



# **Installazione e configurazione**

## **FlexPod**

NetApp  
October 30, 2025

This PDF was generated from <https://docs.netapp.com/it-it/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](https://docs.netapp.com) for the latest.

# Sommario

- Installazione e configurazione ..... 1
  - Installazione bare-metal di FlexPod per piattaforma container OpenShift 4 ..... 1
    - Installazione di FlexPod per piattaforma container OpenShift 4 su VMware ..... 1
  - Red Hat OpenShift su AWS ..... 2
  - NetApp Cloud Volumes ONTAP ..... 3
  - Installazione di Astra Control Center su OpenShift Container Platform ..... 3
    - Requisiti ambientali ..... 4
    - Installare Astra Control Center utilizzando OpenShift OperatorHub ..... 5
    - Configurare Astra Control Center ..... 19

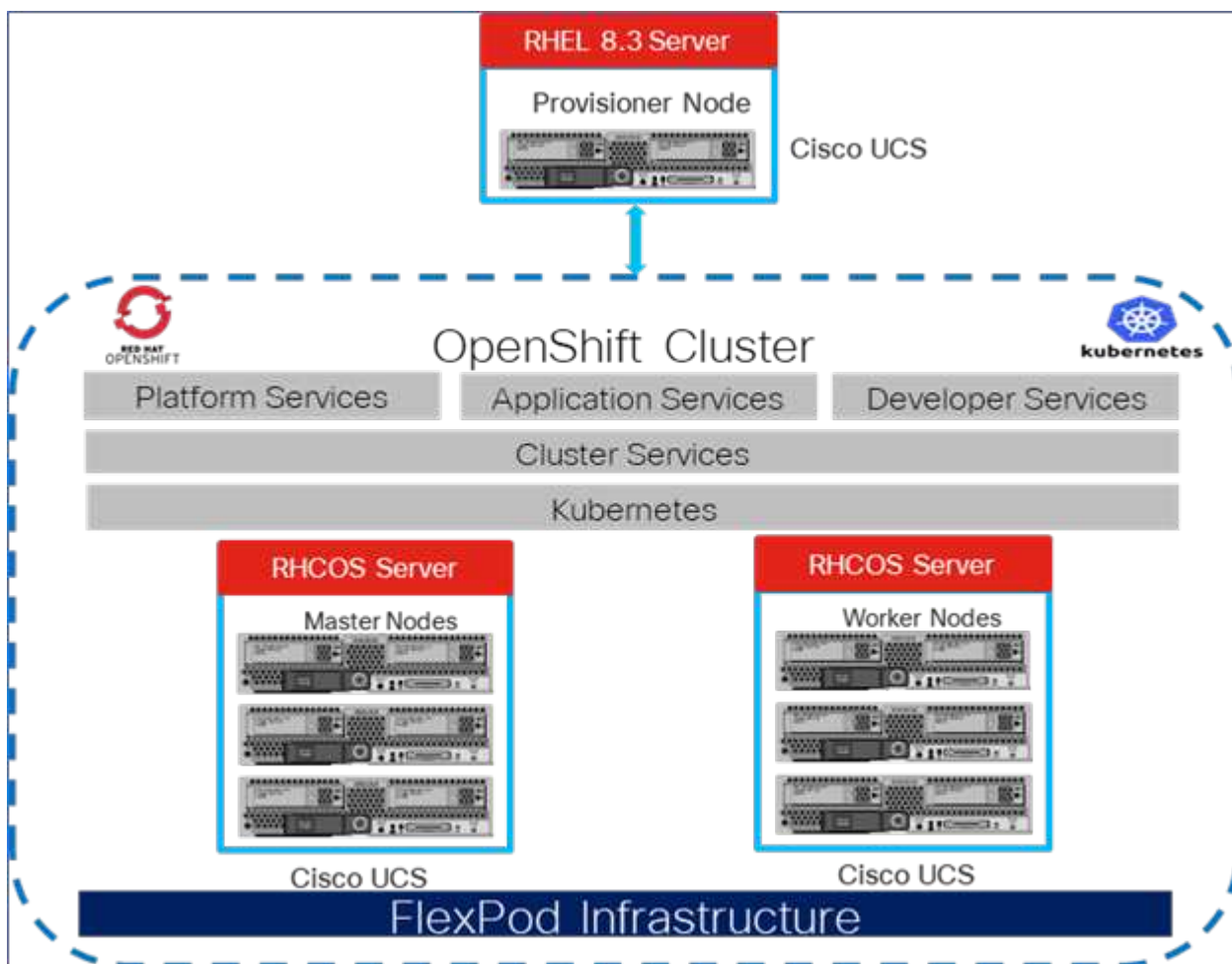
# Installazione e configurazione

## Installazione bare-metal di FlexPod per piattaforma container OpenShift 4

"Precedente: [Componenti della soluzione.](#)"

Per informazioni sulla progettazione bare-metal di FlexPod per la piattaforma container OpenShift 4, sui dettagli di implementazione e sull'installazione e configurazione di NetApp Astra Trident, vedere ["FlexPod con OpenShift Guida alla progettazione e all'implementazione validate di Cisco \(CVD\)"](#). Questo CVD copre l'implementazione di FlexPod e della piattaforma container OpenShift utilizzando Ansible. Il CVD fornisce inoltre informazioni dettagliate sulla preparazione dei nodi di lavoro, sull'installazione di Astra Trident, sul backend dello storage e sulle configurazioni di classe storage, che sono i pochi prerequisiti per l'implementazione e la configurazione di Astra Control Center.

La figura seguente illustra la piattaforma container OpenShift 4 Bare Metal su FlexPod.

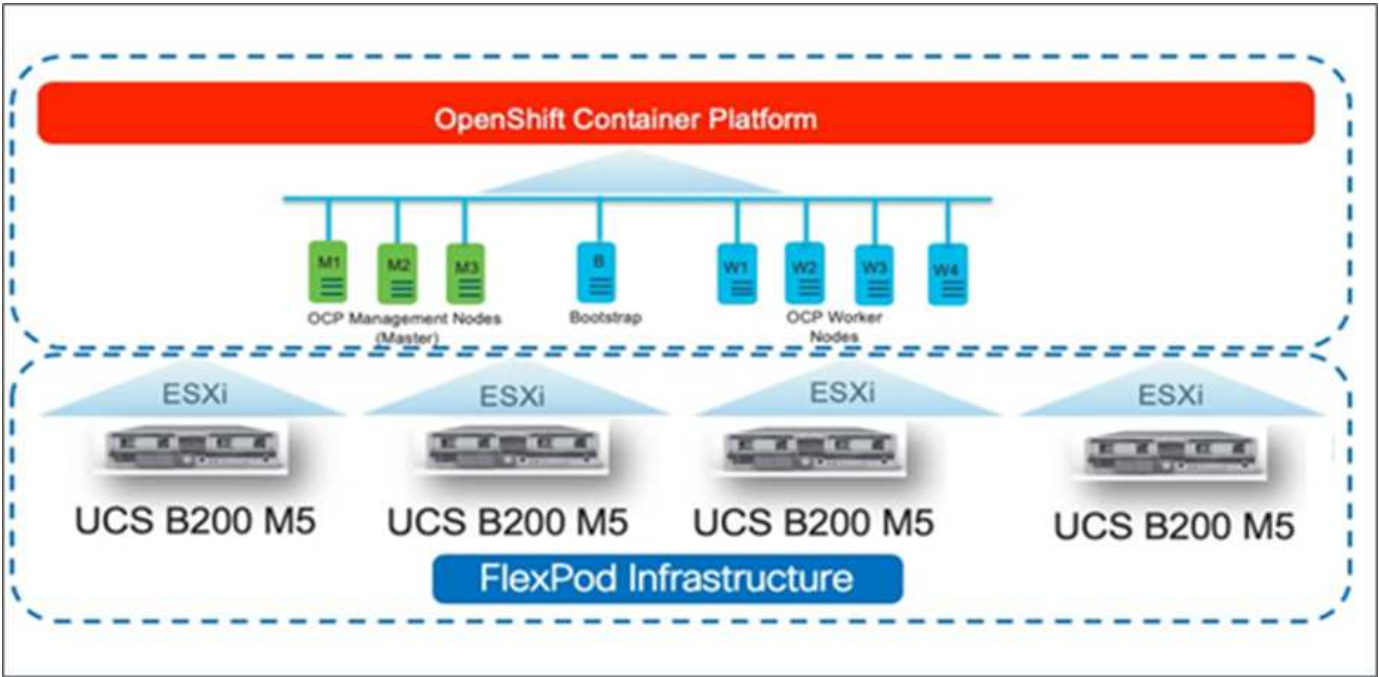


## Installazione di FlexPod per piattaforma container OpenShift 4 su VMware

Per ulteriori informazioni sull'implementazione di Red Hat OpenShift Container Platform 4 su FlexPod con

VMware vSphere, vedere "Data center FlexPod per piattaforma container OpenShift 4".

