Proteger las cargas de trabajo de Kubernetes (versión preliminar)

NetApp Backup and Recovery

NetApp
February 23, 2026

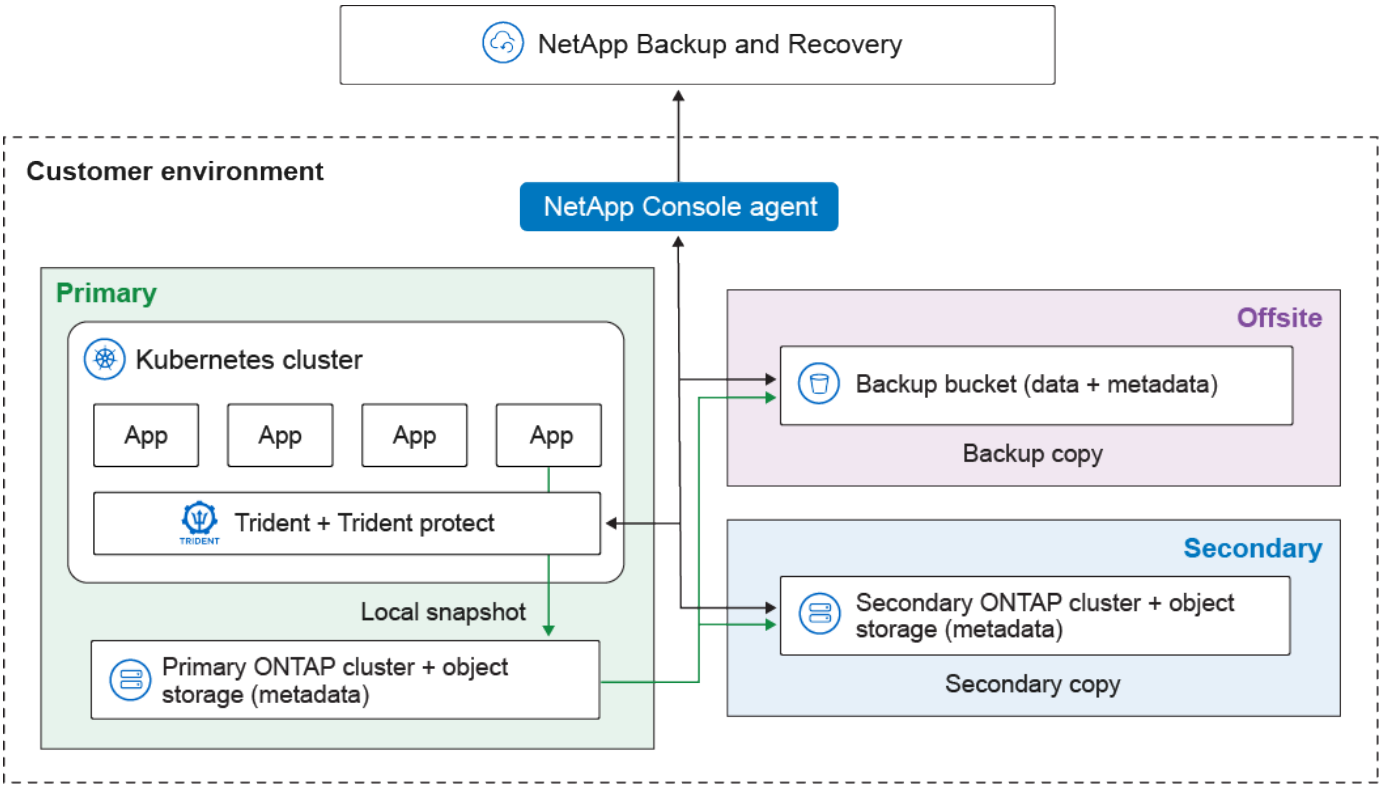
Tabla de contenidos

Proteger las cargas de trabajo de Kubernetes (versión preliminar)

Descripción general de la gestión de cargas de trabajo de Kubernetes

La administración de cargas de trabajo de Kubernetes en NetApp Backup and Recovery le permite descubrir, administrar y proteger sus clústeres y aplicaciones de Kubernetes, todo en un solo lugar. Puede administrar recursos y aplicaciones alojados en sus clústeres de Kubernetes. También puede crear y asociar políticas de protección con sus cargas de trabajo de Kubernetes, todo desde una única interfaz.

El siguiente diagrama muestra los componentes y la arquitectura básica de la copia de seguridad y la recuperación para cargas de trabajo de Kubernetes y cómo se pueden almacenar diferentes copias de sus datos en diferentes ubicaciones:



NetApp Backup and Recovery ofrece los siguientes beneficios para administrar cargas de trabajo de Kubernetes:

- Un único plano de control para proteger aplicaciones que se ejecutan en varios clústeres de Kubernetes. Estas aplicaciones pueden incluir contenedores o máquinas virtuales que se ejecutan en sus clústeres de Kubernetes.
- Integración nativa con NetApp SnapMirror, que permite capacidades de descarga de almacenamiento para todos los flujos de trabajo de respaldo y recuperación.
- Copias de seguridad incrementales permanentes para aplicaciones de Kubernetes, lo que se traduce en objetivos de punto de recuperación (RPO) y objetivos de tiempo de recuperación (RTO) más bajos.

Esta documentación se proporciona como una vista previa de la tecnología. Durante la vista previa, no se recomienda la funcionalidad de Kubernetes para cargas de trabajo de producción. Con esta oferta de vista previa, NetApp se reserva el derecho de modificar los detalles, el contenido y el cronograma de la oferta antes de la disponibilidad general.

Puede realizar las siguientes tareas relacionadas con la gestión de cargas de trabajo de Kubernetes:

- "Descubra las cargas de trabajo de Kubernetes".
- "Administrar clústeres de Kubernetes".
- "Agregar y proteger aplicaciones de Kubernetes".
- "Administrar aplicaciones de Kubernetes".
- "Restaurar aplicaciones de Kubernetes".

Descubra las cargas de trabajo de Kubernetes en NetApp Backup and Recovery

NetApp Backup and Recovery necesita descubrir las cargas de trabajo de Kubernetes antes de protegerlas.

Rol de NetApp Console requerido Superadministrador de backup y recuperación. Conozca más sobre"Roles y privilegios de copia de seguridad y recuperación" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Descubra las cargas de trabajo de Kubernetes

En el inventario de Copia de seguridad y recuperación, descubra las cargas de trabajo de Kubernetes en su entorno. Al agregar una carga de trabajo, se agrega un clúster de Kubernetes a NetApp Backup and Recovery. Luego puede agregar aplicaciones y proteger los recursos del clúster.

Cuando descubres un clúster que está actualmente protegido con Trident Protect, cualquier programación de backup que se haya usado con Trident Protect se desactiva durante el proceso de descubrimiento (las programaciones de backup de Trident Protect no son compatibles con Backup and Recovery). Para proteger las aplicaciones del clúster, "crear una nueva política de protección" o asocia las aplicaciones con una política existente. Luego puedes eliminar las programaciones de backup de Trident Protect si lo necesitas.

Pasos

1. Debe realizar una de las siguientes acciones:
   - Si está descubriendo cargas de trabajo de Kubernetes por primera vez, en NetApp Backup and Recovery, en **Cargas de trabajo**, seleccione el mosaico **Kubernetes**.
   - Si ya ha descubierto cargas de trabajo de Kubernetes, en NetApp Backup and Recovery, seleccione **Inventario** > **Cargas de trabajo** y luego seleccione **Descubrir recursos**.
2. Seleccione el tipo de carga de trabajo **Kubernetes**.
3. Ingrese un nombre de clúster y elija un conector para usar con el clúster.
4. Siga las instrucciones de la línea de comandos que aparecen:
   - Crear un espacio de nombres Trident Protect

- Crear un secreto de Kubernetes
- Agregar un repositorio de Helm
- Instala o actualiza Trident Protect y el conector Trident Protect

  Estos pasos garantizan que NetApp Backup and Recovery pueda interactuar con el clúster.

