Cree backups y restaure datos de Kubernetes

Cloud Backup

NetApp
February 20, 2023

Tabla de Contenido

Cree backups y restaure datos de Kubernetes 1
Proteja los datos de clústeres de Kubernetes mediante Cloud Backup 1
Realizar backups de datos de volúmenes persistentes de Kubernetes en Amazon S3 5
Gestionar backups para sus sistemas Kubernetes 11
Restaurar los datos de Kubernetes a partir de los archivos de backup 22

Cree backups y restaure datos de Kubernetes

Proteja los datos de clústeres de Kubernetes mediante Cloud Backup

Cloud Backup ofrece funcionalidades de backup y restauración para protección y archivado a largo plazo de sus datos de clúster de Kubernetes. Los backups se generan y almacenan automáticamente en un almacén de objetos en su cuenta de cloud público o privado.

Cuando sea necesario, puede restaurar un *volume* completo desde una copia de seguridad al mismo entorno de trabajo o diferente.

Funciones

Funciones de backup:

- Realice backups de copias independientes de sus volúmenes persistentes en un almacenamiento de objetos de bajo coste.
- Aplique una única política de backup a todos los volúmenes de un clúster o asigne diferentes políticas de backup a los volúmenes que tengan objetivos de punto de recuperación únicos.
- Los datos de los backups se protegen con conexiones HTTPS en reposo con cifrado AES de 256 bits y TLS 1.2.
- Permite hasta 4,000 backups de un único volumen.

Funciones de restauración:

- Restaure los datos de un momento específico.
- Restaure un volumen al sistema de origen o a otro sistema.
- Restaura datos en el nivel de bloque, colocando los datos directamente en la ubicación especificada, mientras conserva las ACL originales.

Entornos de trabajo de Kubernetes compatibles y proveedores de almacenamiento de objetos

Cloud Backup le permite realizar backups de volúmenes de Kubernetes de los siguientes entornos de trabajo en el almacenamiento de objetos, en los siguientes proveedores de cloud público y privado:

Entorno de trabajo de fuente	Destino de archivo de copia de seguridad ifdef::aws[]
Clúster de Kubernetes en AWS	Endif de Amazon S3::aws[] ifdef::Azure[]
Clúster de Kubernetes en Azure	Endif de Azure Blob::Azure[] ifdef::gcp[]
Clúster de Kubernetes en Google	Fin de Google Cloud Storage::gcp[]

Es posible restaurar un volumen de un archivo de backup de Kubernetes en los siguientes entornos de trabajo:

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino ifdef::aws[]
Amazon S3	Clúster de Kubernetes en endif de AWS::aws[] ifdef::Azure[]
Azure Blob	Clúster de Kubernetes en endif de Azure::Azure[] ifdef::gcp[]
Google Cloud Storage	Clúster de Kubernetes en Google endif::gcp[]

Coste

Existen dos tipos de costes asociados con el uso de Cloud Backup: Cargos por recursos y cargos por servicio.

gastos de recursos

Se paga un recargo por los recursos al proveedor de cloud por la capacidad de almacenamiento de objetos en el cloud. Desde que Cloud Backup conserva las eficiencias del almacenamiento del volumen de origen, pagará los costes del almacenamiento de objetos del proveedor de cloud por las eficiencias de los datos *After* ONTAP (en cuanto a la menor cantidad de datos después de aplicar la deduplicación y la compresión).

cargos por servicio

NetApp paga los gastos de servicio y cubre tanto el coste de los backups *create* como los volúmenes *restore* de dichos backups. Solo paga por los datos que protege, calculados por la capacidad lógica utilizada de origen (*antes* eficiencia de ONTAP) de los volúmenes de los que se ha realizado un backup en el almacenamiento de objetos. Esta capacidad también se conoce como terabytes de interfaz (FETB).

El servicio de backup consta de dos formas de pago. La primera opción es suscribirse a su proveedor de cloud, lo que le permite pagar por mes. La segunda opción consiste en comprar licencias directamente a NetApp. Lea la Licencia para obtener más información.

Licencia

Cloud Backup está disponible en dos opciones de licencia: Pago por uso (PAYGO) y con su propia licencia (BYOL). Hay disponible una prueba gratuita de 30 días si no tiene licencia.

Prueba gratuita

Al utilizar la prueba gratuita de 30 días, se le notifica el número de días de prueba gratuitos que quedan. Al final de su prueba gratuita, los backups dejan de crearse. Debe suscribirse al servicio o adquirir una licencia para seguir utilizando el servicio.

Los archivos de copia de seguridad no se eliminan cuando el servicio está deshabilitado. El proveedor de cloud seguirá facturando los costes del almacenamiento de objetos por la capacidad que utilizan sus backups a menos que elimine los backups.

Suscripción de pago por uso

Cloud Backup ofrece licencias basadas en consumo en un modelo de pago por uso. Después de suscribirse a través del mercado de su proveedor de nube, paga por GB los datos de los que se ha realizado una copia de seguridad: there no es el pago inicial. Su proveedor de cloud se le factura con cargo mensual.

Debe suscribirse aunque tenga una prueba gratuita o si lleva su propia licencia (BYOL):

- La suscripción garantiza que no se produzcan interrupciones en el servicio una vez que finalice la prueba gratuita.

  Cuando finalice la prueba, se le cobrará cada hora según la cantidad de datos de los que realiza la copia de seguridad.

- Si realiza un backup de más datos de los permitidos en su licencia BYOL, el backup de datos continúa con su suscripción de pago por uso.

  Por ejemplo, si tiene una licencia BYOL de 10 TB, toda la capacidad que supere los 10 TB se cargará a través de la suscripción PAYGO.

No se le cobrará su suscripción de pago por uso durante su prueba gratuita o si no ha superado su licencia BYOL.

"Aprenda a configurar una suscripción de pago por uso".

Con su propia licencia

BYOL se basa en el plazo (12, 24 o 36 meses) en incrementos de 1 TB. Usted paga a NetApp para que utilice el servicio por un periodo, digamos de 1 año, y por una cantidad máxima, digamos 10 TB.

Recibirá un número de serie que introduzca en la página de Blue XP Digital Wallet para activar el servicio. Cuando se alcance cualquiera de los límites, deberá renovar la licencia. La licencia BYOL de copia de seguridad se aplica a todos los sistemas de origen asociados a su "Cuenta BlueXP".

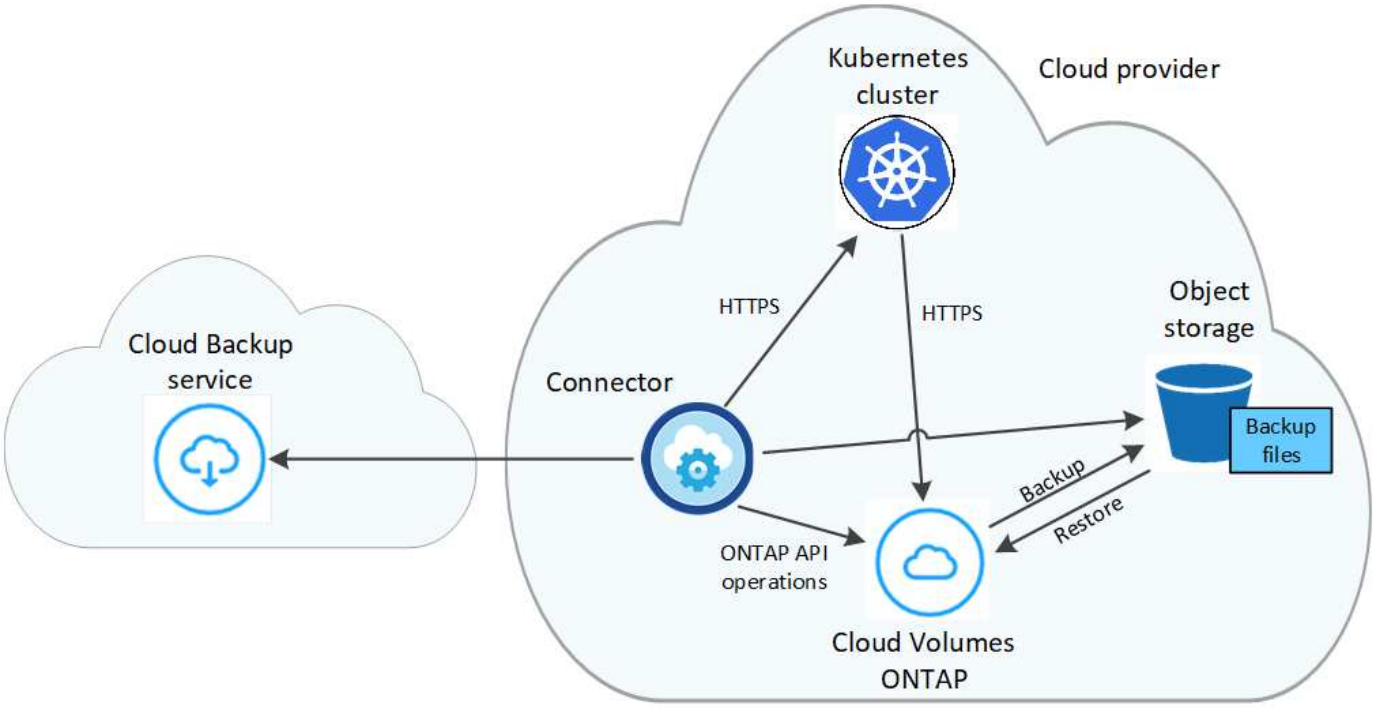
"Aprenda a gestionar sus licencias BYOL".

Cómo funciona Cloud Backup

Cuando habilita Cloud Backup en un sistema Kubernetes, el servicio realiza un backup completo de sus datos. Tras el primer backup, todos los backups adicionales son incrementales, lo que significa que solo se realiza un backup de los bloques modificados y los nuevos bloques. De este modo se minimiza el tráfico de red.

Cualquier acción que se realice directamente desde el entorno de su proveedor de cloud para gestionar o cambiar los archivos de copia de seguridad puede dañar los archivos y provocar una configuración no compatible.

La siguiente imagen muestra la relación entre cada componente:



Clases de almacenamiento o niveles de acceso admitidos

- En AWS, los backups comienzan en la clase de almacenamiento *Standard* y realizan la transición a la clase de almacenamiento *Standard-Infrecuente Access* tras 30 días.

Configuración de retención y programación de backup personalizable por clúster

Al habilitar Cloud Backup para un entorno de trabajo, todos los volúmenes que inicialmente seleccione se incluirán en los backups con la política de backup predeterminada que haya definido. Si desea asignar diferentes políticas de backup a ciertos volúmenes que tienen diferentes objetivos de punto de recuperación (RPO), puede crear políticas adicionales para ese clúster y asignar dichas políticas a otros volúmenes.

Se puede elegir una combinación de backups por hora, diarios, semanales y mensuales de todos los volúmenes.

Una vez que haya alcanzado el número máximo de backups para una categoría o intervalo, se eliminan los backups más antiguos de modo que siempre tendrá los backups más recientes.

Volúmenes compatibles

Cloud Backup es compatible con volúmenes persistentes (VP).

