Utilice Astra

Astra Control Center

NetApp
June 06, 2024

Tabla de contenidos

Utilice Astra

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.

Para obtener más información, consulte "Requisitos de gestión de aplicaciones".

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 que, en general, están diseñados con una arquitectura de "paso por valor" en lugar de "paso por referencia". 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.

  Las siguientes son algunas aplicaciones del operador que siguen estos patrones:

  - "Apache K8ssandra"

    > Para K8ssandra, se admiten operaciones de restauración in situ. Una operación de restauración a un nuevo espacio de nombres o clúster requiere que se apague la instancia original de la aplicación. Esto es para garantizar que la información del grupo de pares no conduzca a la comunicación entre instancias. No se admite la clonación de la aplicación.

  - "Jenkins CI"
  - "Clúster Percona XtraDB"

Es posible que Astra Control no pueda clonar a un operador diseñado con una arquitectura "pase 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.

Instale las aplicaciones en el clúster

La tienes "ha agregado el 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 único.

Gestionar aplicaciones

Una vez que Astra Control detecta espacios de nombres en sus clústeres, puede definir las aplicaciones que desea administrar. Puede elegir "gestione un espacio de nombres completo como una única aplicación o gestione una o varias aplicaciones en el espacio de nombres de forma individual". Todo se reduce al nivel de granularidad que necesita para las operaciones de protección de datos.

Aunque 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.

A modo de ejemplo, puede que desee establecer 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 como una aplicación de espacio de nombres único.

Lo que necesitará

- Se añadió un clúster de Kubernetes a Astra Control.
- Una o más aplicaciones instaladas en el clúster. Obtenga más información sobre los métodos de instalación de aplicaciones compatibles.
- Uno o más pods activos.
- Espacios de nombres especificados en el clúster Kubernetes que se agregó a Astra Control.
- Etiqueta de Kubernetes (opcional) en cualquiera "Recursos de Kubernetes compatibles".

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".

Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".

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

Opciones de gestión de aplicaciones

- Defina los recursos que se van a administrar como una aplicación
- Defina un espacio de nombres para administrar como una aplicación

Opciones de gestión de aplicaciones adicionales

- Desgestionar aplicaciones

Defina los recursos que se van a administrar como una aplicación

Puede especificar el "Los recursos de Kubernetes forman una aplicación" Que desea gestionar con Astra Control. Definir una aplicación le permite agrupar elementos de su clúster de Kubernetes en una única aplicación. Esta colección de recursos de Kubernetes está organizada por criterios de espacio de nombres y selector de etiquetas.

Definir una aplicación le proporciona un control más granular de lo que se debe incluir en una operación Astra Control, que incluye clonado, copias Snapshot y backups.

Al definir aplicaciones, asegúrese de no incluir un recurso de Kubernetes en varias aplicaciones con políticas de protección. La superposición de políticas de protección en recursos de Kubernetes puede provocar conflictos de datos. Obtenga más información acerca de las prácticas recomendadas.

Pasos

1. En la página aplicaciones, seleccione **definir**.
2. En la ventana **definir aplicación**, introduzca el nombre de la aplicación.
3. Seleccione el clúster en el que se ejecuta la aplicación en la lista desplegable **Cluster**.
4. Seleccione el espacio de nombres de la aplicación en la lista desplegable **espacio de nombres**.

   Las aplicaciones solo se pueden definir dentro de un espacio de nombres especificado en un único clúster. Astra Control no admite la capacidad de que las aplicaciones abarquen varios espacios de nombres o clústeres.

5. Introduzca una etiqueta para la aplicación y el espacio de nombres. Puede especificar una sola etiqueta o un criterio de selector de etiquetas (consulta).

   Para obtener más información acerca de las etiquetas de Kubernetes, "Consulte la documentación oficial de Kubernetes".

6. Después de seleccionar **definir**, repita el proceso para otras aplicaciones, según sea necesario.

Cuando termine de definir una aplicación, ésta aparecerá en la lista de aplicaciones de la página aplicaciones. Ahora puede clonarla y crear backups y copias Snapshot.

Es posible que la aplicación que acaba de agregar tenga un icono de advertencia en la columna protegido, lo que indica que no se ha realizado una copia de seguridad y que aún no está programada para las copias de seguridad.

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

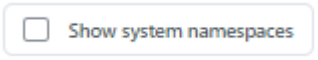
Defina un espacio de nombres para administrar como una aplicación

Puede añadir todos los recursos de Kubernetes en un espacio de nombres a la gestión de Astra Control al definir los recursos de ese espacio de nombres como una aplicación. Este método es preferible a definir las aplicaciones individualmente si piensa administrar y proteger todos los recursos de un espacio de nombres determinado de una manera similar y en intervalos comunes.

Pasos

1. En la página Clusters, seleccione un clúster.
2. Seleccione la ficha **Namespaces**.
3. Seleccione el menú acciones del espacio de nombres que contiene los recursos de aplicación que desea administrar y seleccione **definir como aplicación**.

Si desea gestionar varios espacios de nombres, seleccione los espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **gestionar**.

Active la casilla de verificación **Mostrar espacios de nombres del sistema** para mostrar los espacios de nombres del sistema que normalmente no se usan en la administración de aplicaciones de forma predeterminada. 

"Leer más".

Una vez completado el proceso, las aplicaciones asociadas al espacio de nombres aparecen en la `Associated applications` columna.

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.

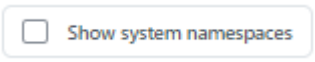
Pasos

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

¿Qué ocurre con los espacios de nombres del sistema?

Astra Control también detecta espacios de nombres de sistemas en un clúster de Kubernetes. No le mostramos estos espacios de nombres del sistema de forma predeterminada porque es raro que necesite realizar backups de los recursos de la aplicación del sistema.

Puede visualizar los espacios de nombres del sistema desde la ficha espacios de nombres de un clúster seleccionado activando la casilla de verificación **Mostrar espacios de nombres del sistema** .



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.

Ejemplo: Separar la normativa de protección para diferentes versiones

En este ejemplo, el equipo de devops gestiona una puesta en marcha de versiones «canaria». El grupo del equipo tiene tres pods que se 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: 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.

Obtenga más información

- "Utilice la API Astra Control"

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".

Además, puede replicar aplicaciones en un clúster remoto como preparación para la recuperación ante desastres.

Flujo de trabajo de protección de aplicaciones

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

[Uno] Proteja 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] 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] Replicar aplicaciones en un clúster remoto

"Replicar aplicaciones" A un clúster remoto mediante la tecnología NetApp SnapMirror. Astra Control replica las instantáneas en un clúster remoto, lo que proporciona una función asíncrona y de recuperación ante desastres.

[Cinco] En caso de desastre, restaure sus aplicaciones con la última copia de seguridad o replicación en el sistema remoto

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). O bien, puede utilizar la replicación en un sistema remoto.

