Restaurar aplicaciones

Trident

NetApp
July 01, 2026

Tabla de contenidos

Restaurar aplicaciones . . . 1
- Restaura aplicaciones usando Trident Protect . . . 1
  - Restaura desde una copia de seguridad a un espacio de nombres diferente . . . 1
  - Restaura desde una copia de seguridad al espacio de nombres original . . . 5
  - Restaurar desde una copia de seguridad en un clúster diferente . . . 8
  - Restaurar desde una snapshot a un namespace diferente . . . 11
  - Restaurar desde una snapshot al namespace original . . . 14
  - Verifica el estado de una operación de restauración . . . 17
- Usa la configuración avanzada de restauración de Trident Protect . . . 17
  - Anotaciones y etiquetas de namespace durante las operaciones de restauración y conmutación por error . . . 17
  - Campos compatibles . . . 19
  - Anotaciones compatibles . . . 19

Restaurar aplicaciones

Restaura aplicaciones usando Trident Protect

Puedes usar Trident Protect para restaurar tu aplicación desde una instantánea o backup. Restaurar desde una instantánea existente será más rápido cuando restaures 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 Trident Protect".

Restaura desde una copia de seguridad a un espacio de nombres diferente

Cuando restauras una copia de seguridad en un espacio de nombres diferente usando un CR de BackupRestore, Trident Protect 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 un programa 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 usas un CR para restaurar a un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR. Trident Protect crea espacios de nombres automáticamente 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 AWS API" 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 transportador de datos, puedes especificar opcionalmente anotaciones en el CR o usando la CLI para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta la "Documentación de Kopia" para más información sobre las opciones que puedes configurar. Usa el comando `tridentctl-protect create --help` para más información sobre cómo especificar anotaciones con la Trident Protect CLI.

Usa un CR

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale 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.destinationApplicationName**: (*opcional*) el nombre para la aplicación restaurada. Si se proporciona, la aplicación restaurada usa este nombre. Si no se proporciona, la aplicación restaurada usa el nombre de la aplicación de origen.
   - **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
       destinationApplicationName: my-new-app-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 de resourceMatchers para definir los recursos que se incluirán o excluirán:

- **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
```

Usa la CLI

Pasos

1. Restaura la copia de seguridad en un espacio de nombres diferente, reemplazando los valores entre corchetes por información de tu entorno. El argumento `namespace-mapping` usa espacios de

nombres separados por dos puntos para mapear los espacios de nombres de origen a los espacios de nombres de destino correctos en el formato `source1:dest1,source2:dest2`. Por ejemplo:

```
tridentctl-protect create backuprestore <my_restore_name> \
--backup <backup_namespace>/<backup_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--destination-app-name<custom_app_name>\
-n <application_namespace>
```

Restaura desde una copia de seguridad al espacio de nombres original

Puedes restaurar una copia de seguridad en el espacio de nombres original en cualquier momento. Cuando realizas una restaurar sin movimiento, Trident Protect gestiona automáticamente los programas de protección y las operaciones en curso para evitar puntos de recuperación no válidos:

- Todos los programas de protección activados para la aplicación se desactivan antes de que comience la restauración. Esto evita que se ejecuten copias de seguridad o instantáneas programadas mientras se restauran los recursos de la aplicación.
- Después de que la restauración se complete correctamente, solo se vuelven a habilitar las programaciones que estaban habilitadas antes de la restauración. Las programaciones que ya estaban deshabilitadas permanecen deshabilitadas.
- Cualquier operación de copia de seguridad o instantánea en curso se cancela antes de que comience la restauración. Si una operación no se cancela en 5 minutos, la restauración continúa y registra una advertencia en el estado de restauración 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 AWS API" 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 transportador de datos, puedes especificar opcionalmente anotaciones en el CR o usando la CLI para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta la "Documentación de Kopia" para más información sobre las opciones que puedes configurar. Usa el comando `tridentctl-protect create --help` para más información sobre cómo especificar anotaciones con la Trident Protect CLI.

Usa un CR

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale 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 de resourceMatchers para definir los recursos que se incluirán o excluirán:
     - **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
```

Usa la CLI

Pasos

1. Restaura la copia de seguridad en el espacio de nombres original, sustituyendo los valores entre corchetes por información de tu entorno. El argumento `backup` utiliza un espacio de nombres y un nombre de copia de seguridad en el formato `<namespace>/<name>`. Por ejemplo:

```
tridentctl-protect create backupinplacerestore <my_restore_name> \
--backup <namespace/backup_to_restore> \
-n <application_namespace>
```

Restaurar desde 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 transportador de datos, puedes especificar opcionalmente anotaciones en el CR o usando la CLI para controlar el comportamiento del almacenamiento temporal que usa Kopia. Consulta la "Documentación de Kopia" para más información sobre las opciones que puedes configurar. Usa el comando `tridentctl-protect create --help` para más información sobre cómo especificar anotaciones con la Trident Protect CLI.
- Cuando usas un CR para restaurar a un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR. Trident Protect crea espacios de nombres automáticamente solo cuando usas la CLI.

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 tu entorno local puede conectarse al bucket de almacenamiento de objetos definido en el AppVault CR cuando ejecutes el comando `tridentctl-protect get appvaultcontent`. Si las restricciones de red impiden el acceso, ejecuta la CLI de Trident Protect desde un pod en el clúster de destino en su lugar.
- 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 AWS API" 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. Verifica que el AppVault CR existe en el clúster de destino usando el complemento CLI de Trident Protect:

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

   Si el AppVault CR no existe en el clúster de destino, créalo siguiendo los pasos en "Usa los objetos de Trident Protect AppVault para gestionar buckets".

