Utilice Astra

Astra Control Center

NetApp
June 06, 2024

Tabla de contenidos

Utilice Astra

Gestionar aplicaciones

Inicie la gestión de aplicaciones

Usted primero "Añada un clúster a la gestión de Astra Control", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para empezar a gestionar las aplicaciones y sus recursos.

Requisitos de gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencia**: Para gestionar aplicaciones mediante Astra Control Center, necesita una licencia Astra Control Center.
- **Namespaces**: Astra Control requiere que una aplicación no abarque más de un único espacio de nombres, pero un espacio de nombres puede contener más de una aplicación.
- **StorageClass**: Si instala una aplicación con un StorageClass definido explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonado debe tener el StorageClass especificado originalmente. Se producirá un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo de almacenamiento.
- **Recursos de Kubernetes**: Las aplicaciones que utilizan los recursos de Kubernetes no recopilados por Astra Control pueden no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:
  - Función de clúster
  - ClusterRoleBinding
  - ConfigMap
  - CustomResourceDefinition
  - Recurso personalizado
  - DemonSet
  - Puesta en marcha
  - DeploymentConfig
  - Entrada
  - MutatingWebhook
  - Claim persistente
  - Pod
  - Replicaset
  - RoleBinding
  - Función
  - Ruta
  - Secreto
  - Servicio

- ServiceAccount
- Statilusionados Set
- ValidadoWebhook

Métodos de instalación de aplicaciones compatibles

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

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

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

- **Helm 3**: Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. La gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador**: Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres. Estos operadores están diseñados generalmente con una arquitectura "pasada por valor" en lugar de "pasada por referencia". Las siguientes son algunas aplicaciones del operador que siguen estos patrones:
  - "Apache K8ssandra"
  - "Jenkins CI"
  - "Clúster Percona XtraDB"

Tenga en cuenta que Astra Control podría no ser capaz de clonar a un operador diseñado con una arquitectura de "paso por referencia" (por ejemplo, el operador CockroachDB). Durante estos tipos de operaciones de clonado, el operador clonado intenta hacer referencia a los secretos de Kubernetes del operador de origen a pesar de tener su propio secreto nuevo como parte del proceso de clonado. Es posible que se produzca un error en la operación de clonado porque Astra Control no conoce los secretos de Kubernetes en el operador de origen.

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

Instale las aplicaciones en el clúster

Ahora que ha agregado su clúster a Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Se puede gestionar cualquier aplicación que esté delimita a un espacio de nombres. Una vez que las POD estén en línea, puede gestionar la aplicación con Astra Control.

Para obtener ayuda sobre la puesta en marcha de aplicaciones validadas de los gráficos Helm, consulte lo siguiente:

- "Desplegar MariaDB desde un gráfico Helm"
- "Implemente MySQL desde un gráfico Helm"
- "Despliegue Postgres desde un gráfico de Helm"
- "Implemente Jenkins a partir de un gráfico Helm"

Gestionar aplicaciones

Astra Control le permite gestionar sus aplicaciones a nivel de espacio de nombres o mediante etiqueta de Kubernetes.

Las aplicaciones instaladas con Helm 2 no son compatibles.

Puede realizar las siguientes actividades para gestionar aplicaciones:

- Gestionar aplicaciones
  - Gestionar aplicaciones por espacio de nombres
  - Gestione aplicaciones mediante la etiqueta Kubernetes
- Ignorar aplicaciones
- Desgestionar aplicaciones

Astra Control en sí no es una aplicación estándar; es una "aplicación del sistema". No debe intentar gestionar Astra Control por sí mismo. Astra Control no se muestra de forma predeterminada para la gestión. Para ver las aplicaciones del sistema, utilice el filtro “Mostrar aplicaciones del sistema”.

Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte "Información sobre API y automatización de Astra".

Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Gestionar aplicaciones por espacio de nombres

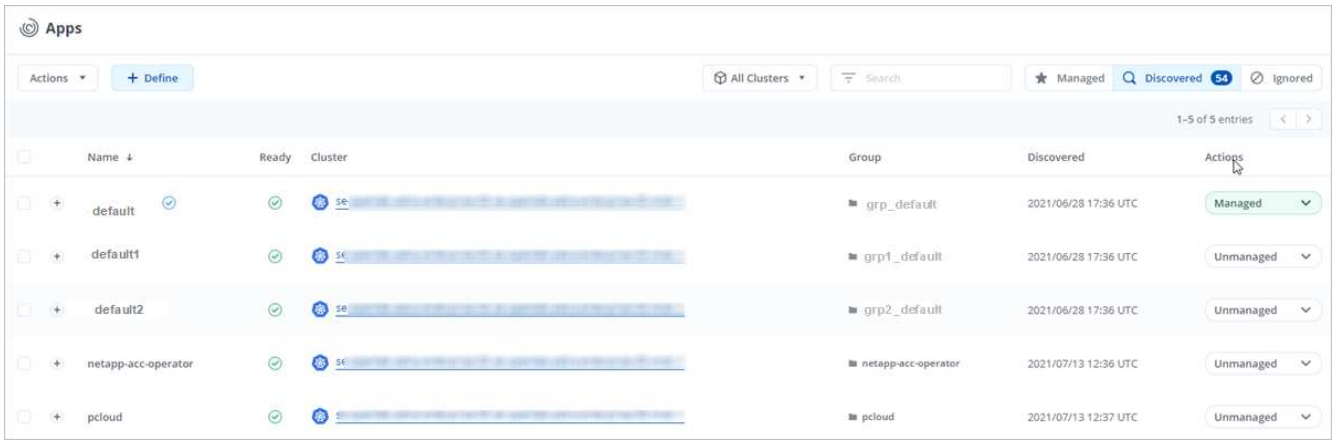
La sección **descubierto** de la página aplicaciones muestra espacios de nombres y cualquier aplicación instalada en Helm o aplicaciones personalizadas etiquetadas en esos espacios de nombres. Puede optar por gestionar cada aplicación por separado o a nivel de espacio de nombres. Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Por ejemplo, puede que desee configurar una normativa de backup para «maria» con una cadencia semanal, pero es posible que deba realizar backups de «mariadb» (que se encuentra en el mismo espacio de nombres) con mayor frecuencia que esta. Según estas necesidades, debería gestionar las aplicaciones por separado, no en un solo espacio de nombres.

Mientras que Astra Control permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones de ese espacio de nombres), la mejor práctica es elegir uno u otro. Las acciones que realice en Astra Control pueden fallar si las acciones se llevan a cabo al mismo tiempo tanto en el espacio de nombres como en el nivel de la aplicación.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **descubierto**.



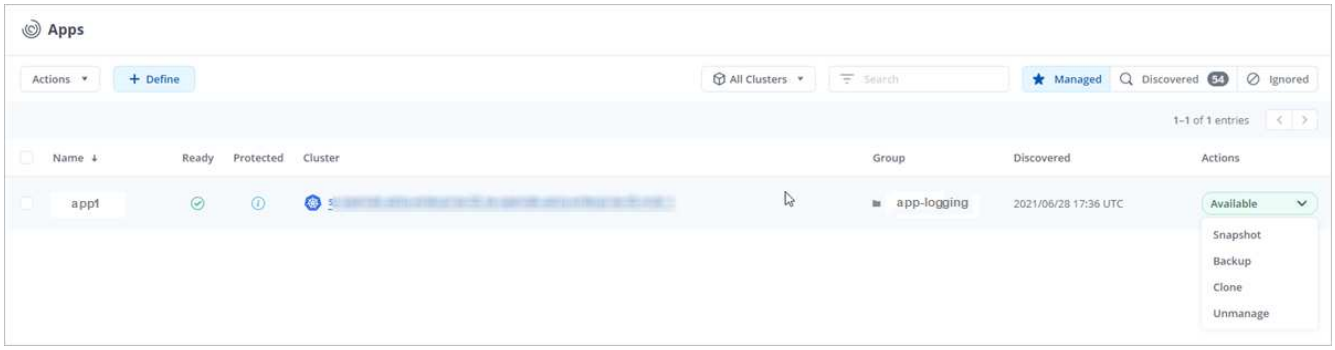
3. Consulte la lista de espacios de nombres detectados. Amplíe el espacio de nombres para ver las aplicaciones y los recursos asociados.

   Astra Control le muestra las aplicaciones Helm y las aplicaciones personalizadas en el espacio de nombres. Si hay etiquetas Helm disponibles, se designarán con un icono de etiqueta.

4. Observe la columna **Grupo** para ver en qué espacio de nombres se está ejecutando la aplicación (está designada con el icono de carpeta).
5. Decida si desea gestionar cada aplicación de forma individual o a nivel de espacio de nombres.
6. Busque la aplicación que desee en el nivel deseado en la jerarquía y, en el menú acciones, seleccione **gestionar**.
7. Si no desea gestionar una aplicación, en el menú acciones situado junto a la aplicación, seleccione **Ignorar**.

   Por ejemplo, si desea gestionar juntas todas las aplicaciones del espacio de nombres "maría" para que tengan las mismas políticas de copia Snapshot y copia de seguridad, debe gestionar el espacio de nombres e ignorar las aplicaciones del espacio de nombres.

8. Para ver la lista de aplicaciones administradas, seleccione **gestionado** como filtro de visualización.



   Observe que la aplicación que acaba de agregar tiene un icono de advertencia debajo de la columna protegida, que indica que no se ha realizado una copia de seguridad y que aún no está programada para las copias de seguridad.

9. Para ver los detalles de una aplicación en particular, seleccione el nombre de la aplicación.

Resultado

Las aplicaciones que eligió administrar ahora están disponibles en la pestaña **gestionado**. Cualquier aplicación ignorada se moverá a la pestaña **ignorada**. Lo ideal es que la ficha descubierto no muestre

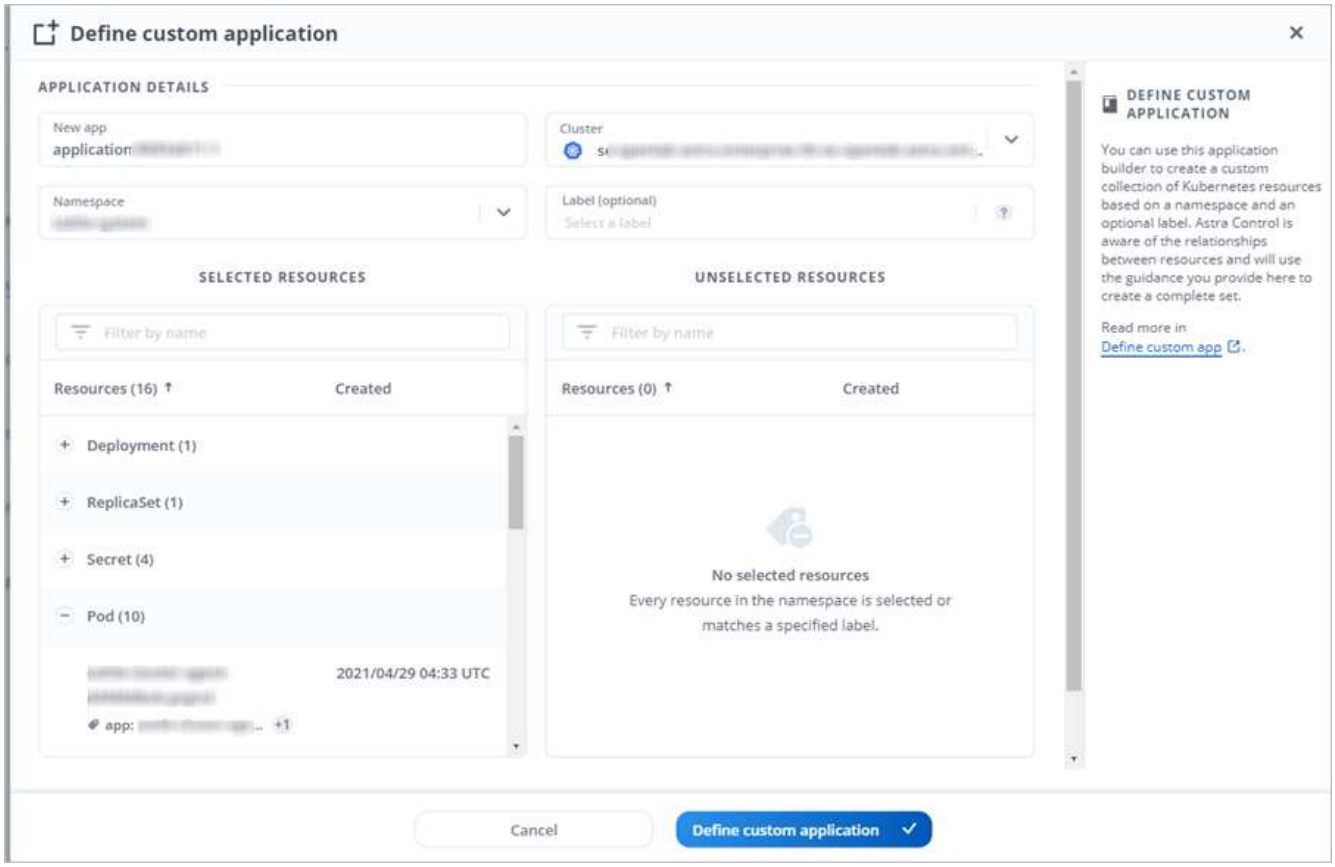
ninguna aplicación, de modo que, a medida que se instalan nuevas aplicaciones, resulta más fácil encontrarlos y gestionarlos.

Gestione aplicaciones mediante la etiqueta Kubernetes

Astra Control incluye una acción en la parte superior de la página de aplicaciones llamada **definir aplicación personalizada**. Puede usar esta acción para gestionar las aplicaciones identificadas con una etiqueta de Kubernetes. "Obtenga más información sobre cómo definir aplicaciones personalizadas mediante etiqueta de Kubernetes".

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **definir**.



3. En el cuadro de diálogo **definir aplicación personalizada**, proporcione la información necesaria para administrar la aplicación:
   a. **Nueva aplicación**: Introduzca el nombre para mostrar de la aplicación.
   b. **Cluster**: Seleccione el clúster en el que reside la aplicación.
   c. **espacio de nombres:** Seleccione el espacio de nombres para la aplicación.
   d. **etiqueta:** Introduzca una etiqueta o seleccione una de las siguientes fuentes.
   e. **Recursos seleccionados**: Vea y gestione los recursos de Kubernetes seleccionados que le gustaría proteger (pods, secretos, volúmenes persistentes, etc.).
      - Para ver las etiquetas disponibles, amplíe un recurso y seleccione el número de etiquetas.
      - Seleccione una de las etiquetas.