5. Después de completar los pasos, seleccione **Descubrir**.

   El clúster se agrega al inventario.

6. Seleccione **Ver** en la carga de trabajo de Kubernetes asociada para ver la lista de aplicaciones, clústeres y espacios de nombres para esa carga de trabajo.

Continuar al panel de control de NetApp Backup and Recovery

Siga estos pasos para ver el panel de control de NetApp Backup and Recovery .

1. Desde el menú de la NetApp Console , seleccione **Protección** > **Copia de seguridad y recuperación**.
2. Seleccione un mosaico de carga de trabajo (por ejemplo, Microsoft SQL Server).
3. Desde el menú Copia de seguridad y recuperación, seleccione **Panel de control**.
4. Revisar la salud de la protección de datos. La cantidad de cargas de trabajo en riesgo o protegidas aumenta según las cargas de trabajo recientemente descubiertas, protegidas y respaldadas.

   "Descubra lo que le muestra el Dashboard".

Agregar y proteger aplicaciones de Kubernetes

Agregar y proteger aplicaciones de Kubernetes

NetApp Backup and Recovery le permite descubrir fácilmente sus clústeres de Kubernetes, sin generar ni cargar archivos kubeconfig. Puede conectar clústeres de Kubernetes e instalar el software necesario mediante comandos simples copiados de la interfaz de usuario de la NetApp Console .

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Agregar y proteger una nueva aplicación de Kubernetes

El primer paso para proteger las aplicaciones de Kubernetes es crear una aplicación dentro de NetApp Backup and Recovery. Cuando creas una aplicación, haces que la consola sepa que la aplicación se está ejecutando en el clúster de Kubernetes.

Antes de empezar

Antes de poder agregar y proteger una aplicación de Kubernetes, debe"Descubra las cargas de trabajo de Kubernetes" .

Añade una aplicación usando la interfaz web

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario**.
2. Elija una instancia de Kubernetes y seleccione **Ver** para ver los recursos asociados con esa instancia.
3. Seleccione la pestaña **Aplicaciones**.
4. Seleccione **Crear aplicación**.
5. Introduzca un nombre para la aplicación.
6. Opcionalmente, elija cualquiera de los siguientes campos para buscar los recursos que desea proteger:
   - Clúster asociado
   - Espacios de nombres asociados
   - Tipos de recursos
   - Selectores de etiquetas
7. Opcionalmente, seleccione **Recursos con alcance de clúster** para elegir cualquier recurso con alcance a nivel de clúster. Si los incluye, se añadirán a la aplicación al crearla.
8. Opcionalmente, seleccione **Buscar** para encontrar los recursos según sus criterios de búsqueda.

   La consola no almacena los parámetros ni los resultados de la búsqueda; los parámetros se utilizan para buscar en el clúster de Kubernetes seleccionado recursos que se puedan incluir en la aplicación.

9. La consola muestra una lista de recursos que coinciden con sus criterios de búsqueda.
10. Si la lista contiene los recursos que desea proteger, seleccione **Siguiente**.
11. Opcionalmente, en el área **Política**, elija una política de protección existente para proteger la aplicación o cree una nueva. Si no selecciona ninguna, la aplicación se creará sin política de protección. Puede"añadir una política de protección" más tarde.
12. En el área **Prescripts y postscripts**, habilite y configure cualquier gancho de ejecución de prescript o postscript que desee ejecutar antes o después de las operaciones de respaldo. Para habilitar prescriptos o posscriptos, debe haber creado previamente al menos uno"plantilla de gancho de ejecución" .
13. Seleccione **Crear**.

Resultado

La aplicación se crea y aparece en la lista de aplicaciones en la pestaña **Aplicaciones** del inventario de Kubernetes. La NetApp Console permite proteger la aplicación según su configuración, y usted puede supervisar el progreso en el área **Supervisión** de respaldo y recuperación.

Agrega una aplicación usando un CR

Pasos

1. Crea el archivo CR de la aplicación de destino:
   a. Crea el archivo de recurso personalizado (CR) y ponle un nombre (por ejemplo, `my-app-name.yaml`).

b. Configura los siguientes atributos:

- **metadata.name**: (*Obligatorio*) El nombre del recurso personalizado de la aplicación. Ten en cuenta el nombre que elijas porque otros archivos CR necesarios para las operaciones de protección hacen referencia a este valor.
- **spec.includedNamespaces**: (*Requerido*) Usa el selector de espacio de nombres y de etiqueta para especificar los espacios de nombres y recursos que utiliza la aplicación. El espacio de nombres de la aplicación debe formar parte de esta lista. El selector de etiqueta es opcional y puedes usarlo para filtrar recursos dentro de cada espacio de nombres especificado.
- **spec.includedClusterScopedResources**: (*Opcional*) Usa este atributo para especificar los recursos de ámbito clúster que se incluirán en la definición de la aplicación. Este atributo te permite seleccionar estos recursos según su grupo, versión, tipo y etiquetas.
  - **groupVersionKind**: (*Obligatorio*) especifica el grupo de API, la versión y el tipo del recurso con alcance de clúster.
  - **labelSelector**: (*Opcional*) Filtra los recursos con ámbito de clúster según sus etiquetas.

c. Configura las siguientes anotaciones, si es necesario:

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**: (*Opcional*) Esta anotación solo es aplicable a aplicaciones definidas a partir de máquinas virtuales, como en entornos KubeVirt, donde se producen congelaciones del sistema de archivos antes de las instantáneas. Especifica si esta aplicación puede escribir en el sistema de archivos durante una instantánea. Si se establece en true, la aplicación ignora la configuración global y puede escribir en el sistema de archivos durante una instantánea. Si se establece en false, la aplicación ignora la configuración global y el sistema de archivos se congela durante una instantánea. Si se especifica pero la aplicación no tiene máquinas virtuales en la definición de la aplicación, se ignora la anotación. Si no se especifica, la aplicación sigue la "configuración global de congelación del sistema de archivos".
- **protect.trident.netapp.io/protection-command**: (*Opcional*) Usa esta anotación para indicar a Backup and Recovery que proteja o deje de proteger la aplicación. Los valores posibles son `protect` o `unprotect`.
- **protect.trident.netapp.io/protection-policy-name**: (*Opcional*) Usa esta anotación para especificar el nombre de la política de protección de NetApp Backup and Recovery que quieres usar para proteger esta aplicación. Esta política de protección ya debe existir en NetApp Backup and Recovery.

Si necesitas aplicar esta anotación después de que ya se haya creado una aplicación, puedes usar el siguiente comando:

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
Ejemplo de YAML:

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. (*Opcional*) agrega filtrado que incluya o excluya recursos marcados con etiquetas específicas:

   - **resourceFilter.resourceSelectionCriteria**: (Obligatorio para el filtrado) Usa `Include` o `Exclude` para incluir o excluir un recurso definido en resourceMatchers. Agrega los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:

     - **resourceFilter.resourceMatchers**: una matriz de objetos resourceMatcher. Si defines múltiples elementos en esta matriz, coinciden como una operación OR y los campos dentro de cada elemento (group, kind, version) coinciden como una operación AND.
       - **resourceMatchers[].group**: (*Opcional*) Grupo del recurso a filtrar.
       - **resourceMatchers[].kind**: (*Opcional*) Tipo del recurso a filtrar.
       - **resourceMatchers[].version**: (*Opcional*) Versión del recurso a filtrar.

- **resourceMatchers[].names**: (*Opcional*) Nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
- **resourceMatchers[].namespaces**: (*Opcional*) Espacios de nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
- **resourceMatchers[].labelSelectors**: (*opcional*) Cadena de selector de etiqueta en el campo metadata.name de Kubernetes del recurso, como se define en "Documentación de Kubernetes". Por ejemplo: `"trident.netapp.io/os=linux"`.

> Cuando se utilizan tanto `resourceFilter` como `labelSelector`, `resourceFilter` se ejecuta primero y luego `labelSelector` se aplica a los recursos resultantes.

