Proteja sus aplicaciones

Astra Control Center

NetApp
November 27, 2023

Tabla de contenidos

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.
- **(sólo clústeres de OpenShift) Agregar directivas**: 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
```

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

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

Configure una política de protección

La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener.

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".

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.

Si su aplicación utiliza una clase de almacenamiento respaldada por `ontap-nas-economy` controlador, las políticas de protección no se pueden utilizar. Migra a un tipo de almacenamiento compatible con Astra Control si quieres programar backups y copias Snapshot.

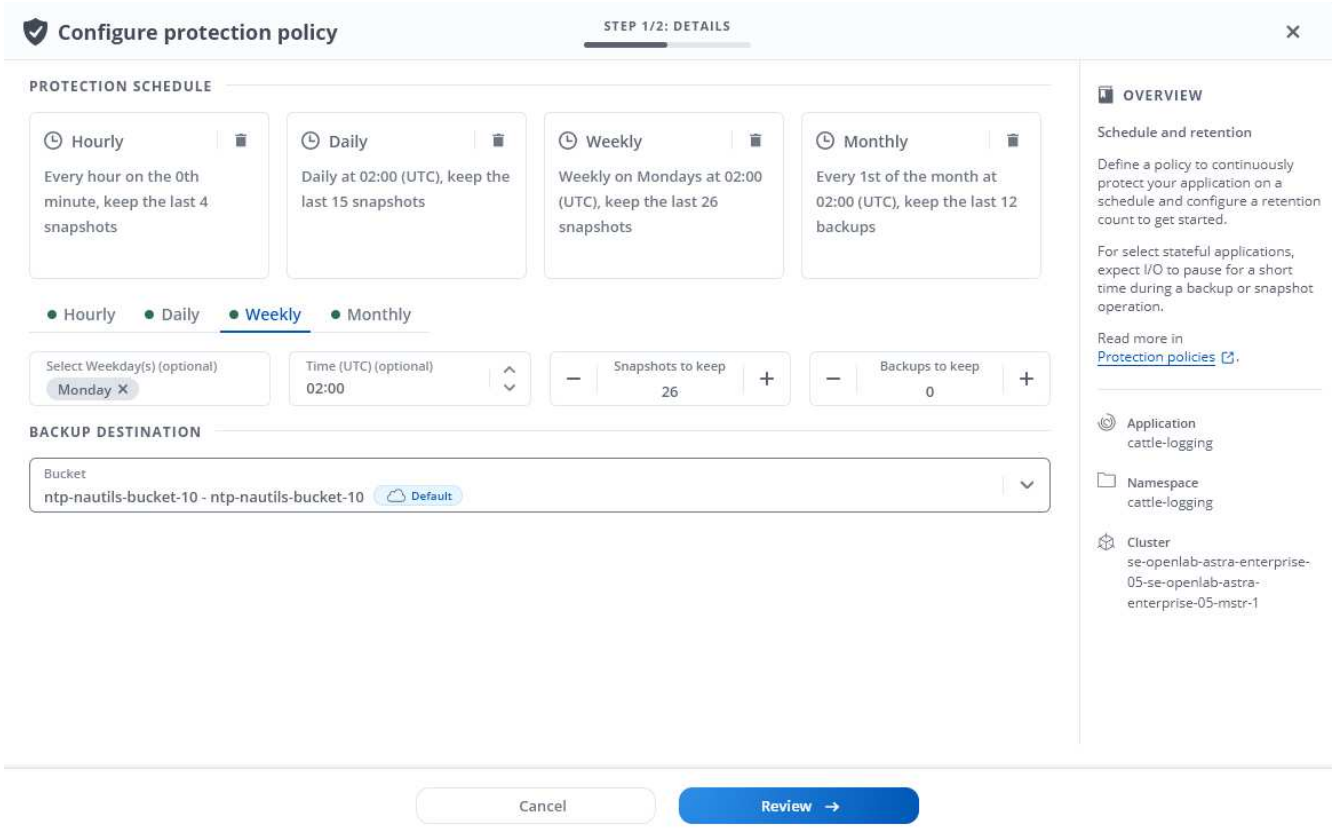
Pasos

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.

> 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

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

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

> 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. Copias de seguridad para aplicaciones respaldadas por el `ontap-nas-economy` son disruptivos y la aplicación no estará disponible hasta que se complete la operación de backup.

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.

Ver Snapshot y backups

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

Pasos

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

   Las instantáneas se muestran de forma predeterminada.

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

Eliminar snapshots

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

No 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.

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.

> 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.

Acerca de esta tarea

- **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 en el caso de que la restauración no se realice 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.
- **(sólo clústeres de OpenShift) Agregar directivas**: 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
```

- * 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.

