



Instalación y configuración

FlexPod

NetApp
October 30, 2025

This PDF was generated from <https://docs.netapp.com/es-es/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.

Tabla de contenidos

- Instalación y configuración 1
 - Instalación de configuración básica de FlexPod para OpenShift Container Platform 4. 1
 - FlexPod para OpenShift Container Platform 4 en una instalación de VMware 1
 - Red Hat OpenShift en AWS 2
 - Cloud Volumes ONTAP de NetApp 3
 - Instalación de Astra Control Center en OpenShift Container Platform 3
 - Requisitos del entorno 4
 - Instale Astra Control Center utilizando OpenShift OperatorHub 5
 - Configure Astra Control Center 19

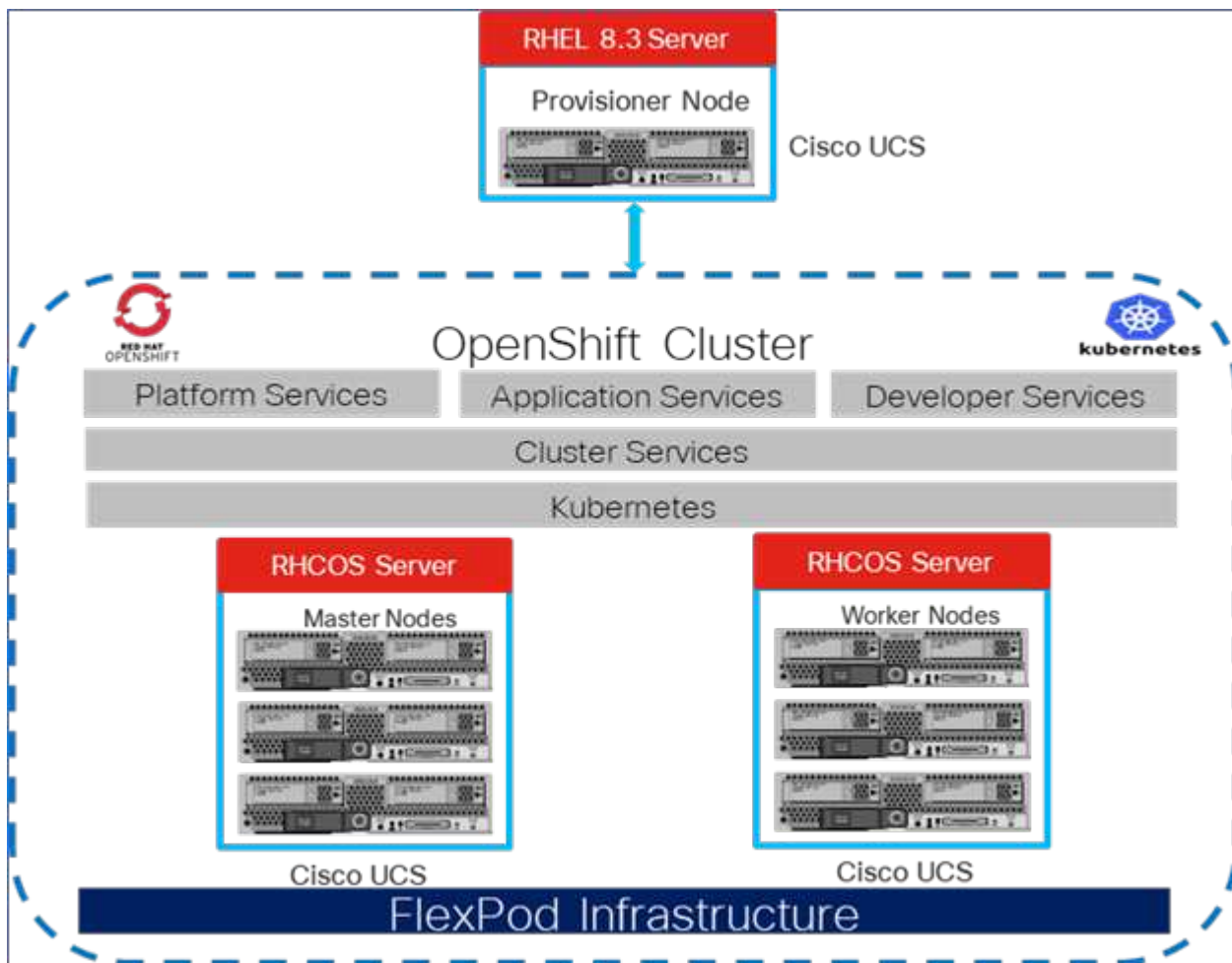
Instalación y configuración

Instalación de configuración básica de FlexPod para OpenShift Container Platform 4

"Anterior: Componentes de la solución."

Para comprender el diseño de configuración básica, los detalles de la implementación y la instalación y la configuración de FlexPod para OpenShift Container Platform 4 de NetApp Astra Trident, consulte ["FlexPod con OpenShift Guía de diseño y puesta en marcha validados de Cisco \(CVD\)"](#). Este CVD abarca la puesta en marcha de FlexPod y OpenShift Container Platform con Ansible. El CVD también proporciona información detallada sobre la preparación de nodos de trabajo, la instalación de Astra Trident, la configuración de back-end de almacenamiento y clase de almacenamiento, que son los pocos requisitos previos para poner en marcha y configurar Astra Control Center.

En la siguiente figura se muestra OpenShift Container Platform 4 Bare Metal en FlexPod.

