



## **Añadir un clúster**

### **Astra Control Service**

NetApp  
April 24, 2024

# Tabla de contenidos

- Añada un clúster a Astra Control Service. . . . . 1
  - Instala Astra Connector para gestionar los clústeres. . . . . 1
  - Agregue un clúster gestionado por el proveedor . . . . . 7
  - Agregue un clúster autogestionado . . . . . 18

# Añada un clúster a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control. Esto te permite utilizar el servicio Astra Control para proteger tus aplicaciones en el clúster.

Según el tipo de clúster que deba añadir a Astra Control Service, deberá realizar distintos pasos para añadir el clúster.

- ["Añade un clúster público gestionado por proveedores a Astra Control Service"](#): Utilice estos pasos para agregar un clúster que tenga una dirección IP pública y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- ["Añada un clúster privado gestionado por un proveedor a Astra Control Service"](#): Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- ["Añade un clúster público autogestionado a Astra Control Service"](#): Utilice estos pasos para agregar un cluster que tenga una dirección IP pública y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.
- ["Añade un clúster privado autogestionado a Astra Control Service"](#): Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

## Instala Astra Connector para gestionar los clústeres

Astra Connector es el software que reside en sus clústeres gestionados y facilita la comunicación entre el clúster gestionado y Astra Control. En el caso de los clústeres que se gestionen mediante Astra Control Service, hay dos versiones disponibles de Astra Connector:

- **Versión anterior de Astra Connector:** ["Instala la versión anterior de Astra Connector"](#) En el clúster, si tiene pensado gestionar el clúster con flujos de trabajo no nativos de Kubernetes.
- [Vista previa técnica] **Conector Astra de Kubernetes declarativo:** ["Instala Astra Connector para clústeres gestionados con flujos de trabajo de Kubernetes declarativos"](#) En el clúster si tiene pensado gestionar el clúster mediante flujos de trabajo de Kubernetes declarativos. Después de instalar Astra Connector en tu clúster, el clúster se añade automáticamente a Astra Control.



El Astra Connector declarativo de Kubernetes solo está disponible como parte del programa para la primera adopción de Astra Control (EAP). Póngase en contacto con su representante de ventas de NetApp para obtener información sobre cómo unirse al EAP.

### Instala la versión anterior de Astra Connector

Astra Control Service utiliza la versión anterior de Astra Connector para permitir la comunicación entre Astra Control Service y clústeres privados que no son nativos de Kubernetes. Tienes que instalar Astra Connector en clústeres privados que quieras gestionar con flujos de trabajo que no sean nativos de Kubernetes.

La versión anterior de Astra Connector admite los siguientes tipos de clústeres privados gestionados con flujos de trabajo no nativos de Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service en AWS (ROSA)
- ROSA con AWS PrivateLink
- Red Hat OpenShift Container Platform en las instalaciones

#### Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster privado que desee administrar con Astra Control Service.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

#### Antes de empezar

- Necesita acceso al clúster privado que desea gestionar con Astra Control Service.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.

#### Pasos

1. Instale el operador Astra Connector anterior en el clúster privado que desea gestionar con flujos de trabajo que no sean nativos de Kubernetes. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/23.07.0-202310251519/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la ["Documentación de Astra Automation"](#) si desea obtener instrucciones.
4. Cree el espacio de nombres de Astra-Connector:

```
kubectl create ns astra-connector
```

5. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis `<>` para que coincidan con tu entorno de Astra Control y la configuración del clúster:
  - **<ASTRA\_CONTROL\_SERVICE\_URL>**: La URL de la interfaz de usuario web del servicio de control de Astra. Por ejemplo:

```
https://astra.netapp.io
```

- **<ASTRA\_CONTROL\_SERVICE\_API\_TOKEN>**: El token de la API Astra Control que obtuviste en el paso anterior.
- **<PRIVATE\_AKS\_CLUSTER\_NAME>**: (Solo clústeres de AKS): El nombre del clúster privado del servicio de Azure Kubernetes. Elimine el comentario y rellene esta línea sólo si está agregando un cluster AKS privado.
- **<ASTRA\_CONTROL\_ACCOUNT\_ID>**: Obtenido de la interfaz de usuario web de Astra Control. Selecciona el icono de la figura en la parte superior derecha de la página y selecciona **Acceso API**.

```
apiVersion: netapp.astraconnector.com/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  natssync-client:
    cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
  imageRegistry:
    name: theotw
    secret: ""
  astra:
    token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
    #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    acceptEULA: yes
```

6. Después de rellenar el `astra-connector-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-connector-cr.yaml
```

7. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

8. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnector -n astra-connector
```

Debería ver una salida similar a la siguiente:

NAME	REGISTERED	ASTRACONNECTORID
STATUS		
astra-connector	true	be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra		



Toma nota del ASTRACONNECTORID, lo necesitarás cuando añadas el clúster a Astra Control.

## El futuro

Ahora que ha instalado Astra Connector, está listo para añadir su clúster privado a Astra Control Service.

- ["Añada un clúster privado gestionado por un proveedor a Astra Control Service"](#): Utilice estos pasos para agregar un clúster que tenga una dirección IP privada y esté gestionado por un proveedor de cloud. Necesitará la cuenta principal de servicio, la cuenta de servicio o la cuenta de usuario del proveedor de cloud.
- ["Añade un clúster privado autogestionado a Astra Control Service"](#): Utilice estos pasos para agregar un cluster que tenga una dirección IP privada y que sea administrado por su organización. Deberá crear un archivo kubeconfig para el cluster que desea agregar.