Limitaciones

- Cuando se crea o edita una política de backup cuando no se asignan volúmenes a la política, el número de backups retenidos puede ser un máximo de 1018. Como solución alternativa, puede reducir el número de copias de seguridad para crear la directiva. Luego, se puede editar la política para crear hasta 4000 backups después de asignar volúmenes a la política.
- Las copias de seguridad de volumen ad-hoc con el botón **Backup Now** no se admiten en los volúmenes Kubernetes.

Realizar backups de datos de volúmenes persistentes de Kubernetes en Amazon S3

Complete unos pasos para empezar a realizar backups de datos desde sus volúmenes persistentes en clústeres EKS Kubernetes al almacenamiento Amazon S3.

Inicio rápido

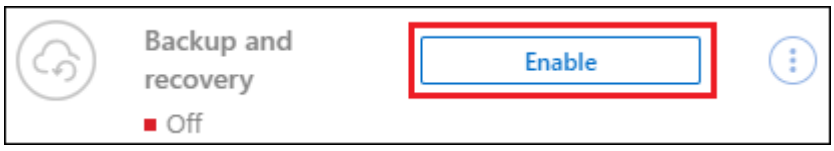
Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1 Revise los requisitos previos

- Ha descubierto el clúster de Kubernetes como entorno de trabajo de BlueXP.
  - Trident debe instalarse en el clúster y la versión de Trident debe ser 21.1 o superior.
  - Todas las RVP que se utilizarán para crear volúmenes persistentes en los que se desea realizar un backup deben tener "snapshotPolicy" configurado en "default".
  - El clúster debe usar Cloud Volumes ONTAP en AWS para su almacenamiento back-end.
  - El sistema Cloud Volumes ONTAP debe ejecutar ONTAP 9.7P5 o posterior.
- Dispone de una suscripción de proveedor de cloud válida para el espacio de almacenamiento en el que se ubicará los backups.
- Se ha suscrito a "Oferta de backup de BlueXP Marketplace", an "Contrato anual de AWS", o usted ha comprado "y activado" Una licencia BYOL de Cloud Backup de NetApp.
- La función IAM que proporciona el conector BlueXP con permisos incluye permisos S3 de la última versión "Política de BlueXP".

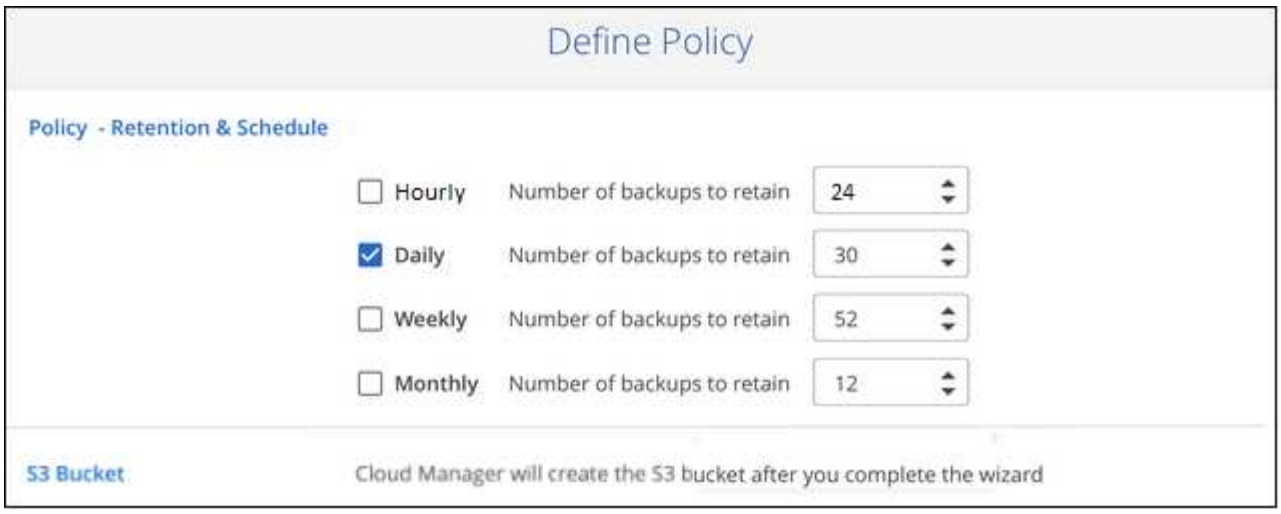
2 Habilite Cloud Backup en su clúster de Kubernetes existente

Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad y recuperación en el panel derecho y, a continuación, siga el asistente de configuración.



3 Defina la política de backup

La política predeterminada realiza backups de volúmenes todos los días y conserva las 30 copias de backup más recientes de cada volumen. Cambie a backups por hora, por día, por semana o por mes, o seleccione una de las políticas definidas por el sistema que proporcionan más opciones. También es posible cambiar la cantidad de copias de backup que se desean retener.



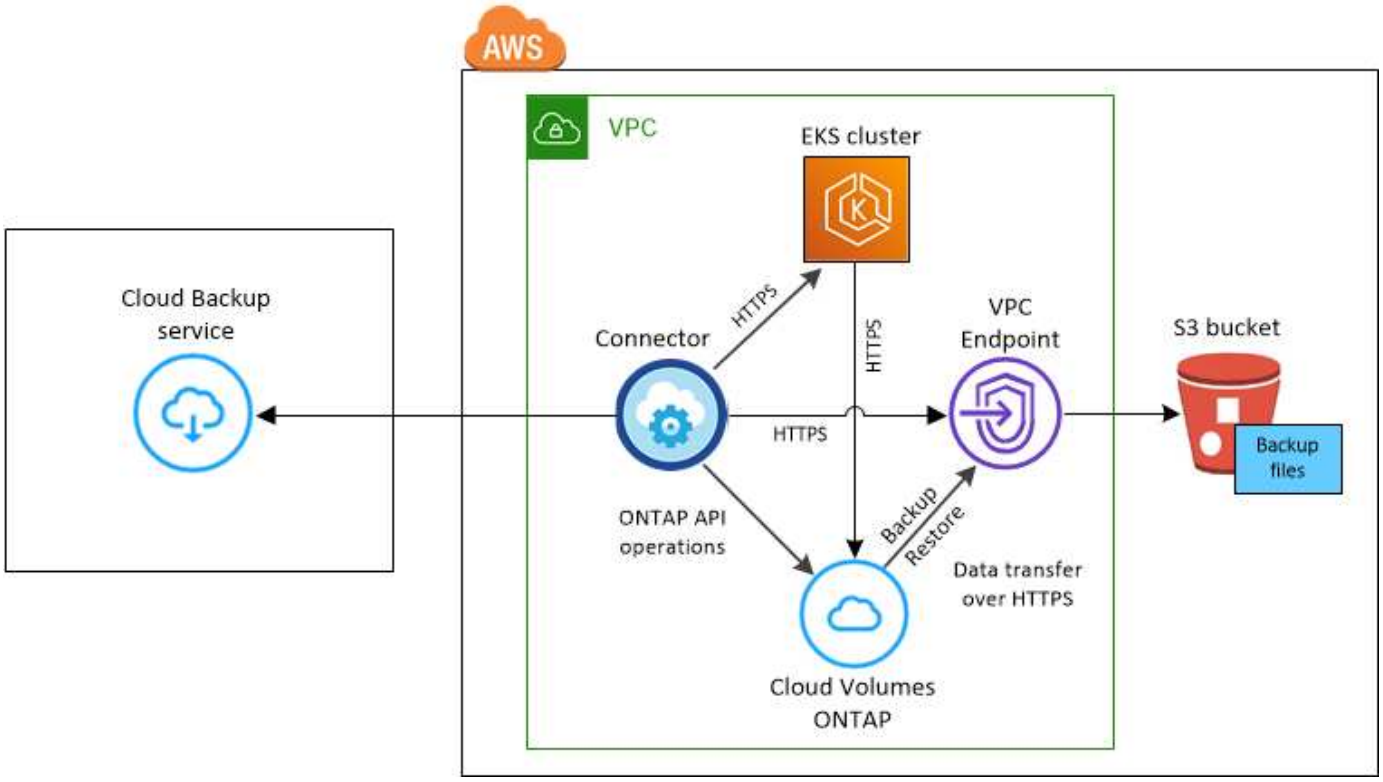
4 **Seleccione los volúmenes de los que desea realizar el backup**

Identificar los volúmenes de los que se desea realizar backup en la página Select Volumes. Un bloque de S3 se crea automáticamente en la misma cuenta y región de AWS que el sistema Cloud Volumes ONTAP, y los archivos de backup se almacenan allí.

Requisitos

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar el backup de volúmenes persistentes de Kubernetes en S3.

La siguiente imagen muestra cada componente y las conexiones que necesita preparar entre ellos:



Tenga en cuenta que el extremo VPC es opcional.

Requisitos del clúster de Kubernetes

- Ha descubierto el clúster de Kubernetes como entorno de trabajo de BlueXP. "Descubra el clúster de Kubernetes".
- Trident debe instalarse en el clúster y la versión de Trident debe ser un mínimo de 21.1. Consulte "cómo instalar Trident" o. "cómo actualizar la versión de Trident".
- El clúster debe usar Cloud Volumes ONTAP en AWS para su almacenamiento back-end.
- El sistema Cloud Volumes ONTAP debe estar en la misma región de AWS que el clúster de Kubernetes, y debe ejecutar ONTAP 9.7P5 o posterior (se recomienda ONTAP 9.8P11 y versiones posteriores).

  Tenga en cuenta que los clústeres de Kubernetes en las ubicaciones locales no son compatibles. Solo son compatibles los clústeres de Kubernetes en las implementaciones de cloud que usan sistemas Cloud Volumes ONTAP.

- Todos los objetos de solicitud de volumen persistente que se usarán para crear los volúmenes persistentes que se desean incluir en el backup deben tener "snapshotPolicy" establecido en "default".

  Puede hacer esto para EVs individuales añadiendo `snapshotPolicy` en anotaciones:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

  Puede hacerlo con todas las RVP asociadas con un almacenamiento back-end determinado agregando el `snapshotPolicy` en valores predeterminados en la `backend.json` archivo:

```
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
  deletionPolicy: retain
```

Requisitos de licencia

Para las licencias de Cloud Backup PAYGO, hay una suscripción disponible en AWS Marketplace que permite poner en marcha Cloud Volumes ONTAP y Cloud Backup. Necesita hacerlo "suscríbase a esta suscripción a BlueXP" Antes de habilitar Cloud Backup. La facturación de Cloud Backup se realiza mediante esta suscripción.

Para obtener un contrato anual que le permita realizar un backup de los datos de Cloud Volumes ONTAP y de ONTAP en las instalaciones, debe suscribirse al "AWS Marketplace" y después "Asocie la suscripción con sus credenciales de AWS".

Para obtener un contrato anual que le permita agrupar Cloud Volumes ONTAP y Cloud Backup, debe establecer el contrato anual cuando cree un entorno de trabajo de Cloud Volumes ONTAP. Esta opción no le permite realizar un backup de los datos en las instalaciones.

Para las licencias BYOL de Cloud Backup, necesita el número de serie de NetApp que le permite usar el servicio durante la duración y la capacidad de la licencia. "Aprenda a gestionar sus licencias BYOL".

