



# **Instalar Astra Control Center**

## **Astra Control Center**

NetApp

November 21, 2023

This PDF was generated from <https://docs.netapp.com/es-es/astra-control-center-2211/get-started/cert-manager-prereqs.html> on November 21, 2023. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Instale Astra Control Center mediante el proceso estándar. . . . . 1
  - Descargue y extraiga Astra Control Center . . . . . 2
  - Instale el complemento Astra kubectl de NetApp. . . . . 3
  - Agregue las imágenes al registro local . . . . . 3
  - Configurar espacio de nombres y secreto para registros con requisitos de autenticación . . . . . 5
  - Instale el operador de Astra Control Center. . . . . 7
  - Configurar Astra Control Center. . . . . 10
  - Complete la instalación del centro de control de Astra y del operador . . . . . 23
  - Comprobar el estado del sistema . . . . . 24
  - Configure la entrada para el equilibrio de carga . . . . . 29
  - Inicie sesión en la interfaz de usuario de Astra Control Center . . . . . 32
  - Solucione los problemas de instalación . . . . . 32
  - El futuro . . . . . 33

# 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. Puede utilizar este procedimiento para instalar Astra Control Center en entornos conectados a Internet o con conexión por aire.

## Otros procedimientos de instalación

- **Instalar con RedHat OpenShift OperatorHub:** Utilice esto ["procedimiento alternativo"](#) Para instalar Astra Control Center en OpenShift con OperatorHub.
- **Instalar en la nube pública con Cloud Volumes ONTAP backend:** Uso ["estos procedimientos"](#) Para instalar Astra Control Center en Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure con un back-end de almacenamiento de Cloud Volumes ONTAP.

Para ver una demostración del proceso de instalación de Astra Control Center, consulte ["este vídeo"](#).

## 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"](#).
- 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 intenta instalar su propio administrador de certificados. De forma predeterminada, Astra Control Center instala su propio administrador de certificados durante la instalación.

## Acerca de esta tarea

El proceso de instalación de Astra Control Center le ayuda a hacer lo siguiente:

- Instale los componentes de Astra en la `netapp-acc` (o nombre personalizado).
- Cree una cuenta predeterminada de administrador de propietario de Astra Control.
- Establecer una dirección de correo electrónico de usuario administrativo y una contraseña de configuración inicial predeterminada. A este usuario se le asigna el rol de propietario que se necesita para iniciar sesión por primera vez en la interfaz de usuario.
- Determine que se están ejecutando todas las pods de Astra Control Center.
- Instale la interfaz de usuario de Astra Control Center.



No elimine el operador Astra Control Center (por ejemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) En cualquier momento durante la instalación o el funcionamiento de Astra Control Center para evitar la eliminación de las dosis.

## Pasos

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

- [Descargue y extraiga 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 extraiga Astra Control Center

1. Vaya a la "[Página de descargas de Astra Control Center Evaluation](#)" En el sitio de soporte de NetApp.
2. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`).
3. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete:

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

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

Se mostrará la salida `Verified OK` después de una verificación correcta.

4. Extraiga las imágenes del paquete Astra Control Center:

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

# Instale el complemento Astra kubectl de NetApp

El complemento de la línea de comandos Astra bectl de NetApp ahorra tiempo en la realización de tareas comunes asociadas a la puesta en marcha y la actualización de Astra Control Center.

## Lo que necesitará

NetApp proporciona binarios de complementos para diferentes arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea.

## Pasos

1. Enumere los binarios disponibles del complemento Astra kubectl de NetApp, y anote el nombre del archivo que necesita para el sistema operativo y la arquitectura de CPU:



La biblioteca de complementos kubectl forma parte del paquete tar y se extrae en la carpeta `kubectl-astra`.

```
ls kubectl-astra/
```

2. Mueva el binario correcto a la ruta actual y cambie el nombre a `kubectl-astra`:

```
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 raíz del tarball. Debería ver este archivo y directorio:

```
acc.manifest.bundle.yaml
acc/
```

2. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:
  - Sustituya `<BUNDLE_FILE>` por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
  - Sustituya `&lt;MY_FULL_REGISTRY_PATH&gt;` por la URL del repositorio de Docker; por ejemplo, `"<a href="https://&lt;docker-registry&gt;" class="bare">https://&lt;docker-registry&gt;"</a>`.
  - Reemplace `<MY_REGISTRY_USER>` por el nombre de usuario.
  - Sustituya `<MY_REGISTRY_TOKEN>` por un token autorizado para el registro.

