



Utilice Astra

Astra Control Center

NetApp
November 20, 2023

This PDF was generated from <https://docs.netapp.com/es-es/astra-control-center-2108/use/manage-apps.html> on November 20, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Utilice Astra 1
 - Gestionar aplicaciones 1
 - Proteja sus aplicaciones 7
 - Ver el estado de las aplicaciones y del clúster 14
 - Gestione su cuenta 16
 - Gestionar bloques 22
 - Gestione el entorno de administración del almacenamiento 23
 - Supervise y proteja la infraestructura 25
 - Actualizar una licencia existente 32
 - Desgestione aplicaciones y clústeres 33
 - Desinstale Astra Control Center 34

Utilice Astra

Gestionar aplicaciones

Inicie la gestión de aplicaciones

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

Instale las aplicaciones en el clúster

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

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

- ["Desplegar MariaDB desde un gráfico Helm"](#)
- ["Implemente MySQL desde un gráfico Helm"](#)
- ["Despliegue Postgres desde un gráfico de Helm"](#)
- ["Implemente Jenkins a partir de un gráfico Helm"](#)

Gestionar aplicaciones

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



Las aplicaciones implementadas con Helm 2 no son compatibles.

Puede realizar las siguientes actividades para gestionar aplicaciones:

- Gestionar aplicaciones
 - [Gestionar aplicaciones por espacio de nombres](#)
 - [Gestione aplicaciones mediante la etiqueta Kubernetes](#)
- [Ignorar aplicaciones](#)
- [Desgestionar aplicaciones](#)



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

Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra, consulte ["Información sobre API y automatización de Astra"](#).



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

Gestionar aplicaciones por espacio de nombres

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

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

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

Pasos

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

The screenshot shows the 'Apps' page in Astra Control. At the top, there's a header with 'Apps', a search bar, and filters for 'Managed', 'Discovered' (54), and 'Ignored'. Below the header is a table with columns: Name, Ready, Cluster, Group, Discovered, and Actions. The table lists five applications: 'default', 'default1', 'default2', 'netapp-acc-operator', and 'pcloud'. Each application has a 'Ready' status (green checkmark), a 'Cluster' (e.g., 'se'), a 'Group' (e.g., 'grp_default'), a 'Discovered' timestamp, and an 'Actions' dropdown menu. The 'default' application is currently set to 'Managed', while the others are 'Unmanaged'.

Name	Ready	Cluster	Group	Discovered	Actions
default	✓	se	grp_default	2021/06/28 17:36 UTC	Managed
default1	✓	se	grp1_default	2021/06/28 17:36 UTC	Unmanaged
default2	✓	se	grp2_default	2021/06/28 17:36 UTC	Unmanaged
netapp-acc-operator	✓	se	netapp-acc-operator	2021/07/13 12:36 UTC	Unmanaged
pcloud	✓	se	pcloud	2021/07/13 12:37 UTC	Unmanaged

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

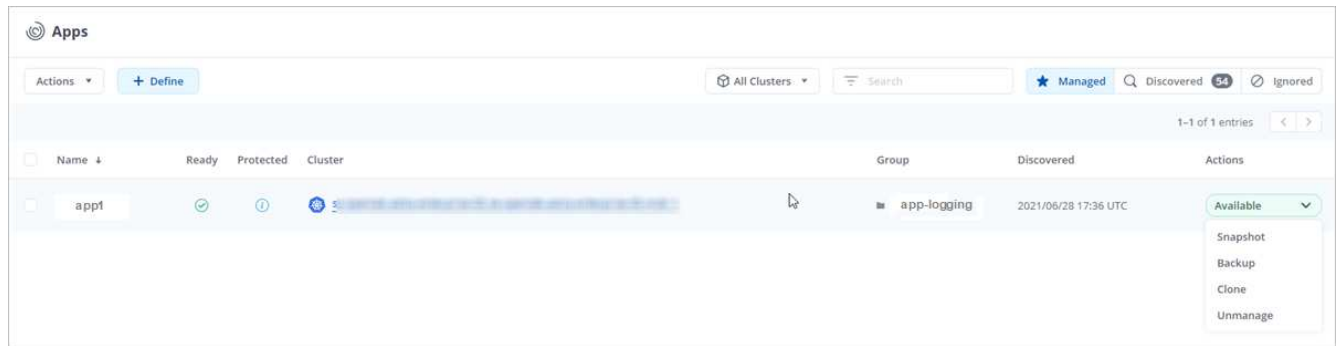
Astra Control le muestra las aplicaciones Helm y las aplicaciones personalizadas en el espacio de nombres. Si hay etiquetas Helm disponibles, se designarán con un icono de etiqueta.

4. Observe la columna **Grupo** para ver en qué espacio de nombres se está ejecutando la aplicación (está designada con el icono de carpeta).
5. Decida si desea gestionar cada aplicación de forma individual o a nivel de espacio de nombres.
6. Busque la aplicación que desee en el nivel deseado en la jerarquía y, en el menú acciones, seleccione **gestionar**.

7. Si no desea gestionar una aplicación, en el menú acciones situado junto a la aplicación, seleccione **Ignorar**.

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

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



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

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

Resultado

Las aplicaciones que eligió administrar ahora están disponibles en la pestaña **gestionado**. Cualquier aplicación ignorada se moverá a la pestaña **ignorada**. Lo ideal es que la ficha descubierto no muestre ninguna aplicación, de modo que, a medida que se instalan nuevas aplicaciones, resulta más fácil encontrarlos y gestionarlos.