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. Después de crear la CR de la aplicación para que coincida con tu entorno, aplica la CR. Por ejemplo:

```
kubectl apply -f my-app-name.yaml
```

Haz backup de aplicaciones Kubernetes ahora usando la interfaz web de Backup and Recovery

NetApp Backup and Recovery te permite hacer backups manuales de aplicaciones Kubernetes usando la interfaz web.

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp

Console para todos los servicios" .

Haz una copia de seguridad de una aplicación de Kubernetes ahora usando la interfaz web

Cree manualmente una copia de seguridad de una aplicación de Kubernetes para establecer una línea de base para futuras copias de seguridad e instantáneas, o para garantizar que los datos más recientes estén protegidos.

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario**.
2. Elija una instancia de Kubernetes y seleccione **Ver** para ver los recursos asociados con esa instancia.
3. Seleccione la pestaña **Aplicaciones**.
4. En la lista de aplicaciones, elija una aplicación que desee respaldar y seleccione el menú Acciones asociado.
5. Seleccione **Hacer copia de seguridad ahora**.
6. Asegúrese de que esté seleccionado el nombre de aplicación correcto.
7. Seleccione **Hacer copia de seguridad**.

Resultado

La consola crea una copia de seguridad de la aplicación y muestra el progreso en el área **Monitoreo** de Copia de seguridad y recuperación. La copia de seguridad se crea según la política de protección asociada a la aplicación.

Haz backup de aplicaciones Kubernetes ahora usando recursos personalizados en Backup and Recovery

NetApp Backup and Recovery te permite hacer backups manuales de aplicaciones Kubernetes usando recursos personalizados (CRs).

Haz una copia de seguridad de una aplicación de Kubernetes ahora usando recursos personalizados

Cree manualmente una copia de seguridad de una aplicación de Kubernetes para establecer una línea de base para futuras copias de seguridad e instantáneas, o para garantizar que los datos más recientes estén protegidos.

> Los recursos con ámbito de clúster se incluyen en un backup, snapshot o clon si se hace referencia a ellos explícitamente en la definición de la aplicación o si tienen referencias a cualquiera de los espacios de nombres de la aplicación.

Antes de empezar

Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de backup s3 de larga duración. Si el token caduca durante la operación de backup, la operación puede fallar.

- Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
- Consulta "Documentación de AWS IAM" para más información sobre las credenciales con los recursos de AWS.

Crea una instantánea local usando un recurso personalizado

Para crear una instantánea de tu aplicación Kubernetes y guardarla localmente, usa el recurso personalizado Snapshot con atributos específicos.

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale el nombre `local-snapshot-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.applicationRef**: el nombre de Kubernetes de la aplicación para hacer snapshot.
   - **spec.appVaultRef**: (*Required*) El nombre de AppVault donde se debe almacenar el contenido de la instantánea (metadatos).
   - **spec.reclaimPolicy**: (*opcional*) Define lo que pasa con la AppArchive de una instantánea cuando se elimina el CR de la instantánea. Esto significa que incluso cuando se establece en `Retain`, la instantánea se eliminará. Opciones válidas:
     - `Retain` (predeterminado)
     - `Delete`

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: Snapshot
     metadata:
       namespace: my-app-namespace
       name: local-snapshot-cr
     spec:
       applicationRef: my-application
       appVaultRef: appvault-name
       reclaimPolicy: Retain
     ```
3. Después de rellenar el archivo `local-snapshot-cr.yaml` con los valores correctos, aplica la CR:

   ```
   kubectl apply -f local-snapshot-cr.yaml
   ```

Haz un backup de una aplicación en un almacén de objetos usando un recurso personalizado

Crea un CR de backup con atributos específicos para hacer backup de tu aplicación en un almacén de objetos.

Pasos

1. Crea el archivo de recurso personalizado (CR) y ponle el nombre `object-store-backup-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.

- **spec.applicationRef**: (*Required*) el nombre de Kubernetes de la aplicación que quieres respaldar.
- **spec.appVaultRef**: (*Requerido, mutuamente excluyente con spec.appVaultTargetsRef*) Si usas el mismo bucket para guardar la instantánea y el backup, este es el nombre de AppVault donde se debe almacenar el contenido del backup.
- **spec.appVaultTargetsRef**: (*Requerido, mutuamente excluyente con spec.appVaultRef*) Si usas diferentes buckets para almacenar el snapshot y el backup, este es el nombre del AppVault donde se debe almacenar el contenido del backup.
- **spec.dataMover**: (*Opcional*) Una cadena que indica qué herramienta de backup usar para la operación de backup. El valor distingue mayúsculas de minúsculas y debe ser `CBS`.
- **spec.reclaimPolicy**: (*Opcional*) Define qué pasa con el contenido del backup (metadatos/datos del volumen) cuando se elimina el Backup CR. Valores posibles:
  - `Delete`
  - `Retain` (predeterminado)
- **spec.cleanupSnapshot**: (*Obligatorio*) Garantiza que la instantánea temporal creada por el CR de copia de seguridad no se elimine después de que se complete la operación de copia de seguridad. Valor recomendado: `false`.

  Ejemplo de YAML cuando usas el mismo bucket para guardar la instantánea y el backup:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

  Ejemplo de YAML cuando usas diferentes buckets para almacenar la instantánea y el backup:

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. Después de rellenar el archivo `object-store-backup-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f object-store-backup-cr.yaml
```

Crea un backup de fanout 3-2-1 usando un recurso personalizado

La copia de seguridad mediante una arquitectura 3-2-1 fanout copia un backup en almacenamiento secundario y también en un almacén de objetos. Para crear un backup 3-2-1 fanout, crea un Backup CR con atributos específicos.

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale el nombre `3-2-1-fanout-backup-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.applicationRef**: (*Required*) el nombre de Kubernetes de la aplicación que quieres respaldar.
   - **spec.appVaultTargetsRef**: (*Required*) El nombre de AppVault donde se debe almacenar el contenido del backup.
   - **spec.dataMover**: (*Opcional*) Una cadena que indica qué herramienta de backup usar para la operación de backup. El valor distingue mayúsculas de minúsculas y debe ser `CBS`.
   - **spec.reclaimPolicy**: (*Opcional*) Define qué pasa con el contenido del backup (metadatos/datos del volumen) cuando se elimina el Backup CR. Valores posibles:
     - `Delete`
     - `Retain` (predeterminado)
   - **spec.cleanupSnapshot**: (*Obligatorio*) Garantiza que la instantánea temporal creada por el CR de copia de seguridad no se elimine después de que se complete la operación de copia de seguridad. Valor recomendado: `false`.
   - **spec.replicateSnapshot**: (*Requerido*) Indica a Backup and Recovery que replique la instantánea en el almacenamiento secundario. Valor requerido: `true`.

- **spec.replicateSnapshotReclaimPolicy**: (*Opcional*) Define qué pasa con la instantánea replicada cuando se elimina. Posibles valores:
  - `Delete`
  - `Retain` (predeterminado)

    Ejemplo de YAML:

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. Después de rellenar el archivo `3-2-1-fanout-backup-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

Anotaciones de backup compatibles

La siguiente tabla describe las anotaciones que puedes usar al crear un backup CR.

Anotación	Tipo	Descripción	Valor predeterminado
protect.trident.netapp.io/backup-completo	cadena	Especifica si una copia de seguridad debe ser no incremental. Establece en `true` para crear una copia de seguridad no incremental. Es buena práctica hacer un backup completo periódicamente y luego hacer backups incrementales entre los backups completos para minimizar el riesgo asociado con las restauraciones.	"false"
protect.trident.netapp.io/snapshot-completion-timeout	cadena	El tiempo máximo permitido para que se complete toda la operación de instantánea.	"60m"

Anotación	Tipo	Descripción	Valor predeterminado
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	cadena	El tiempo máximo permitido para que las instantáneas de volumen alcancen el estado listo para usar.	"30m"
protect.trident.netapp.io/volume-snapshots-created-timeout	cadena	El tiempo máximo permitido para que se creen instantáneas de volumen.	"5m"
protect.trident.netapp.io/pvc-bind-timeout-sec	cadena	Tiempo máximo (en segundos) para esperar a que cualquier PersistentVolumeClaims (PVCs) recién creado alcance la fase `Bound` antes de que la operación falle.	"1200" (20 minutos)

Restaurar aplicaciones de Kubernetes

Restaura aplicaciones de Kubernetes usando la interfaz web

NetApp Backup and Recovery le permite restaurar aplicaciones que haya protegido con una política de protección. Para restaurar una aplicación, esta debe tener al menos un punto de restauración disponible. Un punto de restauración puede ser la instantánea local o la copia de seguridad en el almacén de objetos (o ambas). Puede restaurar una aplicación utilizando el archivo local, secundario o del almacén de objetos.

Antes de empezar

Si vas a restaurar una aplicación que se respaldó usando Trident Protect, asegúrate de que Trident Protect esté instalado tanto en el clúster de origen como en el clúster de destino.

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Pasos

1. En el menú NetApp Backup and Recovery, selecciona **Restaurar**.
2. Elige una aplicación de Kubernetes de la lista y selecciona **Ver y restaurar** para esa aplicación.

   Aparece la lista de puntos de restauración.

3. Selecciona el botón **Restaurar** para el punto de restauración que quieras usar.

Configuración general

1. Elige la ubicación de origen desde la que quieres restaurar.
2. Seleccione el clúster de destino de la lista **Clúster**.

> Restaurar una instantánea local creada por Trident Protect en un clúster diferente no es compatible en este momento.

3. Elige restaurar en los espacios de nombres originales o en nuevos espacios de nombres.
4. Si elegiste restaurar en nuevos espacios de nombres, introduce el espacio o los espacios de nombres de destino que vas a usar.
5. Seleccione **Siguiente**.

Selección de recursos

1. Elija si desea restaurar todos los recursos asociados con la aplicación o utilizar un filtro para seleccionar recursos específicos para restaurar:

Restaurar todos los recursos

1. Seleccione **Restaurar todos los recursos**.
2. Seleccione **Siguiente**.

Restaurar recursos específicos

1. Seleccione **Recursos selectivos**.
2. Elija el comportamiento del filtro de recursos. Si elige **Incluir**, se restaurarán los recursos que seleccione. Si elige **Excluir**, los recursos que seleccione no se restaurarán.
3. Seleccione **Agregar reglas** para agregar reglas que definan filtros para seleccionar recursos. Necesita al menos una regla para filtrar recursos.

   Cada regla puede filtrar según criterios como el espacio de nombres del recurso, las etiquetas, el grupo, la versión y el tipo.
4. Seleccione **Guardar** para guardar cada regla.
5. Cuando haya agregado todas las reglas que necesita, seleccione **Buscar** para ver los recursos disponibles en el archivo de respaldo que coinciden con sus criterios de filtro.

   Los recursos que se muestran son los recursos que existen actualmente en el clúster.
6. Cuando esté satisfecho con los resultados, seleccione **Siguiente**.

Configuración de destino

1. Expande la sección **Configuración de destino** y elige restaurar a la clase de almacenamiento predeterminada, a una clase de almacenamiento diferente o, si estás restaurando a un clúster diferente, asignar las clases de almacenamiento al clúster de destino.
2. Si elegiste restaurar en una clase de almacenamiento diferente, selecciona una clase de almacenamiento de destino que coincida con cada clase de almacenamiento de origen.
3. Opcionalmente, si estás restaurando una copia de seguridad o una instantánea que se hizo usando Trident Protect, revisa los detalles del AppVault usado como bucket de almacenamiento para la operación de restauración. Si hay un cambio en tu entorno o en el estado de AppVault, selecciona **Sync App Vault** para actualizar los detalles.

   Si necesitas crear un AppVault en un clúster de Kubernetes para facilitar la restauración de una copia de seguridad o instantánea creada usando Trident Protect, consulta "Usa los objetos de Trident Protect AppVault para gestionar buckets".

4. Opcionalmente, expande la sección **Restore scripts** y habilita la opción **Postscript** para elegir una plantilla de hook de ejecución que se ejecutará después de que la operación de restauración haya terminado. Si lo necesitas, introduce cualquier argumento que el script necesite y añade selectores de etiquetas para filtrar recursos según las etiquetas de los recursos.
5. Seleccione **Restaurar**.

Restaura aplicaciones Kubernetes usando un recurso personalizado

Puedes usar recursos personalizados para restaurar tus aplicaciones desde una instantánea o copia de seguridad. Restaurar desde una instantánea existente será más rápido al restaurar la aplicación en el mismo clúster.

- Cuando restauras una aplicación, todos los ganchos de ejecución configurados para la aplicación se restauran junto con la app. Si hay un gancho de ejecución posterior a la restauración, se ejecuta automáticamente como parte de la operación de restauración.
- La restauración desde una copia de seguridad a un espacio de nombres diferente o al espacio de nombres original es compatible para los volúmenes qtree. Sin embargo, restaurar desde una instantánea a un espacio de nombres diferente o al espacio de nombres original no es compatible para los volúmenes qtree.
- Puedes usar la configuración avanzada para personalizar las operaciones de restauración. Para saber más, consulta "Usa la configuración avanzada de restauración de recursos personalizada".

Restaura una copia de seguridad en un espacio de nombres diferente

Cuando restauras una copia de seguridad en un espacio de nombres diferente usando un CR de BackupRestore, Backup and Recovery restaura la aplicación en un nuevo espacio de nombres y crea un CR de aplicación para la aplicación restaurada. Para proteger la aplicación restaurada, crea copias de seguridad o instantáneas bajo demanda, o establece una programación de protección.

- Restaurar una copia de seguridad en un espacio de nombres diferente con recursos existentes no alterará ningún recurso que comparta nombres con los de la copia de seguridad. Para restaurar todos los recursos de la copia de seguridad, elimina y vuelve a crear el espacio de nombres de destino o restaura la copia de seguridad en un nuevo espacio de nombres.
- Cuando uses un CR para restaurar en un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR. NetApp Backup and Recovery crea automáticamente espacios de nombres solo cuando usas la CLI.

Antes de empezar

Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de restauración s3 de larga duración. Si el token caduca durante la operación de restauración, la operación puede fallar.

- Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
- Consulta "Documentación de AWS IAM" para más información sobre las credenciales con los recursos de AWS.

Cuando restauras copias de seguridad usando Kopia como el traslador de datos, puedes especificar opcionalmente anotaciones en el CR para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta el "Documentación de Kopia" para más información sobre las opciones que puedes configurar.

Pasos

1. Crea el archivo de recurso personalizado (CR) y ponle el nombre `trident-protect-backup-restore-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.appArchivePath**: la ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Puedes usar el siguiente comando para encontrar esta ruta:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Required*) el nombre del AppVault donde se almacena el contenido de la copia de seguridad.
   - **spec.namespaceMapping**: la asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplaza `my-source-namespace` y `my-destination-namespace` con información de tu entorno.

     ```
     apiVersion: protect.trident.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: my-cr-name
       namespace: my-destination-namespace
     spec:
       appArchivePath: my-backup-path
       appVaultRef: appvault-name
       namespaceMapping: [{"source": "my-source-namespace", "destination":
     "my-destination-namespace"}]
     ```

3. (*Opcional*) Si necesitas seleccionar solo ciertos recursos de la aplicación para restaurar, añade un filtrado que incluya o excluya recursos marcados con etiquetas concretas:

   Trident Protect selecciona algunos recursos automáticamente debido a su relación con los recursos que tú seleccionas. Por ejemplo, si seleccionas un recurso de reclamación de volumen persistente y tiene un pod asociado, Trident Protect también restaurará el pod asociado.

   - **resourceFilter.resourceSelectionCriteria**: (Obligatorio para el filtrado) Usa `Include` o `Exclude` para incluir o excluir un recurso definido en resourceMatchers. Agrega los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:

- **resourceFilter.resourceMatchers**: una matriz de objetos resourceMatcher. Si defines múltiples elementos en esta matriz, coinciden como una operación OR y los campos dentro de cada elemento (group, kind, version) coinciden como una operación AND.
  - **resourceMatchers[].group**: (*Opcional*) Grupo del recurso a filtrar.
  - **resourceMatchers[].kind**: (*Opcional*) Tipo del recurso a filtrar.
  - **resourceMatchers[].version**: (*Opcional*) Versión del recurso a filtrar.
  - **resourceMatchers[].names**: (*Opcional*) Nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
  - **resourceMatchers[].namespaces**: (*Opcional*) Espacios de nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
  - **resourceMatchers[].labelSelectors**: (*opcional*) Cadena de selector de etiqueta en el campo metadata.name de Kubernetes del recurso, como se define en "Documentación de Kubernetes". Por ejemplo: `"trident.netapp.io/os=linux"`.

    Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar el archivo `trident-protect-backup-restore-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaura una copia de seguridad en el espacio de nombres original

Puedes restaurar una copia de seguridad en el espacio de nombres original en cualquier momento.

Antes de empezar

Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de restauración s3 de larga duración. Si el token caduca durante la operación de restauración, la operación

puede fallar.

- Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
- Consulta "Documentación de AWS IAM" para más información sobre las credenciales con los recursos de AWS.

> Cuando restauras copias de seguridad usando Kopia como el traslador de datos, puedes especificar opcionalmente anotaciones en el CR para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta el "Documentación de Kopia" para más información sobre las opciones que puedes configurar.

Pasos

1. Crea el archivo de recurso personalizado (CR) y ponle el nombre `trident-protect-backup-ipr-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.appArchivePath**: la ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Puedes usar el siguiente comando para encontrar esta ruta:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**: (*Required*) el nombre del AppVault donde se almacena el contenido de la copia de seguridad.

     Por ejemplo:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. (*Opcional*) Si necesitas seleccionar solo ciertos recursos de la aplicación para restaurar, añade un filtrado que incluya o excluya recursos marcados con etiquetas concretas:

> Trident Protect selecciona algunos recursos automáticamente debido a su relación con los recursos que tú seleccionas. Por ejemplo, si seleccionas un recurso de reclamación de volumen persistente y tiene un pod asociado, Trident Protect también restaurará el pod asociado.

- **resourceFilter.resourceSelectionCriteria**: (Obligatorio para el filtrado) Usa `Include` o `Exclude` para incluir o excluir un recurso definido en resourceMatchers. Agrega los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
  - **resourceFilter.resourceMatchers**: una matriz de objetos resourceMatcher. Si defines múltiples elementos en esta matriz, coinciden como una operación OR y los campos dentro de cada elemento (group, kind, version) coinciden como una operación AND.
    - **resourceMatchers[].group**: (*Opcional*) Grupo del recurso a filtrar.
    - **resourceMatchers[].kind**: (*Opcional*) Tipo del recurso a filtrar.
    - **resourceMatchers[].version**: (*Opcional*) Versión del recurso a filtrar.
    - **resourceMatchers[].names**: (*Opcional*) Nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
    - **resourceMatchers[].namespaces**: (*Opcional*) Espacios de nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
    - **resourceMatchers[].labelSelectors**: (*opcional*) Cadena de selector de etiqueta en el campo metadata.name de Kubernetes del recurso, como se define en "Documentación de Kubernetes". Por ejemplo: `"trident.netapp.io/os=linux"`.

      Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar el archivo `trident-protect-backup-ipr-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

Restaura una copia de seguridad en un clúster diferente

Puedes restaurar una copia de seguridad en un clúster diferente si hay algún problema con el clúster original.

- Cuando restauras copias de seguridad usando Kopia como el traslador de datos, puedes especificar opcionalmente anotaciones en el CR para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta el "Documentación de Kopia" para más información sobre las opciones que puedes configurar.
- Cuando usas un CR para restaurar en un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR.

Antes de empezar

Asegúrate de que se cumplen los siguientes requisitos previos:

- El clúster de destino tiene Trident Protect instalado.
- El clúster de destino tiene acceso a la ruta del bucket de la misma AppVault que el clúster de origen, donde se almacena la copia de seguridad.
- Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de restauración de larga duración. Si el token caduca durante la operación de restauración, la operación puede fallar.
  - Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
  - Consulta "Documentación de AWS" para más información sobre las credenciales con los recursos de AWS.

Pasos

1. Comprueba la disponibilidad de AppVault CR en el clúster de destino usando el complemento CLI de Trident Protect:

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

Asegúrate de que el espacio de nombres previsto para la restauración de la aplicación existe en el clúster de destino.

2. Ver el contenido de la copia de seguridad de la AppVault disponible desde el clúster de destino:

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

Al ejecutar este comando se muestran las copias de seguridad disponibles en el AppVault, incluidos sus clústeres de origen, los nombres de las aplicaciones correspondientes, las marcas de tiempo y las rutas de archivo.

Ejemplo de salida:

```
+------------+----------+--------+-----------------
+-------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |        TIMESTAMP
|    PATH     |
+------------+----------+--------+-----------------
+-------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+------------+----------+--------+-----------------
+-------------------------+-------------+
```

3. Restaura la aplicación en el clúster de destino usando el nombre AppVault y la ruta de archivo:
4. Crea el archivo de recurso personalizado (CR) y ponle el nombre `trident-protect-backup-restore-cr.yaml`.
5. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.appVaultRef**: (*Required*) el nombre del AppVault donde se almacena el contenido de la copia de seguridad.
   - **spec.appArchivePath**: la ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Puedes usar el siguiente comando para encontrar esta ruta:

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

     Si BackupRestore CR no está disponible, puedes usar el comando mencionado en el paso 2 para ver el contenido de la copia de seguridad.

   - **spec.namespaceMapping**: la asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplaza `my-source-namespace` y `my-destination-namespace` con información de tu entorno.

     Por ejemplo:

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. Después de rellenar el archivo `trident-protect-backup-restore-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

Restaura una instantánea en un espacio de nombres diferente

Puedes restaurar datos de una instantánea usando un archivo de recurso personalizado (CR) ya sea en un espacio de nombres diferente o en el espacio de nombres de origen original. Cuando restauras una instantánea en un espacio de nombres diferente usando un CR de SnapshotRestore, Backup and Recovery restaura la aplicación en un nuevo espacio de nombres y crea un CR de aplicación para la aplicación restaurada. Para proteger la aplicación restaurada, crea copias de seguridad o instantáneas bajo demanda, o establece una programación de protección.

- SnapshotRestore admite el atributo `spec.storageClassMapping`, pero solo cuando las clases de almacenamiento de origen y destino usan el mismo backend de almacenamiento. Si intentas restaurar en un `StorageClass` que usa un backend de almacenamiento diferente, la operación de restauración fallará.
- Cuando usas un CR para restaurar en un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR.

Antes de empezar

Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de restauración s3 de larga duración. Si el token caduca durante la operación de restauración, la operación puede fallar.

- Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
- Consulta "Documentación de AWS IAM" para más información sobre las credenciales con los recursos de AWS.

Pasos

1. Crea el archivo de recurso personalizado (CR) y ponle el nombre `trident-protect-snapshot-restore-cr.yaml`.
2. En el archivo que creaste, configura los siguientes atributos:

- **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
- **spec.appVaultRef**: (*Required*) El nombre de AppVault donde se almacenan los contenidos de la instantánea.
- **spec.appArchivePath**: la ruta dentro de AppVault donde se almacena el contenido de la instantánea. Puedes usar el siguiente comando para encontrar esta ruta:

```
kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.namespaceMapping**: la asignación del espacio de nombres de origen de la operación de restauración al espacio de nombres de destino. Reemplaza `my-source-namespace` y `my-destination-namespace` con información de tu entorno.

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. (*Opcional*) Si necesitas seleccionar solo ciertos recursos de la aplicación para restaurar, añade un filtrado que incluya o excluya recursos marcados con etiquetas concretas:

> Trident Protect selecciona algunos recursos automáticamente debido a su relación con los recursos que tú seleccionas. Por ejemplo, si seleccionas un recurso de reclamación de volumen persistente y tiene un pod asociado, Trident Protect también restaurará el pod asociado.