## Si quiere más información

- ["Añadir un clúster"](#)

## (Vista previa técnica) Instale el Astra Connector declarativo de Kubernetes

Los clústeres gestionados mediante flujos de trabajo de Kubernetes declarativos utilizan Astra Connector para permitir la comunicación entre el clúster gestionado y Astra Control. Tienes que instalar Astra Connector en todos los clústeres que gestionarás con flujos de trabajo de Kubernetes declarativos.

Instalas el conector Astra de Kubernetes declarativo mediante comandos de Kubernetes y archivos de recursos personalizados (CR).

### Acerca de esta tarea

- Cuando realice estos pasos, ejecute estos comandos en el clúster que desee gestionar con Astra Control.
- Si utiliza un host de Bastion, emita estos comandos desde la línea de comandos del host de Bastion.

### Antes de empezar

- Necesitas acceder al clúster que quieras gestionar con Astra Control.
- Necesitas permisos de administrador de Kubernetes para instalar el operador Astra Connector en el clúster.



Si el clúster está configurado con la aplicación de admisión de seguridad de POD, que es el valor predeterminado para los clústeres de Kubernetes 1,25 y posteriores, tiene que habilitar las restricciones PSA en los espacios de nombres correspondientes. Consulte ["Prepare su entorno para la gestión de clústeres con Astra Control"](#) si desea obtener instrucciones.

## Pasos

1. Instale el operador Astra Connector en el clúster que desee gestionar con flujos de trabajo de Kubernetes declarativos. Cuando se ejecuta este comando, el espacio de nombres `astra-connector-operator` se crea y la configuración se aplica al espacio de nombres:

```
kubectl apply -f https://github.com/NetApp/astra-connector-operator/releases/download/24.02.0-202403151353/astraconnector_operator.yaml
```

2. Compruebe que el operador está instalado y listo:

```
kubectl get all -n astra-connector-operator
```

3. Obtén un token de API de Astra Control. Consulte la ["Documentación de Astra Automation"](#) si desea obtener instrucciones.
4. Cree un secreto con el token. Reemplaza `<API_TOKEN>` por el token que has recibido de Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crea un secreto de Docker para extraer la imagen de Astra Connector. Sustituya los valores entre paréntesis `<>` por información de su entorno:



Puedes encontrar la instancia de `<ASTRA_CONTROL_ACCOUNT_ID>` en la interfaz de usuario web de Astra Control. En la interfaz de usuario web, seleccione el icono de figura en la parte superior derecha de la página y seleccione **Acceso API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Cree el archivo Astra Connector CR y asígnele el nombre `astra-connector-cr.yaml`. Actualiza los valores entre paréntesis `<>` para que coincidan con tu entorno de Astra Control y la configuración del clúster:
  - `<ASTRA_CONTROL_ACCOUNT_ID>`: Obtenida de la interfaz de usuario web de Astra Control durante el paso anterior.
  - `<CLUSTER_NAME>`: El nombre que se debe asignar este clúster en Astra Control.
  - `<ASTRA_CONTROL_URL>`: La URL de interfaz de usuario web de Astra Control. Por ejemplo:

```
https://astra.control.url
```

```
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
    self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
    environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Después de rellenar el astra-connector-cr.yaml Con los valores correctos, aplique el CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Compruebe que Astra Connector está completamente implementado:

```
kubectl get all -n astra-connector
```

9. Compruebe que el clúster esté registrado en Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

Debería ver una salida similar a la siguiente:



NAMESPACE	NAME	REGISTERED	ASTRACONNECTORID
STATUS			
astra-connector	astra-connector	true	00ac8-2cef-41ac-8777-ed0583e
	Registered with Astra		

10. Compruebe que el clúster aparezca en la lista de clústeres gestionados de la página **Clusters** de la interfaz de usuario web de Astra Control.

## Agregue un clúster gestionado por el proveedor

### Añade un clúster público gestionado por proveedores a Astra Control Service

Después de configurar tu entorno de cloud, estarás listo para crear un clúster de Kubernetes y luego añadirlo a Astra Control Service.

- [Cree un clúster de Kubernetes](#)
- [Añada el clúster a Astra Control Service](#)
- [Cambie la clase de almacenamiento predeterminada](#)

#### Cree un clúster de Kubernetes

Si todavía no tiene un clúster, puede crear uno que cumpla "[Requisitos del servicio Astra Control para Amazon Elastic Kubernetes Service \(EKS\)](#)". Si todavía no tiene un clúster, puede crear uno que cumpla "[Requisitos del servicio Astra Control para Google Kubernetes Engine \(GKE\)](#)". Si todavía no tiene un clúster, puede crear uno que cumpla "[Requisitos del servicio Astra Control para Azure Kubernetes Service \(AKS\) con Azure NetApp Files](#)" o. "[Requisitos del servicio Astra Control Service para Azure Kubernetes Service \(AKS\) con discos gestionados de Azure](#)".



Astra Control Service es compatible con clústeres AKS que utilizan Azure Active Directory (Azure AD) para la autenticación y la gestión de identidades. Cuando cree el clúster, siga las instrucciones que se indican en "[documentación oficial](#)". Para configurar el clúster de modo que use Azure AD. Debe asegurarse de que sus clústeres cumplen los requisitos de la integración de Azure AD gestionada por AKS.

#### Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el

aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte ["Habilita el aprovisionador de Astra Control"](#) Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte ["Habilita el aprovisionador de Astra Control"](#) Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

## Antes de empezar

### Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. ["Aprenda a crear un usuario de IAM"](#).
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la ["Requisitos del clúster de EKS"](#).
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster ["¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?"](#).
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

### Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. ["Aprenda a configurar un director de servicios"](#).

También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

### Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. ["Aprenda a configurar una cuenta de servicio"](#).
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

## Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte ["Habilita el aprovisionador de Astra Control"](#) para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.

3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

Siga las instrucciones para añadir el clúster.

4. **Proveedor:** Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.
5. **Amazon Web Services:** Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure:** Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform:** Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros:** Esta pestaña es para uso solo con clusters autogestionados.

- a. **Nombre de la instancia de nube:** Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "[instancias de cloud](#)".

- b. Seleccione **Siguiente**.

Astra Control Service muestra una lista de clústeres entre los que puede elegir.

- c. **Clúster:** Selecciona un clúster de la lista para añadirlo a Astra Control Service.



Al seleccionar de la lista de clusters, preste atención a la columna **Eligibility**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

- d. Seleccione **Siguiente**.

- e. (Opcional) **Almacenamiento:** Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.

9. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
10. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:



- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Disco persistente de Google"](#)
  - ["Azure NetApp Files"](#)
  - ["Discos gestionados de Azure"](#)
  - ["Amazon Elastic Block Store"](#)
  - ["Amazon FSX para ONTAP de NetApp"](#)
  - ["Cloud Volumes ONTAP de NetApp"](#)

Más información acerca de ["Clases de almacenamiento para clústeres de Amazon Web Services"](#).  
Más información acerca de ["Clases de almacenamiento para clústeres de AKS"](#). Más información acerca de ["Clases de almacenamiento para clústeres GKE"](#).

- Seleccione **Siguiente**.
- Revisar y aprobar**: Revise los detalles de la configuración.
- Selecciona **Add** para agregar el clúster a Astra Control Service.

## Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

## Cambie la clase de almacenamiento predeterminada

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

## Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede [Cambie la clase de almacenamiento predeterminada con la línea de comandos](#).

### Pasos

1. En la interfaz de usuario de Astra Control Service, 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**.

## Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

### Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-  
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

## Añada un clúster privado gestionado por un proveedor a Astra Control Service

Puede utilizar Astra Control Service para gestionar clústeres privados de Google Kubernetes Engine (GKE). En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- ["Documentación de Azure para clústeres AKS privados"](#)
- ["Documentación de Azure para clústeres de OpenShift privados"](#)

Puede utilizar Astra Control Service para gestionar clústeres privados de Azure Kubernetes Service (AKS) y clústeres privados de Red Hat OpenShift en AKS. En estas instrucciones se asume que ya ha creado un clúster privado de AKS o OpenShift y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres privados de AKS o OpenShift, consulte la siguiente documentación:

- ["Documentación de Azure para clústeres AKS privados"](#)
- ["Documentación de Azure para clústeres de OpenShift privados"](#)

Puede utilizar Astra Control Service para gestionar clústeres privados de Amazon Elastic Kubernetes Service (EKS). En estas instrucciones se asume que ya ha creado un clúster EKS privado y preparado un método seguro para acceder de forma remota; para obtener más información sobre la creación y el acceso a clústeres EKS privados, consulte la ["Documentación de Amazon EKS"](#).

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. [Instala Astra Connector](#)
2. [Configure el almacenamiento persistente](#)
3. [Añada el clúster gestionado por proveedores privados a Astra Control Service](#)

### Instala Astra Connector

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte ["Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes"](#) si desea obtener instrucciones.

### Configure el almacenamiento persistente

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- ["Configure Microsoft Azure con Azure NetApp Files"](#)
- ["Configure Microsoft Azure con discos gestionados de Azure"](#)
- ["Configure Amazon Web Services"](#)
- ["Configure Google Cloud"](#)

### Añada el clúster gestionado por proveedores privados a Astra Control Service

Ahora puede añadir el clúster privado a Astra Control Service.

Al gestionar clústeres de Azure Kubernetes Service y Google Kubernetes Engine, tenga en cuenta que tiene dos opciones para la instalación del aprovisionador de Astra Control y la gestión del ciclo de vida:

- Puedes utilizar el servicio Astra Control para gestionar automáticamente el ciclo de vida del aprovisionador Astra Control. Para hacerlo, asegúrese de que Astra Trident no esté instalado y que Astra Control Provisioner no esté habilitado en el clúster que desee gestionar con Astra Control Service. En este caso, Astra Control Service habilita automáticamente Astra Control Provisioning cuando se comienza a gestionar el clúster, y las actualizaciones del aprovisionador de Astra Control se realizan automáticamente.
