Gestione y proteja aplicaciones

Astra Control Service

NetApp
October 21, 2024

Tabla de contenidos

Gestione y proteja aplicaciones

Inicie la gestión de aplicaciones

Usted primero "Añada un clúster de Kubernetes a Astra Control", Puede instalar aplicaciones en el clúster (fuera de Astra Control) y, a continuación, ir a la página aplicaciones de Astra Control para definir las aplicaciones.

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

Requisitos de gestión de aplicaciones

Astra Control tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencias**: Para administrar más de 10 espacios de nombres, necesitas una suscripción a Astra Control.
- **Namespaces**: Las aplicaciones se pueden definir dentro de uno o más espacios de nombres especificados en un único clúster mediante Astra Control. Una aplicación puede contener recursos que abarcan varios espacios de nombres dentro del mismo clúster. Astra Control no admite la capacidad de definir las aplicaciones en varios clústeres.
- **Clase de almacenamiento**: Si instala una aplicación con una clase de almacenamiento definida explícitamente y necesita clonar la aplicación, el clúster de destino para la operación de clonación debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.
- **Recursos de Kubernetes**: Las aplicaciones que utilizan los recursos de Kubernetes no recopilados por Astra Control pueden no tener funciones completas de gestión de datos de aplicaciones. Astra Control recopila los siguientes recursos de Kubernetes:

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

Métodos de instalación de aplicaciones compatibles

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

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

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

- **Helm 3**: Si utiliza Helm para instalar aplicaciones, Astra Control requiere Helm versión 3. La gestión y clonación de aplicaciones instaladas con Helm 3 (o actualizadas de Helm 2 a Helm 3) son totalmente compatibles. No se admite la administración de aplicaciones instaladas con Helm 2.
- **Aplicaciones implementadas por el operador**: Astra Control admite aplicaciones instaladas con operadores de ámbito de espacio de nombres que, en general, están diseñados con una arquitectura de "paso por valor" en lugar de "paso por referencia". Un operador y la aplicación que instale deben usar el mismo espacio de nombres; es posible que deba modificar el archivo .yaml de despliegue para que el operador se asegure de que así sea.

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

  - "Apache K8ssandra"

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

  - "Jenkins CI"
  - "Clúster Percona XtraDB"

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

Instale las aplicaciones en el clúster

La tienes "ha agregado el clúster" A Astra Control, puede instalar aplicaciones o gestionar las aplicaciones existentes en el clúster. Cualquier aplicación que se limita a uno o más espacios de nombres se puede gestionar.

Astra Control gestionará las aplicaciones con estado solo si el almacenamiento está en una clase de almacenamiento compatible con Astra Control. Astra Control Service es compatible con cualquier clase de almacenamiento que sea compatible con el aprovisionador de control Astra o un controlador CSI genérico.

- "Obtenga información sobre clases de almacenamiento para clústeres GKE"
- "Obtenga información sobre clases de almacenamiento para clústeres de AKS"
- "Obtenga información sobre las clases de almacenamiento para clústeres de AWS"

Defina las aplicaciones

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

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

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

Antes de empezar

- Se añadió un clúster de Kubernetes a Astra Control.
- Una o más aplicaciones instaladas en el clúster. Obtenga más información sobre los métodos de instalación de aplicaciones compatibles.
- Espacios de nombres existentes en el clúster Kubernetes que se añadió a Astra Control.
- (Opcional) una etiqueta de Kubernetes en cualquiera "Recursos de Kubernetes compatibles".

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

Acerca de esta tarea

- Antes de empezar, también debe entender "gestión de espacios de nombres estándar y del sistema".
- Si planea utilizar varios espacios de nombres con sus aplicaciones en Astra Control, tenga en cuenta "modificación de los roles de usuario con restricciones de espacio de nombres" antes de definir aplicaciones.
- Para obtener instrucciones sobre cómo gestionar aplicaciones mediante la API de Astra Control, consulte "Información sobre API y automatización de Astra".

Opciones de gestión de aplicaciones

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

Defina los recursos que se van a administrar como una aplicación

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

Definir una aplicación le proporciona un control más granular de lo que se debe incluir en una operación Astra

Control, que incluye clonado, copias Snapshot y backups.

> Al definir aplicaciones, asegúrese de no incluir un recurso de Kubernetes en varias aplicaciones con políticas de protección. La superposición de políticas de protección en recursos de Kubernetes puede provocar conflictos de datos.

Obtenga más información sobre la adición de recursos con ámbito de clúster a los espacios de nombres de la aplicación.

