



# Installation und Konfiguration

## FlexPod

NetApp  
October 30, 2025

This PDF was generated from <https://docs.netapp.com/de-de/flexpod/hybrid-cloud/flexpod-rho-cvo-flexpod-for-openshift-container-platform-4-bare-metal-installation.html> on October 30, 2025. Always check docs.netapp.com for the latest.

# Inhalt

- Installation und Konfiguration ..... 1
  - FlexPod für OpenShift Container Platform 4 Bare-Metal-Installation ..... 1
    - FlexPod for OpenShift Container Platform 4 auf VMware-Installation ..... 1
  - Red hat OpenShift auf AWS ..... 2
  - NetApp Cloud Volumes ONTAP ..... 3
  - Astra Control Center-Installation auf OpenShift Container Platform ..... 3
    - Umgebungsanforderungen ..... 4
    - Installieren Sie Astra Control Center mit OpenShift OperatorHub ..... 5
    - Einrichten des Astra Control Center ..... 19

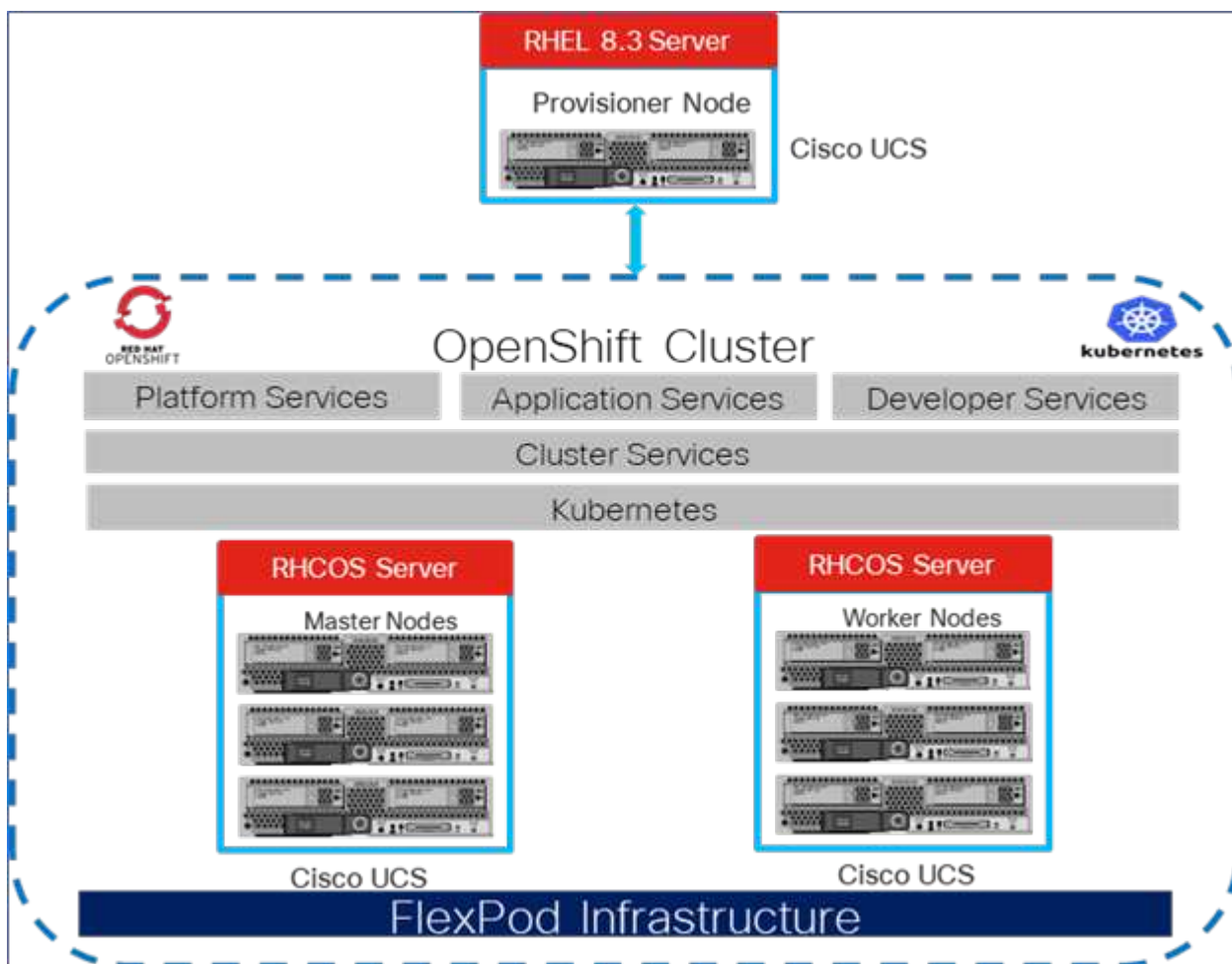
# Installation und Konfiguration

## FlexPod für OpenShift Container Platform 4 Bare-Metal-Installation

"Früher: Lösungskomponenten."

Weitere Informationen zum Bare-Metal-Design, den Implementierungsdetails und der Installation und Konfiguration von NetApp Astra Trident finden Sie unter FlexPod for OpenShift Container Platform 4 "[FlexPod mit OpenShift Cisco Validated Design and Deployment Guide \(CVD\)](#)". Dieses CVD deckt die Implementierung der FlexPod- und OpenShift-Container-Plattform mit Ansible ab. Das CVD bietet auch detaillierte Informationen zum Vorbereiten von Worker-Nodes, zur Astra Trident-Installation, zum Storage-Backend und zu Storage-Klassenkonfigurationen. Diese sind die wenigen Voraussetzungen für die Implementierung und Konfiguration des Astra Control Center.

Die folgende Abbildung zeigt OpenShift Container Platform 4 Bare Metal auf FlexPod.

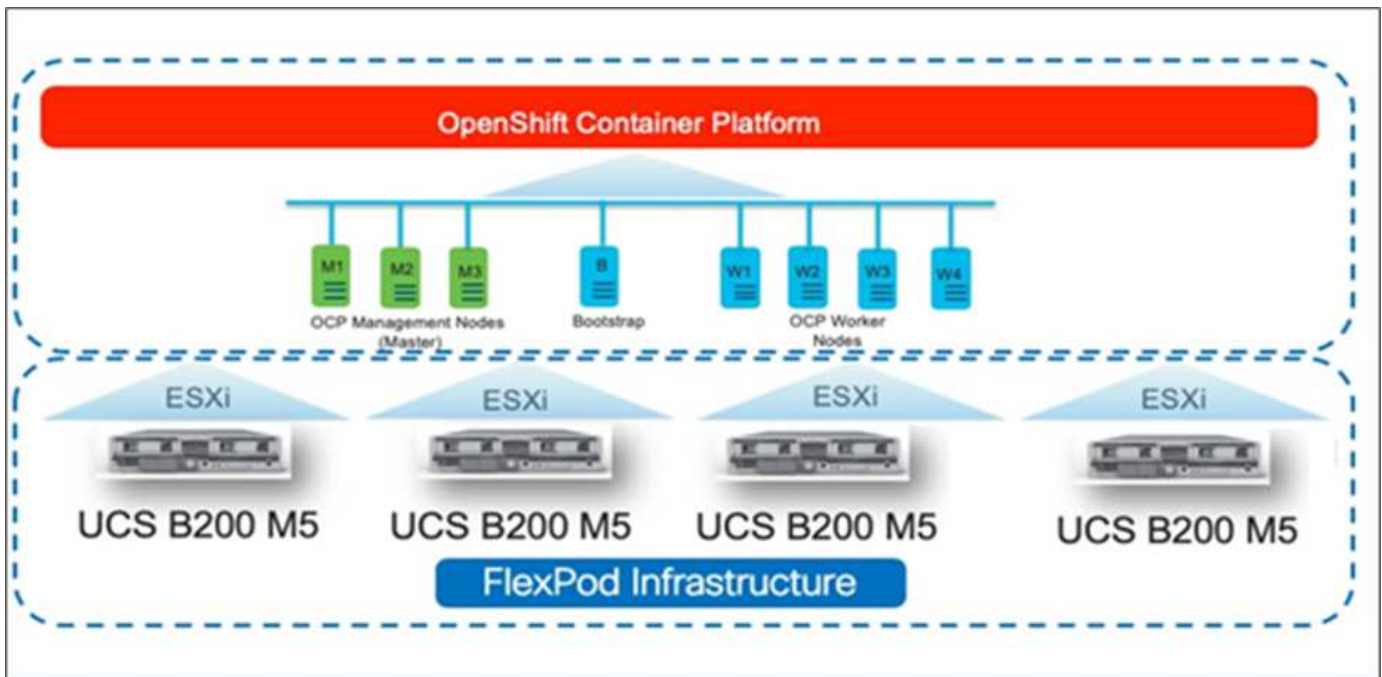


## FlexPod for OpenShift Container Platform 4 auf VMware-Installation

Weitere Informationen zur Bereitstellung der Red hat OpenShift-Container-Plattform 4 auf FlexPod mit VMware

vSphere finden Sie unter ["FlexPod-Datacenter für OpenShift-Container-Plattform 4"](#).

