarchiv auf die Admin-Arbeitsstation herunter und extrahieren Sie den Inhalt. Die aktuelle Version von Trident ist 22.01, die heruntergeladen werden kann "Hier".

```
[netapp-user@rhel7 ~]$ wget
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
--2021-05-06 15:17:30--
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
[following]
--2021-05-06 15:17:30--  https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
```

```
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com (github-
releases.githubusercontent.com)... 185.199.108.154, 185.199.109.154,
185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-
releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38349341 (37M) [application/octet-stream]
Saving to: 'trident-installer-22.01.0.tar.gz'

100%[=================================================================
==============================================>] 38,349,341  88.5MB/s
in 0.4s

2021-05-06 15:17:30 (88.5 MB/s) - 'trident-installer-22.01.0.tar.gz'
saved [38349341/38349341]
```

2. Extrahieren Sie die Trident Installation aus dem heruntergeladenen Paket.

```
[netapp-user@rhel7 ~]$ tar -xzf trident-installer-22.01.0.tar.gz
[netapp-user@rhel7 ~]$ cd trident-installer/
[netapp-user@rhel7 trident-installer]$
```

Installieren Sie den Trident Operator mit Helm

1. Legen Sie zunächst den Speicherort des Benutzer-Clusters fest `kubeconfig` Datei als Umgebungsvariable, damit Sie nicht darauf verweisen müssen, weil Trident keine Option hat, diese Datei zu übergeben.

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/ocp-
install/auth/kubeconfig
```

2. Führen Sie den Helm-Befehl aus, um den Trident-Operator aus dem Tarball im Steuerverzeichnis zu installieren, während der Dreizack-Namespace in Ihrem Benutzer-Cluster erstellt wird.

```
[netapp-user@rhel7 trident-installer]$ helm install trident
helm/trident-operator-22.01.0.tgz --create-namespace --namespace trident
NAME: trident
LAST DEPLOYED: Fri May  7 12:54:25 2021
NAMESPACE: trident
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Thank you for installing trident-operator, which will deploy and manage
NetApp's Trident CSI
storage provisioner for Kubernetes.

Your release is named 'trident' and is installed into the 'trident'
namespace.
Please note that there must be only one instance of Trident (and
trident-operator) in a Kubernetes cluster.

To configure Trident to manage storage resources, you will need a copy
of tridentctl, which is
available in pre-packaged Trident releases.  You may find all Trident
releases and source code
online at https://github.com/NetApp/trident.

To learn more about the release, try:

  $ helm status trident
  $ helm get all trident
```

3. Sie können überprüfen, ob Trident erfolgreich installiert wurde, indem Sie die Pods prüfen, die im Namespace ausgeführt werden, oder die tridentctl-Binärdatei verwenden, um die installierte Version zu überprüfen.

```
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-csi-5z45l                   1/2     Running   2          30s
trident-csi-696b685cf8-htdb2        6/6     Running   0          30s
trident-csi-b74p2                   2/2     Running   0          30s
trident-csi-lrw4n                   2/2     Running   0          30s
trident-operator-7c748d957-gr2gw    1/1     Running   0          36s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+----------------+----------------+
| SERVER VERSION | CLIENT VERSION |
+----------------+----------------+
| 22.01.0          | 22.01.0          |
+----------------+----------------+
```

In einigen Fällen müssen die Kundenumgebungen möglicherweise die Anpassungen der Trident Implementierung erfordern. In diesen Fällen kann der Trident-Operator manuell installiert und die enthaltenen Manifeste aktualisiert werden, um die Implementierung anzupassen.

Trident Operator kann manuell installiert werden

1. Legen Sie zunächst den Speicherort des Benutzer-Clusters fest `kubeconfig` Datei als Umgebungsvariable, damit Sie nicht darauf verweisen müssen, weil Trident keine Option hat, diese Datei zu übergeben.

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/ocp-
install/auth/kubeconfig
```

2. Der `trident-installer` Das Verzeichnis enthält Manifeste für die Definition aller erforderlichen Ressourcen. Erstellen Sie mithilfe der entsprechenden Manifeste das `TridentOrchestrator` Benutzerdefinierte Ressourcendefinition.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml
customresourcedefinition.apiextensions.k8s.io/tridentorchestrators.tride
nt.netapp.io created
```

3. Wenn nicht vorhanden ist, erstellen Sie mithilfe des angegebenen Manifests einen Trident Namespace im Cluster.

```
[netapp-user@rhel7 trident-installer]$ oc apply -f deploy/namespace.yaml
namespace/trident created
```

4. Erstellen Sie die Ressourcen, die für die Trident-Operator, wie z. B. ein, erforderlich sind `ServiceAccount` Für den Operator A `ClusterRole` Und `ClusterRoleBinding` Bis zum `ServiceAccount`, Eine engagierte `PodSecurityPolicy`, Oder der Operator selbst.

```
[netapp-user@rhel7 trident-installer]$ oc create -f deploy/bundle.yaml
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

5. Sie können den Status des Bedieners überprüfen, nachdem er mit den folgenden Befehlen bereitgestellt wurde:

```
[netapp-user@rhel7 trident-installer]$ oc get deployment -n trident
NAME               READY   UP-TO-DATE   AVAILABLE   AGE
trident-operator   1/1     1            1           23s
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-operator-66f48895cc-lzczk   1/1     Running   0          41s
```

6. Mit dem implementierten Operator können wir nun Trident installieren. Dazu muss ein erstellt werden `TridentOrchestrator`.

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created
[netapp-user@rhel7 trident-installer]$ oc describe torc trident
Name:         trident
Namespace:
Labels:       <none>
Annotations:  <none>
API Version:  trident.netapp.io/v1
Kind:         TridentOrchestrator
Metadata:
  Creation Timestamp:  2021-05-07T17:00:28Z
  Generation:          1
  Managed Fields:
    API Version:  trident.netapp.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:spec:
        .:
        f:debug:
```

```
        f:namespace:
    Manager:      kubectl-create
    Operation:    Update
    Time:         2021-05-07T17:00:28Z
    API Version:  trident.netapp.io/v1
    Fields Type:  FieldsV1
    fieldsV1:
      f:status:
        .:
        f:currentInstallationParams:
          .:
          f:IPv6:
          f:autosupportHostname:
          f:autosupportImage:
          f:autosupportProxy:
          f:autosupportSerialNumber:
          f:debug:
          f:enableNodePrep:
          f:imagePullSecrets:
          f:imageRegistry:
          f:k8sTimeout:
          f:kubeletDir:
          f:logFormat:
          f:silenceAutosupport:
          f:tridentImage:
        f:message:
        f:namespace:
        f:status:
        f:version:
    Manager:         trident-operator
    Operation:       Update
    Time:            2021-05-07T17:00:28Z
  Resource Version:  931421
  Self Link:
/apis/trident.netapp.io/v1/tridentorchestrators/trident
  UID:               8a26a7a6-dde8-4d55-9b66-a7126754d81f
Spec:
  Debug:      true
  Namespace:  trident
Status:
  Current Installation Params:
    IPv6:                       false
    Autosupport Hostname:
    Autosupport Image:          netapp/trident-autosupport:21.01
    Autosupport Proxy:
    Autosupport Serial Number:
```

```
    Debug:                        true
    Enable Node Prep:             false
    Image Pull Secrets:
    Image Registry:
    k8sTimeout:           30
    Kubelet Dir:          /var/lib/kubelet
    Log Format:           text
    Silence Autosupport:  false
    Trident Image:        netapp/trident:22.01.0
  Message:                Trident installed
  Namespace:              trident
  Status:                 Installed
  Version:                v22.01.0
Events:
  Type    Reason      Age   From                        Message
  ----    ------      ----  ----                        -------
  Normal  Installing  80s   trident-operator.netapp.io  Installing
Trident
  Normal  Installed   68s   trident-operator.netapp.io  Trident
installed
```

7. Sie können überprüfen, ob Trident erfolgreich installiert wurde, indem Sie die Pods prüfen, die im Namespace ausgeführt werden, oder die tridentctl-Binärdatei verwenden, um die installierte Version zu überprüfen.

```
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-csi-bb64c6cb4-lmd6h         6/6     Running   0          82s
trident-csi-gn59q                   2/2     Running   0          82s
trident-csi-m4szj                   2/2     Running   0          82s
trident-csi-sb9k9                   2/2     Running   0          82s
trident-operator-66f48895cc-lzczk   1/1     Running   0          2m39s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+----------------+----------------+
| SERVER VERSION | CLIENT VERSION |
+----------------+----------------+
| 22.01.0          | 22.01.0          |
+----------------+----------------+
```

Worker-Nodes für Storage vorbereiten

NFS

Bei den meisten Kubernetes-Distributionen kommen Pakete und Utilities zur standardmäßig installierten NFS-Back-Ends einschließlich Red hat OpenShift zum Einsatz.

Bei NFSv3 gibt es jedoch keinen Mechanismus, um die Parallelität zwischen dem Client und dem Server auszuhandeln. Daher muss die maximale Anzahl der clientseitigen sunrpc-Slot-Tabelleneinträge manuell mit dem unterstützten Wert auf dem Server synchronisiert werden, um die beste Leistung für die NFS-Verbindung zu gewährleisten, ohne dass der Server die Fenstergröße der Verbindung verringern muss.

Bei ONTAP ist die unterstützte maximale Anzahl von sunrpc-Slot-Tabelleneinträgen 128, d.h. ONTAP kann 128 gleichzeitige NFS-Anfragen gleichzeitig verarbeiten. Standardmäßig hat Red hat CoreOS/Red hat Enterprise Linux jedoch maximal 65,536 Sunrpc Slot-Tabelleneinträge pro Verbindung. Dieser Wert muss auf 128 gesetzt werden. Dies kann mit Machine Config Operator (MCO) in OpenShift geschehen.

Gehen Sie wie folgt vor, um die maximalen Einträge in den OpenShift Worker Nodes zu ändern:

1. Melden Sie sich bei der OCP-Webkonsole an, und navigieren Sie zu „Compute“ > „Machine Configs“. Klicken Sie Auf Maschinenkonfiguration Erstellen. Kopieren Sie die YAML-Datei und fügen Sie sie ein, und klicken Sie auf Erstellen.

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 98-worker-nfs-rpc-slot-tables
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=utf-
8; base64,b3B0aW9ucyBzdW5ycGMgdGNwX21heF9zbG90X3RhYmxlX2VudHJpZXM9MTI4Cg=
=
          filesystem: root
          mode: 420
          path: /etc/modprobe.d/sunrpc.conf
```

2. Nach der Erstellung des MCO muss die Konfiguration auf alle Arbeitsknoten angewendet und nacheinander neu gestartet werden. Der gesamte Vorgang dauert etwa 20 bis 30 Minuten. Überprüfen Sie, ob die Maschinenkonfiguration mit angewendet wird `oc get mcp` Und stellen Sie sicher, dass der Konfigurationspool für die Maschinenkonfiguration für die Arbeitnehmer aktualisiert wird.

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME     CONFIG                                     UPDATED   UPDATING
DEGRADED
master   rendered-master-a520ae930e1d135e0dee7168   True      False
False
worker   rendered-worker-de321b36eeba62df41feb7bc   True      False
False
```

ISCSI

Um die Worker-Knoten vorzubereiten, die die Zuordnung von Block-Speicher-Volumes über das iSCSI-Protokoll ermöglichen, müssen Sie die erforderlichen Pakete installieren, um diese Funktionalität zu unterstützen.

In Red hat OpenShift wird dieser Vorgang durch Anwendung eines MCO (Machine Config Operator) auf das Cluster durchgeführt, nachdem es bereitgestellt wurde.

Führen Sie die folgenden Schritte aus, um die Worker-Knoten für die Ausführung von iSCSI-Diensten zu konfigurieren:

1. Melden Sie sich bei der OCP-Webkonsole an, und navigieren Sie zu „Compute“ > „Machine Configs“. Klicken Sie Auf Maschinenkonfiguration Erstellen. Kopieren Sie die YAML-Datei und fügen Sie sie ein, und klicken Sie auf Erstellen.

   Wenn Sie kein Multipathing verwenden:

   ```
   apiVersion: machineconfiguration.openshift.io/v1
   kind: MachineConfig
   metadata:
     labels:
       machineconfiguration.openshift.io/role: worker
     name: 99-worker-element-iscsi
   spec:
     config:
       ignition:
         version: 3.2.0
       systemd:
         units:
           - name: iscsid.service
             enabled: true
             state: started
     osImageURL: ""
   ```

   Bei Verwendung von Multipathing:

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 99-worker-ontap-iscsi
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
      - contents:
          source: data:text/plain;charset=utf-
8; base64,ZGVmYXVsdHMgewogICAgICAgIHVzZXJfZnJpZW5kbHlfbmFtZXMgbm8KICAgICA
gICBmaW5kX211bHRpcGF0aHMgbm8KfQoKYmxhY2tsaXN0X2V4Y2VwdGlvbnMgewogICAgICA
gIHByb3BlcnR5ICIoU0NTSV9JREVOVF98SURfV1dOKSIKfQoKYmxhY2tsaXN0IHsKfQoK
          verification: {}
        filesystem: root
        mode: 400
        path: /etc/multipath.conf
    systemd:
      units:
        - name: iscsid.service
          enabled: true
          state: started
        - name: multipathd.service
          enabled: true
          state: started
  osImageURL: ""
```

2. Nach der Erstellung der Konfiguration dauert es etwa 20 bis 30 Minuten, die Konfiguration auf die Worker-Nodes anzuwenden und erneut zu laden. Überprüfen Sie, ob die Maschinenkonfiguration mit angewendet wird `oc get mcp` Und stellen Sie sicher, dass der Konfigurationspool für die Maschinenkonfiguration für die Arbeitnehmer aktualisiert wird. Sie können sich auch bei den Worker-Nodes anmelden, um zu bestätigen, dass der iscsid-Service ausgeführt wird (und der Multipathd-Dienst wird ausgeführt, wenn Multipathing verwendet wird).

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME     CONFIG                                     UPDATED   UPDATING
DEGRADED
master   rendered-master-a520ae930e1d135e0dee7168   True      False
False
worker   rendered-worker-de321b36eeba62df41feb7bc   True      False
False

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status iscsid
● iscsid.service - Open-iSCSI
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; enabled;
vendor preset: disabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
     Docs: man:iscsid(8)
           man:iscsiadm(8)
 Main PID: 1242 (iscsid)
   Status: "Ready to process requests"
    Tasks: 1
   Memory: 4.9M
      CPU: 9ms
   CGroup: /system.slice/iscsid.service
           └─1242 /usr/sbin/iscsid -f

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status multipathd
 ● multipathd.service - Device-Mapper Multipath Device Controller
   Loaded: loaded (/usr/lib/systemd/system/multipathd.service; enabled;
vendor preset: enabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
  Main PID: 918 (multipathd)
    Status: "up"
    Tasks: 7
    Memory: 13.7M
    CPU: 57ms
    CGroup: /system.slice/multipathd.service
            └─918 /sbin/multipathd -d -s
```

Es ist auch möglich zu bestätigen, dass die MachineConfig erfolgreich angewendet wurde und die Dienste wie erwartet durch Ausführen der gestartet wurden `oc debug` Befehl mit den entsprechenden Flags.

Erstellen von Storage-System-Back-Ends

Nach Abschluss der Installation des Astra Trident Operator müssen Sie das Backend für die spezifische

NetApp Storage-Plattform konfigurieren, die Sie verwenden. Folgen Sie den Links unten, um mit der Einrichtung und Konfiguration von Astra Trident fortzufahren.

- "NetApp ONTAP NFS"
- "NetApp ONTAP iSCSI"
- "NetApp Element iSCSI"

Konfiguration von NetApp ONTAP NFS

Um die Trident Integration mit dem NetApp ONTAP Storage-System zu aktivieren, müssen Sie ein Back-End erstellen, das die Kommunikation mit dem Storage-System ermöglicht.

1. Im heruntergeladenen Installationsarchiv stehen Beispiele für Backend-Dateien zur Verfügung `sample-input` Ordnerhierarchie. Kopieren Sie für NetApp ONTAP-Systeme, die NFS bereitstellen, den `backend-ontap-nas.json` Datei in Ihr Arbeitsverzeichnis und bearbeiten Sie die Datei.

   ```
   [netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
   samples/ontap-nas/backend-ontap-nas.json ./
   [netapp-user@rhel7 trident-installer]$ vi backend-ontap-nas.json
   ```

2. BackendName, Management LIF, Daten LIF, svm, Benutzername, bearbeiten Und Kennwortwerte in dieser Datei.

   ```
   {
       "version": 1,
       "storageDriverName": "ontap-nas",
       "backendName": "ontap-nas+10.61.181.221",
       "managementLIF": "172.21.224.201",
       "dataLIF": "10.61.181.221",
       "svm": "trident_svm",
       "username": "cluster-admin",
       "password": "password"
   }
   ```

   > Als Best Practice empfiehlt es sich, den benutzerdefinierten BackendName-Wert als Kombination aus storageDriverName und der DatenLIF zu definieren, die NFS bedienen, um die einfache Identifizierung zu erleichtern.

3. Führen Sie mit dieser Backend-Datei den folgenden Befehl aus, um Ihr erstes Backend zu erstellen.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-nas.json
+------------------------+----------------
+--------------------------------------+--------+---------+
|          NAME          | STORAGE DRIVER |                 UUID
| STATE  | VOLUMES |
+------------------------+----------------
+--------------------------------------+--------+---------+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-
5c87a73c5b1e | online |       0 |
+------------------------+----------------
+--------------------------------------+--------+---------+
```

4. Wenn das Back-End erstellt wird, müssen Sie als nächstes eine Storage-Klasse erstellen. Wie beim Backend gibt es auch eine Beispiel-Speicherklassendatei, die für die im Ordner Sample-Inputs verfügbare Umgebung bearbeitet werden kann. Kopieren Sie ihn in das Arbeitsverzeichnis und nehmen Sie die erforderlichen Änderungen an dem erstellten Backend vor.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist das zu definieren `backendType` Wert für den Namen des Speichertreibers aus dem neu erstellten Back-End. Notieren Sie auch den Wert des Namensfelds, auf den in einem späteren Schritt verwiesen werden muss.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```

> Es gibt ein optionales Feld mit dem Namen `fsType` Das ist in dieser Datei definiert. Diese Zeile kann in NFS-Back-Ends gelöscht werden.

6. Führen Sie die aus `oc` Befehl zum Erstellen der Storage-Klasse.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. Nach Erstellung der Storage-Klasse müssen Sie dann die erste Forderung für ein persistentes Volume (PVC) erstellen. Es gibt ein Beispiel `pvc-basic.yaml` Datei, mit der diese Aktion ausgeführt werden kann, die sich auch in Sample-Inputs befindet.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-
basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

8. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist sicherzustellen, dass die `storageClassName` Feld entspricht dem gerade erstellten. Die PVC-Definition kann je nach Bedarf des bereitzustellenden Workloads weiter angepasst werden.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

9. Erstellen Sie das PVC, indem Sie die ausstellen `oc` Befehl. Die Erstellung kann je nach Größe des erstellten Sicherungsvolumens einige Zeit in Anspruch nehmen, sodass Sie den Prozess nach Abschluss beobachten können.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME    STATUS   VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic   Bound    pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d   1Gi
RWO            basic-csi      7s
```

NetApp ONTAP iSCSI-Konfiguration

Um die Trident Integration mit dem NetApp ONTAP Storage-System zu aktivieren, müssen Sie ein Back-End erstellen, das die Kommunikation mit dem Storage-System ermöglicht.

1. Im heruntergeladenen Installationsarchiv stehen Beispiele für Backend-Dateien zur Verfügung `sample-input` Ordnerhierarchie. Kopieren Sie bei NetApp ONTAP-Systemen, die iSCSI bereitstellen, das `backend-ontap-san.json` Datei in Ihr Arbeitsverzeichnis und bearbeiten Sie die Datei.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/ontap-san/backend-ontap-san.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-san.json
```

2. Bearbeiten Sie die Werte ManagementLIF, dataLIF, svm, Benutzername und Passwort in dieser Datei.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.240",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```

3. Führen Sie mit dieser Backend-Datei den folgenden Befehl aus, um Ihr erstes Backend zu erstellen.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+------------------------+----------------
+--------------------------------------+--------+---------+
|          NAME          | STORAGE DRIVER |                  UUID
| STATE  | VOLUMES |
+------------------------+----------------
+--------------------------------------+--------+---------+
| ontapsan_10.61.181.241 | ontap-san      | 6788533c-7fea-4a35-b797-
fb9bb3322b91 | online |       0 |
+------------------------+----------------
+--------------------------------------+--------+---------+
```

4. Wenn das Back-End erstellt wird, müssen Sie als nächstes eine Storage-Klasse erstellen. Wie beim Backend gibt es auch eine Beispiel-Speicherklassendatei, die für die im Ordner Sample-Inputs verfügbare Umgebung bearbeitet werden kann. Kopieren Sie ihn in das Arbeitsverzeichnis und nehmen Sie die erforderlichen Änderungen an dem erstellten Backend vor.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist das zu definieren `backendType` Wert für den Namen des Speichertreibers aus dem neu erstellten Back-End. Notieren Sie auch den Wert des Namensfelds, auf den in einem späteren Schritt verwiesen werden muss.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```

> Es gibt ein optionales Feld mit dem Namen `fsType` Das ist in dieser Datei definiert. In iSCSI-Back-Ends kann dieser Wert auf einen bestimmten Linux-Dateisystem-Typ (XFS, ext4 usw.) gesetzt oder gelöscht werden, damit OpenShift entscheiden kann, welches Dateisystem verwendet werden soll.

6. Führen Sie die aus `oc` Befehl zum Erstellen der Storage-Klasse.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. Nach Erstellung der Storage-Klasse müssen Sie dann die erste Forderung für ein persistentes Volume (PVC) erstellen. Es gibt ein Beispiel `pvc-basic.yaml` Datei, mit der diese Aktion ausgeführt werden kann, die sich auch in Sample-Inputs befindet.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-
basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

8. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist sicherzustellen, dass die `storageClassName` Feld entspricht dem gerade erstellten. Die PVC-Definition kann je nach Bedarf des bereitzustellenden Workloads weiter angepasst werden.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

9. Erstellen Sie das PVC, indem Sie die ausstellen `oc` Befehl. Die Erstellung kann je nach Größe des erstellten Sicherungsvolumens einige Zeit in Anspruch nehmen, sodass Sie den Prozess nach Abschluss beobachten können.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME    STATUS   VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic   Bound    pvc-7ceac1ba-0189-43c7-8f98-094719f7956c   1Gi
RWO            basic-csi      3s
```

ISCSI-Konfiguration von NetApp Element

Um die Trident Integration mit dem NetApp Element Storage-System zu aktivieren, müssen Sie ein Backend erstellen, das die Kommunikation mit dem Storage-System über das iSCSI-Protokoll ermöglicht.

1. Im heruntergeladenen Installationsarchiv stehen Beispiele für Backend-Dateien zur Verfügung `sample-input` Ordnerhierarchie. Kopieren Sie für NetApp Element-Systeme, die iSCSI-Server bereitstellen, das `backend-solidfire.json` Datei in Ihr Arbeitsverzeichnis und bearbeiten Sie die Datei.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/solidfire/backend-solidfire.json ./
[netapp-user@rhel7 trident-installer]$ vi ./backend-solidfire.json
```

   a. Bearbeiten Sie den Benutzer-, das Kennwort und den MVIP-Wert auf dem `EndPoint` Linie.

   b. Bearbeiten Sie das `SVIP` Wert:

```
 {
    "version": 1,
    "storageDriverName": "solidfire-san",
    "Endpoint": "https://trident:password@172.21.224.150/json-
rpc/8.0",
    "SVIP": "10.61.180.200:3260",
    "TenantName": "trident",
    "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS":
2000, "burstIOPS": 4000}},
              {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS":
6000, "burstIOPS": 8000}},
              {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS":
8000, "burstIOPS": 10000}}]
}
```

2. Führen Sie mit dieser Back-End-Datei den folgenden Befehl aus, um Ihr erstes Backend zu erstellen.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-solidfire.json
+------------------------+----------------
+--------------------------------------+--------+---------+
|          NAME          | STORAGE DRIVER |                  UUID
| STATE  | VOLUMES |
+------------------------+----------------
+--------------------------------------+--------+---------+
| solidfire_10.61.180.200 | solidfire-san  | b90783ee-e0c9-49af-8d26-
3ea87ce2efdf | online |       0 |
+------------------------+----------------
+--------------------------------------+--------+---------+
```

3. Wenn das Back-End erstellt wird, müssen Sie als nächstes eine Storage-Klasse erstellen. Wie beim Backend gibt es auch eine Beispiel-Speicherklassendatei, die für die im Ordner Sample-Inputs verfügbare Umgebung bearbeitet werden kann. Kopieren Sie ihn in das Arbeitsverzeichnis und nehmen Sie die erforderlichen Änderungen an dem erstellten Backend vor.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

4. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist das zu definieren `backendType` Wert für den Namen des Speichertreibers aus dem neu erstellten Back-End. Notieren Sie auch den Wert des Namensfelds, auf den in einem späteren Schritt verwiesen werden muss.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "solidfire-san"
```

> Es gibt ein optionales Feld mit dem Namen `fsType` Das ist in dieser Datei definiert. In iSCSI-Back-Ends kann dieser Wert auf einen bestimmten Linux-Dateisystem-Typ (XFS, ext4 usw.) gesetzt werden. OpenShift kann auch gelöscht werden, damit OpenShift entscheiden kann, welches Dateisystem verwendet werden soll.

5. Führen Sie die aus `oc` Befehl zum Erstellen der Storage-Klasse.

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

6. Nach Erstellung der Storage-Klasse müssen Sie dann die erste Forderung für ein persistentes Volume (PVC) erstellen. Es gibt ein Beispiel `pvc-basic.yaml` Datei, mit der diese Aktion ausgeführt werden kann, die sich auch in Sample-Inputs befindet.

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-
basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

7. Die einzige Bearbeitung, die zu dieser Datei gemacht werden muss, ist sicherzustellen, dass die `storageClassName` Feld entspricht dem gerade erstellten. Die PVC-Definition kann je nach Bedarf des bereitzustellenden Workloads weiter angepasst werden.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

8. Erstellen Sie das PVC, indem Sie die ausstellen `oc` Befehl. Die Erstellung kann je nach Größe des erstellten Sicherungsvolumens einige Zeit in Anspruch nehmen, sodass Sie den Prozess nach Abschluss beobachten können.

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME    STATUS   VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic   Bound    pvc-3445b5cc-df24-453d-a1e6-b484e874349d   1Gi
RWO            basic-csi      5s
```

Erweiterte Konfigurationsoptionen

Load Balancer-Optionen: Red hat OpenShift mit NetApp

In den meisten Fällen stellt Red hat OpenShift Anwendungen für die Außenwelt über Routen zur Verfügung. Ein Service wird durch die Angabe eines extern zugänglichen Host-Namens zugänglich gemacht. Die definierte Route und die vom Dienst identifizierten Endpunkte können von einem OpenShift-Router genutzt werden, um diese benannte Verbindung externen Clients bereitzustellen.

In einigen Fällen müssen jedoch Applikationen zum Einsatz kommen und eine Konfiguration von angepassten Lastausgleich erforderlich sein, um die entsprechenden Services bereitzustellen. Ein Beispiel hierfür ist das NetApp Astra Control Center. Um diesem Bedarf gerecht zu werden, haben wir eine Reihe von benutzerdefinierten Load Balancer-Optionen evaluiert. Die Installation und Konfiguration der Lösung wird in diesem Abschnitt beschrieben.

Auf den folgenden Seiten sind zusätzliche Informationen zu den in Red hat OpenShift mit NetApp validierten Load Balancer-Optionen verfügbar:

- "MetalLB"
- "F5 BIG-IP"

Installation von MetalLB Load Balancer: Red hat OpenShift mit NetApp

Auf dieser Seite werden die Installations- und Konfigurationsanweisungen für den MetalLB Load Balancer aufgeführt.

MetalLB ist ein selbst gehosteter Network Load Balancer, der auf Ihrem OpenShift-Cluster installiert ist und das die Erstellung von OpenShift-Diensten vom Typ Load Balancer in Clustern ermöglicht, die nicht auf einem Cloud-Provider ausgeführt werden. Die zwei Hauptmerkmale der MetalLB, die zur Unterstützung der Load Balancer-Dienste zusammenarbeiten, sind Adresszuweisung und externe Ankündigung.

MetalLB-Konfigurationsoptionen

Basierend darauf, wie MetalLB die IP-Adresse ankündigt, die den Load Balancer-Diensten außerhalb des OpenShift-Clusters zugewiesen ist, arbeitet es in zwei Modi:

- **Layer 2-Modus.** in diesem Modus übernimmt ein Knoten im OpenShift-Cluster die Verantwortung für den Service und antwortet auf ARP-Anfragen, damit er außerhalb des OpenShift-Clusters erreichbar ist. Da nur der Node die IP bereitstellt, kommt es zu einem Bandbreitenengpass und zu langsamen Failover-Einschränkungen. Weitere Informationen finden Sie in der Dokumentation "Hier".
- **BGP-Modus.** in diesem Modus etablieren alle Knoten im OpenShift-Cluster BGP-Peering-Sitzungen mit einem Router und werben die Routen an die Service-IPs weiter. Voraussetzung dafür ist die Integration von MetalLB in einen Router in dieses Netzwerk. Aufgrund des Hashing-Mechanismus in BGP hat es bestimmte Einschränkungen, wenn IP-zu-Node-Zuordnung für einen Service geändert wird. Weitere Informationen finden Sie in der Dokumentation "Hier".

Im Rahmen dieses Dokuments konfigurieren wir MetalLB im Layer-2-Modus.

Installieren des MetalLB Load Balancer

1. Laden Sie die MetalLB-Ressourcen herunter.

```
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/name
space.yaml
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/meta
llb.yaml
```

2. Datei bearbeiten `metallb.yaml` Und entfernen `spec.template.spec.securityContext` Von der Controller-Bereitstellung und dem Lautsprecher DemonSet.

   Zu löschende Zeilen:

```
securityContext:
  runAsNonRoot: true
  runAsUser: 65534
```

3. Erstellen Sie die `metallb-system` Namespace.

```
[netapp-user@rhel7 ~]$ oc create -f namespace.yaml
namespace/metallb-system created
```

4. Erstellen Sie den MetalLB CR.

```
[netapp-user@rhel7 ~]$ oc create -f metallb.yaml
podsecuritypolicy.policy/controller created
podsecuritypolicy.policy/speaker created
serviceaccount/controller created
serviceaccount/speaker created
clusterrole.rbac.authorization.k8s.io/metallb-system:controller created
clusterrole.rbac.authorization.k8s.io/metallb-system:speaker created
role.rbac.authorization.k8s.io/config-watcher created
role.rbac.authorization.k8s.io/pod-lister created
role.rbac.authorization.k8s.io/controller created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:controller
created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:speaker
created
rolebinding.rbac.authorization.k8s.io/config-watcher created
rolebinding.rbac.authorization.k8s.io/pod-lister created
rolebinding.rbac.authorization.k8s.io/controller created
daemonset.apps/speaker created
deployment.apps/controller created
```

5. Bevor Sie den MetalLB-Lautsprecher konfigurieren, gewähren Sie dem Lautsprecher DemonSet erhöhte Berechtigungen, damit er die für den Lastausgleich erforderliche Netzwerkkonfiguration ausführen kann.

```
[netapp-user@rhel7 ~]$ oc adm policy add-scc-to-user privileged -n
metallb-system -z speaker
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:privileged
added: "speaker"
```

6. Konfigurieren Sie MetalLB, indem Sie eine erstellen `ConfigMap` Im `metallb-system` Namespace.

```
[netapp-user@rhel7 ~]$ vim metallb-config.yaml

apiVersion: v1
kind: ConfigMap
metadata:
  namespace: metallb-system
  name: config
data:
  config: |
    address-pools:
    - name: default
      protocol: layer2
      addresses:
      - 10.63.17.10-10.63.17.200

[netapp-user@rhel7 ~]$ oc create -f metallb-config.yaml
configmap/config created
```

7. Wenn nun Load Balancer Dienste erstellt werden, weist MetalLB den Diensten eine externe IP zu und gibt die IP-Adresse durch Antwort auf ARP-Anfragen an.

> Wenn Sie MetalLB im BGP-Modus konfigurieren möchten, überspringen Sie Schritt 6 oben und befolgen Sie das Verfahren in der MetalLB-Dokumentation "Hier".

Installation von F5 BIG-IP Load Balancer

F5 BIG-IP ist ein Application Delivery Controller (ADC), der ein breites Spektrum erweiterter Traffic Management und Sicherheitsservices wie L4-L7 Load Balancing, SSL/TLS-Entlastung, DNS, Firewall und vieles mehr in Produktionsqualität bietet. Diese Services sorgen für eine signifikante Steigerung der Verfügbarkeit, Sicherheit und Performance der Applikationen.

F5 BIG-IP kann auf verschiedene Arten implementiert und genutzt werden: Auf dedizierter Hardware, in der Cloud oder als virtuelle Appliance vor Ort. In der Dokumentation finden Sie Informationen zur Nutzung und Implementierung von F5 BIG-IP nach Bedarf.

Für eine effiziente Integration von F5 BIG-IP-Diensten in Red hat OpenShift bietet F5 den BIG-IP Container Ingress Service (CIS) an. CIS wird als Controller-Pod installiert, der die OpenShift API für bestimmte Custom

Resource Definitions (CRDs) überwacht und die F5 BIG-IP-Systemkonfiguration verwaltet. F5 BIG-IP CIS kann für die Steuerung von Servicetypen für Loadbalancer und Routen in OpenShift konfiguriert werden.

Für die automatische IP-Adresszuweisung zur Wartung des Typs loadbalancer können Sie außerdem den F5 IPAM-Controller nutzen. Der F5 IPAM-Controller wird als Controller-Pod installiert, der OpenShift API für Load Balancer-Dienste mit einer ipamLabel-Anmerkung überwacht, um die IP-Adresse aus einem vorkonfigurierten Pool zuzuweisen.

Auf dieser Seite sind die Installations- und Konfigurationsanweisungen für die F5 BIG-IP CIS- und IPAM-Controller aufgeführt. Voraussetzung ist, dass ein F5 BIG-IP-System implementiert und lizenziert werden muss. Es muss auch für SDN-Dienste lizenziert sein, die standardmäßig in DER BIG-IP VE-Basislizenz enthalten sind.

F5 BIG-IP kann im Standalone- oder Cluster-Modus implementiert werden. Im Rahmen dieser Validierung wurde F5 BIG-IP im Standalone-Modus implementiert, jedoch wird es für Produktionszwecke bevorzugt, ein Cluster VON BIG-IPs zu verwenden, um Single Point of Failure zu vermeiden.

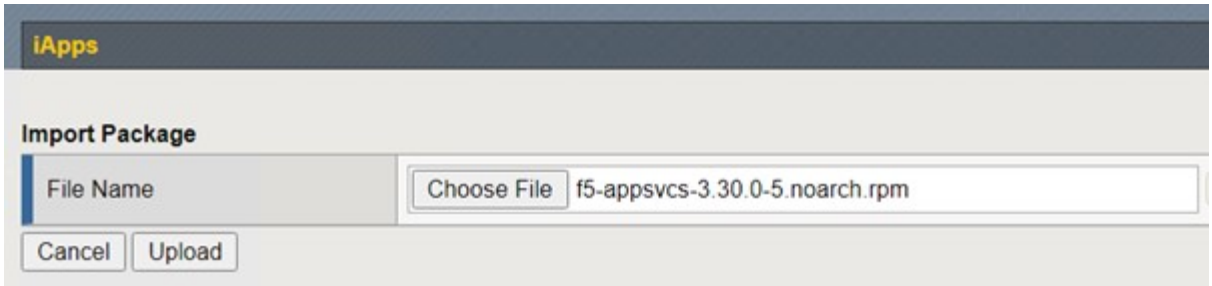
Ein F5 BIG-IP System kann auf dedizierter Hardware, in der Cloud oder als virtuelle Appliance on-Premises mit Versionen über 12.x bereitgestellt werden, damit es mit F5 CIS integriert werden kann. Für dieses Dokument wurde das F5 BIG-IP System als virtuelle Appliance validiert, beispielsweise mit DER BIG-IP VE Edition.

Validierte Versionen

Technologie	Softwareversion
Red hat OpenShift	4.6 EUS, 4.7
F5 BIG-IP VE EDITION	16.1.0
F5 Container Ingress Service	2.5.1
F5 IPAM Controller	0.1.4
F5 AS3	3.30.0

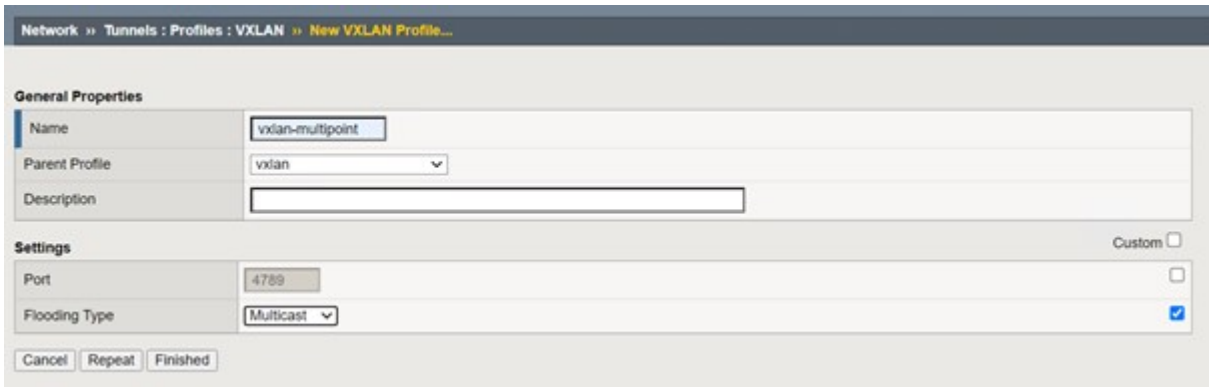
Installation

1. Installieren Sie die Erweiterung F5 Application Services 3, damit BIG-IP-Systeme Konfigurationen in JSON anstelle von Imperativ-Befehlen akzeptieren können. Gehen Sie zu "F5 AS3 GitHub-Repository", Und laden Sie die neueste RPM-Datei.
2. Melden Sie sich bei F5 BIG-IP-System an, navigieren Sie zu iApps > Package Management LX, und klicken Sie auf Importieren.
3. Klicken Sie auf Datei auswählen und wählen Sie die heruntergeladene AS3 RPM-Datei aus, klicken Sie auf OK und anschließend auf Hochladen.

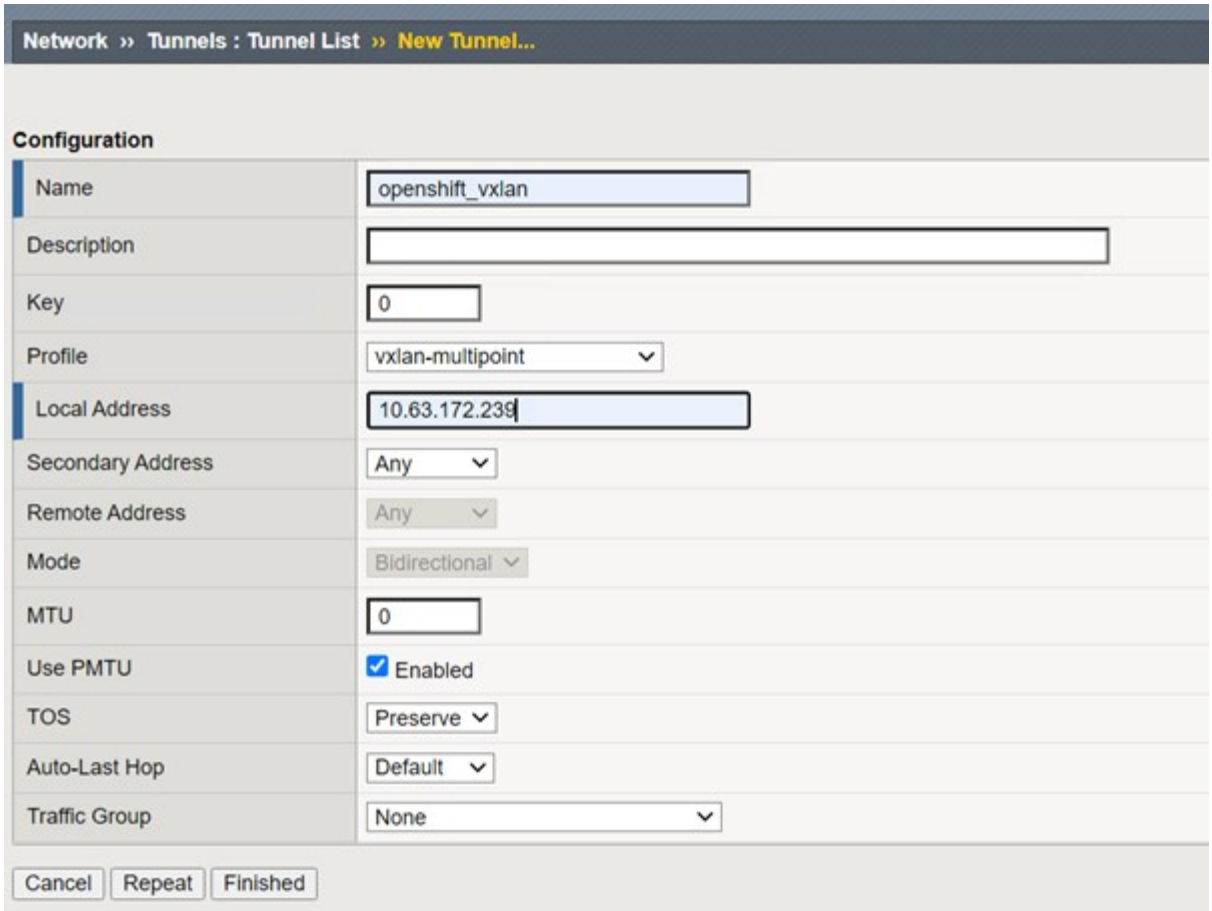


4. Vergewissern Sie sich, dass die AS3-Erweiterung erfolgreich installiert wurde.

5. Konfigurieren Sie dann die Ressourcen, die für die Kommunikation zwischen OpenShift- und BIG-IP-Systemen benötigt werden. Erstellen Sie zunächst einen Tunnel zwischen OpenShift und DEM BIG-IP-Server, indem Sie eine VXLAN-Tunnelschnittstelle auf dem BIG-IP-System für OpenShift SDN erstellen. Navigieren Sie zu Netzwerk > Tunnel > Profile, klicken Sie auf Erstellen, und legen Sie das übergeordnete Profil auf vxlan und den Hochwassertyp auf Multicast fest. Geben Sie einen Namen für das Profil ein und klicken Sie auf Fertig.



6. Navigieren Sie zu Netzwerk > Tunnel > Tunnelliste, klicken Sie auf Erstellen, und geben Sie den Namen und die lokale IP-Adresse für den Tunnel ein. Wählen Sie das Tunnelprofil aus, das im vorherigen Schritt erstellt wurde, und klicken Sie auf Fertig.



7. Melden Sie sich beim Red hat OpenShift-Cluster mit Clusteradministratorrechten an.
8. Erstellen Sie auf OpenShift ein Hostsubnetz für den F5 BIG-IP-Server, der das Subnetz vom OpenShift-Cluster auf den F5 BIG-IP-Server erweitert. Laden Sie die YAML-Hostsubnet-Definition herunter.

```
wget https://github.com/F5Networks/k8s-bigip-
ctlr/blob/master/docs/config_examples/openshift/f5-kctlr-openshift-
hostsubnet.yaml
```

9. Bearbeiten Sie die Hostsubnet-Datei und fügen Sie die BIG-IP-VTEP-IP (VXLAN-Tunnel)-IP für das SDN OpenShift hinzu.

```
apiVersion: v1
kind: HostSubnet
metadata:
  name: f5-server
  annotations:
    pod.network.openshift.io/fixed-vnid-host: "0"
    pod.network.openshift.io/assign-subnet: "true"
# provide a name for the node that will serve as BIG-IP's entry into the
cluster
host: f5-server
# The hostIP address will be the BIG-IP interface address routable to
the
# OpenShift Origin nodes.
# This address is the BIG-IP VTEP in the SDN's VXLAN.
hostIP: 10.63.172.239
```

Ändern Sie HostIP und andere Details, je nach Ihrer Umgebung.