Después de seleccionar una etiqueta, se muestra en el campo **etiqueta**. Astra Control también actualiza la sección **Recursos no seleccionados** para mostrar los recursos que no coinciden con la etiqueta seleccionada.

f. **Recursos no seleccionados**: Verifique los recursos de la aplicación que no desea proteger.

4. Seleccione **definir aplicación personalizada**.

Resultado

Astra Control permite la gestión de la aplicación. Ahora puede encontrarlo en la pestaña **gestionado**.

Ignorar aplicaciones

Si se ha detectado una aplicación, ésta aparece en la lista descubierta. En este caso, puede limpiar la lista descubierta para que las nuevas aplicaciones que se han instalado sean más fáciles de encontrar. O bien, puede que tenga aplicaciones que esté gestionando y, más adelante, decida que ya no desea gestionarlas. Si no desea administrar estas aplicaciones, puede indicar que deben ignorarse.

Además, puede que desee gestionar aplicaciones en un espacio de nombres (gestionado por espacios de nombres). Puede ignorar las aplicaciones que desea excluir del espacio de nombres.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **descubierto** como filtro.
3. Seleccione la aplicación.
4. En el menú acciones, seleccione **Ignorar**.
5. Para designorar, en el menú acciones, seleccione **no ignorar**.

Desgestionar aplicaciones

Cuando ya no desee realizar una copia de seguridad, una instantánea o clonar una aplicación, puede dejar de administrarla.

> Si desgestiona una aplicación, se perderán todos los backups o las instantáneas que se hayan creado anteriormente.

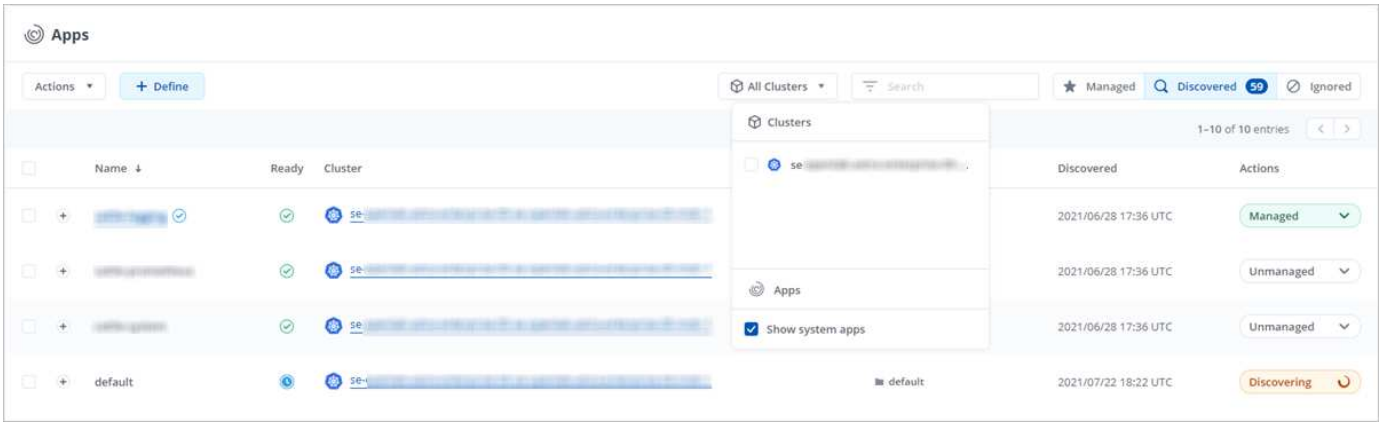
Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione **gestionado** como filtro.
3. Seleccione la aplicación.
4. En el menú acciones, seleccione **Unmanage**.
5. Revise la información.
6. Escriba "desgestionar" para confirmar.
7. Seleccione **Sí, Desactivar aplicación**.

¿y las aplicaciones del sistema?

Astra Control también detecta las aplicaciones del sistema que se ejecutan en un clúster de Kubernetes. Puede mostrar las aplicaciones del sistema seleccionando la casilla de verificación **Mostrar aplicaciones del**

sistema en el filtro de clúster de la barra de herramientas.



No le mostramos estas aplicaciones del sistema de forma predeterminada porque es raro que tenga que hacer una copia de seguridad.

> Astra Control en sí no es una aplicación estándar; es una "aplicación del sistema". No debe intentar gestionar Astra Control por sí mismo. Astra Control no se muestra de forma predeterminada para la gestión. Para ver las aplicaciones del sistema, utilice el filtro “Mostrar aplicaciones del sistema”.

Obtenga más información

- "Utilice la API Astra Control"

Defina un ejemplo de aplicación personalizada

Crear una aplicación personalizada le permite agrupar elementos de su clúster de Kubernetes en una única aplicación.

Una aplicación personalizada le ofrece un control más granular de lo que debe incluirse en una operación de Astra Control, entre las que se incluyen:

- Clonar
- Snapshot
- Backup
- Política de protección

En la mayoría de los casos, querrá utilizar las funciones de Astra Control en toda su aplicación. Sin embargo, también puede crear una aplicación personalizada para utilizar estas funciones con las etiquetas que asigne a los objetos de Kubernetes en un espacio de nombres.

Para crear una aplicación personalizada, vaya a la página aplicaciones y seleccione **+ define**.

A medida que realice las selecciones, la ventana aplicación personalizada mostrará los recursos que se incluirán o excluirán de la aplicación personalizada. Esto le ayuda a asegurarse de que está eligiendo los criterios correctos para definir su aplicación personalizada.

Las aplicaciones personalizadas solo se pueden crear dentro de un espacio de nombres especificado en un único clúster. Astra Control no admite la capacidad de una aplicación personalizada para abarcar varios espacios de nombres o clústeres.

Una etiqueta es una pareja clave/valor que se puede asignar a objetos de Kubernetes para su identificación. Las etiquetas facilitan la ordenación, la organización y la búsqueda de los objetos de Kubernetes. Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

Las directivas que se solapan para el mismo recurso con nombres diferentes pueden provocar conflictos de datos. Si crea una aplicación personalizada para un recurso, asegúrese de que no se clona ni se realiza un backup en ninguna otra política.

Ejemplo: Política de protección independiente para el lanzamiento canario

En este ejemplo, el equipo de devops gestiona una puesta en marcha de versiones canaria. Su grupo tiene tres pods que ejecutan nginx. Dos de los pods están dedicados a la versión estable. El tercer pod es para el lanzamiento canario.

El administrador de Kubernetes del equipo de devops añade la etiqueta `deployment=stable` a los pods de liberación estables. El equipo agrega la etiqueta `deployment=canary` a la cápsula de liberación canaria.

La versión estable del equipo incluye los requisitos de snapshots cada hora y backups diarios. la liberación canaria es más efímera, por lo que quieren crear una Política de Protección a corto plazo menos agresiva para cualquier cosa etiquetada `deployment=canary`.

Para evitar posibles conflictos de datos, el administrador creará dos aplicaciones personalizadas: Una para el lanzamiento canario y otra para el lanzamiento estable. De este modo, los backups, las snapshots y las operaciones de clonado se mantienen independientes para los dos grupos de objetos de Kubernetes.

Pasos

1. Una vez que el equipo agrega el clúster a Astra Control, el siguiente paso es definir una aplicación personalizada. Para ello, el equipo selecciona el botón **+ define** de la página aplicaciones.
2. En la ventana emergente que aparece, el equipo establece `devops-canary-deployment` como nombre de la aplicación. El equipo elige el cluster en la lista desplegable **Cluster**, entonces el espacio de nombres de la aplicación del menú desplegable **namespace**.
3. El equipo puede escribir `deployment=canary` En el campo **Etiquetas**, o seleccione esa etiqueta de los recursos que se muestran a continuación.
4. Después de definir la aplicación personalizada para la implementación canaria, el equipo repite el proceso para la implementación estable.

Cuando el equipo haya terminado de crear las dos aplicaciones personalizadas, pueden tratar estos recursos como cualquier otra aplicación de Astra Control. Pueden clonarlas, crear backups y snapshots, y crear una política de protección personalizada para cada grupo de recursos basada en las etiquetas de Kubernetes.

Proteja sus aplicaciones

Información general sobre la protección

Puede crear backups, clones, snapshots y políticas de protección para sus aplicaciones con Astra Control Center. El backup de sus aplicaciones ayuda a que los servicios y los datos asociados estén disponibles lo

más posible; durante un desastre, la restauración a partir de una copia de seguridad puede garantizar la recuperación completa de una aplicación y sus datos asociados con una interrupción mínima. Los backups, clones y copias Snapshot pueden ayudar a protegerse frente a amenazas comunes como el ransomware, la pérdida accidental de datos y los desastres medioambientales. "Conozca los tipos disponibles de protección de datos en Astra Control Center y cuándo utilizarlas".

Flujo de trabajo de protección de aplicaciones

Puede utilizar el siguiente ejemplo de flujo de trabajo para empezar a proteger las aplicaciones.

[Uno] Realice copias de seguridad de todas las aplicaciones

Para asegurarse de que sus aplicaciones están protegidas inmediatamente, "cree una copia de seguridad manual de todas las aplicaciones".

[Dos] Configure una política de protección para cada aplicación

Para automatizar futuros backups y copias Snapshot, "configure una política de protección para cada aplicación". A modo de ejemplo, puede comenzar con backups semanales y snapshots diarias, con una retención de un mes para ambos. La automatización de backups y snapshots con una política de protección es muy recomendada con respecto a copias de Snapshot y backups manuales.

[Tres] Opcional: Ajuste las políticas de protección

A medida que cambian las aplicaciones y sus patrones de uso, ajuste las políticas de protección según sea necesario para proporcionar la mejor protección.

[Cuatro] En caso de desastre, restaure sus aplicaciones

Si se produce la pérdida de datos, puede recuperarlo "restaurar la copia de seguridad más reciente" la primera para cada aplicación. Luego puede restaurar la snapshot más reciente (si está disponible).

Proteja las aplicaciones con snapshots y backups

Proteja sus aplicaciones tomando snapshots y backups usando una política de protección automatizada o de manera ad hoc. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para proteger aplicaciones.

Si utiliza Helm para implantar aplicaciones, Astra Control Center requiere Helm versión 3. Se admite por completo la gestión y clonación de las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Las aplicaciones implementadas con Helm 2 no son compatibles.

Al crear un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Configure una política de protección

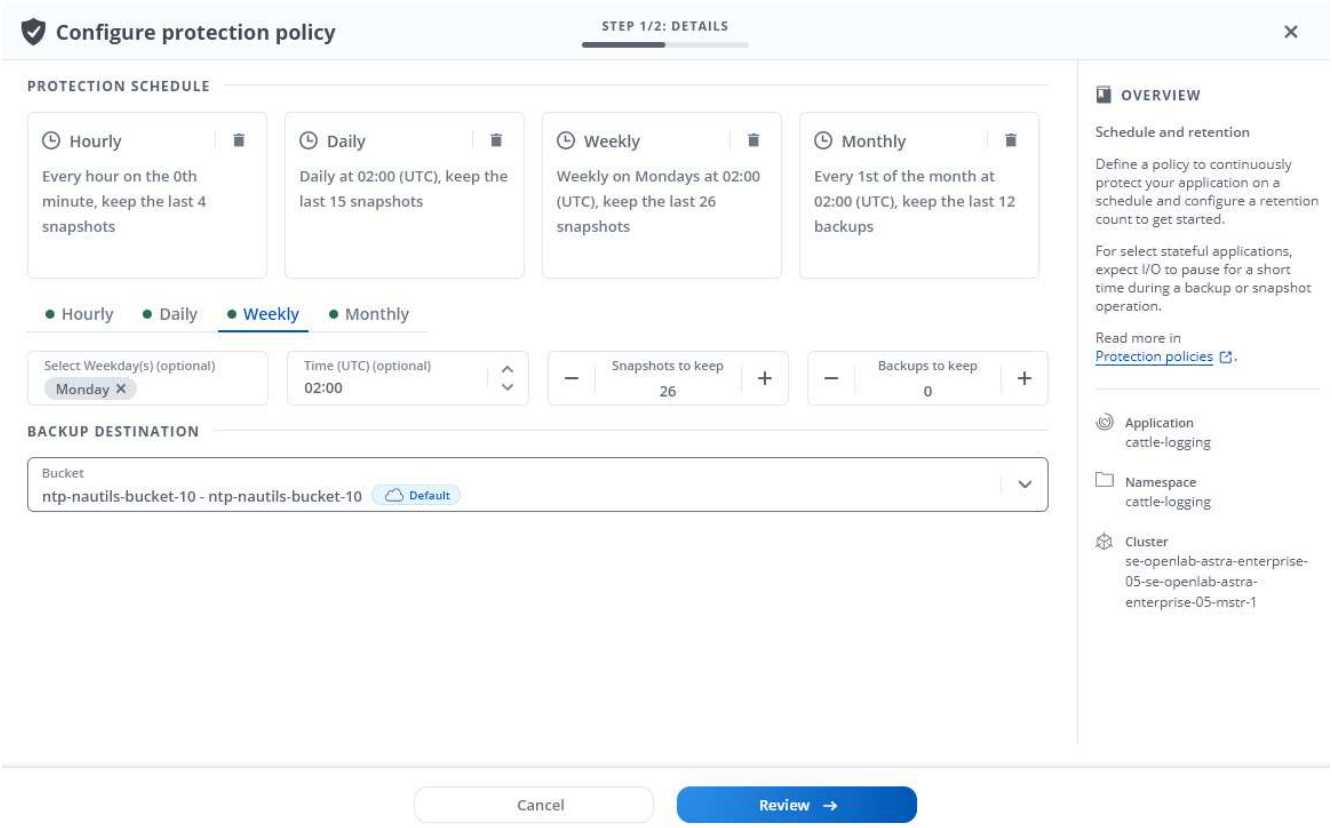
La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener. A modo de ejemplo, una política de protección puede crear backups semanales y copias Snapshot diarias, y conservar los backups y las copias Snapshot por un mes. La frecuencia con la que se crean snapshots y backups y el tiempo que se retienen depende de las necesidades de la organización.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **Configurar política de protección**.
4. Defina una programación de protección eligiendo la cantidad de snapshots y backups que se mantendrán por hora, día, semana y mes.