Die folgende Abbildung zeigt FlexPod für OpenShift Container Plattform 4 auf vSphere.



"Nächste Frage: Red hat OpenShift auf AWS"

## Red hat OpenShift auf AWS

"Früher: FlexPod für OpenShift Container Plattform 4 Bare-Metal-Installation."

Ein separater selbst verwalteter OpenShift-Container-Plattform-4-Cluster wird auf AWS als DR-Standort bereitgestellt. Die Master- und Worker-Nodes erstrecken sich auf drei Verfügbarkeitszonen, um Hochverfügbarkeit zu gewährleisten.

Instances (6) <a href="#">Info</a>								
<input type="text" value="Search"/>								
<input type="button" value="OCP"/> <input type="button" value="X"/> <input type="button" value="Clear filters"/>								
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name	
<input type="checkbox"/>	ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	-	
<input type="checkbox"/>	ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	-	
<input type="checkbox"/>	ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	-	
<input type="checkbox"/>	ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	-	
<input type="checkbox"/>	ocpaws-v58kn-worker-us-east-1b-7nmhc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	-	
<input type="checkbox"/>	ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	-	

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
ip-172-30-164-128.ec2.internal	Ready	worker	29m	v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal	Ready	master	36m	v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal	Ready	master	33m	v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal	Ready	worker	30m	v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal	Ready	master	36m	v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal	Ready	worker	28m	v1.22.8+f34b40c

OpenShift ist als bereitgestellter Einsatz "[Privater Cluster](#)" zu einer vorhandenen VPC auf AWS. Ein privates Cluster der OpenShift Container Platform weist keine externen Endpunkte auf und ist nur über ein internes Netzwerk zugänglich und nicht für das Internet sichtbar. Mit NetApp Cloud Manager wird eine NetApp Single-Node Cloud Volumes ONTAP implementiert, die ein Storage-Back-End für Astra Trident bietet.

Weitere Informationen zur Installation von OpenShift auf AWS finden Sie unter "[OpenShift-Dokumentation](#)".

"Weiter: [NetApp Cloud Volumes ONTAP](#)."

## NetApp Cloud Volumes ONTAP

"Früher: [Red hat OpenShift auf AWS](#)."

Die NetApp Cloud Volumes ONTAP Instanz ist auf AWS implementiert und dient als Backend-Storage für Astra Trident. Bevor Sie eine Cloud Volumes ONTAP Arbeitsumgebung hinzufügen, muss ein Connector bereitgestellt werden. Der Cloud-Manager fordert Sie auf, wenn Sie versuchen, die erste Cloud Volumes ONTAP-Arbeitsumgebung ohne entsprechenden Connector zu erstellen. Informationen zur Implementierung eines Connectors in AWS finden Sie unter "[Einen Konnektor erstellen](#)".

Informationen zur Implementierung von Cloud Volumes ONTAP auf AWS finden Sie unter "[Schnellstart für AWS](#)".

Nach der Implementierung von Cloud Volumes ONTAP können Sie Astra Trident installieren und das Storage-Back-End und die Snapshot-Klasse auf dem OpenShift Container Platform Cluster konfigurieren.

"Als Nächstes: [Astra Control Center-Installation auf OpenShift Container Platform](#)."

## Astra Control Center-Installation auf OpenShift Container Platform

"Früher [NetApp Cloud Volumes ONTAP](#)."

Sie können Astra Control Center entweder auf OpenShift-Cluster auf FlexPod oder auf AWS mit einem Cloud Volumes ONTAP-Storage-Back-End installieren. In dieser Lösung wird Astra Control Center auf dem Bare-Metal-Cluster OpenShift implementiert.

Astra Control Center kann mit dem beschriebenen Standardprozess installiert werden "[Hier](#)" Oder über den Red hat OpenShift OperatorHub. Astra Control Operator ist ein Red hat zertifizierter Operator. In dieser Lösung

wird Astra Control Center mit dem Red hat OperatorHub installiert.

## Umgebungsanforderungen

- Astra Control Center unterstützt mehrere Kubernetes-Distributionen. Für Red hat OpenShift sind die unterstützten Versionen die Red hat OpenShift Container Platform 4.8 oder 4.9.
- Astra Control Center benötigt zusätzlich zu den Anforderungen der Anwendungsressourcen der Umgebung und des Endbenutzers folgende Ressourcen:

Komponenten	Anforderungen
Storage-Back-End-Kapazität	Mindestens 500 GB verfügbar
Worker-Nodes	Mindestens 3 Worker-Nodes mit 4 CPU-Kernen und 12 GB RAM
Vollständig qualifizierte Domänenname (FQDN)-Adresse	Eine FQDN-Adresse für Astra Control Center
Astra Trident	Astra Trident 21.04 oder höher ist installiert und konfiguriert
Eingangs-Controller oder Load-Balancer	Konfigurieren Sie den Ingress-Controller so, dass Astra Control Center mit einer URL oder einem Load-Balancer zur Bereitstellung von IP-Adressen bereitgestellt wird, die sich auf den FQDN beziehen

- Sie benötigen eine bereits vorhandene private Bildregistrierung, in die Sie die Astra Control Center-Bilder übertragen können. Sie müssen die URL der Bildregistrierung angeben, in der Sie die Bilder hochladen.



Einige Images werden bei der Ausführung bestimmter Workflows entfernt und Container werden bei Bedarf erstellt und zerstört.

- Astra Control Center erfordert, dass eine Storage-Klasse erstellt und als Standard-Storage-Klasse eingestellt wird. Astra Control Center unterstützt die folgenden ONTAP-Treiber von Astra Trident:
  - ontap-nas
  - ontap-nas-Flexgroup
  - ontap-san
  - ontap-san-Ökonomie



Astra Trident ist in den implementierten OpenShift-Clustern mit einem ONTAP-Back-End installiert und konfiguriert. Außerdem wird eine Standard-Storage-Klasse definiert.

- Zum Klonen von Applikationen in OpenShift-Umgebungen muss das Astra Control Center OpenShift erlauben, Volumes anzuhängen und die Eigentümerschaft von Dateien zu ändern. Um die ONTAP Exportrichtlinie zu ändern, um diese Vorgänge zu ermöglichen, führen Sie die folgenden Befehle aus:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```



Wenn Sie eine zweite OpenShift-Betriebsumgebung als gemanagte Computing-Ressource hinzufügen möchten, stellen Sie sicher, dass die Astra Trident Volume Snapshot-Funktion aktiviert ist. Lesen Sie den offiziellen Abschnitt zum Aktivieren und Testen von Volume-Snapshots mit Astra Trident "[Astra Trident Anweisungen](#)".

- A "[VolumeSnapClass](#)" Sollte auf allen Kubernetes-Clustern konfiguriert werden, von denen die Applikationen gemanagt werden. Dazu könnte auch der K8s-Cluster gehören, auf dem Astra Control Center installiert ist. Astra Control Center kann Anwendungen auf dem K8s-Cluster verwalten, auf dem es ausgeführt wird.

## Anforderungen für das Applikationsmanagement

- **Lizenzierung.** um Anwendungen mit Astra Control Center zu verwalten, benötigen Sie eine Astra Control Center-Lizenz.
- **Namespaces.** Ein Namespace ist die größte Instanz, die von Astra Control Center als Anwendung verwaltet werden kann. Sie können Komponenten anhand der Anwendungsbezeichnungen und benutzerdefinierten Beschriftungen in einem bestehenden Namespace herausfiltern und als Anwendung eine Untermenge von Ressourcen verwalten.
- **StorageClass.** Wenn Sie eine Anwendung mit einem explizit eingestellten StorageClass installieren und die Anwendung klonen müssen, muss das Zielcluster für den Klonvorgang die ursprünglich angegebene StorageClass haben. Klonen einer Applikation, deren StorageClass explizit auf Cluster festgelegt ist, die nicht dieselbe StorageClass aufweisen, schlägt fehl.
- **Kubernetes-Ressourcen.** Applikationen, die Kubernetes-Ressourcen nutzen, die nicht von Astra Control erfasst sind, verfügen möglicherweise nicht über umfassende Datenmanagementfunktionen für Applikationen. Astra Control kann die folgenden Kubernetes-Ressourcen erfassen:

Kubernetes-Ressourcen		
ClusterCoele	ClusterrollenBding	Konfigmap
KundenressourcenDefinition	Benutzerressource	Kronjob
DemonSet	Horizon PodAutoscaler	Eindringen
BereitstellungConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
Netzwerkrichtlinie	ReplicaSet	Rolle
Rollenverschwarten	Route	Geheim
ValidierenWebhook		

## Installieren Sie Astra Control Center mit OpenShift OperatorHub

Das folgende Verfahren installiert Astra Control Center mithilfe des Red hat OperatorHub. In dieser Lösung ist Astra Control Center auf einem Bare-Metal OpenShift Cluster installiert, das unter FlexPod ausgeführt wird.