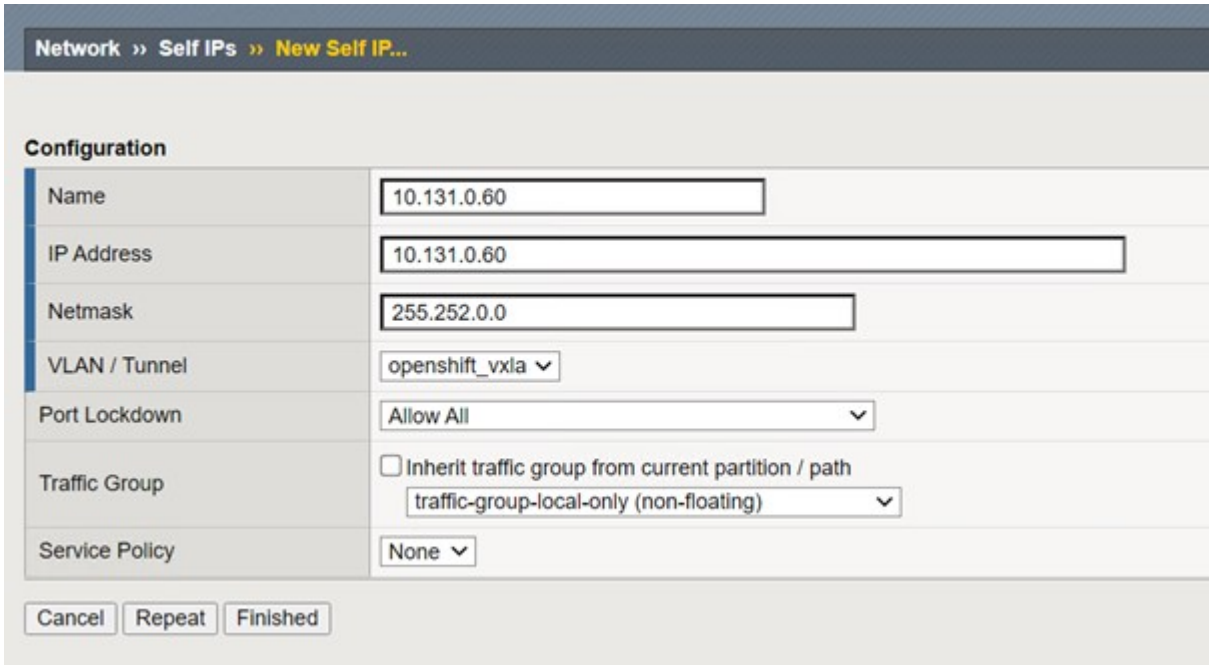
10. Hostsubnet-Ressource erstellen.

```
[admin@rhel-7 ~]$ oc create -f f5-kctlr-openshift-hostsubnet.yaml

hostsubnet.network.openshift.io/f5-server created
```

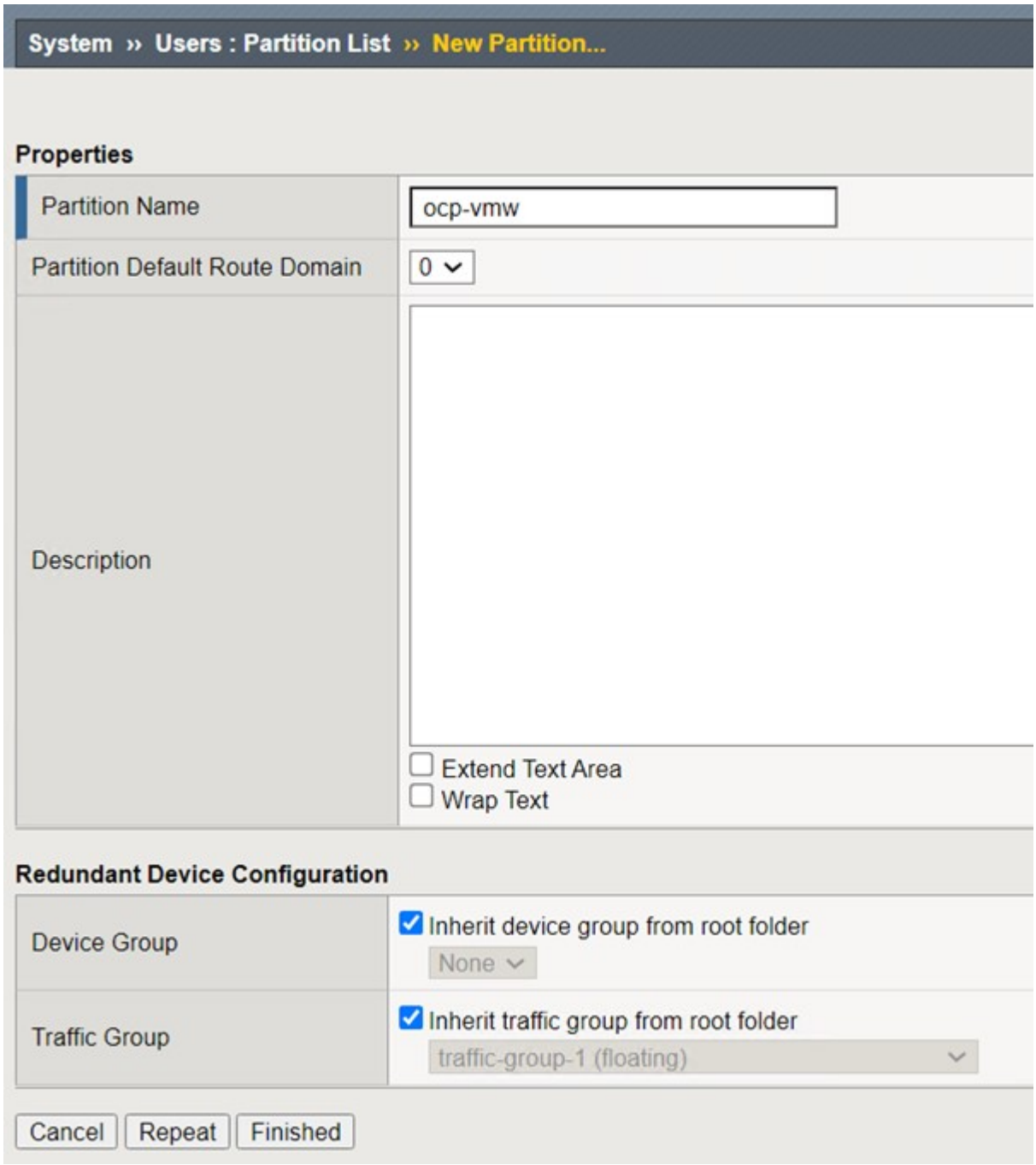
11. Abrufen des Cluster-IP-Subnetzes für das für den F5 BIG-IP-Server erstellte Host-Subnetz.

```
[admin@rhel-7 ~]$ oc get hostsubnet

NAME                          HOST                          HOST IP
SUBNET          EGRESS CIDRS   EGRESS IPS
f5-server                     f5-server                     10.63.172.239
10.131.0.0/23
ocp-vmw-nszws-master-0        ocp-vmw-nszws-master-0        10.63.172.44
10.128.0.0/23
ocp-vmw-nszws-master-1        ocp-vmw-nszws-master-1        10.63.172.47
10.130.0.0/23
ocp-vmw-nszws-master-2        ocp-vmw-nszws-master-2        10.63.172.48
10.129.0.0/23
ocp-vmw-nszws-worker-r8fh4    ocp-vmw-nszws-worker-r8fh4    10.63.172.7
10.130.2.0/23
ocp-vmw-nszws-worker-tvr46    ocp-vmw-nszws-worker-tvr46    10.63.172.11
10.129.2.0/23
ocp-vmw-nszws-worker-wdxhg    ocp-vmw-nszws-worker-wdxhg    10.63.172.24
10.128.2.0/23
ocp-vmw-nszws-worker-wg8r4    ocp-vmw-nszws-worker-wg8r4    10.63.172.15
10.131.2.0/23
ocp-vmw-nszws-worker-wtgfw    ocp-vmw-nszws-worker-wtgfw    10.63.172.17
10.128.4.0/23
```

12. Erstellen Sie auf OpenShift VXLAN mit einer IP im Host-Subnetz-Bereich von OpenShift eine eigene IP-Adresse, die dem F5 BIG-IP-Server entspricht. Melden Sie sich beim F5 BIG-IP-System an, navigieren Sie zu Netzwerk > selbst-IPs, und klicken Sie auf Erstellen. Geben Sie eine IP aus dem Cluster-IP-Subnetz ein, das für das F5 BIG-IP Host-Subnetz erstellt wurde, wählen Sie den VXLAN-Tunnel aus, und geben Sie die anderen Details ein. Klicken Sie anschließend auf Fertig.



13. Erstellen Sie eine Partition im F5 BIG-IP-System, die mit CIS konfiguriert und verwendet werden soll. Navigieren Sie zu System > Users > Partitionsliste, klicken Sie auf Create, und geben Sie die Details ein. Klicken Sie anschließend auf Fertig.



> F5 empfiehlt, auf der von CIS verwalteten Partition keine manuelle Konfiguration durchzuführen.

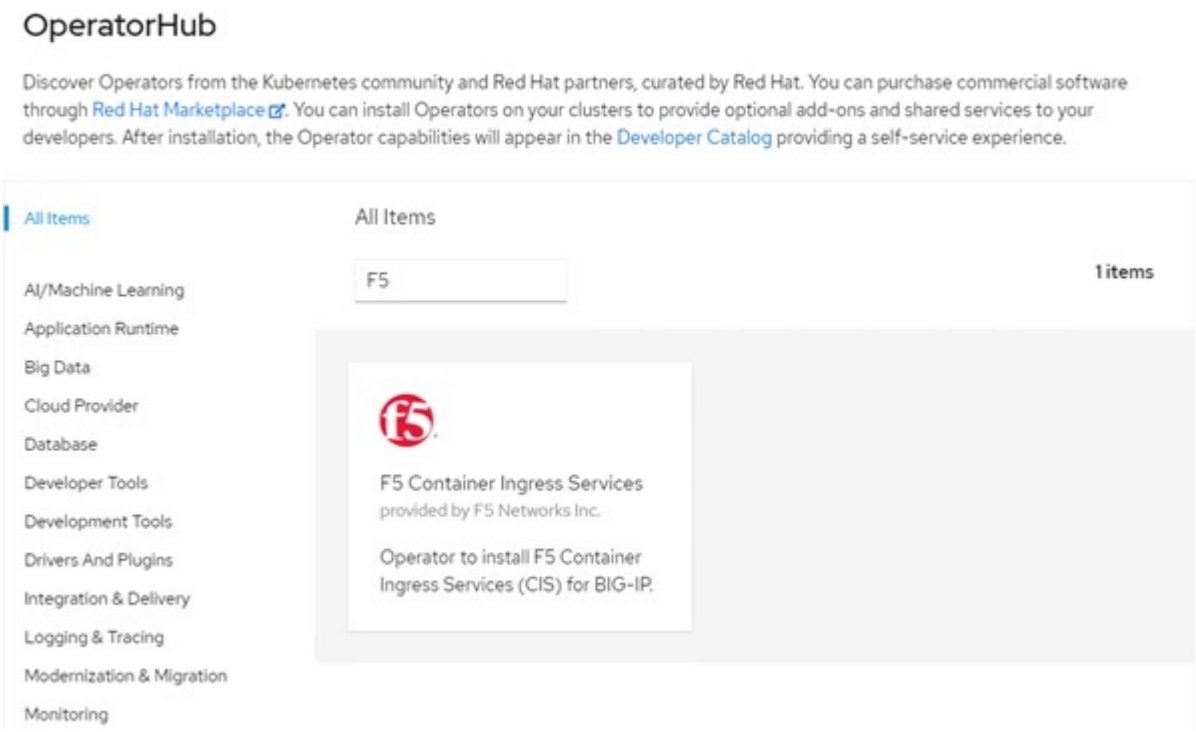
14. Installieren Sie die F5 BIG-IP CIS mit dem Operator von OperatorHub. Melden Sie sich mit Clusteradministratorrechten beim Red hat OpenShift-Cluster an und erstellen Sie mit den Anmeldedaten des F5 BIG-IP-Systems ein Geheimnis, das Voraussetzung für den Operator ist.

```
[admin@rhel-7 ~]$ oc create secret generic bigip-login -n kube-system
--from-literal=username=admin --from-literal=password=admin

secret/bigip-login created
```

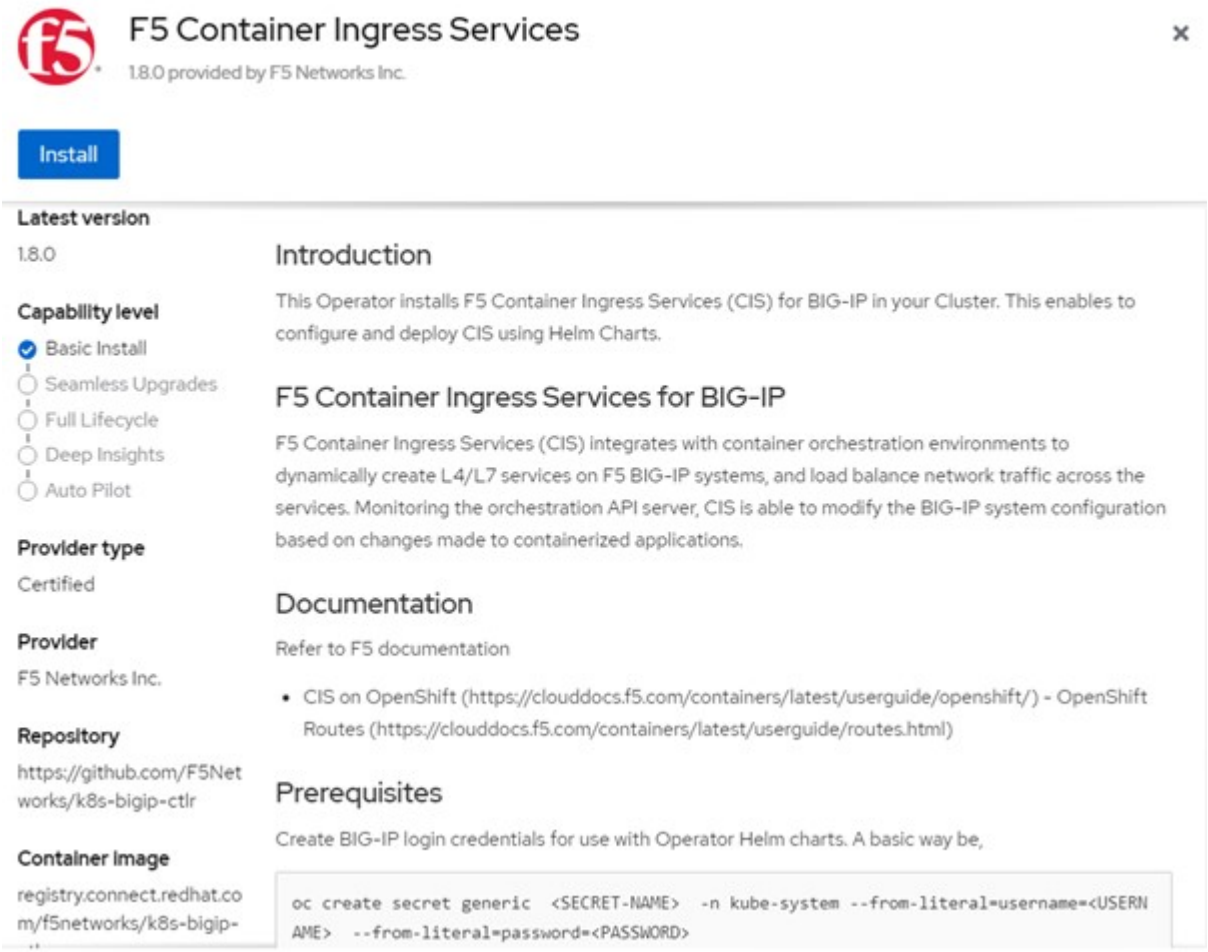
15. Installieren Sie die F5 CIS CRDs.

```
[admin@rhel-7 ~]$ oc apply -f
https://raw.githubusercontent.com/F5Networks/k8s-bigip-
ctlr/master/docs/config_examples/crd/Install/customresourcedefinitions.y
ml

customresourcedefinition.apiextensions.k8s.io/virtualservers.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/tlsprofiles.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/transportservers.cis.f5.co
m created
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com
created
```

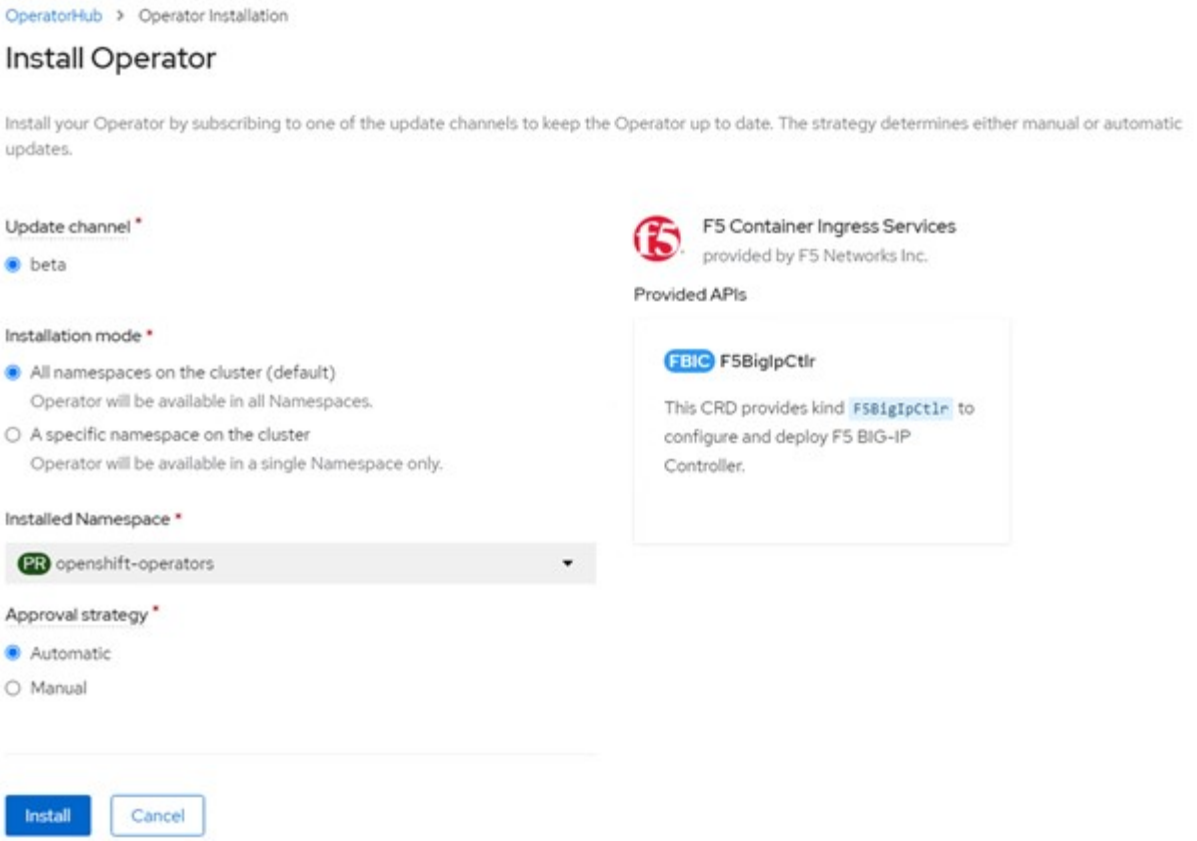
16. Navigieren Sie zu Operators > OperatorHub, suchen Sie nach dem Schlüsselwort F5 und klicken Sie auf die Kachel F5 Container Ingress Service.



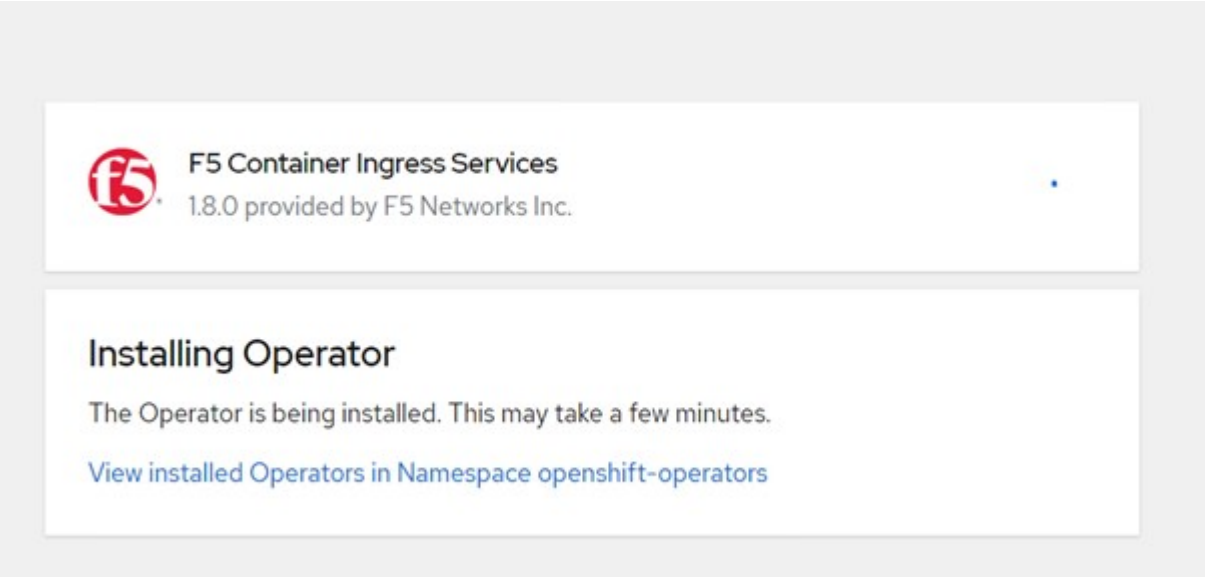
17. Lesen Sie die Bedienerinformationen, und klicken Sie auf Installieren.



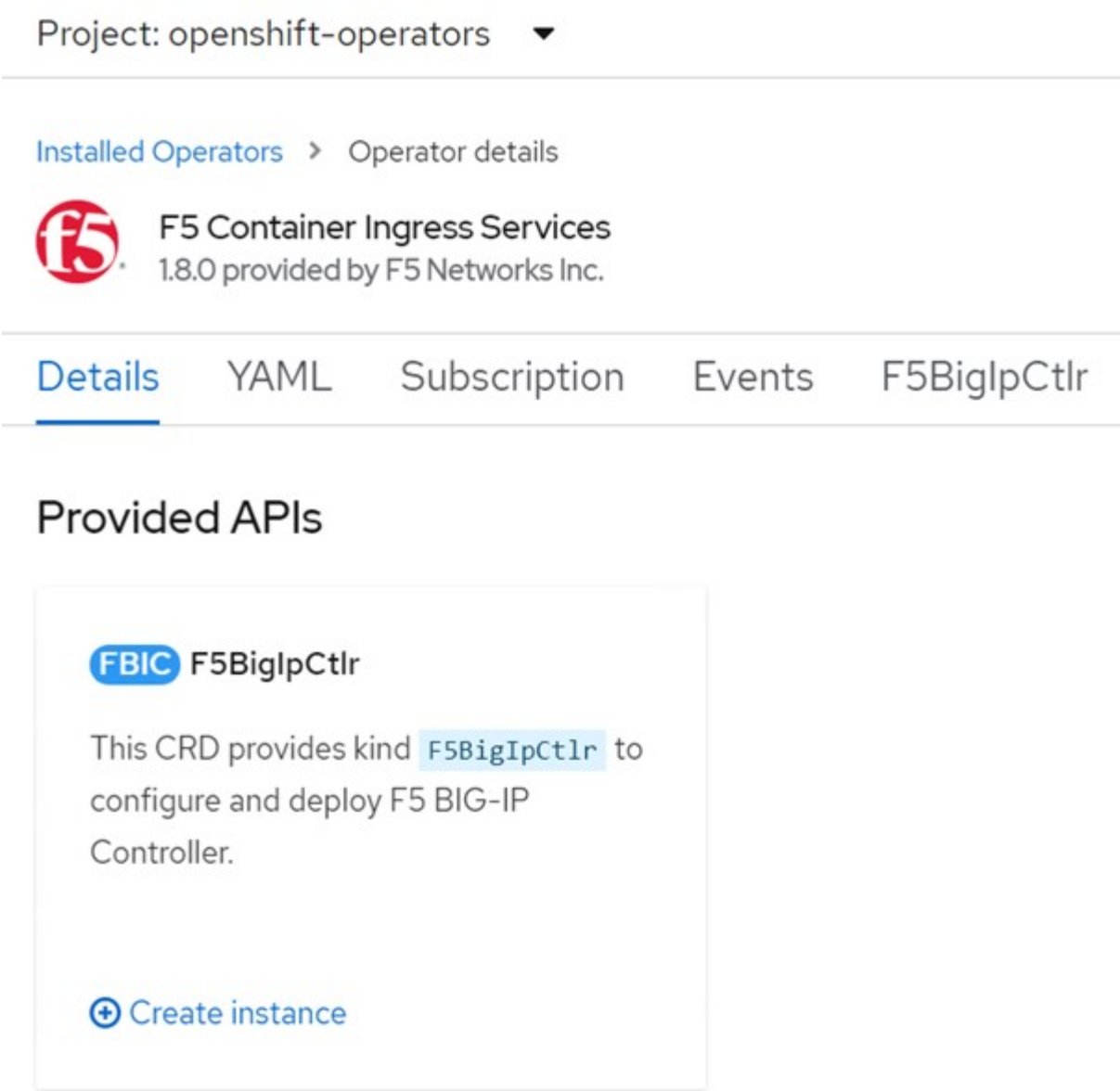
18. Lassen Sie auf dem Bildschirm Install Operator alle Standardparameter stehen, und klicken Sie auf Install.



19. Es dauert eine Weile, bis der Bediener installiert wird.



20. Nach der Installation des Bedieners wird die Meldung Installation erfolgreich angezeigt.
21. Navigieren Sie zu Operatoren > Installed Operators, klicken Sie auf F5 Container Ingress Service und klicken Sie dann unter der Kachel F5BigIpCtlr auf Create Instance.

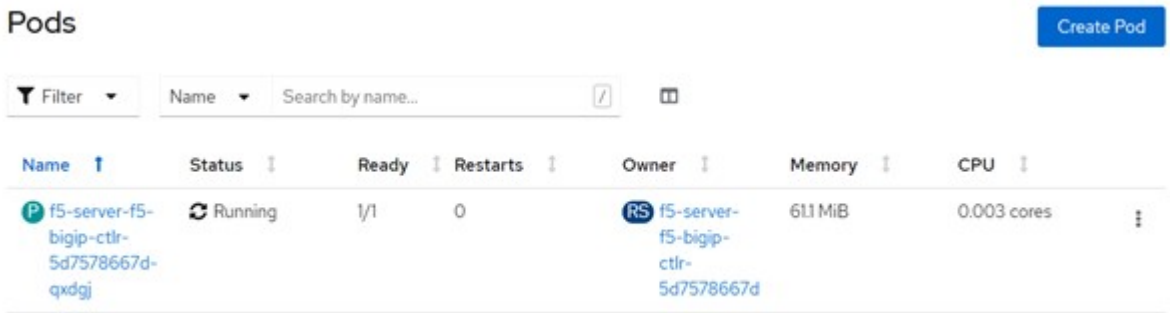


22. Klicken Sie auf YAML View und fügen Sie den folgenden Inhalt ein, nachdem Sie die erforderlichen Parameter aktualisiert haben.

> Aktualisieren Sie die Parameter `bigip_partition`, ` openshift_sdn_Name`, `bigip_url` Und `bigip_login_secret` Geben Sie unten die Werte für Ihr Setup vor dem Kopieren des Inhalts an.

```
apiVersion: cis.f5.com/v1
kind: F5BigIpCtlr
metadata:
  name: f5-server
  namespace: openshift-operators
spec:
  args:
    log_as3_response: true
    agent: as3
    log_level: DEBUG
    bigip_partition: ocp-vmw
    openshift_sdn_name: /Common/openshift_vxlan
    bigip_url: 10.61.181.19
    insecure: true
    pool-member-type: cluster
    custom_resource_mode: true
    as3_validation: true
    ipam: true
    manage_configmaps: true
  bigip_login_secret: bigip-login
  image:
    pullPolicy: Always
    repo: f5networks/cntr-ingress-svcs
    user: registry.connect.redhat.com
  namespace: kube-system
  rbac:
    create: true
  resources: {}
  serviceAccount:
    create: true
  version: latest
```

23. Klicken Sie nach dem Einfügen dieses Inhalts auf Erstellen. Damit werden die CIS-Pods im Namespace des kube-Systems installiert.



Red hat OpenShift bietet standardmäßig eine Möglichkeit, die Dienste über Routen für L7-Lastenausgleich zur Verfügung zu stellen. Ein eingebauter OpenShift-Router ist für die Werbung und den Umgang mit dem Verkehr auf diesen Routen verantwortlich. Sie können die F5 CIS jedoch auch so konfigurieren, dass sie die Routen über ein externes F5 BIG-IP-System unterstützen, das entweder als Hilfrouter oder als Ersatz für den selbst gehosteten OpenShift-Router ausgeführt werden kann. CIS erstellt einen virtuellen Server im BIG-IP-System, der als Router für die OpenShift-Routen fungiert, und BIG-IP übernimmt das Werbe- und Traffic-Routing. Informationen zu Parametern, die diese Funktion aktivieren, finden Sie in der Dokumentation hier. Beachten Sie, dass diese Parameter für die OpenShift Deployment-Ressource in der Apps/v1-API definiert sind. Wenn Sie diese also mit der F5BigIpCtlr Resource cis.f5.com/v1 API verwenden, ersetzen Sie die Bindestriche (-) durch Unterstriche (_) für die Parameternamen.

24. Die Argumente, die an die Erstellung von CIS-Ressourcen übergeben werden, umfassen `ipam: true` Und `custom_resource_mode: true`. Diese Parameter sind für die CIS-Integration mit einem IPAM-Controller erforderlich. Überprüfen Sie, ob die CIS die IPAM-Integration aktiviert hat, indem Sie die F5 IPAM-Ressource erstellen.

```
[admin@rhel-7 ~]$ oc get f5ipam -n kube-system

NAMESPACE   NAME                              AGE
kube-system   ipam.10.61.181.19.ocp-vmw      43s
```

25. Erstellen Sie das Servicekonto, die Rolle und die Einbindung, die für den F5 IPAM-Controller erforderlich sind. Erstellen Sie eine YAML-Datei, und fügen Sie den folgenden Inhalt ein.

```
[admin@rhel-7 ~]$ vi f5-ipam-rbac.yaml

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctlr-clusterrole
rules:
  - apiGroups: ["fic.f5.com"]
    resources: ["ipams","ipams/status"]
    verbs: ["get", "list", "watch", "update", "patch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctlr-clusterrole-binding
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ipam-ctlr-clusterrole
subjects:
  - apiGroup: ""
    kind: ServiceAccount
    name: ipam-ctlr
    namespace: kube-system
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: ipam-ctlr
  namespace: kube-system
```

26. Erstellen Sie die Ressourcen.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-rbac.yaml

clusterrole.rbac.authorization.k8s.io/ipam-ctlr-clusterrole created
clusterrolebinding.rbac.authorization.k8s.io/ipam-ctlr-clusterrole-
binding created
serviceaccount/ipam-ctlr created
```

27. Erstellen Sie eine YAML-Datei, und fügen Sie die nachfolgend angegebene F5 IPAM-Bereitstellungsdefinition ein.

Aktualisieren Sie den ip-Bereich-Parameter in spec.template.spec.Containers[0].args unten, um die ipamLabels und IP-Adressbereiche zu berücksichtigen, die Ihrem Setup entsprechen.

IpamLabels [`range1` Und `range2` Im folgenden Beispiel] müssen für die Dienste des Typs loadbalancer Anmerkungen gemacht werden, damit der IPAM-Controller eine IP-Adresse aus dem definierten Bereich erkennt und zuweist.

```
[admin@rhel-7 ~]$ vi f5-ipam-deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    name: f5-ipam-controller
  name: f5-ipam-controller
  namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: f5-ipam-controller
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: f5-ipam-controller
    spec:
      containers:
      - args:
        - --orchestration=openshift
        - --ip-range='{"range1":"10.63.172.242-10.63.172.249",
"range2":"10.63.170.111-10.63.170.129"}'
        - --log-level=DEBUG
        command:
        - /app/bin/f5-ipam-controller
        image: registry.connect.redhat.com/f5networks/f5-ipam-
controller:latest
        imagePullPolicy: IfNotPresent
        name: f5-ipam-controller
      dnsPolicy: ClusterFirst
      restartPolicy: Always
      schedulerName: default-scheduler
      securityContext: {}
      serviceAccount: ipam-ctlr
      serviceAccountName: ipam-ctlr
```

28. Erstellen Sie die F5 IPAM Controller-Implementierung.

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-deployment.yaml

deployment/f5-ipam-controller created
```

29. Überprüfen Sie, ob die F5 IPAM-Controller-Pods ausgeführt werden.

```
[admin@rhel-7 ~]$ oc get pods -n kube-system

NAME                                        READY   STATUS    RESTARTS
AGE
f5-ipam-controller-5986cff5bd-2bvn6         1/1     Running   0
30s
f5-server-f5-bigip-ctlr-5d7578667d-qxdgj    1/1     Running   0
14m
```

30. Erstellen Sie das F5 IPAM-Schema.

```
[admin@rhel-7 ~]$ oc create -f
https://raw.githubusercontent.com/F5Networks/f5-ipam-
controller/main/docs/_static/schemas/ipam_schema.yaml

customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

Verifizierung

1. Erstellen Sie einen Service vom Typ Load Balancer

```
[admin@rhel-7 ~]$ vi example_svc.yaml

apiVersion: v1
kind: Service
metadata:
  annotations:
    cis.f5.com/ipamLabel: range1
  labels:
    app: f5-demo-test
  name: f5-demo-test
  namespace: default
spec:
  ports:
  - name: f5-demo-test
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: f5-demo-test
  sessionAffinity: None
  type: LoadBalancer
```

```
[admin@rhel-7 ~]$ oc create -f example_svc.yaml

service/f5-demo-test created
```

2. Überprüfen Sie, ob der IPAM-Controller ihm eine externe IP zuweist.

```
[admin@rhel-7 ~]$ oc get svc

NAME           TYPE           CLUSTER-IP       EXTERNAL-IP
PORT(S)        AGE
f5-demo-test   LoadBalancer   172.30.210.108   10.63.172.242
80:32605/TCP   27s
```

3. Erstellen Sie eine Implementierung, und verwenden Sie den erstellten Load Balancer Service.

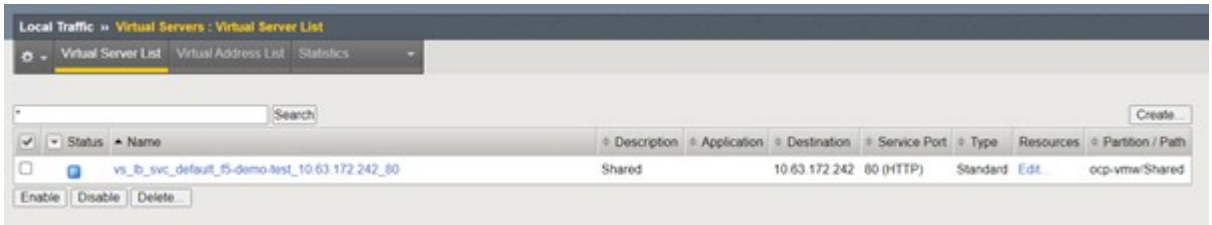
```
[admin@rhel-7 ~]$ vi example_deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: f5-demo-test
  name: f5-demo-test
spec:
  replicas: 2
  selector:
    matchLabels:
      app: f5-demo-test
  template:
    metadata:
      labels:
        app: f5-demo-test
    spec:
      containers:
      - env:
        - name: service_name
          value: f5-demo-test
        image: nginx
        imagePullPolicy: Always
        name: f5-demo-test
        ports:
        - containerPort: 80
          protocol: TCP
```

```
[admin@rhel-7 ~]$ oc create -f example_deployment.yaml

deployment/f5-demo-test created
```

4. Prüfen Sie, ob die Pods ausgeführt werden.

```
[admin@rhel-7 ~]$ oc get pods

NAME                            READY   STATUS    RESTARTS   AGE
f5-demo-test-57c46f6f98-47wwp   1/1     Running   0          27s
f5-demo-test-57c46f6f98-cl2m8   1/1     Running   0          27s
```

5. Prüfen Sie, ob der entsprechende virtuelle Server im BIG-IP-System für den Dienst vom Typ loadbalancer in OpenShift erstellt wird. Navigieren Sie zu lokalem Verkehr > Virtuelle Server > Liste virtueller Server.



Private Bildregistrien Werden Erstellt

Für die meisten Bereitstellungen von Red hat OpenShift verwenden Sie eine öffentliche Registrierung wie "Quay.io" Oder "DockerHub" Erfüllt die meisten Kundenanforderungen. Es gibt jedoch Zeiten, in denen ein Kunde seine eigenen privaten oder angepassten Bilder hosten möchte.

Dieses Verfahren dokumentiert die Erstellung einer privaten Image-Registry, die durch ein persistentes Volume von Astra Trident und NetApp ONTAP unterstützt wird.

> Astra Control Center erfordert eine Registrierung, um die Bilder zu hosten, die die Astra-Container benötigen. Im folgenden Abschnitt werden die Schritte zum Einrichten einer privaten Registrierung auf dem Red hat OpenShift-Cluster sowie das Drücken der Bilder beschrieben, die für die Installation des Astra Control Center erforderlich sind.

Erstellen einer privaten Bildregistrierung

1. Entfernen Sie die Standardanmerkung aus der aktuellen Standard-Storage-Klasse und versehen Sie die Trident-gestützte Storage-Klasse als Standard für das OpenShift-Cluster.

```
[netapp-user@rhel7 ~]$ oc patch storageclass thin -p '{"metadata":
{"annotations": {"storageclass.kubernetes.io/is-default-class":
"false"}}}'
storageclass.storage.k8s.io/thin patched

[netapp-user@rhel7 ~]$ oc patch storageclass ocp-trident -p
'{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-
class": "true"}}}'
storageclass.storage.k8s.io/ocp-trident patched
```

2. Bearbeiten Sie den Operator imageregistry, indem Sie die folgenden Speicherparameter in eingeben `spec` Abschnitt.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

3. Geben Sie die folgenden Parameter in das ein `spec` Abschnitt zum Erstellen einer OpenShift-Route mit einem benutzerdefinierten Hostnamen. Speichern und beenden.

```
routes:
  - hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
    name: netapp-astra-route
```

> Die obige Routenkonfiguration wird verwendet, wenn Sie einen benutzerdefinierten Hostnamen für Ihre Route wünschen. Wenn OpenShift eine Route mit einem Standard-Hostnamen erstellen soll, können Sie dem die folgenden Parameter hinzufügen `spec` Abschnitt: `defaultRoute: true`.

Benutzerdefinierte TLS-Zertifikate

Wenn Sie einen benutzerdefinierten Hostnamen für die Route verwenden, wird standardmäßig die TLS-Standardkonfiguration des OpenShift Ingress-Operators verwendet. Sie können der Route jedoch eine benutzerdefinierte TLS-Konfiguration hinzufügen. Um das zu tun, führen Sie folgende Schritte durch.

a. Erstellen Sie ein Geheimnis mit den TLS-Zertifikaten und dem Schlüssel der Route.

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n
openshift-image-registry –cert/home/admin/netapp-astra/tls.crt
--key=/home/admin/netapp-astra/tls.key
```

b. Bearbeiten Sie den Operator Imageregistry, und fügen Sie dem die folgenden Parameter hinzu `spec` Abschnitt.

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

routes:
  - hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
    name: netapp-astra-route
    secretName: astra-route-tls
```

4. Bearbeiten Sie den Operator Imageregistry erneut, und ändern Sie den Verwaltungsstatus des Bedieners in das `Managed` Bundesland. Speichern und beenden.

```
oc edit configs.imageregistry/cluster

managementState: Managed
```

5. Wenn alle Voraussetzungen erfüllt sind, werden PVCs, Pods und Services für die private Image Registry erstellt. In wenigen Minuten sollte die Registrierung betriebsbereit sein.

```
[netapp-user@rhel7 ~]$oc get all -n openshift-image-registry

NAME                                                    READY   STATUS
RESTARTS   AGE
pod/cluster-image-registry-operator-74f6d954b6-rb7zr   1/1     Running
3          90d
pod/image-pruner-1627257600-f5cpj                       0/1     Completed
0          2d9h
pod/image-pruner-1627344000-swqx9                       0/1     Completed
0          33h
pod/image-pruner-1627430400-rv5nt                       0/1     Completed
0          9h
pod/image-registry-6758b547f-6pnj8                      1/1     Running
0          76m
pod/node-ca-bwb5r                                       1/1     Running
0          90d
pod/node-ca-f8w54                                       1/1     Running
0          90d
pod/node-ca-gjx7h                                       1/1     Running
0          90d
pod/node-ca-lcx4k                                       1/1     Running
0          33d
pod/node-ca-v7zmx                                       1/1     Running
0          7d21h
pod/node-ca-xpppp                                       1/1     Running
0          89d

NAME                                TYPE        CLUSTER-IP       EXTERNAL-
IP   PORT(S)     AGE
service/image-registry              ClusterIP   172.30.196.167   <none>
5000/TCP    15h
service/image-registry-operator     ClusterIP   None             <none>
60000/TCP   90d

NAME                       DESIRED   CURRENT   READY   UP-TO-DATE
AVAILABLE   NODE SELECTOR            AGE
daemonset.apps/node-ca   6         6         6       6            6
kubernetes.io/os=linux   90d

NAME                                                 READY   UP-TO-DATE
AVAILABLE   AGE
deployment.apps/cluster-image-registry-operator   1/1     1            1
90d
```

```
deployment.apps/image-registry                   1/1     1            1
15h

NAME                                                              DESIRED
CURRENT   READY   AGE
replicaset.apps/cluster-image-registry-operator-74f6d954b6   1         1
1       90d
replicaset.apps/image-registry-6758b547f                     1         1
1       76m
replicaset.apps/image-registry-78bfbd7f59                    0         0
0       15h
replicaset.apps/image-registry-7fcc8d6cc8                    0         0
0       80m
replicaset.apps/image-registry-864f88f5b                     0         0
0       15h
replicaset.apps/image-registry-cb47fffb                      0         0
0       10h

NAME                                 COMPLETIONS   DURATION   AGE
job.batch/image-pruner-1627257600   1/1           10s        2d9h
job.batch/image-pruner-1627344000   1/1           6s         33h
job.batch/image-pruner-1627430400   1/1           5s         9h

NAME                         SCHEDULE    SUSPEND   ACTIVE   LAST
SCHEDULE   AGE
cronjob.batch/image-pruner   0 0 * * *   False     0        9h
90d

NAME                                        HOST/PORT
PATH   SERVICES         PORT    TERMINATION   WILDCARD
route.route.openshift.io/public-routes   astra-registry.apps.ocp-
vmw.cie.netapp.com          image-registry   <all>   reencrypt     None
```

6. Wenn Sie die standardmäßigen TLS-Zertifikate für die Registrierungsroute Ingress Operator OpenShift verwenden, können Sie die TLS-Zertifikate mit dem folgenden Befehl abrufen.

```
[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n
openshift-ingress-operator
```

7. Damit OpenShift-Knoten auf die Bilder zugreifen und sie aus der Registrierung ziehen können, fügen Sie die Zertifikate dem Docker-Client auf den OpenShift-Knoten hinzu. Erstellen Sie im eine Konfigurationskarte `openshift-config` Namespace mit den TLS-Zertifikaten und patchen Sie ihn mit der Konfiguration des Cluster-Images, um das Zertifikat vertrauenswürdig zu machen.

```
[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config
--from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}'
--type=merge
```

8. Die interne OpenShift-Registrierung wird durch Authentifizierung gesteuert. Alle OpenShift-Benutzer können auf die OpenShift-Registrierung zugreifen, aber die Vorgänge, die der angemeldete Benutzer durchführen kann, sind von den Benutzerberechtigungen abhängig.
   a. Damit ein Benutzer oder eine Gruppe von Benutzern Bilder aus der Registrierung ziehen kann, müssen den Benutzern die Rolle Registry-Viewer zugewiesen sein.

      ```
      [netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer
      ocp-user

      [netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer
      ocp-user-group
      ```

   b. Damit ein Benutzer oder eine Benutzergruppe Bilder schreiben oder übertragen kann, muss dem/den Benutzer die Rolle des Registrierungs-Editors zugewiesen sein.

      ```
      [netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor
      ocp-user

      [netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor
      ocp-user-group
      ```

9. Damit OpenShift-Knoten auf die Registrierung zugreifen und die Bilder per Push oder Pull übertragen können, müssen Sie einen Pull Secret konfigurieren.

   ```
   [netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-
   credentials --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com
   --docker-username=ocp-user --docker-password=password
   ```

10. Dieses Pull-Secret kann dann auf Dienstkonten gepatcht oder in der entsprechenden Pod-Definition referenziert werden.
    a. Führen Sie den folgenden Befehl aus, um ihn auf Dienstkonten zu patchen.

       ```
       [netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-
       registry-credentials --for=pull
       ```

b. Um den Pull-Secret in der Pod-Definition zu referenzieren, fügen Sie dem den folgenden Parameter hinzu `spec` Abschnitt.

```
imagePullSecrets:
  - name: astra-registry-credentials
```

11. Führen Sie die folgenden Schritte aus, um ein Bild von den Arbeitsstationen getrennt vom OpenShift-Knoten zu schieben oder zu ziehen.

a. Fügen Sie die TLS-Zertifikate zum Docker-Client hinzu.

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-
registry.apps.ocp-vmw.cie.netapp.com

[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

b. Melden Sie sich über den oc-Anmeldebefehl bei OpenShift an.

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO
-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

c. Melden Sie sich mit den OpenShift-Benutzeranmeldeinformationen über den Befehl podman/Docker bei der Registrierung an.

Podman

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-
vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t) --tls
-verify=false
```

+ HINWEIS: Wenn Sie verwenden `kubeadmin` Benutzer, um sich bei der privaten Registrierung anzumelden, dann Token statt Passwort verwenden.

docker

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-
vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

+ HINWEIS: Wenn Sie verwenden `kubeadmin` Benutzer, um sich bei der privaten Registrierung anzumelden, dann Token statt Passwort verwenden.

d. Drücken oder ziehen Sie die Bilder.

Podman

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra/vault-controller:latest
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

docker

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra/vault-controller:latest
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-
vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

Lösungsvalidierung und Anwendungsfälle: Red hat OpenShift mit NetApp

Die auf dieser Seite angegebenen Beispiele finden sich Lösungsvalidierung und Anwendungsfälle für Red hat OpenShift mit NetApp.

- "Implementierung einer Jenkins CI/CD-Pipeline mit persistentem Storage"
- "Konfigurieren Sie Mandantenfähigkeit auf Red hat OpenShift mit NetApp"
- "Red hat OpenShift Virtualisierung mit NetApp ONTAP"
- "Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp"

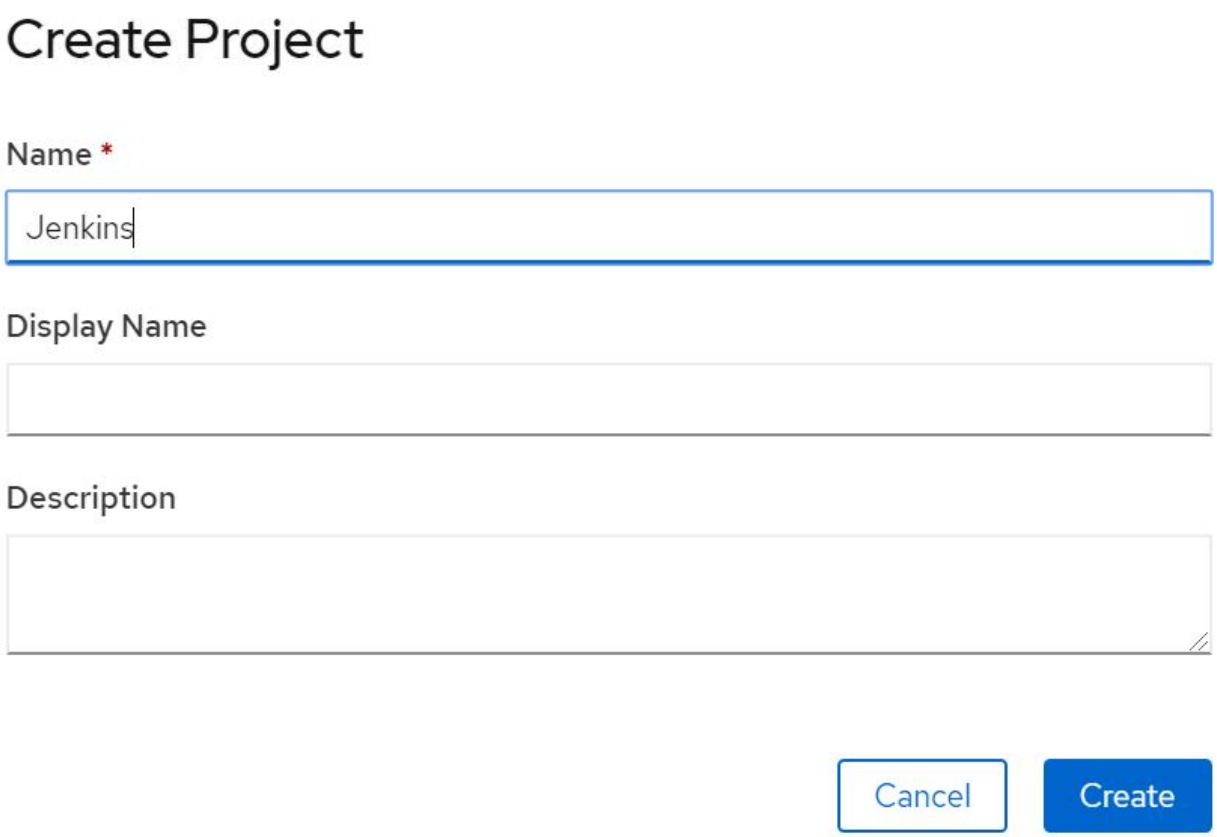
Implementieren Sie eine Jenkins CI/CD-Pipeline mit persistentem Storage: Red hat OpenShift mit NetApp

Dieser Abschnitt erläutert die Schritte zur Implementierung einer CI/CD-Pipeline (Continuous Integration/Continuous Delivery) mit Jenkins zur Validierung des Lösungsbetriebs.