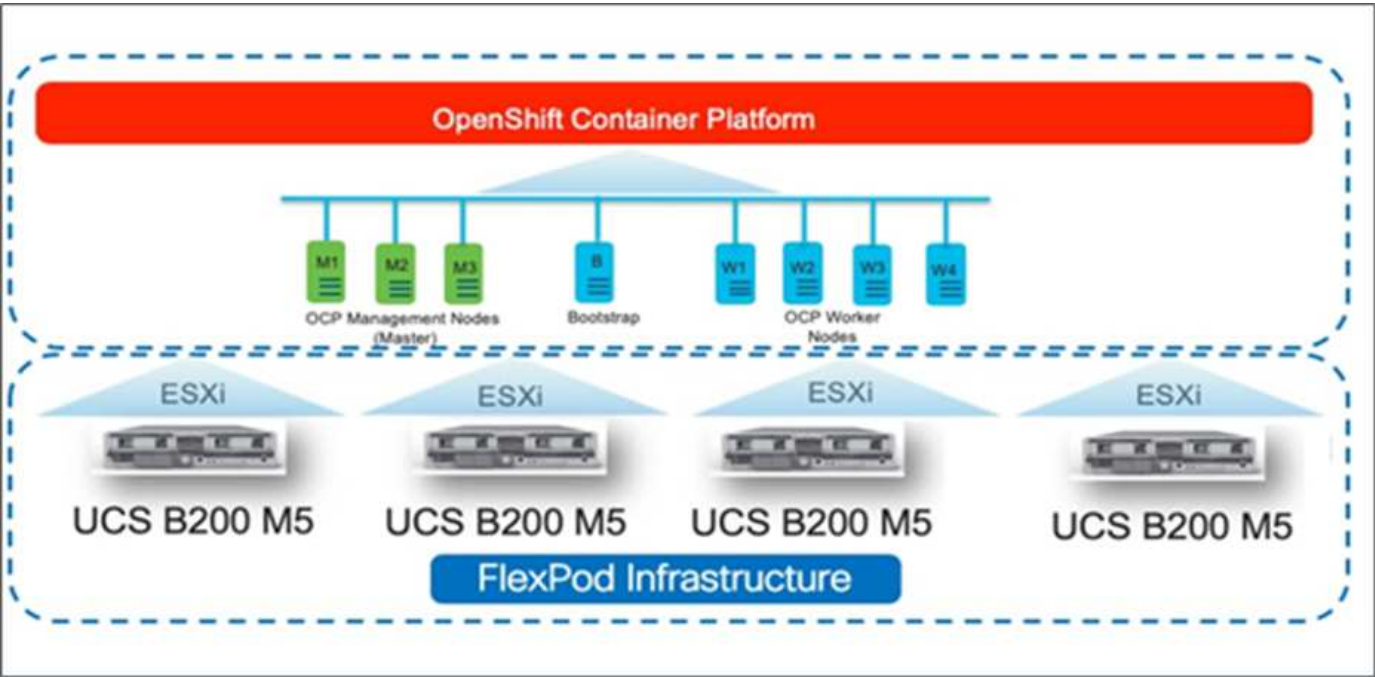


FlexPod para OpenShift Container Platform 4 en una instalación de VMware

Para obtener más información sobre la implementación de Red Hat OpenShift Container Platform 4 en

FlexPod con VMware vSphere, consulte "FlexPod Datacenter para OpenShift Container Platform 4".

La siguiente figura ilustra FlexPod para OpenShift Container Platform 4 en vSphere.



"Siguiente: Red Hat OpenShift en AWS."

Red Hat OpenShift en AWS

"Anterior: Instalación básica de FlexPod para OpenShift Container Platform 4."

Un clúster independiente de OpenShift Container Platform 4 autogestionado se pone en marcha en AWS como sitio de recuperación ante desastres. Los nodos maestro y trabajador abarcan tres zonas de disponibilidad para obtener alta disponibilidad.

Instances (6) Info								
<div><div>Q Search</div><div><div>ocp</div><div>X</div><div>Clear filters</div></div></div>								
<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 se implementa como un **"clúster privado"** En un VPC existente en AWS. Un clúster privado de OpenShift Container Platform no expone puntos finales externos y se puede acceder sólo desde una red interna y no es visible para Internet. Se pone en marcha un Cloud Volumes ONTAP de NetApp de un único nodo mediante Cloud Manager de NetApp, que proporciona un back-end de almacenamiento a Astra Trident.

Para obtener más información acerca de la instalación de OpenShift en AWS, consulte ["Documentación de OpenShift"](#).

"Siguiente: Cloud Volumes ONTAP de NetApp."

Cloud Volumes ONTAP de NetApp

"Anterior: Red Hat OpenShift en AWS."

La instancia de Cloud Volumes ONTAP de NetApp se pone en marcha en AWS y sirve como almacenamiento de back-end a Astra Trident. Antes de agregar un entorno de trabajo de Cloud Volumes ONTAP, se debe desplegar un conector. Cloud Manager le pregunta si intenta crear el primer entorno de trabajo de Cloud Volumes ONTAP sin un conector en su lugar. Para implementar un conector en AWS, consulte ["Cree un conector"](#).

Para implementar Cloud Volumes ONTAP en AWS, consulte ["Inicio rápido para AWS"](#).

Después de la puesta en marcha de Cloud Volumes ONTAP, puede instalar Astra Trident y configurar la clase de snapshot y back-end de almacenamiento en el clúster de OpenShift Container Platform.

"Siguiente: Instalación de Astra Control Center en OpenShift Container Platform."

Instalación de Astra Control Center en OpenShift Container Platform

"Anterior: Cloud Volumes ONTAP de NetApp."

Puede instalar Astra Control Center en un clúster OpenShift que se ejecuta en FlexPod o en AWS con un back-end de almacenamiento de Cloud Volumes ONTAP. En esta solución, Astra Control Center se pone en marcha en el clúster de configuración básica OpenShift.

Astra Control Center se puede instalar utilizando el proceso estándar descrito ["aquí"](#) O desde Red Hat

OpenShift OperatorHub. Astra Control Operator es un operador certificado de Red Hat. En esta solución, Astra Control Center se instala mediante Red Hat OperatorHub.

Requisitos del entorno

- Astra Control Center es compatible con varias distribuciones de Kubernetes; para Red Hat OpenShift, las versiones compatibles incluyen Red Hat OpenShift Container Platform 4.8 o 4.9.
- Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno y de la aplicación del usuario final:

Componentes	Requisito
Capacidad del back-end de almacenamiento	500 GB disponibles como mínimo
Nodos de trabajo	Al menos 3 nodos de trabajo, con 4 núcleos de CPU y 12 GB de RAM cada uno
Dirección del nombre de dominio completo (FQDN)	Una dirección FQDN para Astra Control Center
Astra Trident	Astra Trident 21.04 o posterior instalado y configurado
Controlador de entrada o equilibrador de carga	Configure el controlador de entrada para exponer Astra Control Center con una dirección URL o equilibrador de carga para proporcionar la dirección IP que se resolverá en el FQDN

- Debe tener un registro de imágenes privadas existente en el que pueda insertar las imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargue las imágenes.



Algunas imágenes se van tirando mientras se ejecutan ciertos flujos de trabajo, y cuando es necesario se crean y destruyen contenedores.

- Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con los siguientes controladores de ONTAP proporcionados por Astra Trident:
 - ontap-nas
 - ontap-nas-flexgroup
 - san ontap
 - ontap-san-economía



Asumimos que los clústeres OpenShift puestos en marcha tienen Astra Trident instalado y configurado con un back-end de ONTAP y también se define una clase de almacenamiento predeterminada.

- Para la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Para modificar la política de exportación de ONTAP y permitir estas operaciones, ejecute los siguientes comandos:

```
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
```



Para añadir un segundo entorno operativo OpenShift como recurso informático gestionado, asegúrese de que la función Snapshot de Astra Trident Volume esté habilitada. Para habilitar y probar copias Snapshot de volumen con Astra Trident, consulte el funcionario ["Instrucciones de Astra Trident"](#).

- A. **"VolumeSnapClass"** Debe configurarse en todos los clústeres de Kubernetes desde el lugar donde se gestionan las aplicaciones. Esto también podría incluir el clúster K8s en el que está instalado Astra Control Center. Astra Control Center puede gestionar aplicaciones en el clúster K8s en el que se ejecuta.