La figura seguente illustra FlexPod per piattaforma container OpenShift 4 su vSphere.



"Avanti: Red Hat OpenShift su AWS."

## Red Hat OpenShift su AWS

"Precedente: Installazione bare-metal di FlexPod per piattaforma container OpenShift 4."

Un cluster OpenShift Container Platform 4 separato e autogestito viene implementato su AWS come sito di DR. I nodi master e worker si estendono in tre zone di disponibilità per garantire l'alta disponibilità.

Instances (6) <span>Info</span>								
<input type="text" value="Search"/>								
<span>ocp</span> <span>X</span> <span>Clear filters</span>								
<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-7nmbc	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 viene implementato come ["cluster privato"](#) in un VPC esistente su AWS. Un cluster OpenShift Container Platform privato non espone endpoint esterni ed è accessibile solo da una rete interna e non è visibile su Internet. Un NetApp Cloud Volumes ONTAP a nodo singolo viene implementato utilizzando NetApp Cloud Manager, che fornisce un backend di storage ad Astra Trident.

Per ulteriori informazioni sull'installazione di OpenShift su AWS, vedere ["Documentazione di OpenShift"](#).

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

## NetApp Cloud Volumes ONTAP

["Precedente: Red Hat OpenShift su AWS."](#)

L'istanza di NetApp Cloud Volumes ONTAP viene implementata su AWS e funge da storage back-end per Astra Trident. Prima di aggiungere un ambiente di lavoro Cloud Volumes ONTAP, è necessario implementare un connettore. Cloud Manager ti chiede se provi a creare il tuo primo ambiente di lavoro Cloud Volumes ONTAP senza un connettore. Per implementare un connettore in AWS, vedere ["Creare un connettore"](#).

Per implementare Cloud Volumes ONTAP su AWS, vedere ["Quick Start per AWS"](#).

Una volta implementato Cloud Volumes ONTAP, è possibile installare Astra Trident e configurare il backend dello storage e la classe Snapshot sul cluster della piattaforma container OpenShift.

["Avanti: Installazione di Astra Control Center su OpenShift Container Platform."](#)

## Installazione di Astra Control Center su OpenShift Container Platform

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

È possibile installare Astra Control Center sul cluster OpenShift in esecuzione su FlexPod o su AWS con un backend di storage Cloud Volumes ONTAP. In questa soluzione, Astra Control Center viene implementato sul cluster bare-metal OpenShift.

Astra Control Center può essere installato utilizzando il processo standard descritto ["qui"](#) Oppure da Red Hat OpenShift OperatorHub. Astra Control Operator è un operatore certificato Red Hat. In questa soluzione, Astra Control Center viene installato utilizzando Red Hat OperatorHub.

## Requisiti ambientali

- Astra Control Center supporta più distribuzioni Kubernetes; per Red Hat OpenShift, le versioni supportate includono Red Hat OpenShift Container Platform 4.8 o 4.9.
- Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse applicative dell'ambiente e dell'utente finale:

Componenti	Requisito
Capacità di back-end dello storage	Almeno 500 GB disponibili
Nodi di lavoro	Almeno 3 nodi di lavoro, con 4 core CPU e 12 GB di RAM ciascuno
Indirizzo FQDN (Fully Qualified Domain Name)	Un indirizzo FQDN per Astra Control Center
Astra Trident	Astra Trident 21.04 o versione successiva installata e configurata
Controller di ingresso o bilanciamento del carico	Configurare il controller di ingresso per esporre Astra Control Center con un URL o un bilanciamento del carico per fornire l'indirizzo IP che verrà risolto nell'FQDN

- È necessario disporre di un registro di immagini privato esistente in cui trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui vengono caricate le immagini.



Alcune immagini vengono estratte durante l'esecuzione di determinati flussi di lavoro e i container vengono creati e distrutti quando necessario.

- Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Centro di controllo Astra supporta i seguenti driver ONTAP forniti da Astra Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-economy



Supponiamo che i cluster OpenShift implementati abbiano Astra Trident installato e configurato con un backend ONTAP e sia definita anche una classe di storage predefinita.

- Per la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per modificare il criterio di esportazione ONTAP in modo da consentire queste operazioni, eseguire i seguenti comandi:

```
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
```



Per aggiungere un secondo ambiente operativo OpenShift come risorsa di calcolo gestita, assicurarsi che la funzione Astra Trident Volume snapshot sia attivata. Per abilitare e testare le snapshot dei volumi con Astra Trident, consulta la pagina ufficiale ["Istruzioni di Astra Trident"](#).

- R **"VolumeSnapClass"** Deve essere configurato su tutti i cluster Kubernetes da cui vengono gestite le applicazioni. Questo potrebbe includere anche il cluster K8s su cui è installato Astra Control Center. Astra Control Center è in grado di gestire le applicazioni sul cluster K8s su cui è in esecuzione.

## Requisiti di gestione delle applicazioni

- **Licensing.** per gestire le applicazioni utilizzando Astra Control Center, è necessaria una licenza Astra Control Center.
- **Namespaces.** Uno spazio dei nomi è l'entità più grande che può essere gestita come applicazione da Astra Control Center. È possibile scegliere di filtrare i componenti in base alle etichette dell'applicazione e alle etichette personalizzate in uno spazio dei nomi esistente e gestire un sottoinsieme di risorse come applicazione.
- **StorageClass.** se si installa un'applicazione con un StorageClass esplicitamente impostato ed è necessario clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la StorageClass originariamente specificata. La clonazione di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass ha esito negativo.
- **Kubernetes resources.** le applicazioni che utilizzano risorse Kubernetes non acquisite da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati applicativi. Astra Control può acquisire le seguenti risorse Kubernetes:

Risorse Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	CustomResource	Lavoro di cassa
DemonSet	HorizontalPodAutoscaler	Ingresso
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
NetworkPolicy	ReplicaSet	Ruolo
RoleBinding	Percorso	Segreto
ValidatingWebhook		

## Installare Astra Control Center utilizzando OpenShift OperatorHub

La seguente procedura consente di installare Astra Control Center utilizzando Red Hat OperatorHub. In questa soluzione, Astra Control Center viene installato su un cluster OpenShift bare-metal in esecuzione su FlexPod.

1. Scarica il bundle Astra Control Center (`astra-control-center-[version].tar.gz`) da ["Sito di supporto NetApp"](#).
2. Scaricare il file .zip per i certificati e le chiavi di Astra Control Center da ["Sito di supporto NetApp"](#).
3. Verificare la firma del bundle.