1. Laden Sie das Astra Control Center Bundle herunter (astra-control-center-[version].tar.gz) Vom ["NetApp Support Website"](#).
2. Laden Sie die .zip-Datei für die Astra Control Center-Zertifikate und -Schlüssel aus dem herunter ["NetApp Support Website"](#).
3. Überprüfen Sie die Signatur des Bundles.

```
openssl dgst -sha256 -verify astra-control-center[version].pub  
-signature <astra-control-center[version].sig astra-control-  
center[version].tar.gz
```

4. Extrahieren Sie die Astra-Bilder.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Wechseln Sie in das Astra-Verzeichnis.

```
cd astra-control-center-[version]
```

6. Fügen Sie die Bilder Ihrer lokalen Registrierung hinzu.

```
For Docker:  
docker login [your_registry_path]OR  
For Podman:  
podman login [your_registry_path]
```

7. Verwenden Sie das entsprechende Skript, um die Bilder zu laden, die Bilder zu kennzeichnen und sie in Ihre lokale Registrierung zu übertragen.

Für Docker:

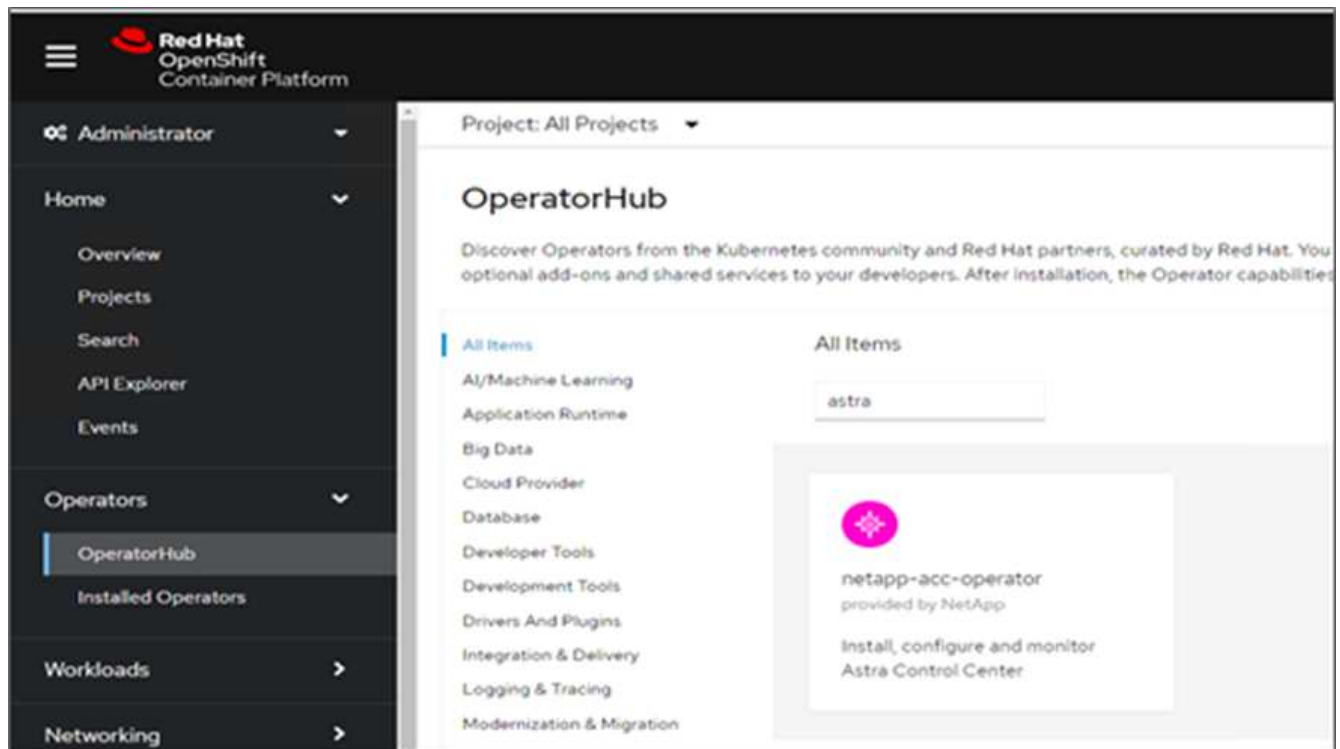
```
export REGISTRY=[Docker_registry_path]  
for astraImageFile in $(ls images/*.tar) ; do  
    # Load to local cache. And store the name of the loaded image trimming  
    the 'Loaded images: '  
    astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded  
image: //' )  
    astraImage=$(echo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



Für Podman:


```
export REGISTRY=[Registry_path]
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
```

8. Melden Sie sich bei der Bare-Metal OpenShift Cluster Webkonsole an. Wählen Sie im Menü „Seite“ die Option „Operatoren“ > „OperatorHub“. Eingabe astra Um die aufzulisten netapp-acc-operator.



netapp-acc-operator Ist ein zertifizierter Red hat OpenShift Operator und ist im OperatorHub-Katalog aufgeführt.

9. Wählen Sie netapp-acc-operator Und klicken Sie auf Installieren.



**netapp-acc-operator**  
 22.4.3 provided by NetApp

Install

**Latest version**  
 22.4.3

**Capability level**  
☒ Basic Install  
☐ Seamless Upgrades  
☐ Full Lifecycle  
☐ Deep Insights  
☐ Auto Pilot

**Source**  
 Certified

**Provider**  
 NetApp

Astra Control is an application-aware data management solution that manages, protects and moves data-rich Kubernetes workloads in both public clouds and on-premises.

Astra Control enables data protection, disaster recovery, and migration for your Kubernetes workloads, leveraging NetApp's industry-leading data management technology for snapshots, backups, replication and cloning.

**How to deploy Astra Control**  
 Refer to [Installation Procedure](#) to deploy Astra Control Center using the Operator.

**Documentation**  
 Refer to [Astra Control Center Documentation](#) to complete the setup and start managing applications.

**NOTE:** The version listed under *Latest version* on this page might not reflect the actual version of NetApp Astra Control Center you are installing. The version in the file name of the Astra Control Center bundle that you download from the NetApp Support Site is the version of Astra Control Center that will be installed.

10. Wählen Sie die entsprechenden Optionen aus, und klicken Sie auf Installieren.

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 \***


**Update approval \*** ⓘ  
☐ Automatic  
☒ Manual

**Namespace creation**  
 Namespace **netapp-acc-operator** does not exist and will be created.

**Manual approval applies to all operators in a namespace**  
 Installing an operator with manual approval causes all operators installed in namespace **netapp-acc-operator** to function as manual approval strategy. To allow automatic approval, all operators installed in the namespace must use automatic approval strategy.


**netapp-acc-operator**  
 provided by NetApp

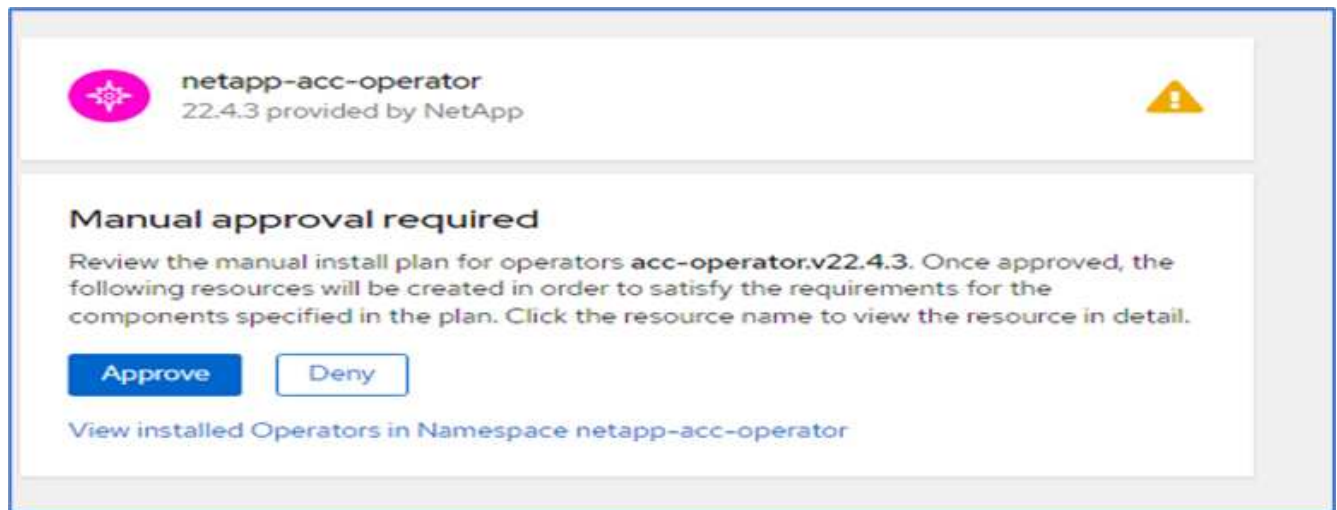
**Provided APIs**  


**Astra Control Center**  
 AstraControlCenter is the Schema for the astracontrolcenters API.

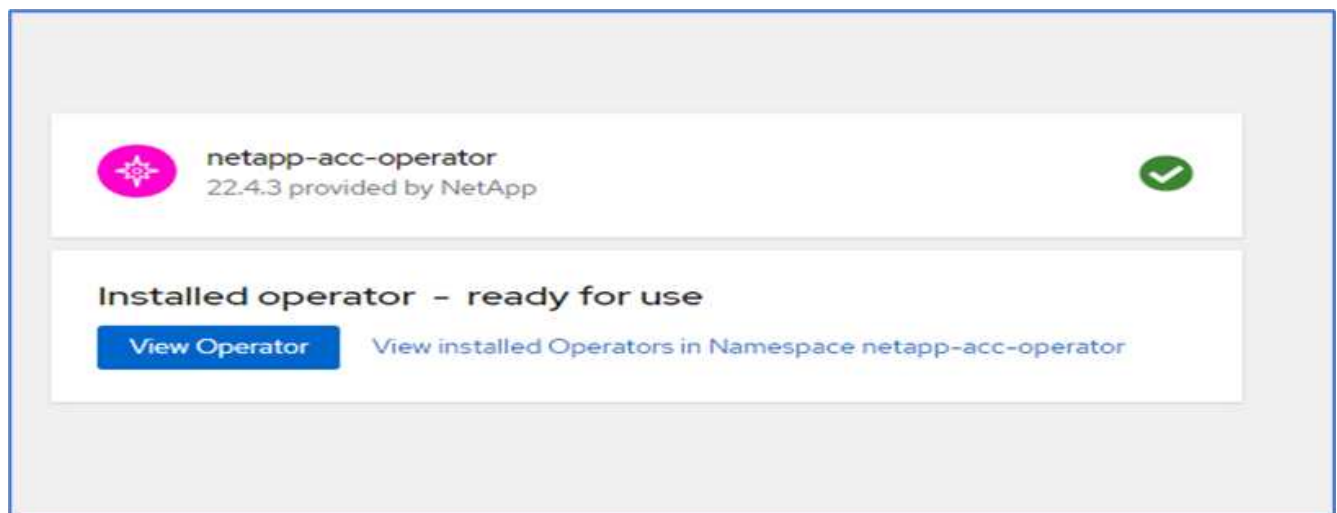
Install

Cancel

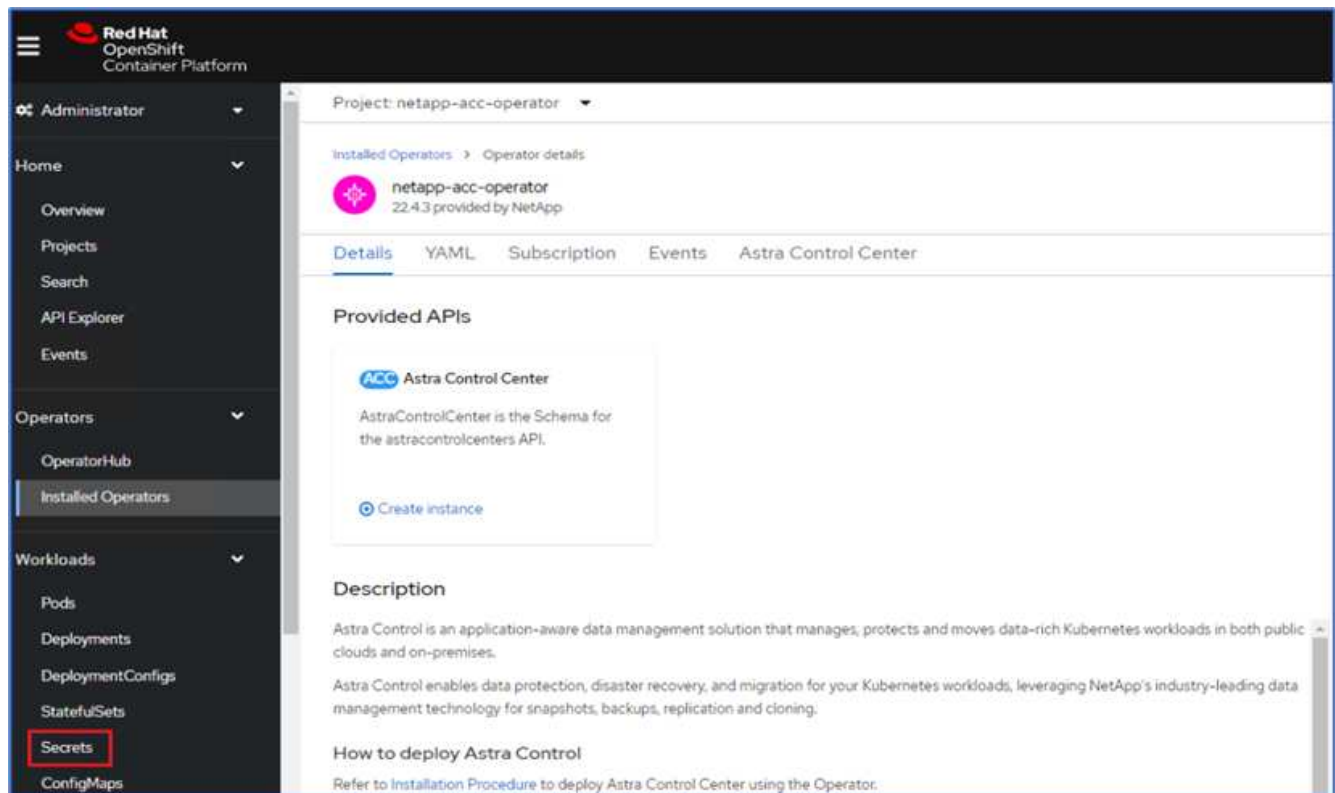
11. Genehmigen Sie die Installation, und warten Sie, bis der Bediener installiert ist.



12. In dieser Phase ist der Bediener erfolgreich installiert und betriebsbereit. Klicken Sie auf Ansichtsverwalter, um die Installation des Astra Control Centers zu starten.



13. Erstellen Sie vor der Installation von Astra Control Center das Pull Secret, um Astra-Bilder aus der Docker-Registry, die Sie früher verschoben haben, herunterzuladen.



14. Damit Sie die Astra Control Center-Bilder von Ihrer privaten Docker-Repo abrufen können, sollten Sie im ein Geheimnis schaffen `netapp-acc-operator` Namespace. Dieser geheime Name wird in einem späteren Schritt im Astra Control Center YAML-Manifest angegeben.

Project: netapp-acc-operator ▼

## Create image pull secret

Image pull secrets let you authenticate against a private image registry.

**Secret name \***

Unique name of the new secret.

**Authentication type**

**Registry server address \***

For example quay.io or docker.io

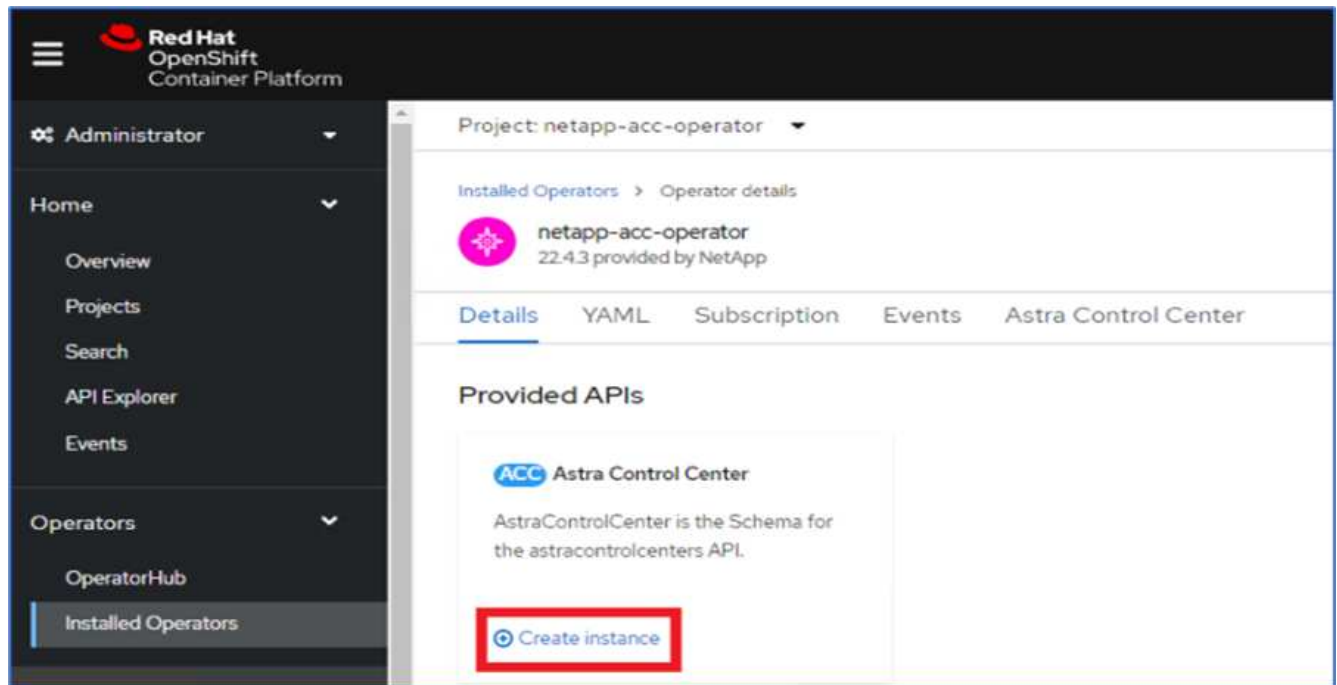
**Username \***

**Password \***

**Email**

[+ Add credentials](#)

15. Wählen Sie im Seitenmenü Operatoren > Installed Operators aus, und klicken Sie im Abschnitt bereitgestellte APIs auf Create Instance.



16. Füllen Sie das Formular AstraControlCenter erstellen aus. Geben Sie den Namen, die Astra-Adresse und die Astra-Version an.

The screenshot shows the 'Create AstraControlCenter' form. The form is titled 'Create AstraControlCenter' and includes a note: 'Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.' The form fields are:

- Name \***: acc
- Labels**: .app=frontend
- Auto Support \***: A checkbox for 'AutoSupport' is checked. The text below states: 'AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. An internet connection is required (port 442) and all support data is anonymized. The default election is true and indicates no 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.'
- Astra Address \***: acc.ocp.flexpod.netapp.com. The text below states: '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 \***: 22.04.0. The text below states: 'Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch'



Geben Sie unter Astra Address die FQDN-Adresse für Astra Control Center an. Diese Adresse wird für den Zugriff auf die Astra Control Center Webkonsole verwendet. Der FQDN sollte auch in einem erreichbaren IP-Netzwerk auflösen und im DNS konfiguriert werden.

17. Geben Sie einen Kontonamen, eine E-Mail-Adresse, einen Administrator-Nachnamen ein, und behalten

Sie die standardmäßige Richtlinie zur Rückgewinnung von Volumes bei. Wenn Sie einen Load Balancer verwenden, setzen Sie den Ingress-Typ auf `AccTraefik`. Wählen Sie andernfalls `Generic` für aus `Ingress.Controller`. Geben Sie unter Image Registry den Registry-Pfad für das Container-Image und den geheimen Schlüssel ein.

The screenshot shows the configuration interface for the 'netapp-acc-operator' project. The left sidebar contains a navigation menu with items like Administrator, Home, Operators, Workloads, Networking, Storage, Builds, Observe, Compute, User Management, and Administration. The main content area is titled 'Project: netapp-acc-operator' and contains several configuration sections:

- Account Name:** A text input field containing 'ocp'.
- Email:** A text input field containing 'abhinav3@netapp.com'.
- Last Name:** A text input field containing 'Singh'.
- Volume Reclaim Policy:** A dropdown menu set to 'Retain'.
- Ingress Type:** A dropdown menu set to 'AccTraefik'.
- Astra Kube Config Secret:** A text input field.
- Image Registry:** A section with a dropdown arrow, containing:
  - Name:** A text input field with a placeholder value.
  - Secret:** A text input field containing 'astra-registry-cred'.



In dieser Lösung wird der Metallb Load Balancer eingesetzt. Daher ist der Eingangstyp `AccTraefik`. Das Astra Control Center Trafik Gateway wird damit als Kubernetes Service des Typ Load Balancer bereitgestellt.

18. Geben Sie den Vornamen des Administrators ein, konfigurieren Sie die Skalierung von Ressourcen und stellen Sie die Storage-Klasse bereit. Klicken Sie auf Erstellen .

**Image Registry**

The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

**First Name**  
Abhinav

The first name of the SRE supporting Astra

**Astra Resources Scaler**  
Default

Scaling options for AstraControlCenter Resource limits.

**Storage Class**  
ocp-nas-sc-gold

The storage class to be used for PVCs. If not set, default storage class will be used.

**Crds**

Options for how ACC should handle CRDs. Options for how ACC should handle CRDs. Options for how ACC should handle CRDs. Options for how ACC should handle CRDs.

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

Der Status der Astra Control Center-Instanz sollte von „Bereitstellen“ auf „bereit“ geändert werden.

Project: netapp-acc-operator

Installed Operators > Operator details

netapp-acc-operator  
22.43 provided by NetApp

Details | YAML | Subscription | Events | **Astra Control Center** | Actions

**AstraControlCenters** [Create AstraControlCenter](#)

Name Search by name...

Name	Kind	Status	Labels	Last updated
ACC acc	AstraControlCenter	Conditions: Ready, PostInstallComplete, Deployed	appacc	8 minutes ago

- Überprüfen Sie, ob alle Systemkomponenten erfolgreich installiert wurden und alle Pods ausgeführt werden.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                     READY   STATUS    RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v         1/1     Running   0           10m
acc-operator-controller-manager-5c656c44c6-tqnmn 2/2     Running   0           13m
```