   Puede definir las programaciones por hora, por día, por semana y por mes de forma simultánea. Una programación no se activa hasta que se establece un nivel de retención.

   En el siguiente ejemplo, se establecen cuatro programaciones de protección: Por hora, día, semana y mes para las copias Snapshot y los backups.



5. Seleccione **Revisión**.
6. Seleccione **Configurar política de protección.**

Resultado

Astra Control Center implementa la normativa de protección de datos mediante la creación y retención de

instantáneas y copias de seguridad con la programación y retención que ha definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

Pasos

1. Seleccione **aplicaciones**.
2. Seleccione la lista desplegable en la columna **acciones** de la aplicación deseada.
3. Seleccione **Snapshot**.
4. Personalice el nombre de la instantánea y, a continuación, seleccione **Revisión**.
5. Revise el resumen de la instantánea y seleccione **Snapshot**.

Resultado

Se inicia el proceso Snapshot. Una instantánea se realiza correctamente cuando el estado es **disponible** en la columna **acciones** de la página **Protección de datos** > **instantáneas**.

Cree un backup

También puede realizar copias de seguridad de una aplicación en cualquier momento.

> Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Pasos

1. Seleccione **aplicaciones**.
2. Seleccione la lista desplegable en la columna **acciones** de la aplicación deseada.
3. Seleccione **copia de seguridad**.
4. Personalice el nombre del backup.
5. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
6. Seleccione un destino para el backup seleccionando de la lista de bloques de almacenamiento.
7. Seleccione **Revisión**.
8. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control Center crea una copia de seguridad de la aplicación.

> Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.

> No existe ninguna forma de detener un backup en ejecución. Si necesita eliminar el backup, espere hasta que se haya completado y, a continuación, utilice las instrucciones de Eliminar backups. Para eliminar una copia de seguridad fallida, "Utilice la API Astra Control".

Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Ver Snapshot y backups

Puede ver las instantáneas y las copias de seguridad de una aplicación desde la pestaña Data Protection.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.

   Las instantáneas se muestran de forma predeterminada.

3. Seleccione **copias de seguridad** para ver la lista de copias de seguridad.

Eliminar snapshots

Elimine las snapshots programadas o bajo demanda que ya no necesite.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione la lista desplegable en la columna **acciones** para la instantánea deseada.
4. Seleccione **Eliminar instantánea**.
5. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete snapshot**.

Resultado

Astra Control Center elimina la instantánea.

Eliminar backups

Elimine los backups programados o bajo demanda que ya no necesita.

No existe ninguna forma de detener un backup en ejecución. Si necesita eliminar el backup, espere hasta que se haya completado y, a continuación, utilice estas instrucciones. Para eliminar una copia de seguridad fallida, "Utilice la API Astra Control".

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. Seleccione la lista desplegable en la columna **acciones** para la copia de seguridad deseada.
5. Seleccione **Eliminar copia de seguridad**.
6. Escriba la palabra "delete" para confirmar la eliminación y, a continuación, seleccione **Yes, Delete backup**.

Resultado

Astra Control Center elimina la copia de seguridad.

Restaurar aplicaciones

Astra Control puede restaurar su aplicación a partir de una instantánea o una copia de seguridad. La restauración a partir de una snapshot existente será más rápida cuando se restaure la aplicación en el mismo clúster. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para restaurar aplicaciones.

Si utiliza Helm para implantar aplicaciones, Astra Control Center requiere Helm versión 3. Se admite por completo la gestión y clonación de las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Las aplicaciones implementadas con Helm 2 no son compatibles.

Si restaura en un clúster diferente, asegúrese de que el clúster utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de restauración si el modo de acceso al volumen persistente de destino es diferente.

Al crear un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Si desea restaurar desde una instantánea, mantenga seleccionado el icono **instantáneas**. De lo contrario, seleccione el icono **copias de seguridad** para restaurar desde una copia de seguridad.
4. Seleccione la lista desplegable de la columna **acciones** para la instantánea o la copia de seguridad desde la que desea restaurar.
5. Seleccione **Restaurar aplicación**.
6. **Detalles de la restauración**: Especifique los detalles de la aplicación restaurada. De forma predeterminada, se muestran el clúster y el espacio de nombres actuales. Deje estos valores intactos para restaurar una aplicación in situ, que revierte la aplicación a una versión anterior de sí misma. Cambie estos valores si desea restaurar a un clúster o espacio de nombres diferentes.
   - Introduzca un nombre y un espacio de nombres para la aplicación.
   - Seleccione el clúster de destino de la aplicación.
   - Seleccione **Revisión**.
7. **Resumen de restauración**: Revise los detalles sobre la acción de restauración, escriba "restore" y seleccione **Restaurar**.

Resultado

Astra Control Center restaura la aplicación en función de la información proporcionada. Si restauró la aplicación en un lugar, el contenido de cualquier volumen persistente existente se reemplaza por el contenido de los volúmenes persistentes de la aplicación restaurada.

> Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Clone y migre aplicaciones

Clone una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. El clonado puede ayudarle si necesita mover aplicaciones y almacenamiento de un clúster de Kubernetes a otro. Por ejemplo, es posible que desee mover cargas de trabajo mediante una canalización de CI/CD y entre espacios de nombres Kubernetes. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para clonar y migrar aplicaciones.

> Si se implementa una aplicación con un StorageClass configurado explícitamente y se necesita clonar la aplicación, el clúster de destino debe tener el StorageClass especificado originalmente. Se producirá un error al clonar una aplicación con un tipo de almacenamiento establecido explícitamente en un clúster que no tenga el mismo tipo de almacenamiento.

> Si clona una instancia de Jenkins CI que ha puesto en marcha un operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.

> Si clona una aplicación entre clústeres, los clústeres de origen y destino deben ser la misma distribución de OpenShift. Por ejemplo, si clona una aplicación de un clúster de OpenShift 4.7, utilice un clúster de destino que también sea OpenShift 4.7.

Cuando Astra Control Center clona una aplicación, crea un clon de la configuración de la aplicación y del almacenamiento persistente.

> Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Al crear un proyecto para alojar una aplicación en un clúster de OpenShift, se asigna un UID de SecurityContext al proyecto (o espacio de nombres de Kubernetes). Para habilitar Astra Control Center para proteger su aplicación y mover la aplicación a otro clúster o proyecto en OpenShift, debe agregar directivas que permitan que la aplicación se ejecute como cualquier UID. Por ejemplo, los siguientes comandos de la CLI de OpenShift otorgan las directivas adecuadas a una aplicación de WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Lo que necesitará

Para clonar aplicaciones en un clúster diferente, necesita un bloque predeterminado. Cuando se agrega su primer bloque, se convierte en el bloque predeterminado.

Pasos

1. Seleccione **aplicaciones**.
2. Debe realizar una de las siguientes acciones:
   - Seleccione la lista desplegable en la columna **acciones** de la aplicación deseada.
   - Seleccione el nombre de la aplicación deseada y seleccione la lista desplegable de estado en la parte superior derecha de la página.
3. Seleccione **Clonar**.
4. **Detalles del clon**: Especifique los detalles del clon:
   - Introduzca un nombre.
   - Introduzca un espacio de nombres para el clon.
   - Elija un clúster de destino para el clon.
   - Elija si desea crear el clon a partir de una snapshot o un backup existente. Si no selecciona esta opción, Astra Control Center crea el clon a partir del estado actual de la aplicación.
5. **Fuente**: Si decide clonar desde una instantánea o copia de seguridad existente, elija la instantánea o copia de seguridad que desea utilizar.
6. Seleccione **Revisión**.
7. **Resumen de clones**: Revise los detalles sobre el clon y seleccione **clon**.

Resultado

Astra Control Center clona esa aplicación basándose en la información que nos ha proporcionado. La operación de clonado se realiza correctamente cuando el nuevo clon de la aplicación está en `Available` en la página **aplicaciones**.

Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Gestione los enlaces de ejecución de aplicaciones

Un enlace de ejecución es una secuencia de comandos personalizada que se puede ejecutar antes o después de una instantánea de una aplicación administrada. Por ejemplo, si tiene una aplicación de base de datos, puede utilizar los enlaces de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez finalizada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Ganchos de ejecución predeterminados y expresiones regulares

Para algunas aplicaciones, Astra Control incluye los enlaces de ejecución predeterminados, proporcionados por NetApp, que gestionan las operaciones de congelación y descongelación antes y después de las copias Snapshot. Astra Control utiliza expresiones regulares para relacionar la imagen de un contenedor de una aplicación con estas aplicaciones:

- MariaDB
  - Expresión regular coincidente: \Bmariadb\b
- MySQL
  - Expresión regular coincidente: \Bmysql\b
- PostgreSQL
  - Expresión regular coincidente: \Bpostgresql\b

Si hay algún dato, los enlaces de ejecución predeterminados proporcionados por NetApp para esa aplicación aparecen en la lista de enlaces de ejecución activos y dichos enlaces se ejecutan automáticamente cuando se hacen snapshots de esa aplicación. Si una de sus aplicaciones personalizadas tiene un nombre de imagen similar que se produce para coincidir con una de las expresiones regulares (y no desea utilizar los ganchos de ejecución predeterminados), puede cambiar el nombre de la imagen, o bien, desactive el enlace de ejecución predeterminado para esa aplicación y utilice un gancho personalizado en su lugar.

No puede eliminar ni modificar los enlaces de ejecución predeterminados.

Notas importantes sobre los enlaces de ejecución personalizados

Tenga en cuenta lo siguiente al planificar enlaces de ejecución para sus aplicaciones.

- Astra Control requiere que los enlaces de ejecución se escriban en el formato de secuencias de comandos de shell ejecutables.
- El tamaño del script está limitado a 128 KB.
- Astra Control utiliza la configuración del enlace de ejecución y cualquier criterio coincidente para determinar qué ganchos son aplicables a una instantánea.
- Todos los fallos del enlace de ejecución son errores de software; otros enlaces y la instantánea siguen intentándose incluso si falla un gancho. Sin embargo, cuando falla un gancho, se registra un suceso de advertencia en el registro de eventos de la página **Activity**.
- Para crear, editar o eliminar enlaces de ejecución, debe ser un usuario con permisos de propietario, administrador o miembro.
- Si un enlace de ejecución tarda más de 25 minutos en ejecutarse, el enlace fallará, creando una entrada de registro de eventos con un código de retorno de "N/A". Se agotará el tiempo de espera de todas las instantáneas afectadas y se marcarán como errores, con una entrada de registro de eventos resultante

que tenga en cuenta el tiempo de espera.

> Puesto que los enlaces de ejecución a menudo reducen o desactivan por completo la funcionalidad de la aplicación con la que se ejecutan, siempre debe intentar minimizar el tiempo que tardan los enlaces de ejecución personalizados.

Cuando se ejecuta una instantánea, los eventos de enlace de ejecución tienen lugar en el siguiente orden:

1. Todos los enlaces de ejecución presnapshot predeterminados que proporcione NetApp se ejecutan en los contenedores adecuados.
2. Todos los enlaces de ejecución de presnapshot personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces presnapshot personalizados como necesite, pero el orden de ejecución de estos enlaces antes de que la instantánea no esté garantizada ni sea configurable.
3. La copia de Snapshot se realiza.
4. Todos los enlaces de ejecución post-snapshot personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces post-snapshot personalizados como necesite, pero el orden de ejecución de estos enlaces después de que la instantánea no esté garantizada ni sea configurable.
5. Todos los enlaces de ejecución post-snapshot predeterminados que proporcione NetApp se ejecutan en los contenedores adecuados.

> Siempre debe probar sus secuencias de comandos de ejecución de enlace antes de habilitarlas en un entorno de producción. Puede utilizar el comando 'kubectl exec' para probar cómodamente los scripts. Después de habilitar los enlaces de ejecución en un entorno de producción, pruebe las instantáneas resultantes para asegurarse de que son coherentes. Para ello, puede clonar la aplicación en un espacio de nombres temporal, restaurar la instantánea y, a continuación, probar la aplicación.

Ver los enlaces de ejecución existentes

Puede ver los enlaces de ejecución predeterminados de una aplicación ya existentes o proporcionados por NetApp.

Pasos

1. Vaya a **aplicaciones** y seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.

   Puede ver todos los enlaces de ejecución habilitados o desactivados en la lista resultante. Puede ver el estado, el origen y el momento en que se ejecuta un gancho (instantánea previa o posterior). Para ver los registros de eventos que rodean los enlaces de ejecución, vaya a la página **actividad** en el área de navegación del lado izquierdo.

Cree un enlace de ejecución personalizado

Puede crear un enlace de ejecución personalizado para una aplicación. Consulte "Ejemplos de gancho de ejecución" para ejemplos de gancho. Necesita tener permisos de propietario, administrador o miembro para crear enlaces de ejecución.

Cuando cree un script de shell personalizado para utilizarlo como un enlace de ejecución, recuerde especificar el shell adecuado al principio del archivo, a menos que esté ejecutando comandos linux o proporcionando la ruta completa a un ejecutable.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione **Añadir un nuevo gancho**.
4. En el área **Detalles del gancho**, dependiendo de cuándo se debe ejecutar el gancho, elija **Pre-Snapshot** o **Post-Snapshot**.
5. Introduzca un nombre único para el gancho.
6. (Opcional) Introduzca cualquier argumento para pasar al gancho durante la ejecución, pulsando la tecla Intro después de cada argumento que introduzca para grabar cada uno.
7. En el área **Imágenes de contenedor**, si el gancho debe funcionar con todas las imágenes de contenedor contenidas en la aplicación, active la casilla de verificación **aplicar a todas las imágenes de contenedor**. Si en su lugar el gancho sólo debe actuar en una o más imágenes contenedoras especificadas, introduzca los nombres de imagen contenedora en el campo **nombres de imagen contenedora para que coincidan**.
8. En el área **Script**, siga uno de estos procedimientos:
   - Cargue un script personalizado.
     i. Seleccione la opción **cargar archivo**.
     ii. Navegue hasta un archivo y cárguelo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
   - Pegar en un script personalizado desde el portapapeles.
     i. Seleccione la opción **Pegar del portapapeles**.
     ii. Seleccione el campo de texto y pegue el texto del script en el campo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
9. Seleccione **Agregar gancho**.