Y gestión de aplicaciones

- **Licencia.** para gestionar aplicaciones con Astra Control Center, necesita una licencia Astra Control Center.
- **Espacios de nombres.** un espacio de nombres es la entidad más grande que puede ser administrada como una aplicación por Astra Control Center. Puede elegir filtrar componentes según las etiquetas de la aplicación y las etiquetas personalizadas de un espacio de nombres existente y gestionar un subconjunto de recursos como aplicación.
- **StorageClass.** Si instala una aplicación con StorageClass definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener el StorageClass especificado originalmente. Se produce un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo de almacenamiento.
- **Recursos Kubernetes.** las aplicaciones que usan recursos Kubernetes no capturados por Astra Control podrían no tener capacidades completas de gestión de datos de aplicaciones. Astra Control puede capturar los siguientes recursos de Kubernetes:

Recursos de Kubernetes		
Función de clúster	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	Recurso personalizado	Cronjob
DemonSet	HorizontalPodAutocaler	Entrada
DeploymentConfig	MutatingWebhook	Claim persistente
Pod	PodDisruptionBudget	PodTemplate
Política de red	Replicaset	Función
RoleBinding	Ruta	Secreto
ValidadoWebhook		

Instale Astra Control Center utilizando OpenShift OperatorHub

El siguiente procedimiento instala Astra Control Center utilizando Red Hat OperatorHub. En esta solución, Astra Control Center se instala en un clúster OpenShift con configuración básica que se ejecuta en FlexPod.

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del ["Sitio de soporte de NetApp"](#).
2. Descargue el archivo `.zip` de los certificados y claves de Astra Control Center desde ["Sitio de soporte de NetApp"](#).
3. Verifique la firma del paquete.

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

4. Extraiga las imágenes de Astra.

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

5. Cambie al directorio Astra.

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

6. Agregue las imágenes al registro local.

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

7. Utilice la secuencia de comandos adecuada para cargar las imágenes, etiquetar las imágenes y empujarlas al registro local.

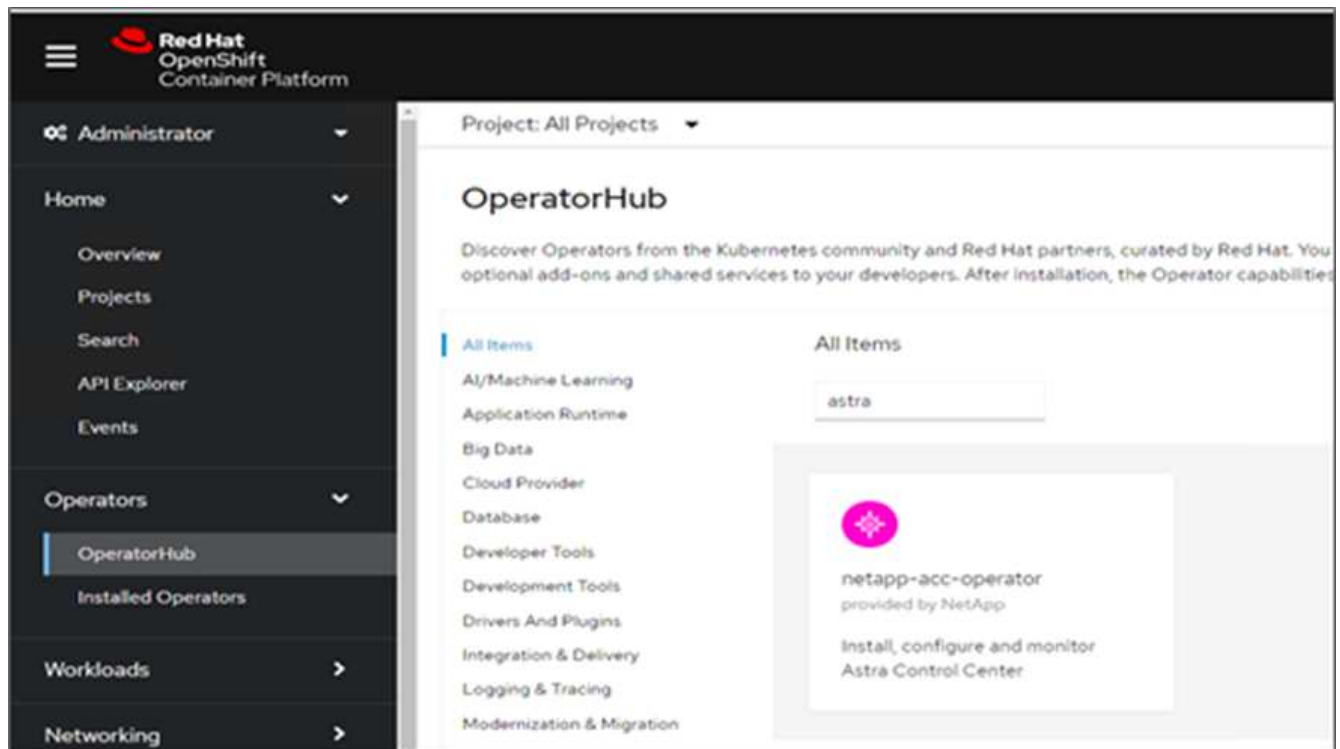
Para Docker:

```
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
```


Para 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. Inicie sesión en la consola web de clúster OpenShift con configuración básica. En el menú lateral, seleccione operadores > OperatorHub. Introduzca astra para enumerar la netapp-acc-operator.



netapp-acc-operator Es un operador Red Hat OpenShift certificado y se encuentra en el catálogo de OperatorHub.

9. Seleccione netapp-acc-operator Y haga clic en instalar.



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. Seleccione las opciones adecuadas y haga clic en instalar.