Proteja las aplicaciones con snapshots y backups

Proteger todas las aplicaciones mediante la toma de snapshots y backups a través de 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
```

Puede realizar las siguientes tareas relacionadas con la protección de los datos de la aplicación:

- Configure una política de protección
- Crear una copia de Snapshot
- Cree un backup
- Ver Snapshot y backups
- Eliminar snapshots
- Cancelar backups
- Eliminar backups

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

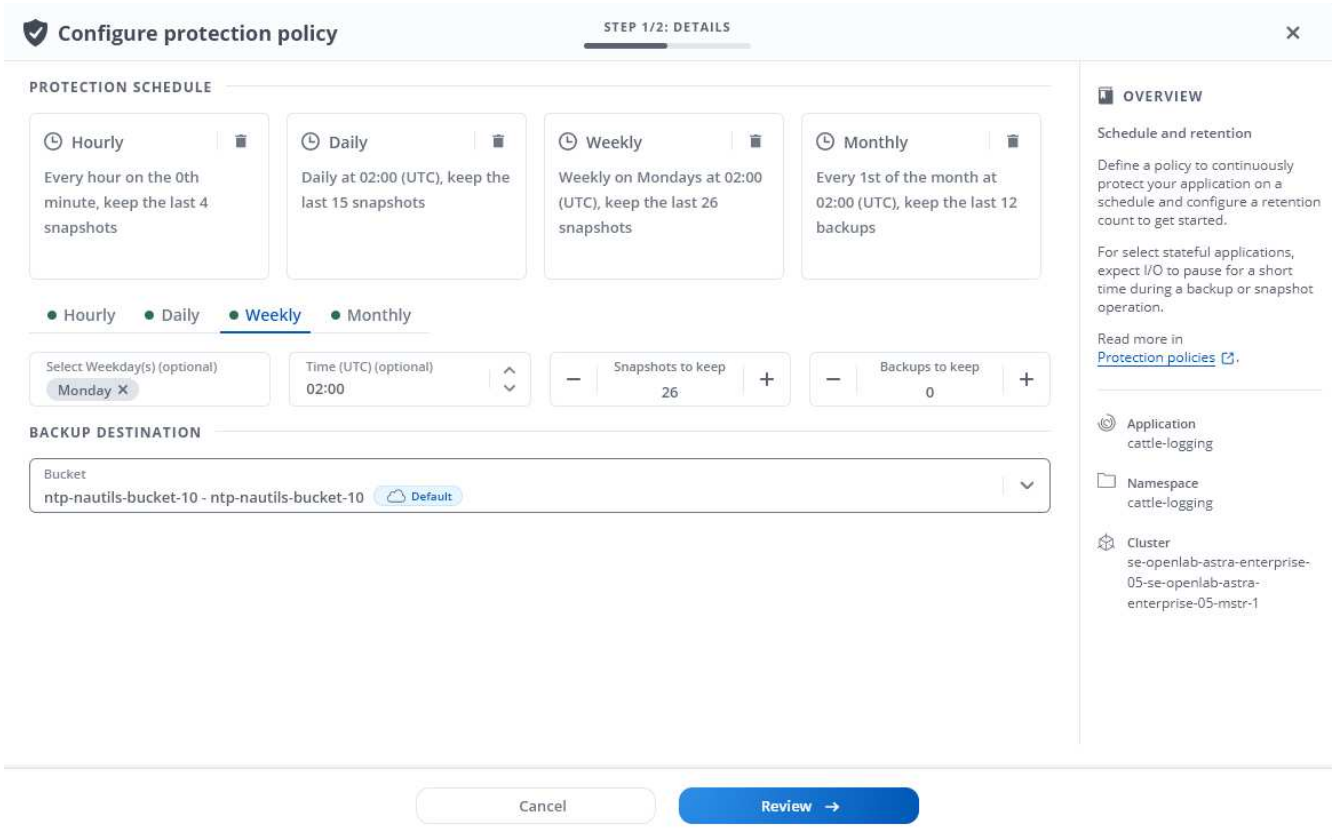
especificar la cantidad de copias que desea retener. A modo de ejemplo, una política de protección puede crear backups semanales y copias Snapshot diarias, y conservar los backups y las copias Snapshot por un mes. La frecuencia con la que se crean snapshots y backups y el tiempo que se retienen depende 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. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **Snapshot**.
3. Personalice el nombre de la instantánea y, a continuación, seleccione **Revisión**.
4. 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. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. 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.
5. Seleccione un destino para el backup seleccionando de la lista de bloques de almacenamiento.
6. Seleccione **Revisión**.
7. 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.

No puede eliminar una copia Snapshot que se está replicando actualmente.

Pasos

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

Resultado

Astra Control Center elimina la instantánea.

Cancelar backups

Es posible cancelar una copia de seguridad que esté en curso.

Para cancelar una copia de seguridad, la copia de seguridad debe estar en estado en ejecución. No es posible cancelar un backup que esté en estado Pending.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** para la copia de seguridad deseada, seleccione **Cancelar**.
5. Escriba la palabra "cancelar" para confirmar la eliminación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

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".

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Seleccione **Protección de datos**.
3. Seleccione **copias de seguridad**.
4. En el menú Opciones de la columna **acciones** de la copia de seguridad deseada, seleccione **Eliminar copia de seguridad**.
5. 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.

Acerca de esta tarea

- Se recomienda tomar una instantánea o realizar una copia de seguridad de la aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup en el caso de que la restauración no se realice correctamente.
- 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.
- Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.
- 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. En el menú Opciones de la columna **acciones** de la instantánea o copia de seguridad desde la que desea restaurar, seleccione **Restaurar aplicación**.
5. **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**.

   > Si se restaura en un espacio de nombres que se eliminó previamente, se crea un espacio de nombres nuevo con el mismo nombre como parte del proceso de restauración. Cualquier usuario que tenga derechos para administrar aplicaciones en el espacio de nombres previamente eliminado debe restaurar manualmente los derechos en el espacio de nombres recién creado.

6. **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 posterior cambio de tamaño de volumen persistente, se producen retrasos de hasta veinte minutos antes de que se muestre el nuevo tamaño del volumen en la interfaz de usuario web. 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.

Replicación de aplicaciones en un sistema remoto mediante la tecnología SnapMirror

Con Astra Control, puede aumentar la continuidad del negocio para sus aplicaciones con un objetivo de punto de recuperación (RPO) y un objetivo de tiempo de recuperación bajo (Recovery Time Objective) mediante funcionalidades de replicación asíncrona de la tecnología SnapMirror de NetApp. Una vez que se ha configurado, esto permite a sus aplicaciones replicar los cambios de aplicaciones y datos de un clúster a otro.

Para ver la comparación entre backups/restauraciones y replicación, consulte "Conceptos de protección de

datos".

Puede replicar aplicaciones en diferentes situaciones, como las siguientes situaciones de solo en las instalaciones, de cloud híbrido y multicloud:

- En el sitio Local A al sitio local B
- Del entorno local al cloud con Cloud Volumes ONTAP
- Cloud con Cloud Volumes ONTAP para infraestructura en las instalaciones
- Cloud con Cloud Volumes ONTAP al cloud (entre distintas regiones del mismo proveedor de cloud o a distintos proveedores de cloud)

Astra Control puede replicar aplicaciones en clústeres locales, de las instalaciones al cloud (mediante Cloud Volumes ONTAP) o entre clouds (Cloud Volumes ONTAP a Cloud Volumes ONTAP).

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

Con Astra Control, puede realizar las siguientes tareas relacionadas con la replicación de aplicaciones:

- Configurar una relación de replicación
- Conectar una aplicación replicada en el clúster de destino (conmutación por error)
- Se ha producido un error al sincronizar una replicación
- Replicación de aplicaciones inversa
- Conmutación tras error de las aplicaciones al clúster de origen original
- Eliminar una relación de replicación de aplicaciones

Requisitos previos de replicación

Consulte "requisitos previos de replicación" antes de empezar.

Configurar una relación de replicación

La configuración de una relación de replicación implica los siguientes elementos que componen la directiva de replicación:

- Elegir la frecuencia con la que desea que Astra Control tome una Snapshot de aplicaciones (que incluye los recursos de Kubernetes de la aplicación, así como las copias Snapshot por volumen para cada uno de los volúmenes de la aplicación)
- Elegir la programación de replicación (se incluyen recursos de Kubernetes, así como datos de volúmenes persistentes)
- Establecer el tiempo para que se tome la instantánea

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, seleccione **Configurar directiva de replicación**. O bien, en el cuadro Protección de aplicaciones, seleccione la opción acciones y seleccione **Configurar directiva de**

replicación.

4. Introduzca o seleccione la siguiente información:
   - Clúster de destino
   - **Clase de almacenamiento de destino**: Seleccione o introduzca la clase de almacenamiento que utiliza la SVM emparejado en el clúster ONTAP de destino.
   - **Tipo de replicación**: "Asincrónica" es actualmente el único tipo de replicación disponible.
   - **Espacio de nombres de destino**: Introduzca un espacio de nombres de destino nuevo o existente para el clúster de destino.

     Se sobrescribirá cualquier recurso en conflicto en el espacio de nombres seleccionado.

   - **Frecuencia de replicación**: Establezca la frecuencia con la que desea que Astra Control tome una instantánea y la replique en su destino.
   - * Offset*: Establezca el número de minutos desde la parte superior de la hora que desea que Astra Control tome una instantánea. Es posible que desee utilizar un offset para no coincidir con otras operaciones programadas. Por ejemplo, si desea tomar la copia Snapshot cada 5 minutos a partir de las 10:02, introduzca "02" como el desplazamiento minutos. El resultado sería 10:02, 10:07, 10:12, etc.
5. Seleccione **Siguiente**, revise el resumen y seleccione **Guardar**.

   Al principio, el estado muestra "app-mirror" antes de que se produzca la primera programación.

   Astra Control crea una instantánea de aplicación que se utiliza para la replicación.

6. Para ver el estado de la instantánea de la aplicación, seleccione la ficha **aplicaciones** > **instantáneas**.

   El nombre de Snapshot utiliza el formato "replication-schedule-<string>". Astra Control conserva la última snapshot utilizada para la replicación. Las snapshots de replicación más antiguas se eliminan una vez que la replicación se completa correctamente.

Resultado

De este modo se crea la relación de replicación.

Astra Control realiza las siguientes acciones como resultado de establecer la relación:

- Crea un espacio de nombres en el destino (si no existe).
- Crea un PVC en el espacio de nombres de destino correspondiente a las RVP de la aplicación de origen.
- Toma una snapshot inicial coherente con las aplicaciones.
- Establece la relación SnapMirror para los volúmenes persistentes mediante la snapshot inicial.

En la página Data Protection, se muestra el estado y estado de la relación de replicación: <Health status> | <Relationship life cycle state>

Por ejemplo: Normal | establecido

Obtenga más información sobre los estados y el estado de la replicación a continuación.

Conectar una aplicación replicada en el clúster de destino (conmutación por error)

Con Astra Control, puede "conmutar por error" las aplicaciones replicadas a un clúster de destino. Este procedimiento detiene la relación de replicación y conecta la aplicación en el clúster de destino. Este procedimiento no detiene la aplicación en el clúster de origen si estaba operativa.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **failover**.
4. En la página de conmutación por error, revise la información y seleccione **failover**.

Resultado

Las siguientes acciones ocurren como resultado del procedimiento de conmutación por error:

- En el clúster de destino, la aplicación se inicia a partir de la snapshot replicada más reciente.
- El clúster de origen y la aplicación (si están operativas) no se han detenido y se seguirá ejecutando.
- El estado de replicación cambia a "recuperación tras fallos" y luego a "recuperación tras fallos" cuando ha finalizado.
- La política de protección de la aplicación de origen se copia en la aplicación de destino en función de los horarios presentes en la aplicación de origen en el momento de la conmutación por error.
- Astra Control muestra la aplicación tanto en los clústeres de origen como de destino y su estado respectivo.

Se ha producido un error al sincronizar una replicación

La operación de resincronización vuelve a establecer la relación de replicación. Puede elegir el origen de la relación para conservar los datos en el clúster de origen o de destino. Esta operación vuelve a establecer las relaciones de SnapMirror para iniciar la replicación de volúmenes en la dirección que se desee.

El proceso detiene la aplicación en el nuevo clúster de destino antes de volver a establecer la replicación.

Durante el proceso de resincronización, el estado del ciclo de vida muestra como "establecer".

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **Resync**.
4. En la página Resync, seleccione la instancia de aplicación de origen o de destino que contenga los datos que desea conservar.

   Elija el origen de resincronización con cuidado, ya que los datos del destino se sobrescribirán.

5. Seleccione **Resync** para continuar.
6. Escriba "Resync" para confirmar.
7. Seleccione **Sí, resincronización** para finalizar.

Resultado

- La página Replication muestra el estado de "establecimiento".
- Astra Control detiene la aplicación en el nuevo clúster de destino.
- Astra Control vuelve a establecer la replicación de volúmenes persistentes en la dirección seleccionada mediante la resincronización de SnapMirror.
- La página Replication muestra la relación actualizada.

Replicación de aplicaciones inversa

Esta es la operación planificada para mover la aplicación al clúster de destino y seguir replicando de nuevo al clúster de origen original. Astra Control detiene la aplicación en el clúster de origen y replica los datos en el destino antes de conmutar por error la aplicación al clúster de destino.

En esta situación, está intercambiando el origen y el destino. El clúster de origen original se convierte en el nuevo clúster de destino, y el clúster de destino original se convierte en el nuevo clúster de origen.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **replicación inversa**.
4. En la página replicación inversa, revise la información y seleccione **replicación inversa** para continuar.

Resultado

Las siguientes acciones ocurren como resultado de la replicación inversa:

- Se realiza una copia Snapshot de los recursos de Kubernetes de las aplicaciones de origen originales.
- Los pods de la aplicación de origen originales se detienen con dignidad al eliminar los recursos de Kubernetes de la aplicación (dejando las RVP y los VP en funcionamiento).
- Una vez apagados los pods, se realizan copias Snapshot de los volúmenes de la aplicación y se replican.
- Las relaciones de SnapMirror se rompen, lo que hace que los volúmenes de destino estén listos para la lectura/escritura.
- Los recursos de Kubernetes de la aplicación se restauran desde la copia Snapshot previa al apagado, utilizando los datos de volumen replicados después del apagado de la aplicación de origen original.
- La replicación se restablece en la dirección inversa.

Conmutación tras error de las aplicaciones al clúster de origen original

Con Astra Control, puede lograr una "recuperación tras fallos" tras una operación de "conmutación por error" mediante la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Astra Control replica (resyncs) cualquier aplicación vuelve a cambiar al clúster de origen original antes de revertir la dirección de replicación.

Este proceso comienza a partir de una relación que ha completado una conmutación por error a un destino e implica los siguientes pasos:

- Comience con un estado de conmutación al respaldo.
- Volver a sincronizar la relación.
- Invierta la replicación.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación, en el menú acciones, seleccione **Resync**.
4. Para realizar una operación de recuperación tras fallos, elija la aplicación con error como origen de la operación de resincronización (cómo conservar los datos escritos en una post conmuta al nodo de respaldo).
5. Escriba "Resync" para confirmar.
6. Seleccione **Sí, resincronización** para finalizar.
7. Una vez finalizada la resincronización, en la ficha Protección de datos > replicación, en el menú acciones, seleccione **replicación inversa**.
8. En la página replicación inversa, revise la información y seleccione **replicación inversa**.

Resultado

Esto combina los resultados de las operaciones de "resincronización" y "relación inversa" para conectar la aplicación en el clúster de origen original con la reanudación de la replicación al clúster de destino original.

Eliminar una relación de replicación de aplicaciones

La eliminación de la relación da como resultado dos aplicaciones independientes sin relación entre ellas.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. En la página Application, seleccione la ficha **Data Protection** > **Replication**.
3. En la ficha Protección de datos > replicación , en el cuadro Protección de aplicaciones o en el diagrama de relaciones, seleccione **Eliminar relación de replicación**.

Resultado

Las siguientes acciones ocurren como resultado de eliminar una relación de replicación:

- Si se establece la relación pero la aplicación aún no se ha conectado en el clúster de destino (se ha producido un error al respecto), Astra Control conserva las RVP creadas durante la inicialización, deja una aplicación gestionada "vacía" en el clúster de destino y conserva la aplicación de destino para mantener las copias de seguridad que se hayan creado.
