Utilice Astra Control Center

Astra Control Center

NetApp
August 11, 2025

Tabla de contenidos

Utilice Astra Control Center

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 definir las aplicaciones y sus recursos.

Puede definir y gestionar aplicaciones que incluyan recursos de almacenamiento con pods en ejecución o aplicaciones que incluyan recursos de almacenamiento sin ningún pods en ejecución. Las aplicaciones que no tienen pods en ejecución se conocen como aplicaciones de solo datos.

Y gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencias**: Para administrar aplicaciones con Astra Control Center, necesitas la licencia de evaluación integrada de Astra Control Center o una licencia completa.
- **Namespaces**: Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.
- **Clase de almacenamiento**: Si instala una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Recursos de Kubernetes**: Las aplicaciones que usan recursos de Kubernetes no recopilados por Astra Control podrían no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

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. Es totalmente compatible con la gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3). 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 diseñadas con una arquitectura “pass-by-value” en lugar de “pass-by-reference”. Un operador y la aplicación que instala deben usar el mismo espacio de nombres; es posible que deba modificar el archivo YAML de implementación para que el operador se asegure de que este es el caso.

  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. Cualquier aplicación que se limita a uno o más espacios de nombres se puede gestionar.

Defina las aplicaciones

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

Aunque Astra Control le permite gestionar por separado ambos niveles de la jerarquía (el espacio de nombres y las aplicaciones en ese espacio de nombres o espacio de nombres expansivo), la práctica recomendada 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.

Antes de empezar

- 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.
- Espacios de nombres existentes en el clúster Kubernetes que se añadió a Astra Control.
- (Opcional) una etiqueta de Kubernetes 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".

Acerca de esta tarea

- Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".
- Si planea utilizar varios espacios de nombres con sus aplicaciones en Astra Control, "modificar los roles de usuario con restricciones de espacio de nombres" Tras actualizar a una versión de Astra Control Center compatible con varios espacios de nombres.
- 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

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. Más información en un ejemplo.

Amplíe para obtener más información sobre cómo agregar recursos de ámbito de cluster a los espacios de nombres de aplicaciones.

Puede importar recursos de clúster asociados a los recursos de espacio de nombres además de los que se incluyen automáticamente Astra Control. Puede agregar una regla que incluirá recursos de un grupo específico, tipo, versión y, opcionalmente, etiqueta. Es posible que desee hacer esto si hay recursos que Astra Control no incluye automáticamente.

No puede excluir ninguno de los recursos con ámbito de clúster que Astra Control incluya automáticamente.

Puede agregar lo siguiente `apiVersions` (Que son los grupos combinados con la versión API):

Tipo de recursos	ApiVersions (grupo + versión)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admission registration.k8s.io/v1
`ValidatingWebhookConfiguration`	admission registration.k8s.io/v1

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. Elija un espacio de nombres para su aplicación en la lista desplegable **espacio de nombres**.

   Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.

5. (Opcional) Introduzca una etiqueta para los recursos de Kubernetes en cada 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. (Opcional) Añada espacios de nombres adicionales para la aplicación seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
7. (Opcional) Introduzca los criterios de etiqueta única o selector de etiquetas para los espacios de nombres adicionales que añada.
8. (Opcional) para incluir recursos de ámbito de clúster además de los que Astra Control incluye

automáticamente, marque **incluir recursos adicionales de ámbito de clúster** y complete lo siguiente:

a. Seleccione **Agregar regla de inclusión**.
b. **Grupo**: En la lista desplegable, seleccione el grupo API de recursos.
c. **Kind**: En la lista desplegable, seleccione el nombre del esquema de objetos.
d. **Versión**: Introduzca la versión API.
e. **Selector de etiquetas**: Opcionalmente, incluya una etiqueta que se agregará a la regla. Esta etiqueta se utiliza para recuperar solo los recursos que coincidan con esta etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster.
f. Revise la regla que se crea en función de las entradas.
g. Seleccione **Agregar**.

Puede crear tantas reglas de recursos con ámbito de clúster como desee. Las reglas aparecen en definir resumen de la aplicación.

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

Cuando termine de definir una aplicación, la aplicación aparecerá en `Healthy` estado 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.

Para ver los recursos agregados a esta aplicación, seleccione la ficha **Recursos**. Seleccione el número después del nombre del recurso en la columna Resource o introduzca el nombre del recurso en la búsqueda para ver los recursos adicionales con ámbito del clúster incluidos.

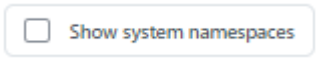
Defina un espacio de nombres para administrar como una aplicación

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 definir varias aplicaciones, seleccione en la lista de espacios de nombres y seleccione el botón **acciones** en la esquina superior izquierda y seleccione **definir como aplicación**. Esto definirá varias aplicaciones individuales en sus espacios de nombres individuales. Para aplicaciones con varios espacios de nombres, consulte Defina los recursos que se van a administrar como una aplicación.

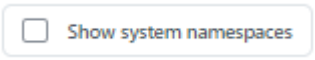
Active la casilla de verificación **Mostrar espacios de nombres del sistema** para mostrar los espacios de nombres del sistema que normalmente no se usan en la administración de aplicaciones de forma predeterminada.  "Leer más".

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

¿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 Center no se muestra de forma predeterminada como una aplicación que puedes gestionar, pero puedes crear backups y restaurar una instancia de Astra Control Center mediante otra instancia de Astra Control Center.

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"
- "Desgestionar una aplicación"

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 SnapMirror de NetApp. 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 Control Center o "La API de control Astra" para proteger aplicaciones.

Acerca de esta tarea

- **Helm implementó aplicaciones**: Si utiliza Helm para implementar 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.
- **(Solo clústeres de OpenShift) Agregar políticas**: Cuando crea un proyecto para alojar una aplicación en un clúster de OpenShift, al proyecto (o espacio de nombres de Kubernetes) se le asigna un UID de SecurityContext. 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
- Habilite el backup y la restauración para las operaciones económicas de ontap-nas
- Cree un backup inmutable
- 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.

Si necesita que backups o snapshots se ejecuten con más frecuencia de una vez por hora, puede hacerlo "Utilice la API REST de Astra Control para crear copias Snapshot y copias de seguridad".

Si va a definir una política de protección que crea backups inmutables para escribir bloques WORM (escritura única y lectura múltiple), asegúrese de que el tiempo de retención de los backups no sea más corto que el período de retención configurado para el bloque.

Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

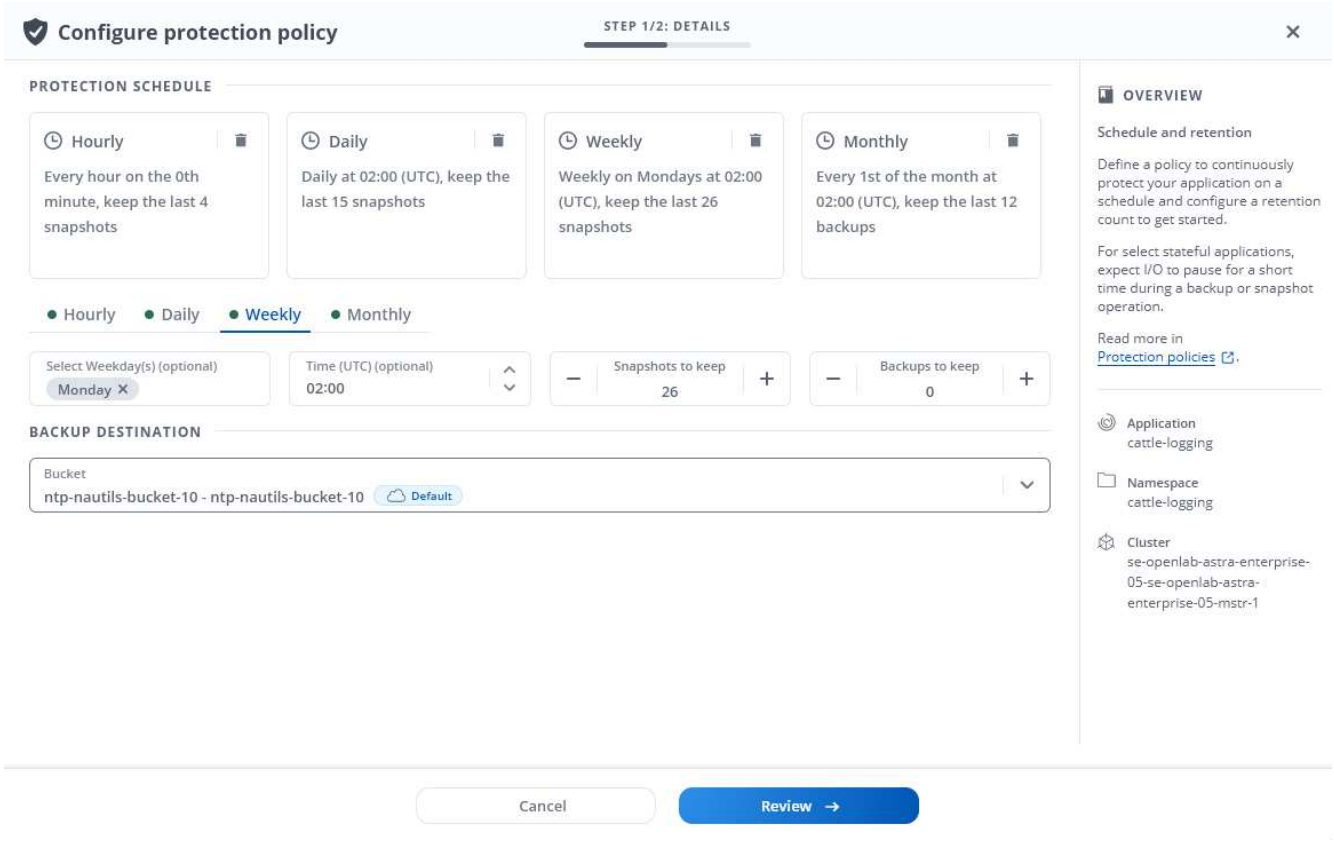
Pasos

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.

   Al establecer un nivel de retención para backups, puede elegir el bloque en el que desea almacenar los backups.

   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 implementa la política de protección de datos mediante la creación y retención de copias Snapshot y copias de seguridad con la política de programación y retención que haya definido.

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

Acerca de esta tarea

Astra Control permite la creación de copias Snapshot con clases de almacenamiento respaldadas por los siguientes controladores:

- `ontap-nas`
- `ontap-san`
- `ontap-san-economy`

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, no se pueden crear instantáneas. Utilice una clase de almacenamiento alternativa para las instantáneas.

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 **Siguiente**.
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 **saludable** en la columna **Estado** de la página **Protección de datos** > **instantáneas**.

Cree un backup

Puede realizar una copia de seguridad de una aplicación en cualquier momento.

Acerca de esta tarea

Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` conductor, usted necesita habilite el backup y la restauración funcionalidad. Asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

> Astra Control permite la creación de backups mediante clases de almacenamiento respaldadas por los siguientes controladores:
>
> - `ontap-nas`
> - `ontap-nas-economy`
> - `ontap-san`
> - `ontap-san-economy`

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 bucket de destino para el backup en la lista de bloques de almacenamiento.
6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control 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.
- Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice las instrucciones de Eliminar backups.
- 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.

Habilite el backup y la restauración para las operaciones económicas de ontap-nas

Astra Control Provisioning ofrece funcionalidad de backup y restauración que puede habilitarse para los back-ends de almacenamiento que utilicen el `ontap-nas-economy` clase de almacenamiento.

Antes de empezar

- Ya tienes "Habilitado Astra Control Provisioning".
- Has definido una aplicación en Astra Control. Esta aplicación tendrá funcionalidad de protección limitada hasta que complete este procedimiento.
- Ya tienes `ontap-nas-economy` se ha seleccionado como la clase de almacenamiento predeterminada para el back-end del almacenamiento.

Expanda para obtener pasos de configuración

1. Realice lo siguiente en el back-end de almacenamiento de ONTAP:

   a. Busque la SVM donde aloja el `ontap-nas-economy`-basado en volúmenes de la aplicación.

   b. Inicie sesión en un terminal conectado a ONTAP donde se crean los volúmenes.

   c. Oculte el directorio de snapshots para la SVM:

   > Este cambio afecta a toda la SVM. El directorio oculto seguirá siendo accesible.

   ```
   nfs modify -vserver <svm name> -v3-hide-snapshot enabled
   ```

   +

   > Compruebe que el directorio de snapshots del back-end de almacenamiento de ONTAP esté oculto. Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.

2. Haga lo siguiente en Astra Trident:

   a. Active el directorio de instantáneas para cada VP que sea `ontap-nas-economy` basado y asociado con la aplicación:

   ```
   tridentctl update volume <pv name> --snapshot-dir=true --pool
   -level=true -n trident
   ```

   b. Confirme que el directorio de snapshots se haya habilitado para cada VP asociado:

   ```
   tridentctl get volume <pv name> -n trident -o yaml | grep
   snapshotDir
   ```

   Respuesta:

   ```
   snapshotDirectory: "true"
   ```

3. En Astra Control, actualiza la aplicación después de habilitar todos los directorios Snapshot asociados para que Astra Control reconozca el valor modificado.

Resultado

La aplicación está lista para realizar backups y restauraciones con Astra Control. Otras aplicaciones también pueden utilizar cada RVP para realizar backups y restauraciones de datos.

Cree un backup inmutable

No se puede modificar, eliminar ni sobrescribir una copia de seguridad inmutable siempre que la política de retención del depósito que almacena la copia de seguridad la prohíba. Puede crear backups inmutables mediante el backup de aplicaciones en bloques que tengan configurada una política de retención. Consulte "Protección de datos" para obtener información importante sobre cómo trabajar con backups inmutables.

Antes de empezar

Debe configurar el bucket de destino con una política de retención. La forma de hacerlo variará en función del proveedor de almacenamiento que utilice. Consulte la documentación del proveedor de almacenamiento para obtener más información:

- **Amazon Web Services**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «gobierno» con un período de retención predeterminado".
- **NetApp StorageGRID**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «cumplimiento» con un período de retención predeterminado".

> Los buckets en Astra Control no informan sobre la capacidad disponible. Antes de realizar backups o clonar aplicaciones gestionadas por Astra Control, comprueba la información del bucket en el sistema de administración del almacenamiento correspondiente.

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, asegúrese de que ha definido un `backendType` parámetro en la "Objeto de almacenamiento de Kubernetes" con un valor de `ontap-nas-economy` antes de ejecutar cualquier operación de protección.

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 bucket de destino para el backup en la lista de bloques de almacenamiento. Se indica un depósito de escritura única y lectura múltiple (WORM) con el estado «bloqueado» junto al nombre del depósito.

   > Si el depósito es de tipo no admitido, se indica cuando pasa el ratón por encima o selecciona el depósito.

6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

Resultado

Astra Control crea un backup inmutable 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.
- Si intentas crear dos backups inmutables de la misma aplicación en el mismo bloque a la vez, Astra Control impide que se inicie el segundo backup. Espere hasta que se complete la primera copia de seguridad antes de iniciar otra.
- No es posible cancelar una copia de seguridad inmutable en ejecución.
- 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.

Se indica una copia de seguridad inmutable con el estado «Locked» junto al bloque que está utilizando.

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 es posible eliminar una copia de Snapshot que se está replicando actualmente.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
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 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 `Running` estado. No puede cancelar una copia de seguridad que esté en `Pending` estado.

No es posible cancelar una copia de seguridad inmutable en ejecución.

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 operación y, a continuación, seleccione **Sí, cancelar copia de seguridad**.

Eliminar backups

Elimine los backups programados o bajo demanda que ya no necesita. No puede eliminar un backup realizado en un bloque inmutable hasta que la política de retención del bloque lo permita.

No se puede eliminar un backup inmutable antes de que caduque el período de retención.

Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice estas instrucciones.

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 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. "API de control Astra" para restaurar aplicaciones.

Antes de empezar

- **Proteja sus aplicaciones primero**: Se recomienda encarecidamente que tome una instantánea o una copia de seguridad de su aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup si la restauración no se realiza correctamente.

- **Comprobar volúmenes de destino**: Si restaura a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento 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. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que falle la operación de restauración. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- **Planificar necesidades de espacio**: Cuando se realiza una restauración in situ de una aplicación que utiliza almacenamiento ONTAP de NetApp, el espacio utilizado por la aplicación restaurada puede duplicarse. Después de realizar una restauración sin movimiento, elimine las instantáneas no deseadas de la aplicación restaurada para liberar espacio de almacenamiento.
- **(Solo clústeres de Red Hat OpenShift) Agregar políticas**: Cuando crea un proyecto para alojar una aplicación en un clúster de OpenShift, al proyecto (o espacio de nombres de Kubernetes) se le asigna un UID de SecurityContext. 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
  ```

- **Controladores de clase de almacenamiento compatibles**: Astra Control admite la restauración de copias de seguridad mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(Solo controlador económico de ontap-nas) Copias de seguridad y restauraciones**: Antes de realizar copias de seguridad o restaurar una aplicación que utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, compruebe que el "El directorio Snapshot del sistema de administración de almacenamiento de ONTAP está oculto". Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.
- * Aplicaciones implementadas de Helm*: Las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. Las aplicaciones implementadas con Helm 2 no son compatibles.

La ejecución de una operación de restauración sin movimiento en una aplicación que comparte recursos con otra aplicación puede tener resultados no intencionados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones. Para obtener más información, consulte este ejemplo.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación.
2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.
3. Elija el tipo de restauración:

- **Restaurar en espacios de nombres originales**: Utilice este procedimiento para restaurar la aplicación en su sitio al cluster original.

> Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` driver, debe restaurar la aplicación utilizando las clases de almacenamiento originales. No puede especificar una clase de almacenamiento diferente si va a restaurar la aplicación en el mismo espacio de nombres.

  i. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación en el lugar, lo que revierte la aplicación a una versión anterior de sí misma.
  ii. Seleccione **Siguiente**.

> 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.

- **Restaurar en nuevos espacios de nombres**: Utilice este procedimiento para restaurar la aplicación en otro clúster o con diferentes espacios de nombres desde el origen.
  i. Especifique el nombre de la aplicación restaurada.
  ii. Elija el clúster de destino de la aplicación que desea restaurar.
  iii. Introduzca un espacio de nombres de destino para cada espacio de nombres de origen asociado a la aplicación.

> Astra Control crea nuevos espacios de nombres de destino como parte de esta opción de restauración. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

  iv. Seleccione **Siguiente**.
  v. Seleccione la instantánea o la copia de seguridad que desea utilizar para restaurar la aplicación.
  vi. Seleccione **Siguiente**.
  vii. Elija una de las siguientes opciones:
    - **Restaurar usando clases de almacenamiento originales**: La aplicación utiliza la clase de almacenamiento asociada originalmente a menos que no exista en el clúster de destino. En este caso, se utilizará la clase de almacenamiento predeterminada para el clúster.
    - **Restaurar usando una clase de almacenamiento diferente**: Seleccione una clase de almacenamiento que exista en el clúster de destino. Todos los volúmenes de aplicaciones, independientemente de sus tipos de almacenamiento asociados originalmente, se migrarán a esta clase de almacenamiento diferente como parte de la restauración.
  viii. Seleccione **Siguiente**.

4. Elija cualquier recurso para filtrar:
   - **Restaurar todos los recursos**: Restaurar todos los recursos asociados con la aplicación original.
   - **Filtrar recursos**: Especificar reglas para restaurar un subconjunto de los recursos originales de la aplicación:
     i. Seleccione incluir o excluir recursos de la aplicación restaurada.

ii. Seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión** y configure la regla para filtrar los recursos correctos durante la restauración de la aplicación. Puede editar una regla o eliminarla y volver a crear una regla hasta que la configuración sea correcta.

> Para obtener más información sobre la configuración de reglas de inclusión y exclusión, consulte Filtre recursos durante una restauración de aplicación.

5. Seleccione **Siguiente**.
6. Revise los detalles sobre la acción de restauración cuidadosamente, escriba “restaurar” (si se le solicita) y seleccione **Restaurar**.

Resultado

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

> Después de una operación de protección de datos (clonado, backup o restauración) y un posterior tamaño de volumen persistente, se produce un retraso de hasta veinte minutos antes de que se muestre el tamaño del nuevo 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.

> 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 que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Filtre recursos durante una restauración de aplicación

Puede agregar una regla de filtro a un "restaurar" operación que especificará los recursos de aplicación existentes que se incluirán o excluirán de la aplicación restaurada. Puede incluir o excluir recursos basados en un espacio de nombres, etiqueta o GVK (GroupVersionKind) especificado.

Amplíe para obtener más información sobre Incluir y excluir escenarios

- **Selecciona una regla de inclusión con espacios de nombres originales (restauración in situ)**: Los recursos de aplicación existentes que definas en la regla se eliminarán y reemplazarán por aquellos de la instantánea o copia de seguridad seleccionada que estés utilizando para la restauración. Cualquier recurso que no especifique en la regla Incluir permanecerá sin cambios.
- **Selecciona una regla de inclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas en la aplicación restaurada. Los recursos que no especifique en la regla Incluir no se incluirán en la aplicación restaurada.
- **Selecciona una regla de exclusión con espacios de nombres originales (restauración in situ)**: Los recursos que especifiques para ser excluidos no se restaurarán y permanecerán sin cambios. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup. Todos los datos de los volúmenes persistentes se eliminarán y volverán a crear si el StatefulSet correspondiente forma parte de los recursos filtrados.
- **Selecciona una regla de exclusión con nuevos espacios de nombres**: Usa la regla para seleccionar los recursos específicos que deseas eliminar de la aplicación restaurada. Los recursos que no especifique para excluir se restaurarán de la Snapshot o el backup.

Las reglas son tipos de inclusión o exclusión. Las reglas que combinan la inclusión y exclusión de recursos no están disponibles.

Pasos

1. Una vez que haya elegido filtrar recursos y seleccionado una opción Incluir o Excluir en el asistente Restaurar aplicación, seleccione **Agregar regla de inclusión** o **Agregar regla de exclusión**.

   No puede excluir ningún recurso en el ámbito del clúster que Astra Control incluya automáticamente.

2. Configure la regla de filtro:

   Debe especificar al menos un espacio de nombres, una etiqueta o un GVK. Asegúrese de que los recursos que retenga después de aplicar las reglas de filtro sean suficientes para mantener la aplicación restaurada en buen estado.

   a. Seleccione un espacio de nombres específico para la regla. Si no hace una selección, se usarán todos los espacios de nombres en el filtro.

      Si la aplicación contenía originalmente varios espacios de nombres y la restauraba en nuevos espacios de nombres, todos los espacios de nombres se crearán incluso si no contienen recursos.

   b. (Opcional) Introduzca un nombre de recurso.

   c. (Opcional) **Selector de etiquetas**: Incluye a. "selector de etiquetas" para agregar a la regla. El selector de etiquetas se utiliza para filtrar sólo los recursos que coincidan con la etiqueta seleccionada.

   d. (Opcional) Seleccione **Usar GVK (GroupVersionKind) configurado para filtrar recursos** para opciones de filtrado adicionales.

      Si utiliza un filtro GVK, debe especificar Versión y Tipo.

i. (Opcional) **Grupo**: En la lista desplegable, seleccione el grupo API de Kubernetes.

ii. **Kind**: En la lista desplegable, seleccione el esquema de objeto para el tipo de recurso de Kubernetes a utilizar en el filtro.

iii. **Versión**: Seleccione la versión de la API de Kubernetes.

3. Revise la regla que se crea en función de las entradas.
4. Seleccione **Agregar**.

Puede crear tantas reglas de inclusión y exclusión de recursos como desee. Las reglas aparecen en el resumen de la aplicación de restauración antes de iniciar la operación.

Complicaciones de restauración in situ para una aplicación que comparte recursos con otra aplicación

Puede realizar una operación de restauración in situ en una aplicación que comparta recursos con otra aplicación y produzca resultados no deseados. Los recursos compartidos entre las aplicaciones se reemplazan cuando se realiza una restauración sin movimiento en una de las aplicaciones.

A continuación se muestra un ejemplo que crea una situación no deseable cuando se usa la replicación SnapMirror de NetApp para una restauración:

1. Defina la aplicación `app1` uso del espacio de nombres `ns1`.
2. Puede configurar una relación de replicación para `app1`.
3. Defina la aplicación `app2` (en el mismo clúster) mediante los espacios de nombres `ns1` y.. `ns2`.
4. Puede configurar una relación de replicación para `app2`.
5. La replicación se invierte para `app2`. Esto provoca la `app1` en el clúster de origen que se va a desactivar.

Replicar aplicaciones entre back-ends de almacenamiento 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 configurado, esto permite a sus aplicaciones replicar los cambios de aplicaciones y datos de un back-end de almacenamiento a otro, en el mismo clúster o entre diferentes clústeres.

Si quiere ver una 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:

- Sitio local A a sitio local A
- 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 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
- Ponga una aplicación replicada en línea 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

La replicación de aplicaciones de Astra Control requiere que se cumplan los siguientes requisitos previos antes de empezar:

Clústeres ONTAP

- **Astra Trident**: Astra Trident versión 22,10 o posterior debe existir en los clústeres de Kubernetes de origen y destino que utilicen ONTAP como backend. Astra Control admite la replicación con la tecnología SnapMirror de NetApp mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-san`
- **Licencias**: Las licencias asíncronas de SnapMirror de ONTAP que utilizan el paquete de protección de datos deben estar habilitadas en los clústeres de ONTAP de origen y de destino. Consulte "Información general sobre las licencias de SnapMirror en ONTAP" si quiere más información.

Interconexión

- **Cluster y SVM**: Los back-ends de almacenamiento ONTAP deben ser peered. Consulte "Información general sobre relaciones entre iguales de clústeres y SVM" si quiere más información.

  > Compruebe que los nombres de las SVM utilizados en la relación de replicación entre dos clústeres de ONTAP sean únicos.

- **Astra Trident y SVM**: Las SVM remotas entre iguales deben estar disponibles para Astra Trident en el clúster de destino.

Astra Control Center

- **Backends administrados**: Necesitas agregar y administrar backends de almacenamiento de ONTAP en el Centro de control de Astra para crear una relación de replicación.

  Solo para el aprovisionador de control de Astra_*: Agregar y administrar los back-ends de almacenamiento

de ONTAP en el Centro de control de Astra es opcional si has habilitado el aprovisionador de control de Astra para el Centro de control de Astra 23,10 o posterior.

- **Clusters administrados**: Agregue y administre los siguientes clusters con Astra Control, idealmente en diferentes dominios o sitios de falla:
  - Clúster de Kubernetes de origen
  - Clúster de Kubernetes de destino
  - Clústeres de ONTAP asociados
- **Cuentas de usuario**: Cuando añades un backend de almacenamiento de ONTAP al Centro de control de Astra, aplica las credenciales de usuario con el rol “admin”. Este rol tiene métodos de acceso `http` y.. `ontapi` Se habilitó en los clústeres de origen y destino de ONTAP. Consulte "Gestionar cuentas de usuario en la documentación de ONTAP" si quiere más información.

  Solo para el aprovisionador de control de Astra: Si has habilitado la funcionalidad de aprovisionamiento de Astra Control, ya no necesitas definir específicamente un rol de administrador para gestionar los clústeres en Astra Control Center, ya que estas credenciales ya no son necesarias en Astra Control Center.

"Pon en marcha Astra Control Center" en un tercer dominio de fallo o centro secundario para proporcionar una recuperación ante desastres sin problemas.

Astra Control Center no admite la replicación de SnapMirror de NetApp para back-ends de almacenamiento que utilizan el protocolo NVMe over TCP.

Configuración de Astra Trident/ONTAP

Astra Control Center requiere que configure al menos un back-end de almacenamiento que admita replicación para los clústeres de origen y destino. Si los clústeres de origen y destino son los mismos, la aplicación de destino debe usar un back-end de almacenamiento diferente al de la aplicación de origen para obtener la mejor resiliencia.

La replicación de Astra Control admite aplicaciones que utilicen una única clase de almacenamiento. Al agregar una aplicación a un espacio de nombres, asegúrese de que la aplicación tenga la misma clase de almacenamiento que otras aplicaciones del espacio de nombres. Cuando agregue una RVP a una aplicación replicada, asegúrese de que la nueva RVP tenga la misma clase de almacenamiento que otras RVP del espacio de nombres.

Configurar una relación de replicación

La configuración de una relación de replicación implica lo siguiente:

- Selección de la frecuencia con la que quieres que Astra Control tome una instantánea de una aplicación (que incluye los recursos de Kubernetes de la aplicación, así como las instantáneas de volumen de 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 la hora para que se realice la snapshot

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.

2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. Seleccione **Configurar política 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:
   - **Cluster de destino**: Introduzca un cluster de destino (puede ser el mismo que el cluster de origen).
   - **Clase de almacenamiento de destino**: Seleccione o introduzca la clase de almacenamiento que utiliza la SVM con pares en el clúster de ONTAP de destino. Como práctica recomendada, la clase de almacenamiento de destino debe apuntar a un back-end de almacenamiento distinto al de la clase de almacenamiento de origen.
   - **Tipo de replicación**: `Asynchronous` actualmente es el único tipo de replicación disponible.
   - **Espacio de nombres de destino**: Introduzca espacios de nombres de destino nuevos o existentes para el clúster de destino.
   - (Opcional) Añada espacios de nombres adicionales seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
   - **Frecuencia de replicación**: Establece la frecuencia con la que quieres que Astra Control tome una instantánea y la replique en el destino.
   - **Offset**: Establece el número de minutos desde la parte superior de la hora en que quieres que Astra Control tome una instantánea. Es posible que desee utilizar un offset para no coincidir con otras operaciones programadas.

   Reajuste los programas de copia de seguridad y replicación para evitar superposiciones de programas. Por ejemplo, realice backups en la parte superior de la hora cada hora y programe la replicación para que comience con un desplazamiento de 5 minutos y un intervalo de 10 minutos.

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 snapshot de aplicación utilizada para la replicación.

6. Para ver el estado de la instantánea de la aplicación, seleccione la pestaña **Aplicaciones** > **Snapshots**.

   El nombre de la snapshot usa el formato de `replication-schedule-<string>`. Astra Control conserva la última snapshot utilizada para la replicación. Cualquier instantánea de replicación más antigua se elimina 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.
- Realiza una instantánea inicial coherente con las aplicaciones.
- Establece la relación de SnapMirror para volúmenes persistentes mediante la snapshot inicial.

La página **Protección de datos** muestra el estado y el estado de la relación de replicación:
<Health status> | <Relationship life cycle state>

Por ejemplo:
Normal | Establecido

Obtenga más información acerca de los estados y el estado de replicación al final de este tema.

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

Mediante Astra Control, puede conmutar al respaldo las aplicaciones replicadas en 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. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, seleccione **Error**.
4. En la página de conmutación por error, revise la información y seleccione **failover**.

Resultado

Las siguientes acciones se producen como resultado del procedimiento de failover:

- La aplicación de destino se inicia en función de la última instantánea replicada.
- 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 según los horarios presentes en la aplicación de origen en el momento de la conmutación por error.
- Si la aplicación de origen tiene uno o más ganchos de ejecución posteriores a la restauración habilitados, esos ganchos de ejecución se ejecutan para la aplicación de destino.
- 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. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, selecciona **Resincronizar**.

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 back-end del almacenamiento de destino y continuar replicando de nuevo al back-end del almacenamiento de origen original. Astra Control detiene la aplicación de origen y replica los datos en el destino antes de conmutar por error a la aplicación de destino.

En esta situación, está intercambiando el origen y el destino.

Pasos

1. En la navegación izquierda de Astra Control, seleccione **aplicaciones**.
2. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. 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 toma una instantánea de los recursos de Kubernetes de la aplicación de origen original.
- 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).
- Después de que los pods se cierran, se toman y replican instantáneas de los volúmenes de la aplicación.
- 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 a partir de la instantánea previa al cierre, utilizando los datos del volumen replicados después de que se cerró 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 conseguir un «retorno tras la recuperación» después de una operación de

conmutación por error utilizando la siguiente secuencia de operaciones. En este flujo de trabajo para restaurar la dirección de replicación original, Astra Control replica (resincroniza) cualquier cambio de aplicación en la aplicación de origen original antes de revertir la dirección de la replicación.

Este proceso se inicia desde una relación que ha completado una conmutación al nodo de respaldo 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. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. En el menú Acciones, selecciona **Resincronizar**.
4. Para una operación de conmutación por error, seleccione la aplicación con error como origen de la operación de resincronización (conservando los datos escritos después de la conmutación por error).
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. Seleccione la pestaña **Protección de datos** > **Replicación**.
3. 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.
  - Se establece la relación (por lo que una instantánea se ha replicado correctamente y es posible la recuperación tras fallos), pero la instantánea más reciente ha fallado o no se ha podido replicar.

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 los RVP estén disponibles, comprueba la relación de replicación, crea snapshots de la aplicación periódicamente e identifica cualquier RVP de origen nuevo en la aplicación. Si es así, Astra Control crea los recursos para incluirlos en la replicación.
- **Fallo**: Astra Control rompe las relaciones de SnapMirror y restaura los recursos de Kubernetes de la aplicación a partir de la última instantánea de la aplicación replicada con éxito.
- **Fallo de más**: Astra Control deja de replicar desde el clúster de origen, utiliza la instantánea de la aplicación replicada más reciente (exitosa) 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

Puede clonar una aplicación existente para crear una aplicación duplicada en el mismo clúster de Kubernetes o en otro clúster. Cuando Astra Control 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 Control Center o "API de control Astra" para clonar y migrar aplicaciones.

Antes de empezar

- **Comprobar volúmenes de destino**: Si clona a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de clonado si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que se produzca un error en la operación de clonado. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- Para clonar aplicaciones en un clúster diferente, debe asegurarse de que las instancias de cloud que contienen los clústeres de origen y destino (si no son iguales) tienen un bloque predeterminado. Deberá asignar un bloque predeterminado para cada instancia de cloud.
- Durante las operaciones de clonado, las aplicaciones que necesitan un recurso IngressClass o enlaces web para funcionar correctamente no deben tener esos recursos ya definidos en el clúster de destino.