Desactivar un gancho de ejecución

Puede desactivar un gancho de ejecución si desea impedir temporalmente que se ejecute antes o después de una instantánea de una aplicación. Necesita tener permisos de propietario, administrador o miembro para desactivar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú desplegable **acciones** para un gancho que desee desactivar.
4. Seleccione **Desactivar**.

Eliminar un gancho de ejecución

Puede eliminar un enlace de ejecución por completo si ya no lo necesita. Necesita tener permisos de propietario, administrador o miembro para eliminar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú desplegable **acciones** para obtener un enlace que desee eliminar.
4. Seleccione **Eliminar**.

Ejemplos de gancho de ejecución

Utilice los siguientes ejemplos para obtener una idea de cómo estructurar los enlaces de ejecución. Puede utilizar estos enlaces como plantillas o como scripts de prueba.

Ejemplo de éxito simple

Este es un ejemplo de un simple enlace que se realiza correctamente y escribe un mensaje en la salida estándar y en un error estándar.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
```

```
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo de éxito simple (versión de bash)

Este es un ejemplo de un simple enlace que funciona y escribe un mensaje en la salida estándar y en un error estándar, escrito para bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo sencillo de éxito (versión zsh)

Este es un ejemplo de un simple enlace que se realiza correctamente y escribe un mensaje en la salida estándar y en un error estándar, escrito para el shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#
```

```
#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Éxito con argumentos ejemplo

En el siguiente ejemplo se muestra cómo se pueden utilizar args en un gancho.

```
#!/bin/sh
```

```
# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2
```

```
# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Ejemplo de gancho de instantánea previa/posinstantánea

En el siguiente ejemplo se muestra cómo se puede utilizar el mismo script tanto para una instantánea previa como para un enlace posterior a una instantánea.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
```

```
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
```

```
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

Ejemplo de fallo

En el siguiente ejemplo se muestra cómo puede controlar los fallos en un gancho.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Ejemplo de fallo detallado

En el ejemplo siguiente se muestra cómo puede controlar los errores en un enlace, con un registro más detallado.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
```

```
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
```

```
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

Fallo con un ejemplo de código de salida

En el siguiente ejemplo se muestra un error de enlace con un código de salida.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
```

```
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Ejemplo de éxito tras fallo

El siguiente ejemplo muestra un gancho que falla la primera vez que se ejecuta, pero que tiene éxito después de la segunda ejecución.

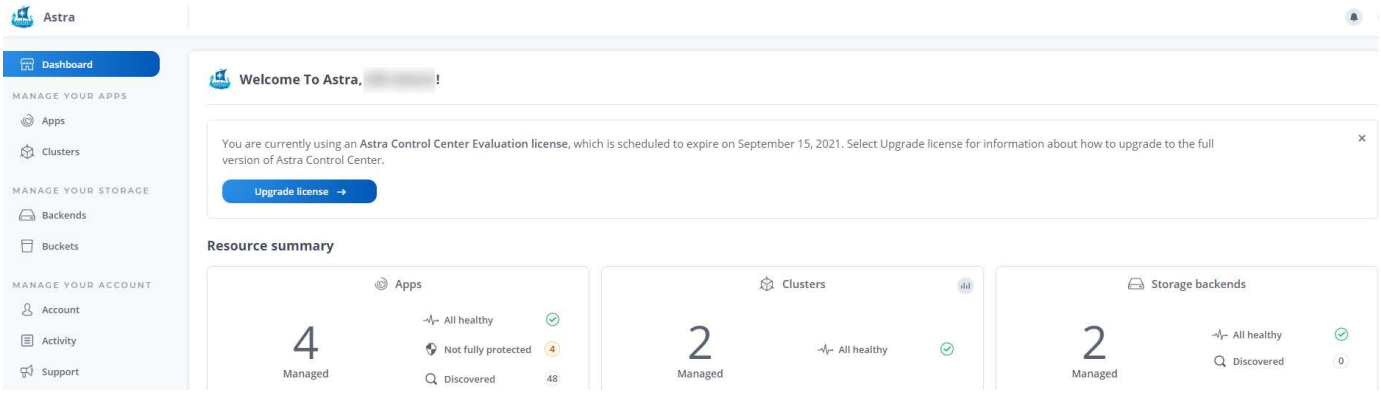
```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}



#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

Ver el estado de las aplicaciones y del clúster

Ver un resumen del estado de las aplicaciones y el clúster

Seleccione * Dashboard* para ver una vista de alto nivel de sus aplicaciones, clusters, back-ends de almacenamiento y su estado.



No se trata sólo de números o Estados estáticos --usted puede profundizar en cada uno de estos. Por ejemplo, si las aplicaciones no están completamente protegidas, puede pasar el ratón sobre el icono para identificar qué aplicaciones no están completamente protegidas, lo que incluye un motivo.

Aplicaciones

El mosaico **aplicaciones** le ayuda a identificar lo siguiente:

- Cuántas aplicaciones gestiona actualmente con Astra.
- Si esas aplicaciones gestionadas están en buen estado.
- Si las aplicaciones están totalmente protegidas (están protegidas si hay backups recientes disponibles).
- El número de aplicaciones que se han detectado, pero que aún no se han administrado.

  Lo ideal sería que este número fuera cero porque gestionaría o ignoraría aplicaciones después de que se descubrieran. Y, a continuación, supervisaría el número de aplicaciones detectadas en el Panel de control para identificar cuándo los desarrolladores añaden nuevas aplicaciones a un clúster.

Icono de clústeres

El mosaico **Clusters** proporciona detalles similares sobre el estado de los clústeres que está administrando utilizando Astra Control Center, y puede profundizar para obtener más detalles como usted puede con una app.

Icono de los back-ends de almacenamiento

El mosaico **back-ends** de almacenamiento proporciona información para ayudarle a identificar el estado de los back-ends de almacenamiento, incluidos:

- Cuántos back-ends de almacenamiento se gestionan
- Si estos back-ends administrados son en buen estado
- Si los back-ends están totalmente protegidos
- La cantidad de back-ends que se detectan, pero todavía no se gestionan.

Consulte el estado y los detalles de los clústeres

Después de añadir clústeres que debe gestionar Astra Control Center, puede ver detalles sobre el clúster, como su ubicación, los nodos de trabajo, los volúmenes persistentes y las clases de almacenamiento.

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster cuyos detalles desea ver.
3. Consulte la información en las pestañas **Descripción general**, **almacenamiento** y **actividad** para encontrar la información que busca.
   - **Descripción general**: Detalles sobre los nodos de trabajo, incluido su estado.
   - **almacenamiento**: Los volúmenes persistentes asociados con el cálculo, incluyendo la clase de almacenamiento y el estado.
   - **Actividad**: Muestra las actividades relacionadas con el cluster.

> También puede ver la información del clúster a partir de Astra Control Center **Dashboard**. En la ficha **Clusters** de **Resumen de recursos**, puede seleccionar los clústeres administrados, que le llevará a la página **Clusters**. Después de llegar a la página **Clusters**, siga los pasos descritos anteriormente.

Ver el estado y los detalles de una aplicación

Una vez que empiece a gestionar una aplicación, Astra ofrece detalles sobre la aplicación que permite identificar su estado (si está en buen estado), su estado de protección (si está totalmente protegida en caso de fallo), los pods, el almacenamiento persistente y mucho más.

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Encuentre la información que busca:

   Estado de la aplicación

   Proporciona un estado que refleja el estado de la aplicación en Kubernetes. Por ejemplo, ¿los pods y los volúmenes persistentes están en línea? Si una aplicación no es saludable, deberá ir y solucionar el problema en el clúster mirando los registros de Kubernetes. Astra no proporciona información para ayudarle a arreglar una aplicación rota.

   Estado de protección de aplicaciones

   Proporciona el estado de la protección de la aplicación:

   - **totalmente protegido**: La aplicación tiene una programación de copia de seguridad activa y una copia de seguridad exitosa que tiene menos de una semana de antigüedad
   - **parcialmente protegido**: La aplicación tiene una programación de copia de seguridad activa, una programación de instantáneas activa o una copia de seguridad o instantánea correcta
   - **desprotegido**: Aplicaciones que no están completamente protegidas o parcialmente protegidas.

     no puede estar completamente protegido hasta que tenga una copia de seguridad reciente. Esto es importante porque los backups se almacenan en un almacén de objetos lejos de los volúmenes persistentes. Si un fallo o accidente limpia el cluster y es almacenamiento persistente, necesitará una copia de seguridad para recuperar. Una Snapshot no le permite recuperar.

Descripción general

Información sobre el estado de los pods asociados con la aplicación.

Protección de datos

Permite configurar una política de protección de datos y ver las Snapshot y los backups existentes.

Reducida

Muestra los volúmenes persistentes a nivel de aplicación. El estado de un volumen persistente es desde el punto de vista del clúster de Kubernetes.

Recursos

Permite verificar qué recursos se están gestionando y haciendo backup.

Actividad

Muestra las actividades relacionadas con la aplicación.

> También puede ver la información de la aplicación, empezando por Astra Control Center **Dashboard**. En la ficha **aplicaciones** de **Resumen de recursos**, puede seleccionar las aplicaciones administradas, que le llevará a la página **aplicaciones**. Después de llegar a la página **aplicaciones**, siga los pasos descritos anteriormente.

Gestione su cuenta

Gestionar usuarios

Puede añadir, eliminar y editar usuarios de la instalación de Astra Control Center mediante la interfaz de usuario de Astra Control Center. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para gestionar usuarios.

Añadir usuarios

Los propietarios y administradores de cuentas pueden agregar más usuarios a la instalación de Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Agregar usuario**.
4. Introduzca el nombre del usuario, la dirección de correo electrónico y una contraseña temporal.

   El usuario deberá cambiar la contraseña en el primer inicio de sesión.

5. Seleccione una función de usuario con los permisos de sistema adecuados.

   Cada rol proporciona los siguientes permisos:

   - Un **Visor** puede ver los recursos.
   - Un **Miembro** tiene permisos de función de Viewer y puede administrar aplicaciones y clústeres, pero no puede anular la administración de aplicaciones o clústeres, ni eliminar instantáneas o copias de seguridad.

- Un **Admin** tiene permisos de rol de miembro y puede agregar y quitar cualquier otro usuario excepto el propietario.
- **Owner** tiene permisos de función de administrador y puede agregar y eliminar cualquier cuenta de usuario.

6. Seleccione **Agregar**.

Gestionar contraseñas

Puede gestionar las contraseñas de las cuentas de usuario en Astra Control Center.

Cambie la contraseña

Puede cambiar la contraseña de su cuenta de usuario en cualquier momento.

Pasos

1. Seleccione el icono Usuario situado en la parte superior derecha de la pantalla.
2. Seleccione **Perfil**.
3. Seleccione la lista desplegable **acciones** y seleccione **Cambiar contraseña**.
4. Introduzca una contraseña que se ajuste a los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.
6. Seleccione **Cambiar contraseña**.

Restablecer la contraseña de otro usuario

Si su cuenta tiene permisos de rol de administrador o propietario, puede restablecer las contraseñas de otras cuentas de usuario así como las suyas propias. Al restablecer una contraseña, asigna una contraseña temporal que el usuario tendrá que cambiar al iniciar sesión.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios**, seleccione la lista desplegable en la columna **Estado** para el usuario.
3. Seleccione **Restablecer contraseña**.
4. Introduzca una contraseña temporal que cumpla los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.

   La próxima vez que el usuario inicie sesión, se le solicitará que cambie la contraseña.

6. Seleccione **Restablecer contraseña**.

Cambiar el rol de un usuario

Los usuarios con el rol propietario pueden cambiar el rol de todos los usuarios, mientras que los usuarios con el rol Admin pueden cambiar el rol de los usuarios que tienen el rol Admin, Member o Viewer.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios**, seleccione la lista desplegable en la columna **rol** para el usuario.

3. Seleccione una nueva función y, a continuación, seleccione **Cambiar rol** cuando se le solicite.

Resultado

Astra Control Center actualiza los permisos del usuario en función de la nueva función que haya seleccionado.

Quitar usuarios

Los usuarios con el rol propietario o administrador pueden eliminar otros usuarios de la cuenta en cualquier momento.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. En la ficha **usuarios**, seleccione la casilla de verificación en la fila de cada usuario que desee quitar.
3. Seleccione **acciones** y seleccione **Eliminar usuario/s**.
4. Cuando se le solicite, confirme la eliminación escribiendo la palabra "eliminar" y, a continuación, seleccione **Sí, Eliminar usuario**.

