



# **Realice backups y restauraciones de datos de ONTAP**

## **BlueXP backup and recovery**

NetApp  
June 02, 2025

# Tabla de contenidos

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Realice backups y restauraciones de datos de ONTAP .....                                                    | 1  |
| Protege tus datos de volúmenes de ONTAP con backup y recuperación de BlueXP .....                           | 1  |
| Funciones .....                                                                                             | 2  |
| Entornos de trabajo compatibles para operaciones de backup y restauración .....                             | 3  |
| Volúmenes compatibles .....                                                                                 | 5  |
| Coste .....                                                                                                 | 5  |
| Licencia .....                                                                                              | 6  |
| Funcionamiento del backup y la recuperación de BlueXP .....                                                 | 7  |
| Consideraciones sobre la política de organización en niveles de FabricPool .....                            | 11 |
| Planifique su viaje de protección con la copia de seguridad y recuperación de BlueXP .....                  | 11 |
| Qué funciones de protección utilizará .....                                                                 | 11 |
| Qué arquitectura de backup utilizará .....                                                                  | 13 |
| Utilizará las políticas predeterminadas para snapshots, replicaciones y backups .....                       | 15 |
| ¿Dónde residen mis políticas? .....                                                                         | 16 |
| ¿Desea crear su propio contenedor de almacenamiento de objetos .....                                        | 17 |
| El modo de puesta en marcha de BlueXP Connector utiliza .....                                               | 17 |
| Administre políticas de respaldo para volúmenes ONTAP con BlueXP Backup and Recovery .....                  | 19 |
| Ver políticas para un entorno de trabajo .....                                                              | 19 |
| Crear políticas .....                                                                                       | 20 |
| Editar una política .....                                                                                   | 22 |
| Eliminar una política .....                                                                                 | 22 |
| Obtenga más información .....                                                                               | 23 |
| Opciones de política de copia de seguridad a objeto en la copia de seguridad y recuperación de BlueXP ..... | 23 |
| Opciones de programación de backups .....                                                                   | 23 |
| Opciones de protección contra DataLock y Ransomware .....                                                   | 24 |
| Opciones de almacenamiento de archivado .....                                                               | 32 |
| Administre las opciones de almacenamiento de copia de seguridad en objetos en la página                     |    |
| Configuración avanzada de la copia de seguridad y recuperación de BlueXP .....                              | 34 |
| Ver la configuración de backup en el nivel del clúster .....                                                | 34 |
| Cambie el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos ..           | 36 |
| Cambie si las copias snapshot históricas se exportan como archivos de backup .....                          | 36 |
| Cambie si las instantáneas "anuales" se eliminan del sistema de origen .....                                | 37 |
| Habilitar o deshabilitar los análisis de ransomware .....                                                   | 37 |
| Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3 con la copia de             |    |
| seguridad y recuperación de BlueXP .....                                                                    | 38 |
| Inicio rápido .....                                                                                         | 38 |
| Verifique la compatibilidad con la configuración .....                                                      | 39 |
| Verifique los requisitos de licencia .....                                                                  | 40 |
| Prepare el conector BlueXP .....                                                                            | 41 |
| Compruebe los requisitos de red de ONTAP para replicar volúmenes .....                                      | 44 |
| Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP .....                        | 44 |
| Active backups en sus ONTAP Volumes .....                                                                   | 46 |
| El futuro .....                                                                                             | 50 |

|                                                                                                                                                              |     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en el almacenamiento de blobs de Azure con BlueXP Backup and Recovery .....               | 50  |
| Inicio rápido .....                                                                                                                                          | 50  |
| Verifique la compatibilidad con la configuración .....                                                                                                       | 51  |
| Verifique los requisitos de licencia .....                                                                                                                   | 52  |
| Prepare el conector BlueXP .....                                                                                                                             | 53  |
| Compruebe los requisitos de red de ONTAP para replicar volúmenes .....                                                                                       | 55  |
| Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP .....                                                                         | 55  |
| Active backups en sus ONTAP Volumes .....                                                                                                                    | 57  |
| El futuro .....                                                                                                                                              | 61  |
| Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con la copia de seguridad y recuperación de BlueXP .....          | 62  |
| Inicio rápido .....                                                                                                                                          | 62  |
| Verifique la compatibilidad con la configuración .....                                                                                                       | 63  |
| Verifique los requisitos de licencia .....                                                                                                                   | 64  |
| Prepare el conector BlueXP .....                                                                                                                             | 64  |
| Compruebe los requisitos de red de ONTAP para replicar volúmenes .....                                                                                       | 66  |
| Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP .....                                                                         | 66  |
| Preparar Google Cloud Storage como destino de backup .....                                                                                                   | 68  |
| Active backups en sus ONTAP Volumes .....                                                                                                                    | 70  |
| El futuro .....                                                                                                                                              | 74  |
| Realice una copia de seguridad de los datos locales de ONTAP en Amazon S3 con la copia de seguridad y recuperación de BlueXP .....                           | 75  |
| Inicio rápido .....                                                                                                                                          | 75  |
| Identifique el método de conexión .....                                                                                                                      | 76  |
| Prepare el conector BlueXP .....                                                                                                                             | 77  |
| Verifique los requisitos de licencia .....                                                                                                                   | 78  |
| Prepare los clústeres ONTAP .....                                                                                                                            | 79  |
| Prepare Amazon S3 como destino de backup .....                                                                                                               | 81  |
| Active backups en sus ONTAP Volumes .....                                                                                                                    | 86  |
| El futuro .....                                                                                                                                              | 90  |
| Realice una copia de seguridad de los datos de ONTAP locales en el almacenamiento de blobs de Azure con la copia de seguridad y recuperación de BlueXP ..... | 90  |
| Inicio rápido .....                                                                                                                                          | 90  |
| Identifique el método de conexión .....                                                                                                                      | 91  |
| Prepare el conector BlueXP .....                                                                                                                             | 93  |
| Verifique los requisitos de licencia .....                                                                                                                   | 96  |
| Prepare los clústeres ONTAP .....                                                                                                                            | 96  |
| Preparar Azure Blob como destino de backup .....                                                                                                             | 98  |
| Active backups en sus ONTAP Volumes .....                                                                                                                    | 98  |
| El futuro .....                                                                                                                                              | 103 |
| Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con la copia de seguridad y recuperación de BlueXP .....                | 103 |
| Inicio rápido .....                                                                                                                                          | 103 |
| Identifique el método de conexión .....                                                                                                                      | 104 |

|                                                                                                                                          |     |
|------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Prepare el conector BlueXP . . . . .                                                                                                     | 106 |
| Prepare la conexión a redes para el conector . . . . .                                                                                   | 107 |
| Verifique los requisitos de licencia . . . . .                                                                                           | 108 |
| Prepare los clústeres ONTAP . . . . .                                                                                                    | 108 |
| Preparar Google Cloud Storage como destino de backup . . . . .                                                                           | 110 |
| Active backups en sus ONTAP Volumes . . . . .                                                                                            | 112 |
| El futuro . . . . .                                                                                                                      | 116 |
| Realice una copia de seguridad de los datos locales de ONTAP en ONTAP S3 con la copia de seguridad y recuperación de BlueXP . . . . .    | 117 |
| Inicio rápido . . . . .                                                                                                                  | 117 |
| Identifique el método de conexión . . . . .                                                                                              | 118 |
| Prepare el conector BlueXP . . . . .                                                                                                     | 120 |
| Verifique los requisitos de licencia . . . . .                                                                                           | 121 |
| Prepare los clústeres ONTAP . . . . .                                                                                                    | 121 |
| Prepare ONTAP S3 como destino de backup . . . . .                                                                                        | 123 |
| Active backups en sus ONTAP Volumes . . . . .                                                                                            | 124 |
| El futuro . . . . .                                                                                                                      | 128 |
| Realice una copia de seguridad de los datos locales de ONTAP en StorageGRID con la copia de seguridad y recuperación de BlueXP . . . . . | 128 |
| Inicio rápido . . . . .                                                                                                                  | 129 |
| Identifique el método de conexión . . . . .                                                                                              | 130 |
| Prepare el conector BlueXP . . . . .                                                                                                     | 130 |
| Verifique los requisitos de licencia . . . . .                                                                                           | 131 |
| Prepare los clústeres ONTAP . . . . .                                                                                                    | 131 |
| Preparar StorageGRID como destino de backup . . . . .                                                                                    | 133 |
| Active backups en sus ONTAP Volumes . . . . .                                                                                            | 136 |
| El futuro . . . . .                                                                                                                      | 140 |
| Migre volúmenes usando SnapMirror a Cloud Resync con respaldo y recuperación de BlueXP . . . . .                                         | 141 |
| Funcionamiento del backup y recuperación de datos SnapMirror de BlueXP para la resincronización en el cloud . . . . .                    | 141 |
| Notas de procedimiento . . . . .                                                                                                         | 142 |
| Cómo migrar volúmenes mediante SnapMirror para resincronizar con la nube . . . . .                                                       | 143 |
| Administre copias de seguridad de sus sistemas ONTAP con BlueXP Backup and Recovery . . . . .                                            | 145 |
| Vea el estado de backup de los volúmenes en sus entornos de trabajo . . . . .                                                            | 145 |
| Activar backup en volúmenes adicionales en un entorno de trabajo . . . . .                                                               | 146 |
| Cambie la configuración de backup asignada a los volúmenes existentes . . . . .                                                          | 147 |
| Crear un backup manual de volúmenes en cualquier momento . . . . .                                                                       | 149 |
| Consulte la lista de backups de cada volumen . . . . .                                                                                   | 150 |
| Ejecuta un análisis de ransomware en un backup de volúmenes en el almacenamiento de objetos . . . . .                                    | 151 |
| Gestione la relación de replicación con el volumen de origen . . . . .                                                                   | 152 |
| Edite una política de backup en el cloud existente . . . . .                                                                             | 153 |
| Añada una nueva política de backup en el cloud . . . . .                                                                                 | 156 |
| Eliminar backups . . . . .                                                                                                               | 159 |
| Elimine las relaciones de backup de volúmenes . . . . .                                                                                  | 161 |
| Desactiva el backup y la recuperación de BlueXP para un entorno de trabajo . . . . .                                                     | 162 |

|                                                                                             |     |
|---------------------------------------------------------------------------------------------|-----|
| Cancela el registro de backup y recuperación de BlueXP para un entorno de trabajo . . . . . | 163 |
| Restaura datos de ONTAP desde archivos de respaldo con BlueXP Backup and Recovery . . . . . | 164 |
| La Consola de restauración . . . . .                                                        | 165 |
| Comparación de examinar y restaurar y buscar y restaurar . . . . .                          | 166 |
| Restaura datos de ONTAP mediante Examinar y Restaurar . . . . .                             | 167 |
| Restaura datos de ONTAP con Search & Restore . . . . .                                      | 180 |

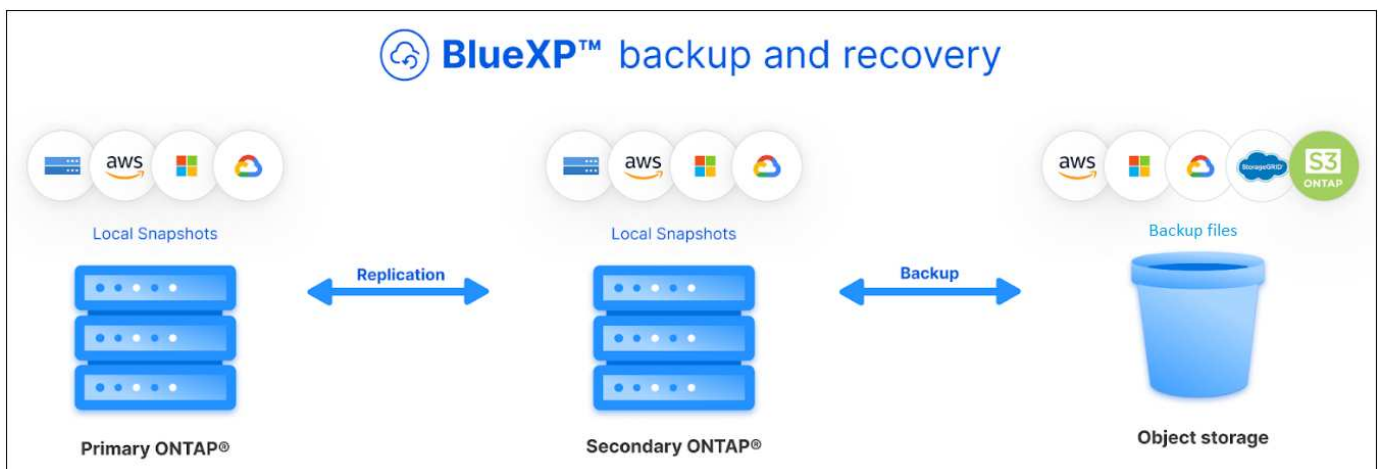
# Realice backups y restauraciones de datos de ONTAP

## Protege tus datos de volúmenes de ONTAP con backup y recuperación de BlueXP

El servicio de backup y recuperación de datos de BlueXP ofrece funcionalidades de backup y restauración para proteger y archivar a largo plazo los datos de sus volúmenes de ONTAP. Puede implementar una estrategia 3-2-1 donde tiene 3 copias de los datos de origen en 2 sistemas de almacenamiento diferentes junto con una copia 1 en el cloud.

Tras la activación, el backup y la recuperación crean backups incrementales permanentes de bloques que se almacenan en otro clúster de ONTAP y en el almacenamiento de objetos en el cloud. Además del volumen de origen, dispone de:

- Copia Snapshot del volumen en el sistema de origen
- Se replica el volumen en un sistema de almacenamiento diferente
- Backup del volumen en el almacenamiento de objetos



El backup y la recuperación de datos de BlueXP aprovecha la tecnología de replicación de datos de SnapMirror de NetApp para garantizar que todos los backups estén totalmente sincronizados creando copias de Snapshot y transfiriéndolas a las ubicaciones de backup.

Algunas de las ventajas del enfoque de 3-2-1 son las siguientes:

- Múltiples copias de datos proporcionan protección multicapa contra amenazas de ciberseguridad internas (internas) y externas.
- Varios tipos de medios garantizan la viabilidad de la conmutación al nodo de respaldo en caso de fallo físico o lógico de un tipo de medio.
- La copia in situ facilita la restauración rápida, con copias externas listas en caso de que la copia in situ esté comprometida.

Cuando sea necesario, puede restaurar un *volume* entero, una *folder* o uno o varios *files*, desde cualquiera de las copias de seguridad en el mismo entorno de trabajo o en otro diferente.

## Funciones

- Características de replicación:\*
- Replicar datos entre sistemas de almacenamiento de ONTAP para permitir las operaciones de backup y recuperación ante desastres.
- Garantice la fiabilidad de su entorno de recuperación ante desastres con una gran disponibilidad.
- Cifrado ONTAP en vuelo nativo configurado mediante clave precompartida (PSK) entre los dos sistemas.
- Los datos copiados son inmutables hasta que sean editables y estén listos para su uso.
- La replicación se repara automáticamente en caso de fallo de transferencia.
- En comparación con el "[Servicio de replicación de BlueXP](#)", La replicación en el backup y la recuperación de BlueXP incluye las siguientes características:
  - Replique varios volúmenes de FlexVol de una vez en un sistema secundario.
  - Restaure un volumen replicado en el sistema de origen o en otro sistema mediante la interfaz de usuario de.

Consulte "[Limitaciones de replicación](#)" Para acceder a una lista de funciones de replicación que no están disponibles con el backup y la recuperación de datos de BlueXP.

- Características de copia de seguridad a objeto:\*
- Realice backups de copias independientes de sus volúmenes de datos 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.
- Cree una política de backup que se aplicará a todos los volúmenes futuros que se creen en el clúster.
- Cree archivos de backup inmutables para que estén bloqueados y protegidos durante el período de retención.
- Analice archivos de copia de seguridad para detectar posibles ataques de ransomware y quite/reemplace automáticamente las copias de seguridad infectadas.
- Apilar los archivos de backup antiguos en el almacenamiento de archivado para ahorrar costes.
- Elimine la relación de backup para poder archivar volúmenes de origen innecesarios y retener backups de volúmenes.
- Realice backups de un cloud a otro y desde sistemas en las instalaciones a un cloud público o privado.
- Los datos de los backups se protegen con conexiones HTTPS en reposo con cifrado AES de 256 bits y TLS 1.2.
- Utilice sus propias claves gestionadas por el cliente para el cifrado de datos en lugar de utilizar las claves de cifrado predeterminadas de su proveedor de cloud.
- Permite hasta 4,000 backups de un único volumen.
- Restaurar características:\*
- Restaure datos desde un momento específico a partir de copias Snapshot locales, volúmenes replicados o backups de volúmenes en el almacenamiento de objetos.
- Restaure un volumen, una carpeta o archivos individuales, al sistema de origen o a otro sistema.
- Restaure los datos a un entorno de trabajo utilizando una cuenta o suscripción diferente o que se encuentre en una región diferente.

- Realice una *restauración rápida* de un volumen desde un almacenamiento en el cloud a un sistema Cloud Volumes ONTAP o a un sistema local; perfecto para situaciones de recuperación ante desastres en las que necesite proporcionar acceso a un volumen lo antes posible.
- Restaure los datos a nivel de bloque, colocando los datos directamente en la ubicación que especifique, conservando las ACL originales.
- Examine y busque en catálogos de archivos para seleccionar fácilmente carpetas y archivos individuales para restaurar un solo archivo.

## Entornos de trabajo compatibles para operaciones de backup y restauración

El backup y la recuperación de BlueXP admite entornos de trabajo de ONTAP y proveedores de nube pública y privada.

### Regiones admitidas

El backup y la recuperación de datos de BlueXP es compatible con Cloud Volumes ONTAP en muchas regiones de Amazon Web Services, Microsoft Azure y Google Cloud.

["Obtenga más información utilizando el Mapa de regiones globales"](#)

### Destinos de backup admitidos

El backup y la recuperación de datos de BlueXP te permite realizar backups de volúmenes de ONTAP desde los siguientes entornos de trabajo de origen en los siguientes entornos de trabajo secundarios y almacenamiento de objetos en proveedores de cloud público y privado. Las copias Snapshot residen en el entorno de trabajo de origen.

| Entorno de trabajo de fuente  | Entorno de trabajo secundario (Replicación)                         | Almacén de objetos de destino (copia de seguridad) |
|-------------------------------|---------------------------------------------------------------------|----------------------------------------------------|
| Cloud Volumes ONTAP en AWS    | Cloud Volumes ONTAP en AWS<br>Sistema ONTAP en las instalaciones    | Endif de Amazon S3::aws[]<br>ifdef::Azure[]        |
| Cloud Volumes ONTAP en Azure  | Cloud Volumes ONTAP en Azure<br>Sistema ONTAP en las instalaciones  | Endif de Azure Blob::Azure[]<br>ifdef::gcp[]       |
| Cloud Volumes ONTAP en Google | Cloud Volumes ONTAP en Google<br>Sistema ONTAP en las instalaciones | Fin de Google Cloud Storage::gcp[]                 |



| Entorno de trabajo de fuente       | Entorno de trabajo secundario (Replicación)               | Almacén de objetos de destino (copia de seguridad)                                                                                                                                                                    |
|------------------------------------|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sistema ONTAP en las instalaciones | Cloud Volumes ONTAP<br>Sistema ONTAP en las instalaciones | ifndef::aws[]<br><br>Amazon S3<br><br><br><br><br><br><br><br><br><br>Azure Blob<br><br><br><br><br><br><br><br><br><br>Google Cloud Storage<br><br><br><br><br><br><br><br><br><br>StorageGRID de NetApp<br>ONTAP S3 |

### Destinos de restauración admitidos

Es posible restaurar datos ONTAP desde un archivo de backup que se encuentra en un entorno de trabajo secundario (un volumen replicado) o en almacenamiento de objetos (un archivo de backup) para los siguientes entornos de trabajo. Las copias Snapshot residen en el entorno de trabajo de origen y se pueden restaurar únicamente en ese mismo sistema.

| Ubicación del archivo de copia de seguridad |                                                                     | Entorno de trabajo de destino                                                                                                |
|---------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Almacén de objetos (Backup)                 | Sistema secundario (Replicación)                                    |                                                                                                                              |
| Amazon S3                                   | Cloud Volumes ONTAP en AWS<br>Sistema ONTAP en las instalaciones    | ifndef::aws[]<br><br>Cloud Volumes ONTAP en la endif del sistema ONTAP en las instalaciones de AWS::aws[]<br>ifndef::Azure[] |
| Azure Blob                                  | Cloud Volumes ONTAP en Azure<br>Sistema ONTAP en las instalaciones  | Cloud Volumes ONTAP en Azure<br>on-premises ONTAP system<br>endif::Azure[] ifndef::gcp[]                                     |
| Google Cloud Storage                        | Cloud Volumes ONTAP en Google<br>Sistema ONTAP en las instalaciones | Cloud Volumes ONTAP en Google<br>on-local ONTAP system endif::gcp[]                                                          |
| StorageGRID de NetApp                       | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           | Sistema ONTAP en las instalaciones                                                                                           |
| ONTAP S3                                    | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           | Sistema ONTAP en las instalaciones                                                                                           |

Tenga en cuenta que las referencias a "sistemas ONTAP en las instalaciones" incluyen sistemas FAS, AFF y ONTAP Select.

## Volúmenes compatibles

El backup y la recuperación de BlueXP admiten los siguientes tipos de volúmenes:

- Volúmenes FlexVol de lectura y escritura
- FlexGroup Volumes (requiere ONTAP 9.12.1 o posterior)
- SnapLock Enterprise Volumes (requiere ONTAP 9.11.1 o posterior)
- SnapLock Compliance para volúmenes en las instalaciones (requiere ONTAP 9.14 o posterior)
- Volúmenes de destino de protección de datos (DP) de SnapMirror



El backup y la recuperación de datos de BlueXP no admiten backups de volúmenes de FlexCache.

Consulte las secciones de ["Limitaciones de backup y restauración"](#) para requisitos y limitaciones adicionales.

## Coste

Existen dos tipos de costes asociados al uso del backup y la recuperación de datos de BlueXP con los sistemas ONTAP: Los cargos por recursos y los cargos por servicio. Ambos cargos son para la copia de seguridad en la parte objeto del servicio.

No se cobra ningún cargo por crear copias de Snapshot o volúmenes replicados, aparte del espacio en disco necesario para almacenar las copias de Snapshot y los volúmenes replicados.

### gastos de recursos

El proveedor de cloud paga los recursos por la capacidad de almacenamiento de objetos y por la escritura y lectura de archivos de backup en el cloud.

- Para Backup en el almacenamiento de objetos, paga a su proveedor de cloud por los costes de almacenamiento de objetos.

Como el backup y la recuperación de datos de BlueXP conserva las eficiencias de almacenamiento del volumen de origen, usted paga los costes de almacenamiento de objetos del proveedor de cloud para las eficiencias *después* de la ONTAP de los datos (para una menor cantidad de datos después de aplicar la deduplicación y la compresión).

- Para restaurar datos con la opción de búsqueda y restauración, el proveedor de cloud aprovisiona determinados recursos y hay un coste por TIB asociado con la cantidad de datos que escanean sus solicitudes de búsqueda. (Estos recursos no son necesarios para examinar y restaurar.)
  - En AWS, ["Amazon Athena"](#) y.. ["Pegamento de AWS"](#) Los recursos se implementan en un nuevo bloque de S3.
  - En Azure, una ["Espacio de trabajo de Azure Synapse"](#) y.. ["Almacenamiento de lagos de datos de Azure"](#) se aprovisionan en su cuenta de almacenamiento para almacenar y analizar los datos.
- En Google, se pone en marcha un nuevo bloque y el ["Servicios de Google Cloud BigQuery"](#) se aprovisionan en el nivel de cuenta/proyecto.
- Si piensa restaurar datos de volumen desde un archivo de backup que se ha movido al almacenamiento de objetos archivados, el proveedor de cloud tendrá una tarifa por recuperación por GiB y una tarifa por solicitud.
- Si tiene pensado analizar un archivo de backup en busca de ransomware durante el proceso de

restauración de datos de volumen (si ha habilitado DataLock y Ransomware Protection para sus backups en el cloud), también incurrirá en costes adicionales de salida de su proveedor de cloud.

## cargos por servicio

Los cargos por servicio se pagan a NetApp y cubren tanto el coste de *create* backups en el almacenamiento de objetos como de *restore* volúmenes, o archivos, a partir de dichos backups. Solo debe pagar por los datos que protege en el almacenamiento de objetos, calculados mediante la capacidad usada lógica de origen (*before* ONTAP efficiencies) de los volúmenes ONTAP de los que se realizan backups en el almacenamiento de objetos. Esta capacidad también se conoce como terabytes de interfaz (FETB).

El servicio de backup consta de tres formas de pago. La primera opción es suscribirse a su proveedor de cloud, lo que le permite pagar por mes. La segunda opción es conseguir un contrato anual. La tercera opción consiste en adquirir licencias directamente a NetApp. Lea la [Licencia](#) para obtener más información.

## Licencia

El backup y la recuperación de datos de BlueXP están disponibles con los siguientes modelos de consumo:

- **BYOL:** Una licencia comprada a NetApp que se puede usar con cualquier proveedor de cloud.
- **PAYGO:** Una suscripción por hora desde el mercado de su proveedor de la nube.
- **Anual:** Un contrato anual del mercado de su proveedor de cloud.

Una licencia de backup solo se requiere para backup y restauración desde el almacenamiento de objetos. La creación de copias Snapshot y volúmenes replicados no requiere una licencia.

## Con su propia licencia

BYOL está basada en término (1, 2 o 3 años) en capacidad y en incrementos de 1 TiB. Usted paga a NetApp para que utilice el servicio por un período de tiempo, digamos 1 año, y por una cantidad máxima, digamos 10 TiB.

Recibirás un número de serie que introduzcas en la página de la cartera digital de BlueXP para habilitar el servicio. Cuando se alcance cualquiera de los límites, deberá renovar la licencia. La licencia de licencia BYOL de Backup se aplica a todos los sistemas de origen asociados con su organización o cuenta de BlueXP .

["Aprenda a gestionar sus licencias BYOL"](#).

## Suscripción de pago por uso

El backup y la recuperación de BlueXP ofrece licencias basadas en el consumo en un modelo de pago por uso. Después de suscribirse a través del mercado de su proveedor de cloud, paga por GiB los datos de los que se ha realizado el backup: No hay ningún pago por adelantado. Su proveedor de cloud se le factura con cargo mensual.

["Aprenda a configurar una suscripción de pago por uso"](#).

Tenga en cuenta que está disponible una prueba gratuita de 30 días cuando se inscriba inicialmente con una suscripción a PAYGO.

## Contrato anual

Cuando utiliza AWS, hay dos contratos anuales disponibles para 1, 2 o 3 años:

- Un plan de "Backup en el cloud" que le permite realizar backups de datos de Cloud Volumes ONTAP y de datos de ONTAP en las instalaciones.
- Un plan «CVO Professional» que te permite agrupar el backup y la recuperación de datos de Cloud Volumes ONTAP y BlueXP. Esto incluye backups ilimitados de volúmenes de Cloud Volumes ONTAP cargados con esta licencia (la capacidad de backup no se cuenta con la licencia).

Cuando usa Azure, hay dos contratos anuales disponibles para 1, 2 o 3 años:

- Un plan de "Backup en el cloud" que le permite realizar backups de datos de Cloud Volumes ONTAP y de datos de ONTAP en las instalaciones.
- Un plan «CVO Professional» que te permite agrupar el backup y la recuperación de datos de Cloud Volumes ONTAP y BlueXP. Esto incluye backups ilimitados de volúmenes de Cloud Volumes ONTAP cargados con esta licencia (la capacidad de backup no se cuenta con la licencia).

Cuando usas GCP, puedes solicitar una oferta privada a NetApp y, después, seleccionar el plan al suscribirte desde Google Cloud Marketplace durante la activación del backup y la recuperación de BlueXP .

["Aprenda a establecer contratos anuales".](#)

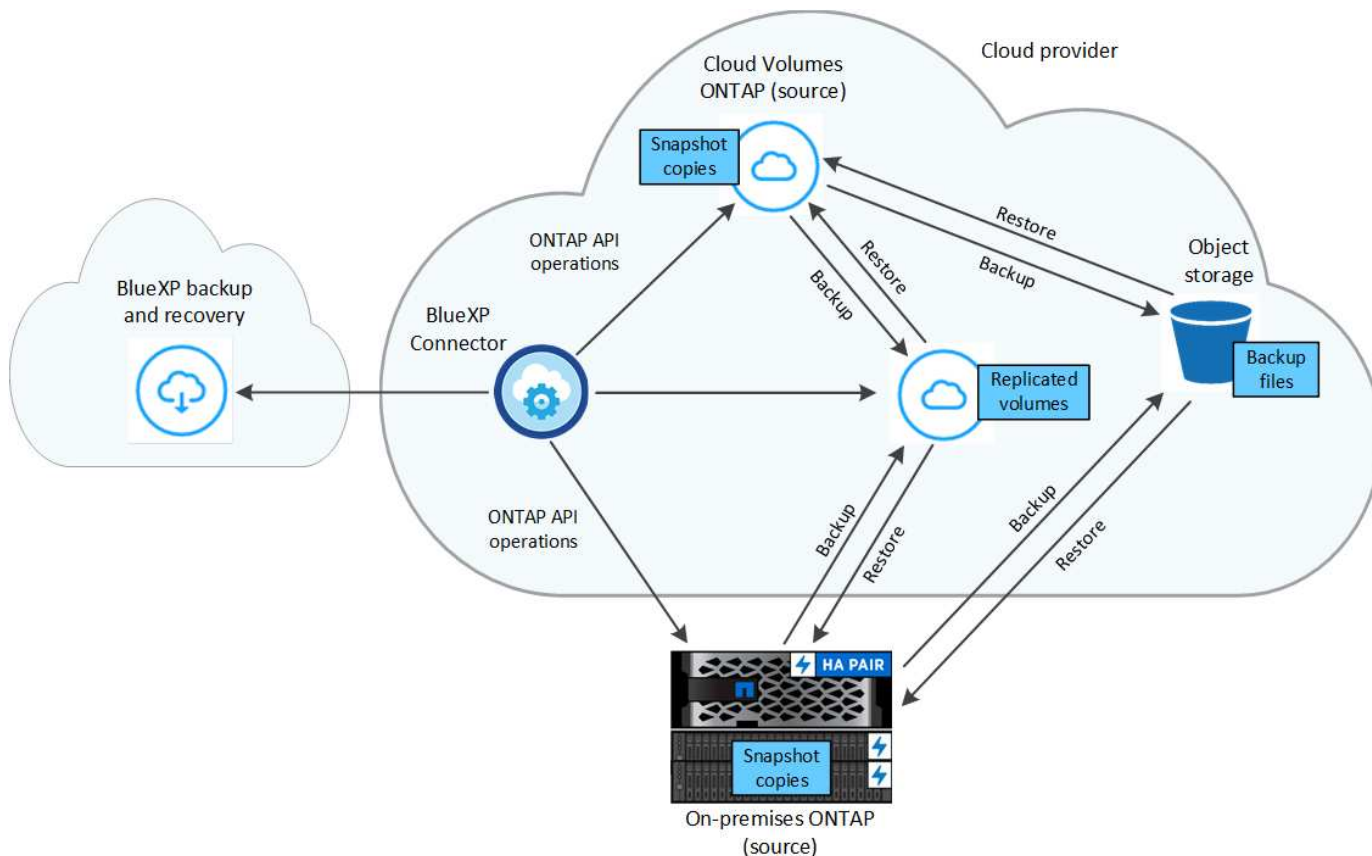
## Funcionamiento del backup y la recuperación de BlueXP

Cuando habilita el backup y la recuperación de BlueXP en un sistema Cloud Volumes ONTAP o ONTAP en las instalaciones, 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. El backup en el almacenamiento de objetos se crea sobre ["Tecnología SnapMirror Cloud de NetApp"](#).



Cualquier acción realizada directamente desde su entorno de proveedor de nube para administrar o cambiar los archivos de copia de seguridad en la nube puede dañar los archivos y dar lugar a una configuración no compatible.

La siguiente imagen muestra la relación entre cada componente:



Este diagrama muestra los volúmenes que se replican en un sistema Cloud Volumes ONTAP, pero los volúmenes también se pueden replicar en un sistema ONTAP on-premises.

## La ubicación de los backups

Los backups residen en distintas ubicaciones según el tipo de backup:

- *Snapshot copies* residen en el volumen de origen en el entorno de trabajo de origen.
- *Los volúmenes replicados* residen en el sistema de almacenamiento secundario: Un sistema Cloud Volumes ONTAP o ONTAP en las instalaciones.
- *Backup copies* se almacenan en un almacén de objetos que BlueXP crea en tu cuenta de cloud. Hay un almacén de objetos por clúster/entorno de trabajo y BlueXP asigna el nombre del almacén de objetos de la siguiente forma: "netapp-backup-clusterUUID". Asegúrese de no eliminar este almacén de objetos.
  - En AWS, BlueXP activa el "[Función de acceso público en bloque de Amazon S3](#)" En el bloque de S3.
  - En Azure, BlueXP utiliza un grupo de recursos nuevo o existente con una cuenta de almacenamiento para el contenedor Blob. BlueXP "[bloquea el acceso público a los datos blob](#)" de forma predeterminada.
  - En GCP, BlueXP usa un proyecto nuevo o existente con una cuenta de almacenamiento para el depósito de Google Cloud Storage.
  - En StorageGRID, BlueXP utiliza una cuenta de inquilino existente para el bloque de S3.
  - En ONTAP S3, BlueXP utiliza una cuenta de usuario existente para el bloque de S3.

Si desea cambiar el almacén de objetos de destino de un clúster en el futuro, tendrá que hacerlo "[Cancela el registro de backup y recuperación de BlueXP para el entorno de trabajo](#)", Y, a continuación, habilita el backup y la recuperación de BlueXP con la nueva información del proveedor de nube.

## Programación de copia de seguridad y configuración de retención personalizables

Cuando habilita el backup y la recuperación de BlueXP para un entorno de trabajo, todos los volúmenes que seleccionó inicialmente se someten a un backup con las políticas que seleccionó. Puede seleccionar políticas independientes para copias de Snapshot, volúmenes replicados y archivos de backup. Si desea asignar diferentes políticas de backup a ciertos volúmenes que tienen distintos objetivos de punto de recuperación (RPO), puede crear políticas adicionales para ese clúster y asignar esas políticas a los otros volúmenes una vez activado el backup y la recuperación de BlueXP.

Se puede elegir una combinación de backups por hora, diarios, semanales, mensuales y anuales de todos los volúmenes. Para backup en objeto también puede seleccionar una de las políticas definidas por el sistema que proporcionan backups y retención durante 3 meses, 1 año y 7 años. Las políticas de protección de backup que se crearon en el clúster con ONTAP System Manager o la interfaz de línea de comandos de ONTAP también aparecerán como selecciones. Esto incluye las políticas creadas con etiquetas de SnapMirror personalizadas.