> Durante la clonación de aplicaciones en entornos OpenShift, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Por este motivo, es necesario configurar una política de exportación de volúmenes ONTAP para permitir estas operaciones. Puede hacerlo con los siguientes comandos:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

Limitaciones de clones

- **Clases de almacenamiento explícitas**: Si implementa una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Aplicaciones respaldadas por la economía de ontap-nas**: No puede usar operaciones de clonación si la clase de almacenamiento de su aplicación está respaldada por el `ontap-nas-economy` controlador. Sin embargo, usted puede "habilite el backup y la restauración para las operaciones económicas de ontap-nas".
- **Clones y restricciones de usuario**: 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 a un nuevo espacio de nombres en el mismo clúster o a 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 que una operación de clonado o restauración crea un nuevo

espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

- **Los clones utilizan cubos predeterminados**: Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar opcionalmente 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.
- **Con Jenkins CI**: Si clona una instancia de Jenkins CI desplegada por el operador, debe restaurar manualmente los datos persistentes. Esta es una limitación del modelo de puesta en marcha de la aplicación.
- **Con bloques S3**: Los bloques S3 de Astra Control Center no informan de 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.
- **Con una versión específica de PostgreSQL**: Los clones de aplicaciones dentro del mismo clúster fallan constantemente con el gráfico BitNami PostgreSQL 11.5.0. Para clonar correctamente, utilice una versión anterior o posterior del gráfico.

Consideraciones sobre OpenShift

- **Clusters y OpenShift versiones**: 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.
- **Proyectos y UID**: Cuando se crea 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. Especifique los detalles del clon:
   - Introduzca un nombre.
   - Elija un clúster de destino para el clon.
   - Introduzca los espacios de nombres de destino para el clon. Cada espacio de nombres de origen asociado a la aplicación se asigna al espacio de nombres de destino que defina.

Astra Control crea nuevos espacios de nombres de destino como parte de la operación de clonación. Los espacios de nombres de destino que especifique no deben estar ya presentes en el clúster de destino.

- Seleccione **Siguiente**.
- Elija mantener la clase de almacenamiento original asociada a la aplicación o seleccionar una clase de almacenamiento diferente.

Puedes migrar una clase de almacenamiento de una aplicación a una clase de almacenamiento de proveedor de nube nativo u otro tipo de almacenamiento compatible, y migrar una aplicación desde una clase de almacenamiento respaldada por `ontap-nas-economy` a una clase de almacenamiento respaldada por `ontap-nas` en el mismo clúster o copie la aplicación en otro clúster con una clase de almacenamiento respaldada por `ontap-nas-economy` controlador.

Si selecciona otra clase de almacenamiento y esta clase de almacenamiento no existe en el momento de la restauración, se devolverá un error.

5. Seleccione **Siguiente**.
6. Revise la información sobre el clon y seleccione **Clonar**.

Resultado

Astra Control clona la aplicación en función de la información proporcionada. La operación de clonado se realiza correctamente cuando se encuentra el nuevo clon de la aplicación `Healthy` en la página **aplicaciones**.

Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Después de una operación de protección de datos (clonado, backup o restauración) y un posterior cambio de tamaño 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 dispone de una aplicación de base de datos, puede utilizar un enlace de ejecución para pausar todas las transacciones de la base de datos antes de realizar una instantánea y reanudar las transacciones una vez completada la instantánea. De este modo se garantiza la creación de instantáneas coherentes con la aplicación.

Tipos de enlaces de ejecución

Astra Control Center admite los siguientes tipos de ganchos de ejecución, basados en el momento en el que

se pueden ejecutar:

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

Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución a una aplicación, puede agregar filtros a un enlace de ejecución para gestionar los contenedores que coincidirá el enlace. Los filtros son útiles para aplicaciones que usan la misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito diferente (como Elasticsearch). Los filtros le permiten crear escenarios donde los enlaces de ejecución se ejecutan en algunos, pero no necesariamente todos los contenedores idénticos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agregue a un enlace de ejecución utiliza una expresión regular para hacer coincidir los contenedores del clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor. Las expresiones regulares para los filtros utilizan la sintaxis expresión regular 2 (RE2), que no admite la creación de un filtro que excluye contenedores de la lista de coincidencias. Para obtener información sobre la sintaxis que admite Astra Control para las expresiones regulares en los filtros de enlace de ejecución, consulte "Soporte de sintaxis de expresión regular 2 (RE2)".

> Si se agrega un filtro de espacio de nombres a un enlace de ejecución que se ejecuta después de una operación de restauración o clonado y el origen y destino de la restauración o clonado se encuentran en diferentes espacios de nombres, el filtro de espacio de nombres solo se aplica al espacio de nombres de destino.

Notas importantes sobre los enlaces de ejecución personalizados

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

> Debido a 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 la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

- La función de enlaces de ejecución está deshabilitada de forma predeterminada para las nuevas implementaciones de Astra Control.
  - Debe activar la función de enlaces de ejecución antes de poder utilizar los enlaces de ejecución.
  - Los usuarios propietario o administrador pueden habilitar o deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en la cuenta de Astra Control actual. Consulte Active la función de enlaces de ejecución y.. Desactive la función de enlaces de ejecución si desea obtener

instrucciones.

    - El estado de habilitación de la función se preserva durante las actualizaciones de Astra Control.

- 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).
- Si Astra Control Center conmuta por error una aplicación de origen replicada a la aplicación de destino, todos los ganchos de ejecución posteriores a la conmutación al nodo de respaldo que estén habilitados para la aplicación de origen se ejecutan para la aplicación de destino una vez completada la conmutación por error.

> Si has ejecutado ganchos posteriores a la restauración con Astra Control Center 23,04 y actualizado tu Astra Control Center a la versión 23,07 o posterior, los ganchos de ejecución posteriores a la restauración ya no se ejecutarán tras una replicación de conmutación al respaldo. Necesitas crear nuevos ganchos de ejecución posteriores a la conmutación por error para tus aplicaciones. También puede cambiar el tipo de operación de los ganchos posteriores a la restauración existentes destinados a recuperaciones tras fallos de «post-restore» a «post-failover».

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 todos los diferentes tipos de ganchos se vería 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	Se ejecutan los ganchos de failover
1	Clonar	N	N	Nuevo	Igual	Y	N	Y	N
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y	N
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y	N
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y	N
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	N	Y	N
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y	N
7	Restaurar	Y	N	Existente	Igual	N	N	Y	N
8	Restaurar	N	Y	Existente	Igual	N	N	Y	N
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.	N
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.	N
11	Backup	Y	N.A.	N.A.	N.A.	N	N	N.A.	N
12	Conmutación al respaldo	Y	N.A.	Creado por replicación	Diferente	N	N	N	Y
13	Conmutación al respaldo	Y	N.A.	Creado por replicación	Igual	N	N	N	Y

Ejemplos de gancho de ejecución

Visite la "Proyecto Verda GitHub de NetApp" Para descargar enlaces de ejecución real para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios enlaces de ejecución personalizados.

Active la función de enlaces de ejecución

Si es un usuario propietario o administrador, puede activar la función de enlaces de ejecución. Cuando habilita la función, todos los usuarios definidos en esta cuenta de Astra Control pueden usar ganchos de ejecución y ver los ganchos de ejecución y los scripts de enlace existentes.

Pasos

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

3. Seleccione **Enable execution hooks**.

   Aparece la pestaña **Cuenta** > **Ajustes de función**.

4. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
5. Selecciona **Activar**.
6. Observe la advertencia de seguridad que aparece.
7. Seleccione **Sí, habilite los ganchos de ejecución**.

Desactive la función de enlaces de ejecución

Si eres un usuario propietario o administrador, puedes deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en esta cuenta de Astra Control. Debe suprimir todos los enlaces de ejecución existentes antes de desactivar la función de enlaces de ejecución. Consulte Eliminar un gancho de ejecución para obtener instrucciones sobre cómo eliminar un enlace de ejecución existente.

Pasos

1. Vaya a **Cuenta** y luego seleccione la pestaña **Ajustes de función**.
2. Seleccione la ficha **ganchos de ejecución**.
3. En el panel * Ganchos de ejecución *, seleccione el menú de configuración.
4. Seleccione **Desactivar**.
5. Observe la advertencia que aparece.
6. Tipo `disable` para confirmar que desea deshabilitar la función para todos los usuarios.
7. Seleccione **Sí, desactivar**.

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 de un gancho, cuántos contenedores coinciden, la hora de creación y cuándo se ejecuta (antes o después de la operación). Puede seleccionar la + icono junto al nombre del gancho para expandir la lista de contenedores en los que se ejecutará. Para ver los registros de eventos que rodean los enlaces de ejecución de esta aplicación, vaya a la ficha **actividad**.

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

Cada enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Puede agregar una o más secuencias de comandos a las que puedan hacer referencia los enlaces de ejecución. Muchos ganchos de ejecución pueden hacer referencia al mismo script; esto le permite actualizar muchos ganchos de ejecución cambiando solo un script.

Pasos

1. Asegúrese de que la función de enlaces de ejecución es activado.
2. Vaya a **cuenta**.
3. Seleccione la ficha **Scripts**.
4. Seleccione **Agregar**.
5. 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.
6. 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

Puedes crear un gancho de ejecución personalizado para una aplicación y añadirlo a Astra Control. 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. Asegúrese de que la función de enlaces de ejecución es activado.
2. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
3. Seleccione la ficha **ganchos de ejecución**.
4. Seleccione **Agregar**.
5. En el área **Detalles del gancho**:
   a. Determine cuándo debe funcionar el gancho seleccionando un tipo de operación en el menú desplegable **operación**.
   b. Introduzca un nombre único para el gancho.
   c. (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.
6. (Opcional) en el área **Detalles de filtro de gancho**, puede añadir filtros para controlar en qué contenedores se ejecuta el gancho de ejecución:
   a. Seleccione **Agregar filtro**.
   b. En la columna **Tipo de filtro Hook**, elija un atributo en el que filtrar en el menú desplegable.
   c. En la columna **Regex**, introduzca una expresión regular que se utilizará como filtro. Astra Control utiliza "Sintaxis de regex de expresión regular 2 (RE2)".

      Si filtra el nombre exacto de un atributo (como un nombre de pod) sin ningún otro texto en el campo de expresión regular, se realiza una coincidencia de subcadena. Para que coincida con un nombre exacto y sólo con ese nombre, utilice la sintaxis de coincidencia de cadena exacta (por ejemplo, `^exact_podname$`).

   d. Para añadir más filtros, seleccione **Agregar filtro**.

      Se combinan varios filtros para un enlace de ejecución con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

7. Cuando termine, seleccione **Siguiente**.
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 **Siguiente**.
10. Revise la configuración del gancho de ejecución.
11. Seleccione **Agregar**.

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.

Edite un gancho de ejecución

Puede editar un enlace de ejecución si desea cambiar sus atributos, filtros o la secuencia de comandos que utiliza. Necesita tener permisos de propietario, administrador o miembro para editar 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 un gancho que desee editar.
4. Seleccione **Editar**.
5. Haga los cambios necesarios, seleccione **Siguiente** después de completar cada sección.
6. Seleccione **Guardar**.

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**.

5. En el cuadro de diálogo que aparece, escriba "delete" para confirmar.
6. Seleccione **Sí, elimine el enlace de ejecución**.

Si quiere más información

- "Proyecto Verda GitHub de NetApp"

Protege Astra Control Center con Astra Control Center

A fin de garantizar mejor la resiliencia frente a errores graves en el clúster de Kubernetes donde se ejecuta Astra Control Center, protege la aplicación de Astra Control Center en sí misma. Puedes realizar backups y restauraciones de Astra Control Center con una instancia secundaria del Astra Control Center o utilizar la replicación de Astra si el almacenamiento subyacente utiliza ONTAP.

En estos casos, se pone en marcha y se configura una segunda instancia de Astra Control Center en un dominio de fallos diferente y se ejecuta en un segundo clúster de Kubernetes distinto al de la instancia principal del Astra Control Center. La segunda instancia de Astra Control se usa para crear backups y restaurar potencialmente la instancia principal de Astra Control Center. Una instancia del Astra Control Center, restaurada o replicada, seguirá proporcionando la gestión de los datos de aplicaciones para las aplicaciones del cluster de aplicaciones y restaurará la accesibilidad a los backups y copias Snapshot de esas aplicaciones.

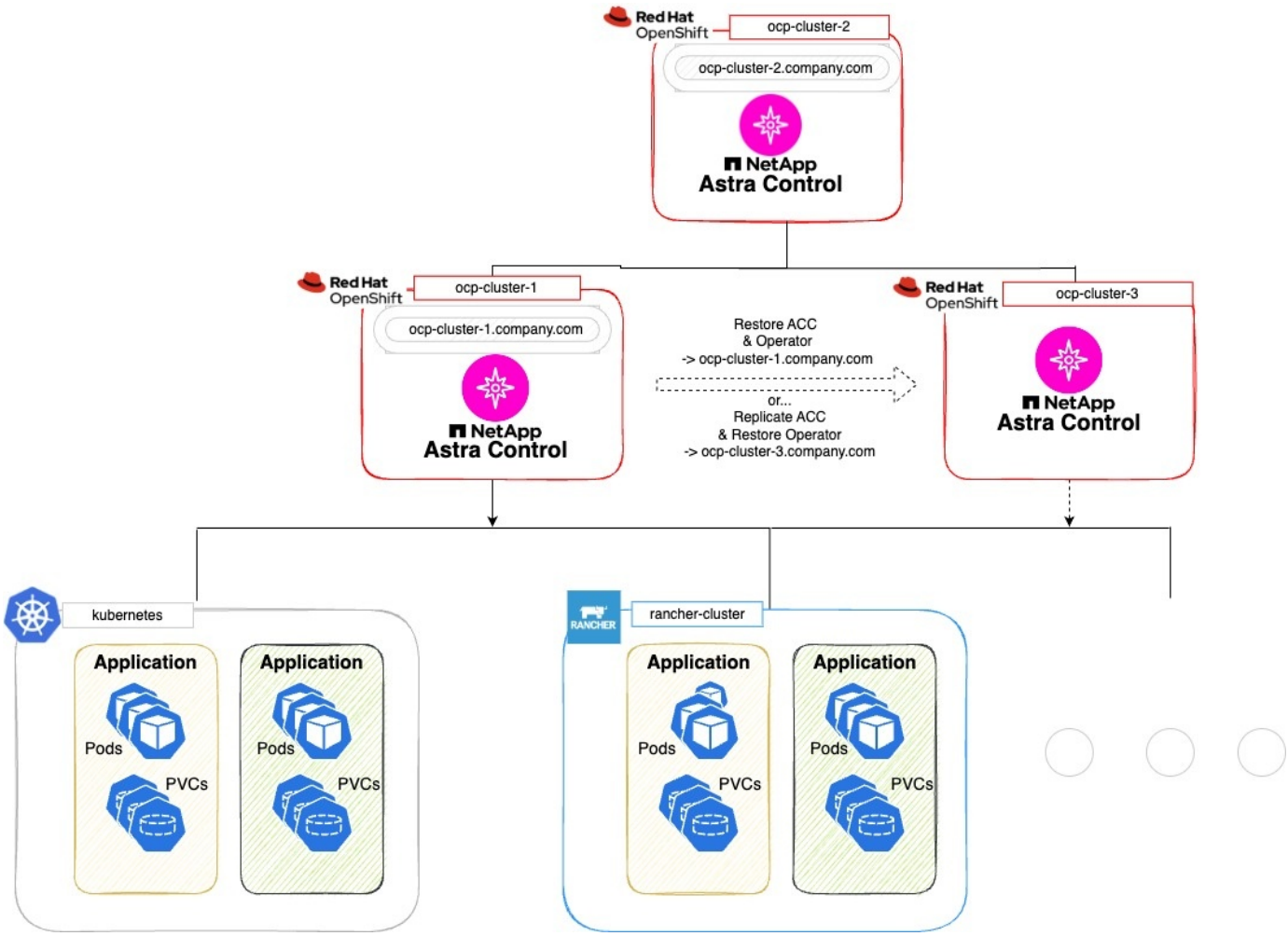
Antes de empezar

Asegúrate de tener lo siguiente antes de configurar las situaciones de protección para Astra Control Center:

- **Un clúster de Kubernetes que ejecuta la instancia principal de Astra Control Center**: Este clúster aloja la instancia principal de Astra Control Center que gestiona los clústeres de aplicaciones.
- **Un segundo clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que ejecuta la instancia secundaria de Astra Control Center**: Este clúster aloja la instancia de Astra Control Center que gestiona la instancia principal de Astra Control Center.
- **Un tercer clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal**: Este clúster alojará la instancia restaurada o replicada de Astra Control Center. Debe tener disponible el mismo espacio de nombres de Astra Control Center que actualmente se pone en marcha en el volumen principal. Por ejemplo, si Astra Control Center se pone en marcha en un espacio de nombres `netapp-acc` en el clúster de origen, el espacio de nombres `netapp-acc` Debe estar disponible y no lo deben usar ninguna aplicación del clúster de Kubernetes de destino.
- **Cubetas compatibles con S3**: Cada instancia de Astra Control Center tiene un cubo de almacenamiento de objetos accesible compatible con S3.
- **Un equilibrador de carga configurado**: El equilibrador de carga proporciona una dirección IP para Astra y debe tener conectividad de red con los clústeres de aplicaciones y los dos buckets S3.
- **Los clústeres cumplen con los requisitos del Centro de control de Astra**: Cada clúster utilizado en la protección del Centro de control de Astra cumple "requisitos generales de Astra Control Center".

Acerca de esta tarea

Estos procedimientos describen los pasos necesarios para restaurar Astra Control Center en un clúster nuevo mediante uno de ellos backup y restauración o. replicación. Los pasos se basan en la configuración de ejemplo que se describe a continuación:



En esta configuración de ejemplo, se muestra lo siguiente:

- **Un clúster de Kubernetes que ejecuta la instancia principal de Astra Control Center**:
  - Clúster de OpenShift: `ocp-cluster-1`
  - Instancia primaria de Astra Control Center: `ocp-cluster-1.company.com`
  - Este cluster gestiona los clusters de aplicaciones.
- **El segundo clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que ejecuta la instancia secundaria de Astra Control Center**:
  - Clúster de OpenShift: `ocp-cluster-2`
  - Instancia secundaria de Astra Control Center: `ocp-cluster-2.company.com`
  - Este clúster se utilizará para crear una copia de seguridad de la instancia principal de Astra Control Center o configurar la replicación en un clúster diferente (en este ejemplo, la `ocp-cluster-3` clúster).
- **Un tercer clúster de Kubernetes del mismo tipo de distribución de Kubernetes que el principal que se utilizará para las operaciones de restauración**:
  - Clúster de OpenShift: `ocp-cluster-3`
  - Tercera instancia de Astra Control Center: `ocp-cluster-3.company.com`
  - Este clúster se utilizará para la restauración o replicación de conmutación al nodo de respaldo de Astra

Control Center.

> Lo ideal sería que el clúster de aplicaciones se situara fuera de los tres clústeres de Astra Control Center, tal y como muestran los clústeres de kubernetes y rancher en la imagen anterior.

No se muestra en el diagrama:

- Todos los clústeres tienen back-ends de ONTAP con Trident instalado.
- En esta configuración, los clusters de OpenShift utilizan MetalLB como equilibrador de carga.
- La controladora Snapshot y VolumeSnapshotClass también se instalan en todos los clústeres, como se describe en la "requisitos previos".

Paso 1 Opción: Realizar copias de seguridad y restaurar Astra Control Center

Este procedimiento describe los pasos necesarios para restaurar Astra Control Center en un nuevo clúster mediante el backup y la restauración.

En este ejemplo, Astra Control Center siempre se instala en la `netapp-acc` el espacio de nombres y el operador se instalan en la `netapp-acc-operator` espacio de nombres.

> Aunque no se describe, el operador de Astra Control Center también puede ponerse en marcha en el mismo espacio de nombres que Astra CR.

Antes de empezar

- Ha instalado el Astra Control Center principal en un clúster.
- Ha instalado el Astra Control Center secundario en un clúster diferente.

Pasos

1. Gestiona la aplicación principal del Centro de control de Astra y el clúster de destino desde la instancia del Centro de control de Astra secundaria (ejecutándose en `ocp-cluster-2` clúster):
   a. Inicia sesión en la instancia secundaria de Astra Control Center.
   b. "Añada el clúster de Astra Control Center principal" (`ocp-cluster-1`).
   c. "Añada el tercer clúster de destino" (`ocp-cluster-3`) que se utilizará para la restauración.
2. Gestiona Astra Control Center y el operador del Astra Control Center en el Astra Control Center secundario:
   a. En la página aplicaciones, seleccione **definir**.
   b. En la ventana **Definir aplicación**, introduzca el nombre de la nueva aplicación (`netapp-acc`).
   c. Elige el clúster que ejecuta el Astra Control Center principal (`ocp-cluster-1`) De la lista desplegable **Cluster**.
   d. Elija la `netapp-acc` Espacio de nombres para Astra Control Center en la lista desplegable **Namespace**.
   e. En la página Recursos de Cluster, seleccione **Incluir recursos adicionales de ámbito de cluster**.
   f. Seleccione **Agregar regla de inclusión**.
   g. Seleccione estas entradas y seleccione **Agregar**:

- Selector de etiquetas: <label name>
- Grupo: Apiextensions.k8s.io
- Versión: V1
- Clase: CustomResourceDefinition

h. Confirme la información de la aplicación.

i. Seleccione **definir**.

Después de seleccionar **Definir**, repita el proceso Definir solicitud para el operador `netapp-acc-operator`) y seleccione `netapp-acc-operator` Espacio de nombres en el Asistente de Definición de Aplicación.

3. Crea backups de Astra Control Center y el operador:
   a. En el Astra Control Center secundario, accede a la página Applications seleccionando la pestaña Applications.
   b. "Realice un backup" La aplicación Astra Control Center (`netapp-acc`).
   c. "Realice un backup" el operador (`netapp-acc-operator`).
4. Después de haber realizado el backup de Astra Control Center y el operador, simular un escenario de recuperación ante desastres mediante "Desinstalación de Astra Control Center" del clúster principal.

> Restaurarás Astra Control Center en un nuevo clúster (el tercer clúster de Kubernetes descrito en este procedimiento) y usarás el mismo DNS que el clúster principal para el Astra Control Center recién instalado.

5. Mediante el centro secundario de Astra Control Center, "restaurar" La instancia principal de la aplicación Astra Control Center desde su backup:
   a. Selecciona **Aplicaciones** y luego selecciona el nombre de la aplicación Astra Control Center.
   b. En el menú Opciones de la columna Acciones, seleccione **Restaurar**.
   c. Elija el **Restaurar a nuevos espacios de nombres** como el tipo de restauración.
   d. Introduzca el nombre de la restauración (`netapp-acc`).
   e. Elija el tercer clúster de destino (`ocp-cluster-3`).
   f. Actualice el espacio de nombres de destino para que sea el mismo espacio de nombres que el original.
   g. En la página Restore Source, seleccione la copia de seguridad de la aplicación que se utilizará como origen de la restauración.
   h. Seleccione **Restaurar usando clases de almacenamiento originales**.
   i. Seleccione **Restaurar todos los recursos**.
   j. Revise la información de restauración y, a continuación, seleccione **Restaurar** para iniciar el proceso de restauración que restaura Astra Control Center al clúster de destino (`ocp-cluster-3`). La restauración se completa cuando la aplicación entra `available` estado.
6. Configure Astra Control Center en el clúster de destino:
   a. Abra un terminal y conéctese usando kubeconfig al clúster de destino (`ocp-cluster-3`) Que contiene el Astra Control Center restaurado.

b. Confirme que el `ADDRESS` La columna de la configuración de Astra Control Center hace referencia al nombre DNS del sistema principal:

```
kubectl get acc -n netapp-acc
```

Respuesta:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. Si la `ADDRESS` En la respuesta anterior no tiene el FQDN de la instancia principal de Astra Control Center, actualice la configuración para hacer referencia a los DNS de Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

i. Cambie el `astraAddress` inferior `spec:` Al FQDN (`ocp-cluster-1.company.com` En este ejemplo) de la instancia principal de Astra Control Center.

ii. Guarde la configuración.

iii. Confirme que la dirección se ha actualizado:

```
kubectl get acc -n netapp-acc
```

b. Vaya a la Restaure el operador del centro de control de Astra sección de este documento para completar el proceso de restauración.

Paso 1 Opción: Protección del centro de control Astra con replicación

Este procedimiento describe los pasos necesarios para configurar "Replicación de Astra Control Center" Para proteger la instancia principal de Astra Control Center.

En este ejemplo, Astra Control Center siempre se instala en la `netapp-acc` el espacio de nombres y el operador se instalan en la `netapp-acc-operator` espacio de nombres.

Antes de empezar

- Ha instalado el Astra Control Center principal en un clúster.
- Ha instalado el Astra Control Center secundario en un clúster diferente.

Pasos

1. Gestione la aplicación principal del Centro de Astra Control y el clúster de destino desde la instancia de Astra Control Center secundaria:
   a. Inicia sesión en la instancia secundaria de Astra Control Center.

b. "Añada el clúster de Astra Control Center principal" (`ocp-cluster-1`).

c. "Añada el tercer clúster de destino" (`ocp-cluster-3`) que se utilizará para la replicación.

2. Gestiona Astra Control Center y el operador del Astra Control Center en el Astra Control Center secundario:

a. Selecciona **Clusters** y selecciona el clúster que contiene el Astra Control Center principal (`ocp-cluster-1`).

b. Seleccione la ficha **Namespaces**.

c. Seleccione `netapp-acc` y.. `netapp-acc-operator` espacios de nombres.

d. Seleccione el menú Acciones y seleccione **Definir como aplicaciones**.

e. Seleccione **Ver en aplicaciones** para ver las aplicaciones definidas.

3. Configurar Backends para Replicación:

> La replicación requiere que el clúster principal de Astra Control Center y el clúster de destino (`ocp-cluster-3`) Utilice back-ends de almacenamiento ONTAP con diferentes pares.
> Después de que cada backend se encuentre y se agregue a Astra Control, el backend aparecerá en la pestaña **Descubierto** de la página Backends.

a. "Agregue un backend con pares" A Astra Control Center en el clúster principal.

b. "Agregue un backend con pares" A Astra Control Center en el clúster de destino.

4. Configurar replicación:

a. En la pantalla Aplicaciones, seleccione `netapp-acc` cliente más.

b. Seleccione **Configurar política de replicación**.

c. Seleccione `ocp-cluster-3` como el clúster de destino.

d. Seleccione la clase de almacenamiento.

e. Introduzca `netapp-acc` como espacio de nombres de destino.

f. Cambie la frecuencia de replicación si lo desea.

g. Seleccione **Siguiente**.

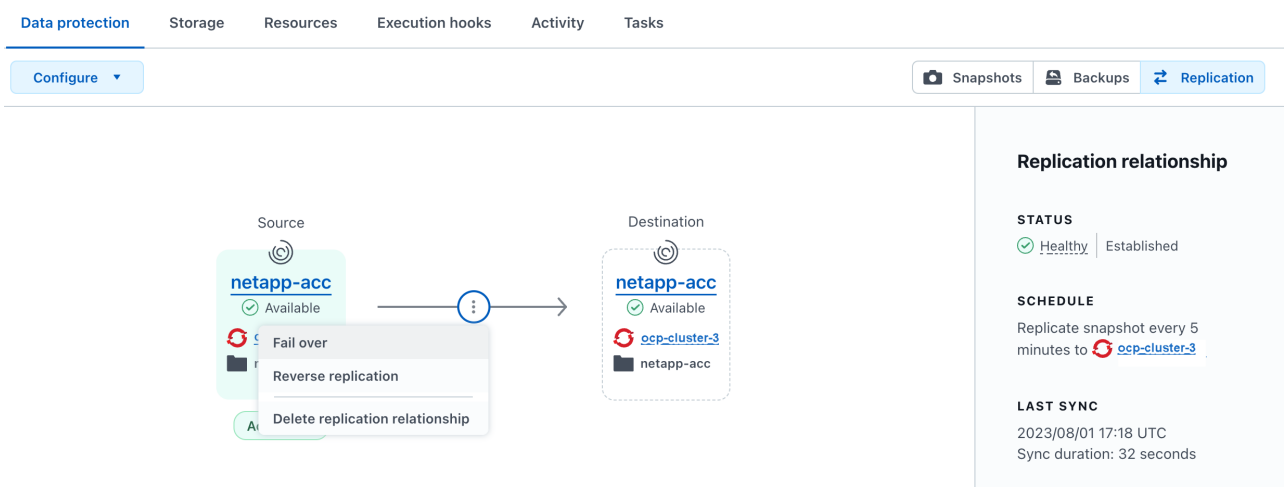
h. Confirme que la configuración es correcta y seleccione **Guardar**.

La relación de replicación de `Establishing` para `Established`. Cuando está activa, esta replicación se producirá cada cinco minutos hasta que se elimine la configuración de replicación.

5. Realice una conmutación al nodo de respaldo de la replicación en el otro clúster si el sistema principal está dañado o ya no se puede acceder a él:

> Asegúrate de que el clúster de destino no tenga Astra Control Center instalado para garantizar una conmutación al nodo de respaldo correcta.

a. Seleccione el icono de elipses verticales y seleccione **fail over**.



b. Confirme los detalles y seleccione **fail over** para comenzar el proceso de failover.

   El estado de la relación de replicación cambia a. `Failing over` y después `Failed over` cuando finalice.

6. Complete la configuración de failover:

   a. Abra un terminal y conéctelo usando el kubeconfig del tercer grupo (`ocp-cluster-3`). Este clúster ahora tiene Astra Control Center instalado.

   b. Determinar el nombre de dominio completo de Astra Control Center en el tercer clúster (`ocp-cluster-3`).

   c. Actualiza la configuración para hacer referencia a los DNS de Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

      i. Cambie el `astraAddress` inferior `spec:` Con el FQDN (`ocp-cluster-3.company.com`) del tercer cluster de destino.

      ii. Guarde la configuración.

      iii. Confirme que la dirección se ha actualizado:

```
kubectl get acc -n netapp-acc
```

   d. Confirme que todos los CRD de traefik necesarios están presentes:

```
kubectl get crds | grep traefik
```

   CRD DE traefik requeridos:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Si faltan algunos de los CRD anteriores:
   i. Vaya a. "documentación de traefik".
   ii. Copie el área Definiciones en un archivo.
   iii. Aplicar cambios:

```
kubectl apply -f <file name>
```

   iv. Reiniciar traefik:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Vaya a la Restaure el operador del centro de control de Astra sección de este documento para completar el proceso de restauración.

Paso 2: Restaure el operador del centro de control de Astra

Mediante el Astra Control Center secundario, restaure el operador principal del Astra Control Center desde el backup. El espacio de nombres de destino debe ser el mismo que el de origen. En caso de que Astra Control Center se eliminara del clúster de origen principal, seguirán existiendo backups para realizar los mismos pasos de restauración.

Pasos

1. Selecciona **Aplicaciones** y luego selecciona el nombre de la app del operador (`netapp-acc-operator`).

2. En el menú Opciones de la columna Acciones, seleccione **Restaurar**
3. Elija el **Restaurar a nuevos espacios de nombres** como el tipo de restauración.
4. Elija el tercer clúster de destino (`ocp-cluster-3`).
5. Cambie el espacio de nombres para que sea el mismo que el asociado al clúster de origen principal (`netapp-acc-operator`).
6. Seleccione la copia de seguridad realizada anteriormente como origen de restauración.
7. Seleccione **Restaurar usando clases de almacenamiento originales**.
8. Seleccione **Restaurar todos los recursos**.
9. Revise los detalles y haga clic en **Restaurar** para iniciar el proceso de restauración.

   La página Aplicaciones muestra el operador del Centro de control de Astra que se está restaurando en el tercer clúster de destino (`ocp-cluster-3`). Cuando el proceso se completa, el estado se muestra como `Available`. En un plazo de diez minutos, la dirección DNS debería resolverse en la página.

Resultado

Astra Control Center, sus clústeres registrados y las aplicaciones gestionadas con sus copias Snapshot y backups ahora están disponibles en el tercer clúster de destino (`ocp-cluster-3`). Cualquier política de protección que tuviera en el original también está ahí en la nueva instancia. Puede seguir realizando copias Snapshot y backups programadas o bajo demanda.

Resolución de problemas

Determine el estado del sistema y si los procesos de protección se han realizado correctamente.

- **Los pods no están funcionando**: Confirma que todos los pods están activos y en funcionamiento:

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

  Si hay algunos pods en la `CrashLookBackOff` estado, reinícielos y deben realizar la transición a. `Running` estado.

- **Confirmar el estado del sistema**: Confirma que el sistema Astra Control Center está en `ready` provincia:

  ```
  kubectl get acc -n netapp-acc
  ```

  Respuesta:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- **Confirmar el estado de implementación**: Muestra la información de implementación de Astra Control Center para confirmarlo `Deployment State` es `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **La interfaz de usuario restaurada de Astra Control Center devuelve un error 404**: Si esto sucede cuando lo has seleccionado `AccTraefik` como opción de entrada, marque la CRD de traefik para asegurarse de que todos están instalados.

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 del clúster y gestione las clases de almacenamiento

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. También es posible cambiar la clase de almacenamiento predeterminada para los clústeres gestionados.

Ver el estado y los detalles del clúster

Puede ver detalles sobre el clúster, como la 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.

Cambie la clase de almacenamiento predeterminada

Es posible cambiar la clase de almacenamiento predeterminada para un clúster de. Cuando Astra Control gestiona un clúster, realiza un seguimiento de la clase de almacenamiento predeterminada del clúster.

> No cambie la clase de almacenamiento con comandos kubectl. Utilice este procedimiento en su lugar. Astra Control revertirá los cambios si se realizan con kubectl.

Pasos

1. En la interfaz de usuario web de Astra Control Center, seleccione **Clusters**.
2. En la página **Clusters**, seleccione el clúster que desea cambiar.
3. Seleccione la ficha **almacenamiento**.
4. Seleccione la categoría **clases de almacenamiento**.

5. Seleccione el menú **acciones** para la clase de almacenamiento que desea establecer como predeterminada.
6. Seleccione **establecer como predeterminado**.

Ver el estado y los detalles de una aplicación

Después de empezar a gestionar una aplicación, Astra Control proporciona detalles sobre la aplicación que te permiten identificar el estado de comunicación (si Astra Control puede comunicarse con la aplicación), su estado de protección (si está totalmente protegido 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. Revise la información.

   Estado de la aplicación

   Proporciona un estado que refleja si Astra Control puede comunicarse con la aplicación.

   - **App Protection Status**: Proporciona un 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 que están asociados con la aplicación.
   - **Protección de datos**: Permite configurar una directiva de protección de datos y ver las instantáneas y copias de seguridad existentes.
   - **Almacenamiento**: 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 haciendo copias de seguridad y gestionando.
   - **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

Gestione usuarios locales y roles

Puede añadir, eliminar y editar 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. "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 Control. En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP. En la siguiente documentación, se ofrece más información:

- "Utilice la API Astra Control para gestionar la autenticación y los usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar grupos y usuarios remotos"
- "Utilice la interfaz de usuario de Astra Control para gestionar la autenticación remota"

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 "Gestione usuarios locales y 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**.

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. "API de control Astra" para administrar roles.

Agregar una restricción de espacio de nombres a una función

Un usuario Administrador o propietario puede agregar restricciones de espacio de nombres a las funciones de miembro o de visor.

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"

Administrar la autenticación remota

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 Control.

En un nivel elevado, la configuración implica integrar Astra con LDAP y definir los usuarios y grupos de Astra Control correspondientes a las definiciones LDAP. Puede utilizar la API Astra Control o la interfaz de usuario web para configurar la autenticación LDAP y los usuarios y grupos LDAP.

> Astra Control Center usa el atributo de inicio de sesión de usuario, configurado cuando la autenticación remota está habilitada, para buscar usuarios remotos y hacer un seguimiento de ellos. En este campo debe existir un atributo de una dirección de correo electrónico («correo») o nombre principal de usuario («userPrincipalName») para cualquier usuario remoto que desee aparecer en Astra Control Center. Este atributo se utiliza como nombre de usuario en Astra Control Center para la autenticación y en búsquedas de usuarios remotos.

Añada un certificado para la autenticación LDAPS

Agregue el certificado TLS privado del servidor LDAP para que Astra Control Center pueda autenticarse con el servidor LDAP cuando utilice una conexión LDAPS. Sólo tiene que hacerlo una vez o cuando caduque el certificado que ha instalado.

Pasos

1. Vaya a **cuenta**.
2. Seleccione la ficha **certificados**.
3. Seleccione **Agregar**.
4. Cargue el `.pem` archiva o pega el contenido del archivo desde el portapapeles.
5. Seleccione la casilla de verificación **Trusted**.
6. Seleccione **Agregar certificado**.

Habilite la autenticación remota

Puede habilitar la autenticación LDAP y configurar la conexión entre Astra Control y el servidor LDAP remoto.

Antes de empezar

Si planea utilizar LDAPS, asegúrese de que el certificado TLS privado del servidor LDAP está instalado en Astra Control Center para que Astra Control Center pueda autenticarse con el servidor LDAP. Consulte Añada un certificado para la autenticación LDAPS si desea obtener instrucciones.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **conectar**.
4. Introduzca la dirección IP del servidor, el puerto y el protocolo de conexión preferido (LDAP o LDAPS).

   Como práctica recomendada, use LDAPS al conectarse con el servidor LDAP. Debe instalar el certificado TLS privado del servidor LDAP en Astra Control Center antes de conectarse con LDAPS.

5. Introduzca las credenciales de la cuenta de servicio en formato de correo electrónico (administrator@example.com). Astra Control utilizará estas credenciales al conectar con el servidor LDAP.
6. En la sección **Coincidencia de usuario**, haz lo siguiente:
   a. Introduzca el DN base y un filtro de búsqueda de usuario adecuado que se utilizará al recuperar la información de usuario del servidor LDAP.
   b. (Opcional) Si el directorio utiliza el atributo de inicio de sesión del usuario `userPrincipalName` en lugar de `mail`, entre `userPrincipalName` En el atributo correcto en el campo **Atributo de inicio de sesión de usuario**.
7. En la sección **coincidencia de grupo**, introduzca el DN base de búsqueda de grupo y un filtro de búsqueda de grupo personalizado adecuado.

   Asegúrese de utilizar el nombre completo (DN) de base correcto y un filtro de búsqueda apropiado para **coincidencia de usuario** y **coincidencia de grupo**. El DN base indica a Astra Control en qué nivel del árbol de directorios iniciar la búsqueda, y el filtro de búsqueda limita las partes del árbol de directorios de las búsquedas de Astra Control.

8. Seleccione **Enviar**.

Resultado

El estado del panel **autenticación remota** pasa a **pendiente** y a **conectado** cuando se establece la conexión con el servidor LDAP.

Desactivar la autenticación remota

Puede deshabilitar temporalmente una conexión activa con el servidor LDAP.

Cuando se deshabilita una conexión a un servidor LDAP, se guardan todas las opciones y se conservan todos los usuarios y grupos remotos que se agregaron a Astra Control desde ese servidor LDAP. Puede volver a conectarse a este servidor LDAP en cualquier momento.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Desactivar**.

Resultado

El estado del panel **autenticación remota** pasa a **Desactivada**. Se conservan todos los ajustes de autenticación remota, usuarios remotos y grupos remotos, y se puede volver a habilitar la conexión en cualquier momento.

Edite la configuración de autenticación remota

Si ha desactivado la conexión al servidor LDAP o el panel **autenticación remota** se encuentra en el estado "error de conexión", puede editar los valores de configuración.

> No puede editar la dirección IP o la dirección URL del servidor LDAP cuando el panel **autenticación remota** está en estado "Desactivada". Necesita hacerlo Desconecte la autenticación remota primero.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **Editar**.
4. Realice los cambios necesarios y seleccione **Editar**.

Desconecte la autenticación remota

Puede desconectarse de un servidor LDAP y eliminar los ajustes de configuración de Astra Control.

> Si es un usuario LDAP y se desconecta, la sesión finalizará inmediatamente Cuando se desconecta del servidor LDAP, todas las opciones de configuración de ese servidor LDAP se eliminan de Astra Control, así como todos los usuarios y grupos remotos que se hayan agregado de ese servidor LDAP.

Pasos

1. Vaya a **cuenta > conexiones**.
2. En el panel **autenticación remota**, seleccione el menú de configuración.
3. Seleccione **desconectar**.

Resultado

El estado del panel **autenticación remota** pasa a **desconectado**. La configuración de autenticación remota, los usuarios remotos y los grupos remotos se eliminan de Astra Control.

Administrar grupos y usuarios remotos

Si ha activado la autenticación LDAP en el sistema Astra Control, puede buscar usuarios y grupos LDAP e incluirlos en los usuarios aprobados del sistema.

Agregar un usuario remoto

Los propietarios y administradores de cuentas pueden agregar usuarios remotos a Astra Control. Astra Control Center admite hasta 10.000 usuarios remotos de LDAP.

> Astra Control Center usa el atributo de inicio de sesión de usuario, configurado cuando la autenticación remota está habilitada, para buscar usuarios remotos y hacer un seguimiento de ellos. En este campo debe existir un atributo de una dirección de correo electrónico («correo») o nombre principal de usuario («userPrincipalName») para cualquier usuario remoto que desee aparecer en Astra Control Center. Este atributo se utiliza como nombre de usuario en Astra Control Center para la autenticación y en búsquedas de usuarios remotos.

> No puede agregar un usuario remoto si ya existe en el sistema un usuario local con la misma dirección de correo electrónico (basada en el atributo de correo o nombre principal de usuario). Para agregar el usuario como usuario remoto, elimine primero el usuario local del sistema.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **usuarios remotos**.
4. Seleccione **Agregar**.
5. Opcionalmente, busque un usuario LDAP introduciendo la dirección de correo electrónico del usuario en el campo **Filtrar por correo electrónico**.
6. Seleccione uno o varios usuarios de la lista.
7. Asigne un rol al usuario.

   > Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este usuario y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   > Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo usuario aparece en la lista de usuarios remotos. En esta lista, puede ver restricciones activas en el usuario, así como administrar el usuario desde el menú **acciones**.

Agregar un grupo remoto

Para agregar muchos usuarios remotos a la vez, los propietarios de cuentas y los administradores pueden agregar grupos remotos a Astra Control. Cuando se añade un grupo remoto, todos los usuarios remotos de

ese grupo están disponibles para iniciar sesión en Astra Control y heredarán el mismo rol que el grupo.

Astra Control Center admite hasta 5.000 grupos remotos LDAP.

Pasos

1. Vaya al área **cuenta**.
2. Seleccione la ficha **usuarios y grupos**.
3. En el extremo derecho de la página, seleccione **grupos remotos**.
4. Seleccione **Agregar**.

   En esta ventana, puede ver una lista de los nombres comunes y nombres distintivos de los grupos LDAP que Astra Control ha recuperado del directorio.

5. Opcionalmente, busque un grupo LDAP introduciendo el nombre común del grupo en el campo **filtro por nombre común**.
6. Seleccione uno o varios grupos de la lista.
7. Asigne un rol a los grupos.

   El rol que seleccione se asigna a todos los usuarios de este grupo. Si asigna roles diferentes a un usuario y al grupo del usuario, tiene prioridad el rol más permisivo.

8. Opcionalmente, asigne una o más restricciones de espacio de nombres a este grupo y seleccione **restringir rol a restricciones** para aplicarlas. Puede agregar una nueva restricción de espacio de nombres seleccionando **Agregar restricción**.

   Cuando a un usuario se le asignan varias funciones a través de la pertenencia a grupos LDAP, las restricciones de la función más permisiva son las únicas que surtan efecto. Por ejemplo, si un usuario con una función de visor local se une a tres grupos que están enlazados a la función Member, la suma de las restricciones de las funciones Member se aplicará y se ignoran todas las restricciones de la función Viewer.

9. Seleccione **Agregar**.

Resultado

El nuevo grupo aparece en la lista de grupos remotos. Los usuarios remotos de este grupo no aparecen en la lista de usuarios remotos hasta que cada usuario remoto inicia sesión. En esta lista, puede ver detalles sobre el grupo, así como administrar el grupo desde el menú **acciones**.

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 al añadir un clúster nuevo, consulte "Añada un clúster de Kubernetes".

> Si creas tu propio archivo kubeconfig, debes definir solo **one** elemento de contexto en él. Consulte "Documentación de Kubernetes" para obtener información sobre la creación de archivos kubeconfig.

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 Control Center o "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 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 su configuración de aplicaciones y almacenamiento persistente en el mismo clúster.

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

- NetApp ONTAP S3
- 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 bloques Generic S3, es posible que Astra Control Center no admita 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.
- Eliminado: No se puede acceder al depósito 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
- Establecer el bloque predeterminado
- 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 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**.

Establecer el bloque predeterminado

Cuando se realiza un clon entre clústeres, Astra Control requiere un bloque predeterminado. Siga estos pasos para establecer un bloque predeterminado para todos los clústeres.

Pasos

1. Vaya a **instancias de cloud**.
2. Seleccione el menú en la columna **acciones** para la instancia de nube de la lista.
3. Seleccione **Editar**.
4. En la lista **bloque**, seleccione el segmento que desea que sea el predeterminado.
5. Seleccione **Guardar**.

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.
- No puede quitar un depósito de escritura única y lectura múltiple (WORM) antes de que haya caducado el período de retención del proveedor de cloud del depósito. Los depósitos WORM están marcados con «bloqueados» junto al nombre del bloque.

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

Antes de empezar

- 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
- Editar los detalles de autenticación del back-end de almacenamiento
- Gestionar un back-end de almacenamiento detectado
- Desgestione un back-end de almacenamiento
- Quite 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 el panel del back-end de almacenamiento de Dashboard 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

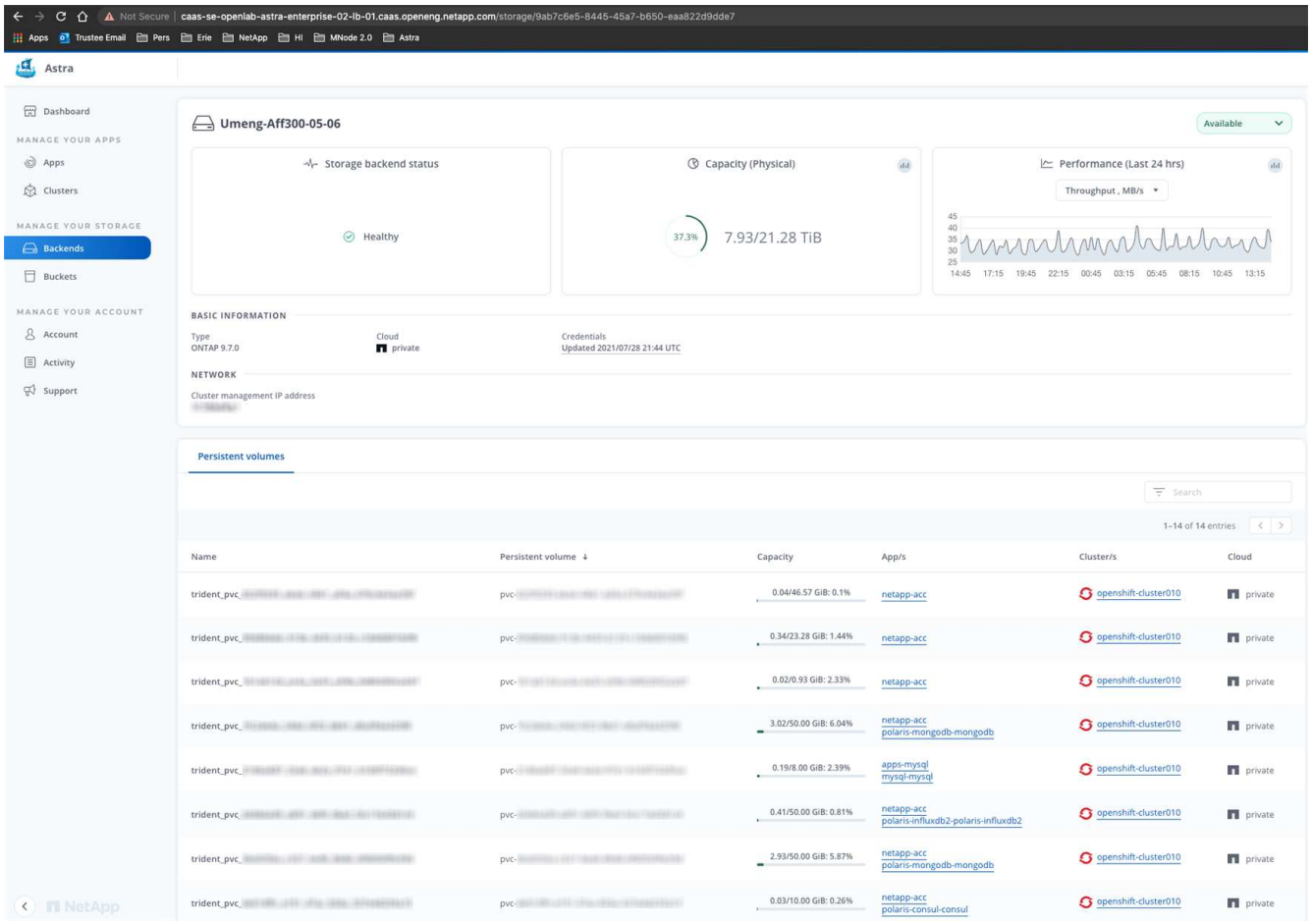
Vea información sobre el estado, la capacidad y el rendimiento del back-end (rendimiento de IOPS y/o latencia).

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.

Editar los detalles de autenticación del back-end de almacenamiento

El Centro de control de Astra ofrece dos modos de autenticación de un back-end de ONTAP.

- **Autenticación basada en credenciales**: El nombre de usuario y la contraseña de un usuario de ONTAP con los permisos requeridos. Debe utilizar un rol de inicio de sesión de seguridad predefinido, como admin, para garantizar la máxima compatibilidad con las versiones de ONTAP.
- **Autenticación basada en certificados**: Astra Control Center también puede comunicarse con un clúster de ONTAP utilizando un certificado instalado en el backend. Debe usar el certificado de cliente, la clave y el certificado de CA de confianza si se utilizan (recomendado).

Puede actualizar los back-ends existentes para pasar de un tipo de autenticación a otro método. Solo se admite un método de autenticación a la vez.

Para obtener más información sobre la activación de la autenticación basada en certificados, consulte "Habilite la autenticación en el back-end de almacenamiento de ONTAP".

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione el back-end de almacenamiento.
3. En el campo Credenciales, seleccione el icono **Editar**.
4. En la página Editar, seleccione una de las siguientes opciones.
   - **Usar credenciales de administrador**: Ingrese la dirección IP de administración del clúster de ONTAP y las credenciales de administración. Las credenciales deben ser credenciales para todo el clúster.

     El usuario cuyas credenciales introduzca aquí debe tener la `ontapi` Método de acceso de inicio de sesión de usuario habilitado en System Manager de ONTAP en el clúster de ONTAP. Si planea utilizar la replicación de SnapMirror, aplique las credenciales de usuario con el rol "admin", que tiene los métodos de acceso `ontapi` y.. `http`, En clústeres ONTAP de origen y destino. Consulte "Gestionar cuentas de usuario en la documentación de ONTAP" si quiere más información.

   - **Utilice un certificado**: Cargue el certificado `.pem` archivo, la clave de certificado `.key` archivo y, opcionalmente, el archivo de entidad de certificación.
5. Seleccione **Guardar**.

Gestionar un back-end de almacenamiento detectado

Puede seleccionar gestionar un back-end de almacenamiento no gestionado pero detectado. Cuando gestionas un back-end de almacenamiento, Astra Control indica si ha caducado un certificado para la autenticación.

Pasos

1. En la navegación de la izquierda, seleccione **Backends**.
2. Seleccione la opción **Descubrido**.
3. Seleccione el back-end de almacenamiento.
4. En el menú Opciones de la columna **Acciones**, selecciona **Administrar**.
5. Realice los cambios.
6. Seleccione **Guardar**.

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.

Antes de empezar

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

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. Desde la opción **Acciones**, selecciona **Desgestionar**.
   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**, selecciona **Eliminar**.
   c. Escriba "eliminar" para confirmar la acción.
   d. Seleccione **Sí, quite el backend de almacenamiento**.

Obtenga más información

- "Utilice la API Astra Control"

Supervisar tareas en ejecución

Puede ver detalles sobre las tareas en ejecución y las tareas que se han completado, han fallado o han sido canceladas en las últimas 24 horas en Astra Control. Por ejemplo, puede ver el estado de una operación de backup, restauración o clonado en ejecución, y ver detalles como un porcentaje completado y el tiempo restante estimado. Es posible

ver el estado de una operación programada que se haya ejecutado o una operación que se inició manualmente.

Mientras ve una tarea en ejecución o completada, puede expandir los detalles de la tarea para ver el estado de cada una de las subtareas. La barra de progreso de la tarea es verde para las tareas en curso o completadas, azul para las tareas canceladas y rojo para las tareas que han fallado debido a un error.

Para las operaciones de clonado, las subtareas consisten en una operación de restauración de Snapshot y de Snapshot.

Para ver más información sobre las tareas fallidas, consulte "Controlar la actividad de la cuenta".

Pasos

1. Mientras se está ejecutando una tarea, vaya a **aplicaciones**.
2. Seleccione el nombre de una aplicación de la lista.
3. En los detalles de la aplicación, seleccione la ficha **tareas**.

   Puede ver detalles de tareas actuales o pasadas y filtrar por estado de tarea.

Las tareas se conservan en la lista **tareas** durante un máximo de 24 horas. Puede configurar este límite y otros ajustes del monitor de tareas mediante "API de control Astra".

Supervise la infraestructura con conexiones Cloud Insights, Prometheus o 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, configure Prometheus o 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.

- Conéctese a Cloud Insights
- Conéctese a Prometheus
- Conectar a Fluentd

Añada un servidor proxy para las conexiones a Cloud Insights 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** de 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.

Cuando Astra Control Center se empareja con Cloud Insights, no debes usar la opción **Modificar implementación** en Cloud Insights.

Después de habilitar la conexión Cloud Insights, puede ver la información de rendimiento en la página **Backends**, así como conectarse a Cloud Insights después de seleccionar un backend de almacenamiento. También puede encontrar la información en el **Tablero** en la sección Clúster y conectarse a Cloud Insights desde allí.

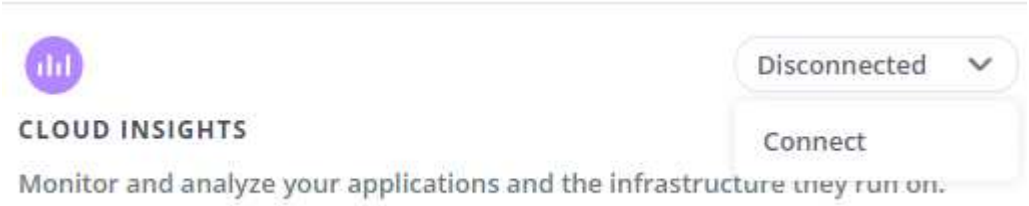
Antes de empezar

- 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.



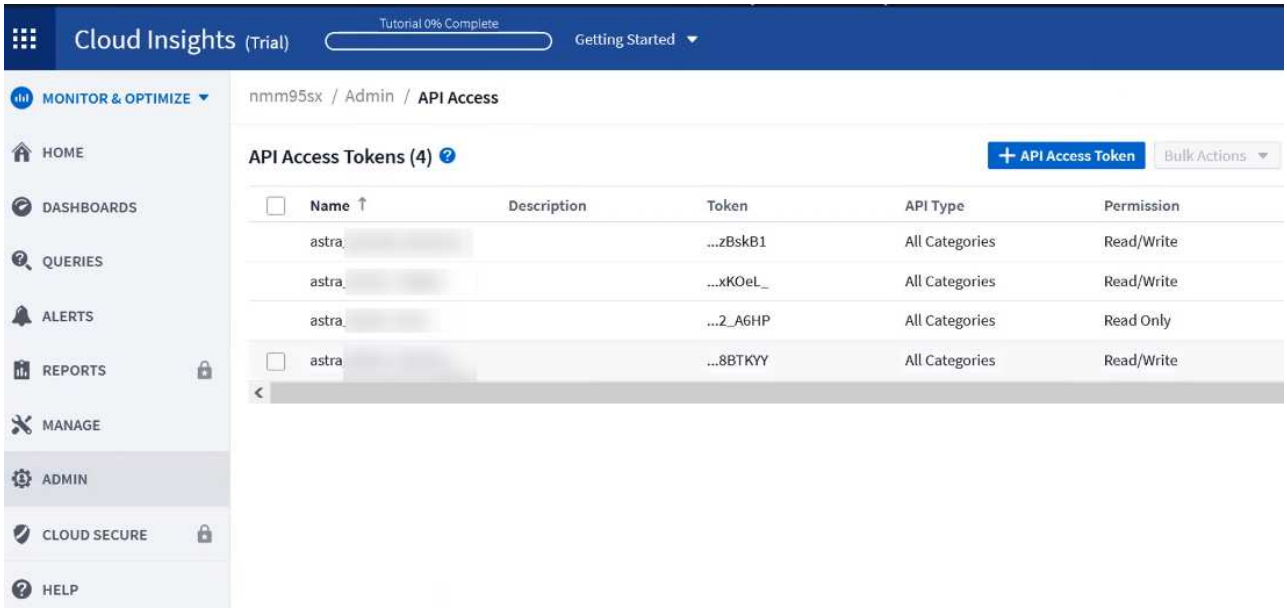
4. Introduzca los tokens de la API Cloud Insights y la URL del inquilino. La URL del inquilino tiene el siguiente formato, como ejemplo:

```
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: Ingesta 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.

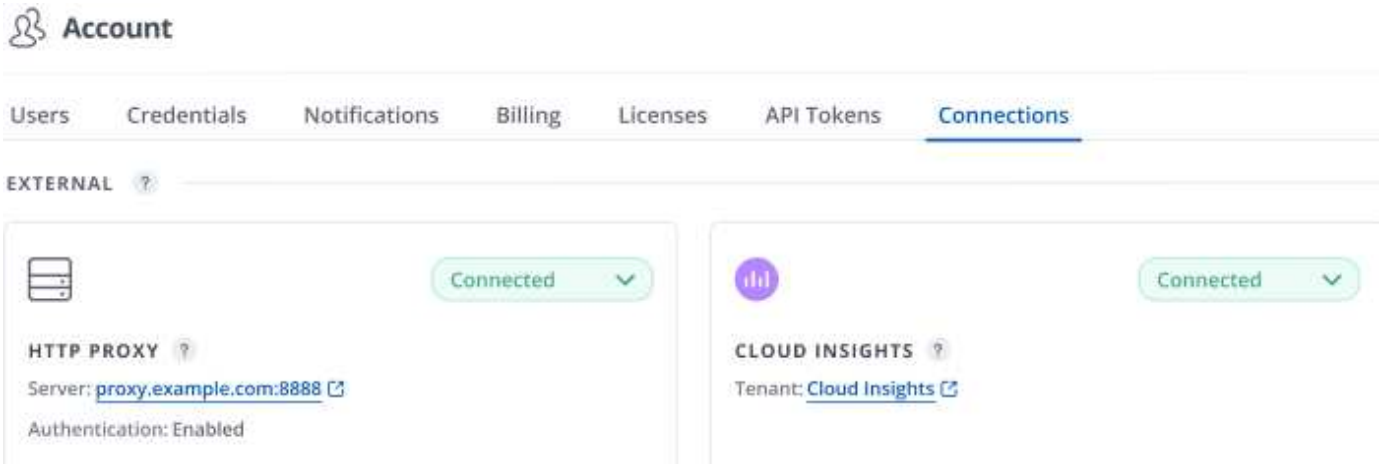
5. Seleccione **conectar**.