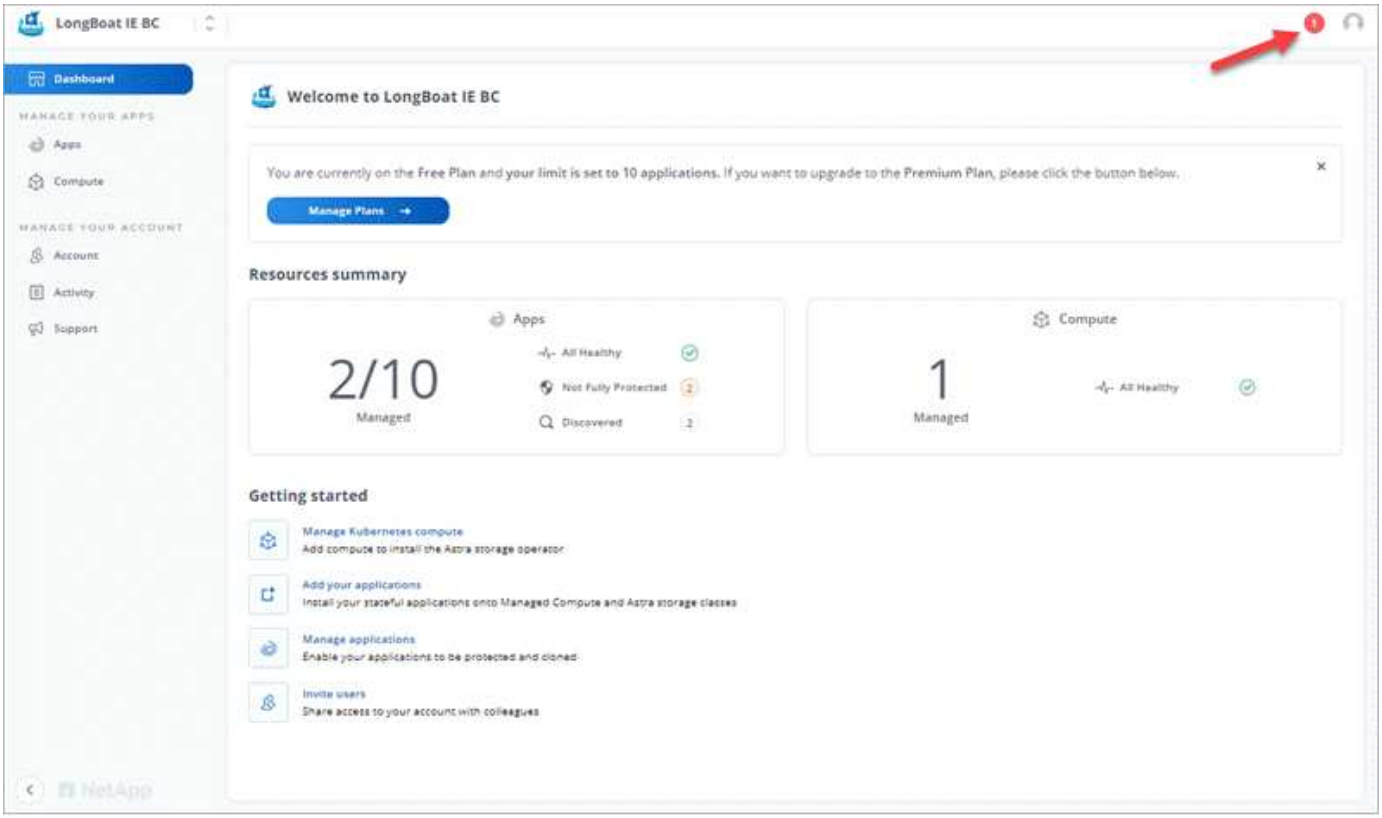
Resultado

Astra Control Center elimina al usuario de la cuenta.

Ver y gestionar notificaciones

Astra le notifica cuando las acciones se han completado o han fallado. Por ejemplo, verá una notificación si una copia de seguridad de una aplicación se ha completado correctamente.

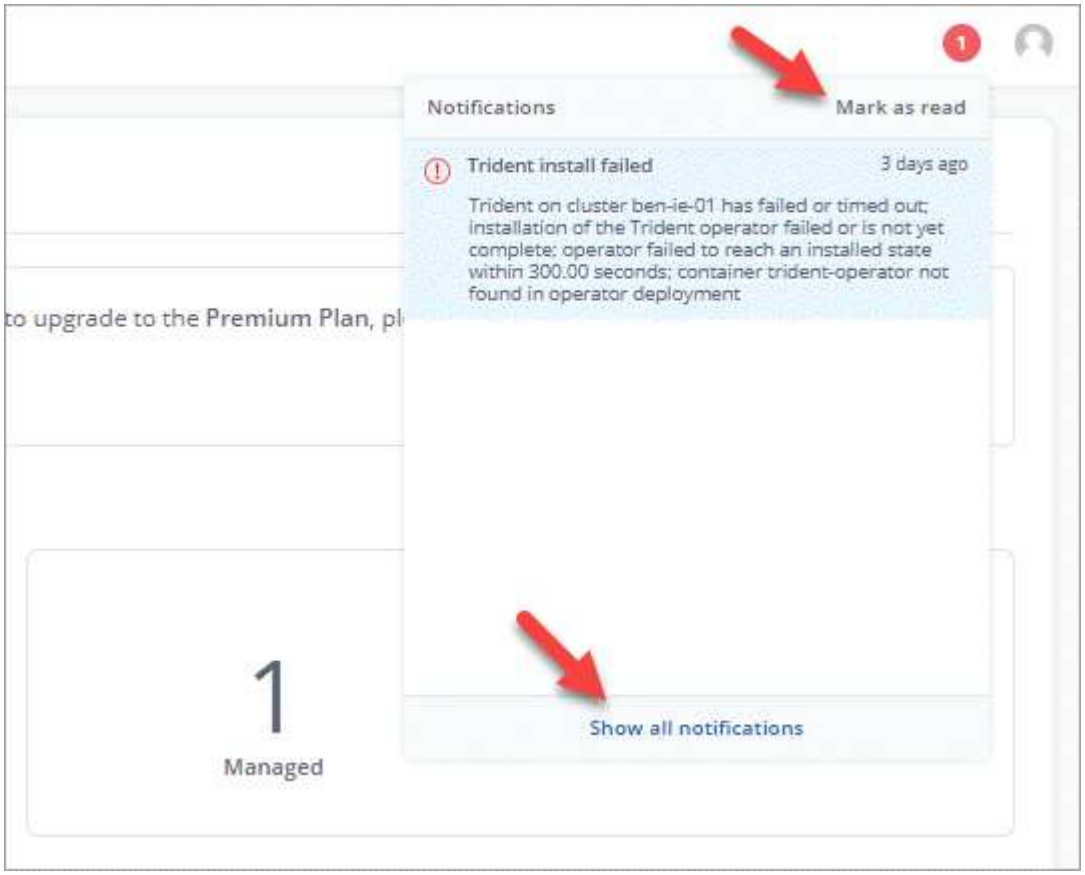
El número de notificaciones sin leer está disponible en la parte superior derecha de la interfaz:



Puede ver estas notificaciones y marcarlas como leídas (esto puede ser útil si desea borrar notificaciones no leídas como nosotros).

Pasos

1. Seleccione el número de notificaciones sin leer en la parte superior derecha.



2. Revise las notificaciones y seleccione **Marcar como leído** o **Mostrar todas las notificaciones**.

   Si ha seleccionado **Mostrar todas las notificaciones**, se cargará la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, seleccione **Acción** y seleccione **Marcar como leído**.

Añada y elimine credenciales

Añada y elimine credenciales de proveedores de cloud privado local como ONTAP S3, clústeres de Kubernetes gestionados con OpenShift o clústeres de Kubernetes no gestionados de su cuenta en cualquier momento. Astra Control Center utiliza estas credenciales para descubrir los clústeres y las aplicaciones de Kubernetes en los clústeres, y para aprovisionar recursos en su nombre.

Tenga en cuenta que todos los usuarios de Astra Control Center comparten los mismos conjuntos de credenciales.

Añada credenciales

Puede agregar credenciales a Astra Control Center cuando gestiona los clústeres. Para añadir credenciales con un clúster nuevo, consulte "Añada un clúster de Kubernetes".

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.

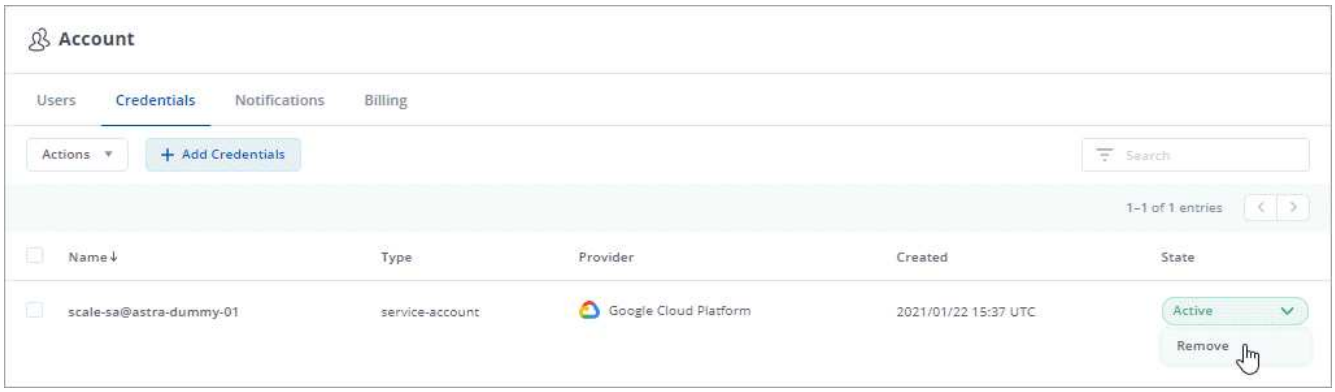
Quite las credenciales

Eliminar credenciales de una cuenta en cualquier momento. Solo debe quitar credenciales después de "desgestione todos los clústeres asociados".

El primer conjunto de credenciales que agregue a Astra Control Center está siempre en uso porque Astra Control Center utiliza las credenciales para autenticarse en el bloque de copia de seguridad. Lo mejor es no eliminar estas credenciales.

Pasos

1. Seleccione **cuenta > credenciales**.
2. Seleccione la lista desplegable de la columna **Estado** para las credenciales que desea quitar.
3. Seleccione **Quitar**.



4. Escriba la palabra "quitar" para confirmar la eliminación y, a continuación, seleccione **Sí, Eliminar credenciales**.

Resultado

Astra Control Center elimina las credenciales de la cuenta.

Controlar la actividad de la cuenta

Puede ver los detalles de las actividades en su cuenta de Astra Control. Por ejemplo, cuando se invitó a nuevos usuarios, cuando se agregaba un clúster o cuando se tomaba una snapshot. También puede exportar la actividad de su cuenta a un archivo CSV.

Ver toda la actividad de la cuenta en Astra Control

1. Seleccione **actividad**.
2. Utilice los filtros para restringir la lista de actividades o utilice el cuadro de búsqueda para encontrar exactamente lo que busca.
3. Seleccione **Exportar a CSV** para descargar la actividad de su cuenta en un archivo CSV.

Ver la actividad de la cuenta de una aplicación específica

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **actividad**.

Ver la actividad de la cuenta de los clústeres

1. Seleccione **Clusters** y, a continuación, seleccione el nombre del clúster.
2. Seleccione **actividad**.

Tome la acción para resolver eventos que requieren atención

1. Seleccione **actividad**.
2. Seleccione un evento que requiera atención.
3. Seleccione la opción desplegable **tomar acción**.

   En esta lista, puede ver las posibles acciones correctivas que puede adoptar, ver la documentación relacionada con el problema y obtener soporte para ayudar a resolver el problema.

Actualizar una licencia existente

Puede convertir una licencia de evaluación a una licencia completa, o puede actualizar una evaluación existente o una licencia completa con una nueva licencia. Si no tiene una licencia completa, trabaje con su contacto de ventas de NetApp para obtener un número de serie y una licencia completa. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para actualizar una licencia existente.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp".
2. Acceda a la página de descarga de Astra Control Center, introduzca el número de serie y descargue el archivo de licencia completo de NetApp (NLF).
3. Inicie sesión en la interfaz de usuario de Astra Control Center.
4. En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
5. En la página **cuenta** > **Licencia**, seleccione el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta** > **licencias** 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.

Gestionar bloques

Un proveedor de bloques de almacenamiento de objetos es esencial si desea realizar backups de las aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Con Astra Control Center, agregue un proveedor de almacenes de objetos como destino de copia de seguridad fuera del clúster para sus aplicaciones.

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 proveedores 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.

No se puede eliminar un bloque; sin embargo, puede editarlo.

Un cubo puede estar en uno de estos estados:

- Pending: Se ha programado la detección del bloque.
- Disponible: El cucharón está disponible para su uso.
- Removido: El cucharón no está accesible actualmente.

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

Puede realizar estas tareas relacionadas con la gestión de bloques:

- "Añadir un bucket"
- Editar un bloque

> Los bloques de S3 de Astra Control Center no informan sobre la capacidad disponible. Antes de realizar una copia de seguridad o clonar aplicaciones gestionadas por Astra Control Center, compruebe la información de los bloques en el sistema de gestión ONTAP o StorageGRID.

Quite las credenciales

Elimine las credenciales de S3 de una cuenta en cualquier momento mediante la API Astra Control.

Para obtener más información, consulte "Utilice la API Astra Control".

> El primer conjunto de credenciales que agregue a Astra Control siempre está en uso porque Astra Control utiliza las credenciales para autenticar el bloque de copia de seguridad. Es mejor no eliminar estas credenciales.

Editar un bloque

Puede cambiar la información de credenciales de acceso de un bloque y cambiar si un bloque seleccionado es el bloque predeterminado.

> 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. Consulte "Notas de la versión".

Pasos

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú acciones, seleccione **Editar**.
3. Cambie cualquier información que no sea el tipo de segmento.

   No puede modificar el tipo de segmento.

4. Seleccione **Actualizar**.

Obtenga más información

- "Utilice la API Astra Control"

Gestione el entorno de administración del almacenamiento

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. Puede supervisar la capacidad del almacenamiento y los detalles del estado, incluido el rendimiento si el Centro de control Astra está conectado a Cloud Insights.

Para obtener instrucciones sobre cómo gestionar los back-ends de almacenamiento con la API Astra Control, consulte "Información sobre API y automatización de Astra".

Es posible completar las siguientes tareas relacionadas con la gestión de un back-end de almacenamiento:

- "Añada un back-end de almacenamiento"
- Ver detalles del back-end de almacenamiento
- Desgestione un back-end de almacenamiento

Ver detalles del back-end de almacenamiento

Puede ver la información del back-end de almacenamiento desde Dashboard o desde la opción Backends.

Consulte los detalles del back-end de almacenamiento en la Consola

Pasos

1. En la navegación de la izquierda, seleccione **Tablero**.
2. Revise la sección Storage backend que muestra el estado:
   - **Insalubre**: El almacenamiento no está en un estado óptimo. Esto puede deberse a un problema de latencia o a que una aplicación está degradada debido a un problema de contenedor, por ejemplo.
   - **Todo sano**: El almacenamiento ha sido gestionado y se encuentra en un estado óptimo.
   - **Descubierto**: El almacenamiento ha sido descubierto, pero no gestionado por Astra Control.

