



# **Manos a la obra**

## **Astra Control Center**

NetApp  
June 06, 2024

# Tabla de contenidos

- Manos a la obra ..... 1
  - Requisitos del Centro de Control de Astra ..... 1
  - Inicio rápido para Astra Control Center ..... 7
  - Información general de la instalación ..... 9
  - Configure Astra Control Center ..... 57
  - Preguntas frecuentes para Astra Control Center ..... 77

# Manos a la obra

## Requisitos del Centro de Control de Astra

Comience verificando la preparación de su entorno operativo, clústeres de aplicaciones, aplicaciones, licencias y explorador web.

- [Requisitos del entorno operativo](#)
- [Compatibles con los back-ends de almacenamiento](#)
- [Requisitos del clúster de aplicaciones](#)
- [Y gestión de aplicaciones](#)
- [Requisitos previos de replicación](#)
- [Acceso a Internet](#)
- [Licencia](#)
- [Entrada para clústeres de Kubernetes en las instalaciones](#)
- [Requisitos de red](#)
- [Exploradores web compatibles](#)

### Requisitos del entorno operativo

Astra Control Center se ha validado en los siguientes tipos de entornos operativos:

- Google Anthos 1.10 o 1.11
- Kubernetes 1.22 a 1.24
- Rancher Kubernetes Engine (RKE):
  - RKE 1.2.16 w/ Rancher 2.5.12 y RKE 1.3.3 w/ 2.6.3
  - RKE 2 (v1.23.6+rke2r2) con Rancher 2.6.3
- OpenShift Container Platform de Red Hat 4.8, 4.9 o 4.10
- VMware Tanzania Kubernetes Grid 1.4 o 1.5
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2 o 1.13

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno. Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad del back-end de almacenamiento	500 GB disponibles como mínimo
Nodos de trabajo	Al menos 3 nodos de trabajo en total, con 4 núcleos de CPU y 12 GB de RAM cada uno
Dirección FQDN	Una dirección FQDN para Astra Control Center

Componente	Requisito
Astra Trident	Astra Trident 21.10.1 o una versión más reciente instalada y configurada Astra Trident 22.07 o más reciente para la replicación de aplicaciones basada en SnapMirror



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

- **Registro de imágenes:** Debe tener un registro de imágenes Docker privado existente en el que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.
- **Configuración de Astra Trident/ONTAP:** 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
  - san ontap
  - ontap-san-economía



Durante la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Por este motivo, es necesario configurar una política de exportación de volúmenes ONTAP para permitir estas operaciones. Puede hacerlo con los siguientes comandos:

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



Si tiene pensado añadir un segundo entorno operativo OpenShift como recurso informático gestionado, debe asegurarse de que la función Astra Trident Volume Snapshot esté habilitada. Para habilitar y probar copias Snapshot de volumen con Astra Trident, ["Consulte las instrucciones oficiales de la Astra Trident"](#).

## Requisitos del clúster de Grid de VMware Tanzania Kubernetes

Al alojar Astra Control Center en un clúster VMware Tanzu Kubernetes Grid (TKG) o Tanzu Kubernetes Grid Integrated Edition (TKGi), tenga en cuenta las siguientes consideraciones.

- Desactive la implementación predeterminada de la clase de almacenamiento TKG o TKGi en cualquier cluster de aplicaciones que Astra Control deba gestionar. Para ello, edite la `TanzuKubernetesCluster` recurso en el clúster de espacio de nombres.
- Como parte de la instalación de Astra Control Center, los siguientes recursos se crean en un entorno restringido de directiva de seguridad de POD (PSP):
  - directiva de seguridad de pod
  - Rol de RBAC

- RBAC RoleBinding la función RBAC y los recursos RoleBinding se crean en la `netapp-acc` espacio de nombres.
- Tenga en cuenta los requisitos específicos para Astra Trident al implementar Astra Control Center en un entorno TKG o TKGi. Para obtener más información, consulte "[Documentación de Astra Trident](#)".



El token predeterminado del archivo de configuración de VMware TKG y TKGi caduca diez horas después de la implementación. Si utiliza productos de la cartera de Tanzu, debe generar un archivo de configuración de tanzu Kubernetes Cluster con un token que no caduca para evitar problemas de conexión entre Astra Control Center y clústeres de aplicaciones administradas. Si desea obtener instrucciones, visite "[La documentación de producto del centro de datos NSX-T de VMware.](#)"

## Requisitos de clúster de Google Anthos

Al alojar Astra Control Center en un clúster de Google Anthos, tenga en cuenta que Google Anthos incluye de forma predeterminada el equilibrador de carga de MetalLB y el servicio de puerta de enlace de entrada Istio, lo que le permite utilizar simplemente las capacidades de entrada genéricas de Astra Control Center durante la instalación. Consulte "[Configurar Astra Control Center](#)" para obtener más detalles.

## Compatibles con los back-ends de almacenamiento

Astra Control Center admite los siguientes back-ends de almacenamiento.

- NetApp ONTAP 9.5 o sistemas AFF y FAS más recientes
- ONTAP 9.8 de NetApp o sistemas AFF y FAS más recientes para la replicación de aplicaciones basadas en SnapMirror
- Cloud Volumes ONTAP de NetApp

Para utilizar Astra Control Center, compruebe que dispone de las siguientes licencias de ONTAP, en función de lo que necesite:

- FlexClone
- SnapMirror: Opcional. Solo es necesario para la replicación en sistemas remotos mediante la tecnología SnapMirror. Consulte "[Información sobre licencias de SnapMirror](#)".
- Licencia de S3: Opcional. Solo se necesita para bloques ONTAP S3

Quizás desee comprobar si el sistema ONTAP tiene las licencias necesarias. Consulte "[Gestione licencias de ONTAP](#)".

## Requisitos del clúster de aplicaciones

Astra Control Center tiene los siguientes requisitos para los clústeres que tiene previsto gestionar desde Astra Control Center. Estos requisitos también se aplican si el clúster que tiene previsto gestionar es el clúster de entorno operativo que aloja Astra Control Center.

- La versión más reciente de Kubernetes "[componente de controladora snapshot](#)" está instalado
- Una Astra Trident "[volumesnapshotclass object](#)" ha sido definido por un administrador
- Existe una clase de almacenamiento de Kubernetes predeterminada en el clúster
- Se configura al menos una clase de almacenamiento para que use Astra Trident



Su clúster de aplicaciones debe tener un `kubeconfig.yaml` archivo que define sólo un elemento `context`. Consulte la documentación de Kubernetes para ["información sobre la creación de archivos kubeconfig"](#).



Cuando administre clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en `kubeconfig` Archivo proporcionado por Rancher para utilizar un contexto de plano de control en lugar del contexto del servidor API Rancher. Esto reduce la carga en el servidor API de Rancher y mejora el rendimiento.

## Y gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencia:** Para gestionar aplicaciones mediante Astra Control Center, necesita una licencia Astra Control Center.
- **Namespaces:** Astra Control requiere que una aplicación no abarque más de un único espacio de nombres, pero un espacio de nombres puede contener más de una aplicación.
- **StorageClass:** Si instala una aplicación con StorageClass definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonado debe tener el StorageClass especificado originalmente. Se producirá 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 de Kubernetes:** Las aplicaciones que usan recursos de Kubernetes no recopilados por Astra Control podrían no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

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

## Requisitos previos de replicación

La replicación de aplicaciones de Astra Control requiere que se cumplan los siguientes requisitos previos antes de comenzar:

- Para lograr una recuperación ante desastres sin problemas, le recomendamos que ponga en marcha Astra Control Center en un tercer dominio de fallo o ubicación secundaria.
- El clúster de Kubernetes host de la aplicación y un clúster de Kubernetes de destino deben estar disponibles y conectados a dos clústeres de ONTAP, lo cual es ideal para diferentes dominios de fallo o sitios.

- Los clústeres de ONTAP y la SVM de host se deben emparejar. Consulte ["Información general sobre relaciones entre iguales de clústeres y SVM"](#).
- La SVM remota emparejada debe estar disponible para Trident en el clúster de destino.
- La versión 22.07 de Trident o superior debe existir en los clústeres ONTAP de origen y destino.
- Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben habilitarse en los clústeres de ONTAP de origen y de destino. Consulte ["Información general sobre las licencias de SnapMirror en ONTAP"](#).
- Al añadir un back-end de almacenamiento de ONTAP a Astra Control Center, aplique las credenciales de usuario con la función "admin", que cuenta con métodos de acceso `http y. ontapi` Habilitado en ambos clústeres de ONTAP. Consulte ["Gestionar cuentas de usuario"](#) si quiere más información.
- Astra Control debe gestionar los clústeres de Kubernetes de origen y destino, y los clústeres de ONTAP.



Puede replicar simultáneamente una aplicación diferente (que se ejecute en el otro clúster o sitio) en la dirección opuesta. Por ejemplo, las aplicaciones A, B, C se pueden replicar del centro de datos 1 al centro de datos 2 y las aplicaciones X, y, Z se pueden replicar del centro de datos 2 al centro de datos 1.

Aprenda cómo ["Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror"](#).

## Métodos de instalación de aplicaciones compatibles

Astra Control es compatible con los siguientes métodos de instalación de aplicaciones:

- **Fichero manifiesto:** Astra Control admite aplicaciones instaladas desde un archivo manifiesto mediante `kubectl`. Por ejemplo:

```
kubectl apply -f myapp.yaml
```

- **Helm 3:** Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. Es totalmente compatible con la gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3). No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador:** Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres. A continuación, se enumeran algunas aplicaciones que se han validado para este modelo de instalación:
  - ["Apache K8ssandra"](#)
  - ["Jenkins CI"](#)
  - ["Clúster Percona XtraDB"](#)



Un operador y la aplicación que instale deben usar el mismo espacio de nombres; es posible que deba modificar el archivo `.yaml` de despliegue para que el operador se asegure de que así sea.

## Acceso a Internet

Debe determinar si tiene acceso externo a Internet. Si no lo hace, es posible que algunas funcionalidades sean limitadas, como recibir datos de supervisión y métricas de Cloud Insights de NetApp, o enviar paquetes de soporte al ["Sitio de soporte de NetApp"](#).

## Licencia

Astra Control Center requiere una licencia de Astra Control Center para obtener todas las funciones. Obtenga una licencia de evaluación o una licencia completa de NetApp. Necesita una licencia para proteger sus aplicaciones y datos. Consulte "[Características de Astra Control Center](#)" para obtener más detalles.

Puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Puede inscribirse para obtener una prueba gratuita registrándose "[aquí](#)".

Para obtener más información sobre las licencias necesarias para los back-ends de almacenamiento de ONTAP, consulte "[Compatibles con los back-ends de almacenamiento](#)".

Para obtener información detallada sobre cómo funcionan las licencias, consulte "[Licencia](#)".

## Entrada para clústeres de Kubernetes en las instalaciones

Puede elegir el tipo de entrada de red que utiliza Astra Control Center. De forma predeterminada, Astra Control Center implementa la puerta de enlace Astra Control Center (service/trafik) como un recurso para todo el clúster. Astra Control Center también admite el uso de un equilibrador de carga de servicio, si están permitidos en su entorno. Si prefiere utilizar un equilibrador de carga de servicio y no tiene uno configurado, puede utilizar el equilibrador de carga MetalLB para asignar automáticamente una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga.



Si va a alojar Astra Control Center en un clúster de cuadrícula de Tanzania Kubernetes, utilice `kubect1 get nsxlbmonitors -A` comando para ver si ya tiene un monitor de servicio configurado para aceptar tráfico de entrada. Si existe una, no debe instalar MetalLB, ya que el monitor de servicio existente anulará cualquier nueva configuración de equilibrador de carga.

Para obtener más información, consulte "[Configure la entrada para el equilibrio de carga](#)".

## Requisitos de red

El entorno operativo que aloja Astra Control Center se comunica mediante los siguientes puertos TCP. Debe asegurarse de que estos puertos estén permitidos a través de cualquier firewall y configurar firewalls para permitir que cualquier tráfico de salida HTTPS que se origine en la red Astra. Algunos puertos requieren conectividad de ambos modos entre el entorno que aloja Astra Control Center y cada clúster gestionado (se indica si procede).



Puede poner en marcha Astra Control Center en un clúster de Kubernetes de doble pila y Astra Control Center puede gestionar las aplicaciones y los back-ends de almacenamiento que se hayan configurado para un funcionamiento de doble pila. Para obtener más información sobre los requisitos de los clústeres de doble pila, consulte "[Documentación de Kubernetes](#)".



Origen	Destino	Puerto	Protocolo	Específico
PC cliente	Astra Control Center	443	HTTPS	Acceso de interfaz de usuario/API: Asegúrese de que este puerto está abierto de ambas formas entre el clúster que aloja a Astra Control Center y cada clúster gestionado
Consumidor de métricas	Nodo de trabajo de Astra Control Center	9090	HTTPS	Comunicación de datos de métricas: Asegúrese de que cada clúster gestionado pueda acceder a este puerto en el clúster que aloja a Astra Control Center (se requiere una comunicación bidireccional)
Astra Control Center	Servicio Cloud Insights alojado	443	HTTPS	Comunicación de Cloud Insights
Astra Control Center	Proveedor de bloques de almacenamiento Amazon S3	443	HTTPS	Comunicación del almacenamiento de Amazon S3
Astra Control Center	AutoSupport de NetApp	443	HTTPS	Comunicación AutoSupport de NetApp

## Exploradores web compatibles

Astra Control Center es compatible con las versiones recientes de Firefox, Safari y Chrome con una resolución mínima de 1280 x 720.

## El futuro

Vea la ["inicio rápido"](#) descripción general.

## Inicio rápido para Astra Control Center

Esta página ofrece una descripción general de alto nivel de los pasos necesarios para empezar con Astra Control Center. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

¡Pruébela! Si desea probar Astra Control Center, puede utilizar una licencia de evaluación de 90 días. Consulte ["información sobre licencias"](#) para obtener más detalles.

**1**

### Revise los requisitos del clúster de Kubernetes

- Astra funciona con clústeres de Kubernetes con un back-end de almacenamiento de ONTAP configurado para Trident o un back-end de almacenamiento de Astra Data Store.
- Los clústeres deben ejecutarse en buen estado, con al menos tres nodos de trabajo en línea.
- El clúster debe ejecutar Kubernetes.

Obtenga más información sobre la ["Requisitos del Centro de Control de Astra"](#).

**2**

### Descargue e instale Astra Control Center

- Descargue Astra Control Center desde ["Página de descargas del Centro de control de Astra del sitio de soporte de NetApp"](#).
- Instale Astra Control Center en su entorno local.