- **resourceFilter.resourceSelectionCriteria**: (Obligatorio para el filtrado) Usa `Include` o `Exclude` para incluir o excluir un recurso definido en resourceMatchers. Agrega los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
  - **resourceFilter.resourceMatchers**: una matriz de objetos resourceMatcher. Si defines múltiples elementos en esta matriz, coinciden como una operación OR y los campos dentro de cada elemento (group, kind, version) coinciden como una operación AND.
    - **resourceMatchers[].group**: (*Opcional*) Grupo del recurso a filtrar.
    - **resourceMatchers[].kind**: (*Opcional*) Tipo del recurso a filtrar.
    - **resourceMatchers[].version**: (*Opcional*) Versión del recurso a filtrar.
    - **resourceMatchers[].names**: (*Opcional*) Nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.

- **resourceMatchers[].namespaces**: (*Opcional*) Espacios de nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
- **resourceMatchers[].labelSelectors**: (*opcional*) Cadena de selector de etiqueta en el campo metadata.name de Kubernetes del recurso, como se define en "Documentación de Kubernetes". Por ejemplo: `"trident.netapp.io/os=linux"`.

  Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar el archivo `trident-protect-snapshot-restore-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

Restaura una instantánea al espacio de nombres original

Puedes restaurar una instantánea al espacio de nombres original en cualquier momento.

Antes de empezar

Asegúrate de que la caducidad del token de sesión de AWS sea suficiente para cualquier operación de restauración s3 de larga duración. Si el token caduca durante la operación de restauración, la operación puede fallar.

- Consulta "Documentación de la API de AWS" para más información sobre cómo comprobar la expiración del token de sesión actual.
- Consulta "Documentación de AWS IAM" para más información sobre las credenciales con los recursos de AWS.

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale el nombre `trident-protect-snapshot-`

`ipr-cr.yaml`.

2. En el archivo que creaste, configura los siguientes atributos:
   - **metadata.name**: (*Required*) El nombre de este recurso personalizado; elige un nombre único y sensato para tu entorno.
   - **spec.appVaultRef**: (*Required*) El nombre de AppVault donde se almacenan los contenidos de la instantánea.
   - **spec.appArchivePath**: la ruta dentro de AppVault donde se almacena el contenido de la instantánea. Puedes usar el siguiente comando para encontrar esta ruta:

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
```

3. (*Opcional*) Si necesitas seleccionar solo ciertos recursos de la aplicación para restaurar, añade un filtrado que incluya o excluya recursos marcados con etiquetas concretas:

> Trident Protect selecciona algunos recursos automáticamente debido a su relación con los recursos que tú seleccionas. Por ejemplo, si seleccionas un recurso de reclamación de volumen persistente y tiene un pod asociado, Trident Protect también restaurará el pod asociado.

   - **resourceFilter.resourceSelectionCriteria**: (Obligatorio para el filtrado) Usa `Include` o `Exclude` para incluir o excluir un recurso definido en resourceMatchers. Agrega los siguientes parámetros resourceMatchers para definir los recursos que se van a incluir o excluir:
     - **resourceFilter.resourceMatchers**: una matriz de objetos resourceMatcher. Si defines múltiples elementos en esta matriz, coinciden como una operación OR y los campos dentro de cada elemento (group, kind, version) coinciden como una operación AND.
       - **resourceMatchers[].group**: (*Opcional*) Grupo del recurso a filtrar.
       - **resourceMatchers[].kind**: (*Opcional*) Tipo del recurso a filtrar.
       - **resourceMatchers[].version**: (*Opcional*) Versión del recurso a filtrar.
       - **resourceMatchers[].names**: (*Opcional*) Nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
       - **resourceMatchers[].namespaces**: (*Opcional*) Espacios de nombres en el campo metadata.name de Kubernetes del recurso que se va a filtrar.
       - **resourceMatchers[].labelSelectors**: (*opcional*) Cadena de selector de etiqueta en el campo metadata.name de Kubernetes del recurso, como se define en "Documentación de

Kubernetes". Por ejemplo: `"trident.netapp.io/os=linux"`.

Por ejemplo:

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. Después de rellenar el archivo `trident-protect-snapshot-ipr-cr.yaml` con los valores correctos, aplica la CR:

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

Usa la configuración avanzada de restauración de recursos personalizada

Puedes personalizar las operaciones de restauración usando configuraciones avanzadas como anotaciones, configuración del espacio de nombres y opciones de almacenamiento para cumplir con tus requisitos específicos.

Anotaciones y etiquetas de namespace durante las operaciones de restauración y conmutación por error

Durante las operaciones de restauración y conmutación por error, las etiquetas y anotaciones en el espacio de nombres de destino se hacen coincidir con las etiquetas y anotaciones en el espacio de nombres de origen. Las etiquetas o anotaciones del espacio de nombres de origen que no existen en el espacio de nombres de destino se añaden, y cualquier etiqueta o anotación que ya exista se sobrescribe para que coincida con el valor del espacio de nombres de origen. Las etiquetas o anotaciones que existen solo en el espacio de nombres de destino permanecen sin cambios.

Si usas Red Hat OpenShift, es importante que notes el papel fundamental de las anotaciones de espacios de nombres en entornos OpenShift. Las anotaciones de espacios de nombres aseguran que los pods restaurados sigan los permisos y configuraciones de seguridad apropiados definidos por las restricciones de contexto de seguridad (SCC) de OpenShift y puedan acceder a los volúmenes sin problemas de permisos. Para más información, consulta el "OpenShift documentación de restricciones de contexto de seguridad".

Puedes evitar que se sobrescriban anotaciones específicas en el espacio de nombres de destino configurando la variable de entorno de Kubernetes `RESTORE_SKIP_NAMESPACE_ANNOTATIONS` antes de realizar la restauración o la conmutación por error. Por ejemplo:

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

Al realizar una operación de restauración o conmutación por error, las anotaciones y etiquetas de espacios de nombres especificadas en `restoreSkipNamespaceAnnotations` y `restoreSkipNamespaceLabels` se excluyen de la operación de restauración o conmutación por error. Asegúrate de que estos ajustes estén configurados durante la instalación inicial de Helm. Para saber más, consulta "Configura los ajustes adicionales del helm chart de Trident Protect".

Si instalaste la aplicación de origen usando Helm con la `--create-namespace` flag, se da un tratamiento especial a la clave de etiqueta `name`. Durante el proceso de restauración o conmutación por error, Trident Protect copia esta etiqueta al espacio de nombres de destino, pero actualiza el valor al valor del espacio de nombres de destino si el valor del origen coincide con el espacio de nombres de origen. Si este valor no coincide con el espacio de nombres de origen, se copia al espacio de nombres de destino sin cambios.

Ejemplo

El siguiente ejemplo presenta un espacio de nombres de origen y uno de destino, cada uno con anotaciones y etiquetas diferentes. Puedes ver el estado del espacio de nombres de destino antes y después de la operación, y cómo se combinan o sobrescriben las anotaciones y etiquetas en el espacio de nombres de destino.

Antes de la operación de restauración o conmutación por error

La siguiente tabla ilustra el estado de los espacios de nombres de origen y destino de ejemplo antes de la operación de restauración o conmutación por error:

Espacio de nombres	Anotaciones	Etiquetas
Namespace ns-1 (fuente)	• annotation.one/key: "valoractualizado" • annotation.two/key: "true"	• entorno=producción • compliance=hipaa • name=ns-1

Espacio de nombres	Anotaciones	Etiquetas
Namespace ns-2 (destino)	• annotation.one/key: "true" • annotation.three/key: "false"	• role=database

Después de la operación de restauración

La siguiente tabla ilustra el estado del espacio de nombres de destino de ejemplo después de la operación de restauración o conmutación por error. Se han añadido algunas claves, se han sobrescrito otras y la etiqueta `name` se ha actualizado para que coincida con el espacio de nombres de destino:

Espacio de nombres	Anotaciones	Etiquetas
Namespace ns-2 (destino)	• annotation.one/key: "valoractualizado" • annotation.two/key: "true" • annotation.three/key: "false"	• name=ns-2 • compliance=hipaa • entorno=producción • role=database

Campos compatibles

Esta sección describe los campos adicionales disponibles para las operaciones de restauración.

Asignación de clases de almacenamiento

El atributo `spec.storageClassMapping` define una asignación de una clase de almacenamiento presente en la aplicación de origen a una nueva clase de almacenamiento en el clúster de destino. Puedes usar esto cuando migres aplicaciones entre clústeres con diferentes clases de almacenamiento o cuando cambies el backend de almacenamiento para operaciones de BackupRestore.

Ejemplo:

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

Anotaciones compatibles

En esta sección se enumeran las anotaciones admitidas para configurar diversos comportamientos en el sistema. Si el usuario no establece explícitamente una anotación, el sistema usará el valor predeterminado.

Anotación	Tipo	Descripción	Valor predeterminado
protect.trident.netapp.io/data-mover-timeout-sec	cadena	El tiempo máximo (en segundos) permitido para que la operación de movimiento de datos se quede en pausa.	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	cadena	El límite de tamaño máximo (en megabytes) para la caché de contenido de Kopia.	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	cadena	Tiempo máximo (en segundos) de espera para que cualquier PersistentVolumeClaims (PVCs) recién creado alcance la `Bound` fase antes de que la operación falle. Aplica a todos los tipos de CR de restauración (BackupRestore, BackupInplaceRestore, SnapshotRestore, SnapshotInplaceRestore). Usa un valor más alto si tu backend de almacenamiento o clúster suele requerir más tiempo.	"1200" (20 minutos)

Administrar clústeres de Kubernetes

NetApp Backup and Recovery le permite descubrir y administrar sus clústeres de Kubernetes para que pueda proteger los recursos alojados en los clústeres.

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Para descubrir clústeres de Kubernetes, consulte"Descubra las cargas de trabajo de Kubernetes" .

Editar la información del clúster de Kubernetes

Puede editar un clúster si necesita cambiar su nombre.

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario** > **Clústeres**.
2. En la lista de clústeres, elija el clúster que desee editar y seleccione el menú Acciones asociado.
3. Seleccione **Editar clúster**.
4. Realice los cambios necesarios en el nombre del clúster. El nombre del clúster debe coincidir con el que utilizó con el comando Helm durante el proceso de descubrimiento.
5. Seleccione **Listo**.

Eliminar un clúster de Kubernetes

Para dejar de proteger un clúster de Kubernetes, deshabilite la protección y elimine las aplicaciones asociadas; luego, elimine el clúster de NetApp Backup and Recovery. NetApp Backup and Recovery no

elimina el clúster ni sus recursos; solo elimina el clúster del inventario de la NetApp Console .

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario** > **Clústeres**.
2. En la lista de clústeres, elija el clúster que desee editar y seleccione el menú Acciones asociado.
3. Seleccione **Eliminar clúster**.
4. Revise la información en el cuadro de diálogo de confirmación y seleccione **Eliminar**.

Administrar aplicaciones de Kubernetes

NetApp Backup and Recovery le permite desproteger y eliminar sus aplicaciones de Kubernetes y los recursos asociados.

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Desproteger una aplicación de Kubernetes

Puede desproteger una aplicación si ya no desea protegerla. Cuando desprotege una aplicación, NetApp Backup and Recovery deja de protegerla pero conserva todas las copias de seguridad y las instantáneas asociadas.

> No puedes desproteger una aplicación mientras todavía se están ejecutando operaciones de protección para ella. Espera a que termine la operación o, como alternativa, eliminar el punto de restauración la operación de protección en ejecución está usando. Luego podrás desproteger la aplicación.

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario**.
2. Elija una instancia de Kubernetes y seleccione **Ver** para ver los recursos asociados con esa instancia.
3. Seleccione la pestaña **Aplicaciones**.
4. En la lista de aplicaciones, elija una aplicación que desee desproteger y seleccione el menú Acciones asociado.
5. Seleccione **Desproteger**.
6. Lea el aviso y, cuando esté listo, seleccione **Desproteger**.

Eliminar una aplicación de Kubernetes

Elimina una aplicación que ya no necesitas. NetApp Backup and Recovery detiene la protección y elimina todas las copias de seguridad y las instantáneas de las aplicaciones eliminadas.

Pasos

1. En NetApp Backup and Recovery, seleccione **Inventario**.
2. Elija una instancia de Kubernetes y seleccione **Ver** para ver los recursos asociados con esa instancia.
3. Seleccione la pestaña **Aplicaciones**.

4. En la lista de aplicaciones, elija la aplicación que desee eliminar y seleccione el menú Acciones asociado.
5. Seleccione **Eliminar**.
6. Habilite **Eliminar instantáneas y copias de seguridad** para eliminar todas las instantáneas y copias de seguridad de la aplicación.

   Ya no podrás restaurar la aplicación utilizando estas instantáneas y copias de seguridad.

7. Confirme la acción y seleccione **Eliminar**.

Eliminar un punto de restauración para una aplicación de Kubernetes

Es posible que tengas que eliminar un punto de restauración para una aplicación si necesitas desprotegerla y actualmente se están ejecutando operaciones de protección.

Pasos