```
kubectrl astra packages push-images -m <BUNDLE_FILE> -r
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
<MY_REGISTRY_TOKEN>
```

## Podman

1. Cambie al directorio raíz del tarball. Debería ver este archivo y directorio:

```
acc.manifest.bundle.yaml
acc/
```

2. Inicie sesión en su registro:

```
podman login <YOUR_REGISTRY>
```

3. Prepare y ejecute una de las siguientes secuencias de comandos personalizadas para la versión de Podman que utilice. Sustituya `<MY_FULL_REGISTRY_PATH>` por la URL del repositorio que incluye cualquier subdirectorio.

```
<strong>Podman 4</strong>
```

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```

**Podman 3**

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=22.11.0-82
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //'')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done

```



La ruta de acceso de imagen que crea el script debe parecerse a la siguiente, dependiendo de la configuración del Registro:

<https://netappdownloads.jfrog.io/docker-astra-control-prod/netapp/astra/acc/22.11.0-82/image:version>

## 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]
```



Antes de completar la instalación, asegúrese de que KUBECONFIG apunta al clúster en el que desea instalar Astra Control Center. El KUBECONFIG sólo puede contener un contexto.

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/22.11.0-82`).

```
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, vuelva a crear el espacio de nombres y, a continuación, vuelva a generar el secreto para el espacio de nombres.

c. Cree el `netapp-acc` (o nombre personalizado).

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

Respuesta de ejemplo:



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

- d. Cree un secreto para netapp-acc (o nombre 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
```

## 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](#).

```
<strong>astra_control_center_operator_deploy.yaml</strong>
```

```

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
  strategy:
    type: Recreate
  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
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
            - name: ACCOP_HELM_INSTALLTIMEOUT
              value: 5m
          image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
          livenessProbe:
            httpGet:
              path: /healthz
              port: 8081
            initialDelaySeconds: 15

```

```
    periodSeconds: 20
  name: manager
  readinessProbe:
    httpGet:
      path: /readyz
      port: 8081
    initialDelaySeconds: 5
    periodSeconds: 10
  resources:
    limits:
      cpu: 300m
      memory: 750Mi
    requests:
      cpu: 100m
      memory: 75Mi
  securityContext:
    allowPrivilegeEscalation: false
imagePullSecrets: []
  securityContext:
    runAsUser: 65532
  terminationGracePeriodSeconds: 10
```

### 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.yaml`) para realizar las configuraciones de cuenta, soporte, registro y otras necesarias:

```
vim astra_control_center.yaml
```



Una muestra anotada de AYLMA sigue estos pasos.

2. Modifique o confirme los siguientes ajustes:

`<code>accountName</code>`

Ajuste	Orientación	Tipo	Ejemplo
accountName	Cambie el accountName Cadena con el nombre que desea asociar a la cuenta Astra Control Center. Sólo puede haber un nombre de cuenta.	cadena	Example

`<code>astraVersion</code>`

Ajuste	Orientación	Tipo	Ejemplo
astraVersion	La versión de Astra Control Center para implementar. No se necesita ninguna acción para este ajuste, ya que el valor se rellenará previamente.	cadena	22.11.0-82

`<code>astraAddress</code>`

Ajuste	Orientación	Tipo	Ejemplo
<code>astraAddress</code>	<p>Cambie el <code>astraAddress</code> Cadena al FQDN (recomendado) o dirección IP que desea utilizar en su navegador para acceder a Astra Control Center. Esta dirección define cómo se encontrará Astra Control Center en su centro de datos y es el mismo FQDN o la dirección IP que ha aprovisionado desde su equilibrador de carga cuando ha finalizado <a href="#">"Requisitos del Centro de Control de Astra"</a>. NOTA: No utilizar <code>http://</code> o <code>https://</code> en la dirección. Copie este FQDN para utilizarlo en un <a href="#">paso posterior</a>.</p>	cadena	<code>astra.example.com</code>

## <code>autoSupport</code>

Las selecciones de esta sección determinan si participará en la aplicación de soporte proactivo de NetApp, Active IQ de NetApp y dónde se envían los datos. Se requiere una conexión a Internet (puerto 442) y todos los datos de soporte se anóniman.

Ajuste	Uso	Orientación	Tipo	Ejemplo
<code>autoSupport.enrolled</code>	Uno de los dos <code>enrolled</code> o <code>url</code> los campos deben seleccionarse	Cambiar <code>enrolled</code> Para <code>AutoSupport</code> a. <code>false</code> para sitios sin conexión a internet o <code>retención true</code> para sitios conectados. Un valor de <code>true</code> Permite enviar datos anónimos a NetApp con fines de soporte. La elección predeterminada es <code>false</code> E indica que no se enviará ningún dato de soporte a NetApp.	Booleano	<code>false</code> (este valor es el predeterminado)
<code>autoSupport.url</code>	Uno de los dos <code>enrolled</code> o <code>url</code> los campos deben seleccionarse	Esta URL determina dónde se enviarán los datos anónimos.	cadena	<a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>

`<code>email</code>`

Ajuste	Orientación	Tipo	Ejemplo
email	Cambie el email cadena en la dirección inicial predeterminada del administrador. Copie esta dirección de correo electrónico para su uso en un <a href="#">paso posterior</a> . Esta dirección de correo electrónico se utilizará como nombre de usuario de la cuenta inicial para iniciar sesión en la interfaz de usuario y se le notificarán los eventos de Astra Control.	cadena	admin@example.com

`<code>firstName</code>`

Ajuste	Orientación	Tipo	Ejemplo