Opcionalmente, instale Astra Control Center utilizando Red Hat OperatorHub.

Opcionalmente, instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP.

Más información acerca de ["Instalación de Astra Control Center"](#).

**3**

### Complete algunas tareas de configuración inicial

- Añada una licencia de Astra Control y todas las licencias de ONTAP compatibles.
- Añada un clúster de Kubernetes y Astra Control Center descubre los detalles.
- Añada un back-end de almacenamiento de ONTAP.
- Opcionalmente, agregue un bucket de almacén de objetos que almacenará las copias de seguridad de la aplicación.

Obtenga más información sobre la ["proceso de configuración inicial"](#).

**4**

### Utilice Astra Control Center

Cuando termine de configurar Astra Control Center, a continuación puede hacer lo siguiente:

- Gestionar una aplicación. Obtenga más información sobre cómo ["gestionar aplicaciones"](#).
- Proteja las aplicaciones configurando políticas de protección para aplicaciones, replicando aplicaciones en sistemas remotos, y clonando y migrando aplicaciones. Obtenga más información sobre cómo ["proteja sus aplicaciones"](#).
- Gestionar cuentas (incluidos usuarios, roles, LDAP para autenticación de usuarios, credenciales, conexiones de repositorio, etc.). Obtenga más información sobre cómo ["gestionar usuarios"](#).
- De manera opcional, conéctese a Cloud Insights de NetApp para mostrar métricas sobre el estado del sistema, la capacidad y el rendimiento dentro de la IU del centro de control de Astra. Más información acerca de ["Conectando a Cloud Insights"](#).

["Instalar Astra Control Center"](#).

## Obtenga más información

- ["Utilice la API Astra Control"](#)

## Información general de la instalación

Elija y complete uno de los siguientes procedimientos de instalación de Astra Control Center:

- ["Instale Astra Control Center mediante el proceso estándar"](#)
- ["\(Si utiliza Red Hat OpenShift\) instale Astra Control Center mediante OpenShift OperatorHub"](#)
- ["Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP"](#)

### Instale Astra Control Center mediante el proceso estándar

Para instalar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y realice los siguientes pasos para instalar Astra Control Center Operator y Astra Control Center en su entorno. Puede utilizar este procedimiento para instalar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Para entornos Red Hat OpenShift, puede utilizar un ["procedimiento alternativo"](#) Para instalar Astra Control Center con OpenShift OperatorHub.

#### Lo que necesitará

- ["Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center"](#).
- Si ha configurado o desea configurar directivas de seguridad de POD en su entorno, familiarícese con las directivas de seguridad de POD y cómo afectan a la instalación de Astra Control Center. Consulte ["Comprender las restricciones de directivas de seguridad de POD"](#).
- Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

```
kubectl get clusteroperators
```

- Asegúrese de que todos los servicios de API se encuentren en buen estado y estén disponibles:

```
kubectl get apiservices
```

- Asegúrese de que el FQDN de Astra que tiene previsto utilizar se puede enrutar a este clúster. Esto significa que tiene una entrada DNS en el servidor DNS interno o que está utilizando una ruta URL principal que ya está registrada.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos ["requisitos previos"](#) Por lo tanto, Astra Control Center no instala su propio cert-Manager.

#### Acerca de esta tarea

El proceso de instalación de Astra Control Center realiza lo siguiente:

- Instala los componentes de Astra en `netapp-acc` (o nombre personalizado).
- Crea una cuenta predeterminada.
- Establece una dirección de correo electrónico de usuario administrativo predeterminada y una contraseña única predeterminada. A este usuario se le asigna el rol de propietario del sistema que se necesita para iniciar sesión por primera vez en la interfaz de usuario.
- Le ayuda a determinar que se están ejecutando todas las pods de Astra Control Center.
- Instala la interfaz de usuario de Astra.



(Se aplica sólo a la versión Astra Data Store Early Access Program (EAP)) Si tiene intención de gestionar Astra Data Store mediante Astra Control Center y habilitar los flujos de trabajo de VMware, implemente Astra Control Center únicamente en `pcloud` espacio de nombres y no en `netapp-acc` espacio de nombres o un espacio de nombres personalizado que se describe en los pasos de este procedimiento.



No ejecute el siguiente comando durante todo el proceso de instalación para evitar eliminar todas las POD de Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`



Si utiliza Podman de Red Hat en lugar de Docker Engine, los comandos de Podman se pueden utilizar en lugar de los comandos de Docker.

## Pasos

Para instalar Astra Control Center, lleve a cabo los siguientes pasos:

- [Descargue y desembale el paquete Astra Control Center](#)
- [Instale el complemento Astra kubectl de NetApp](#)
- [Agregue las imágenes al registro local](#)
- [Configurar espacio de nombres y secreto para registros con requisitos de autenticación](#)
- [Instale el operador de Astra Control Center](#)
- [Configurar Astra Control Center](#)
- [Complete la instalación del centro de control de Astra y del operador](#)
- [Comprobar el estado del sistema](#)
- [Configure la entrada para el equilibrio de carga](#)
- [Inicie sesión en la interfaz de usuario de Astra Control Center](#)

## Descargue y desembale el paquete Astra Control Center

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 de ["Sitio de soporte de NetApp"](#).
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

4. Extraiga las imágenes:

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

## Instale el complemento Astra kubectl de NetApp

La Astra de NetApp `kubectl` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

### Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux y Mac, puede utilizar `uname -a` comando para recopilar esta información.

### Pasos

1. Enumere la Astra de NetApp disponible `kubectl` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubectl-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubectl` utilidad. En este ejemplo, la `kubectl` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

## Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

## Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:

- Sustituya BUNDLE\_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, acc.manifest.yaml).
- Sustituya MY\_REGISTRATION por la URL del repositorio de Docker.
- Sustituya MY\_REGISTRATION\_USER por el nombre de usuario.
- Sustituya MY\_REGISTRATION\_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY  
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

## Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR\_REGISTRY> como se indica en los comentarios:

```

# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //'')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done

```

## Configurar espacio de nombres y secreto para registros con requisitos de autenticación

1. Exporte el KUBECONFIG para el clúster de host de Astra Control Center:

```
export KUBECONFIG=[file path]
```

2. Si utiliza un registro que requiere autenticación, debe hacer lo siguiente:

- a. Cree el netapp-acc-operator espacio de nombres:

```
kubectl create ns netapp-acc-operator
```

Respuesta:

```
namespace/netapp-acc-operator created
```

- b. Cree un secreto para `netapp-acc-operator` espacio de nombres. Añada información sobre Docker y ejecute el siguiente comando:



El marcador de posición `your_registry_path` debe coincidir con la ubicación de las imágenes que ha cargado anteriormente (por ejemplo, `[Registry_URL]/netapp/astra/astracc/22.08.1-26`).

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-operator --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

Respuesta de ejemplo:

```
secret/astra-registry-cred created
```



Si elimina el espacio de nombres después de que se genere el secreto, deberá volver a generar el secreto para el espacio de nombres después de volver a crear el espacio de nombres.

- c. Cree el `netapp-acc` (o espacio de nombres personalizado).

```
kubectl create ns [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
namespace/netapp-acc created
```

- d. Cree un secreto para `netapp-acc` (o espacio de nombres personalizado). Añada información sobre Docker y ejecute el siguiente comando:

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

Respuesta

```
secret/astra-registry-cred created
```



- a. `[[substep_kubeconfig_secret]]`(opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación, asegúrese de proporcionar el kubeconfig como secreto dentro del espacio de nombres Astra Control Center que tiene intención de implementar utilizando este comando:

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom namespace]
```

## Instale el operador de Astra Control Center

1. Cambie el directorio:

```
cd manifests
```

2. Edite la implementación del operador de Astra Control Center YAML (`astra_control_center_operator_deploy.yaml`) para referirse a su registro local y secreto.

```
vim astra_control_center_operator_deploy.yaml
```



Una muestra anotada de AYLMA sigue estos pasos.

- a. Si utiliza un registro que requiere autenticación, reemplace la línea predeterminada de `imagePullSecrets: []` con lo siguiente:

```
imagePullSecrets:  
- name: <astra-registry-cred>
```

- b. Cambiar `[your_registry_path]` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un [paso anterior](#).
- c. Cambiar `[your_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un [paso anterior](#).
- d. (Para instalaciones que utilizan la vista previa de Astra Data Store) Consulte este problema conocido con respecto a "[Los aprovisionadores de clases de almacenamiento y los cambios adicionales que deberá realizar en la YAML](#)".

```

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
    name: acc-operator-controller-manager
    namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
            image: [your_registry_path]/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          command:
            - /manager
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
      imagePullSecrets: []

```

### 3. Instale el operador de Astra Control Center:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Respuesta de ejemplo:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

4. Verifique que los pods se estén ejecutando:

```
kubectl get pods -n netapp-acc-operator
```

## Configurar Astra Control Center

1. Edite el archivo de recursos personalizados (CR) del Centro de control de Astra (astra\_control\_center\_min.yaml) Para realizar las configuraciones de cuenta, AutoSupport, Registro y otras necesarias:



astra\_control\_center\_min.yaml Es la CR predeterminada y es adecuada para la mayoría de las instalaciones. Familiarícese con todos "[Opciones CR y sus valores potenciales](#)" Garantizar la puesta en marcha correcta de Astra Control Center en su entorno. Si se requieren personalizaciones adicionales para su entorno, puede utilizar astra\_control\_center.yaml Como CR alternativo.

```
vim astra_control_center_min.yaml
```



Si está utilizando un registro que no requiere autorización, debe eliminar secret línea dentro imageRegistry o se producirá un error en la instalación.

a. Cambiar [your\_registry\_path] a la ruta de acceso del registro en la que ha insertado las imágenes en el paso anterior.

- b. Cambie el `accountName` cadena al nombre que desea asociar a la cuenta.
- c. Cambie el `astraAddress` Cadena al FQDN que desea utilizar en su navegador para acceder a Astra. No utilizar `http://` o `https://` en la dirección. Copie este FQDN para utilizarlo en un [paso posterior](#).
- d. Cambie el `email` cadena en la dirección inicial predeterminada del administrador. Copie esta dirección de correo electrónico para su uso en un [paso posterior](#).
- e. Cambiar `enrolled` Para AutoSupport a. `false` para sitios sin conexión a internet o retención `true` para sitios conectados.
- f. Si utiliza un administrador de certificados externo, añada las siguientes líneas a. `spec`:

```
spec:
  crds:
    externalCertManager: true
```

- g. (Opcional) Añada un nombre `firstName` y apellidos `lastName` del usuario asociado con la cuenta. Este paso se puede realizar ahora o una versión posterior dentro de la interfaz de usuario.
- h. (Opcional) cambie el `storageClass` Valor en otro recurso de la clase de almacenamiento de Trident, si es necesario para su instalación.
- i. (Opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación y ya lo tiene [se ha creado el secreto que contiene el kubeconfig para este cluster](#), Proporcione el nombre del secreto agregando un nuevo campo a este archivo YLMA llamado `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`
- j. Realice uno de los siguientes pasos:

- **Otro controlador de entrada (`ingressType:Generic`):** Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

La instalación predeterminada de Astra Control Center configura su puerta de enlace (`service/traefik`) ser del tipo `ClusterIP`. Esta instalación predeterminada requiere que configure además un dispositivo de entrada/controlador de Kubernetes para enrutar el tráfico hacia él. Si desea utilizar una entrada, consulte ["Configure la entrada para el equilibrio de carga"](#).

- **Equilibrador de carga de servicio (`ingressType:AccTraefik`):** Si no desea instalar un controlador IngressController o crear un recurso de entrada, establezca `ingressType` para `AccTraefik`.

Esto despliega el Astra Control Center `traefik` Puerta de enlace como servicio de tipo Kubernetes LoadBalancer.

Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga.



Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte ["Requisitos"](#).

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
```

## Complete la instalación del centro de control de Astra y del operador

1. Si todavía no lo ha hecho en un paso anterior, cree el `netapp-acc` espacio de nombres (o personalizado):

```
kubectl create ns [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
namespace/netapp-acc created
```

2. Instale Astra Control Center en `netapp-acc` (o su espacio de nombres personalizado):

```
kubectl apply -f astra_control_center_min.yaml -n [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
astracontrolcenter.astra.netapp.io/astra created
```

## Comprobar el estado del sistema



Si prefiere utilizar OpenShift, puede utilizar comandos de OC comparables para realizar los pasos de verificación.

1. Compruebe que todos los componentes del sistema se han instalado correctamente.

```
kubectl get pods -n [netapp-acc or custom namespace]
```

Cada pod debe tener el estado de `Running`. Pueden tardar varios minutos en implementar los pods del sistema.