activity-589c6d59f4-x2sfs	1/1	Running	0
6m4s			
api-token-authentication-4q5lj	1/1	Running	0
5m26s			
api-token-authentication-pzptd	1/1	Running	0
5m27s			
api-token-authentication-tbtg6	1/1	Running	0
5m27s			
asup-669df8d49-qps54	1/1	Running	0
5m26s			
authentication-5867c5f56f-dnpp2	1/1	Running	0
3m54s			
bucket-service-85495bc475-5zcc5	1/1	Running	0
5m55s			
cert-manager-67f486bbc6-txhh6	1/1	Running	0
9m5s			
cert-manager-cainjector-75959db744-4l5p5	1/1	Running	0
9m6s			
cert-manager-webhook-765556b869-g6wdf	1/1	Running	0
9m6s			
cloud-extension-5d595f85f-txrfl	1/1	Running	0
5m27s			
cloud-insights-service-674649567b-5s4wd	1/1	Running	0
5m49s			
composite-compute-6b58d48c69-46vhc	1/1	Running	0
6m11s			
composite-volume-6d447fd959-chnrt	1/1	Running	0
5m27s			
credentials-66668f8ddd-8qc5b	1/1	Running	0
7m20s			
entitlement-fd6fc5c58-wxnmh	1/1	Running	0
6m20s			
features-756bbb7c7c-rgcrm	1/1	Running	0
5m26s			
fluent-bit-ds-278pg	1/1	Running	0
3m35s			
fluent-bit-ds-5pqc6	1/1	Running	0
3m35s			
fluent-bit-ds-8l7cq	1/1	Running	0
3m35s			
fluent-bit-ds-9qbft	1/1	Running	0
3m35s			
fluent-bit-ds-nj475	1/1	Running	0
3m35s			
fluent-bit-ds-x9pd8	1/1	Running	0
3m35s			

graphql-server-698d6f4bf-kftwc	1/1	Running	0
3m20s			
identity-5d4f4c87c9-wjz6c	1/1	Running	0
6m27s			
influxdb2-0	1/1	Running	0
9m33s			
krakend-657d44bf54-8cb56	1/1	Running	0
3m21s			
license-594bbdc-rghdg	1/1	Running	0
6m28s			
login-ui-6c65fbbbd4-jg8wz	1/1	Running	0
3m17s			
loki-0	1/1	Running	0
9m30s			
metrics-facade-75575f69d7-hnlk6	1/1	Running	0
6m10s			
monitoring-operator-65dff79cfb-z78vk	2/2	Running	0
3m47s			
nats-0	1/1	Running	0
10m			
nats-1	1/1	Running	0
9m43s			
nats-2	1/1	Running	0
9m23s			
nautilus-7bb469f857-4hlc6	1/1	Running	0
6m3s			
nautilus-7bb469f857-vz94m	1/1	Running	0
4m42s			
openapi-8586db4bcd-gwvtf	1/1	Running	0
5m41s			
packages-6bdb949cfb-nrq8l	1/1	Running	0
6m35s			
polaris-consul-consul-server-0	1/1	Running	0
9m22s			
polaris-consul-consul-server-1	1/1	Running	0
9m22s			
polaris-consul-consul-server-2	1/1	Running	0
9m22s			
polaris-mongodb-0	2/2	Running	0
9m22s			
polaris-mongodb-1	2/2	Running	0
8m58s			
polaris-mongodb-2	2/2	Running	0
8m34s			
polaris-ui-5df7687dbd-trcnf	1/1	Running	0
3m18s			

polaris-vault-0 9m18s	1/1	Running	0
polaris-vault-1 9m18s	1/1	Running	0
polaris-vault-2 9m18s	1/1	Running	0
public-metrics-7b96476f64-j88bw 5m48s	1/1	Running	0
storage-backend-metrics-5fd6d7cd9c-vc4j 5m59s	1/1	Running	0
storage-provider-bb85ff965-m7qrq 5m25s	1/1	Running	0
telegraf-ds-4zqgz 3m36s	1/1	Running	0
telegraf-ds-cp9x4 3m36s	1/1	Running	0
telegraf-ds-h4n59 3m36s	1/1	Running	0
telegraf-ds-jnp2q 3m36s	1/1	Running	0
telegraf-ds-pdz5j 3m36s	1/1	Running	0
telegraf-ds-znqtp 3m36s	1/1	Running	0
telegraf-rs-rt64j 3m36s	1/1	Running	0
telemetry-service-7dd9c74bfc-sfkzt 6m19s	1/1	Running	0
tenancy-d878b7fb6-wf8x9 6m37s	1/1	Running	0
traefik-6548496576-5v2g6 98s	1/1	Running	0
traefik-6548496576-g82pq 3m8s	1/1	Running	0
traefik-6548496576-psn49 38s	1/1	Running	0
traefik-6548496576-qrkfd 2m53s	1/1	Running	0
traefik-6548496576-srs6r 98s	1/1	Running	0
trident-svc-679856c67-78kbt 5m27s	1/1	Running	0
vault-controller-747d664964-xmn6c 7m37s	1/1	Running	0