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

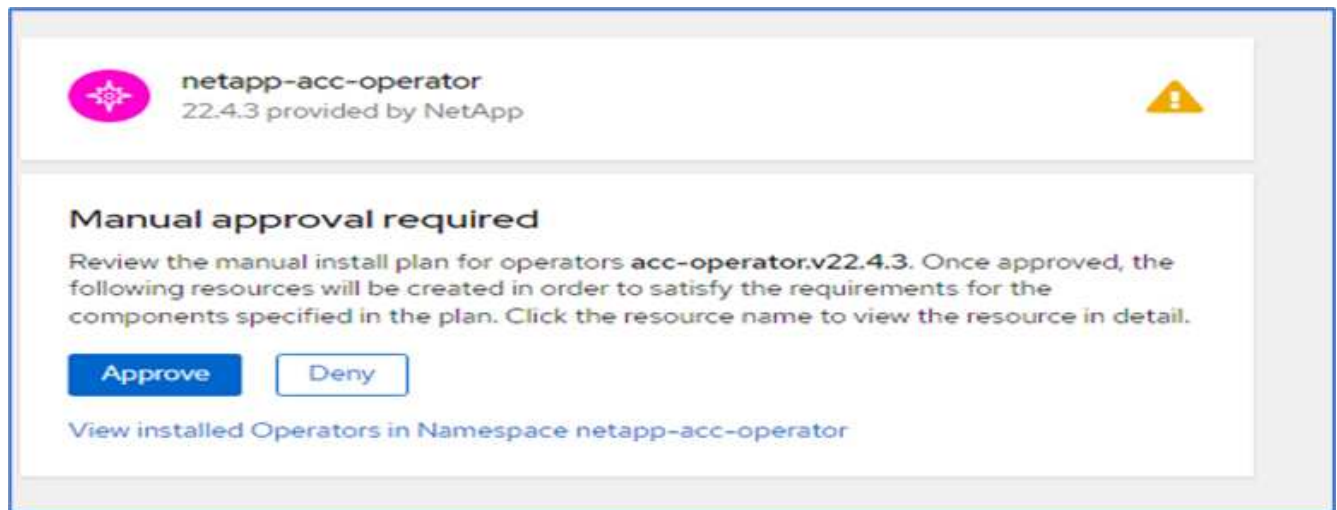
Provided APIs


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

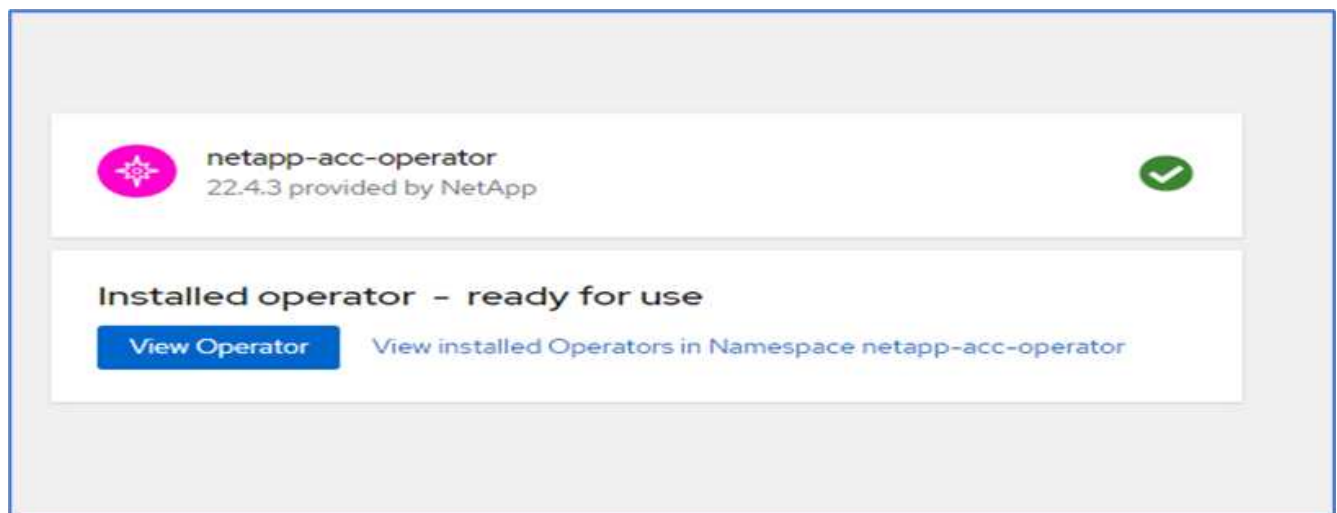
Install

Cancel

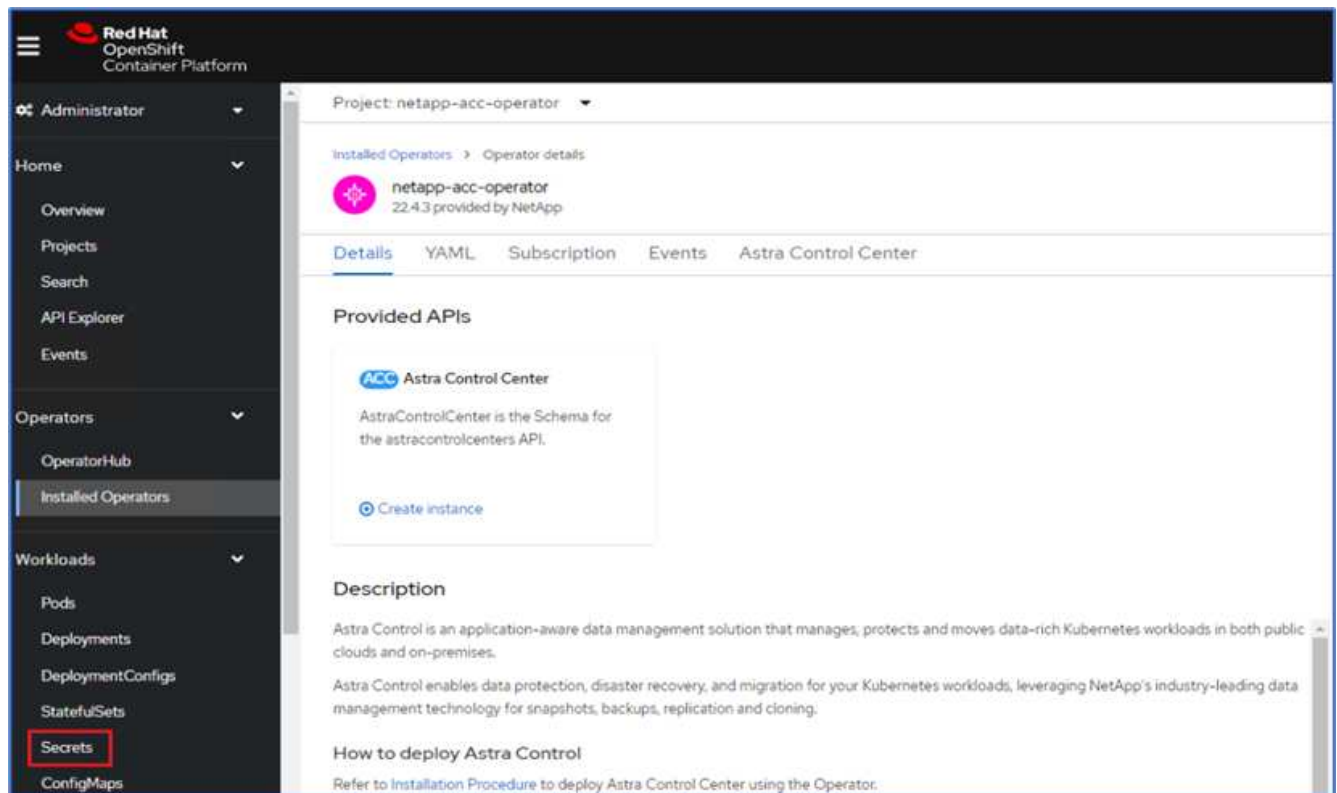
11. Apruebe la instalación y espere a que se instale el operador.



12. En esta fase, el operador se instala correctamente y está listo para su uso. Haga clic en Ver operador para iniciar la instalación de Astra Control Center.



13. Antes de instalar Astra Control Center, cree el secreto de extracción para descargar imágenes Astra del registro Docker que ha introducido anteriormente.



14. Para extraer las imágenes de Astra Control Center de su Docker Private repo, cree un secreto en la `netapp-acc-operator` espacio de nombres. Este nombre secreto se proporciona en el manifiesto Astra Control Center YAML en un paso posterior.