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

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

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

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

Pasos

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

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

5. (Opcional) Introduzca una etiqueta para los recursos de Kubernetes en cada espacio de nombres. Puede especificar una sola etiqueta o un criterio de selector de etiquetas (consulta).

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

6. (Opcional) Añada espacios de nombres adicionales para la aplicación seleccionando **Agregar espacio de nombres** y eligiendo el espacio de nombres en la lista desplegable.
7. (Opcional) Introduzca los criterios de etiqueta única o selector de etiquetas para los espacios de nombres adicionales que añada.
8. (Opcional) para incluir recursos de ámbito de clúster además de los que Astra Control incluye automáticamente, marque **incluir recursos adicionales de ámbito de clúster** y complete lo siguiente:
   a. Seleccione **Agregar regla de inclusión**.
   b. **Grupo**: En la lista desplegable, seleccione el grupo API de recursos.
   c. **Kind**: En la lista desplegable, seleccione el nombre del esquema de objetos.
   d. **Versión**: Introduzca la versión API.
   e. **Selector de etiquetas**: Opcionalmente, incluya una etiqueta que se agregará a la regla. Esta etiqueta se utiliza para recuperar solo los recursos que coincidan con esta etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster.
   f. Revise la regla que se crea en función de las entradas.
   g. Seleccione **Agregar**.

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

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

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

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

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

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

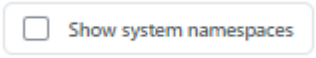
Defina un espacio de nombres para administrar como una aplicación

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

Pasos

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

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

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

"Leer más".

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

[Vista PREVIA TÉCNICA] Defina una aplicación utilizando un recurso personalizado de Kubernetes

Puede especificar los recursos de Kubernetes que desee gestionar con Astra Control definiéndolos como aplicación mediante un recurso personalizado (CR). Puede añadir recursos de ámbito en clúster si desea gestionar esos recursos individualmente o todos los recursos de Kubernetes en un espacio de nombres si, por ejemplo, tiene la intención de gestionar y proteger todos los recursos de un espacio de nombres particular de una forma similar y con intervalos comunes.

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre (por ejemplo, `astra_mysql_app.yaml`).
2. Asigne un nombre a la aplicación en `metadata.name`.
3. Defina los recursos de aplicación que se van a gestionar:

spec.includedClusterScopedResources

Incluye los tipos de recursos de ámbito del clúster además de los que Astra Control incluye automáticamente:

- **spec.includedClusterScopedResources**: *(Opcional)* Una lista de tipos de recursos de ámbito de cluster que se incluirán.
  - **GroupVersionKind**: *(Opcional)* identifica inequívocamente un tipo.
    - **GROUP**: *(requerido si se usa groupVersionKind)* Grupo API del recurso a incluir.
    - **VERSIÓN**: *(requerido si se usa groupVersionKind)* Versión API del recurso a incluir.
    - **Kind**: *(requerido si se usa groupVersionKind)* tipo de recurso a incluir.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. Los requisitos son ANDed.
      - **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
      - **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
      - **VALORES**: *(requerido si se utiliza matchExpressions)_Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe _not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

spec.includedNamespaces

Incluya espacios de nombres y recursos dentro de esos recursos en la aplicación:

- **spec.includedNamespaces**: _(required)_Define el espacio de nombres y los filtros opcionales para la selección de recursos.
  - **Namespace**: *(required)* El espacio de nombres que contiene los recursos de la aplicación que desea administrar con Astra Control.
  - **LabelSelector**: *(Opcional)* Una consulta de etiqueta para un conjunto de recursos. Se utiliza para recuperar solo los recursos que coinciden con la etiqueta. Si no proporciona una etiqueta, Astra Control recopila todas las instancias del tipo de recurso especificado para ese clúster. El resultado de matchLabels y matchExpressions son ANDed.
    - **MatchLabels**: *(Opcional)* Un mapa de {key,value} pares. Un único {key,value} en el mapa matchLabels es equivalente a un elemento de matchExpressions que tiene un campo clave de “key”, operador como “in” y matriz de valores que contiene solo “value”. Los requisitos son ANDed.
    - **MatchExpressions**: *(Opcional)* Una lista de los requisitos del selector de etiquetas. `key` y.. `operator` son obligatorios. Los requisitos son ANDed.