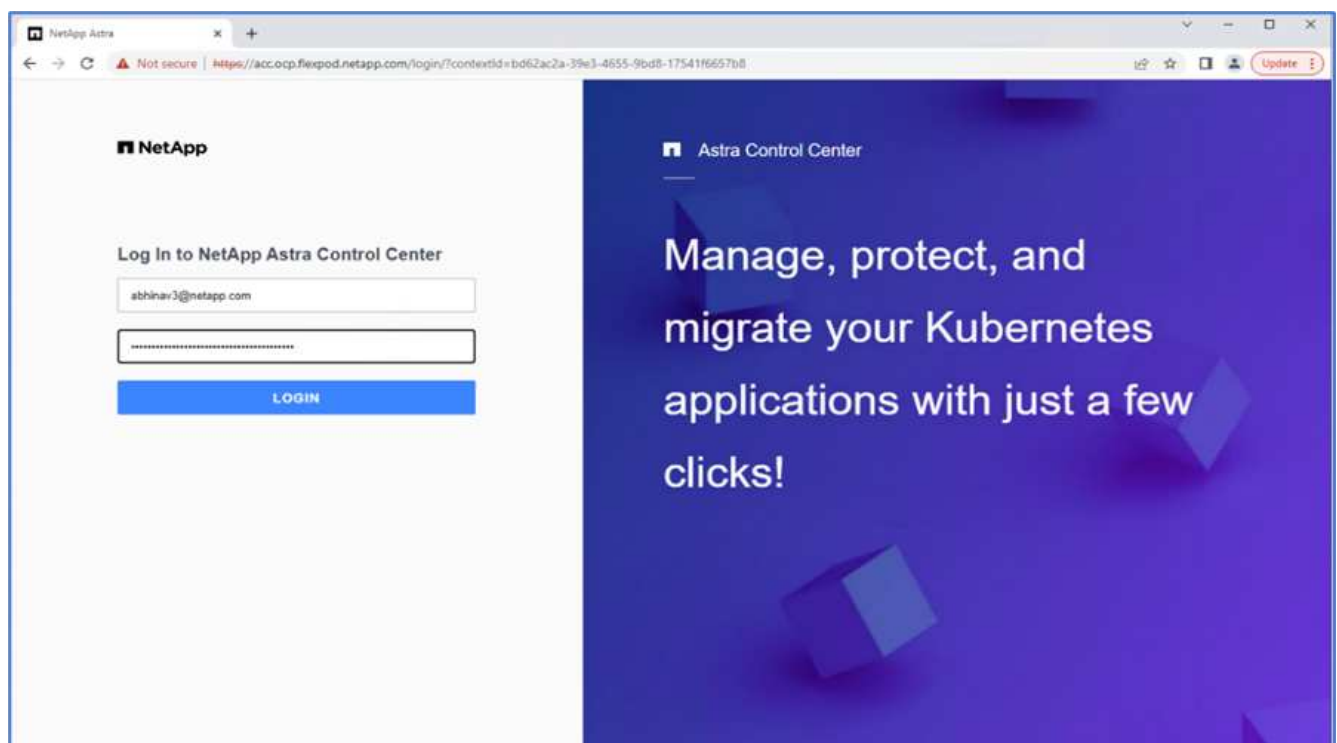


Jeder Pod sollte den Status „laufen“ aufweisen. Es kann mehrere Minuten dauern, bevor die System-Pods implementiert sind.

20. Wenn alle Pods ausgeführt werden, führen Sie den folgenden Befehl aus, um das einmalige Passwort abzurufen. Prüfen Sie in der YAML-Version der Ausgabe das `status.deploymentState` Feld für den bereitgestellten Wert, und kopieren Sie anschließend die `status.uuid` Wert: Das Passwort lautet ACC-Anschließend der UUID-Wert. (ACC-[UUID]).

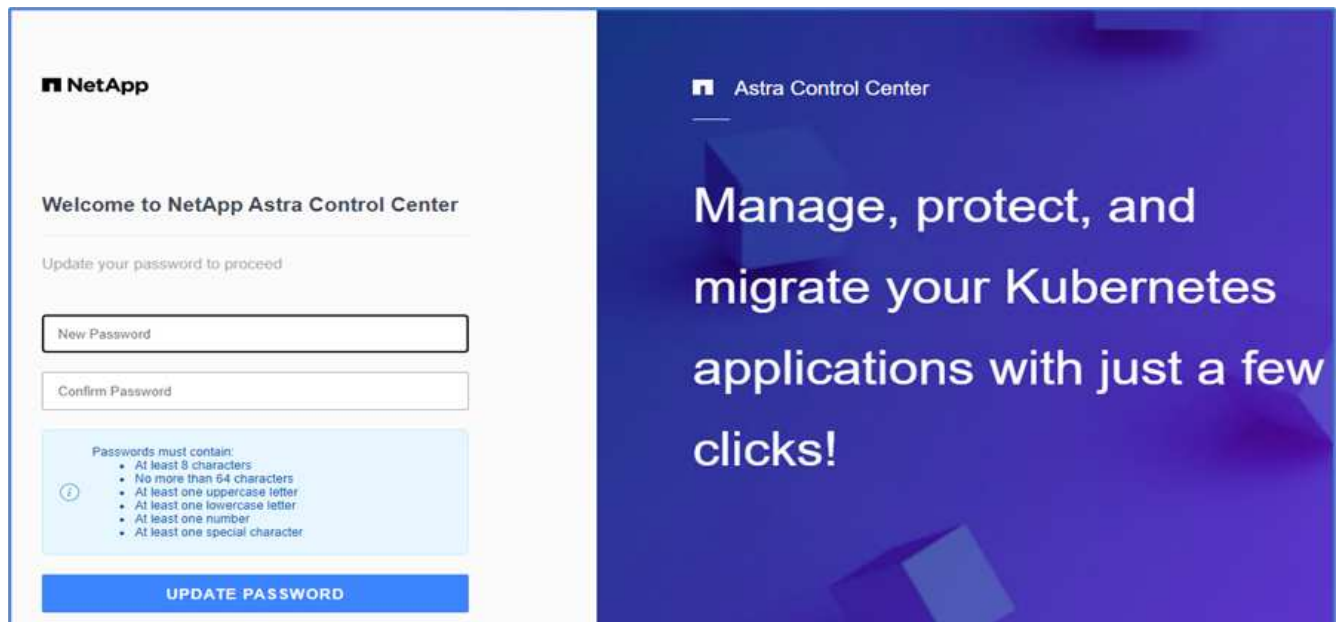
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Navigieren Sie in einem Browser zur URL mithilfe des FQDN, den Sie bereitgestellt haben.
22. Melden Sie sich mit dem Standardbenutzernamen an. Dies ist die E-Mail-Adresse, die während der Installation angegeben wurde, und das einmalige Passwort ACC-[UUID].



Wenn Sie dreimal ein falsches Kennwort eingeben, ist das Administratorkonto 15 Minuten lang gesperrt.

23. Ändern Sie das Passwort, und fahren Sie fort.