- Puede gestionar el ciclo de vida de Astra Control Provisionador tú mismo. Para ello, habilite el aprovisionador de Astra Control en el clúster antes de gestionar el clúster con Astra Control Service. En este caso, Astra Control Service detecta que Astra Control Provisioning ya está habilitado y no lo reinstala ni gestiona las actualizaciones del aprovisionador de Astra Control. Consulte ["Habilita el aprovisionador de Astra Control"](#) Para seguir los pasos, habilita el aprovisionador de Astra Control.

Al gestionar clústeres de Amazon Web Services con Astra Control Service, si necesita back-ends de almacenamiento que solo puede utilizarse con el aprovisionador de Astra Control, tendrá que habilitar el aprovisionador de Astra Control manualmente en el clúster antes de gestionarlo con el servicio de Astra Control. Consulte ["Habilita el aprovisionador de Astra Control"](#) Para conocer los pasos que hay que seguir para habilitar el aprovisionador de Astra Control.

## Antes de empezar

### Amazon Web Services

- Debe tener el archivo JSON que contenga las credenciales del usuario de IAM que creó el clúster. ["Aprenda a crear un usuario de IAM"](#).
- Se requiere el aprovisionador de Astra Control para Amazon FSx para NetApp ONTAP. Si tienes pensado usar Amazon FSx para NetApp ONTAP como back-end de almacenamiento para tu clúster de EKS, consulte la información del aprovisionador de control de Astra en la ["Requisitos del clúster de EKS"](#).
- (Opcional) Si necesita proporcionarlo `kubectl` Consulte las instrucciones de la sección para obtener acceso al comando de un clúster a otros usuarios de IAM que no son el creador del clúster ["¿Cómo puedo proporcionar acceso a otros usuarios de IAM y a otras funciones tras la creación del clúster en Amazon EKS?"](#).
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Amazon Web Services. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

### Microsoft Azure

- Debe tener el archivo JSON que contenga el resultado de la CLI de Azure cuando cree el principal del servicio. ["Aprenda a configurar un director de servicios"](#).

También necesitará su ID de suscripción de Azure si no lo ha añadido al archivo JSON.

- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Microsoft Azure. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

### Google Cloud

- Debe tener el archivo de clave de cuenta de servicio para una cuenta de servicio que tenga los permisos necesarios. ["Aprenda a configurar una cuenta de servicio"](#).
- Si el clúster es privado, el ["redes autorizadas"](#) Debe permitir la dirección IP del servicio Astra Control:  
  
52.188.218.166/32
- Si tiene pensado utilizar Cloud Volumes ONTAP de NetApp como back-end de almacenamiento, debe configurar Cloud Volumes ONTAP para que funcione con Google Cloud. Consulte el Cloud Volumes ONTAP ["documentación de configuración"](#).

## Pasos

1. (Opcional) Si añade un clúster de Amazon EKS o desea gestionar la instalación y actualizaciones de Astra Control Provisionador, habilite Astra Control Provisionador en el clúster. Consulte ["Habilita el aprovisionador de Astra Control"](#) para pasos de habilitación.
2. Abra la interfaz de usuario web de Astra Control Service en un navegador.
3. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

Siga las instrucciones para añadir el clúster.

4. **Proveedor:** Seleccione su proveedor de cloud y, a continuación, proporcione las credenciales necesarias para crear una nueva instancia de cloud, o seleccione una instancia de cloud existente para utilizar.



5. **Amazon Web Services:** Proporcione detalles sobre su cuenta de usuario de Amazon Web Services IAM cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

El archivo JSON debe contener las credenciales del usuario IAM que creó el clúster.

6. **Microsoft Azure:** Proporcione detalles sobre el principal de servicio de Azure cargando un archivo JSON o pegando el contenido de ese archivo JSON desde el portapapeles.

El archivo JSON debe contener el resultado de la CLI de Azure al crear el principal del servicio. También puede incluir su ID de suscripción para que se agregue automáticamente a Astra. De lo contrario, deberá introducir manualmente el ID después de proporcionar JSON.

7. **Google Cloud Platform:** Proporcione el archivo de clave de cuenta de servicio cargando el archivo o pegando el contenido del portapapeles.

Astra Control Service utiliza la cuenta de servicio para descubrir los clústeres que se ejecutan en Google Kubernetes Engine.

8. **Otros:** Esta pestaña es para uso solo con clusters autogestionados.

- a. **Nombre de la instancia de nube:** Proporcione un nombre para la nueva instancia de nube que se creará al agregar este clúster. Más información acerca de "[instancias de cloud](#)".

- b. Seleccione **Siguiente**.

Astra Control Service muestra una lista de clústeres entre los que puede elegir.

- c. **Clúster:** Selecciona un clúster de la lista para añadirlo a Astra Control Service.



Al seleccionar de la lista de clusters, preste atención a la columna **Eligibility**. Si un clúster es «no elegible» o «parcialmente elegible», pase el cursor por encima del estado para determinar si hay un problema con el clúster. Por ejemplo, podría identificar que el clúster no tiene un nodo de trabajo.

9. Seleccione **Siguiente**.

10. (Opcional) **Almacenamiento:** Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.

- a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.

- b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:



- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Disco persistente de Google"](#)
- ["Azure NetApp Files"](#)
- ["Discos gestionados de Azure"](#)
- ["Amazon Elastic Block Store"](#)
- ["Amazon FSX para ONTAP de NetApp"](#)
- ["Cloud Volumes ONTAP de NetApp"](#)

Más información acerca de ["Clases de almacenamiento para clústeres de Amazon Web Services"](#).  
Más información acerca de ["Clases de almacenamiento para clústeres de AKS"](#). Más información acerca de ["Clases de almacenamiento para clústeres GKE"](#).

- c. Seleccione **Siguiente**.
- d. **Revisar y aprobar**: Revise los detalles de la configuración.
- e. Selecciona **Add** para agregar el clúster a Astra Control Service.

## Resultado

Si este es el primer clúster que se ha añadido para este proveedor de cloud, Astra Control Service crea un almacén de objetos para el proveedor de cloud para realizar backups de las aplicaciones que se ejecutan en clústeres aptos. (Cuando añada clústeres posteriores para este proveedor de cloud, no se crearán más almacenes de objetos). Si ha especificado una clase de almacenamiento predeterminada, Astra Control Service establece la clase de almacenamiento predeterminada que ha especificado. En el caso de clústeres gestionados en Amazon Web Services o Google Cloud Platform, Astra Control Service también crea una cuenta de administrador en el clúster. Estas acciones pueden tardar varios minutos.

## Cambie la clase de almacenamiento predeterminada

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

## Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede [Cambie la clase de almacenamiento predeterminada con la línea de comandos](#).

### Pasos

1. En la interfaz de usuario de Astra Control Service, 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**.

## Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

### Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata": {"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

# Agregue un clúster autogestionado

## Añade un clúster público autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

### Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres públicos autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14

En estas instrucciones se asume que ya ha creado un clúster autogestionado.

- [Añada el clúster a Astra Control Service](#)
- [Cambie la clase de almacenamiento predeterminada](#)

### Añada el clúster a Astra Control Service

Después de iniciar sesión en Astra Control Service, el primer paso es empezar a gestionar los clústeres. Antes de añadir un clúster al servicio Astra Control Service, tendrá que realizar tareas específicas y asegurarse de que el clúster cumple determinados requisitos.

## Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga ["estas instrucciones"](#) para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