- **KEY**: *(requerido si se usa matchExpressions)* La clave de etiqueta asociada con el selector de etiquetas.
- **OPERATOR**: *(requerido si se usa matchExpressions)* representa la relación de una clave con un conjunto de valores. Los operadores válidos son `In`, `NotIn`, `Exists` y.. `DoesNotExist`.
- **Valores**: *(requerido si se usa matchExpressions)* Una matriz de valores de cadena. Si el operador es `In` o. `NotIn`, la matriz de valores debe *not* estar vacía. Si el operador es `Exists` o. `DoesNotExist`, la matriz de valores debe estar vacía.

Ejemplo YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

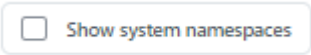
4. Después de rellenar el `astra_mysql_app.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

¿Qué ocurre con los espacios de nombres del sistema?

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

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



Astra Control en sí no es una aplicación estándar; es una "aplicación del sistema". No debe intentar gestionar Astra Control por sí mismo. Astra Control no se muestra de forma predeterminada para la gestión.

Proteja las aplicaciones con snapshots y backups

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

Más información acerca de "Protección de datos en Astra Control".

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

- Configure una política de protección
- Crear una copia de Snapshot
- Cree un backup
- Habilite el backup y la restauración para las operaciones económicas de ontap-nas
- Cree un backup inmutable
- Ver Snapshot y backups
- Eliminar snapshots
- Cancelar backups
- Eliminar backups

Configure una política de protección

La política de protección protege una aplicación mediante la creación de snapshots, backups o ambos con una programación definida. Puede optar por crear snapshots y backups por hora, día, semana y mes, y especificar la cantidad de copias que desea retener. Puede definir una política de protección con la interfaz de usuario web de Astra Control o un archivo de recursos personalizados (CR).

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

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

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

Configure una política de protección con la interfaz de usuario web

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. Definir una programación de protección seleccionando la cantidad de Snapshot y backups que se deben mantener en las programaciones por hora, por día, por semana y por 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.

   [Captura de pantalla de una directiva de configuración de ejemplo en la que puede elegir hacer Snapshots y backups cada hora, día, semana o mes.]

5. [**Vista previa tecnológica**] Elija un depósito de destino para las copias de seguridad o instantáneas de la lista de depósitos de almacenamiento.
6. Seleccione **Revisión**.
7. Seleccione **Configurar política de protección.**

[Tech preview] Configurar una política de protección con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-schedule-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tus necesidades de entorno de Astra Control, configuración del clúster y protección de datos:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.
   - <BACKUPS_RETAINED>: La cantidad de backups que se retendrán. Cero indica que no se debe crear ningún backup.
   - <SNAPSHOTS_RETAINED>: La cantidad de snapshots que se retendrán. Cero indica que no se debe crear ninguna instantánea.
   - <GRANULARITY>: La frecuencia con la que debe ejecutarse la programación. Los posibles valores, junto con los campos asociados necesarios:
     - `hourly` (requiere que especifique `spec.minute`)
     - `daily` (requiere que especifique `spec.minute` y.. `spec.hour`)
     - `weekly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfWeek`)

    - `monthly` (requiere que especifique `spec.minute`, `spec.hour`, y. `spec.dayOfMonth`)
  - <DAY_OF_MONTH>: *(Opcional)* el día del mes (1 - 31) en el que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `monthly`.
  - <DAY_OF_WEEK>: *(Opcional)* El día de la semana (0 - 7) en el que se debe ejecutar la programación. Los valores de 0 o 7 indican el domingo. Este campo es necesario si la granularidad se establece en `weekly`.
  - <HOUR_OF_DAY>: *(Opcional)* La hora del día (0 - 23) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `daily`, `weekly`, o. `monthly`.
  - <MINUTE_OF_HOUR>: *(Opcional)* El minuto de la hora (0 - 59) que debe ejecutarse la programación. Este campo es necesario si la granularidad se establece en `hourly`, `daily`, `weekly`, o. `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Después de rellenar el `astra-control-schedule-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Resultado

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

Crear una copia de Snapshot

Puede crear una snapshot bajo demanda en cualquier momento.

Acerca de esta tarea

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

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

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

Cree una copia Snapshot de con la interfaz de usuario web de

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. [**Vista previa tecnológica**] Elija un cubo de destino para la instantánea de la lista de cubos de almacenamiento.
5. Revise el resumen de la instantánea y seleccione **Snapshot**.

