



Restaurar aplicaciones de Kubernetes

NetApp Backup and Recovery

NetApp

February 10, 2026

Tabla de contenidos

- Restaurar aplicaciones de Kubernetes 1
 - Restaura aplicaciones de Kubernetes usando la interfaz web 1
 - Restaura aplicaciones Kubernetes usando un recurso personalizado 3
 - Restaura una copia de seguridad en un espacio de nombres diferente 3
 - Restaura una copia de seguridad en el espacio de nombres original 5
 - Restaura una copia de seguridad en un clúster diferente 7
 - Restaura una instantánea en un espacio de nombres diferente 10
 - Restaura una instantánea al espacio de nombres original 12
- Usa la configuración avanzada de restauración de recursos personalizada 14
 - Anotaciones y etiquetas de namespace durante las operaciones de restauración y conmutación por error 14
 - Campos compatibles 16
 - Anotaciones compatibles 16

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 trasladador 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 trasladador 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 trasladador 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"}]

```

- 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 <SNAPSHOT_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_key_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) | <ul style="list-style-type: none">• <code>annotation.one/key</code>: "valoractualizado"• <code>annotation.two/key</code>: "true" | <ul style="list-style-type: none">• <code>entorno</code>=producción• <code>compliance</code>=hipaa• <code>name</code>=ns-1 |

| Espacio de nombres | Anotaciones | Etiquetas |
|--------------------------|---|---|
| Namespace ns-2 (destino) | <ul style="list-style-type: none"> • annotation.one/key: "true" • annotation.three/key: "false" | <ul style="list-style-type: none"> • 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) | <ul style="list-style-type: none"> • annotation.one/key: "valoractualizado" • annotation.two/key: "true" • annotation.three/key: "false" | <ul style="list-style-type: none"> • 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 <code>Bound</code> fase antes de que la operación falle. Aplica a todos los tipos de CR de restauración (<code>BackupRestore</code> , <code>BackupInplaceRestore</code> , <code>SnapshotRestore</code> , <code>SnapshotInplaceRestore</code>). Usa un valor más alto si tu backend de almacenamiento o clúster suele requerir más tiempo. | "1200" (20 minutos) |

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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