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

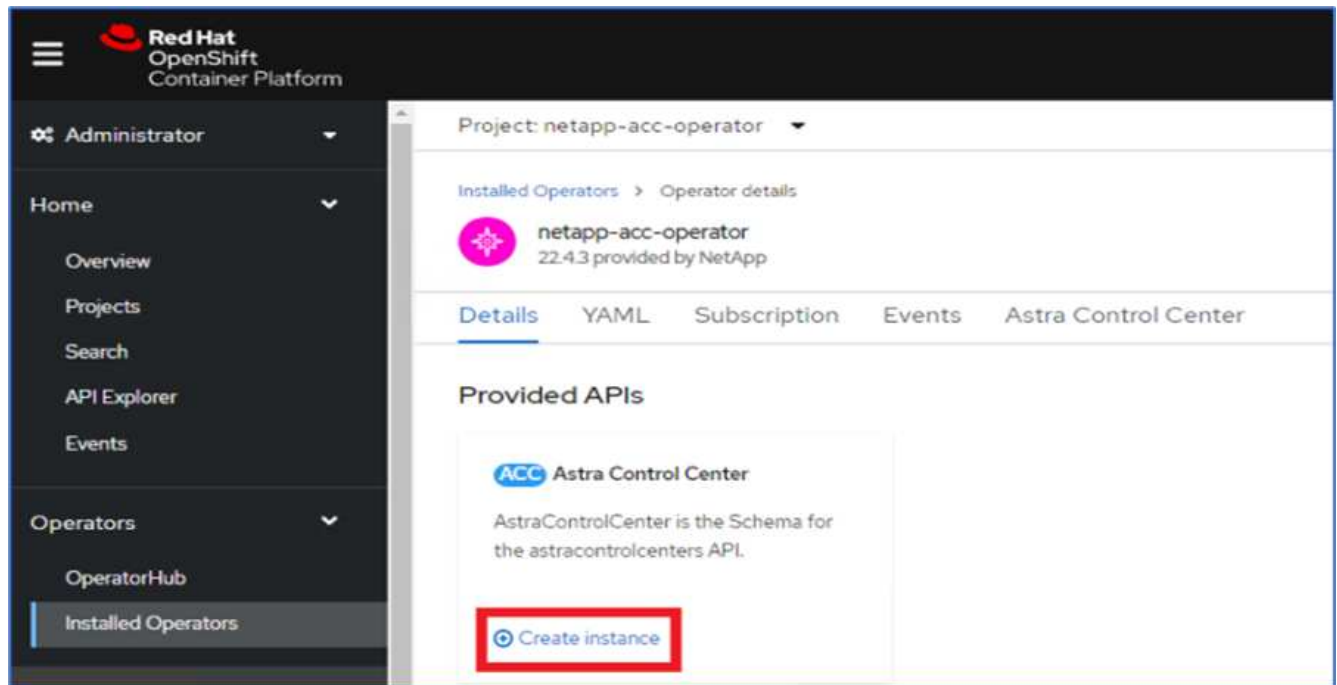
Username *

Password *

Email

[+ Add credentials](#)

15. En el menú lateral, seleccione operadores > operadores instalados y haga clic en Crear instancia en la sección API que se proporciona.



- Complete el formulario Create AstraControlCenter. Proporcione el nombre, la dirección Astra y la versión Astra.

The screenshot shows the 'Create AstraControlCenter' form. The form is titled 'Create AstraControlCenter' and includes a note: 'Create by completing the form. Default values may be provided by the Operator authors.' The form is configured via 'Form view'. The fields are as follows:

- Name ***: acc
- Labels**: .app=frontend
- Auto Support ***: A checkbox labeled 'AutoSupport' with a note: '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. A note 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. A note 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'



En Dirección Astra, proporcione la dirección FQDN para Astra Control Center. Esta dirección se utiliza para acceder a la consola web de Astra Control Center. El FQDN también debe resolver una red IP accesible y se debe configurar en el DNS.

- Escriba un nombre de cuenta, una dirección de correo electrónico, el apellido del administrador y conserve

la política de reclamación de volumen predeterminada. Si está utilizando un equilibrador de carga, establezca el tipo de entrada en AccTraefik. De lo contrario, seleccione Genérico para Ingress.Controller. En el Registro de imágenes, introduzca la ruta de acceso y el secreto del Registro de imágenes del contenedor.

The screenshot shows the Astra Control Center configuration interface. The left sidebar has a dark theme with the following menu items: Administrator, Home, Operators (expanded), OperatorHub, Installed Operators (selected), Workloads, Networking, Storage, Builds, Observe, Compute, User Management, and Administration. The main content area is titled 'Project: netapp-acc-operator'. It contains several configuration sections: 'Account Name' with a value of 'ocp', 'Email' with 'abhinav3@netapp.com', 'Last Name' with 'Singh', 'Volume Reclaim Policy' set to 'Retain', 'Ingress Type' set to 'AccTraefik', and 'Image Registry' with a redacted name and secret 'astra-registry-cred'.



En esta solución, se utiliza el equilibrador de carga de Metallb. Por lo tanto, el tipo de entrada es AccTraefik. De esta forma se expone la puerta de enlace Traefik de Astra Control Center como un servicio Kubernetes de tipo LoadBalancer.

18. Introduzca el nombre del administrador, configure el escalado de recursos y proporcione la clase de almacenamiento. Haga clic en Crear.

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](#)

El estado de la instancia de Astra Control Center debe cambiar de implementar a preparado.

Project: netapp-acc-operator

Installed Operators > Operator details

netapp-acc-operator
22.43 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	app:acc	8 minutes ago

- Compruebe que todos los componentes del sistema se hayan instalado correctamente y que todos los pods estén en ejecución.

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

NAME	RESTARTS	AGE	READY	STATUS
acc-helm-repo-77745b49b5-7zg2v	1	10m	1/1	Running
acc-operator-controller-manager-5c656c44c6-tqnmn	2	13m	2/2	Running

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

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 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