La política de Snapshot aplicada al volumen debe tener una de las etiquetas que utilice en la política de replicación y el backup a la política de objetos. Si no se encuentran etiquetas coincidentes, no se crearán archivos de copia de seguridad. Por ejemplo, si desea crear volúmenes replicados «semanales» y archivos de backup, debe usar una política de Snapshot que cree copias Snapshot «semanales».

Una vez que haya alcanzado el número máximo de copias de seguridad de una categoría o intervalo, se eliminan las copias de seguridad más antiguas, de modo que siempre tenga las copias de seguridad más actualizadas (para que las copias de seguridad obsoletas no sigan ocupando espacio).

Consulte "[Programaciones de backup](#)" para obtener más información acerca de las opciones de programación disponibles.

Tenga en cuenta que puede "[crear un backup bajo demanda de un volumen](#)" Desde la consola de backup en cualquier momento, además de los archivos de backup creados a partir de las copias de seguridad programadas.



El período de retención para backups de volúmenes de protección de datos es el mismo que se define en la relación de SnapMirror de origen. Puede cambiar esto si lo desea con la API de.

## Configuración de protección de archivos de copia de seguridad

Si su clúster utiliza ONTAP 9.11.1 o posterior, puede proteger sus backups en el almacenamiento de objetos contra la eliminación y los ataques de ransomware. Cada política de copia de seguridad ofrece una sección de *DataLock* y *Protección de ransomware* que se puede aplicar a sus archivos de copia de seguridad durante un período de tiempo específico: El *período de retención*.

- *DataLock* protege los archivos de copia de seguridad de que no se modifican o eliminan.
- *Ransomware Protection* analiza sus archivos de copia de seguridad para buscar pruebas de un ataque de ransomware cuando se crea un archivo de copia de seguridad y cuando se restauran los datos de un archivo de copia de seguridad.

Los análisis programados de protección contra ransomware se habilitan de forma predeterminada. La configuración predeterminada para la frecuencia de exploración es de 7 días. El análisis se realiza sólo en la última copia Snapshot. Los análisis programados se pueden desactivar para reducir los costes. Puede habilitar o deshabilitar los análisis de ransomware programados en la última copia de Snapshot usando la opción de la página Configuración avanzada. Si la activa, las exploraciones se realizan semanalmente de

forma predeterminada. Puede cambiar esa programación a días o semanas o deshabilitarla, lo que ahorrará costes.

El período de retención de la copia de seguridad es el mismo que el período de retención del programa de copia de seguridad, más un búfer máximo de 31 días. Por ejemplo, las copias de seguridad *Weekly* con 5 copias retenidas bloquearán cada archivo de copia de seguridad durante 5 semanas. *Mensual* los backups con 6 copias retenidas bloquearán cada archivo de copia de seguridad durante 6 meses.

Actualmente, existe soporte disponible si su destino de backup es Amazon S3, Azure Blob o StorageGRID de NetApp. En futuras versiones se añadirán otros destinos proveedores de almacenamiento.

Para obtener más detalles, consulte esta información:

- ["Cómo funcionan DataLock y la protección contra ransomware"](#).
- ["Cómo actualizar las opciones de protección contra ransomware en la página Configuración avanzada"](#).



No se puede habilitar DataLock si se dispone de la organización en niveles de los backups en el almacenamiento de archivado.

## Almacenamiento de archivado para ficheros de backup antiguos

Al usar cierto almacenamiento en cloud, se pueden mover los archivos de backup antiguos a un nivel de acceso/clase de almacenamiento más económico tras un determinado número de días. También puede optar por enviar sus archivos de copia de seguridad al almacenamiento de archivos inmediatamente sin ser escrito en el almacenamiento en la nube estándar. Tenga en cuenta que el almacenamiento de archivado no se puede utilizar si ha habilitado DataLock.

- 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.

Si el clúster utiliza ONTAP 9.10.1 o posterior, puede optar por organizar en niveles backups antiguos en almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive* en la interfaz de usuario de backup y recuperación de BlueXP después de un determinado número de días para optimizar aún más los costes. ["Obtenga más información acerca del almacenamiento de archivado de AWS"](#).

- En Azure, los backups están asociados con el nivel de acceso *Cool*.

Si el clúster utiliza ONTAP 9.10.1 o posterior, puedes optar por organizar en niveles backups antiguos en el almacenamiento *Azure Archive* en la interfaz de usuario de backup y recuperación de BlueXP después de un determinado número de días para optimizar aún más los costes. ["Obtenga más información sobre el almacenamiento de archivado de Azure"](#).

- En GCP, las copias de seguridad están asociadas con la clase de almacenamiento *Standard*.

Si el clúster utiliza ONTAP 9.12.1 o posterior, puedes optar por organizar en niveles los backups antiguos en el almacenamiento *Archive* en la interfaz de usuario de backup y recuperación de BlueXP después de un determinado número de días para optimizar aún más los costes. ["Más información sobre el almacenamiento de archivos de Google"](#).

- En StorageGRID, las copias de seguridad están asociadas con la clase de almacenamiento *Standard*.

Si su clúster de instalaciones utiliza ONTAP 9.12.1 o superior y su sistema StorageGRID utiliza 11.4 o más, puede archivar archivos de backup antiguos al almacenamiento de archivado en cloud público tras un determinado número de días. Actualmente es compatible con los niveles de almacenamiento de AWS



S3 Glacier/S3 Glacier Deep Archive o Azure Archive. ["Obtenga más información sobre el archivado de archivos de backup desde StorageGRID"](#).

Consulte ["Configuración de almacenamiento de archivado"](#) para obtener más información acerca del archivado de archivos de copia de seguridad antiguos.

## Consideraciones sobre la política de organización en niveles de FabricPool

Hay ciertos aspectos que debes tener en cuenta cuando el volumen del que vas a realizar el backup reside en un agregado de FabricPool y tiene asignada una política de organización en niveles distinta a la de `none`:

- El primer backup de un volumen organizado en niveles de FabricPool requiere la lectura de todos los datos locales y por niveles (del almacén de objetos). Una operación de backup no "recalienta" los datos fríos organizados por niveles en almacenamiento de objetos.

Esta operación podría provocar un aumento único en el coste de leer los datos del proveedor de cloud.

- Los backups posteriores son incrementales y no tienen este efecto.
- Si la política de organización en niveles se asigna al volumen cuando se crea inicialmente, no se verá este problema.
- Tenga en cuenta el impacto de los backups antes de asignar el `all` la política de organización en niveles en los volúmenes. Como los datos se organizan en niveles de inmediato, el backup y la recuperación de datos de BlueXP leerán datos del nivel de cloud en lugar de del nivel local. Como las operaciones de backup simultáneas comparten el enlace de red con el almacén de objetos en cloud, se puede producir una degradación del rendimiento si los recursos de red se saturan. En este caso, puede que desee configurar de forma proactiva varias interfaces de red (LIF) para reducir este tipo de saturación de red.

## Planifique su viaje de protección con la copia de seguridad y recuperación de BlueXP

El servicio de backup y recuperación de datos de BlueXP permite crear hasta tres copias de los volúmenes de origen para proteger los datos. Hay muchas opciones que puede seleccionar al habilitar este servicio en sus volúmenes, por lo que debe revisar sus opciones para estar preparado.

Repasaremos las siguientes opciones:

- Qué funciones de protección usarán: Copias Snapshot, volúmenes replicados y/o backup en cloud
- Qué arquitectura de backup utilizará: Un backup en cascada o ramificado de sus volúmenes
- Utilizarán las políticas de backup predeterminadas o tendrán que crear políticas personalizadas
- ¿Desea que el servicio cree los buckets de cloud para usted o desea crear sus contenedores de almacenamiento de objetos antes de empezar
- Qué modo de puesta en marcha de BlueXP Connector utiliza (modo estándar, restringido o privado)

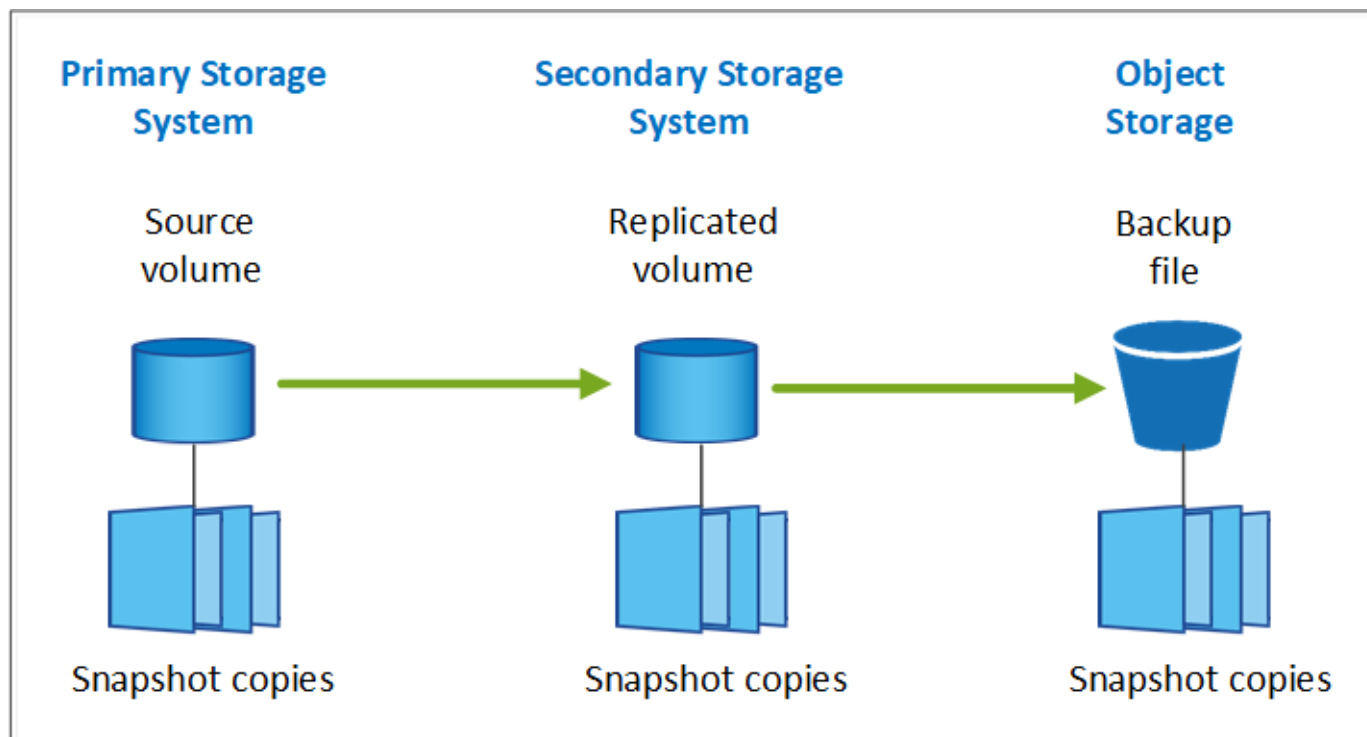
## Qué funciones de protección utilizará

Antes de seleccionar las funciones que va a utilizar, aquí hay una explicación rápida de lo que hace cada función y qué tipo de protección proporciona.



| Tipo de backup     | Descripción                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Snapshot           | Crea una imagen de un momento específico de solo lectura de un volumen dentro del volumen de origen como copia Snapshot. Es posible usar la copia Snapshot para recuperar archivos individuales o para restaurar todo el contenido de un volumen. |
| Replicación        | Crea una copia secundaria de los datos en otro sistema de almacenamiento de ONTAP y actualiza continuamente los datos secundarios. Sus datos estarán actualizados y disponibles siempre que haga falta.                                           |
| Backup en el cloud | Crea backups de sus datos en el cloud para protegerlos y archivarlos a largo plazo. Si es necesario, puede restaurar un volumen, una carpeta o archivos individuales desde el backup en el mismo entorno de trabajo o en uno diferente.           |

Las copias Snapshot son la base de todos los métodos de backup y se requieren para usar el servicio de backup y recuperación. Una copia Snapshot es una imagen de un momento específico de solo lectura de un volumen. La imagen consume un espacio de almacenamiento mínimo y apenas supone una sobrecarga de rendimiento, ya que sólo registra los cambios realizados en los archivos desde que se realizó la última copia Snapshot. La copia Snapshot que se crea en el volumen se usa para mantener el volumen replicado y el archivo de backup sincronizados con los cambios que se hacen en el volumen de origen, como se muestra en la figura.



Puede elegir crear volúmenes replicados en otro sistema de almacenamiento de ONTAP y archivos de backup en el cloud. O puede elegir simplemente crear volúmenes replicados o archivos de copia de seguridad - es su elección.

En resumen, estos son los flujos de protección válidos que puede crear para volúmenes en su entorno de trabajo de ONTAP:

- Volumen de origen → Copia Snapshot → Volumen replicado → Archivo de backup
- Volumen de origen → Copia Snapshot → Archivo de backup

- Volumen de origen → Copia Snapshot → Volumen replicado



La creación inicial de un volumen replicado o un archivo de copia de seguridad incluye una copia completa de los datos de origen — esto se denomina *transferencia de línea base*. Las transferencias posteriores solo contienen copias diferenciales de los datos de origen (la instantánea).

## Comparación de los diferentes métodos de copia de seguridad

En la siguiente tabla se muestra una comparación generalizada de los tres métodos de copia de seguridad. Si bien el espacio de almacenamiento de objetos generalmente es menos costoso que el almacenamiento en disco local, si cree que puede restaurar los datos desde el cloud con frecuencia, las tasas de salida por parte de los proveedores de cloud pueden reducir parte de sus ahorros. Tendrá que identificar con qué frecuencia necesita restaurar los datos de los archivos de backup en el cloud.

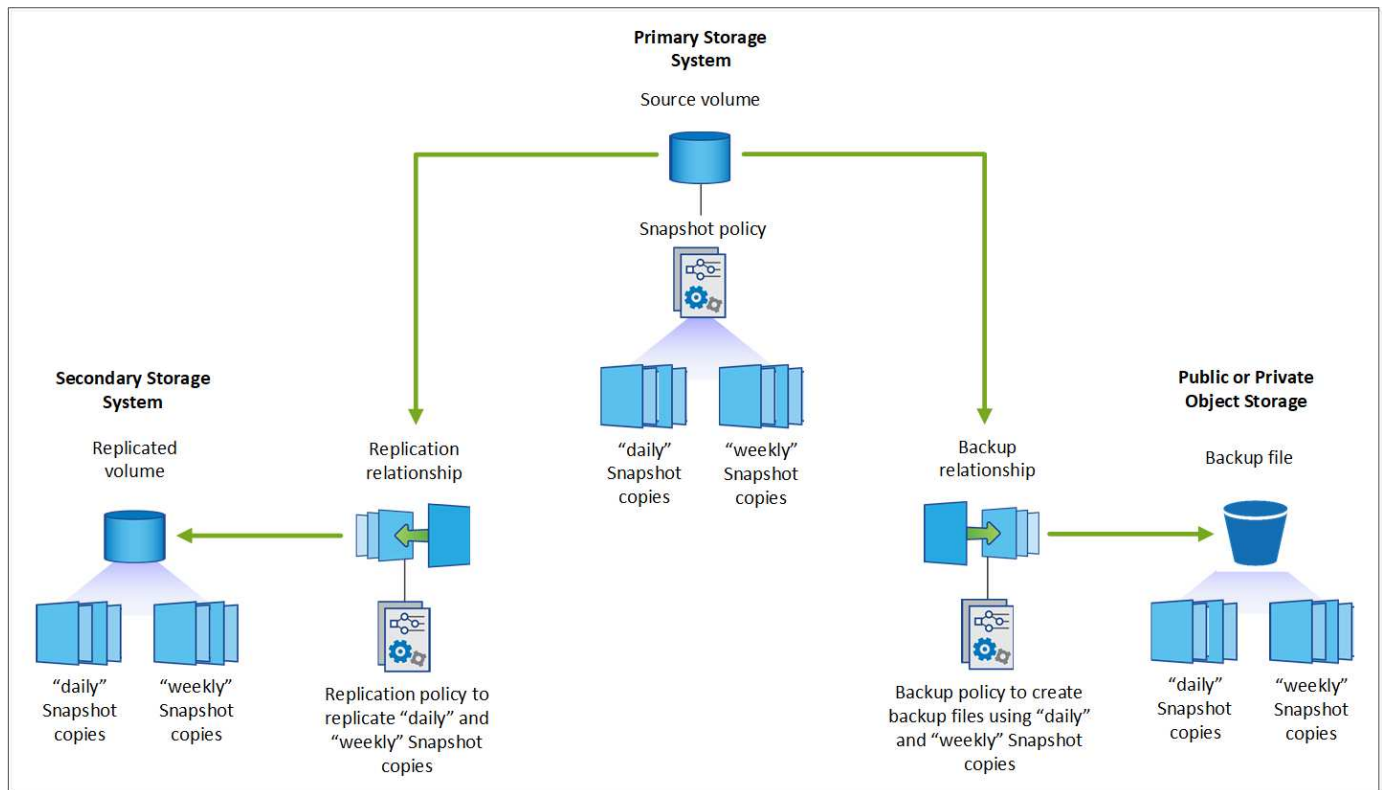
Además de estos criterios, el almacenamiento en la nube ofrece opciones de seguridad adicionales si usa la función DataLock y Ransomware Protection, y ahorros adicionales en costos al seleccionar clases de almacenamiento de archivado para archivos de copia de seguridad más antiguos. ["Más información sobre la protección de DataLock y Ransomware"](#) y.. ["configuración de almacenamiento de archivado"](#).

| Tipo de backup | Velocidad de backup | Coste de los backups     | Velocidad de restauración | Coste de la restauración   |
|----------------|---------------------|--------------------------|---------------------------|----------------------------|
| Instantánea    | Alto                | Bajo (espacio en disco)  | Alto                      | Bajo                       |
| Replicación    | Mediano             | Medio (espacio en disco) | Mediano                   | Medio (red)                |
| Cloud Backup   | Bajo                | Bajo (espacio de objeto) | Bajo                      | Altas (tasas de proveedor) |

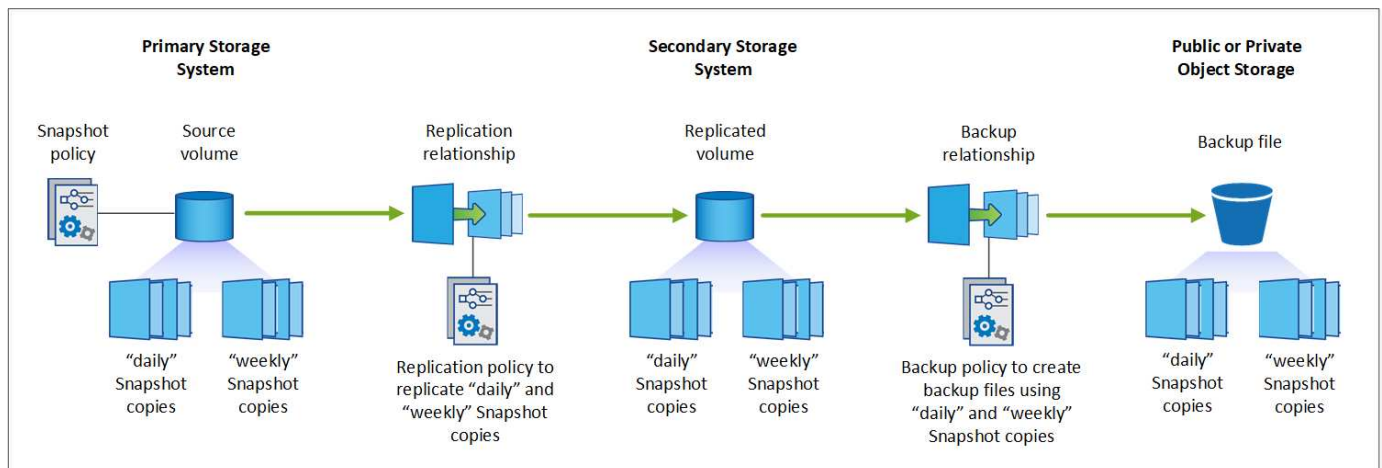
## Qué arquitectura de backup utilizará

Al crear volúmenes replicados y archivos de backup, puede elegir una arquitectura ramificada o en cascada para realizar backup de sus volúmenes.

Una arquitectura **fan-out** transfiere la copia snapshot de forma independiente tanto al sistema de almacenamiento de destino como al objeto de copia de seguridad en la nube.



Una arquitectura **Cascade** transfiere primero la copia snapshot al sistema de almacenamiento de destino y, a continuación, el sistema transfiere la copia al objeto de copia de seguridad en la nube.



## Comparación de las diferentes opciones de arquitectura

Esta tabla proporciona una comparación de las arquitecturas ramificadas y en cascada.

| Dispersión                                                                                                                  | Cascada                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Pequeña repercusión en el rendimiento del sistema de origen, ya que envía copias snapshot a 2 sistemas distintos            | Menor efecto en el rendimiento del sistema de almacenamiento de origen, ya que envía la copia de Snapshot una sola vez |
| Es más fácil de configurar porque todas las políticas, redes y configuraciones de ONTAP se realizan en el sistema de origen | Requiere que se realice un poco de configuración de redes y ONTAP también desde el sistema secundario.                 |

## Utilizará las políticas predeterminadas para snapshots, replicaciones y backups

Puede usar las políticas predeterminadas que proporciona NetApp para crear sus backups, o bien puede crear políticas personalizadas. Al utilizar el asistente de activación para habilitar el servicio de backup y recuperación para los volúmenes, puede seleccionar entre las políticas predeterminadas y todas las demás políticas que ya existan en el entorno de trabajo (Cloud Volumes ONTAP o ONTAP en las instalaciones). Si desea utilizar una política diferente a las políticas existentes, puede crear la política antes de iniciar o mientras utiliza el asistente de activación.

- La política de Snapshot predeterminada crea copias Snapshot por hora, diarias y semanales, reteniendo 6 copias Snapshot por hora, 2 diarias y 2 copias Snapshot semanales.
- La política de replicación predeterminada replica copias snapshot diarias y semanales, reteniendo 7 copias snapshot diarias y 52 semanales.
- La política de backup predeterminada replica copias snapshot diarias y semanales, reteniendo 7 copias snapshot diarias y 52 semanales.

Si crea políticas personalizadas para replicación o backup, las etiquetas de la política (por ejemplo, «diaria» o «semanal») deben coincidir con las etiquetas que existen en sus políticas de snapshots o no se crearán los volúmenes replicados y los archivos de backup.

Puede crear Snapshot, replicación y backup en políticas de almacenamiento de objetos en la interfaz de usuario de backup y recuperación de BlueXP . Consulte la sección para [añada una nueva política de backup](#) obtener más información.

Además de utilizar el backup y la recuperación de datos de BlueXP para crear políticas personalizadas, puede usar System Manager o la interfaz de línea de comandos (CLI) de ONTAP:

- ["Cree una política de Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP"](#)
- ["Cree una política de replicación mediante System Manager o la CLI de ONTAP"](#)

**Nota:** Cuando utilice System Manager, seleccione **Asíncrono** como el tipo de política para las políticas de replicación y seleccione **Asíncrono** y **Copia de seguridad en la nube** para realizar copias de seguridad en las políticas de objetos.

Aquí se muestran algunos comandos CLI de ONTAP de ejemplo que pueden ser útiles si está creando políticas personalizadas. Tenga en cuenta que debe utilizar el vserver *admin* (VM de almacenamiento) como `<vserver_name>` en estos comandos.

| Descripción de la política  | Comando                                                                                                                                                                                                                                                                                                            |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Política de snapshot simple | <code>snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly</code>                                                                                                                                                            |
| Backup sencillo en el cloud | <code>snapmirror policy create -policy &lt;policy_name&gt; -transfer -priority normal -vserver &lt;vserver_name&gt; -create -snapshot-on-source false -type vault<br/>snapmirror policy add-rule -policy &lt;policy_name&gt; -vserver &lt;vserver_name&gt; -snapmirror-label &lt;snapmirror_label&gt; -keep</code> |

| Descripción de la política                                       | Comando                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup en el cloud con DataLock y protección frente a ransomware | <pre> snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver &lt;vserver_name&gt; snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days </pre>                                                                                   |
| Backup en cloud con clase de almacenamiento de archivado         | <pre> snapmirror policy create -vserver &lt;vserver_name&gt; -policy &lt;policy_name&gt; -archive-after-days &lt;days&gt; -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy &lt;policy_name&gt; -vserver &lt;vserver_name&gt; -snapmirror-label &lt;snapmirror_label&gt; -keep </pre> |
| Replicación sencilla a otro sistema de almacenamiento            | <pre> snapmirror policy create -policy &lt;policy_name&gt; -type async-mirror -vserver &lt;vserver_name&gt; snapmirror policy add-rule -policy &lt;policy_name&gt; -vserver &lt;vserver_name&gt; -snapmirror-label &lt;snapmirror_label&gt; -keep </pre>                                                             |



Solo se pueden utilizar políticas de almacén para relaciones de backup a cloud.

## ¿Dónde residen mis políticas?

Las políticas de copia de seguridad residen en diferentes ubicaciones dependiendo de la arquitectura de copia de seguridad que se vaya a utilizar: Fan-out o Cascading. Las políticas de replicación y las políticas de backup no están diseñadas de la misma manera porque las replicaciones emparejan dos sistemas de almacenamiento de ONTAP y el backup en objetos utiliza un proveedor de almacenamiento como destino.

- Las políticas de Snapshot residen siempre en el sistema de almacenamiento principal.
- Las políticas de replicación residen siempre en el sistema de almacenamiento secundario.
- Las políticas de backup a objeto se crean en el sistema donde reside el volumen de origen. Este es el clúster principal para configuraciones de distribución ramificada y el clúster secundario para configuraciones en cascada.

Estas diferencias se muestran en la tabla.

| Arquitectura   | Política de Snapshot | Política de replicación | Política de backup |
|----------------|----------------------|-------------------------|--------------------|
| <b>Fan-out</b> | Primario             | Secundario              | Primario           |
| <b>Cascada</b> | Primario             | Secundario              | Secundario         |

Por lo tanto, si tiene pensado crear políticas personalizadas al utilizar la arquitectura en cascada, deberá crear la replicación y el backup a políticas de objetos en el sistema secundario donde se crearán los volúmenes replicados. Si tiene pensado crear normativas personalizadas al utilizar la arquitectura de dispersión, deberá crear las normativas de replicación en el sistema secundario donde se crearán los volúmenes replicados y realizar un backup en las políticas de objetos en el sistema primario.

Si usa las directivas predeterminadas que existen en todos los sistemas ONTAP, entonces todo está configurado.

## ¿Desea crear su propio contenedor de almacenamiento de objetos

Cuando crea archivos de copia de seguridad en el almacenamiento de objetos para un entorno de trabajo, de forma predeterminada, el servicio de copia de seguridad y recuperación crea el contenedor (cuenta de almacenamiento o depósito) para los archivos de copia de seguridad en la cuenta de almacenamiento de objetos que haya configurado. El bucket AWS o GCP se denomina «netapp-backup-<uuid>» de forma predeterminada. La cuenta de almacenamiento de Azure Blob se llama «netappbackup<uuid>».

Puede crear el contenedor usted mismo en la cuenta del proveedor de objetos si desea utilizar un prefijo determinado o asignar propiedades especiales. Si desea crear su propio contenedor, debe crearlo antes de iniciar el asistente de activación. El backup y la recuperación de datos de BlueXP puede utilizar cualquier bloque y bloque compartido. El asistente de activación de copia de seguridad detectará automáticamente los contenedores aprovisionados para la cuenta y las credenciales seleccionadas para que pueda seleccionar el que desea utilizar.

Puede crear el bloque en BlueXP o desde su proveedor de cloud.

- ["Crea buckets de Amazon S3 a partir de BlueXP"](#)
- ["Crea cuentas de almacenamiento de Azure Blob desde BlueXP"](#)
- ["Crea buckets de almacenamiento de Google Cloud a partir de BlueXP"](#)

**Nota:** En este momento no puede usar sus propios buckets S3 al crear copias de seguridad en sistemas StorageGRID o en ONTAP S3.

Si tiene pensado utilizar un prefijo de bloque diferente al «netapp-backup-xxxxxx», deberá modificar los permisos S3 para el rol Connector IAM. Para obtener más detalles, consulte cómo crear backups en AWS S3.

### Configuración avanzada del cucharón

Si planeas mover archivos de copia de seguridad antiguos al almacenamiento de archivado, o si planeas habilitar la protección DataLock y Ransomware para bloquear tus archivos de copia de seguridad y escanearlos en busca de un posible ransomware, tendrás que crear el contenedor con ciertas opciones de configuración:

- El almacenamiento de archivado en sus propios bloques se admite en el almacenamiento de AWS S3 en este momento si se utiliza software de ONTAP 9.10.1 o superior en sus clústeres. De forma predeterminada, los backups comienzan en la clase de almacenamiento S3 *Standard*. Asegúrese de crear el depósito con las reglas de ciclo de vida adecuadas:
  - Mueva los objetos en todo el ámbito del depósito a S3 *Standard-IA* después de 30 días.
  - Mueva los objetos con la etiqueta «smc\_push\_to\_archive: True» a *Glacier Flexible Retrieval* (anteriormente S3 Glacier)
- La protección contra bloqueo de datos y ransomware es compatible con el almacenamiento de AWS cuando se usa software de ONTAP 9.11.1 o posterior en los clústeres, y en el almacenamiento de Azure cuando se utiliza el software de ONTAP 9.12.1 o posterior.
  - Para AWS, debe habilitar el bloqueo de objetos en el bloque con un período de retención de 30 días.
  - Para Azure, debe crear la clase de almacenamiento con compatibilidad de inmutabilidad a nivel de versión.

### El modo de puesta en marcha de BlueXP Connector utiliza

Si ya usas BlueXP para gestionar tu almacenamiento, ya se ha instalado un conector BlueXP. Si tienes pensado utilizar el mismo conector con backup y recuperación de datos de BlueXP, ya lo tienes todo. Si

necesita usar un conector diferente, deberá instalarlo antes de iniciar la implementación de copia de seguridad y recuperación.

BlueXP ofrece múltiples modos de implementación que le permiten utilizar BlueXP de forma que se adapte a sus necesidades empresariales y de seguridad. *Standard Mode* aprovecha la capa SaaS de BlueXP para proporcionar todas las funciones, mientras que *restricted mode* y *private mode* están disponibles para organizaciones que tienen restricciones de conectividad.

["Obtenga más información sobre los modos de implementación de BlueXP".](#)

### **Soporte para sitios con conectividad completa a Internet**

Cuando se utiliza el backup y la recuperación de BlueXP en un sitio con conectividad completa a Internet (también conocido como *standard mode* o *SaaS mode*), puedes crear volúmenes replicados en cualquier sistema Cloud Volumes ONTAP o ONTAP on-premises gestionado por BlueXP, además, puede crear archivos de backup en el almacenamiento de objetos en cualquiera de los proveedores de cloud admitidos. ["Consulte la lista completa de destinos de backup compatibles"](#).

Para obtener una lista de ubicaciones de conector válidas, consulte uno de los siguientes procedimientos de copia de seguridad para el proveedor de nube en el que planea crear archivos de copia de seguridad. Existen algunas restricciones en las que el conector debe instalarse manualmente en una máquina Linux o implementarse en un proveedor de nube específico.

- ["Realice backup de los datos de Cloud Volumes ONTAP en Amazon S3"](#)
- ["Realice un backup de los datos de ONTAP en las instalaciones en Amazon S3"](#)
- ["Realice backups de los datos de Cloud Volumes ONTAP en Azure Blob"](#)
- ["Realice un backup de los datos de ONTAP en las instalaciones en Azure Blob"](#)
- ["Realice backups de los datos de Cloud Volumes ONTAP en Google Cloud"](#)
- ["Realice un backup de los datos de ONTAP en las instalaciones en Google Cloud"](#)
- ["Realice un backup de los datos de ONTAP en las instalaciones en StorageGRID"](#)
- ["Realice un backup del ONTAP en las instalaciones a ONTAP S3"](#)

### **Soporte para sitios con conectividad a Internet limitada**

El backup y la recuperación de datos de BlueXP se pueden utilizar en un sitio con una conectividad a Internet limitada (también conocida como *restricted mode*) para hacer copias de seguridad de datos de volumen. En este caso, tendrá que poner en marcha el conector BlueXP en la región de cloud de destino.

- Puede realizar un backup de los datos de sistemas ONTAP en las instalaciones o sistemas Cloud Volumes ONTAP instalados en las regiones comerciales de AWS en Amazon S3. ["Realice backup de los datos de Cloud Volumes ONTAP en Amazon S3"](#).
- Puede realizar backup de datos de sistemas ONTAP en las instalaciones o sistemas Cloud Volumes ONTAP instalados en regiones comerciales de Azure en Azure Blob. ["Realice backups de los datos de Cloud Volumes ONTAP en Azure Blob"](#).

### **Compatibilidad con sitios sin conectividad a Internet**

El backup y la recuperación de BlueXP se pueden utilizar en un sitio sin conectividad a Internet (también conocido como *modo privado* o *dark* sitios) para hacer copias de seguridad de los datos del volumen. En este caso, tendrá que poner en marcha el conector BlueXP en un host Linux en el mismo sitio.



- Puede realizar backups de datos de sistemas ONTAP locales en las instalaciones en sistemas StorageGRID de NetApp locales. ["Realice un backup de los datos de ONTAP en las instalaciones en StorageGRID"](#).
- Puede realizar backups de datos de sistemas ONTAP locales en las instalaciones de en sistemas ONTAP locales o sistemas Cloud Volumes ONTAP configurados para el almacenamiento de objetos S3. ["Realice un backup de los datos de ONTAP en las instalaciones en ONTAP S3"](#).

## Administre políticas de respaldo para volúmenes ONTAP con BlueXP Backup and Recovery

Con la copia de seguridad y recuperación de BlueXP, utilice las políticas de copia de seguridad predeterminadas proporcionadas por NetApp para crear sus copias de seguridad o cree políticas personalizadas. Las políticas rigen la frecuencia de las copias de seguridad, el tiempo que se realiza la copia de seguridad y el número de archivos de copia de seguridad que se retienen.

Al utilizar el asistente de activación para habilitar el servicio de backup y recuperación para los volúmenes, puede seleccionar entre las políticas predeterminadas y todas las demás políticas que ya existan en el entorno de trabajo (Cloud Volumes ONTAP o ONTAP en las instalaciones). Si desea utilizar una política diferente a las políticas existentes, puede crear la política antes o mientras utiliza el asistente de activación.

Para obtener más información sobre las políticas de backup predeterminadas proporcionadas, consulte ["Planifica tu proceso de protección"](#).