## Ejemplo de respuesta

NAME	READY	STATUS	RESTARTS
AGE			
acc-helm-repo-6b44d68d94-d8m55 13m	1/1	Running	0
activity-78f99ddf8-hltct 10m	1/1	Running	0
api-token-authentication-457nl 9m28s	1/1	Running	0
api-token-authentication-dgwsz 9m28s	1/1	Running	0
api-token-authentication-hmqqc 9m28s	1/1	Running	0
asup-75fd554dc6-m6qzh 9m38s	1/1	Running	0
authentication-6779b4c85d-92gds 8m11s	1/1	Running	0
bucket-service-7cc767f8f8-lqwr8 9m31s	1/1	Running	0
certificates-549fd5d6cb-5kmd6 9m56s	1/1	Running	0
certificates-549fd5d6cb-bkjh9 9m56s	1/1	Running	0
cloud-extension-7bcb7948b-hn8h2 10m	1/1	Running	0
cloud-insights-service-56ccf86647-fgg69 9m46s	1/1	Running	0
composite-compute-677685b9bb-7vgsf 10m	1/1	Running	0
composite-volume-657d6c5585-dnq79 9m49s	1/1	Running	0
credentials-755fd867c8-vrlmt 11m	1/1	Running	0
entitlement-86495cdf5b-nwhh2 10m	1/1	Running	2
features-5684fb8b56-8d6s8 10m	1/1	Running	0
fluent-bit-ds-rhx7v 7m48s	1/1	Running	0
fluent-bit-ds-rjms4 7m48s	1/1	Running	0
fluent-bit-ds-zf5ph 7m48s	1/1	Running	0
graphql-server-66d895f544-w6hjd 3m29s	1/1	Running	0

identity-744df448d5-rlcmm	1/1	Running	0
10m			
influxdb2-0	1/1	Running	0
13m			
keycloak-operator-75c965cc54-z7csw	1/1	Running	0
8m16s			
krakend-798d6df96f-9z2sk	1/1	Running	0
3m26s			
license-5fb7d75765-f8mjg	1/1	Running	0
9m50s			
login-ui-7d5b7df85d-l2s7s	1/1	Running	0
3m20s			
loki-0	1/1	Running	0
13m			
metrics-facade-599b9d7fcc-gtmgl	1/1	Running	0
9m40s			
monitoring-operator-67cc74f844-cdplp	2/2	Running	0
8m11s			
nats-0	1/1	Running	0
13m			
nats-1	1/1	Running	0
13m			
nats-2	1/1	Running	0
12m			
nautilus-769f5b74cd-k5jxm	1/1	Running	0
9m42s			
nautilus-769f5b74cd-kd9gd	1/1	Running	0
8m59s			
openapi-84f6ccd8ff-76kvp	1/1	Running	0
9m34s			
packages-6f59fc67dc-4g2f5	1/1	Running	0
9m52s			
polaris-consul-consul-server-0	1/1	Running	0
13m			
polaris-consul-consul-server-1	1/1	Running	0
13m			
polaris-consul-consul-server-2	1/1	Running	0
13m			
polaris-keycloak-0	1/1	Running	0
8m7s			
polaris-keycloak-1	1/1	Running	0
5m49s			
polaris-keycloak-2	1/1	Running	0
5m15s			
polaris-keycloak-db-0	1/1	Running	0
8m6s			



polaris-keycloak-db-1	1/1	Running	0
5m49s			
polaris-keycloak-db-2	1/1	Running	0
4m57s			
polaris-mongodb-0	2/2	Running	0
13m			
polaris-mongodb-1	2/2	Running	0
12m			
polaris-mongodb-2	2/2	Running	0
12m			
polaris-ui-565f56bf7b-zwr8b	1/1	Running	0
3m19s			
polaris-vault-0	1/1	Running	0
13m			
polaris-vault-1	1/1	Running	0
13m			
polaris-vault-2	1/1	Running	0
13m			
public-metrics-6d86d66444-2wbz1	1/1	Running	0
9m30s			
storage-backend-metrics-77c5d98dcd-dbhg5	1/1	Running	0
9m44s			
storage-provider-78c885f57c-6zcv4	1/1	Running	0
9m36s			
telegraf-ds-212m9	1/1	Running	0
7m48s			
telegraf-ds-qfzgh	1/1	Running	0
7m48s			
telegraf-ds-shrms	1/1	Running	0
7m48s			
telegraf-rs-bjpkt	1/1	Running	0
7m48s			
telemetry-service-6684696c64-qzfdf	1/1	Running	0
10m			
tenancy-6596b6c54d-vmppm	1/1	Running	0
10m			
traefik-7489dc59f9-6mnst	1/1	Running	0
3m19s			
traefik-7489dc59f9-xrkkg	1/1	Running	0
3m4s			
trident-svc-6c8dc458f5-jswcl	1/1	Running	0
10m			
vault-controller-6b954f9b76-gz9nm	1/1	Running	0
11m			

2. (Opcional) para asegurarse de que la instalación ha finalizado, puede ver el `acc-operator` registra utilizando el siguiente comando.

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```



`accHost` el registro del clúster es una de las últimas operaciones y, si no se produce un error en la implementación, no provocará un error. En el caso de un error de registro del clúster que se indica en los registros, puede volver a intentar el registro a través del flujo de trabajo de `add cluster` "[En la interfaz de usuario de](#)" O API.

3. Cuando todos los pods estén en ejecución, verifique que la instalación se haya realizado correctamente (`READY` es `True`) Y obtenga la contraseña única que utilizará cuando inicie sesión en Astra Control Center:

```
kubectl get AstraControlCenter -n netapp-acc
```

Respuesta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.08.1-26	10.111.111.111
	True		



Copie el valor de UUID. La contraseña es `ACC-` Seguido del valor UUID (`ACC-[UUID]` o, en este ejemplo, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

## Configure la entrada para el equilibrio de carga

Puede configurar una controladora de entrada de Kubernetes que gestione el acceso externo a los servicios, como el equilibrio de carga en un clúster.

Este procedimiento explica cómo configurar un controlador de entrada (`ingressType: Generic`). Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.



Si no desea configurar un controlador de entrada, puede configurarlo `ingressType: AccTraefik`). Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga. Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte "[Requisitos](#)".

Los pasos varían en función del tipo de controlador de entrada que utilice:

- Entrada Istio
- Controlador de entrada nginx
- Controlador OpenShift Ingress

### Lo que necesitará

- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.
- Se utilizan versiones de Kubernetes entre e incluidas v1.19 y v1.22.

### Pasos para la entrada de Istio

1. Configurar la entrada de Istio.



En este procedimiento se asume que Istio se implementa utilizando el perfil de configuración "predeterminado".

2. Recopile o cree el certificado y el archivo de claves privadas deseados para la puerta de enlace de entrada.

Es posible usar un certificado firmado por CA o autofirmado. El nombre común debe ser la dirección Astra (FQDN).

Comando de ejemplo:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048  
-keyout tls.key -out tls.crt
```

3. Cree un secreto `tls secret name` de tipo `kubernetes.io/tls` Para una clave privada TLS y un certificado en `istio-system namespace` Tal como se describe en los secretos TLS.

Comando de ejemplo:

```
kubectl create secret tls [tls secret name]  
--key="tls.key"  
--cert="tls.crt" -n istio-system
```



El nombre del secreto debe coincidir con el `spec.tls.secretName` proporcionado en `istio-ingress.yaml` archivo.

4. Implemente un recurso de entrada en `netapp-acc` Espacio de nombres (o con nombre personalizado) mediante el uso del tipo de recurso `v1beta1` (obsoleto en la versión de Kubernetes menor que o 1.22) o `v1` para un esquema obsoleto o nuevo:

Salida:

```
apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
    - hosts:
      - <ACC address>
      secretName: [tls secret name]
  rules:
    - host: [ACC address]
      http:
        paths:
          - path: /
            pathType: Prefix
            backend:
              serviceName: traefik
              servicePort: 80
```

Para el nuevo esquema v1, siga este ejemplo:

```
kubectl apply -f istio-Ingress.yaml
```

Salida:

```

apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80

```

5. Implementar Astra Control Center como es habitual.
6. Compruebe el estado de la entrada:

```
kubectl get ingress -n netapp-acc
```

Respuesta:

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
ingress	istio	astra.example.com	172.16.103.248	80, 443	1h

### Pasos para el controlador de entrada Nginx

1. Cree un secreto de tipo[kubernetes.io/tls] Para una clave privada TLS y un certificado en netapp-acc (o nombre personalizado) como se describe en ["Secretos TLS"](#).

2. Implemente un recurso de entrada en `netapp-acc` (o nombre personalizado) mediante el `v1beta1` (Obsoleto en la versión de Kubernetes inferior a o 1.22) o `v1` tipo de recurso para un esquema obsoleto o nuevo:

a. Para un `v1beta1` esquema obsoleto, siga este ejemplo:

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
          serviceName: traefik
          servicePort: 80
          pathType: ImplementationSpecific
```

b. Para la `v1` nuevo esquema, siga este ejemplo:

```

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
      - path:
        backend:
          service:
            name: traefik
            port:
              number: 80
        pathType: ImplementationSpecific

```

### Pasos para el controlador de entrada de OpenShift

1. Obtenga su certificado y consiga los archivos de clave, certificado y CA listos para su uso por la ruta OpenShift.
2. Cree la ruta OpenShift:

```

oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem

```

### Inicie sesión en la interfaz de usuario de Astra Control Center

Después de instalar Astra Control Center, cambiará la contraseña del administrador predeterminado e inicie sesión en el panel de interfaz de usuario de Astra Control Center.

#### Pasos

1. En un explorador, introduzca el FQDN que utilizó en `astraAddress` en la `astra_control_center_min.yaml` CR cuando [Ha instalado Astra Control Center](#).
2. Acepte los certificados autofirmados cuando se le solicite.



Se puede crear un certificado personalizado después de iniciar sesión.

3. En la página de inicio de sesión de Astra Control Center, introduzca el valor utilizado `email` en `astra_control_center_min.yaml` CR cuando [Ha instalado Astra Control Center](#), seguido de la contraseña única (`ACC-[UUID]`).



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

4. Seleccione **Iniciar sesión**.
5. Cambie la contraseña cuando se le solicite.



Si este es su primer inicio de sesión y olvida la contraseña y aún no se han creado otras cuentas de usuario administrativas, comuníquese con el servicio de soporte de NetApp para obtener ayuda para la recuperación de contraseñas.

6. (Opcional) quite el certificado TLS autofirmado existente y sustitúyalo por un ["Certificado TLS personalizado firmado por una entidad de certificación \(CA\)"](#).

## Solucione los problemas de instalación

Si alguno de los servicios está en `Error` puede inspeccionar los registros. Busque códigos de respuesta API en la gama 400 a 500. Esos indican el lugar donde ocurrió un fracaso.

### Pasos

1. Para inspeccionar los registros del operador de Astra Control Center, introduzca lo siguiente:

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n netapp-acc-operator -o name) -c manager
```

## El futuro

Complete la implementación llevando a cabo ["tareas de configuración"](#).

=  
:allow-uri-read:

## Comprender las restricciones de directivas de seguridad de POD

Astra Control Center admite la limitación de privilegios mediante directivas de seguridad de POD (PSP). Las políticas de seguridad de POD permiten limitar los usuarios o grupos que pueden ejecutar contenedores y los privilegios que dichos contenedores pueden tener.

Algunas distribuciones de Kubernetes, como RKE2, tienen una política de seguridad de POD predeterminada que es demasiado restrictiva y provoca problemas al instalar Astra Control Center.

Puede utilizar la información y los ejemplos que se incluyen aquí para comprender las directivas de seguridad de POD que Astra Control Center crea y configurar las directivas de seguridad de POD que proporcionan la protección necesaria sin interferir con las funciones de Astra Control Center.



## PSP instalado por Astra Control Center

Astra Control Center crea varias directivas de seguridad de POD durante la instalación. Algunas de ellas son permanentes y algunas se crean durante ciertas operaciones y se eliminan una vez que se completa la operación.

### Se crean PSP durante la instalación

Durante la instalación de Astra Control Center, el operador Astra Control Center instala una directiva de seguridad de POD personalizada, un objeto Role y un objeto RoleBinding para admitir la implementación de los servicios Astra Control Center en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME	PRIV	CAPS	SELINUX	RUNASUSER
FSGROUP SUPGROUP READONLYROOTFS		VOLUMES		
avp-ppsp	false		RunAsAny	RunAsAny
RunAsAny RunAsAny	false	*		
netapp-astra-deployment-ppsp	false		RunAsAny	RunAsAny
RunAsAny RunAsAny	false	*		

```
kubectl get role
```

NAME	CREATED AT
netapp-astra-deployment-role	2022-06-27T19:34:58Z

```
kubectl get rolebinding
```

NAME	ROLE
AGE	
netapp-astra-deployment-rb	Role/netapp-astra-deployment-role
32m	

### Se crean PSP durante las operaciones de backup

Durante las operaciones de copia de seguridad, Astra Control Center crea una política de seguridad de POD dinámica, un objeto ClusterRole y un objeto RoleBinding. Estos permiten utilizar el proceso de backup, que se produce en un espacio de nombres aparte.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME	SELINUX	RUNASUSER	PRIV	FSGROUP	CAPS	SUPGROUP	READONLYROOTFS	VOLUMES
netapp-astra-backup			false		DAC_READ_SEARCH			
RunAsAny	RunAsAny	RunAsAny	RunAsAny	RunAsAny	false		*	

```
kubectl get role
```

NAME	CREATED AT
netapp-astra-backup	2022-07-21T00:00:00Z

```
kubectl get rolebinding
```

NAME	ROLE	AGE
netapp-astra-backup	Role/netapp-astra-backup	62s

## Se crean PSP durante la gestión del clúster

Cuando gestiona un clúster, Astra Control Center instala el operador de supervisión de netapp en el clúster gestionado. Este operador crea una directiva de seguridad de POD, un objeto ClusterRole y un objeto RoleBinding para implementar servicios de telemetría en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME	SELINUX	RUNASUSER	PRIV	FSGROUP	CAPS	SUPGROUP	READONLYROOTFS	VOLUMES
netapp-monitoring-bsp-nkmo			true		AUDIT_WRITE,NET_ADMIN,NET_RAW			
RunAsAny	RunAsAny	RunAsAny	RunAsAny	RunAsAny	false		*	

```
kubectl get role
```

NAME	CREATED AT
netapp-monitoring-role-privileged	2022-07-21T00:00:00Z

```
kubectl get rolebinding
```

NAME	ROLE	AGE
netapp-monitoring-role-binding-privileged	Role/netapp-monitoring-role-privileged	2m5s

## Active la comunicación de red entre espacios de nombres

Algunos entornos utilizan construcciones de NetworkPolicy para restringir el tráfico entre espacios de nombres. El operador Astra Control Center, Astra Control Center y el complemento Astra para VMware vSphere están todos en espacios de nombres diferentes. Los servicios de estos distintos espacios de nombres deben poder comunicarse entre sí. Para activar esta comunicación, siga estos pasos.

### Pasos

1. Elimine los recursos de NetworkPolicy que existan en el espacio de nombres de Astra Control Center:

```
kubectl get networkpolicy -n netapp-acc
```

2. Para cada objeto NetworkPolicy devuelto por el comando anterior, utilice el siguiente comando para eliminarlo. Sustituya <OBJECT\_NAME> por el nombre del objeto devuelto:

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Aplique el siguiente archivo de recursos para configurar el objeto de política de red ACC-avp con el fin de permitir que los servicios de Astra Plugin para VMware vSphere puedan realizar solicitudes a los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. Aplique el siguiente archivo de recursos para configurar el objeto de directiva de red-operador de ACC con el fin de permitir que el operador de Astra Control Center se comunice con los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```

apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME

```

### Quite las limitaciones de recursos

Algunos entornos utilizan los objetos ResourceQuotas y LimitRanges para evitar que los recursos de un espacio de nombres consuman toda la CPU y memoria disponibles en el clúster. Astra Control Center no establece límites máximos, por lo que no se ajusta a esos recursos. Debe eliminarlos de los espacios de nombres en los que planea instalar Astra Control Center.

Puede utilizar los siguientes pasos para recuperar y eliminar estas cuotas y límites. En estos ejemplos, el resultado del comando se muestra inmediatamente después del comando.