[Vista previa técnica] Crear una instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación que se va a realizar la instantánea.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la instantánea.
   - <RECLAIM_POLICY>: *(Opcional)* define lo que ocurre con una instantánea cuando se elimina la CR de instantánea. Opciones válidas:
     - `Retain`
     - `Delete` (predeterminado)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Después de rellenar el `astra-control-snapshot-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

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.

> Sepa cómo se maneja el espacio de almacenamiento al realizar un backup de una aplicación alojada en el almacenamiento de Azure NetApp Files. Consulte "Backups de aplicaciones" si quiere más información.

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

Acerca de esta tarea

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

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

Cree un backup con la interfaz de usuario web de

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. [**Tech preview**] Elija un depósito de destino para la copia de seguridad de la lista de depósitos de almacenamiento.
6. Seleccione **Siguiente**.
7. Revise el resumen de copia de seguridad y seleccione **copia de seguridad**.

[Vista previa técnica] Cree un backup con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de este recurso personalizado; elija un nombre único y sensible para su entorno.
   - <APPLICATION_NAME>: El nombre de Kubernetes de la aplicación de la que se va a realizar el backup.
   - <APPVAULT_NAME>: El nombre del AppVault donde se debe almacenar el contenido de la copia de seguridad.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Después de rellenar el `astra-control-backup-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Resultado

Astra Control crea una copia de seguridad de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si necesita cancelar una copia de seguridad en ejecución, utilice las instrucciones de Cancelar backups. Para eliminar la copia de seguridad, espere hasta que haya finalizado y, a continuación, utilice las instrucciones de Eliminar backups.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

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

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

Antes de empezar

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

Expanda para obtener pasos de configuración

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

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

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

   c. Oculte el directorio de snapshots para la SVM:

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

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

+

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

2. Haga lo siguiente en Astra Control Provisioner o Astra Trident:

   a. Habilite el directorio snapshot para cada VP basado en ontap-nas y asociado con la aplicación:

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

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

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

   Respuesta:

```
snapshotDirectory: "true"
```

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

Resultado

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

Cree un backup inmutable

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

Antes de empezar

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

- **Amazon Web Services**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «gobierno» con un período de retención predeterminado".
- **Google Cloud**: "Configure un depósito con una política de retención y especifique un período de retención".
- **Microsoft Azure**: "Configure un depósito de almacenamiento BLOB con una política de retención basada en tiempo en el ámbito de nivel de contenedor".
- **NetApp StorageGRID**: "Habilite S3 Object Lock al crear el bloque y establezca un modo de retención predeterminado de «cumplimiento» con un período de retención predeterminado".

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

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

Pasos

1. Seleccione **aplicaciones**.
2. En el menú Opciones de la columna **acciones** de la aplicación deseada, seleccione **copia de seguridad**.
3. Personalice el nombre del backup.
4. Elija si desea realizar una copia de seguridad de la aplicación desde una instantánea existente. Si selecciona esta opción, puede elegir entre una lista de snapshots existentes.
5. Seleccione un bucket de destino para el backup en la lista de bloques de almacenamiento. Se indica un depósito de escritura única y lectura múltiple (WORM) con el estado «bloqueado» junto al nombre del depósito.

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

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

Resultado

Astra Control crea un backup inmutable de la aplicación.

- Si la red tiene una interrupción del servicio o es anormalmente lenta, es posible que se agote el tiempo de espera de una operación de backup. Esto provoca un error en el backup.
- Si intentas crear dos backups inmutables de la misma aplicación en el mismo bloque a la vez, Astra Control impide que se inicie el segundo backup. Espere hasta que se complete la primera copia de seguridad antes de iniciar otra.
- No es posible cancelar una copia de seguridad inmutable en ejecución.
- Después de una operación de protección de datos (clonado, backup, restauración) y un cambio de tamaño posterior de volumen persistente, se demora hasta veinte minutos antes de que se muestre el tamaño del nuevo volumen en la interfaz de usuario. La operación de protección de datos se realiza correctamente en cuestión de minutos, y se puede utilizar el software de gestión para el back-end de almacenamiento para confirmar el cambio de tamaño del volumen.

Ver Snapshot y backups

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

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

Pasos

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

   Las instantáneas se muestran de forma predeterminada.

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

Eliminar snapshots

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

Pasos

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

Resultado

Astra Control elimina la instantánea.

Cancelar backups

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

Para cancelar una copia de seguridad, la copia de seguridad debe estar en `Running` estado. No puede cancelar una copia de seguridad que esté en `Pending` estado.

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

Pasos

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

Eliminar backups

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

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.

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

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.