firstName	El nombre del administrador inicial predeterminado asociado con la cuenta Astra. El nombre utilizado aquí aparecerá en un encabezado de la interfaz de usuario después del primer inicio de sesión.	cadena	SRE

`<code>LastName</code>`

Ajuste	Orientación	Tipo	Ejemplo
lastName	Apellido del administrador inicial predeterminado asociado con la cuenta Astra. El nombre utilizado aquí aparecerá en un encabezado de la interfaz de usuario después del primer inicio de sesión.	cadena	Admin



## <code>imageRegistry</code>

Las selecciones realizadas en esta sección definen el registro de imágenes del contenedor que aloja las imágenes de la aplicación Astra, el operador del centro de control Astra y el repositorio de Astra Control Center Helm.

Ajuste	Uso	Orientación	Tipo	Ejemplo
<code>imageRegistry.name</code>	Obligatorio	El nombre del registro de imágenes en el que se insertó las imágenes en el <a href="#">paso anterior</a> . No utilizar <code>http://</code> o <code>https://</code> en el nombre del registro.	cadena	<code>example.registry.com/astra</code>
<code>imageRegistry.secret</code>	Obligatorio si la cadena introducida para <code>imageRegistry.name</code> requiere a <code>secret</code> .  IMPORTANT: If you are using a registry that does not require authorization, you must delete this <code>`secret</code> línea dentro <code>imageRegistry</code> o se producirá un error en la instalación.	El nombre del secreto Kubernetes utilizado para autenticarse con el registro de imágenes.	cadena	<code>astra-registry-cred</code>

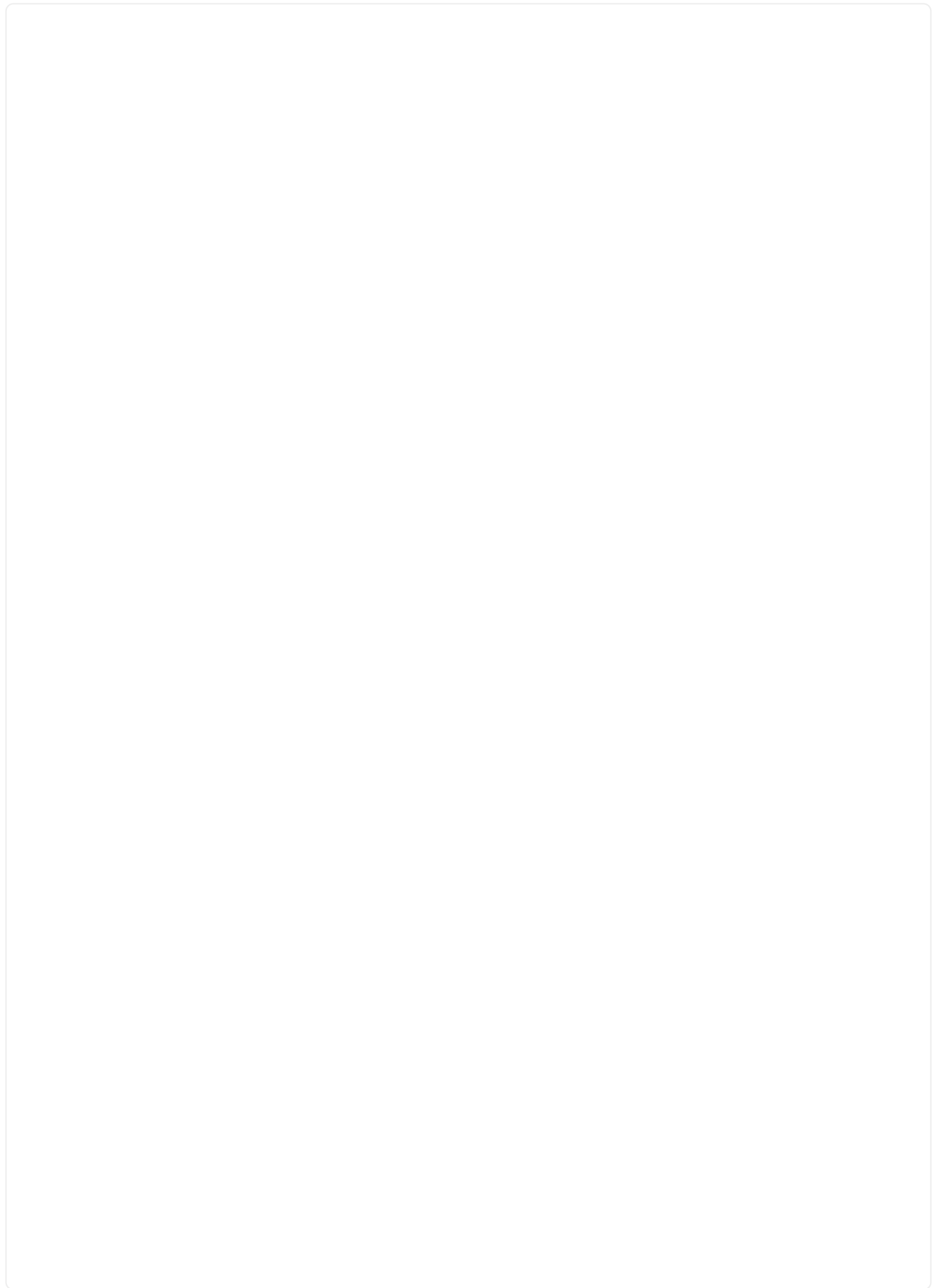
`<code>storageClass</code>`

Ajuste	Orientación	Tipo	Ejemplo
storageClass	<p>Cambie el storageClass valor desde ontap-gold En otro recurso de la clase de almacenamiento de Trident, según lo requiera su instalación. Ejecute el comando <code>kubect1 get sc</code> para determinar las clases de almacenamiento configuradas existentes. Se debe introducir una de las clases de almacenamiento basadas en Trident en el archivo de manifiesto (<code>astra-control-center- &lt;version&gt;.manifes t</code>) Y se utilizará para Astra PVs. Si no está establecida, se utilizará la clase de almacenamiento predeterminada. <b>NOTA:</b> Si se ha configurado una clase de almacenamiento predeterminada, asegúrese de que es la única clase de almacenamiento que tiene la anotación predeterminada.</p>	cadena	ontap-gold

**<code>volumeReclaimPolicy</code>**

Ajuste	Orientación	Tipo	Opciones
<code>volumeReclaimPolicy</code>	De esta forma se establece la política de reclamaciones para los vehículos de Astra. Configuración de esta directiva como <code>Retain</code> Conserva los volúmenes persistentes una vez que Astra se elimina. Configuración de esta directiva como <code>Delete</code> elimina los volúmenes persistentes después de eliminar astra. Si no se establece este valor, se conservan los VP.	cadena	<ul style="list-style-type: none"><li>• <code>Retain</code> (Este es el valor predeterminado)</li><li>• <code>Delete</code></li></ul>

`<code>ingressType</code>`