Erstellen Sie die Ressourcen, die für eine Implementierung mit Jenkins erforderlich sind

Um die Ressourcen zu erstellen, die für die Implementierung der Jenkins-Applikation erforderlich sind, gehen Sie wie folgt vor:

1. Erstellen Sie ein neues Projekt namens Jenkins.



2. In diesem Beispiel haben wir Jenkins mit persistentem Storage implementiert. Um den Jenkins-Build zu unterstützen, erstellen Sie das PVC. Navigieren Sie zu Storage > Persistent Volume Claims und klicken Sie auf Create Persistent Volume Claim. Wählen Sie die Speicherklasse aus, die erstellt wurde, stellen Sie sicher, dass der Name des Persistent Volume Claim jenkins ist, wählen Sie die entsprechende Größe und den entsprechenden Zugriffsmodus aus, und klicken Sie dann auf Erstellen.

Project: jenkins

Create Persistent Volume Claim

Edit YAML

Storage Class

SC basic

Storage class for the new claim.

Persistent Volume Claim Name *

jenkins

A unique name for the storage claim within the project.

Access Mode *

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

Permissions to the mounted drive.

Size *

100 GiB

Desired storage capacity.

Use label selectors to request storage

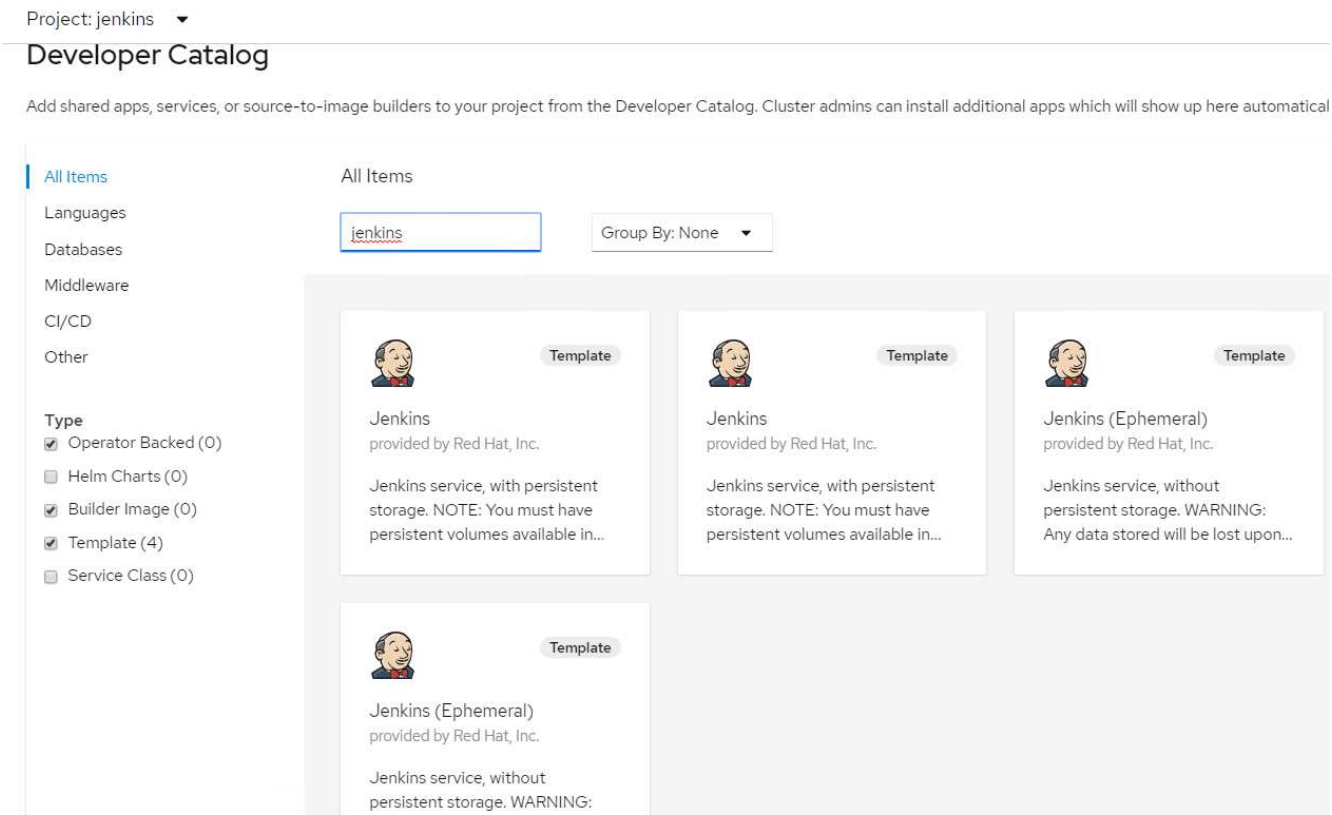
Use label selectors to define how storage is created.

Create Cancel

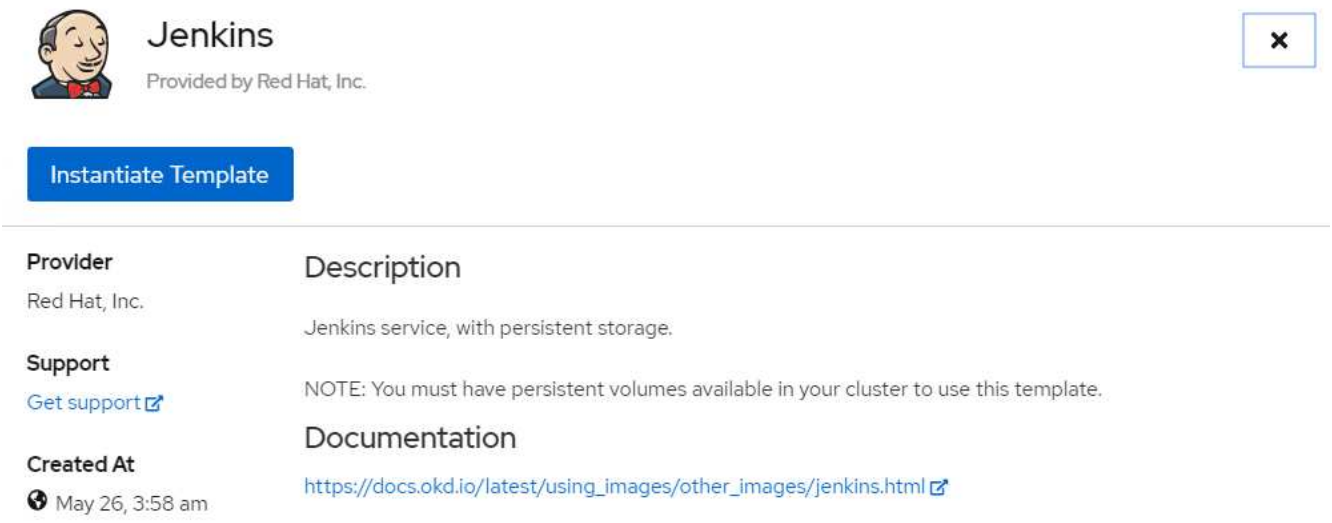
Implementieren Sie Jenkins mit persistentem Storage

Um Jenkins mit persistentem Storage zu implementieren, gehen Sie wie folgt vor:

1. Ändern Sie in der oberen linken Ecke die Rolle von Administrator zu Entwickler. Klicken Sie auf + Hinzufügen und wählen Sie aus Katalog. Suchen Sie in der Suchleiste nach jenkins. Wählen Sie Jenkins Service mit persistentem Storage.

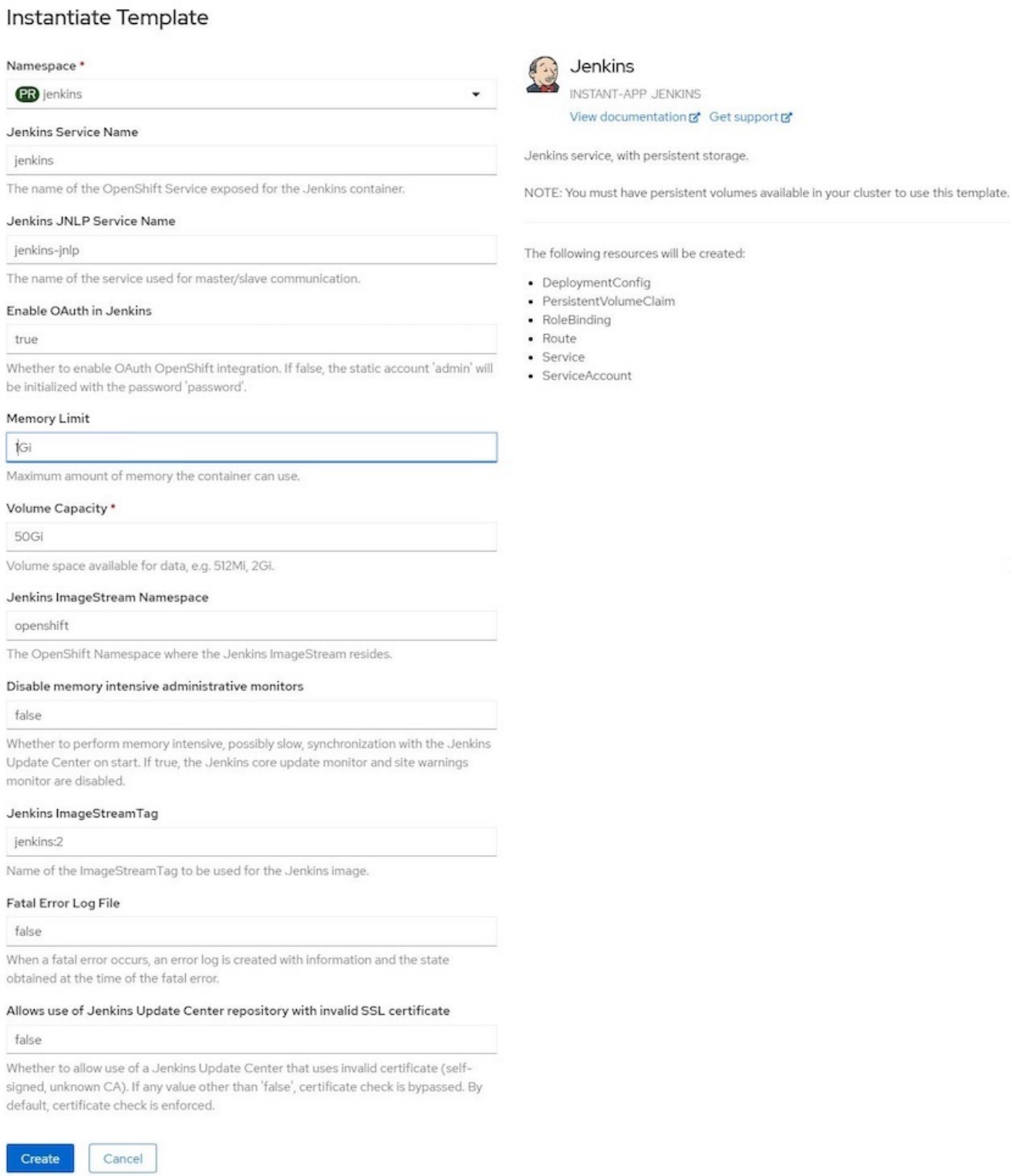


2. Klicken Sie Auf `Instantiate Template`.



3. Standardmäßig werden die Details für die Jenkins-Anwendung ausgefüllt. Ändern Sie die Parameter entsprechend Ihren Anforderungen, und klicken Sie auf Erstellen. Bei diesem Prozess werden alle

erforderlichen Ressourcen zur Unterstützung von Jenkins auf OpenShift erstellt.



4. Die Jenkins-Pods dauern etwa 10 bis 12 Minuten, bis Sie in den Status „bereit“ versetzt wurden.

Project: jenkins

Pods

Create Pod

Filter by name...

1 Running | 0 Pending | 0 Terminating | 0 CrashLoopBackOff | 1 Completed | 0 Failed | 0 Unknown

Select all filters

1 of 2 Items

Name	Namespace	Status	Ready	Owner	Memory	CPU
P jenkins-1-c77n9	NS jenkins	Running	1/1	RC jenkins-1	-	0.004 cores

5. Navigieren Sie, nachdem die Pods instanziiert sind, zu Netzwerk > Routen. Um die Jenkins Webseite zu öffnen, klicken Sie auf die URL für die jenkins Route.

Project: jenkins

Routes

Create Route

Filter by name...

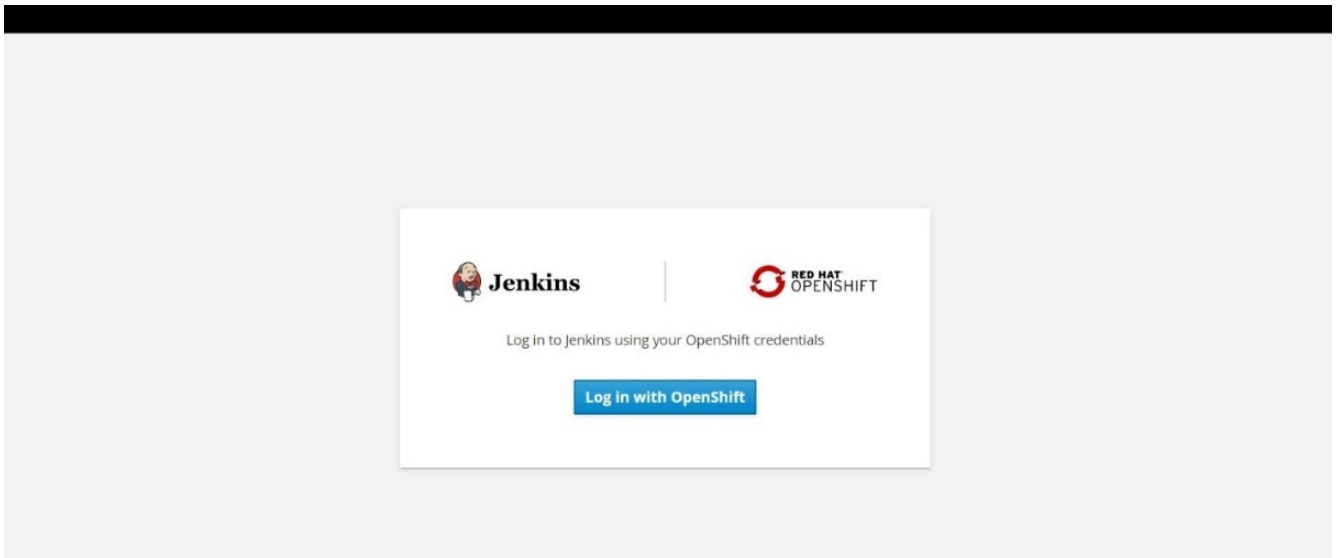
1 Accepted | 0 Rejected | 0 Pending

Select all filters

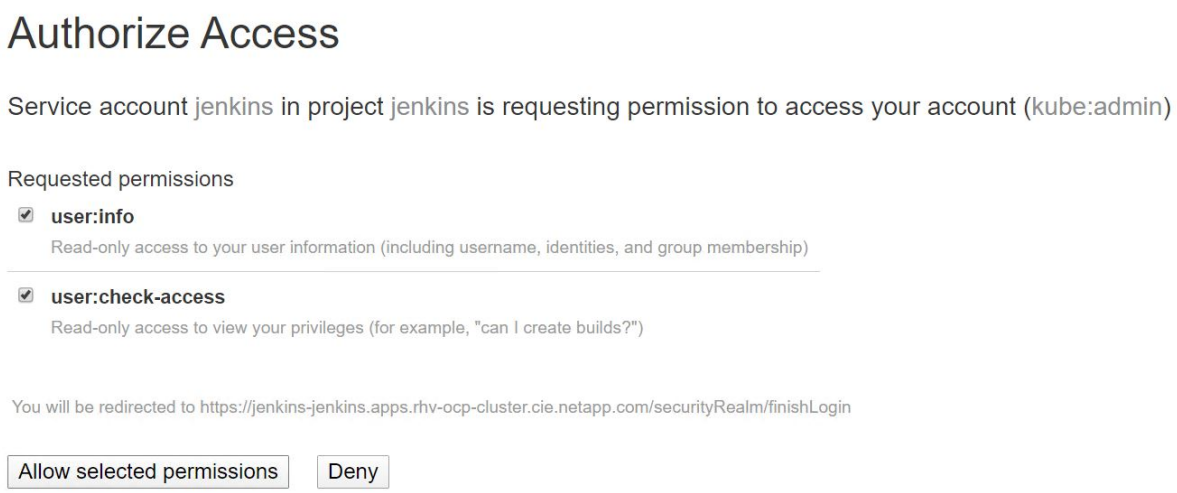
1 Item

Name	Namespace	Status	Location	Service
RT jenkins	NS jenkins	Accepted	https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com	S jenkins

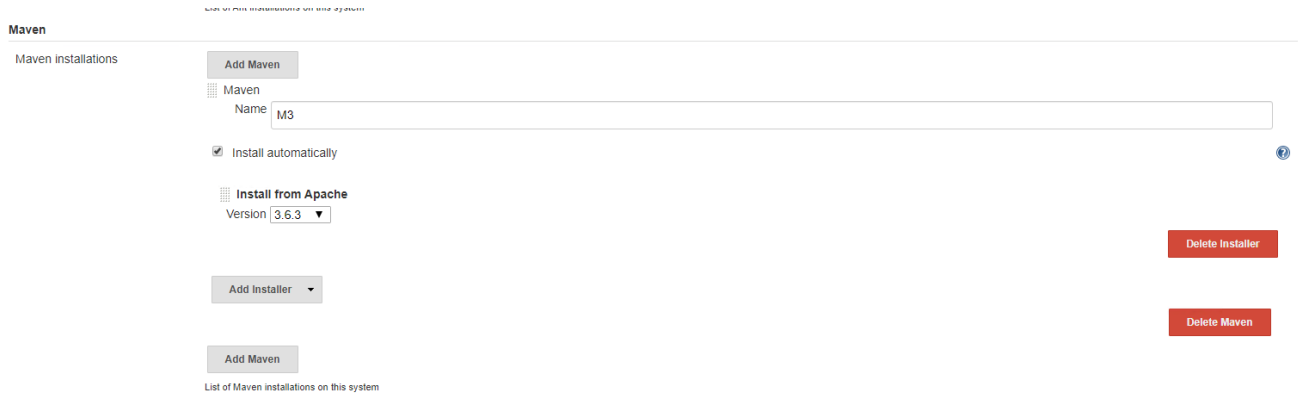
6. Da OpenShift OAuth beim Erstellen der Jenkins-App verwendet wurde, klicken Sie auf Anmelden mit OpenShift.



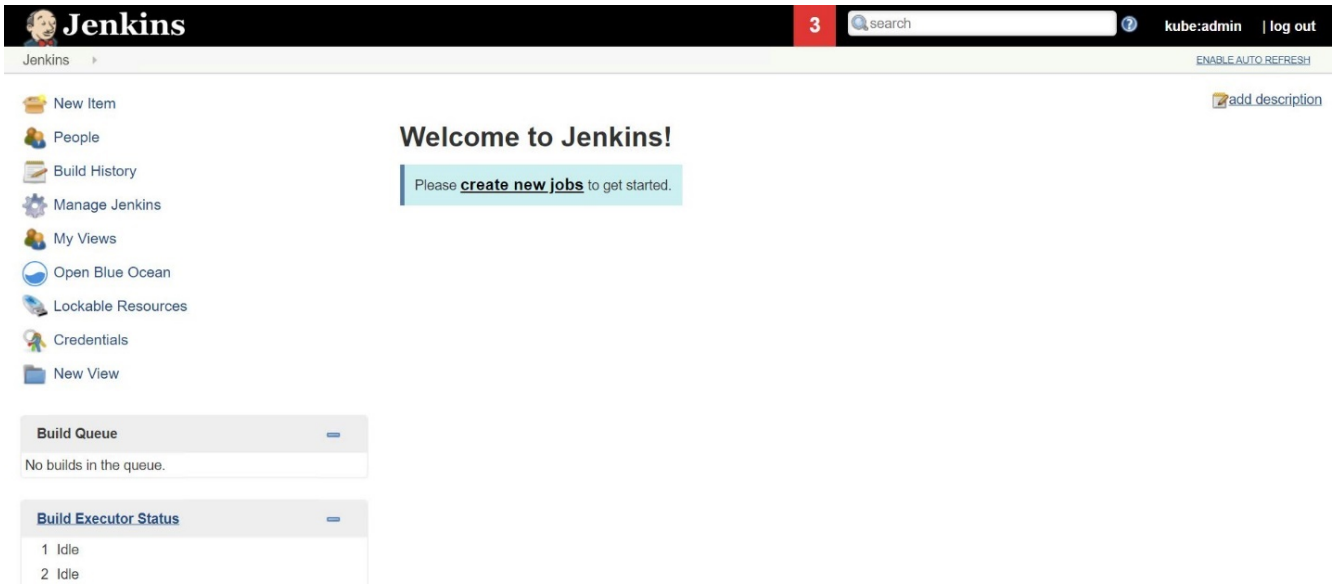
7. Autorisieren Sie das Jenkins Service-Konto, um auf die OpenShift-Benutzer zuzugreifen.



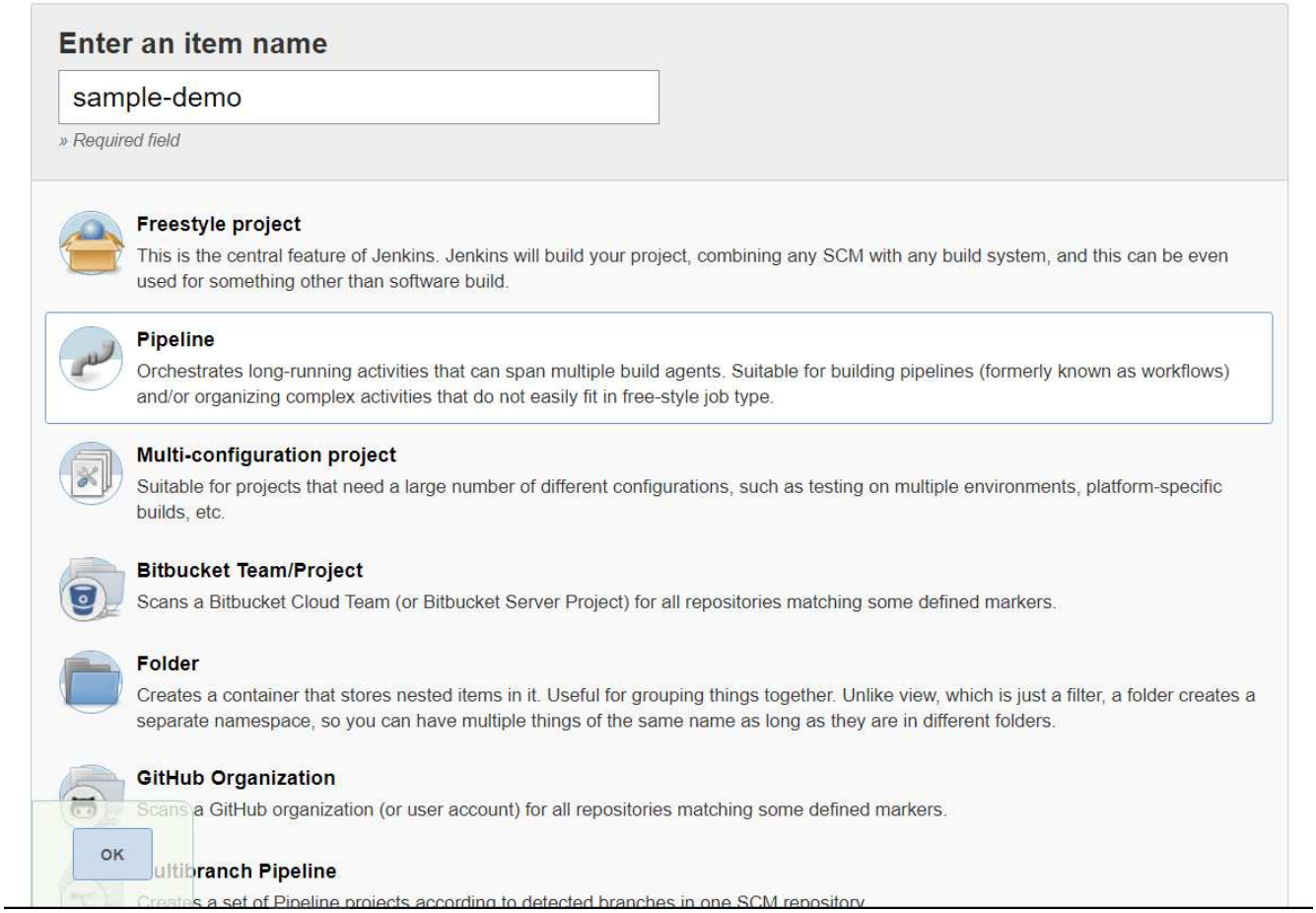
8. Die Jenkins Willkommensseite wird angezeigt. Da wir einen Maven-Build verwenden, füllen Sie zuerst die Maven-Installation aus. Navigieren Sie zu Manage Jenkins > Global Tool Configuration, und klicken Sie dann im Maven-Unterkopf auf Add Maven. Geben Sie den Namen Ihrer Wahl ein, und stellen Sie sicher, dass die Option automatisch installieren ausgewählt ist. Klicken Sie auf Speichern .



9. Sie können jetzt eine Pipeline erstellen, um den CI/CD-Workflow zu demonstrieren. Klicken Sie auf der Startseite im linken Menü auf Neue Jobs oder Neues Element erstellen.



10. Geben Sie auf der Seite Artikel erstellen den Namen Ihrer Wahl ein, wählen Sie Pipeline aus, und klicken Sie auf OK.



11. Wählen Sie die Registerkarte Pipeline aus. Wählen Sie im Dropdown-Menü Testprobe-Pipeline Github + Maven aus. Der Code wird automatisch ausgefüllt. Klicken Sie auf Speichern .

General | Build Triggers | Advanced Project Options | **Pipeline**

Advanced...

Pipeline

Definition: Pipeline script

Script: GitHub + Maven

```
1  node {
2     def mvnHome
3     stage('Preparation') { // for display purposes
4        // Get some code from a GitHub repository
5        git 'https://github.com/jglick/simple-maven-project-with-tests.git'
6        // Get the Maven tool.
7        // ** NOTE: This 'M3' Maven tool must be configured
8        // **       in the global configuration.
9        mvnHome = tool 'M3'
10    }
11    stage('Build') {
12       // Run the maven build
13       withEnv(["MVN_HOME=$mvnHome"]) {
14          if (isUnix()) {
15             sh '"$MVN_HOME/bin/mvn" -Dmaven.test.failure.ignore clean package'
16          } else {
17             bat(/"%MVN_HOME%\bin\mvn" -Dmaven.test.failure.ignore clean package/)
```

☑ Use Groovy Sandbox

Pipeline Syntax

Save | Apply

12. Klicken Sie auf Jetzt erstellen, um die Entwicklung durch die Vorbereitungs-, Build- und Testphase auszulösen. Es kann einige Minuten dauern, bis der gesamte Build-Prozess abgeschlossen ist und die Ergebnisse des Builds angezeigt werden.

13. Bei Codeänderungen kann die Pipeline so neu aufgebaut werden, dass sie die neue Version der Software patcht, die kontinuierliche Integration und kontinuierliche Bereitstellung ermöglicht. Klicken Sie auf Letzte Änderungen, um die Änderungen von der vorherigen Version zu verfolgen.

Konfiguration der Mandantenfähigkeit auf Red hat OpenShift mit NetApp ONTAP

Mandantenfähigkeit auf Red hat OpenShift mit NetApp konfigurieren

Viele Unternehmen, die mehrere Anwendungen oder Workloads in Containern ausführen, implementieren meist ein Red hat OpenShift-Cluster pro Applikation oder Workload. Auf diese Weise können sie eine strenge Isolation für die Applikation oder den Workload implementieren, die Performance optimieren und Sicherheitsschwachstellen reduzieren. Die Bereitstellung eines separaten Red hat OpenShift-Clusters für jede Applikation stellt jedoch eigene Probleme dar. Es erhöht den betrieblichen Overhead, der jedes Cluster einzeln überwachen und managen muss. Außerdem erhöht es die Kosten, die durch dedizierte Ressourcen für verschiedene Applikationen entstehen, und behindert die effiziente Skalierbarkeit.

Um diese Probleme zu beheben, kann man in Betracht ziehen, alle Anwendungen oder Workloads in einem einzigen Red hat OpenShift-Cluster auszuführen. In einer solchen Architektur stellen jedoch die Schwachstellen bei der Ressourcen-Isolierung und Applikationssicherheit eine der größten Herausforderungen dar. Sicherheitsschwachstellen bei einem Workload können natürlich auf einen anderen Workload überlaufen, wodurch die Aufprallzone erhöht wird. Darüber hinaus kann jede abrupte, unkontrollierte Ressourcenauslastung einer Applikation die Performance einer anderen Applikation beeinträchtigen, da standardmäßig keine Ressourcenzuordnungsrichtlinie vorhanden ist.

Daher interessieren sich Unternehmen für Lösungen, die sich in beiden Welten optimal einsetzen lassen: Sie können dadurch beispielsweise alle Workloads in einem einzelnen Cluster ausführen und dennoch die Vorteile

eines dedizierten Clusters für jeden Workload bieten.

Eine solche effektive Lösung ist die Konfiguration der Mandantenfähigkeit auf Red hat OpenShift. Mandantenfähigkeit ist eine Architektur, in der mehrere Mandanten gleichzeitig im selben Cluster nebeneinander existieren können, wobei Ressourcen, Sicherheit usw. voneinander isoliert werden. In diesem Zusammenhang kann ein Mandant als Teilbereich der Cluster-Ressourcen angesehen werden, die so konfiguriert sind, dass er für einen exklusiven Zweck von einer bestimmten Benutzergruppe verwendet werden kann. Die Konfiguration der Mandantenfähigkeit auf einem Red hat OpenShift-Cluster bietet folgende Vorteile:

- A - Verringerung von Investitions- und Betriebskosten durch gemeinsame Nutzung von Cluster-Ressourcen
- Geringerer Betriebs- und Managementaufwand
- Schutz der Workloads vor Kreuzkontamination von Sicherheitsverletzungen
- Schutz von Workloads vor unerwarteter Performance-Verschlechterung aufgrund von Ressourcenkonflikten

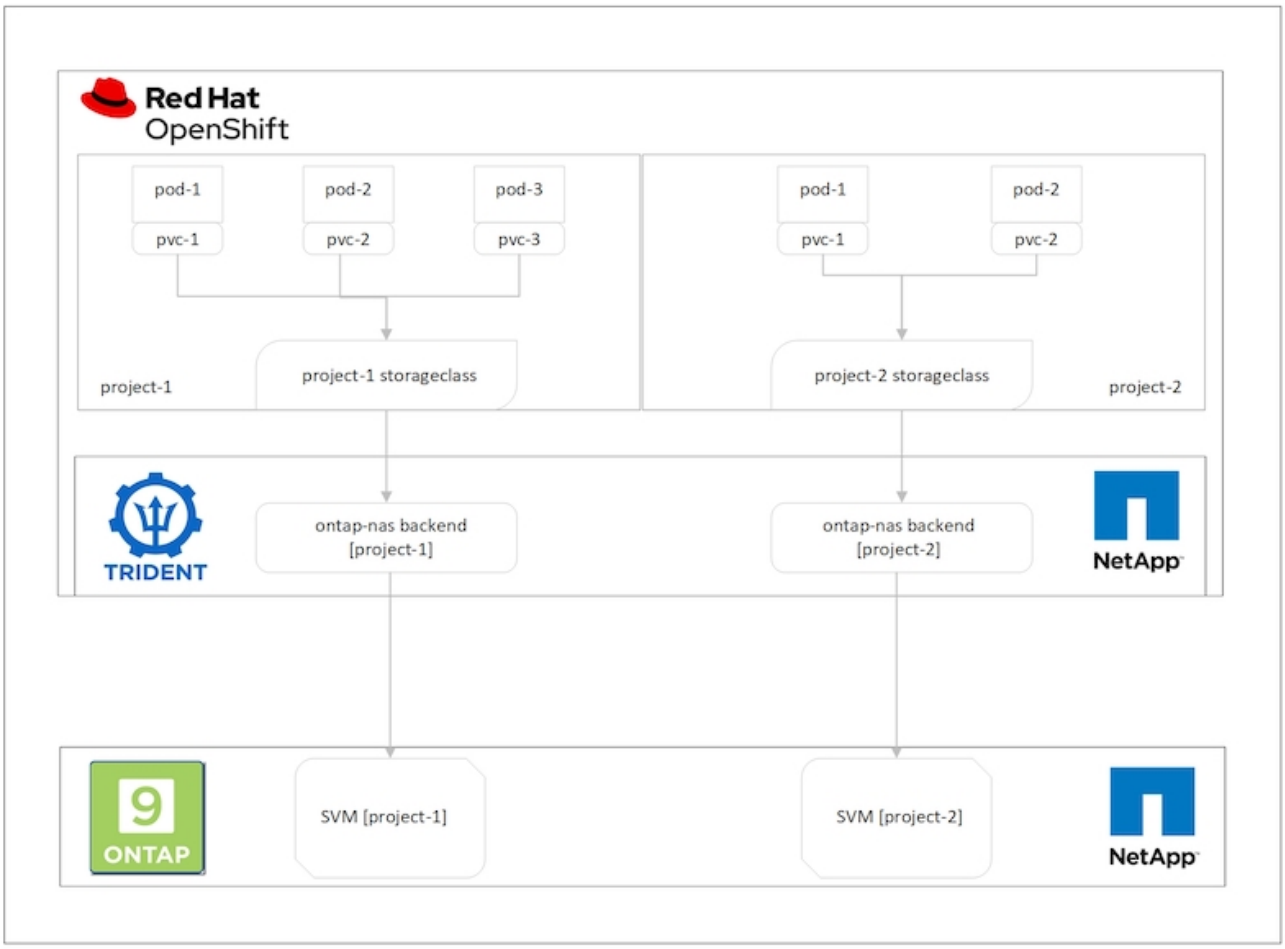
Für einen vollständig realisierten, mandantenfähigen OpenShift-Cluster müssen Quoten und Einschränkungen für Cluster-Ressourcen konfiguriert werden, die zu verschiedenen Ressourcen-Buckets gehören: computing, Storage, Netzwerk, Sicherheit usw. Obwohl wir in dieser Lösung bestimmte Aspekte aller Ressourcen-Buckets abdecken, Die Best Practices für die Isolierung und Sicherung von Daten, die von mehreren Workloads bereitgestellt oder genutzt werden, stehen im selben Red hat OpenShift Cluster im Mittelpunkt. Dazu müssen Mandantenfähigkeit auf Storage-Ressourcen konfiguriert werden, die durch Astra Trident und NetApp ONTAP dynamisch zugewiesen werden.

Der Netapp Architektur Sind

Auch wenn die von NetApp ONTAP unterstützten Red hat OpenShift und Astra Trident standardmäßig keine Isolierung zwischen Workloads bieten, bieten sie zahlreiche Funktionen für die Konfiguration der Mandantenfähigkeit. Wenn wir uns ein besseres Bild davon machen möchten, wie eine mandantenfähige Lösung auf einem Red hat OpenShift-Cluster mit Astra Trident von NetApp ONTAP entworfen wird, können wir uns ein Beispiel mit einer Reihe von Anforderungen nehmen und die damit zu berücksichtigende Konfiguration beschreiben.

Nehmen wir einmal an, dass ein Unternehmen zwei seiner Workloads auf einem Red hat OpenShift-Cluster ausführt. Dies ist Teil von zwei Projekten, an denen zwei verschiedene Teams arbeiten. Die Daten für diese Workloads liegen auf PVCs, die durch Astra Trident dynamisch auf einem NetApp ONTAP NAS-Back-End bereitgestellt werden. Das Unternehmen muss für diese beiden Workloads eine mandantenfähige Lösung entwerfen und die Ressourcen für diese Projekte isolieren, um sicherzustellen, dass Sicherheit und Performance erhalten bleiben. Dabei geht es vor allem um die Daten, die die Applikationen unterstützen.

Die folgende Abbildung zeigt die mandantenfähige Lösung auf einem Red hat OpenShift-Cluster mit Astra Trident, der durch NetApp ONTAP unterstützt wird.



Technologieanforderungen erfüllt

1. NetApp ONTAP Storage-Cluster
2. Red hat OpenShift-Cluster
3. Astra Trident

Red hat OpenShift – Clusterressourcen

Aus der Clusteransicht des Red hat OpenShift ist das Projekt die Ressource auf oberster Ebene. Ein OpenShift-Projekt kann als Clusterressource betrachtet werden, die das gesamte OpenShift-Cluster in mehrere virtuelle Cluster unterteilt. Daher bildet die Isolierung auf Projektebene eine Grundlage für die Konfiguration der Mandantenfähigkeit.

Anschließend können Sie die RBAC im Cluster konfigurieren. Es empfiehlt sich, dass alle Entwickler an einem einzelnen Projekt oder Workload in einer einzelnen Benutzergruppe im Identitätsanbieter (IdP) konfiguriert werden. Red hat OpenShift ermöglicht die IdP-Integration und die Synchronisierung von Benutzergruppen. So können Benutzer und Gruppen aus dem IdP in das Cluster importiert werden. So können Cluster-Administratoren den Zugriff auf die für ein Projekt dedizierten Cluster-Ressourcen für eine Benutzergruppe oder -Gruppe, die an diesem Projekt arbeitet, trennen und dadurch unberechtigten Zugriff auf Cluster-Ressourcen einschränken. Weitere Informationen zur IdP-Integration mit Red hat OpenShift finden Sie in der Dokumentation "Hier".

NetApp ONTAP

Es ist wichtig, den gemeinsam genutzten Speicher zu isolieren, der als persistenter Speicheranbieter für einen Red hat OpenShift-Cluster dient. Dadurch muss sichergestellt werden, dass die auf dem Speicher für jedes Projekt erstellten Volumes den Hosts so angezeigt werden, als ob sie in einem separaten Speicher erstellt werden. Erstellen Sie dazu auf NetApp ONTAP so viele SVMs (Storage Virtual Machines), wie es Projekte oder Workloads gibt, und weisen Sie jede SVM einem Workload zu.

Astra Trident

Nachdem Sie für verschiedene Projekte, die auf NetApp ONTAP erstellt wurden, unterschiedliche SVMs vorhanden sind, müssen Sie jede SVM einem anderen Trident-Back-End zuordnen. Die Back-End-Konfiguration auf Trident treibt die Zuweisung von persistentem Storage zu OpenShift-Cluster-Ressourcen an. Außerdem sind Details der SVM zu zugeordnet. Dies sollte mindestens der Protokolltreiber für das Backend sein. Optional können Sie damit definieren, wie die Volumes im Storage bereitgestellt werden, und Grenzen für die Größe von Volumes oder die Nutzung von Aggregaten festlegen. Details zur Definition der Trident Back-Ends finden sich "Hier".

Red hat OpenShift – Speicherressourcen

Nach der Konfiguration der Trident Back-Ends wird als nächster Schritt die Konfiguration von StorageClasses durchgeführt. Konfigurieren Sie so viele Storage-Klassen wie Back-Ends, wobei jede Storage-Klasse Zugriff erlaubt, Volumes nur an einem Back-End zu erweitern. Wir können die StorageClass einem bestimmten Trident Back-End zuordnen, indem wir während der Definition der Storage-Klasse den StoragePools Parameter verwenden. Die Details zur Definition einer Storage-Klasse sind verfügbar "Hier". Somit gibt es eine 1:1-Zuordnung von StorageClass zu Trident Back-End, die auf eine SVM verweist. So wird sichergestellt, dass alle Storage-Anforderungen über die StorageClass, die diesem Projekt zugewiesen ist, von der für dieses Projekt dedizierten SVM bedient werden.

Da Storage-Klassen keine Ressourcen mit Namespaces sind, wie stellen wir sicher, dass Storage-Forderungen für eine Storage-Klasse eines Projekts durch Pods in einem anderen Namespace oder Projekt abgelehnt werden? Die Antwort ist die Verwendung von ResourceQuotas. ResourceQuotas sind Objekte, die die Gesamtauslastung von Ressourcen pro Projekt steuern. Sie kann die Anzahl und die Gesamtanzahl der Ressourcen begrenzen, die von Objekten im Projekt verbraucht werden können. Mithilfe von ResourceQuotas lassen sich nahezu alle Ressourcen eines Projekts beschränken. Mit dieser effizienten Nutzung können Unternehmen Kosten und Ausfälle aufgrund von überdimensionierten Ressourcen oder überhöhten Ressourcen senken. Siehe Dokumentation "Hier" Finden Sie weitere Informationen.

Bei diesem Anwendungsfall müssen wir die Pods in einem bestimmten Projekt beschränken, wenn wir Storage aus Storage-Klassen beanspruchen, die nicht für ihr Projekt reserviert sind. Um dies zu erreichen, müssen wir die Anforderungen für persistente Volumes für andere Speicherklassen durch Festlegung begrenzen `<storage-class-name>.storageclass.storage.k8s.io/persistentvolumeclaims` Bis 0. Darüber hinaus muss ein Clusteradministrator sicherstellen, dass die Entwickler in einem Projekt keinen Zugriff haben, um die ResourceQuotas zu ändern.

Konfiguration

Bei mandantenfähigen Lösungen kann der Benutzer nicht auf mehr Cluster-Ressourcen zugreifen, als erforderlich ist. So sind alle Ressourcen, die als Teil der mandantenfähige Konfiguration konfiguriert werden müssen, in die Bereiche Cluster-Admin, Storage-Admin und Entwickler unterteilt, die an den einzelnen Projekten arbeiten.

In der folgenden Tabelle sind die verschiedenen Aufgaben aufgeführt, die von verschiedenen Benutzern ausgeführt werden müssen:

Rolle	Aufgaben
* Cluster-Admin*	Erstellung von Projekten für verschiedene Applikationen oder Workloads
	ClusterRoles and Roles Bindings für Storage-Admin erstellen
	Erstellen Sie Rollen und RolleBindungen für Entwickler, die bestimmten Projekten Zugriff zuweisen
	[Optional] Konfigurieren Sie Projekte, um PODs für bestimmte Nodes zu planen
* Storage-Admin*	SVMs auf NetApp ONTAP erstellen
	Erstellen von Trident Back-Ends
	Erstellen von StorageClasses
	Erstellen von Storage-RessourcenQuotas
Entwickler	Validieren des Zugriffs zum Erstellen oder Patchen von PVCs oder Pods im zugewiesenen Projekt
	Validieren des Zugriffs zum Erstellen oder Patchen von PVCs oder Pods in einem anderen Projekt
	Validieren des Zugriffs zum Anzeigen oder Bearbeiten von Projekten, ResourceQuotas und StorageClasses

Konfiguration

Voraussetzungen

- NetApp ONTAP Cluster
- Red hat OpenShift-Cluster
- Trident wird auf dem Cluster installiert
- Admin-Workstation mit installierten tridentctl- und oc-Tools, die zur €Pfad hinzugefügt wurden
- Administratorzugriff auf ONTAP
- Cluster-Admin-Zugriff auf OpenShift-Cluster
- Cluster ist mit Identity Provider integriert
- Der Identitätsanbieter ist so konfiguriert, dass er in verschiedenen Teams effizient zwischen Benutzern unterscheiden kann

Konfiguration: Aufgaben für den Cluster-Admin

Die folgenden Aufgaben werden vom Red hat OpenShift Cluster-Admin ausgeführt:

1. Melden Sie sich als Cluster-Administrator beim Red hat OpenShift-Cluster an.
2. Erstellen Sie zwei Projekte, die unterschiedlichen Projekten entsprechen.

```
oc create namespace project-1
oc create namespace project-2
```

3. Erstellen Sie die Entwicklerrolle für Projekt-1.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
      - replicationcontrollers
```

```
      - services
      - limitranges
      - namespaces
      - componentstatuses
      - nodes
  - verbs:
      - '*'
    apiGroups:
      - trident.netapp.io
    resources:
      - tridentsnapshots
EOF
```

Die in diesem Abschnitt angegebene Rollendefinition ist nur ein Beispiel. Entwicklerrollen müssen auf Basis von Anforderungen des Endanwenders definiert werden.

1. Erstellen Sie in ähnlicher Weise Entwicklerrollen für Project-2.
2. Alle OpenShift- und NetApp-Storage-Ressourcen werden in der Regel durch einen Storage-Administrator gemanagt. Der Zugriff für Storage-Administratoren wird durch die bei der Installation von Trident erstellte Trident-Rolle gesteuert. Darüber hinaus benötigt der Storage Administrator Zugriff auf ResourceQuotas, um den Storage-Verbrauch zu steuern.
3. Erstellen Sie eine Rolle zum Verwalten von ResourceQuotas in allen Projekten im Cluster, um sie an den Storage-Administrator anzuschließen.

```
cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - resourcequotas
  - verbs:
      - '*'
    apiGroups:
      - quota.openshift.io
    resources:
      - '*'
EOF
```

4. Stellen Sie sicher, dass der Cluster mit dem Identitätsanbieter der Organisation integriert ist und dass Benutzergruppen mit Clustergruppen synchronisiert werden. Das folgende Beispiel zeigt, dass der Identitäts-Provider in das Cluster integriert und mit den Benutzergruppen synchronisiert wurde.

```
$ oc get groups
NAME                          USERS
ocp-netapp-storage-admins     ocp-netapp-storage-admin
ocp-project-1                 ocp-project-1-user
ocp-project-2                 ocp-project-2-user
```

1. Clusterrollenbinden für Storage-Administratoren konfigurieren.