Además, necesita tener una cuenta de AWS para el espacio de almacenamiento donde se ubicará la copia de seguridad.

Regiones admitidas de AWS

Cloud Backup es compatible en todas las regiones de AWS "Donde se admite Cloud Volumes ONTAP".

Se requieren permisos de backup de AWS

La función IAM que proporciona permisos BlueXP debe incluir permisos S3 de la última versión "Política de BlueXP".

A continuación se muestran los permisos específicos de S3 de la política:

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:DeleteObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

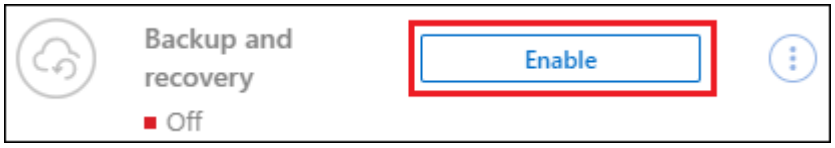
Habilitación de Cloud Backup

Habilite Cloud Backup en cualquier momento directamente desde el entorno de trabajo de Kubernetes.

Pasos

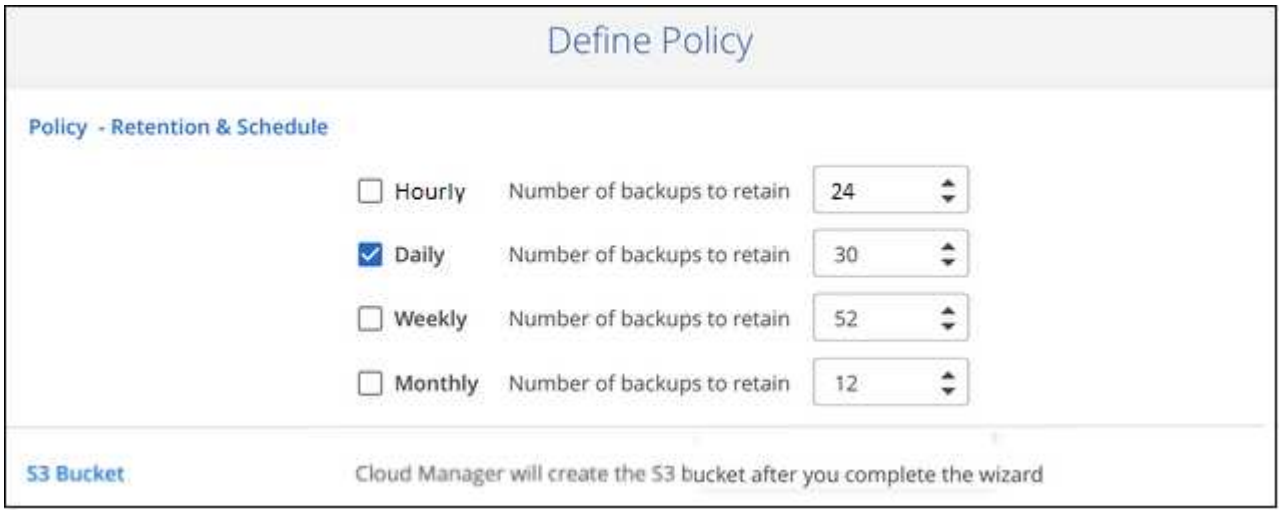
1. Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad y recuperación en el panel derecho.

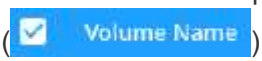
   Si el destino de Amazon S3 para sus backups existe como entorno de trabajo en Canvas, puede arrastrar el clúster de Kubernetes al entorno de trabajo Amazon S3 para iniciar el asistente de configuración.



2. Introduzca los detalles de la política de copia de seguridad y haga clic en **Siguiente**.

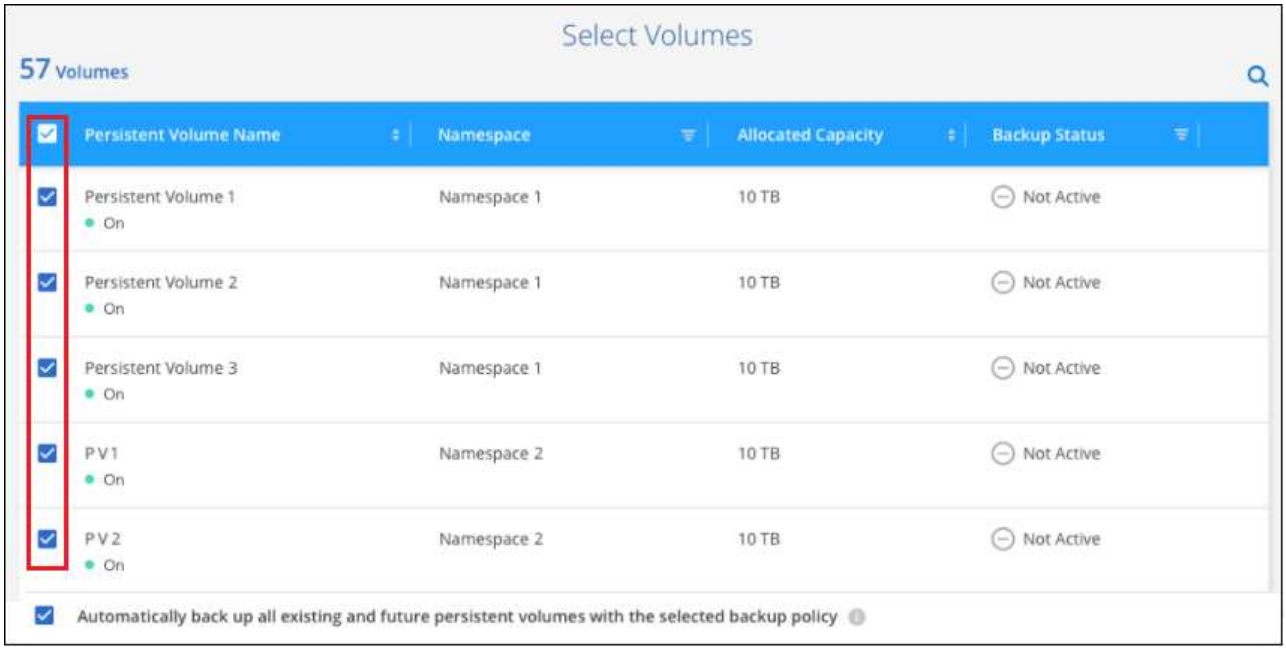
   Es posible definir la programación de backups y elegir la cantidad de backups que se retendrán.



3. Seleccione los volúmenes persistentes de los que desea realizar un backup.
   - Para realizar una copia de seguridad de todos los volúmenes, active la casilla de la fila de título (

).
   - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (

).



4. Si desea que todos los volúmenes actuales y futuros tengan habilitada la copia de seguridad, solo tiene que dejar activada la casilla de verificación "copia de seguridad automática de futuros volúmenes…". Si deshabilita esta configuración, deberá habilitar manualmente las copias de seguridad para volúmenes futuros.
5. Haga clic en **Activar copia de seguridad** y Cloud Backup comenzará a realizar las copias de seguridad iniciales de cada volumen seleccionado.

Resultado

Un bloque de S3 se crea automáticamente en la misma cuenta y región de AWS que el sistema Cloud Volumes ONTAP, y los archivos de backup se almacenan allí.

La consola de Kubernetes se muestra para que pueda supervisar el estado de los backups.

El futuro

Puede hacerlo "inicie y detenga backups de los volúmenes o cambie el backup programación". También puede hacerlo "restaure volúmenes completos desde un archivo de backup" Como un volumen nuevo en el mismo clúster de Kubernetes o diferente en AWS (en la misma región).

Gestionar backups para sus sistemas Kubernetes

Es posible gestionar backups de sus sistemas Kubernetes cambiando la programación de backup, habilitar/deshabilitar backups de volúmenes, eliminar backups, etc.

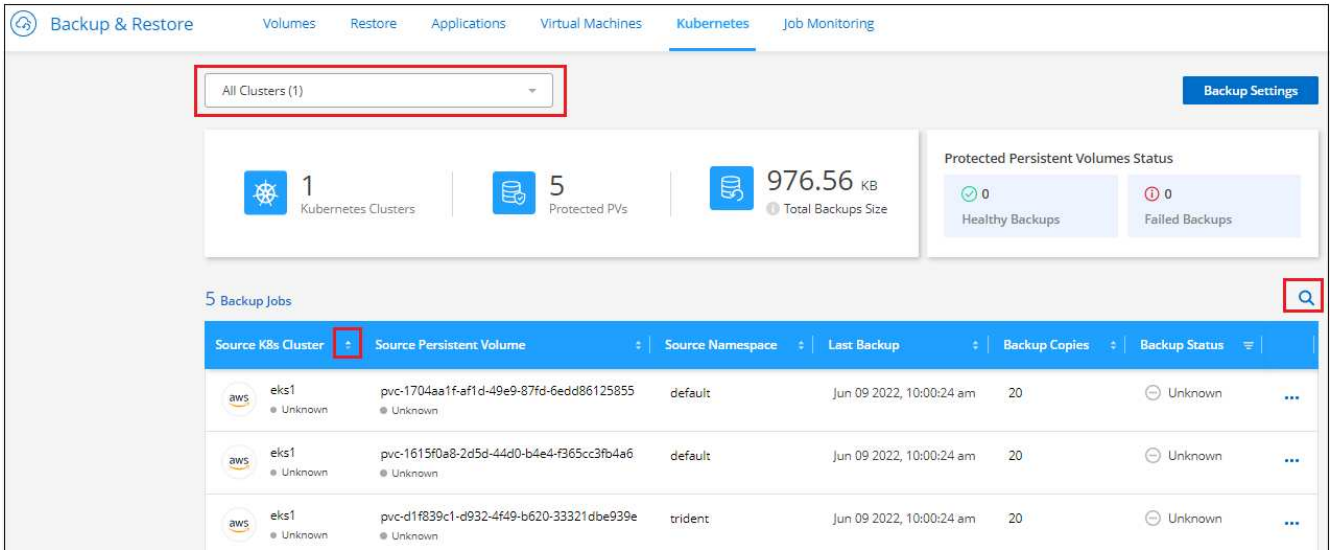
> No gestione ni modifique los archivos de backup directamente desde su entorno de proveedor de cloud. Esto puede dañar los archivos y dar como resultado una configuración no compatible.

Ver los volúmenes de los que se está realizando backup

Es posible ver una lista de todos los volúmenes de los que Cloud Backup está haciendo backup en ese momento.

Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Kubernetes** para ver la lista de volúmenes persistentes para sistemas Kubernetes.



Si busca volúmenes específicos en ciertos clústeres, puede refinar la lista por clúster y volumen, o puede utilizar el filtro de búsqueda.