Puede utilizar este procedimiento para cualquiera de los dos 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 el `ontap-nas-economy` controlador.

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

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.

Migre del almacenamiento económico de ontap-nas al almacenamiento ontap-nas

Puedes utilizar un Astra Control "restauración de aplicaciones" o. "clon de aplicación" operación para migrar volúmenes de aplicaciones desde un tipo de almacenamiento respaldado por `ontap-nas-economy`, que permite opciones limitadas de protección de aplicaciones, a una clase de almacenamiento respaldada por `ontap-nas` Con toda su gama de opciones de protección Astra Control. La operación de clonado o restauración migra los volúmenes basados en qtree que usan una `ontap-nas-economy` back-end a volúmenes estándar respaldados por `ontap-nas`. Volúmenes, independientemente de si lo sean `ontap-nas-economy` con un respaldo exclusivo o mixto, se migrará a la clase de almacenamiento de destino. Una vez finalizada la migración, las opciones de protección dejan de limitarse.

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:

- **ONTAP clusters**:
  - **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.
  - **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.
- **Peering**:
  - **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**:

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

  - **Clusters administrados**: Los siguientes clusters deben ser agregados y administrados por 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.
- **Configuración de Astra Trident / ONTAP**: Astra Control Center requiere que configure al menos un backend de almacenamiento que admita la replicación tanto para los clústeres de origen como de 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.
- **Clase de almacenamiento respaldada por la economía de ontap-nas**: Si su aplicación utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, la parte de backup de una operación de clonado causa interrupciones. La aplicación de origen no está disponible hasta que se complete el backup. La porción de restauración de la operación de clonado no es disruptiva.
- **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 crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.
- **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.

     Puede migrar una clase de almacenamiento de una aplicación a un tipo de almacenamiento de proveedor de nube nativo u otra clase de almacenamiento compatible, 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 crear un espacio de nombres nuevo mediante una operación de clonado o restauración, el propietario/administrador de la cuenta puede editar las restricciones de la cuenta de usuario miembro y actualizar las restricciones de roles para que el usuario afectado conceda acceso al nuevo espacio de nombres.

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

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

- 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, los ganchos de ejecución posteriores a la restauración ya no se ejecutarán tras una replicación de conmutación al nodo de 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

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
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.

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. Vaya a **cuenta**.
2. Seleccione la ficha **Scripts**.
3. Seleccione **Agregar**.
4. Debe realizar una de las siguientes acciones:
   - Cargue un script personalizado.
     i. Seleccione la opción **cargar archivo**.
     ii. Navegue hasta un archivo y cárguelo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
     v. Seleccione **Guardar script**.
   - Pegar en un script personalizado desde el portapapeles.
     i. Seleccione la opción **Pegar o Tipo**.
     ii. Seleccione el campo de texto y pegue el texto del script en el campo.
     iii. Asigne al script un nombre único.
     iv. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
5. Seleccione **Guardar script**.

Resultado

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

Eliminar un script

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

Pasos

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

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

Cree un enlace de ejecución personalizado

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. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione **Agregar**.
4. En el área **Detalles del gancho**:
   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.
5. (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.

6. Cuando termine, seleccione **Siguiente**.
7. 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.

8. Seleccione **Siguiente**.
9. Revise la configuración del gancho de ejecución.
10. 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.