Gestione aplicaciones mediante la etiqueta Kubernetes

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

Pasos

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

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

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

4. Haga clic en **definir aplicación personalizada**.

Resultado

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

Ignorar aplicaciones

Si se ha detectado una aplicación, ésta aparece en la lista descubierta. En este caso, puede limpiar la lista descubierta para que las nuevas aplicaciones que se han instalado sean más fáciles de encontrar. O bien,

puede que tenga aplicaciones que esté gestionando y, más adelante, decida que ya no desea gestionarlas. Si no desea administrar estas aplicaciones, puede indicar que deben ignorarse.

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

Pasos

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

Desgestionar aplicaciones

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



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

Pasos

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

¿y las aplicaciones del sistema?

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

Name	Ready	Cluster	Actions
...
...
...
default	Discovering

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



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

Obtenga más información

- ["Utilice la API Astra"](#)

Defina un ejemplo de aplicación personalizada

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

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

- Clonar
- Snapshot
- Backup
- Política de protección

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

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

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



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

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



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

Ejemplo: Política de protección independiente para el lanzamiento canario

En este ejemplo, el equipo de devops gestiona una puesta en marcha de versiones canaria. Su grupo tiene

tres pods que ejecutan nginx. Dos de los pods están dedicados a la versión estable. El tercer pod es para el lanzamiento canario.

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

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

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

Pasos

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

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

Proteja sus aplicaciones

Proteja las aplicaciones con snapshots y backups

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

Snapshot y backups

Un *snapshot* es una copia puntual de una aplicación que se almacena en el mismo volumen provisionado que la aplicación. Por lo general son rápidas. Las snapshots locales se usan para restaurar la aplicación a un momento específico anterior. Las copias Snapshot son útiles para los clones rápidos; las copias Snapshot incluyen todos los objetos de Kubernetes para la aplicación, incluidos los archivos de configuración.

Se almacena un *backup* en el almacén de objetos externo. Un backup puede tardar más lentamente en comparación con las copias Snapshot locales. Puede migrar una aplicación restaurando su copia de seguridad en un clúster diferente. También es posible elegir un período de retención más largo para backups.



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.

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.

Pasos

1. Haga clic en **aplicaciones** y, a continuación, en el nombre de una aplicación.
2. Haga clic en **Protección de datos**.
3. Haga clic en **Configurar directiva 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.

Configure protection policy

STEP 1/2: DETAILS

✕

PROTECTION SCHEDULE

🕒 Hourly

Every hour on the 0th minute, keep the last 4 snapshots

🕒 Daily

Daily at 02:00 (UTC), keep the last 15 snapshots

🕒 Weekly

Weekly on Mondays at 02:00 (UTC), keep the last 26 snapshots

🕒 Monthly

Every 1st of the month at 02:00 (UTC), keep the last 12 backups

● Hourly

● Daily

● **Weekly**

● Monthly

Select Weekday(s) (optional)

Monday X

Time (UTC) (optional)

02:00

– Snapshots to keep +

26

– Backups to keep +

0

BACKUP DESTINATION

Bucket

ntp-nautilus-bucket-10 - ntp-nautilus-bucket-10

Default

OVERVIEW

Schedule and retention

Define a policy to continuously protect your application on a schedule and configure a retention count to get started.

For select stateful applications, expect I/O to pause for a short time during a backup or snapshot operation.

Read more in [Protection policies](#)

Application

cattle-logging

Namespace

cattle-logging

Cluster

se-openlab-astra-enterprise-05-se-openlab-astra-enterprise-05-mstr-1

Cancel

Review →

5. Haga clic en **Revisión**.

6. Haga clic en **establecer directiva 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

- Haga clic en **aplicaciones**.
- Haga clic en la lista desplegable de la columna **acciones** de la aplicación deseada.
- Haga clic en **Snapshot**.
- Personalice el nombre de la instantánea y, a continuación, haga clic en **Revisión**.
- Revise el resumen de la instantánea y haga clic en **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.

9



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



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. Haga clic en **aplicaciones** y, a continuación, en el nombre de una aplicación.
2. Haga clic en **Protección de datos**.

Las instantáneas se muestran de forma predeterminada.

3. Haga clic en **copias de seguridad** para ver la lista de copias de seguridad.

Eliminar snapshots

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

Pasos

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

Resultado

Astra Control Center elimina la instantánea.

Eliminar backups

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



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

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

Resultado

Astra Control Center elimina la copia de seguridad.

Restaurar aplicaciones

Astra Control Center puede restaurar su aplicación a partir de una instantánea o una copia de seguridad. Los backups de almacenamiento persistente y las snapshots se transfieren del almacén de objetos, por lo que la restauración de una snapshot existente al mismo clúster será más rápida que otros métodos. Puede utilizar la interfaz de usuario de Astra o ["La API Astra"](#) para restaurar aplicaciones.