El backup y la recuperación de datos de BlueXP ofrece tres tipos de backups de los datos de ONTAP: Snapshots, replicaciones y backups en el almacenamiento de objetos. Sus políticas residen en distintas ubicaciones según la arquitectura que se utilice y el tipo de backup:

| Arquitectura | Ubicación de almacenamiento de la política de Snapshot | Ubicación de almacenamiento de la política de replicación | Backup en la ubicación de almacenamiento de políticas de objetos |
|--------------|--------------------------------------------------------|-----------------------------------------------------------|------------------------------------------------------------------|
| Fan-out      | Primario                                               | Secundario                                                | Primario                                                         |
| Cascada      | Primario                                               | Secundario                                                | Secundario                                                       |

Cree políticas de backup con las siguientes herramientas en función del entorno, sus preferencias y el tipo de protección:

- Interfaz de usuario de BlueXP
- Interfaz de usuario de System Manager
- CLI de ONTAP



Cuando utilice System Manager, seleccione **Asynchronous** como el tipo de política para las políticas de replicación y seleccione **Asynchronous** y **Back up to cloud** para realizar copias de seguridad en las políticas de objetos.

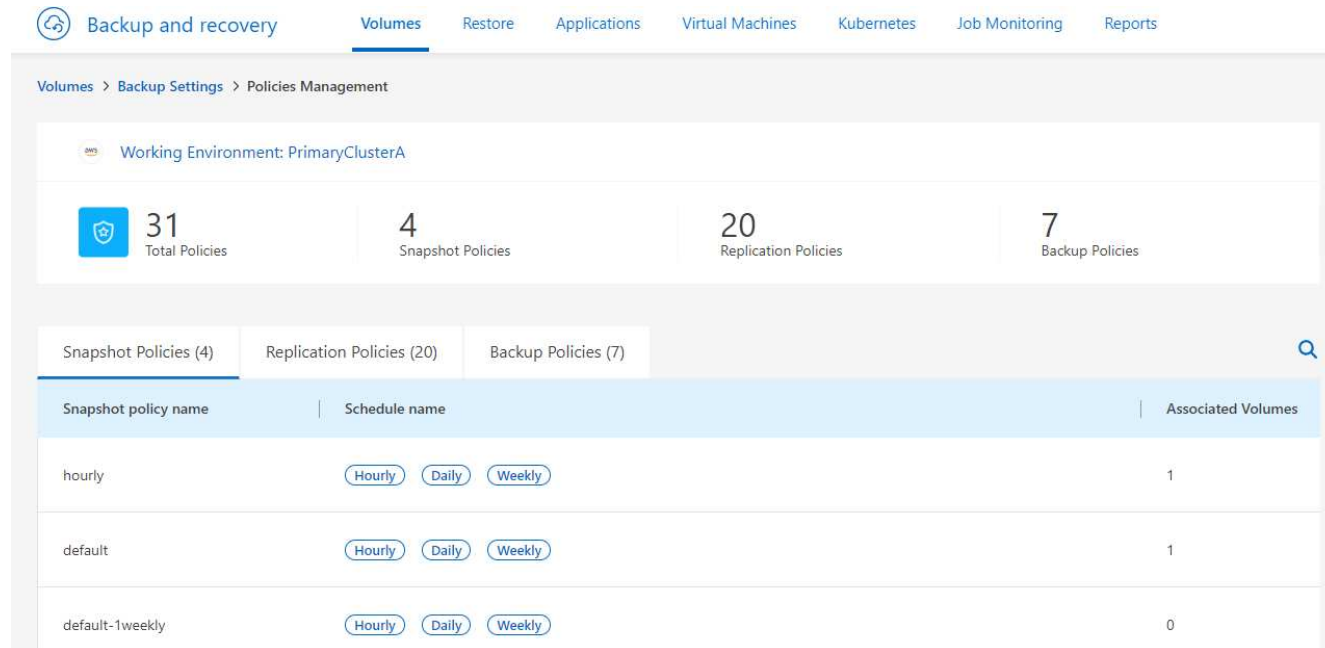
### Ver políticas para un entorno de trabajo

1. En la interfaz de usuario de BlueXP, selecciona **Volúmenes > Configuración de copia de seguridad**.



- En la página Configuración de copia de seguridad, seleccione el entorno de trabajo, seleccione las acciones \*  Y seleccione **Administración de políticas**.

Aparece la página Gestión de Políticas.



| Snapshot policy name | Schedule name                                                       | Associated Volumes |
|----------------------|---------------------------------------------------------------------|--------------------|
| hourly               | <a href="#">Hourly</a> <a href="#">Daily</a> <a href="#">Weekly</a> | 1                  |
| default              | <a href="#">Hourly</a> <a href="#">Daily</a> <a href="#">Weekly</a> | 1                  |
| default-1weekly      | <a href="#">Hourly</a> <a href="#">Daily</a> <a href="#">Weekly</a> | 0                  |

Las políticas de Snapshot se muestran de forma predeterminada.

- Para ver otras políticas que existen en el entorno de trabajo, seleccione **Políticas de replicación** o **Políticas de copia de seguridad**. Si las políticas existentes se pueden utilizar para sus planes de respaldo, está todo configurado. Si necesita tener una política con características diferentes, puede crear nuevas políticas desde esta página.

## Crear políticas

Puede crear políticas que rijan sus copias de Snapshot, replicaciones y backups en el almacenamiento de objetos:

- [Cree una política de Snapshot antes de iniciar la snapshot](#)
- [Cree una política de replicación antes de iniciar la replicación](#)
- [Cree una política de almacenamiento de backup a objetos antes de iniciar el backup](#)

### Cree una política de Snapshot antes de iniciar la snapshot

Parte de su estrategia 3-2-1 implica la creación de una copia Snapshot del volumen en el sistema de almacenamiento \* primario \*.

Parte del proceso de creación de políticas implica identificar etiquetas de Snapshot y SnapMirror que denoten la programación y retención. Puede utilizar etiquetas predefinidas o crear las suyas propias.

### Pasos

- En la interfaz de usuario de BlueXP, selecciona **Volúmenes > Configuración de copia de seguridad**.
- En la página Configuración de copia de seguridad, seleccione el entorno de trabajo, seleccione las acciones \*  Y seleccione **Administración de políticas**.

Aparece la página Gestión de Políticas.

3. En la página Políticas, selecciona **Crear política > Crear política de Snapshot**.
4. Escriba el nombre de la política.
5. Seleccione la programación de Snapshot o las programaciones. Puede tener un máximo de 5 etiquetas. O bien, cree una programación.
6. Si decide crear una programación:
  - a. Seleccione la frecuencia horaria, diaria, semanal, mensual o anual.
  - b. Especifique las etiquetas de Snapshot que indican la programación y la retención.
  - c. Introduzca cuándo y con qué frecuencia se tomará la snapshot.
  - d. Retention: Introduzca el número de Snapshots que se van a conservar.
7. Seleccione **Crear**.

### Ejemplo de política de instantáneas usando arquitectura en cascada

En este ejemplo, se crea una política de Snapshot con dos clústeres:

1. Clúster 1:
  - a. Seleccione Cluster 1 en la página policy.
  - b. Ignore las secciones de política Replicación y Copia de Seguridad en Objetos.
  - c. Cree la política de Snapshot.
2. Clúster 2:
  - a. Seleccione Cluster 2 en la página Policy.
  - b. Ignore la sección Snapshot policy.
  - c. Configure las políticas de replicación y backup en objetos.

### Cree una política de replicación antes de iniciar la replicación

Su estrategia 3-2-1 podría incluir la replicación de un volumen en otro sistema de almacenamiento. La política de replicación reside en el sistema de almacenamiento **secundario**.

#### Pasos

1. En la página Políticas, selecciona **Crear política > Crear política de replicación**.
2. En la sección Policy Details, especifique el nombre de la política.
3. Especifique las etiquetas de SnapMirror (máximo de 5) que indican la retención de cada etiqueta.
4. Especifique el programa de transferencia.
5. Seleccione **Crear**.

### Cree una política de almacenamiento de backup a objetos antes de iniciar el backup

Su estrategia 3-2-1 puede incluir realizar un backup de un volumen en un almacenamiento de objetos.

Esta normativa de almacenamiento reside en diferentes ubicaciones del sistema de almacenamiento según la arquitectura de backup:

- Fan-out: Sistema de almacenamiento principal
- En cascada: Sistema de almacenamiento secundario

## Pasos

1. En la página de administración de políticas, selecciona **Crear política > Crear política de copia de seguridad**.
2. En la sección Policy Details, especifique el nombre de la política.
3. Especifique las etiquetas de SnapMirror (máximo de 5) que indican la retención de cada etiqueta.
4. Especifique la configuración, incluido el programa de transferencia y cuándo archivar las copias de seguridad.
5. (Opcional) Para mover archivos de copia de seguridad antiguos a una clase de almacenamiento o nivel de acceso más baratos después de un cierto número de días, seleccione la opción **Archive** e indique el número de días que deben transcurrir antes de que los datos se archiven. Introduzca **0** como el "Archivo después de días" para enviar su archivo de copia de seguridad directamente al almacenamiento de archivos.

["Obtenga más información sobre la configuración de almacenamiento de archivado"](#).

6. (Opcional) Para evitar que sus copias de seguridad se modifiquen o eliminen, seleccione la opción **DataLock & Ransomware protection**.

Si su clúster utiliza ONTAP 9.11.1 o posterior, puede optar por proteger sus backups de la eliminación configurando *DataLock* y *Ransomware protection*.

["Obtenga más información acerca de los ajustes de DataLock disponibles"](#).

7. Seleccione **Crear**.

## Editar una política

Puede editar una política de Snapshot, replicación o backup personalizada.

El cambio en la política de backup afecta a todos los volúmenes que usan esa política.

## Pasos

1. En la página de administración de políticas, seleccione la política, seleccione las acciones \*  Y seleccione **Editar política**.



El proceso es el mismo para las políticas de replicación y backup.

2. En la página Edit Policy, realice los cambios.
3. Seleccione **Guardar**.

## Eliminar una política

Es posible eliminar políticas que no estén asociadas a ningún volumen.

Si hay una política asociada con un volumen y desea eliminar la política, primero debe quitar la política del volumen.

## Pasos

1. En la página de administración de políticas, seleccione la política, seleccione las acciones \* ... Y seleccione **Delete Snapshot policy**.
2. Seleccione **Eliminar**.

## Obtenga más información

Para obtener instrucciones sobre la creación de políticas con System Manager o la interfaz de línea de comandos de ONTAP, consulte lo siguiente:

["Cree una política de Snapshot mediante System Manager"](#)

["Cree una política de Snapshot mediante la CLI de ONTAP"](#)

["Cree una política de replicación mediante System Manager"](#)

["Cree una política de replicación mediante la CLI de ONTAP"](#)

["Cree un backup a la política de almacenamiento de objetos mediante System Manager"](#)

["Cree un backup en la política de almacenamiento de objetos mediante la CLI de ONTAP"](#)

## Opciones de política de copia de seguridad a objeto en la copia de seguridad y recuperación de BlueXP

El backup y la recuperación de datos de BlueXP te permite crear políticas de backup con una variedad de configuraciones para tus sistemas ONTAP y Cloud Volumes ONTAP on-premises.



Estas configuraciones de políticas son relevantes únicamente para el almacenamiento de backup en objetos. Ninguna de estas configuraciones afecta a las políticas de Snapshot o de replicación. En el futuro se añadirán configuraciones de directiva similares para instantáneas y replicaciones.

## Opciones de programación de backups

El backup y la recuperación de datos de BlueXP te permite crear varias políticas de backup con programaciones únicas para cada entorno de trabajo (clúster). Es posible asignar diferentes políticas de backup a volúmenes con diferentes objetivos de punto de recuperación (RPO).

Cada directiva de copia de seguridad proporciona una sección para *Labels & Retention* que puede aplicar a sus archivos de copia de seguridad. Tenga en cuenta que la política de Snapshot aplicada al volumen debe ser una de las políticas reconocidas por los archivos de backup y recuperación o backup de BlueXP no se creará.

| Name                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Default_Policy_Name         |        |                             |    |       |                             |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|--------|-----------------------------|----|-------|-----------------------------|----|
| <b>Labels &amp; Retention</b> <div> <div> 12 Labels </div> <div> <input checked="" type="checkbox"/> Hourly<br/> <input checked="" type="checkbox"/> Daily<br/> <input type="checkbox"/> Weekly<br/> <input type="checkbox"/> Monthly<br/> <input type="checkbox"/> Yearly </div> <div> Selected Labels (2) (Select up to 5 Labels) <table border="1"> <tbody> <tr> <td>Hourly</td> <td>Number of Backups to Retain</td> <td>12</td> </tr> <tr> <td>Daily</td> <td>Number of Backups to Retain</td> <td>30</td> </tr> </tbody> </table> </div> </div> |                             | Hourly | Number of Backups to Retain | 12 | Daily | Number of Backups to Retain | 30 |
| Hourly                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Number of Backups to Retain | 12     |                             |    |       |                             |    |
| Daily                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Number of Backups to Retain | 30     |                             |    |       |                             |    |
| DataLock & Ransomware Protection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | None                        |        |                             |    |       |                             |    |
| Archival Policy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Disabled                    |        |                             |    |       |                             |    |

Hay dos partes del programa; la etiqueta y el valor de retención:

- **Label** define la frecuencia con la que se crea (o actualiza) un archivo de copia de seguridad desde el volumen. Puede seleccionar entre los siguientes tipos de etiquetas:
  - Puede elegir uno o una combinación de, **cada hora**, **diario**, **semanal**, **mensual**, y **anualmente** plazos.
  - Puede seleccionar una de las políticas definidas por el sistema que proporcione backup y retención durante 3 meses, 1 año o 7 años.
  - Si creó políticas de protección de backup personalizadas en el clúster mediante ONTAP System Manager o la CLI de ONTAP, puede seleccionar una de esas políticas.
- El valor **Retention** define cuántos archivos de copia de seguridad se conservan para cada etiqueta (intervalo de tiempo). Una vez alcanzado el número máximo de backups en una categoría o intervalo, se eliminan los backups más antiguos de modo que siempre habrá los backups más recientes. Esto también ahorra costes de almacenamiento ya que los backups obsoletos no continúan ocupar espacio en el cloud.

Por ejemplo, diga que cree una política de copia de seguridad que cree copias de seguridad 7 **semanales** y 12 **mensuales**:

- cada semana y cada mes se crea un archivo de copia de seguridad para el volumen
- en la 8ª semana, se retira el primer backup semanal y se añade el nuevo backup semanal para la 8ª semana (con un máximo de 7 backups semanales)
- al 13 mes se elimina la primera copia de seguridad mensual, y se añade la nueva copia de seguridad mensual a 13 meses (se mantiene un máximo de 12 copias de seguridad mensuales)

Tenga en cuenta que los backups anuales se eliminarán automáticamente del sistema de origen tras transferirlos al almacenamiento de objetos. Este comportamiento predeterminado se puede cambiar "[En la página Advanced Settings](#)" Para el entorno de trabajo.

## Opciones de protección contra DataLock y Ransomware

El backup y la recuperación de BlueXP ofrece soporte para la protección DataLock y Ransomware para los backups de volúmenes. Estas funciones le permiten bloquear los archivos de backup y analizarlos para

detectar posibles ransomware en los archivos de backup. Este es un ajuste opcional que se puede definir en las políticas de backup cuando se desea contar con protección adicional para los backups de volúmenes para un clúster de.

Ambas características protegen sus archivos de copia de seguridad para que siempre tenga un archivo de copia de seguridad válido para recuperar los datos en caso de un intento de ataque de ransomware en sus copias de seguridad. También resulta útil satisfacer ciertos requisitos normativos en los que los backups deben bloquearse y conservarse durante un cierto período de tiempo. Cuando se habilita la opción DataLock and Ransomware Protection, el bloque de cloud que se aprovisiona como parte de la activación del backup y la recuperación de BlueXP tendrá habilitado el bloqueo de objetos y el control de versiones de objetos.

["Consulte el blog de protección de DataLock y Ransomware para obtener más información".](#)

Esta función no ofrece protección para los volúmenes de origen, solo para los backups de esos volúmenes de origen. Utilice algunos de los ["Protecciones contra el ransomware proporcionadas por ONTAP"](#) para proteger sus volúmenes de origen.



- Si tienes pensado utilizar la protección DataLock y Ransomware, puedes habilitarla al crear tu primera política de backup y activar el backup y la recuperación de BlueXP para ese clúster. Más adelante, puede habilitar o deshabilitar el análisis de ransomware utilizando la configuración avanzada de copia de seguridad y recuperación de BlueXP .
- Cuando BlueXP analiza un archivo de backup de ransomware al restaurar datos de volumen, tu proveedor de cloud incurrirá en costes adicionales de salida para acceder al contenido del archivo de backup.

## Qué es DataLock

DataLock protege sus archivos de copia de seguridad de ser modificados o eliminados durante un cierto período de tiempo - también llamado *almacenamiento inmutable*. Esta funcionalidad utiliza la tecnología del proveedor de almacenamiento de objetos para el «bloqueo de objetos». El período de tiempo durante el que el archivo de copia de seguridad está bloqueado (y retenido) se denomina período de retención de DataLock. Se basa en el programa de políticas de backup y la configuración de retención que haya definido, además de un búfer máximo de 31 días. Cualquier política de retención de DataLock que sea inferior a 31 días se redondea a un mínimo de 31 días.

Tenga en cuenta que los backups antiguos se eliminan una vez que caduca el período de retención de DataLock, no después de que caduque el período de retención de la política de backup.

Veamos algunos ejemplos de cómo funciona:

- Si crea un programa de copia de seguridad mensual con 12 retenciones, cada copia de seguridad se bloquea durante 12 meses (más un búfer máximo de 31 días) antes de que se elimine.
- Si crea una política de backup que crea 30 backups diarios, 7 semanales y 12 mensuales, habrá tres periodos de retención bloqueados. Los backups «30 diarios» se conservarían durante 44 días (30 días más un búfer máximo de 31 días), los backups «7 semanales» se conservarían durante 9 semanas (7 semanas más un búfer máximo de 31 días) y los backups «12 mensuales» se conservarían durante 12 meses (más un búfer máximo de 31 días).
- Si crea una programación de backup horaria con 24 retentions, puede pensar que los backups están bloqueados durante 24 horas. Sin embargo, dado que es inferior al mínimo de 30 días, cada copia de seguridad se bloqueará y conservará durante 44 días (30 días más un búfer máximo de 31 días).

En este último caso, puede observar que si cada archivo de copia de seguridad se bloquea durante 30 días (más un búfer de 31 días como máximo), acabará con muchos más archivos de copia de seguridad

de los que normalmente se conservarían con una política de retención de 24 horas. Normalmente, cuando el backup y la recuperación de BlueXP crea el archivo de backup de 25th, se eliminaría el backup más antiguo para mantener las retenciones máximas en 24 (según la política). En este caso, la configuración de retención de DataLock anula la configuración de retención de directivas de la política de copia de seguridad. Esto podría afectar a los costes de almacenamiento, ya que los archivos de backup se guardarán en el almacén de objetos durante un periodo de tiempo más largo.

## Qué es la protección contra Ransomware

La protección contra ransomware analiza sus archivos de backup para buscar pruebas de un ataque de ransomware. La detección de ataques de ransomware se realiza mediante una comparación de suma de comprobación. Si se identifica un posible ransomware en un archivo de copia de seguridad nuevo frente al anterior, ese archivo de copia de seguridad más reciente se reemplaza por el archivo de copia de seguridad más reciente que no muestra signos de un ataque de ransomware. (El archivo que se identificó como un ataque de ransomware se elimina un día después de su reemplazo).

Los análisis de ransomware se producen en los siguientes puntos en el proceso de backup y restauración:

- Cuando se crea un archivo de copia de seguridad.

También puede habilitar o deshabilitar los análisis de ransomware.

La exploración no se realiza en el archivo de copia de seguridad cuando se escribe por primera vez en el almacenamiento en nube, pero cuando se escribe el archivo de copia de seguridad **siguiente**. Por ejemplo, si tiene un programa de backup semanal establecido para el martes, el martes 14 se crea un backup. A continuación, se crea el martes 21 otro backup. El escaneado de ransomware se ejecuta en el archivo de copia de seguridad desde el 14 en este momento.

- Cuando intenta restaurar datos desde un archivo de copia de seguridad

Puede elegir ejecutar un análisis antes de restaurar datos de un archivo de copia de seguridad o omitir este análisis.

- Manualmente

Puede ejecutar un análisis de protección contra ransomware bajo demanda en cualquier momento para verificar el estado de un archivo de backup específico. Esto puede resultar útil si tuvo un problema de ransomware en un volumen en particular y desea verificar que los backups de ese volumen no se vean afectados.

## Opciones de bloqueo de datos y protección frente a ransomware

Cada política de copia de seguridad proporciona una sección para *DataLock* y *Protección de ransomware* que puede aplicar a sus archivos de copia de seguridad.

| AWS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Azure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><p><b>DataLock &amp; Ransomware Protection</b></p><p>Backup copies are protected from being modified or deleted, and they are scanned for ransomware threats.</p><p><input checked="" type="radio"/> None</p><p><input type="radio"/> Governance<br/>Users with specific permissions can overwrite or delete protected backup files during the retention period</p><p><input type="radio"/> Compliance<br/>No users can overwrite or delete protected backup files during the retention period</p></div> | <div><p><b>DataLock &amp; Ransomware Protection</b></p><p>Backup copies are protected from being modified or deleted, and they are scanned for ransomware threats.</p><p><input checked="" type="radio"/> None</p><p><input type="radio"/> Unlocked<br/>Backup files are protected during the retention period. The retention period can be increased or decreased. Typically used for 24 hours just to test the system.</p><p><input type="radio"/> Locked<br/>Backup files are protected during the retention period. The retention period can be increased, but it can't be decreased. Satisfies full regulatory compliance.</p></div> |
| <div><p><b>StorageGRID</b></p><div><p><b>DataLock &amp; Ransomware Protection</b></p><p>Backup copies are protected from being modified or deleted, and they are scanned for ransomware threats.</p><p><input checked="" type="radio"/> None</p><p><input type="radio"/> Compliance<br/>No users can overwrite or delete protected backup files during the retention period</p></div></div>                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Los análisis de protección contra ransomware están habilitados de forma predeterminada. La configuración predeterminada para la frecuencia de exploración es de 7 días. El análisis se realiza sólo en la última copia Snapshot. Puede habilitar o deshabilitar los análisis de ransomware en la última copia Snapshot usando la opción de la página Advanced Settings. Si la activa, las exploraciones se realizan cada 7 días de forma predeterminada.

Puede cambiar esa programación a días o semanas o deshabilitarla, lo que ahorrará costes.

Consulte "[Cómo actualizar las opciones de protección contra ransomware en la página Configuración avanzada](#)".

Puede elegir entre los siguientes ajustes para cada política de backup:



## AWS

- **Ninguno** (predeterminado)

La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Gobierno**

DataLock se establece en el modo *Governance* en el que se encuentran los usuarios `s3:BypassGovernanceRetention` permiso ("[consulte a continuación](#)") puede sobrescribir o eliminar archivos de copia de seguridad durante el período de retención. La protección contra ransomware está habilitada.

- **Cumplimiento**

DataLock se establece en el modo *Compliance* en el que ningún usuario puede sobrescribir ni eliminar archivos de copia de seguridad durante el período de retención. La protección contra ransomware está habilitada.

## Azure

- **Ninguno** (predeterminado)

La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Desbloqueado**

Los archivos de copia de seguridad se protegen durante el período de retención. El período de retención se puede aumentar o disminuir. Normalmente se usa durante 24 horas para probar el sistema. La protección contra ransomware está habilitada.

- **Bloqueado**

Los archivos de copia de seguridad se protegen durante el período de retención. El período de retención se puede aumentar, pero no se puede disminuir. Satisface todo el cumplimiento normativo. La protección contra ransomware está habilitada.

## StorageGRID

- **Ninguno** (predeterminado)

La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Cumplimiento**

DataLock se establece en el modo *Compliance* en el que ningún usuario puede sobrescribir ni eliminar archivos de copia de seguridad durante el período de retención. La protección contra ransomware está habilitada.

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

Puede habilitar la protección de datos Lock y ransomware en volúmenes de ONTAP desde los siguientes entornos de trabajo al usar almacenamiento de objetos en los siguientes proveedores de cloud público y privado. En próximos lanzamientos, se añadirán más proveedores de cloud.

| Entorno de trabajo de fuente       | Destino de archivo de copia de seguridad<br>ifdef::aws[]                                                                           |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Cloud Volumes ONTAP en AWS         | Endif de Amazon S3::aws[] ifdef::Azure[]                                                                                           |
| Cloud Volumes ONTAP en Azure       | Endif de Azure Blob::Azure[] ifdef::gcp[]<br>endif::gcp[]                                                                          |
| Sistema ONTAP en las instalaciones | Ifdef::aws[] Amazon S3 endif::aws[] ifdef::Azure[]<br>endif de Azure Blob::Azure[] ifdef::gcp[]<br>endif::gcp[] NetApp StorageGRID |

## Requisitos

- Para AWS:
  - Los clústeres deben ejecutar ONTAP 9.11.1 o posterior
  - El conector puede ponerse en marcha en el cloud o en sus instalaciones
  - Los siguientes permisos S3 deben formar parte del rol IAM que proporciona el conector con permisos. Residen en la sección "backupS3Policy" para el recurso "arn:aws:s3::netapp-backup-\*":

## Permisos de AWS S3

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectEtiquetado
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketEtiquetado
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionEtiquetado
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

["Vea el formato JSON completo para la directiva donde puede copiar y pegar los permisos necesarios"](#).

- Para Azure:
  - Los clústeres deben ejecutar ONTAP 9.12.1 o posterior
  - El conector puede ponerse en marcha en el cloud o en sus instalaciones
- Para StorageGRID:
  - Los clústeres deben ejecutar ONTAP 9.11.1 o posterior
  - Sus sistemas StorageGRID deben ejecutar 11.6.0.3 o posterior
  - El conector debe estar desplegado en sus instalaciones (se puede instalar en un sitio con o sin acceso

a Internet)

- Los siguientes permisos S3 deben formar parte del rol IAM que proporciona el conector permisos:

#### **Permisos de StorageGRID S3**

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectEtiquetado
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketEtiquetado
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionEtiquetado
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

#### **Restricciones**

- La función de protección DataLock y Ransomware no está disponible si configuró un almacenamiento de archivado en la política de backup.
- La opción DataLock que seleccione al activar el backup y la recuperación de BlueXP debe utilizarse para todas las políticas de backup para ese clúster.
- No puede utilizar varios modos DataLock en un único cluster.
- Si activa DataLock, se bloquearán todas las copias de seguridad de los volúmenes. No se pueden mezclar backups de volúmenes bloqueados y no bloqueados para un solo clúster.

- La protección de DataLock y ransomware se aplica a backups de volúmenes nuevos con una política de backup con protección de datos Lock y ransomware habilitada. Posteriormente, puede activar o desactivar estas funciones mediante la opción Configuración avanzada.
- Los volúmenes de FlexGroup pueden usar la protección DataLock y Ransomware solo si se utilizan ONTAP 9.13.1 o posterior.

## Consejos sobre cómo mitigar los costes de DataLock

Puede habilitar o deshabilitar la función Ransomware Scan mientras mantiene activa la función DataLock. Para evitar cargos adicionales, se pueden deshabilitar los análisis programados de ransomware. Esto le permite personalizar su configuración de seguridad y evitar incurrir en costes por parte del proveedor de la nube.

Incluso si se deshabilitan los análisis programados de ransomware, puede seguir realizando análisis bajo demanda cuando sea necesario.

Puede elegir diferentes niveles de protección:

- **DataLock *without* ransomware scans:** Proporciona protección para los datos de copia de seguridad en el almacenamiento de destino que puede estar en el modo Gobernanza o Cumplimiento.
  - **Modo de gobernanza:** Ofrece flexibilidad a los administradores para sobrescribir o eliminar datos protegidos.
  - **Modo de cumplimiento:** Proporciona una completa imposibilidad de borrado hasta que expire el período de retención. De este modo se cumplen los requisitos más estrictos de seguridad de datos de entornos altamente regulados. Los datos no se pueden sobrescribir ni modificar a lo largo de su ciclo de vida, lo que ofrece el nivel más sólido de protección para sus copias de backup.



En su lugar, Microsoft Azure utiliza el modo Bloquear y desbloquear.

- **DataLock *with* ransomware scans:** Proporciona una capa adicional de seguridad para sus datos. Esta función ayuda a detectar cualquier intento de cambiar las copias de backup. Si se realiza algún intento, se crea discretamente una nueva versión de los datos. La frecuencia de exploración se puede cambiar a 1, 2, 3, 4, 5, 6 o 7 días. Si los escaneos se establecen en cada 7 días, los costos disminuyen significativamente.

Para obtener más consejos sobre cómo mitigar los costes de DataLock, consulte

<https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-BlueXP-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475>

Además, puede obtener estimaciones del costo asociado con DataLock visitando el "[Calculadora de coste total de propiedad \(TCO\) de backup y recuperación de BlueXP](#)".

## Opciones de almacenamiento de archivado

Al utilizar el almacenamiento en cloud de AWS, Azure o Google, puede mover archivos de backup antiguos a un tipo de almacenamiento de archivado más económico o a un nivel de acceso transcurridos un cierto número de días. También puede optar por enviar sus archivos de copia de seguridad al almacenamiento de archivos inmediatamente sin ser escrito en el almacenamiento en la nube estándar. Simplemente ingrese **0** como el "Archivo después de días" para enviar su archivo de copia de seguridad directamente al almacenamiento de archivos. Esto puede ser especialmente útil para los usuarios que rara vez necesitan acceder a los datos de backups en la nube o los usuarios que están reemplazando una solución de copia de seguridad a cinta.

No es posible acceder a los datos de los niveles de archivado inmediatamente cuando sea necesario y el

coste de recuperación será superior, por lo que debe tener en cuenta con qué frecuencia puede necesitar restaurar los datos de los archivos de backup antes de decidir archivar los archivos de backup.



- Aunque seleccione «0» para enviar todos los bloques de datos al almacenamiento en cloud de archivado, los bloques de metadatos se escriben siempre en almacenamiento en cloud estándar.
- El almacenamiento de archivado no se puede utilizar si ha habilitado DataLock.
- No puede cambiar la política de archivado después de seleccionar **0** días (archivo inmediatamente).

Cada directiva de copia de seguridad proporciona una sección para *Archival Policy* que puede aplicar a los archivos de copia de seguridad.

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                        |   |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
| Name                             | Default_Policy_Name                                                                                                                                                                                                                                                                                                                                                                                                    | ▼ |
| Labels & Retention               | 30 Daily                                                                                                                                                                                                                                                                                                                                                                                                               | ▼ |
| DataLock & Ransomware Protection | None                                                                                                                                                                                                                                                                                                                                                                                                                   | ▼ |
| Archival Policy                  | <div>Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.</div> <div><input checked="" type="checkbox"/> Tier Backups to Archive</div> <div>Archive After (Days)<br/><input type="text" value="30"/></div> <div>Storage Class<br/><input type="text" value="S3 Glacier"/></div> |   |

- 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.

Si el clúster utiliza ONTAP 9.10.1 o superior, puede organizar en niveles los backups antiguos en el almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive*. ["Obtenga más información acerca del almacenamiento de archivado de AWS"](#).

- Si seleccionas ningún nivel de archivado en tu primera política de backup al activar el backup y la recuperación de BlueXP, *S3 Glacier* será tu única opción de archivado para futuras políticas.
  - Si selecciona *S3 Glacier* en su primera política de copia de seguridad, puede cambiar a la capa *S3 Glacier Deep Archive* para futuras políticas de copia de seguridad para ese cluster.
  - Si selecciona *S3 Glacier Deep Archive* en su primera política de copia de seguridad, ese nivel será el único nivel de archivado disponible para futuras políticas de copia de seguridad para ese cluster.
- En Azure, los backups están asociados con el nivel de acceso *Cool*.

Si su clúster utiliza ONTAP 9.10.1 o superior, puede organizar en niveles los backups anteriores en el almacenamiento de *Azure Archive*. ["Obtenga más información sobre el almacenamiento de archivado de Azure"](#).

- En GCP, las copias de seguridad están asociadas con la clase de almacenamiento *Standard*.

Si tu clúster on-premises utiliza ONTAP 9.12.1 o posterior, puedes elegir organizar en niveles los backups antiguos en el almacenamiento *Archive* en la interfaz de usuario de backup y recuperación de BlueXP

después de un determinado número de días para optimizar los costes. ["Más información sobre el almacenamiento de archivos de Google"](#).

- En StorageGRID, las copias de seguridad están asociadas con la clase de almacenamiento *Standard*.

Si su clúster de on-prem utiliza ONTAP 9.12.1 o superior y su sistema StorageGRID utiliza 11.4 o superior, puede archivar archivos de backup antiguos en el almacenamiento de archivado en cloud público.

+ \*\* para AWS, puede organizar los backups en niveles en el almacenamiento AWS *S3 Glacier* o *S3 Glacier Deep Archive*. ["Obtenga más información acerca del almacenamiento de archivado de AWS"](#).

+ \*\* para Azure, puede organizar en niveles los backups antiguos para el almacenamiento *Azure Archive*. ["Obtenga más información sobre el almacenamiento de archivado de Azure"](#).

+

["Obtenga más información sobre el archivado de archivos de backup desde StorageGRID"](#).

## Administre las opciones de almacenamiento de copia de seguridad en objetos en la página Configuración avanzada de la copia de seguridad y recuperación de BlueXP

Puede cambiar la configuración de almacenamiento de backup en objetos y a nivel de clúster que estableció al activar el backup y la recuperación de BlueXP para cada sistema ONTAP mediante la página Configuración avanzada. También puede modificar algunos ajustes que se aplican como ajustes de copia de seguridad "predeterminados". Esto incluye cambiar la tasa de transferencia de los backups al almacenamiento de objetos, tanto si las copias de Snapshot históricas se exportan como archivos de backup como habilitar o deshabilitar los análisis de ransomware para un entorno de trabajo.



Estos ajustes solo están disponibles para el almacenamiento de backup en objetos. Ninguna de estas opciones afecta a la configuración Snapshot o de replicación. En el futuro se añadirán configuraciones similares de replicaciones a nivel de clúster para instantáneas y replicaciones.