### Pasos

1. Obtenga las cuotas de recursos en el espacio de nombres ACC-netapp:

```
kubectl get quota -n netapp-acc
```

Respuesta:

```

NAME          AGE   REQUEST                                     LIMIT
pods-high     16s   requests.cpu: 0/20, requests.memory: 0/100Gi
limits.cpu: 0/200, limits.memory: 0/1000Gi
pods-low      15s   requests.cpu: 0/1, requests.memory: 0/1Gi
limits.cpu: 0/2, limits.memory: 0/2Gi
pods-medium   16s   requests.cpu: 0/10, requests.memory: 0/20Gi
limits.cpu: 0/20, limits.memory: 0/200Gi

```

2. Elimine todas las cuotas de recursos por nombre:

```
kubectl delete resourcequota pods-high -n netapp-acc
```

```
kubectl delete resourcequota pods-low -n netapp-acc
```

```
kubectl delete resourcequota pods-medium -n netapp-acc
```

3. Obtenga los rangos de límites en el espacio de nombres ACC-netapp:

```
kubectl get limits -n netapp-acc
```

Respuesta:

NAME	CREATED AT
cpu-limit-range	2022-06-27T19:01:23Z

4. Eliminar los rangos de límites por nombre:

```
kubectl delete limitrange cpu-limit-range -n netapp-acc
```

=

:allow-uri-read:

## Instale Astra Control Center utilizando OpenShift OperatorHub

Si utiliza Red Hat OpenShift, puede instalar Astra Control Center mediante el operador certificado de Red Hat. Utilice este procedimiento para instalar Astra Control Center desde "[Catálogo de Red Hat Ecosystem](#)" o con Red Hat OpenShift Container Platform.

Después de completar este procedimiento, debe volver al procedimiento de instalación para completar el "[pasos restantes](#)" para verificar que la instalación se ha realizado correctamente e iniciar sesión.

### Lo que necesitará

- "[Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center](#)".
- En el clúster OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado (available es true):

```
oc get clusteroperators
```

- Desde su clúster OpenShift, asegúrese de que todos los servicios API se encuentran en buen estado (available es true):

```
oc get apiservices
```

- Cree una dirección FQDN para Astra Control Center en su centro de datos.
- Obtenga los permisos necesarios y acceda a Red Hat OpenShift Container Platform para realizar los pasos de instalación descritos.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos ["requisitos previos"](#) Por lo tanto, Astra Control Center no instala su propio cert-Manager.

## Pasos

- [Descargue y desembale el paquete Astra Control Center](#)
- [Instale el complemento Astra kubect1 de NetApp](#)
- [Agregue las imágenes al registro local](#)
- [Busque la página de instalación del operador](#)
- [Instale el operador](#)
- [Instalar Astra Control Center](#)

## Descargue y desembale el paquete Astra Control Center

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 de ["Sitio de soporte de NetApp"](#).
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

4. Extraiga las imágenes:

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

## Instale el complemento Astra kubect1 de NetApp

La Astra de NetApp `kubect1` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

### Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux y Mac, puede utilizar `uname -a` comando para recopilar esta información.

## Pasos

1. Enumere la Astra de NetApp disponible `kubect1` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubect1-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubect1` utilidad. En este ejemplo, la `kubect1` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

```
cp kubect1-astra/<binary-name> /usr/local/bin/kubect1-astra
```

### Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

## Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:

- Sustituya BUNDLE\_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, acc.manifest.yaml).
- Sustituya MY\_REGISTRATION por la URL del repositorio de Docker.
- Sustituya MY\_REGISTRATION\_USER por el nombre de usuario.
- Sustituya MY\_REGISTRATION\_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY  
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

## Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR\_REGISTRY> como se indica en los comentarios:



```

# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //'')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')

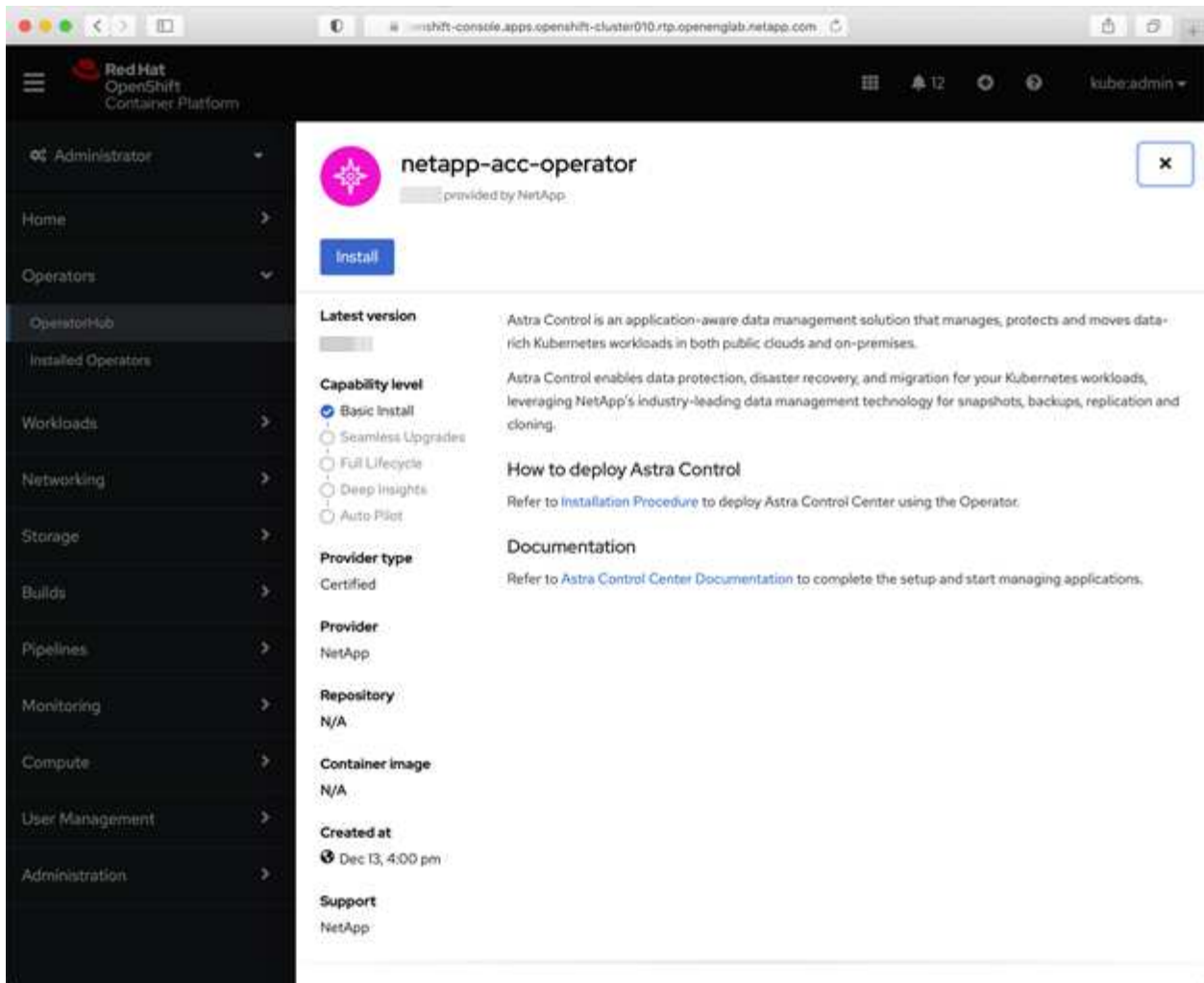
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done

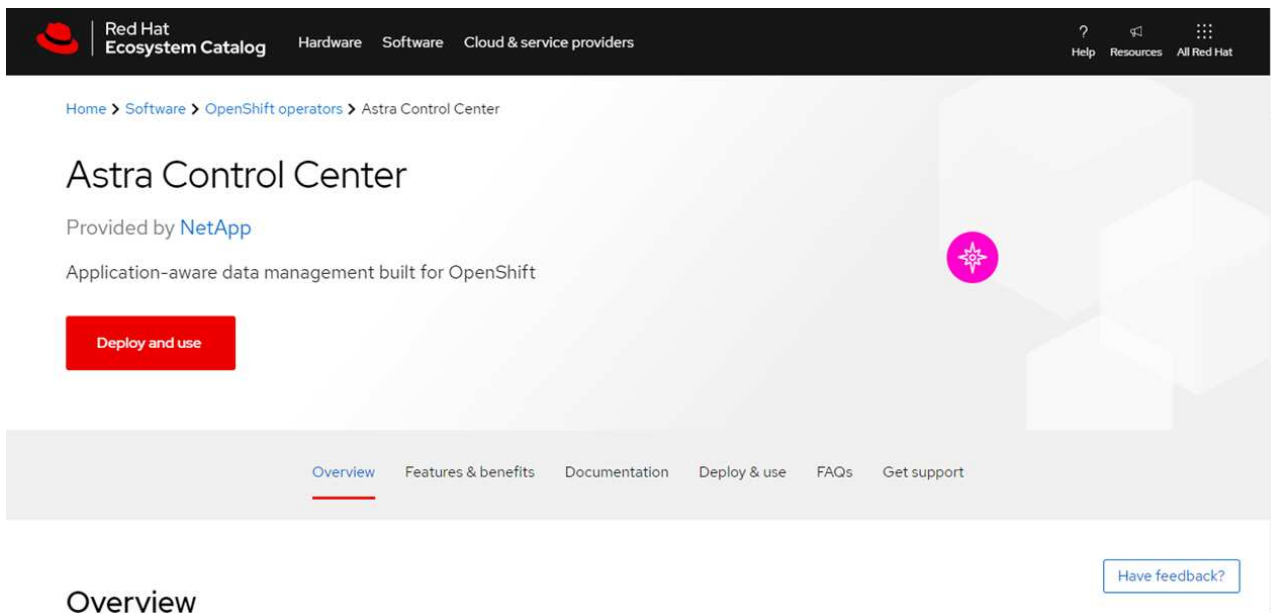
```

## Busque la página de instalación del operador

1. Realice uno de los siguientes procedimientos para acceder a la página de instalación del operador:
  - Desde la consola web de Red Hat OpenShift:




- i. Inicie sesión en la IU de OpenShift Container Platform.
  - ii. En el menú lateral, seleccione **operadores > OperatorHub**.
  - iii. Seleccione el operador NetApp Astra Control Center.
  - iv. Seleccione **instalar**.
- En el catálogo de ecosistemas de Red Hat:




- Overview**
- i. Seleccione Astra Control Center de NetApp "operador".
  - ii. Seleccione **desplegar y utilizar**.

## Instale el operador


1. Complete la página **Install Operator** e instale el operador:

 El operador estará disponible en todos los espacios de nombres del clúster.

- a. Seleccione el espacio de nombres del operador o `netapp-acc-operator` el espacio de nombres se creará automáticamente como parte de la instalación del operador.
- b. Seleccione una estrategia de aprobación manual o automática.

 Se recomienda la aprobación manual. Solo debe tener una instancia de operador en ejecución por clúster.

- c. Seleccione **instalar**.

 Si ha seleccionado una estrategia de aprobación manual, se le pedirá que apruebe el plan de instalación manual para este operador.

2. Desde la consola, vaya al menú OperatorHub y confirme que el operador se ha instalado correctamente.

## Instalar Astra Control Center

1. En la consola de la vista de detalles del operador del Centro de control de Astra, seleccione `Create instance` En la sección proporcionada API.
2. Complete el `Create AstraControlCenter` campo de formulario:
  - a. Mantenga o ajuste el nombre del Centro de control de Astra.
  - b. (Opcional) Habilitar o deshabilitar AutoSupport. Se recomienda conservar la funcionalidad de AutoSupport.

- c. Introduzca la dirección de Astra Control Center. No entre `http://` o `https://` en la dirección.
  - d. Introduzca la versión de Astra Control Center; por ejemplo, 21.12.60.
  - e. Introduzca un nombre de cuenta, una dirección de correo electrónico y un apellido de administrador.
  - f. Conserve la política de reclamaciones de volumen predeterminada.
  - g. En **Registro de imágenes**, introduzca la ruta de registro de la imagen del contenedor local. No entre `http://` o `https://` en la dirección.
  - h. Si utiliza un registro que requiere autenticación, introduzca el secreto.
    - i. Introduzca el nombre del administrador.
    - j. Configure el escalado de recursos.
  - k. Conserve la clase de almacenamiento predeterminada.
    - l. Defina las preferencias de manejo de CRD.
3. Seleccione `Create`.

## El futuro

Compruebe que la instalación de Astra Control Center se ha realizado correctamente y complete el "[pasos restantes](#)" para iniciar sesión. Además, completará la implementación siguiendo este proceso "[tareas de configuración](#)".

## Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP

Con Astra Control Center, puede gestionar sus aplicaciones en un entorno de cloud híbrido con clústeres de Kubernetes e instancias de Cloud Volumes ONTAP autogestionados. Puede poner en marcha Astra Control Center en sus clústeres de Kubernetes en las instalaciones o en uno de los clústeres de Kubernetes autogestionados en el entorno de cloud.

Con una de estas puestas en marcha, puede realizar operaciones de gestión de datos de aplicaciones utilizando Cloud Volumes ONTAP como back-end de almacenamiento. También es posible configurar un bloque de S3 como destino de backup.

Para instalar Astra Control Center en Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure con una back-end de almacenamiento de Cloud Volumes ONTAP, realice los siguientes pasos en función de su entorno de cloud.

- [Ponga en marcha Astra Control Center en Amazon Web Services](#)
- [Ponga en marcha Astra Control Center en Google Cloud Platform](#)
- [Ponga en marcha Astra Control Center en Microsoft Azure](#)

Puede gestionar sus aplicaciones en distribuciones con clústeres de Kubernetes autogestionados, como OpenShift Container Platform (OCP). Sólo se validan los clústeres OCP autogestionados para la implantación de Astra Control Center.

### Ponga en marcha Astra Control Center en Amazon Web Services

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Amazon Web Services (AWS).

## Lo que necesitará para AWS

Antes de poner en marcha Astra Control Center en AWS, necesitará los siguientes elementos:

- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de AWS, Access ID y Secret Key con permisos que permiten crear cubos y conectores
- Acceso e inicio de sesión del Elastic Container Registry (ECR) de la cuenta de AWS
- Se requieren entradas de zona alojada de AWS y ruta 53 para acceder a la interfaz de usuario de Astra Control

## Requisitos de los entornos operativos para AWS

Astra Control Center requiere los siguientes entornos operativos para AWS:


- OpenShift Container Platform de Red Hat 4.8



Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
<b>Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp</b>	300 GB como mínimo disponible
<b>Nodos de trabajo (requisitos de AWS EC2)</b>	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
<b>Equilibrador de carga</b>	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
<b>FQDN</b>	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
<b>Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)</b>	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento

Componente	Requisito
<b>Registro de imágenes</b>	<p>Debe tener un registro privado existente, como AWS Elastic Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>El clúster alojado de Astra Control Center y el clúster gestionado deben tener acceso al mismo registro de imágenes para poder realizar copias de seguridad y restaurar aplicaciones mediante la imagen basada en Restic.</p> </div>
<b>Configuración de Astra Trident/ONTAP</b>	<p>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 las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-nas</code> <code>csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-san</code> <code>csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-nas</code> <code>csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-san</code> <code>csi.trident.netapp.io</code></li> </ul>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.