- Si la aplicación se ha conectado en el clúster de destino (con errores), Astra Control conserva las RVP y las aplicaciones de destino. Las aplicaciones de origen y destino se tratan ahora como aplicaciones independientes. Las programaciones de backup permanecen en ambas aplicaciones, pero no se asocian entre sí.

estado de la relación de replicación y estados del ciclo de vida de la relación

Astra Control muestra el estado de la relación y los estados del ciclo de vida de la relación de replicación.

Estados de la relación de replicación

Los siguientes Estados indican el estado de la relación de replicación:

- **Normal**: La relación se establece o se ha establecido, y la instantánea más reciente se ha transferido con éxito.

- **Advertencia**: La relación está fallando o ya falló (y por lo tanto ya no protege la aplicación de origen).
- **Crítico**
  - La relación se ha establecido o se ha realizado una conmutación por error, y el último intento de reconciliación ha fallado.
  - Se establece la relación y se produce un error en el último intento de reconciliar la adición de una nueva RVP.
  - La relación está establecida (por lo que se ha replicado un snapshot correcto y es posible la recuperación tras fallos), pero la snapshot más reciente ha fallado o ha fallado para replicarse.

estados de ciclo de vida de replicación

Los siguientes estados reflejan las diferentes etapas del ciclo de vida de la replicación:

- **Establecer**: Se está creando una nueva relación de replicación. Astra Control crea un espacio de nombres en caso necesario, crea reclamaciones de volúmenes persistentes (RVP) en los nuevos volúmenes en el clúster de destino y crea relaciones con SnapMirror. Este estado también puede indicar que la replicación está resincronizada o invirtiendo la replicación.
- **Establecido**: Existe una relación de replicación. Astra Control comprueba periódicamente que las RVP están disponibles, comprueba la relación de replicación, crea periódicamente instantáneas de la aplicación e identifica cualquier EVs de origen nuevo en la aplicación. Si es así, Astra Control crea los recursos para incluirlos en la replicación.
- **Recuperación tras fallos**: Astra Control rompe las relaciones de SnapMirror y restaura los recursos Kubernetes de la aplicación desde la última instantánea de aplicación replicada correctamente.
- * Fallo en*: Astra Control deja de replicar desde el clúster de origen, utiliza la instantánea de aplicación replicada más reciente (correcta) en el destino y restaura los recursos de Kubernetes.
- **Resyncing**: Astra Control reenvía los nuevos datos del origen de resincronización al destino de resincronización mediante SnapMirror resync. Es posible que esta operación sobrescriba algunos de los datos del destino en función de la dirección de la sincronización. Astra Control detiene la aplicación que se ejecuta en el espacio de nombres de destino y elimina la aplicación Kubernetes. Durante el proceso de resincronización, el estado muestra como "establecer".
- **Inversión**: Es la operación planificada para mover la aplicación al clúster de destino mientras continúa la réplica al clúster de origen original. Astra Control detiene la aplicación en el clúster de origen y replica los datos en el destino antes de conmutar por error la aplicación al clúster de destino. Durante la replicación inversa, el estado aparece como "establecer".
- **Eliminación**:
  - Si la relación de replicación se ha establecido pero aún no se ha realizado una conmutación por error, Astra Control elimina las RVP que se crearon durante la replicación y elimina la aplicación administrada de destino.
  - Si la replicación ya ha fallado, Astra Control conserva las EVs y la aplicación de destino.

Clone y migre aplicaciones

Clone una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control Center clona una aplicación, crea un clon de la configuración de la aplicación y del almacenamiento persistente.

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.

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.

Acerca de esta tarea

- 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.
- 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.
- Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar un ID de bloque. Sin embargo, en una operación de clonado de aplicaciones, siempre se utiliza el bloque predeterminado que se ha definido. No existe ninguna opción para cambiar bloques para un clon. Si desea controlar qué segmento se utiliza, puede hacer lo mismo "cambiar el valor predeterminado del segmento" o haga un "Backup" seguido de un "restaurar" por separado.
- Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.

Consideraciones sobre OpenShift

- 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.
- 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**.
2. Debe realizar una de las siguientes acciones:
   - Seleccione el menú Opciones de 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 acción personalizada que puede configurar para que se ejecute junto con una operación de protección de datos de una aplicación gestionada. 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.

Tipos de enlaces de ejecución

Astra Control admite los siguientes tipos de enlaces de ejecución, en función de cuándo se pueden ejecutar:

- Copia previa de Snapshot
- Possnapshot
- Previo al backup
- Después del backup
- Después de la restauración

Notas importantes sobre los enlaces de ejecución personalizados

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

- Un enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Muchos enlaces de ejecución pueden hacer referencia al mismo script.
- Astra Control requiere que las secuencias de comandos que utilizan los enlaces de ejecución se escriban en el formato de secuencias de comandos de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Astra Control utiliza la configuración del enlace de ejecución y cualquier criterio coincidente para determinar qué ganchos se aplican a una operación de instantánea, copia de seguridad o restauración.
- Todos los fallos del enlace de ejecución son fallos de software; otros ganchos y la operación de protección de datos se siguen intentando 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.
- Para las operaciones de protección de datos ad hoc, todos los eventos de enlace se generan y guardan en el registro de eventos de la página **actividad**. Sin embargo, en el caso de las operaciones de protección de datos programadas, solo se registran los eventos de fallo de enlace en el registro de eventos (los eventos generados por las propias operaciones de protección de datos programadas aún se registran).

> 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. Si inicia una operación de copia de seguridad o de instantánea con los enlaces de ejecución asociados pero, a continuación, la cancela, los ganchos pueden ejecutarse si ya se ha iniciado la operación de copia de seguridad o de Snapshot. Esto significa que un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

Orden de ejecución

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

1. Los ganchos de ejecución de preoperación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos ganchos de prefuncionamiento personalizados como necesite, pero el orden de ejecución de estos enlaces antes de la operación no está garantizado ni configurable.
2. Se realiza la operación de protección de datos.
3. Los enlaces de ejecución de post-operación personalizados aplicables se ejecutan en los contenedores adecuados. Puede crear y ejecutar tantos enlaces de post-operación personalizados como necesite, pero el orden de ejecución de estos enlaces después de la operación no está garantizado ni configurable.

Si crea varios enlaces de ejecución del mismo tipo (por ejemplo, presnapshot), no se garantiza el orden de ejecución de esos enlaces. Sin embargo, el orden de ejecución de ganchos de diferentes tipos está garantizado. Por ejemplo, el orden de ejecución de una configuración que tiene los cinco tipos diferentes de

ganchos sería así:

1. Ganchos de precopia de seguridad ejecutados
2. Ganchos presnapshot ejecutados
3. Ganchos posteriores a la instantánea ejecutados
4. Se han ejecutado los enlaces posteriores a la copia de seguridad
5. Ganchos posteriores a la restauración ejecutados

Puede ver un ejemplo de esta configuración en el número de escenario 2 de la tabla de la Determine si se ejecutará un gancho.

> 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 copias Snapshot y backups resultantes para garantizar que sean coherentes. Para ello, puede clonar la aplicación en un espacio de nombres temporal, restaurar la instantánea o la copia de seguridad y, a continuación, probar la aplicación.

Determine si se ejecutará un gancho

Utilice la siguiente tabla para determinar si se ejecutará un enlace de ejecución personalizado para su aplicación.

Tenga en cuenta que todas las operaciones de aplicaciones de alto nivel consisten en ejecutar una de las operaciones básicas de copia Snapshot, backup o restauración. Según el supuesto, una operación de clonado puede consistir en diversas combinaciones de estas operaciones, de modo que lo que enlaza la ejecución de una operación de clonado será diferente.

Las operaciones de restauración sin movimiento requieren una snapshot o un backup existentes, por lo que estas operaciones no ejecutan datos instantáneos ni enlaces de backup.

> Si comienza pero luego cancela una copia de seguridad que incluye una instantánea y hay enlaces de ejecución asociados, es posible que se ejecuten algunos enlaces y es posible que otros no. Esto significa que un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado. Tenga en cuenta los siguientes puntos para realizar backups cancelados con enlaces de ejecución asociados:
>
> - Los enlaces de copia de seguridad previa y posterior siempre se ejecutan.
> - Si la copia de seguridad incluye una nueva instantánea y se ha iniciado la instantánea, se ejecutan los enlaces de preinstantánea y posterior a la instantánea.
> - Si la copia de seguridad se cancela antes del inicio de la instantánea, no se ejecutan los enlaces presnapshot y post snapshot.

Situación	Funcionamiento	Snapshot existente	Backup existente	Espacio de nombres	Clúster	Funcionan los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos
1	Clonar	N	N	Nuevo	Igual	Y	N	Y

Situación	Funcionamiento	Snapshot existente	Backup existente	Espacio de nombres	Clúster	Funcionan los enlaces de instantáneas	Funcionamiento de los ganchos de backup	Restaurar ejecución de ganchos
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	Y	Y
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y
7	Restaurar	Y	N	Existente	Igual	N	N	Y
8	Restaurar	N	Y	Existente	Igual	N	N	Y
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.
11	Backup	Y	N.A.	N.A.	N.A.	N	Y	N.A.

Ver los enlaces de ejecución existentes

Puede ver los enlaces de ejecución personalizados existentes para una aplicación.

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 (pre o post-operación). 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.

Ver los scripts existentes

Puede ver los scripts cargados existentes. También puede ver qué scripts están en uso, y qué enlaces los están utilizando, en esta página.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.

   En esta página puede ver una lista de los scripts cargados existentes. La columna **Used by** muestra los enlaces de ejecución que utilizan cada script.

Agregar un script

Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos enlaces de ejecución pueden hacer referencia a la misma secuencia de comandos; esto permite actualizar muchos enlaces de ejecución sólo cambiando una secuencia de comandos.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Seleccione **Agregar**.
4. Debe realizar una de las siguientes acciones:
   - 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.
     v. Seleccione **Guardar script**.
   - Pegar en un script personalizado desde el portapapeles.
     i. Seleccione la opción **Pegar o Tipo**.
     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.
5. Seleccione **Guardar script**.

Resultado

La nueva secuencia de comandos aparece en la lista de la ficha **Scripts**.

Eliminar un script

Puede eliminar una secuencia de comandos del sistema si ya no es necesaria y no se utiliza en ningún anzuelo de ejecución.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Elija la secuencia de comandos que desee quitar y seleccione el menú en la columna **acciones**.
4. Seleccione **Eliminar**.

> Si la secuencia de comandos está asociada con uno o más enlaces de ejecución, la acción **Eliminar** no estará disponible. Para eliminar la secuencia de comandos, primero edite los enlaces de ejecución asociados y asócielos a una secuencia de comandos diferente.

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 específicos 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 **Agregar**.
4. En el área **Detalles del gancho**, determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.
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:
   - Agregue un nuevo script.
     i. Seleccione **Agregar**.
     ii. Debe realizar una de las siguientes acciones:
     - 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.
       V. Seleccione **Guardar script**.
     - Pegar en un script personalizado desde el portapapeles.
       I. Seleccione la opción **Pegar o Tipo**.
       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.
   - Seleccione un script existente de la lista.

   Esto indica al enlace de ejecución que utilice esta secuencia de comandos.
9. Seleccione **Agregar gancho**.

Compruebe el estado de un enlace de ejecución

Después de que una operación de instantánea, backup o restauración finalice la ejecución, puede comprobar el estado de los enlaces de ejecución que se ejecutan como parte de la operación. Puede utilizar esta información de estado para determinar si desea mantener el enlace de ejecución, modificarlo o eliminarlo.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **Protección de datos**.
3. Seleccione **instantáneas** para ver las instantáneas en ejecución, o **copias de seguridad** para ver las copias de seguridad en ejecución.

   El estado * gancho* muestra el estado de la ejecución del gancho de ejecución una vez completada la operación. Puede pasar el ratón sobre el estado para obtener más detalles. Por ejemplo, si hay fallos de enlace de ejecución durante una instantánea, pasar el ratón sobre el estado de enlace de esa instantánea proporciona una lista de los enlaces de ejecución fallidos. Para ver las razones de cada fallo, puede consultar la página **actividad** en el área de navegación del lado izquierdo.

Ver el uso de las secuencias de comandos

Puede ver qué enlaces de ejecución utilizan una secuencia de comandos determinada en la interfaz de usuario web de Astra Control.

Pasos

1. Seleccione **cuenta**.
2. Seleccione la ficha **Scripts**.

   La columna **usado por** de la lista de scripts contiene detalles sobre qué ganchos están utilizando cada script de la lista.

3. Seleccione la información de la columna **utilizado por** para un script que le interese.

   Aparece una lista más detallada, con los nombres de los ganchos que utilizan la secuencia de comandos y el tipo de operación con la que están configurados para ejecutarse.

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 Opciones de la columna **acciones** para el gancho que desea 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 Opciones de la columna **acciones** para el gancho que desea 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
```