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

#### 4. Estrarre le immagini Astra.

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

#### 5. Passare alla directory Astra.

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

#### 6. Aggiungere le immagini al registro locale.

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

#### 7. Utilizzare lo script appropriato per caricare le immagini, etichettarle e inserirle nel registro locale.

Per 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
```

Per Podman:

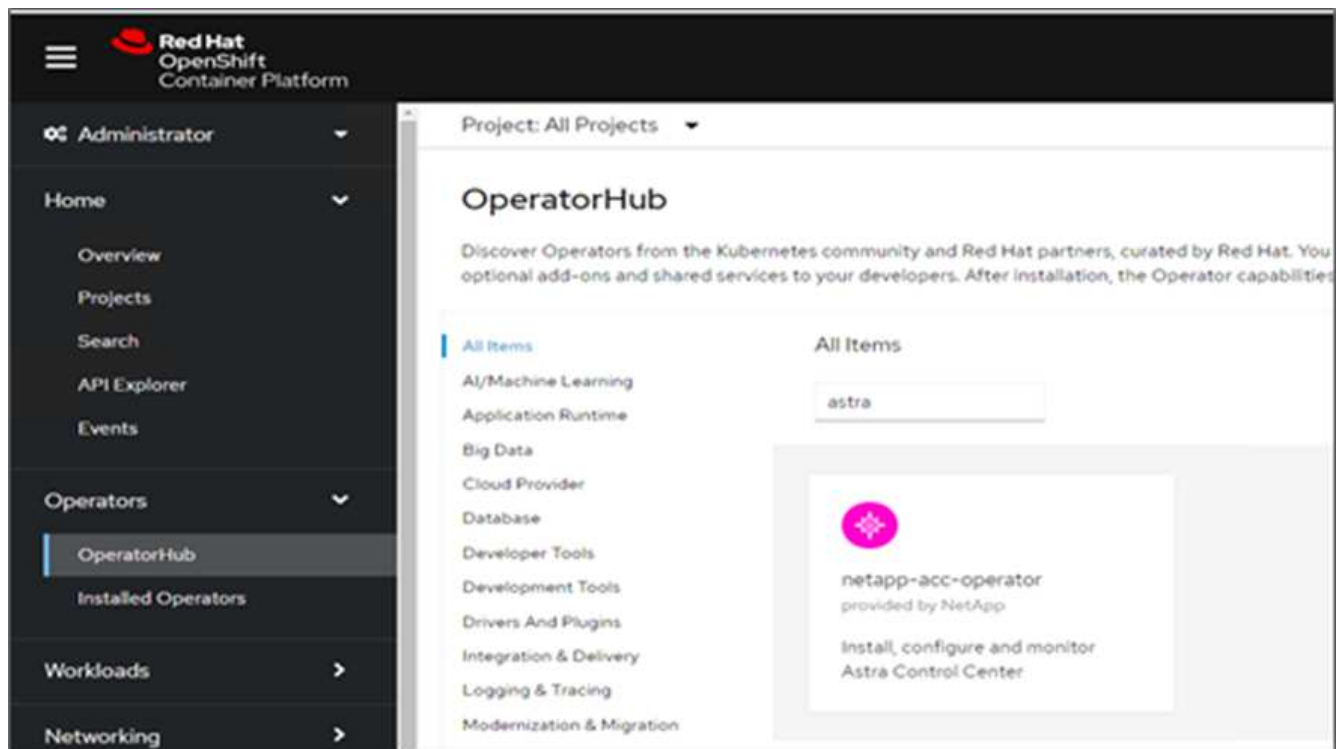