Puede cambiar las siguientes opciones en la página Configuración avanzada:

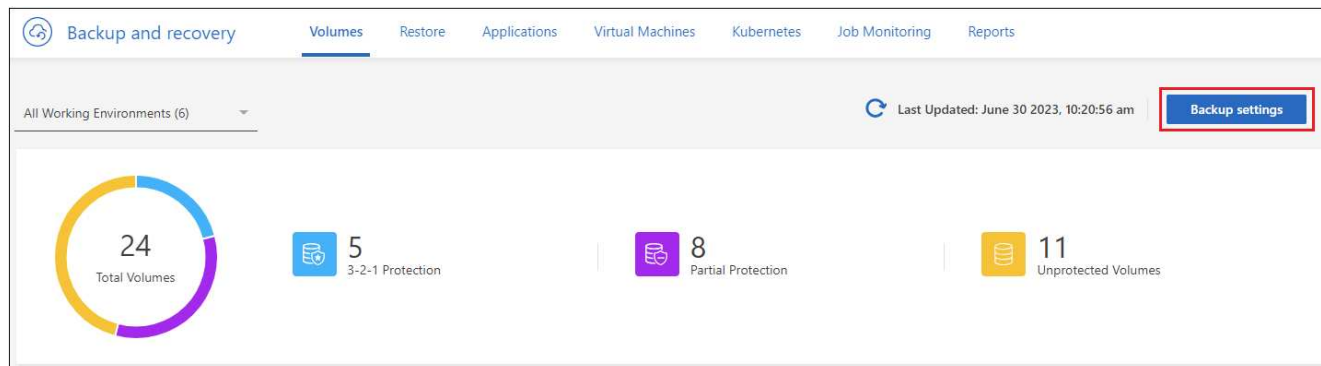
- Cambio del ancho de banda de red asignado para cargar backups en el almacenamiento de objetos mediante la opción Tasa de transferencia máxima
- Cambiar si las copias Snapshot históricas se exportan como archivos de backup y se incluyen en los archivos de backup básicos iniciales para volúmenes futuros
- Cambiar si las copias Snapshot "anuales" se eliminan del sistema de origen
- Habilitar o deshabilitar los análisis de ransomware para un entorno de trabajo, incluidos los análisis programados

## Ver la configuración de backup en el nivel del clúster

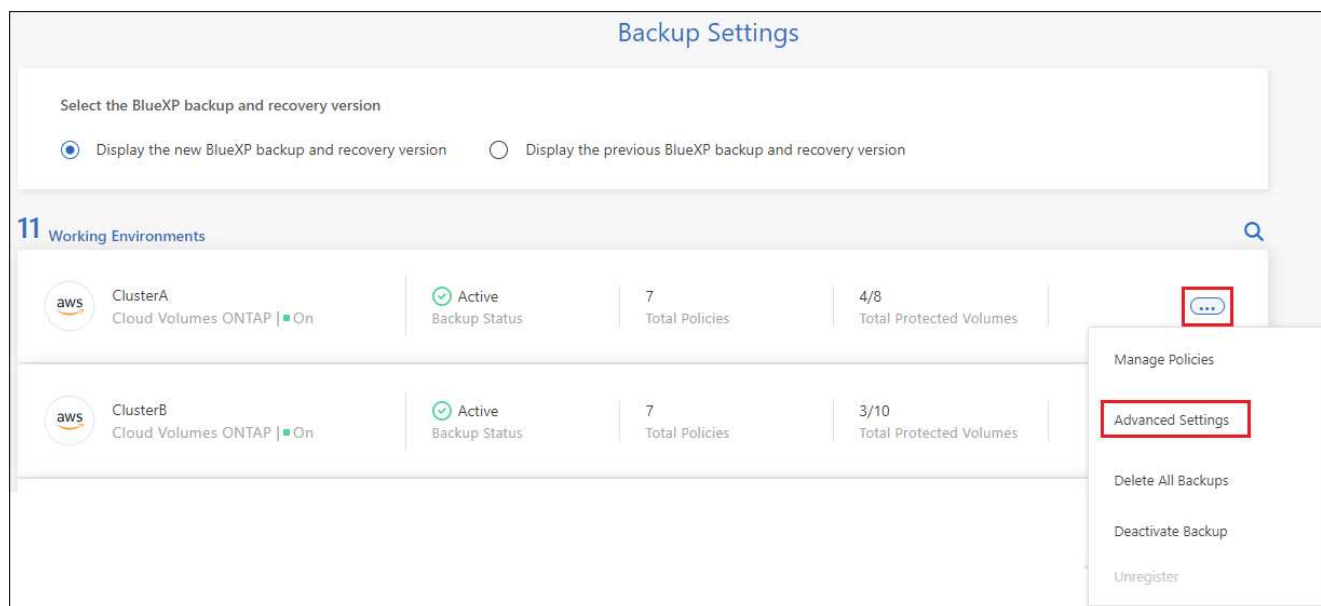
Es posible ver la configuración de backup a nivel de clúster de cada entorno de trabajo.

### Pasos

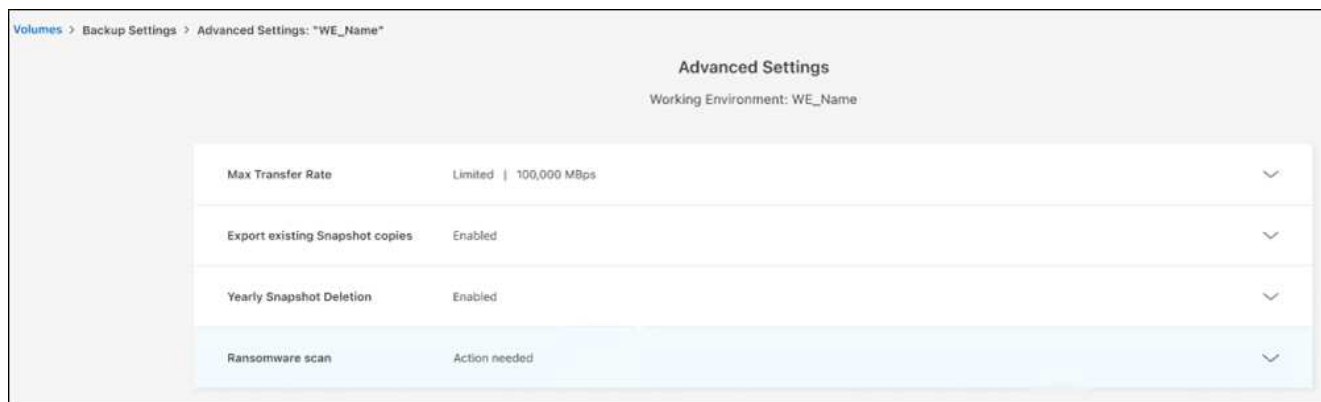
1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.



3. En la página *Backup Settings*, haga clic en ... Para el entorno de trabajo y seleccione **Configuración avanzada**.



La página *Advanced Settings* muestra la configuración actual de ese entorno de trabajo.



4. Amplíe la opción y realice el cambio.

Todas las operaciones de backup después del cambio utilizarán los nuevos valores.



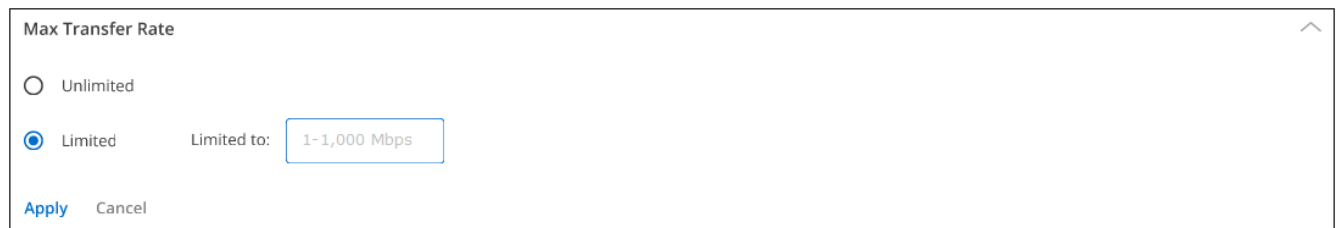
Tenga en cuenta que algunas opciones no están disponibles según la versión de ONTAP en el clúster de origen y basadas en el destino del proveedor de cloud en el que residen los backups.

## Cambie el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos

Al activar el backup y la recuperación de BlueXP en un entorno de trabajo, de forma predeterminada, ONTAP puede usar una cantidad ilimitada de ancho de banda para transferir los datos de backup de los volúmenes del entorno de trabajo al almacenamiento de objetos. Si observa que el tráfico de backup afecta a las cargas de trabajo de usuario normales, puede reducir la cantidad de ancho de banda de red que se usa durante la transferencia mediante la opción Tasa de transferencia máxima de la página Advanced Settings.

### Pasos

1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.
2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo y seleccione **Configuración avanzada**.
3. En la página Configuración avanzada, expanda la sección **Tasa de transferencia máxima**.



Max Transfer Rate

☐ Unlimited

☒ Limited      Limited to:

Apply    Cancel

4. Elija un valor entre 1 y 1.000 Mbps como velocidad de transferencia máxima.
5. Seleccione el botón de opción **limitado** e introduzca el ancho de banda máximo que puede utilizarse, o seleccione **ilimitado** para indicar que no hay límite.
6. Seleccione **aplicar**.

Esta configuración no afecta al ancho de banda asignado a ninguna otra relación de replicación que se pueda configurar para volúmenes en el entorno de trabajo.

## Cambie si las copias snapshot históricas se exportan como archivos de backup

Si hay copias Snapshot locales para los volúmenes que coinciden con la etiqueta de programación de backup que utiliza en este entorno de trabajo (por ejemplo, diario, semanal, etc.), puede exportar estas copias Snapshot históricas al almacenamiento de objetos como archivos de backup. Esto permite inicializar backups en el cloud al mover copias de Snapshot más antiguas a la copia de backup de referencia.

Tenga en cuenta que esta opción solo se aplica a nuevos archivos de backup de nuevos volúmenes de lectura/escritura y no es compatible con volúmenes de protección de datos (DP).

### Pasos

1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.
2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo y seleccione **Configuración avanzada**.
3. En la página Configuración avanzada, expanda la sección **Exportar copias snapshot existentes**.

Export existing Snapshot copies

☒ Export existing Snapshot copies to object storage as backup files

All historical Snapshot copies of read/write volumes that match the Backup schedule label (daily, weekly, etc.) will be copied to object storage as backup files to ensure the most complete data protection.

Apply Cancel

4. Seleccione si desea que se exporten las copias de Snapshot existentes.

5. Seleccione **aplicar**.

## Cambie si las instantáneas "anuales" se eliminan del sistema de origen

Cuando se selecciona la etiqueta de backup "anual" para una política de backup para cualquiera de los volúmenes, la copia de Snapshot que se crea es muy grande. De forma predeterminada, estas copias de Snapshot anuales se eliminan automáticamente del sistema de origen después de transferirse al almacenamiento de objetos. Puede cambiar este comportamiento predeterminado en la sección Eliminación anual de Snapshot.

### Pasos

1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.
2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo y seleccione **Configuración avanzada**.
3. En la página Configuración avanzada, expanda la sección **Eliminación de instantánea anual**.

Yearly Snapshot Deletion
Enabled

☒ Enabled  
Yearly Snapshot copies are deleted from the source system after being transferred to object storage as backups.

☐ Disabled  
Yearly Snapshot copies are retained on the source system. Note that these snapshots can be large.

Apply Cancel

4. Seleccione **Desactivado** para conservar las instantáneas anuales en el sistema de origen.

5. Seleccione **aplicar**.

## Habilitar o deshabilitar los análisis de ransomware

Los análisis de protección contra ransomware están habilitados de forma predeterminada. La configuración predeterminada para la frecuencia de exploración es de 7 días. El análisis se realiza sólo en la última copia Snapshot. Puede habilitar o deshabilitar los análisis de ransomware en la última copia Snapshot usando la opción de la página Advanced Settings. Si la activa, las exploraciones se realizan cada 7 días de forma predeterminada.

Puede cambiar esa programación a días o semanas o deshabilitarla, lo que ahorrará costes.



Habilitar los análisis de ransomware incurrirá en cargos adicionales en función del proveedor de cloud.

Los análisis programados de ransomware se ejecutan solo en la última copia Snapshot.

Si se deshabilitan los análisis programados de ransomware, puede seguir ejecutando análisis bajo demanda y seguir realizando el análisis durante una operación de restauración.

Consulte "[Gestionar políticas](#)" para obtener más información sobre la gestión de políticas que implementan la detección de ransomware.

### Pasos

1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.
2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo y seleccione **Configuración avanzada**.
3. En la página Configuración avanzada, expanda la sección **Ransomware scan**.
4. Habilitar o deshabilitar **Ransomware Scan**.
5. Seleccione **scheduled ransomware scan**.
6. De manera opcional, cambie el análisis predeterminado de cada semana a días o semanas.
7. Establezca la frecuencia en días o semanas que debe ejecutarse el análisis.
8. Seleccione **aplicar**.

## Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3 con la copia de seguridad y recuperación de BlueXP

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en Amazon S3.

### Inicio rápido

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

1

#### Verifique la compatibilidad con la configuración

- Está ejecutando Cloud Volumes ONTAP 9,8 o posterior en AWS (se recomienda ONTAP 9.8P13 y versiones posteriores).
- 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 backup y recuperación de BlueXP de NetApp.
- Tiene un conector instalado en AWS:
  - El Conector se puede instalar en un sitio con acceso completo a Internet ("modo estándar") o con conectividad a Internet limitada ("modo restringido").
  - La función IAM que proporciona el conector BlueXP con permisos incluye permisos S3 de la última versión "[Política de BlueXP](#)".

**2**

### **Prepare el conector BlueXP**

Si ya tiene un conector desplegado en una región de AWS, entonces está todo listo. De lo contrario, tendrás que instalar un conector BlueXP en AWS para realizar backups de los datos de Cloud Volumes ONTAP en AWS. El Conector se puede instalar en un sitio con acceso completo a Internet (“modo estándar”) o con conectividad a Internet limitada (“modo restringido”).

**3**

### **Verifique los requisitos de licencia**

Tendrás que comprobar los requisitos de licencias tanto para AWS como para BlueXP.

**4**

### **Compruebe los requisitos de red de ONTAP para replicar volúmenes**

Asegúrese de que los sistemas de almacenamiento principal y secundario cumplan con los requisitos de red y versión de ONTAP.

**5**

### **Habilita el backup y la recuperación de datos de BlueXP**

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

**6**

### **Active backups en sus ONTAP Volumes**

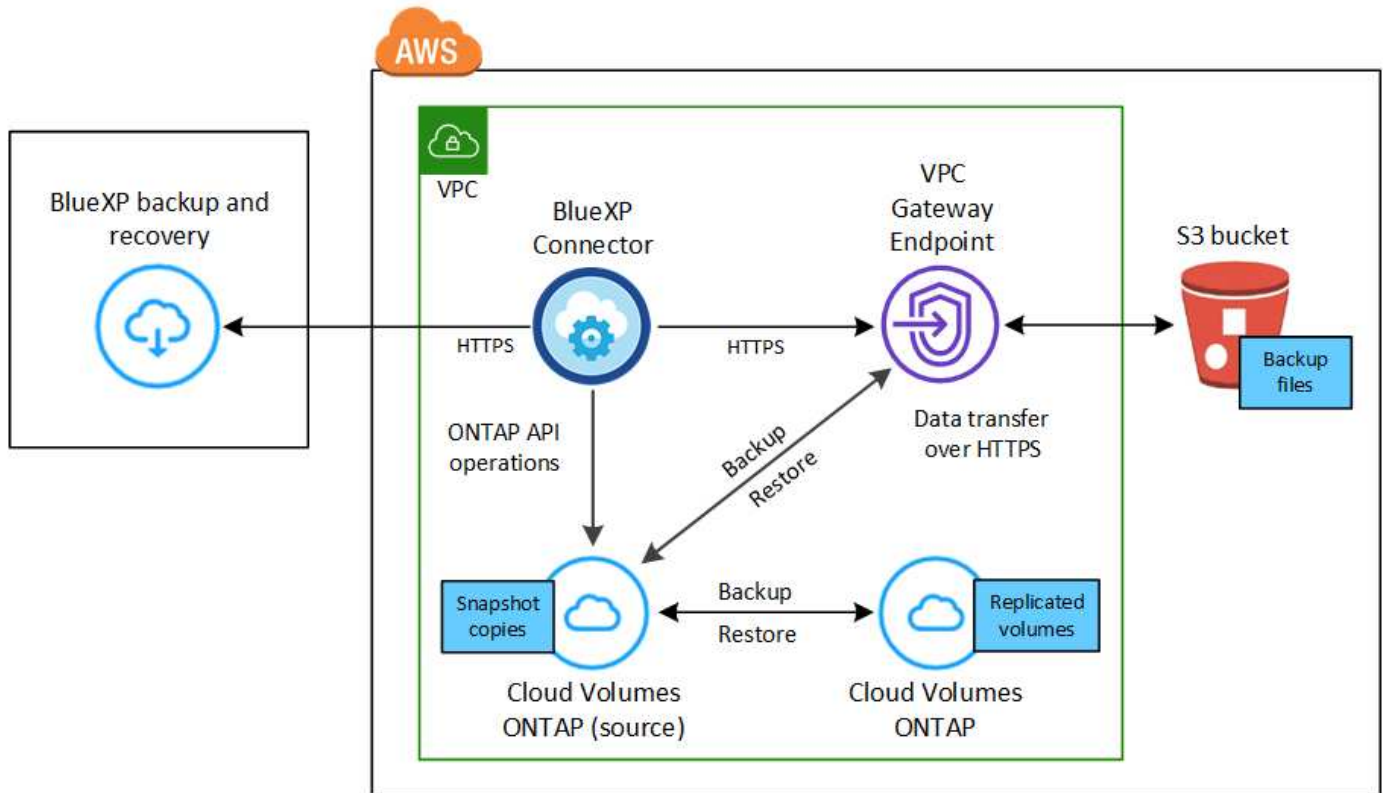
Siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

## **Verifique la compatibilidad con la configuración**

Lea los siguientes requisitos para asegurarse de que tenga una configuración compatible antes de comenzar a realizar el backup de volúmenes en S3.

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

Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.



El extremo de la puerta de enlace VPC ya debe existir en su VPC. ["Más información sobre los extremos de puerta de enlace"](#).

### Versiones de ONTAP compatibles

Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.

### Información requerida para usar claves gestionadas por el cliente para el cifrado de datos

Puede elegir sus propias claves gestionadas por el cliente para el cifrado de datos en el asistente de activación en lugar de utilizar las claves de cifrado predeterminadas de Amazon S3. En este caso, tendrá que tener ya configuradas las claves de cifrado gestionadas. ["Vea cómo usar sus propias claves"](#).

### Verifique los requisitos de licencia

Para obtener la licencia PAYGO de backup y recuperación de BlueXP, hay una suscripción de BlueXP disponible en AWS Marketplace que permite la implementación de backup y recuperación de datos de Cloud Volumes ONTAP y BlueXP. Necesita hacerlo ["suscríbase a esta suscripción a BlueXP"](#) Antes de habilitar el backup y la recuperación de datos de BlueXP. La facturación para el backup y la recuperación de BlueXP se realiza a través de 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 disponer de un contrato anual que te permita agrupar el backup y la recuperación de Cloud Volumes ONTAP y BlueXP, debes configurar el contrato anual cuando crees un entorno de trabajo de Cloud Volumes ONTAP. Esta opción no le permite realizar un backup de los datos en las instalaciones.

Para la licencia BYOL de backup y recuperación de BlueXP, necesita el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias"](#)

**BYOL**". Debe utilizar una licencia BYOL cuando el sistema Connector y Cloud Volumes ONTAP se pongan en marcha en un sitio oscuro.

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

## Prepare el conector BlueXP

El conector debe instalarse en una región de AWS con acceso a Internet completo o limitado (modo "estándar" o "restringido"). ["Consulta los modos de puesta en marcha de BlueXP para obtener más información"](#).

- ["Más información sobre conectores"](#)
- ["Implemente un conector en AWS en modo estándar \(acceso completo a Internet\)"](#)
- ["Instale el conector en modo restringido \(acceso saliente limitado\)"](#)

## Verifique o agregue permisos al conector

La función IAM que proporciona permisos BlueXP debe incluir permisos S3 de la última versión ["Política de BlueXP"](#). Si la política no contiene todos estos permisos, consulte ["Documentación de AWS: Editar políticas de IAM"](#).

A continuación se muestran los permisos específicos de la directiva:

```

{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:PutObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "athena:StartQueryExecution",
    "athena:GetQueryResults",
    "athena:GetQueryExecution",
    "glue:GetDatabase",
    "glue:GetTable",

```

```

        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}

```



Cuando cree backups en regiones de AWS China, debe cambiar el nombre de recurso de AWS «arn» en todas las secciones *Resource* de las políticas de IAM de «aws» a «aws-cn», por ejemplo `arn:aws-cn:s3:::netapp-backup-*`.

### Permisos necesarios de AWS Cloud Volumes ONTAP

Cuando tu sistema Cloud Volumes ONTAP ejecuta el software de ONTAP 9.12.1 o posterior, el rol de IAM que ofrece ese entorno de trabajo con permisos debe incluir un nuevo conjunto de permisos S3 específicamente para backup y recuperación de BlueXP de la versión más reciente "[Política de Cloud Volumes ONTAP](#)".

Si ha creado el entorno de trabajo de Cloud Volumes ONTAP con BlueXP versión 3.9.23 o superior, estos permisos ya deberían formar parte del rol IAM. De lo contrario, tendrá que agregar los permisos que faltan.

### Regiones admitidas de AWS

La copia de seguridad y recuperación de BlueXP es compatible con todas las regiones de AWS, incluidas las regiones de AWS GovCloud.

### Configuración necesaria para crear backups en una cuenta de AWS diferente

De manera predeterminada, los backups se crean con la misma cuenta que la utilizada para el sistema Cloud Volumes ONTAP. Si desea usar una cuenta de AWS diferente para sus backups, debe realizar lo siguiente:

- Compruebe que los permisos "s3:PutBucketPolicy" y "s3:PutBucketOwnershipControls" forman parte de la función IAM que proporciona permisos al conector BlueXP.
- Añada las credenciales de cuenta de AWS de destino en BlueXP. "[Descubra cómo hacerlo](#)".
- Añada los siguientes permisos en las credenciales de usuario de la segunda cuenta:



```
"athena:StartQueryExecution",  
"athena:GetQueryResults",  
"athena:GetQueryExecution",  
"glue:GetDatabase",  
"glue:GetTable",  
"glue:CreateTable",  
"glue:CreateDatabase",  
"glue:GetPartitions",  
"glue:BatchCreatePartition",  
"glue:BatchDeletePartition"
```

### Crea tus propios cubos

De forma predeterminada, el servicio crea buckets para usted. Si desea utilizar sus propios depósitos, puede crearlos antes de iniciar el asistente de activación de copias de seguridad y, a continuación, seleccionar esos depósitos en el asistente.

["Obtenga más información sobre cómo crear sus propios cubos".](#)

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP".](#)

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.
- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en subredes diferentes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).

## Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP

Habilitar el backup y la recuperación de datos de BlueXP es muy sencillo. Los pasos difieren ligeramente dependiendo de si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

### Habilitar la copia de seguridad y recuperación de BlueXP en un nuevo sistema

El backup y la recuperación de BlueXP están habilitados de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.

Consulte ["Inicio de Cloud Volumes ONTAP en AWS"](#) Para conocer los requisitos y detalles de cómo crear el sistema Cloud Volumes ONTAP.

### Pasos

1. En BlueXP Canvas, selecciona **Agregar entorno de trabajo**, elige el proveedor de la nube y selecciona **Agregar nuevo**. Selecciona **Crear Cloud Volumes ONTAP**.
2. Seleccione **Amazon Web Services** como proveedor de la nube y, a continuación, elija un único nodo o sistema de alta disponibilidad.
3. Rellene la página Details & Credentials.
4. En la página Servicios, deje el servicio habilitado y seleccione **Continuar**.



5. Complete las páginas del asistente para implementar el sistema.

### Resultado

El backup y la recuperación de datos de BlueXP están activados en el sistema. Después de crear volúmenes en estos sistemas Cloud Volumes ONTAP, inicie el backup y la recuperación de datos de BlueXP y. ["active el backup en cada volumen que desee proteger"](#).

### Habilitar la copia de seguridad y recuperación de BlueXP en un sistema existente

Habilita el backup y la recuperación de BlueXP en un sistema existente en cualquier momento directamente desde el entorno de trabajo.

### Pasos

1. En BlueXP Canvas, selecciona el entorno de trabajo y selecciona **Habilitar** junto al servicio de 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 al entorno de trabajo Amazon S3 para iniciar el asistente de configuración.



Para modificar la configuración de copia de seguridad o agregar replicación, consulte ["Gestión de backups de ONTAP"](#).

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.



Si el destino de AWS para sus backups existe como entorno de trabajo en Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de AWS.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, selecciona las **Acciones** ... Icono y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:
  - Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
  - Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

### Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el](#)

backup para volúmenes adicionales en el entorno de trabajo" (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.
  - Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
  - Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
  - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).
2. Seleccione **Siguiente**.

## Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye del sistema de almacenamiento primario al secundario, y del almacenamiento secundario al objeto.

- **Fan Out:** La información fluye del sistema de almacenamiento primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

### 3. **Instantánea local:** Elija una política de Snapshot existente o cree una nueva.



Para crear una política personalizada antes de activar la instantánea, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

### 4. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del volumen replicado.
- **Política de replicación:** Elija una política de replicación existente o cree una.



Para crear una política personalizada, consulte ["Crear una política"](#)..

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

### 5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Amazon Web Services**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor y la región donde se almacenarán las copias de seguridad.

Introduzca la cuenta de AWS utilizada para almacenar los backups. Esta cuenta puede ser diferente de la ubicación en la que reside el sistema Cloud Volumes ONTAP.

Si desea utilizar una cuenta AWS diferente para las copias de seguridad, debe agregar las credenciales de la cuenta AWS de destino en BlueXP y agregar los permisos "s3:PutBucketPolicy" y "s3:PutBucketOwnershipControls" a la función IAM que proporciona permisos a BlueXP.

Seleccione la región donde se almacenarán las copias de seguridad. Esta puede ser una región diferente a la ubicación en la que reside el sistema Cloud Volumes ONTAP.

Cree un nuevo depósito o seleccione uno existente.

- **Clave de cifrado:** Si creaste un nuevo depósito, ingresa la información de la clave de cifrado que se te haya proporcionado del proveedor. Elija si utilizará las claves de cifrado predeterminadas de AWS o si elige sus propias claves gestionadas por el cliente de su cuenta de AWS para gestionar el cifrado de

sus datos. ("[Vea cómo usar sus propias claves de cifrado](#)").

Si decide utilizar sus propias claves gestionadas por el cliente, introduzca el almacén de claves y la información de clave.



Si eligió un depósito existente, la información de cifrado ya está disponible, por lo que no necesita introducirla ahora.

- **Política de copia de seguridad:** Seleccione una política de almacenamiento de copia de seguridad a objeto existente o cree una.



Para crear una política personalizada antes de activar el backup, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
  - Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
  - En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte "[Configuración de políticas de backup en objeto](#)".
  - Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen de almacenamiento principal.

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta que ha introducido, y los archivos de copia de seguridad se almacenan allí.

La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la "[Panel de control de trabajos](#)".

### Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

### El futuro

- Puede hacerlo "[gestione los archivos de copia de seguridad y las políticas de copia de seguridad](#)". Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo "[gestione la configuración de backup en el nivel del clúster](#)". Esto incluye cambiar las claves de almacenamiento que utiliza ONTAP para acceder al almacenamiento en cloud, cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo "[restaure volúmenes, carpetas o archivos individuales desde un archivo de backup](#)". A un sistema Cloud Volumes ONTAP en AWS o a un sistema ONTAP en las instalaciones.

## Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en el almacenamiento de blobs de Azure con BlueXP Backup and Recovery

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en el almacenamiento de blobs de Azure.

### Inicio rápido

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

1

#### Verifique la compatibilidad con la configuración

- Está ejecutando Cloud Volumes ONTAP 9,8 o posterior en Azure (se recomienda ONTAP 9.8P13 y versiones posteriores).
- 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](#)", o usted ha comprado "[y activado](#)" Una licencia BYOL de backup y recuperación de BlueXP de NetApp.

2

### Prepare el conector BlueXP

Si ya tiene un conector implementado en una región de Azure, entonces está todo listo. De lo contrario, tendrás que instalar un conector BlueXP en Azure para realizar backups de los datos de Cloud Volumes ONTAP en almacenamiento de Azure Blob. El Conector se puede instalar en un sitio con acceso completo a Internet ("modo estándar") o con conectividad a Internet limitada ("modo restringido").

[Prepare el conector BlueXP](#)

3

### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencias tanto de Azure como de BlueXP.

Consulte [Verifique los requisitos de licencia](#).

4

### Compruebe los requisitos de red de ONTAP para replicar volúmenes

Asegúrese de que los sistemas de origen y destino cumplen con los requisitos de red y versión de ONTAP.

[Compruebe los requisitos de red de ONTAP para replicar volúmenes](#).

5

### Habilita el backup y la recuperación de datos de BlueXP

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

[Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP](#).

6

### Active backups en sus ONTAP Volumes

Siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

[Active backups en sus ONTAP Volumes](#).

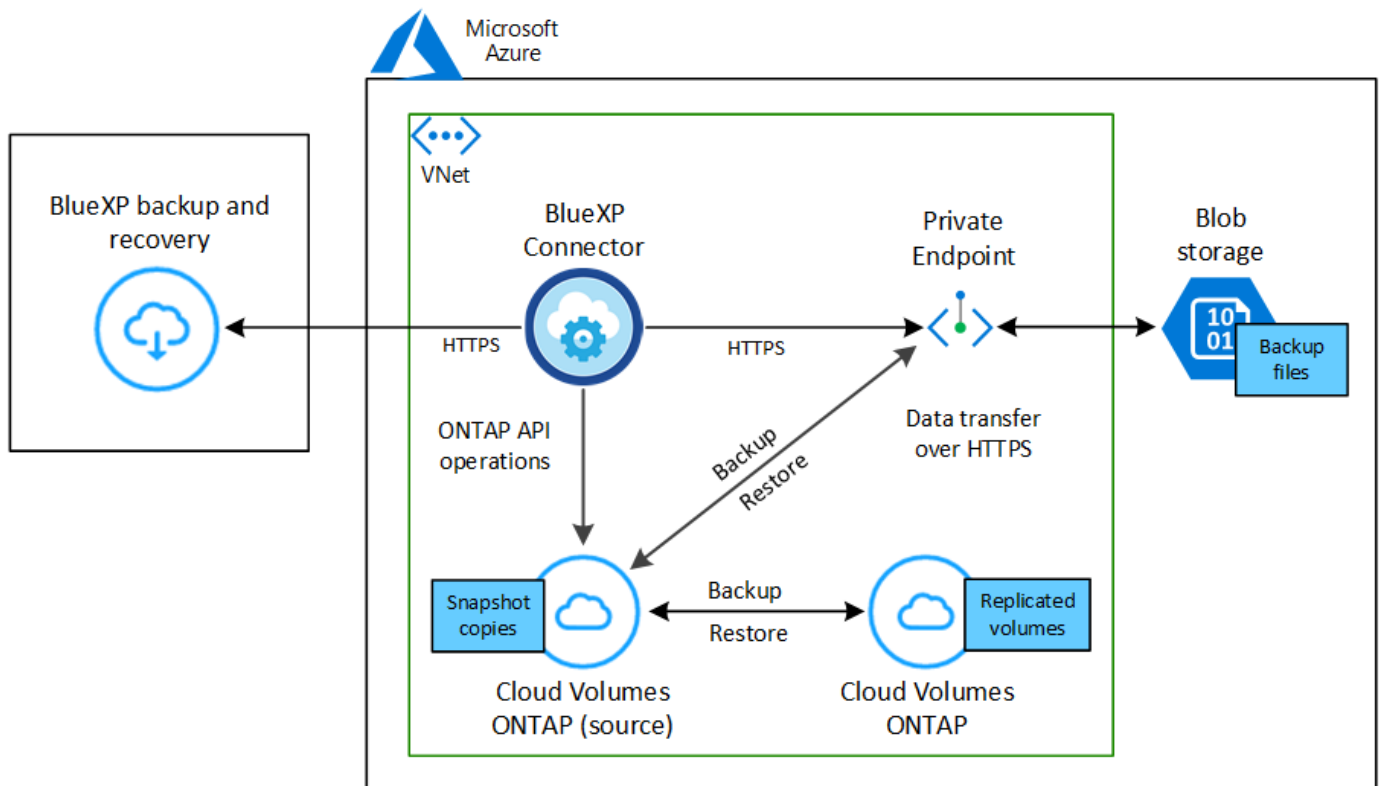
## Verifique la compatibilidad con la configuración

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar backups de volúmenes en el almacenamiento de Azure Blob.

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

Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.





### Versiones de ONTAP compatibles

Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.

### Regiones de Azure compatibles

La copia de seguridad y recuperación de BlueXP se admite en todas las regiones de Azure, incluidas las regiones de Azure Government.

De forma predeterminada, el backup y la recuperación de BlueXP aprovisiona el Blob Container con redundancia local (LRS) para la optimización de costes. Puedes cambiar esta configuración a Redundancia de zona (ZRS) una vez activado el backup y la recuperación de BlueXP, si quieres asegurarte de que tus datos se replican entre diferentes zonas. Consulte las instrucciones de Microsoft para ["cambiar el modo de replicar la cuenta de almacenamiento"](#).

### Configuración necesaria para crear backups en una suscripción diferente de Azure

De forma predeterminada, las copias de seguridad se crean con la misma suscripción que la utilizada para el sistema Cloud Volumes ONTAP. Si desea utilizar una suscripción de Azure diferente para sus backups, debe hacerlo ["Inicie sesión en el portal de Azure y vincule las dos suscripciones"](#).

### Verifique los requisitos de licencia

Para las licencias PAYGO de backup y recuperación de BlueXP, es necesaria una suscripción a través de Azure Marketplace antes de habilitar el backup y la recuperación de BlueXP. La facturación para el backup y la recuperación de BlueXP se realiza a través de esta suscripción. ["Puede suscribirse desde la página Detalles Credentials del asistente de entorno de trabajo"](#).

Para la licencia BYOL de backup y recuperación de BlueXP, necesita el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#). Debe utilizar una licencia BYOL cuando el conector y el sistema Cloud Volumes ONTAP estén implementados en un sitio oscuro (en el «modo privado»).

Además, necesita tener una suscripción a Microsoft Azure para el espacio de almacenamiento en el que se ubicará los backups.

## Prepare el conector BlueXP

El conector se puede instalar en una región de Azure con acceso a Internet completo o limitado (modo "estándar" o "restringido"). ["Consulta los modos de puesta en marcha de BlueXP para obtener más información"](#).

- ["Más información sobre conectores"](#)
- ["Implementar un conector en Azure en modo estándar \(acceso completo a Internet\)"](#)
- ["Instale el conector en modo restringido \(acceso saliente limitado\)"](#)

## Verifique o agregue permisos al conector

Para utilizar la funcionalidad de búsqueda y restauración de backup y recuperación de BlueXP, necesita contar con permisos específicos en la función de Connector para que pueda acceder a Azure Synapse Workspace y a la cuenta de almacenamiento de lago de datos. Consulte los siguientes permisos y siga los pasos si necesita modificar la directiva.