El token del registro de AWS caduca en 12 horas, después del cual deberá renovar el secreto del registro de imagen Docker.

### Información general sobre la implementación para AWS

He aquí una descripción general del proceso de instalación de Astra Control Center para AWS con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Compruebe que dispone de suficientes permisos IAM.](#)
2. [Instale un clúster RedHat OpenShift en AWS.](#)
3. [Configure AWS.](#)
4. [Configure Cloud Manager de NetApp.](#)
5. [Instalar Astra Control Center.](#)

## Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "[Credenciales iniciales de AWS](#)".

## Instale un clúster RedHat OpenShift en AWS

Instale un clúster RedHat OpenShift Container Platform en AWS.

Para obtener instrucciones de instalación, consulte "[Instalación de un clúster en AWS en OpenShift Container Platform](#)".

## Configure AWS

A continuación, configure AWS para crear una red virtual, configurar instancias de computación EC2, crear un bloque de AWS S3, crear un Elastic Container Register (ECR) para alojar las imágenes de Astra Control Center y empujar las imágenes a este registro.

Siga la documentación de AWS para completar los pasos siguientes. Consulte "[Documentación de instalación de AWS](#)".

1. Cree una red virtual AWS.
2. Revise las instancias de computación EC2. Puede ser un servidor con configuración básica o máquinas virtuales en AWS.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en AWS para cumplir los requisitos de Astra. Consulte "[Requisitos del Centro de Control de Astra](#)".
4. Cree al menos un bloque de AWS S3 para almacenar los backups.
5. Cree un AWS Elastic Container Registry (ECR) para alojar todas las imágenes ACC.



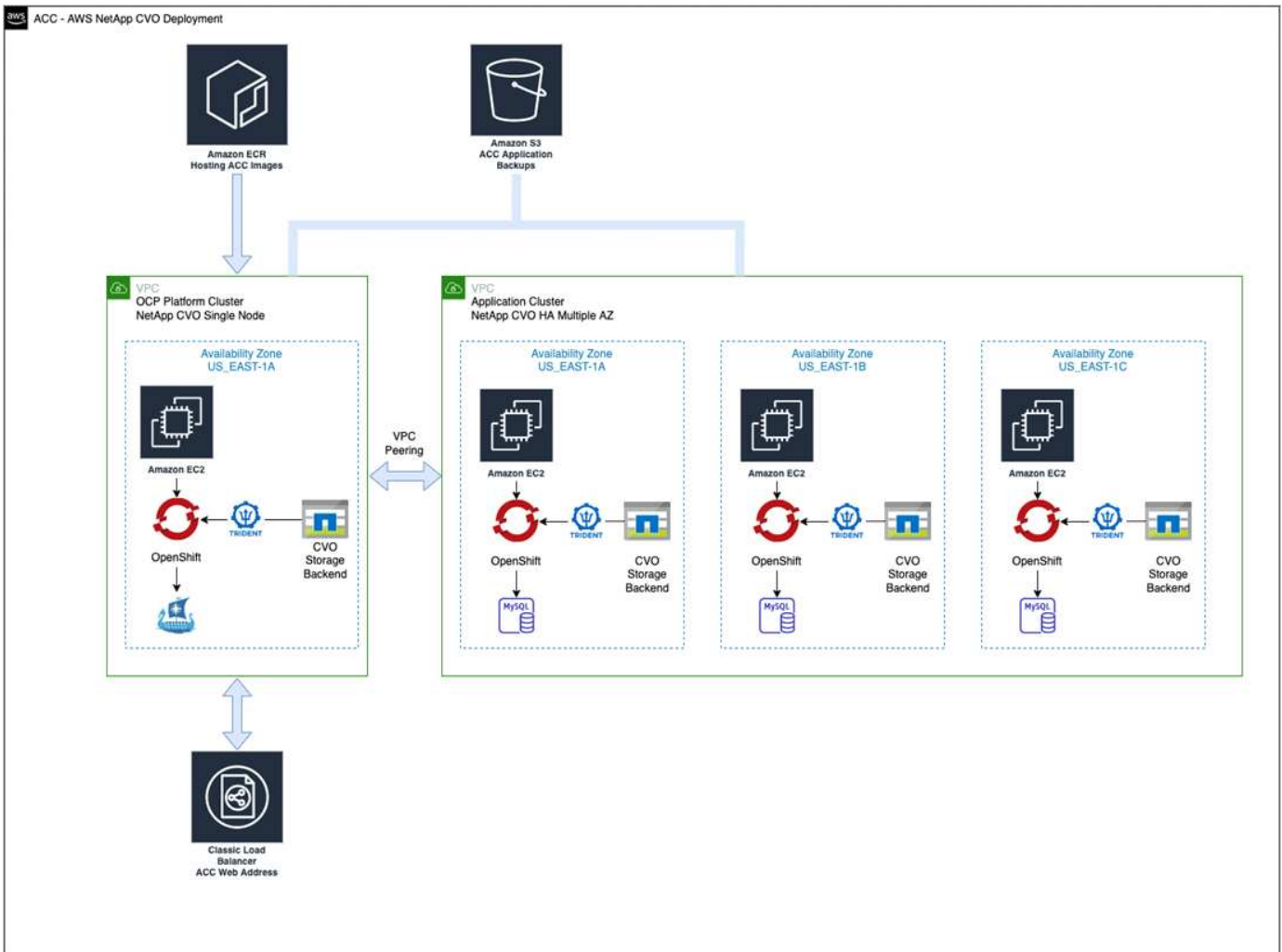
Si no crea la ECR, Astra Control Center no puede acceder a los datos de supervisión de un clúster que contenga Cloud Volumes ONTAP con un back-end de AWS. El problema se produce cuando el clúster que intenta detectar y gestionar mediante Astra Control Center no tiene acceso a AWS ECR.

6. Inserte las imágenes ACC en el registro definido.



El token del registro de contenedor elástico de AWS (ECR) caduca al cabo de 12 horas y provoca errores en las operaciones de clonado de varios clústeres. Este problema ocurre cuando se gestiona un back-end de almacenamiento desde Cloud Volumes ONTAP configurado para AWS. Para corregir este problema, vuelva a autenticarse con la ECR y genere un nuevo secreto para que las operaciones de clonación se reanuden correctamente.

A continuación mostramos un ejemplo de una puesta en marcha de AWS:



### Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a AWS, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte lo siguiente:

- ["Introducción a Cloud Volumes ONTAP en AWS"](#).
- ["Cree un conector en AWS mediante Cloud Manager"](#)

### Pasos

1. Añada sus credenciales a Cloud Manager.
2. Crear un área de trabajo.
3. Agregue un conector para AWS. Elija AWS como proveedor.
4. Cree un entorno de trabajo para su entorno de cloud.
  - a. Ubicación: "Amazon Web Services (AWS)"
  - b. Tipo: "Cloud Volumes ONTAP ha"
5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
  - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del clúster**.



- b. En la esquina superior derecha, tenga en cuenta la versión de Trident.
- c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el proveedor.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.

- 6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.



Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de implementación del nodo que se ejecutan en AWS.

### Instalar Astra Control Center

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



AWS utiliza el tipo de bloque Generic S3.

### Ponga en marcha Astra Control Center en Google Cloud Platform

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Google Cloud Platform (GCP).

#### Qué necesitará para GCP

Antes de implementar Astra Control Center en GCP, necesitará los siguientes elementos:

- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.10
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Cuenta de servicio de GCP con permisos que le permiten crear cubos y conectores


#### Requisitos del entorno operativo para GCP



Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible

Componente	Requisito
<b>Nodos de trabajo (requisitos de computación de GCP)</b>	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
<b>Equilibrador de carga</b>	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
<b>FQDN (ZONA DNS DE GCP)</b>	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
<b>Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)</b>	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento
<b>Registro de imágenes</b>	<p>Debe tener un registro privado existente, como Google Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>
<b>Configuración de Astra Trident/ONTAP</b>	<p>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 las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-nas csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-ha-san csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-nas csi.trident.netapp.io</code></li> <li>• <code>vsaworkingenvironment-&lt;&gt;-single-san csi.trident.netapp.io</code></li> </ul>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

#### Información general de puesta en marcha para GCP

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center en un clúster OCP autogestionado en GCP con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Instale un clúster RedHat OpenShift en GCP.](#)
2. [Cree un proyecto de GCP y una nube privada virtual.](#)
3. [Compruebe que dispone de suficientes permisos IAM.](#)
4. [Configure GCP.](#)
5. [Configure Cloud Manager de NetApp.](#)
6. [Instalar y configurar Astra Control Center.](#)

### **Instale un clúster RedHat OpenShift en GCP**

El primer paso es instalar un clúster RedHat OpenShift en GCP.

Para obtener instrucciones de instalación, consulte lo siguiente:

- ["Instalar un clúster OpenShift en GCP"](#)
- ["Creación de una cuenta de servicio de GCP"](#)

### **Cree un proyecto de GCP y una nube privada virtual**

Cree al menos un proyecto de GCP y una nube privada virtual (VPC).



OpenShift podría crear sus propios grupos de recursos. Además de ellas, debe definir también un VPC de GCP. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

### **Compruebe que dispone de suficientes permisos IAM**

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte ["Credenciales y permisos iniciales de GCP"](#).

### **Configure GCP**

A continuación, configure GCP para crear un VPC, configure instancias de computación, cree un almacenamiento de objetos de Google Cloud, cree un Registro de contenedor de Google para alojar las imágenes de Astra Control Center y empuje las imágenes a este registro.

Siga la documentación de GCP para completar los siguientes pasos. Consulte [instalación del clúster OpenShift en GCP](#).

1. Cree un proyecto de GCP y VPC en el GCP que planea utilizar para el clúster de OCP con el back-end de CVO.
2. Revise las instancias de computación. Puede tratarse de un servidor de configuración básica o máquinas virtuales en GCP.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestro y trabajador, cambie el tipo de instancia de GCP para que cumpla los requisitos de Astra. Consulte ["Requisitos del Centro de Control de Astra"](#).
4. Cree al menos un bloque de almacenamiento en cloud de GCP para almacenar sus backups.

5. Crear un secreto, que es necesario para el acceso a bloques.
6. Cree un registro de Google Container para alojar todas las imágenes de Astra Control Center.
7. Configure el acceso al registro de contenedores de Google para inserción/extracción de Docker para todas las imágenes de Astra Control Center.

Ejemplo: Las imágenes ACC se pueden insertar en este registro introduciendo la siguiente secuencia de comandos:

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

Este script requiere un archivo de manifiesto de Astra Control Center y su ubicación del Registro de imágenes de Google.

Ejemplo:

```
manifestfile=astra-control-center-<version>.manifest
GCP_CR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

8. Configure zonas DNS.

### Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a GCP, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte ["Introducción a Cloud Volumes ONTAP en GCP"](#).

### Lo que necesitará

- Acceso a la cuenta de servicio de GCP con los permisos y roles de IAM necesarios

### Pasos

1. Añada sus credenciales a Cloud Manager. Consulte ["Adición de cuentas de GCP"](#).
2. Agregue un conector para GCP.
  - a. Elija "GCP" como el proveedor.

- b. Introduzca las credenciales de GCP. Consulte ["Creación de un conector en GCP desde Cloud Manager"](#).
  - c. Asegúrese de que el conector está en marcha y cambie a dicho conector.
3. Cree un entorno de trabajo para su entorno de cloud.
    - a. Ubicación: "GCP"
    - b. Tipo: "Cloud Volumes ONTAP ha"
  4. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
    - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del clúster**.
    - b. En la esquina superior derecha, tenga en cuenta la versión de Trident.
    - c. Tenga en cuenta las clases de almacenamiento del clúster de Cloud Volumes ONTAP que muestran "NetApp" como el proveedor.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.

5. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.



Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en GCP.

### Instalar Astra Control Center

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



GCP utiliza el tipo de bloque Generic S3.

1. Genere el secreto Docker para obtener imágenes de la instalación de Astra Control Center:

```
kubectl create secret docker-registry <secret name>
--docker-server=<Registry location>
--docker-username=_json_key
--docker-password="$(cat <GCP Service Account JSON file>)"
--namespace=pcloud
```

### Ponga en marcha Astra Control Center en Microsoft Azure

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado que se aloja en un cloud público de Microsoft Azure.

#### Lo que necesitará para Azure

Antes de poner en marcha Astra Control Center en Azure, necesitará los siguientes elementos:


- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.8
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de Azure con permisos que le permiten crear cubos y conectores

#### Requisitos del entorno operativo para Azure

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Consulte ["Requisitos del entorno operativo del Centro de control de Astra"](#).

Componente	Requisito
<b>Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp</b>	300 GB como mínimo disponible
<b>Nodos de trabajo (requisitos de computación de Azure)</b>	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
<b>Equilibrador de carga</b>	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
<b>FQDN (zona DNS de Azure)</b>	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
<b>Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)</b>	Como back-end de almacenamiento, se usará Astra Trident 21.04 o posterior instalado y configurado, y NetApp ONTAP versión 9.5 o posterior
<b>Registro de imágenes</b>	<p>Debe disponer de un registro privado existente, como Azure Container Registry (ACR), al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div style="display: flex; align-items: center;">  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>

Componente	Requisito
<b>Configuración de Astra Trident/ONTAP</b>	<p>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 las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> <li>• vsaworkingenvironment-⟨⟩-ha-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-⟨⟩-ha-san csi.trident.netapp.io</li> <li>• vsaworkingenvironment-⟨⟩-single-nas csi.trident.netapp.io</li> <li>• vsaworkingenvironment-⟨⟩-single-san csi.trident.netapp.io</li> </ul>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

### Información general sobre la implementación para Azure

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center para Azure.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Instale un clúster RedHat OpenShift en Azure.](#)
2. [Cree grupos de recursos de Azure.](#)
3. [Compruebe que dispone de suficientes permisos IAM.](#)
4. [Configure Azure.](#)
5. [Configure Cloud Manager de NetApp.](#)
6. [Instalar y configurar Astra Control Center.](#)

### Instale un clúster RedHat OpenShift en Azure

El primer paso es instalar un clúster RedHat OpenShift en Azure.

Para obtener instrucciones de instalación, consulte la documentación de RedHat en "[Instalación del clúster OpenShift en Azure](#)" y.. "[Instalar una cuenta de Azure](#)".

### Cree grupos de recursos de Azure

Cree al menos un grupo de recursos de Azure.



OpenShift podría crear sus propios grupos de recursos. Además de estos, también debe definir los grupos de recursos de Azure. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

### Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "[Credenciales y permisos de Azure](#)".

### Configure Azure

A continuación, configure Azure para crear una red virtual, configurar instancias de computación, crear un contenedor de Azure Blob, crear un registro de contenedores de Azure (ACR) para alojar las imágenes de Astra Control Center y colocar las imágenes en este registro.

Siga la documentación de Azure para completar los siguientes pasos. Consulte "[Instalando el clúster de OpenShift en Azure](#)".

1. Cree una red virtual de Azure.
2. Revise las instancias de computación. Puede ser un servidor con configuración básica o máquinas virtuales en Azure.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en Azure para cumplir los requisitos de Astra. Consulte "[Requisitos del Centro de Control de Astra](#)".
4. Cree al menos un contenedor de Azure Blob para almacenar los backups.
5. Cree una cuenta de almacenamiento. Necesitará una cuenta de almacenamiento para crear un contenedor que se utilizará como bloque en Astra Control Center.
6. Cree un secreto, que es necesario para el acceso a bloques.
7. Cree un Azure Container Registry (ACR) para alojar todas las imágenes de Astra Control Center.
8. Configure el acceso ACR para pulsar/extraer todas las imágenes del Centro de control de Astra.
9. Inserte las imágenes ACC en este registro introduciendo el siguiente script:

```
az acr login -n <AZ ACR URL/Location>  
This script requires ACC manifest file and your Azure ACR location.
```

### Ejemplo:



```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

## 10. Configure zonas DNS.

### Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a Azure, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte ["Introducción a Cloud Manager en Azure"](#).