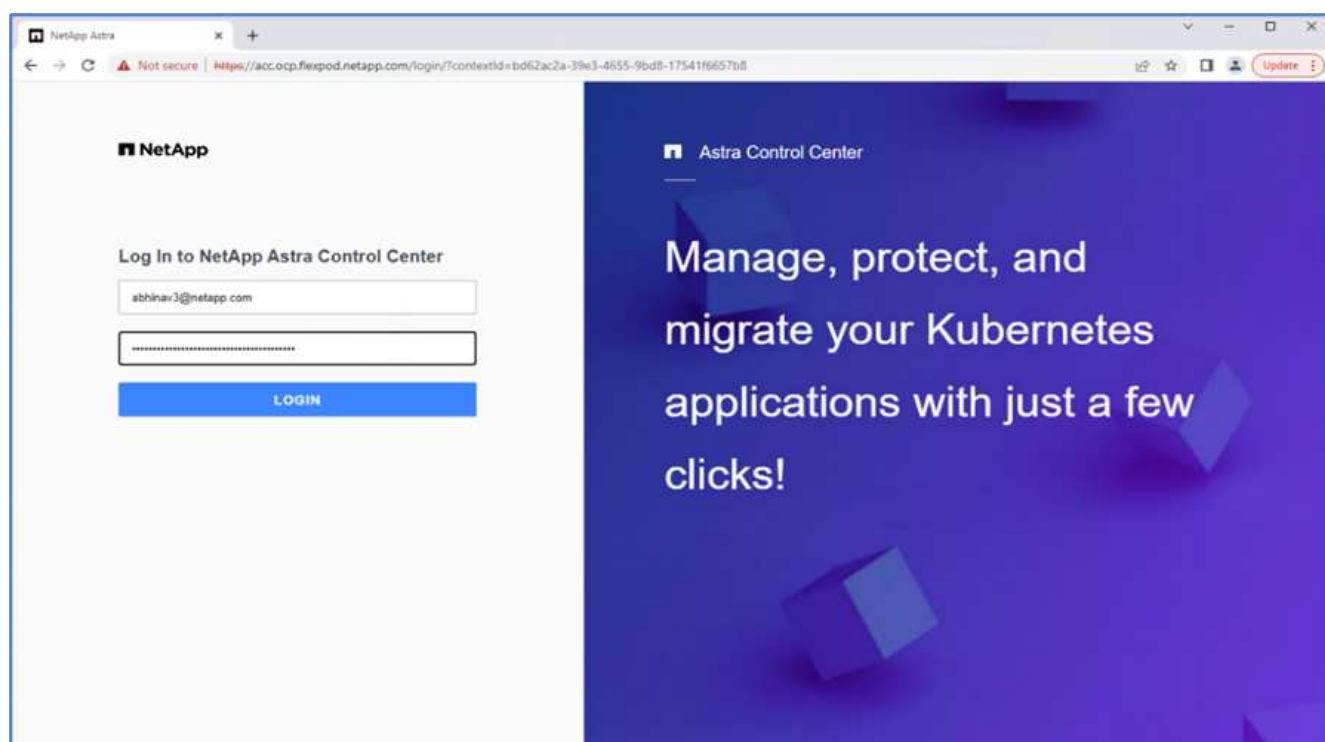


Cada pod debe tener el estado de ejecución. Puede tardar varios minutos en implementar los pods del sistema.

20. Cuando todos los pods estén en ejecución, ejecute el siguiente comando para recuperar la contraseña una vez. En la versión YAML de la salida, compruebe la `status.deploymentState` para el valor desplegado y, a continuación, copie el `status.uuid` valor. La contraseña es ACC- Seguido del valor UUID. (ACC-[UUID]).

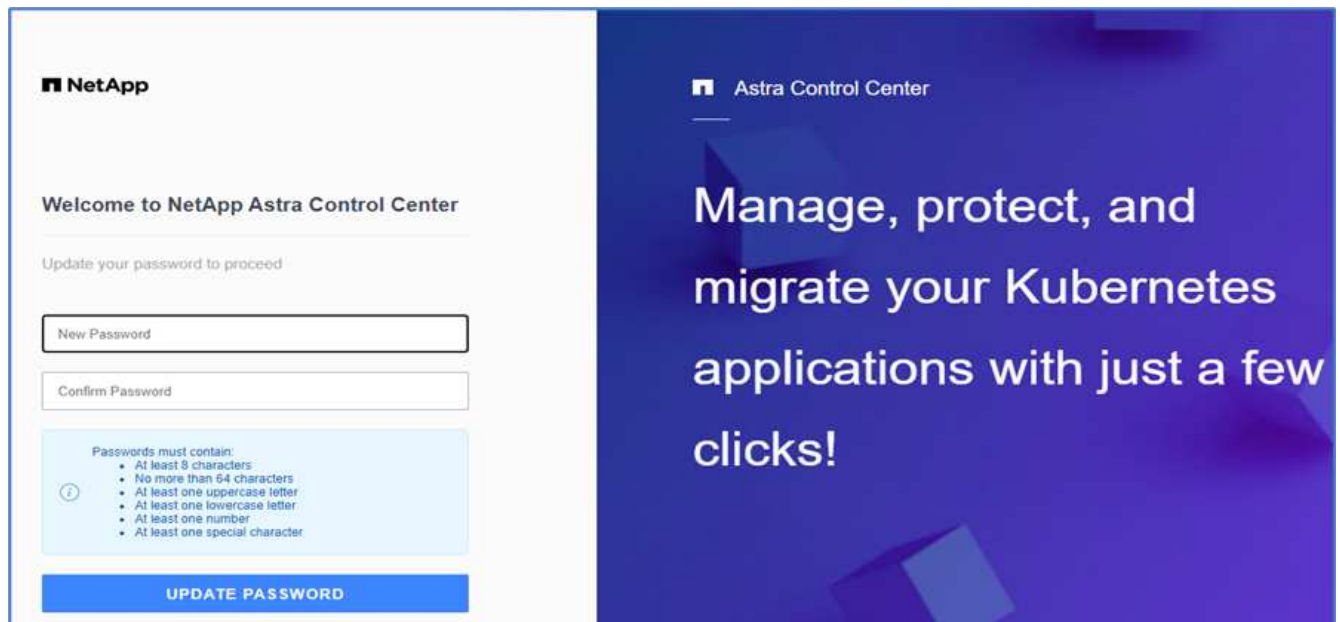
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. En un explorador, desplácese hasta la URL usando el FQDN que haya proporcionado.
22. Inicie sesión utilizando el nombre de usuario predeterminado, que es la dirección de correo electrónico proporcionada durante la instalación y la contraseña única ACC-[UUID].



Si introduce una contraseña incorrecta tres veces, la cuenta de administrador estará bloqueada durante 15 minutos.