### Antes de empezar

- Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") en su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#). Debe ser Subscription **Owner** o **Contributor** para registrar el proveedor de recursos.
- El puerto 1433 debe estar abierto para la comunicación entre Connector y los servicios SQL de Azure Synapse.

### Pasos

1. Identifique la función asignada a la máquina virtual conector:
  - a. En el portal de Azure, abra el servicio de máquinas virtuales.
  - b. Seleccione la máquina virtual conector.
  - c. En Configuración, seleccione **identidad**.
  - d. Seleccione **Asignaciones de roles de Azure**.
  - e. Anote la función personalizada asignada a la máquina virtual conector.
2. Actualice el rol personalizado:
  - a. En el portal de Azure, abra su suscripción a Azure.
  - b. Selecciona **Control de acceso (IAM) > Roles**.
  - c. Seleccione los puntos suspensivos (...) para el rol personalizado y luego seleccione **Editar**.
  - d. Seleccione **JSON** y agregue los siguientes permisos:

```

"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"

```

"Vea el formato JSON completo para la política"

e. Haga clic en **revisar + actualizar** y, a continuación, haga clic en **Actualizar**.

## Información requerida para usar claves gestionadas por el cliente para el cifrado de datos

Puede utilizar sus propias claves gestionadas por el cliente para el cifrado de datos en el asistente de activación en lugar de utilizar las claves de cifrado gestionadas por Microsoft predeterminadas. En este caso, deberá tener la suscripción de Azure, el nombre del almacén de claves y la clave. "[Vea cómo usar sus propias claves](#)".

El backup y la recuperación de BlueXP admite *Azure access policies*, el modelo de permisos *Azure role-based access control* (Azure RBAC) y *Managed Hardware Security Model* (HSM) (consulte "[¿Qué es el HSM gestionado por Azure Key Vault?](#)").

## Cree su cuenta de almacenamiento de Azure Blob

De forma predeterminada, el servicio crea cuentas de almacenamiento para usted. Si desea utilizar sus propias cuentas de almacenamiento, puede crearlas antes de iniciar el asistente de activación de copia de seguridad y, a continuación, seleccionar esas cuentas de almacenamiento en el asistente.

["Obtenga más información sobre la creación de sus propias cuentas de almacenamiento"](#).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. "[Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP](#)".

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predeterminado.
- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en subredes diferentes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).

## Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP

Habilitar el backup y la recuperación de datos de BlueXP es muy sencillo. Los pasos difieren ligeramente dependiendo de si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

### Habilitar la copia de seguridad y recuperación de BlueXP en un nuevo sistema

El backup y la recuperación de BlueXP están habilitados de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.

Consulte "[Inicio de Cloud Volumes ONTAP en Azure](#)" Para conocer los requisitos y detalles de cómo crear el sistema Cloud Volumes ONTAP.



Si quieres elegir el nombre del grupo de recursos, **deshabilita** el backup y la recuperación de BlueXP al implementar Cloud Volumes ONTAP. Siga los pasos de [Habilitar el backup y la recuperación de datos de BlueXP en un sistema existente](#) Para habilitar el backup y la recuperación de BlueXP, y, a continuación, elegir el grupo de recursos.

## Pasos

1. En BlueXP Canvas, selecciona **Agregar entorno de trabajo**, elige el proveedor de la nube y selecciona **Agregar nuevo**. Selecciona **Crear Cloud Volumes ONTAP**.
2. Seleccione **Microsoft Azure** como proveedor de la nube y luego elija un solo nodo o sistema de alta disponibilidad.
3. En la página define Azure Credentials, introduzca el nombre de las credenciales, el ID de cliente, el secreto de cliente y el ID de directorio. A continuación, haga clic en **Continue**.
4. Rellene la página Detalles y credenciales y asegúrese de que la suscripción a Azure Marketplace esté en su sitio y haga clic en **continuar**.
5. En la página Servicios, deje el servicio activado y haga clic en **continuar**.



6. Complete las páginas del asistente para implementar el sistema.

## Resultado

El backup y la recuperación de datos de BlueXP están activados en el sistema. Después de crear volúmenes en estos sistemas Cloud Volumes ONTAP, inicie el backup y la recuperación de datos de BlueXP y. "[active el backup en cada volumen que desee proteger](#)".

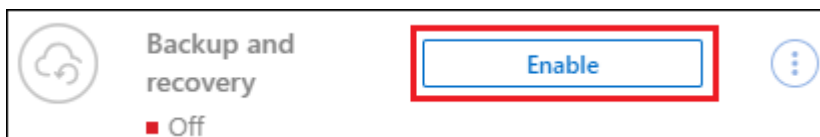
## Habilitar la copia de seguridad y recuperación de BlueXP en un sistema existente

Habilita el backup y la recuperación de BlueXP en cualquier momento directamente desde el entorno de trabajo.

## Pasos

1. En BlueXP Canvas, selecciona el entorno de trabajo y selecciona **Habilitar** junto al servicio de copia de seguridad y recuperación en el panel derecho.

Si el destino de Azure Blob para sus backups existe como un entorno de trabajo en el lienzo, puede arrastrar el clúster al entorno de trabajo de Azure Blob para iniciar el asistente de configuración.



2. Completa las páginas del asistente para implementar el backup y la recuperación de datos de BlueXP.
3. Cuando desee iniciar backups, continúe con [Active backups en sus ONTAP Volumes](#).

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.



Si el destino de Azure para sus backups existe como entorno de trabajo en Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de Azure Blob.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, selecciona las **Acciones** ... Y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:
  - Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
  - Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

### Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los

siguientes: Política de Snapshot, política de replicación, política de backup en objeto.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el backup para volúmenes adicionales en el entorno de trabajo"](#) (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.
  - Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
  - Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes. (Los volúmenes de FlexGroup se pueden seleccionar de uno a la vez). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título.  
).
  - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen ( Volume\_1).

2. Seleccione **Siguiente**.

## Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.

- **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.

2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:

- **Cascading:** La información fluye del sistema de almacenamiento primario al secundario, y del almacenamiento secundario al objeto.
- **Fan Out:** La información fluye del sistema de almacenamiento primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una.



Para crear una política personalizada antes de activar la instantánea, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

4. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del volumen replicado.
- **Política de replicación:** Elija una política de replicación existente o cree una.



Para crear una política personalizada antes de activar la replicación, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Microsoft Azure**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor.

Introduzca la región en la que se almacenarán las copias de seguridad. Esta puede ser una región diferente a la ubicación en la que reside el sistema Cloud Volumes ONTAP.

Cree una nueva cuenta de almacenamiento o seleccione una existente.

Introduzca la suscripción de Azure utilizada para almacenar los backups. Esta suscripción puede ser diferente a la ubicación en la que reside el sistema Cloud Volumes ONTAP. Si desea utilizar una suscripción de Azure diferente para sus backups, debe hacerlo ["Inicie sesión en el portal de Azure y vincule las dos suscripciones"](#).



Cree su propio grupo de recursos que gestione el contenedor Blob o seleccione el tipo y el grupo de recursos.



Si desea proteger los archivos de copia de seguridad para evitar que se modifiquen o eliminen, asegúrese de que la cuenta de almacenamiento se haya creado con almacenamiento inmutable habilitado mediante un período de retención de 30 días.



Si desea organizar en niveles archivos de copia de seguridad antiguos en Azure Archive Storage para obtener una mayor optimización de los costes, asegúrese de que la cuenta de almacenamiento tenga la regla de ciclo de vida adecuada.

- **Clave de cifrado:** Si creó una nueva cuenta de almacenamiento de Azure, ingrese la información de clave de cifrado que le dio el proveedor. Elija si utilizará las claves de cifrado predeterminadas de Azure o elija sus propias claves gestionadas por el cliente de su cuenta de Azure para administrar el cifrado de sus datos.

Si decide utilizar sus propias claves gestionadas por el cliente, introduzca el almacén de claves y la información de clave. "[Aprende a usar tus propias claves](#)".



Si eligió una cuenta de almacenamiento de Microsoft existente, la información de cifrado ya está disponible, por lo que no necesita ingresarla ahora.

- **Redes:** Elige el espacio IP y si vas a usar un Punto Final Privado. El punto final privado está desactivado de forma predeterminada.
  - i. El espacio IP del clúster de ONTAP en el que residen los volúmenes de los que desea realizar backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.
  - ii. Opcionalmente, seleccione si utilizará un punto final privado de Azure que haya configurado previamente. "[Obtenga más información sobre el uso de un extremo privado de Azure](#)".
- **Política de copia de seguridad:** Seleccione una política de almacenamiento de copia de seguridad a objeto existente.



Para crear una política personalizada antes de activar el backup, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte "[Configuración de políticas de backup en objeto](#)".
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen primario.

Se crea un contenedor de almacenamiento Blob en el grupo de recursos introducido, y los archivos de backup se almacenan allí.

De forma predeterminada, el backup y la recuperación de BlueXP aprovisiona el Blob Container con redundancia local (LRS) para la optimización de costes. Puede cambiar esta configuración a redundancia de zona (ZRS) si desea asegurarse de que los datos se replican entre zonas diferentes. Consulte las instrucciones de Microsoft para ["cambiar el modo de replicar la cuenta de almacenamiento"](#).

La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

## Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

## El futuro

- Puede hacerlo ["gestione los archivos de copia de seguridad y las políticas de copia de seguridad"](#). Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo ["gestione la configuración de backup en el nivel del clúster"](#). Esto incluye cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo ["restaure volúmenes, carpetas o archivos individuales desde un archivo de backup"](#) A un sistema Cloud Volumes ONTAP en Azure o a un sistema ONTAP en las instalaciones.

# Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con la copia de seguridad y recuperación de BlueXP

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en Google Cloud Storage.

## Inicio rápido

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

1

### Verifique la compatibilidad con la configuración

- Está ejecutando Cloud Volumes ONTAP 9,8 o posterior en GCP (se recomienda ONTAP 9.8P13 y versiones posteriores).
- Tiene una suscripción válida para GCP para el espacio de almacenamiento donde se ubicará la copia de seguridad.
- Tienes una cuenta de servicio en tu proyecto de Google Cloud que tiene un rol personalizado con un conjunto reducido de permisos.



El rol Storage Admin ya no es necesario para la cuenta de servicio que permite acceder al backup y la recuperación de datos de BlueXP para acceder a los buckets de almacenamiento de Google Cloud.

- Se ha suscrito a "[Oferta de backup de BlueXP Marketplace](#)", o usted ha comprado "[y activado](#)" Una licencia BYOL de backup y recuperación de BlueXP de NetApp.

2

### Prepare el conector BlueXP

Si ya tienes un conector implementado en una región de GCP, entonces estás todo listo. De lo contrario, tendrás que instalar un conector BlueXP en GCP para realizar backups de los datos de Cloud Volumes ONTAP en Google Cloud Storage. El Conector se puede instalar en un sitio con acceso completo a Internet ("modo estándar") o con conectividad a Internet limitada ("modo restringido").

3

### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencias tanto para Google Cloud como para BlueXP.

4

### Compruebe los requisitos de red de ONTAP para replicar volúmenes

Asegúrese de que los sistemas de origen y destino cumplen con los requisitos de red y versión de ONTAP.

5

### Habilita el backup y la recuperación de datos de BlueXP

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

6

### Prepare Google Cloud como destino de backup

Configura permisos para que Connector cree y administre el bucket de Google Cloud.

De manera opcional, puede configurar sus propias claves gestionadas personalizadas para el cifrado de datos en lugar de utilizar las claves de cifrado de Google Cloud predeterminadas. [Descubre cómo preparar tu entorno de Google Cloud para recibir backups de ONTAP.](#)

7

### Active backups en sus ONTAP Volumes

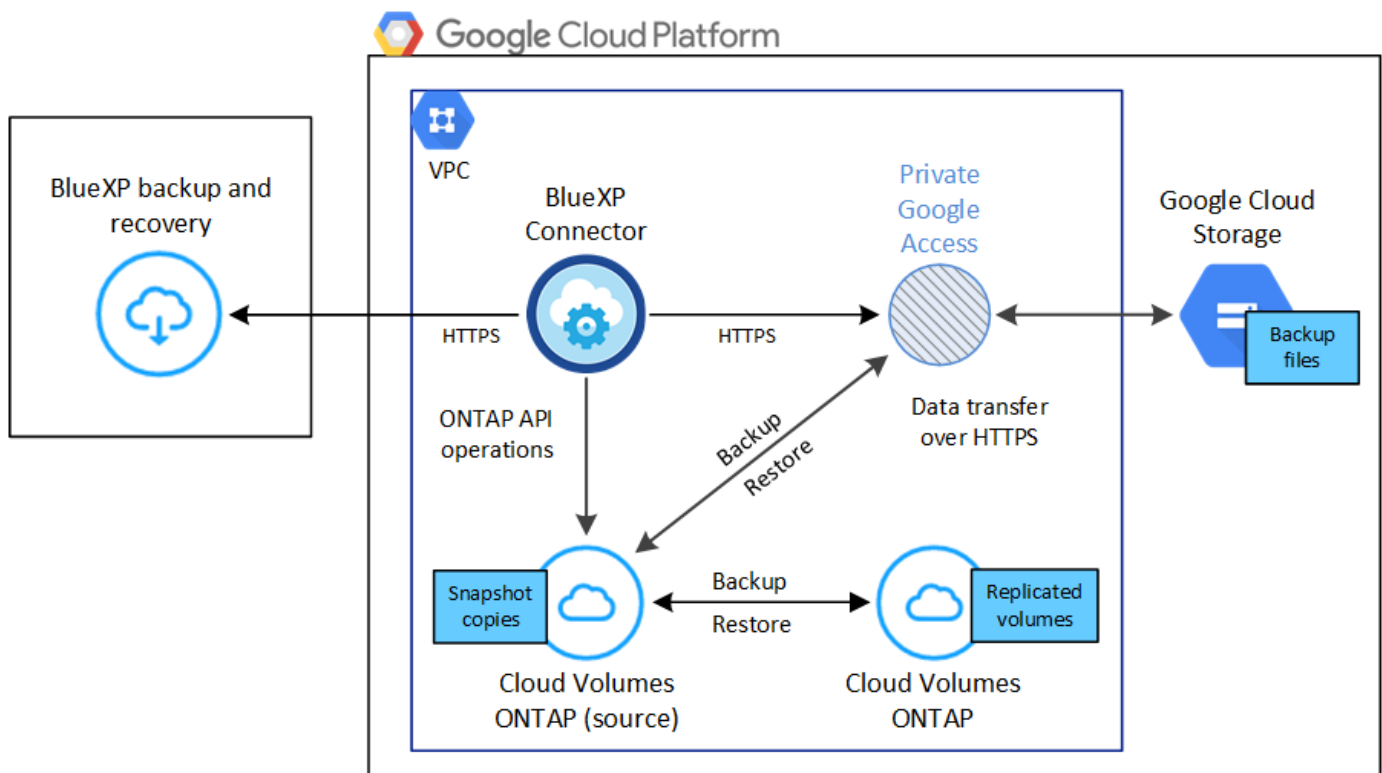
Siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

## Verifique la compatibilidad con la configuración

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de empezar a realizar backups de volúmenes en Google Cloud Storage.

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

Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.



### Versiones de ONTAP compatibles

Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.

## Regiones compatibles de GCP

La copia de seguridad y recuperación de BlueXP es compatible con todas las regiones de GCP.

## Cuenta de servicio de GCP

Necesitas tener una cuenta de servicio en tu proyecto de Google Cloud que tenga el rol personalizado.

["Aprenda a crear una cuenta de servicio"](#)



El rol Storage Admin ya no es necesario para la cuenta de servicio que permite acceder al backup y la recuperación de datos de BlueXP para acceder a los buckets de almacenamiento de Google Cloud.

## Verifique los requisitos de licencia

Para obtener la licencia PAYGO de backup y recuperación de BlueXP, hay una suscripción de BlueXP disponible en Google Marketplace que permite la implementación de backup y recuperación de datos de Cloud Volumes ONTAP y BlueXP. Necesita hacerlo ["suscríbase a esta suscripción a BlueXP"](#) Antes de habilitar el backup y la recuperación de datos de BlueXP. La facturación para el backup y la recuperación de BlueXP se realiza a través de esta suscripción. ["Puede suscribirse desde la página Detalles Credentials del asistente de entorno de trabajo"](#).

Para la licencia BYOL de backup y recuperación de BlueXP, necesita el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).

Además, necesita una suscripción de Google para el espacio de almacenamiento en el que se localizarán los backups.

## Prepare el conector BlueXP

El conector debe estar instalado en una región de Google con acceso a Internet.

- ["Más información sobre conectores"](#)
- ["Ponga en marcha un conector en Google Cloud"](#)

## Verifique o agregue permisos al conector

Para utilizar la funcionalidad de «búsqueda y restauración» de backup y recuperación de BlueXP, necesitas contar con permisos específicos en la función del conector para que pueda acceder al servicio de Google Cloud BigQuery. Consulte los siguientes permisos y siga los pasos si necesita modificar la directiva.

### Pasos

1. En la ["Consola de Google Cloud"](#), Vaya a la página **roles**.
2. Mediante la lista desplegable situada en la parte superior de la página, seleccione el proyecto o la organización que contiene la función que desea editar.
3. Seleccione un rol personalizado.
4. Seleccione **Editar rol** para actualizar los permisos del rol.
5. Seleccione **Agregar permisos** para agregar los siguientes permisos nuevos al rol.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Selecciona **Actualizar** para guardar el rol editado.

### Información necesaria para el uso de claves de cifrado gestionadas por el cliente (CMEK)

Puede utilizar sus propias claves gestionadas por el cliente para el cifrado de datos en lugar de utilizar las claves de cifrado predeterminadas gestionadas por Google. Se admiten tanto claves entre regiones como entre proyectos, por lo que puede elegir un proyecto para un depósito que sea diferente al proyecto de la clave CMEK. Si planea utilizar sus propias claves gestionadas por el cliente:

- Necesitará tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado gestionadas por el cliente"](#).
- Deberá verificar que estos permisos necesarios se incluyan en la función del conector:

```
cloudkms.cryptoKeys.get  
cloudkms.cryptoKeys.getIamPolicy  
cloudkms.cryptoKeys.list  
cloudkms.cryptoKeys.setIamPolicy  
cloudkms.keyRings.get  
cloudkms.keyRings.getIamPolicy  
cloudkms.keyRings.list  
cloudkms.keyRings.setIamPolicy
```

- Deberás verificar que la API de Google "Cloud Key Management Service (KMS)" esté habilitada en tu proyecto. Consulte ["Documentación de Google Cloud: Habilitar API"](#) para obtener más detalles.

### Consideraciones de CMEK:

- Se admiten tanto las claves generadas por software como las de HSM (respaldadas por hardware).
- Se admiten las claves de Cloud KMS creadas o importadas recientemente.
- Sólo se admiten claves regionales; las claves globales no son compatibles.
- Actualmente, sólo se admite el propósito "cifrado/descifrado simétrico".
- Al agente de servicios asociado con la cuenta de almacenamiento se le asigna el rol IAM «CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)» mediante el backup y la recuperación de datos de BlueXP.

## Crea tus propios cubos

De forma predeterminada, el servicio crea buckets para usted. Si desea utilizar sus propios depósitos, puede crearlos antes de iniciar el asistente de activación de copias de seguridad y, a continuación, seleccionar esos depósitos en el asistente.

["Obtenga más información sobre cómo crear sus propios cubos"](#).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.
- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en subredes diferentes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).

## Habilita el backup y la recuperación de datos de BlueXP en Cloud Volumes ONTAP

Habilitar el backup y la recuperación de datos de BlueXP es muy sencillo. Los pasos difieren ligeramente dependiendo de si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

### Habilitar la copia de seguridad y recuperación de BlueXP en un nuevo sistema

El backup y la recuperación de BlueXP se pueden habilitar cuando completas el asistente del entorno de trabajo para crear un nuevo sistema Cloud Volumes ONTAP.

Debe tener una cuenta de servicio configurada. Si no selecciona ninguna cuenta de servicio al crear el sistema Cloud Volumes ONTAP, tendrá que apagar el sistema y agregar la cuenta de servicio a Cloud Volumes ONTAP desde la consola de GCP.

Consulte ["Lanzamiento de Cloud Volumes ONTAP en GCP"](#) Para conocer los requisitos y detalles de cómo crear el sistema Cloud Volumes ONTAP.

### Pasos

1. En BlueXP Canvas, selecciona **Agregar entorno de trabajo**, elige el proveedor de la nube y selecciona **Agregar nuevo**. Selecciona **Crear Cloud Volumes ONTAP**.

2. **Elija una ubicación:** Seleccione **Google Cloud Platform**.
3. **elegir Tipo:** Seleccione **Cloud Volumes ONTAP** (ya sea de un solo nodo o de alta disponibilidad).
4. **Detalles y credenciales:** Introduzca la siguiente información:
  - a. Haga clic en **Editar proyecto** y seleccione un proyecto nuevo si el que desea utilizar es diferente del proyecto predeterminado (donde reside el conector).
  - b. Especifique el nombre del clúster.
  - c. Active el conmutador **cuenta de servicio** y seleccione la cuenta de servicio que tenga la función predefinida Administrador de almacenamiento. Esto es necesario para habilitar los backups y la organización en niveles.
  - d. Especifique las credenciales.

Asegúrese de que existe una suscripción a GCP Marketplace.

Details & Credenciales

Project1  
Google Cloud Project

MPAWSSubscription1222  
Marketplace Subscription

Edit Project

**Details**

Working Environment Name (Cluster Name)

TamiVSA

Service Account ⓘ ☒

Service Account Name

ServiceAccount1

+ Add Labels Optional Field | Up to four labels

**Credenciales**

User Name

admin

Password

\*\*\*\*\*

Confirm Password

\*\*\*\*\*

5. **Servicios:** Deja habilitado el servicio de copia de seguridad y recuperación de BlueXP y haz clic en **Continuar**.

Services

 Backup to Cloud ☒ ▼

6. Complete las páginas del asistente para implementar el sistema como se describe en "[Lanzamiento de Cloud Volumes ONTAP en GCP](#)".





Para modificar la configuración de copia de seguridad o agregar replicación, consulte ["Gestión de backups de ONTAP"](#).

## Resultado

El backup y la recuperación de datos de BlueXP están activados en el sistema. Después de crear volúmenes en estos sistemas Cloud Volumes ONTAP, inicie el backup y la recuperación de datos de BlueXP y ["active el backup en cada volumen que desee proteger"](#).

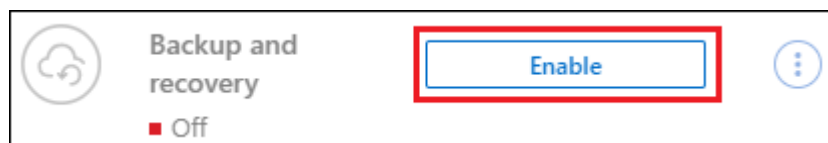
## Habilitar la copia de seguridad y recuperación de BlueXP en un sistema existente

Puedes habilitar el backup y la recuperación de datos de BlueXP en cualquier momento directamente desde el entorno de trabajo.

## Pasos

1. En BlueXP Canvas, selecciona el entorno de trabajo y selecciona **Habilitar** junto al servicio de copia de seguridad y recuperación en el panel derecho.

Si el destino de Google Cloud Storage para sus copias de seguridad existe como un entorno de trabajo en el lienzo, puede arrastrar el clúster al entorno de trabajo de Google Cloud Storage para iniciar el asistente de configuración.



Para modificar la configuración de copia de seguridad o agregar replicación, consulte ["Gestión de backups de ONTAP"](#).

## Preparar Google Cloud Storage como destino de backup

Preparar Google Cloud Storage como destino de copia de seguridad implica los siguientes pasos:

- Configure los permisos.
- (Opcional) Cree sus propios buckets. (El servicio creará cubos para usted si lo desea.)
- (Opcional) Configurar claves gestionadas por el cliente para el cifrado de los datos

## Configure los permisos

Debe proporcionar claves de acceso de almacenamiento para una cuenta de servicio que tenga permisos específicos mediante un rol personalizado. Una cuenta de servicio permite el backup y la recuperación de datos de BlueXP para autenticar y acceder a los depósitos de Cloud Storage que se usan para almacenar backups. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

## Pasos

1. En la ["Consola de Google Cloud"](#), Vaya a la página **roles**.
2. ["Crear un rol nuevo"](#) con los siguientes permisos:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. En la consola de Google Cloud, "[Vaya a la página de cuentas de servicio](#)".
4. Seleccione su proyecto de cloud.
5. Seleccione **Crear cuenta de servicio** y proporcione la información requerida:
  - a. **Detalles de la cuenta de servicio:** Introduzca un nombre y una descripción.
  - b. **Conceder acceso a esta cuenta de servicio al proyecto:** Seleccione la función personalizada que acaba de crear.
  - c. Seleccione **Listo**.
6. Vaya a. "[Configuración de almacenamiento para GCP](#)" y crear claves de acceso para la cuenta de servicio:
  - a. Seleccione un proyecto y seleccione **Interoperabilidad**. Si aún no lo ha hecho, seleccione **Habilitar acceso a interoperabilidad**.
  - b. En **Claves de acceso para cuentas de servicio**, selecciona **Crear una clave para una cuenta de servicio**, selecciona la cuenta de servicio que acabas de crear y haz clic en **Crear clave**.

Tendrá que introducir las claves en el backup y la recuperación de BlueXP más adelante cuando configure el servicio de backup.

## Crea tus propios cubos

De forma predeterminada, el servicio crea buckets para usted. O bien, si desea utilizar sus propios depósitos, puede crearlos antes de iniciar el asistente de activación de copias de seguridad y, a continuación, seleccionar esos bloques en el asistente.

["Obtenga más información sobre cómo crear sus propios cubos"](#).

## Configurar claves de cifrado gestionadas por el cliente (CMEK) para el cifrado de datos

Puede utilizar sus propias claves gestionadas por el cliente para el cifrado de datos en lugar de utilizar las claves de cifrado predeterminadas gestionadas por Google. Se admiten tanto claves entre regiones como entre proyectos, por lo que puede elegir un proyecto para un depósito que sea diferente al proyecto de la clave CMEK.

Si planea utilizar sus propias claves gestionadas por el cliente:

- Necesitará tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado gestionadas por el cliente"](#).
- Deberá verificar que estos permisos necesarios se incluyan en la función del conector:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Deberás verificar que la API de Google "Cloud Key Management Service (KMS)" esté habilitada en tu proyecto. Consulte ["Documentación de Google Cloud: Habilitar API"](#) para obtener más detalles.

### Consideraciones de CMEK:

- Se admiten tanto las claves generadas por software como las de HSM (respaldado por hardware).
- Se admiten las claves de Cloud KMS creadas o importadas recientemente.
- Solo se admiten claves regionales; las claves globales no son compatibles.
- Actualmente, sólo se admite el propósito "cifrado/descifrado simétrico".
- Al agente de servicios asociado con la cuenta de almacenamiento se le asigna el rol IAM «CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)» mediante el backup y la recuperación de datos de BlueXP.

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

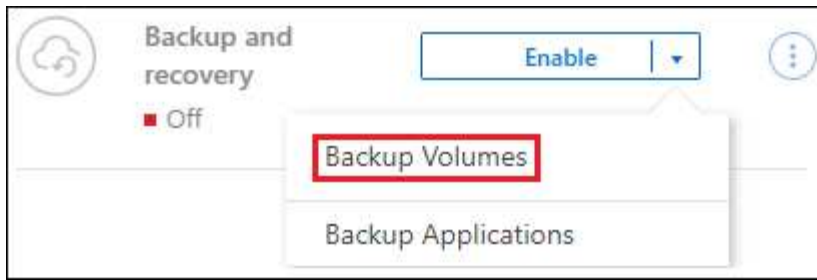
- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.



Si el destino de GCP para sus backups existe como entorno de trabajo en Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de GCP.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, seleccione las **Acciones** ... Y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:

- Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
- Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

### Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo "[active el backup para volúmenes adicionales en el entorno de trabajo](#)" (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

### Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.

- Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
- Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
- Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).

## 2. Seleccione **Siguiente**.

### Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

### Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye del sistema de almacenamiento primario al secundario, y del almacenamiento secundario al objeto.
  - **Fan Out:** La información fluye del sistema de almacenamiento primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte "[Planifica tu proceso de protección](#)".

3. **Instantánea local:** Elija una política de Snapshot existente o cree una.



Para crear una política personalizada antes de activar el backup, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
  - Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
  - Seleccione **Crear**.
4. **Replicación:** Establezca las siguientes opciones:
    - **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del

volumen replicado.

- **Política de replicación:** Elija una política de replicación existente o cree una.



Para crear una política personalizada antes de activar la replicación, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Google Cloud**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor y la región donde se almacenarán las copias de seguridad.

Cree un nuevo depósito o seleccione uno existente.

- **Clave de cifrado:** Si creaste un nuevo cubo de Google, ingresa la información de la clave de cifrado que se te haya proporcionado del proveedor. Elige si usarás las claves de cifrado predeterminadas de Google Cloud o si elegirás tus propias claves gestionadas por el cliente en tu cuenta de Google para gestionar el cifrado de tus datos.

Si decide utilizar sus propias claves gestionadas por el cliente, introduzca el almacén de claves y la información de clave.



Si elegiste un depósito de Google Cloud existente, la información de cifrado ya está disponible, por lo que no necesitas introducirla ahora.

- **Política de copia de seguridad:** Selecciona una política de almacenamiento de copia de seguridad a objeto existente o cree una.



Para crear una política personalizada antes de activar el backup, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen del sistema de almacenamiento principal.

Se crea un depósito de Google Cloud Storage en la cuenta de servicio indicada por la clave de acceso de Google y la clave secreta que ha introducido, y los archivos de copia de seguridad se almacenan allí.

Las copias de seguridad se asocian de forma predeterminada con la clase de almacenamiento *Standard*. Puede utilizar las clases de almacenamiento de bajo coste *Nearline*, *Coldline* o *Archive*. Sin embargo, configuras la clase de almacenamiento con Google, no con la interfaz de usuario de backup y recuperación de BlueXP. Consulte el tema de Google ["Cambiar la clase de almacenamiento predeterminada de un bloque"](#) para obtener más detalles.

La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

## Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

## El futuro

- Puede hacerlo ["gestione los archivos de copia de seguridad y las políticas de copia de seguridad"](#). Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo ["gestione la configuración de backup en el nivel del clúster"](#). Esto incluye cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.

- También puede hacerlo ["restaure volúmenes, carpetas o archivos individuales desde un archivo de backup"](#) A un sistema Cloud Volumes ONTAP en Google o a un sistema ONTAP en las instalaciones.

## Realice una copia de seguridad de los datos locales de ONTAP en Amazon S3 con la copia de seguridad y recuperación de BlueXP

Complete unos pocos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP locales a un sistema de almacenamiento secundario y al almacenamiento en la nube de Amazon S3.



Entre los «sistemas ONTAP en las instalaciones» se incluyen los sistemas FAS, AFF y ONTAP Select.

### Inicio rápido

Comience rápidamente siguiendo estos pasos. En las siguientes secciones del tema se proporcionan detalles sobre cada paso.

1

#### Identifica el método de conexión que usará

Elija si va a conectar su clúster de ONTAP en las instalaciones directamente a AWS S3 a través de una Internet pública, o si va a usar una VPN o AWS Direct Connect y enrutar el tráfico a través de una interfaz privada de VPC Endpoint a AWS S3.

[Identifique el método de conexión.](#)

2

#### Prepare el conector BlueXP

Si ya tiene un conector puesto en marcha en AWS VPC o en sus instalaciones, todo estará configurado. De lo contrario, deberá crear un conector BlueXP para realizar backups de los datos de ONTAP en almacenamiento AWS S3. También deberá personalizar los ajustes de red del conector para que pueda conectarse a AWS S3.

[Aprenda a crear un conector y a definir la configuración de red necesaria.](#)

3

#### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencias tanto para AWS como para BlueXP.

Consulte [Verifique los requisitos de licencia.](#)

4

#### Prepare los clústeres ONTAP

Detecte sus clústeres de ONTAP en BlueXP, compruebe que los clústeres cumplan con los requisitos mínimos y personalice la configuración de red para que los clústeres se puedan conectar a AWS S3.



## 5

### Prepare Amazon S3 como destino de backup

Configurar permisos para que Connector cree y gestione el bloque de S3. También tendrá que configurar permisos para el clúster de ONTAP en las instalaciones para que pueda leer y escribir datos en el bloque de S3.

De manera opcional, puede configurar sus propias claves gestionadas a medida para el cifrado de datos en lugar de utilizar las claves de cifrado predeterminadas de Amazon S3. [Descubre cómo preparar tu entorno de AWS S3 para recibir backups de ONTAP.](#)

## 6

### Active backups en sus ONTAP Volumes

Seleccione el entorno de trabajo y haga clic en **Activar > copia de seguridad de volúmenes** junto al servicio copia de seguridad y recuperación del panel derecho. A continuación, siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

[Active backups en sus ONTAP Volumes.](#)

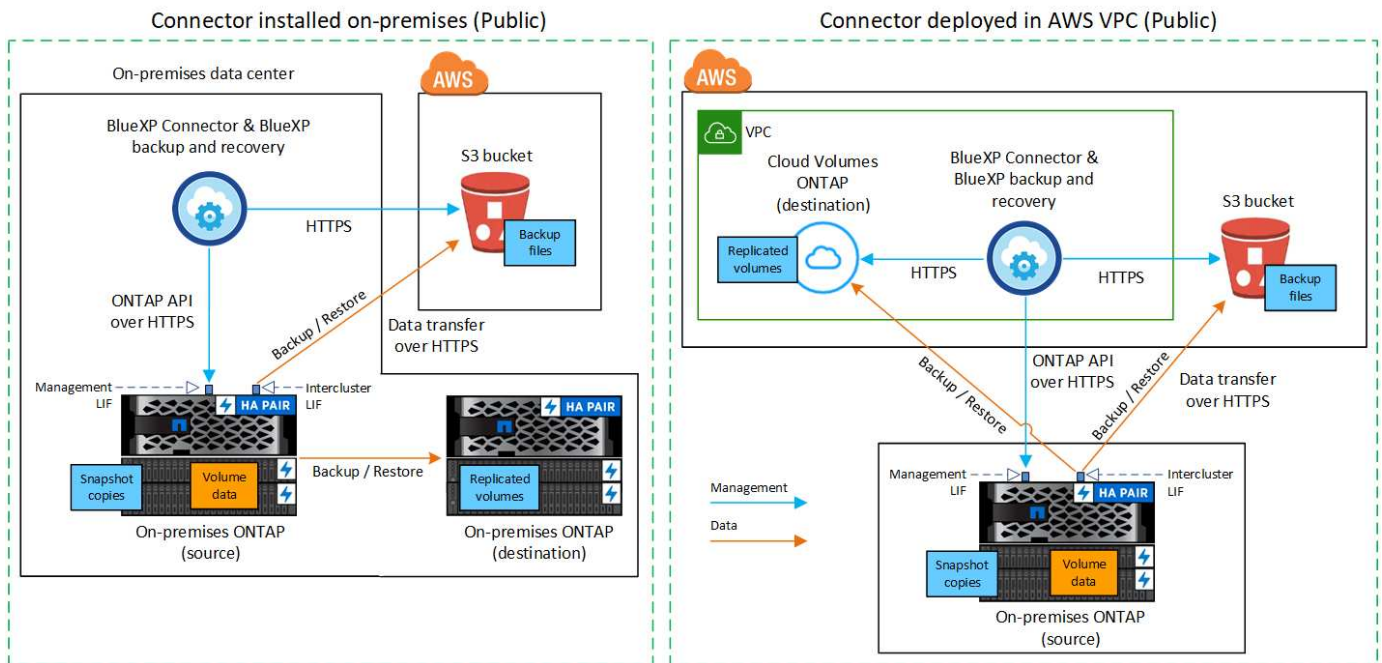
## Identifique el método de conexión

Elija cuáles de los dos métodos de conexión utilizará al configurar backups de sistemas ONTAP locales en AWS S3.