### Lo que necesitará

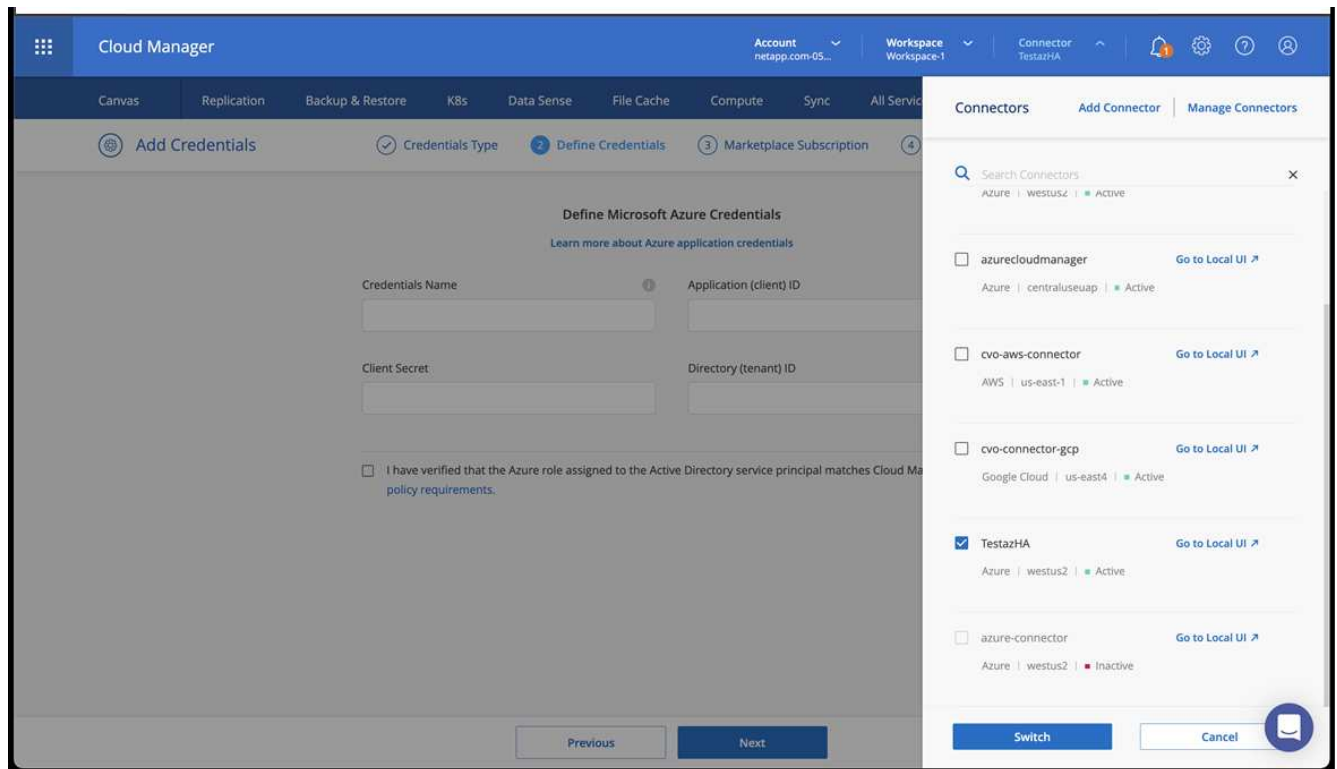
Acceso a la cuenta de Azure con los permisos y roles de IAM necesarios

### Pasos

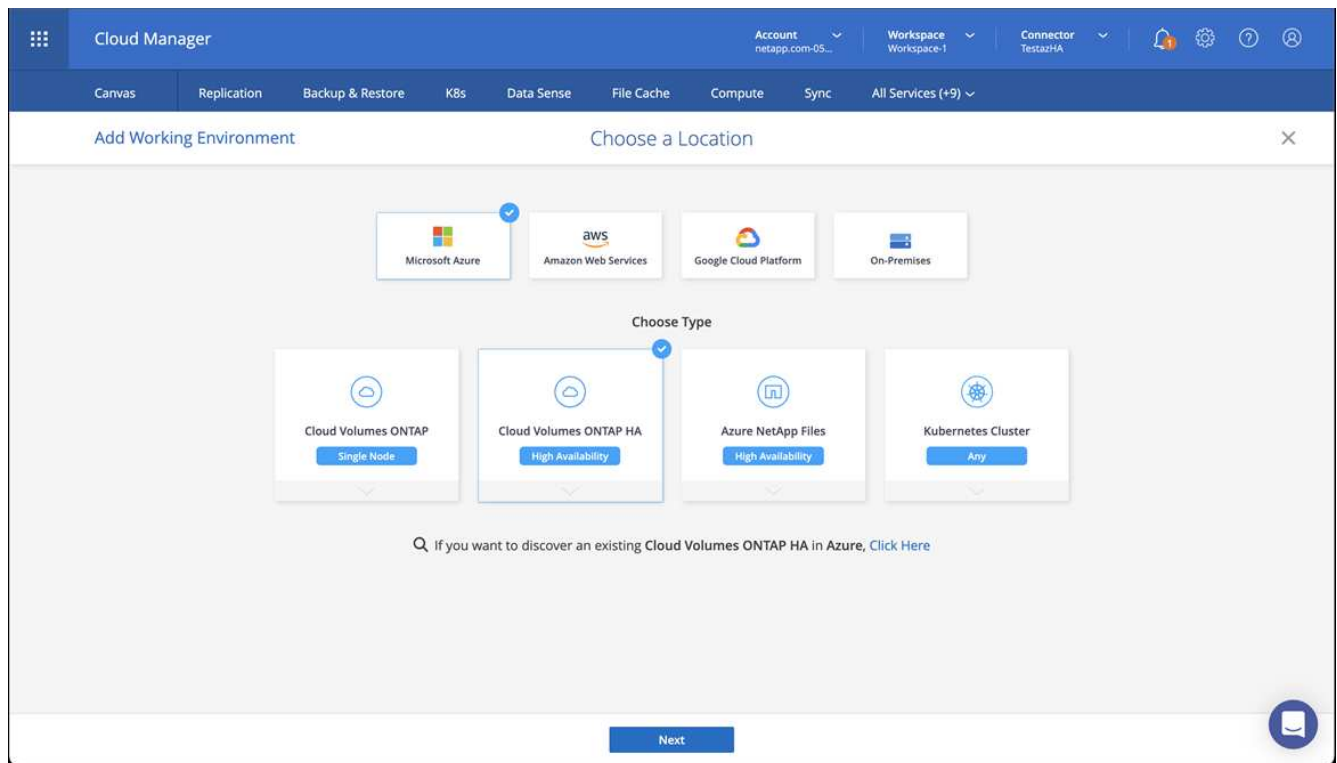
1. Añada sus credenciales a Cloud Manager.
2. Agregue un conector para Azure. Consulte ["Políticas de Cloud Manager"](#).
  - a. Elija **Azure** como proveedor.
  - b. Introduzca las credenciales de Azure, incluidos el ID de aplicación, el secreto de cliente y el ID del directorio (inquilino).

Consulte ["Crear un conector en Azure desde Cloud Manager"](#).

3. Asegúrese de que el conector está en marcha y cambie a dicho conector.

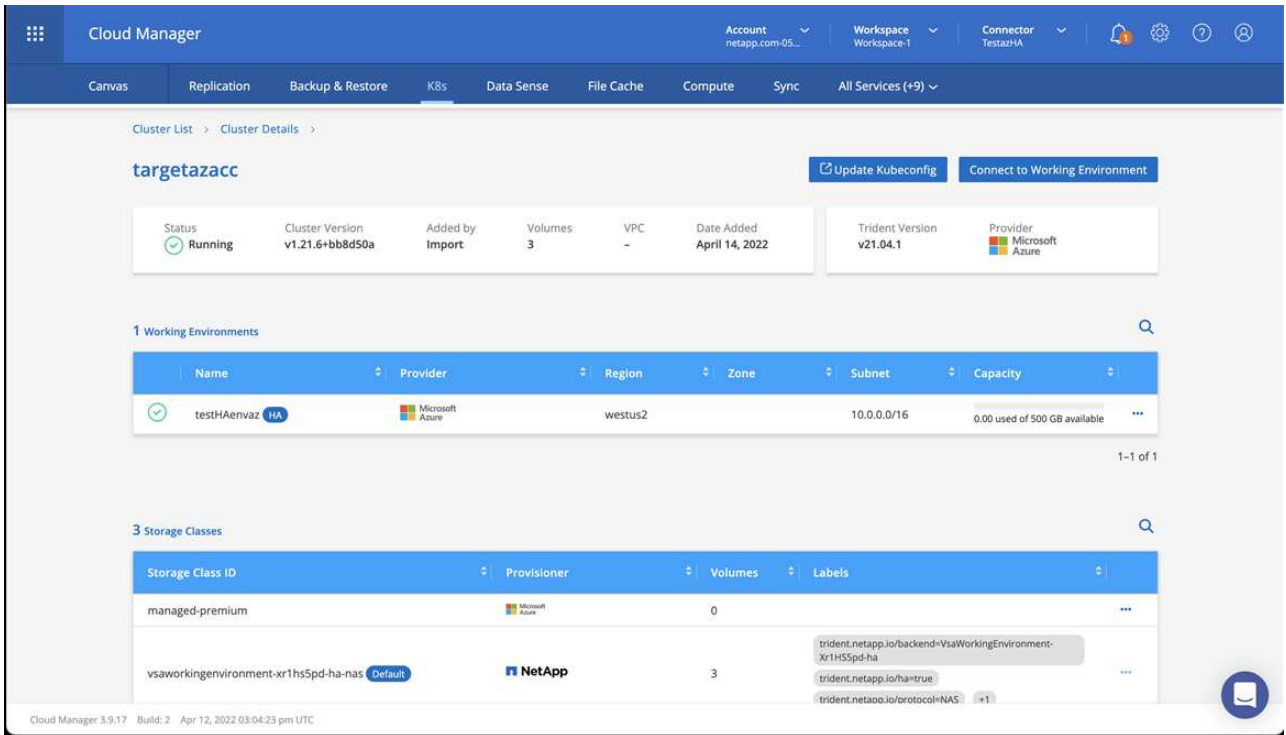


4. Cree un entorno de trabajo para su entorno de cloud.
  - a. Ubicación: "Microsoft Azure".
  - b. Tipo: "Cloud Volumes ONTAP ha".



5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
  - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del**

## clúster.



b. En la esquina superior derecha, tenga en cuenta la versión de Trident.

c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el proveedor.

Esto importa su clúster de Red Hat OpenShift y asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.

6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.
7. Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si ha está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en Azure.

### Instalar y configurar Astra Control Center

Instale Astra Control Center con el estándar ["instrucciones de instalación"](#).

Con Astra Control Center, añada un bucket de Azure. Consulte ["Configure Astra Control Center y añada cucharones"](#).

## Configure Astra Control Center

Astra Control Center admite y supervisa ONTAP y Astra Data Store como back-end de almacenamiento. Después de instalar Astra Control Center, inicie sesión en la interfaz de usuario y cambie la contraseña, le interesa configurar una licencia, añadir clústeres, gestionar el almacenamiento y añadir bloques.

### Tareas

- [Agregue una licencia de Astra Control Center](#)

- [Añada el clúster](#)
- [Añada un back-end de almacenamiento](#)
- [Añadir un bucket](#)

## Agregue una licencia de Astra Control Center

Puede añadir una licencia nueva con la interfaz de usuario o ["API"](#) Para obtener todas las funciones de Astra Control Center. Sin una licencia, el uso de Astra Control Center se limita a gestionar usuarios y agregar nuevos clústeres.

Para obtener más información sobre cómo se calculan las licencias, consulte ["Licencia"](#).



Para actualizar una evaluación existente o una licencia completa, consulte ["Actualizar una licencia existente"](#).

Las licencias de Astra Control Center miden los recursos de CPU mediante unidades de CPU de Kubernetes. La licencia debe tener en cuenta los recursos de CPU asignados a los nodos de trabajo de todos los clústeres de Kubernetes gestionados. Antes de agregar una licencia, debe obtener el archivo de licencia (NLF) de ["Sitio de soporte de NetApp"](#).

También puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Puede inscribirse para obtener una prueba gratuita registrándose ["aquí"](#).



Si su instalación crece para superar el número de unidades CPU con licencia, Astra Control Center le impide gestionar nuevas aplicaciones. Se muestra una alerta cuando se supera la capacidad.

### Lo que necesitará

Al descargar Astra Control Center desde ["Sitio de soporte de NetApp"](#) También puede descargar el archivo de licencia de NetApp (NLF). Asegúrese de tener acceso a este archivo de licencia.