Supervise 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, sino que se puede profundizar en cada uno de ellos. 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.

   Si hay un clúster en `removed` estado aunque la conectividad del clúster y de la red parece correcta (los intentos externos de acceder al clúster mediante las API de Kubernetes se han realizado correctamente), es posible que la imagen que proporcionó a Astra Control ya no sea válida. Esto puede deberse a la rotación o a la caducidad del certificado en el clúster. Para corregir este problema, actualice las credenciales asociadas con el clúster en Astra Control mediante "API de control Astra".

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

También se puede utilizar LDAP para realizar autenticación para los usuarios seleccionados.

Utilice LDAP

LDAP es un protocolo estándar del sector para acceder a información de directorio distribuida y una opción muy popular para la autenticación empresarial. Puede conectar Astra Control Center a un servidor LDAP para realizar la autenticación de los usuarios seleccionados de Astra. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra correspondientes a las definiciones LDAP. Consulte "Autenticación LDAP" si quiere más información.

Invitar a los usuarios

Los propietarios y administradores de cuentas pueden invitar a nuevos usuarios a Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. Seleccione **Invitar usuario**.
4. Introduzca el nombre y la dirección de correo electrónico del usuario.
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, anular la administración de aplicaciones y eliminar instantáneas y 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. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones** .

   Para obtener más información sobre cómo agregar restricciones, consulte "Gestionar roles".

7. Seleccione **Invitar usuarios**.

   El usuario recibe un correo electrónico informándole de que ha sido invitado a Astra Control Center. El correo electrónico incluye una contraseña temporal, que deberá cambiar en el primer inicio de sesión.

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, anular la administración de aplicaciones y eliminar instantáneas y 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. Para agregar restricciones a un usuario con un rol de miembro o de visor, active la casilla de verificación **restringir la función a restricciones** .

   Para obtener más información sobre cómo agregar restricciones, consulte "Gestionar roles".

7. 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. En el menú Opciones de la columna **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. Seleccione la lista desplegable **acciones**.
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 pedirá 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. Seleccione la lista desplegable **acciones**.
3. Seleccione **Editar rol**.
4. Seleccione un rol nuevo.
5. Para aplicar restricciones a la función, active la casilla de verificación **restringir la función a restricciones** y seleccione una restricción de la lista.

   Si no hay restricciones, puede agregar una restricción. Para obtener más información, consulte "Gestionar roles".

6. Seleccione **Confirmar**.

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** , active la casilla de verificación en la fila de cada usuario que desee quitar.
3. En el menú Opciones de la columna **acciones**, 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.

Gestionar roles

Es posible gestionar roles si se añaden restricciones de espacio de nombres y se restringen los roles del usuario a dichas restricciones. Esto le permite controlar el acceso a los recursos de su organización. Puede utilizar la interfaz de usuario de Astra Control o. "La API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Admin o Owner puede agregar restricciones de espacio de nombres.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor.
4. Seleccione **Editar rol**.
5. Active la casilla de verificación **restringir rol a restricciones**.

   La casilla de verificación sólo está disponible para funciones de miembro o de visor. Puede seleccionar un rol diferente de la lista desplegable **rol**.

6. Seleccione **Agregar restricción**.

   Se puede ver la lista de restricciones disponibles por espacio de nombres o por etiqueta de espacio de nombres.

7. En la lista desplegable **Tipo de restricción**, seleccione **espacio de nombres Kubernetes** o **etiqueta de espacio de nombres Kubernetes** dependiendo de cómo estén configurados los espacios de nombres.
8. Seleccione uno o más espacios de nombres o etiquetas de la lista para redactar una restricción que restrinja las funciones a esos espacios de nombres.
9. Seleccione **Confirmar**.

   La página **Editar función** muestra la lista de restricciones que ha elegido para esta función.

10. Seleccione **Confirmar**.

En la página **cuenta**, puede ver las restricciones de cualquier rol de miembro o de visor en la columna **rol**.

> Si habilita restricciones para una función y selecciona **Confirmar** sin agregar restricciones, se considera que la función tiene restricciones completas (se deniega el acceso a cualquier recurso asignado a espacios de nombres).

Quitar una restricción de espacio de nombres de una función

Un usuario Admin o Owner puede eliminar una restricción de espacio de nombres de una función.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **usuarios**.
3. En la columna **acciones**, seleccione el botón de menú para un usuario con la función Miembro o Visor que tiene restricciones activas.
4. Seleccione **Editar rol**.

   El cuadro de diálogo **Editar función** muestra las restricciones activas para la función.

5. Seleccione **X** a la derecha de la restricción que debe eliminar.
6. Seleccione **Confirmar**.

Si quiere más información

- "Roles de usuario y espacios de nombres"

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.

Puede gestionar estas notificaciones desde la parte superior derecha de la interfaz:

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**.
2. Seleccione la ficha **credenciales**.
3. Seleccione el menú Opciones de la columna **Estado** para obtener las credenciales que desea quitar.
4. Seleccione **Quitar**.
5. 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.

Si gestiona los clústeres de Kubernetes desde Astra Control y Astra Control se conecta a Cloud Insights, Astra Control envía registros de eventos a Cloud Insights. La información de registro, incluida la información sobre la implementación de POD y los archivos adjuntos de PVC, aparece en el registro de actividad de control de Astra. Utilice esta información para identificar cualquier problema en los clústeres de Kubernetes que está gestionando.