```
cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF
```

Für Storage-Administratoren müssen zwei Rollen gebunden sein: trident-Operator und Ressourcen-Quotas.

1. Erstellen Sie RoleBindungen für Entwickler, die die Rolle Entwickler-Projekt-1 an die entsprechende Gruppe (ocp-Projekt-1) in Projekt-1 binden.

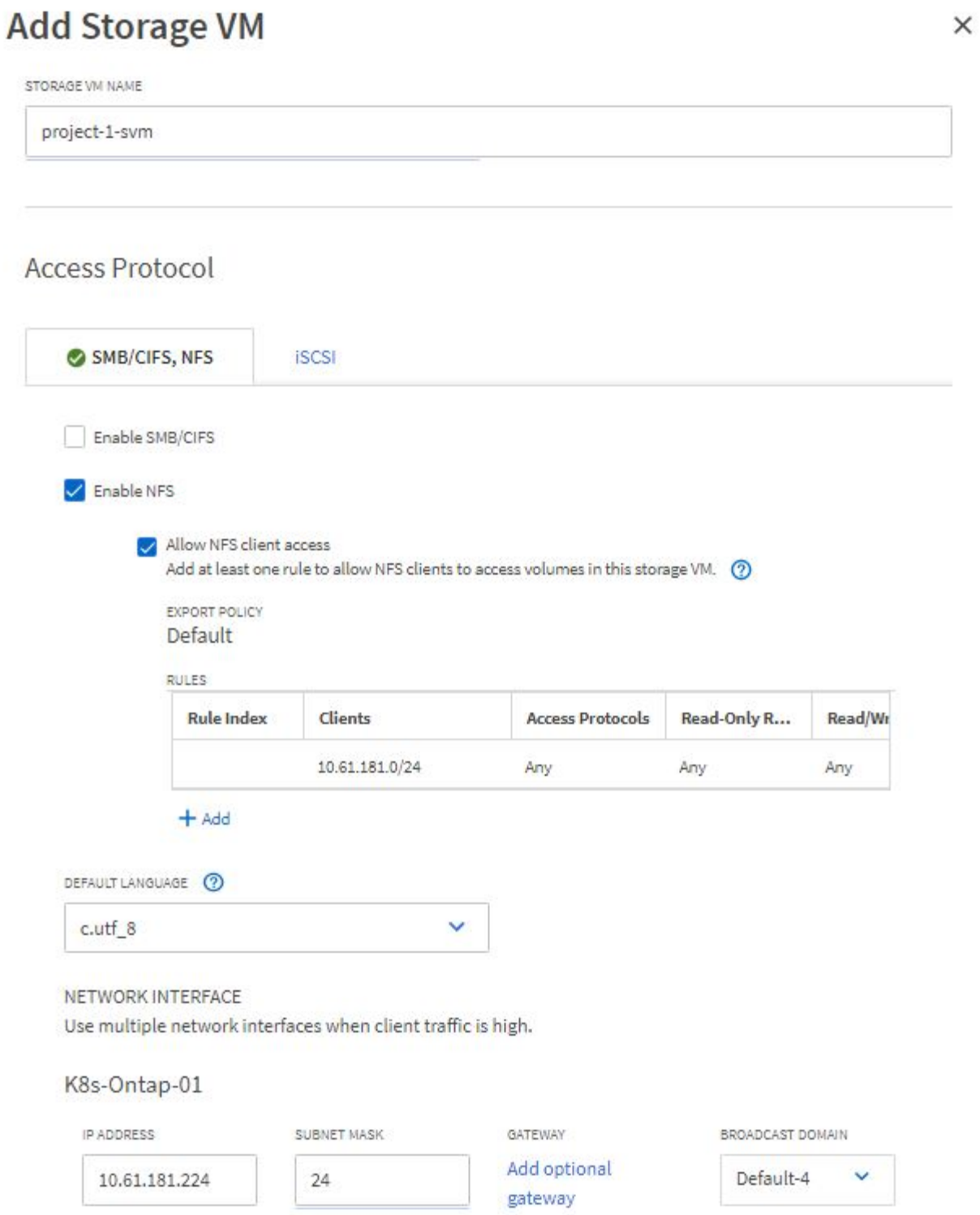
```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF
```

2. Erstellen Sie in Projekt-2 auch Rollen für Entwickler, die die Entwicklerrollen an die entsprechende Benutzergruppe binden.

Konfiguration: Storage-Admin-Aufgaben

Die folgenden Ressourcen müssen von einem Storage-Administrator konfiguriert werden:

1. Melden Sie sich als Administrator bei dem NetApp ONTAP Cluster an.
2. Navigieren Sie zu Storage > Storage VMs, und klicken Sie auf Hinzufügen. Erstellen Sie zwei SVMs, eine für Projekt-1 und die andere für Projekt-2, indem Sie die erforderlichen Details angeben. Erstellen Sie außerdem ein vsadmin-Konto, um die SVM und ihre Ressourcen zu managen.



1. Melden Sie sich als Storage-Administrator beim Red hat OpenShift-Cluster an.
2. Erstellen Sie das Back-End für Projekt-1, und ordnen Sie es der dem Projekt zugewiesenen SVM zu. NetApp empfiehlt, das vsadmin Konto des SVM zu verwenden, um das Back-End mit SVM zu verbinden, anstatt den ONTAP-Cluster-Administrator zu verwenden.

```
cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_1",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.224",
    "svm": "project-1-svm",
    "username": "vsadmin",
    "password": "NetApp123"
}
EOF
```

In diesem Beispiel verwenden wir den ontap-nas-Treiber. Verwenden Sie den entsprechenden Treiber, wenn Sie das Backend basierend auf dem Anwendungsfall erstellen.

Wir gehen davon aus, dass Trident im Projekt Trident installiert wird.

1. Ähnliches Erstellen des Trident-Back-End für Projekt-2 und Zuordnen dieses zu Projekt-2 zu der SVM.
2. Erstellen Sie dann die Speicherklassen. Erstellen Sie die Storage-Klasse für Projekt-1, und konfigurieren Sie sie so, dass die Speicherpools vom Backend für Projekt-1 verwendet werden, indem Sie den StoragePools-Parameter einstellen.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF
```

3. Erstellen Sie ebenso eine Storage-Klasse für Projekt-2, und konfigurieren Sie sie so, dass die Speicherpools vom Backend für Projekt-2 verwendet werden.
4. Erstellen Sie ein ResourceQuota zur Einschränkung von Ressourcen im Projekt-1, in dem Storage aus Storage-Storage für andere Projekte angefordert wird.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

5. Erstellen Sie auch ein ResourceQuota zur Einschränkung von Ressourcen in Projekt-2, bei dem Storage aus Storage-Storage für andere Projekte angefordert wird.

Validierung

Führen Sie die folgenden Schritte aus, um die mandantenfähige Architektur zu validieren, die in den vorherigen Schritten konfiguriert wurde:

Validieren des Zugriffs zur Erstellung von VES oder Pods im zugewiesenen Projekt

1. Melden Sie sich als ocp-Project-1-user an, Entwickler in Projekt-1.
2. Überprüfen Sie den Zugriff, um ein neues Projekt zu erstellen.

```
oc create ns sub-project-1
```

3. Erstellen Sie in Projekt-1 ein PVC mit der Speicherklasse, die Projekt-1 zugewiesen ist.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Überprüfen Sie das mit der PVC verbundene PV.

```
oc get pv
```

5. Überprüfen, ob das PV und sein Volume in einer für Projekt-1 auf NetApp ONTAP dedizierten SVM erstellt werden.

```
volume show -vserver project-1-svm
```

6. Erstellen Sie im Projekt-1 einen Pod, und mounten Sie den im vorherigen Schritt erstellten PVC.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
       claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: test-pvc-project-1
EOF
```

7. Überprüfen Sie, ob der POD läuft und ob er das Volume montiert hat.

```
oc describe pods test-pvc-pod -n project-1
```

Validieren des Zugriffs zur Erstellung von PVCs oder Pods in einem anderen Projekt oder Verwenden von Ressourcen für ein anderes Projekt

1. Melden Sie sich als ocp-Project-1-user an, Entwickler in Projekt-1.
2. Erstellen Sie in Projekt-1 ein PVC mit der Lagerhalle, die Projekt-2 zugewiesen ist.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF
```

3. PVC in Projekt-2 erstellen.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Stellen Sie sicher, dass PVCs vorhanden sind `test-pvc-project-1-sc-2` Und `test-pvc-project-2-sc-1` Wurden nicht erstellt.

```
oc get pvc -n project-1
oc get pvc -n project-2
```

5. Erstellen eines Pods in Projekt-2.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
EOF
```

Validieren des Zugriffs zum Anzeigen und Bearbeiten von Projekten, ResourceQuotas und StorageClasses

1. Melden Sie sich als ocp-Project-1-user an, Entwickler in Projekt-1.
2. Zugriff prüfen, um neue Projekte zu erstellen.

```
oc create ns sub-project-1
```

3. Validieren des Zugriffs auf Projekte

```
oc get ns
```

4. Überprüfen Sie, ob der Benutzer ResourceQuotas in Projekt-1 anzeigen oder bearbeiten kann.

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. Überprüfen Sie, ob der Benutzer Zugriff hat, um die Speicherageklösse anzuzeigen.

```
oc get sc
```

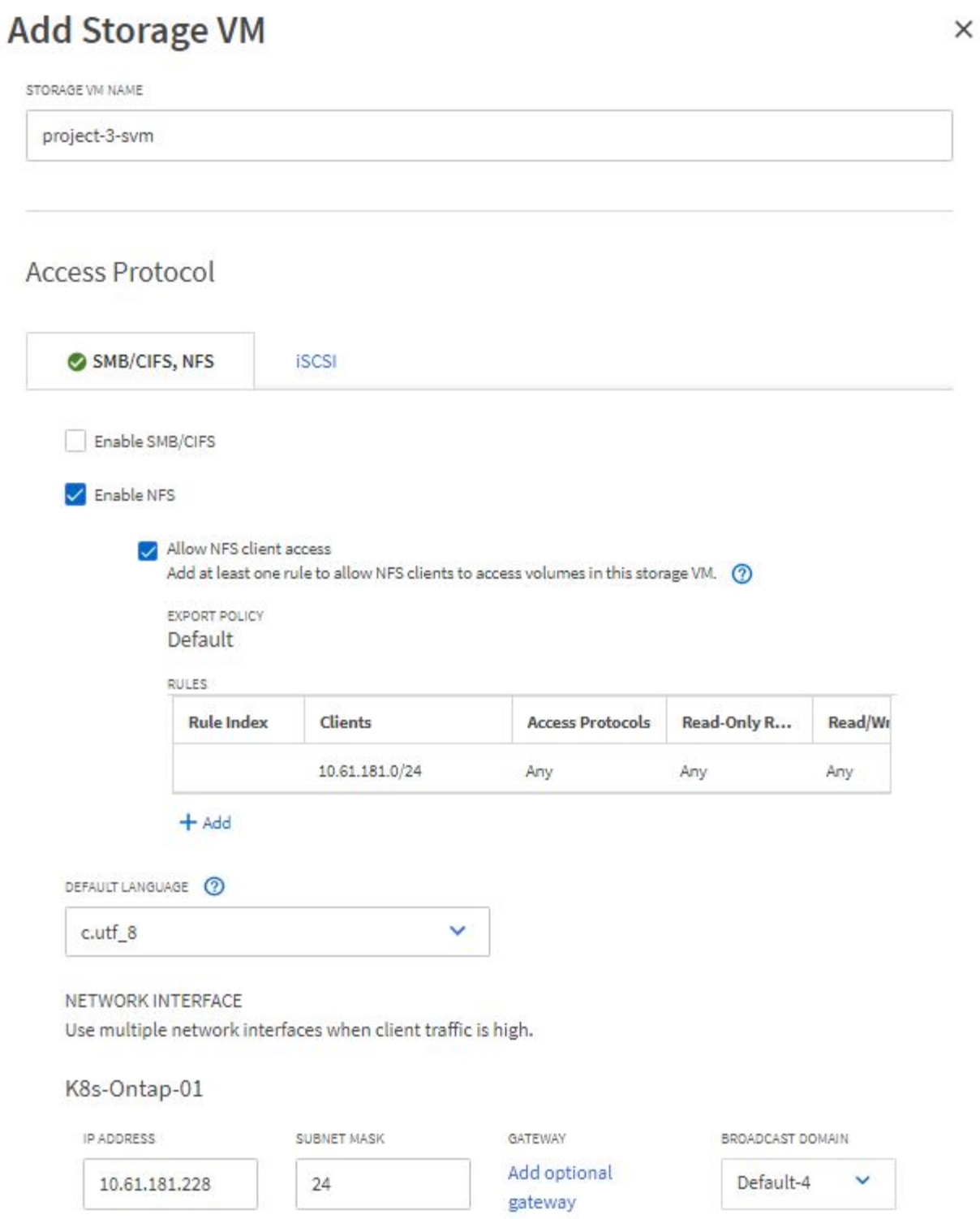
6. Überprüfen Sie den Zugriff, um die Lagerflächen zu beschreiben.
7. Validieren Sie den Zugriff des Benutzers, um die Speicherageclasses zu bearbeiten.

```
oc edit sc project-1-sc
```

Skalierung: Mehr Projekte hinzufügen

In einer mandantenfähigen Konfiguration erfordert das Hinzufügen neuer Projekte mit Storage-Ressourcen eine zusätzliche Konfiguration, um sicherzustellen, dass Mandantenfähigkeit nicht verletzt wird. Gehen Sie wie folgt vor, um weitere Projekte in einem mandantenfähigen Cluster hinzuzufügen:

1. Melden Sie sich als Storage-Administrator beim NetApp ONTAP Cluster an.
2. Navigieren Sie zu `Storage` → `Storage VMs` Und klicken `Add`. Erstellen Sie eine neue SVM für Projekt-3. Erstellen Sie außerdem ein vsadmin-Konto, um die SVM und ihre Ressourcen zu managen.



1. Melden Sie sich als Clusteradministrator beim Red hat OpenShift Cluster an.
2. Erstellen Sie ein neues Projekt.

```
oc create ns project-3
```

3. Stellen Sie sicher, dass die Benutzergruppe für Projekt-3 auf IdP erstellt und mit dem OpenShift-Cluster

synchronisiert wird.

```
oc get groups
```

4. Die Entwicklerrolle für Project-3 erstellen.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
```

```
      - replicationcontrollers
      - services
      - limitranges
      - namespaces
      - componentstatuses
      - nodes
  - verbs:
      - '*'
    apiGroups:
      - trident.netapp.io
    resources:
      - tridentsnapshots
EOF
```

Die in diesem Abschnitt angegebene Rollendefinition ist nur ein Beispiel. Die Entwicklerrolle muss basierend auf den Anforderungen des Endbenutzers definiert werden.

1. Erstellen Sie RoleBending für Entwickler in Project-3, um die Rolle Developer-project-3 an die entsprechende Gruppe (ocp-project-3) in Projekt-3 zu binden.

```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF
```

2. Melden Sie sich als Storage-Administrator beim Red hat OpenShift-Cluster an
3. Erstellen Sie ein Trident-Back-End und ordnen Sie es der für Projekt-3 dedizierten SVM zu. NetApp empfiehlt, das vsadmin Konto des SVM zu verwenden, um das Backend mit der SVM zu verbinden, anstatt den ONTAP-Cluster-Administrator zu verwenden.

```
cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_3",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.228",
    "svm": "project-3-svm",
    "username": "vsadmin",
    "password": "NetApp!23"
}
EOF
```

> In diesem Beispiel verwenden wir den ontap-nas-Treiber. Verwenden Sie den entsprechenden Treiber, um das Backend basierend auf dem Anwendungsfall zu erstellen.

> Wir gehen davon aus, dass Trident im Projekt Trident installiert wird.