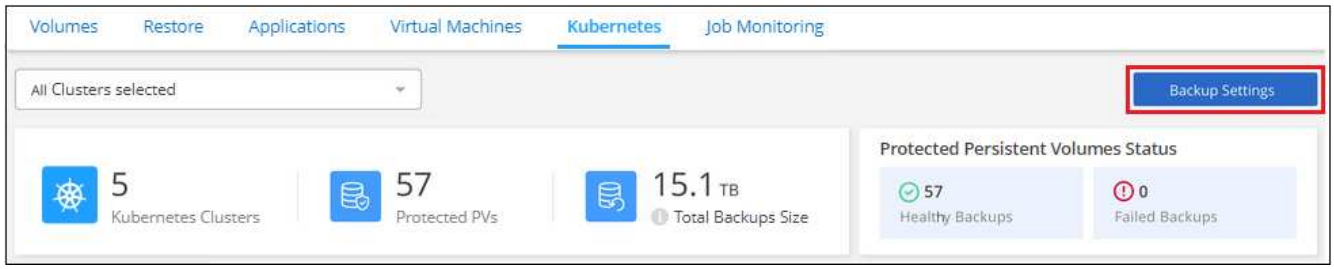
Habilitar y deshabilitar backups de volúmenes

Puede detener el backup de un volumen si no necesita copias de backup de ese volumen, y no quiere pagar por el coste de almacenar los backups. También puede añadir un nuevo volumen a la lista de backups si

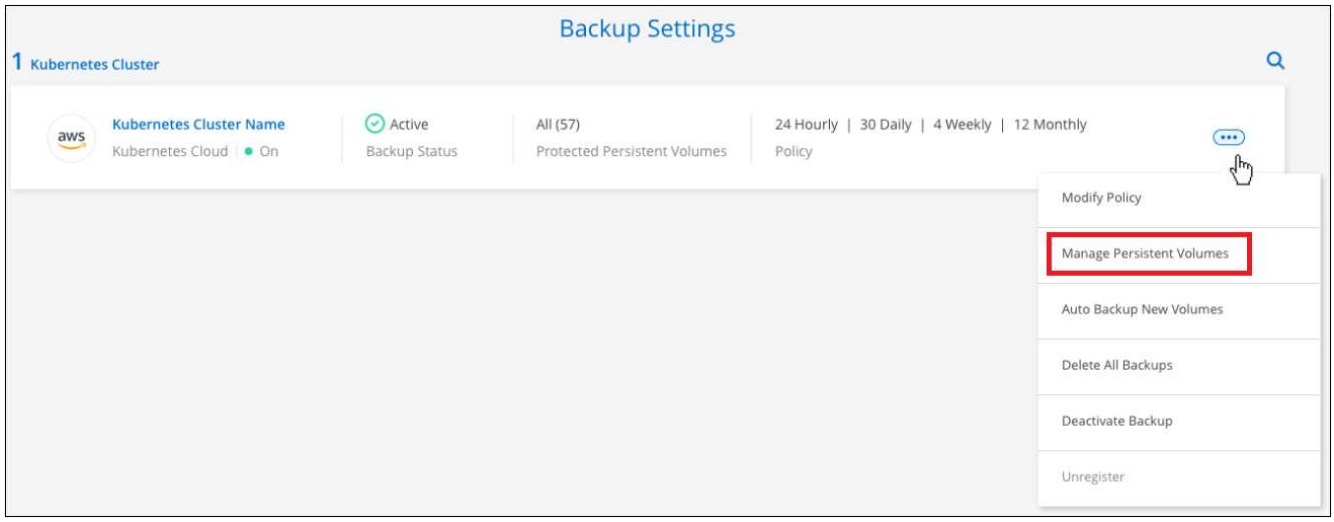
actualmente no se está realizando un backup.

Pasos

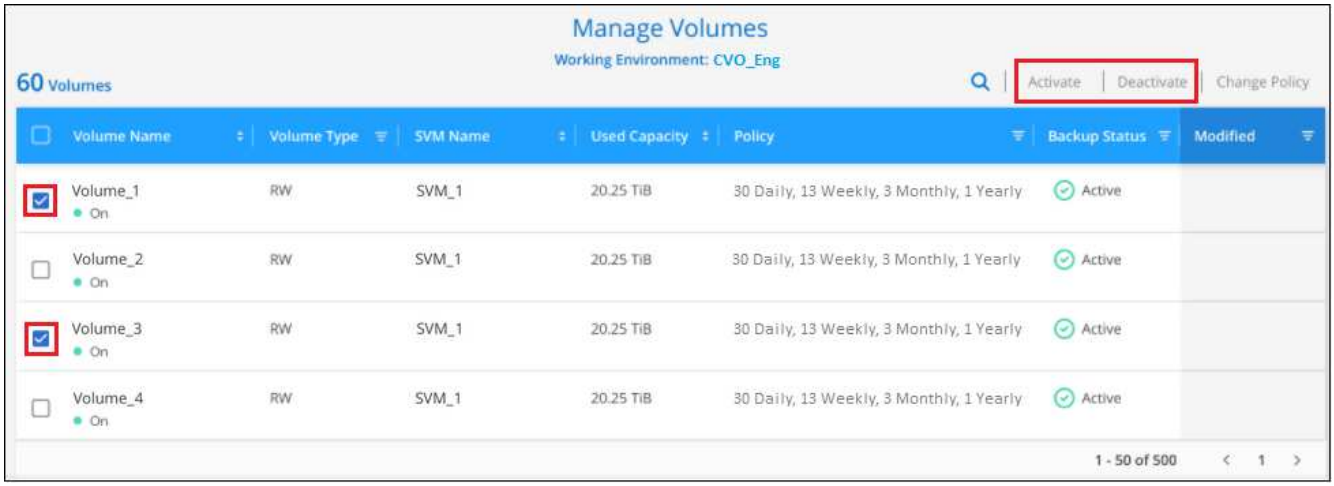
1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ••• Para el clúster de Kubernetes y seleccione **gestionar volúmenes persistentes**.



3. Seleccione la casilla de verificación para un volumen o volúmenes que desee cambiar y, a continuación, haga clic en **Activar** o **Desactivar** dependiendo de si desea iniciar o detener copias de seguridad para el volumen.



4. Haga clic en **Guardar** para confirmar los cambios.

Nota: cuando detenga la copia de seguridad de un volumen, su proveedor de cloud seguirá cobrándose por

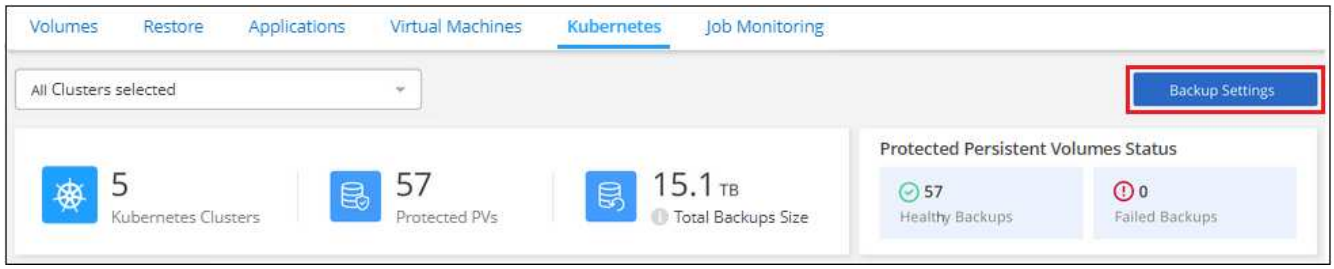
los costes de almacenamiento de objetos de la capacidad que utilizan las copias de seguridad a menos que usted eliminar los backups.

Editar una política de backup existente

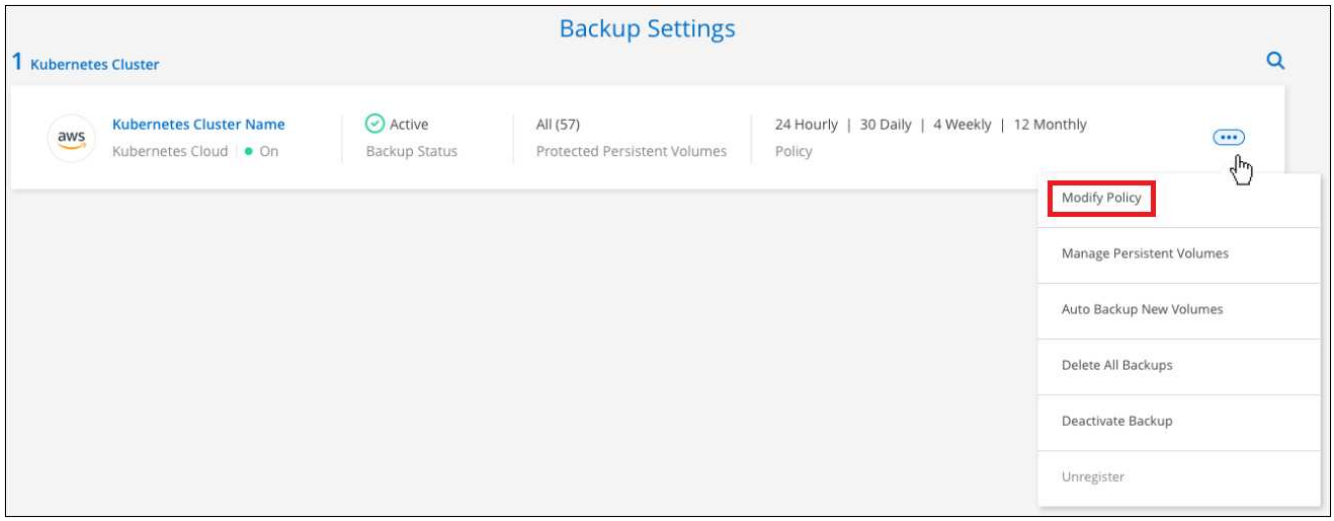
Puede cambiar los atributos de una política de backup que se aplique actualmente a los volúmenes en un entorno de trabajo. Los cambios que se aplican en la política de backup afectan a todos los volúmenes existentes que usan la política.

Pasos

1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.

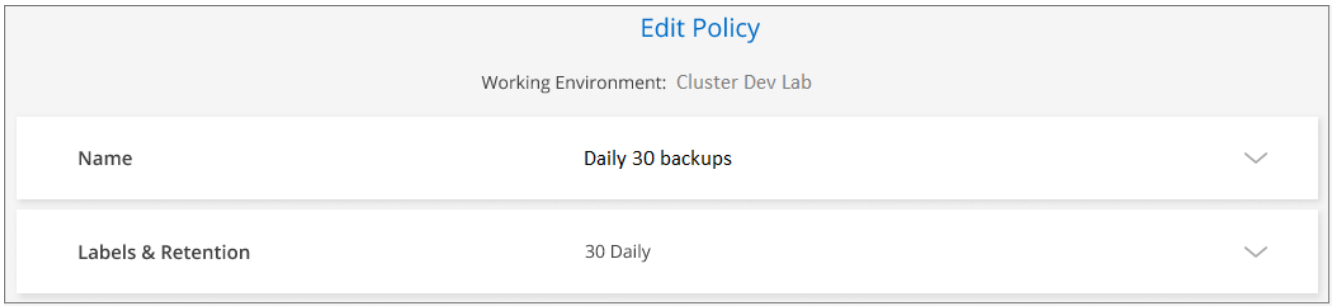


2. En la página *Backup Settings*, haga clic en ••• Para el entorno de trabajo en el que desea cambiar la configuración y seleccione **Administrar directivas**.