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.

Si quiere más información

- "Licencias de Astra Control Center"

Gestionar conexiones de repositorios

Puede conectar repositorios a Astra Control para utilizarlos como referencia para imágenes y artefactos de instalación de paquetes de software. Al importar paquetes de software, Astra Control hace referencia a imágenes de instalación en el repositorio de imágenes y binarios y otros artefactos en el repositorio de artefactos.

Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Un repositorio de Docker en ejecución al que se puede acceder
- Un repositorio de artefactos en ejecución (como Artifactory) al que se puede acceder

Conecte un repositorio de imágenes Docker

Puede conectar un repositorio de imágenes Docker para almacenar imágenes de instalación del paquete, como las de Astra Data Store. Al instalar paquetes, Astra Control importa los archivos de imagen del paquete desde el repositorio de imágenes.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **Docker Image Repository**, seleccione el menú de la parte superior derecha.
4. Seleccione **conectar**.
5. Añada la URL y el puerto para el repositorio.
6. Introduzca las credenciales del repositorio.
7. Seleccione **conectar**.

Resultado

El repositorio está conectado. En la sección **Docker Image Repository**, el repositorio debe mostrar un estado conectado.

Desconecte un repositorio de imágenes Docker

Puede eliminar la conexión a un repositorio de imágenes Docker si ya no es necesario.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **Docker Image Repository**, seleccione el menú de la parte superior derecha.
4. Seleccione **desconectar**.
5. Seleccione **Sí, desconecte el repositorio de imágenes Docker**.

Resultado

El repositorio está desconectado. En la sección **Docker Image Repository**, el repositorio debe mostrar un estado desconectado.

Conecte un repositorio de artefactos

Puede conectar un repositorio de artefactos a artefactos host como los binarios de paquetes de software. Al instalar paquetes, Astra Control importa los artefactos para los paquetes de software desde el repositorio de imágenes.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **repositorio de artefactos**, seleccione el menú de la parte superior derecha.
4. Seleccione **conectar**.
5. Añada la URL y el puerto para el repositorio.
6. Si se requiere autenticación, active la casilla de verificación **usar autenticación** e introduzca las credenciales del repositorio.
7. Seleccione **conectar**.

Resultado

El repositorio está conectado. En la sección **repositorio de artefactos**, el repositorio debe mostrar un estado conectado.

Desconecte un repositorio de artefactos

Puede eliminar la conexión a un repositorio de artefactos si ya no es necesaria.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **conexiones**.
3. En la sección **repositorio de artefactos**, seleccione el menú de la parte superior derecha.
4. Seleccione **desconectar**.
5. Seleccione **Sí, desconectar el repositorio de artefactos**.

Resultado

El repositorio está desconectado. En la sección **repositorio de artefactos**, el repositorio debe mostrar un estado conectado.

Obtenga más información

- "Gestione los paquetes de software"

Gestione los paquetes de software

NetApp ofrece funcionalidades adicionales para Astra Control Center con paquetes de software que puede descargar en el sitio de soporte de NetApp. Después de conectar los repositorios de Docker y artefactos, puede cargar e importar paquetes para agregar esta funcionalidad a Astra Control Center. Puede utilizar la CLI o la interfaz de usuario web de Astra Control Center para gestionar los paquetes de software.

Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Un repositorio de imágenes Docker conectado para contener imágenes de paquetes de software. Para obtener más información, consulte "Gestionar conexiones de repositorios".
- Un repositorio de artefactos conectado para contener binarios y artefactos de paquetes de software. Para obtener más información, consulte "Gestionar conexiones de repositorios".
- Un paquete de software del sitio de soporte de NetApp

Cargue imágenes de paquetes de software en los repositorios

Astra Control Center hace referencia a imágenes de paquetes y artefactos en repositorios conectados. Puede cargar imágenes y artefactos en los repositorios con la CLI.

Pasos

1. Descargue el paquete de software del sitio de soporte de NetApp y guárdelo en un equipo que tenga el `kubectl` utilidad instalada.
2. Extraiga el archivo de paquete comprimido y cambie el directorio a la ubicación del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
3. Inserte las imágenes de los paquetes en el repositorio de Docker. Realice las siguientes sustituciones:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

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

4. Si el paquete tiene artefactos, copie los artefactos en el repositorio de artefactos. Sustituya BUNDLE_FILE por el nombre del archivo de paquete Astra Control y NETWORK_LOCATION por la ubicación de red para copiar los archivos de artefactos a:

   ```
   kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
   ```

Añada un paquete de software

Puede importar paquetes de software mediante un archivo de paquete Astra Control Center. De esta forma, se instala el paquete y se pone el software a disposición de Astra Control Center.

Agregue un paquete de software mediante la interfaz de usuario web de Astra Control

Puede utilizar la interfaz de usuario web de Astra Control Center para agregar un paquete de software que se ha cargado en los repositorios conectados.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **Paquetes**.
3. Seleccione el botón **Agregar**.
4. En el cuadro de diálogo de selección de archivos, seleccione el icono de carga.
5. Elija un archivo de paquete de Astra Control, en `.yaml` formato, para cargar.
6. Seleccione **Agregar**.

Resultado

Si el archivo de paquete es válido y las imágenes y artefactos del paquete se encuentran en los repositorios conectados, el paquete se agrega a Astra Control Center. Cuando el estado de la columna **Estado** cambia a **disponible**, puede utilizar el paquete. Puede pasar el ratón sobre el estado de un paquete para obtener más información.

> Si no se encuentran una o más imágenes o artefactos para un paquete en su repositorio, aparece un mensaje de error para ese paquete.

Añada un paquete de software mediante la CLI

Es posible usar la CLI para importar un paquete de software que haya cargado en los repositorios conectados. Para ello, primero debe registrar el ID de cuenta de Astra Control Center y un token de API.

Pasos

1. Con un navegador web, inicie sesión en la interfaz de usuario web de Astra Control Center.
2. En el panel de control, seleccione el icono de usuario en la parte superior derecha.
3. Seleccione **acceso API**.
4. Observe el ID de cuenta cerca de la parte superior de la pantalla.
5. Seleccione **generar símbolo de API**.
6. En el cuadro de diálogo resultante, seleccione **generar símbolo de API**.
7. Observe el token resultante y seleccione **Cerrar**. En la CLI, cambie los directorios a la ubicación de `.yaml` archivo de paquete en el contenido del paquete extraído.
8. Importe el paquete utilizando el archivo de paquete, realizando las siguientes sustituciones:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle.
   - Sustituya EL SERVIDOR por el nombre DNS de la instancia de Astra Control.
   - Reemplace ACCOUNT_ID y TOKEN con el ID de cuenta y el token de API que haya registrado anteriormente.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

Resultado

Si el archivo de paquete es válido y las imágenes y artefactos del paquete se encuentran en los repositorios conectados, el paquete se agrega a Astra Control Center.

Si no se encuentran una o más imágenes o artefactos para un paquete en su repositorio, aparece un mensaje de error para ese paquete.

Quite un paquete de software

Puede utilizar la interfaz de usuario web de Astra Control Center para eliminar un paquete de software importado previamente en Astra Control Center.

Pasos

1. En el área de navegación **Administrar su cuenta**, seleccione **cuenta**.
2. Seleccione la ficha **Paquetes**.

   En esta página puede ver la lista de paquetes instalados y sus Estados.

3. En la columna **acciones** del paquete, abra el menú acciones.
4. Seleccione **Eliminar**.

Resultado

El paquete se elimina de Astra Control Center, pero las imágenes y artefactos del paquete permanecen en sus repositorios.

Obtenga más información

- "Gestionar conexiones de repositorios"

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.

Use uno de los siguientes proveedores de bloques de Amazon simple Storage Service (S3):

- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp
- Microsoft Azure
- Genérico S3

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

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
- Gire o elimine las credenciales del cucharón
- Retirar un cucharón

> 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.

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 Opciones de la columna **acciones**, seleccione **Editar**.
3. Cambie cualquier información que no sea el tipo de segmento.

   > No puede modificar el tipo de segmento.

4. Seleccione **Actualizar**.

Gire o elimine las credenciales del cucharón

Astra Control utiliza las credenciales de bloque para obtener acceso y proporcionar claves secretas para un bloque de S3, de forma que Astra Control Center pueda comunicarse con el cucharón.

Rotar las credenciales del cucharón

Si gira las credenciales, gírelos durante una ventana de mantenimiento cuando no haya copias de seguridad en curso (programadas o bajo demanda).

Pasos para editar y girar credenciales

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú Opciones de la columna **acciones**, seleccione **Editar**.
3. Cree la nueva credencial.
4. Seleccione **Actualizar**.

Quitar las credenciales del bloque

Debe eliminar las credenciales de bloque solo si se han aplicado credenciales nuevas a un bloque o si ya no se utiliza el bloque de forma activa.

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. No elimine estas credenciales si el bloque está en uso activo, ya que esto dará lugar a fallos de copia de seguridad y a falta de disponibilidad de copia de seguridad.

Si elimina las credenciales de bloque activas, consulte "solución de problemas de eliminación de credenciales del bloque".

Para obtener instrucciones sobre cómo eliminar credenciales de S3 mediante la API Astra Control, consulte "Información sobre API y automatización de Astra".

Retirar un cucharón

Puede eliminar un cubo que ya no esté en uso o que no esté sano. Se recomienda hacer esto para mantener la configuración del almacén de objetos sencilla y actualizada.

No se puede eliminar un bloque predeterminado. Si desea eliminar ese bloque, seleccione primero otro bloque como predeterminado.

Lo que necesitará

- Antes de empezar, debe comprobar que no hay copias de seguridad en ejecución o completadas para este bloque.
- Debe comprobar que el bloque no se esté utilizando en ninguna política de protección activa.

Si lo hay, no podrá continuar.

Pasos

1. En la navegación de la izquierda, seleccione **Cuchos**.
2. En el menú **acciones**, seleccione **Quitar**.

   Astra Control garantiza en primer lugar que no existan normativas de programación utilizando el bloque para copias de seguridad y que no haya copias de seguridad activas en el bloque que va a eliminar.

3. Escriba "eliminar" para confirmar la acción.
4. Seleccione **Sí, retire la cuchara**.

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
- Actualizar una licencia de back-end de almacenamiento de Astra Data Store
- Actualice un back-end de almacenamiento de Astra Data Store
- Quite un back-end de almacenamiento
- Añada nodos a un clúster de back-end de almacenamiento
- Quite nodos de un clúster de 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.

