



Agregar y proteger aplicaciones de Kubernetes

NetApp Backup and Recovery

NetApp
February 10, 2026

Tabla de contenidos

- Agregar y proteger aplicaciones de Kubernetes 1
 - Agregar y proteger aplicaciones de Kubernetes 1
 - Agregar y proteger una nueva aplicación de Kubernetes 1
- Haz backup de aplicaciones Kubernetes ahora usando la interfaz web de Backup and Recovery 5
 - Haz una copia de seguridad de una aplicación de Kubernetes ahora usando la interfaz web 6
- Haz backup de aplicaciones Kubernetes ahora usando recursos personalizados en Backup and Recovery 6
 - Haz una copia de seguridad de una aplicación de Kubernetes ahora usando recursos personalizados .. 6
 - Anotaciones de backup compatibles 10

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 prescripts o postscripts, 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:

```
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:

```
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
```

- 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 <code>true</code> 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)

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.