### Pasos

1. Inicie sesión en la interfaz de usuario de Astra Control Center.
2. Seleccione **cuenta > Licencia**.
3. Seleccione **Agregar licencia**.
4. Busque el archivo de licencia (NLF) que descargó.
5. Seleccione **Agregar licencia**.

La página **cuenta > Licencia** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.



Si dispone de una licencia de evaluación, asegúrese de almacenar su ID de cuenta para evitar la pérdida de datos en caso de que se produzca un error en Astra Control Center si no envía los ASUP.

## Añada el clúster

Para comenzar a gestionar las aplicaciones, añada un clúster de Kubernetes y gestiónelo como un recurso de

computación. Es necesario añadir un clúster para Astra Control Center para descubrir sus aplicaciones Kubernetes. Para Astra Data Store, queremos añadir el clúster de aplicaciones Kubernetes que contiene aplicaciones que utilizan volúmenes provisionados por Astra Data Store.



Le recomendamos que Astra Control Center gestione el clúster en el que se implementa primero antes de añadir otros clústeres a Astra Control Center para su gestión. Disponer del cluster inicial en administración es necesario para enviar datos Kubemetrics y datos asociados al cluster para mediciones y resolución de problemas. Puede utilizar la función **Agregar clúster** para administrar un clúster con Astra Control Center.



Cuando Astra Control gestiona un clúster, realiza un seguimiento de la clase de almacenamiento predeterminada del clúster. Si cambia la clase de almacenamiento con `kubectl` Comandos, Control Astra revierte el cambio. Para cambiar la clase de almacenamiento predeterminada de un clúster gestionado por Astra Control, utilice uno de los siguientes métodos:

- Utilice la API Astra Control `PUT /managedClusters` asimismo, asigne una clase de almacenamiento predeterminada diferente con el `DefaultStorageClass` parámetro.
- Utilice la interfaz de usuario web de Astra Control para asignar una clase de almacenamiento predeterminada diferente. Consulte [Cambie la clase de almacenamiento predeterminada](#).

#### Lo que necesitará

- Antes de añadir un clúster, revise y realice la operación necesaria "[requisitos previos](#)".

#### Pasos

1. En **Dashboard** de la interfaz de usuario de Astra Control Center, seleccione **Agregar** en la sección Clusters.
2. En la ventana **Agregar clúster** que se abre, cargue un `kubeconfig.yaml` archivar o pegar el contenido de un `kubeconfig.yaml` archivo.



La `kubeconfig.yaml` el archivo debe incluir **sólo la credencial de cluster para un cluster**.



## Add 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  
No file selected



Credential name



Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "[Documentación de Kubernetes](#)" para obtener información acerca de cómo crear `kubeconfig` archivos.

- Introduzca un nombre de credencial. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
- Seleccione **Configurar almacenamiento**.
- Seleccione la clase de almacenamiento que se va a utilizar para este clúster de Kubernetes y seleccione **Review**.



Debe seleccionar una clase de almacenamiento de Trident con el respaldo del almacenamiento de ONTAP o el almacén de datos Astra.

Add cluster
STEP 2/3: STORAGE

---

**CONFIGURE STORAGE**

Existing storage classes are discovered and verified as eligible for use with Astra. You can use your existing default, or choose to set a new default at this time.  
Applications with persistent volumes on eligible storage classes are validated for use with Astra.

Default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligible
<input checked="" type="radio"/>	basic-csi	csi.trident.netapp.io	Delete		✔
<input type="radio"/>	thin	kubernetes.io/vsphere-volume	Delete		⚠

- Revise la información y si todo parece bien, seleccione **Agregar clúster**.

## Resultado

El clúster entra en el estado **detectando** y luego cambia a **ejecutando**. Ha añadido correctamente un clúster de Kubernetes y ahora lo gestiona en Astra Control Center.



Después de agregar un clúster para administrarlo en Astra Control Center, puede que el operador de supervisión tarde unos minutos en implementar. Hasta entonces, el icono de notificación se vuelve rojo y registra un evento **Comprobación de estado del agente de supervisión fallida**. Puede ignorar esto porque el problema se resuelve cuando Astra Control Center obtiene el estado correcto. Si el problema no se resuelve en unos minutos, vaya al clúster y ejecute `oc get pods -n netapp-monitoring` como punto de partida. Deberá consultar los registros del operador de supervisión para depurar el problema.

## Añada un back-end de almacenamiento

Puede añadir un back-end de almacenamiento para que Astra Control pueda gestionar sus recursos. Es posible poner en marcha un back-end de almacenamiento en un clúster gestionado o utilizar un back-end de almacenamiento existente.

Gestionar los clústeres de almacenamiento en Astra Control como back-end de almacenamiento le permite obtener vínculos entre los volúmenes persistentes (VP) y el back-end de almacenamiento, así como mediciones de almacenamiento adicionales.

### Lo que necesitará para las puestas en marcha existentes de Astra Data Store

- Ha añadido el clúster de aplicaciones de Kubernetes y el clúster de computación subyacente.



Después de añadir su clúster de aplicaciones Kubernetes para Astra Data Store y lo gestiona Astra Control, el clúster aparece como `unmanaged` en la lista de back-ends detectados. A continuación, debe añadir el clúster informático que contiene Astra Data Store y es la base para el clúster de aplicaciones de Kubernetes. Puede hacerlo desde **Backends** en la interfaz de usuario. Seleccione el menú Actions para el clúster, seleccione Manage, y. "añada el clúster". Tras el estado del clúster de `unmanaged` Los cambios en el nombre del clúster de Kubernetes, puede continuar con la adición de un back-end.

### Lo que necesitará para las nuevas puestas en marcha de Astra Data Store

- Ya tienes "ha cargado la versión del paquete de instalación que pretende implementar" A una ubicación accesible a Astra Control.
- Añadió el clúster Kubernetes que pretende usar para la implementación.
- Ha cargado el [Licencia de Astra Data Store](#) Para su implementación en una ubicación a la que pueda acceder Astra Control.

### Opciones

- [Instale recursos de almacenamiento](#)
- [Utilice un back-end de almacenamiento existente](#)

### Instale recursos de almacenamiento

Puede poner en marcha un nuevo almacén de datos de Astra y gestionar el back-end de almacenamiento asociado.

### Pasos

1. Navegue desde el panel o el menú backends (backends):
  - En **Dashboard**: En el Resumen de recursos, seleccione un enlace del panel Storage Backends y seleccione **Add** en la sección Backends.
  - Desde **Backends**:
    - i. En el área de navegación de la izquierda, seleccione **Backends**.
    - ii. Seleccione **Agregar**.
2. Seleccione la opción de implementación **Astra Data Store** en la ficha **despliegue**.
3. Seleccione el paquete Astra Data Store para implementar:
  - a. Introduzca un nombre para la aplicación Astra Data Store.
  - b. Elija la versión de Astra Data Store que desea implementar.



Si todavía no ha cargado la versión que pretende implementar, puede utilizar la opción **Agregar paquete** o salir del asistente y utilizar "gestión de paquetes" para cargar el paquete de instalación.

4. Seleccione una licencia de Astra Data Store que haya cargado previamente o utilice la opción **Agregar licencia** para cargar una licencia para usar con la aplicación.



Las licencias de Astra Data Store con permisos completos están asociadas con el clúster de Kubernetes y estos clústeres asociados deben aparecer automáticamente. Si no hay un clúster gestionado, puede seleccionar la opción **Agregar un clúster** para agregar uno a la administración de Astra Control. Para las licencias de Astra Data Store, si no se ha establecido ninguna asociación entre la licencia y el clúster, puede definir esta asociación en la siguiente página del asistente.

5. Si no ha añadido un clúster Kubernetes a Astra Control Management, debe hacerlo desde la página **Kubernetes Cluster**. Seleccione un clúster existente de la lista o seleccione **agregue el clúster subyacente** para agregar un clúster a Astra Control Management.
6. Seleccione un tamaño de plantilla para el clúster de Kubernetes que proporcione recursos para el almacén de datos Astra. Puede elegir una de las siguientes opciones:
  - Si lo desea `Recommended Kubernetes worker node requirements`, seleccione una plantilla de grande a pequeña en función de lo que permita su licencia.
  - Si lo desea `Custom Kubernetes worker node requirements`, seleccione el número de núcleos y la memoria total que desea para cada nodo del clúster. También se puede mostrar el número de nodos elegibles del clúster que cumplen con los criterios de selección de los núcleos y la memoria.



Al seleccionar una plantilla, seleccione nodos más grandes con más memoria y núcleos para cargas de trabajo más grandes o un mayor número de nodos para cargas de trabajo más pequeñas. Debe seleccionar una plantilla en función de lo que permita su licencia. Cada opción de plantilla recomendada sugiere el número de nodos elegibles que cumplen con el patrón de plantilla para la memoria y los núcleos y la capacidad de cada nodo.

7. Configure los nodos:
  - a. Agregue una etiqueta de nodo para identificar el pool de nodos de trabajo que admiten este clúster de almacén de datos Astra.



Debe añadirse la etiqueta a cada nodo individual del clúster que se utilizará para la puesta en marcha de Astra Data Store antes de que falle el inicio de la implementación o la implementación.

- b. Configure la capacidad (GIB) por nodo manualmente o seleccione la capacidad máxima permitida de nodo.
  - c. Configure un número máximo de nodos permitidos en el clúster o permita el número máximo de nodos en el clúster.
8. (Sólo licencias completas del almacén de datos Astra) Introduzca la clave de la etiqueta que desea utilizar para los dominios de protección.



Cree al menos tres etiquetas únicas para la clave de cada nodo. Por ejemplo, si la clave es `astra.datastore.protection.domain`, puede crear las siguientes etiquetas:  
`astra.datastore.protection.domain=domain1`, `astra.datastore.protection.domain=domain2`, y `astra.datastore.protection.domain=domain3`.

9. Configure la red de administración:
  - a. Introduzca una dirección IP de gestión para la gestión interna de Astra Data Store que se encuentra en la misma subred que las direcciones IP de nodos de trabajo.



- b. Elija utilizar el mismo NIC tanto para la administración como para las redes de datos o configúrelo por separado.
  - c. Introduzca el pool de direcciones IP de red de datos, la máscara de subred y la puerta de enlace para acceder al almacenamiento.
10. Revise la configuración y seleccione **despliegue** para comenzar la instalación.

## Resultado

Tras una instalación correcta, el back-end aparece en `available` estado en la lista de los back-ends, junto con información de rendimiento activa.



Es posible que deba actualizar la página para que se muestre el back-end.

## Utilice un back-end de almacenamiento existente

Puede traer un back-end de almacenamiento de ONTAP o Astra Data Store al centro de control de Astra.

## Pasos

1. Navegue desde el panel o el menú backends (backends):
  - En **Dashboard**: En el Resumen de recursos, seleccione un enlace del panel Storage Backends y seleccione **Add** en la sección Backends.
  - Desde **Backends**:
    - i. En el área de navegación de la izquierda, seleccione **Backends**.
    - ii. Seleccione **gestionar** en un back-end detectado desde el clúster administrado o seleccione **Agregar** para administrar un back-end existente adicional.
2. Seleccione la ficha **utilizar existente**.
3. Realice una de las siguientes acciones según el tipo de backend:
  - **Almacén de datos Astra**:
    - i. Seleccione **Astra Data Store**.
    - ii. Seleccione el clúster de cálculo administrado y seleccione **Siguiente**.
    - iii. Confirme los detalles del backend y seleccione **Agregar backend de almacenamiento**.
  - **ONTAP**:
    - i. Seleccione **ONTAP** y seleccione **Siguiente**.
    - ii. Introduzca la dirección IP de gestión del clúster de ONTAP y las credenciales de administrador.



El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, habilite los métodos de acceso `ontapi` y `http` Para el usuario en ambos clústeres de ONTAP. Consulte "[Gestionar cuentas de usuario](#)" si quiere más información.

- iii. Seleccione **Revisión**.
- iv. Confirme los detalles del backend y seleccione **Agregar backend de almacenamiento**.

## Resultado

El back-end aparece en `available` estado en la lista con información resumida.



Es posible que deba actualizar la página para que se muestre el back-end.

## Añadir un bucket

Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina.

Cuando se agrega un bloque, Astra Control Marca un bloque como el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado.

No necesita un bucket si va a clonar la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster.

Utilice cualquiera de los siguientes tipos de bloques:

- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp
- Genérico S3



Amazon Web Services (AWS) y Google Cloud Platform (GCP) utilizan el tipo de bloque Generic S3.

- Microsoft Azure



Aunque Astra Control Center es compatible con Amazon S3 como proveedor de cubos de S3 genérico, Astra Control Center podría no admitir todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

- Microsoft Azure

Para obtener instrucciones sobre cómo añadir cubos con la API Astra Control, consulte "[Información sobre API y automatización de Astra](#)".

### Pasos

1. En el área de navegación de la izquierda, seleccione **Cuchos**.
  - a. Seleccione **Agregar**.
  - b. Seleccione el tipo de bloque.



Cuando agregue un bloque, seleccione el proveedor de segmento correcto y proporcione las credenciales correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como tipo y acepta credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los futuros backups de aplicaciones y restauraciones usando este bucket.

- c. Cree un nuevo nombre de bloque o introduzca un nombre de bloque existente y una descripción opcional.



El nombre del bloque y la descripción aparecen como una ubicación de copia de seguridad que puede elegir más tarde al crear una copia de seguridad. El nombre también aparece durante la configuración de la política de protección.

- d. Introduzca el nombre o la dirección IP del extremo de S3.
- e. Si desea que este bloque sea el bloque predeterminado para todos los backups, compruebe la `Make this bucket the default bucket for this private cloud` opción.



Esta opción no aparece para el primer bloque que cree.

- f. Continúe añadiendo [información sobre credenciales](#).

### Añada credenciales de acceso de S3

Añada credenciales de acceso de S3 en cualquier momento.

#### Pasos

1. En el cuadro de diálogo Cuchos, seleccione la ficha **Agregar** o **utilizar existente**.
  - a. Introduzca un nombre para la credencial que la distingue de otras credenciales en Astra Control.
  - b. Escriba el identificador de acceso y la clave secreta pegando el contenido del portapapeles.

### Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de.

#### Pasos

1. En la interfaz de usuario web de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.
5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

### El futuro

Ahora que ha iniciado sesión y agregado clústeres a Astra Control Center, está listo para empezar a utilizar las funciones de gestión de datos de aplicaciones de Astra Control Center.