```

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


```

- Accedere alla console web del cluster OpenShift bare-metal. Dal menu laterale, selezionare Operator (operatori) > OperatorHub. Invio astra per visualizzare l'elenco di netapp-acc-operator.



netapp-acc-operator È un operatore Red Hat OpenShift certificato ed è elencato nel catalogo OperatorHub.

- Selezionare netapp-acc-operator E fare clic su Installa.



**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. Selezionare le opzioni appropriate e fare clic su Install (Installa).

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 \***


 netapp-acc-operator (Operator recommended)

**Update approval \*** ⓘ
 

☐ Automatic
 ☒ Manual


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

**Provided APIs**

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

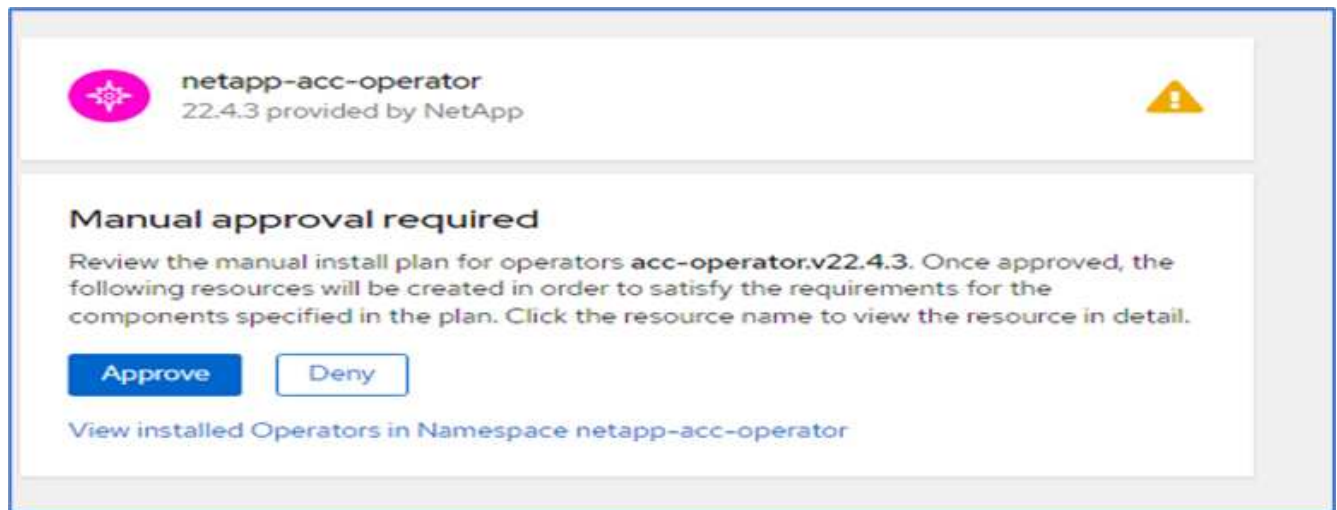
**Namespace creation**  
 Namespace **netapp-acc-operator** does not exist and will be created.

**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.

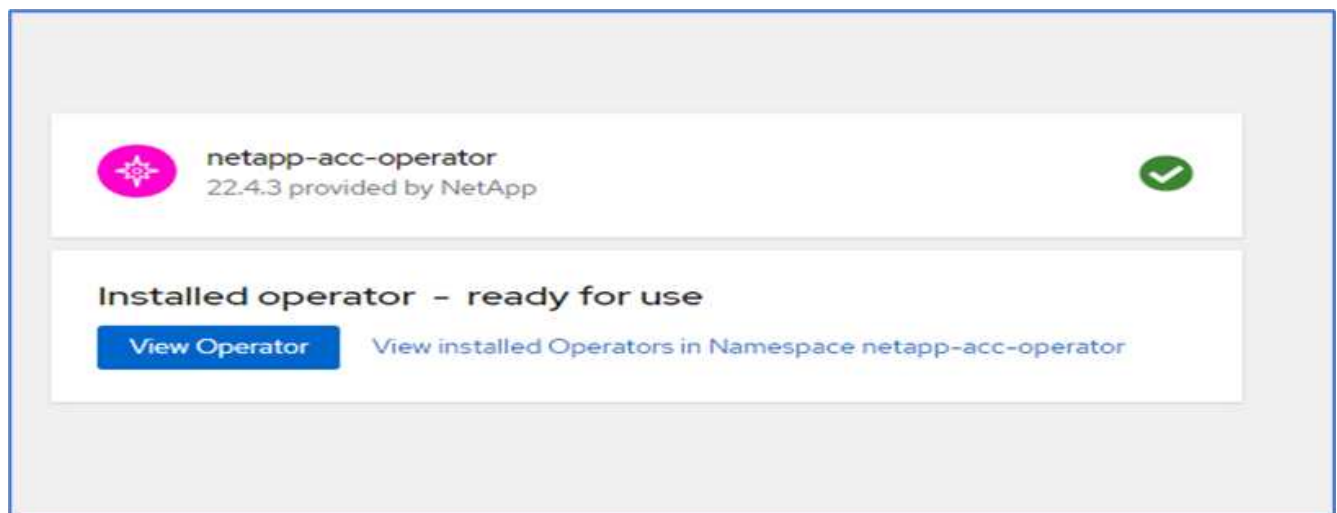
Install

Cancel

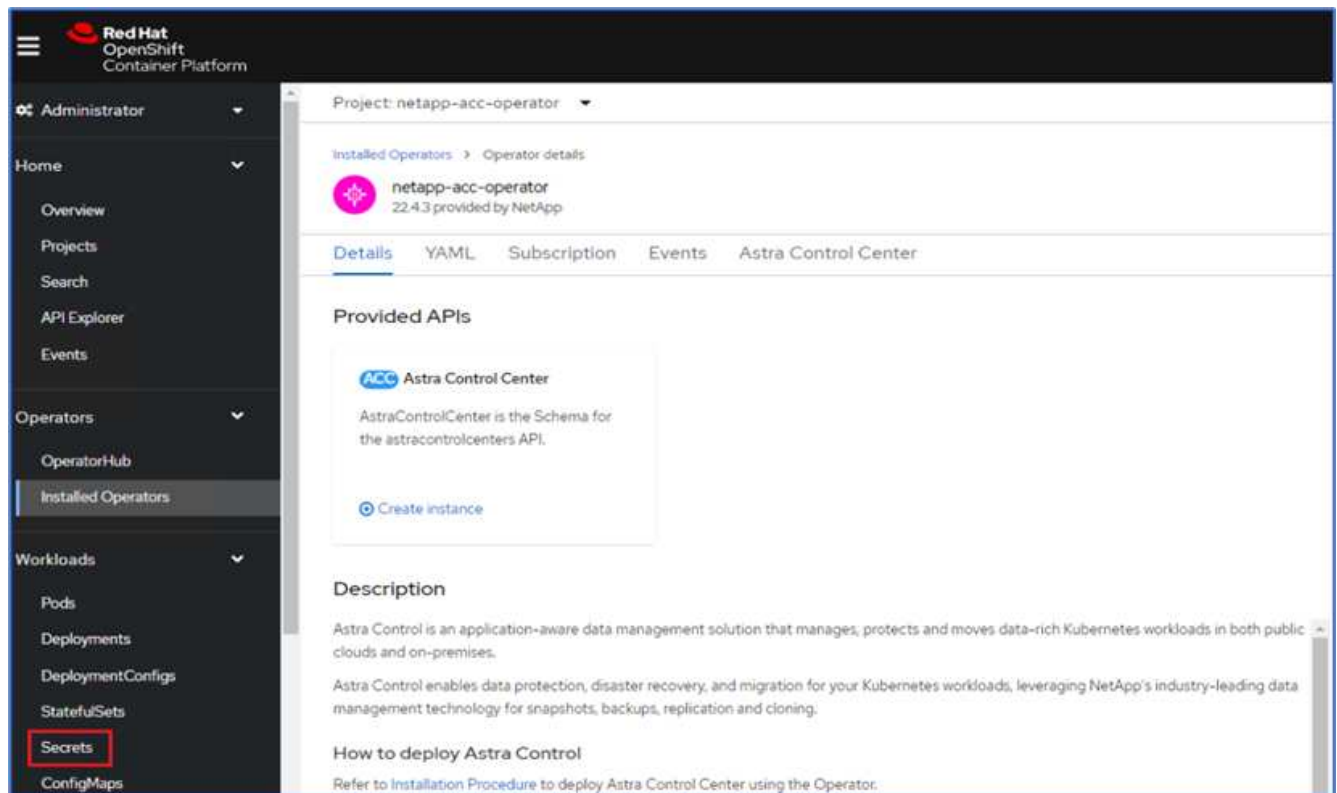
11. Approvare l'installazione e attendere l'installazione dell'operatore.



12. A questo punto, l'operatore viene installato correttamente e pronto per l'uso. Fare clic su View Operator (Visualizza operatore) per avviare l'installazione di Astra Control Center.



13. Prima di installare Astra Control Center, creare il segreto pull per scaricare le immagini Astra dal registro Docker precedentemente inserito.



14. Per estrarre le immagini di Astra Control Center dal tuo repo privato Docker, crea un segreto in `netapp-acc-operator` namespace. Questo nome segreto viene fornito nel manifesto YAML di Astra Control Center in un passaggio successivo.

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

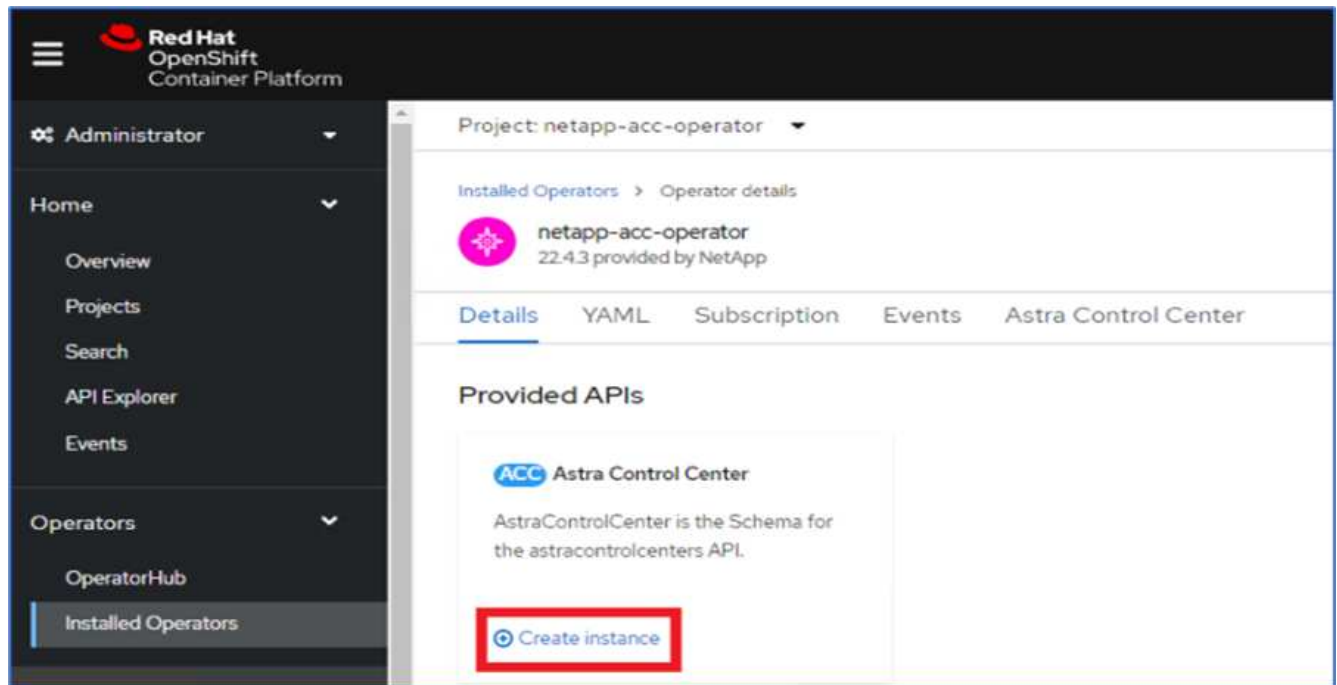
**Username \***

**Password \***

**Email**

[+ Add credentials](#)

15. Dal menu laterale, selezionare Operator > Installed Operators (operatori > operatori installati) e fare clic su Create Instance (Crea istanza) nella sezione delle API fornite.



16. Completare il modulo Create AstraControlCenter. Fornire il nome, l'indirizzo Astra e la versione di Astra.

The screenshot shows the 'Create AstraControlCenter' form in the Red Hat OpenShift Container Platform interface. The sidebar on the left is the same as in the previous screenshot. The main content area displays the 'Create AstraControlCenter' form. At the top, it says 'Project: netapp-acc-operator' and 'netapp-acc-operator > Create AstraControlCenter'. Below this is the title 'Create AstraControlCenter' and a note: 'Create by completing the form. Default values may be provided by the Operator authors.' The 'Configure via' section has two options: 'Form view' (selected) and 'YAML view'. A note states: 'Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.' The form fields are:
 

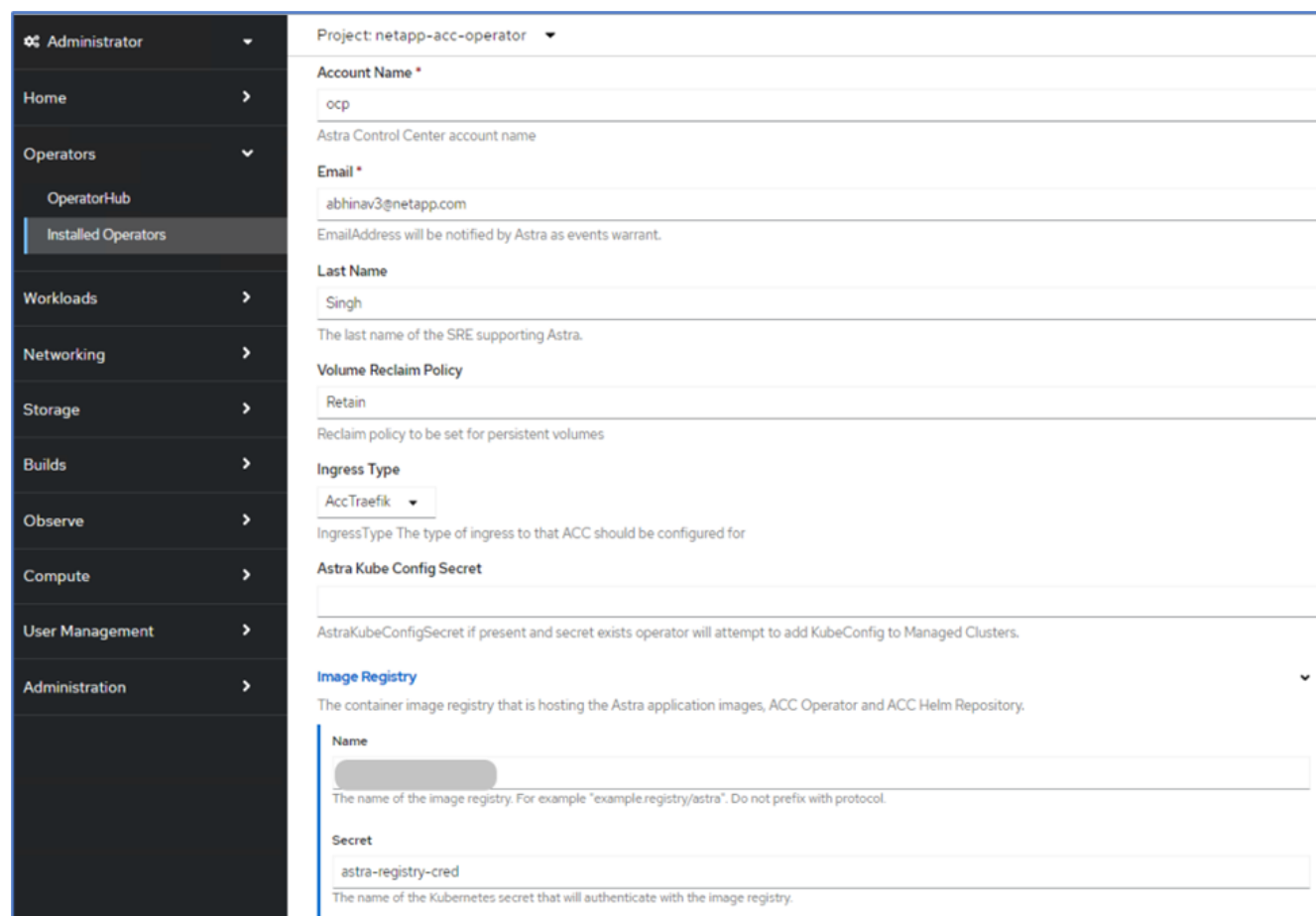