En la página Storage Backend Details, en Astra Data Store, puede consultar la siguiente información:

- Clúster de almacén de datos de Astra
  - Rendimiento, IOPS y latencia
  - Capacidad utilizada en comparación con la capacidad total
- Para cada volumen de clúster de Astra Data Store
  - Capacidad utilizada en comparación con la capacidad total
  - Rendimiento

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

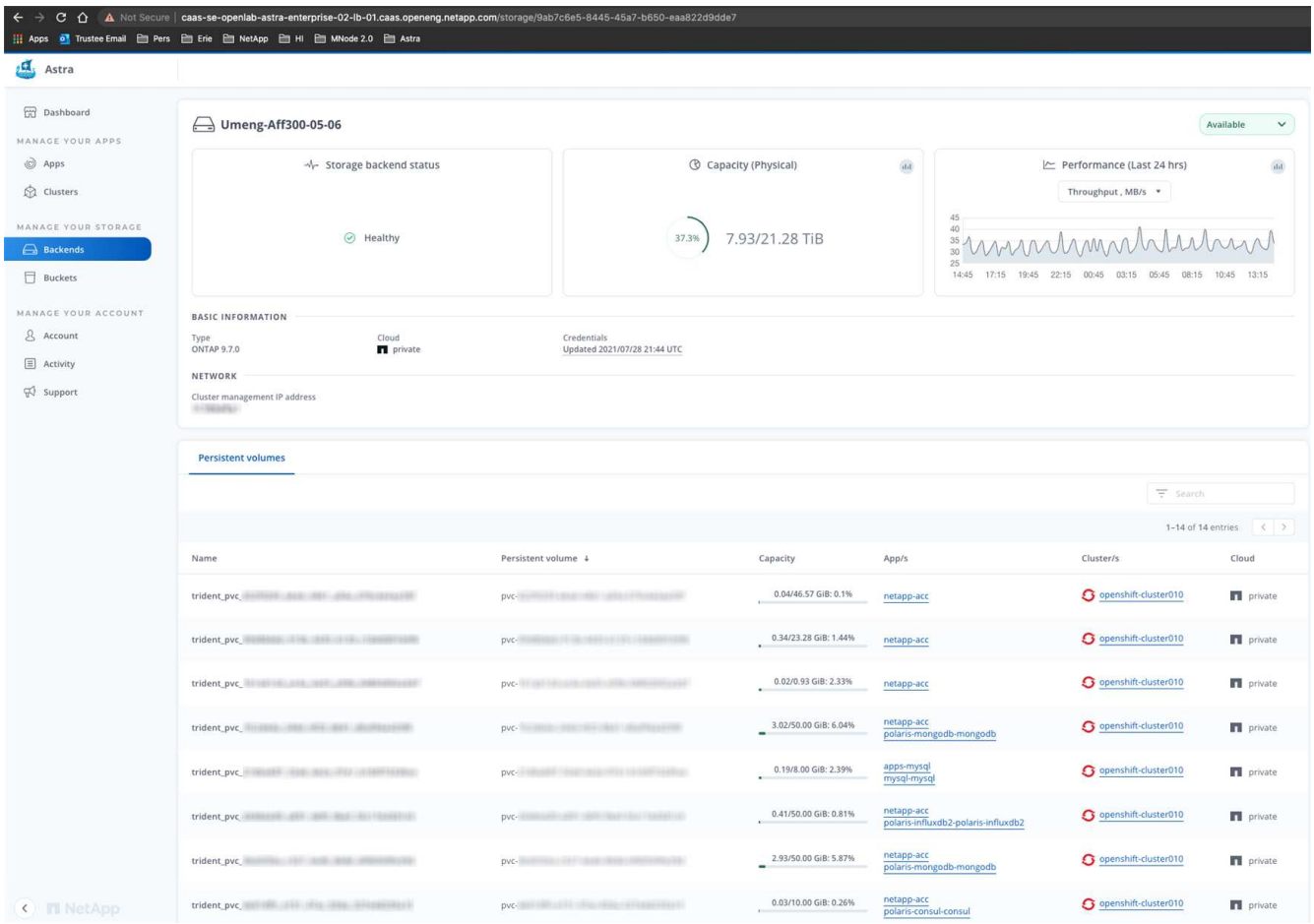
Vea información sobre el estado, la capacidad y el rendimiento del back-end (rendimiento de IOPS y/o latencia).

Puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado. Con Cloud Insights, puede ver información adicional. Consulte "Documentación de Cloud Insights".

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 de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el menú Opciones de la columna **acciones**, seleccione **Unmanage**.
4. Escriba "desgestionar" para confirmar la acción.
5. Seleccione **Sí, anular la administración del backend de almacenamiento**.

Quite un back-end de almacenamiento

Puede eliminar un back-end de almacenamiento que ya no se esté utilizando. Se recomienda hacer esto para mantener su configuración sencilla y actualizada.

Si va a eliminar un back-end de Astra Data Store, vCenter no debe haberlo creado.

Lo que necesitará

- Asegúrese de que el back-end de almacenamiento no esté gestionado.
- Asegúrese de que el back-end de almacenamiento no tenga ningún volumen asociado con el clúster de almacén de datos de Astra.

Pasos

1. En la navegación izquierda, seleccione **Backends**.
2. Si se gestiona el back-end, desgestione.
   a. Seleccione **gestionado**.
   b. Seleccione el back-end de almacenamiento.
   c. En la opción **acciones**, seleccione **Unmanage**.
   d. Escriba "desgestionar" para confirmar la acción.
   e. Seleccione **Sí, anular la administración del backend de almacenamiento**.
3. Seleccione **descubierto**.
   a. Seleccione el back-end de almacenamiento.
   b. En la opción **acciones**, seleccione **Quitar**.
   c. Escriba "eliminar" para confirmar la acción.
   d. Seleccione **Sí, quite el backend de almacenamiento**.

Actualizar una licencia de back-end de almacenamiento de Astra Data Store

Puede actualizar la licencia de un back-end de almacenamiento de Astra Data Store para admitir una implementación mayor o funciones mejoradas.

Lo que necesitará

- Un back-end de almacenamiento de Astra Data Store implementado y gestionado
- Un archivo de licencia de Astra Data Store (póngase en contacto con su representante de ventas de NetApp para adquirir una licencia de Astra Data Store)

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.

2. Seleccione el nombre de un back-end de almacenamiento.
3. En **Información básica**, puede ver el tipo de licencia instalada.

   Si pasa el ratón por encima de la información de la licencia, aparece un cuadro emergente con más información, como información sobre la caducidad y los derechos.

4. En **Licencia**, seleccione el icono de edición junto al nombre de la licencia.
5. En la página **Actualizar licencia**, siga uno de estos procedimientos:

Estado de la licencia	Acción
Se ha añadido al menos una licencia a Astra Data Store.	Seleccione una licencia de la lista.
No se han añadido licencias a Astra Data Store.	a. Seleccione el botón **Agregar**. b. Seleccione un archivo de licencia para cargar. c. Seleccione **Agregar** para cargar el archivo de licencia.

6. Seleccione **Actualizar**.

Actualice un back-end de almacenamiento de Astra Data Store

Puede actualizar su entorno de administración de Astra Data Store desde Astra Control Center. Para ello, primero debe cargar un paquete de actualización; Astra Control Center utilizará este paquete de actualización para actualizar Astra Data Store.

Lo que necesitará

- Un back-end de almacenamiento gestionado de Astra Data Store
- Un paquete de actualización de Astra Data Store cargado (consulte "Gestione los paquetes de software")

Pasos

1. Seleccione **Backends**.
2. Elija un back-end de almacenamiento de Astra Data Store de la lista y seleccione el menú correspondiente en la columna **acciones**.
3. Seleccione **Actualizar**.
4. Seleccione una versión de actualización de la lista.

   Si tiene varios paquetes de actualización en el repositorio que son versiones diferentes, puede abrir la lista desplegable para seleccionar la versión que necesita.

5. Seleccione **Siguiente**.
6. Seleccione **Iniciar actualización**.

Resultado

La página **backends** muestra un estado **Upgrade** en la columna **Status** hasta que la actualización se haya completado.

Añada nodos a un clúster de back-end de almacenamiento

Puede agregar nodos a un clúster de almacén de datos de Astra, hasta el número de nodos admitidos por el tipo de licencia instalada para Astra Data Store.

Lo que necesitará

- Un back-end de almacenamiento de Astra Data Store con licencia y puesto en marcha
- Ha agregado el paquete de software Astra Data Store en Astra Control Center
- Uno o más nodos nuevos para añadir al clúster

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el nombre de un back-end de almacenamiento.
3. En Basic Information, puede ver el número de nodos en este clúster de back-end de almacenamiento.
4. En **Nodes**, seleccione el icono de edición junto al número de nodos.
5. En la página **Add Nodes**, introduzca información sobre el nuevo nodo o nodos:
   a. Asigne una etiqueta de nodo para cada nodo.
   b. Debe realizar una de las siguientes acciones:
      - Si desea que Astra Data Store utilice siempre el número máximo de nodos disponibles según su licencia, active la casilla de verificación * utilizar siempre hasta el número máximo de nodos permitidos*.
      - Si no desea que Astra Data Store utilice siempre el número máximo de nodos disponibles, seleccione el número deseado de nodos totales que desea utilizar.
   c. Si implementó Astra Data Store con Protection Domains habilitado, asigne el nodo o los nodos nuevos a Protection Domains.
6. Seleccione **Siguiente**.
7. Introduzca la dirección IP y la información de red para cada nodo nuevo. Introduzca una sola dirección IP para un solo nodo nuevo o un pool de direcciones IP para varios nodos nuevos.

   Si Astra Data Store puede utilizar las direcciones IP configuradas durante la implementación, no necesita introducir ninguna información de dirección IP.

8. Seleccione **Siguiente**.
9. Revise la configuración de los nodos nuevos.
10. Seleccione **Agregar nodos**.

Quite nodos de un clúster de back-end de almacenamiento

Puede eliminar nodos de un clúster de almacén de datos de Astra. Estos nodos pueden estar en buen estado o con errores.

Al quitar un nodo de un clúster Astra Data Store, se mueven sus datos a otros nodos del clúster y se quita el nodo de Astra Data Store.