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



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



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

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

Pasos

1. Haga clic en **aplicaciones** y, a continuación, en el nombre de una aplicación.
2. Haga clic en **Protección de datos**.
3. Si desea restaurar desde una instantánea, mantenga seleccionado el icono **instantáneas**. De lo contrario, haga clic en el icono **copias de seguridad** para restaurar desde una copia de seguridad.
4. Haga clic en la lista desplegable de la columna **acciones** para la instantánea o la copia de seguridad desde la que desea restaurar.
5. Haga clic en **Restaurar aplicación**.
6. **Detalles de la restauración:** Especifique los detalles de la restauración:
 - Introduzca un nombre y un espacio de nombres para la aplicación.



Si va a restaurar una aplicación que se ha eliminado, elija un nombre y espacio de nombres diferentes para la aplicación que el nombre original. Si el nombre de la aplicación restaurada es el mismo que la aplicación eliminada, la operación de restauración fallará.

- Seleccione el clúster de destino de la aplicación.
 - Haga clic en **Revisión**.
7. **Resumen de restauración:** Revise los detalles sobre la acción de restauración y haga clic en **Restaurar**.

Resultado

Astra Control Center restaura la aplicación en función de la información proporcionada.



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

Clone y migre aplicaciones

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

API Astra" para clonar y migrar aplicaciones.



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

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



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



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

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

Lo que necesitará

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

Pasos

1. Haga clic en **aplicaciones**.
2. Debe realizar una de las siguientes acciones:
 - Haga clic en la lista desplegable de la columna **acciones** de la aplicación deseada.
 - Haga clic en el nombre de la aplicación deseada y seleccione la lista desplegable de estado en la parte superior derecha de la página.
3. Haga clic en **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. Haga clic en **Revisión**.
7. **Resumen de clones:** Revise los detalles sobre el clon y haga clic en **Clonar**.

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` estado en la página **aplicaciones**.

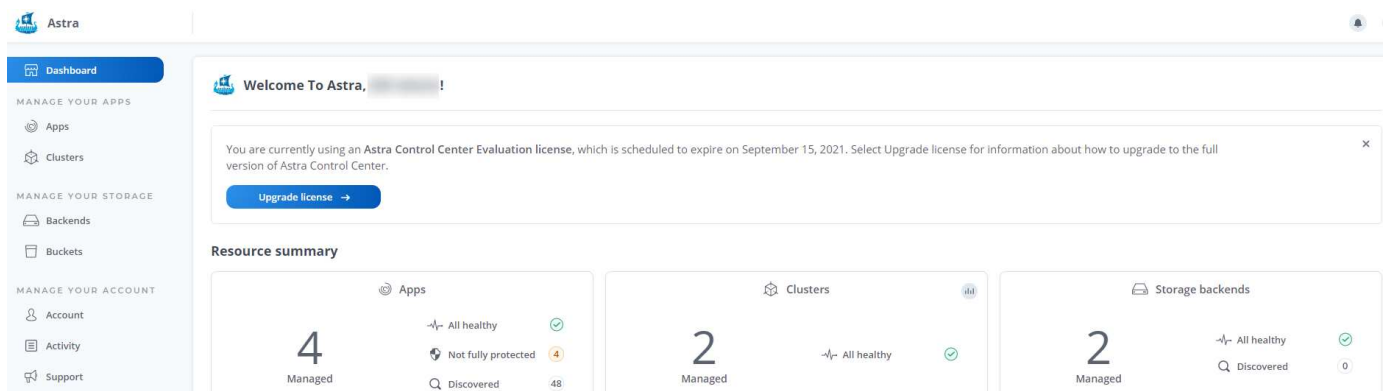


Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente 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.

Ver el estado de las aplicaciones y del clúster

Ver un resumen del estado de las aplicaciones y el clúster

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



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

Aplicaciones

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

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

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

Icono de clústeres

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

app.

Icono de los back-ends de almacenamiento

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

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

Consulte el estado y los detalles de los clústeres

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

Pasos

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



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

Ver el estado y los detalles de una aplicación

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

Pasos

1. En la interfaz de usuario de Astra Control Center, seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. Haga clic en alrededor para encontrar la información que está buscando:

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 **Apps**, siga los pasos descritos anteriormente.

Gestione su cuenta

Gestionar usuarios

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

Añadir usuarios

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

Pasos

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

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

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

Cada rol proporciona los siguientes permisos:

- Un **Visor** puede ver los recursos.
- Un **Miembro** tiene permisos de función de Viewer y puede administrar aplicaciones y clústeres, pero no puede anular la administración de aplicaciones o clústeres, ni eliminar instantáneas o copias de seguridad.
- Un **Admin** tiene permisos de rol de miembro y puede agregar y quitar cualquier otro usuario excepto el propietario.
- **Owner** tiene permisos de función de administrador y puede agregar y eliminar cualquier cuenta de usuario.

6. Haga clic en **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. Haga clic en el icono Usuario situado en la parte superior derecha de la pantalla.
2. Seleccione **Perfil**.
3. Haga clic en la lista desplegable **acciones** y seleccione **Cambiar contraseña**.
4. Introduzca una contraseña que se ajuste a los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.
6. Haga clic en **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**, haga clic en **cuenta**.
2. En la ficha **usuarios**, seleccione la lista desplegable en la columna **Estado** para el usuario.
3. Seleccione **Restablecer contraseña**.
4. Introduzca una contraseña temporal que cumpla los requisitos de contraseña.
5. Introduzca una vez más la contraseña para confirmarla.