> 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**.

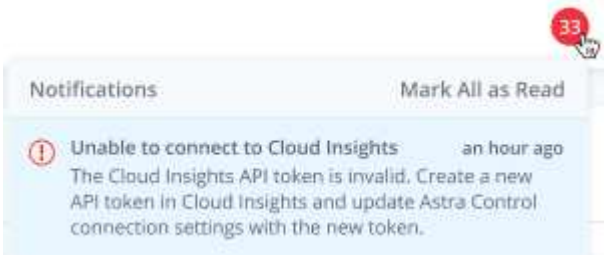
> Para retroceder y avanzar fácilmente entre el Centro de control de Astra y las interfaces de usuario de Cloud Insights, asegúrese de que ha iniciado sesión en ambos.

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.

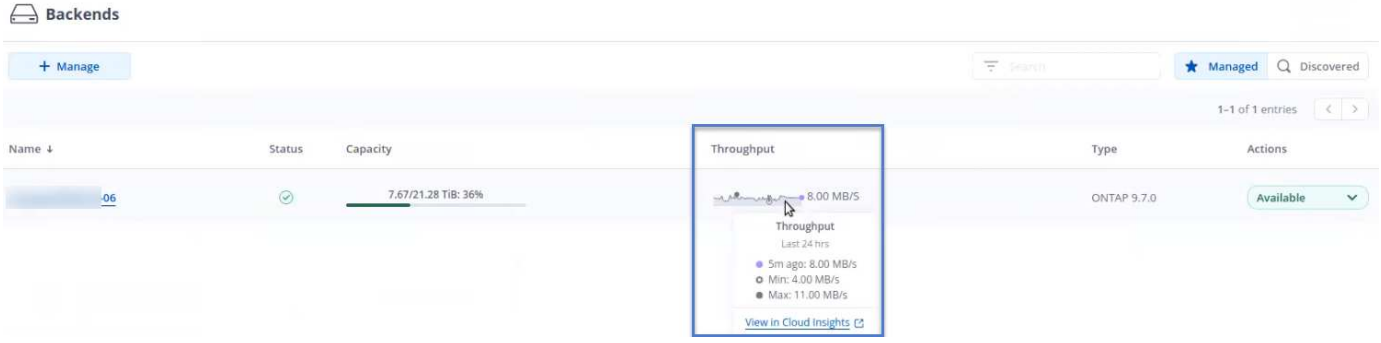


Si la conexión falló por algún motivo, el estado muestra **error**. Puede encontrar el motivo del fallo en **Notificaciones** en la parte superior derecha de la interfaz de usuario.



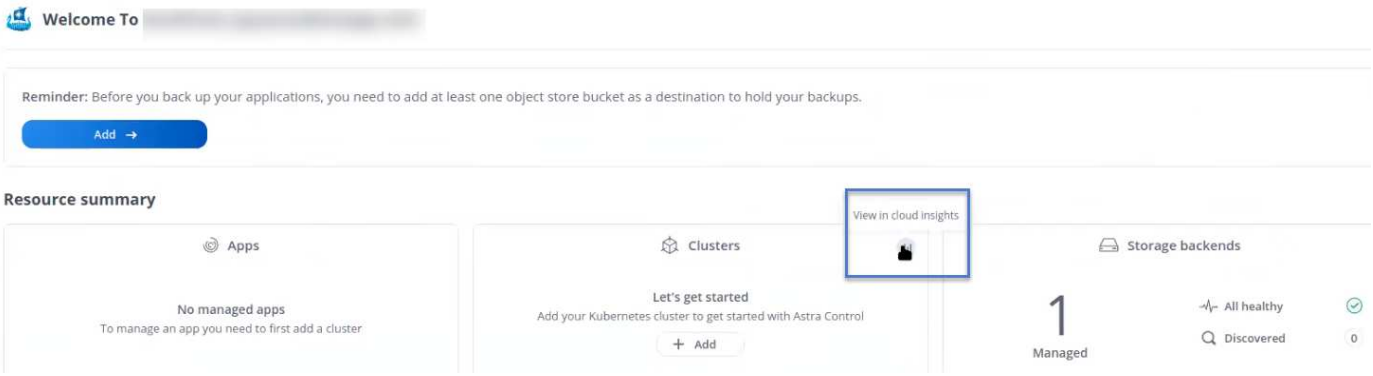
También puede encontrar la misma información en **cuenta** > **Notificaciones**.

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** de 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**.

Conéctese a Prometheus

Puede supervisar los datos del Centro de control de Astra con Prometheus. Puede configurar Prometheus para recopilar métricas desde el extremo de métricas del clúster de Kubernetes, y también puede utilizar Prometheus para visualizar los datos de métricas.

Para obtener más información sobre el uso de Prometheus, consulte su documentación en "Introducción a Prometheus".

Lo que necesitará

Asegúrese de que ha descargado e instalado el paquete Prometheus en el clúster Astra Control Center o en un clúster diferente que pueda comunicarse con el clúster Astra Control Center.

Siga las instrucciones de la documentación oficial para "Instale Prometheus".

Prometheus debe poder comunicarse con el clúster Kubernetes de Astra Control Center. Si Prometheus no está instalado en el clúster de Astra Control Center, debe asegurarse de que puede comunicarse con el servicio de métricas que se ejecuta en el clúster de Astra Control Center.

Configure Prometheus

Astra Control Center expone un servicio de mediciones en el puerto TCP 9090 del clúster de Kubernetes. Debe configurar Prometheus para recopilar métricas de este servicio.

Pasos

1. Inicie sesión en el servidor Prometheus.
2. Añada la entrada del clúster en el `prometheus.yml` archivo. En la `yml` file, añada una entrada similar a la siguiente para su clúster en el `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Si establece la `tls_config insecure_skip_verify` para `true`, El protocolo de cifrado TLS no es necesario.

3. Reinicie el servicio Prometheus:

```
sudo systemctl restart prometheus
```

Prometheus de acceso

Acceda a la URL de Prometheus.

Pasos

1. En un explorador, introduzca la URL Prometheus con el puerto 9090.

2. Compruebe su conexión seleccionando **Estado** > **objetivos**.

Ver datos en Prometheus

Puede utilizar Prometheus para ver los datos de Astra Control Center.

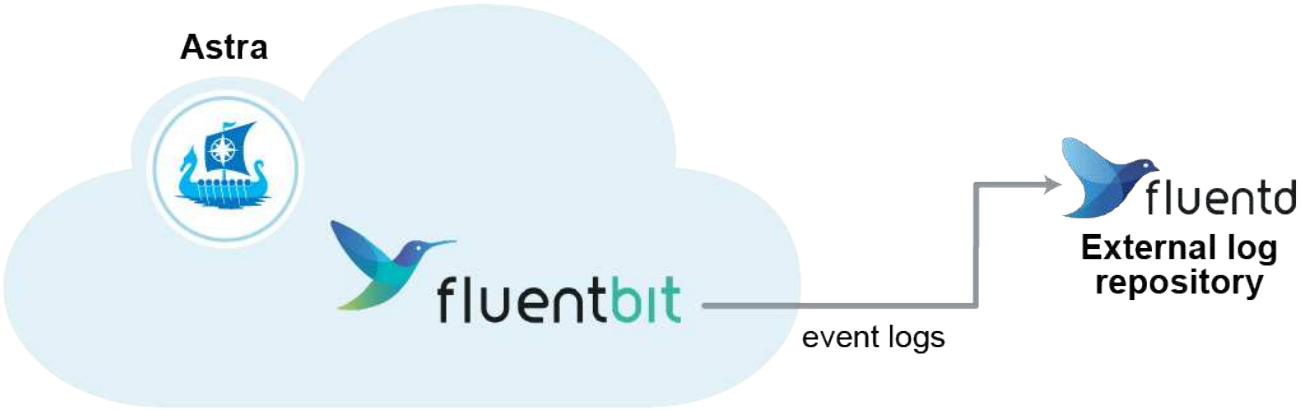
Pasos

1. En un navegador, introduzca la URL de Prometheus.
2. En el menú Prometheus, seleccione **Gráfico**.
3. Para utilizar el Explorador de métricas, seleccione el icono situado junto a **Ejecutar**.
4. Seleccione `scrape_samples_scraped` Y seleccione **Ejecutar**.
5. Para ver el raspado de muestras a lo largo del tiempo, seleccione **Gráfico**.

Si se recopilaron varios datos de clúster, las métricas de cada clúster aparecen en un color diferente.

Conectar a Fluentd

Puede enviar registros (eventos de Kubernetes) desde un sistema supervisado por Astra Control Center a su extremo de Fluentd. La conexión fluentd está desactivada de forma predeterminada.



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

Antes de empezar

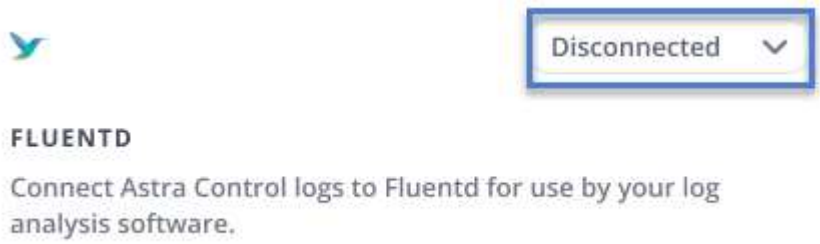
- Una cuenta de Astra Control Center con privilegios **admin**/**owner**.
- Astra Control Center se ha instalado y se ejecuta en un clúster de Kubernetes.

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** de 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.

Al anular la gestión de una aplicación:

- 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 aplicación.
3. En el menú Opciones de la columna acciones, seleccione **Unmanage**.
4. Revise la información.
5. Escriba "desgestionar" para confirmar.
6. Seleccione **Sí, anular administración de la aplicación**.

Resultado

Astra Control Center deja de gestionar la aplicación.

Desgestione un clúster

Deje de gestionar el clúster que ya no desea gestionar desde Astra Control Center.

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

Cuando se desadministra un clúster:

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

Pasos

1. En la barra de navegación izquierda, seleccione **Clusters**.
2. Seleccione la casilla de comprobación del clúster que ya no desee administrar.
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**. Después de eso, el clúster se eliminará de la página **Clusters** y ya no será gestionado por Astra Control Center.

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. Puede utilizar este procedimiento para actualizar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Estas instrucciones describen el proceso de actualización de Astra Control Center desde la segunda versión más reciente a esta versión actual. No puede actualizar directamente desde una versión que tenga dos o más versiones de la versión actual. Si la versión de Astra Control Center que tienes instalada es varias versiones detrás de la última versión, es posible que debas realizar actualizaciones en cadena a versiones más recientes hasta que el Astra Control Center instalado esté a solo una versión de la última versión. Para obtener una lista completa de las versiones lanzadas, consulte "notas de la versión".

Antes de empezar

Antes de actualizar, asegúrese de que su entorno siga cumpliendo con el "Requisitos mínimos para la puesta en marcha de Astra Control Center". Su entorno debe tener lo siguiente:

- **A "compatible" Versión Astra Trident**

  Expanda para obtener los pasos

  Determine la versión de Trident que ejecuta:

  ```
  kubectl get tridentversion -n trident
  ```

  Actualiza Astra Trident, si es necesario, mediante estos "instrucciones".

La versión 23,10 es la última versión de Astra Control Center que será compatible con Astra Trident. Se recomienda encarecidamente que usted "Habilita el aprovisionador de Astra Control" Para acceder a funciones avanzadas de aprovisionamiento de almacenamiento y gestión más allá de las que ofrece Astra Trident. Ambos tendrás que actualizar a Astra Control Center 23,10 y habilitar Astra Control Provisioner para utilizar esta funcionalidad ampliada. El aprovisionador de Astra Control no funcionará con versiones anteriores de Astra Control Center.

- **Una distribución de Kubernetes soportada**

Expanda para obtener los pasos

Determine la versión de Kubernetes que ejecuta:

```
kubectl get nodes -o wide
```

- **Recursos suficientes del cluster**

Expanda para obtener los pasos

Determine los recursos de clúster disponibles:

```
kubectl describe node <node name>
```

- **Un registro que puedes usar para insertar y cargar imágenes de Astra Control Center**
- **Una clase de almacenamiento predeterminada**

Expanda para obtener los pasos

Determine su clase de almacenamiento predeterminada:

```
kubectl get storageclass
```

- **Servicios API saludables y disponibles**

Expanda para obtener los pasos

Asegúrese de que todos los servicios de API se encuentren en buen estado y estén disponibles:

```
kubectl get apiservices
```

- **(Solo OpenShift) Operadores de clúster sanos y disponibles**

Expanda para obtener los pasos

Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

```
kubectl get clusteroperators
```

- **Acceda al registro de imágenes de NetApp Astra Control**:
  Tiene la opción de obtener imágenes de instalación y mejoras de funcionalidades para Astra Control, como Astra Control Provisioner, desde el registro de imágenes de NetApp.

  Expanda para obtener los pasos

  a. Registra tu ID de cuenta de Astra Control que tendrás que iniciar sesión en el registro.

     Puedes ver tu ID de cuenta en la interfaz de usuario web de Astra Control Service. Selecciona el icono de la figura en la parte superior derecha de la página, selecciona **Acceso API** y escribe tu ID de cuenta.

  b. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.

  c. Inicia sesión en el Registro de Astra Control:

     ```
     docker login cr.astra.netapp.io -u <account-id> -p <api-token>
     ```

Acerca de esta tarea

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

Cierre la sesión de la interfaz de usuario de Astra Control Center antes de comenzar la actualización.

- Descargue y extraiga Astra Control Center
- Elimine el complemento Astra kubectl de NetApp y vuelva a instalarlo
- Agregue las imágenes al registro local
- Instale el operador actualizado de Astra Control Center
- Actualice Astra Control Center
- Comprobar el estado del sistema

No elimine el operador Astra Control Center (por ejemplo, `kubectl delete -f astra_control_center_operator_deploy.yaml`) En cualquier momento durante la actualización o el funcionamiento de Astra Control Center para evitar la eliminación de las dosis.

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

Descargue y extraiga Astra Control Center

Puede elegir descargar el paquete Astra Control Center desde el sitio de soporte de NetApp o utilizar Docker para extraer el paquete del registro de imágenes del servicio de control de Astra.

Sitio de soporte de NetApp

1. Descargue el paquete que contiene Astra Control Center (`astra-control-center-[version].tar.gz`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (`astra-control-center-certs-[version].tar.gz`) para verificar la firma del paquete.

   Amplíe para obtener más detalles

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

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

   Se mostrará la salida `Verified OK` después de una verificación correcta.

3. Extraiga las imágenes del paquete Astra Control Center:

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

Registro de imágenes de Astra Control

1. Inicia sesión en el servicio Astra Control.
2. En el Dashboard, selecciona **Desplegar una instancia autogestionada de Astra Control**.
3. Sigue las instrucciones para iniciar sesión en el registro de imágenes de Astra Control, extraer la imagen de instalación de Astra Control Center y extraer la imagen.

Elimine el complemento Astra kubectl de NetApp y vuelva a instalarlo

Puede utilizar el complemento de línea de comandos kubectl de Astra de NetApp para insertar imágenes en un repositorio de Docker local.

1. Determine si tiene instalado el plugin:

   ```
   kubectl astra
   ```

2. Realice una de estas acciones:
   - Si el plugin está instalado, el comando debe devolver la ayuda del plugin kubectl y puede eliminar la versión existente de kubectl-astra: `delete /usr/local/bin/kubectl-astra`.
   - Si el comando devuelve un error, el plugin no está instalado y puede continuar con el siguiente paso

para instalarlo.