- Name \***: acc
- Labels**: app=frontend
- Auto Support \***: A checkbox with a right arrow, currently unchecked. The text below it says: 'AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. An internet connection is required (port 442) and all 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 it says: '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 it says: 'Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch.'



In Astra Address (Indirizzo Astra), fornire l'indirizzo FQDN per Astra Control Center. Questo indirizzo viene utilizzato per accedere alla console Web di Astra Control Center. Il nome FQDN deve anche essere impostato su una rete IP raggiungibile e deve essere configurato nel DNS.

17. Immettere un nome account, un indirizzo e-mail, il cognome dell'amministratore e mantenere la policy di

recupero del volume predefinita. Se si utilizza un bilanciamento del carico, impostare il tipo di ingresso su AccTraefik. In caso contrario, selezionare Generico per Ingress.Controller. In Image Registry (Registro immagini), immettere il percorso e il segreto del Registro di sistema dell'immagine contenitore.



Project: netapp-acc-operator

**Account Name \***  
ocp  
Astra Control Center account name

**Email \***  
abhinav3@netapp.com  
EmailAddress will be notified by Astra as events warrant.

**Last Name**  
Singh  
The last name of the SRE supporting Astra.

**Volume Reclaim Policy**  
Retain  
Reclaim policy to be set for persistent volumes

**Ingress Type**  
AccTraefik  
IngressType The type of ingress to that ACC should be configured for

**Astra Kube Config Secret**  
  
AstraKubeConfigSecret if present and secret exists operator will attempt to add KubeConfig to Managed Clusters.

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

**Name**  
  
The name of the image registry. For example "example.registry/astra". Do not prefix with protocol.

**Secret**  
astra-registry-cred  
The name of the Kubernetes secret that will authenticate with the image registry.



In questa soluzione viene utilizzato il bilanciamento del carico Metallb. Pertanto, il tipo di ingresso è AccTraefik. Questo espone il gateway traefik di Astra Control Center come un servizio Kubernetes di tipo LoadBalancer.

18. Inserire il nome admin, configurare la scalabilità delle risorse e fornire la classe di storage. Fare clic su Crea.

**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](#)

Lo stato dell'istanza di Astra Control Center deve passare da Deploying (implementazione) a Ready (Pronto).

Project: netapp-acc-operator

Installed Operators > Operator details

netapp-acc-operator  
22.4.3 provided by NetApp

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

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

Name Search by name...

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

- Verificare che tutti i componenti del sistema siano stati installati correttamente e che tutti i pod siano in esecuzione.