Ajuste	Orientación	Tipo	Opciones
ingressType	<p>Utilice uno de los siguientes tipos de entrada: <b>*Generic*</b> (ingressType: "Generic") (Predeterminado) Utilice esta opción cuando tenga otro controlador de entrada en uso o prefiera usar su propio controlador de entrada. Después de implementar Astra Control Center, deberá configurar el <b>"controlador de entrada"</b> Para exponer Astra Control Center con una URL. <b>AccTraefik</b> (ingressType: "AccTraefik") Utilice esta opción cuando prefiera no configurar un controlador de entrada. 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 aún 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</p>	cadena	<ul style="list-style-type: none"> <li>• Generic (este es el valor predeterminado)</li> <li>• AccTraefik</li> </ul>

**<code>astraResourcesScaler</code>**

Ajuste	Orientación	Tipo	Opciones
<code>astraResourcesScaler</code>	Opciones de escalado para los límites de recursos de AstraControlCenter. De forma predeterminada, Astra Control Center se despliega con solicitudes de recursos establecidas para la mayoría de los componentes de Astra. Esta configuración permite que la pila de software de Astra Control Center tenga un mejor rendimiento en entornos con un mayor nivel de carga y escalabilidad de las aplicaciones. Sin embargo, en situaciones que utilizan grupos de desarrollo o pruebas más pequeños, el campo <code>CR</code> <code>astraResourcesScaler</code> se puede establecer en <code>Off</code> . De este modo se deshabilitan las solicitudes de recursos y se puede implementar en clústeres más pequeños.	cadena	<ul style="list-style-type: none"><li>• <code>Default</code> (Este es el valor predeterminado)</li><li>• <code>Off</code></li></ul>

`<code>crds</code>`

Sus selecciones en esta sección determinan cómo Astra Control Center debe manejar los CRD.

Ajuste	Orientación	Tipo	Ejemplo
<code>crds.externalCertManager</code>	Si utiliza un administrador de certificados externo, cambie <code>externalCertManager</code> para <code>true</code> . El valor predeterminado <code>false</code> Hace que Astra Control Center instale sus propios CRD de administrador de certificados durante la instalación. Los <code>crds</code> son objetos de todo el clúster y su instalación podría tener un impacto en otras partes del clúster. Puede utilizar este indicador para indicar a Astra Control Center que el administrador del clúster instalará y gestionará estos CRD fuera de Astra Control Center.	Booleano	<code>False</code> (este valor es el predeterminado)
<code>crds.externalTraefik</code>	De forma predeterminada, Astra Control Center instalará los CRD de Traefik necesarios. Los <code>crds</code> son objetos de todo el clúster y su instalación podría tener un impacto en otras partes del clúster. Puede utilizar este indicador para indicar a Astra Control Center que el administrador del clúster instalará y gestionará estos CRD fuera de Astra Control Center.	Booleano	<code>False</code> (este valor es el predeterminado)