Consulte los detalles del backends de almacenamiento en la opción Backends

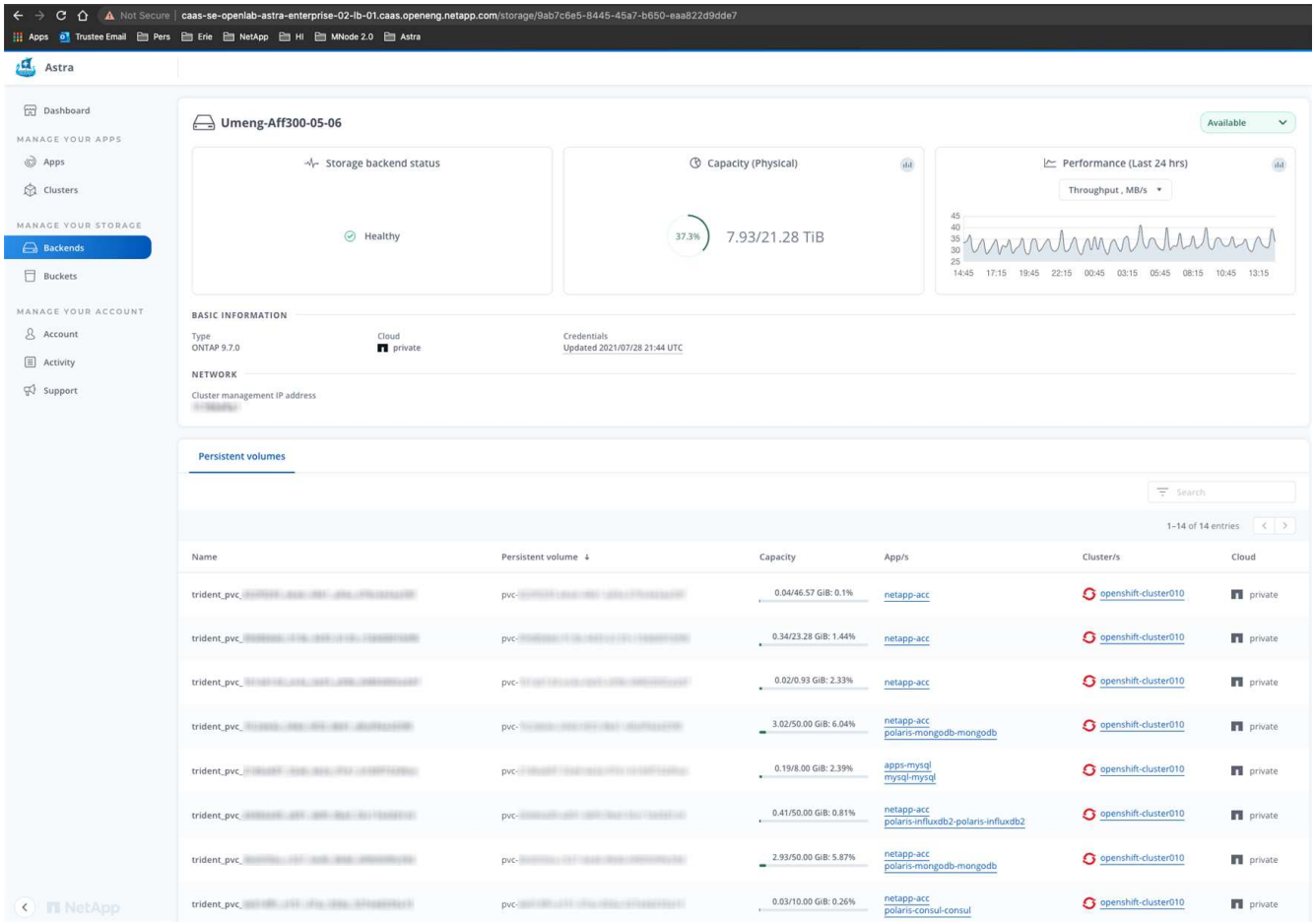
Vea información sobre el estado, la capacidad y el rendimiento del back-end (rendimiento de IOPS y/o latencia).

Con una conexión a Cloud Insights, puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado.

Pasos

1. En el área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.

> Si conectas a Cloud Insights de NetApp, aparecerán extractos de datos de Cloud Insights en la página backends.



3. Para ir directamente a Cloud Insights, seleccione el icono **Cloud Insights** junto a la imagen de métricas.

Desgestione un back-end de almacenamiento

Puede anular la gestión del back-end.

Pasos

1. En la navegación izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el menú acciones, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar la eliminación.
5. Seleccione **Sí, quite el backend de almacenamiento**.

Obtenga más información

- "Utilice la API Astra Control"

Supervise y proteja la infraestructura

Puede configurar varios ajustes opcionales para mejorar su experiencia con Astra Control Center. Si la red en la que ejecuta Astra Control Center requiere un proxy para conectarse a Internet (para cargar los paquetes de soporte en el sitio de soporte de NetApp o establecer una conexión con Cloud Insights), debe configurar un servidor proxy en Astra Control Center. Para supervisar y obtener información sobre toda su infraestructura, cree una conexión con Cloud Insights de NetApp. Para recopilar eventos Kubernetes de sistemas supervisados por Astra Control Center, añada una conexión fluentd.

Agregar un servidor proxy

Si la red en la que ejecuta Astra Control Center requiere un proxy para conectarse a Internet (para cargar los paquetes de soporte en el sitio de soporte de NetApp o establecer una conexión con Cloud Insights), debe configurar un servidor proxy en Astra Control Center.

Astra Control Center no valida los detalles introducidos para su servidor proxy. Asegúrese de introducir los valores correctos.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** en la lista desplegable para agregar un servidor proxy.

4. Introduzca el nombre o la dirección IP del servidor proxy y el número de puerto del proxy.
5. Si su servidor proxy requiere autenticación, marque la casilla de verificación e introduzca el nombre de usuario y la contraseña.
6. Seleccione **conectar**.

Resultado

Si se guardó la información de proxy introducida, la sección **proxy HTTP** de la página **cuenta** > **conexiones** indica que está conectada y muestra el nombre del servidor.

Edite la configuración del servidor proxy

Puede editar la configuración del servidor proxy.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** en la lista desplegable para editar la conexión.
4. Edite los detalles del servidor y la información de autenticación.
5. Seleccione **Guardar**.

Desactive la conexión del servidor proxy

Puede desactivar la conexión del servidor proxy. Se le advertirá antes de desactivar que se pueden producir posibles interrupciones en otras conexiones.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación.

Conéctese a Cloud Insights

Para supervisar y obtener información sobre toda su infraestructura, conecte Cloud Insights de NetApp con su instancia de Astra Control Center. Cloud Insights está incluido en su licencia de Astra Control Center.

Debe accederse a Cloud Insights desde la red que utiliza Astra Control Center, o indirectamente mediante un servidor proxy.

Cuando el Centro de control de Astra está conectado a Cloud Insights, se crea un POD de unidad de adquisición. Este pod recoge datos de los back-ends de almacenamiento gestionados por Astra Control Center y los empuja a Cloud Insights. Este pod requiere 8 GB de RAM y 2 núcleos de CPU.

Después de activar la conexión Cloud Insights, puede ver la información de rendimiento en la página **backends** así como conectarse a Cloud Insights desde aquí después de seleccionar un back-end de almacenamiento. También puede encontrar la información en **Panel** en la sección clúster, y también puede conectarse a Cloud Insights desde allí.

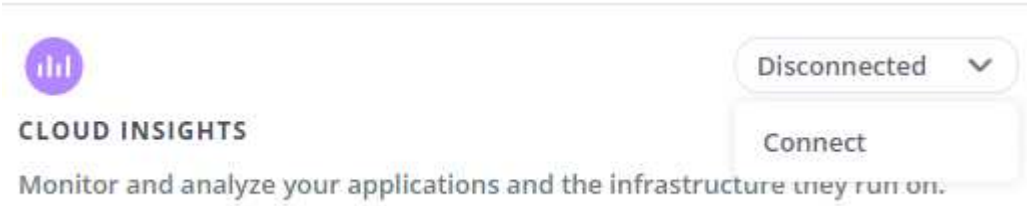
Lo que necesitará

- Una cuenta de Astra Control Center con privilegios **admin**/**owner**.
- Una licencia válida de Astra Control Center.
- Un servidor proxy si la red en la que se ejecuta Astra Control Center requiere un proxy para conectarse a Internet.

Si no tiene experiencia en Cloud Insights, familiarícese con las funciones y las funcionalidades. Consulte "Documentación de Cloud Insights".

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** donde aparece **Desconectado** en la lista desplegable para agregar la conexión.

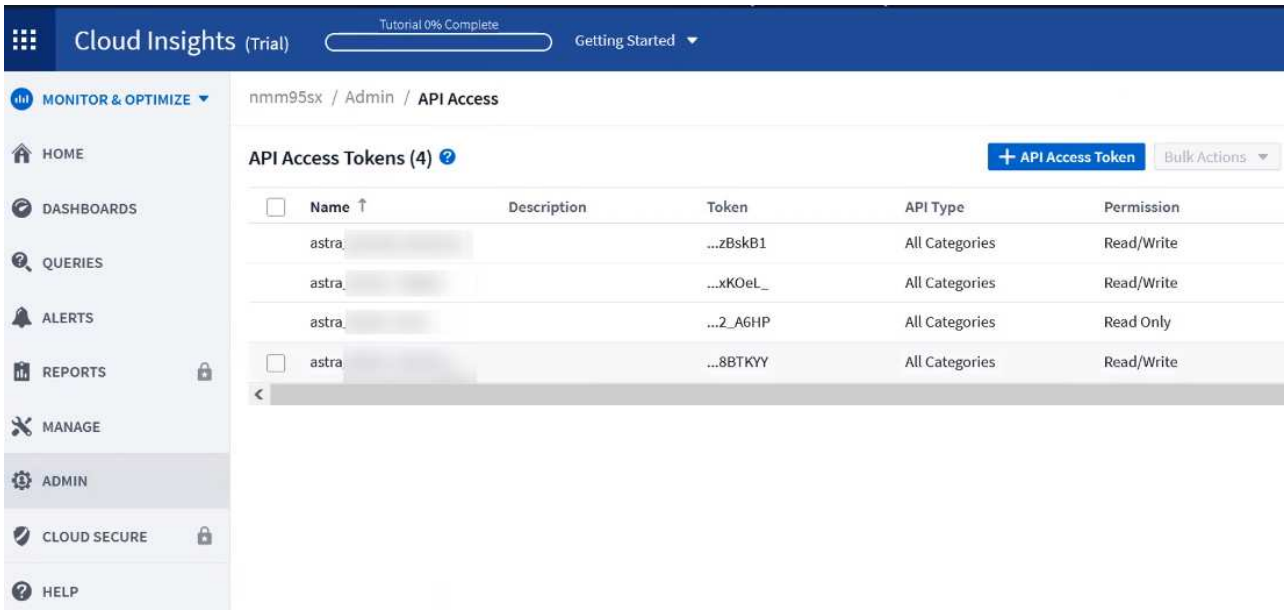


4. Introduzca los tokens de la API Cloud Insights y la URL del inquilino. La URL del inquilino tiene el siguiente formato, como ejemplo:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Obtiene la URL de inquilino al obtener la licencia de Cloud Insights. Si no tiene la URL de inquilino, consulte "Documentación de Cloud Insights".

a. Para obtener la "Token de API", Inicie sesión en la dirección URL del inquilino de Cloud Insights.
b. En Cloud Insights, genere un token de acceso de **lectura/escritura** y un símbolo de acceso de API **sólo lectura** haciendo clic en **Admin** > **acceso de API**.



c. Copie la tecla **sólo lectura**. Deberá pegarlo en la ventana Centro de control de Astra para habilitar la conexión a Cloud Insights. Para los permisos de clave de token de acceso a la API de lectura, seleccione: Activos, Alertas, Unidad de adquisición y recolección de datos.

d. Copie la tecla **Read/Write**. Deberá pegarlo en la ventana Centro de control de Astra **Connect Cloud Insights**. Para los permisos de clave de acceso a la API de lectura/escritura, seleccione: Activos, ingestión de datos, ingestión de registros, unidad de adquisición, Y recopilación de datos.

> Le recomendamos que genere una tecla **sólo lectura** y una tecla **Leer/escribir**, y que no utilice la misma clave para ambos propósitos. De forma predeterminada, el período de caducidad del token se establece en un año. Le recomendamos que mantenga la selección predeterminada para dar al token la duración máxima antes de que caduque. Si el token caduca, la telemetría se detendrá.

e. Pegue las claves que ha copiado de Cloud Insights en Astra Control Center.

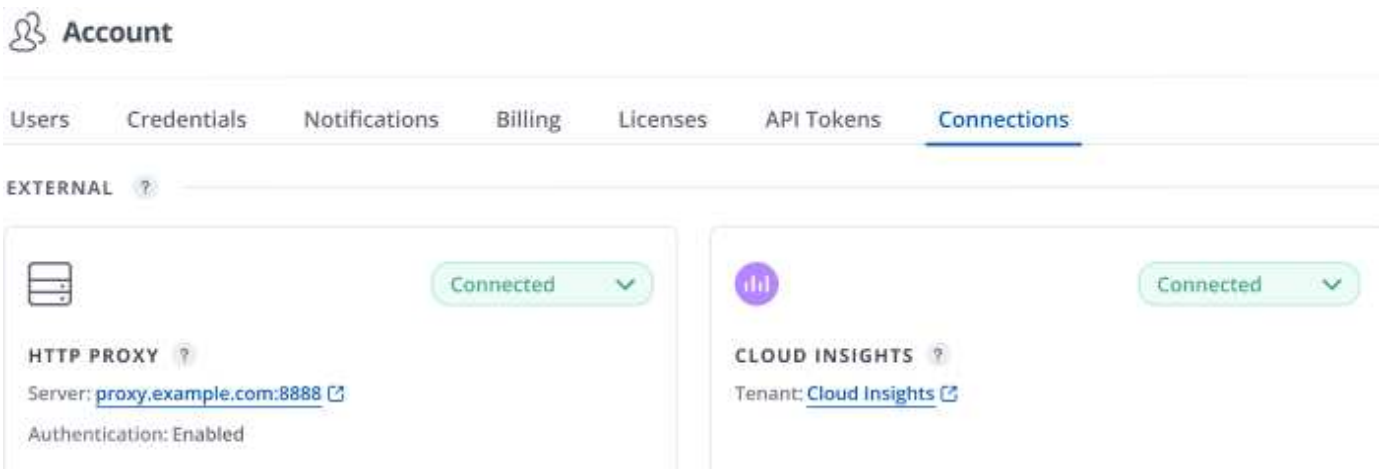
5. Seleccione **conectar**.

