Configure Astra Control Center

Astra Control Center

NetApp
June 07, 2024

Tabla de contenidos

Configure Astra Control Center

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

Tareas

- Agregue una licencia de Astra Control Center
- Añada el clúster
- Añada un back-end de almacenamiento
- Añadir un bucket

Agregue una licencia de Astra Control Center

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

Para obtener más información sobre cómo se calculan las licencias, consulte "Licencia".

> Para actualizar una evaluación existente o una licencia completa, consulte "Actualizar una licencia existente".

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

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

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

Lo que necesitará

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

Pasos

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

La página **cuenta** > **Licencia** muestra la información de la licencia, la fecha de caducidad, el número de serie

de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

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

Añada el clúster

Para comenzar a gestionar las aplicaciones, añada un clúster de Kubernetes y gestiónelo como un recurso de computación. Es necesario añadir un clúster para Astra Control Center para descubrir sus aplicaciones Kubernetes. Para Astra Data Store, queremos añadir el clúster de aplicaciones Kubernetes que contiene aplicaciones que utilizan volúmenes aprovisionados por Astra Data Store.

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

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

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

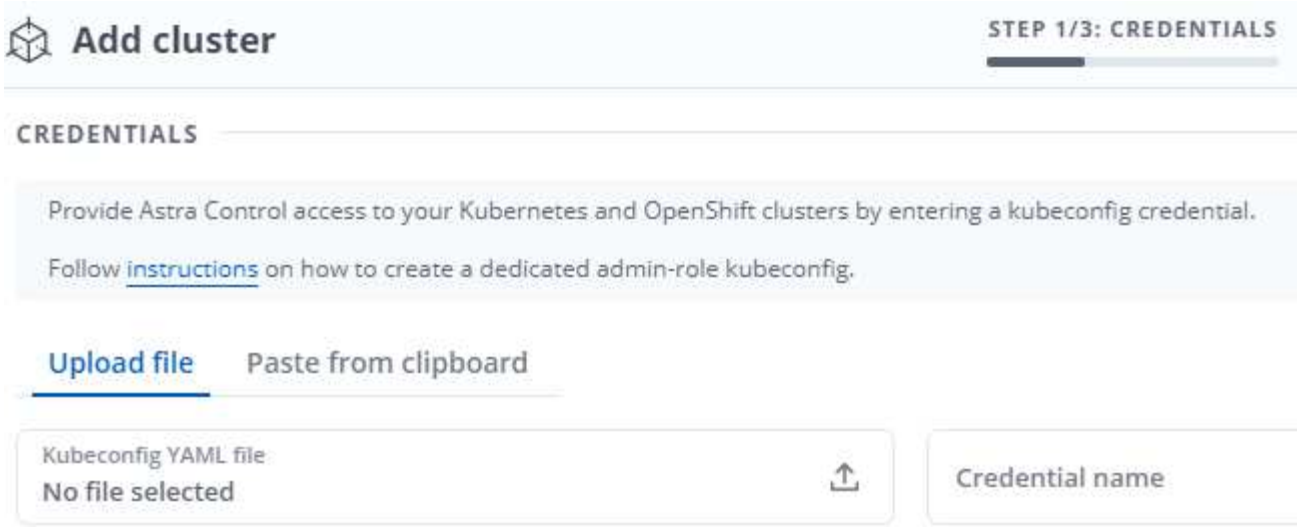
Lo que necesitará

- Antes de añadir un clúster, revise y realice la operación necesaria "requisitos previos".

Pasos

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

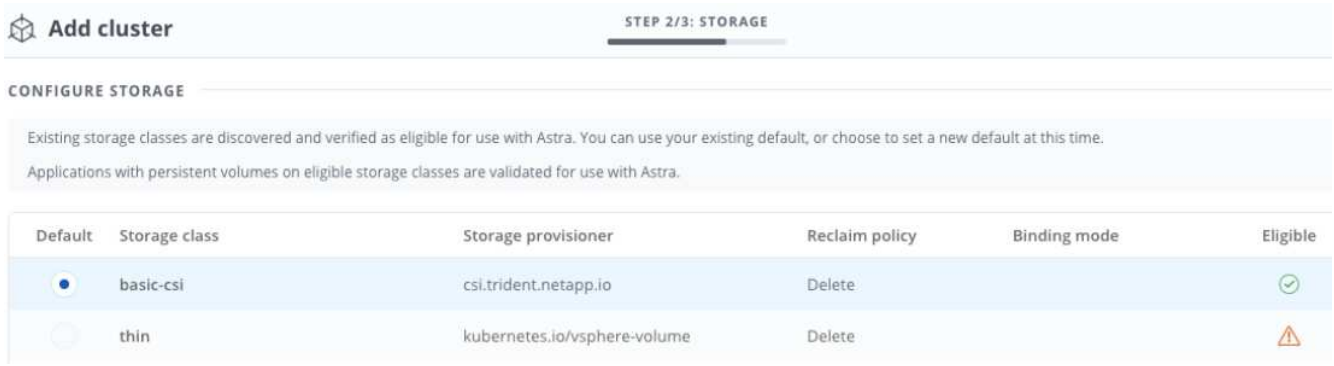
   La `kubeconfig.yaml` el archivo debe incluir **sólo la credencial de cluster para un cluster**.