3. En la página *Manage Policies*, haga clic en **Edit Policy** para la política de copia de seguridad que desea cambiar en ese entorno de trabajo.

4. En la página *Edit Policy*, cambie la programación y la retención de la copia de seguridad y haga clic en **Save**.



Configurar una política de backup que se asignará a volúmenes nuevos

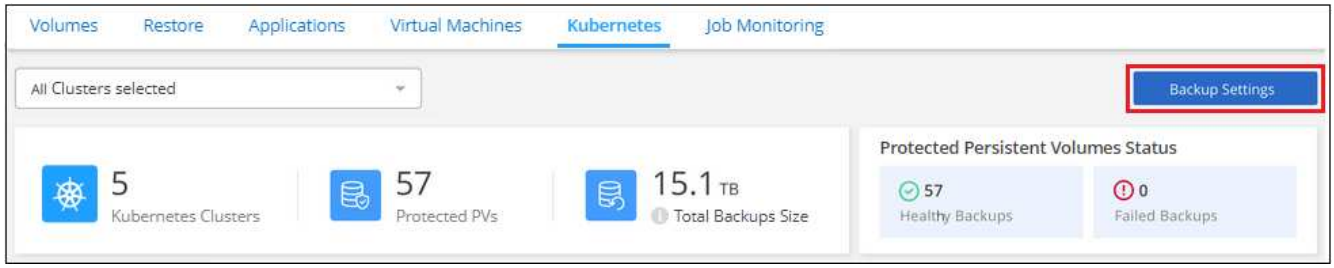
Si no seleccionó la opción para asignar automáticamente una política de backup a los volúmenes nuevos cuando activó Cloud Backup en el clúster de Kubernetes, puede elegir esta opción en la página *Backup Settings* más adelante. Si se asigna una política de backup a volúmenes recién creados, se garantizan que todos los datos estén protegidos.

Tenga en cuenta que la política que desea aplicar a los volúmenes ya debe existir.

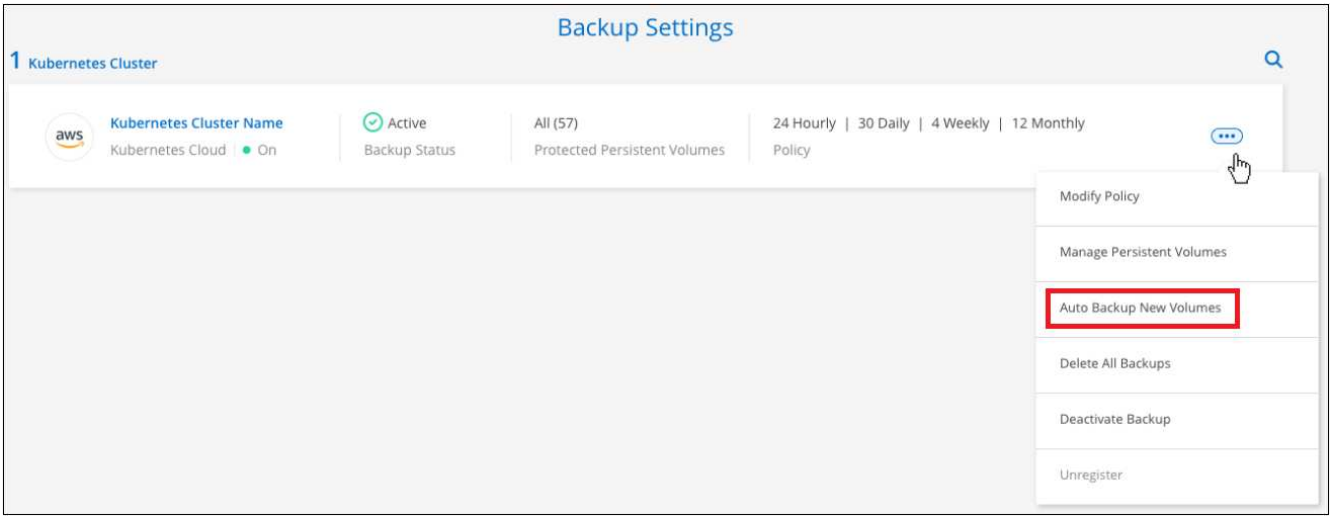
También puede deshabilitar este ajuste para que los volúmenes nuevos no se hagan backup automáticamente. En ese caso, deberá habilitar manualmente los backups para cualquier volumen concreto del que desee realizar backup en el futuro.

Pasos

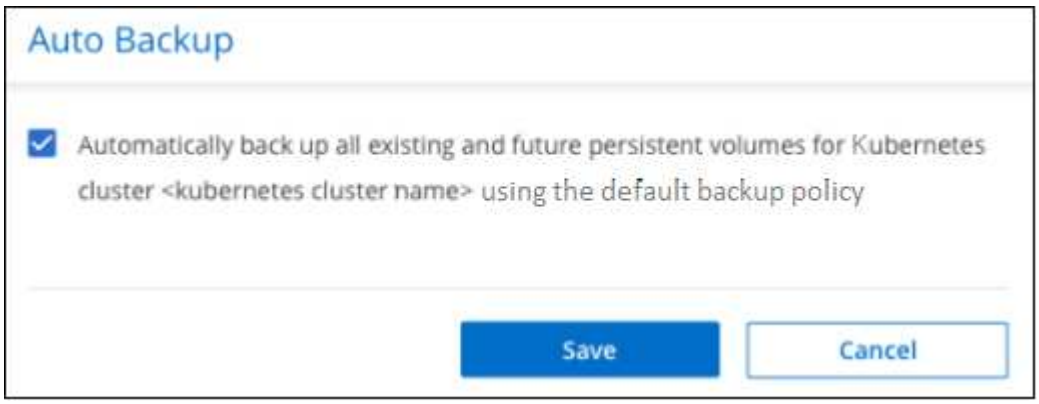
1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ••• Para el clúster Kubernetes donde existen los volúmenes, y seleccione **copia de seguridad automática de nuevos volúmenes**.



3. Seleccione la casilla de verificación "copia de seguridad automática de futuros volúmenes persistentes…", elija la política de copia de seguridad que desea aplicar a nuevos volúmenes y haga clic en **Guardar**.



Resultado

Ahora esta política de backup se aplicará a todos los volúmenes nuevos que se creen en este clúster de Kubernetes.

Ver la lista de backups de cada volumen

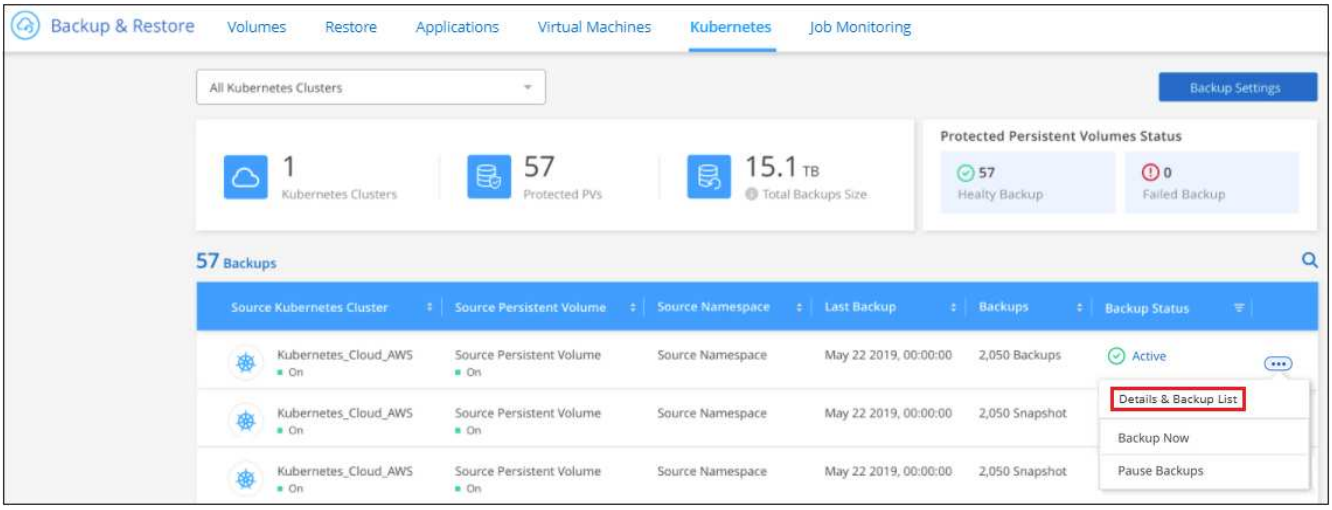
Es posible ver la lista de todos los archivos de backup que existen para cada volumen. Esta página muestra detalles sobre el volumen de origen, la ubicación de destino y los detalles de backup, como el último backup realizado, la política actual de backup, el tamaño del archivo de backup y mucho más.

Esta página también permite realizar las siguientes tareas:

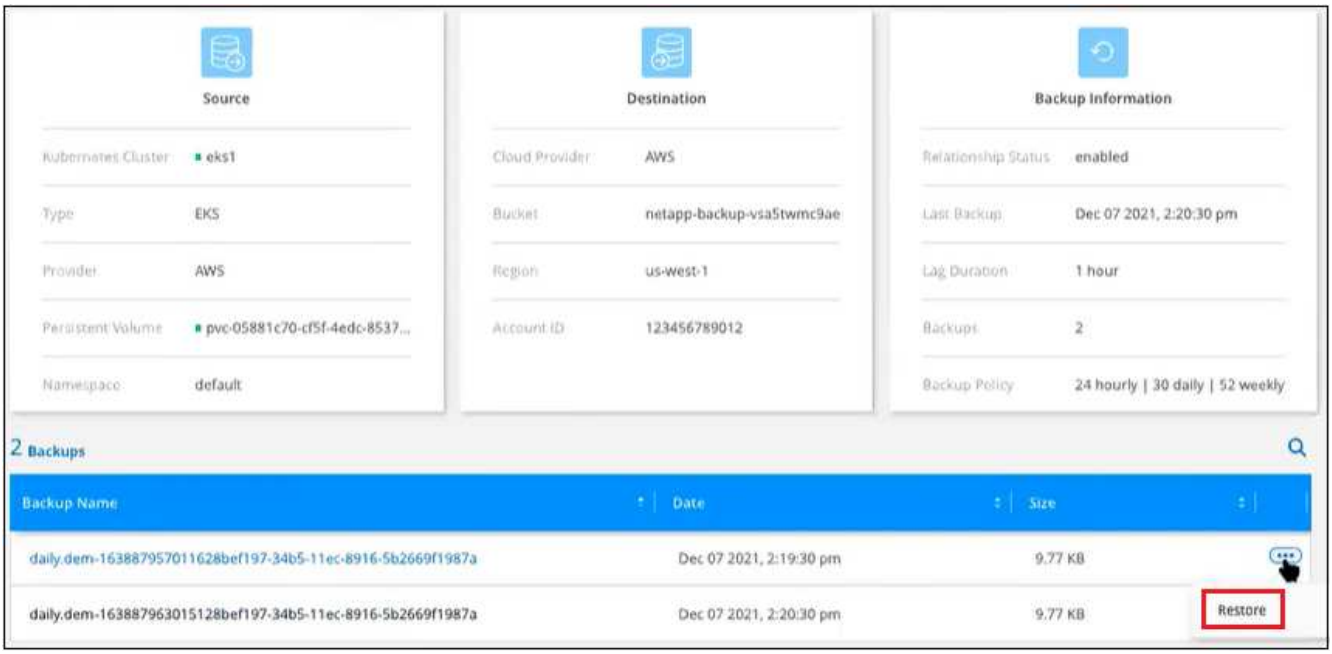
- Elimine todos los archivos de backup del volumen
- Elimine los archivos de backup individuales del volumen
- Descargue un informe de backup para el volumen

Pasos

1. En la ficha **Kubernetes**, haga clic en ••• Para el volumen de origen y seleccione **Detalles y lista de copia de seguridad**.