[Tech preview] Proteger todo un clúster

Es posible crear un backup automático programado de cualquiera de los espacios de nombres no gestionados de un clúster o de todos ellos. Estos flujos de trabajo los proporciona NetApp como una cuenta de servicio de Kubernetes, enlaces de roles y un trabajo cron orquestado con un script de Python.

Cómo funciona

Cuando configura e instala el flujo de trabajo de backup de clúster completo, un trabajo con cron se ejecuta periódicamente y protege cualquier espacio de nombres que aún no esté gestionado, lo que crea automáticamente políticas de protección basadas en los programas que elija durante la instalación.

Si no desea proteger todos los espacios de nombres no administrados en el clúster con el flujo de trabajo de backup de clúster completo, en su lugar, puede utilizar el flujo de trabajo de backup basado en etiquetas. El flujo de trabajo de backup basado en etiquetas también usa una tarea CRON, pero, en lugar de proteger todos los espacios de nombres no gestionados, identifica los espacios de nombres por etiquetas que se proporcionan para proteger, opcionalmente, los espacios de nombres según políticas de backup bronce, plata o oro.

Cuando se crea un nuevo espacio de nombres que se ajusta al alcance del flujo de trabajo elegido, se protege automáticamente, sin necesidad de que el administrador realice ninguna acción. Estos flujos de trabajo se implementan por clúster, de modo que diferentes clústeres pueden utilizar cualquier flujo de trabajo con niveles de protección únicos, según la importancia del clúster.

Ejemplo: Protección de clúster completa

Como ejemplo, cuando configura e instala el flujo de trabajo de backup completo del clúster, las aplicaciones en cualquier espacio de nombres se gestionan periódicamente y se protegen sin que el administrador intervenga. El espacio de nombres no tiene que existir en el momento de instalar el flujo de trabajo; si se agrega un espacio de nombres en el futuro, se protegerá.

Ejemplo: Protección basada en etiquetas

Para obtener más granularidad, puede utilizar el flujo de trabajo basado en etiquetas. Por ejemplo, puede instalar este flujo de trabajo y decirle a los usuarios que apliquen una de varias etiquetas a cualquier espacio de nombres que quieran proteger, según el nivel de protección que necesiten. Esto permite a los usuarios crear el espacio de nombres con una de estas etiquetas, y no tienen que notificar a un administrador. Su nuevo espacio de nombres y todas las aplicaciones que contiene quedan protegidas de forma automática.

Cree una copia de seguridad programada de todos los espacios de nombres

Es posible crear un backup programado de todos los espacios de nombres en un clúster mediante el flujo de trabajo de backup de clúster completo.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:
   - "Archivo CRD Components.yaml"
   - "protectCluster.py Script Python"
2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Crear una copia de seguridad programada de espacios de nombres específicos

Puede crear un backup programado de espacios de nombres específicos mediante sus etiquetas mediante el flujo de trabajo de backup basado en etiquetas.

Pasos

1. Descargue los siguientes archivos en una máquina que tenga acceso a la red al clúster:
   - "Archivo CRD Components.yaml"
   - "protectCluster.py Script Python"
2. Para configurar e instalar el kit de herramientas: "siga las instrucciones incluidas".

Restaurar aplicaciones

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

> Si 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.

Antes de empezar

- **Proteja sus aplicaciones primero**: Se recomienda encarecidamente que tome una instantánea o una copia de seguridad de su aplicación antes de restaurarla. Esto le permitirá clonar desde la snapshot o backup si la restauración no se realiza correctamente.
- **Comprobar volúmenes de destino**: Si restaura a una clase de almacenamiento diferente, asegúrese de que la clase de almacenamiento utilice el mismo modo de acceso de volumen persistente (por ejemplo, ReadWriteMany). Se producirá un error en la operación de restauración si el modo de acceso al volumen persistente de destino es diferente. Por ejemplo, si el volumen persistente de origen utiliza el modo de acceso RWX, seleccionando una clase de almacenamiento de destino que no pueda proporcionar RWX, como Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, hará que falle la operación de restauración. Para obtener más información sobre los modos de acceso a volúmenes persistentes, consulte la "Kubernetes" documentación.
- **Planificar necesidades de espacio**: Cuando se realiza una restauración in situ de una aplicación que utiliza almacenamiento ONTAP de NetApp, el espacio utilizado por la aplicación restaurada puede duplicarse. Después de realizar una restauración sin movimiento, elimine las instantáneas no deseadas de la aplicación restaurada para liberar espacio de almacenamiento.
- **Controladores de clase de almacenamiento compatibles**: Astra Control admite la restauración de copias de seguridad mediante clases de almacenamiento respaldadas por los siguientes controladores:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- **(Solo controlador económico de ontap-nas) Copias de seguridad y restauraciones**: Antes de realizar copias de seguridad o restaurar una aplicación que utiliza una clase de almacenamiento respaldada por el `ontap-nas-economy` controlador, compruebe que el "El directorio Snapshot del sistema de administración de almacenamiento de ONTAP está oculto". Si no se oculta este directorio, se puede perder el acceso a la aplicación, especialmente si se utiliza NFSv3.