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

6. Haga clic en **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**, haga clic en **cuenta**.
2. En la ficha **usuarios**, seleccione la lista desplegable en la columna **rol** para el usuario.
3. Seleccione una nueva función y, a continuación, haga clic en **Cambiar rol** cuando se le solicite.

Resultado

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

Quitar usuarios

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

Pasos

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

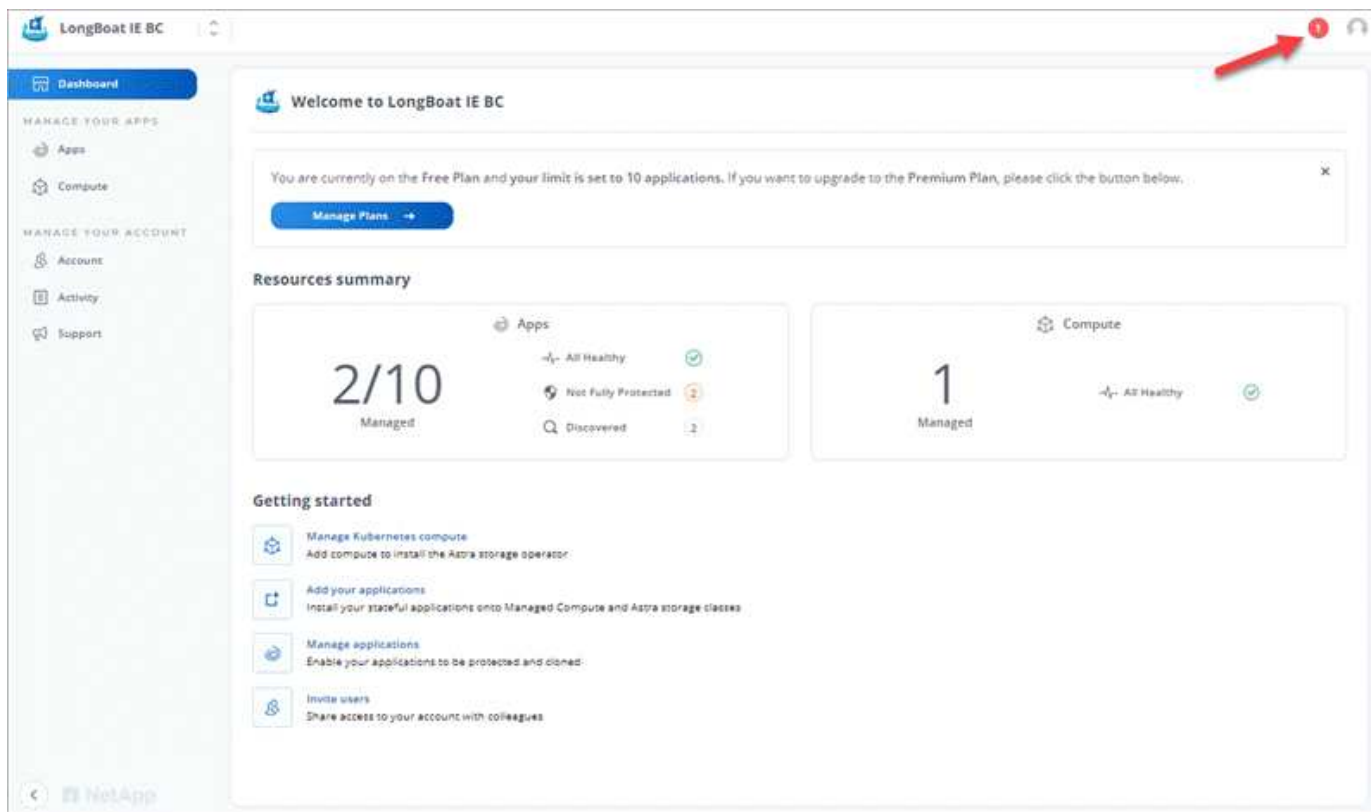
Resultado

Astra Control Center elimina al usuario de la cuenta.

Ver y gestionar notificaciones

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

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



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

Pasos

1. Haga clic en el número de notificaciones no leídas en la parte superior derecha.



2. Revise las notificaciones y haga clic en **Marcar como leído** o **Mostrar todas las notificaciones**.

Si hace clic en **Mostrar todas las notificaciones**, se carga la página Notificaciones.

3. En la página **Notificaciones**, vea las notificaciones, seleccione las que desea marcar como leídas, haga clic en **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

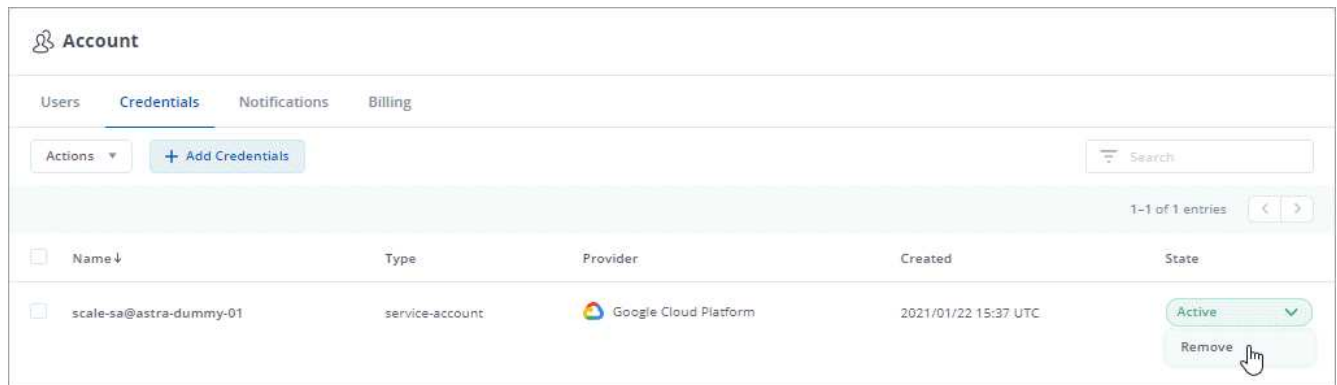
Eliminar credenciales de una cuenta en cualquier momento. Solo debe quitar credenciales después de ["desgestione todos los clústeres asociados"](#).