1. En el menú NetApp Backup and Recovery, selecciona **Restaurar**.
2. Elige una aplicación de Kubernetes de la lista y selecciona **Ver y restaurar** para esa aplicación.

   Aparece la lista de puntos de restauración.

3. Elige el punto de recuperación que necesitas eliminar y selecciona el icono de Acciones ••• > **Eliminar punto de recuperación** para borrarlo.

Administrar plantillas de gancho de ejecución de NetApp Backup and Recovery para cargas de trabajo de Kubernetes

Un gancho de ejecución es una acción personalizada que se ejecuta con una operación de protección de datos en una aplicación Kubernetes administrada. Por ejemplo, cree instantáneas consistentes con la aplicación utilizando un gancho de ejecución para pausar las transacciones de la base de datos antes de una instantánea y reanudarlas después. Al crear una plantilla de gancho de ejecución, especifique el tipo de gancho, el script a ejecutar y los filtros para los contenedores de destino. Utilice la plantilla para vincular ganchos de ejecución a sus aplicaciones.

NetApp Backup and Recovery congela y descongela sistemas de archivos para aplicaciones como KubeVirt durante la protección de datos. Puedes desactivar este comportamiento globalmente o para aplicaciones específicas usando la documentación de Trident Protect:

- Para deshabilitar este comportamiento para todas las aplicaciones, consulte "Protección de datos con máquinas virtuales KubeVirt" .
- Para deshabilitar este comportamiento para una aplicación específica, consulte "Definir una aplicación" .

Rol de NetApp Console requerido

Administrador de la organización o administrador de SnapCenter . "Obtenga información sobre los roles de acceso de NetApp Backup and Recovery" . "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios" .

Tipos de ganchos de ejecución

NetApp Backup and Recovery admite los siguientes tipos de ganchos de ejecución, según cuándo se puedan ejecutar:

- Pre-instantánea
- Post-instantánea
- Copia de seguridad previa
- Post-copia de seguridad
- Post-restauración

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. Todos los ganchos de ejecución de preoperación personalizados aplicables se ejecutan en los contenedores apropiados. Puede crear varios ganchos de preoperación personalizados, pero su orden de ejecución no está garantizado ni es configurable.
2. Si corresponde, se producen bloqueos del sistema de archivos.
3. Se realiza la operación de protección de datos.
4. Los sistemas de archivos congelados se descongelan, si corresponde.
5. NetApp Backup and Recovery ejecuta cualquier gancho de ejecución previo a la operación personalizado aplicable en los contenedores apropiados. Puede crear varios ganchos posteriores a la operación personalizados, pero su orden de ejecución no está garantizado ni es configurable.

Si crea varios ganchos del mismo tipo, no se garantiza su orden de ejecución. Los ganchos de diferentes tipos siempre se ejecutan en el orden especificado. Por ejemplo, el siguiente es el orden de ejecución de una configuración que tiene todos los diferentes tipos de ganchos:

1. Ganchos previos a la instantánea ejecutados
2. Ganchos posteriores a la instantánea ejecutados
3. Ganchos de pre-copia de seguridad ejecutados
4. Ganchos posteriores a la copia de seguridad ejecutados

Pruebe los scripts de ejecución de gancho antes de habilitarlos en producción. Utilice 'kubectl exec' para probar scripts, luego verifique las instantáneas y las copias de seguridad clonando la aplicación en un espacio de nombres temporal y restaurándola.

Si un gancho de ejecución previo a la instantánea agrega, cambia o elimina recursos de Kubernetes, esos cambios se incluyen en la instantánea o la copia de seguridad y en cualquier operación de restauración posterior.

Notas importantes sobre los ganchos de ejecución personalizados

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

- Un gancho de ejecución debe utilizar un script para realizar acciones. Muchos ganchos de ejecución

pueden hacer referencia al mismo script.

- Los ganchos de ejecución deben escribirse en el formato de scripts de shell ejecutables.
- El tamaño del script está limitado a 96 KB.
- Las configuraciones de gancho de ejecución y cualquier criterio coincidente se utilizan para determinar qué ganchos son aplicables a una operación de instantánea, copia de seguridad o restauración.

> Los ganchos de ejecución pueden reducir o deshabilitar la funcionalidad de la aplicación. Haga que sus ganchos personalizados se ejecuten lo más rápido posible. Si inicia una operación de copia de seguridad o instantánea con ganchos de ejecución asociados pero luego la cancela, los ganchos aún podrán ejecutarse si la operación de copia de seguridad o instantánea ya ha comenzado. Esto significa que la lógica utilizada en un gancho de ejecución posterior a una copia de seguridad no puede asumir que la copia de seguridad se completó.

Filtros de gancho de ejecución

Cuando agrega o edita un gancho de ejecución para una aplicación, puede agregar filtros al gancho de ejecución para administrar con qué contenedores coincidirá el gancho. Los filtros son útiles para las aplicaciones que utilizan 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 en los que los ganchos de ejecución se ejecutan en algunos, pero no necesariamente en todos los contenedores idénticos. Si crea varios filtros para un único gancho de ejecución, se combinan con un operador AND lógico. Puede tener hasta 10 filtros activos por gancho de ejecución.

Cada filtro que agrega a un gancho de ejecución utiliza una expresión regular para que coincida con los contenedores en su clúster. Cuando un gancho coincide con un contenedor, el gancho ejecutará su script asociado en ese contenedor. Las expresiones regulares para filtros utilizan la sintaxis de Expresión regular 2 (RE2), que no admite la creación de un filtro que excluya contenedores de la lista de coincidencias. Para obtener información sobre la sintaxis que NetApp Backup and Recovery admite para expresiones regulares en filtros de gancho de ejecución, consulte "Compatibilidad con la sintaxis de expresiones regulares 2 (RE2)" .

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

Ejemplos de ganchos de ejecución

Visita el "Proyecto NetApp Verda en GitHub" para descargar ganchos de ejecución reales para aplicaciones populares como Apache Cassandra y Elasticsearch. También puede ver ejemplos y obtener ideas para estructurar sus propios ganchos de ejecución personalizados.

Crear una plantilla de gancho de ejecución

Puede crear una plantilla de gancho de ejecución personalizada que pueda utilizar para realizar acciones antes o después de una operación de protección de datos en una aplicación.

> Las plantillas que crees aquí solo se pueden usar cuando proteges cargas de trabajo de Kubernetes.

Pasos

1. En la consola, vaya a **Protección** > **Copia de seguridad y recuperación**.
2. Seleccione la pestaña **Configuración**.
3. Expande la sección **Plantilla de gancho de ejecución**.
4. Seleccione **Crear plantilla de gancho de ejecución**.
5. Introduzca un nombre para el gancho de ejecución.
6. Opcionalmente, elija un tipo de enlace. Por ejemplo, un enlace posterior a la restauración se ejecuta una vez finalizada la operación.
7. En el cuadro de texto **Script**, ingrese el script de shell ejecutable que desea ejecutar como parte de la plantilla de gancho de ejecución. Opcionalmente, puede seleccionar **Cargar script** para cargar un archivo de script en su lugar.
8. Seleccione **Crear**.

   Después de crear la plantilla, ésta aparece en la lista de plantillas en la sección **Plantilla de gancho de ejecución**.

Crea y gestiona informes de protección para cargas de trabajo de Kubernetes en NetApp Backup and Recovery

En NetApp Backup and Recovery, crea informes de protección para cargas de trabajo de Kubernetes para ver el estado y los detalles de la protección, incluidos los recuentos de copias de seguridad correctas y fallidas, los tipos de copia de seguridad, la información sobre el estado del clúster y más.

Rol requerido de NetApp Console Backup and Recovery super admin, Backup and Recovery backup admin o Backup and Recovery restore admin. Aprende sobre "Roles y privilegios de copia de seguridad y recuperación". "Obtenga información sobre los roles de acceso a la NetApp Console para todos los servicios".

Crear un informe de protección

Crea un informe de protección para ver el estado de protección de tus clústeres.

Pasos

1. En el menú NetApp Backup and Recovery , seleccione la opción **Informes**.
2. Seleccione **Crear informe**.
3. Introduzca los detalles del alcance del informe:
   - **Nombre del informe**: Ingrese un nombre único para el informe.
   - **Tipo de informe**: Elige si quieres un informe por cuenta o por carga de trabajo (selecciona Kubernetes de la lista).
   - **Selecciona cluster**: Si seleccionaste por carga de trabajo, elige el cluster de la lista para el que quieres generar el informe y selecciona **Aceptar**. Elige **Seleccionar todo** para generar un informe para todos los clusters.
4. Introduce el intervalo del informe: elige si quieres que el informe incluya datos del último día, de los últimos 7 días, de los últimos 30 días, del último trimestre o del último año.
5. Introduce los detalles de configuración del informe: elige si quieres ejecutar el informe solo una vez o programar una generación de informes recurrente. Para los informes programados, elige la frecuencia de

recurrencia y selecciona una fecha de inicio.

a. Introduce los detalles de entrega por correo electrónico: (para informes programados solamente) Si quieres que el informe se entregue por correo electrónico, introduce una o varias direcciones de correo electrónico que deban recibir el informe programado.

Configure las notificaciones por correo electrónico en la página Configuración. Para obtener detalles sobre cómo configurar las notificaciones por correo electrónico, consulte"Configurar ajustes" .

6. Seleccione **Crear**.

Descarga un informe de protección

Descarga un informe de protección generado como archivo JSON o documento PDF para que puedas verlo y compartirlo.

Pasos

1. En el menú NetApp Backup and Recovery , seleccione la opción **Informes**.
2. En la página **Informes**, selecciona el menú **Informes** para ver la lista de informes de protección generados.
3. Para el informe que quieres descargar, selecciona el icono de Acciones ••• > **Download**.
   - Selecciona **Descargar JSON** para descargar el informe en formato JSON.
   - Selecciona **Download PDF** para descargar el informe como documento PDF.

Ver un informe de protección

Visualiza rápidamente los detalles interactivos de un informe de protección dentro de NetApp Backup and Recovery. Puedes ver información resumida del trabajo, el estado de la protección de datos, detalles de la configuración y mucho más.

Pasos

1. En el menú NetApp Backup and Recovery , seleccione la opción **Informes**.
2. En la página **Informes**, selecciona el menú **Informes** para ver la lista de informes de protección generados.
3. Para el informe que quieres ver, selecciona el icono de Acciones ••• > **Ver informe**.

   Aparecen los detalles del informe.

Eliminar un informe de protección

Elimina un informe de protección cuando ya no lo necesites.

Pasos

1. En el menú NetApp Backup and Recovery , seleccione la opción **Informes**.
2. En la página **Informes**, selecciona el menú **Informes** para ver la lista de informes de protección generados.
3. Para el informe que quieres eliminar, selecciona el icono de Acciones ••• > **Delete**.
4. Confirma la acción seleccionando **Suprimir**.

Información de copyright

Información de la marca comercial