Se muestra la lista de todos los archivos de backup junto con detalles sobre el volumen de origen, la ubicación de destino y los detalles de la copia de seguridad.



Eliminar backups

Cloud Backup le permite eliminar un único archivo de backup, eliminar todos los backups de un volumen o eliminar todos los backups de todos los volúmenes de un clúster de Kubernetes. Es posible eliminar todos los backups si ya no se necesitan los backups o si se eliminó el volumen de origen y se desean quitar todos los backups.

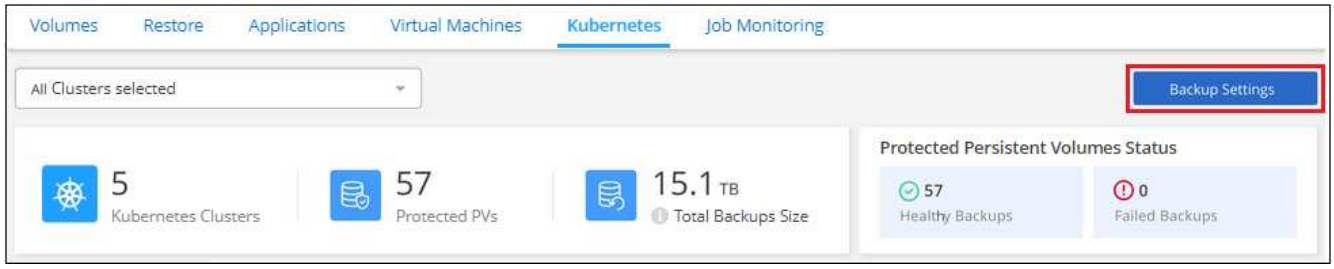
> Si piensa eliminar un entorno de trabajo o clúster que tiene copias de seguridad, debe eliminar las copias de seguridad **antes de** eliminando el sistema. Cloud Backup no elimina automáticamente las copias de seguridad cuando se elimina un sistema y no hay compatibilidad actual en la interfaz de usuario para eliminar las copias de seguridad después de que el sistema se haya eliminado. Seguirá cobrándose los costes de almacenamiento de objetos por los backups restantes.

Eliminar todos los archivos de copia de seguridad de un entorno de trabajo

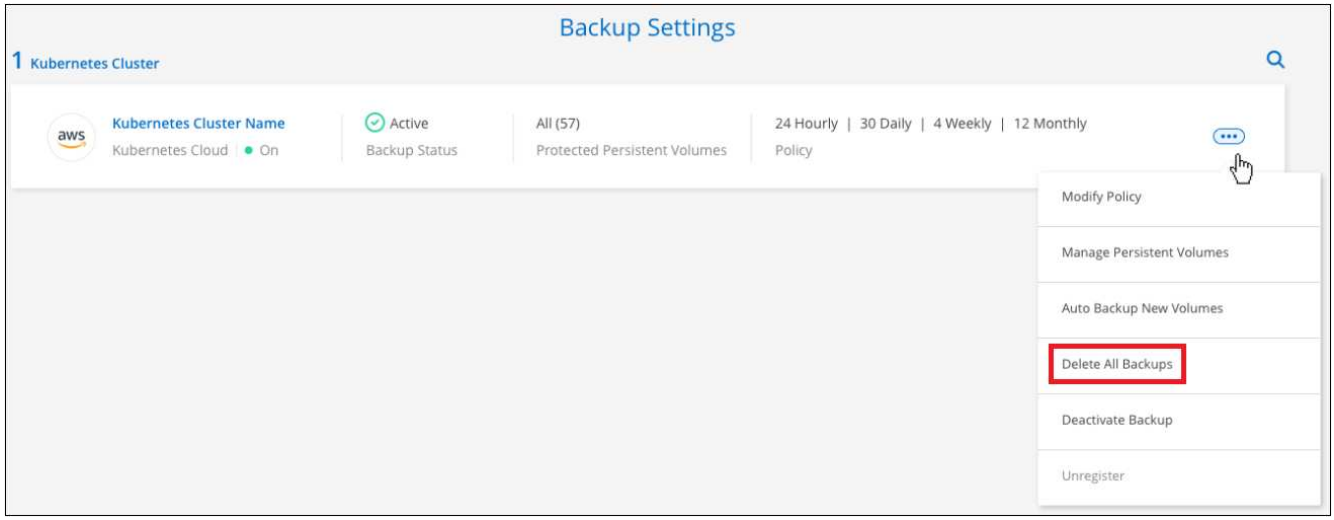
La eliminación de todos los backups de un entorno de trabajo no deshabilita los futuros backups de los volúmenes en este entorno de trabajo. Si desea detener la creación de backups de todos los volúmenes en un entorno de trabajo, puede desactivar los backups como se describe aquí.

Pasos

1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.



2. Haga clic en ••• Para el clúster Kubernetes en el que desea eliminar todas las copias de seguridad y seleccione **Eliminar todas las copias de seguridad**.



3. En el cuadro de diálogo de confirmación, introduzca el nombre del entorno de trabajo y haga clic en **Eliminar**.

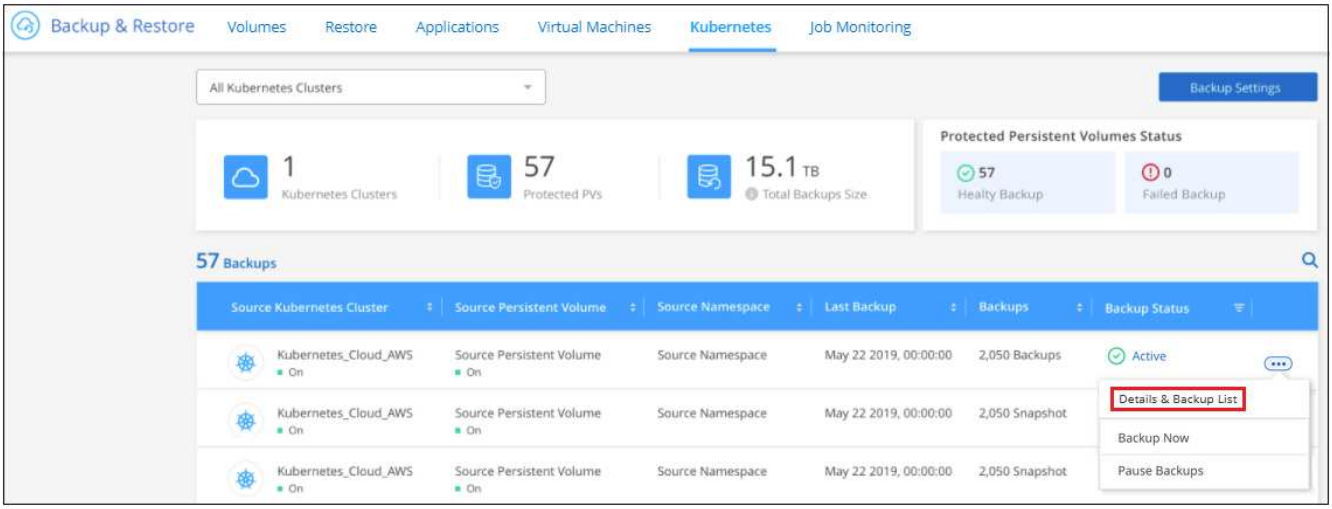
Eliminación de todos los archivos de backup de un volumen

La eliminación de todos los backups de un volumen también deshabilita los futuros backups para ese volumen.

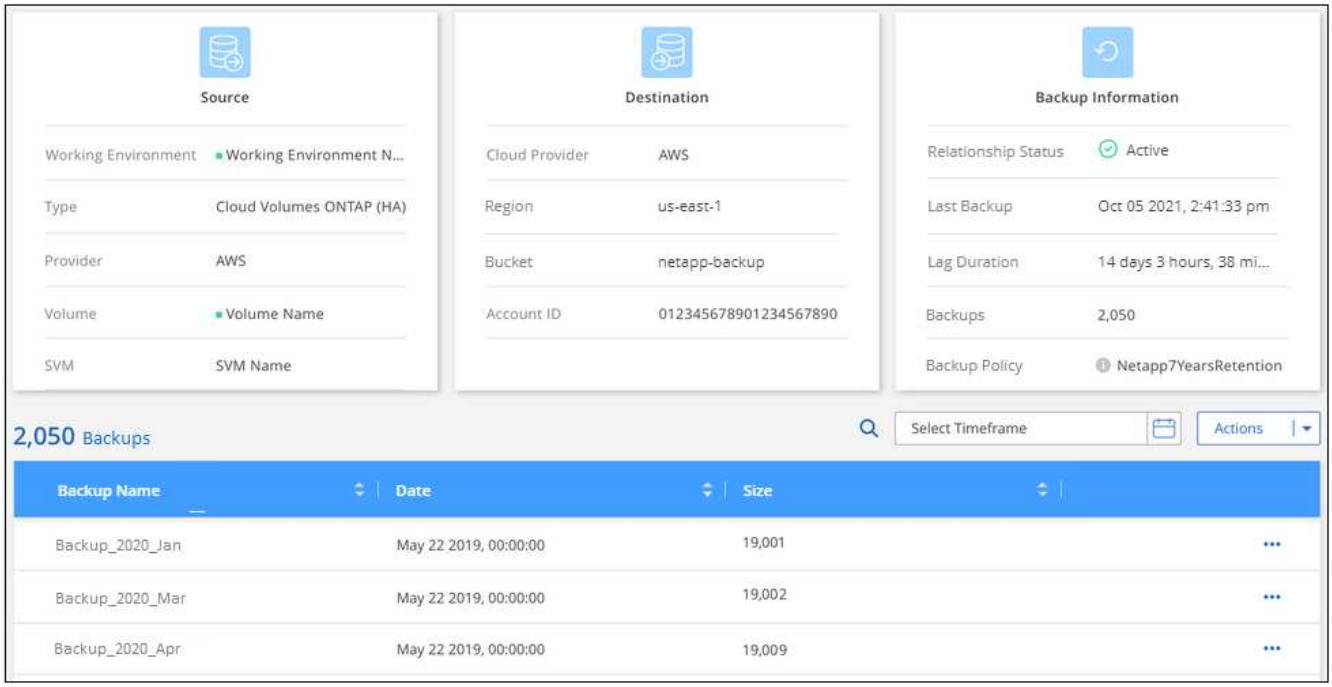
Puede hacerlo reinicie haciendo backups para el volumen En cualquier momento desde la página Manage backups.