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

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



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

Resultado

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

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

Añada un back-end de almacenamiento

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

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

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

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

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

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

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

Opciones

- Instale recursos de almacenamiento
- Utilice un back-end de almacenamiento existente

Instale recursos de almacenamiento

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

Pasos

1. Navegue desde el panel o el menú backends (backends):
    - En **Dashboard**: En el Resumen de recursos, seleccione un enlace del panel Storage Backends y seleccione **Add** en la sección Backends.

- Desde **Backends**:
  i. En el área de navegación de la izquierda, seleccione **Backends**.
  ii. Seleccione **Agregar**.

2. Seleccione la opción de implementación **Astra Data Store** en la ficha **despliegue**.
3. Seleccione el paquete Astra Data Store para implementar:
   a. Introduzca un nombre para la aplicación Astra Data Store.
   b. Elija la versión de Astra Data Store que desea implementar.

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

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

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

5. Si no ha añadido un clúster Kubernetes a Astra Control Management, debe hacerlo desde la página **Kubernetes Cluster**. Seleccione un clúster existente de la lista o seleccione **agregue el clúster subyacente** para agregar un clúster a Astra Control Management.
6. Seleccione el tamaño de la plantilla de implementación para el clúster de Kubernetes que proporcionará recursos para el almacén de datos Astra.

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

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

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

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

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

9. Configure la red de administración:
   a. Introduzca una dirección IP de gestión para la gestión interna de Astra Data Store que se encuentra en la misma subred que las direcciones IP de nodos de trabajo.
   b. Elija utilizar el mismo NIC tanto para la administración como para las redes de datos o configúrelo por separado.
   c. Introduzca el pool de direcciones IP de red de datos, la máscara de subred y la puerta de enlace para acceder al almacenamiento.
10. Revise la configuración y seleccione **despliegue** para comenzar la instalación.

Resultado

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

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

Utilice un back-end de almacenamiento existente

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

Pasos

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

Resultado

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

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

Añadir un bucket

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

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

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

Utilice cualquiera de los siguientes tipos de bloques:

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

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

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

Pasos

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

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

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

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

   d. Introduzca el nombre o la dirección IP del extremo de S3.
   e. Si desea que este bloque sea el bloque predeterminado para todos los backups, compruebe la `Make`

`this bucket the default bucket for this private cloud` opción.

> Esta opción no aparece para el primer bloque que cree.

f. Continúe añadiendo información sobre credenciales.

Añada credenciales de acceso de S3

Añada credenciales de acceso de S3 en cualquier momento.

Pasos

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

Cambie la clase de almacenamiento predeterminada

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

Pasos

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

El futuro

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

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

Obtenga más información

- "Utilice la API Astra Control"
- "Problemas conocidos"

Requisitos previos para añadir un clúster

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

Qué necesitará antes de añadir un clúster

- Uno de los siguientes tipos de clústeres:
  - Clústeres que ejecutan OpenShift 4.6.8, 4.7, 4.8 o 4.9
  - Clústeres que ejecutan Rancher 2.5.8, 2.5.9 o 2.6 con RKE1
  - Clústeres que ejecutan Kubernetes 1.20 a 1.23
  - Clústeres que ejecutan VMware Tanzania Kubernetes Grid 1.4
  - Clústeres que ejecutan VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2

    Asegúrese de que los clústeres tienen uno o más nodos de trabajo con al menos 1 GB de RAM disponibles para ejecutar los servicios de telemetría.

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

- Clases de almacenamiento de Astra Trident configuradas con un "back-end de almacenamiento admitido" (necesario para cualquier tipo de clúster)
- El superusuario y el ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center. Ejecute el siguiente comando en la línea de comandos de la ONTAP:
  `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`
- Una Astra Trident `volumesnapshotclass` objeto definido por un administrador. Vea la Astra Trident "instrucciones" Para habilitar y probar Volume Snapshots con Astra Trident.
- Compruebe que solo tiene una única clase de almacenamiento predeterminada definida para el clúster de Kubernetes.

Ejecutar las comprobaciones de elegibilidad

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

Pasos

1. Compruebe la versión de Trident.

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

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

```
NAME      VERSION
trident   21.04.0
```

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

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

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

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

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

Cree una imagen de rol administrativo

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

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

Pasos

1. Cree una cuenta de servicio del siguiente modo:

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

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

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

+

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

a. Aplicar la cuenta de servicio:

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

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

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

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

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

+

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

a. Aplique el enlace de roles del clúster:

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

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

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

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

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

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

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

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

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

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

CONTEXT=$(kubectl config current-context)

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

```
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

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

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

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

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

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

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

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

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

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

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

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

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

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

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

El futuro

Ahora que ha comprobado que se cumplen los requisitos previos, está listo "añadir un clúster".

Obtenga más información

- "Documentación de Trident"
- "Utilice la API Astra Control"

Agregue un certificado TLS personalizado

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

Lo que necesitará

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

Quite el certificado autofirmado

Quite el certificado TLS autofirmado existente.

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

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

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

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

Añadir un nuevo certificado

Añada un nuevo certificado TLS firmado por una CA.

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

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

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

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

#spec:
#  selfSigned: {}

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

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

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

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

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

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

5. Cree el certificado con el comando siguiente:

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

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

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

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

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

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

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

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

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

Cree una directiva de seguridad de POD personalizada

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

Pasos

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

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

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

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

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

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