> Después de seleccionar **conectar,** el estado de la conexión cambia a **pendiente** en la sección **Cloud Insights** de la página **cuenta** > **conexiones**. Puede pasar unos minutos para que la conexión esté activada y el estado cambie a **conectado**.

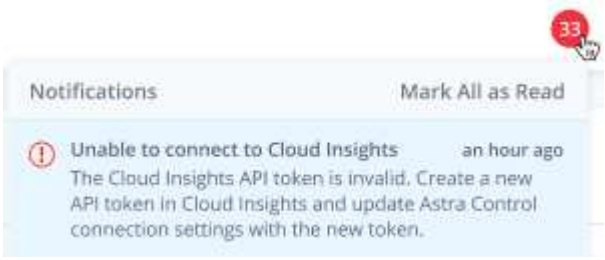
> Para retroceder y avanzar fácilmente entre el Centro de control de Astra y las interfaces de usuario de Cloud Insights, asegúrese de que ha iniciado sesión en ambos.

Ver datos en Cloud Insights

Si la conexión se realizó correctamente, la sección **Cloud Insights** de la página **cuenta** > **conexiones** indica que está conectada y muestra la dirección URL del inquilino. Puede visitar Cloud Insights para ver los datos que se han recibido y mostrado correctamente.

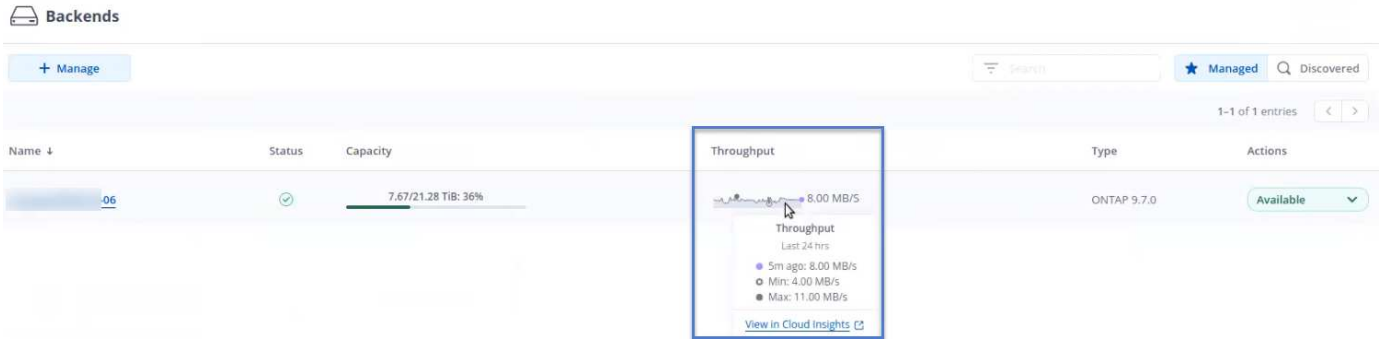


Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.



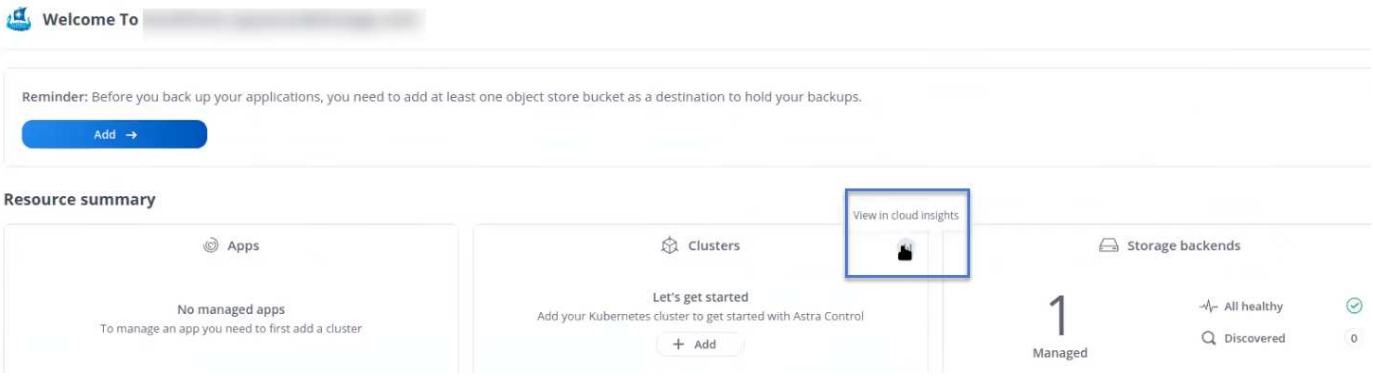
También puede encontrar la misma información en **cuenta** > **Notificaciones**.

Desde Astra Control Center, puede ver la información sobre el rendimiento en la página **backends**, así como conectarse a Cloud Insights desde aquí tras seleccionar un backend de almacenamiento.



Para ir directamente a Cloud Insights, seleccione el icono **Cloud Insights** junto a la imagen de métricas.

También puede encontrar la información en el **Panel**.



Después de habilitar la conexión Cloud Insights, si quita los back-ends que agregó en Astra Control Center, los back-ends dejan de informar a Cloud Insights.

Editar conexión Cloud Insights

Puede editar la conexión Cloud Insights.

Solo puede editar las claves de API. Para cambiar la URL de inquilino de Cloud Insights, le recomendamos que desconecte la conexión de Cloud Insights y se conecte con la nueva URL.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** en la lista desplegable para editar la conexión.
4. Edite la configuración de la conexión Cloud Insights.
5. Seleccione **Guardar**.

Deshabilite la conexión Cloud Insights

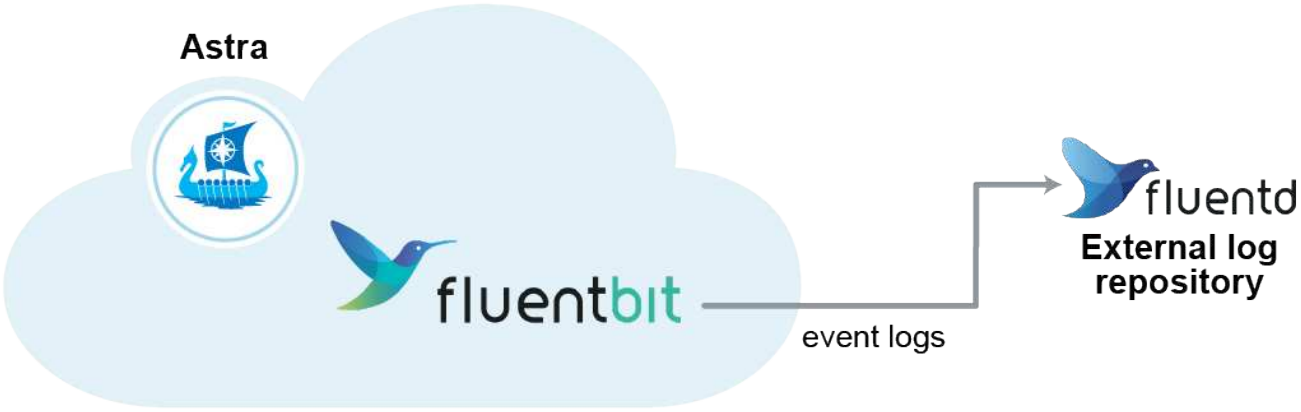
Puede deshabilitar la conexión Cloud Insights para un clúster de Kubernetes gestionado por Astra Control Center. Al deshabilitar la conexión Cloud Insights, no se eliminan los datos de telemetría ya cargados en Cloud Insights.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación. Después de confirmar la operación, en la página **cuenta** > **conexiones**, el estado de Cloud Insights cambia a **pendiente**. El estado tarda unos minutos en cambiar a **desconectado**.

Conectar a Fluentd

Puede enviar registros (eventos Kubernetes) desde Astra Control Center a su terminal Fluentd. La conexión fluentd está desactivada de forma predeterminada.



Sólo se reenvían a Fluentd los registros de eventos de los clusters gestionados.

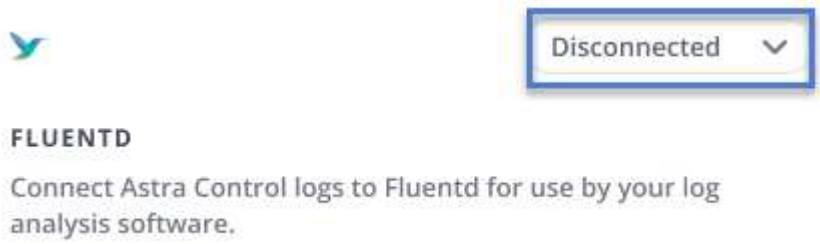
Lo que necesitará

- Una cuenta de Astra Control Center con privilegios **admin**/**owner**.
- Astra Control Center se ha instalado y se ejecuta en un clúster de Kubernetes.

Astra Control Center no valida los detalles que introduzca para su servidor Fluentd. Asegúrese de introducir los valores correctos.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **conectar** en la lista desplegable en la que aparece **Desconectado** para agregar la conexión.



4. Introduzca la dirección IP del host, el número de puerto y la clave compartida para el servidor Fluentd.
5. Seleccione **conectar**.

Resultado

Si se guardaron los datos introducidos para el servidor Fluentd, la sección **Fluentd** de la página **cuenta** > **conexiones** indica que está conectado. Ahora puede visitar el servidor Fluentd que ha conectado y ver los registros de eventos.

Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.

También puede encontrar la misma información en **cuenta** > **Notificaciones**.

Si tiene problemas con la recopilación de registros, debe iniciar sesión en el nodo de trabajo y asegurarse de que los registros están disponibles en `/var/log/containers/`.

Edite la conexión fluentd

Puede editar la conexión Fluentd a su instancia de Astra Control Center.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **Editar** en la lista desplegable para editar la conexión.
4. Cambie la configuración del extremo fluentd.
5. Seleccione **Guardar**.

Desactive la conexión fluentd

Puede desactivar la conexión Fluentd a la instancia de Astra Control Center.

Pasos

1. Inicie sesión en Astra Control Center utilizando una cuenta con privilegios **admin**/**owner**.
2. Seleccione **cuenta** > **conexiones**.
3. Seleccione **desconectar** en la lista desplegable para desactivar la conexión.
4. En el cuadro de diálogo que se abre, confirme la operación.

Actualizar una licencia existente

Puede convertir una licencia de evaluación a una licencia completa, o puede actualizar una evaluación existente o una licencia completa con una nueva licencia. Si no tiene una licencia completa, trabaje con su contacto de ventas de NetApp para obtener un número de serie y una licencia completa. Puede utilizar la interfaz de usuario de Astra o. "La API de control Astra" para actualizar una licencia existente.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp".
2. Acceda a la página de descarga de Astra Control Center, introduzca el número de serie y descargue el archivo de licencia completo de NetApp (NLF).
3. Inicie sesión en la interfaz de usuario de Astra Control Center.
4. En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
5. En la página **cuenta** > **Licencia**, seleccione el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta** > **licencias** 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.

Desgestione aplicaciones y clústeres

Elimine las aplicaciones o clústeres que ya no desee gestionar desde Astra Control Center.

Desgestionar una aplicación

Detenga la gestión de las aplicaciones de las que ya no desee realizar copias de seguridad, copias Snapshot o clones de Astra Control Center.

- Se eliminarán todos los backups y las snapshots existentes.
- Las aplicaciones y los datos siguen estando disponibles.

Pasos

1. En la barra de navegación izquierda, seleccione **aplicaciones**.
2. Seleccione la casilla de verificación de las aplicaciones que ya no desea gestionar.
3. En el menú **Acción**, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar.
5. Confirme que desea anular la administración de las aplicaciones y, a continuación, seleccione **Sí, anular la administración de la aplicación**.

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

Anule la gestión del clúster que ya no desea administrar desde Astra Control Center.

- Con esta acción, Astra Control Center no gestiona su clúster. No realiza cambios en la configuración del clúster y no elimina el clúster.
- Trident no se desinstalará del clúster. "Descubra cómo desinstalar Trident".

> Antes de anular la administración del clúster, debe anular la administración de las aplicaciones asociadas al clúster.

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla del clúster que ya no desea gestionar en Astra Control Center.
3. En el menú **acciones**, seleccione **Unmanage**.
4. Confirme que desea anular la administración del clúster y, a continuación, seleccione **Sí, anular la administración del clúster**.

Resultado

El estado del clúster cambia a **Extracción** y después de que el clúster se eliminará de la página **Clusters** y Astra Control Center ya no lo gestiona.

Si el Centro de control de Astra y Cloud Insights no están conectados, al anular la gestión del clúster se quitan todos los recursos que se instalaron para enviar datos de telemetría. **Si el Centro de control de Astra y Cloud Insights están conectados**, al anular la gestión del clúster sólo se elimina el `fluentbit` y.. `event-exporter` pods.

Actualice Astra Control Center

Para actualizar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y complete estas instrucciones para actualizar los componentes de Astra Control Center en su entorno. Puede utilizar este procedimiento para actualizar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Lo que necesitará

- "Antes de comenzar la actualización, asegúrese de que su entorno cumple los requisitos mínimos para la implementación de Astra Control Center".
- Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

  Ejemplo de OpenShift:

  ```
  oc get clusteroperators
  ```

- Asegúrese de que todos los servicios de API están en buen estado y disponibles.

  Ejemplo de OpenShift:

  ```
  oc get apiservices
  ```

- Cierre la sesión en Astra Control Center.

Acerca de esta tarea

El proceso de actualización del Centro de control de Astra le guiará por los siguientes pasos de alto nivel:

- Descargue el paquete Astra Control Center
- Desembale el paquete y cambie el directorio
- Agregue las imágenes al registro local
- Instale el operador actualizado de Astra Control Center
- Actualice Astra Control Center
- Actualizar servicios de terceros
- Comprobar el estado del sistema

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

Realice actualizaciones en una ventana de mantenimiento cuando no se estén ejecutando las programaciones, los backups y las snapshots.

Los comandos de Podman se pueden utilizar en lugar de los comandos de Docker si está utilizando Podman de Red Hat en lugar de Docker Engine.