```
<strong>astra_control_center.yaml</strong>
```

```
apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  astraResourcesScaler: "Default"
  additionalValues: {}
  crds:
    externalTraefik: false
    externalCertManager: false
```

## 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.yaml -n [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

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

## Comprobar el estado del sistema

Puede verificar el estado del sistema con comandos kubectl. Si prefiere utilizar OpenShift, puede utilizar comandos de OC comparables para realizar los pasos de verificación.

### Pasos

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-76d8d845c9-ggds2 14m	1/1	Running	0
activity-6cc67ff9f4-z48mr (8m32s ago) 9m	1/1	Running	2
api-token-authentication-7s67v 8m56s	1/1	Running	0
api-token-authentication-bplb4 8m56s	1/1	Running	0
api-token-authentication-p2c9z 8m56s	1/1	Running	0
asup-6cdfbc6795-md8vn 9m14s	1/1	Running	0
authentication-9477567db-8hnc9 7m4s	1/1	Running	0
bucket-service-f4dbdfcd6-wqzkw 8m48s	1/1	Running	0
cert-manager-bb756c7c4-wm2cv 14m	1/1	Running	0
cert-manager-cainjector-c9bb86786-8wrf5 14m	1/1	Running	0
cert-manager-webhook-dd465db99-j2w4x 14m	1/1	Running	0
certificates-68dff9cdd6-kcvml (8m43s ago) 9m2s	1/1	Running	2
certificates-68dff9cdd6-rsnsb 9m2s	1/1	Running	0
cloud-extension-69d48c956c-2s8dt (8m43s ago) 9m24s	1/1	Running	3
cloud-insights-service-7c4f48b978-7gvlh (8m50s ago) 9m28s	1/1	Running	3
composite-compute-7d9ff5f68-nxbhl 8m51s	1/1	Running	0
composite-volume-57b4756d64-nl66d 9m13s	1/1	Running	0
credentials-6dbc55f89f-qpzff 11m	1/1	Running	0
entitlement-67bfb6d7-gl6kp (8m33s ago) 9m38s	1/1	Running	4
features-856cc4dccc-mxbdb 9m20s	1/1	Running	0
fluent-bit-ds-4rtsp 6m54s	1/1	Running	0

fluent-bit-ds-9rql1	1/1	Running	0
6m54s			
fluent-bit-ds-w5mp7	1/1	Running	0
6m54s			
graphql-server-7c7cc49776-jz2kn	1/1	Running	0
2m29s			
identity-87c59c975-9jpnf	1/1	Running	0
9m6s			
influxdb2-0	1/1	Running	0
13m			
keycloak-operator-84ff6d59d4-qcnmc	1/1	Running	0
7m1s			
krakend-cbf6c7df9-mdtzv	1/1	Running	0
2m30s			
license-5b888b78bf-plj6j	1/1	Running	0
9m32s			
login-ui-846b4664dd-fz8hv	1/1	Running	0
2m24s			
loki-0	1/1	Running	0
13m			
metrics-facade-779cc9774-n26rw	1/1	Running	0
9m18s			
monitoring-operator-974db78f-pkspq	2/2	Running	0
6m58s			
nats-0	1/1	Running	0
13m			
nats-1	1/1	Running	0
13m			
nats-2	1/1	Running	0
13m			
nautilus-7bdc7ddc54-49tfn	1/1	Running	0
7m50s			
nautilus-7bdc7ddc54-cwc79	1/1	Running	0
9m36s			
openapi-5584ff9f46-gbrdj	1/1	Running	0
9m17s			
openapi-5584ff9f46-z9mzk	1/1	Running	0
9m17s			
packages-bfc58cc98-lpxq9	1/1	Running	0
8m58s			
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 (6m15s ago) 6m56s	1/1	Running	3
polaris-keycloak-1 4m22s	1/1	Running	0
polaris-keycloak-2 3m41s	1/1	Running	0
polaris-keycloak-db-0 6m56s	1/1	Running	0
polaris-keycloak-db-1 4m23s	1/1	Running	0
polaris-keycloak-db-2 3m36s	1/1	Running	0
polaris-mongodb-0 13m	2/2	Running	0
polaris-mongodb-1 13m	2/2	Running	0
polaris-mongodb-2 12m	2/2	Running	0
polaris-ui-5ccff47897-8rzgh 2m33s	1/1	Running	0
polaris-vault-0 13m	1/1	Running	0
polaris-vault-1 13m	1/1	Running	0
polaris-vault-2 13m	1/1	Running	0
public-metrics-6cb7bfc49b-p54xm (8m29s ago) 9m31s	1/1	Running	1
storage-backend-metrics-5c77994586-kjn48 8m52s	1/1	Running	0
storage-provider-769fdc858c-62w54 8m54s	1/1	Running	0
task-service-9ffc484c5-kx9f4 (8m44s ago) 9m34s	1/1	Running	3
telegraf-ds-bphb9 6m54s	1/1	Running	0
telegraf-ds-rtsm2 6m54s	1/1	Running	0
telegraf-ds-s9h5h 6m54s	1/1	Running	0
telegraf-rs-lbpv7 6m54s	1/1	Running	0
telemetry-service-57cfb998db-zjx78 (8m40s ago) 9m26s	1/1	Running	1
tenancy-5d5dfbcf9f-vmboxh 9m5s	1/1	Running	0

traefik-7b87c4c474-jmcp2	1/1	Running	0
2m24s			
traefik-7b87c4c474-t9k8x	1/1	Running	0
2m24s			
trident-svc-c78f5b6bd-nwdsq	1/1	Running	0
9m22s			
vault-controller-55bbc96668-c6425	1/1	Running	0
11m			
vault-controller-55bbc96668-lq9n9	1/1	Running	0
11m			
vault-controller-55bbc96668-rfkkg	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 que se produzca un error de registro del clúster que se indica en los registros, puede volver a intentar realizar el registro a través de la ["Añada el flujo de trabajo del clúster 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 de configuración inicial que utilizará cuando inicie sesión en Astra Control Center:

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

Respuesta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	22.11.0-82	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 un controlador de entrada de Kubernetes que gestione el acceso externo a los servicios. Estos procedimientos proporcionan ejemplos de configuración para un controlador de entrada si utilizó el valor predeterminado de `ingressType: "Generic"` En el recurso personalizado Astra Control Center (`astra_control_center.yaml`). No es necesario utilizar este procedimiento si se ha especificado `ingressType: "AccTraefik"` En el recurso personalizado Astra Control Center (`astra_control_center.yaml`).

Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

Los pasos de configuración varían en función del tipo de controlador de entrada que utilice. Astra Control Center admite muchos tipos de controladores Ingress. Estos procedimientos de configuración ofrecen ejemplos de los siguientes tipos de controladores de entrada:

- 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.

## 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 tipo de recurso `v1` para un esquema (`istio-Ingress.yaml` se utiliza en este ejemplo):