23. Cambie la contraseña y continúe.

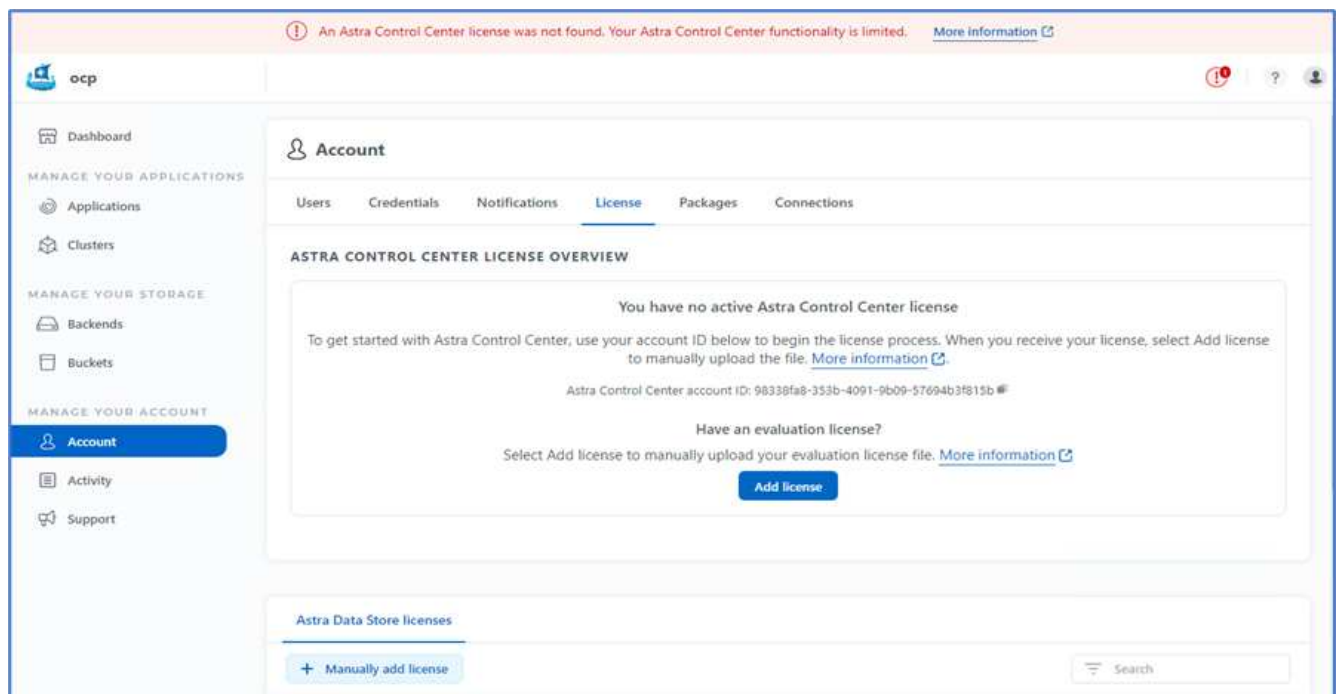


Para obtener más información acerca de la instalación de Astra Control Center, consulte "[Descripción general de la instalación de Astra Control Center](#)" página.

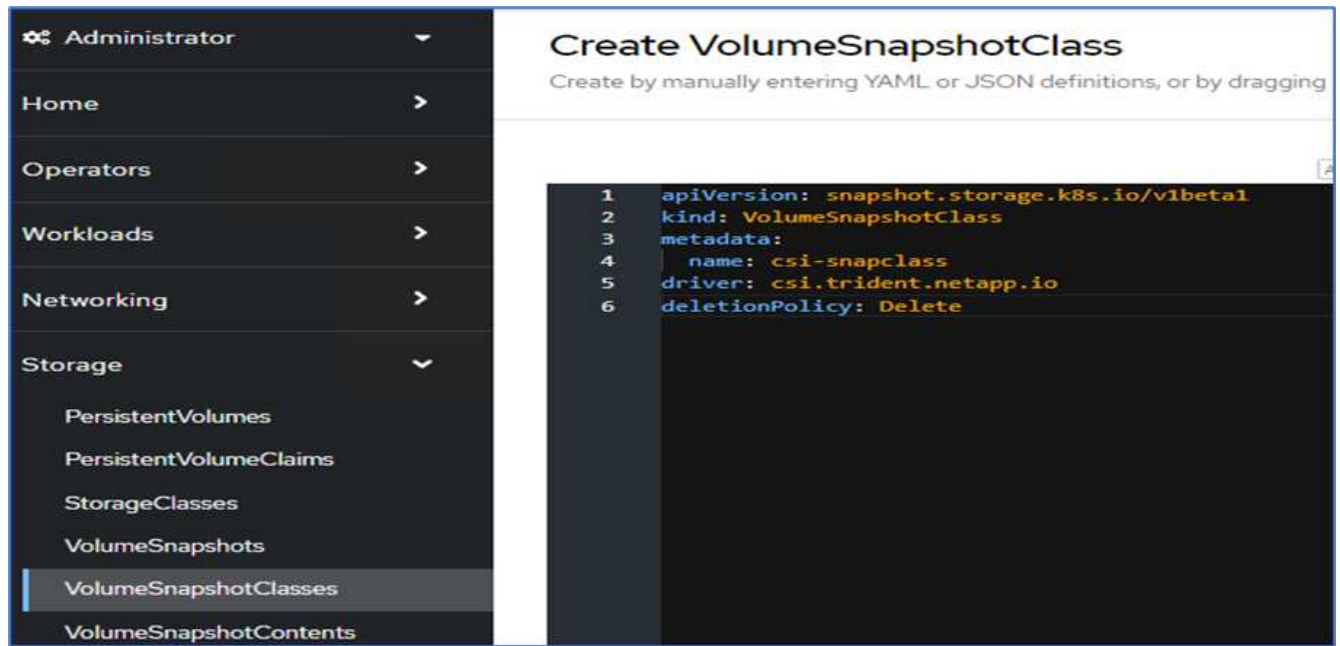
Configure Astra Control Center

Después de instalar Astra Control Center, inicie sesión en la interfaz de usuario, cargue la licencia, añada clústeres, gestione el almacenamiento y añada bloques.

1. En la página de inicio de cuenta, vaya a la ficha Licencia y seleccione Agregar licencia para cargar la licencia Astra.



2. Antes de agregar el clúster OpenShift, cree una clase de snapshot Astra Trident Volume desde la consola web de OpenShift. La clase de snapshot Volume se configura con la `csi.trident.netapp.io` controlador.



- Para añadir el clúster de Kubernetes, vaya a Clusters en la página de inicio y haga clic en Add Kubernetes Cluster. A continuación, cargue el kubeconfig archivo para el clúster y escriba un nombre de credencial. Haga clic en Siguiente.

Add Kubernetes cluster STEP 1/3: CREDENTIALS

CREDENTIALS

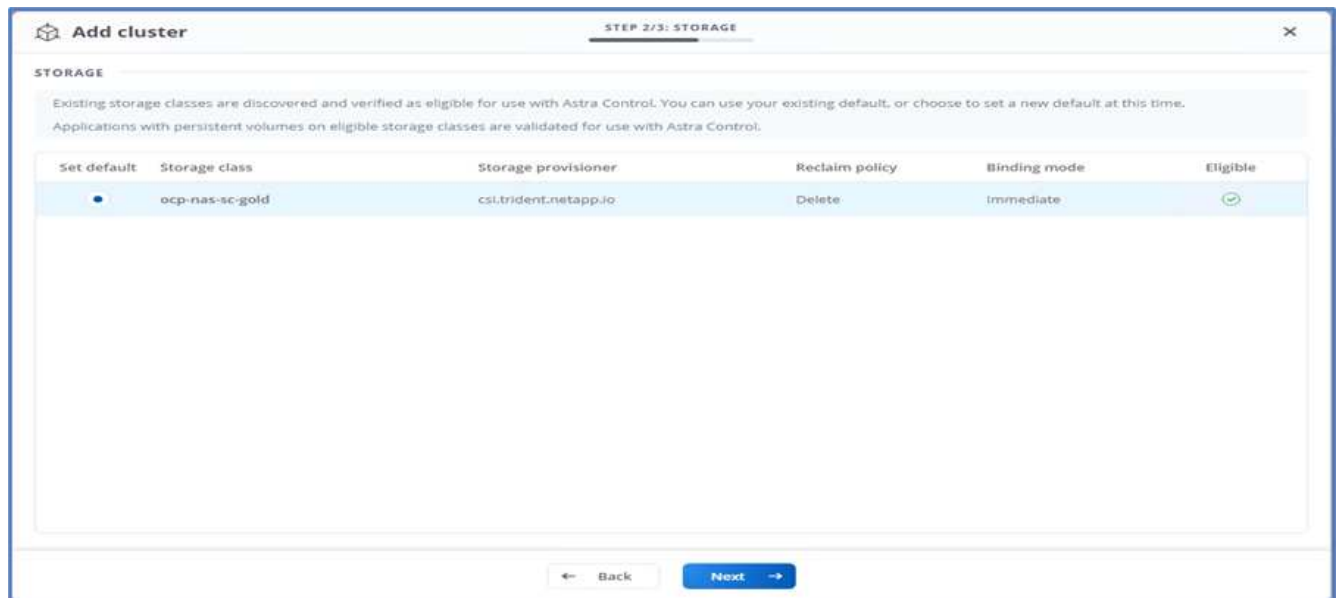
Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.
Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