2. Visualiza el contenido de la copia de seguridad disponible en AppVault en el clúster de destino y anota `appArchivePath` de la copia de seguridad que quieres restaurar:

```
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:

> Cuando utilices un CR, asegúrate de que el espacio de nombres previsto para la restauración de la aplicación existe en el clúster de destino.

Usa un CR

1. Crea el archivo de recurso personalizado (CR) y asígnale 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.appVaultRef**: (*Required*) el nombre del AppVault donde se almacena el contenido de la copia de seguridad.
   - **spec.appArchivePath**: (*Obligatorio*) La ruta dentro de AppVault donde se almacena el contenido de la copia de seguridad. Usa el comando del paso 2 para ver el contenido de la copia de seguridad y encontrar `appArchivePath` la copia de seguridad que quieres restaurar.
   - **spec.destinationApplicationName**: (*opcional*) el nombre para la aplicación restaurada. Si se proporciona, la aplicación restaurada usa este nombre. Si no se proporciona, la aplicación restaurada usa el nombre de la aplicación de origen.
   - **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
  destinationApplicationName: my-new-app-name
  namespaceMapping: [{"source": "my-source-namespace", "
destination": "my-destination-namespace"}]
```

3. 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
```

Usa la CLI

1. Usa el siguiente comando para restaurar la aplicación, reemplazando los valores entre corchetes por la información de tu entorno. El argumento namespace-mapping utiliza espacios de nombres separados por dos puntos para asignar los espacios de nombres de origen a los espacios de nombres de destino correctos en el formato source1:dest1,source2:dest2. Por ejemplo:

```
tridentctl-protect create backuprestore <restore_name> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--appvault <appvault_name> \
--path <backup_path> \
--destination-app-name <custom_app_name> \
--context <destination_cluster_name> \
-n <application_namespace>
```

Restaurar desde una snapshot a un namespace 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. Cuando restauras una instantánea en un espacio de nombres diferente usando un CR de SnapshotRestore, Trident Protect 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 un programa 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 a un nuevo espacio de nombres, debes crear manualmente el espacio de nombres de destino antes de aplicar el CR. Trident Protect crea espacios de nombres automáticamente 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 AWS API" 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.

Usa un CR

Pasos

1. Crea el archivo de recurso personalizado (CR) y asígnale 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.destinationApplicationName**: (*opcional*) el nombre para la aplicación restaurada. Si se proporciona, la aplicación restaurada usa este nombre. Si no se proporciona, la aplicación restaurada usa el nombre de la aplicación de origen.
   - **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 de resourceMatchers para definir los recursos que se incluirán o excluirán:

- **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
```

Usa la CLI

Pasos

1. Restaura la instantánea en un espacio de nombres diferente, reemplazando los valores entre corchetes con información de tu entorno.

- El `snapshot`argumento usa un espacio de nombres y un nombre de instantánea en el formato `<namespace>/<name>`.
- El argumento `namespace-mapping` usa espacios de nombres separados por dos puntos para mapear los espacios de nombres de origen a los espacios de nombres de destino correctos en el formato `source1:dest1,source2:dest2`.

  Por ejemplo:

```
tridentctl-protect create snapshotrestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
--namespace-mapping <source_to_destination_namespace_mapping> \
--destination-app-name <custom_app_name> \
-n <application_namespace>
```

Restaurar desde una snapshot al namespace original

Puedes restaurar una instantánea en el espacio de nombres original en cualquier momento. Cuando realizas una restaurar sin movimiento, Trident Protect gestiona automáticamente los programas de protección y las operaciones en curso para evitar puntos de recuperación no válidos:

- Todos los programas de protección activados para la aplicación se desactivan antes de que comience la restauración. Esto evita que se ejecuten copias de seguridad o instantáneas programadas mientras se restauran los recursos de la aplicación.
- Después de que la restauración se complete correctamente, solo se vuelven a habilitar las programaciones que estaban habilitadas antes de la restauración. Las programaciones que ya estaban deshabilitadas permanecen deshabilitadas.
- Cualquier operación de copia de seguridad o instantánea en curso se cancela antes de que comience la restauración. Si una operación no se cancela en 5 minutos, la restauración continúa y registra una advertencia en el estado de restauración 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 AWS API" 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.

Usa un CR

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 de resourceMatchers para definir los recursos que se incluirán o excluirán:
     - **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 CLI

Pasos

1. Restaura la instantánea en el espacio de nombres original, reemplazando los valores entre corchetes por información de tu entorno. Por ejemplo:

```
tridentctl-protect create snapshotinplacerestore <my_restore_name> \
--snapshot <namespace/snapshot_to_restore> \
-n <application_namespace>
```

Verifica el estado de una operación de restauración

Puedes usar la línea de comandos para comprobar el estado de una operación de restauración que está en curso, ha finalizado o ha fallado.

Pasos

1. Usa el siguiente comando para obtener el estado de la operación de restauración, reemplazando los valores entre corchetes por la información de tu entorno:

```
kubectl get backuprestore -n <namespace_name> <my_restore_cr_name> -o
jsonpath='{.status}'
```

Usa la configuración avanzada de restauración de Trident Protect

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 "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` quedan excluidas de la operación de restauración o conmutación por error. Asegúrate de que estos ajustes se configuren 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
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)