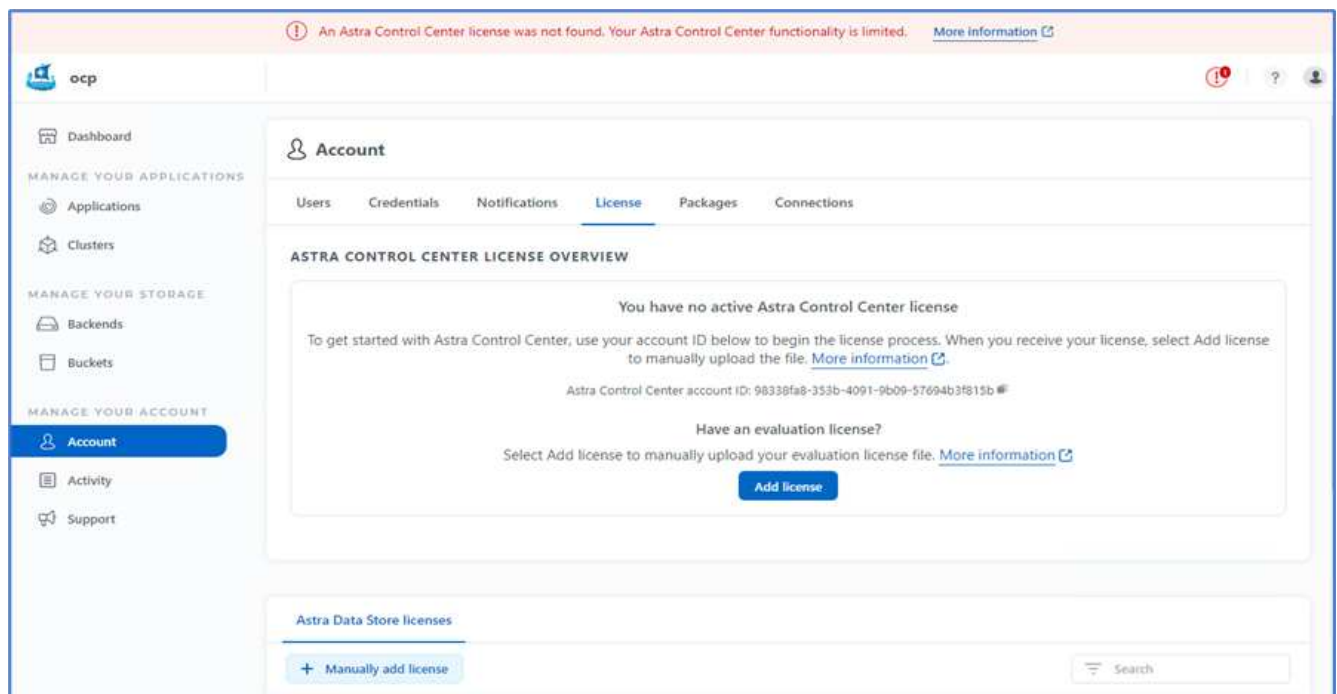


Weitere Informationen zur Installation des Astra Control Center finden Sie im "[Astra Control Center – Übersicht über die Installation](#)" Seite.

## Einrichten des Astra Control Center

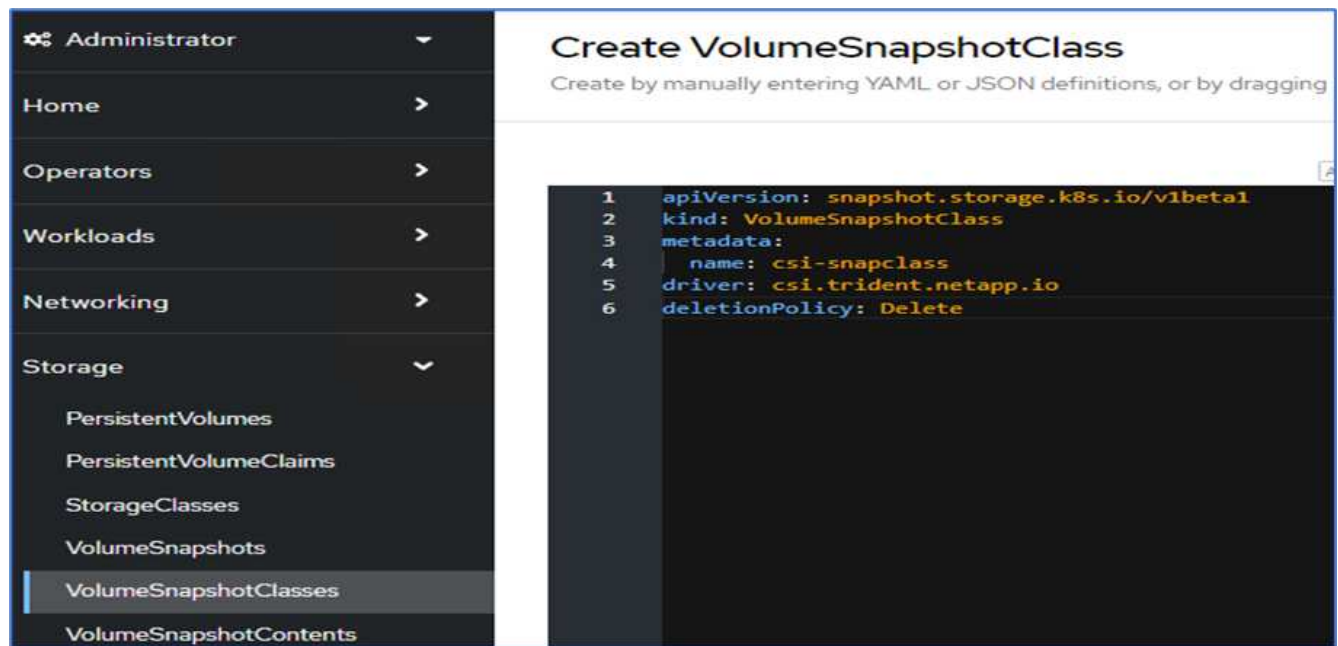
Melden Sie sich nach der Installation von Astra Control Center in der UI an, laden Sie die Lizenz hoch, fügen Sie Cluster hinzu, managen Sie den Storage und fügen Sie Buckets hinzu.

1. Gehen Sie auf der Homepage unter Konto auf die Registerkarte Lizenz und wählen Sie Lizenz hinzufügen, um die Astra-Lizenz hochzuladen.

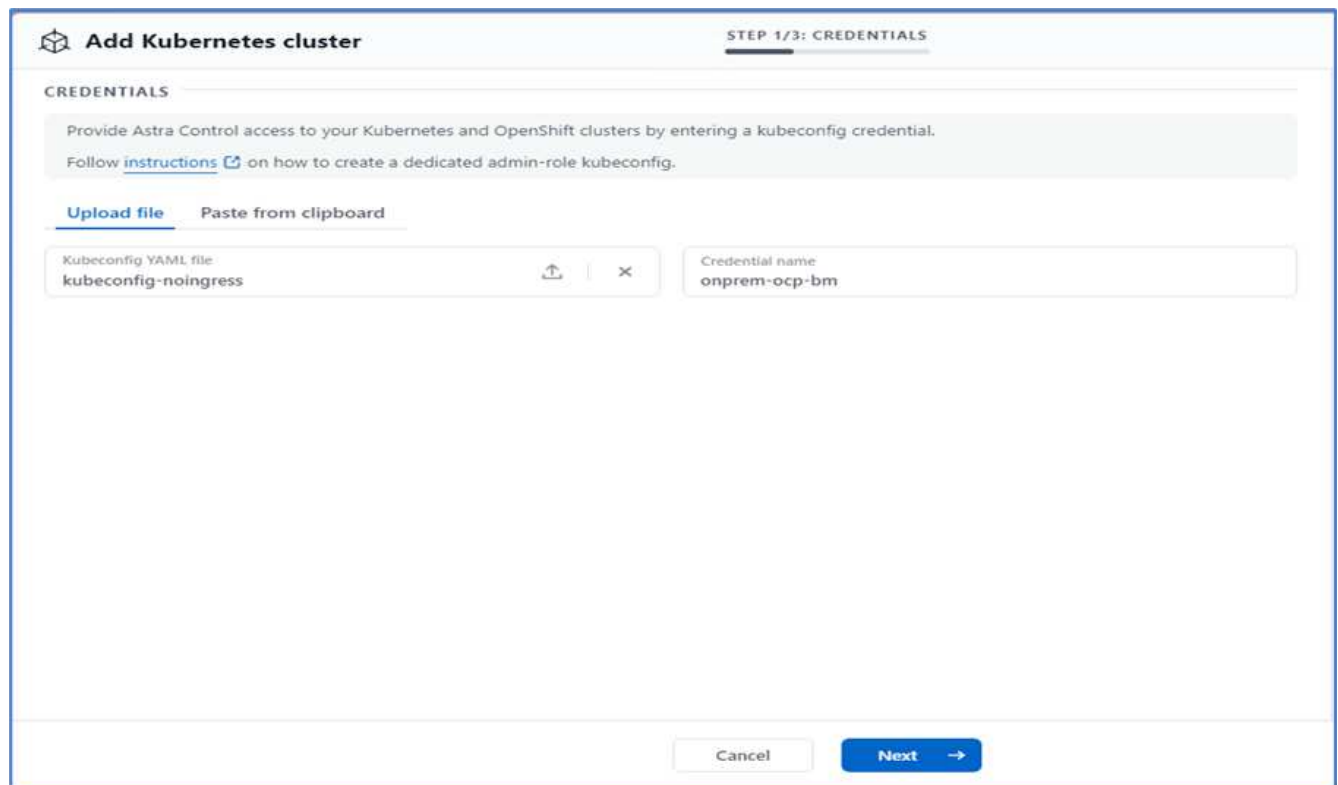


2. Erstellen Sie vor dem Hinzufügen des OpenShift-Clusters über die OpenShift-Webkonsole einen Astra Trident Volume Snapshot. Die Klasse Volume Snapshot wird mit dem konfiguriert