Upload file | Paste from clipboard

Kubeconfig YAML file:

Credential name:

- Las clases de almacenamiento existentes se detectan de forma automática. Seleccione la clase de almacenamiento predeterminada, haga clic en Next y después en Add cluster.

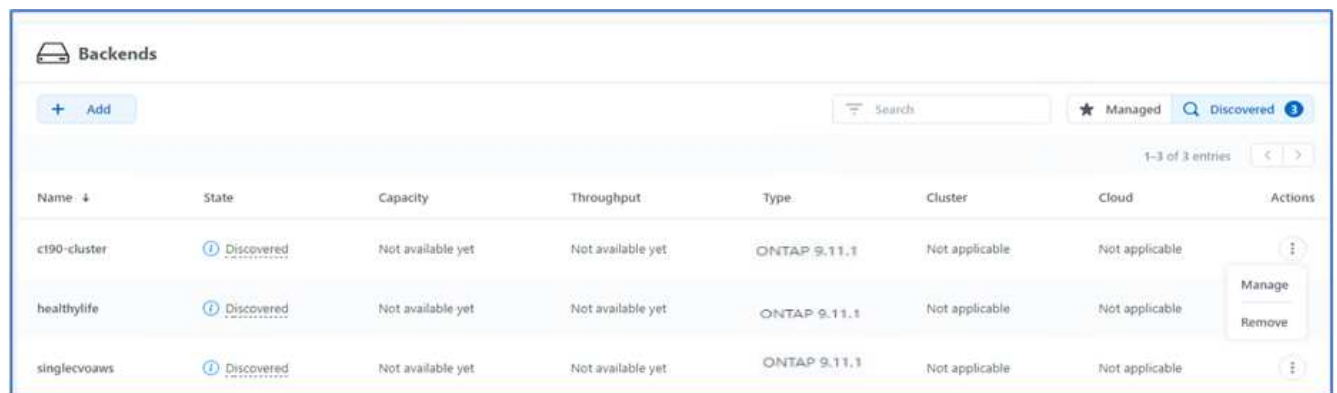


- El cl ster se a ade en unos minutos. Para agregar cl steres de OpenShift Container Platform adicionales, repita los pasos 1 4.



Para a adir un entorno operativo OpenShift adicional como recurso inform tico gestionado, aseg rese de que Astra Trident "Objetos VolumeSnapshotClass" est n definidos.

- Para gestionar el almacenamiento, vaya a backends (backends), haga clic en los tres puntos de la secci n Actions (acciones) en el backend que desea gestionar. Haga clic en gestionar.



- Proporcione las credenciales de ONTAP y haga clic en Next. Revise la informaci n y haga clic en Managed. Los back-ends deber an ser el siguiente ejemplo.

Backends							
<div> <div>+ Add</div> <div> <div>Search</div> <div> <div>★ Managed</div> <div>🔍 Discovered</div> </div> </div> </div> <div>1-3 of 3 entries</div>							
Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
c190-cluster	Available	0.4/10.64 TiB: 3.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
healthylife	Available	5.16/106.42 TiB: 4.8%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮
singlecvoaws	Available	0.07/0.62 TiB: 11.9%	Not available yet	ONTAP 9.11.1	Not applicable	Not applicable	⋮

8. Para agregar un cucharón a Astra Control, seleccione cucharones y haga clic en Agregar.

astra

Dashboard

MANAGE YOUR APPLICATIONS

Applications

Clusters

MANAGE YOUR STORAGE

Backends

Buckets

MANAGE YOUR ACCOUNT

Account

Activity

Buckets

+ Add

Name ↓	Description	State	Type

9. Seleccione el tipo de bloque y proporcione el nombre de bloque, el nombre del servidor S3, la dirección IP y la credencial S3. Haga clic en Update.

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

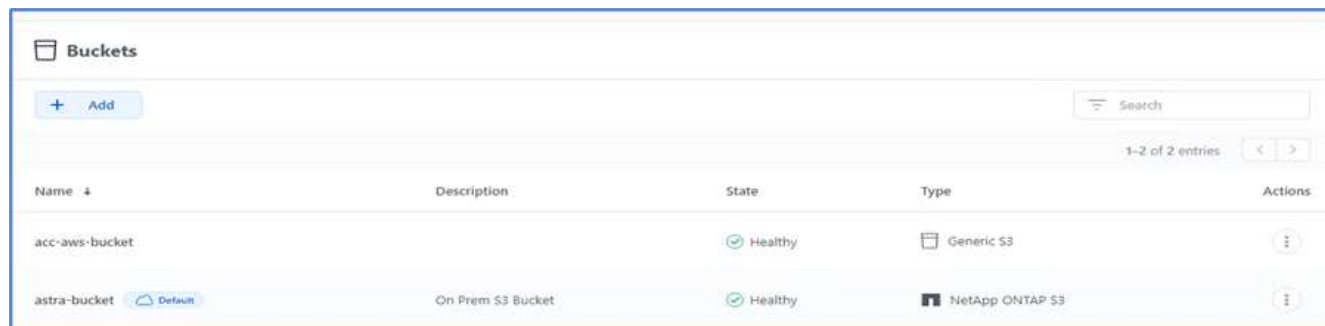
Edit your existing object store bucket. If the selected object store is not currently defined as the default bucket for the cloud, you can replace the currently defined default bucket. Read more in [Storage buckets](#).

22



En esta solución, se usan los bloques AWS S3 y ONTAP S3. También puede utilizar StorageGRID.

El estado de la cuchara debe ser saludable.



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	

Como parte del registro del clúster de Kubernetes con Astra Control Center para la gestión de datos para aplicaciones, Astra Control crea automáticamente vinculaciones de roles y un espacio de nombres de supervisión de NetApp para recopilar métricas y registros de los pods de la aplicación y los nodos de trabajo. Cree una de las clases de almacenamiento basado en ONTAP compatibles por defecto.

Usted primero ["Añada un clúster a la gestión de Astra Control"](#), Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para gestionar las aplicaciones y sus recursos. Para obtener más información sobre la gestión de aplicaciones con Astra, consulte ["Requisitos de gestión de aplicaciones"](#).

["Siguiente: Información general sobre la validación de la solución."](#)

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.