1. Erstellen Sie die Storage-Klasse für Projekt-3, und konfigurieren Sie sie so, dass die Speicherpools vom Back-End für Projekt-3 verwendet werden.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF
```

2. Erstellen Sie ein ResourceQuota zur Einschränkung von Ressourcen im Projekt-3, in dem Storage aus Storage-Speicherageclasses für andere Projekte angefordert wird.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

3. Patchen Sie die ResourceQuotas in anderen Projekten, um Ressourcen in diesen Projekten vom Zugriff auf den Speicher aus der für Projekt-3 vorgesehenen Speicherklasse zu beschränken.

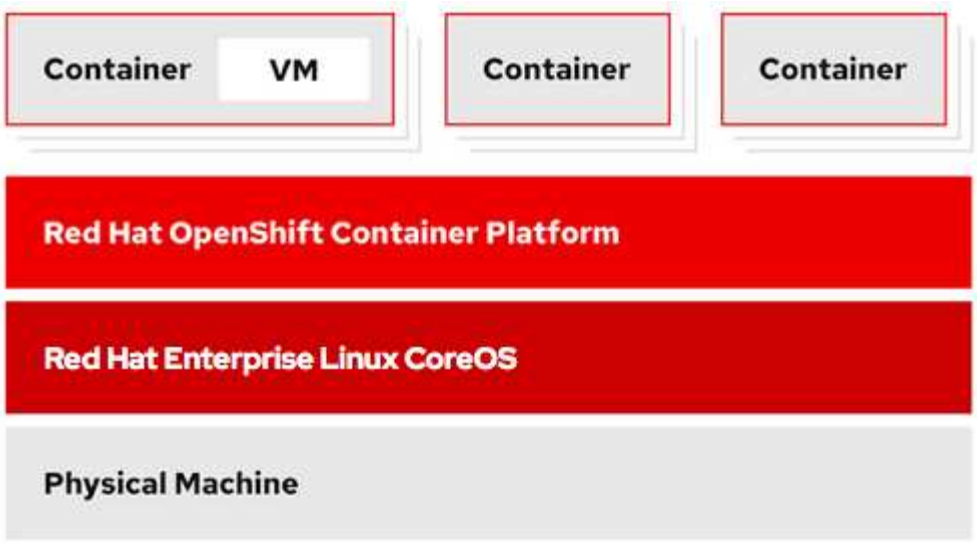
```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
```

Red hat OpenShift Virtualisierung mit NetApp ONTAP

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 VMs-Festplatten, VM-Snapshots usw. werden auch von der OpenShift Virtualization mit Unterstützung von Astra Trident unterstützt, wenn die NetApp ONTAP unterstützt wird. 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".

Bereitstellung für OpenShift Virtualization

Implementieren Sie eine Virtualisierung mit Red hat OpenShift mit NetApp ONTAP

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
- Astra Trident ist auf dem OpenShift-Cluster installiert
- Ein Trident Back-End, das mit einer SVM auf ONTAP Cluster konfiguriert ist
- StorageClass: Ist auf dem OpenShift-Cluster mit Astra Trident als bereitstellungsunternehmen konfiguriert
- 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.

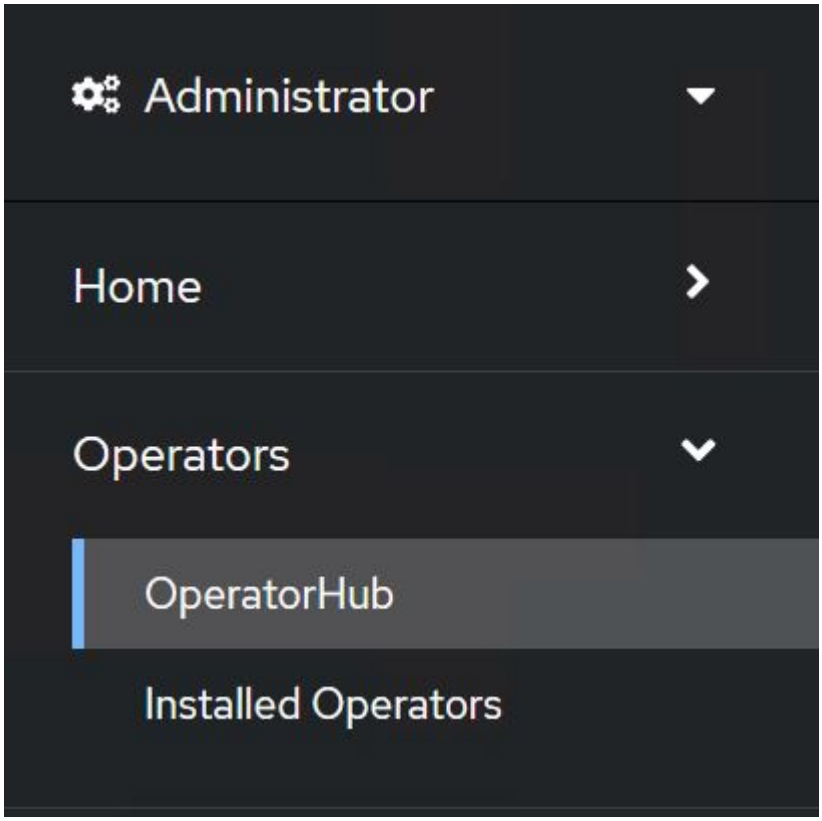
Optional können Sie auch einen Teilbereich der OpenShift-Cluster-Nodes angeben, um die OpenShift-Virtualisierungsbetreiber, -Controller und -VMs zu hosten, indem Sie die Regeln für die Knotenplatzierung konfigurieren. Befolgen Sie die Dokumentation, um die Regeln für die Knotenplatzierung für OpenShift 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.

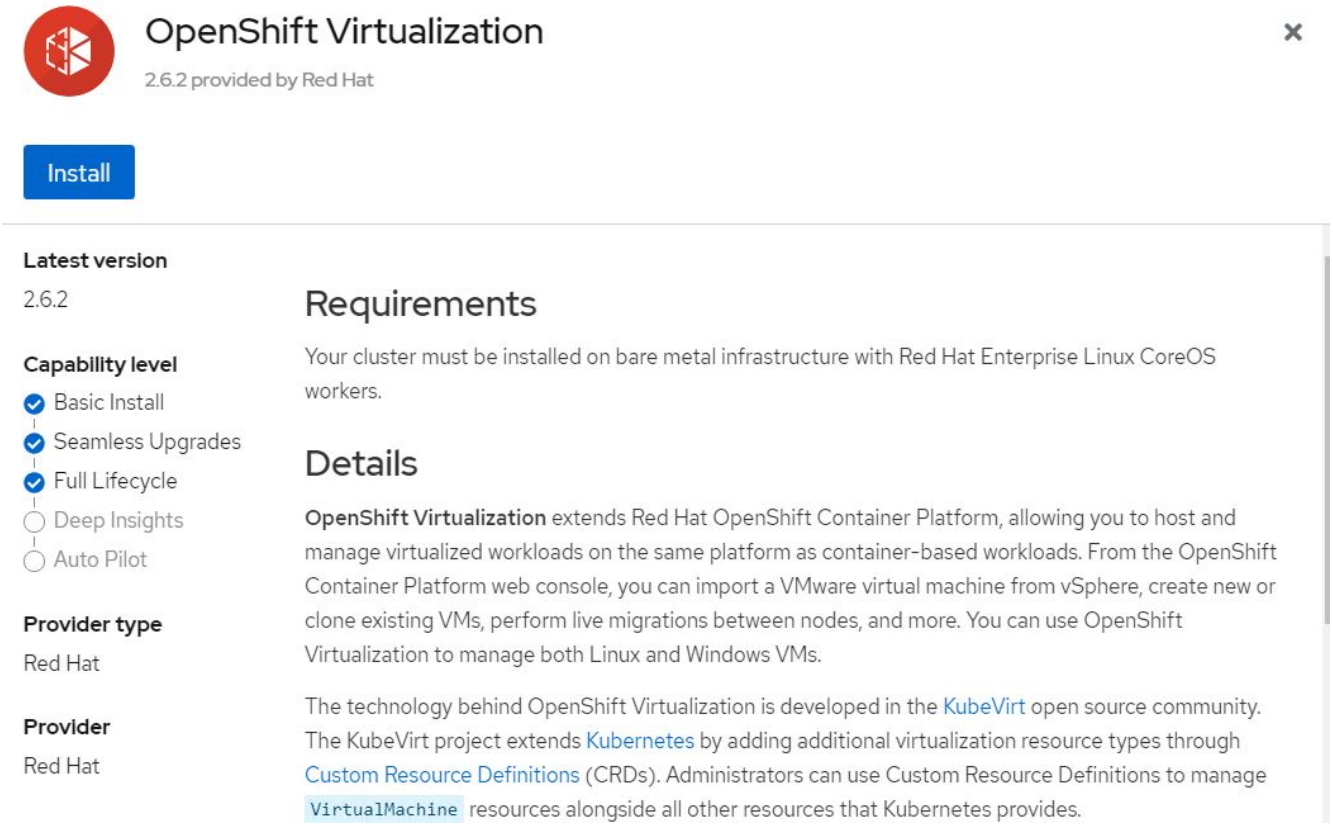
Implementieren Sie eine Virtualisierung mit Red hat OpenShift mit NetApp ONTAP

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

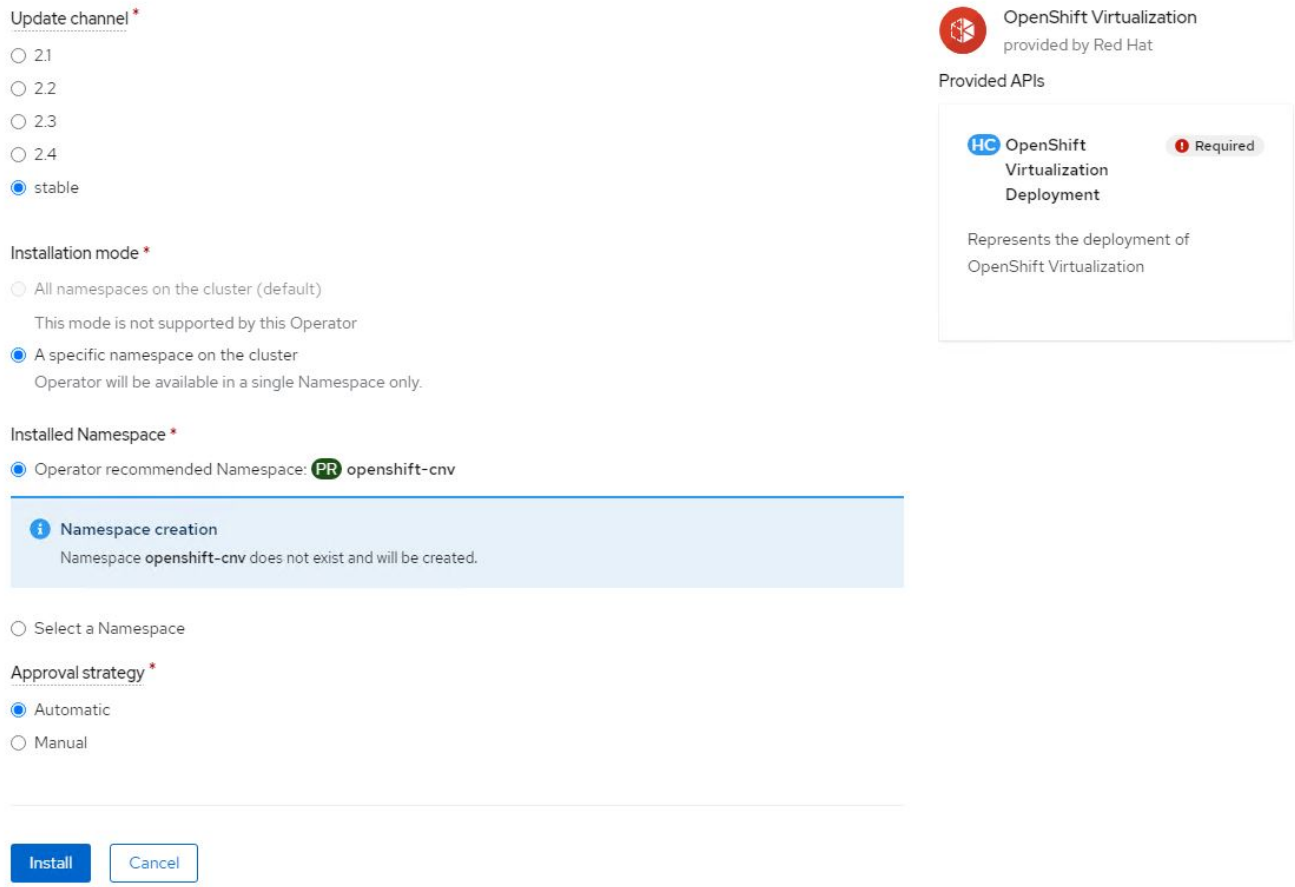
1. Melden Sie sich beim Bare-Metal-Cluster Red hat OpenShift mit Zugriff auf den Cluster-Administrator an.
2. Wählen Sie in der Dropdown-Liste Perspektive den Eintrag Administrator aus.
3. Navigieren Sie zu Operators > OperatorHub, und suchen Sie nach OpenShift Virtualization.



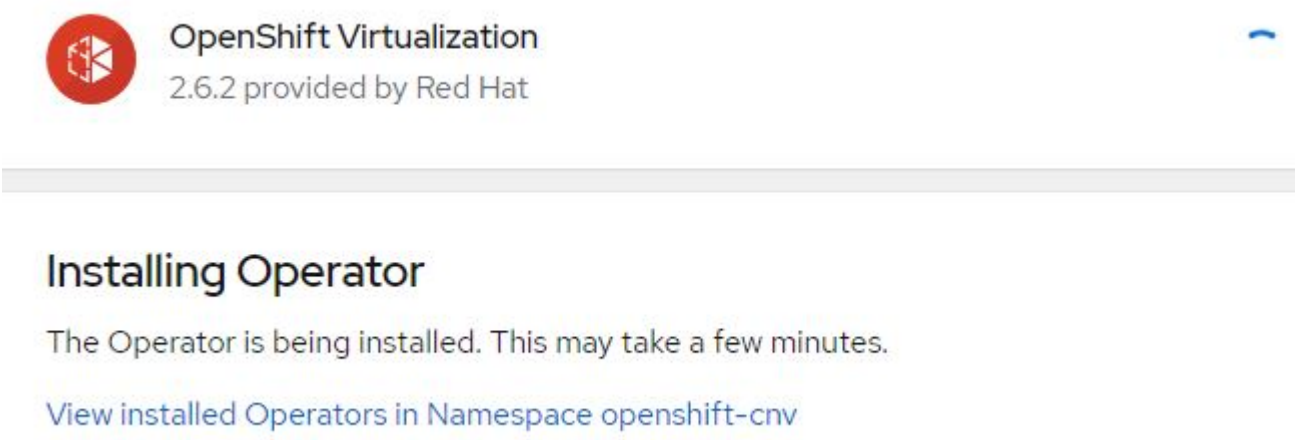
4. Wählen Sie die Kachel OpenShift Virtualization aus, und klicken Sie auf Installieren.



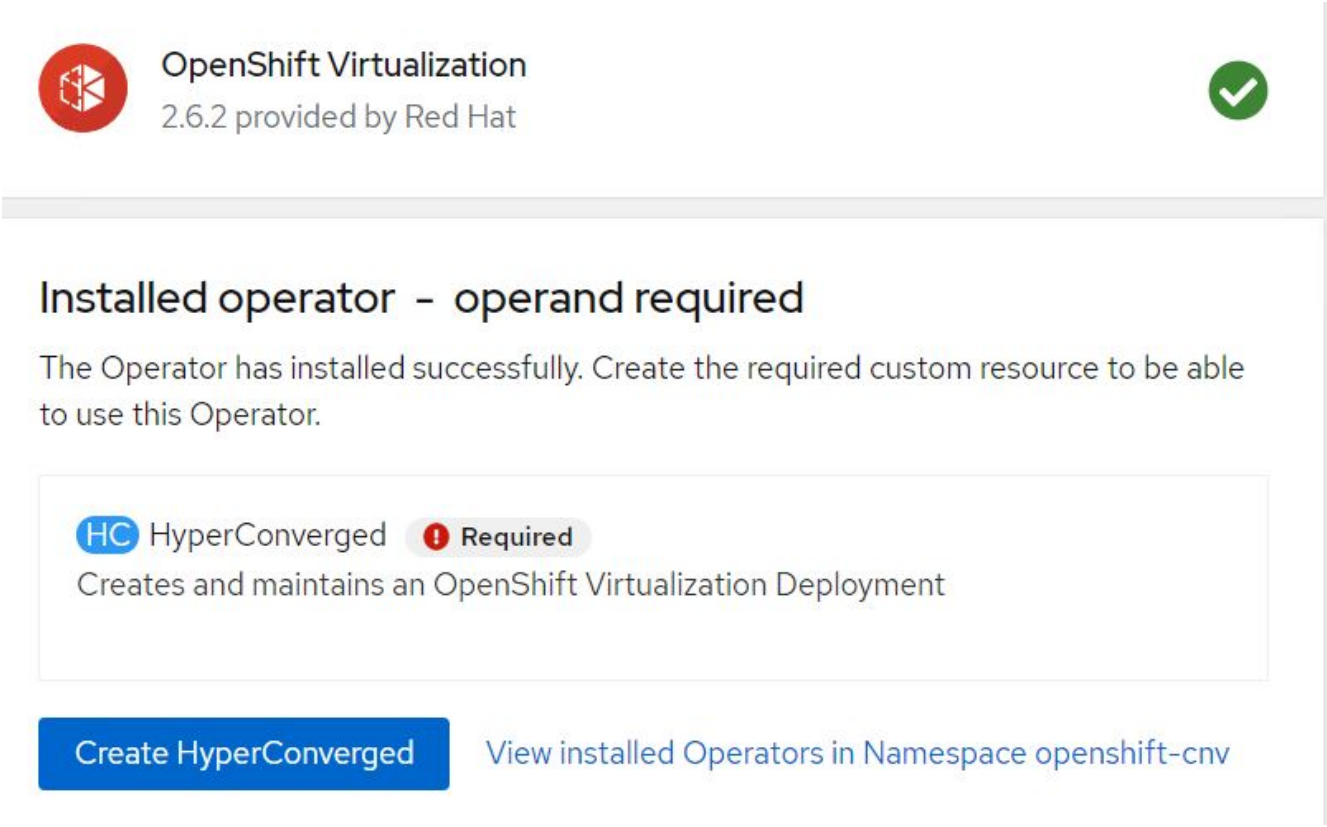
5. Lassen Sie auf dem Bildschirm Install Operator alle Standardparameter stehen, und klicken Sie auf Install.



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



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



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 *

kubevirt-hyperconverged

Labels

app=frontend

Infra

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarely 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.

Create Cancel

9. 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 Search by name...

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

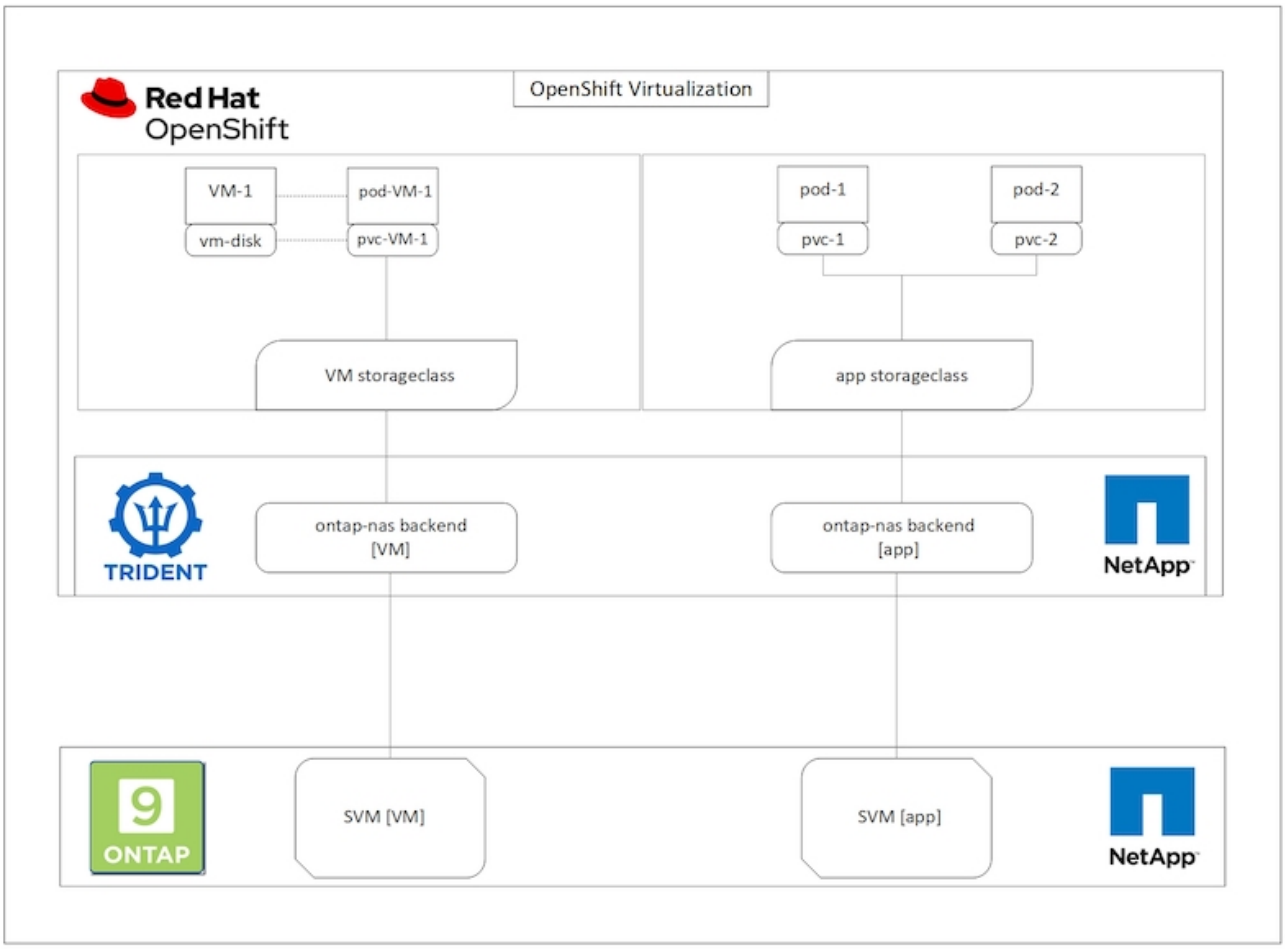
Workflows

Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

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.



Gehen Sie wie folgt vor, um eine virtuelle Maschine im OpenShift-Cluster zu erstellen:

1. Navigieren Sie zu Workloads > Virtualisierung > Virtuelle Maschinen, und klicken Sie auf Erstellen > mit Assistenten.
2. Wählen Sie das gewünschte Betriebssystem aus, und klicken Sie auf Weiter.
3. Wenn für das ausgewählte Betriebssystem keine Startquelle konfiguriert ist, müssen Sie es konfigurieren. Wählen Sie unter „Startquelle“ aus, ob Sie das BS-Image aus einer URL oder aus einer Registrierung importieren möchten, und geben Sie die entsprechenden Details an. Erweitern Sie Advanced und wählen Sie die Trident-gestützte StorageClass aus. Klicken Sie anschließend auf Weiter.

Boot source

This template does not have a boot source. Provide a custom boot source for this **CentOS 8.0+ VM** virtual machine.

Boot source type *

Import via URL (creates PVC)

Import URL *

https://access.cdn.redhat.com/content/origin/files/sha256/58/588167f828001e57688ec4b9b31c11a59d532489f527488ebc89ac5e952...

Example: For RHEL, visit the **RHEL download page** (requires login) and copy the download link URL of the KVM guest image

☑ Mount this as a CD-ROM boot source

Persistent Volume Claim size *

5 GiB

Ensure your PVC size covers the requirements of the uncompressed image and any other space requirements. More storage can be added later.

Advanced

Storage class *

basic (default)

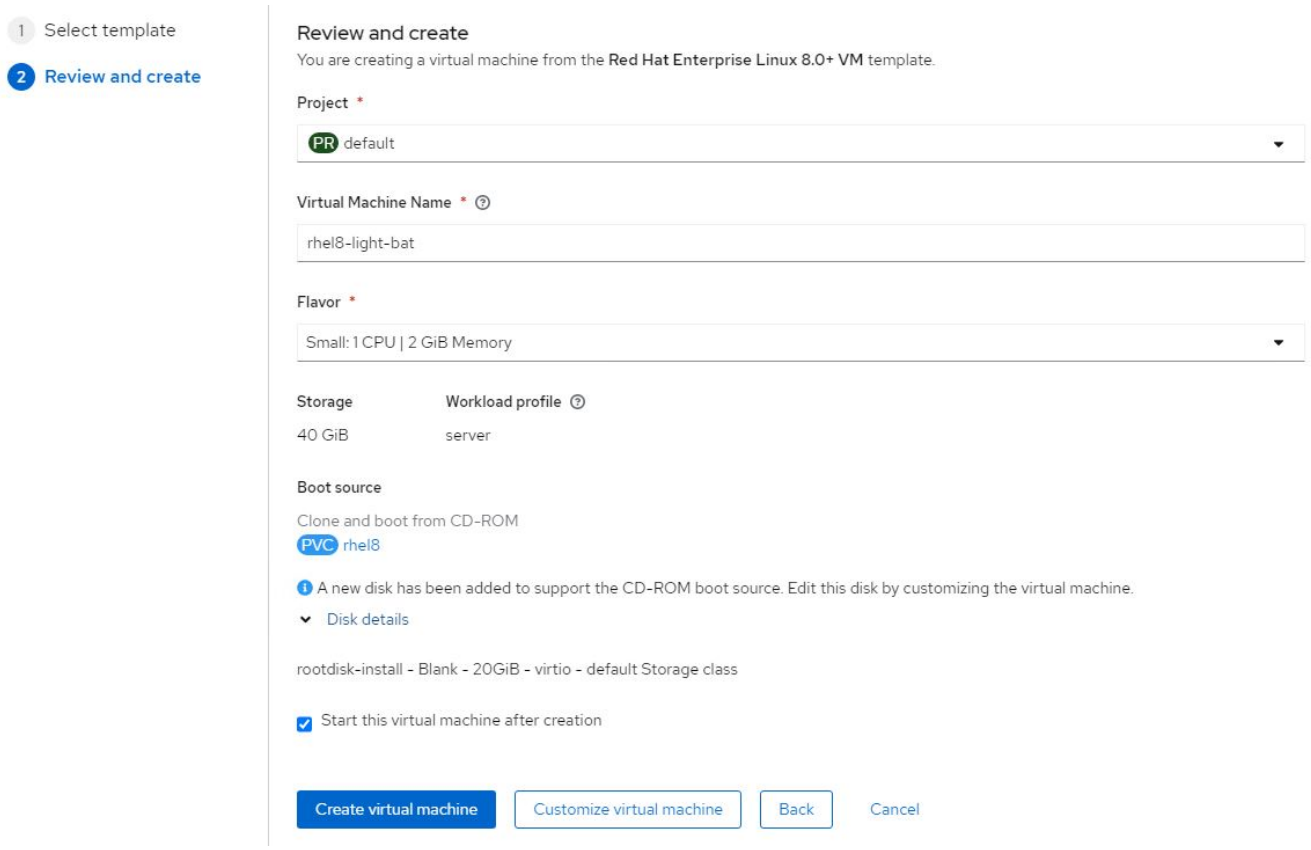
Access mode *

Single User (RWO)

Volume mode *

Filesystem

4. Wenn für das ausgewählte Betriebssystem bereits eine Startquelle konfiguriert ist, kann der vorherige Schritt übersprungen werden.
5. Wählen Sie im Bereich „Prüfen und Erstellen“ das Projekt aus, in dem Sie die VM erstellen möchten, und geben Sie die VM-Details an. Vergewissern Sie sich, dass die Startquelle für den Klon- und Bootvorgang von CD-ROM ausgewählt ist, wobei die entsprechende PVC für das ausgewählte Betriebssystem zugewiesen ist.



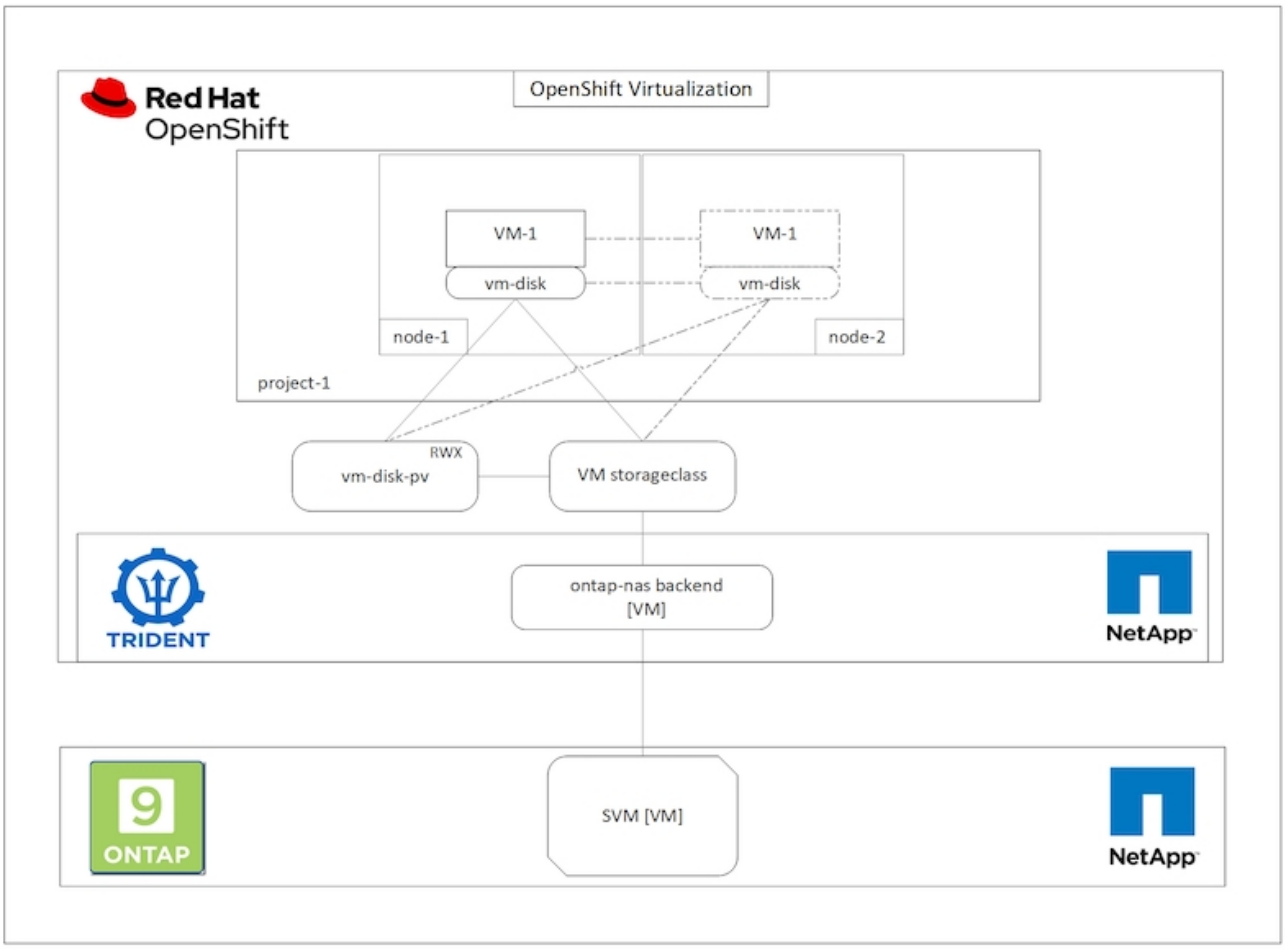
6. Wenn Sie die virtuelle Maschine anpassen möchten, klicken Sie auf Virtuelle Maschine anpassen und ändern Sie die erforderlichen Parameter.
7. Klicken Sie auf Virtual Machine erstellen, um die virtuelle Maschine zu erstellen. Dadurch wird ein entsprechender Pod im Hintergrund bereitgestellt.

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 VES werden dann geklont und als RootDisks an virtuelle Maschinen angehängt, wenn sie mit den entsprechenden Vorlagen in einem Projekt erstellt werden.

Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

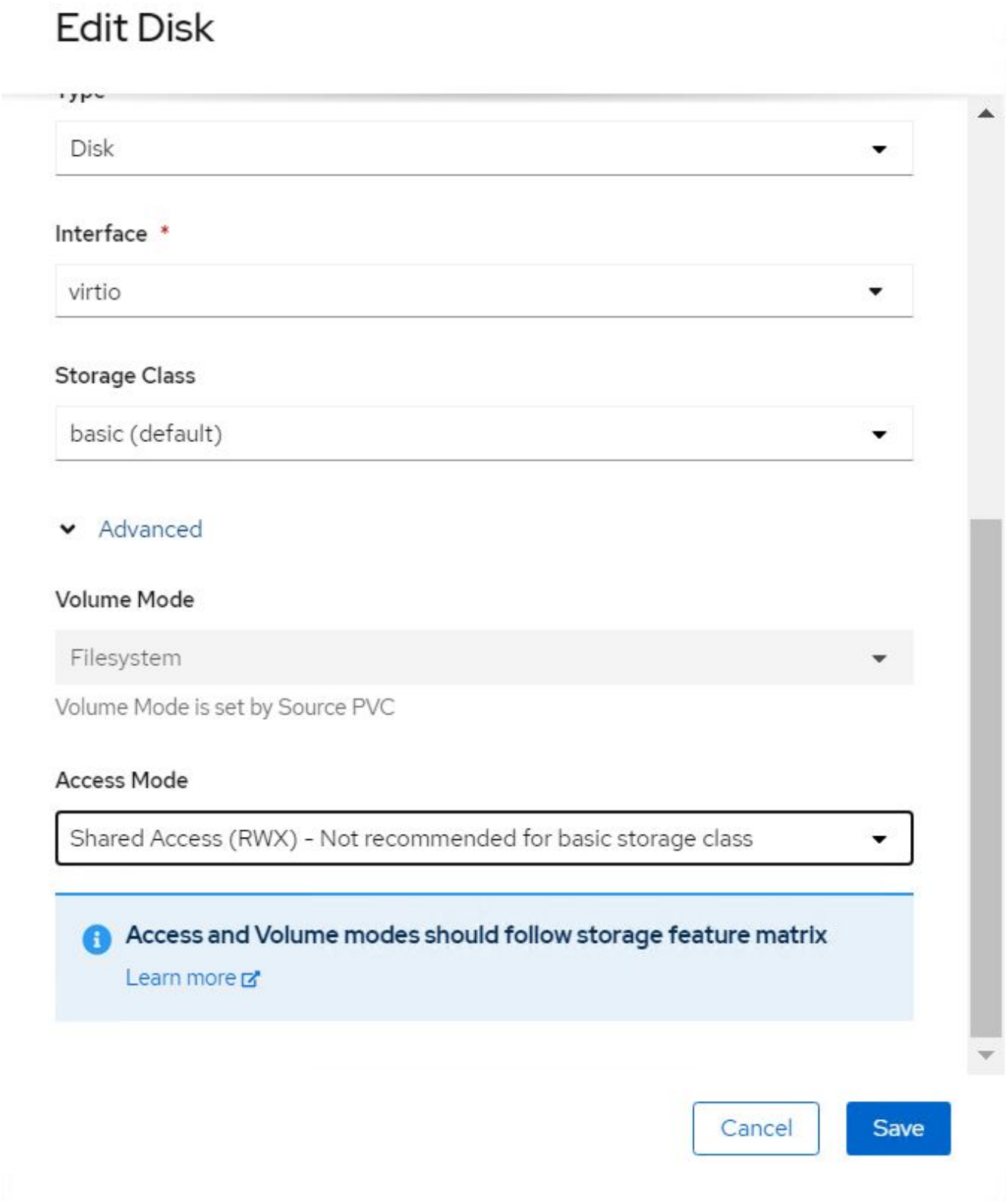
VM-Live-Migration

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. Astra Trident Back-End ist mit einer SVM auf einem NetApp ONTAP-Cluster konfiguriert, der für das NFS-Protokoll aktiviert ist und Shared ReadWriteViele Zugriffsmöglichkeiten für PVCs unterstützt. Daher können VMs mit PVCs, die über von Trident über NFS-fähige SVM bereitgestellt werden, ohne Ausfallzeiten migriert werden.



So erstellen Sie eine VM, die an PVCs mit gemeinsam genutzten ReadWriteViele Zugriffsmöglichkeiten gebunden ist:

1. Navigieren Sie zu Workloads > Virtualisierung > Virtuelle Maschinen, und klicken Sie auf Erstellen > mit Assistenten.
2. Wählen Sie das gewünschte Betriebssystem aus, und klicken Sie auf Weiter. Nehmen wir an, dass auf dem ausgewählten Betriebssystem bereits eine Startquelle konfiguriert war.
3. Wählen Sie im Bereich „Prüfen und Erstellen“ das Projekt aus, in dem Sie die VM erstellen möchten, und geben Sie die VM-Details an. Vergewissern Sie sich, dass die Startquelle für den Klon- und Bootvorgang von CD-ROM ausgewählt ist, wobei die entsprechende PVC für das ausgewählte Betriebssystem zugewiesen ist.
4. Klicken Sie auf Virtual Machine anpassen und dann auf Storage.
5. Klicken Sie auf die Ellipsen neben der Rootdisk, und stellen Sie sicher, dass die mit Trident bereitgestellte Speicheraglass ausgewählt ist. Erweitern Sie den Eintrag Erweitert, und wählen Sie für den Zugriffsmodus den Eintrag Shared Access (RWX) aus. Klicken Sie dann auf Speichern.



6. Klicken Sie auf Überprüfen und bestätigen und dann auf Virtuelle Maschine erstellen.

Gehen Sie wie folgt vor, um eine VM manuell auf einen anderen Knoten im OpenShift-Cluster zu migrieren.

1. Navigieren Sie zu Workloads > Virtualisierung > Virtual Machines.

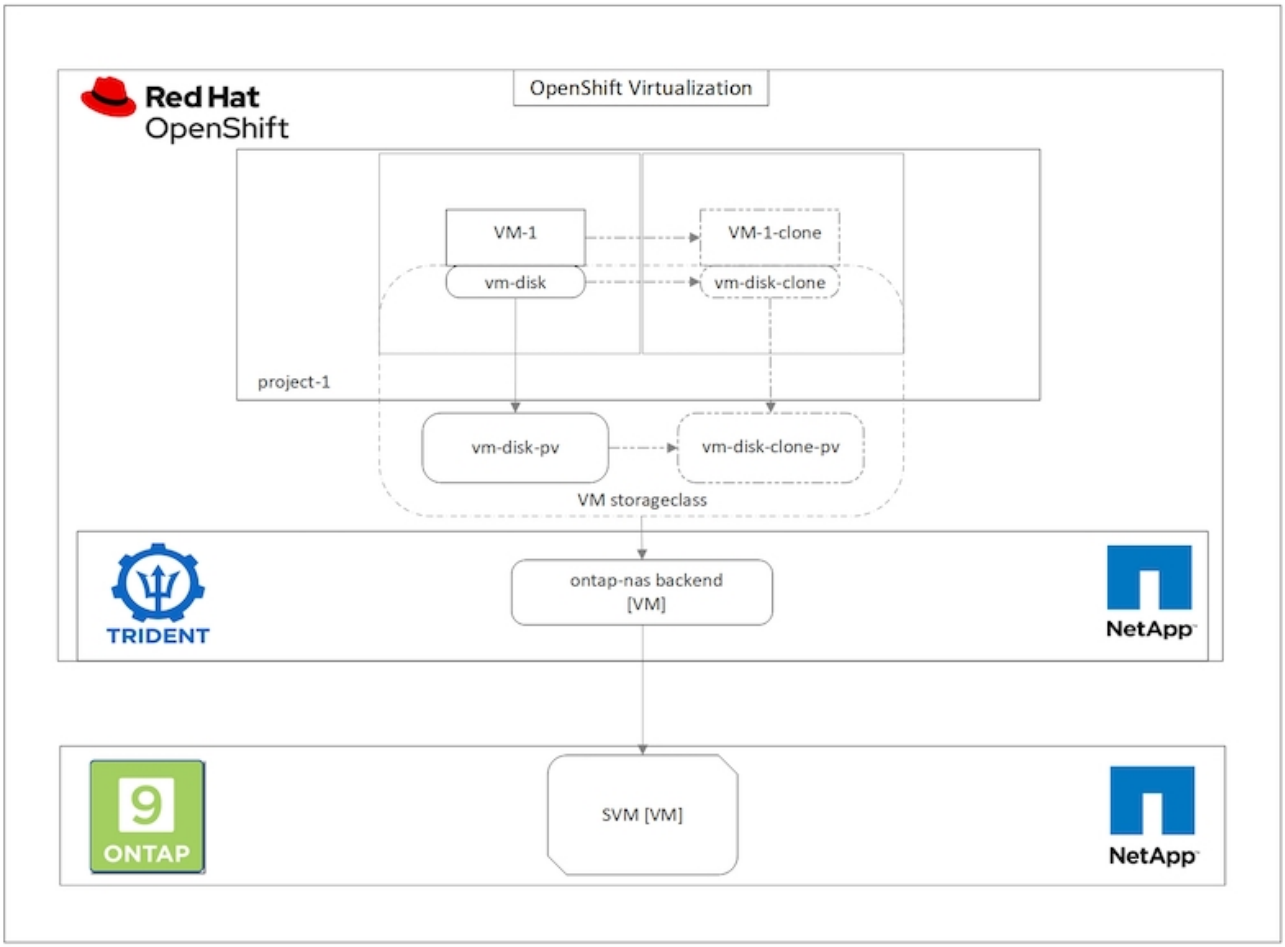
2. Klicken Sie für die zu migrierenden VMs auf die Auslassungspunkte, und klicken Sie dann auf die Virtual Machine migrieren.
3. Klicken Sie auf Migrieren, wenn die Meldung angezeigt wird, um zu bestätigen.

> 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

Klonen von VMs

Das Klonen einer vorhandenen VM in OpenShift wird durch die Unterstützung der Funktion „Volume CSI“ von Astra Trident ermöglicht. 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.

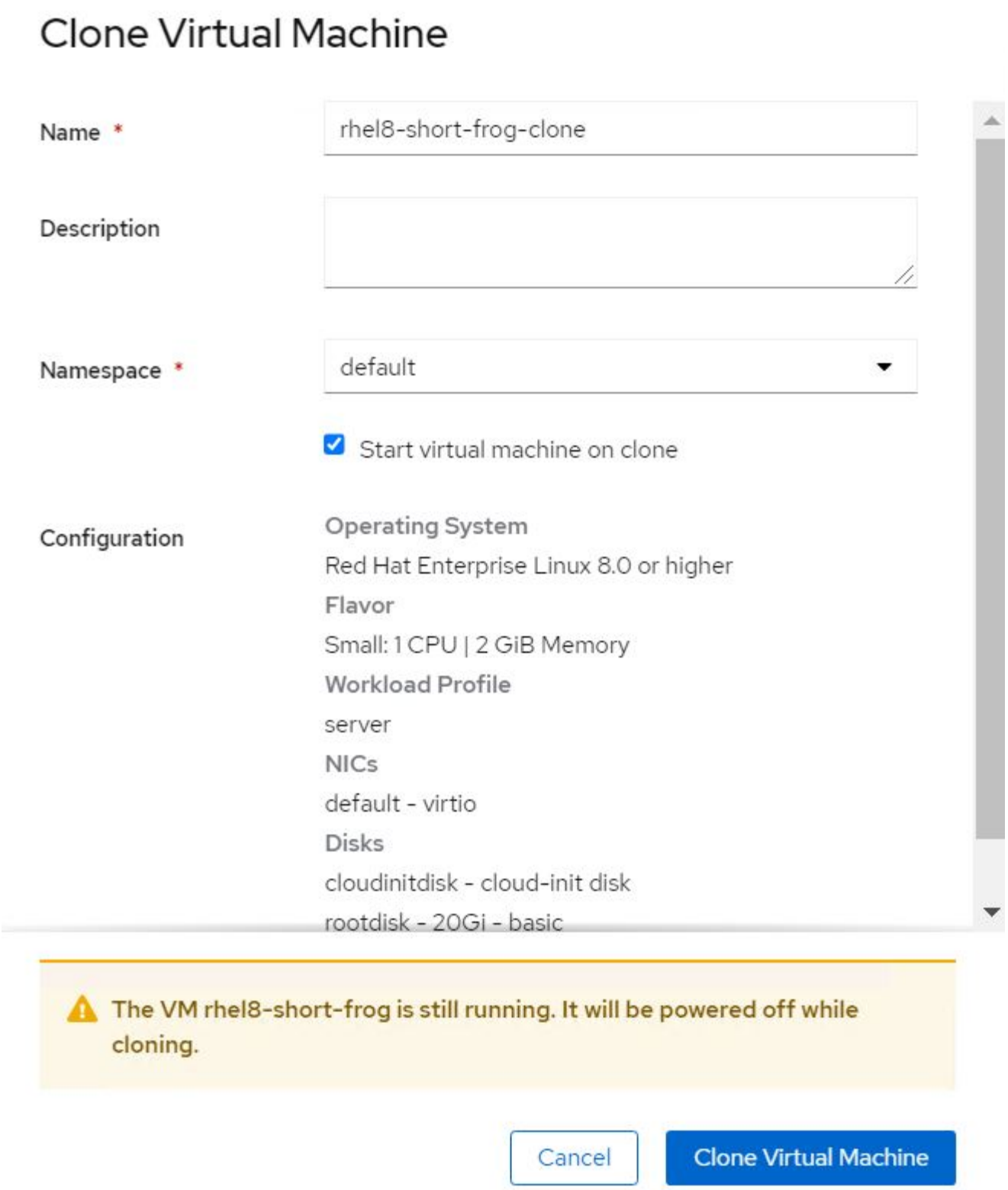
VMs in einem OpenShift-Cluster können auf zwei Arten geklont werden:

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

Durch Herunterfahren der Quell-VM

Das Klonen einer vorhandenen VM durch das Herunterfahren der VM ist eine native OpenShift-Funktion, die mit Unterstützung von Astra 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.

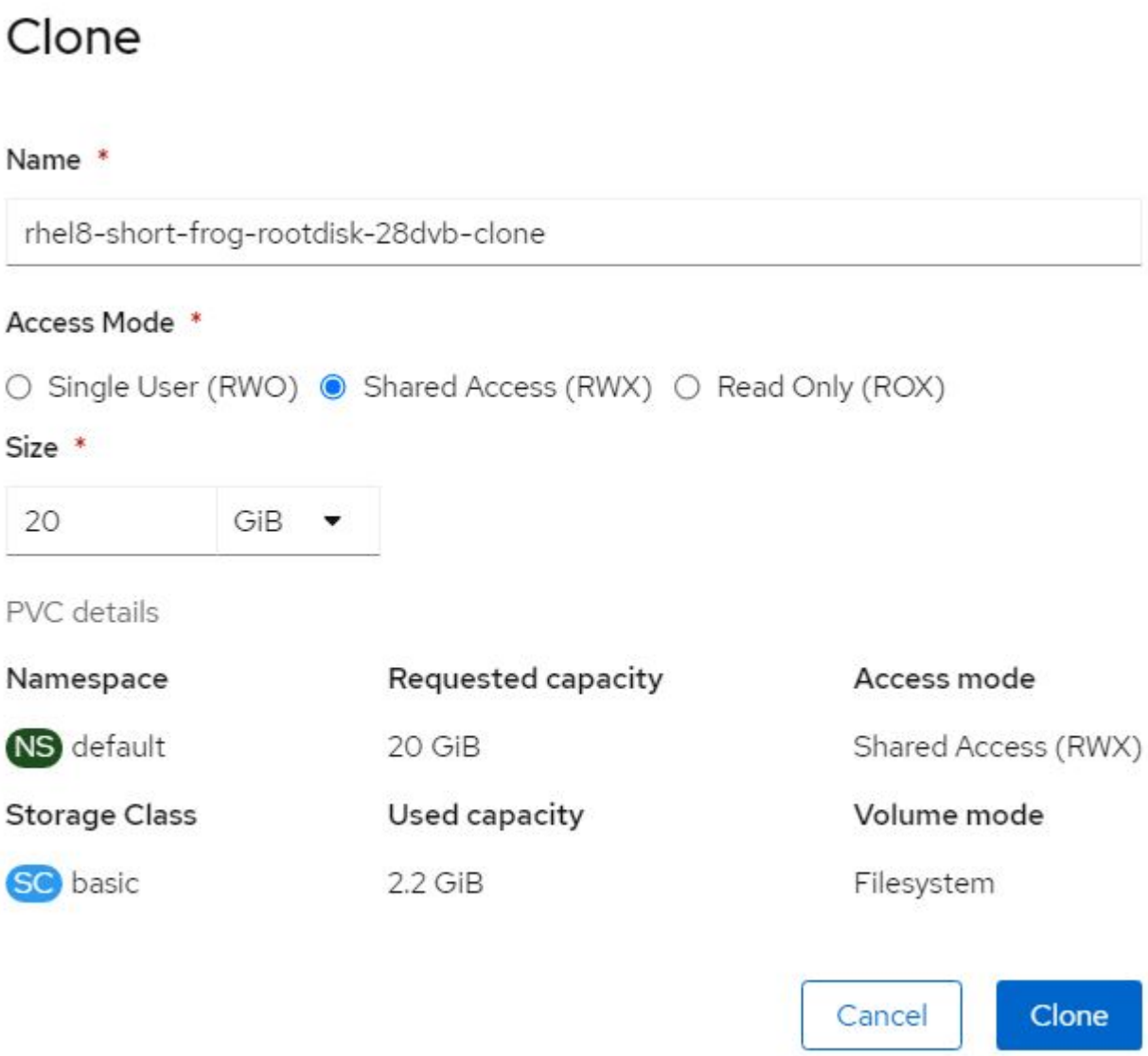


3. Klicken Sie auf Virtual Machine klonen. Dadurch wird die Quell-VM heruntergefahren und die Erstellung der Klon-VM initiiert.
4. Nach Abschluss dieses Schritts können Sie auf den Inhalt der geklonten VM zugreifen und diesen überprüfen.

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.



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-28dvb-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.

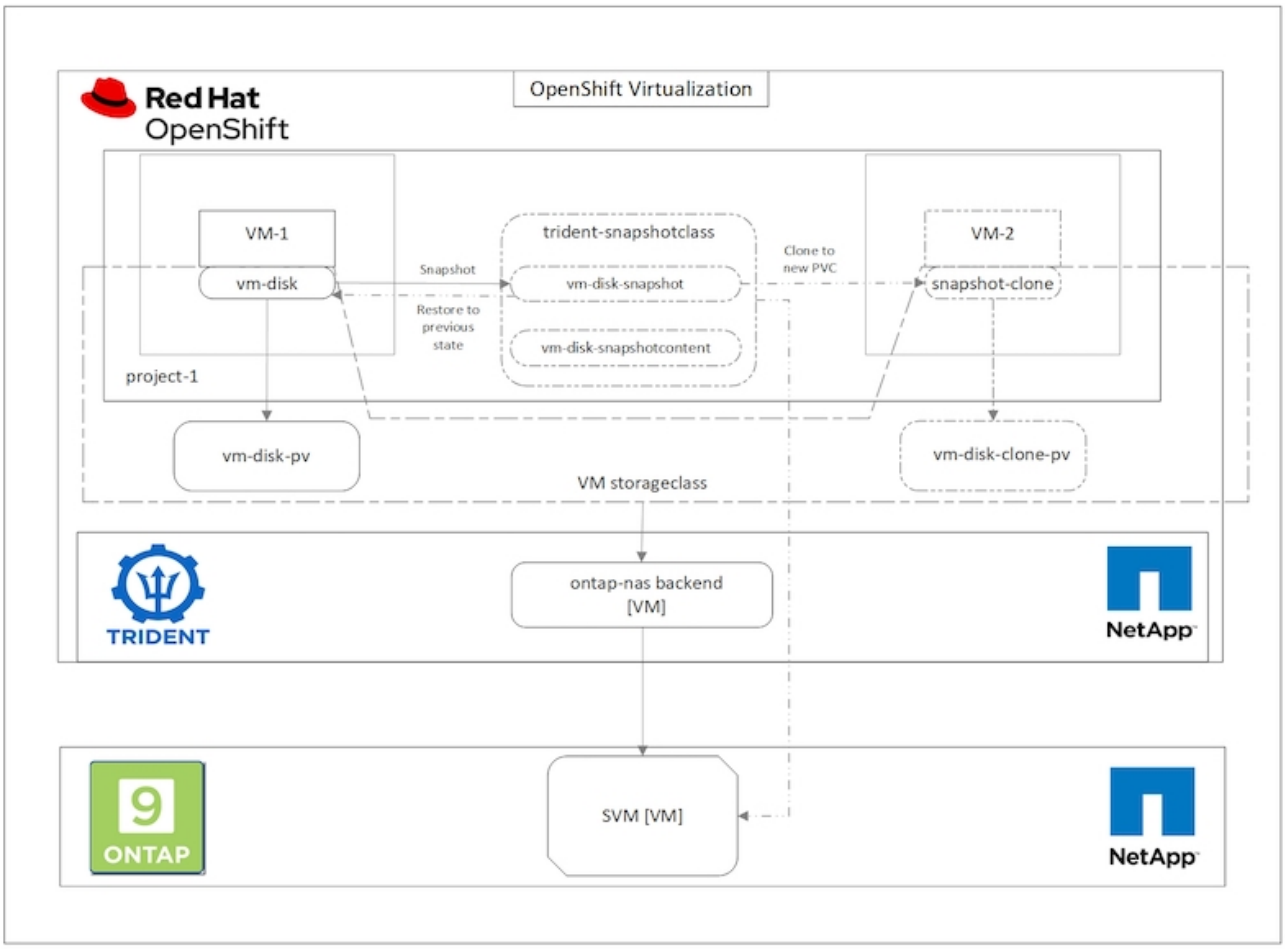
Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

Erstellen Sie eine VM aus einem Snapshot

Mit Astra Trident und Red hat OpenShift können Benutzer in von ihr bereitgestellten Storage-Klassen einen Snapshot eines persistenten Volumes 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.

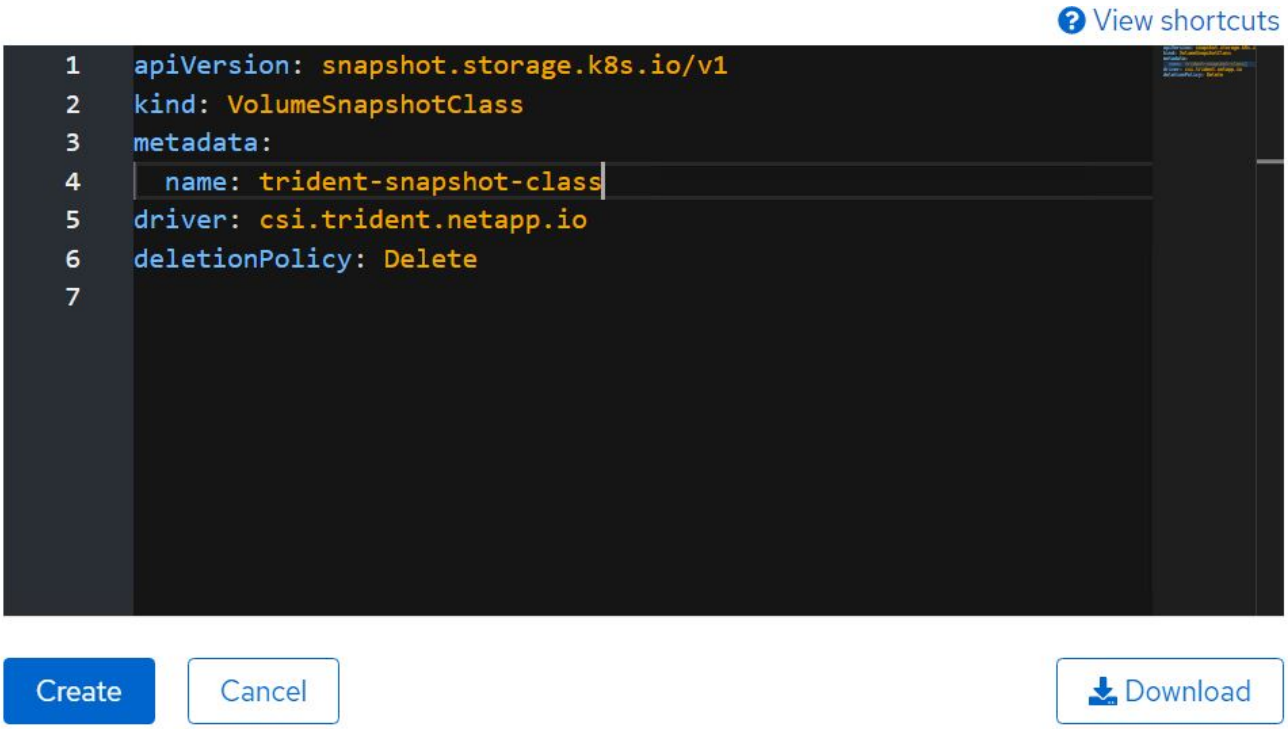
Für Snapshot-Vorgänge in OpenShift müssen die Ressourcen VolumeSnapshotClass, VolumeSnapshot und VolumeSnapshotContent definiert werden.

- Ein VolumeSnapshotContent ist der tatsächliche Snapshot, der von einem Volume im Cluster erstellt wurde. Es handelt sich um eine Cluster-weite Ressource, die dem PersistenzVolume 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.

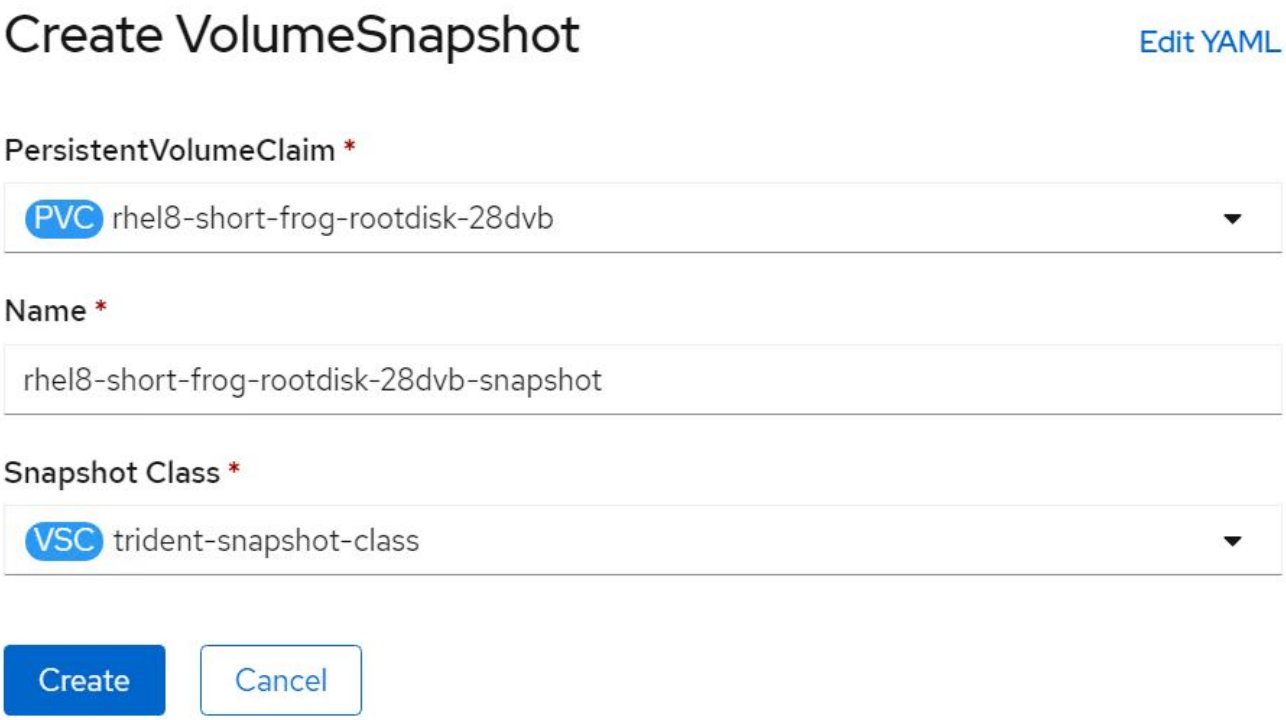


Um einen Snapshot einer VM zu erstellen, führen Sie die folgenden Schritte aus:

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.



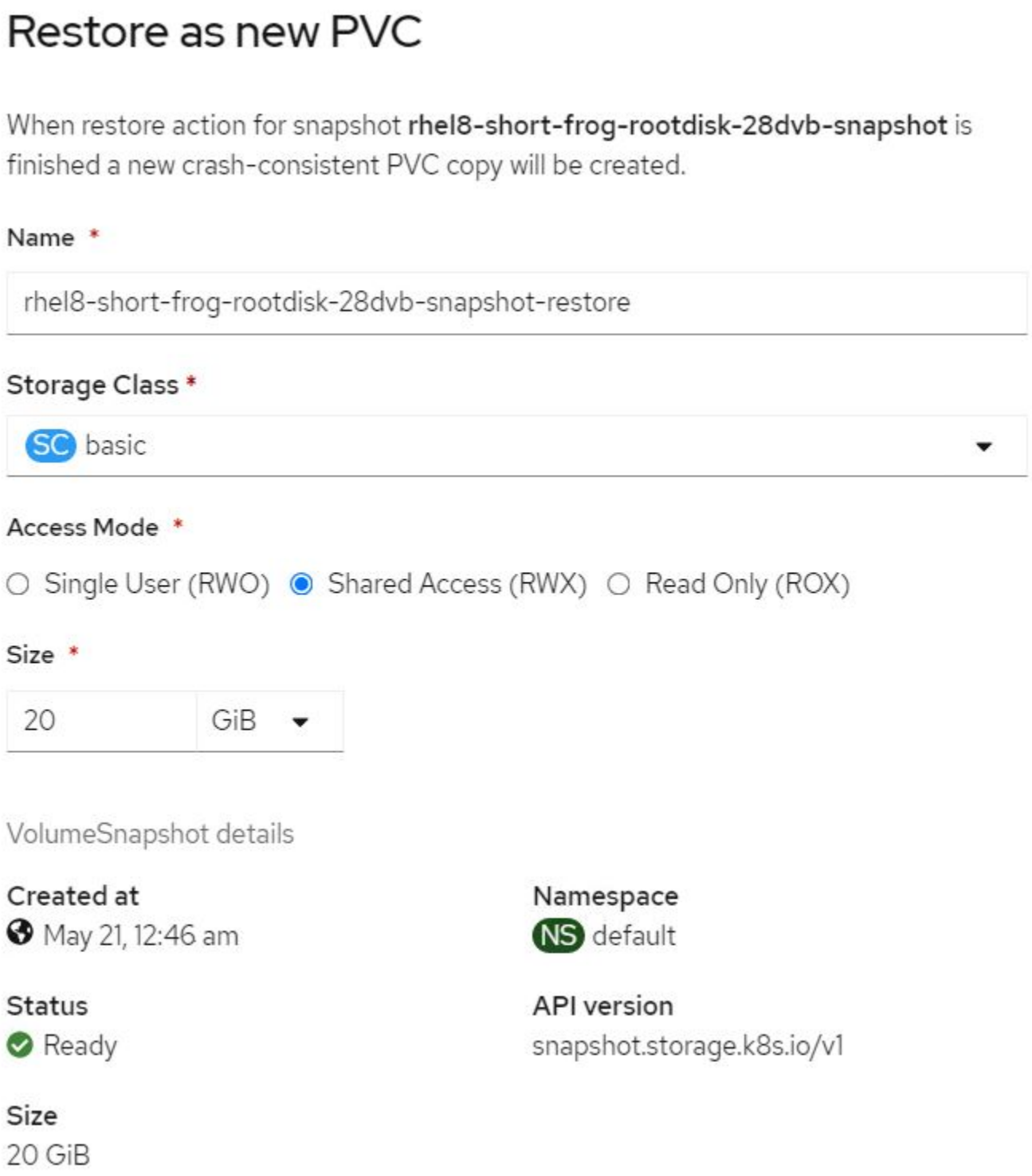
3. Identifizieren Sie die PVC, die an die Quell-VM angeschlossen ist, und erstellen Sie dann einen Snapshot dieser PVC. Navigieren Sie zu `Storage > VolumeSnapshots` Und klicken Sie auf VolumeSnapshots erstellen.
4. Wählen Sie das PVC aus, für das Sie den Snapshot erstellen möchten, geben Sie den Namen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



5. 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.



3. Erstellen Sie dann eine neue VM aus diesem PVC. Navigieren Sie zu Workloads > 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-28dvb-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.

Workflows: Red hat OpenShift Virtualisierung mit NetApp ONTAP

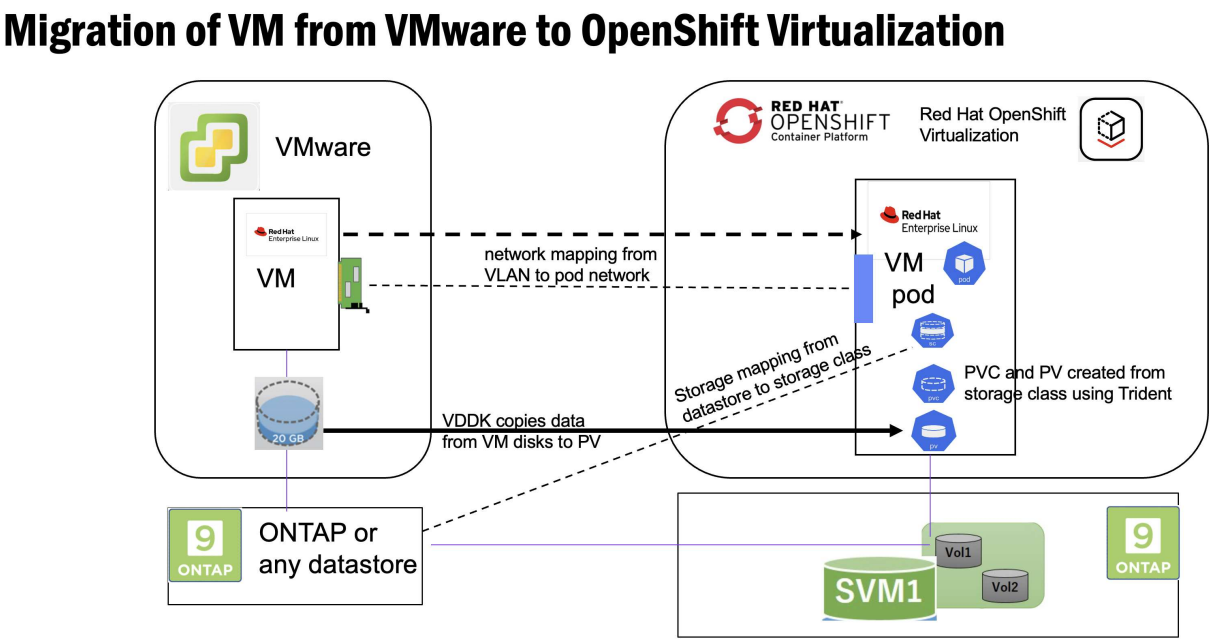
Migration der VM von VMware zu OpenShift-Virtualisierung mithilfe des Migration Toolkit für Virtualisierung

In diesem Abschnitt erfahren Sie, wie Sie mithilfe des Migration Toolkit for Virtualization (MTV) Virtual Machines von VMware auf OpenShift-Virtualisierung migrieren, die auf der OpenShift-Container-Plattform ausgeführt und mithilfe von Astra 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 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.



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
- "Astra 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

```yaml
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 dreigesichte 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.

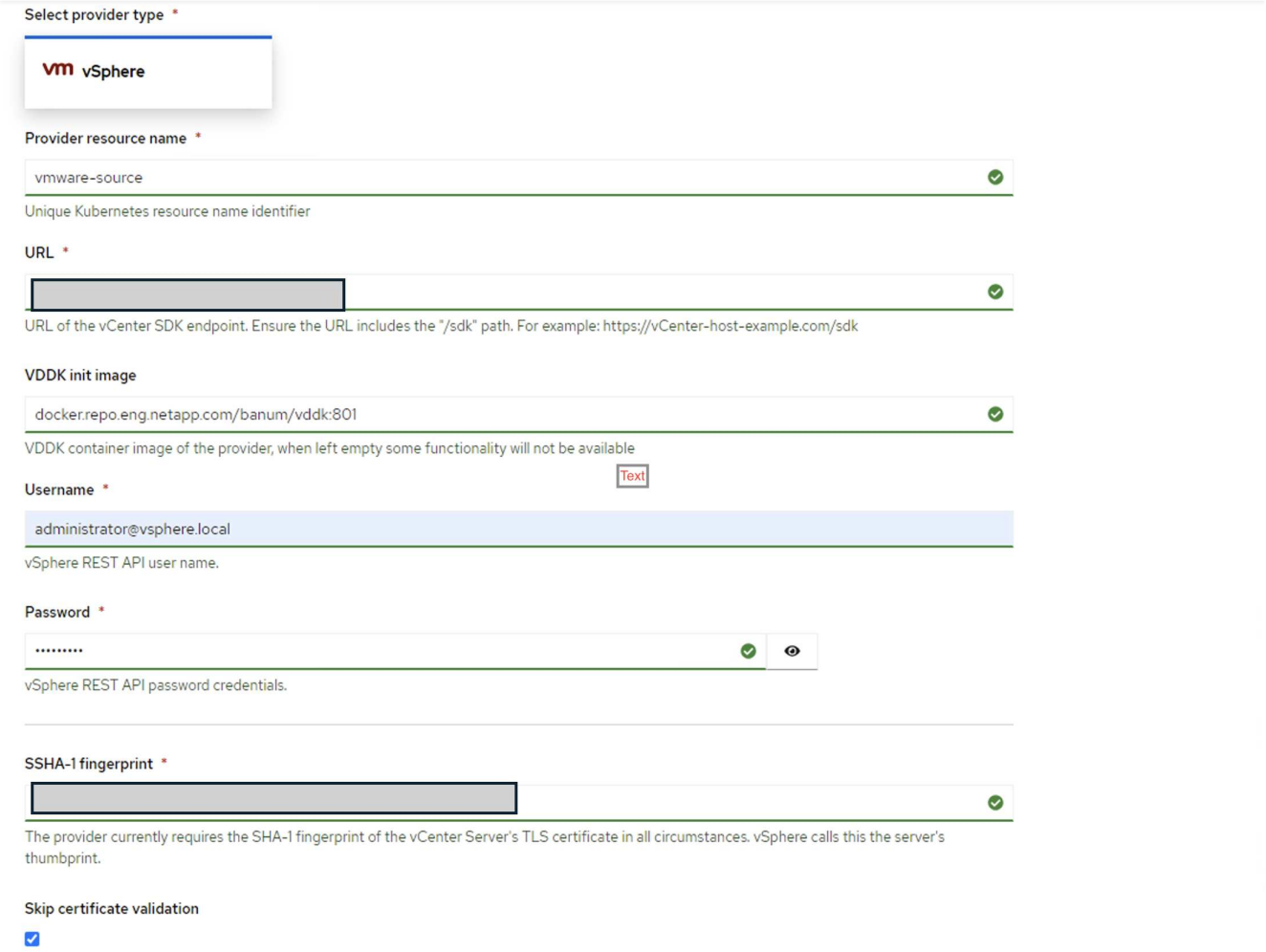
Quellanbieter Erstellen

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:



> 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

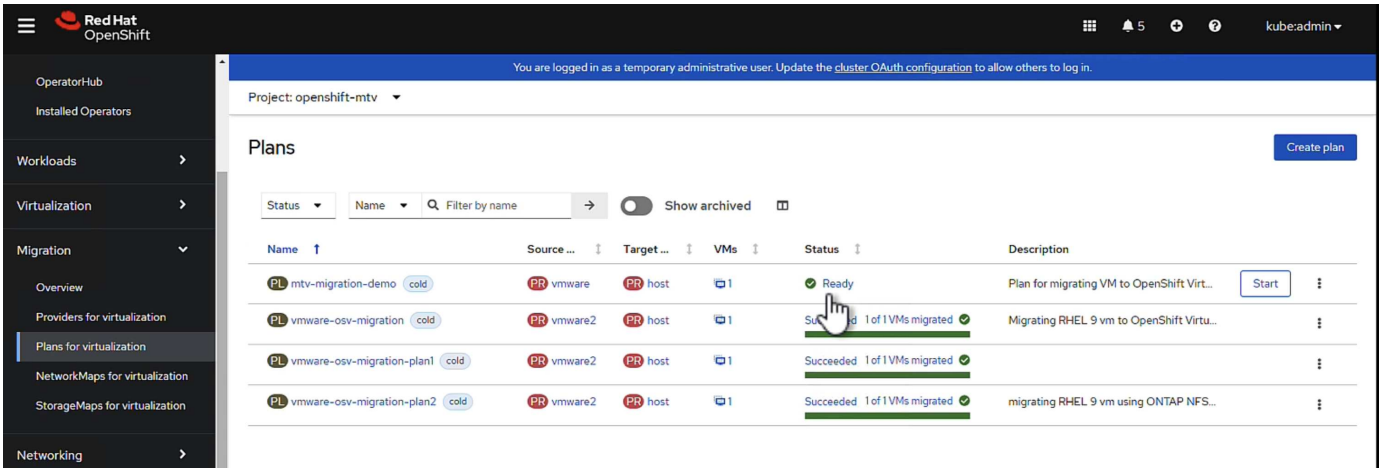
Der Host-Cluster wird automatisch hinzugefügt, da der OpenShift-Virtualisierungsanbieter der Quellanbieter ist.

Migrationsplan Erstellen

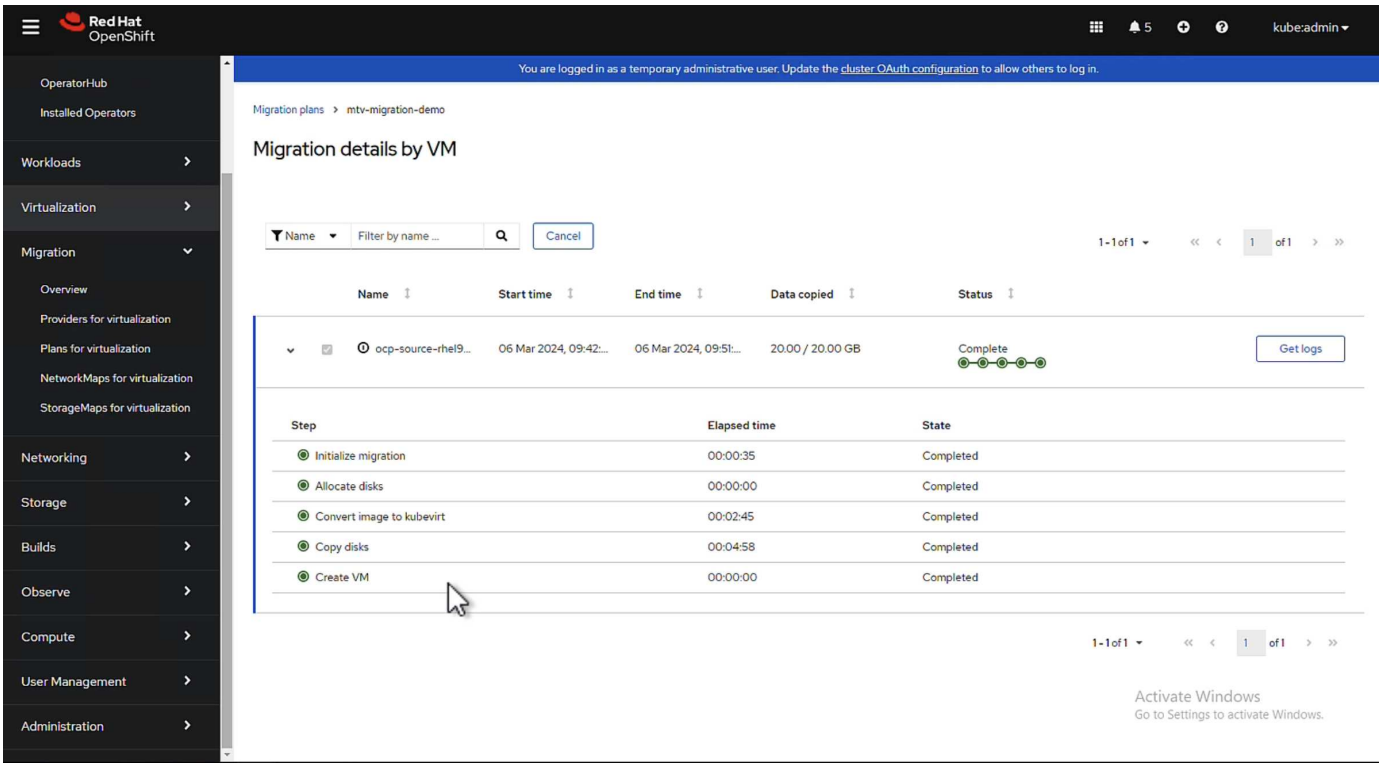
Befolgen Sie die Anweisungen "Hier" Um einen Migrationsplan zu erstellen.

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.



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 posgresql-Datenbanken überprüfen. Die Datenbanken, Tabellen und die Einträge in der Tabelle sollten identisch sein mit denen, die auf der Quell-VM erstellt wurden.