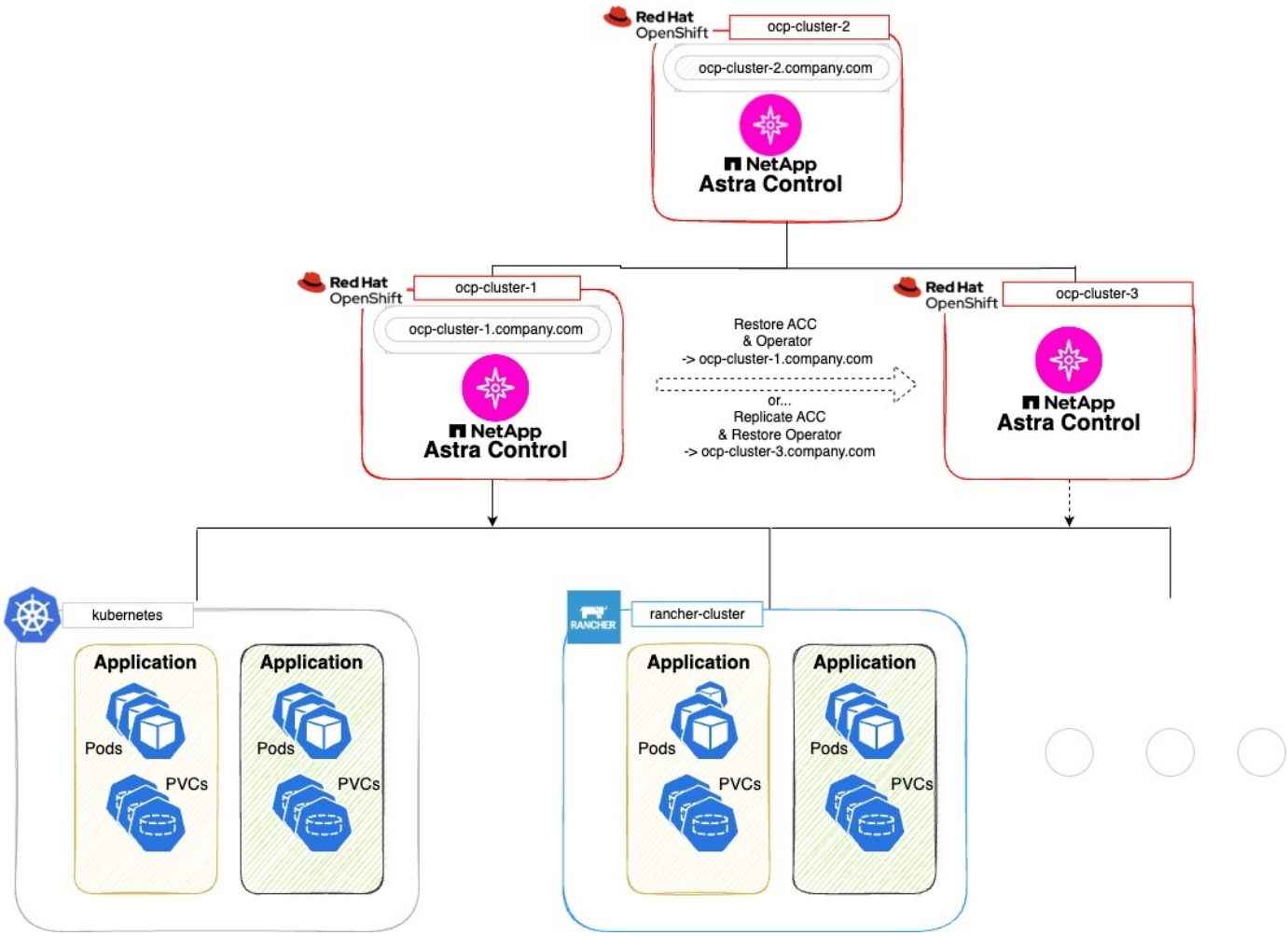
Antes de empezar

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: acc-crd
- 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 23.07.0-24 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**.

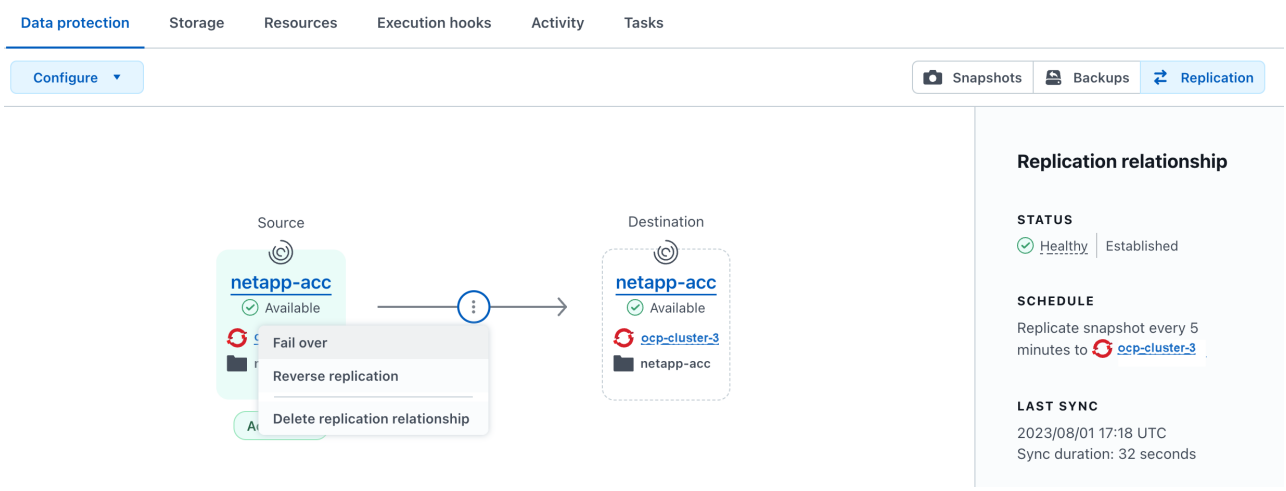
   h. Confirme que la configuración es correcta y seleccione **Guardar**.

      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 23.07.0-24 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.

Información de copyright

Información de la marca comercial