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. Haga clic en **cuenta > credenciales**.
2. Haga clic en la lista desplegable de la columna **Estado** para obtener las credenciales que desea quitar.
3. Haga clic en **Quitar**.



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

Resultado

Astra Control Center elimina las credenciales de la cuenta.

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 Astra"](#) para actualizar una licencia existente.

Pasos

1. Inicie sesión en el 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**, haga clic en el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta > licencias** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

Gestionar bloques

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

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

Utilice cualquiera de los siguientes proveedores de bloques:

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



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

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

Un cubo puede estar en uno de estos estados:

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

Para obtener instrucciones sobre cómo gestionar los cubos con la API Astra, consulte ["Información sobre API y automatización de Astra"](#).

Puede realizar estas tareas relacionadas con la gestión de bloques:

- ["Añadir un bucket"](#)
- [Editar un bloque](#)



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

Quite las credenciales

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

Para obtener más información, consulte ["Utilice la API Astra Control"](#).



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

Editar un bloque

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



Cuando agregue un cubo, seleccione el tipo de proveedor de cucharón correcto con las credenciales que sean correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como el tipo con credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los backups y las restauraciones futuras de aplicaciones que utilizan este bloque. Consulte ["Notas de la versión"](#).

Pasos

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



No puede modificar el tipo de segmento.

4. Seleccione **Actualizar**.

Obtenga más información

- ["Utilice la API Astra"](#)

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, consulte ["Información sobre API y automatización de Astra"](#).

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

- ["Añada un back-end de almacenamiento"](#)
- [Ver detalles del back-end de almacenamiento](#)
- [Desgestione un back-end de almacenamiento](#)

Ver detalles del back-end de almacenamiento

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

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

Pasos

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

Consulte los detalles del backends de almacenamiento en la opción Backends

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

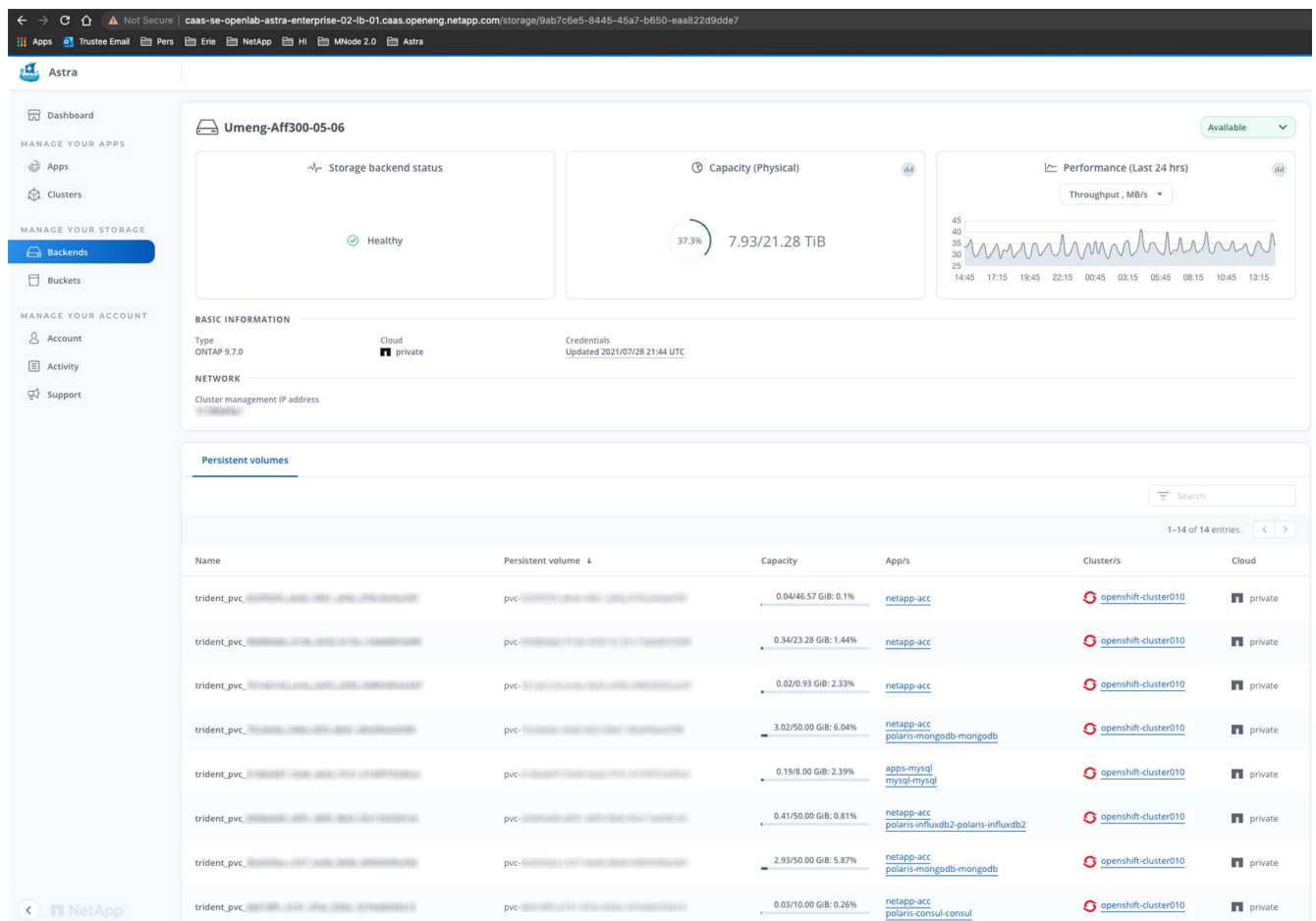
Con una conexión a Cloud Insights, puede ver los volúmenes que usan las aplicaciones de Kubernetes, que se almacenan en un back-end de almacenamiento seleccionado.