Data Protection for OpenShift Virtualization

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

Autor: Banu Sundhar, NetApp

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

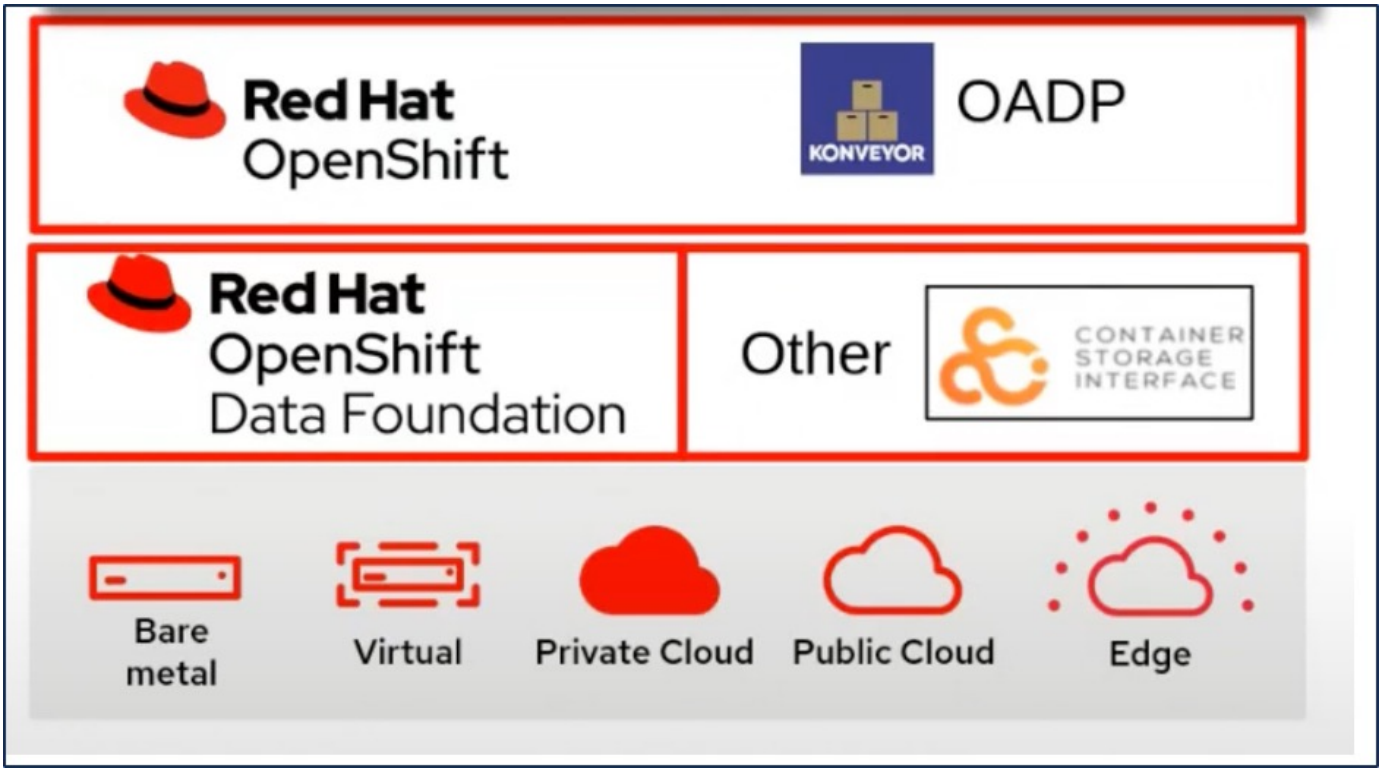
Virtuelle Maschinen in der OpenShift-Virtualisierungsumgebung sind Container-Anwendungen, die in den Workerknoten der OpenShift-Container-Plattform ausgeführt werden. Es ist wichtig, die VM-Metadaten sowie die persistenten Festplatten der VMs zu schützen, damit Sie sie bei Verlust oder Beschädigung wiederherstellen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

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

- ONTAP Objekt-Storage
- StorageGRID

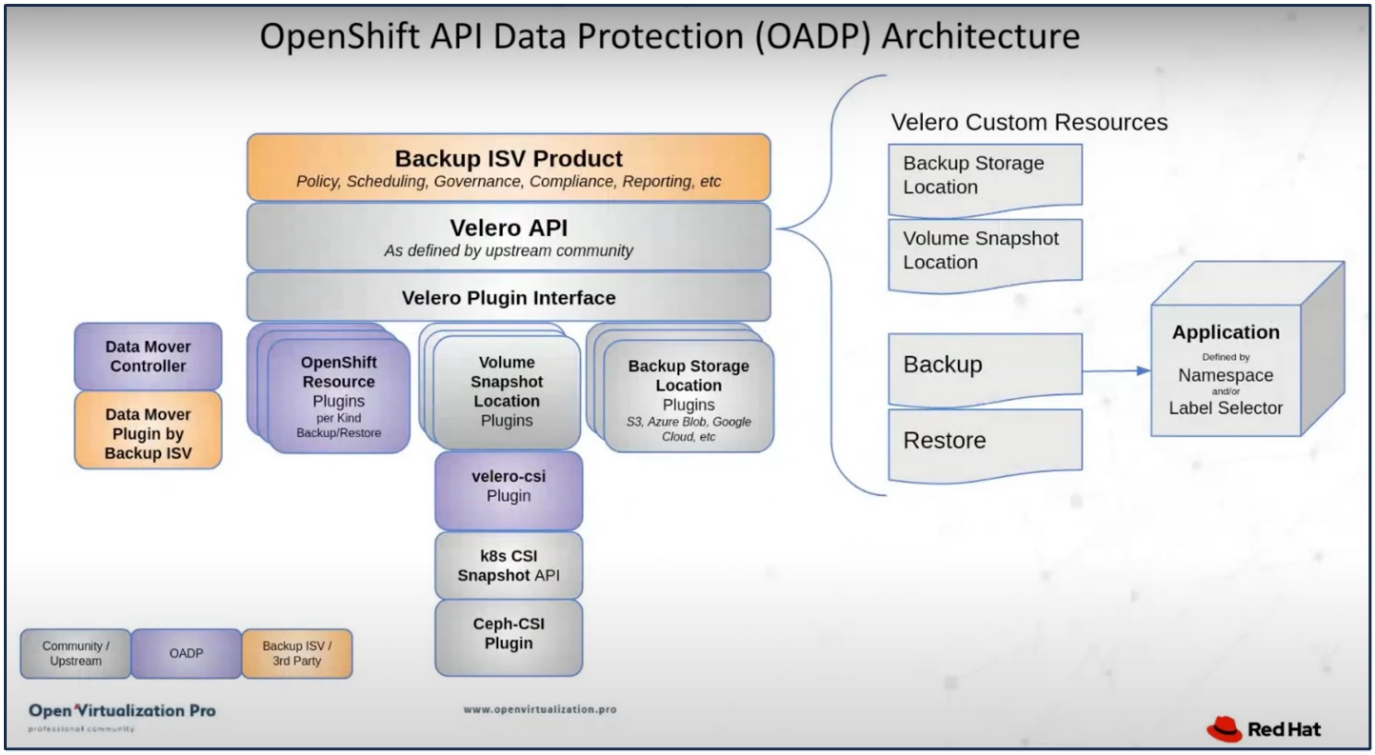
Wir führen dann bei Bedarf ein Restore aus dem Backup durch.

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



Red hat OpenShift nutzt die von den OpenSource Communities entwickelten Lösungen für den Datenschutz.

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



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

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

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

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

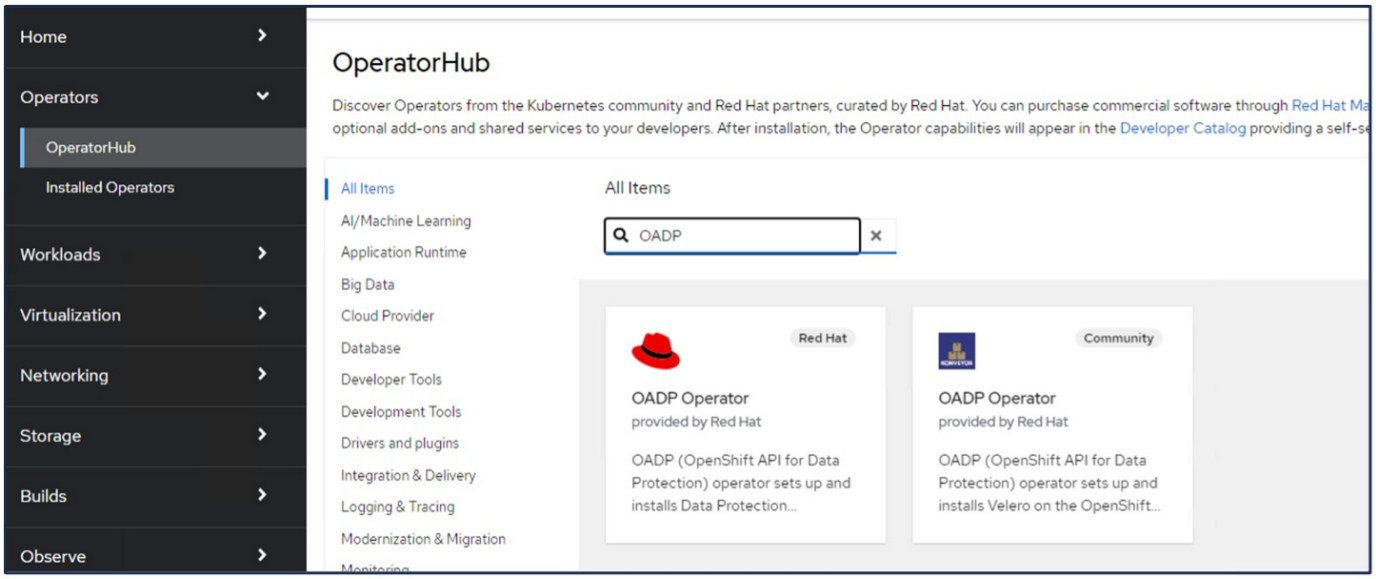
Voraussetzungen

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

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

Schritte zum Installieren des OADP-Bedieners

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



OADP Operator

1.3.0 provided by Red Hat

Install

Channel

stable-1.3

Version

1.3.0

Capability level

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

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

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

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

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

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

Project: All Projects

Installed Operators

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

Name | Search by name... /

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

Voraussetzungen für die Velero-Konfiguration mit ONTAP S3-Details

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

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

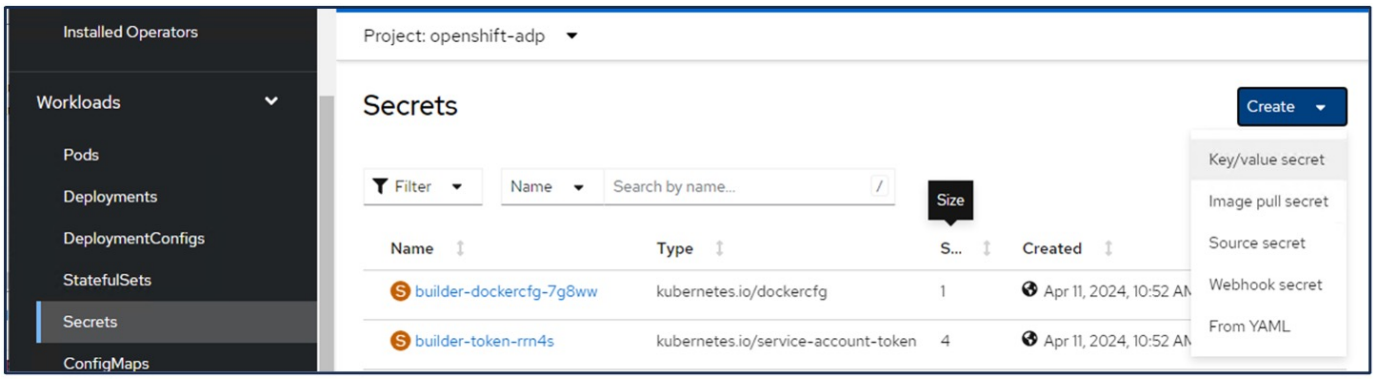
Voraussetzungen für die Velero-Konfiguration mit StorageGRID S3-Details

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

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

Schritte zum Konfigurieren von Velero

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



Project: openshift-adp

Create key/value secret

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

Secret name *

cloud-credentials

Unique name of the new secret.

Key *

cloud

Value

Browse...

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

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

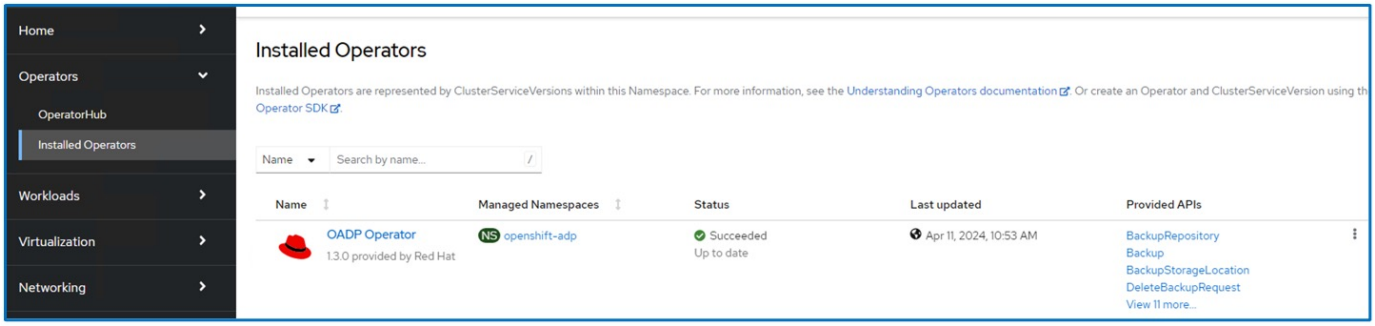
Add key/value

Create Cancel

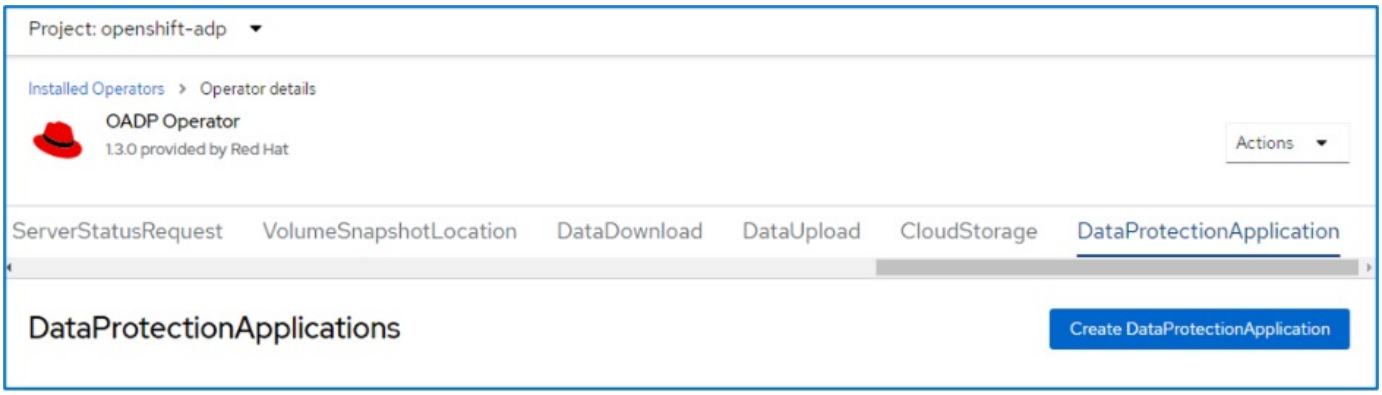
Um einen Schlüssel mit dem Namen sg-s3-credentials aus der CLI zu erstellen, können Sie den folgenden Befehl verwenden.

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

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

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

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



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



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

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

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

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

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

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

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

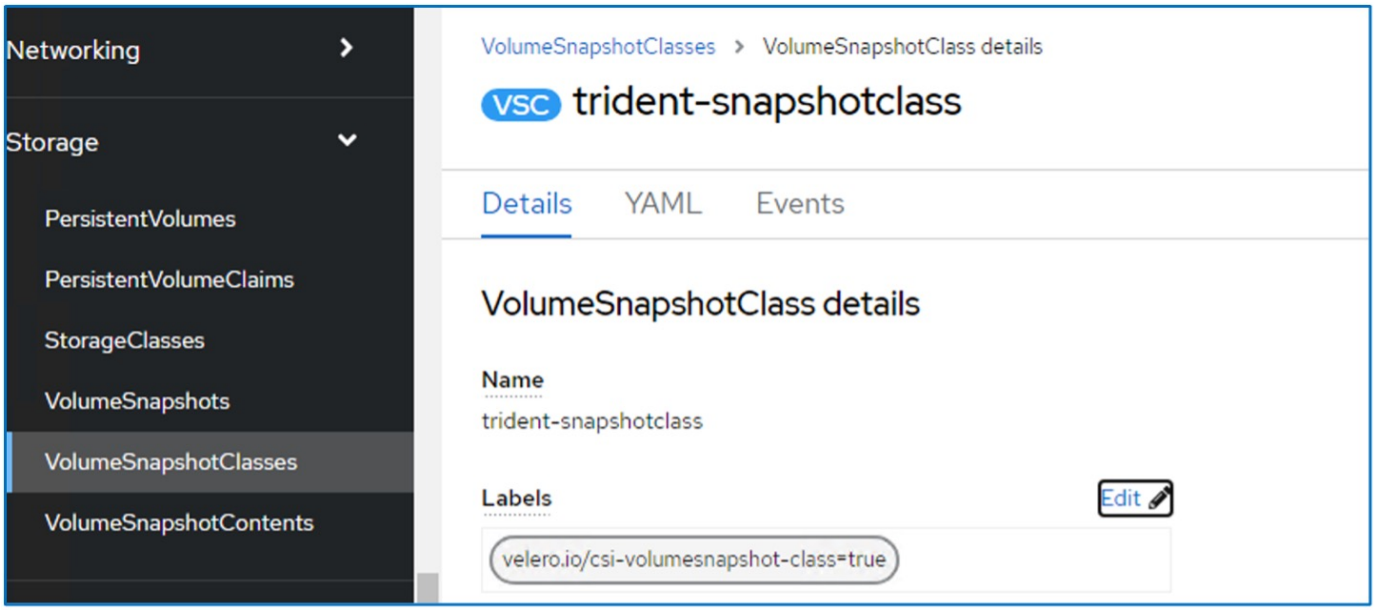
Schnappschusspositionen
Wenn Sie CSI-Snapshots (Container Storage Interface) verwenden, müssen Sie keinen Snapshot-Speicherort angeben, da Sie einen VolumeSnapshotClass CR erstellen, um den CSI-Treiber zu registrieren. In unserem Beispiel verwenden Sie Astra Trident CSI und Sie haben bereits VolumeSnapShotClass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

CSI-Plugin aktivieren

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

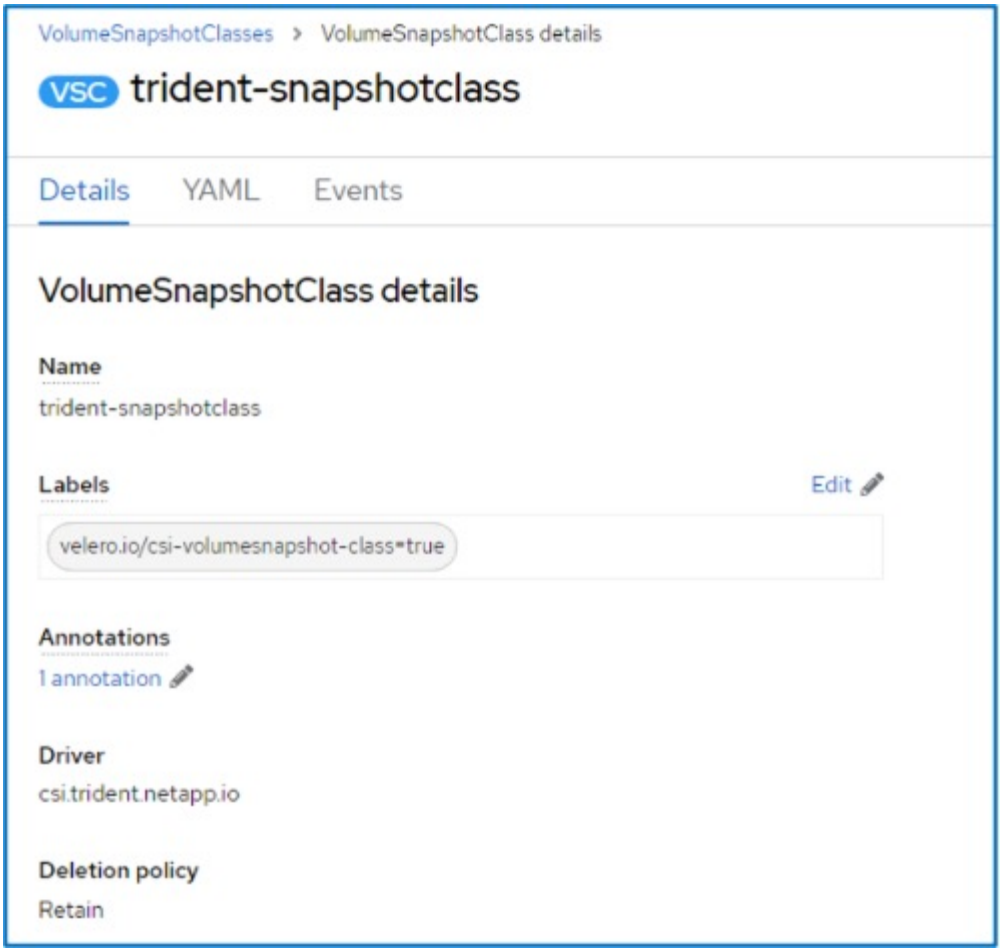
- Sie müssen die Dreizack-VolumeSnapshotClass erstellen lassen.

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

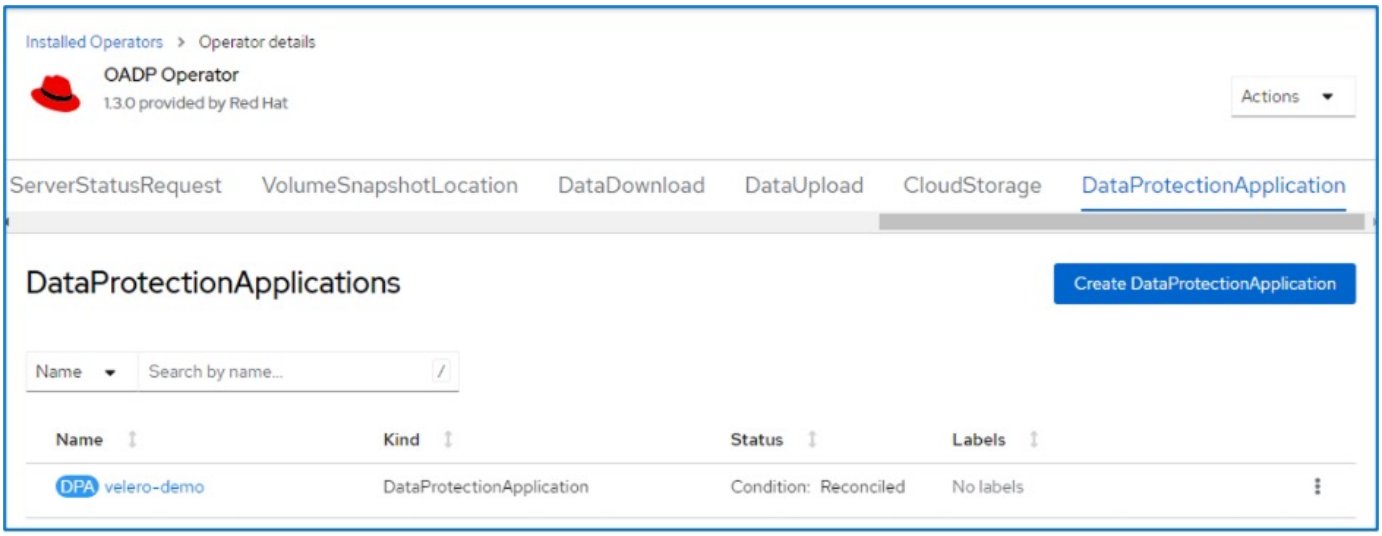


Stellen Sie sicher, dass die Snapshots auch dann bestehen können, wenn die VolumeSnapshot-Objekte gelöscht werden. Dies kann durch Setzen der **deletionPolicy** auf behalten erfolgen. Wenn nicht, geht durch das Löschen eines Namespace sämtliche darin gesicherten PVCs verloren.

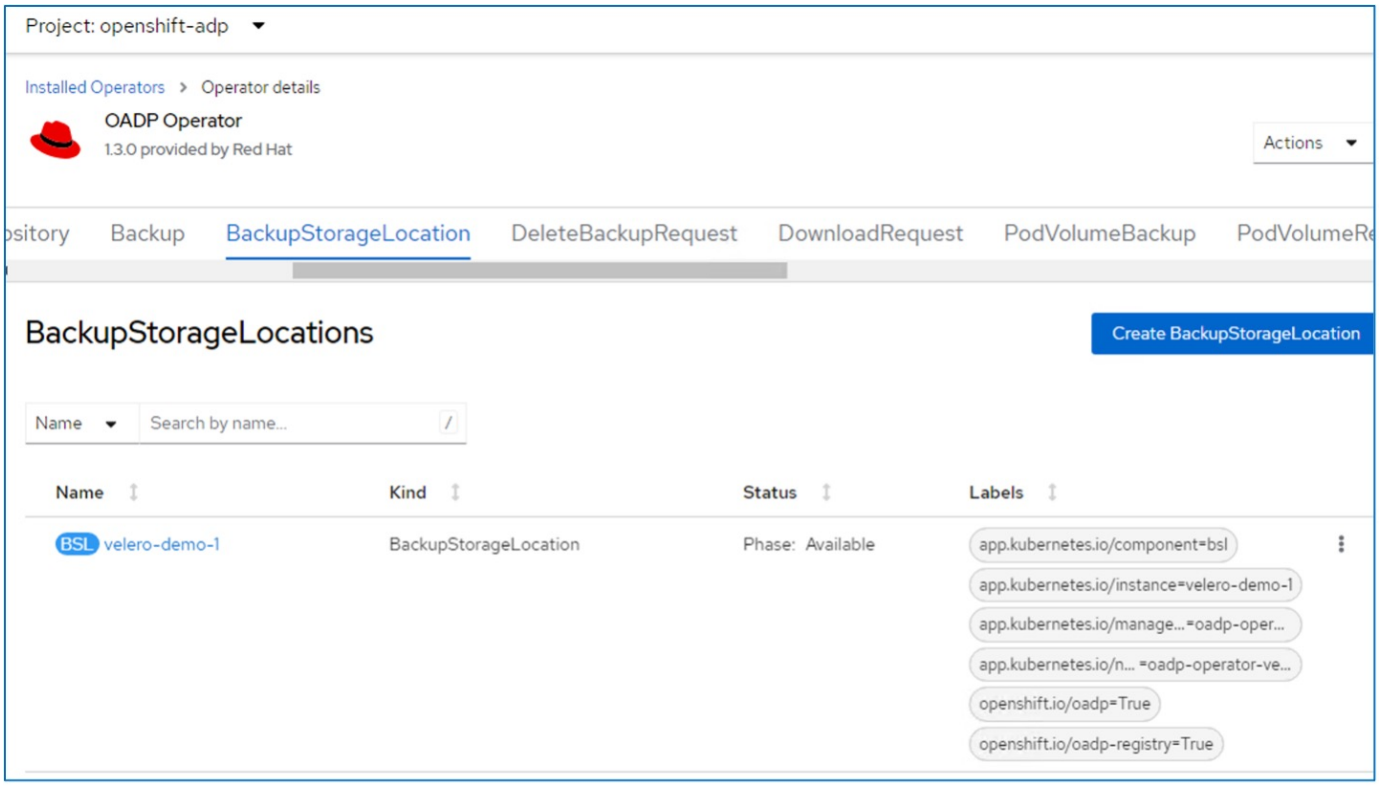
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



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



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



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

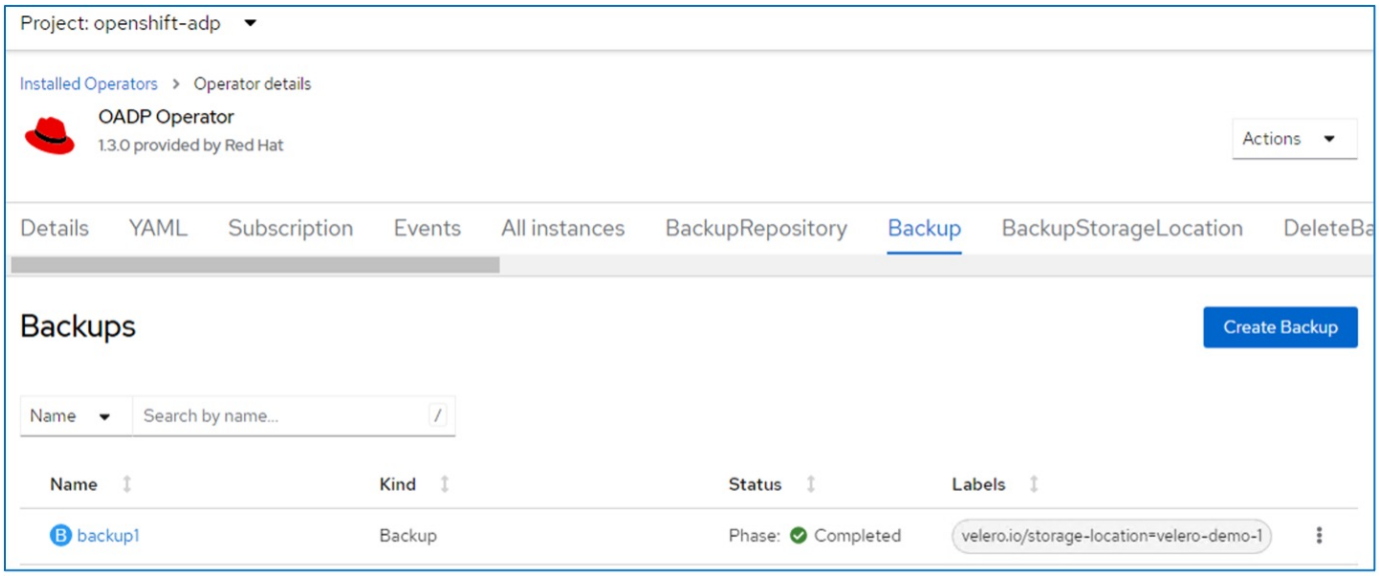
Schritte zum Erstellen einer Sicherung einer VM

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

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

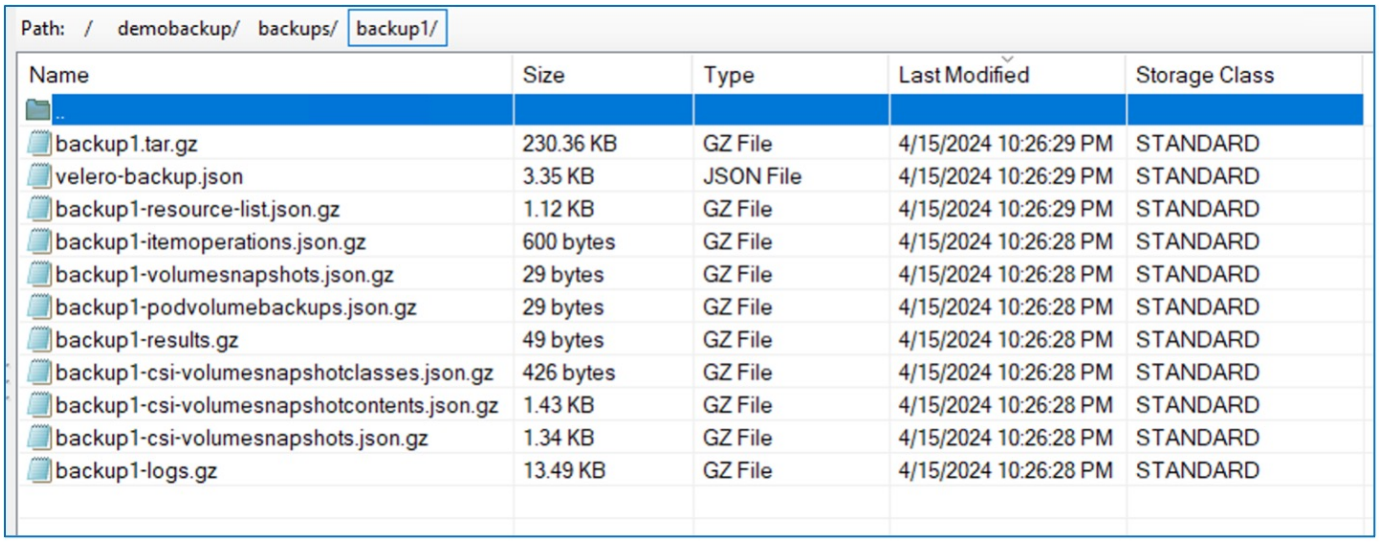
```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
previously created
                                    when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

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



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

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



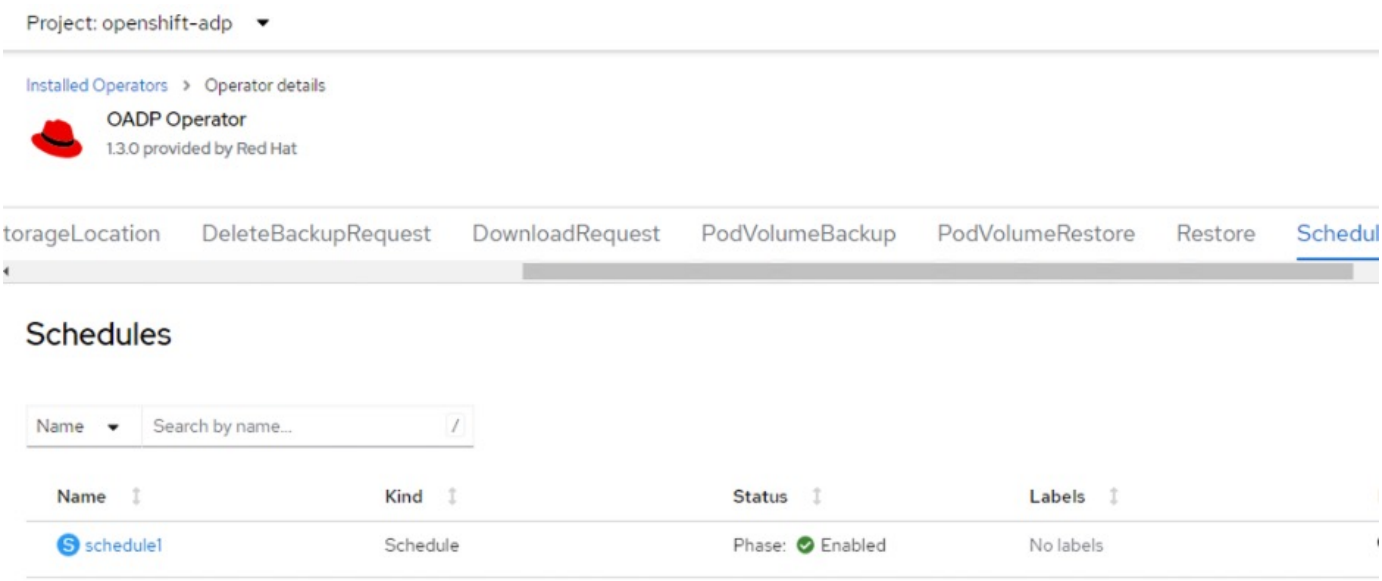
Erstellen geplanter Backups für VMs in OpenShift Virtualization

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

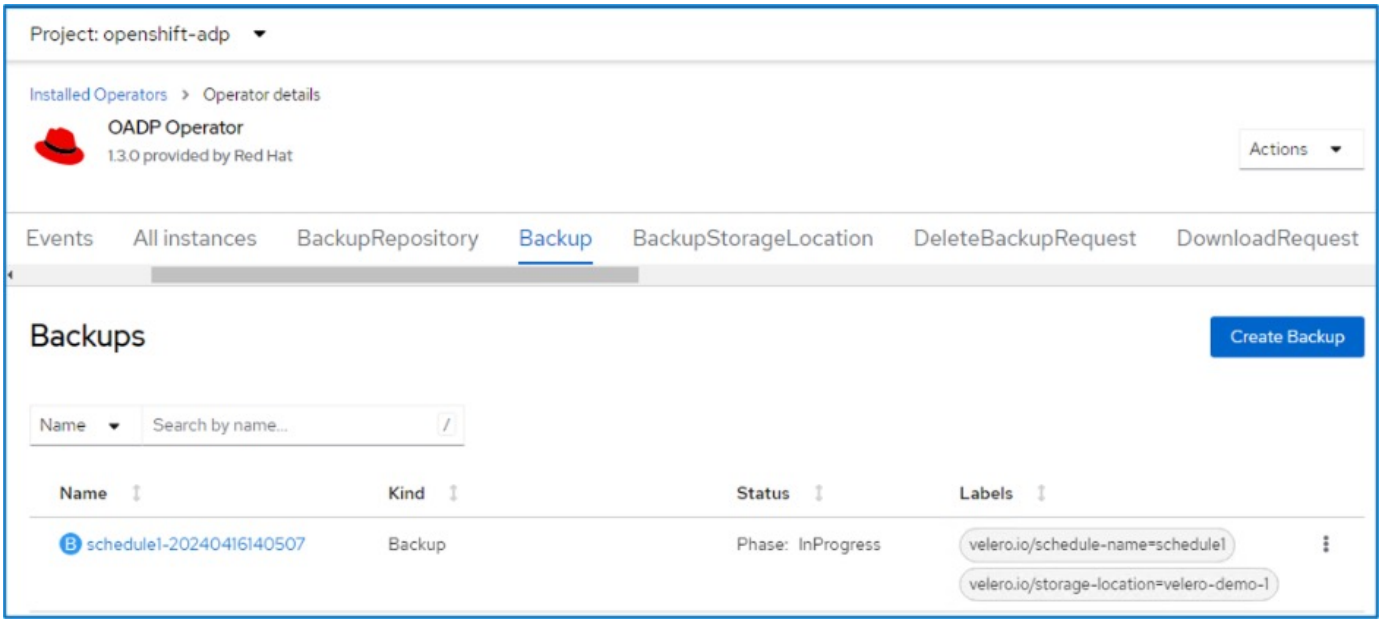
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

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

Sobald der Zeitplan erstellt wurde, wird er aktiviert.



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



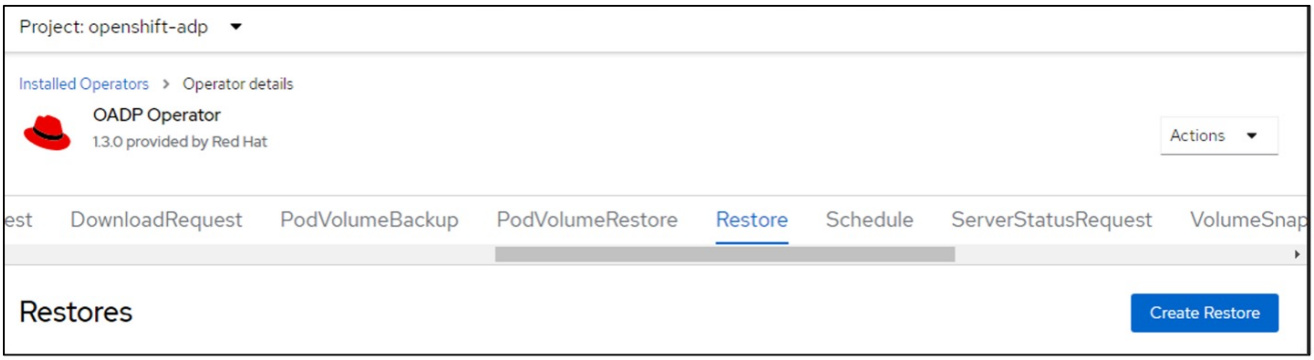
Stellen Sie eine VM aus einem Backup wieder her

Voraussetzungen

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

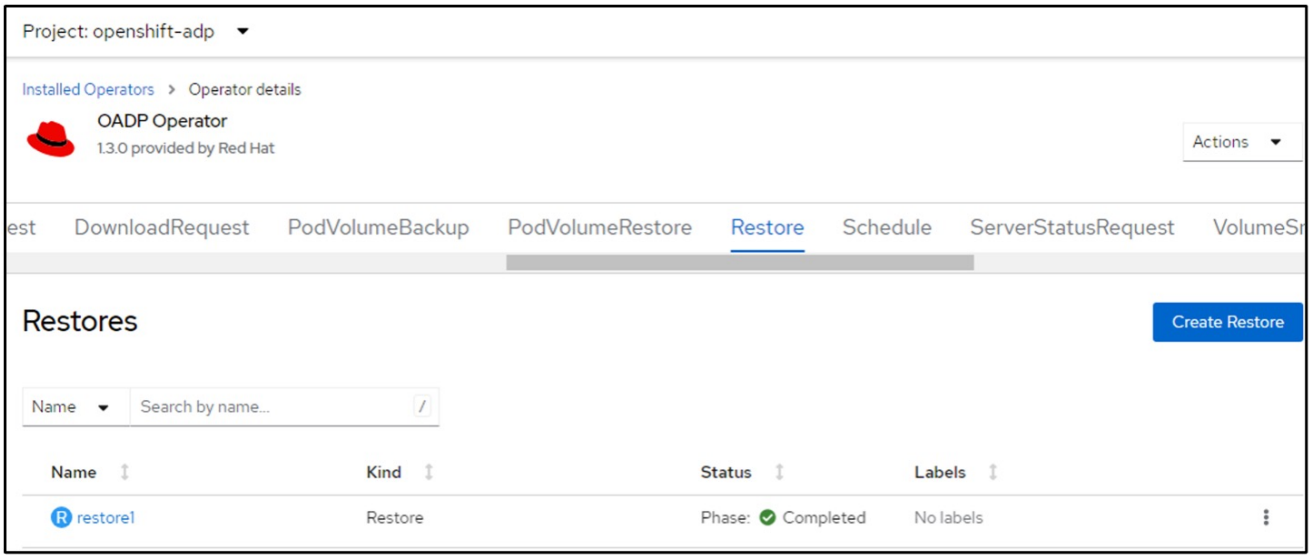
Restore auf denselben Namespace

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




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

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



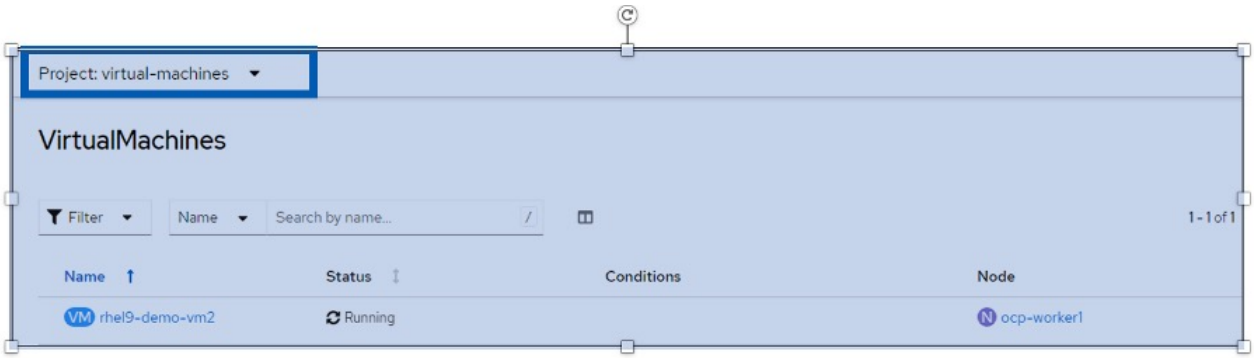
Wiederherstellung in einem anderen Namespace

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

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

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

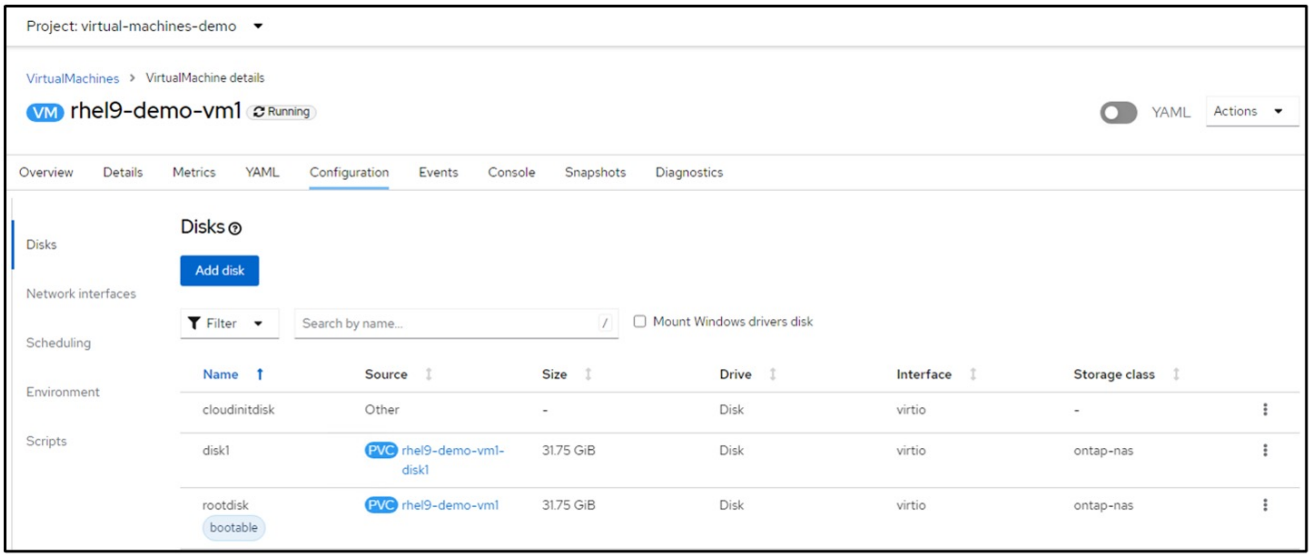
Wenn in der Phase „Abgeschlossen“ angezeigt wird, sehen Sie, dass die virtuellen Maschinen zum Zeitpunkt der Snapshot-Erstellung wieder in den Status versetzt wurden. (Wenn das Backup bei der Ausführung der VM erstellt wurde, wird durch die Wiederherstellung der VM aus dem Backup die wiederhergestellte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

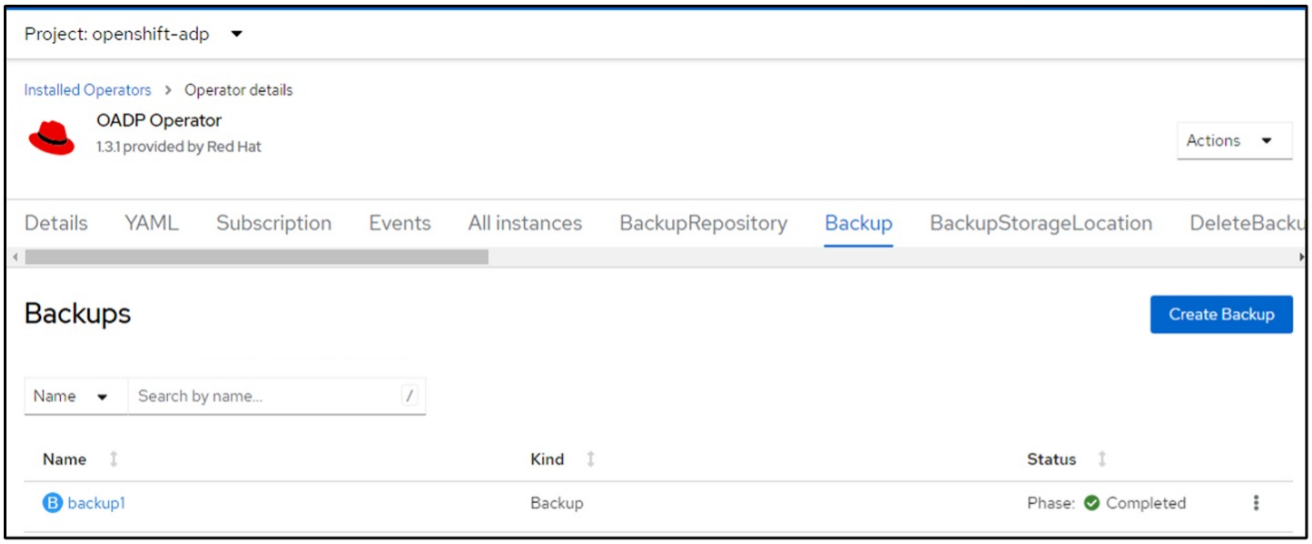


Wiederherstellung auf eine andere Storage-Klasse

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

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





Simulieren Sie einen Verlust der VM durch Löschen der VM.

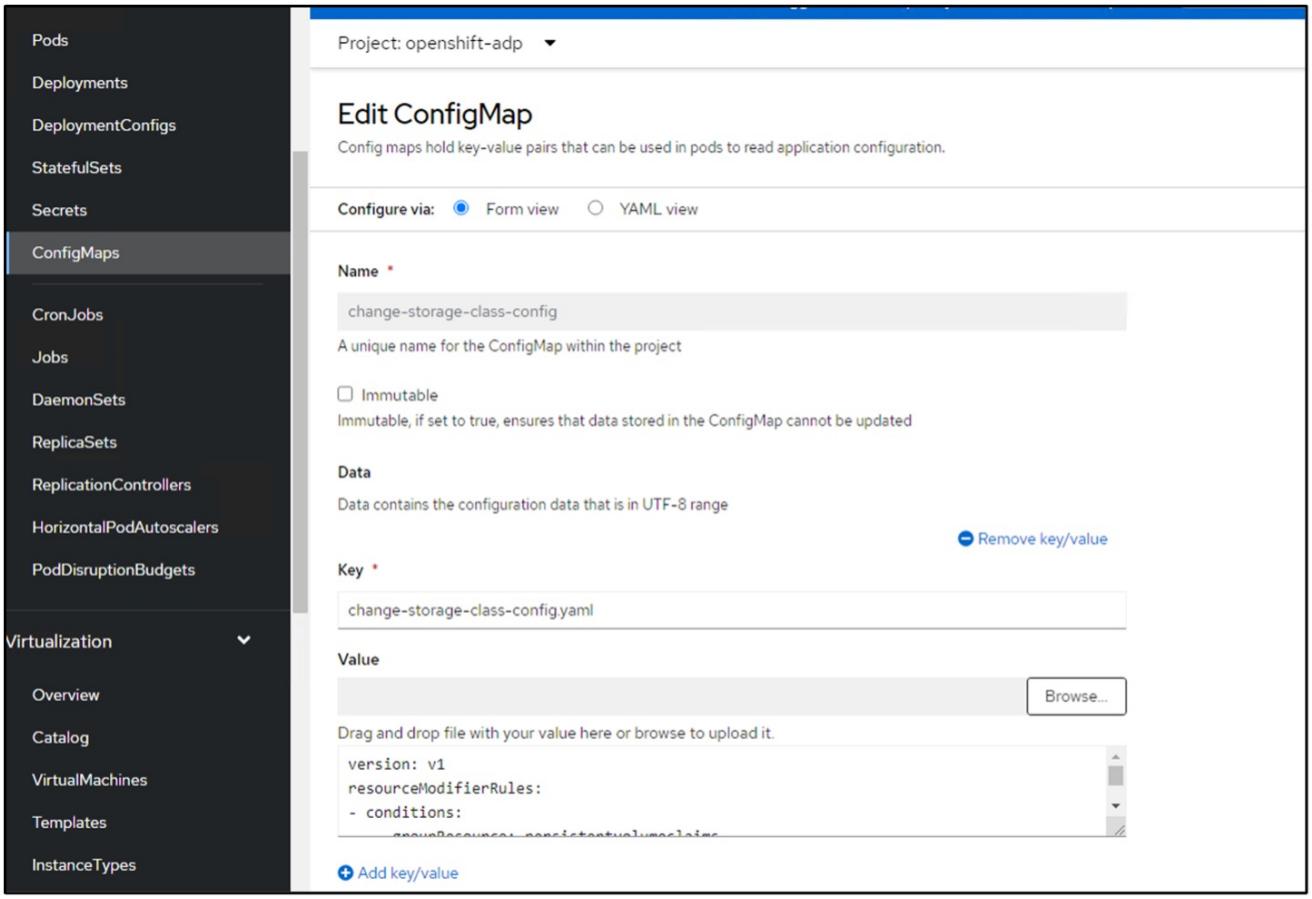
Um die VM mithilfe einer anderen Storage-Klasse, z. B. der Storage-Klasse ontap-nas-eco, wiederherzustellen, müssen Sie die folgenden zwei Schritte durchführen:

Schritt 1

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

Name: Change-Storage-class-config (kann ein beliebiger Name sein)
Schlüssel: Change-Storage-class-config.yaml:
Wert:

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



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

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

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



BinaryData
====

Events:  <none>
```