```
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          10m
```



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-txrf1	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-gwwvf	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	1/1	Running	0
9m18s			
polaris-vault-1	1/1	Running	0
9m18s			
polaris-vault-2	1/1	Running	0
9m18s			
public-metrics-7b96476f64-j88bw	1/1	Running	0
5m48s			
storage-backend-metrics-5fd6d7cd9c-vcb4j	1/1	Running	0
5m59s			
storage-provider-bb85ff965-m7qrq	1/1	Running	0
5m25s			
telegraf-ds-4zqgz	1/1	Running	0
3m36s			
telegraf-ds-cp9x4	1/1	Running	0
3m36s			
telegraf-ds-h4n59	1/1	Running	0
3m36s			
telegraf-ds-jnp2q	1/1	Running	0
3m36s			
telegraf-ds-pdz5j	1/1	Running	0
3m36s			
telegraf-ds-znqtp	1/1	Running	0
3m36s			
telegraf-rs-rt64j	1/1	Running	0
3m36s			
telemetry-service-7dd9c74bfc-sfkzt	1/1	Running	0
6m19s			
tenancy-d878b7fb6-wf8x9	1/1	Running	0
6m37s			
traefik-6548496576-5v2g6	1/1	Running	0
98s			
traefik-6548496576-g82pq	1/1	Running	0
3m8s			
traefik-6548496576-psn49	1/1	Running	0
38s			
traefik-6548496576-qrkfd	1/1	Running	0
2m53s			
traefik-6548496576-srs6r	1/1	Running	0
98s			
trident-svc-679856c67-78kbt	1/1	Running	0
5m27s			
vault-controller-747d664964-xmn6c	1/1	Running	0
7m37s			

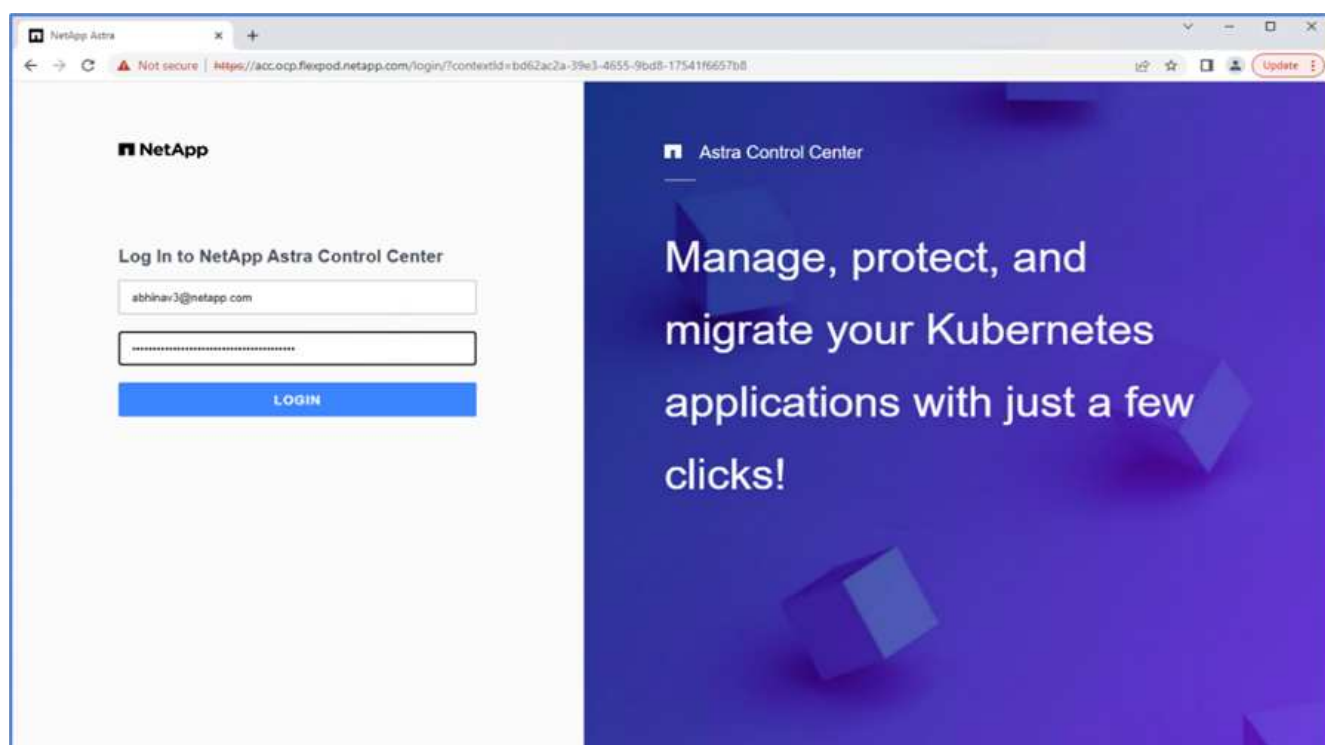


Ogni pod deve avere lo stato di esecuzione. L'implementazione dei pod di sistema potrebbe richiedere alcuni minuti.

20. Quando tutti i pod sono in esecuzione, eseguire il seguente comando per recuperare la password monouso. Nella versione YAML dell'output, selezionare `status.deploymentState` per il valore implementato, quindi copiare `status.uuid` valore. La password è ACC- Seguito dal valore UUID. (ACC-[UUID]).

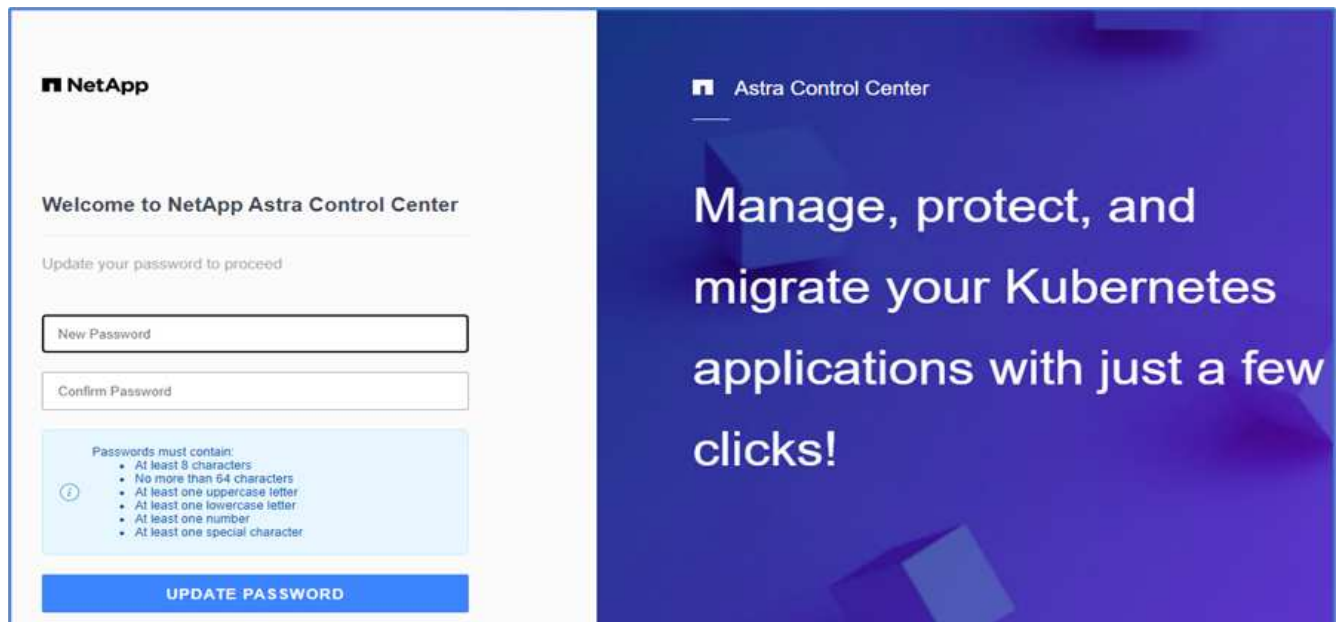
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. In un browser, accedere all'URL utilizzando l'FQDN fornito.
22. Effettuare l'accesso utilizzando il nome utente predefinito, ovvero l'indirizzo e-mail fornito durante l'installazione e la password monouso ACC-[UUID].



Se si immette una password errata per tre volte, l'account amministratore viene bloccato per 15 minuti.

23. Modificare la password e procedere.

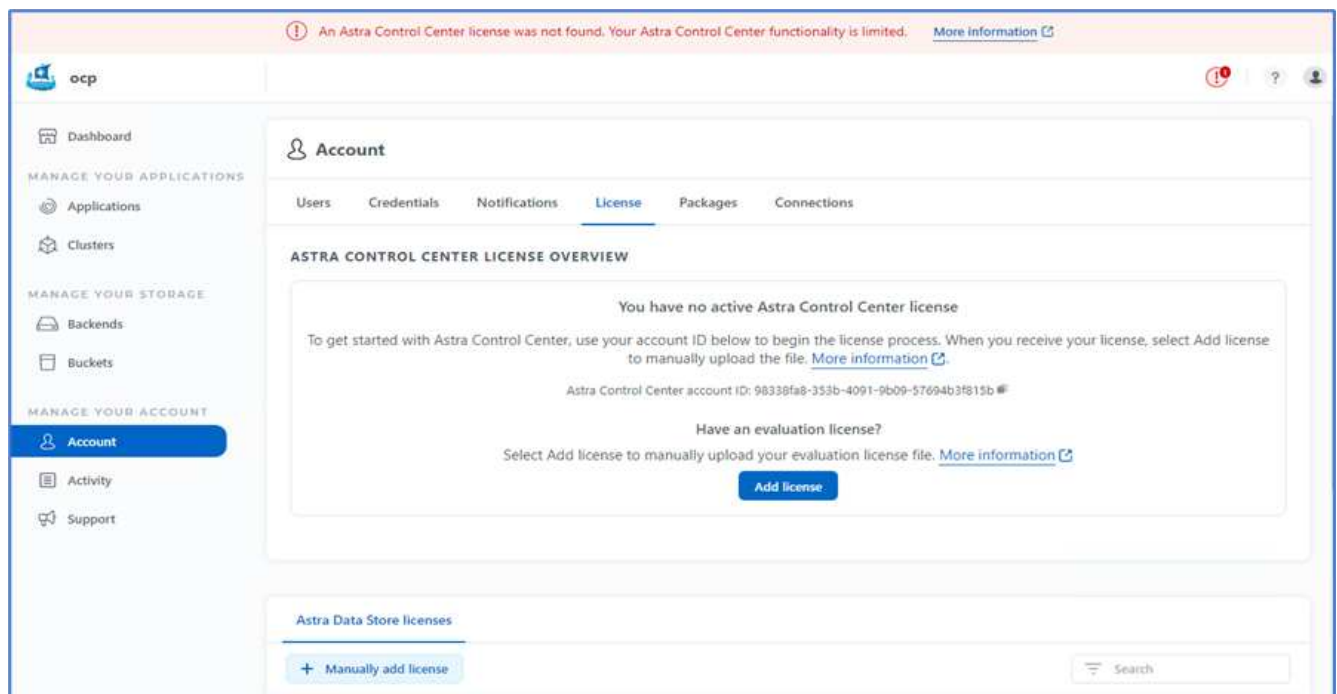