> 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.

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.
     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. También puede usar este procedimiento para migrar una aplicación a una clase de almacenamiento diferente.
     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**.

[Vista previa técnica] Restaurar a partir del backup mediante un recurso personalizado (CR)

Es posible restaurar datos desde un backup con un archivo de recurso personalizado (CR) en otro espacio de nombres o en el espacio de nombres de origen original.

Restaurar desde una copia de seguridad con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```yaml
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-backup-restore-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-backup-restore-cr.yaml
   ```

Restaure desde un backup al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-backup-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su

entorno.

- <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
- <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-backup-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Vista PREVIA TÉCNICA] Restauración a partir de una instantánea con un recurso personalizado (CR)

Puede restaurar datos desde una copia Snapshot con un archivo de recurso personalizado (CR) en un espacio de nombres diferente o en el espacio de nombres de origen original.

Restaurar desde instantánea con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-restore-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su entorno.
   - <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
   - <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: El espacio de nombres de origen de la operación de restauración.
   - <DESTINATION_NAMESPACE>: El espacio de nombres de destino de la operación de restauración.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-snapshot-restore-cr.yaml` Con los valores correctos, aplique el CR:

   ```
   kubectl apply -f astra-control-snapshot-restore-cr.yaml
   ```

Restauración de una snapshot al espacio de nombres original con un CR

Pasos

1. Cree el archivo de recursos personalizados (CR) y asígnele un nombre `astra-control-snapshot-ipr-cr.yaml`. Actualiza los valores entre paréntesis <> para que coincidan con tu entorno de Astra Control y la configuración del clúster:
   - <CR_NAME>: El nombre de esta operación de CR; seleccione un nombre sensible para su

entorno.

- <APPVAULT_NAME>: El nombre del AppVault donde se almacena el contenido del backup.
- <BACKUP_PATH>: Ruta dentro de AppVault, donde se almacena el contenido del backup. Por ejemplo:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Directiva no resuelta en <stdin> - Include:../_include/selective-restore-cr.adoc[]

1. Después de rellenar el `astra-control-snapshot-ipr-cr.yaml` Con los valores correctos, aplique el CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Resultado

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

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

> Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación en un nuevo espacio de nombres en el mismo clúster o en cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.

Filtre recursos durante una restauración de aplicación

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

Lea más 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.

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.

> 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.

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 haber asignado un bloque predeterminado para la instancia de cloud que contiene el clúster de origen. Si la instancia de cloud de origen no tiene un conjunto de bloques predeterminado, se producirá un error en la operación de clonado entre clústeres.
- 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.

Limitaciones de clones

- **Clases de almacenamiento explícitas**: Si implementa una aplicación con una clase de almacenamiento

definida explícitamente y necesita clonar la aplicación, el clúster de destino debe tener la clase de almacenamiento especificada originalmente. Se producirá un error al clonar una aplicación con una clase de almacenamiento definida explícitamente a un clúster que no tenga la misma clase de almacenamiento.

- **Aplicaciones respaldadas por la economía de ontap-nas**: No puede usar operaciones de clonación si la clase de almacenamiento de su aplicación está respaldada por el `ontap-nas-economy` controlador. Sin embargo, usted puede "habilite el backup y la restauración para las operaciones económicas de ontap-nas".
- **Clones y restricciones de usuario**: Cualquier usuario miembro con restricciones de espacio de nombres por nombre/ID de espacio de nombres o por etiquetas de espacio de nombres puede clonar o restaurar una aplicación a un nuevo espacio de nombres en el mismo clúster o a cualquier otro clúster de la cuenta de su organización. Sin embargo, el mismo usuario no puede acceder a la aplicación clonada o restaurada en el nuevo espacio de nombres. Después de que una operación de clonado o restauración crea un nuevo espacio de nombres, el administrador/propietario de la cuenta puede editar la cuenta de usuario miembro y actualizar las restricciones de roles para el usuario afectado a fin de otorgar acceso al nuevo espacio de nombres.
- **Los clones utilizan cubos predeterminados**:
  - Durante una copia de seguridad de la aplicación o una restauración de la aplicación, puede especificar un bloque que se va a utilizar. Debe especificar un bloque predeterminado cuando se clona en clústeres, pero especificar un bloque es opcional cuando se clona dentro del mismo clúster.
  - Cuando se clona en un clúster, la instancia de cloud que contiene el clúster de origen de la operación de clonado debe tener un conjunto de bloques predeterminado.
  - 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.

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 a un espacio de nombres de destino.

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

   - Seleccione **Siguiente**.

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

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

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

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

Resultado

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

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

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 Service admite los siguientes tipos de ganchos de ejecución, según cuándo se puedan ejecutar:

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

Filtros de gancho de ejecución

Al agregar o editar un enlace de ejecución a una aplicación, puede agregar filtros a un enlace de ejecución para gestionar los contenedores que coincidirá el enlace. Los filtros son útiles para aplicaciones que usan la

misma imagen de contenedor en todos los contenedores, pero pueden usar cada imagen para un propósito diferente (como Elasticsearch). Los filtros le permiten crear escenarios donde los enlaces de ejecución se ejecutan en algunos, pero no necesariamente todos los contenedores idénticos. Si crea varios filtros para un único enlace de ejecución, se combinan con un operador y lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

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

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

Notas importantes sobre los enlaces de ejecución personalizados

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

> Debido a que los enlaces de ejecución a menudo reducen o desactivan por completo la funcionalidad de la aplicación con la que se ejecutan, siempre debe intentar minimizar el tiempo que tardan los enlaces de ejecución personalizados.
> Si inicia una operación de copia de seguridad o de instantánea con los enlaces de ejecución asociados pero, a continuación, la cancela, los ganchos pueden ejecutarse si ya se ha iniciado la operación de copia de seguridad o de Snapshot. Esto significa que la lógica utilizada en un enlace de ejecución posterior a la copia de seguridad no puede suponer que la copia de seguridad se ha completado.

- La función de enlaces de ejecución está deshabilitada de forma predeterminada para las nuevas implementaciones de Astra Control.
  - Debe activar la función de enlaces de ejecución antes de poder utilizar los enlaces de ejecución.
  - Los usuarios propietario o administrador pueden habilitar o deshabilitar la función de enlaces de ejecución para todos los usuarios definidos en la cuenta de Astra Control actual. Consulte Active la función de enlaces de ejecución y.. Desactive la función de enlaces de ejecución si desea obtener instrucciones.
  - El estado de habilitación de la función se preserva durante las actualizaciones de Astra Control.
- Un enlace de ejecución debe utilizar una secuencia de comandos para realizar acciones. Muchos enlaces de ejecución pueden hacer referencia al mismo script.
- Astra Control requiere que las secuencias de comandos que utilizan los enlaces de ejecución se escriban en el formato de secuencias de comandos de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Astra Control utiliza la configuración del enlace de ejecución y cualquier criterio coincidente para determinar qué ganchos se aplican a una operación de instantánea, copia de seguridad o restauración.
- Todos los fallos del enlace de ejecución son fallos de software; otros ganchos y la operación de protección de datos se siguen intentando incluso si falla un gancho. Sin embargo, cuando falla un gancho, se registra un suceso de advertencia en el registro de eventos de la página **Activity**.

- Para crear, editar o eliminar enlaces de ejecución, debe ser un usuario con permisos de propietario, administrador o miembro.
- Si un enlace de ejecución tarda más de 25 minutos en ejecutarse, el enlace fallará, creando una entrada de registro de eventos con un código de retorno de "N/A". Se agotará el tiempo de espera de todas las instantáneas afectadas y se marcarán como errores, con una entrada de registro de eventos resultante que tenga en cuenta el tiempo de espera.
- Para las operaciones de protección de datos ad hoc, todos los eventos de enlace se generan y guardan en el registro de eventos de la página **Actividad**. Sin embargo, en el caso de las operaciones de protección de datos programadas, solo se registran los eventos de fallo de enlace en el registro de eventos (los eventos generados por las propias operaciones de protección de datos programadas aún se registran).

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
1	Clonar	N	N	Nuevo	Igual	Y	N	Y
2	Clonar	N	N	Nuevo	Diferente	Y	Y	Y
3	Clonar o restaurar	Y	N	Nuevo	Igual	N	N	Y
4	Clonar o restaurar	N	Y	Nuevo	Igual	N	N	Y
5	Clonar o restaurar	Y	N	Nuevo	Diferente	N	N	Y
6	Clonar o restaurar	N	Y	Nuevo	Diferente	N	N	Y
7	Restaurar	Y	N	Existente	Igual	N	N	Y
8	Restaurar	N	Y	Existente	Igual	N	N	Y
9	Snapshot	N.A.	N.A.	N.A.	N.A.	Y	N.A.	N.A.
10	Backup	N	N.A.	N.A.	N.A.	Y	Y	N.A.
11	Backup	Y	N.A.	N.A.	N.A.	N	N	N.A.