```
insecure-skip-tls-verify: true
```

- **Sólo rancher:** Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig 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.
- **Requisitos del aprovisionador de Astra Control:** Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident:** Antes de instalar o actualizar el aprovisionador de Astra Control, revise el ["compatibles con front-ends, back-ends y configuraciones de host"](#).
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control:** Se recomienda instalar Astra Trident 23,10 o posterior y activar ["Funcionalidad de almacenamiento avanzada de Astra Control Provisioning"](#). En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento:** Al menos un backend de almacenamiento debe ser ["Configuradas en Astra Trident"](#) en el clúster.
  - **Configure una clase de almacenamiento:** Al menos una clase de almacenamiento debe ser ["Configuradas en Astra Trident"](#) en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen:** "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

## Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

Siga las instrucciones para añadir el clúster.

2. **Proveedor:** Seleccione la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.

- a. **Otros:** Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.



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.

3. **Nombre de credencial:** Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
4. **Identificador de ruta privado:** Este campo es solo para uso con clusters privados.
5. Seleccione **Siguiente**.
6. (Opcional) **Almacenamiento:** Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
  - a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
  - b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.



Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:

- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Disco persistente de Google"](#)
  - ["Azure NetApp Files"](#)
  - ["Discos gestionados de Azure"](#)
  - ["Amazon Elastic Block Store"](#)
  - ["Amazon FSX para ONTAP de NetApp"](#)
  - ["Cloud Volumes ONTAP de NetApp"](#)

Más información acerca de ["Clases de almacenamiento para clústeres de Amazon Web Services"](#). Más información acerca de ["Clases de almacenamiento para clústeres de AKS"](#). Más información acerca de ["Clases de almacenamiento para clústeres GKE"](#).

- c. Seleccione **Siguiente**.
- d. **Revisar y aprobar**: Revise los detalles de la configuración.
- e. Selecciona **Add** para agregar el clúster a Astra Control Service.

## Cambie la clase de almacenamiento predeterminada

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

### Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede [Cambie la clase de almacenamiento predeterminada con la línea de comandos](#).

#### Pasos

1. En la interfaz de usuario de Astra Control Service, 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**.

### Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

#### Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-  
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

## Añade un clúster privado autogestionado a Astra Control Service

Una vez configurado su entorno, estará listo para crear un clúster de Kubernetes y, a continuación, añadirlo al servicio Astra Control.

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Puede agregar un clúster autogestionado a Astra Control Service cargando un `kubeconfig.yaml` archivo. Deberá asegurarse de que el clúster cumple los requisitos que se indican aquí.

### Distribuciones de Kubernetes compatibles

Puede utilizar Astra Control Service para gestionar los siguientes tipos de clústeres privados autogestionados:

Distribución de Kubernetes	Versiones compatibles
Kubernetes (ascendente)	1,27 a 1,29
Motor Kubernetes de rancher (RKE)	RKE 1: Versiones 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versiones 1.23.16 y 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versiones 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
OpenShift Container Platform de Red Hat	4,12 hasta 4,14



En estas instrucciones se asume que ya ha creado un clúster privado y ha preparado un método seguro para acceder de forma remota a él.

Tienes que realizar las siguientes tareas para añadir tu clúster privado a Astra Control Service:

1. [Instala Astra Connector](#)
2. [Configure el almacenamiento persistente](#)
3. [Añada el clúster autogestionado privado a Astra Control Service](#)

### **Instala Astra Connector**

Antes de agregar un clúster privado, tiene que instalar Astra Connector en el clúster para que Astra Control se pueda comunicar con él. Consulte ["Instala la versión anterior de Astra Connector para clústeres privados gestionados con flujos de trabajo que no sean nativos de Kubernetes"](#) si desea obtener instrucciones.

### **Configure el almacenamiento persistente**

Configure el almacenamiento persistente para el clúster. Consulte la documentación para empezar para obtener más información sobre la configuración del almacenamiento persistente:

- ["Configure Microsoft Azure con Azure NetApp Files"](#)
- ["Configure Microsoft Azure con discos gestionados de Azure"](#)
- ["Configure Amazon Web Services"](#)
- ["Configure Google Cloud"](#)

### **Añada el clúster autogestionado privado a Astra Control Service**

Ahora puede añadir el clúster privado a Astra Control Service.

## Antes de empezar

Un clúster autogestionado es un clúster que usted aprovisiona y gestiona directamente. Astra Control Service admite clústeres autogestionados que se ejecutan en un entorno de cloud público. Los clústeres autogestionados pueden utilizar Astra Control Provisioner para interactuar con los servicios de almacenamiento de NetApp o pueden usar controladores de la interfaz de almacenamiento de contenedores (CSI) para interactuar con Amazon Elastic Block Store (EBS), los discos gestionados de Azure y el disco persistente de Google.

Astra Control Service es compatible con clústeres autogestionados que utilizan las siguientes distribuciones de Kubernetes:

- OpenShift Container Platform de Red Hat
- Motor Kubernetes del rancher
- Subida de Kubernetes

Su clúster autogestionado debe cumplir con los siguientes requisitos:

- El clúster debe estar accesible a través de Internet.
- Si está utilizando o planea utilizar almacenamiento habilitado con controladores CSI, se deben instalar los controladores CSI adecuados en el clúster. Para obtener más información sobre el uso de los controladores CSI para integrar el almacenamiento, consulte la documentación del servicio de almacenamiento.
- Tiene acceso al archivo kubeconfig de cluster que incluye solo un elemento de contexto. Siga ["estas instrucciones"](#) para generar un archivo kubeconfig.
- Si va a agregar el clúster mediante un archivo kubeconfig que hace referencia a una entidad de certificación (CA) privada, agregue la siguiente línea al `cluster` sección del archivo kubeconfig. Esto permite a Astra Control añadir el clúster:

```
insecure-skip-tls-verify: true
```

- **Sólo rancher:** Al administrar clústeres de aplicaciones en un entorno Rancher, modifique el contexto predeterminado del clúster de aplicaciones en el archivo kubeconfig 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.
- **Requisitos del aprovisionador de Astra Control:** Debes tener un aprovisionador de Astra Control configurado correctamente, incluidos sus componentes de Astra Trident, para gestionar clústeres.
  - **Revise los requisitos del entorno de Astra Trident:** Antes de instalar o actualizar el aprovisionador de Astra Control, revise el ["compatibles con front-ends, back-ends y configuraciones de host"](#).
  - **Habilitar la funcionalidad de aprovisionamiento de Astra Control:** Se recomienda instalar Astra Trident 23,10 o posterior y activar ["Funcionalidad de almacenamiento avanzada de Astra Control Provisioning"](#). En las siguientes versiones, Astra Control no será compatible con Astra Trident si el aprovisionador de Astra Control también no está habilitado.
  - **Configurar un backend de almacenamiento:** Al menos un backend de almacenamiento debe ser ["Configuradas en Astra Trident"](#) en el clúster.
  - **Configure una clase de almacenamiento:** Al menos una clase de almacenamiento debe ser ["Configuradas en Astra Trident"](#) en el clúster. Si se configura una clase de almacenamiento

predeterminada, asegúrese de que es la clase de almacenamiento **Only** que tiene la anotación predeterminada.

- **Configure un controlador de instantáneas de volumen e instale una clase de instantáneas de volumen:** "Instale una controladora Snapshot de volumen" Para poder crear instantáneas en Astra Control. "Cree" al menos uno `VolumeSnapshotClass` Mediante Astra Trident.

## Pasos

1. En el Panel de control, seleccione **gestionar clúster Kubernetes**.

Siga las instrucciones para añadir el clúster.

2. **Proveedor:** Seleccione la pestaña **Otro** para agregar detalles sobre tu cluster autogestionado.
3. **Otros:** Proporcione detalles sobre su cluster autogestionado cargando un `kubeconfig.yaml` o bien, pegue el contenido de `kubeconfig.yaml` desde el portapapeles.



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

4. **Nombre de credencial:** Proporciona un nombre para la credencial de clúster autogestionada que estás cargando en Astra Control. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
5. **Identificador de ruta privado:** Introduce el identificador de ruta privado, que puedes obtener del Astra Connector. Si consulta el Astra Connector a través del `kubectl get astrconnector -n astrconnector` comando, el identificador de ruta privada se denomina `ASTRACONNECTORID`.



El identificador de ruta privada es el nombre asociado con Astra Connector que permite gestionar un clúster de Kubernetes privado con Astra. En este contexto, un clúster privado es un clúster de Kubernetes que no expone su servidor API a Internet.

6. Seleccione **Siguiente**.
7. (Opcional) **Almacenamiento:** Opcionalmente, seleccione la clase de almacenamiento que desea que las aplicaciones de Kubernetes implementadas en este clúster utilicen de forma predeterminada.
  - a. Para seleccionar una nueva clase de almacenamiento predeterminada para el clúster, active la casilla de verificación **Asignar una nueva clase de almacenamiento predeterminada**.
  - b. Seleccione una nueva clase de almacenamiento predeterminada de la lista.

Cada servicio de almacenamiento de proveedor de cloud muestra la siguiente información sobre el precio, el rendimiento y la resiliencia:



- Cloud Volumes Service para Google Cloud: Información de precio, rendimiento y resiliencia
- Google Persistent Disk: No hay información de precio, rendimiento ni resiliencia disponible
- Azure NetApp Files: Información sobre rendimiento y resiliencia
- Discos administrados de Azure: No hay información de precios, rendimiento ni resiliencia disponible
- Amazon Elastic Block Store: No dispone de información de precio, rendimiento o resiliencia
- Amazon FSX para ONTAP de NetApp: Sin información de precio, rendimiento ni resiliencia disponible
- Cloud Volumes ONTAP de NetApp: No hay información de precio, rendimiento ni resiliencia disponible

Cada clase de almacenamiento puede utilizar uno de los siguientes servicios:

- ["Cloud Volumes Service para Google Cloud"](#)
- ["Disco persistente de Google"](#)
- ["Azure NetApp Files"](#)
- ["Discos gestionados de Azure"](#)
- ["Amazon Elastic Block Store"](#)
- ["Amazon FSX para ONTAP de NetApp"](#)
- ["Cloud Volumes ONTAP de NetApp"](#)

Más información acerca de ["Clases de almacenamiento para clústeres de Amazon Web Services"](#).  
Más información acerca de ["Clases de almacenamiento para clústeres de AKS"](#). Más información acerca de ["Clases de almacenamiento para clústeres GKE"](#).

- c. Seleccione **Siguiente**.
- d. **Revisar y aprobar**: Revise los detalles de la configuración.
- e. Selecciona **Add** para agregar el clúster a Astra Control Service.

## Cambie la clase de almacenamiento predeterminada

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

### Cambie la clase de almacenamiento predeterminada con Astra Control

Puede cambiar la clase de almacenamiento predeterminada para un clúster de Astra Control. Si su clúster utiliza un servicio de fondo de almacenamiento previamente instalado, es posible que no pueda utilizar este método para cambiar la clase de almacenamiento predeterminada (la acción **establecer como predeterminada** no se puede seleccionar). En este caso, usted puede [Cambie la clase de almacenamiento predeterminada con la línea de comandos](#).

## Pasos

1. En la interfaz de usuario de Astra Control Service, 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**.

#### Cambie la clase de almacenamiento predeterminada con la línea de comandos

Es posible cambiar la clase de almacenamiento predeterminada para un clúster mediante comandos de Kubernetes. Este método funciona independientemente de la configuración del clúster.

#### Pasos

1. Inicie sesión en su clúster de Kubernetes.
2. Enumere las clases de almacenamiento del clúster:

```
kubectl get storageclass
```

3. Quite la designación predeterminada de la clase de almacenamiento predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-  
class":"false"}}}'
```

4. Seleccione una clase de almacenamiento diferente de forma predeterminada. Sustituya <SC\_NAME> por el nombre de la clase de almacenamiento:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":  
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confirme la nueva clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

## Comprueba la versión de Astra Trident

Para añadir un clúster autogestionado que utilice el proveedor de Astra Control o Astra Trident para los servicios de almacenamiento, asegúrese de que la versión instalada de Astra Trident sea la versión 23,10 o la más reciente.

#### Pasos

1. Determine la versión de Astra Trident que ejecuta:

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

Si Astra Trident está instalado, verá una salida similar a la siguiente:

NAME	VERSION
trident	24.02.0

Si Astra Trident no está instalado, verá una salida similar a la siguiente:

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

2. Debe realizar una de las siguientes acciones:

- Si utiliza Astra Trident 23,01 o una versión anterior, utilice estos ["instrucciones"](#) Para actualizar a una versión más reciente de Astra Trident antes de actualizar a Astra Control Provisioner. Puede hacerlo ["realice una actualización directa"](#) Para Astra Control Provisioner 24,02 si tu Astra Trident está en una ventana de cuatro versiones de la versión 24,02. Por ejemplo, puedes actualizar directamente de Astra Trident 23,04 a Astra Control Provisioner 24,02.
- Si utiliza Astra Trident 23,10 o una versión posterior, compruebe que el aprovisionador de Astra Control haya sido ["activado"](#). El aprovisionador de Astra Control no funcionará con versiones de Astra Control Center anteriores a la 23,10. ["Actualiza tu aprovisionador de Astra Control"](#) De modo que tiene la misma versión que Astra Control Center que vas a actualizar para acceder a la funcionalidad más reciente.

3. Asegúrese de que los pods estén ejecutando:

```
kubectl get pods -n trident
```

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

```
kubectl get sc
```

Respuesta de ejemplo:

NAME	PROVISIONER	AGE	RECLAIMPOLICY
VOLUMEBINDINGMODE	ALLOWVOLUMEEXPANSION		
ontap-gold (default)	csi.trident.netapp.io		Delete
Immediate	true	5d23h	

## Cree un archivo kubeconfig

Puede añadir un clúster a Astra Control Service mediante un archivo kubeconfig. En función del tipo de cluster que desee agregar, es posible que necesite crear manualmente un archivo kubeconfig para el cluster mediante pasos específicos.

- [Cree un archivo kubeconfig para los clústeres de Amazon EKS](#)
- [Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS \(ROSA\)](#)
- [Cree un archivo kubeconfig para otros tipos de clusters](#)

### Cree un archivo kubeconfig para los clústeres de Amazon EKS

Siga estas instrucciones para crear un archivo kubeconfig y un secreto de token permanente para los clústeres de Amazon EKS. Se necesita un secreto de token permanente para los clústeres alojados en EKS.

#### Pasos

1. Siga las instrucciones de la documentación de Amazon para generar un archivo kubeconfig:

["Creación o actualización de un archivo kubeconfig para un clúster de Amazon EKS"](#)

2. Cree una cuenta de servicio del siguiente modo:

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

Ajuste el nombre de la cuenta de servicio según sea necesario. El espacio de nombres `kube-system` es necesario para estos pasos. Si cambia aquí el nombre de la cuenta de servicio, debe aplicar los mismos cambios en los siguientes pasos.

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

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Aplicar la cuenta de servicio:

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

4. Cree un ClusterRoleBinding archivo llamado `astracontrol-clusterrolebinding.yaml`.

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

```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system

```

5. Aplique el enlace de roles del clúster:

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

6. Se ha llamado a crear un archivo secreto de token de cuenta de servicio astracontrol-secret.yaml.

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

```

apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
  type: kubernetes.io/service-account-token

```

7. Aplique el secreto de token:

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

8. Recupere el secreto de token:

```

kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d

```

9. Sustituya el user Sección del archivo kubeconfig de AWS EKS con el token, como se muestra en el



siguiente ejemplo:

```
user:
  token: k8s-aws-
  v1.aHR0cHM6Ly9zdHMudXMtd2VzdC0yLmFtYXpvcnF3cy5jb20vP0FjdGlrbj1HZXRDYWxsZ
  XJJZGVudGl0eSZWZXJzaW9uPTIwMTETMDYtMTUuWC1BbXotQWxnbn3JpdGhtPUFXUzQtSE1BQ
  y1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS01BM1JEWddkU0haWU9LSEQ2SyUyRjIwMjMwN
  DAzJTJGdXMtd2VzdC0yJTJGc3RzJTJGYXdzNF9yZXF1ZXN0JlgtQW16LURhdGU9MjAyMzA0M
  DNUMjA0MzQwWiZYLUFteilFeHBpcmVzPTYwJlgtQW16LVNpZ25lZEhlYWRLcnM9aG9zdCUzQ
  ngtazhzLWF3cy1pZCZYLUFteil1TaWduYXRlcuU9YjU4ZWM0NzdiM2NkZGYxNGRhNzU4MGI2Z
  WQ2ZyY2NzI2YWIwM2UyNThjMjRhNTJjNmVhNjc4MTRlNjJkOTg2Mg
```

## Cree un archivo kubeconfig para los clústeres de Red Hat OpenShift Service en AWS (ROSA)

Siga estas instrucciones para crear un archivo kubeconfig para clústeres de Red Hat OpenShift Service en AWS (ROSA).