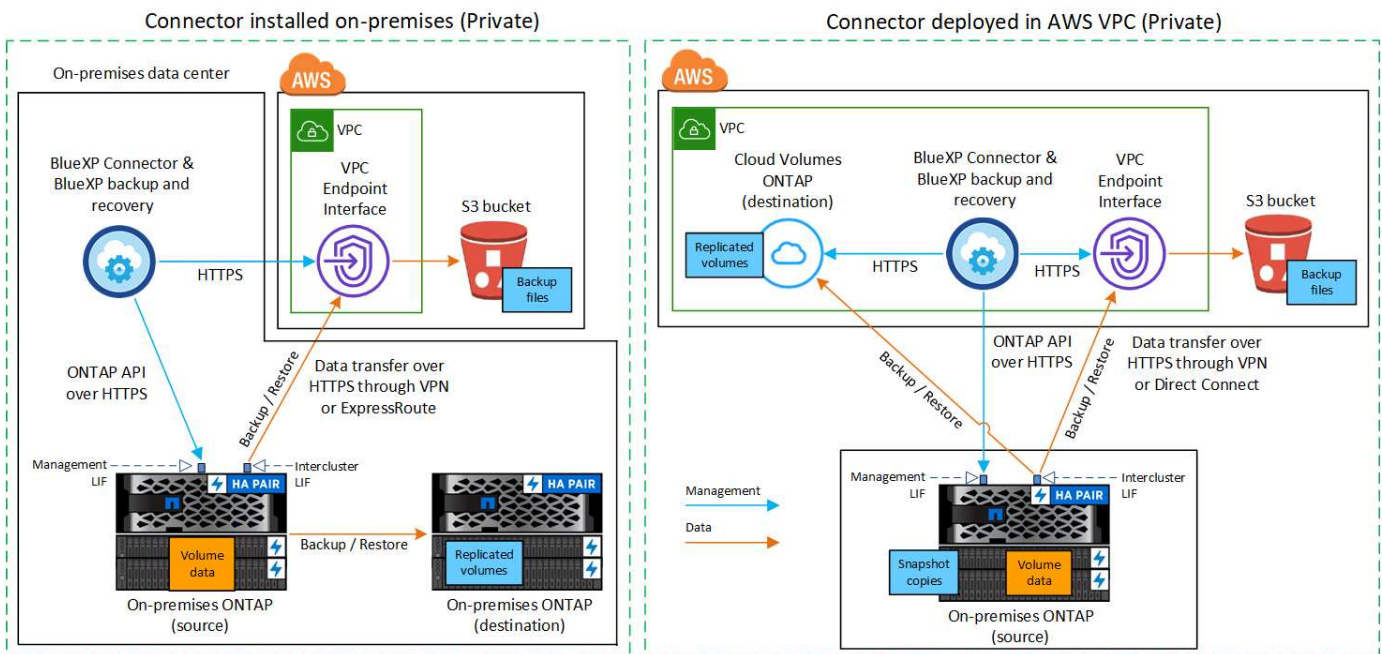
- **Conexión pública** - Conecte directamente el sistema ONTAP a AWS S3 utilizando un punto final S3 público.
- **Conexión privada:** Utilice una VPN o AWS Direct Connect y enrute el tráfico a través de una interfaz de punto final de VPC que utilice una dirección IP privada.

Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.

El siguiente diagrama muestra el método **de conexión pública** y las conexiones que necesita preparar entre los componentes. Puede usar un conector que haya instalado en sus instalaciones o un conector que haya implementado en el VPC de AWS.



El siguiente diagrama muestra el método **de conexión privada** y las conexiones que necesita preparar entre los componentes. Puede usar un conector que haya instalado en sus instalaciones o un conector que haya implementado en el VPC de AWS.



## Prepare el conector BlueXP

El conector BlueXP es el software principal para la funcionalidad BlueXP. Se necesita un conector para realizar una copia de seguridad y restaurar los datos de ONTAP.

### Cree o cambie conectores

Si ya tiene un conector puesto en marcha en AWS VPC o en sus instalaciones, todo estará configurado.

Si no es así, deberá crear un conector en una de esas ubicaciones para realizar backups de los datos de ONTAP en almacenamiento AWS S3. No puede utilizar un conector puesto en marcha en otro proveedor de cloud.

- ["Más información sobre conectores"](#)
- ["Instale un conector en AWS"](#)
- ["Instale un conector en sus instalaciones"](#)
- ["Instale un conector en una región de AWS GovCloud"](#)

El backup y la recuperación de BlueXP son compatibles con las regiones de GovCloud cuando Connector se implementa en la nube, no cuando se instala en tus instalaciones. Además, debe poner en marcha el conector desde AWS Marketplace. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

## Prepare los requisitos de red del conector

Asegúrese de que se cumplen los siguientes requisitos de red:

- Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:
  - Una conexión HTTPS a través del puerto 443 al servicio de backup y recuperación de BlueXP y al almacenamiento de objetos S3 (["consulte la lista de extremos"](#))
  - Una conexión HTTPS a través del puerto 443 para la LIF de gestión del clúster ONTAP
  - Se requieren reglas adicionales de grupos de seguridad entrantes y salientes para las implementaciones de AWS GovCloud. Consulte ["Reglas para el conector en AWS"](#) para obtener más detalles.
- ["Asegúrese de que Connector tenga permisos para gestionar el bloque S3"](#).
- Si tiene una conexión de conexión directa o VPN desde el clúster de ONTAP al VPC y desea que la comunicación entre el conector y S3 permanezca en su red interna de AWS (una conexión **privada**), tendrá que habilitar una interfaz de extremo VPC a S3. [Consulte cómo configurar una interfaz de extremo VPC](#).

## Verifique los requisitos de licencia

Tendrás que verificar los requisitos de licencia para AWS y BlueXP:

- Antes de activar el backup y la recuperación de BlueXP para tu clúster, deberás suscribirte a una oferta de pago por uso (PAYGO) BlueXP Marketplace desde AWS, o comprar y activar una licencia BYOL de backup y recuperación de BlueXP desde NetApp. Estas licencias son para su cuenta y se pueden utilizar en varios sistemas.
  - Para las licencias PAYGO de backup y recuperación de BlueXP, necesitarás una suscripción al ["Oferta de NetApp BlueXP en AWS Marketplace"](#). La facturación para el backup y la recuperación de BlueXP se realiza a través de esta suscripción.
  - Para la licencia BYOL de backup y recuperación de BlueXP, necesitará el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).
- Necesita tener una suscripción a AWS para el espacio de almacenamiento de objetos donde se ubicará los backups.

## Regiones apoyadas

Puede crear copias de seguridad desde sistemas locales a Amazon S3 en todas las regiones, incluidas las regiones de AWS GovCloud. Especifique la región en la que se almacenarán las copias de seguridad al configurar el servicio.

## Prepare los clústeres ONTAP

Tendrá que preparar su sistema ONTAP de origen en las instalaciones y cualquier sistema ONTAP o Cloud Volumes ONTAP secundario en las instalaciones.

La preparación de los clústeres de ONTAP implica los siguientes pasos:

- Descubra tus sistemas de ONTAP en BlueXP
- Compruebe los requisitos del sistema ONTAP
- Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos
- Compruebe los requisitos de red de ONTAP para replicar volúmenes

### Descubre tus sistemas de ONTAP en BlueXP

Tanto su sistema ONTAP de origen en las instalaciones como todos los sistemas ONTAP o Cloud Volumes ONTAP secundarios en las instalaciones deben estar disponibles en BlueXP Canvas.

Tendrá que conocer la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster.

["Aprenda a detectar un clúster"](#).

### Compruebe los requisitos del sistema ONTAP

Asegúrese de que se cumplen los siguientes requisitos de ONTAP:

- Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.
- Una licencia de SnapMirror (incluida como parte del paquete Premium o del paquete de protección de datos).

**Nota:** El "paquete de nube híbrida" no es necesario cuando se utiliza la copia de seguridad y recuperación de BlueXP.

Aprenda cómo ["gestione las licencias de clúster"](#).

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["configure la hora del clúster"](#).
- Si va a replicar datos, debe comprobar que los sistemas de origen y de destino ejecutan versiones de ONTAP compatibles antes de replicar datos.

["Consulte versiones de ONTAP compatibles para relaciones de SnapMirror"](#).

### Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos

Debe configurar los siguientes requisitos en el sistema que se conecta al almacenamiento de objetos.

- Para una arquitectura de copia de seguridad ramificada, configure los siguientes ajustes en el sistema *primary*.

- Para una arquitectura de copia de seguridad en cascada, configure los siguientes ajustes en el sistema *secondary*.

Se necesitan los siguientes requisitos de red de clúster de ONTAP:

- El clúster requiere una conexión HTTPS de entrada desde el conector a la LIF de administración del clúster.
- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. Estas LIF de interconexión de clústeres deben poder acceder al almacén de objetos.

El clúster inicia una conexión HTTPS de salida a través del puerto 443 desde las LIF de interconexión de clústeres hasta el almacenamiento de Amazon S3 para las operaciones de backup y restauración. ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos no inicia nunca, solo responde.

- Las LIF entre clústeres deben estar asociadas al *IPspace* que ONTAP debería usar para conectarse al almacenamiento de objetos. ["Obtenga más información acerca de los espacios IP"](#).

Al configurar el backup y la recuperación de BlueXP, se le pedirá que utilice el espacio IP. Debe elegir el espacio IP al que están asociadas estas LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

Si utiliza un espacio IP diferente a la opción "predeterminada", es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.

Todas las LIF entre clústeres del espacio IP deben tener acceso al almacén de objetos. Si no puede configurar este espacio IP para el espacio IP actual, deberá crear un espacio IP dedicado en el que todas las LIF de interconexión de clústeres tengan acceso al almacén de objetos.

- Los servidores DNS deben haberse configurado para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Descubra cómo ["Configure los servicios DNS para la SVM"](#).
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones de backup y recuperación de BlueXP desde ONTAP al almacenamiento de objetos a través del puerto 443 y el tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).
- Si utiliza un extremo de interfaz VPC privado en AWS para la conexión de S3, para que se pueda usar HTTPS/443, deberá cargar el certificado de extremo S3 en el clúster de ONTAP. [Consulte cómo configurar una interfaz de extremo de VPC y cargar el certificado de S3](#).
- ["Compruebe que su clúster de ONTAP tenga permisos para acceder al bloque de S3"](#).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los

pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predeterminado.

## Prepare Amazon S3 como destino de backup

Preparar Amazon S3 como destino de copia de seguridad implica los siguientes pasos:

- Configure los permisos S3.
- (Opcional) Crea tus propios cubos de S3. (El servicio creará cubos para usted si lo desea.)
- (Opcional) Configurar claves AWS gestionadas por el cliente para el cifrado de datos.
- (Opcional) Configure el sistema para una conexión privada mediante una interfaz de punto final de VPC.

### Configure permisos de S3

Tendrá que configurar dos conjuntos de permisos:

- Permisos para que el conector cree y gestione el bloque de S3.
- Permisos para el clúster ONTAP en las instalaciones para que pueda leer y escribir datos en el bloque de S3.

### Pasos

1. Asegúrese de que el conector tiene los permisos necesarios. Para obtener más información, consulte ["Permisos de políticas de BlueXP"](#).



Cuando cree backups en regiones de AWS China, debe cambiar el nombre de recurso de AWS «arn» en todas las secciones *Resource* de las políticas de IAM de «aws» a «aws-cn», por ejemplo `arn:aws-cn:s3:::netapp-backup-*`.

2. Al activar el servicio, el Asistente de copia de seguridad le solicitará que introduzca una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda realizar backups y restaurar los datos en el bloque de S3. Para ello, deberá crear un usuario de IAM con los siguientes permisos.

Consulte la ["Documentación de AWS: Crear un rol para delegar permisos en un usuario de IAM"](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/**",
      "Effect": "Allow"
    }
  ]
}

```



## Crea tus propios cubos

De forma predeterminada, el servicio crea buckets para usted. O bien, si desea utilizar sus propios depósitos, puede crearlos antes de iniciar el asistente de activación de copias de seguridad y, a continuación, seleccionar esos bloques en el asistente.

["Obtenga más información sobre cómo crear sus propios cubos".](#)

Si creas tus propios buckets, debes usar el nombre de bucket de «netapp-backup». Si necesita utilizar un nombre personalizado, edite el `ontapcloud-instance-policy-netapp-backup` IAMRole para los CVO existentes y agregue la siguiente lista a los permisos S3. Usted necesita incluir "Resource": "arn:aws:s3:::\*" y asigne todos los permisos necesarios que se deben asociar al depósito.

```
«Acción»: [
«S3:ListBucket»
«S3:GetBucketLocation»
]
«Recurso»: «arn:aws:S3::*»,
"Efector": "Permitir"
},
{
«Acción»: [
«S3:GetObject»,
«S3:PutObject»,
«S3>DeleteObject»,
«S3:ListAllMyBuckets»,
«S3:PutObjectTagging»,
«S3:GetObjectTagging»,
«S3:RestoreObject»,
«S3:GetBucketObjectLockConfiguration»,
«S3:GetObjectRetention»,
«S3:PutBucketObjectLockConfiguration»,
«S3:PutObjectRetention»
]
«Recurso»: «arn:aws:S3::*»,
```

## Configure claves AWS gestionadas por el cliente para el cifrado de datos

Si desea utilizar las claves de cifrado predeterminadas de Amazon S3 para cifrar los datos que se transmiten entre su clúster local y el bloque de S3, entonces está todo establecido porque la instalación predeterminada utiliza ese tipo de cifrado.

Si, en cambio, quieres utilizar tus propias claves gestionadas por el cliente para el cifrado de datos en lugar de usar las claves predeterminadas, debes que las claves gestionadas de cifrado ya estén configuradas antes de iniciar el asistente de backup y recuperación de BlueXP.

["Consulta cómo usar tus propias claves de cifrado de Amazon con Cloud Volumes ONTAP".](#)

["Consulta cómo usar tus propias claves de cifrado de Amazon con la copia de seguridad y recuperación de BlueXP".](#)



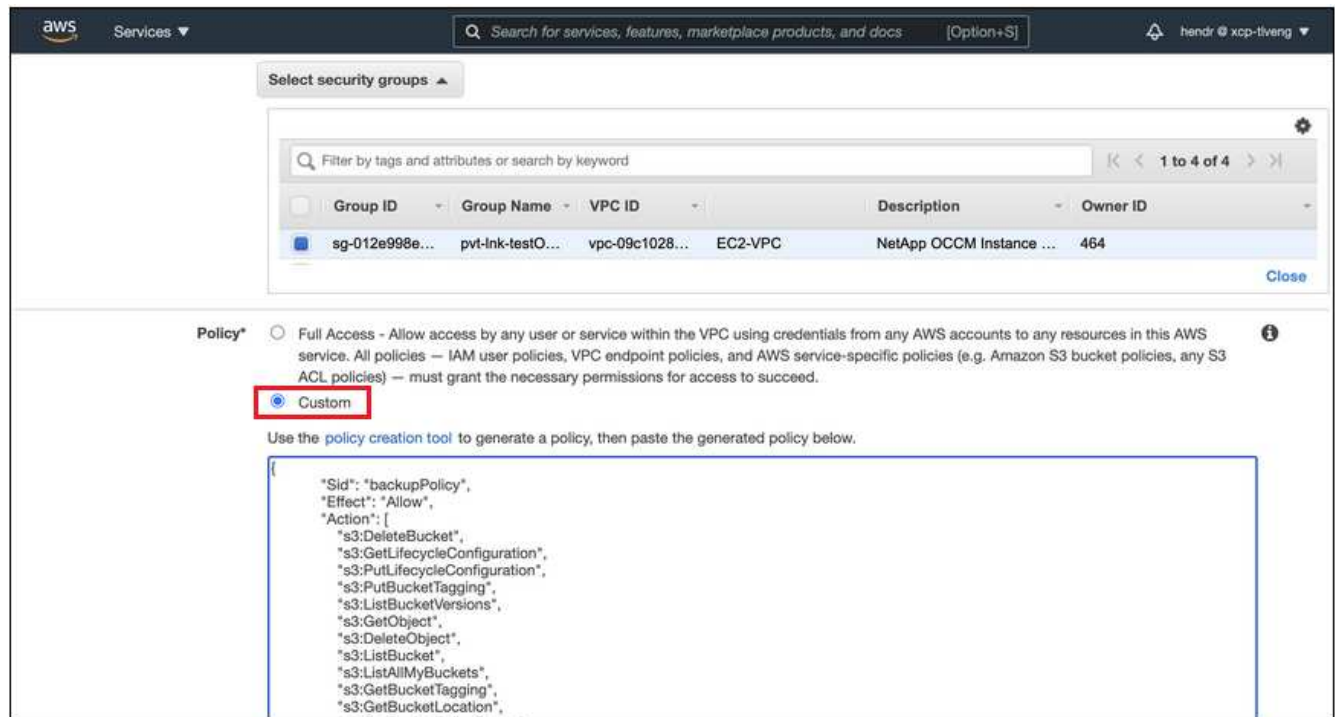
## Configure el sistema para una conexión privada mediante una interfaz de extremo VPC

Si desea utilizar una conexión a Internet pública estándar, el conector establece todos los permisos y no hay nada más que deba hacer. Este tipo de conexión se muestra en la "[primer diagrama](#)".

Si desea disponer de una conexión más segura a través de Internet desde el centro de datos en las instalaciones al VPC, hay una opción para seleccionar una conexión de AWS PrivateLink en el asistente de activación de copias de seguridad. Es necesario si planea utilizar una VPN o AWS Direct Connect para conectar su sistema local a través de una interfaz VPC Endpoint que utilice una dirección IP privada. Este tipo de conexión se muestra en la "[segundo diagrama](#)".

### Pasos

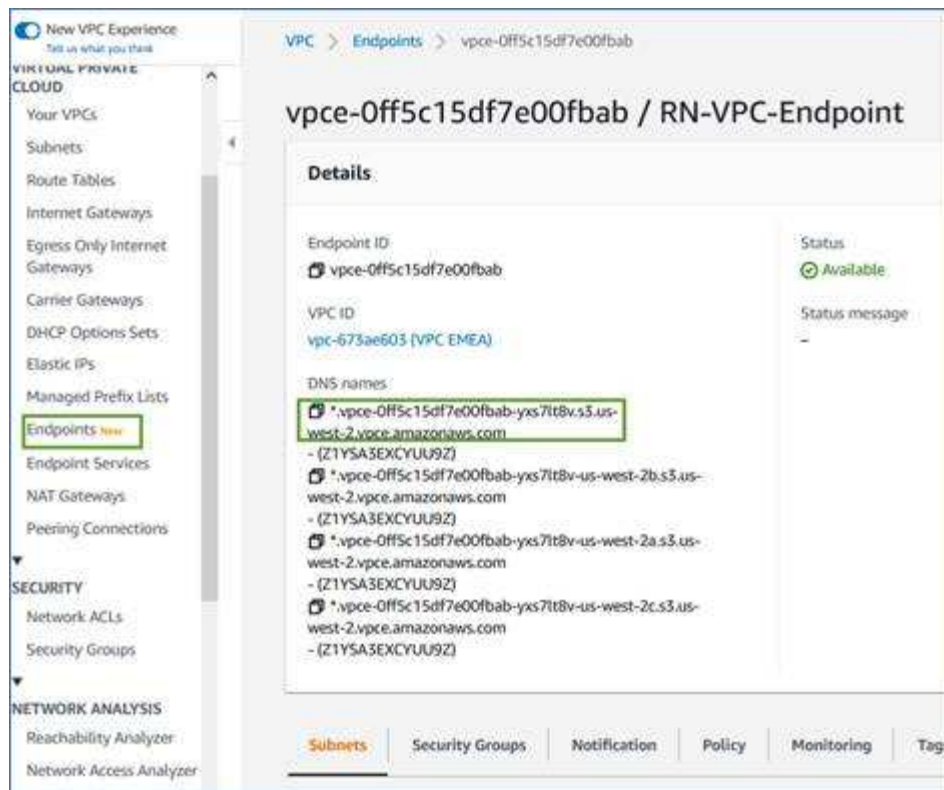
1. Cree una configuración de extremo de interfaz mediante la consola de Amazon VPC o la línea de comandos. "[Consulte los detalles sobre el uso de AWS PrivateLink para Amazon S3](#)".
2. Modifique la configuración del grupo de seguridad asociada al conector BlueXP. Debe cambiar la política a "personalizada" (desde "acceso completo") y debe hacerlo [Añada los permisos S3 desde la política de backup](#) como se ha mostrado anteriormente.



Si está utilizando el puerto 80 (HTTP) para la comunicación con el extremo privado, está configurado. Puede habilitar el backup y la recuperación de datos de BlueXP en el clúster ahora.

Si utiliza el puerto 443 (HTTPS) para comunicarse con el extremo privado, debe copiar el certificado del extremo VPC S3 y añadirlo al clúster de ONTAP, como se muestra en los siguientes 4 pasos.

3. Obtenga el nombre DNS del extremo desde la consola de AWS.



- Obtenga el certificado del extremo VPC S3. Para hacerlo ["Iniciar sesión en la máquina virtual que aloja BlueXP Connector"](#) y ejecute el siguiente comando. Al introducir el nombre DNS del punto final, agregue "bucket" al principio, reemplazando el "\*":

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

- En el resultado de este comando, copie los datos del certificado S3 (todos los datos entre las etiquetas DE CERTIFICADO INICIAL / FINAL, e incluídas):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaD8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvboZ/oO2NWLLFCqI+xmKLCmiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

- Inicie sesión en la CLI del clúster de ONTAP y aplique el certificado que copió con el siguiente comando (reemplace su propio nombre de máquina virtual de almacenamiento):

```
cluster1::> security certificate install -vserver cluster1 -type server-  
ca  
Please enter Certificate: Press <Enter> when done
```

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:

- En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.

Si el destino de Amazon S3 para sus backups existe como un entorno de trabajo en Canvas, puede arrastrar el clúster ONTAP al almacenamiento de objetos de Amazon S3.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, selecciona las **Acciones** ... Y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:

- Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
- Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

### Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el backup para volúmenes adicionales en el entorno de trabajo"](#) (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.
  - Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
  - Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
  - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).
2. Seleccione **Siguiente**.

## Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye del almacenamiento primario al secundario al almacenamiento de objetos y del almacenamiento secundario al de objetos.
  - **Fan Out:** La información fluye del primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una política.



Para crear una política personalizada antes de activar la instantánea, consulte ["Crear una política"](#).

4. Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
  - En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte ["Configuración de políticas de backup en objeto"](#).
- Seleccione **Crear**.

5. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del volumen replicado.
- **Política de replicación:** Elija una política de replicación existente o cree una política.



Para crear una política personalizada antes de activar la replicación, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

6. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Amazon Web Services**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor y la región de AWS donde se almacenarán las copias de seguridad.

La clave de acceso y la clave secreta corresponden al usuario IAM que se ha creado para proporcionar acceso al clúster ONTAP al bloque de S3.

- **Bucket:** Elija un cubo S3 existente o cree uno nuevo. Consulte ["Añadir bloques S3"](#).
- **Clave de cifrado:** Si creaste un nuevo depósito de S3, ingresa la información de la clave de cifrado que se te haya proporcionado del proveedor. Elija si utilizará las claves de cifrado predeterminadas de Amazon S3 o elija sus propias claves gestionadas por el cliente de su cuenta de AWS para administrar el cifrado de sus datos.



Si eligió un depósito existente, la información de cifrado ya está disponible, por lo que no necesita introducirla ahora.

- **Redes:** Elige el espacio IP y si vas a usar un Punto Final Privado. El punto final privado está

desactivado de forma predeterminada.

- i. El espacio IP del clúster de ONTAP en el que residen los volúmenes de los que desea realizar backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.
  - ii. Si lo desea, puede elegir si va a utilizar un AWS PrivateLink que haya configurado previamente. ["Consulte detalles sobre el uso de AWS PrivateLink para Amazon S3"](#).
- **Política de copia de seguridad:** Seleccione una política de copia de seguridad existente o cree una política.



Para crear una política personalizada antes de activar el backup, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
  - Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
  - Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

7. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos primarios contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen de almacenamiento principal.

El bucket S3 se crea en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta que ha introducido, y los archivos de copia de seguridad se almacenan allí. La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

## Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

## El futuro

- Puede hacerlo "[gestione los archivos de copia de seguridad y las políticas de copia de seguridad](#)". Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo "[gestione la configuración de backup en el nivel del clúster](#)". Esto incluye cambiar las claves de almacenamiento que utiliza ONTAP para acceder al almacenamiento en cloud, cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo "[restaure volúmenes, carpetas o archivos individuales desde un archivo de backup](#)". A un sistema Cloud Volumes ONTAP en AWS o a un sistema ONTAP en las instalaciones.

## Realice una copia de seguridad de los datos de ONTAP locales en el almacenamiento de blobs de Azure con la copia de seguridad y recuperación de BlueXP

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP locales a un sistema de almacenamiento secundario y al almacenamiento de blobs de Azure.



Entre los «sistemas ONTAP en las instalaciones» se incluyen los sistemas FAS, AFF y ONTAP Select.

## Inicio rápido

Comience rápidamente siguiendo estos pasos. En las siguientes secciones del tema se proporcionan detalles sobre cada paso.



### Identifica el método de conexión que usará

Elija si conectará su clúster local de ONTAP directamente a Azure a través de la Internet pública, o si usará una VPN o Azure ExpressRoute y enrutará el tráfico a través de una interfaz privada de VPC Endpoint a Azure.

[Identifique el método de conexión.](#)



**2**

### Prepare el conector BlueXP

Si ya tiene un conector implementado en su vnet de Azure o en sus instalaciones, todo estará configurado. De lo contrario, deberá crear un conector BlueXP para realizar backups de los datos de ONTAP en almacenamiento de Azure Blob. También tendrá que personalizar la configuración de red del conector para que pueda conectarse a Azure.

[Aprenda a crear un conector y a definir la configuración de red necesaria.](#)

**3**

### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencias tanto de Azure como de BlueXP.

Consulte [Verifique los requisitos de licencia](#).

**4**

### Prepare los clústeres ONTAP

Detecta tus clústeres de ONTAP en BlueXP, comprueba que los clústeres cumplan con los requisitos mínimos y personaliza la configuración de red para que los clústeres se puedan conectar a Azure.

[Descubra cómo preparar sus clústeres de ONTAP.](#)

**5**

### Preparar Azure Blob como destino de backup

Configure los permisos para que Connector cree y gestione el bucket de Azure. También necesitará configurar permisos para el clúster de ONTAP en las instalaciones para que pueda leer y escribir datos en el bucket de Azure.

De manera opcional, puede configurar sus propias claves gestionadas personalizadas para el cifrado de datos en lugar de utilizar las claves de cifrado de Azure predeterminadas. [Descubre cómo preparar tu entorno de Azure para recibir backups de ONTAP.](#)

**6**

### Active backups en sus ONTAP Volumes

Seleccione el entorno de trabajo y haga clic en **Activar > copia de seguridad de volúmenes** junto al servicio copia de seguridad y recuperación del panel derecho. A continuación, siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

[Active backups en sus ONTAP Volumes.](#)

## Identifique el método de conexión

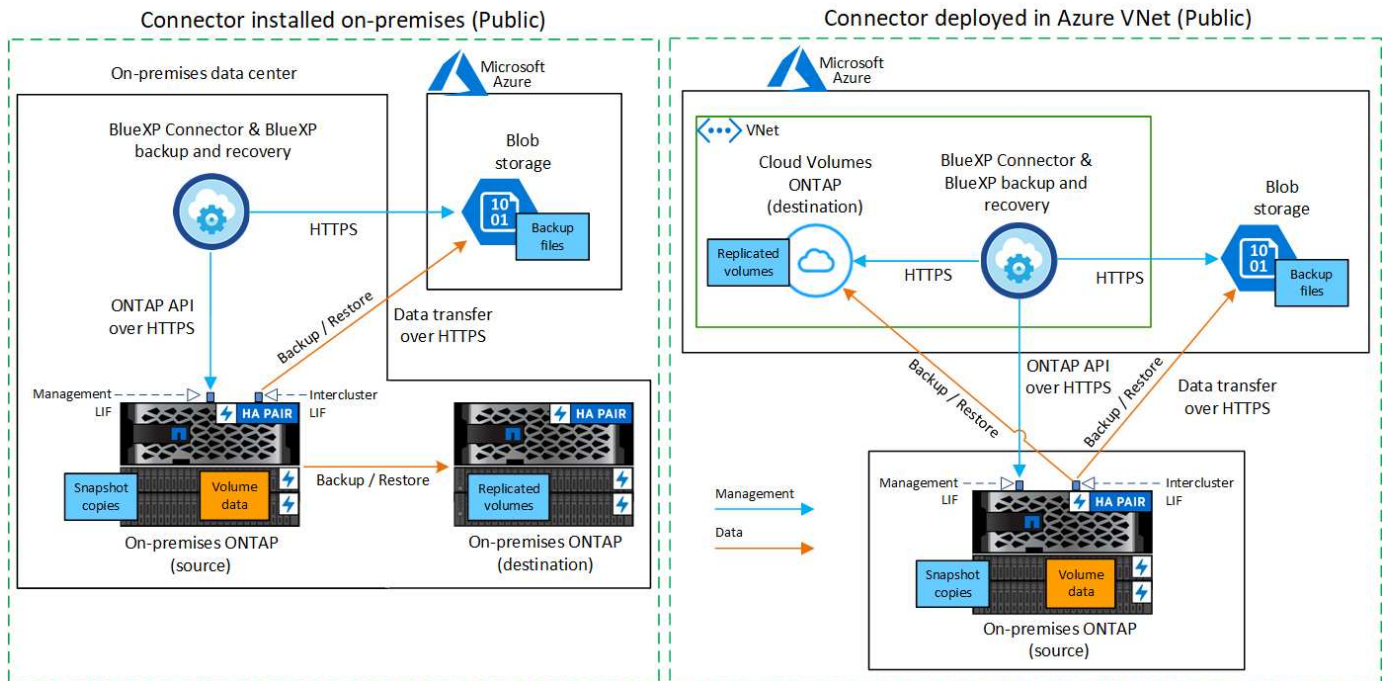
Elija cuál de los dos métodos de conexión utilizará al configurar backups desde sistemas ONTAP en las instalaciones en Azure Blob.

- **\* Conexión pública \*** - Conecte directamente el sistema ONTAP al almacenamiento de Azure Blob utilizando un punto final público de Azure.
- **Conexión privada** - Utilice una VPN o ExpressRoute y enrute el tráfico a través de un punto final privado de vnet que utilice una dirección IP privada.

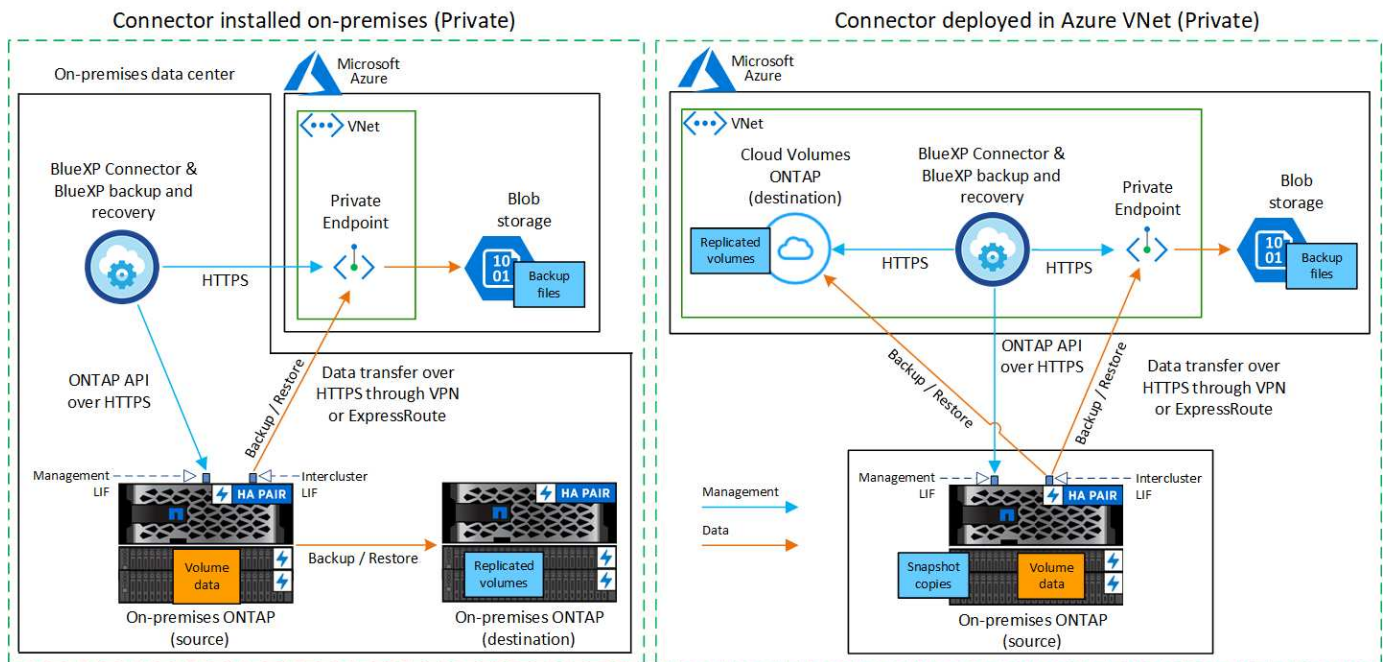


Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.

El siguiente diagrama muestra el método **de conexión pública** y las conexiones que necesita preparar entre los componentes. Puede utilizar un conector que haya instalado en sus instalaciones o un conector que haya implementado en la vnet de Azure.



El siguiente diagrama muestra el método **de conexión privada** y las conexiones que necesita preparar entre los componentes. Puede utilizar un conector que haya instalado en sus instalaciones o un conector que haya implementado en la vnet de Azure.



## Prepare el conector BlueXP

El conector BlueXP es el software principal para la funcionalidad BlueXP. Se necesita un conector para realizar una copia de seguridad y restaurar los datos de ONTAP.

### Cree o cambie conectores

Si ya tiene un conector implementado en su vnet de Azure o en sus instalaciones, todo estará configurado.

Si no es así, deberá crear un conector en una de esas ubicaciones para realizar backups de los datos de ONTAP en el almacenamiento de Azure Blob. No puede utilizar un conector puesto en marcha en otro proveedor de cloud.

- ["Más información sobre conectores"](#)
- ["Instale un conector en Azure"](#)
- ["Instale un conector en sus instalaciones"](#)
- ["Instale un conector en una región gubernamental de Azure"](#)

El backup y la recuperación de BlueXP son compatibles con regiones gubernamentales de Azure cuando el conector se implementa en la nube, no cuando se instala en tus instalaciones. Además, debe poner en marcha el conector desde Azure Marketplace. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

### Prepare la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

#### Pasos

1. Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:
  - Una conexión HTTPS a través del puerto 443 al servicio de backup y recuperación de BlueXP y al almacenamiento de objetos Blob (["consulte la lista de extremos"](#))
  - Una conexión HTTPS a través del puerto 443 para la LIF de gestión del clúster ONTAP
  - Para que la funcionalidad de búsqueda y restauración de copia de seguridad y recuperación de BlueXP funcione, debe estar abierto el puerto 1433 para la comunicación entre Connector y los servicios SQL de Azure Synapse.
  - Se requieren reglas adicionales de grupos de seguridad entrantes para implementaciones gubernamentales de Azure y Azure. Consulte ["Reglas para Connector en Azure"](#) para obtener más detalles.
2. Habilite un extremo privado de vnet con el almacenamiento de Azure. Esto es necesario si tiene una conexión ExpressRoute o VPN de su clúster ONTAP a vnet y desea que la comunicación entre el conector y el almacenamiento BLOB permanezca en su red privada virtual (una conexión **privada**).

### Verifique o agregue permisos al conector

Para utilizar la funcionalidad de búsqueda y restauración de backup y recuperación de BlueXP, necesita contar con permisos específicos en la función de Connector para que pueda acceder a Azure Synapse Workspace y a la cuenta de almacenamiento de lago de datos. Consulte los siguientes permisos y siga los pasos si necesita modificar la directiva.

#### Antes de empezar

Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") en su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#). Debe ser Subscription **Owner** o **Contributor** para registrar el proveedor de recursos.

## Pasos

1. Identifique la función asignada a la máquina virtual conector:
  - a. En el portal de Azure, abra el servicio Virtual Machines.
  - b. Seleccione la máquina virtual conector.
  - c. En **Configuración**, selecciona **Identidad**.
  - d. Seleccione **Asignaciones de roles de Azure**.
  - e. Anote la función personalizada asignada a la máquina virtual conector.
2. Actualice el rol personalizado:
  - a. En el portal de Azure, abra su suscripción a Azure.
  - b. Selecciona **Control de acceso (IAM) > Roles**.
  - c. Seleccione los puntos suspensivos (...) para el rol personalizado y luego seleccione **Editar**.
  - d. Seleccione **JSON** y agregue los siguientes permisos:

```

"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"

```

["Vea el formato JSON completo para la política"](#)

e. Selecciona **Revisar + actualizar** y luego selecciona **Actualizar**.

## Verifique los requisitos de licencia

Tendrás que verificar los requisitos de licencias para Azure y BlueXP:

- Antes de poder activar el backup y la recuperación de BlueXP para tu clúster, deberás suscribirte a una oferta de pago por uso (PAYGO) BlueXP Marketplace desde Azure, o comprar y activar una licencia BYOL de backup y recuperación de BlueXP desde NetApp. Estas licencias son para su cuenta y se pueden utilizar en varios sistemas.
  - Para las licencias PAYGO de backup y recuperación de BlueXP, necesitarás una suscripción al ["Oferta de NetApp BlueXP en Azure Marketplace"](#). La facturación para el backup y la recuperación de BlueXP se realiza a través de esta suscripción.
  - Para la licencia BYOL de backup y recuperación de BlueXP, necesitará el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).
- Necesita tener una suscripción de Azure para el espacio de almacenamiento de objetos donde se ubicará los backups.

### Regiones apoyadas

Puede crear copias de seguridad desde sistemas locales a Azure Blob en todas las regiones, incluidas las regiones de Azure Government. Especifica la región en la que se almacenarán las copias de seguridad al configurar el servicio.

## Prepare los clústeres ONTAP

Tendrá que preparar su sistema ONTAP de origen en las instalaciones y cualquier sistema ONTAP o Cloud Volumes ONTAP secundario en las instalaciones.

La preparación de los clústeres de ONTAP implica los siguientes pasos:

- Descubre tus sistemas de ONTAP en BlueXP
- Compruebe los requisitos del sistema ONTAP
- Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos
- Compruebe los requisitos de red de ONTAP para replicar volúmenes

### Descubre tus sistemas de ONTAP en BlueXP

Tanto su sistema ONTAP de origen en las instalaciones como todos los sistemas ONTAP o Cloud Volumes ONTAP secundarios en las instalaciones deben estar disponibles en BlueXP Canvas.

Tendrá que conocer la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster.

["Aprenda a detectar un clúster"](#).

### Compruebe los requisitos del sistema ONTAP

Asegúrese de que se cumplen los siguientes requisitos de ONTAP:

- Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.
- Una licencia de SnapMirror (incluida como parte del paquete Premium o del paquete de protección de

datos).

**Nota:** El “paquete de nube híbrida” no es necesario cuando se utiliza la copia de seguridad y recuperación de BlueXP.

Aprenda cómo ["gestione las licencias de clúster"](#).

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["configure la hora del clúster"](#).
- Si va a replicar datos, debe comprobar que los sistemas de origen y de destino ejecutan versiones de ONTAP compatibles antes de replicar datos.

["Consulte versiones de ONTAP compatibles para relaciones de SnapMirror"](#).

## Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos

Debe configurar los siguientes requisitos en el sistema que se conecta al almacenamiento de objetos.

- Para una arquitectura de copia de seguridad ramificada, configure los siguientes ajustes en el sistema *primary*.
- Para una arquitectura de copia de seguridad en cascada, configure los siguientes ajustes en el sistema *secondary*.

Se necesitan los siguientes requisitos de red de clúster de ONTAP:

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 desde la LIF entre clústeres al almacenamiento BLOB de Azure para realizar operaciones de backup y restauración.

ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

- ONTAP requiere una conexión entrante desde el conector hasta la LIF de administración del clúster. El conector puede residir en una vnet de Azure.
- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos. ["Obtenga más información acerca de los espacios IP"](#).

Al configurar el backup y la recuperación de BlueXP, se le pedirá que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

- Las LIF de interconexión de clústeres y los nodos pueden acceder al almacén de objetos.
- Los servidores DNS se configuraron para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Descubra cómo ["Configure los servicios DNS para la SVM"](#).
- Si utiliza un espacio IP diferente al predeterminado, es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones del servicio de backup y recuperación de BlueXP desde ONTAP al almacenamiento de objetos a través del puerto 443 y el tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS por el puerto 53 (TCP/UDP).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.

## Preparar Azure Blob como destino de backup

1. Puede utilizar sus propias claves gestionadas de forma personalizada para el cifrado de datos en el asistente de activación en lugar de utilizar las claves de cifrado gestionadas por Microsoft predeterminadas. En este caso, deberá tener la suscripción a Azure, el nombre de almacén de claves y la clave. ["Aprende a usar tus propias claves"](#).

Tenga en cuenta que la copia de seguridad y la recuperación admiten *políticas de acceso de Azure* como modelo de permiso. Actualmente no se admite el modelo de permiso *Azure Role-Based Access Control* (Azure RBAC).

2. Si desea disponer de una conexión más segura a través de Internet pública desde el centro de datos local hasta el vnet, existe una opción para configurar un extremo privado de Azure en el asistente de activación. En este caso, deberá conocer la red y la subred de esta conexión. ["Consulte los detalles sobre el uso de un punto final privado"](#).

### Cree su cuenta de almacenamiento de Azure Blob

De forma predeterminada, el servicio crea cuentas de almacenamiento para usted. Si desea utilizar sus propias cuentas de almacenamiento, puede crearlas antes de iniciar el asistente de activación de copia de seguridad y, a continuación, seleccionar esas cuentas de almacenamiento en el asistente.

["Obtenga más información sobre la creación de sus propias cuentas de almacenamiento"](#).

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)



- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

## Inicie el asistente

### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.



Si el destino de Azure para sus backups existe como entorno de trabajo en Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de Azure Blob.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, selecciona las **Acciones** ... Y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:
  - Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
  - Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

## Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el backup para volúmenes adicionales en el entorno de trabajo"](#) (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.



## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.
  - Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
  - Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
  - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).
2. Seleccione **Siguiente**.

## Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye de lo primario a lo secundario, y de lo secundario al almacenamiento de objetos.
  - **Fan Out:** La información fluye del primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una nueva.



Para crear una política personalizada antes de activar la instantánea, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

4. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del volumen replicado.
- **Política de replicación:** Elija una política de replicación existente o cree una nueva.



Para crear una política personalizada antes de activar la replicación, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Microsoft Azure**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor y la región donde se almacenarán las copias de seguridad.

Cree una nueva cuenta de almacenamiento o seleccione una existente.

Cree su propio grupo de recursos que gestione el contenedor Blob o seleccione el tipo y el grupo de recursos.



Si desea proteger los archivos de copia de seguridad para evitar que se modifiquen o eliminen, asegúrese de que la cuenta de almacenamiento se haya creado con almacenamiento inmutable habilitado mediante un período de retención de 30 días.



Si desea organizar en niveles archivos de copia de seguridad antiguos en Azure Archive Storage para obtener una mayor optimización de los costes, asegúrese de que la cuenta de almacenamiento tenga la regla de ciclo de vida adecuada.

- **Clave de cifrado:** Si creó una nueva cuenta de almacenamiento de Azure, ingrese la información de clave de cifrado que le dio el proveedor. Elija si utilizará las claves de cifrado predeterminadas de Azure o elija sus propias claves gestionadas por el cliente de su cuenta de Azure para administrar el cifrado de sus datos.

Si decide utilizar sus propias claves gestionadas por el cliente, introduzca el almacén de claves y la información de clave.



Si eligió una cuenta de almacenamiento de Microsoft existente, la información de cifrado ya está disponible, por lo que no necesita ingresarla ahora.

- **Redes:** Elige el espacio IP y si vas a usar un Punto Final Privado. El punto final privado está desactivado de forma predeterminada.
  - i. El espacio IP del clúster de ONTAP en el que residen los volúmenes de los que desea realizar backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.
  - ii. Opcionalmente, seleccione si utilizará un punto final privado de Azure que haya configurado previamente. ["Obtenga más información sobre el uso de un extremo privado de Azure"](#).
- **Política de copia de seguridad:** Seleccione una política existente de copia de seguridad para almacenamiento de objetos o cree una nueva.



Para crear una política personalizada antes de activar el backup, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte ["Configuración de políticas de backup en objeto"](#).
- Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen primario.

Se crea una cuenta de almacenamiento Blob en el grupo de recursos introducido, y los archivos de backup se almacenan allí. La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la "[Panel de control de trabajos](#)".

### Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

### El futuro

- Puede hacerlo "[gestione los archivos de copia de seguridad y las políticas de copia de seguridad](#)". Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo "[gestione la configuración de backup en el nivel del clúster](#)". Esto incluye cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo "[restaure volúmenes, carpetas o archivos individuales desde un archivo de backup](#)". A un sistema Cloud Volumes ONTAP en Azure o a un sistema ONTAP en las instalaciones.

## Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con la copia de seguridad y recuperación de BlueXP

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP primarios locales a un sistema de almacenamiento secundario y a Google Cloud Storage.



Entre los «sistemas ONTAP en las instalaciones» se incluyen los sistemas FAS, AFF y ONTAP Select.

### Inicio rápido

Comience rápidamente siguiendo estos pasos. En las siguientes secciones del tema se proporcionan detalles sobre cada paso.



#### Identifica el método de conexión que usarás

Elige si conectarás tu clúster local de ONTAP directamente a Google Cloud Storage a través de Internet

pública, o si usará una VPN o una interconexión de Google Cloud y enrutará el tráfico a través de una interfaz privada de Google Access que utilice una dirección IP privada.

2

### Prepare el conector BlueXP

Si ya tiene un conector puesto en marcha en su VPC de Google Cloud Platform, todo estará configurado. De lo contrario, tendrá que crear un conector BlueXP para realizar backups de los datos de ONTAP en el almacenamiento de Google Cloud. También tendrá que personalizar la configuración de red del conector para que pueda conectarse a Google Cloud.

3

### Prepare la conexión en red para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

4

### Verifique los requisitos de licencia

Tendrá que comprobar los requisitos de licencias tanto para Google Cloud como para BlueXP.

5

### Prepare los clústeres ONTAP

Detecte sus clústeres de ONTAP en BlueXP, compruebe que los clústeres cumplan con los requisitos mínimos y personalice la configuración de red para que los clústeres se puedan conectar a Google Cloud.

6

### Prepare Google Cloud como destino de backup

Configura permisos para que Connector cree y administre el bucket de Google Cloud. También necesitará configurar permisos para el clúster de ONTAP en las instalaciones para que pueda leer y escribir datos en el bucket de Google Cloud.

De manera opcional, puede configurar sus propias claves gestionadas personalizadas para el cifrado de datos en lugar de utilizar las claves de cifrado de Google Cloud predeterminadas.

7

### Active backups en sus ONTAP Volumes

Seleccione el entorno de trabajo y haga clic en **Activar > copia de seguridad de volúmenes** junto al servicio copia de seguridad y recuperación del panel derecho. A continuación, siga el asistente de configuración para seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

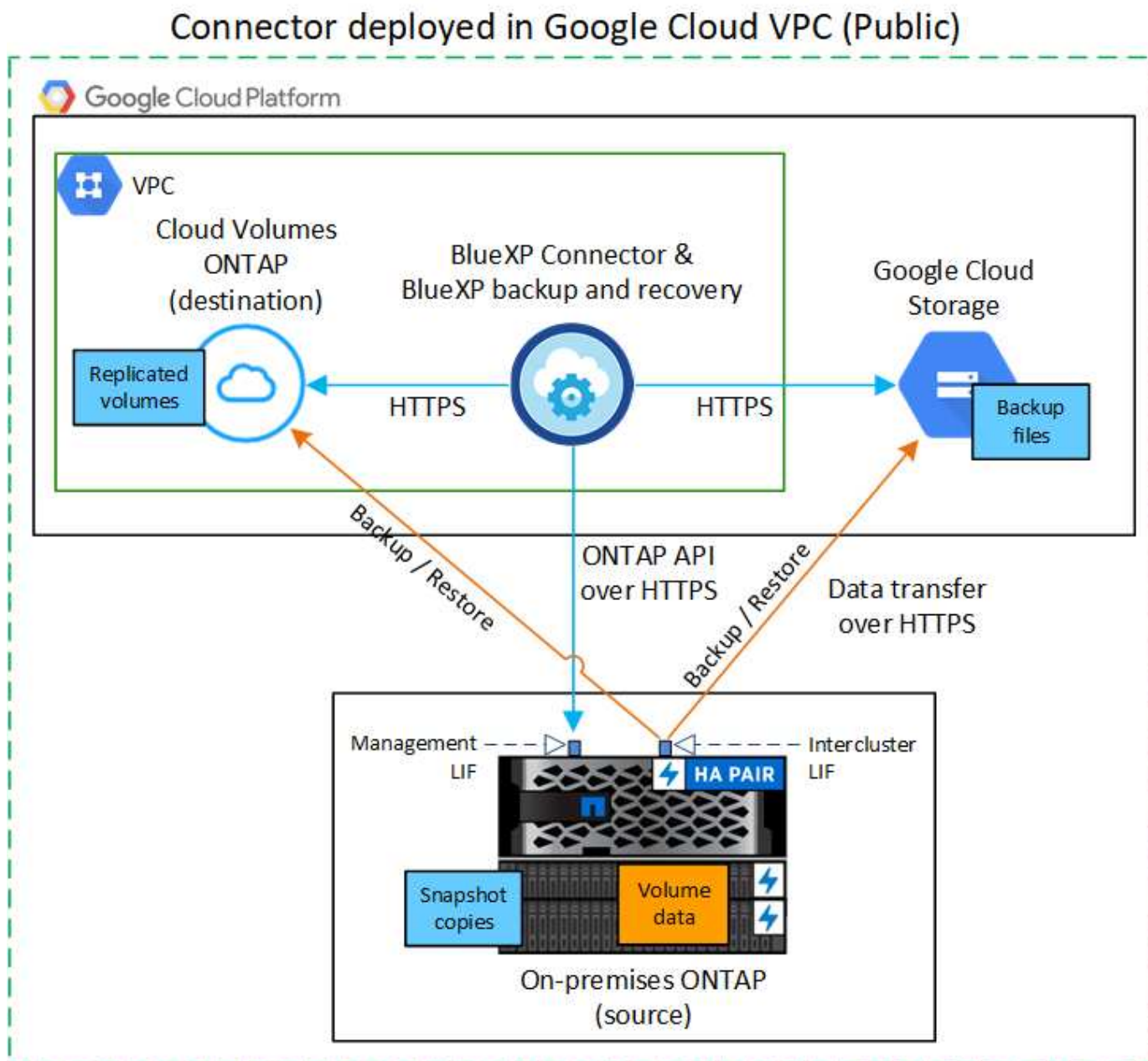
## Identifique el método de conexión

Elija cuál de los dos métodos de conexión utilizará al configurar copias de seguridad de sistemas ONTAP locales en Google Cloud Storage.

- **Conexión pública** - Conecte directamente el sistema ONTAP al almacenamiento en la nube de Google usando un punto final público de Google.
- **Conexión privada:** Utilice una VPN o Google Cloud Interconnect y enrute el tráfico a través de una interfaz privada de Google Access que utilice una dirección IP privada.

Opcionalmente, puede conectarse a un sistema ONTAP secundario para volúmenes replicados también mediante la conexión pública o privada.

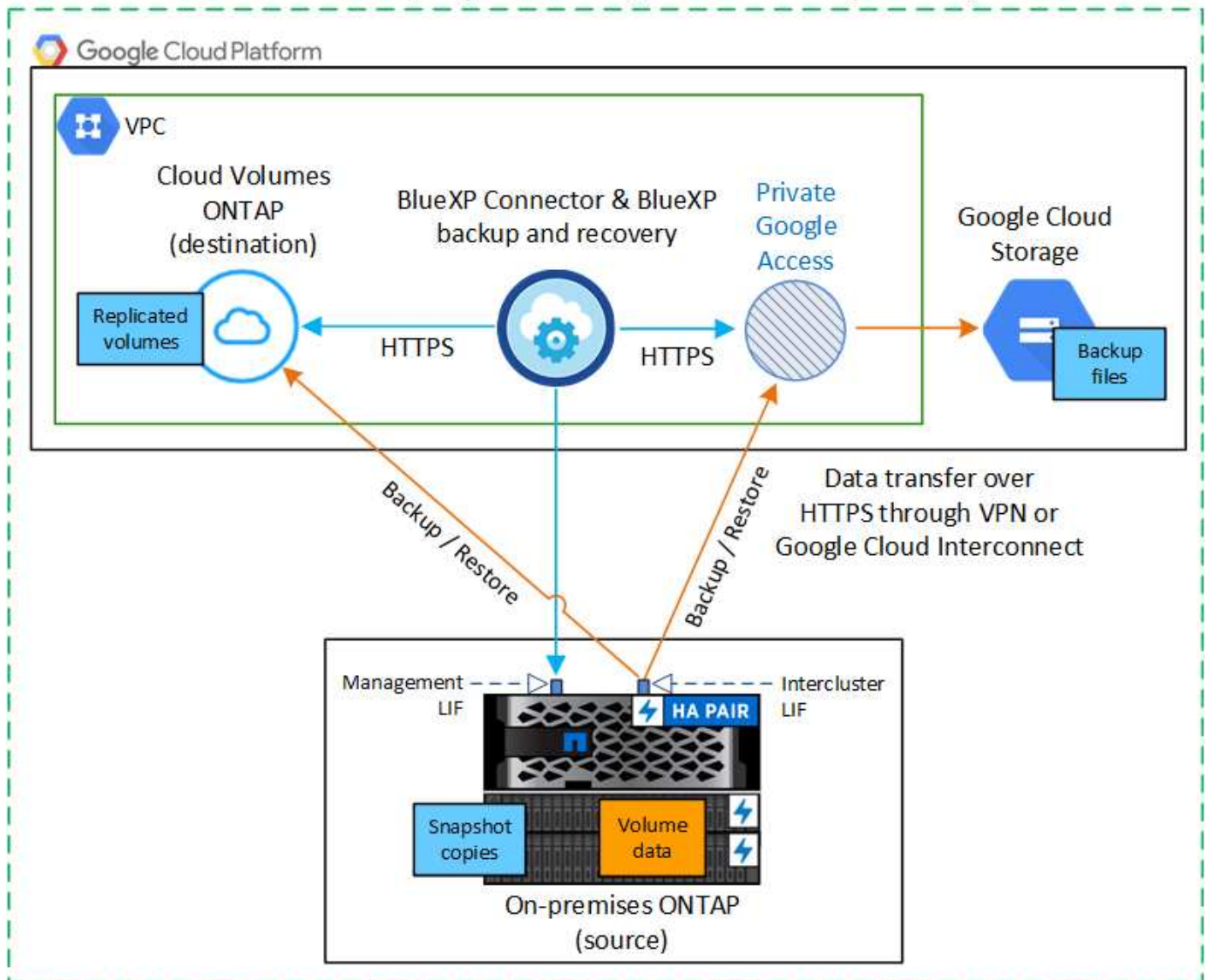
El siguiente diagrama muestra el método **de conexión pública** y las conexiones que necesita preparar entre los componentes. El conector se debe poner en marcha en el VPC de Google Cloud Platform.



El siguiente diagrama muestra el método **de conexión privada** y las conexiones que necesita preparar entre los componentes. El conector se debe poner en marcha en el VPC de Google Cloud Platform.



## Connector deployed in Google Cloud VPC (Private)



## Prepare el conector BlueXP

El conector BlueXP es el software principal para la funcionalidad BlueXP. Se necesita un conector para realizar una copia de seguridad y restaurar los datos de ONTAP.

### Cree o cambie conectores

Si ya tiene un conector puesto en marcha en su VPC de Google Cloud Platform, todo estará configurado.

Si no es así, tendrás que crear un conector en esa ubicación para hacer una copia de seguridad de los datos de ONTAP en Google Cloud Storage. No puede utilizar un conector puesto en marcha en otro proveedor de cloud o en las instalaciones.

- ["Más información sobre conectores"](#)
- ["Instalar un conector en GCP"](#)

## Prepare la conexión a redes para el conector

Asegúrese de que el conector tiene las conexiones de red necesarias.

### Pasos

1. Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:
  - Una conexión HTTPS a través del puerto 443 al servicio de backup y recuperación de BlueXP y a tu almacenamiento de Google Cloud ("[consulte la lista de extremos](#)")
  - Una conexión HTTPS a través del puerto 443 para la LIF de gestión del clúster ONTAP
2. Active Google Access privado (o Private Service Connect) en la subred en la que planea implementar el conector. "[Acceso privado a Google](#)" o "[Conexión de servicios privados](#)". Son necesarias si tiene una conexión directa de su clúster ONTAP al VPC y desea que la comunicación entre el conector y Google Cloud Storage permanezca en su red privada virtual (una conexión **privada**).

Siga las instrucciones de Google para configurar estas opciones de acceso privado. Asegúrese de que los servidores DNS se han configurado para señalar `www.googleapis.com` y `storage.googleapis.com` a las direcciones IP internas (privadas) correctas.

### Verifique o agregue permisos al conector

Para utilizar la funcionalidad de «búsqueda y restauración» de backup y recuperación de BlueXP, necesitas contar con permisos específicos en la función del conector para que pueda acceder al servicio de Google Cloud BigQuery. Revise los permisos a continuación y siga los pasos si necesita modificar la política.

### Pasos

1. En la "[Consola de Google Cloud](#)", vaya a la página **roles**.
2. Mediante la lista desplegable situada en la parte superior de la página, seleccione el proyecto o la organización que contiene la función que desea editar.
3. Seleccione un rol personalizado.
4. Seleccione **Editar rol** para actualizar los permisos del rol.
5. Seleccione **Agregar permisos** para agregar los siguientes permisos nuevos al rol.