Ejemplos de gancho de ejecución

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

estructurar sus propios enlaces de ejecución personalizados.

Active la función de enlaces de ejecución

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

Pasos

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

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

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

Desactive la función de enlaces de ejecución

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

Pasos

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

Ver los enlaces de ejecución existentes

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

Pasos

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

   Puede ver todos los enlaces de ejecución habilitados o desactivados en la lista resultante. Puede ver el estado de un gancho, cuántos contenedores coinciden, la hora de creación y cuándo se ejecuta (antes o después de la operación). Puede seleccionar la + icono junto al nombre del gancho para expandir la lista de contenedores en los que se ejecutará. Para ver los registros de eventos que rodean los enlaces de

ejecución de esta aplicación, vaya a la ficha **actividad**.

Ver los scripts existentes

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

Pasos

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

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

Agregar un script

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

Pasos

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

Resultado

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

Eliminar un script

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

Pasos

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

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

Cree un enlace de ejecución personalizado

Puedes crear un gancho de ejecución personalizado para una aplicación y añadirlo a Astra Control. Consulte Ejemplos de gancho de ejecución para ejemplos de gancho. Necesita tener permisos de propietario, administrador o miembro para crear enlaces de ejecución.

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

Pasos

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

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

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

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

7. Cuando termine, seleccione **Siguiente**.
8. En el área **Script**, siga uno de estos procedimientos:
   - Agregue un nuevo script.
     i. Seleccione **Agregar**.
     ii. Debe realizar una de las siguientes acciones:
       - Cargue un script personalizado.
         I. Seleccione la opción **cargar archivo**.
         II. Navegue hasta un archivo y cárguelo.
         III. Asigne al script un nombre único.
         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
         V. Seleccione **Guardar script**.
       - Pegar en un script personalizado desde el portapapeles.
         I. Seleccione la opción **Pegar o Tipo**.
         II. Seleccione el campo de texto y pegue el texto del script en el campo.
         III. Asigne al script un nombre único.
         IV. (Opcional) Introduzca cualquier nota que los otros administradores deben conocer sobre el script.
   - Seleccione un script existente de la lista.

     Esto indica al enlace de ejecución que utilice esta secuencia de comandos.
9. Seleccione **Siguiente**.
10. Revise la configuración del gancho de ejecución.
11. Seleccione **Agregar**.

Compruebe el estado de un enlace de ejecución

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

Pasos

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

2. Seleccione la ficha **Protección de datos**.
3. Seleccione **instantáneas** para ver las instantáneas en ejecución, o **copias de seguridad** para ver las copias de seguridad en ejecución.

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

Ver el uso de las secuencias de comandos

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

Pasos

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

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

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

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

Edite un gancho de ejecución

Puede editar un enlace de ejecución si desea cambiar sus atributos, filtros o la secuencia de comandos que utiliza. Necesita tener permisos de propietario, administrador o miembro para editar los enlaces de ejecución.

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para un gancho que desee editar.
4. Seleccione **Editar**.
5. Haga los cambios necesarios, seleccione **Siguiente** después de completar cada sección.
6. Seleccione **Guardar**.

Desactivar un gancho de ejecución

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

Pasos

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

2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea desactivar.
4. Seleccione **Desactivar**.

Eliminar un gancho de ejecución

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

Pasos

1. Seleccione **aplicaciones** y, a continuación, seleccione el nombre de una aplicación administrada.
2. Seleccione la ficha **ganchos de ejecución**.
3. Seleccione el menú Opciones de la columna **acciones** para el gancho que desea eliminar.
4. Seleccione **Eliminar**.
5. En el cuadro de diálogo que aparece, escriba "delete" para confirmar.
6. Seleccione **Sí, elimine el enlace de ejecución**.

Si quiere más información

- "Proyecto Verda GitHub de NetApp"