El proceso requiere las siguientes condiciones:

- Debe haber suficiente espacio libre en los otros nodos para recibir los datos.

- Debe haber 4 o más nodos en el clúster.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el nombre de un back-end de almacenamiento.
3. Seleccione la ficha **Nodes**.
4. En el menú acciones, seleccione **Quitar**.
5. Confirme la eliminación introduciendo "eliminar".
6. Seleccione **Sí, eliminar nodo**.

Obtenga más información

- "Utilice la API Astra Control"

Supervise la infraestructura con conexiones Cloud Insights y Fluentd

Puede configurar varios ajustes opcionales para mejorar su experiencia con 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.

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.

También puede supervisar el rendimiento del back-end de almacenamiento de Astra Data Store, las IOPS y la capacidad desde la página Astra Control Center Storage Backends. Consulte "Gestione los back-ends de almacenamiento".

Añada un servidor proxy para conexiones a Cloud Insight o al sitio de soporte de NetApp

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, active 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.

Además, si gestiona los clústeres de Astra Data Store con Astra Control (que está conectado a Cloud Insights), se crea una unidad de adquisición en el almacén de datos Astra para cada clúster de Astra Data Store y las métricas se envían desde Astra Data Store al sistema Cloud Insights emparejado. Cada 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.

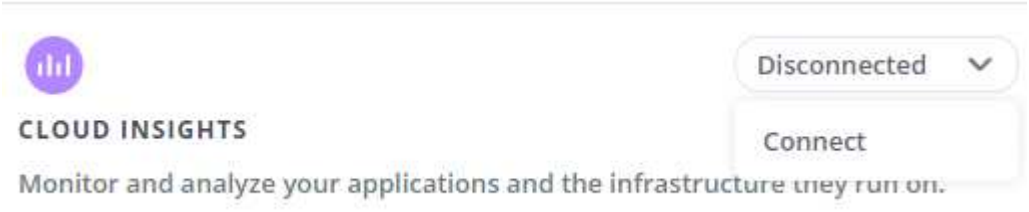
Lo que necesitará

- 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:

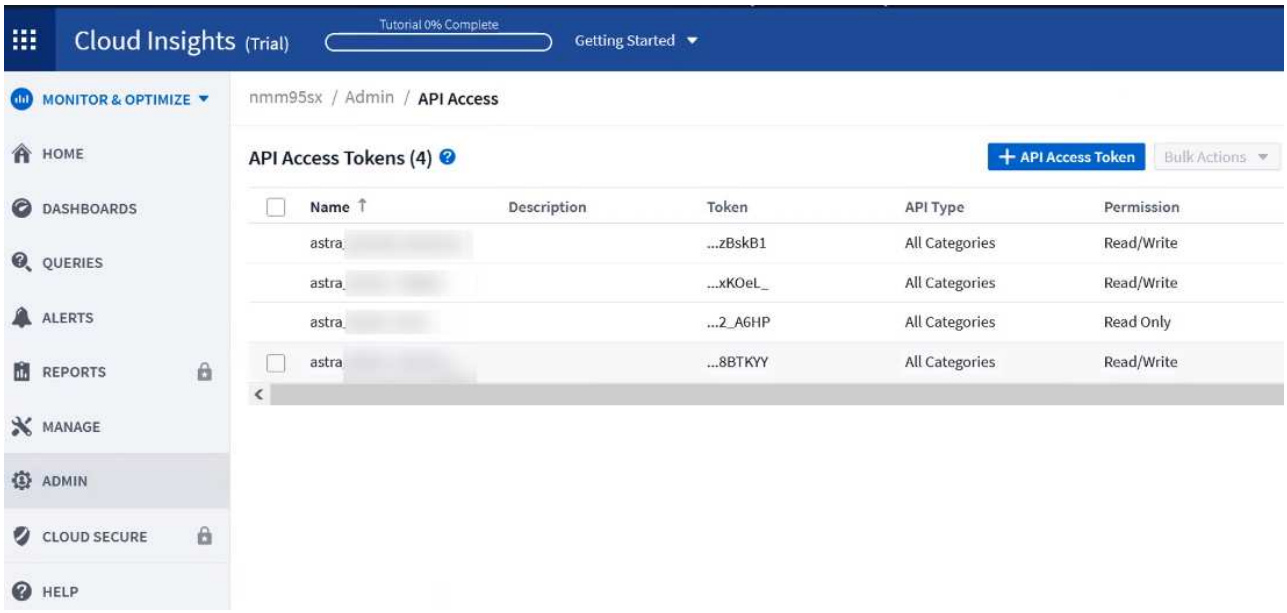
```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

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**.

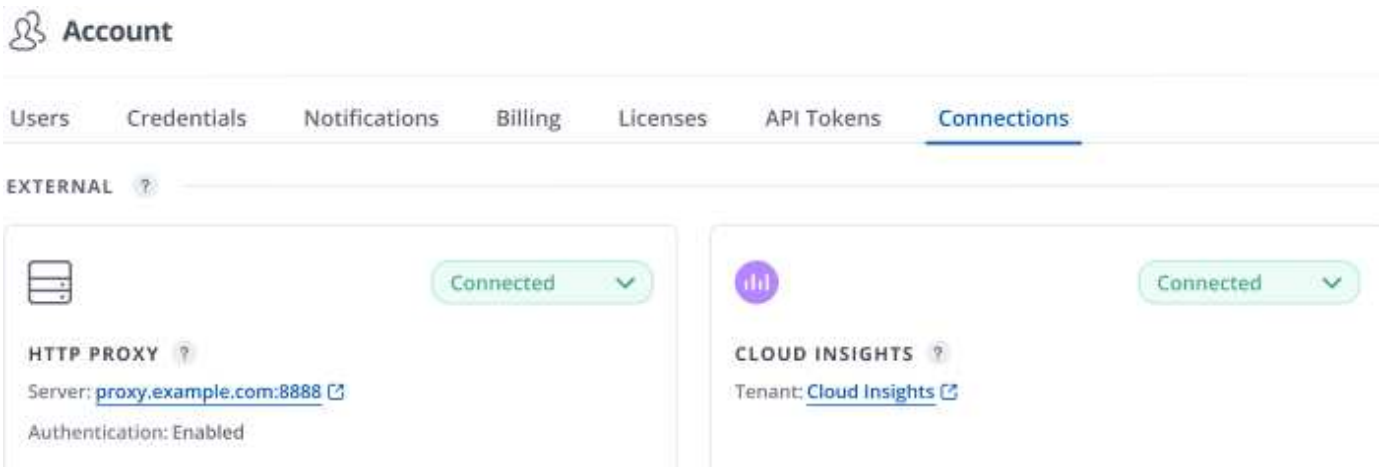
> Después de seleccionar **conectar,** el estado de la conexión cambia a **pendiente** en la sección **Cloud Insights** de la página **cuenta** > **conexiones**. Puede pasar unos minutos para que la conexión esté activada y el estado cambie a **conectado**.

> 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.

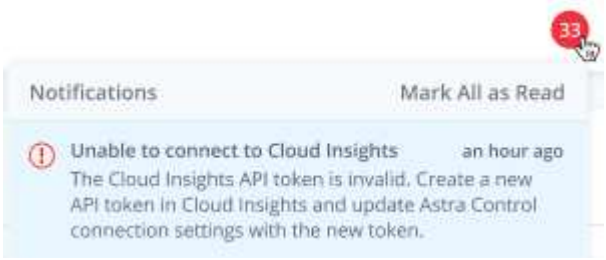
Ver datos en Cloud Insights

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.

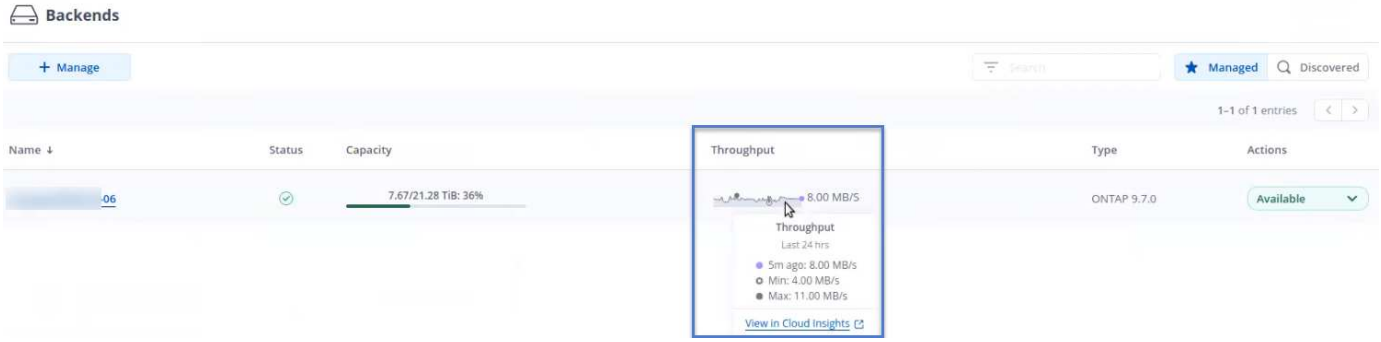


Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.



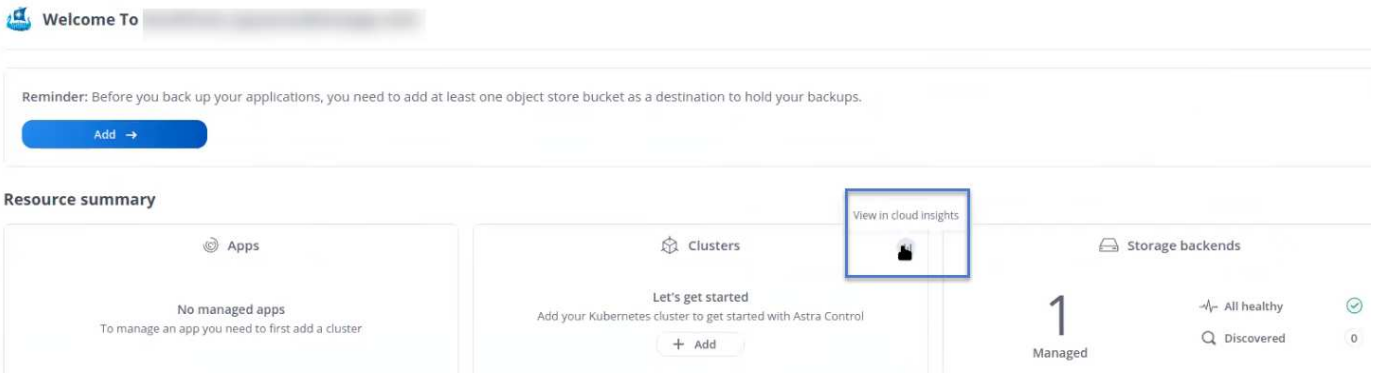
También puede encontrar la misma información en **cuenta** > **Notificaciones**.

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

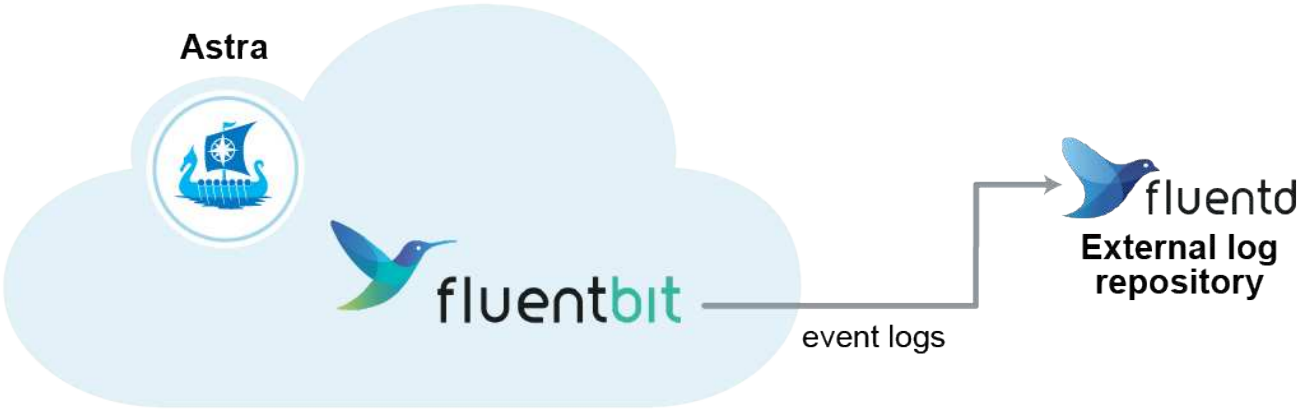
Puede deshabilitar la conexión Cloud Insights para un clúster de Kubernetes gestionado por Astra Control Center. Al deshabilitar la conexión Cloud Insights, no se eliminan los datos de telemetría ya cargados en Cloud Insights.

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.

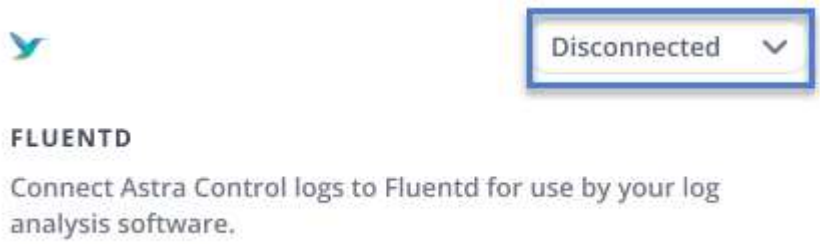
Lo que necesitará

- 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.

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 administrar.
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 de comprobación del clúster que ya no desea gestionar en Astra Control Center.
3. En el menú Opciones de la columna **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.