Per ulteriori informazioni sull'installazione di Astra Control Center, consultare "[Panoramica dell'installazione di Astra Control Center](#)" pagina.

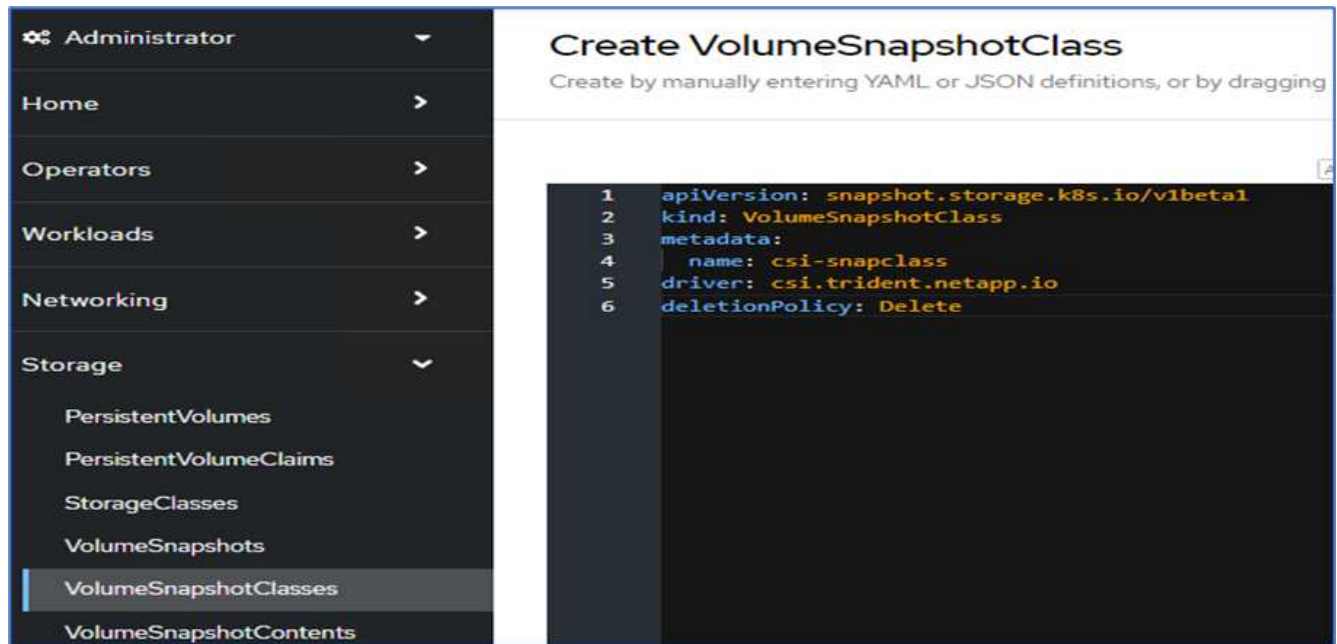
## Configurare Astra Control Center

Dopo aver installato Astra Control Center, accedere all'interfaccia utente, caricare la licenza, aggiungere cluster, gestire lo storage e aggiungere bucket.

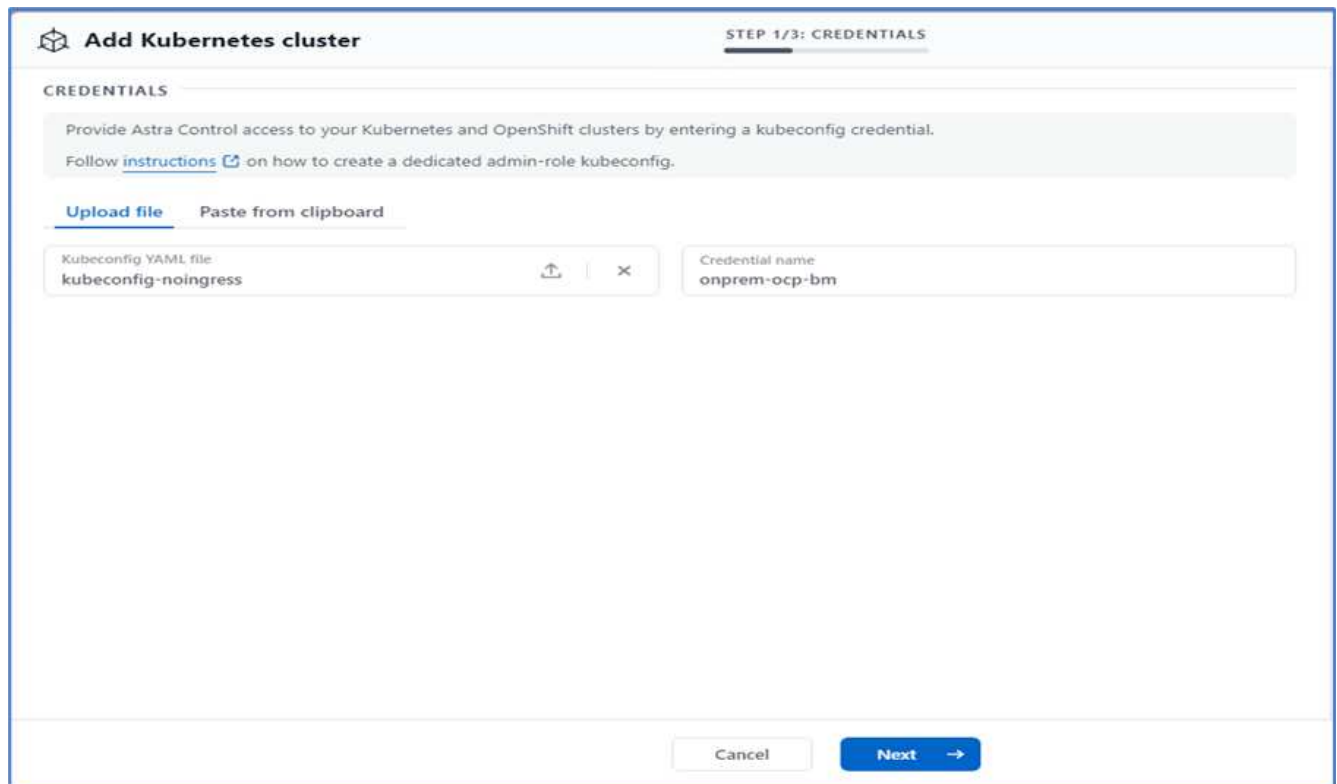
1. Nella home page, sotto account, andare alla scheda License (licenza) e selezionare Add License (Aggiungi licenza) per caricare la licenza Astra.



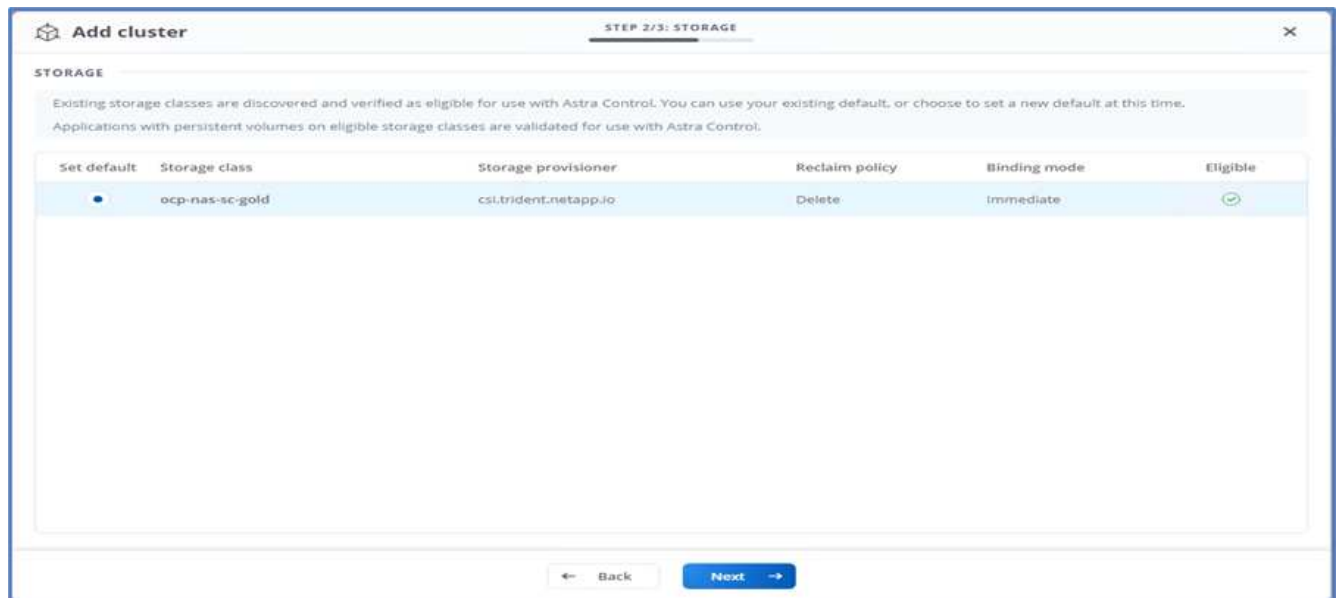
2. Prima di aggiungere il cluster OpenShift, creare una classe di snapshot Astra Trident Volume dalla console Web OpenShift. La classe Volume snapshot viene configurata con `csi.trident.netapp.io` driver.



3. Per aggiungere il cluster Kubernetes, accedere a Clusters nella home page e fare clic su Add Kubernetes Cluster (Aggiungi cluster Kubernetes). Quindi caricare `kubeconfig` per il cluster e fornire un nome di credenziale. Fare clic su Avanti.



4. Le classi di storage esistenti vengono rilevate automaticamente. Selezionare la classe di storage predefinita, fare clic su Next (Avanti), quindi su Add cluster (Aggiungi cluster).

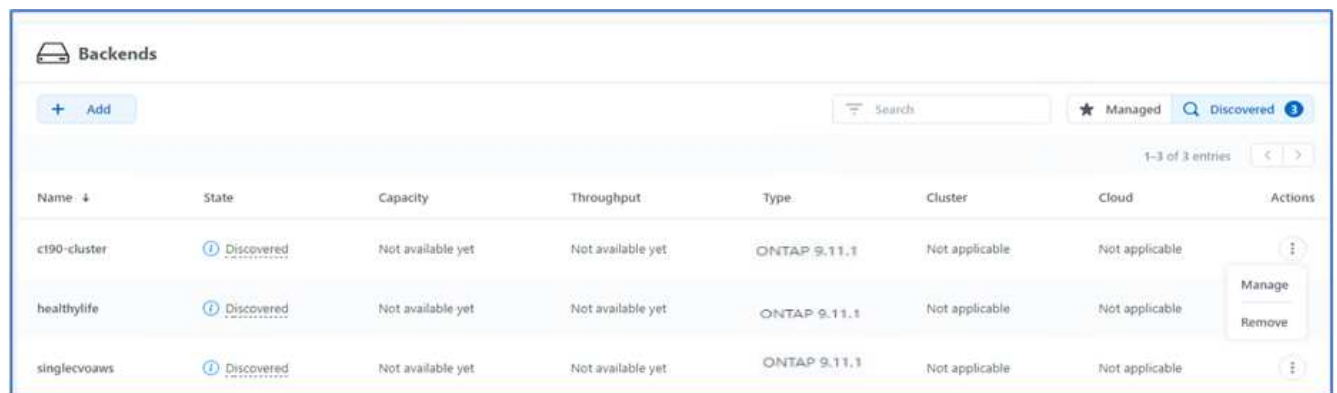


5. Il cluster viene aggiunto in pochi minuti. Per aggiungere altri cluster OpenShift Container Platform, ripetere i passaggi 1–4.



Per aggiungere un ambiente operativo OpenShift aggiuntivo come risorsa di calcolo gestita, assicurarsi che Astra Trident "Oggetti VolumeSnapshotClass" sono definiti.

6. Per gestire lo storage, accedere a Backend, fare clic sui tre punti in azioni rispetto al backend che si desidera gestire. Fare clic su Gestisci.



7. Fornire le credenziali ONTAP e fare clic su Avanti. Esaminare le informazioni e fare clic su Managed (gestito). I backend dovrebbero essere simili all'esempio seguente.

Backends

Add

Search

★

Managed

Discovered

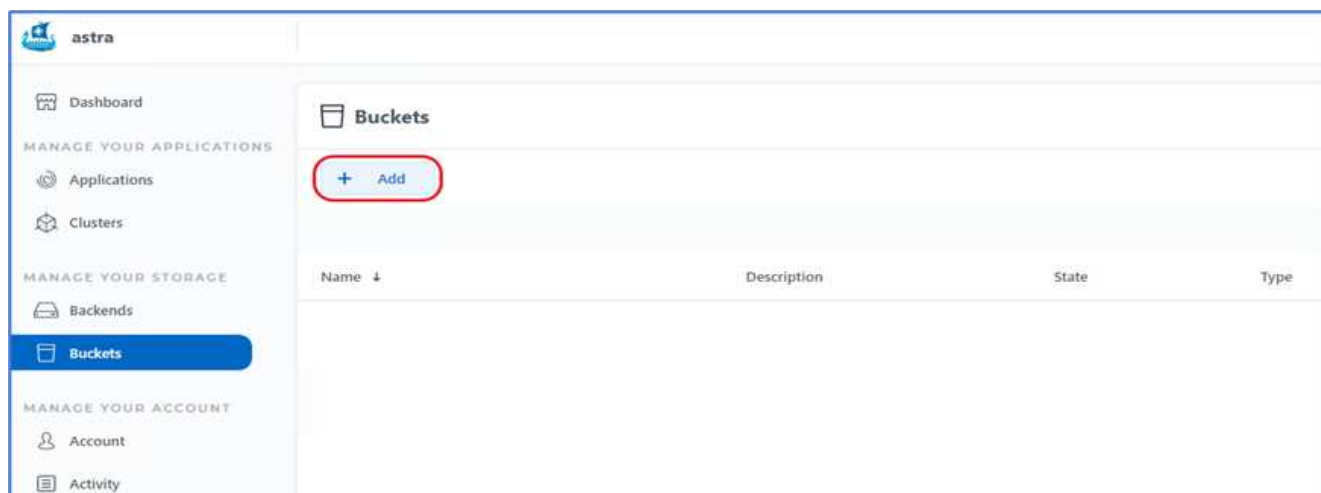
1-3 of 3 entries

<

>

Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