Pasos

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



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



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

Desgestione un back-end de almacenamiento

Puede anular la gestión del back-end.

Pasos

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

Obtenga más información

- ["Utilice la API Astra"](#)

Supervise y proteja la infraestructura

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

cree una conexión con Cloud Insights de NetApp. Para recopilar eventos Kubernetes de sistemas supervisados por Astra Control Center, añada una conexión fluentd.



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 aquí.

Agregar un servidor proxy

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



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

Pasos

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



HTTP PROXY

Configure Astra Control to send traffic through a proxy server.

Disconnected



Connect

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

Resultado

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



HTTP PROXY ?

Server: proxy.example.com:8888

Authentication: Enabled

Connected



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.

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.

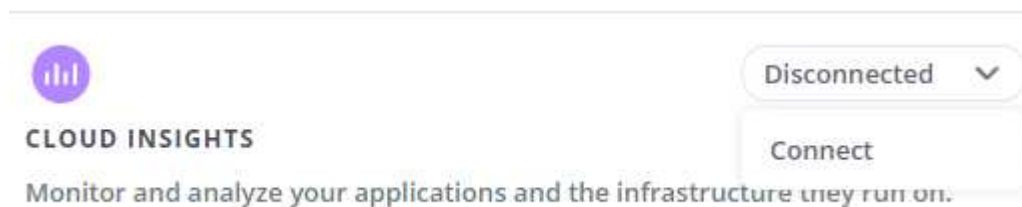


Si no tiene experiencia en Cloud Insights, familiarícese con las funciones y las funcionalidades ["aquí"](#).

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.