Descargue el paquete Astra Control Center

1. Descargue el paquete de actualización de Astra Control Center (`astra-control-center-[version].tar.gz`) del "Sitio de soporte de NetApp".
2. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

Desembale el paquete y cambie el directorio

1. Extraiga las imágenes:

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

2. Cambie al directorio Astra.

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

Agregue las imágenes al registro local

1. Agregue los archivos del directorio imagen de Astra Control Center al registro local.

   Consulte una secuencia de comandos de ejemplo para la carga automática de imágenes a continuación.

   a. Inicie sesión en su registro de Docker:

   ```
   docker login [your_registry_path]
   ```

   b. Cargue las imágenes en Docker.

   c. Etiquete las imágenes.

   d. empuje las imágenes al registro local.

```
export REGISTRY=[your_registry_path]
for astraImageFile in $(ls images/*.tar)
  # Load to local cache. And store the name of the loaded image
trimming the 'Loaded images: '
  do astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

Instale el operador actualizado de Astra Control Center

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

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

   b. Cambiar `[your_registry_path]` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

   c. Cambiar `[your_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un paso anterior.

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

2. Instale el operador actualizado de Astra Control Center:

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

Respuesta de ejemplo:

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

Actualice Astra Control Center

1. Edite el recurso personalizado de Astra Control Center (CR) y cambie la versión de Astra (`astraVersion` dentro de `Spec`) número a la última:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> Cambiar la versión Astra es el único requisito para una actualización a Astra Control Center. La ruta de acceso del Registro debe coincidir con la ruta de acceso del Registro en la que ha insertado las imágenes en un paso anterior.

2. Compruebe que los POD terminan y estén disponibles de nuevo:

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

3. Compruebe que todos los componentes del sistema se han actualizado correctamente.

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

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

Respuesta de ejemplo:

```
NAME                                          READY   STATUS    RESTARTS
AGE
acc-helm-repo-5f75c5f564-bzqmt                1/1     Running   0
11m
activity-6b8f7cccb9-mlrn4                     1/1     Running   0
9m2s
api-token-authentication-6hznt                1/1     Running   0
8m50s
api-token-authentication-qpfgb                1/1     Running   0
8m50s
api-token-authentication-sqnb7                1/1     Running   0
8m50s
asup-5578bbdd57-dxkbp                         1/1     Running   0
9m3s
authentication-56bff4f95d-mspmq               1/1     Running   0
7m31s
bucketservice-6f7968b95d-9rrrl                1/1     Running   0
8m36s
cert-manager-5f6cf4bc4b-82khn                 1/1     Running   0
6m19s
cert-manager-cainjector-76cf976458-sdrbc      1/1     Running   0
6m19s
cert-manager-webhook-5b7896bfd8-2n45j         1/1     Running   0
6m19s
cloud-extension-749d9f684c-8bdhq              1/1     Running   0
9m6s
cloud-insights-service-7d58687d9-h5tzw        1/1     Running   2
8m56s
composite-compute-968c79cb5-nv7l4             1/1     Running   0
9m11s
composite-volume-7687569985-jg9gg             1/1     Running   0
8m33s
credentials-5c9b75f4d6-nx9cz                  1/1     Running   0
8m42s
entitlement-6c96fd8b78-zt7f8                  1/1     Running   0
8m28s
features-5f7bfc9f68-gsjnl                     1/1     Running   0
8m57s
fluent-bit-ds-h88p7                           1/1     Running   0
7m22s
fluent-bit-ds-krhnj                           1/1     Running   0
7m23s
fluent-bit-ds-l5bjj                           1/1     Running   0
7m22s
```

```
fluent-bit-ds-lrclb                          1/1     Running   0
7m23s
fluent-bit-ds-s5t4n                          1/1     Running   0
7m23s
fluent-bit-ds-zpr6v                          1/1     Running   0
7m22s
graphql-server-5f5976f4bd-vbb4z              1/1     Running   0
7m13s
identity-56f78b8f9f-8h9p9                    1/1     Running   0
8m29s
influxdb2-0                                  1/1     Running   0
11m
krakend-6f8d995b4d-5khkl                     1/1     Running   0
7m7s
license-5b5db87c97-jmxzc                     1/1     Running   0
9m
login-ui-57b57c74b8-6xtv7                    1/1     Running   0
7m10s
loki-0                                       1/1     Running   0
11m
monitoring-operator-9dbc9c76d-8znck          2/2     Running   0
7m33s
nats-0                                       1/1     Running   0
11m
nats-1                                       1/1     Running   0
10m
nats-2                                       1/1     Running   0
10m
nautilus-6b9d88bc86-h8kfb                    1/1     Running   0
8m6s
nautilus-6b9d88bc86-vn68r                    1/1     Running   0
8m35s
openapi-b87d77dd8-5dz9h                      1/1     Running   0
9m7s
polaris-consul-consul-5ljfb                  1/1     Running   0
11m
polaris-consul-consul-s5d5z                  1/1     Running   0
11m
polaris-consul-consul-server-0               1/1     Running   0
11m
polaris-consul-consul-server-1               1/1     Running   0
11m
polaris-consul-consul-server-2               1/1     Running   0
11m
polaris-consul-consul-twmpq                  1/1     Running   0
11m
```

```
polaris-mongodb-0                          2/2     Running   0
11m
polaris-mongodb-1                          2/2     Running   0
10m
polaris-mongodb-2                          2/2     Running   0
10m
polaris-ui-84dc87847f-zrg8w                1/1     Running   0
7m12s
polaris-vault-0                            1/1     Running   0
11m
polaris-vault-1                            1/1     Running   0
11m
polaris-vault-2                            1/1     Running   0
11m
public-metrics-657698b66f-67pgt            1/1     Running   0
8m47s
storage-backend-metrics-6848b9fd87-w7x8r   1/1     Running   0
8m39s
storage-provider-5ff5868cd5-r9hj7          1/1     Running   0
8m45s
telegraf-ds-dw4hg                          1/1     Running   0
7m23s
telegraf-ds-k92gn                          1/1     Running   0
7m23s
telegraf-ds-mmxjl                          1/1     Running   0
7m23s
telegraf-ds-nhs8s                          1/1     Running   0
7m23s
telegraf-ds-rj7lw                          1/1     Running   0
7m23s
telegraf-ds-tqrkb                          1/1     Running   0
7m23s
telegraf-rs-9mwgj                          1/1     Running   0
7m23s
telemetry-service-56c49d689b-ffrzx         1/1     Running   0
8m42s
tenancy-767c77fb9d-g9ctv                   1/1     Running   0
8m52s
traefik-5857d87f85-7pmx8                   1/1     Running   0
6m49s
traefik-5857d87f85-cpxgv                   1/1     Running   0
5m34s
traefik-5857d87f85-lvmlb                   1/1     Running   0
4m33s
traefik-5857d87f85-t2xlk                   1/1     Running   0
4m33s
```

```
traefik-5857d87f85-v9wpf                  1/1     Running   0
7m3s
trident-svc-595f84dd78-zb8l6              1/1     Running   0
8m54s
vault-controller-86c94fbf4f-krttq         1/1     Running   0
9m24s
```

4. Compruebe que las condiciones de estado de Astra indican que la actualización está completa y lista:

```
kubectl get -o yaml -n [netapp-acc or custom namespace]
astracontrolcenters.astra.netapp.io astra
```

Respuesta:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

Actualizar servicios de terceros

Los servicios de otros fabricantes Traefik y Cert-Manager no se actualizan durante los pasos de actualización anteriores. Opcionalmente, puede actualizarlos con el procedimiento descrito aquí o conservar versiones de servicio existentes si su sistema lo requiere. La siguiente es la secuencia de actualización recomendada de Trafik y Certs-Manager:

1. Configure ACC-helm-repo para actualizar Traefik y Cert-Manager
2. Actualizar el servicio Traefik utilizando ACC-helm-repo
3. Actualice el servicio de Cert-Manager

Configure ACC-helm-repo para actualizar Traefik y Cert-Manager

1. Busque la `enterprise-helm-repo` Que se carga en la caché de Docker local:

```
docker images enterprise-helm-repo
```

Respuesta:

```
REPOSITORY              TAG          IMAGE ID       CREATED         SIZE
enterprise-helm-repo    21.10.218    7a182d6b30f3   20 hours ago    464MB
```

2. Inicie un contenedor utilizando la etiqueta del paso anterior:

```
docker run -dp 8082:8080 enterprise-helm-repo:21.10.218
```

Respuesta:

```
940436e67fa86d2c4559ac4987b96bb35588313c2c9ddc9cec195651963f08d8
```

3. Agregue el campo Helm repo a los repositorios locales de host:

```
helm repo add acc-helm-repo http://localhost:8082/
```

Respuesta:

```
"acc-helm-repo" has been added to your repositories
```

4. Guarde el siguiente script de Python como un archivo, por ejemplo, `set_previous_values.py`:

> Este script de Python crea dos archivos que se utilizan en pasos posteriores de actualización para conservar los valores del timón.

```
#!/usr/bin/env python3
import json
import os

NAMESPACE = "netapp-acc"

os.system(f"helm get values traefik -n {NAMESPACE} -o json >
traefik_values.json")
os.system(f"helm get values cert-manager -n {NAMESPACE} -o json >
cert_manager_values.json")

# reformat traefik values
f = open("traefik_values.json", "r")
traefik_values = {'traefik': json.load(f)}
f.close()

with open('traefik_values.json', 'w') as output_file:
    json.dump(traefik_values, output_file)

# reformat cert-manager values
f = open("cert_manager_values.json", "r")
cm_values = {'cert-manager': json.load(f)}
f.close()

cm_values['global'] = cm_values['cert-manager']['global']
del cm_values['cert-manager']['global']

with open('cert_manager_values.json', 'w') as output_file:
    json.dump(cm_values, output_file)

print('Done')
```

5. Ejecute el script:

```
python3.7 ./set_previous_values.py
```

Actualizar el servicio Traefik utilizando ACC-helm-repo

Debe tener configurar según el timón-repo antes de completar el siguiente procedimiento.

1. Descargue el paquete Traefik usando una herramienta segura de transferencia de archivos, como GNU wget:

```
wget http://localhost:8082/traefik-0.2.0.tgz
```

2. Extraiga las imágenes:

```
tar -vxzf traefik-0.2.0.tgz
```

3. Aplique los CRD de Traefik:

```
kubectl apply -f ./traefik/charts/traefik/crds/
```

4. Busque la versión de la carta de Helm que desea utilizar con la actualización de Traefik:

```
helm search repo acc-helm-repo/traefik
```

Respuesta:

```
NAME                                    CHART VERSION   APP VERSION
DESCRIPTION
acc-helm-repo/traefik                   0.2.0           2.5.3       Helm
chart for Traefik Ingress controller
acc-helm-repo/traefik-ingressroutes   0.2.0           2.5.3       A Helm
chart for Kubernetes
```

5. Valide el archivo travefik_Values.json para la actualización:
   a. Abra el archivo travefik_Values.json.
   b. Compruebe si hay un valor para `imagePullSecret` campo. Si está vacío, quite el siguiente texto del archivo:

```
"imagePullSecrets": [{"name": ""}],
```

   c. Asegúrese de que la imagen de trafik se dirige a la ubicación correcta y tiene el nombre correcto:

```
image: [your_registry_path]/traefik
```

6. Actualice su configuración de Traefik:

```
helm upgrade --version 0.2.0 --namespace netapp-acc -f
traefik_values.json traefik acc-helm-repo/traefik
```

Respuesta:

```
Release "traefik" has been upgraded. Happy Helming!
NAME: traefik
LAST DEPLOYED: Mon Oct 25 22:53:19 2021
NAMESPACE: netapp-acc
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

Actualice el servicio de Cert-Manager

Debe haber completado el Actualización de Traefik y.. Añadido ACC-helm-repo en Helm antes de completar el siguiente procedimiento.

1. Encuentra la versión de la carta de timón que deberás utilizar con tu gerente de cert actualizado:

```
helm search repo acc-helm-repo/cert-manager
```

Respuesta:

```
NAME CHART VERSION APP VERSION DESCRIPTION
acc-helm-repo/cert-manager 0.3.0 v1.5.4 A Helm chart for cert-manager
acc-helm-repo/cert-manager-certificates 0.1.0 1.16.0 A Helm chart for
Kubernetes
```

2. Valide el archivo cert_Manager_Values.json para actualizar:
   a. Abra el archivo cert_Manager_Values.json.
   b. Compruebe si hay un valor para `imagePullSecret` campo. Si está vacío, quite el siguiente texto del archivo:

```
"imagePullSecrets": [{"name": ""}],
```

   c. Asegúrese de que las tres imágenes del administrador de certificados se dirigen a la ubicación correcta y tienen los nombres correctos.
3. Actualice su configuración de Cert-Manager:

```
helm upgrade --version 0.3.0 --namespace netapp-acc -f
cert_manager_values.json cert-manager acc-helm-repo/cert-manager
```

Respuesta:

```
Release "cert-manager" has been upgraded. Happy Helming!
NAME: cert-manager
LAST DEPLOYED: Tue Nov 23 11:20:05 2021
NAMESPACE: netapp-acc
STATUS: deployed
REVISION: 2
TEST SUITE: None
```

Comprobar el estado del sistema

1. Inicie sesión en Astra Control Center.
2. Compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.

Desinstale Astra Control Center

Es posible que necesite eliminar los componentes de Astra Control Center si va a actualizar de una versión de prueba a una versión completa del producto. Para retirar el Centro de control Astra y el operador del Centro de control Astra, ejecute las instrucciones descritas en este procedimiento en secuencia.

Lo que necesitará

- Utilice la interfaz de usuario de Astra Control Center para anular la gestión de todos "de clúster".

Pasos

1. Eliminar Astra Control Center. El comando de ejemplo siguiente se basa en una instalación predeterminada. Modifique el comando si ha realizado configuraciones personalizadas.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Resultado:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utilice el siguiente comando para eliminar la `netapp-acc` espacio de nombres:

   ```
   kubectl delete ns netapp-acc
   ```

   Resultado:

   ```
   namespace "netapp-acc" deleted
   ```

3. Utilice el siguiente comando para eliminar los componentes del sistema del operador de Astra Control Center:

```
kubectl delete -f astra_control_center_operator_deploy.yaml
```

Resultado:

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

Obtenga más información

- "Problemas conocidos para la desinstalación"