Pasos

1. En la ficha **Kubernetes**, haga clic en ••• Para el volumen de origen y seleccione **Detalles y lista de copia de seguridad**.



Se muestra la lista de todos los archivos de copia de seguridad.



2. Haga clic en **acciones** > **Eliminar todas las copias de seguridad**.

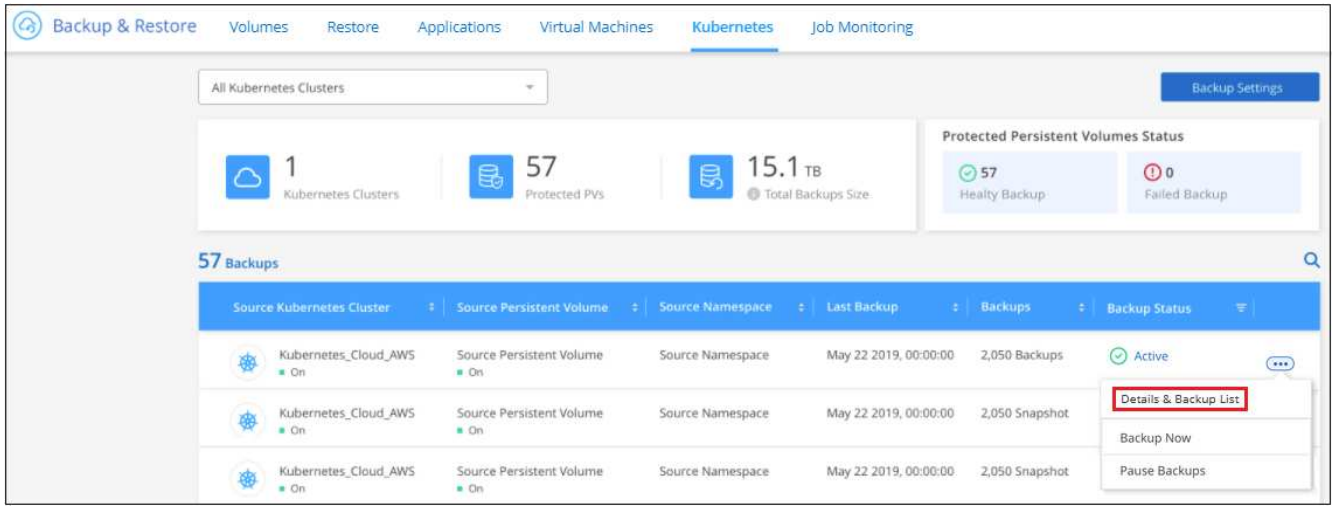
3. En el cuadro de diálogo de confirmación, introduzca el nombre del volumen y haga clic en **Eliminar**.

Eliminar un único archivo de backup para un volumen

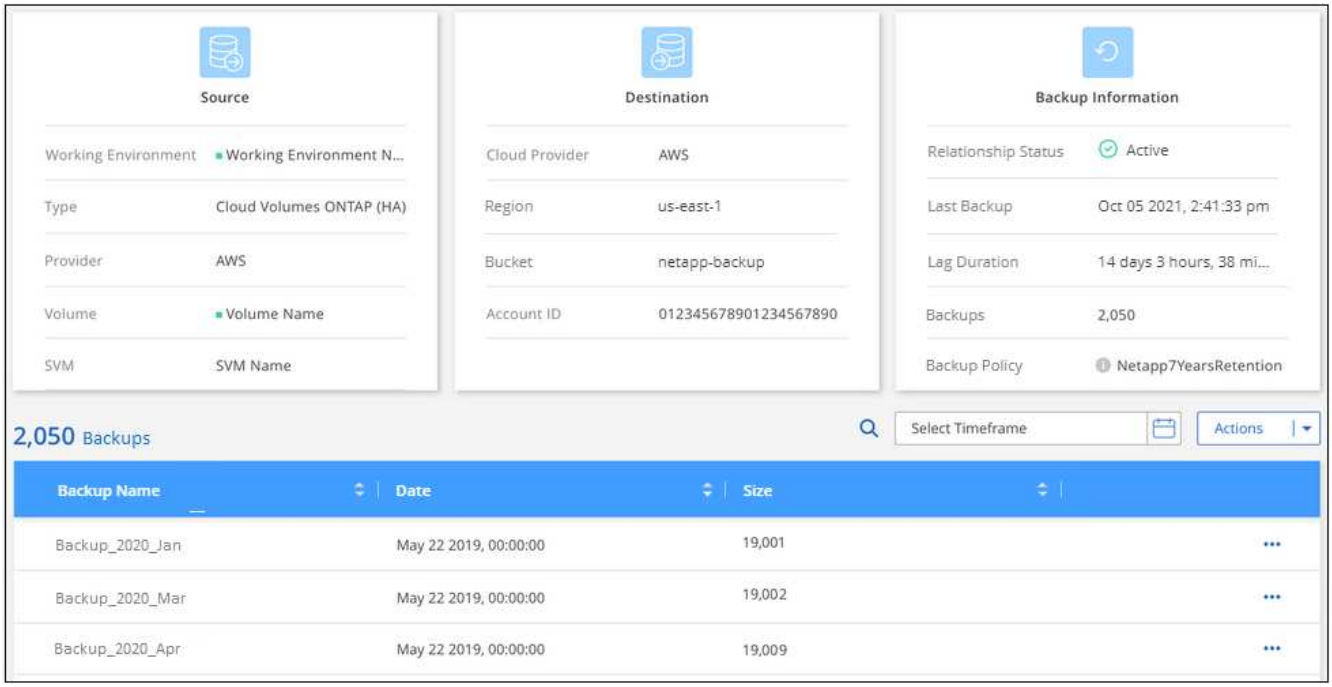
Puede eliminar un único archivo de copia de seguridad. Esta función solo está disponible si el backup de volumen se creó a partir de un sistema con ONTAP 9.8 o posterior.

Pasos

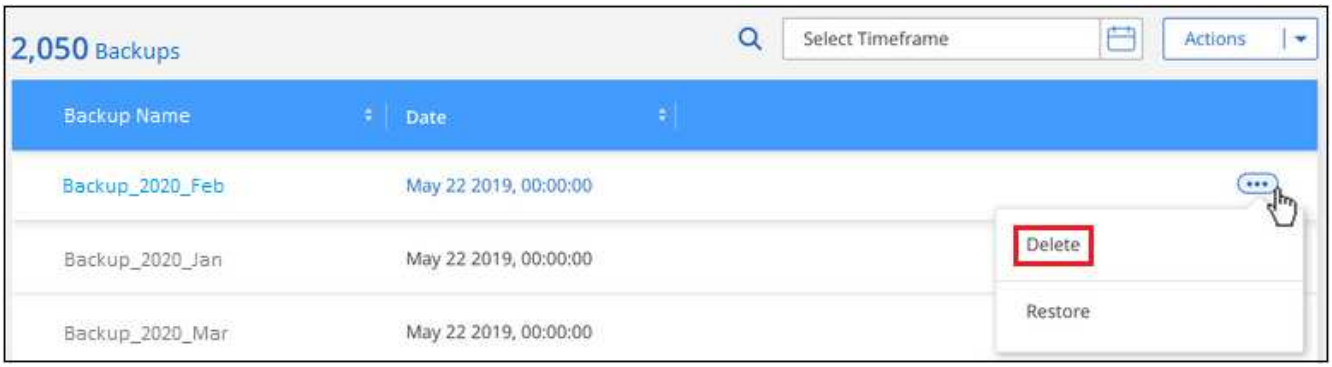
1. En la ficha **Kubernetes**, haga clic en ••• Para el volumen de origen y seleccione **Detalles y lista de copia de seguridad**.



Se muestra la lista de todos los archivos de copia de seguridad.



2. Haga clic en ••• Para el archivo de copia de seguridad de volumen que desea eliminar y haga clic en **Eliminar**.



3. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

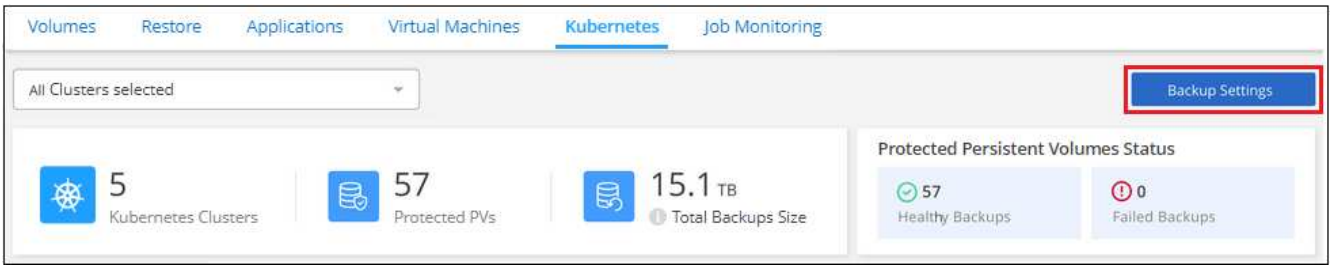
Desactivación de Cloud Backup en un entorno de trabajo

Al deshabilitar Cloud Backup para un entorno de trabajo, se desactivan los backups de cada volumen en el sistema y también se deshabilita la capacidad para restaurar un volumen. No se eliminarán los backups existentes. Esto no anula el registro del servicio de backup de este entorno de trabajo y básicamente le permite pausar toda la actividad de backup y restauración durante un periodo de tiempo.

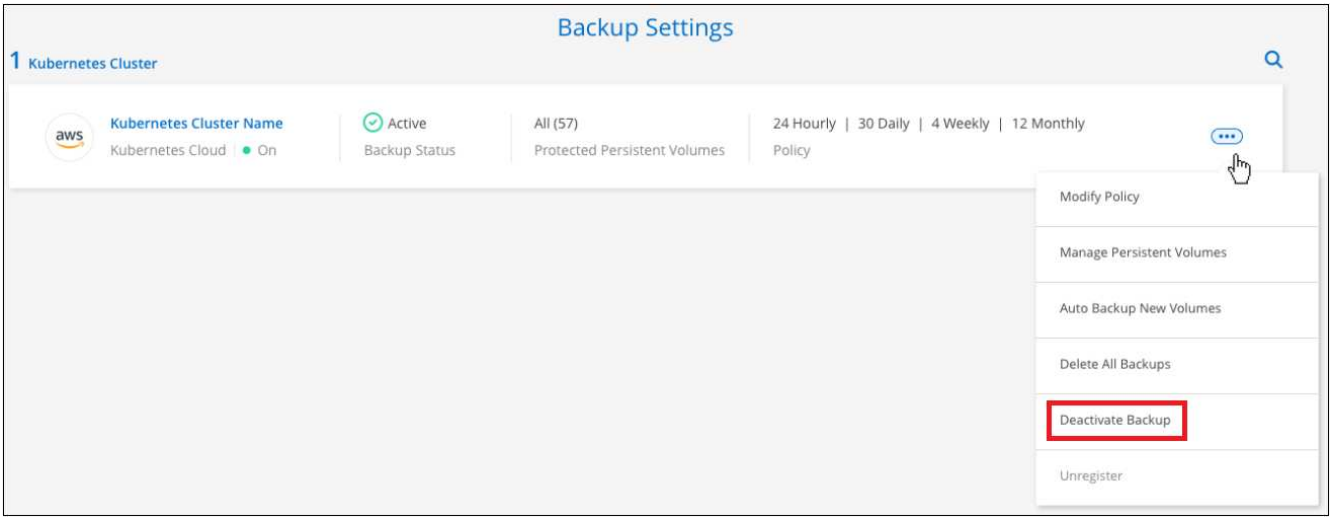
Tenga en cuenta que su proveedor de cloud seguirá facturando los costes del almacenamiento de objetos por la capacidad que utilicen sus backups a menos que usted eliminar los backups.