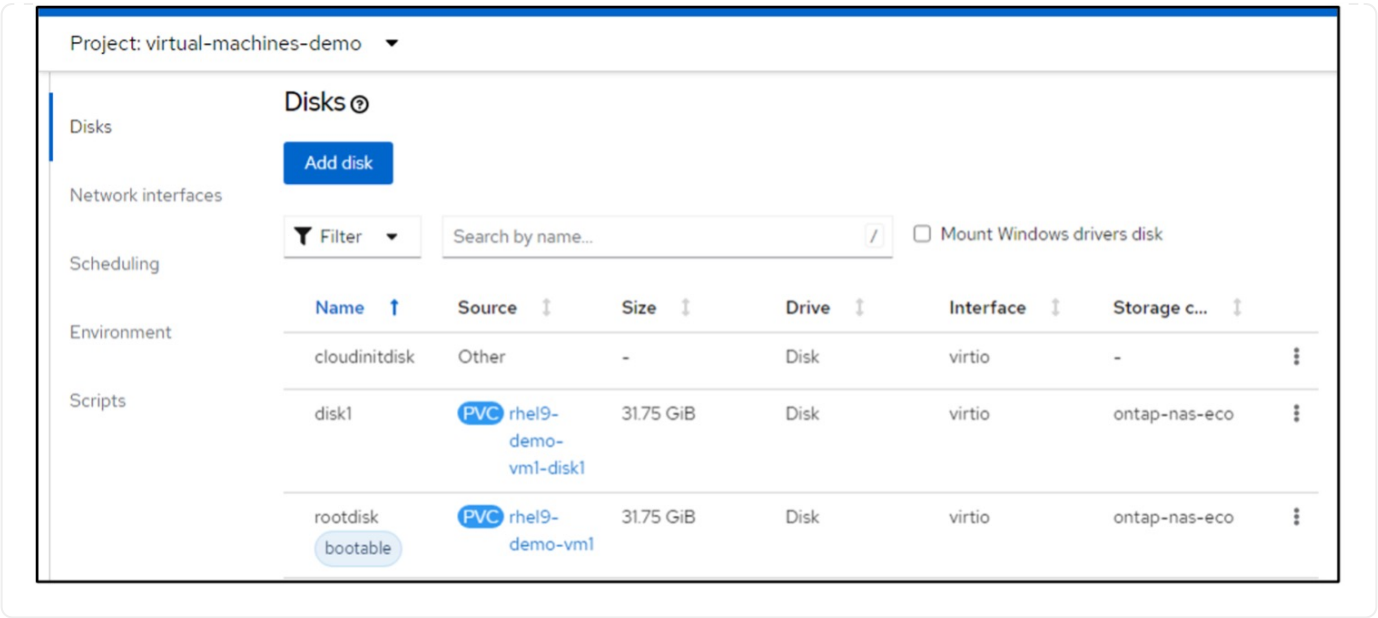
Diese Konfigurationszuordnung wendet die Ressourcenänderungsregel an, wenn die Wiederherstellung erstellt wird. Für alle Ansprüche auf persistente Volumes, die mit RHEL beginnen, wird ein Patch eingesetzt, der den Namen der Storage-Klasse auf ontap-nas-Eco ersetzt.

Schritt 2

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

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

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



Löschen von Backups und Restores in mit Velero

Löschen eines Backups

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

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

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

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

Führen Sie den folgenden Löschbefehl über die Velero CLI aus

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

Sie können den Restore CR auch über die Velero CLI löschen

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

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

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

Überwachung mittels Cloud Insights

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

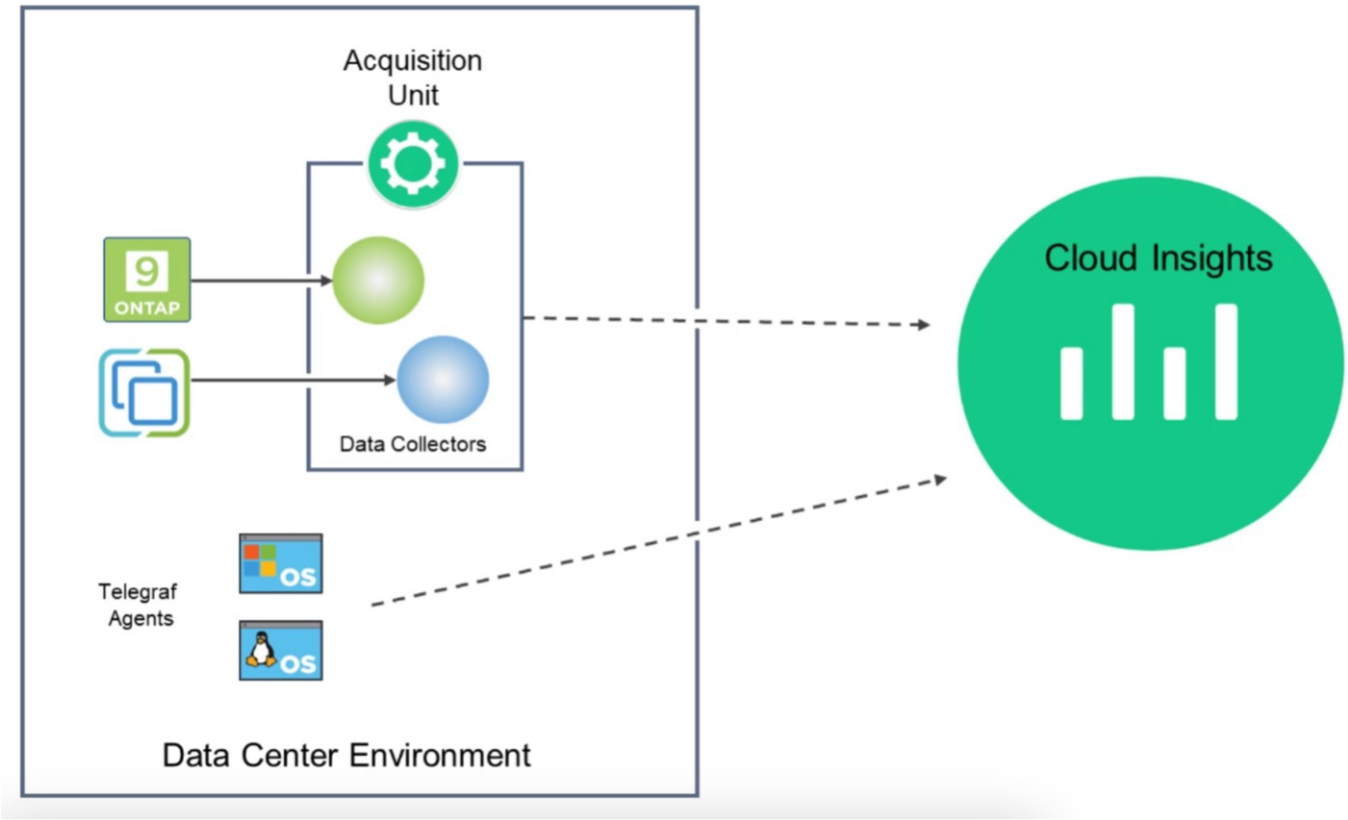
Datensammler
Es gibt 3 Arten von Datensammlern:
* Infrastruktur (Speichergeräte, Netzwerk-Switches, Rechnerinfrastruktur)
* Betriebssysteme (wie VMware oder Windows)
* Dienste (wie Kafka)

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:

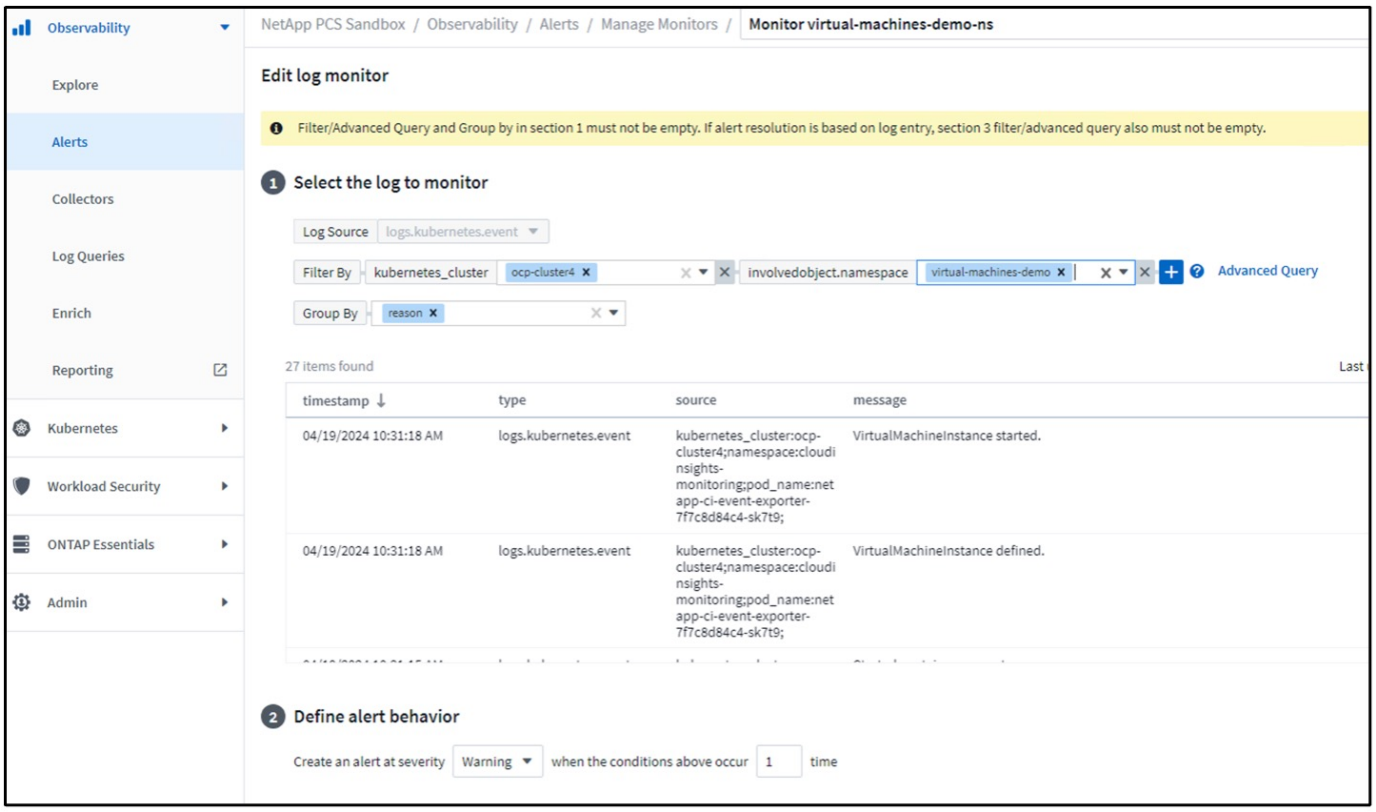
1. Ein Kubernetes Monitoring Operator und Datensammler zum Erfassen von Kubernetes-Daten
   Vollständige Anweisungen finden Sie im "Dokumentation".
2. Eine Einheit zur Erfassung von Daten aus ONTAP Storage, die persistenten Storage für VM-Festplatten bereitstellt
   Vollständige Anweisungen finden Sie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

Überwachung auf Basis von Ereignissen und Erstellung von Warnungen

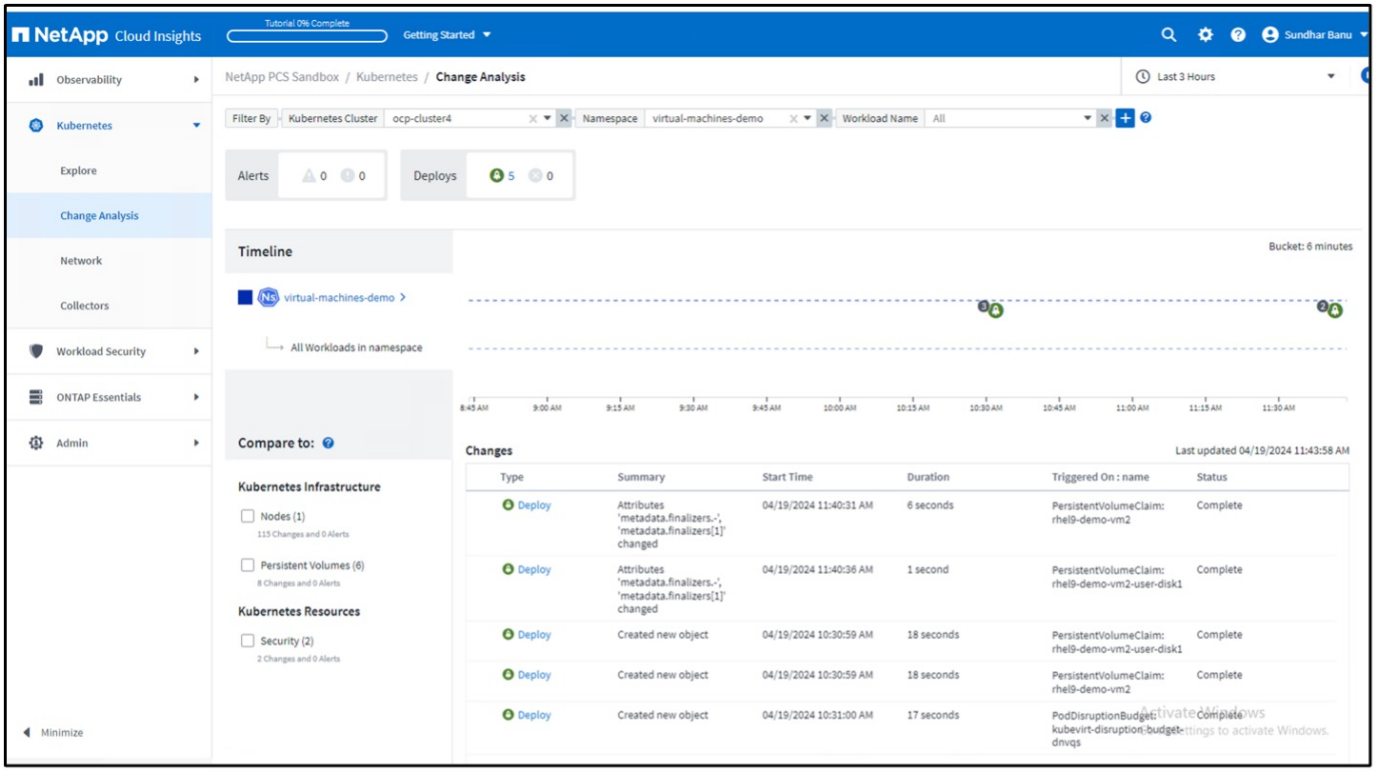
Hier ist ein Beispiel, bei dem der Namespace, der eine VM in OpenShift Virtualization enthält, anhand von Ereignissen überwacht wird. In diesem Beispiel wird ein Monitor basierend auf **logs.kubernetes**.Event für den angegebenen Namespace im Cluster erstellt.



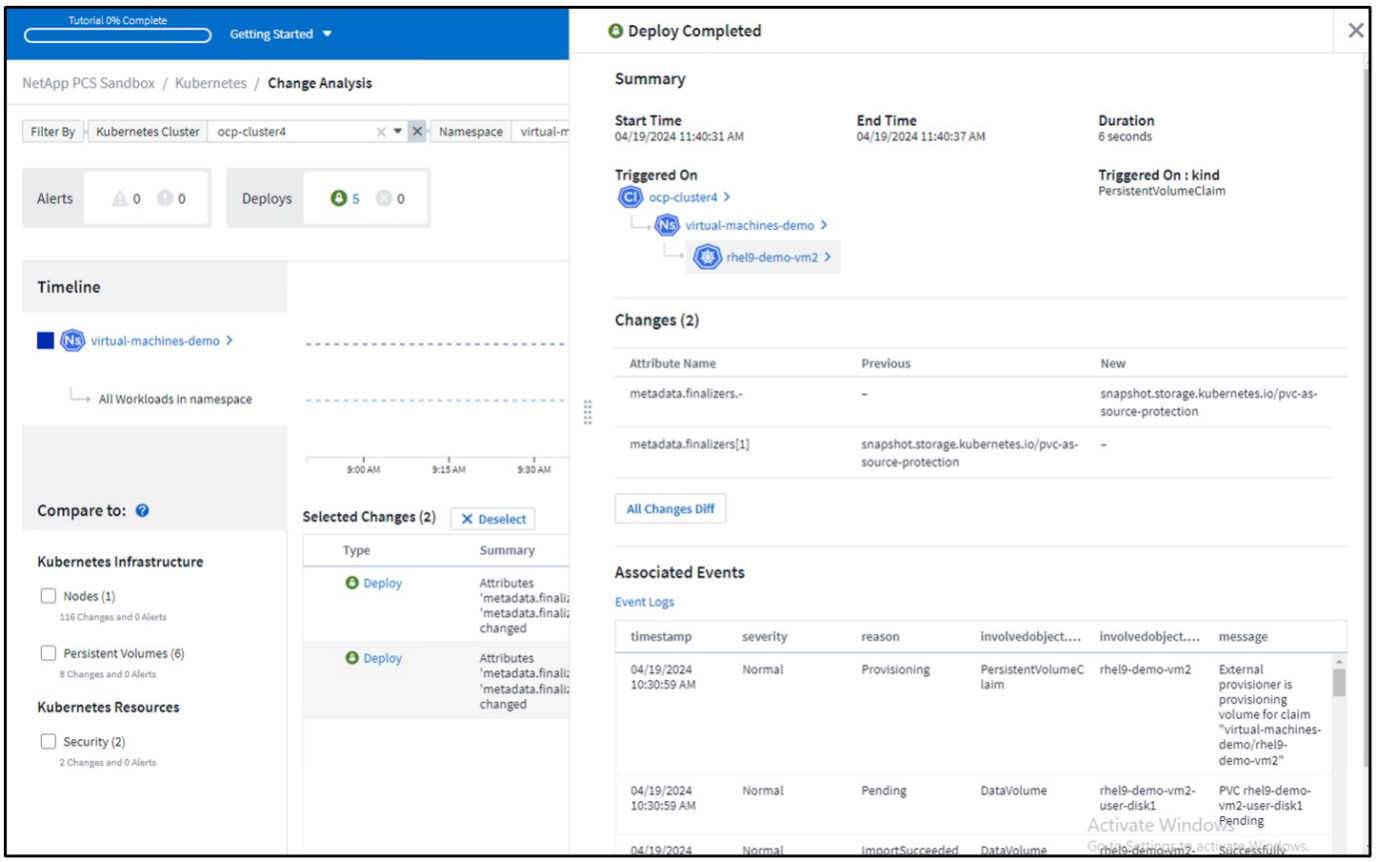
Diese Abfrage enthält alle Ereignisse für die virtuelle Maschine im Namespace. (Im Namespace befindet sich nur eine virtuelle Maschine). Eine erweiterte Abfrage kann auch so konstruiert werden, dass sie auf der Grundlage des Ereignisses gefiltert wird, bei dem der Grund „Fehlgeschlagen“ oder „FailedMount“ 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.

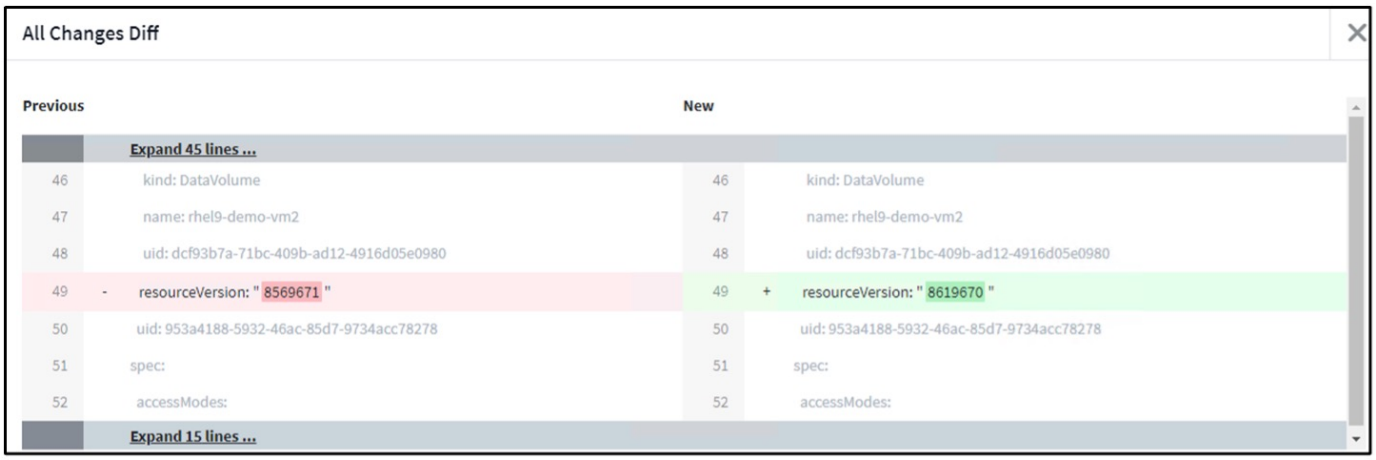
Änderungsanalyse

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.



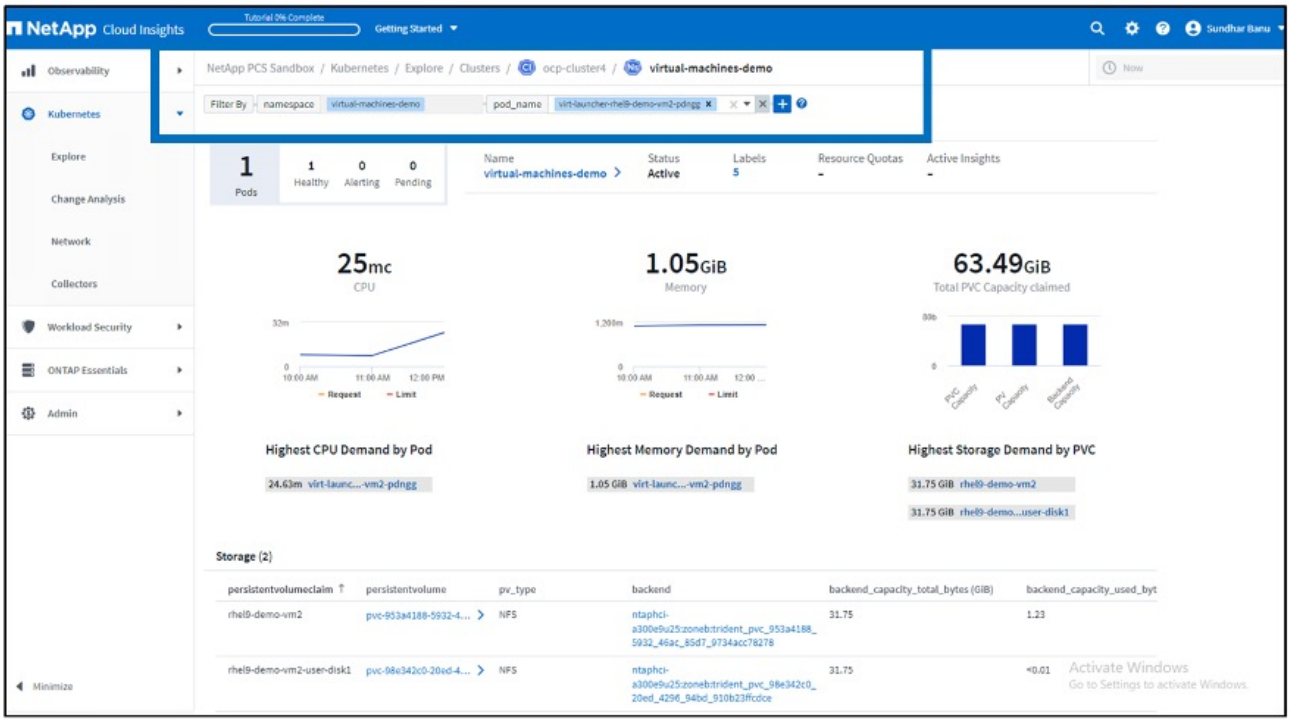
Im obigen Beispiel wird die Änderungsanalyse auf dem OpenShift-Cluster für den Namespace konfiguriert, der eine OpenShift-Virtualisierungs-VM enthält. Das Dashboard zeigt Änderungen gegenüber der Zeitachse an. Sie können nach unten gehen, um zu sehen, was sich geändert hat, und klicken Sie auf Alle Änderungen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



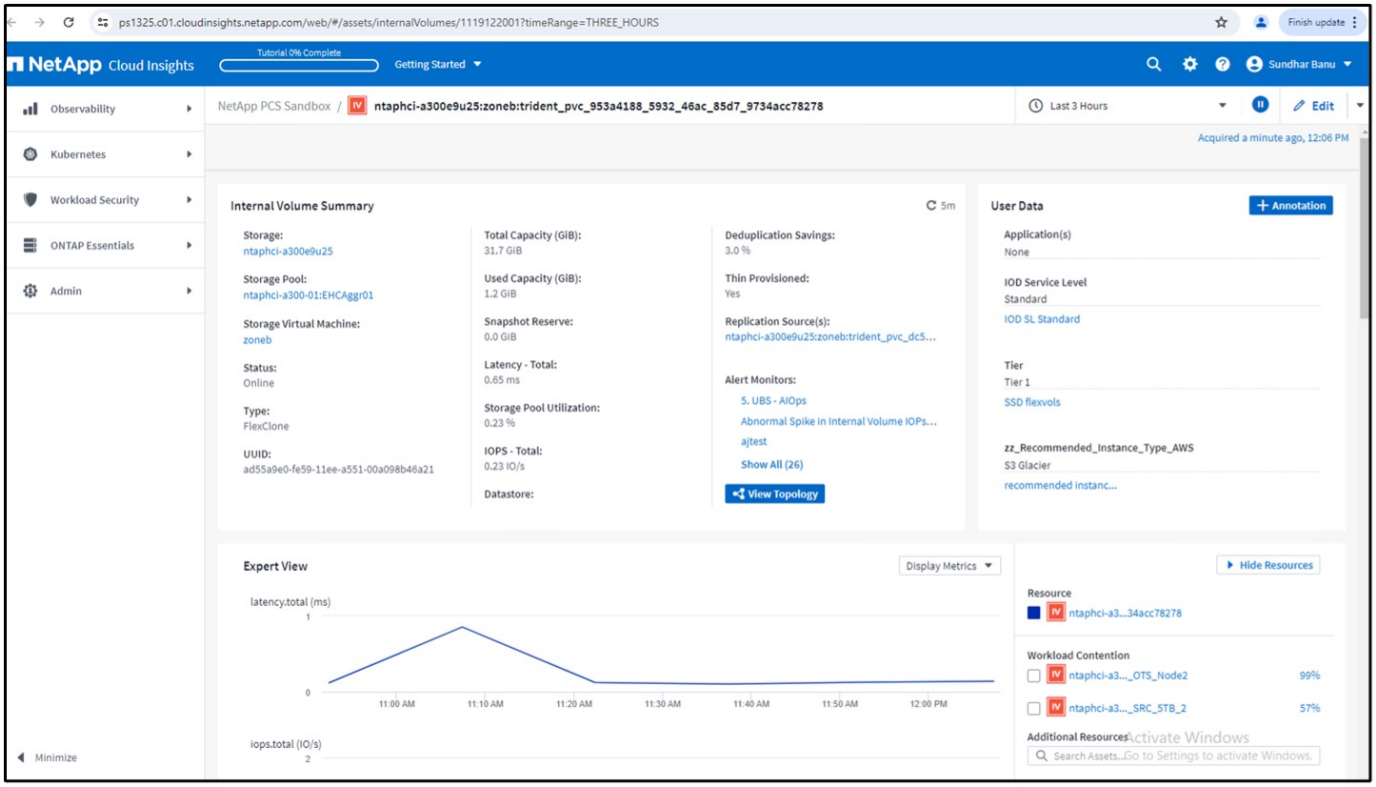


Back-End-Speicherzuordnung

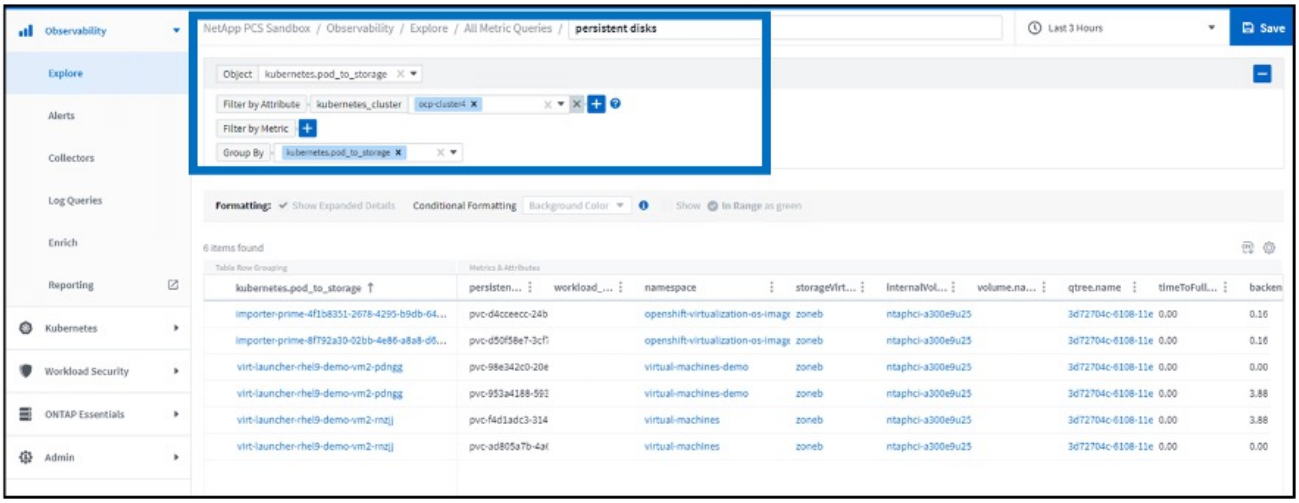
Mit Cloud Insights können Sie den Back-End Storage der VM-Festplatten und verschiedene Statistiken zu den VES problemlos einsehen.



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

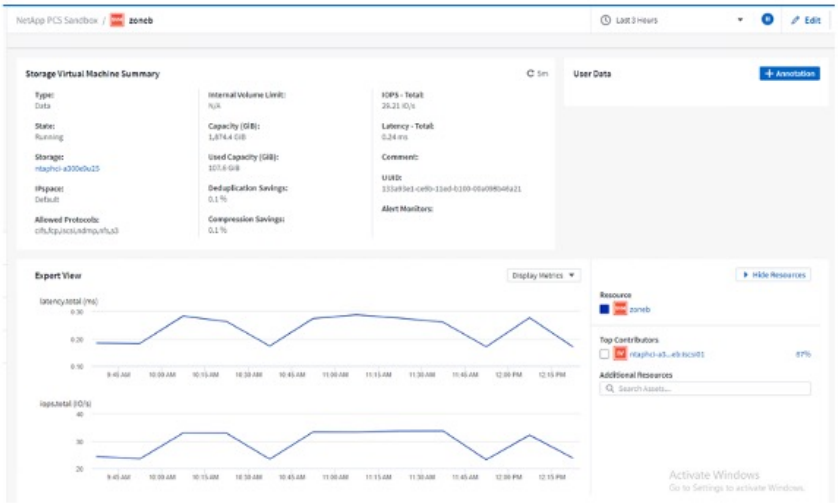


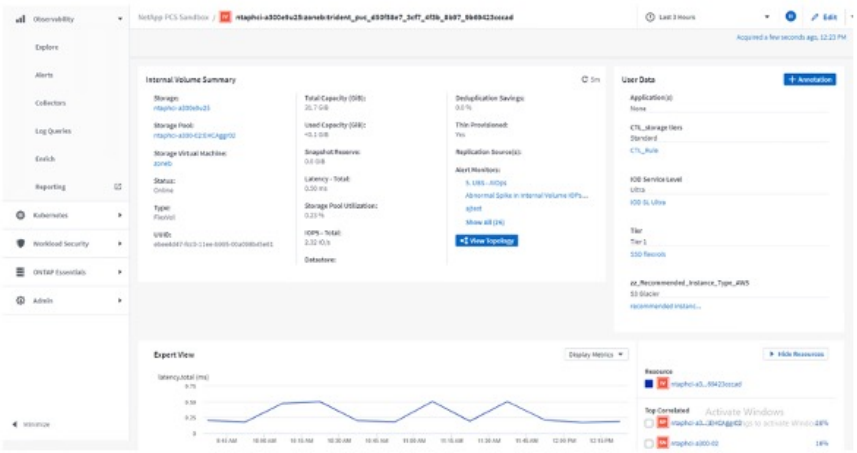
Eine weitere Möglichkeit, sich das gesamte Pod-zu-Storage-Mapping anzusehen, ist das Erstellen einer Abfrage „Alle Metriken“ aus dem Observability Menü unter Explore.



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	





Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

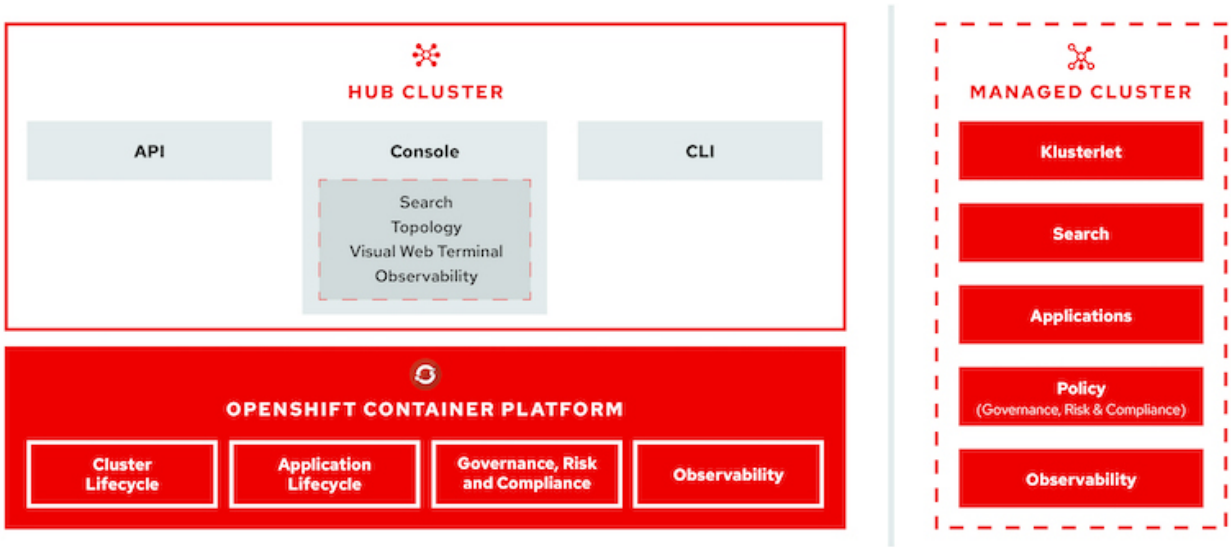
Advanced Cluster Management für Kubernetes: Red hat OpenShift mit NetApp

Für den Übergang von Container-Applikationen von der Entwicklung in die Produktion sind in vielen Unternehmen mehrere Red hat OpenShift Cluster erforderlich, um das Testen und die Implementierung dieser Applikation zu unterstützen. Dazu hosten Unternehmen in der Regel mehrere Anwendungen oder Workloads auf OpenShift-Clustern. Daher verwaltet jedes Unternehmen eine Reihe von Clustern. OpenShift-Administratoren müssen sich daher der zusätzlichen Herausforderung stellen, mehrere Cluster in einer Reihe von Umgebungen zu managen und zu warten, die sich auf mehrere lokale Datacenter und Public Clouds erstrecken. Um diese Herausforderungen zu bewältigen, hat Red hat das Advanced Cluster Management für Kubernetes eingeführt.

Mit Red hat Advanced Cluster Management für Kubernetes können Sie die folgenden Aufgaben ausführen:

1. Diverse Cluster lassen sich über Datacenter und Public Clouds hinweg erstellen, importieren und managen
2. Implementieren und managen Sie Applikationen oder Workloads über eine einzige Konsole auf mehreren Clustern
3. Überwachen und analysieren Sie den Zustand und den Status verschiedener Cluster-Ressourcen
4. Überwachung und Durchsetzung von Sicherheits-Compliance über mehrere Cluster hinweg

Red hat Advanced Cluster Management für Kubernetes wird als Add-on zu einem Red hat OpenShift-Cluster installiert und verwendet dieses Cluster als zentralen Controller für alle Vorgänge. Dieser Cluster wird als Hub-Cluster bezeichnet und stellt eine Managementebene bereit, über die Benutzer eine Verbindung zu Advanced Cluster Management herstellen können. Alle anderen OpenShift-Cluster, die entweder über die Advanced Cluster Management-Konsole importiert oder erstellt werden, werden vom Hub-Cluster gemanagt und werden als verwaltete Cluster bezeichnet. Es installiert einen Agent namens Klusterlet auf den gemanagten Clustern, um sie mit dem Hub-Cluster zu verbinden und Anfragen nach unterschiedlichen Aktivitäten im Zusammenhang mit Cluster Lifecycle Management, Applikations-Lifecycle-Management, Beobachtbarkeit und Sicherheits-Compliance zu erfüllen.



Weitere Informationen finden Sie in der Dokumentation "Hier".

Einsatz

Implementieren Sie Advanced Cluster Management für Kubernetes

Voraussetzungen

1. Ein Red hat OpenShift-Cluster (größer als Version 4.5) für den Hub-Cluster
2. Red hat OpenShift-Cluster (mehr als Version 4.4.3) für verwaltete Cluster
3. Cluster-Admin-Zugriff auf den Red hat OpenShift-Cluster
4. Eine Red hat Subskription für Advanced Cluster Management für Kubernetes

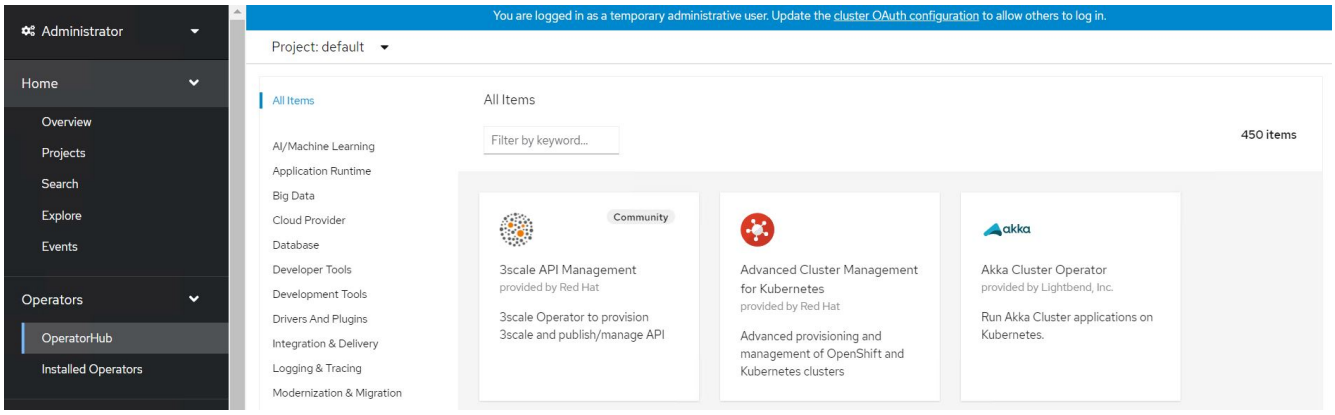
Advanced Cluster Management ist ein Add-On für den OpenShift-Cluster. Es gibt daher bestimmte Anforderungen und Einschränkungen für die Hardwareressourcen, die auf den Funktionen basieren, die auf dem Hub und den verwalteten Clustern verwendet werden. Sie müssen diese Probleme bei der Dimensionierung der Cluster berücksichtigen. Siehe Dokumentation "Hier" Entnehmen.

Wenn optional der Hub-Cluster dedizierte Nodes für das Hosting von Infrastrukturkomponenten hat und erweiterte Cluster-Management-Ressourcen nur auf diesen Nodes installiert werden sollen, müssen diesen Nodes entsprechend Tolerationen und Selektoren hinzugefügt werden. Weitere Informationen finden Sie in der Dokumentation "Hier".

Implementieren Sie Advanced Cluster Management für Kubernetes

So installieren Sie Advanced Cluster Management für Kubernetes auf einem OpenShift-Cluster:

1. Wählen Sie einen OpenShift-Cluster als Hub-Cluster aus und melden Sie sich mit Clusteradministratorrechten an.
2. Navigieren Sie zu Operators > Operators Hub, und suchen Sie nach Advanced Cluster Management für Kubernetes.



3. Wählen Sie Advanced Cluster Management für Kubernetes aus, und klicken Sie auf Installieren.

4. Geben Sie im Bildschirm „Install Operator“ die erforderlichen Details ein (NetApp empfiehlt, die Standardparameter zu behalten), und klicken Sie auf Install.

OperatorHub > Operator Installation

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

- release-2.0
- release-2.1
- release-2.2

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 open-cluster-management

Namespace creation
Namespace **open-cluster-management** does not exist and will be created.