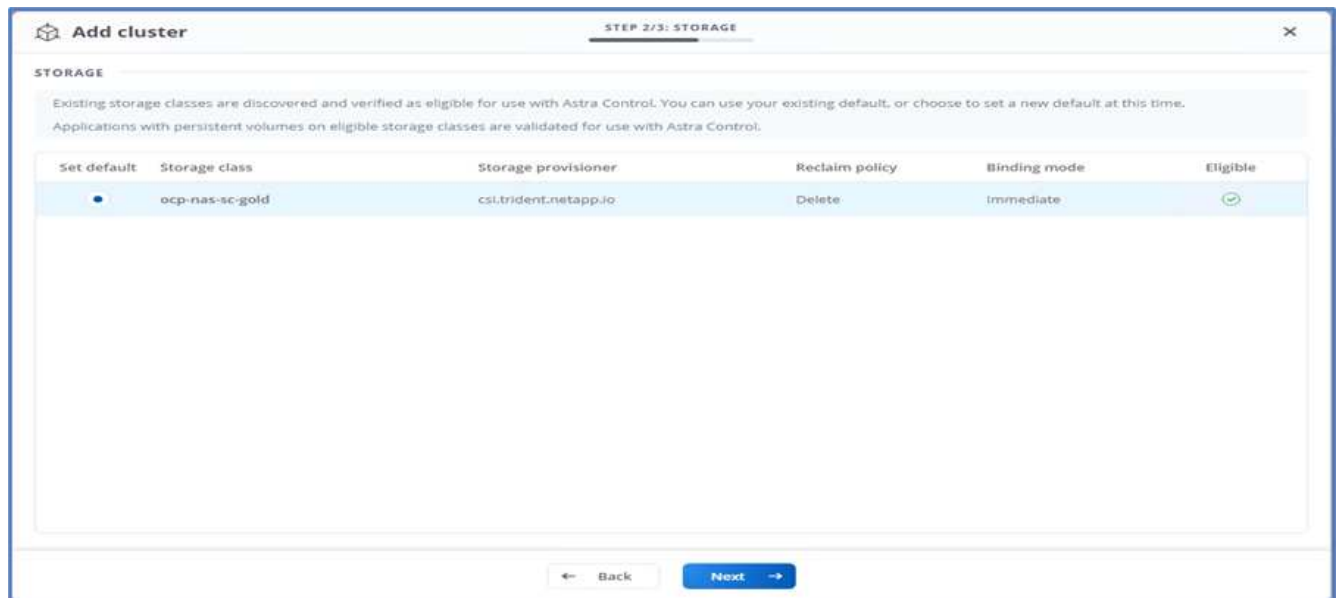
csi.trident.netapp.io Treiber.



3. Zum Hinzufügen des Kubernetes-Clusters wechseln Sie auf der Startseite zu Clusters und klicken auf Kubernetes-Cluster hinzufügen. Laden Sie anschließend die hoch kubeconfig Datei für den Cluster und geben einen Namen für die Anmeldeinformationen an. Klicken Sie Auf Weiter.



4. Die vorhandenen Speicherklassen werden automatisch erkannt. Wählen Sie die Standard-Storage-Klasse aus, klicken Sie auf Weiter und klicken Sie dann auf Cluster hinzufügen.

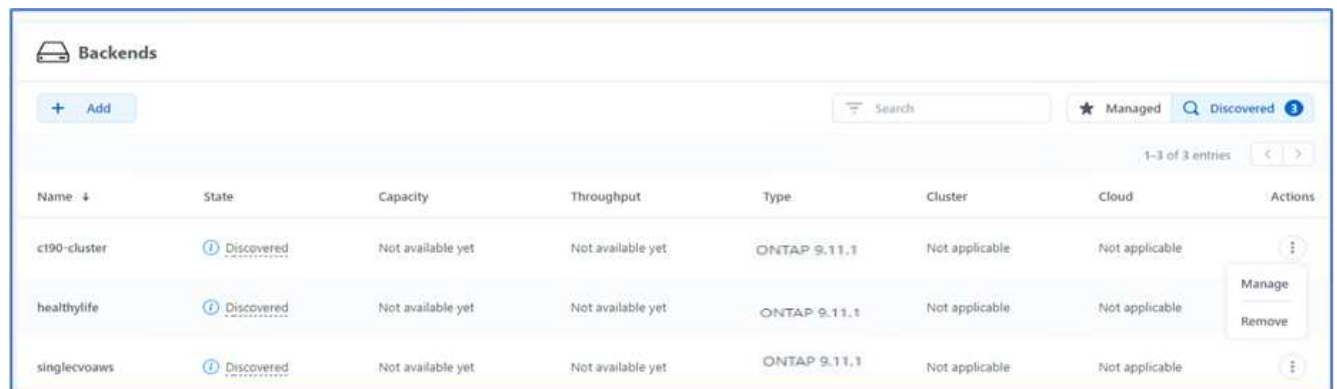


5. Der Cluster wird in wenigen Minuten hinzugefügt. Um weitere Cluster der OpenShift Container Platform hinzuzufügen, wiederholen Sie die Schritte 1 bis 4.



Wenn Sie eine zusätzliche OpenShift-Betriebsumgebung als verwaltete Computing-Ressource hinzufügen möchten, sollten Sie den Astra Trident in die Umgebung einbinden "[VolumeSnapshotClass-Objekte](#)" Werden definiert.

6. Um den Speicher zu verwalten, gehen Sie zu Backend, klicken Sie auf die drei Punkte unter Aktionen gegen das Backend, das Sie verwalten möchten. Klicken Sie Auf Verwalten.



7. Geben Sie die ONTAP Zugangsdaten ein und klicken Sie auf Weiter. Überprüfen Sie die Informationen, und klicken Sie auf verwaltet. Die Back-Ends sollten wie im folgenden Beispiel aussehen.

Backends							
<a href="#">+ Add</a>		<input type="text" value="Search"/>		<a href="#">★ Managed</a> <a href="#">🔍 Discovered</a>		1-3 of 3 entries <a href="#">&lt;</a> <a href="#">&gt;</a>	
Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
<a href="#">c190-cluster</a>	✓ Available	0.4/10.64 TiB: 3.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
<a href="#">healthylife</a>	✓ Available	5.16/106.42 TiB: 4.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
<a href="#">singlecvoaws</a>	✓ Available	0.07/0.62 TiB: 11.9%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮

8. Um Astra Control einen Bucket hinzuzufügen, wählen Sie Eimer aus, und klicken Sie auf Hinzufügen.

- Dashboard
- MANAGE YOUR APPLICATIONS
  - Applications
  - Clusters
- MANAGE YOUR STORAGE
  - Backends
  - Buckets**
- MANAGE YOUR ACCOUNT
  - Account
  - Activity

### Buckets

[+ Add](#)

Name ↓	Description	State	Type

9. Wählen Sie den Bucket-Typ aus und geben Sie den Bucket-Namen, den S3-Servernamen oder die IP-Adresse und S3-Zugangsdaten an. Klicken Sie Auf Aktualisieren.

### Edit bucket

STORAGE BUCKET

Edit the access details of your existing object store bucket.

Type: Generic S3

Existing bucket name: acc-aws-bucket

Description (optional):

S3 server name or IP address: s3.us-east-1.amazonaws.com

☐ Make this bucket the default bucket for this cloud

SELECT CREDENTIALS

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.

[Add](#)
[Use existing](#)

Access ID:

Secret key:

Credential name:

[Cancel](#)
[Update ✓](#)

EDITING STORAGE BUCKETS

Edit your existing object store bucket. If the selected bucket is not currently defined as the default bucket for the cloud, you can replace the currently defined default bucket. [Read more in Storage buckets](#)





In dieser Lösung werden AWS S3 und ONTAP S3 Buckets verwendet. Sie können auch StorageGRID verwenden.

Der Bucket-Status sollte sich in einem ordnungsgemäßen Zustand befinden.

The screenshot shows the 'Buckets' page in the Astra Control interface. It features a table with columns for Name, Description, State, Type, and Actions. Two buckets are listed: 'acc-aws-bucket' (Generic S3) and 'astra-bucket' (NetApp ONTAP S3). Both are in a 'Healthy' state. The 'astra-bucket' is marked as the 'Default' bucket.

Name	Description	State	Type	Actions
acc-aws-bucket		Healthy	Generic S3	
astra-bucket	On Prem S3 Bucket	Healthy	NetApp ONTAP S3	

Im Rahmen der Kubernetes-Cluster-Registrierung mit Astra Control Center für applikationskonsistentes Datenmanagement erstellt Astra Control automatisch Rollenbindungen und einen NetApp Monitoring Namespace, mit dem Kennzahlen und Protokolle von den Applikations-Pods und den Worker-Nodes erfasst werden. Nutzen Sie als Standard eine der unterstützten ONTAP-basierten Storage-Klassen.

Nach Ihnen "[Fügen Sie dem Astra Control Management einen Cluster hinzu](#)", Sie können Apps auf dem Cluster installieren (außerhalb von Astra Control) und dann auf der Seite Apps in Astra Control die Apps und ihre Ressourcen verwalten. Weitere Informationen zum Verwalten von Apps mit Astra finden Sie im "[Anforderungen für das Applikationsmanagement](#)".

"[Weiter: Übersicht zur Lösungsvalidierung](#)"

## Copyright-Informationen

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

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

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

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

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

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

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

## Markeninformationen

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