Pasos

1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ••• En el entorno de trabajo o en el clúster Kubernetes, donde desea desactivar las copias de seguridad y seleccionar **Desactivar copia de seguridad**.



3. En el cuadro de diálogo de confirmación, haga clic en **Desactivar**.

Aparece un botón **Activar copia de seguridad** para ese entorno de trabajo mientras la copia de seguridad está desactivada. Haga clic en este botón para volver a habilitar la funcionalidad de backup para ese entorno de trabajo.

Cancelación del registro de Cloud Backup para un entorno de trabajo

Es posible cancelar el registro de Cloud Backup para un entorno de trabajo si ya no desea usar la funcionalidad de backup y quiere dejar de estar cargado por backups en ese entorno de trabajo. Normalmente, esta función se usa cuando se planea eliminar un clúster de Kubernetes y se desea cancelar el servicio de backup.

También puede usar esta función si desea cambiar el almacén de objetos de destino donde se almacenan los backups del clúster. Después de cancelar el registro de Cloud Backup para el entorno laboral, puede habilitar Cloud Backup para ese clúster mediante la nueva información del proveedor de cloud.

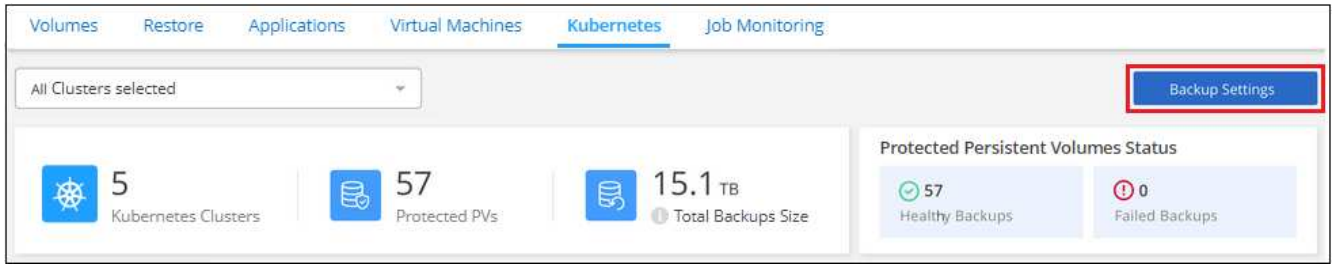
Para poder cancelar el registro de Cloud Backup, debe realizar los siguientes pasos en el siguiente orden:

- Desactivar Cloud Backup en el entorno de trabajo
- Eliminar todos los backups de ese entorno de trabajo

La opción cancelar el registro no estará disponible hasta que se completen estas dos acciones.

Pasos

1. En la ficha **Kubernetes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ••• Para el clúster Kubernetes, donde desea cancelar el registro del servicio de copia de seguridad y seleccione **Unregister**.

3. En el cuadro de diálogo de confirmación, haga clic en **Unregister**.

Restaurar los datos de Kubernetes a partir de los archivos de backup

Los backups se almacenan en un almacén de objetos en su cuenta de cloud para que pueda restaurar datos desde un momento específico. Es posible restaurar un volumen completo de Kubernetes persistente desde un archivo de backup guardado.

Puede restaurar un volumen persistente (como un volumen nuevo) en el mismo entorno de trabajo o en otro entorno de trabajo que utilice la misma cuenta de cloud.

Entornos de trabajo y proveedores de almacenamiento de objetos compatibles

Es posible restaurar un volumen de un archivo de backup de Kubernetes en los siguientes entornos de trabajo:

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino ifdef::aws[]
Amazon S3	Clúster de Kubernetes en endif de AWS::aws[] ifdef::Azure[]
Azure Blob	Clúster de Kubernetes en endif de Azure::Azure[] ifdef::gcp[]
Google Cloud Storage	Clúster de Kubernetes en Google endif::gcp[]

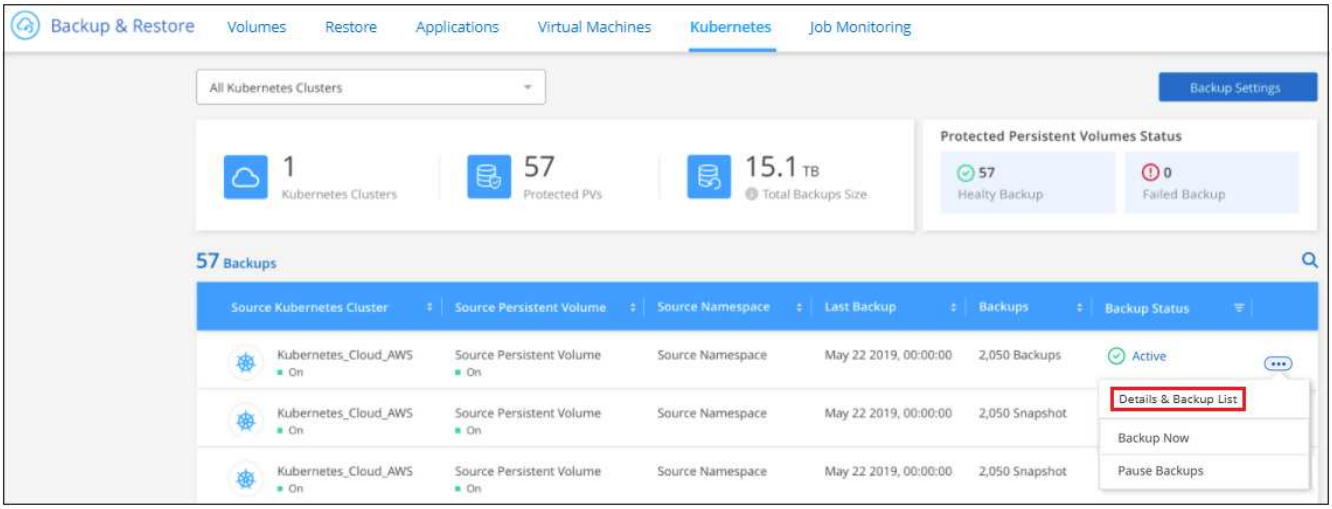
Restaurar volúmenes desde un archivo de backup de Kubernetes

Al restaurar un volumen persistente a partir de un archivo de copia de seguridad, BlueXP crea un volumen *new* utilizando los datos de la copia de seguridad. Es posible restaurar los datos en un volumen del mismo clúster de Kubernetes o en un clúster de Kubernetes diferente que se encuentre en la misma cuenta de cloud que el clúster de Kubernetes de origen.

Antes de comenzar, se debe conocer el nombre del volumen que se desea restaurar y la fecha del archivo de backup que se desea usar para crear el volumen recién restaurado.

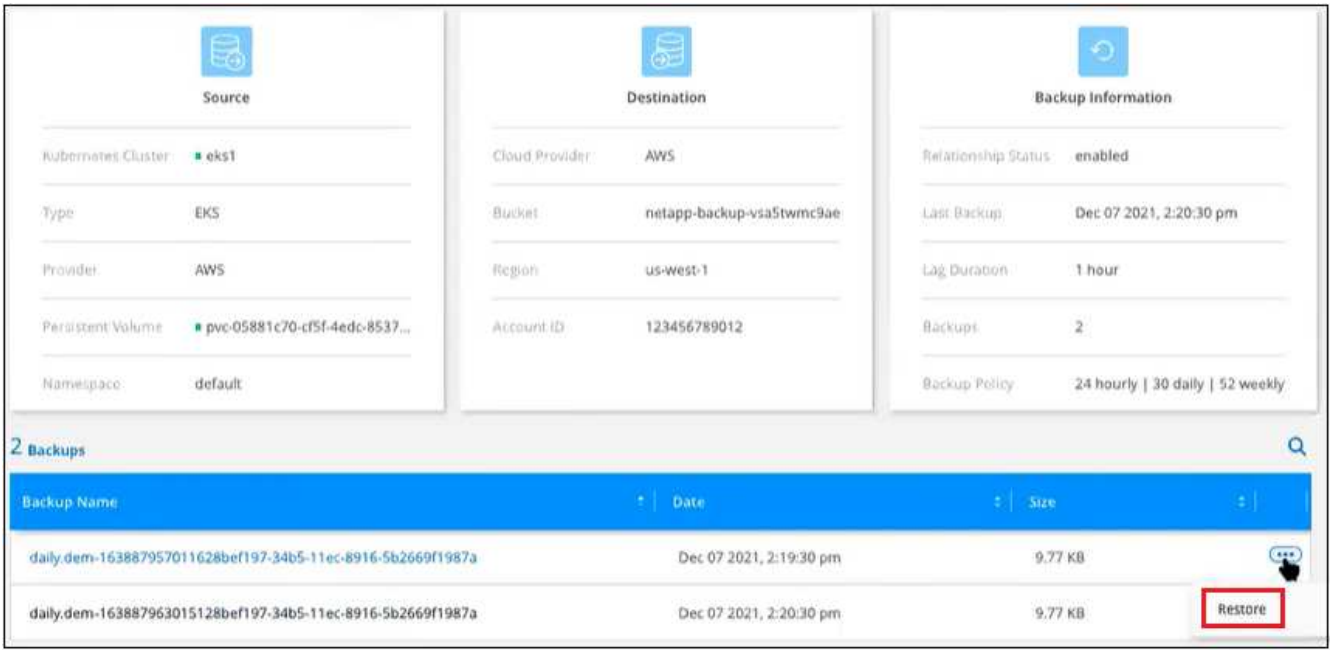
Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Kubernetes** y aparecerá el panel de Kubernetes.



3. Busque el volumen que desea restaurar, haga clic en •••Y, a continuación, haga clic en **Lista de detalles y copias de seguridad**.

   La lista de todos los archivos de backup de ese volumen se muestra junto con detalles sobre el volumen de origen, la ubicación de destino y los detalles de backup.



4. Busque el archivo de backup específico que desea restaurar según la Marca de fecha/hora, haga clic en •••Y luego **Restaurar**.
5. En la página *Select Destination*, seleccione el *Kubernetes cluster* donde desea restaurar el volumen, el *Namespace*, el *Storage Class* y el nuevo *Persistent volume name*.

6. Haga clic en **Restaurar** y volverá al panel de Kubernetes para poder revisar el progreso de la operación de restauración.

Resultado

BlueXP crea un nuevo volumen en el clúster de Kubernetes según el backup seleccionado. Puede hacerlo "gestione la configuración de backup para este nuevo volumen" según sea necesario.