## Pasos

1. Inicie sesión en el clúster ROSA.
2. Cree una cuenta de servicio:

```
oc create sa astracontrol-service-account
```

- ### 3. Añada un rol de clúster:

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-  
service-account
```

4. Con el siguiente ejemplo, cree un archivo de configuración secreto de cuenta de servicio:

**secret-astra-sa.yaml**

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Cree el secreto:

```
oc create -f secret-astra-sa.yaml
```

6. Edite la cuenta de servicio que ha creado y agregue el nombre secreto de la cuenta de servicio de Astra Control a secrets sección:

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

7. 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-dvfcd"},
{ "name": "secret-astracontrol-service-account"}
]
```

Los índices de cada elemento de la secrets la matriz comienza con 0. En el ejemplo anterior, el índice para astracontrol-service-account-dockercfg-dvfcd sería 0 y el índice para secret-astracontrol-service-account sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

8. 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.

**create-kubeconfig.sh**

```
# 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
```

9. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

## Cree un archivo kubeconfig para otros tipos de clusters

Siga estas instrucciones para crear un archivo kubeconfig de rol limitado o ampliado para Rancher, upstream Kubernetes y Red Hat OpenShift clusters.

Para los clústeres que se gestionan mediante kubeconfig, opcionalmente puede crear un rol de administrador de permisos limitado o de permisos ampliados para Astra Control Service.

Este procedimiento le ayuda a crear un kubeconfig independiente si cualquiera de los siguientes escenarios se aplica a su entorno:

- Deseas limitar los permisos de Astra Control a los clústeres que gestiona
- Usas varios contextos y no puedes usar el comando predeterminado de Astra Control configurado durante la instalación o un rol limitado con un solo contexto no funcionará en tu entorno

### Antes de empezar

Asegúrese de que tiene lo siguiente para el clúster que tiene intención de administrar antes de completar los pasos del procedimiento:

- A. "versión compatible" de kubectl está instalado.
- Acceso kubectl al clúster que pretendes añadir y gestionar mediante Astra Control Service



Para este procedimiento, no necesita acceso kubectl al clúster que ejecuta Astra Control Service.

- Una imagen de referencia activa para el clúster que pretende gestionar con derechos de administrador del clúster para el contexto activo

## Pasos

### 1. Cree una cuenta de servicio:

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

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

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

- b. Aplicar la cuenta de servicio:

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

### 2. Cree uno de los siguientes roles de clúster con permisos suficientes para que Astra Control gestione un clúster:

## Rol de clúster limitado

Este rol contiene los permisos mínimos necesarios para que Astra Control gestione un clúster:

- a. Cree un ClusterRole archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```

- horizontalpodautoscalers
- ingresses
- jobs
- namespaces
- networkpolicies
- persistentvolumeclaims
- poddisruptionbudgets
- pods
- podtemplates
- replicaset
- replicationcontrollers
- replicationcontrollers/scale
- rolebindings
- roles
- secrets
- serviceaccounts
- services
- statefulsets
- tridentmirrorrelationships
- tridentnapshotinfos
- volumesnapshots
- volumesnapshotcontents
verbs:
- delete

# Watch resources
# Necessary to monitor progress
- apiGroups:
  - ""
  resources:
  - pods
  - replicationcontrollers
  - replicationcontrollers/scale
  verbs:
  - watch

# Update resources
- apiGroups:
  - ""
  - build.openshift.io
  - image.openshift.io
  resources:
  - builds/details
  - replicationcontrollers
  - replicationcontrollers/scale
  - imagestreams/layers

```

```
- imagestreamtags
- imagetags
verbs:
- update
```

- b. (Solo para clústeres de OpenShift) Añada lo siguiente al final del `astra-admin-account.yaml` archivo:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

- c. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

### Rol del clúster ampliado

Este rol contiene permisos ampliados para que un clúster lo gestione Astra Control. Puedes usar este rol si utilizas varios contextos y no puedes utilizar el comando `kubeconfig` predeterminado de Astra Control configurado durante la instalación o un rol limitado con un único contexto no funcionará en tu entorno:



Lo siguiente `ClusterRole` Los pasos son un ejemplo general de Kubernetes. Consulte la documentación de la distribución de Kubernetes para obtener instrucciones específicas de su entorno.

- a. Cree un `ClusterRole` archivo llamado, por ejemplo, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```



```

apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'

```

b. Aplique el rol de clúster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Cree el enlace de rol de clúster para el rol del clúster a la cuenta de servicio:

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

```
<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: astra-admin-account
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default

```

b. Aplique el enlace de roles del clúster:

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

4. Crear y aplicar el secreto de token:

- a. Cree un archivo secreto de token llamado `secret-astracontrol-service-account.yaml`.

```
<strong>secret-astracontrol-service-account.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

- b. Aplique el secreto de token:

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

5. Agregue el secreto de token a la cuenta de servicio agregando su nombre a la `secrets` array (la última línea del siguiente ejemplo):

```
kubectl edit sa astracontrol-service-account
```

```

apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>

```

6. 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-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]

```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-48xhx` sería 0 y el índice para `secret-astracontrol-service-account` sería 1. En la salida, anote el número de índice del secreto de la cuenta de servicio. Necesitará este número de índice en el siguiente paso.

7. 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
```

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

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

8. (Opcional) cambie el nombre de la Marca de prestigio por un nombre significativo para el clúster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

## 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 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.