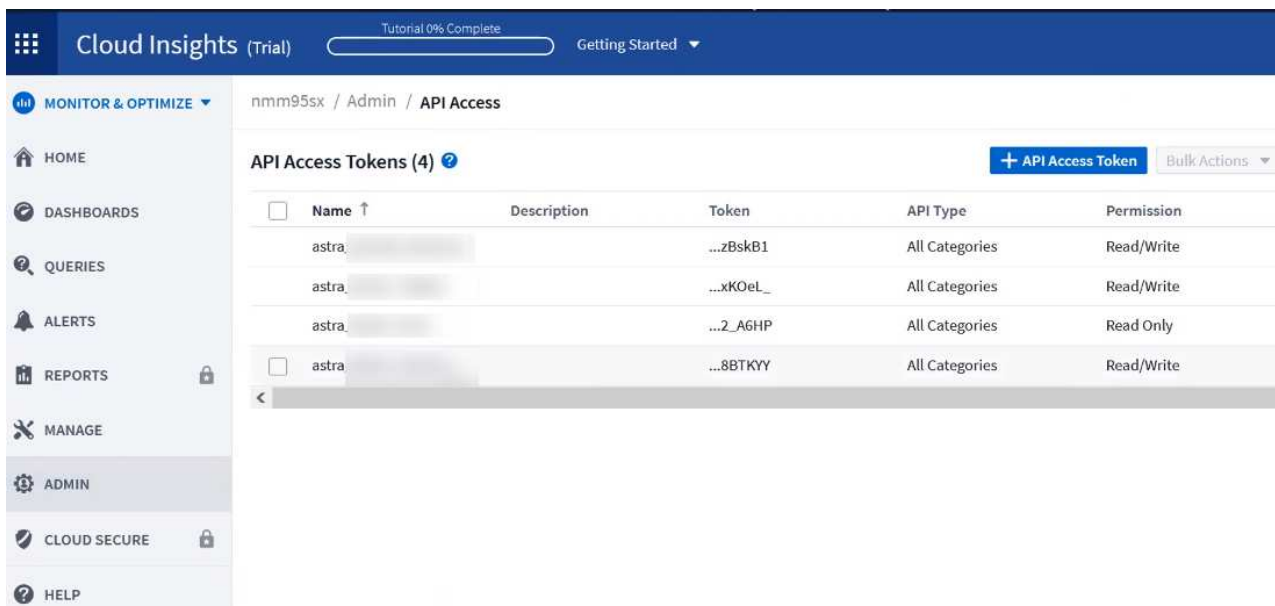


4. Introduzca los tokens de la API Cloud Insights y la URL del inquilino. La URL del inquilino tiene el siguiente formato, como ejemplo:

```
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"](#).

- Para obtener la **"Token de API"**, Inicie sesión en la dirección URL del inquilino de Cloud Insights.
- En Cloud Insights, genere un token API de tipo **sólo lectura**.



- Copie la tecla **sólo lectura**. Deberá pegarlo en la ventana Centro de control de Astra para habilitar la conexión a Cloud Insights.
- En Cloud Insights, genere un token de API de tipo **lectura/escritura**.
- Copie la tecla **Read/Write**. Deberá pegarlo en la ventana Centro de control de Astra **Connect Cloud Insights**.



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.

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

5. Seleccione **conectar**.



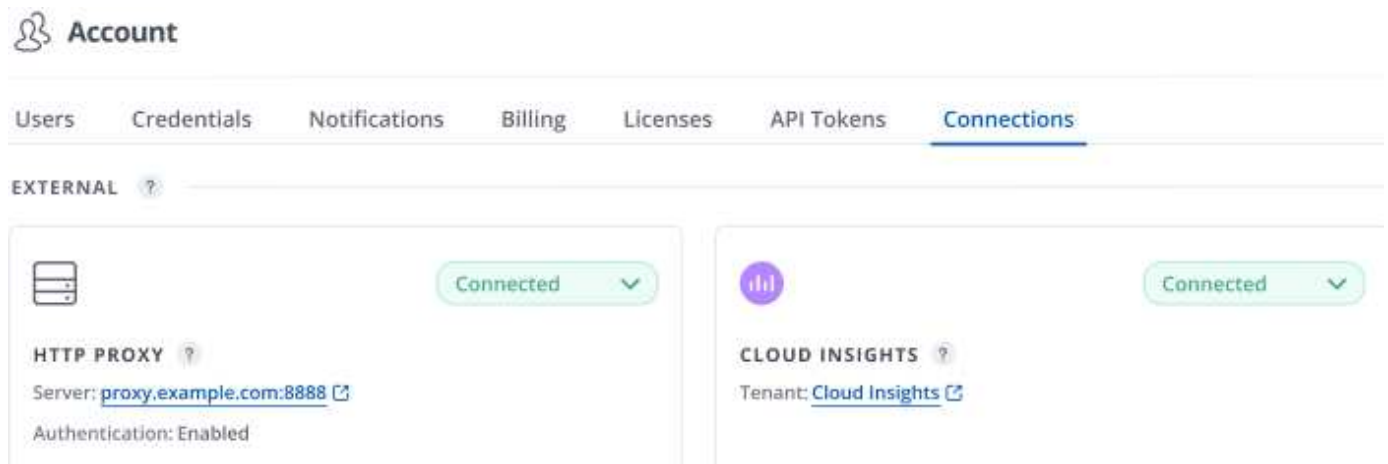
Después de seleccionar **conectar**, el estado de la conexión cambia a **pendiente** en la sección **Cloud Insights** de la página **cuenta > conexiones**. Puede pasar unos minutos para que la conexión esté activada y el estado cambie a **conectado**.



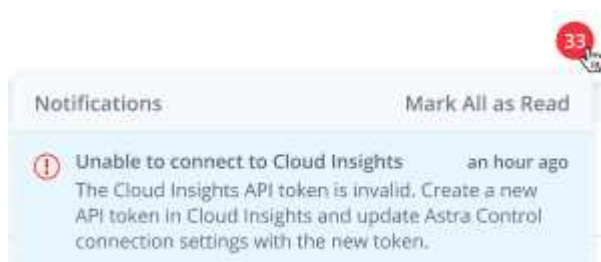
Para retroceder y avanzar fácilmente entre el Centro de control de Astra y las interfaces de usuario de Cloud Insights, asegúrese de que ha iniciado sesión en ambos.

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.

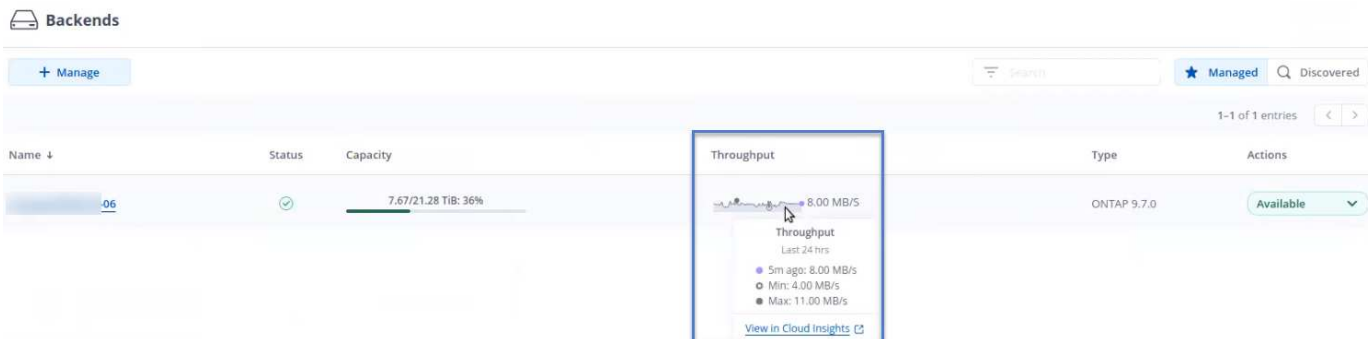


Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.



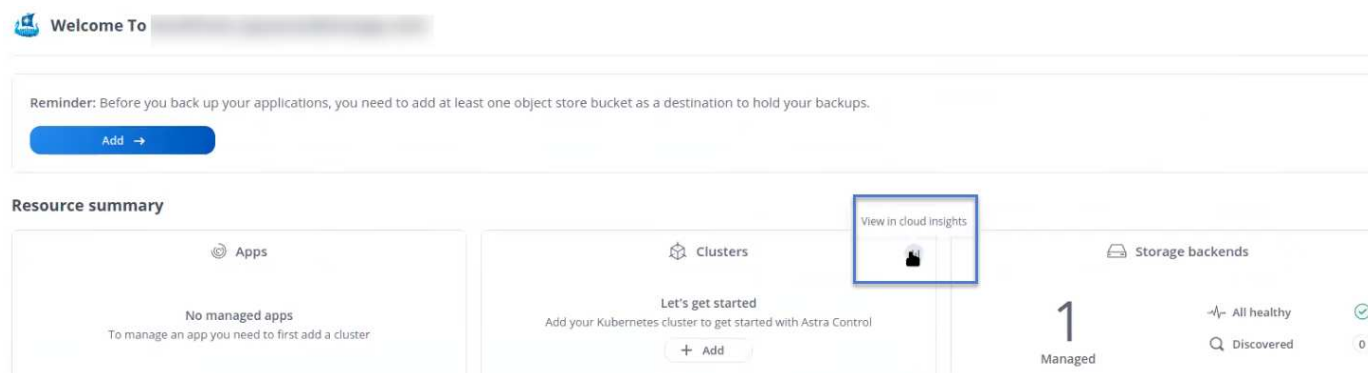
También puede encontrar la misma información en **cuenta > Notificaciones**.

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

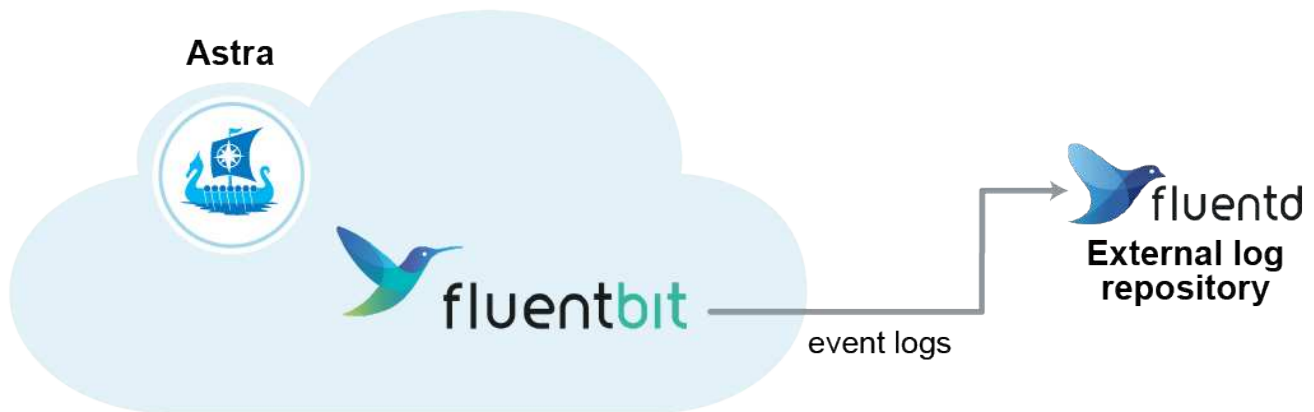
Puede deshabilitar la conexión Cloud Insights para un clúster de Kubernetes gestionado por Astra Control Center. Al deshabilitar la conexión Cloud Insights, no se eliminan los datos de telemetría ya cargados en Cloud Insights.

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.



FLUENTD

Connect Astra Control logs to Fluentd for use by your log analysis software.

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

Resultado

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

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

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



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

Edite la conexión fluentd

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

Pasos

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

Desactive la conexión fluentd

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

Pasos

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

Actualizar una licencia existente

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

Pasos

1. Inicie sesión en el 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**, haga clic en el menú desplegable de estado de la licencia existente y seleccione **Reemplazar**.
6. Busque el archivo de licencia que descargó.
7. Seleccione **Agregar**.

La página **cuenta > licencias** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

Desgestione aplicaciones y clústeres

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

Desgestionar una aplicación

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

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

Pasos

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

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

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

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



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

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla del clúster que ya no desea gestionar en Astra Control Center.

3. En el menú **acciones**, seleccione **Unmanage**.
4. Confirme que desea anular la administración del clúster y, a continuación, seleccione **Sí, anular la administración del clúster**.

Resultado

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



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

Desinstale Astra Control Center

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

Lo que necesitará

- Utilice la interfaz de usuario de Astra Control Center para anular la gestión de todos ["de clúster"](#).

Pasos

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

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

Resultado:

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

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

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

Resultado:

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

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

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

Resultado:

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

Obtenga más información

- ["Problemas conocidos para la desinstalación"](#)

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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