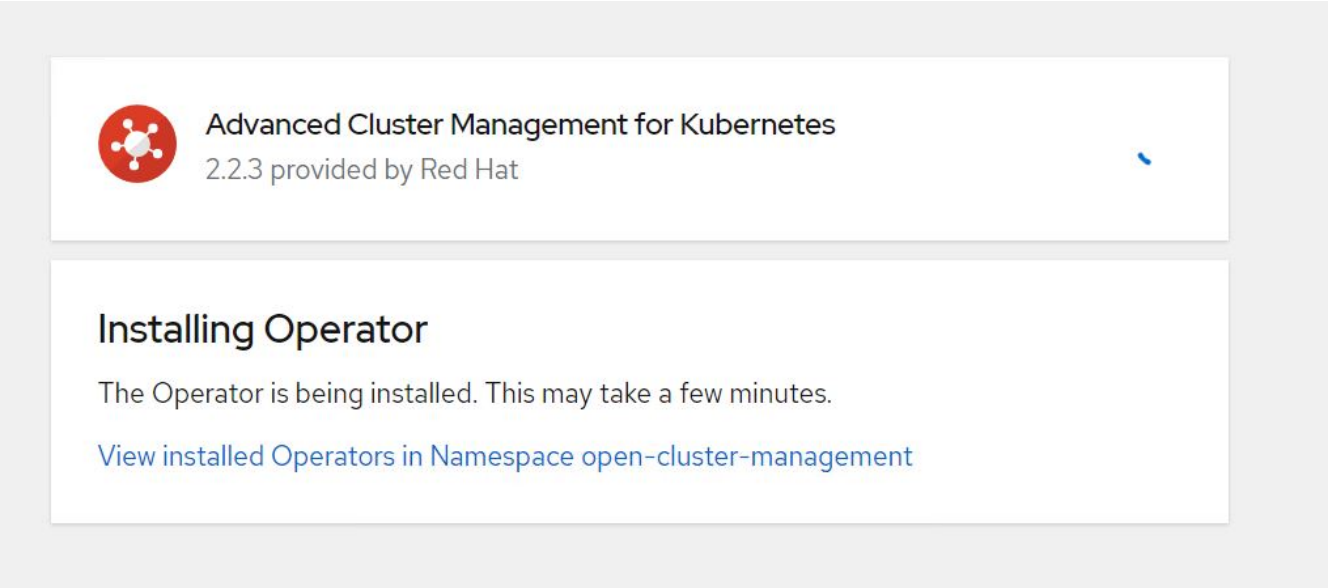
- Select a Namespace

Approval strategy *

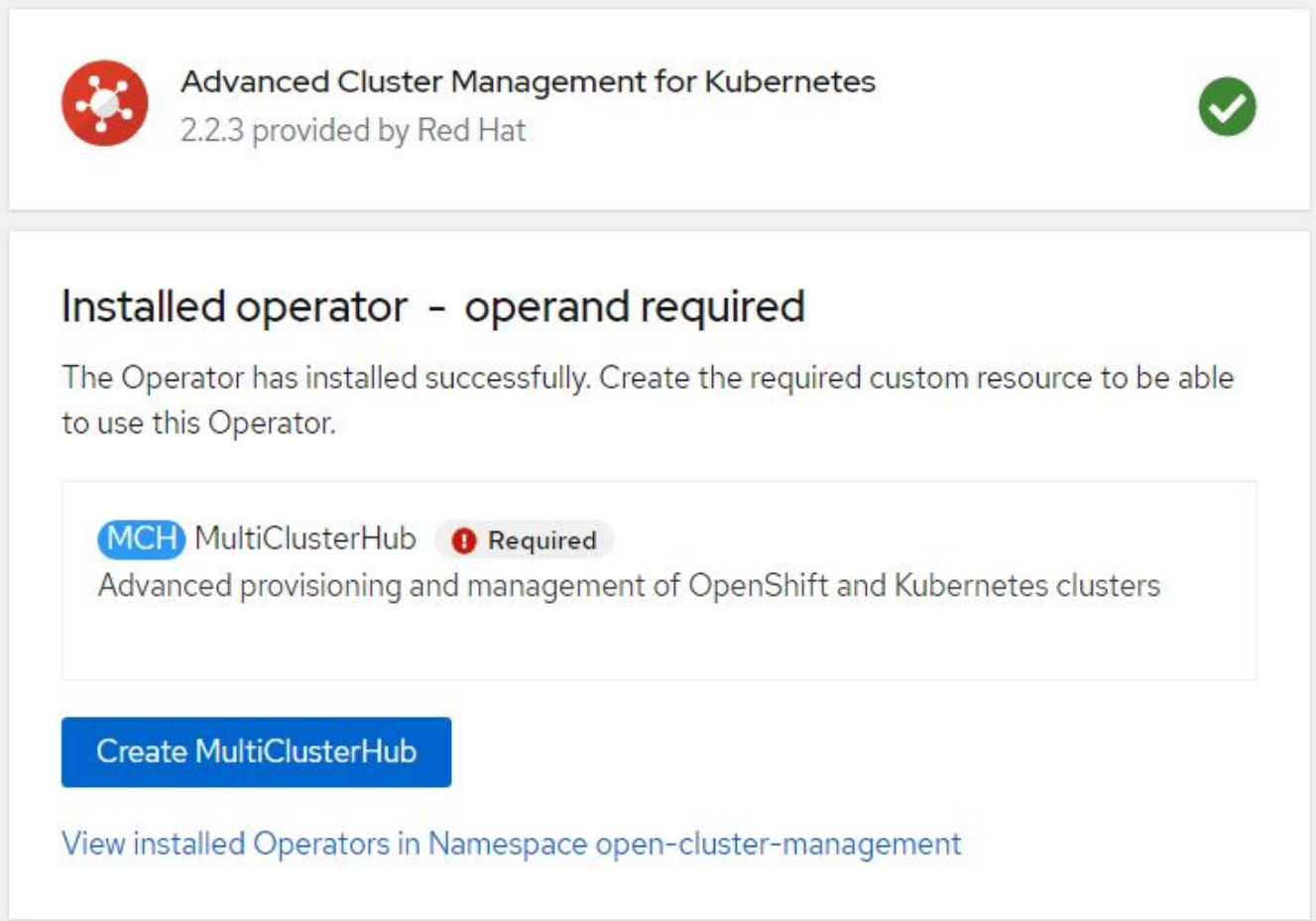
- Automatic
- Manual

Install Cancel

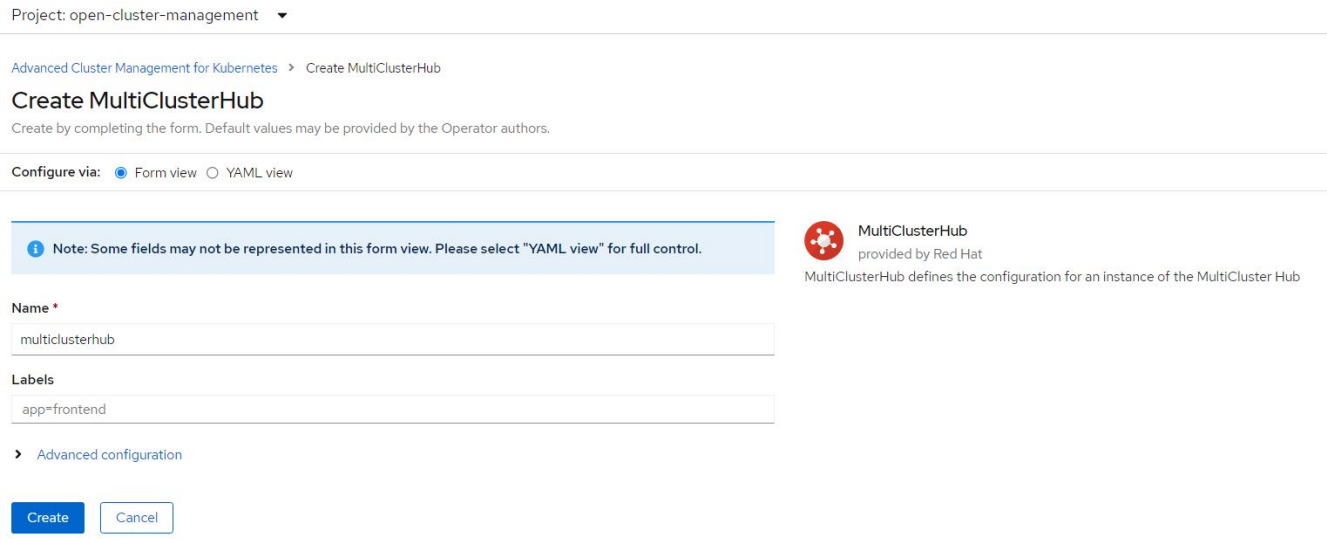
5. Warten Sie, bis die Installation des Bedieners abgeschlossen ist.



6. Klicken Sie nach der Installation des Operators auf MultiClusterHub erstellen.



7. Klicken Sie auf dem Bildschirm MultiClusterHub erstellen nach Einrichtung der Details auf Erstellen. Hierdurch wird die Installation eines Multi-Cluster-Hubs initiiert.



8. Nachdem alle Pods im Open-Cluster-Management Namespace in den aktiven Status verschoben und der Operator in den Status „erfolgreich“ verlagert wurde, wird Advanced Cluster Management für Kubernetes installiert.

Project: open-cluster-management

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 | Search by name...

Name	Managed Namespaces	Status	Provided APIs
Advanced Cluster Management for Kubernetes 2.2.3 provided by Red Hat	NS open-cluster-management	Succeeded Up to date	MultiClusterHub ClusterManager ClusterDeployment ClusterState View 25 more...

9. Es dauert einige Zeit, bis die Hub-Installation abgeschlossen ist, und anschließend wechselt der Multicluster-Hub in den laufenden Zustand.

Installed Operators > Operator details

Advanced Cluster Management for Kubernetes
2.2.3 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | MultiClusterHub | ClusterManager | ClusterDeployment | ClusterSt

MultiClusterHubs

Create MultiClusterHub

Name | Search by name...

Name	Kind	Status	Labels
MCH multiclusterhub	MultiClusterHub	Phase: Running	No labels

10. Der Service erstellt eine Route im Open-Cluster-Management Namespace. Stellen Sie eine Verbindung mit der URL auf der Route her, um auf die Konsole für die erweiterte Cluster-Verwaltung zuzugreifen.

Project: open-cluster-management

Routes

Create Route

Filter | Name | mul

Name mul ✕ Clear all filters

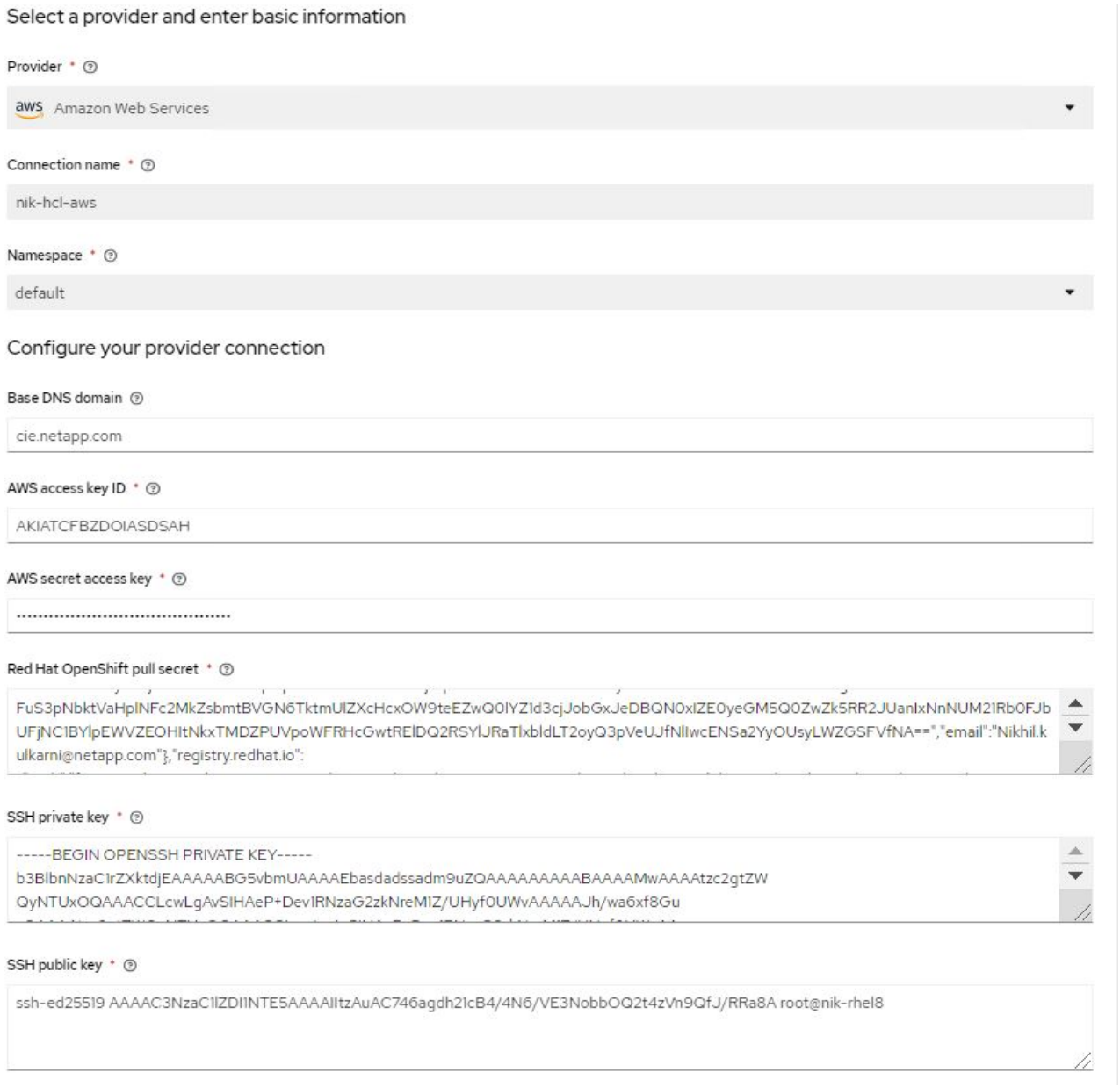
Name	Status	Location	Service
RT multicloud-console	Accepted	https://multicloud-console.apps.ocp-vmware2.cie.netapp.com	S management-ingress

Merkmale: Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

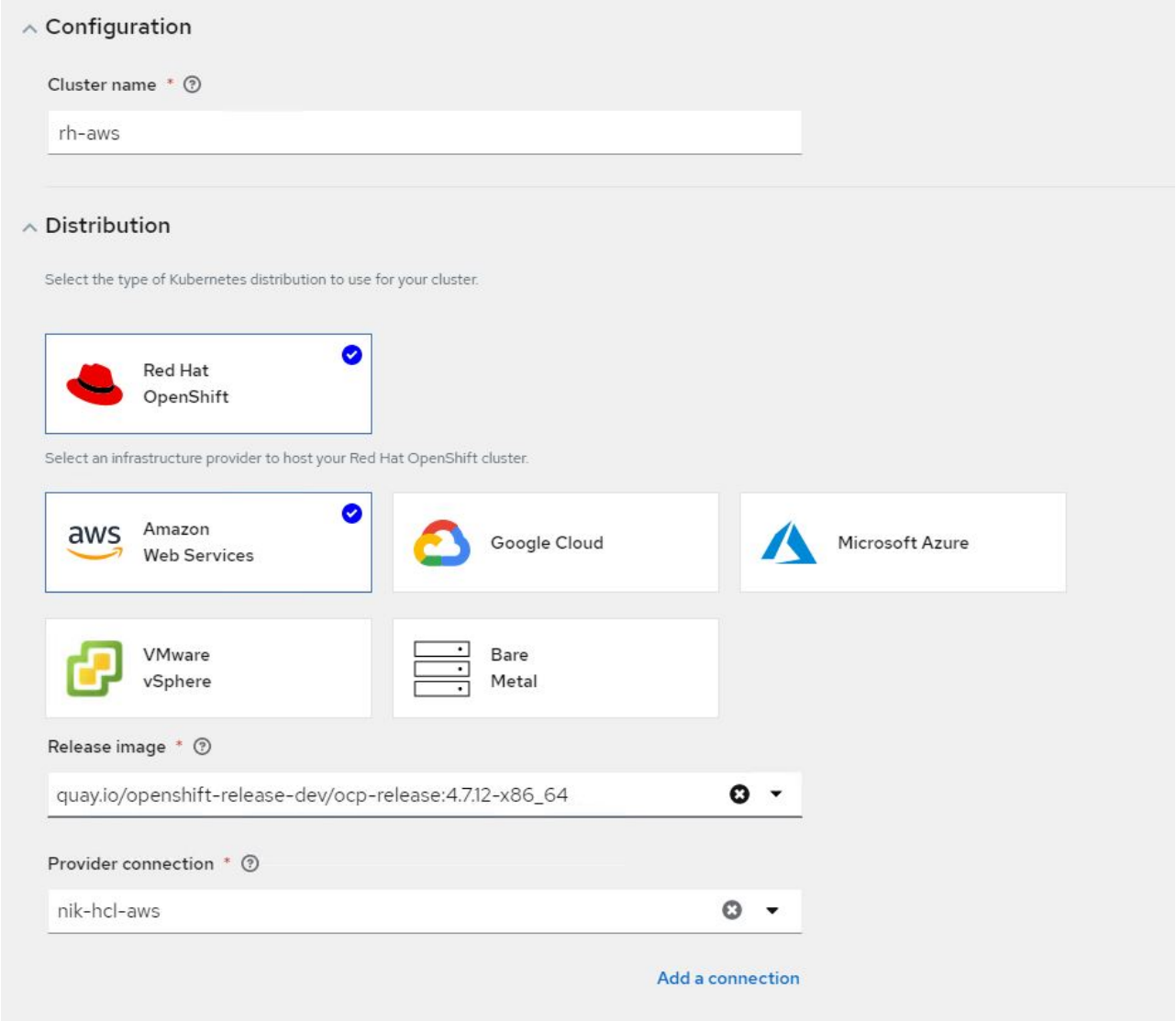
Cluster Lifecycle Management

Um unterschiedliche OpenShift-Cluster zu verwalten, können Sie sie entweder erstellen oder in Advanced Cluster Management importieren.

1. Navigieren Sie zunächst zu „Automatisieren Sie Infrastrukturen“ > „Cluster“.
2. Gehen Sie wie folgt vor, um einen neuen OpenShift-Cluster zu erstellen:
   a. Erstellen Sie eine Provider-Verbindung: Navigieren Sie zu Provider Connections und klicken Sie auf Add a Connection, geben Sie alle Details zum ausgewählten Provider-Typ an, und klicken Sie auf Add.

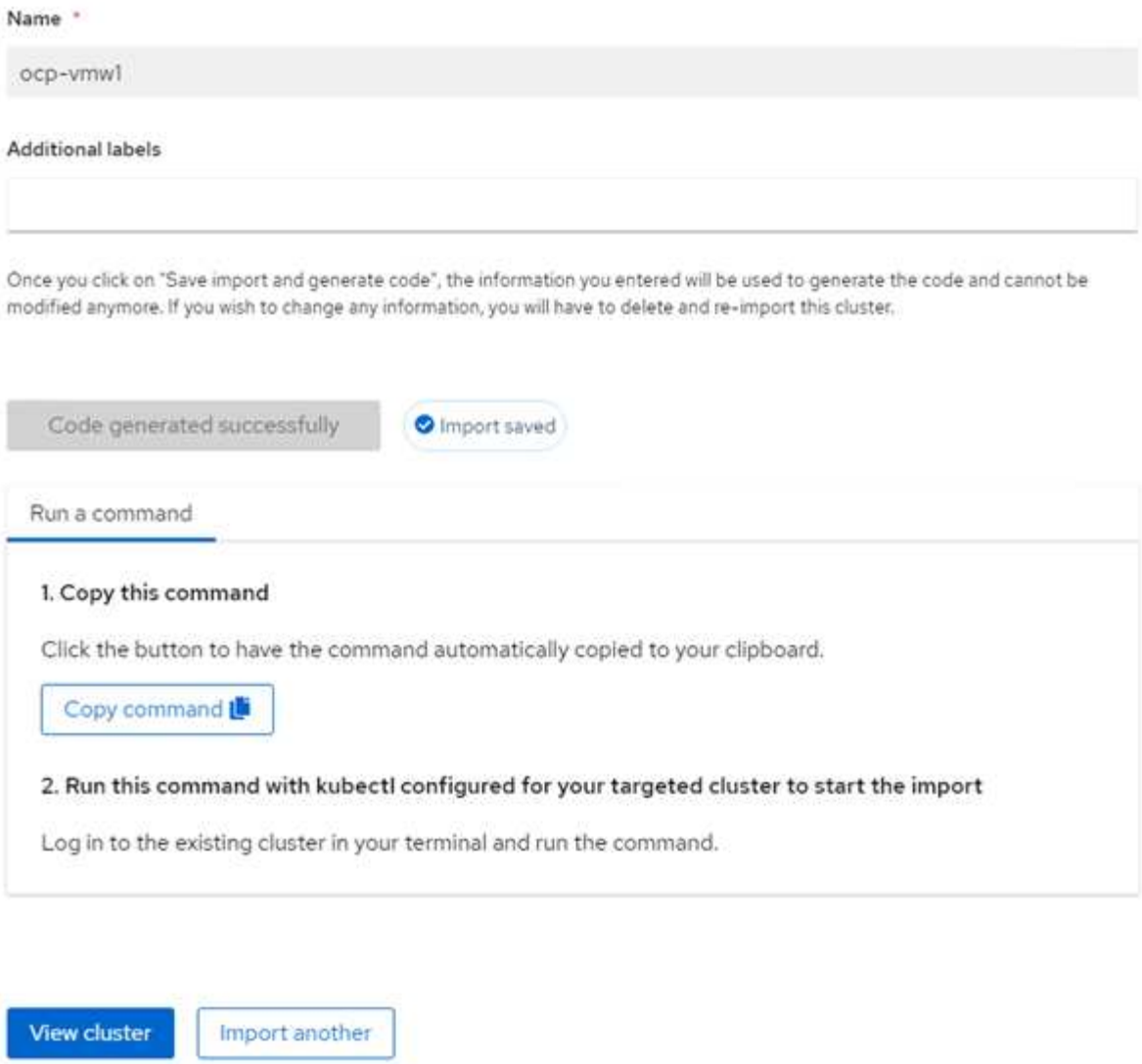


   b. Navigieren Sie zum Erstellen eines neuen Clusters zu Clusters und klicken Sie auf Cluster hinzufügen > Cluster erstellen. Geben Sie die Details für den Cluster und den entsprechenden Anbieter ein, und klicken Sie auf Erstellen.



c. Nach dem Erstellen des Clusters wird es in der Cluster-Liste mit dem Status „bereit“ angezeigt.

3. So importieren Sie ein vorhandenes Cluster:
   a. Navigieren Sie zu Clusters, und klicken Sie auf Cluster hinzufügen > vorhandenen Cluster importieren.
   b. Geben Sie den Namen des Clusters ein, und klicken Sie auf Importieren speichern und Code generieren. Ein Befehl zum Hinzufügen des vorhandenen Clusters wird angezeigt.
   c. Klicken Sie auf Copy Command und führen Sie den Befehl auf dem Cluster aus, der dem Hub-Cluster hinzugefügt werden soll. So wird die Installation der erforderlichen Agents im Cluster initiiert, und nach Abschluss dieses Vorgangs wird das Cluster in der Cluster-Liste mit Status Ready angezeigt.



4. Nachdem Sie mehrere Cluster erstellt und importiert haben, können Sie diese von einer einzigen Konsole aus überwachen und managen.

Merkmale: Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

Lifecycle Management von Applikationen

Um eine Anwendung zu erstellen und sie über mehrere Cluster hinweg zu verwalten,

1. Navigieren Sie in der Seitenleiste zu „Anwendungen verwalten“, und klicken Sie auf „Anwendung erstellen“. Geben Sie die Details der Anwendung an, die Sie erstellen möchten, und klicken Sie auf Speichern.

Applications /

Create an application YAML: Off

Cancel Save

Name*

demo-app

Namespace*

default

Repository location for resources

Repository types

Select the type of repository where resources that you want to deploy are located

Git

URL*

https://github.com/open-cluster-management/acm-hive-openshift-releases.git

Branch

main

Path

clusterImageSets/fast/4.7

2. Nach der Installation der Anwendungskomponenten wird die Anwendung in der Liste angezeigt.

Applications

Refresh every 15s

Last update: 7:36:23 PM

Overview Advanced configuration

Create application

Search

Name	Namespace	Clusters	Resource	Time window	Created
demo-app	default	Local	Git		8 days ago

1 - 1 of 1 1 of 1

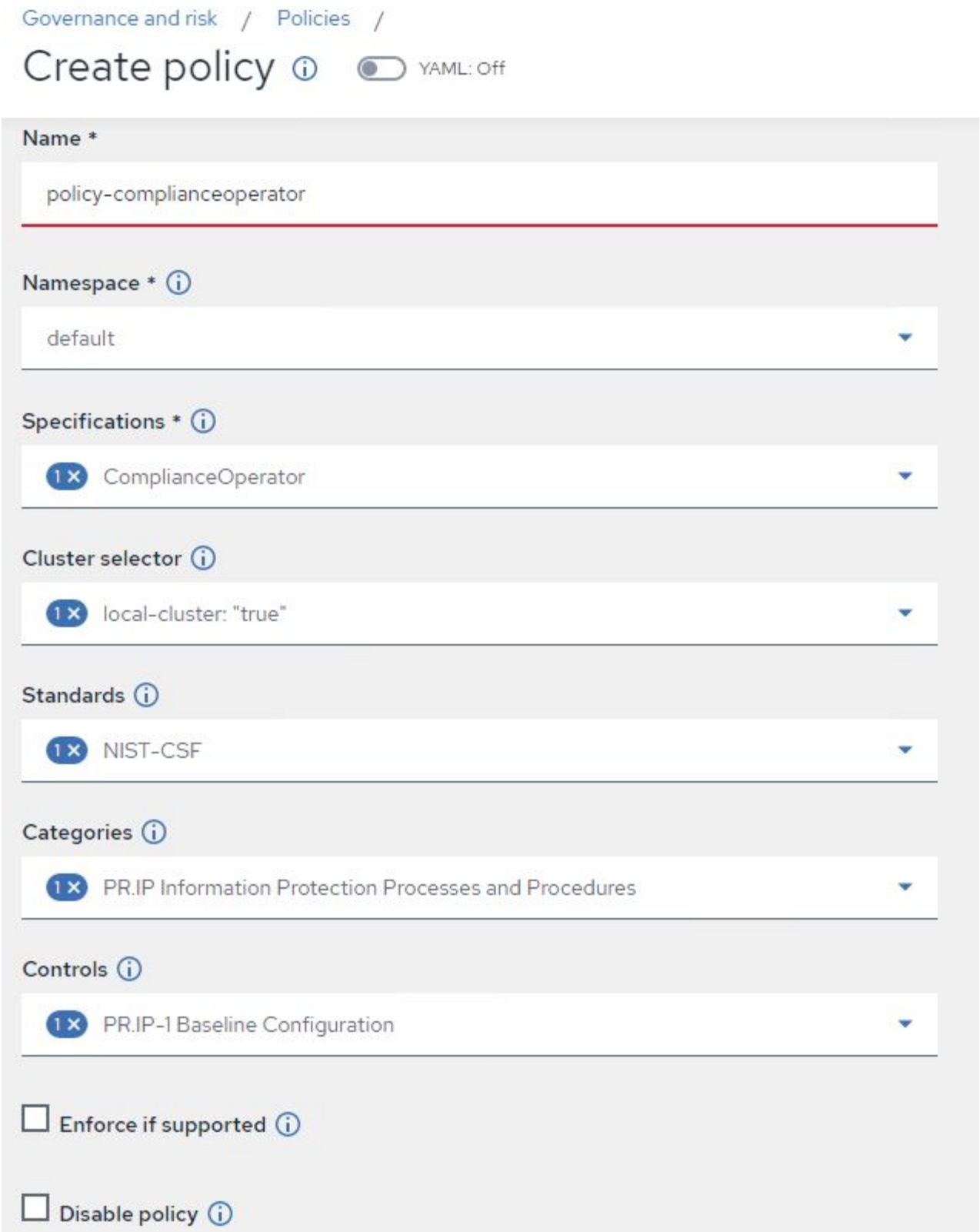
3. Die Anwendung kann nun über die Konsole überwacht und verwaltet werden.

Merkmale: Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

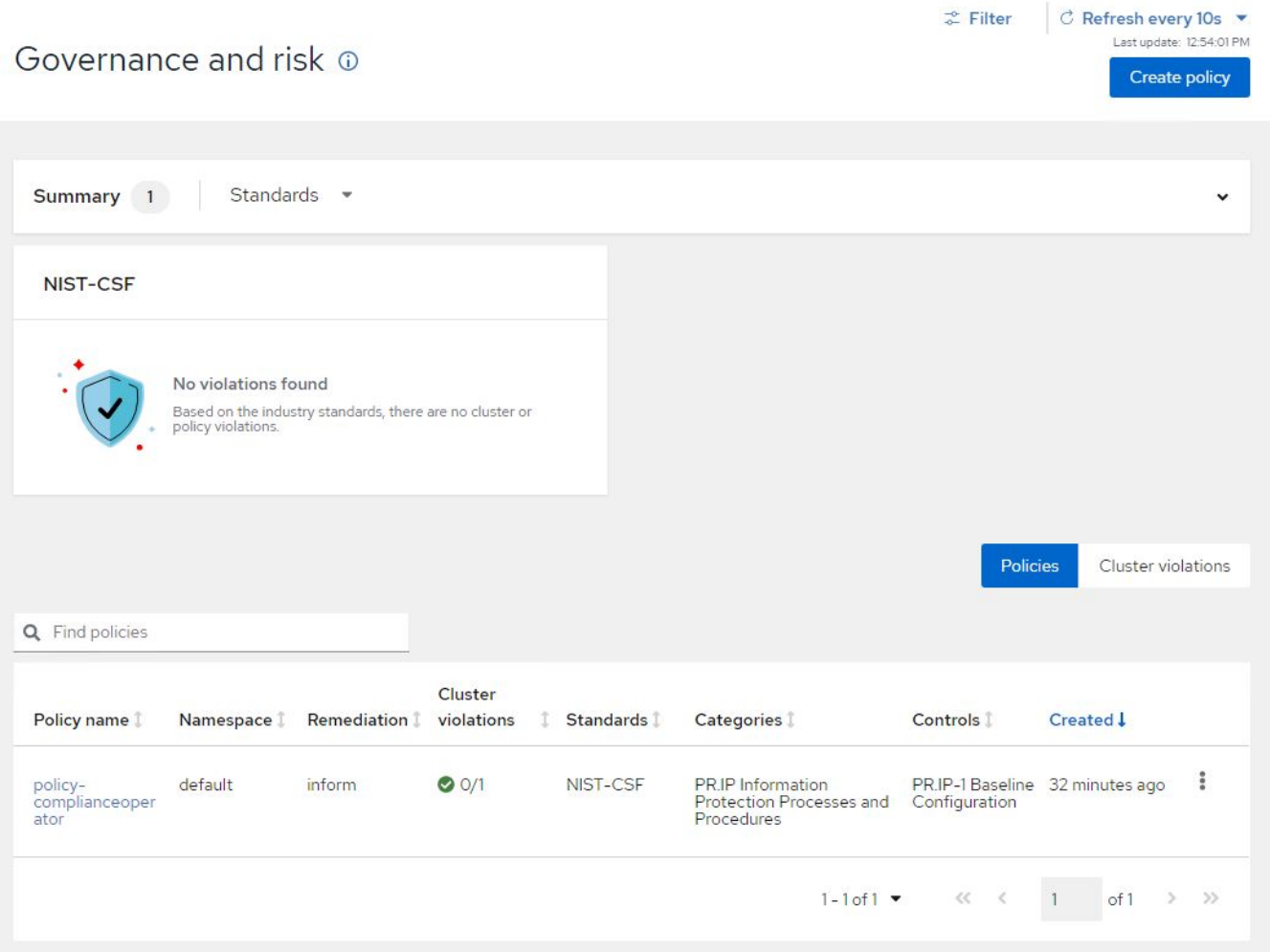
Governance und Risiko

Mit dieser Funktion können Sie Compliance-Richtlinien für verschiedene Cluster definieren und sicherstellen, dass die Cluster diesen Anforderungen entsprechen. Sie können die Richtlinien so konfigurieren, dass Abweichungen oder Verstöße gegen die Regeln informiert oder korrigiert werden.

1. Navigieren Sie über die Seitenleiste zu Governance und Risiko.
2. Um Compliance-Richtlinien zu erstellen, klicken Sie auf Create Policy, geben Sie die Details der Richtlinienstandards ein, und wählen Sie die Cluster aus, die dieser Richtlinie entsprechen sollen. Wenn Sie die Verstöße dieser Richtlinie automatisch beheben möchten, aktivieren Sie das Kontrollkästchen Enforce, falls unterstützt, und klicken Sie auf Create.



3. Nachdem alle erforderlichen Richtlinien konfiguriert wurden, können alle Richtlinien oder Cluster-Verstöße über das Advanced Cluster Management überwacht und korrigiert werden.

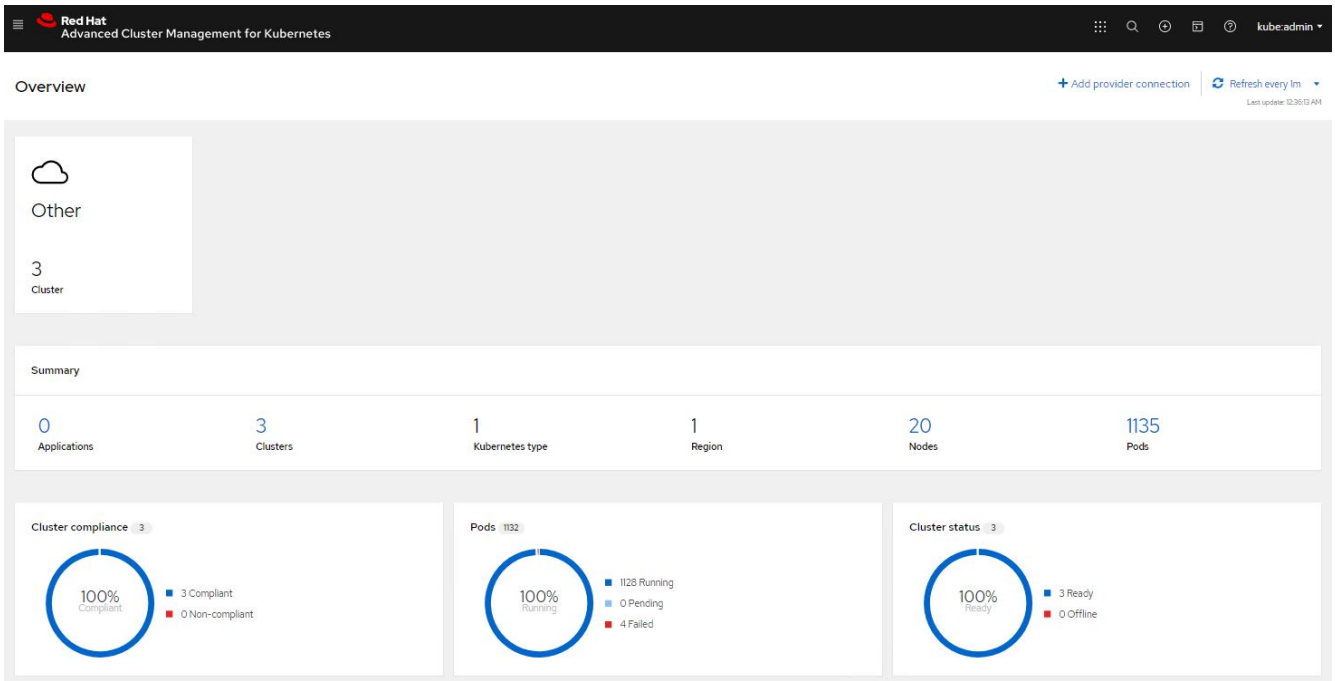


Merkmale: Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

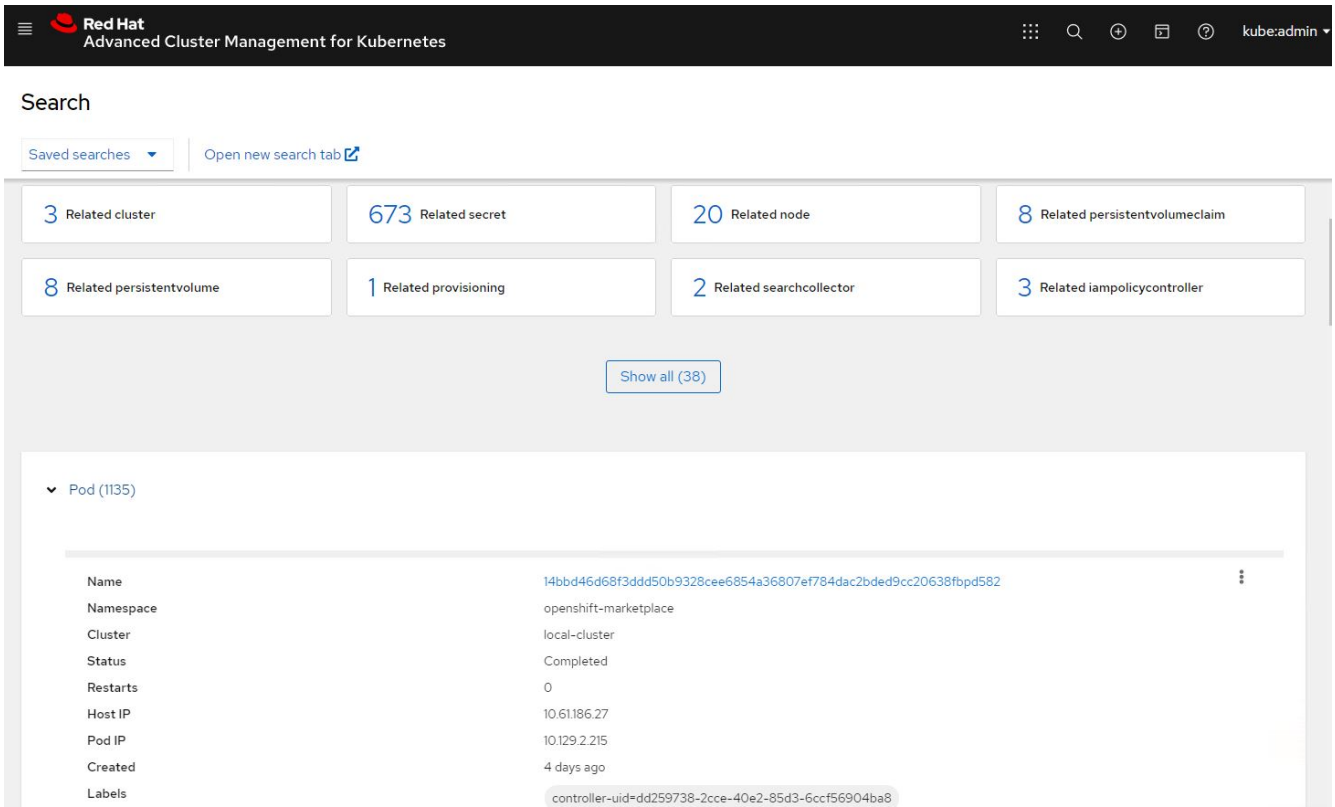
Beobachtbarkeit

Advanced Cluster Management für Kubernetes bietet eine Möglichkeit, Nodes, Pods und Applikationen sowie Workloads über alle Cluster hinweg zu überwachen.

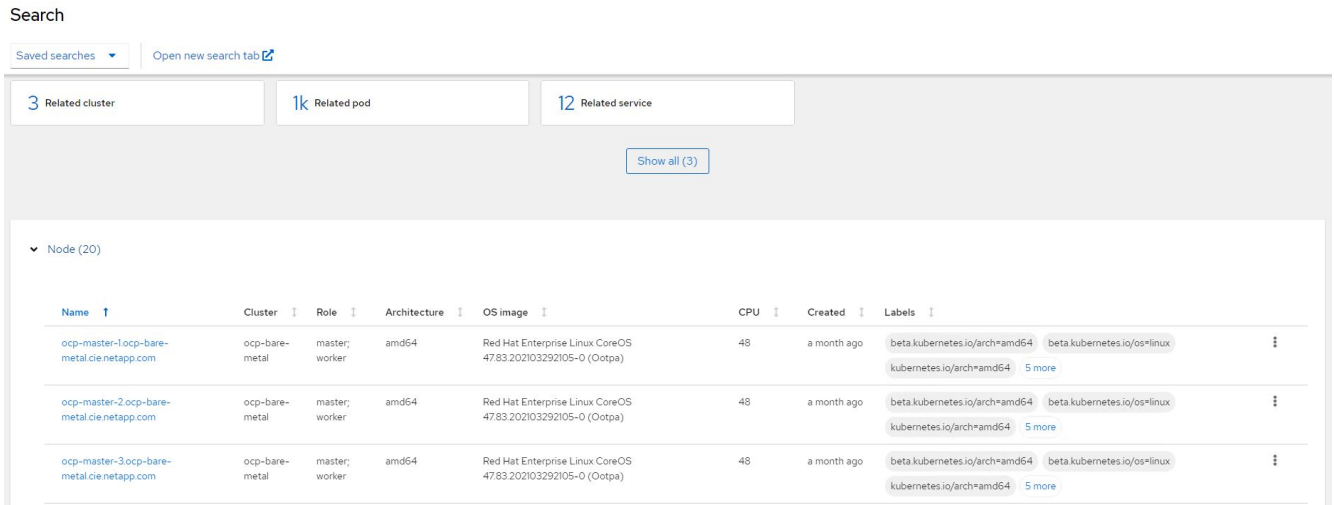
1. Navigieren Sie zu Umgebungen beobachten > Übersicht.



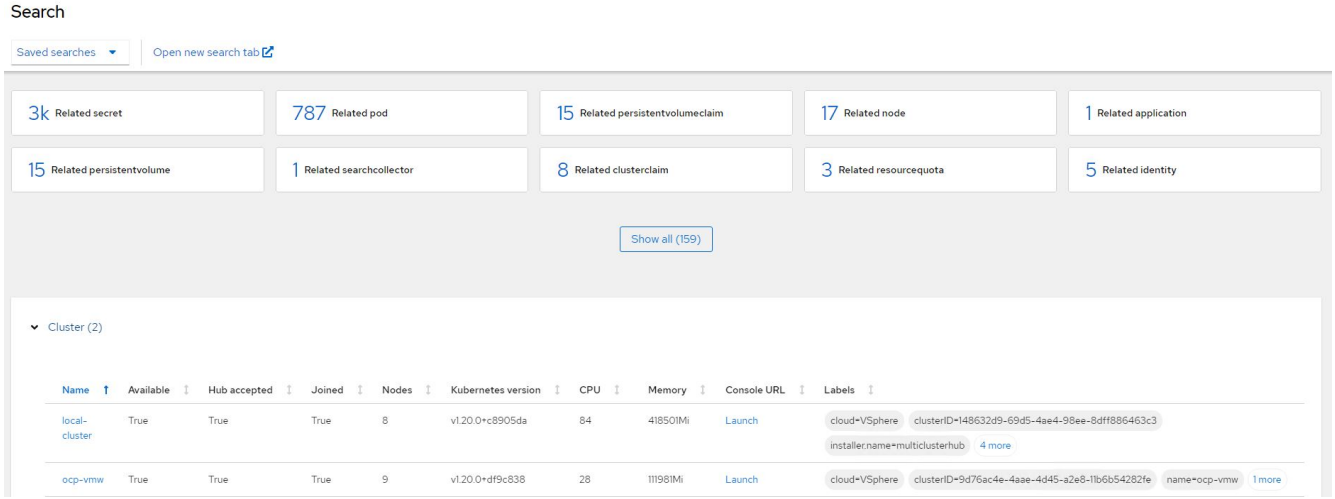
2. Alle Pods und Workloads über alle Cluster hinweg werden überwacht und basierend auf verschiedenen Filtern sortiert. Klicken Sie auf Pods, um die entsprechenden Daten anzuzeigen.



3. Alle Nodes in den Clustern werden auf Basis verschiedener Datenpunkte überwacht und analysiert. Klicken Sie auf Knoten, um mehr Informationen zu den entsprechenden Details zu erhalten.



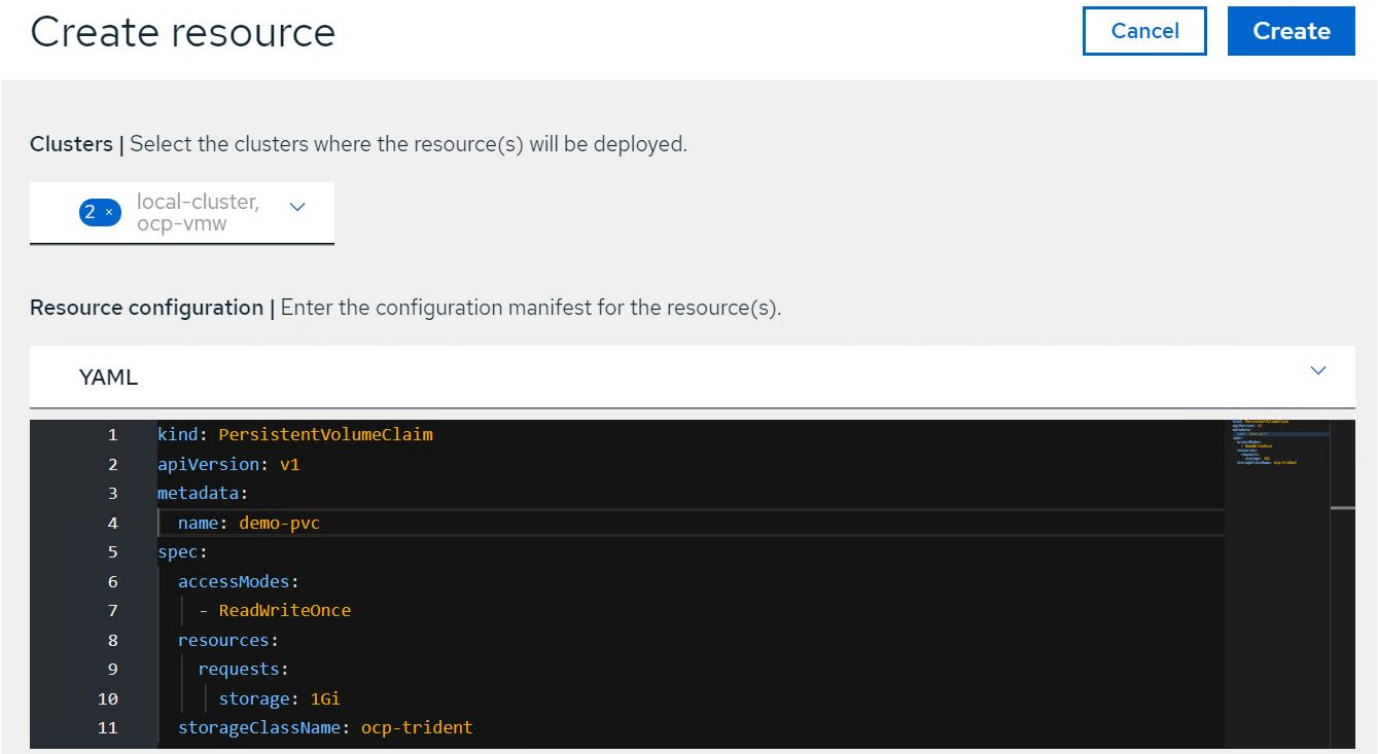
4. Alle Cluster werden basierend auf unterschiedlichen Cluster-Ressourcen und -Parametern überwacht und organisiert. Klicken Sie auf Cluster, um Cluster-Details anzuzeigen.



Merkmale: Erweitertes Cluster Management für Kubernetes auf Red hat OpenShift mit NetApp

Erstellen Sie Ressourcen auf mehreren Clustern

Dank erweitertem Cluster Management für Kubernetes können Benutzer Ressourcen auf einem oder mehreren gemanagten Clustern gleichzeitig über die Konsole erstellen. Wenn Sie beispielsweise OpenShift-Cluster an verschiedenen Standorten mit unterschiedlichen NetApp ONTAP-Clustern haben und an beiden Standorten PVC bereitstellen möchten, können Sie in der oberen Leiste auf das (+)-Zeichen klicken. Wählen Sie dann die Cluster aus, auf denen Sie die PVC erstellen möchten, fügen Sie die Ressource YAML ein und klicken Sie auf Erstellen.



Videos und Demos: Red hat OpenShift mit NetApp

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

Mit Red hat MTV VMs zu OpenShift-Virtualisierung mit NetApp ONTAP-Speicher migrieren

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

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/"

- Astra Trident – Dokumentation

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Astra Control Center - Dokumentation

  "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/"

- Dokumentation der Red hat OpenStack Platform

  "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/"

- Dokumentation zu VMware vSphere

  "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 Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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