```
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: [netapp-acc or custom namespace]
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. Aplicar los cambios:

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

6. Compruebe el estado de la entrada:

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



Respuesta:

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

## 7. Finalice la instalación de Astra Control Center.

### 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` espacio de nombres (o con nombre personalizado) mediante el tipo de recurso `v1` para un esquema (`nginx-Ingress.yaml` se utiliza en 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
```

## 3. Aplicar los cambios:

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



NetApp recomienda la instalación de la controladora nginx como una puesta en marcha en lugar de como una `daemonSet`.

## 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 navegador, introduzca el FQDN (incluido el `https://` prefijo) que utilizó en el `astraAddress` en la `astra_control_center.yaml` CR cuando [Ha instalado Astra Control Center](#).
2. Acepte los certificados autofirmados si se le solicita.



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.yaml` CR cuando [Ha instalado Astra Control Center](#), seguido de la contraseña de configuración inicial (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 éste es su primer inicio de sesión y olvida la contraseña y no se han creado otras cuentas de usuario administrativas, póngase en contacto con ["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:

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

## El futuro

- (Opcional) en función de su entorno, post-instalación completa "[pasos de configuración](#)".
- Complete la implementación llevando a cabo "[tareas de configuración](#)".

=

:allow-uri-read:

## Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

## Información de la marca comercial

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