3. Instale el complemento:

   a. Enumere los binarios disponibles del complemento Astra kubectl de NetApp, y anote el nombre del archivo que necesita para el sistema operativo y la arquitectura de CPU:

      La biblioteca de complementos kubectl forma parte del paquete tar y se extrae en la carpeta `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Mueva el binario correcto a la ruta actual y cambie el nombre a. `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Agregue las imágenes al registro local

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

Docker

1. Cambie al directorio raíz del tarball. Debería ver el `acc.manifest.bundle.yaml` archivo y estos directorios:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Inserte las imágenes del paquete en el directorio de imágenes de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el `push-images` comando:

   - Sustituya <BUNDLE_FILE> por el nombre del archivo Astra Control Bundle (`acc.manifest.bundle.yaml`).
   - Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio de Docker; por ejemplo, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Reemplace <MY_REGISTRY_USER> por el nombre de usuario.
   - Sustituya <MY_REGISTRY_TOKEN> por un token autorizado para el registro.

     ```
     kubectl astra packages push-images -m <BUNDLE_FILE> -r
     <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
     <MY_REGISTRY_TOKEN>
     ```

Podman

1. Cambie al directorio raíz del tarball. Debería ver este archivo y directorio:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Inicie sesión en su registro:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Prepare y ejecute una de las siguientes secuencias de comandos personalizadas para la versión de Podman que utilice. Sustituya <MY_FULL_REGISTRY_PATH> por la URL del repositorio que incluye cualquier subdirectorio.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

La ruta de acceso de imagen que crea el script debe parecerse a la siguiente, dependiendo de la configuración del Registro:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

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 o edite la línea predeterminada de `imagePullSecrets: []` con lo siguiente:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

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

   c. Cambiar `ASTRA_IMAGE_REGISTRY` para la `acc-operator` 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
```

Ejemplo de astra_control_center_operator_deploy.yaml:

```
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
  strategy:
    type: Recreate
  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: ASTRA_IMAGE_REGISTRY/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
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

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.as
tra.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. Edite el recurso personalizado de Astra Control Center (CR):

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

2. Cambie el número de versión de Astra (`astraVersion` dentro de `spec`) de `23.07.0` para `23.10.0`:

> No puede actualizar directamente desde una versión que tenga dos o más versiones de la versión actual. Para obtener una lista completa de las versiones lanzadas, consulte "notas de la versión".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Compruebe que la ruta del Registro de imágenes coincide con la ruta del Registro a la que ha insertado las imágenes en paso anterior. Actualizar `imageRegistry` dentro de `spec` si el registro ha cambiado desde la última instalación.

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. Añada lo siguiente a su `crds` configuración dentro de `spec`:

```
crds:
  shouldUpgrade: true
```

5. 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
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Guarde y salga del editor de archivos. Se aplicarán los cambios y comenzará la actualización.
7. (Opcional) Verifique que los POD terminan y estén disponibles de nuevo:

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

8. Espere a que las condiciones de estado de Astra Control indiquen que la actualización está completa y lista (`True`):

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

Respuesta:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.10.0-68
10.111.111.111  True
```

Para supervisar el estado de actualización durante la operación, ejecute el siguiente comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Para inspeccionar los registros del operador de Astra Control Center, ejecute el siguiente comando:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Comprobar el estado del sistema

1. Inicie sesión en Astra Control Center.
2. Compruebe que la versión se ha actualizado. Consulte la página **Soporte** de la interfaz de usuario.
3. Compruebe que todos los clústeres y aplicaciones gestionados siguen presentes y protegidos.

Habilita el aprovisionador de Astra Control

Las versiones 23,10 y posteriores de Astra Trident incluyen la opción de usar Astra Control Provisioning, que permite a los usuarios de Astra Control con licencia acceder a funcionalidades avanzadas de aprovisionamiento del almacenamiento. El aprovisionador Astra Control ofrece esta funcionalidad ampliada, además de la funcionalidad estándar basada en CSI de Astra Trident.

En las siguientes actualizaciones de Astra Control, Astra Control Provisioner reemplazará a Astra Trident como aprovisionador de almacenamiento y orquestador en la arquitectura de Astra Control. Por este motivo, es muy recomendable que los usuarios de Astra Control habiliten el aprovisionador de Astra Control. Astra Trident seguirá siendo de código abierto y se seguirá lanzando, manteniendo, admitiendo y actualizando con las nuevas funciones CSI y otras de NetApp.

Acerca de esta tarea

Debes seguir este procedimiento si eres un usuario del Centro de control de Astra con licencia y quieres utilizar la funcionalidad de aprovisionamiento de Astra Control. También debes seguir este procedimiento si eres usuario de Astra Trident y quieres utilizar la funcionalidad adicional que proporciona el aprovisionador de Astra Control sin utilizar también Astra Control.

En cada caso, la funcionalidad de aprovisionamiento no está habilitada de forma predeterminada en Astra Trident 23,10, pero se puede habilitar mediante este proceso.

Antes de empezar

Si habilita el aprovisionador de Astra Control, primero haga lo siguiente:

Astra Control proporciona a los usuarios aprovisionamiento con Astra Control Center

- **Obtén una licencia de Astra Control Center**: Necesitarás una "Licencia de Astra Control Center" Para habilitar el aprovisionador de Astra Control y acceder a las funcionalidades que ofrece.
- **Instalar o actualizar a Astra Control Center 23,10**: Necesitarás esta versión si planeas usar Astra Control Provisionador con Astra Control.
- **Confirme que su clúster tiene una arquitectura de sistema AMD64**: La imagen del aprovisionador de Astra Control se proporciona en las arquitecturas de CPU AMD64 y ARM64, pero solo AMD64 es compatible con Astra Control Center.
- **Obtén una cuenta del Servicio de control de Astra para acceder al registro**: Si tienes la intención de usar el Registro de control de Astra en lugar del Sitio de soporte de NetApp para descargar la imagen del aprovisionador de control de Astra, completa el registro para un "Cuenta de Astra Control Service". Después de completar, enviar el formulario y crear una cuenta de BlueXP, recibirás un correo electrónico de bienvenida de Astra Control Service.
- **Si tienes Astra Trident instalado, confirma que su versión está dentro de una ventana de cuatro versiones**: Puedes realizar una actualización directa a Astra Trident 23,10 con el aprovisionador de control de Astra si tu Astra Trident está dentro de una ventana de cuatro versiones de la versión 23,10. Por ejemplo, puedes actualizar directamente de Astra Trident 22,10 a 23,10.

El aprovisionador de Astra Control solo para los usuarios

- **Obtén una licencia de Astra Control Center**: Necesitarás una "Licencia de Astra Control Center" Para habilitar el aprovisionador de Astra Control y acceder a las funcionalidades que ofrece.
- **Si tienes Astra Trident instalado, confirma que su versión está dentro de una ventana de cuatro versiones**: Puedes realizar una actualización directa a Astra Trident 23,10 con el aprovisionador de control de Astra si tu Astra Trident está dentro de una ventana de cuatro versiones de la versión 23,10. Por ejemplo, puedes actualizar directamente de Astra Trident 22,10 a 23,10.
- **Obtén una cuenta de Astra Control Service para acceder al registro**: Necesitarás acceder al registro para descargar imágenes de Astra Control Provisionador. Para comenzar, complete el registro para una "Cuenta de Astra Control Service". Después de completar, enviar el formulario y crear una cuenta de BlueXP, recibirás un correo electrónico de bienvenida de Astra Control Service.

(Paso 1) Descargue y extraiga el aprovisionador de Astra Control

Los usuarios del Centro de control de Astra pueden descargar la imagen mediante el método de registro Sitio de soporte de NetApp o Astra Control. Los usuarios de Astra Trident que deseen utilizar el aprovisionador de control de Astra sin Astra Control deben utilizar el método de registro.

(Opcional) Sitio de soporte de NetApp

1. Descarga el bundle Astra Control Provisioner (`trident-acp-[version].tar`) del "Página de descargas de Astra Control Center".
2. (Recomendado pero opcional) Descargue el paquete de certificados y firmas para Astra Control Center (astra-control-center-certs-[version].tar.gz) para verificar la firma del paquete tar trident-acp-[version].

Amplíe para obtener más detalles

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

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Cargue la imagen del aprovisionador de Astra Control:

```
docker load < trident-acp-23.10.0.tar
```

Respuesta:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Etiquete la imagen:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Introduzca la imagen en el registro personalizado:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Opción) Registro de imágenes de Astra Control

Puede utilizar Podman en lugar de Docker para los comandos de este procedimiento. Si se utiliza un entorno de Windows, se recomienda PowerShell.

1. Acceda al registro de imágenes de Astra Control de NetApp:
   a. Inicie sesión en la interfaz de usuario web de Astra Control Service y seleccione el icono de figura situado en la parte superior derecha de la página.
   b. Seleccione **acceso API**.
   c. Escriba su ID de cuenta.
   d. En la misma página, selecciona **Generar token de API** y copia la cadena de token de API en el portapapeles y guárdalo en tu editor.
   e. Inicia sesión en el registro de Astra Control usando el método que prefieras:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. Si tiene un registro personalizado, siga estos pasos para el método preferido para mover la imagen a su registro personalizado. Si no está utilizando un registro, siga los pasos del operador Trident en la "siguiente sección".

> Puede usar Podman en lugar de Docker para los siguientes comandos. Si se utiliza un entorno de Windows, se recomienda PowerShell.

Docker

a. Extrae la imagen del aprovisionador de Astra Control del registro:

> La imagen extraída no soportará múltiples plataformas y solo soportará la misma plataforma que el host que sacó la imagen, como Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform <cluster platform>
```

Ejemplo:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Etiquete la imagen:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Introduzca la imagen en el registro personalizado:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Grúa

a. Copie el manifiesto de Astra Control Provisioner en su registro personalizado:

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

(Paso 2) Habilitar el aprovisionador de Astra Control en Astra Trident

Determine si el método de instalación original ha utilizado un y complete los pasos apropiados de acuerdo con su método original.

> No utilice Helm para habilitar el aprovisionador de Astra Control. Si ha utilizado Helm para la instalación original y está actualizando a la versión 23,10, tendrá que utilizar el operador Trident o tridentctl para ejecutar la habilitación del aprovisionador de control de Astra.

Operador Astra Trident

1. "Descarga el instalador de Astra Trident y extráigalo".
2. Complete estos pasos si todavía no ha instalado Astra Trident o si ha quitado el operador de la implementación original de Astra Trident:
   a. Cree el CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. Cree el espacio de nombres trident (`kubectl create namespace trident`) o confirme que el espacio de nombres trident sigue existiendo (`kubectl get all -n trident`). Si el espacio de nombres se ha eliminado, vuelva a crearlo.
3. Actualice Astra Trident a 23.10.0:

> Para los clústeres que ejecutan Kubernetes 1,24 o una versión anterior, utilice `bundle_pre_1_25.yaml`. Para los clústeres que ejecutan Kubernetes 1,25 o posterior, utilice `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer-
23.10.0/deploy/<bundle-name.yaml>
```

4. Compruebe que Astra Trident está ejecutando:

```
kubectl get torc -n trident
```

   Respuesta:

```
NAME      AGE
trident   21m
```

5. Si tienes un registro que usa secretos, crea un secreto para extraer la imagen del aprovisionador de Astra Control:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

6. Edite el CR de TridentOrchestrator y realice las siguientes modificaciones:

```
kubectl edit torc trident -n trident
```

a. Establezca una ubicación de registro personalizada para la imagen de Astra Trident o extráigala del registro de Astra Control (`tridentImage: <my_custom_registry>/trident:23.10.0` o. `tridentImage: netapp/trident:23.10.0`).

b. Habilita el aprovisionador de Astra Control (`enableACP: true`).

c. Establezca la ubicación de registro personalizada para la imagen del aprovisionador de Astra Control o sáquela del registro de Astra Control (`acpImage: <my_custom_registry>/trident-acp:23.10.0` o. `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. Si estableció la imagen descubre los secretos anteriormente en este procedimiento, puede establecerlos aquí (`imagePullSecrets: - <secret_name>`). Utilice el mismo nombre secreto que estableció en los pasos anteriores.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Guarde y salga del archivo. El proceso de despliegue comenzará automáticamente.
8. Compruebe que se han creado el operador, el despliegue y los replicasets.

```
kubectl get all -n trident
```

Solo debe haber **una instancia** del operador en un clúster de Kubernetes. No cree varias implementaciones del operador Trident de Astra.

9. Compruebe el `trident-acp` container se está ejecutando y eso `acpVersion` es `23.10.0` con el estado de `Installed`:

```
kubectl get torc -o yaml
```

Respuesta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

1. "Descarga el instalador de Astra Trident y extráigalo".
2. "Si ya tiene un Astra Trident existente, desinstálelo del clúster que lo aloja".
3. Instale Astra Trident con el aprovisionador de control de Astra habilitado (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Confirme que se ha habilitado el aprovisionador de Astra Control:

```
./tridentctl -n trident version
```

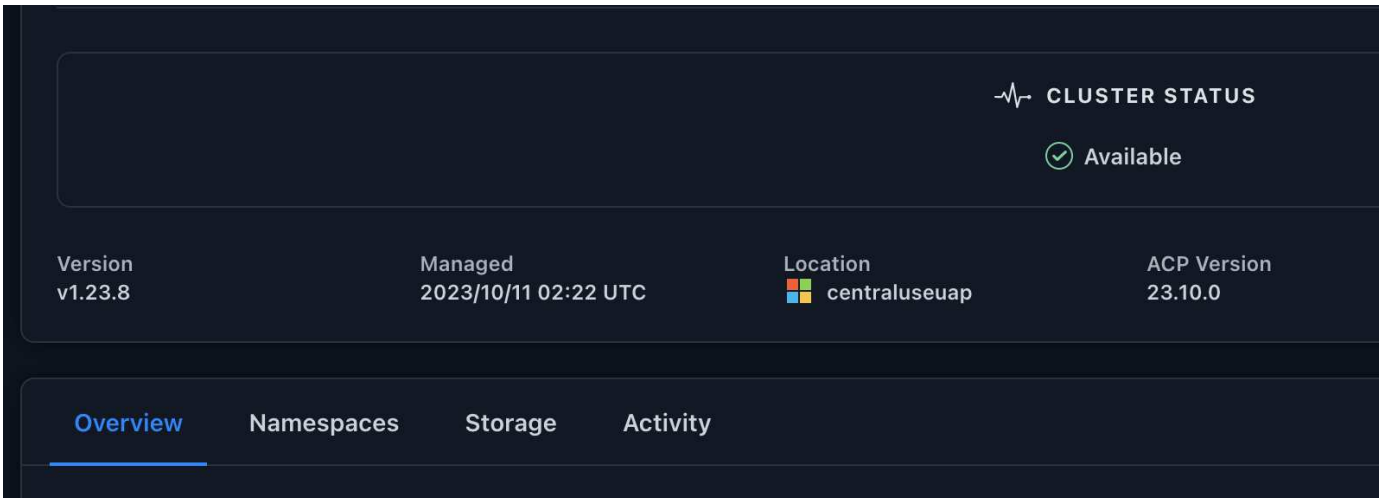
Respuesta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Resultado

Está habilitada la funcionalidad de aprovisionamiento de Astra Control y es posible usar cualquier función disponible para la versión que esté ejecutando.

(Solo para usuarios de Astra Control Center) Después de instalar Astra Control Provisioner, el clúster que aloja el aprovisionador en la interfaz de usuario de Astra Control Center mostrará un `ACP version` en lugar de `Trident version` campo y núm. de versión instalada actual.



Si quiere más información

- "Documentación sobre actualizaciones de Astra Trident"

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.

Antes de empezar

1. "Anular la gestión de todas las aplicaciones" en los clústeres.
2. "Anule la gestión de todos los clústeres".

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.yaml -n netapp-acc
   ```

   Resultado:

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

2. Utilice el siguiente comando para eliminar la `netapp-acc` espacio de nombres (o con nombre personalizado):

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

Resultado de ejemplo:

```
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"