<a href="#">c190-cluster</a>	<div><div></div><div>Available</div></div>	<div><div></div><div>0.4/10.64 TiB: 3.8%</div></div>	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	<div><div></div></div>
<a href="#">healthylife</a>	<div><div></div><div>Available</div></div>	<div><div></div><div>5.16/106.42 TiB: 4.8%</div></div>	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	<div><div></div></div>
<a href="#">singlecvoaws</a>	<div><div></div><div>Available</div></div>	<div><div></div><div>0.07/0.62 TiB: 11.9%</div></div>	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	<div><div></div></div>

8. Per aggiungere un bucket ad Astra Control, selezionare Bucket e fare clic su Add (Aggiungi).



9. Selezionare il tipo di bucket e fornire il nome del bucket, il nome del server S3 o l'indirizzo IP e la credenziale S3. Fare clic su Aggiorna.

### 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

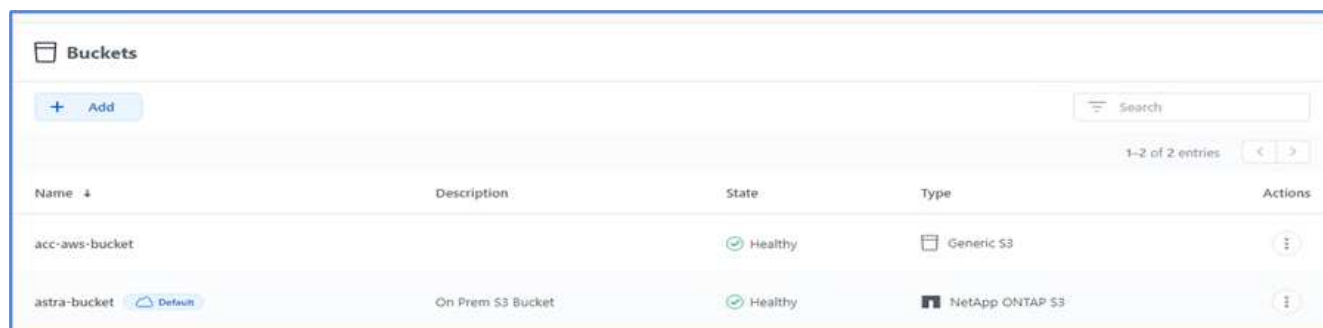
Edit your existing object store bucket. If the selected bucket is not currently defined as the default bucket for the cloud, you can replace the currently defined default bucket. Read more in [Storage buckets](#).





In questa soluzione vengono utilizzati entrambi i bucket AWS S3 e ONTAP S3. È anche possibile utilizzare StorageGRID.

Lo stato del bucket deve essere integro.



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	

Come parte della registrazione del cluster Kubernetes con Astra Control Center per la gestione dei dati applicativa, Astra Control crea automaticamente associazioni di ruoli e uno spazio dei nomi di monitoraggio NetApp per raccogliere metriche e log dai pod di applicazioni e dai nodi di lavoro. Impostare una delle classi di storage basate su ONTAP supportate come predefinita.

Dopo di lei ["Aggiungere un cluster alla gestione di Astra Control"](#), È possibile installare le applicazioni sul cluster (al di fuori di Astra Control) e quindi andare alla pagina Apps (applicazioni) in Astra Control per gestire le applicazioni e le relative risorse. Per ulteriori informazioni sulla gestione delle applicazioni con Astra, consultare ["Requisiti di gestione delle applicazioni"](#).

["Pagina successiva: Panoramica sulla convalida della soluzione."](#)

## Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.