```
kubectl get clusteroperators
```

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

```
kubectl 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 (opcional)
- Comprobar el estado del sistema
- Configure la entrada para el equilibrio de carga

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 https:mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp].
2. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

Desembale el paquete y cambie el directorio

1. Extraiga las imágenes:

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

Agregue las imágenes al registro local

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

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:
   - Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, `acc.manifest.yaml`).
   - Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
   - Sustituya MY_REGISTRATION_USER por el nombre de usuario.
   - Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

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

Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

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

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

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

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

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

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

Instale el operador actualizado de Astra Control Center

1. Cambie el directorio:

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

   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.

d. Añada los siguientes valores a la `env` sección:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

```
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"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. 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
```

4. Verifique que los pods se estén ejecutando:

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

Actualice Astra Control Center

1. Editar el recurso personalizado de Astra Control Center (CR) (`astra_control_center_min.yaml`) Y cambie la versión Astra (`astraVersion` dentro de `Spec`) número a la última:

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

> 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. Añada las siguientes líneas dentro de `additionalValues` dentro de `Spec` En el Centro de control de Astra CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Debe realizar una de las siguientes acciones:
   a. Si no tiene su propio IngressController o Ingress y ha estado utilizando el Astra Control Center con su puerta de enlace Traefik como servicio de tipo LoadBalancer y desea continuar con esa configuración, especifique otro campo `ingressType` (si aún no está presente) y configúrelo en `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Si desea cambiar a la implementación de entrada genérica predeterminada de Astra Control Center, proporcione su propia configuración IngressController/Ingress (con terminación TLS, etc.), abra una ruta a Astra Control Center y establezca `ingressType` para `Generic`.

      ```
      ingressType: Generic
      ```

      Si omite el campo, el proceso se convierte en la implementación genérica. Si no desea la implementación genérica, asegúrese de agregar el campo.

4. (Opcional) Verifique que los POD terminan y estén disponibles de nuevo:

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

5. Espere a que las condiciones de estado de Astra indiquen 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
```

6. Vuelva a iniciar sesión y compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.
7. Si el operador no actualizó el gerente de cert, actualice los servicios de terceros, a continuación.

Actualizar servicios de terceros (opcional)

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.

- **Traefik**: Por defecto, Astra Control Center gestiona el ciclo de vida de la implementación de Traefik. Ajuste `externalTraefik` para `false` (Predeterminado) indica que no existe ninguna Traefik externa en el sistema y que Astra Control Center está instalando y gestionando Traefik. En este caso, `externalTraefik` se establece en `false`.

  Por otro lado, si usted tiene su propio despliegue de Traefik, set `externalTraefik` para `true`. En este caso, usted mantiene la implementación y Astra Control Center no actualizará los CRD, a menos que `shouldUpgrade` se establece en `true`.

- **Cert-Manager**: De forma predeterminada, Astra Control Center instala el cert-Manager (y CRD) a menos que usted establezca `externalCertManager` para `true`. Configurado `shouldUpgrade` para `true` Para que Astra Control Center actualice los CRD.

Traefik se actualiza si se cumple alguna de las siguientes condiciones:

- ExternalTraefik: Falso
- ExternalTraefik: Verdadero Y deberíldUpgrade: Verdadero.

Pasos

1. Edite el `acc` CR:

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

2. Cambie el `externalTraefik` y la `shouldUpgrade` campo para uno de los dos `true` o. `false` según se necesite.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

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.

Configure la entrada para el equilibrio de carga

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

- La actualización predeterminada utiliza la implementación de ingreso genérico. En este caso, también deberá configurar un controlador de entrada o un recurso de entrada.
- Si no desea un controlador de entrada y desea conservar lo que ya tiene, configure `ingressType` para `AccTraefik`.

> Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte "Requisitos".

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

- Controlador de entrada nginx
- Controlador OpenShift Ingress

Lo que necesitará

- En la especificación CR,
  - Si `crd.externalTraefik` está presente, debe estar configurado en `false` O.
  - Si `crd.externalTraefik` es `true`, `crd.shouldUpgrade` también debería ser `true`.
- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.
- Se utilizan versiones de Kubernetes entre e incluidas v1.19 y v1.21.

Pasos para el controlador de entrada Nginx

1. Utilice el secreto existente `secure-testing-cert` o cree un secreto de tipo[`kubernetes.io/tls`] Para una clave privada TLS y un certificado en `netapp-acc` (o nombre personalizado) como se describe en "Secretos TLS".
2. Implemente un recurso de entrada en `netapp-acc` espacio de nombres (o con nombre personalizado) para un esquema obsoleto o nuevo:

   a. Para un esquema obsoleto, siga este ejemplo:

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

b. Para un nuevo esquema, siga este ejemplo:

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

Pasos para el controlador de entrada de OpenShift

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

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

Compruebe la configuración de entrada

Puede verificar la configuración de entrada antes de continuar.

1. Asegúrese de que Traefik ha cambiado a. `clusterIP` Desde LoadBalancer:

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

2. Verificar rutas en Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

El resultado debe estar vacío.

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.

Si tiene algún problema con la desinstalación, consulte Solución de problemas de desinstalación.

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
```

Solución de problemas de desinstalación

Utilice las siguientes soluciones alternativas para solucionar cualquier problema que tenga al desinstalar Astra Control Center.

La desinstalación de Astra Control Center no puede limpiar el módulo de control del operador de supervisión en el clúster gestionado

Si no ha desgestionar los clústeres antes de desinstalar Astra Control Center, puede eliminar manualmente los POD del espacio de nombres para la supervisión de netapp y el espacio de nombres con los siguientes comandos:

Pasos

1. Eliminar `acc-monitoring` agente:

   ```
   kubectl delete agents acc-monitoring -n netapp-monitoring
   ```

   Resultado:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Elimine el espacio de nombres:

   ```
   kubectl delete ns netapp-monitoring
   ```

Resultado:

```
namespace "netapp-monitoring" deleted
```

3. Confirme los recursos eliminados:

```
kubectl get pods -n netapp-monitoring
```

Resultado:

```
No resources found in netapp-monitoring namespace.
```

4. Confirme que se ha eliminado el agente de supervisión:

```
kubectl get crd|grep agent
```

Resultado de la muestra:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Eliminar información de definición de recursos personalizada (CRD):

```
kubectl delete crds agents.monitoring.netapp.com
```

Resultado:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La desinstalación de Astra Control Center no limpia los CRD de Traefik

Puede eliminar manualmente los CRD de Traefik. Los CRD son recursos globales y su eliminación podría afectar a otras aplicaciones del cluster.

Pasos

1. Enumere los CRD de Traefik instalados en el clúster:

```
kubectl get crds |grep -E 'traefik'
```

Respuesta

```
ingressroutes.traefik.containo.us              2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us           2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us           2021-06-23T23:29:12Z
middlewares.traefik.containo.us                2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us             2021-06-23T23:29:12Z
serverstransports.traefik.containo.us          2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                 2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                  2021-06-23T23:29:14Z
traefikservices.traefik.containo.us            2021-06-23T23:29:15Z
```

2. Eliminar CRD:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

Obtenga más información

- "Problemas conocidos para la desinstalación"