- ["Gestionar usuarios"](#)
- ["Inicie la gestión de aplicaciones"](#)
- ["Proteja sus aplicaciones"](#)
- ["Clone aplicaciones"](#)
- ["Gestionar notificaciones"](#)
- ["Conéctese a Cloud Insights"](#)
- ["Agregue un certificado TLS personalizado"](#)

## Obtenga más información

- ["Utilice la API Astra Control"](#)
- ["Problemas conocidos"](#)

## Requisitos previos para añadir un clúster

Debe asegurarse de que se cumplan las condiciones previas antes de añadir un clúster. También debe ejecutar las comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

### Qué necesitará antes de añadir un clúster

Asegúrese de que su clúster cumpla los requisitos descritos en ["Requisitos del clúster de aplicaciones"](#).



Si tiene pensado añadir un segundo clúster OpenShift 4.6, 4.7 o 4.8 como un recurso informático gestionado, debe asegurarse de que la función de Snapshot de volumen de Astra Trident esté habilitada. Consulte la Astra Trident oficial ["instrucciones"](#) Para habilitar y probar Volume Snapshots con Astra Trident.

- Clases de almacenamiento de Astra Trident configuradas con un ["back-end de almacenamiento admitido"](#) (necesario para cualquier tipo de clúster)
- El superusuario y el ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center. Ejecute el siguiente comando en la línea de comandos de la ONTAP:  

```
export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534
```
- Una Astra Trident `volumesnapshotclass` objeto definido por un administrador. Vea la Astra Trident ["instrucciones"](#) Para habilitar y probar Volume Snapshots con Astra Trident.
- Compruebe que solo tiene una única clase de almacenamiento predeterminada definida para el clúster de Kubernetes.

## Ejecutar las comprobaciones de elegibilidad

Ejecute las siguientes comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

### Pasos

1. Compruebe la versión de Trident.

```
kubectl get tridentversions -n trident
```

Si Trident existe, se muestra una salida similar a la siguiente:

```
NAME      VERSION
trident   21.04.0
```

Si Trident no existe, se muestra un resultado similar al siguiente:

```
error: the server doesn't have a resource type "tridentversions"
```



Si Trident no está instalado o la versión instalada no es la más reciente, debe instalar la versión más reciente de Trident antes de continuar. Consulte ["Documentación de Trident"](#) si desea obtener instrucciones.

2. Compruebe si las clases de almacenamiento están usando los controladores de Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get sc
NAME                                PROVISIONER                                RECLAIMPOLICY
VOLUMEBINDINGMODE  ALLOWVOLUMEEXPANSION  AGE
ontap-gold (default)  csi.trident.netapp.io  Delete
Immediate           true                   5d23h
thin                 kubernetes.io/vsphere-volume  Delete
Immediate           false                  6d
```

## Cree una imagen de rol administrativo

Asegúrese de que dispone de lo siguiente en su máquina antes de realizar los pasos siguientes:

- kubectl v1.19 o posterior instalado
- Una imagen marcada activa con los derechos de administrador del clúster para el contexto activo

### Pasos

1. Cree una cuenta de servicio del siguiente modo:

- a. Cree un archivo de cuenta de servicio llamado `astraccontrol-service-account.yaml`.

Ajuste el nombre y el espacio de nombres según sea necesario. Si se realizan cambios aquí, debe aplicar los mismos cambios en los pasos siguientes.

```
<strong>astraccontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astraccontrol-service-account
  namespace: default
```

- a. Aplicar la cuenta de servicio:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. (Opcional) Si el clúster utiliza una directiva de seguridad de POD restrictiva que no permite la creación de POD privilegiadas o permite que los procesos dentro de los contenedores Pod se ejecuten como usuario raíz, cree una directiva de seguridad de POD personalizada para el clúster que permita a Astra Control crear y administrar POD. Para ver instrucciones, consulte "[Cree una directiva de seguridad de POD personalizada](#)".
3. Conceda permisos de administrador del clúster de la siguiente manera:

- a. Cree un ClusterRoleBinding archivo llamado astracontrol-clusterrolebinding.yaml.

Ajuste los nombres y espacios de nombres modificados al crear la cuenta de servicio según sea necesario.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

- a. Aplique el enlace de roles del clúster:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

4. Enumere los secretos de la cuenta de servicio, reemplazando <context> con el contexto correcto para su instalación:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

El final de la salida debe ser similar a lo siguiente:

```
"secrets": [
  { "name": "astracontrol-service-account-dockercfg-vhz87"},
  { "name": "astracontrol-service-account-token-r59kr"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-vhz87` sería 0 y el índice para `astracontrol-service-account-token-r59kr` sería 1. En la salida, anote el índice del nombre de la cuenta de servicio que contiene la palabra "token".

5. Genere la kubeconfig de la siguiente manera:

- Cree un `create-kubeconfig.sh` archivo. Sustituya `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp
```

```

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp

```

b. Origen de los comandos para aplicarlos al clúster de Kubernetes.

```
source create-kubeconfig.sh
```

6. (opcional) cambie el nombre de la kubeconfig por un nombre significativo para el clúster. Proteja las credenciales del clúster.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```



## El futuro

Ahora que ha comprobado que se cumplen los requisitos previos, está listo ["añadir un clúster"](#).

## Obtenga más información

- ["Documentación de Trident"](#)
- ["Utilice la API Astra Control"](#)

## Agregue un certificado TLS personalizado

Puede quitar el certificado TLS autofirmado existente y reemplazarlo con un certificado TLS firmado por una entidad de certificación (CA).

### Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Acceso administrativo a un shell de comandos en el clúster para ejecutar `kubectl` comandos
- Archivos de claves privadas y certificados de la CA

### Quite el certificado autofirmado

Quite el certificado TLS autofirmado existente.

1. Con SSH, inicie sesión en el clúster Kubernetes que aloja Astra Control Center como usuario administrativo.
2. Busque el secreto TLS asociado con el certificado actual mediante el comando siguiente, reemplazo `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Elimine el secreto y certificado instalados actualmente con los comandos siguientes:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

### Añadir un nuevo certificado

Añada un nuevo certificado TLS firmado por una CA.

1. Utilice el siguiente comando para crear el nuevo secreto TLS con la clave privada y los archivos de certificado de la CA, reemplazando los argumentos entre paréntesis `<>` con la información adecuada:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

- Utilice el siguiente comando y el ejemplo para editar el archivo de definición de recursos personalizados (CRD) del clúster y cambiar el `spec.selfSigned` valor a `spec.ca.secretName` Para hacer referencia al secreto TLS que ha creado anteriormente:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

- Utilice el siguiente comando y el resultado de ejemplo para validar que los cambios son correctos y que el clúster está listo para validar certificados, sustituir `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time: 2021-07-01T23:50:27Z
    Message:             Signing CA verified
    Reason:              KeyPairVerified
    Status:              True
    Type:                Ready
  Events:               <none>
```

- Cree el `certificate.yaml` archivo utilizando el ejemplo siguiente, reemplazando los valores de marcador de posición entre corchetes `<>` con la información apropiada:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #Replace with the correct Astra Control
  Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Cree el certificado con el comando siguiente:

```
kubectl apply -f certificate.yaml
```

6. Con el siguiente comando y el resultado de ejemplo, valide que el certificado se ha creado correctamente y con los argumentos especificados durante la creación (como nombre, duración, plazo de renovación y nombres DNS).

```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration: 125h0m0s
  Issuer Ref:
    Kind:      ClusterIssuer
    Name:      cert-manager-certificates
  Renew Before: 61h0m0s
  Secret Name: <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time: 2021-07-02T00:45:41Z
    Message:             Certificate is up to date and has not expired
    Reason:              Ready
    Status:              True
    Type:               Ready
  Not After:           2021-07-07T05:45:41Z
  Not Before:          2021-07-02T00:45:41Z
  Renewal Time:        2021-07-04T16:45:41Z
  Revision:            1
Events:               <none>
```

7. Edite la opción Ingress CRD TLS para que apunte al nuevo secreto de certificado utilizando el siguiente comando y ejemplo, reemplazando los valores de marcador de posición entre paréntesis <> con la información adecuada:

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-namespace>
....

# tls:
#   options:
#     name: default
#     secretName: secure-testing-cert
#     store:
#       name: default

tls:
  options:
    name: default
  secretName: <certificate-secret-name>
  store:
    name: default
```

8. Con un explorador web, vaya a la dirección IP de implementación de Astra Control Center.
9. Compruebe que los detalles del certificado coinciden con los detalles del certificado que ha instalado.
10. Exporte el certificado e importe el resultado en el administrador de certificados en su navegador web.

## Cree una directiva de seguridad de POD personalizada

Astra Control debe crear y gestionar pods de Kubernetes en los clústeres que gestiona. Si el clúster utiliza una directiva de seguridad de POD restrictiva que no permite la creación de POD con privilegios ni permite que los procesos dentro de los contenedores Pod se ejecuten como usuario raíz, debe crear una directiva de seguridad de POD menos restrictiva para permitir que Astra Control cree y administre estas POD.

### Pasos

1. Cree una directiva de seguridad de POD para el clúster que sea menos restrictiva que la predeterminada y guárdela en un archivo. Por ejemplo:

```

apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'

```

2. Cree un nuevo rol para la política de seguridad del pod.

```

kubectl-admin create role psp:astracontrol \
  --verb=use \
  --resource=podsecuritypolicy \
  --resource-name=astracontrol

```

3. Vincule el nuevo rol a la cuenta de servicio.

```

kubectl-admin create rolebinding default:psp:astracontrol \
  --role=psp:astracontrol \
  --serviceaccount=astracontrol-service-account:default

```

# Preguntas frecuentes para Astra Control Center

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

## Descripción general

En las siguientes secciones se ofrecen respuestas a algunas preguntas adicionales que puede encontrar a medida que utiliza Astra Control Center. Para obtener más aclaraciones, por favor, diríjase a [astra.feedback@netapp.com](mailto:astra.feedback@netapp.com)

## Acceso a Astra Control Center

- ¿Cuál es la URL de Astra Control?\*

Astra Control Center utiliza autenticación local y una dirección URL específica para cada entorno.

Para la dirección URL, en un explorador, introduzca el nombre de dominio completo (FQDN) establecido en el campo `spec.astraAddress` del archivo `astra_control_Center_min.yaml` custom resource definition (CRD) cuando instaló Astra Control Center. El mensaje de correo electrónico es el valor que se ha establecido en el campo `SPEC.Email` del `astra_control_Center_min.ylma` CRD.

## Licencia

### Estoy utilizando la licencia de Evaluación. ¿Cómo puedo cambiar a la licencia completa?

Si desea cambiar fácilmente a una licencia completa, obtenga el archivo de licencia de NetApp (NLF).

- Pasos\*
- En la navegación de la izquierda, seleccione **cuenta > Licencia**.
- Seleccione **Agregar licencia**.
- Busque el archivo de licencia que ha descargado y seleccione **Agregar**.

### Estoy utilizando la licencia de Evaluación. ¿Puedo seguir gestionando aplicaciones?

Sí, puede comprobar la funcionalidad de administración de aplicaciones con la licencia de evaluación.

## Registrar clústeres de Kubernetes

### Necesito añadir nodos de trabajo a mi clúster Kubernetes después de añadir a Astra Control. ¿Qué debo hacer?

Los nodos de trabajo nuevos se pueden agregar a los pools existentes. Estos serán descubiertos automáticamente por Astra Control. Si los nuevos nodos no están visibles en Astra Control, compruebe si los nuevos nodos de trabajo están ejecutando el tipo de imagen admitido. También puede verificar el estado de los nuevos nodos de trabajo mediante el `kubectl get nodes` comando.

### ¿Cómo descontrolo correctamente un clúster?

1. ["Desgestione las aplicaciones desde Astra Control"](#).
2. ["Desgestione el clúster desde Astra Control"](#).

### ¿Qué ocurre con mis aplicaciones y datos después de eliminar el clúster Kubernetes de Astra Control?

La eliminación de un clúster de Astra Control no realizará ningún cambio en la configuración del clúster (aplicaciones y almacenamiento persistente). Las instantáneas de Astra Control o las copias de seguridad tomadas de las aplicaciones en ese clúster no estarán disponibles para restaurar. Los backups de almacenamiento persistentes creados por Astra Control permanecen en Astra Control, pero no están disponibles para la restauración.



Quite siempre un clúster de Astra Control antes de eliminarlo mediante cualquier otro método. La eliminación de un clúster con otra herramienta mientras Astra Control sigue gestionando puede causar problemas para su cuenta Astra Control.

- ¿Trident de NetApp se desinstala automáticamente de un clúster cuando lo descontrola? cuando se desvincula un clúster de Astra Control Center, Trident no se desinstala automáticamente del clúster. Para desinstalar Trident, tendrá que hacerlo ["Siga estos pasos en la documentación de Trident"](#).

## Gestionar aplicaciones

- ¿Puede Astra Control implementar una aplicación?\*

Astra Control no implementa aplicaciones. Las aplicaciones deben implementarse fuera de Astra Control.

### ¿Qué sucede con las aplicaciones después de dejar de administrarlas desde Astra Control?

Se eliminarán todos los backups o las snapshots existentes. Las aplicaciones y los datos siguen estando disponibles. Las operaciones de administración de datos no estarán disponibles para aplicaciones no administradas o para cualquier copia de seguridad o copia Snapshot que pertenezcan a él.

### ¿Puede Astra Control gestionar una aplicación que utiliza un almacenamiento que no sea de NetApp?

No Aunque Astra Control puede detectar aplicaciones que utilizan almacenamiento de terceros, no puede gestionar una aplicación que utilice almacenamiento de terceros.

**¿Debo administrar Astra Control mismo?** no, no debería gestionar Astra Control por sí mismo porque es una "app del sistema".

**¿Afectan los POD que no son saludables a la gestión de aplicaciones?** Si una aplicación gestionada tiene pods en estado incorrecto, Astra Control no puede crear nuevos backups y clones.

## Operaciones de gestión de datos

- hay instantáneas en mi cuenta que no creé. ¿de dónde vienen?\*

En algunas situaciones, Astra Control creará automáticamente una instantánea como parte de un proceso de backup, clonado o restauración.

### Mi aplicación utiliza varios VP. ¿Tomará Astra Control instantáneas y copias de seguridad de todas estas EVs?

Sí. Una operación de instantánea en una aplicación de Astra Control incluye una instantánea de todos los VP vinculados a las RVP de la aplicación.

### ¿Puedo gestionar las instantáneas tomadas por Astra Control directamente a través de una interfaz o almacenamiento de objetos diferente?

No Las copias Snapshot y las copias de seguridad realizadas por Astra Control solo se pueden gestionar con





## Información de copyright

Copyright © 2024 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 INTERRUPTIÓN 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.