```
bigquery.jobs.get  
bigquery.jobs.list  
bigquery.jobs.listAll  
bigquery.datasets.create  
bigquery.datasets.get  
bigquery.jobs.create  
bigquery.tables.get  
bigquery.tables.getData  
bigquery.tables.list  
bigquery.tables.create
```

6. Seleccione **Actualizar** para guardar el rol editado.



## Verifique los requisitos de licencia

- Antes de poder activar el backup y la recuperación de BlueXP para tu clúster, deberás suscribirte a una oferta de pago por uso (PAYGO) BlueXP Marketplace en Google, o comprar y activar una licencia BYOL de backup y recuperación de BlueXP de NetApp. Estas licencias son para su cuenta y se pueden utilizar en varios sistemas.
  - Para las licencias PAYGO de backup y recuperación de BlueXP, necesitarás una suscripción al ["Oferta de NetApp BlueXP en Google Marketplace"](#). La facturación para el backup y la recuperación de BlueXP se realiza a través de esta suscripción.
  - Para la licencia BYOL de backup y recuperación de BlueXP, necesitará el número de serie de NetApp que le permita usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).
- Es necesario disponer de una suscripción a Google para el espacio de almacenamiento de objetos en el que se localizarán los backups.

## Regiones apoyadas

Puede crear copias de seguridad desde sistemas locales en Google Cloud Storage en todas las regiones. Especifique la región en la que se almacenarán las copias de seguridad al configurar el servicio.

## Prepare los clústeres ONTAP

Tendrá que preparar su sistema ONTAP de origen en las instalaciones y cualquier sistema ONTAP o Cloud Volumes ONTAP secundario en las instalaciones.

La preparación de los clústeres de ONTAP implica los siguientes pasos:

- Descubra sus sistemas de ONTAP en BlueXP
- Compruebe los requisitos del sistema ONTAP
- Compruebe los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos
- Compruebe los requisitos de red de ONTAP para replicar volúmenes

## Descubre tus sistemas de ONTAP en BlueXP

Tanto su sistema ONTAP de origen en las instalaciones como todos los sistemas ONTAP o Cloud Volumes ONTAP secundarios en las instalaciones deben estar disponibles en BlueXP Canvas.

Tendrá que conocer la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster.

["Aprenda a detectar un clúster"](#).

## Compruebe los requisitos del sistema ONTAP

Asegúrese de que se cumplen los siguientes requisitos de ONTAP:

- Se recomienda un mínimo de ONTAP 9.8; ONTAP 9.8P13 y posterior.
- Una licencia de SnapMirror (incluida como parte del paquete Premium o del paquete de protección de datos).

**Nota:** El "paquete de nube híbrida" no es necesario cuando se utiliza la copia de seguridad y recuperación

de BlueXP.

Aprenda cómo ["gestione las licencias de clúster"](#).

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["configure la hora del clúster"](#).
- Si va a replicar datos, debe comprobar que los sistemas de origen y de destino ejecutan versiones de ONTAP compatibles antes de replicar datos.

["Consulte versiones de ONTAP compatibles para relaciones de SnapMirror"](#).

## Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos

Debe configurar los siguientes requisitos en el sistema que se conecta al almacenamiento de objetos.

- Para una arquitectura de copia de seguridad ramificada, configure los siguientes ajustes en el sistema *primary*.
- Para una arquitectura de copia de seguridad en cascada, configure los siguientes ajustes en el sistema *secondary*.

Se necesitan los siguientes requisitos de red de clúster de ONTAP:

- El clúster de ONTAP inicia una conexión HTTPS a través del puerto 443 de la LIF entre clústeres a Google Cloud Storage para operaciones de backup y restauración.

ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

- ONTAP requiere una conexión entrante desde el conector hasta la LIF de administración del clúster. El conector puede residir en un VPC de Google Cloud Platform.
- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos. ["Obtenga más información acerca de los espacios IP"](#).

Al configurar el backup y la recuperación de BlueXP, se le pedirá que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

- Las LIF de interconexión de clústeres de los nodos pueden acceder al almacén de objetos.
- Los servidores DNS se configuraron para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Descubra cómo ["Configure los servicios DNS para la SVM"](#).

Si utiliza Google Access privado o Private Service Connect, asegúrese de que los servidores DNS se han configurado para señalar `storage.googleapis.com` A la dirección IP interna (privada) correcta.

- Tenga en cuenta que si utiliza un espacio IP diferente al predeterminado, es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones de backup y recuperación de BlueXP desde ONTAP al almacenamiento de objetos a través del puerto 443, así como el tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.

## Preparar Google Cloud Storage como destino de backup

Preparar Google Cloud Storage como destino de copia de seguridad implica los siguientes pasos:

- Configure los permisos.
- (Opcional) Cree sus propios buckets. (El servicio creará cubos para usted si lo desea.)
- (Opcional) Configurar claves gestionadas por el cliente para el cifrado de los datos

### Configure los permisos

Debe proporcionar claves de acceso de almacenamiento para una cuenta de servicio que tenga permisos específicos mediante un rol personalizado. Una cuenta de servicio permite el backup y la recuperación de datos de BlueXP para autenticar y acceder a los depósitos de Cloud Storage que se usan para almacenar backups. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

### Pasos

1. En la ["Consola de Google Cloud"](#), Vaya a la página **roles**.
2. ["Crear un rol nuevo"](#) con los siguientes permisos:

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. En la consola de Google Cloud, "[Vaya a la página de cuentas de servicio](#)".
4. Seleccione su proyecto de cloud.
5. Seleccione **Crear cuenta de servicio** y proporcione la información requerida:
  - a. **Detalles de la cuenta de servicio:** Introduzca un nombre y una descripción.
  - b. **Conceder acceso a esta cuenta de servicio al proyecto:** Seleccione la función personalizada que acaba de crear.
  - c. Seleccione **Listo**.
6. Vaya a. "[Configuración de almacenamiento para GCP](#)" y crear claves de acceso para la cuenta de servicio:
  - a. Seleccione un proyecto y seleccione **Interoperabilidad**. Si aún no lo ha hecho, seleccione **Habilitar acceso a interoperabilidad**.
  - b. En **Claves de acceso para cuentas de servicio**, selecciona **Crear una clave para una cuenta de servicio**, selecciona la cuenta de servicio que acabas de crear y haz clic en **Crear clave**.

Tendrá que introducir las claves en el backup y la recuperación de BlueXP más adelante cuando configure el servicio de backup.

## Crea tus propios cubos

De forma predeterminada, el servicio crea buckets para usted. O bien, si desea utilizar sus propios depósitos, puede crearlos antes de iniciar el asistente de activación de copias de seguridad y, a continuación, seleccionar esos bloques en el asistente.

["Obtenga más información sobre cómo crear sus propios cubos"](#).

## Configurar claves de cifrado gestionadas por el cliente (CMEK) para el cifrado de datos

Puede utilizar sus propias claves gestionadas por el cliente para el cifrado de datos en lugar de utilizar las claves de cifrado predeterminadas gestionadas por Google. Se admiten tanto claves entre regiones como entre proyectos, por lo que puede elegir un proyecto para un depósito que sea diferente al proyecto de la clave CMEK.

Si planea utilizar sus propias claves gestionadas por el cliente:

- Necesitará tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado gestionadas por el cliente"](#).
- Deberá verificar que estos permisos necesarios se incluyan en la función del conector:

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- Deberás verificar que la API de Google "Cloud Key Management Service (KMS)" esté habilitada en tu proyecto. Consulte ["Documentación de Google Cloud: Habilitar API"](#) para obtener más detalles.

### Consideraciones de CMEK:

- Se admiten tanto las claves generadas por software como las de HSM (respaldado por hardware).
- Se admiten las claves de Cloud KMS creadas o importadas recientemente.
- Solo se admiten claves regionales; las claves globales no son compatibles.
- Actualmente, sólo se admite el propósito "cifrado/descifrado simétrico".
- Al agente de servicios asociado con la cuenta de almacenamiento se le asigna el rol IAM «CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)» mediante el backup y la recuperación de datos de BlueXP.

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.



Si el destino de Google Cloud Storage para sus copias de seguridad existe como un entorno de trabajo en Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de Google Cloud.

- Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, selecciona las **Acciones** ... Y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tiene replicación o copia de seguridad en el almacenamiento de objetos ya activado). .

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:

- Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
- Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

### Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo "[active el backup para volúmenes adicionales en el entorno de trabajo](#)" (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

### Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.

- Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
- Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).

- Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).

## 2. Seleccione **Siguiente**.

### Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

### Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige replicación y copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye de lo primario a lo secundario y de lo secundario al almacenamiento de objetos.
  - **Fan Out:** La información fluye del primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una nueva.



Para crear una política personalizada antes de activar la instantánea, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

4. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del

volumen replicado.

- **Política de replicación:** Elija una política de replicación existente o cree una nueva.



Para crear una política personalizada antes de activar la replicación, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

##### 5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **Google Cloud**.
- **Configuración del proveedor:** Introduzca los detalles del proveedor y la región donde se almacenarán las copias de seguridad.

Cree un nuevo depósito o seleccione uno que ya haya creado.



Si desea organizar en niveles los archivos de backup antiguos en el almacenamiento de Google Cloud Archive para obtener una mayor optimización de los costes, asegúrese de que el bloque tenga la regla de ciclo de vida adecuada.

Introduzca la clave de acceso y la clave secreta de Google Cloud.

- **Clave de cifrado:** Si creaste una nueva cuenta de almacenamiento de Google Cloud, ingresa la información de la clave de cifrado que se te ha proporcionado del proveedor. Elija si utilizará las claves de cifrado predeterminadas de Google Cloud o si elige sus propias claves gestionadas por el cliente en su cuenta de Google Cloud para gestionar el cifrado de sus datos.



Si eligió una cuenta de almacenamiento de Google Cloud existente, la información de cifrado ya está disponible, por lo que no necesita ingresarla ahora.

Si decide utilizar sus propias claves gestionadas por el cliente, introduzca el timbre y el nombre de la clave. ["Obtenga más información sobre las claves de cifrado gestionadas por el cliente"](#).

- **Networking:** Elige el espacio IP.

El espacio IP del clúster de ONTAP en el que residen los volúmenes de los que desea realizar backup. Las LIF entre clústeres de este espacio IP deben tener acceso a Internet saliente.

- **Política de copia de seguridad:** Seleccione una política existente de copia de seguridad para almacenamiento de objetos o cree una nueva.



Para crear una política personalizada antes de activar el backup, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.



- Seleccione **Crear**.

- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen de origen.

Se crea automáticamente un bloque de Google Cloud Storage en la cuenta de servicio indicada por la clave de acceso de Google y la clave secreta introducida; además, los archivos de backup se almacenan allí. La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

## Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

## El futuro

- Puede hacerlo ["gestione los archivos de copia de seguridad y las políticas de copia de seguridad"](#). Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo ["gestione la configuración de backup en el nivel del clúster"](#). Esto incluye cambiar las

claves de almacenamiento que utiliza ONTAP para acceder al almacenamiento en cloud, cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.

- También puede hacerlo ["restaure volúmenes, carpetas o archivos individuales desde un archivo de backup"](#) A un sistema Cloud Volumes ONTAP en Google o a un sistema ONTAP en las instalaciones.

## Realice una copia de seguridad de los datos locales de ONTAP en ONTAP S3 con la copia de seguridad y recuperación de BlueXP

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas ONTAP locales primarios. Puede enviar backups a un sistema de almacenamiento secundario de ONTAP (un volumen replicado) o a un bloque en un sistema ONTAP configurado como servidor S3 (un archivo de backup), o a ambos.

El sistema ONTAP principal en las instalaciones puede ser un sistema FAS, AFF o ONTAP Select. El sistema ONTAP secundario puede ser un sistema ONTAP o Cloud Volumes ONTAP en las instalaciones. El almacenamiento de objetos puede estar en un sistema ONTAP en las instalaciones o en un sistema Cloud Volumes ONTAP en el que haya habilitado un servidor de almacenamiento de objetos Simple Storage Service (S3).

### Inicio rápido

Comience rápidamente siguiendo estos pasos. En las siguientes secciones del tema se proporcionan detalles sobre cada paso.

1

#### Identifica el método de conexión que usarás

Revise cómo conectará su clúster ONTAP principal en las instalaciones al clúster de ONTAP secundario para su replicación y al clúster de ONTAP configurado como servidor S3 para backup en el almacenamiento de objetos.

[Identifique el método de conexión.](#)

2

#### Prepare el conector BlueXP

Si ya has puesto en marcha un conector BlueXP, ya está todo listo. De lo contrario, deberás crear un conector BlueXP para realizar copias de seguridad de los datos de ONTAP en ONTAP S3. También tendrá que personalizar la configuración de red del conector para que pueda conectarse a ONTAP S3.

[Aprenda a crear un conector y a definir la configuración de red necesaria.](#)

3

#### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencia para tus sistemas de ONTAP y para el backup y la recuperación de BlueXP.

[Verifique los requisitos de licencia.](#)

## 4

### Prepare los clústeres ONTAP

Detecte sus clústeres de ONTAP principal y secundario en BlueXP, compruebe que los clústeres cumplan con los requisitos mínimos y personalice la configuración de red para que los clústeres se puedan conectar al almacenamiento de objetos ONTAP S3.

[Descubra cómo preparar sus clústeres de ONTAP.](#)

## 5

### Prepare ONTAP S3 como destino de backup

Configure permisos para el conector para que pueda administrar el bucket de ONTAP S3. También necesitará configurar permisos para el clúster de ONTAP de origen en las instalaciones para que pueda leer y escribir datos en el bucket de ONTAP S3.

[Descubra cómo preparar su entorno de ONTAP S3 para recibir backups de ONTAP.](#)

## 6

### Active backups en sus ONTAP Volumes

Seleccione el entorno de trabajo principal y haga clic en **Activar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho. A continuación, siga el asistente de configuración para seleccionar los volúmenes de los que desea realizar un backup y las políticas de Snapshot, replicación y backup en objetos que usará.

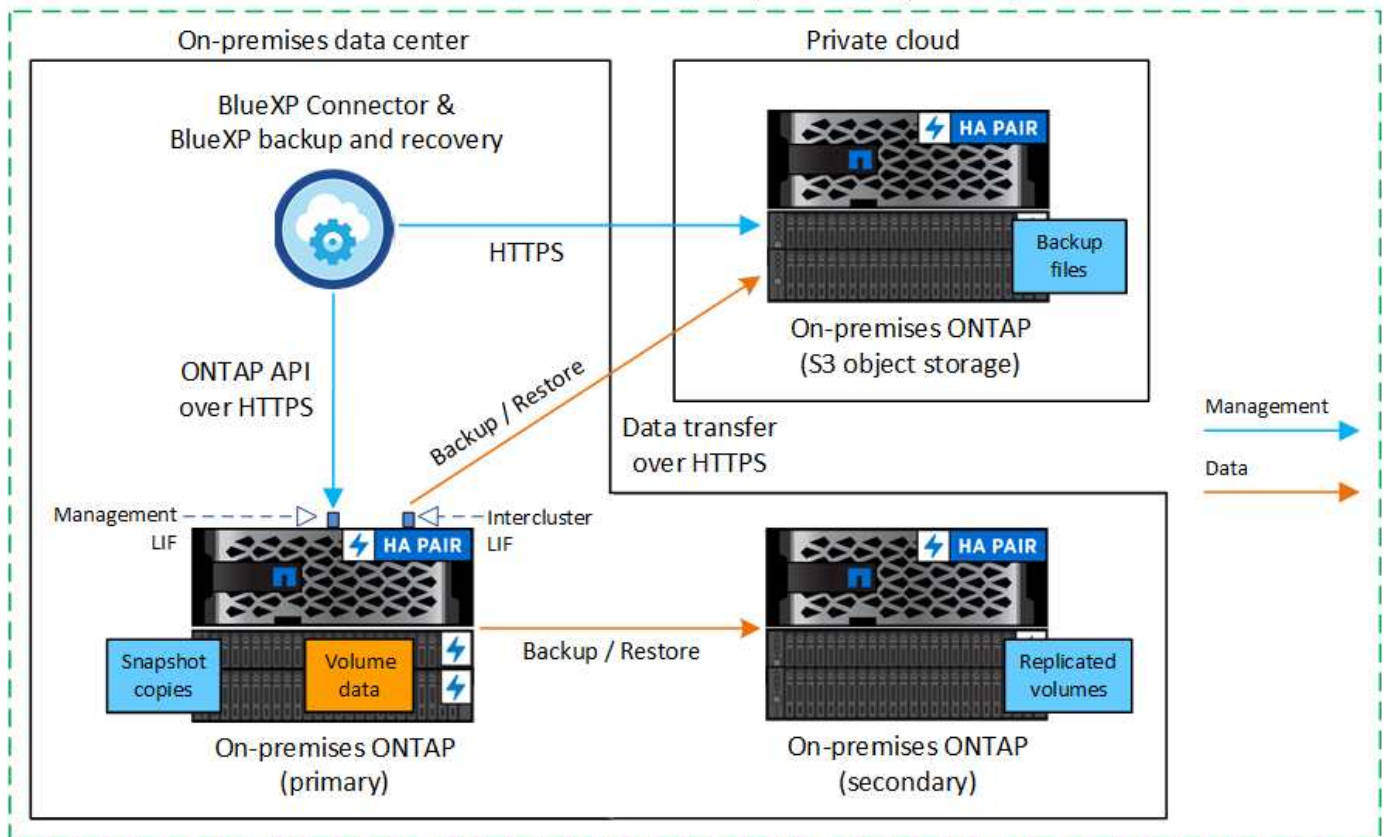
[Active backups en sus ONTAP Volumes.](#)

## Identifique el método de conexión

Existen muchas configuraciones en las que puede crear backups en un bloque de S3 en un sistema ONTAP. A continuación se muestran dos escenarios.

La siguiente imagen muestra cada componente cuando se realiza un backup de un sistema ONTAP principal en las instalaciones en un sistema ONTAP en las instalaciones configurado para S3 y las conexiones que necesita preparar entre ellos. También muestra una conexión con un sistema de ONTAP secundario en la misma ubicación local para replicar volúmenes.

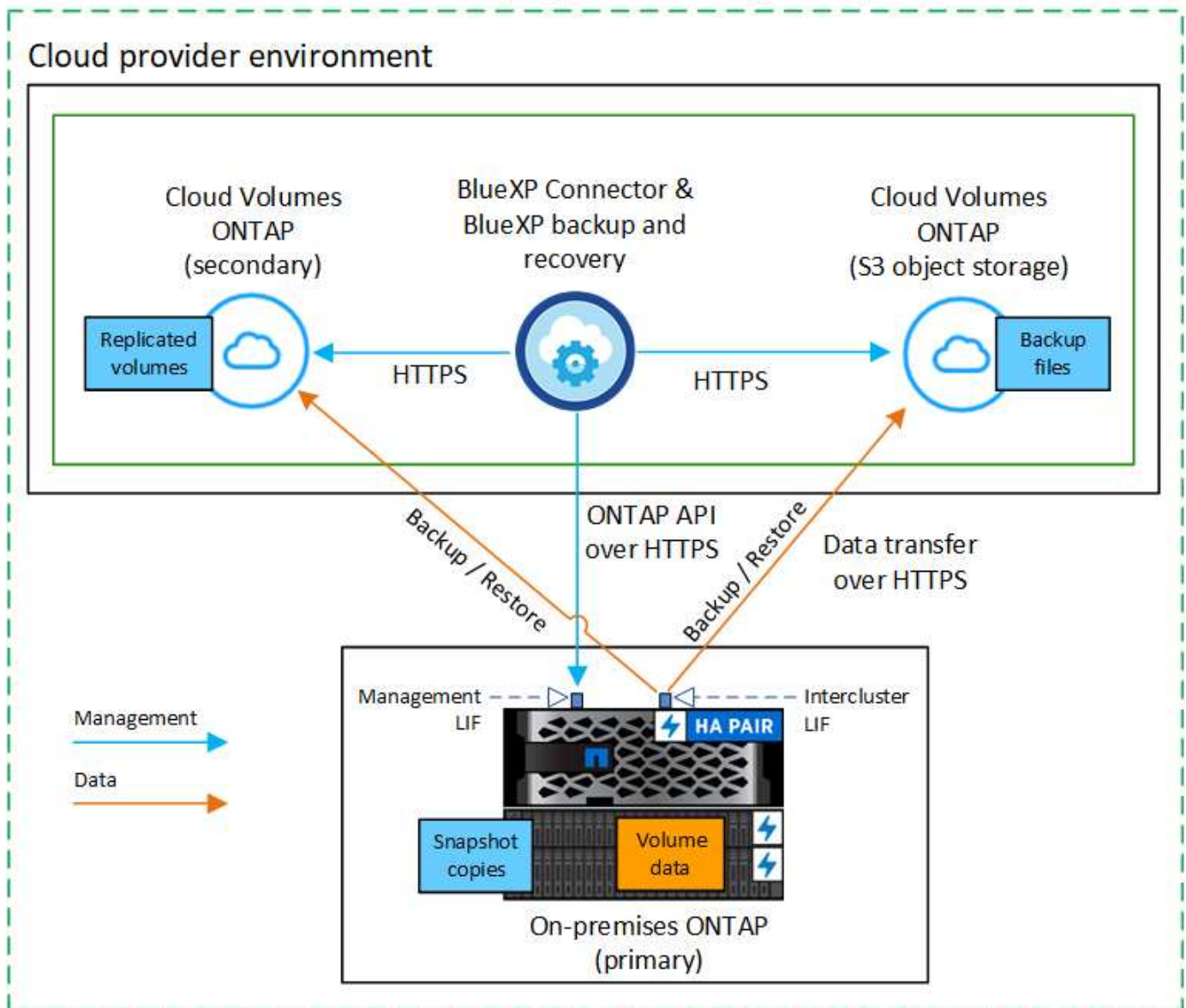
## Connector installed on-premises (Public)



Cuando el conector y el sistema principal de ONTAP en las instalaciones se instalan en una ubicación en las instalaciones sin acceso a Internet (una puesta en marcha en modo «privado»), el sistema ONTAP S3 debe estar ubicado en el mismo centro de datos en las instalaciones.

La siguiente imagen muestra cada componente cuando se realiza un backup de un sistema ONTAP principal en las instalaciones en un sistema Cloud Volumes ONTAP configurado para S3 y las conexiones que necesita preparar entre ellos. También muestra una conexión con un sistema Cloud Volumes ONTAP secundario en el mismo entorno de proveedor de cloud para replicar volúmenes.

## Connector deployed in cloud (Public)



En este escenario, el conector debe ponerse en marcha en el mismo entorno de proveedor de cloud en el que se despliegan los sistemas Cloud Volumes ONTAP.

## Prepare el conector BlueXP

El conector BlueXP es el software principal para la funcionalidad BlueXP. Se necesita un conector para realizar una copia de seguridad y restaurar los datos de ONTAP.

### Cree o cambie conectores

Cuando realiza el backup de los datos en ONTAP S3, debe haber un conector BlueXP disponible en las instalaciones o en el cloud. Deberá instalar un nuevo conector o asegurarse de que el conector seleccionado actualmente se encuentra en una de estas ubicaciones. El conector local se puede instalar en un sitio con o sin acceso a Internet.

- ["Más información sobre conectores"](#)

- ["Instale el conector en su entorno de nube"](#)
- ["Instalación del conector en un host Linux con acceso a Internet"](#)
- ["Instalación del conector en un host Linux sin acceso a Internet"](#)
- ["Cambio entre conectores"](#)

## Prepare los requisitos de red del conector

Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:

- Una conexión HTTPS a través del puerto 443 al servidor ONTAP S3
- Una conexión HTTPS por el puerto 443 a la LIF de gestión del clúster de ONTAP de origen
- Una conexión a Internet saliente a través del puerto 443 para backup y recuperación de BlueXP (no es necesaria si Connector está instalado en un sitio «oscuro»).

## Consideraciones sobre el modo privado (sitio oscuro)

La funcionalidad de backup y recuperación de BlueXP está integrada en BlueXP Connector. Cuando se instala en modo privado, deberá actualizar el software Connector periódicamente para obtener acceso a nuevas funciones. Compruebe la ["Backup y recuperación de BlueXP Novedades"](#) Para ver las nuevas funciones de cada versión de backup y recuperación de BlueXP. Cuando desee utilizar las nuevas funciones, siga los pasos a. ["Actualice el software del conector"](#).

Al utilizar el backup y la recuperación de BlueXP en un entorno SaaS estándar, los datos de configuración de backup y recuperación de BlueXP se realizan en el cloud. Al utilizar el backup y la recuperación de BlueXP en un sitio sin acceso a Internet, los datos de configuración de backup y recuperación de BlueXP se copian en el bloque ONTAP S3, donde se almacenan los backups. Si alguna vez tiene un fallo de conector en su sitio de modo privado, puede hacerlo ["Restaura los datos de backup y recuperación de BlueXP en un nuevo conector"](#).

## Verifique los requisitos de licencia

Antes de poder activar el backup y la recuperación de BlueXP para tu clúster, tendrás que comprar y activar una licencia BYOL de backup y recuperación de BlueXP de NetApp. La licencia se realiza para backup y restauración en el almacenamiento de objetos. No se necesita licencia para crear copias de Snapshot ni volúmenes replicados. Esta licencia es para la cuenta y puede utilizarse en varios sistemas.

Necesitará el número de serie de NetApp que le permita utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).



Las licencias PAYGO no se admiten al realizar copias de seguridad de archivos en ONTAP S3.

## Prepare los clústeres ONTAP

Tendrá que preparar su sistema ONTAP de origen en las instalaciones y cualquier sistema ONTAP o Cloud Volumes ONTAP secundario en las instalaciones.

La preparación de los clústeres de ONTAP implica los siguientes pasos:

- Descubra tus sistemas de ONTAP en BlueXP
- Compruebe los requisitos del sistema ONTAP



- Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos
- Compruebe los requisitos de red de ONTAP para replicar volúmenes

## Descubre tus sistemas de ONTAP en BlueXP

Tanto su sistema ONTAP de origen en las instalaciones como todos los sistemas ONTAP o Cloud Volumes ONTAP secundarios en las instalaciones deben estar disponibles en BlueXP Canvas.

Tendrá que conocer la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster.

["Aprenda a detectar un clúster"](#).

## Compruebe los requisitos del sistema ONTAP

Asegúrese de que se cumplen los siguientes requisitos de ONTAP:

- Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.
- Una licencia de SnapMirror (incluida como parte del paquete Premium o del paquete de protección de datos).

**Nota:** El "paquete de nube híbrida" no es necesario cuando se utiliza la copia de seguridad y recuperación de BlueXP.

Aprenda cómo ["gestione las licencias de clúster"](#).

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["configure la hora del clúster"](#).
- Si va a replicar datos, debe comprobar que los sistemas de origen y de destino ejecutan versiones de ONTAP compatibles antes de replicar datos.

["Consulte versiones de ONTAP compatibles para relaciones de SnapMirror"](#).

## Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos

Debe asegurarse de que se cumplen los siguientes requisitos en el sistema que se conecta al almacenamiento de objetos.



- Si se utiliza una arquitectura de backup ramificada, los ajustes deben configurarse en el sistema de almacenamiento *primary*.
- Cuando se utiliza una arquitectura de backup en cascada, los ajustes deben configurarse en el sistema de almacenamiento *secondary*.

["Obtenga más información sobre los tipos de arquitectura de backup"](#).

Se necesitan los siguientes requisitos de red de clúster de ONTAP:

- El clúster de ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario desde la LIF entre clústeres hasta el servidor ONTAP S3 para realizar operaciones de backup y restauración. El puerto se puede configurar durante la configuración de copia de seguridad.

ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos

nunca se inicia, solo responde.

- ONTAP requiere una conexión entrante desde el conector hasta la LIF de administración del clúster.
- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos. ["Obtenga más información acerca de los espacios IP"](#).

Al configurar el backup y la recuperación de BlueXP, se le pedirá que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

- Las LIF de interconexión de clústeres de los nodos pueden acceder al almacén de objetos (no es necesario cuando se instala el conector en un sitio «oscuro»).
- Los servidores DNS se configuraron para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Descubra cómo ["Configure los servicios DNS para la SVM"](#).
- Si utiliza un espacio IP diferente al predeterminado, es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones del servicio de backup y recuperación de BlueXP desde ONTAP al almacenamiento de objetos a través del puerto que especificó (normalmente con el puerto 443) y el tráfico de resolución de nombres de la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.

## Prepare ONTAP S3 como destino de backup

Debe habilitar un servidor de almacenamiento de objetos de servicio simple de almacenamiento (S3) en el clúster de ONTAP que vaya a usar para backups de almacenamiento de objetos. Consulte ["Documentación de ONTAP S3"](#) para obtener más detalles.

**Nota:** Puedes descubrir este clúster en BlueXP Canvas, pero no se identifica como un servidor de almacenamiento de objetos S3, y no puedes arrastrar y soltar un entorno de trabajo de origen en este entorno



de trabajo S3 para iniciar la activación de la copia de seguridad.

Este sistema ONTAP debe cumplir los siguientes requisitos.

### Versiones de ONTAP compatibles

Se requiere ONTAP 9,8 y versiones posteriores para sistemas ONTAP on-premises.

Se requiere ONTAP 9.9.1 y versiones posteriores para los sistemas Cloud Volumes ONTAP.

### Credenciales de S3

Debe haber creado un usuario S3 para controlar el acceso a su almacenamiento ONTAP S3. ["Consulte los documentos de ONTAP S3 para obtener más información"](#).

Cuando configura un backup en ONTAP S3, el asistente de backup le solicita una clave de acceso S3 y una clave secreta para una cuenta de usuario. La cuenta de usuario permite el backup y la recuperación de BlueXP para autenticar y acceder a los bloques de ONTAP S3 que se utilizan para almacenar backups. Las claves son necesarias para que ONTAP S3 sepa quién está haciendo la solicitud.

Estas claves de acceso deben estar asociadas a un usuario que tenga los siguientes permisos:

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- Seleccione los volúmenes de los que desea realizar el backup
- Defina la estrategia y las políticas de backup
- Revise las selecciones

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.
  - Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, seleccione la opción **Acciones (...)** y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tenga activada la replicación o la copia de seguridad en el almacenamiento de objetos).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas

locales, las replicaciones y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:

- Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
- Si no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

## Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el backup para volúmenes adicionales en el entorno de trabajo"](#) (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.

- Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
- Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
- Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).

2. Seleccione **Siguiente**.

## Defina la estrategia de backup

La definición de la estrategia de backup implica la configuración de las siguientes opciones:

- Opciones de protección: Si desea implementar una o todas las opciones de backup: Snapshots locales, replicación y backup en almacenamiento de objetos
- Arquitectura: Si desea utilizar una arquitectura de backup de dispersión o en cascada
- Política de Snapshot local
- Objetivo y política de replicación
- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir Estrategia de Copia de Seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Crea copias instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Copia de seguridad:** Realiza copias de seguridad de los volúmenes en un depósito en un sistema ONTAP configurado para S3.
2. **Arquitectura:** Si elige tanto la replicación como la copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** Los datos de respaldo fluyen del sistema primario al secundario, y luego del almacenamiento secundario al de objetos.
  - **Fan Out:** Los datos de respaldo fluyen del sistema primario al secundario y del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una nueva.



Si desea crear una política personalizada antes de activar la Snapshot, puede usar System Manager o la CLI de ONTAP `snapmirror policy create` comando. Consulte.



Para crear una política personalizada utilizando este servicio antes de activar la instantánea, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
  - Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
  - Seleccione **Crear**.
4. **Replicación:** Si seleccionaste **Replicación**, establece las siguientes opciones:
    - **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado de destino (o agregados para volúmenes de FlexGroup) y un prefijo o sufijo que se añadirá al nombre del volumen replicado.
    - **Política de replicación:** Elija una política de replicación existente o cree una nueva.

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:
  - **Proveedor:** Selecciona **ONTAP S3**.
  - **Configuración del proveedor:** Ingrese los detalles del FQDN del servidor S3, el puerto y la clave de acceso y la clave secreta de los usuarios.

La clave de acceso y la clave secreta se aplican al usuario que se creó para otorgar al clúster de

ONTAP acceso al bloque de S3.

- **\* Redes\*:** Elija el espacio IP en el clúster ONTAP de origen donde residen los volúmenes de los que desea realizar la copia de seguridad. Las LIF entre clústeres de este espacio IP deben tener acceso saliente a Internet (no es necesario cuando el conector se instala en un sitio «oscuro»).



Al seleccionar el espacio IP correcto, se garantiza que el backup y la recuperación de BlueXP puedan configurar una conexión desde ONTAP a su almacenamiento de objetos de ONTAP S3.

- **Política de copia de seguridad:** Seleccione una política de copia de seguridad existente o cree una nueva.



Puede crear una política con System Manager o la CLI de ONTAP. Para crear una política personalizada mediante la CLI de ONTAP `snapmirror policy create` consulte.



Para crear una política personalizada antes de activar el backup con la interfaz de usuario de, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte ["Configuración de políticas de backup en objeto"](#).
- Seleccione **Crear**.
- **Exporte las copias Snapshot existentes al almacenamiento de objetos como archivos de copia de seguridad:** Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar (por ejemplo, diaria, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.

6. Seleccione **Siguiente**.

## Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup. Si las políticas no coinciden, no se crearán backups.
3. Seleccione **Activar copia de seguridad**.

## Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos del almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen de almacenamiento principal.

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta que ha introducido, y los archivos de copia de seguridad se almacenan allí.

La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

### **Muestra los comandos de la API**

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

#### **Pasos**

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

### **El futuro**

- Puede hacerlo ["gestione los archivos de copia de seguridad y las políticas de copia de seguridad"](#). Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo ["gestione la configuración de backup en el nivel del clúster"](#). Esto incluye cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo ["restaure volúmenes, carpetas o archivos individuales desde un archivo de backup"](#) En un sistema ONTAP en las instalaciones.

## **Realice una copia de seguridad de los datos locales de ONTAP en StorageGRID con la copia de seguridad y recuperación de BlueXP**

Complete algunos pasos en la copia de seguridad y recuperación de BlueXP para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP locales primarios a un sistema de almacenamiento secundario y al almacenamiento de objetos en sus sistemas NetApp StorageGRID.



Entre los «sistemas ONTAP en las instalaciones» se incluyen los sistemas FAS, AFF y ONTAP Select.

## Inicio rápido

Comience rápidamente siguiendo estos pasos. En las siguientes secciones del tema se proporcionan detalles sobre cada paso.

1

### Identifica el método de conexión que usarás

Revise cómo conectará su clúster local de ONTAP directamente a StorageGRID a través de la Internet pública, o si utilizará una VPN y enrutará el tráfico a través de una interfaz privada de punto final de VPC a StorageGRID.

[Identifique el método de conexión.](#)

2

### Prepare el conector BlueXP

Si ya tiene un conector puesto en marcha en sus instalaciones, entonces está todo listo. De lo contrario, tendrás que crear un conector BlueXP para realizar backups de los datos de ONTAP en StorageGRID. También tendrá que personalizar la configuración de red del conector para que pueda conectarse a StorageGRID.

[Aprenda a crear un conector y a definir la configuración de red necesaria.](#)

3

### Verifique los requisitos de licencia

Tendrás que comprobar los requisitos de licencias tanto para StorageGRID como para BlueXP.

Consulte [Verifique los requisitos de licencia.](#)

4

### Prepare los clústeres ONTAP

Detecta tus clústeres de ONTAP en BlueXP, comprueba que los clústeres cumplan con los requisitos mínimos y personaliza la configuración de red para que los clústeres se puedan conectar a StorageGRID.

[Descubra cómo preparar sus clústeres de ONTAP.](#)

5

### Preparar StorageGRID como destino de backup

Configure los permisos para que Connector cree y gestione el bucket de StorageGRID. También necesitará configurar permisos para el clúster de ONTAP en las instalaciones para que pueda leer y escribir datos en el bloque.

De manera opcional, puede configurar sus propias claves gestionadas personalizadas para el cifrado de datos, en lugar de tener que usar las claves de cifrado de StorageGRID predeterminadas. [Descubra cómo preparar su entorno de StorageGRID para recibir backups de ONTAP.](#)

6

### Active backups en sus ONTAP Volumes

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

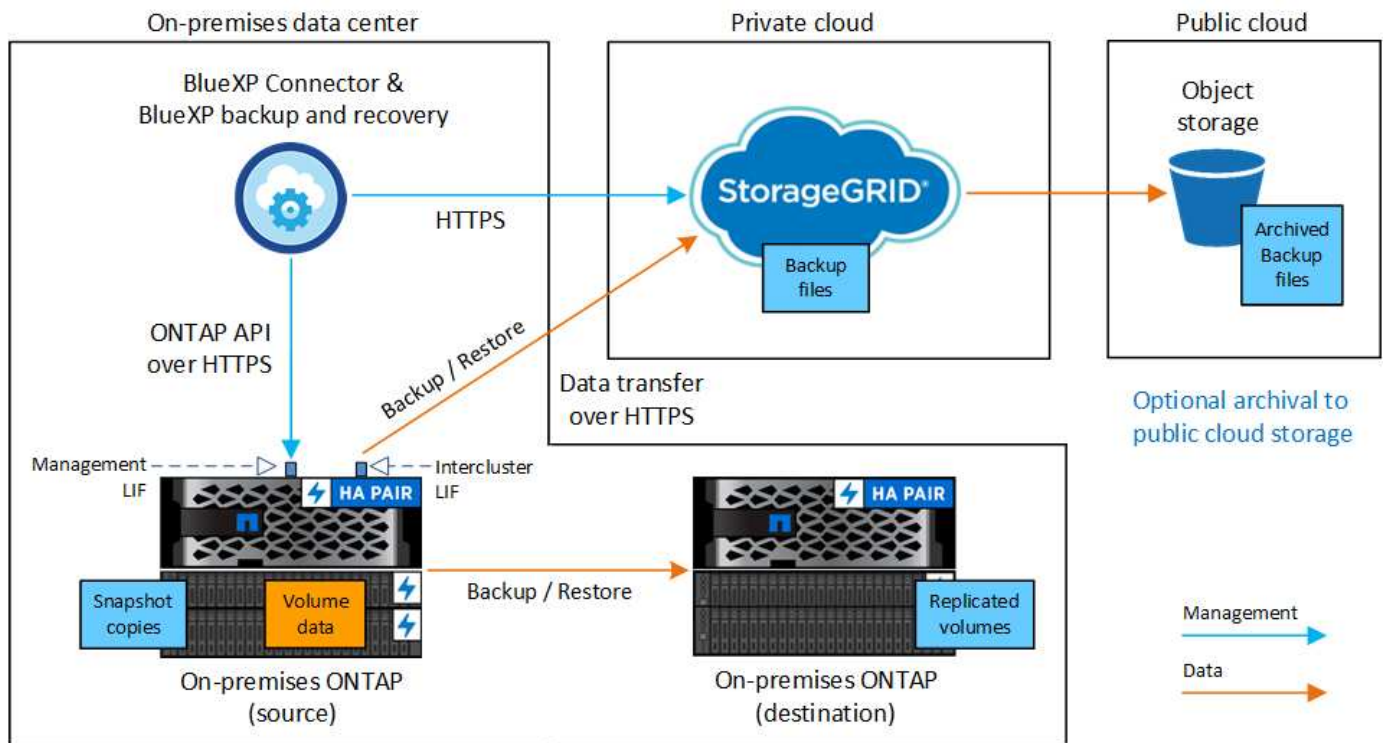
seleccionar las políticas de replicación y backup que usará y los volúmenes de los que desea realizar un backup.

[Active backups en sus ONTAP Volumes.](#)

## Identifique el método de conexión

La siguiente imagen muestra cada componente cuando se realiza un backup de un sistema ONTAP local en StorageGRID y las conexiones necesarias para preparar entre ellos.

Opcionalmente, se puede conectar a un sistema ONTAP secundario en la misma ubicación local para replicar volúmenes.



Cuando el conector y el sistema ONTAP en las instalaciones se instalan en una ubicación en las instalaciones sin acceso a Internet (un «sitio oscuro»), el sistema StorageGRID debe estar ubicado en el mismo centro de datos en las instalaciones. No se admite el archivado de archivos de backup antiguos en el cloud público en configuraciones de sitios oscuros.

## Prepare el conector BlueXP

El conector BlueXP es el software principal para la funcionalidad BlueXP. Se necesita un conector para realizar una copia de seguridad y restaurar los datos de ONTAP.

### Cree o cambie conectores

Cuando haces backups de los datos en StorageGRID, debe haber un conector BlueXP disponible en las instalaciones. Deberá instalar un nuevo conector o asegurarse de que el conector seleccionado actualmente reside en las instalaciones. El conector se puede instalar en un sitio con o sin acceso a Internet.

- ["Más información sobre conectores"](#)
- ["Instalación del conector en un host Linux con acceso a Internet"](#)



- ["Instalación del conector en un host Linux sin acceso a Internet"](#)
- ["Cambio entre conectores"](#)

## Prepare los requisitos de red del conector

Asegúrese de que la red en la que está instalado el conector habilita las siguientes conexiones:

- Una conexión HTTPS a través del puerto 443 al nodo de puerta de enlace StorageGRID
- Una conexión HTTPS a través del puerto 443 para la LIF de gestión del clúster ONTAP
- Una conexión a Internet saliente a través del puerto 443 para backup y recuperación de BlueXP (no es necesaria si Connector está instalado en un sitio «oscuro»).

## Consideraciones sobre el modo privado (sitio oscuro)

- La funcionalidad de backup y recuperación de BlueXP está integrada en BlueXP Connector. Cuando se instala en modo privado, deberá actualizar el software Connector periódicamente para obtener acceso a nuevas funciones. Compruebe la ["Backup y recuperación de BlueXP Novedades"](#) Para ver las nuevas funciones de cada versión de backup y recuperación de BlueXP. Cuando desee utilizar las nuevas funciones, siga los pasos a. ["Actualice el software del conector"](#).

La nueva versión de backup y recuperación de datos de BlueXP, que incluye la capacidad de programar y crear copias de Snapshot y volúmenes replicados, además de crear backups en el almacenamiento de objetos, requiere que esté utilizando la versión 3.9.31 o superior de BlueXP Connector. Por lo tanto, se recomienda que obtenga esta última versión para gestionar todos sus backups.

- Cuando utilizas backup y recuperación de BlueXP en un entorno SaaS, se realiza un backup de los datos de configuración de backup y recuperación de BlueXP en el cloud. Al utilizar el backup y la recuperación de BlueXP en un sitio sin acceso a Internet, los datos de configuración de backup y recuperación de BlueXP se copian en el bloque de StorageGRID, donde se almacenan los backups. Si alguna vez tiene un fallo de conector en su sitio de modo privado, puede hacerlo ["Restaura los datos de backup y recuperación de BlueXP en un nuevo conector"](#).

## Verifique los requisitos de licencia

Antes de poder activar el backup y la recuperación de BlueXP para tu clúster, tendrás que comprar y activar una licencia BYOL de backup y recuperación de BlueXP de NetApp. Esta licencia es para la cuenta y puede utilizarse en varios sistemas.

Necesitará el número de serie de NetApp que le permita utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#).



No se admite la licencia de PAYGO cuando se realiza una copia de seguridad de archivos en StorageGRID.

## Prepare los clústeres ONTAP

Tendrá que preparar su sistema ONTAP de origen en las instalaciones y cualquier sistema ONTAP o Cloud Volumes ONTAP secundario en las instalaciones.

La preparación de los clústeres de ONTAP implica los siguientes pasos:

- Descubre tus sistemas de ONTAP en BlueXP



- Compruebe los requisitos del sistema ONTAP
- Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos
- Compruebe los requisitos de red de ONTAP para replicar volúmenes

## Descubre tus sistemas de ONTAP en BlueXP

Tanto su sistema ONTAP de origen en las instalaciones como todos los sistemas ONTAP o Cloud Volumes ONTAP secundarios en las instalaciones deben estar disponibles en BlueXP Canvas.

Tendrá que conocer la dirección IP de gestión del clúster y la contraseña de la cuenta de usuario administrador para añadir el clúster.

["Aprenda a detectar un clúster"](#).

## Compruebe los requisitos del sistema ONTAP

Asegúrese de que se cumplen los siguientes requisitos de ONTAP:

- Se recomienda un mínimo de ONTAP 9,8; ONTAP 9.8P13 y posterior.
- Una licencia de SnapMirror (incluida como parte del paquete Premium o del paquete de protección de datos).

**Nota:** El “paquete de nube híbrida” no es necesario cuando se utiliza la copia de seguridad y recuperación de BlueXP.

Aprenda cómo ["gestione las licencias de clúster"](#).

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["configure la hora del clúster"](#).
- Si va a replicar datos, debe comprobar que los sistemas de origen y de destino ejecutan versiones de ONTAP compatibles antes de replicar datos.

["Consulte versiones de ONTAP compatibles para relaciones de SnapMirror"](#).

## Comprobar los requisitos de red de ONTAP para realizar backup de los datos en el almacenamiento de objetos

Debe configurar los siguientes requisitos en el sistema que se conecta al almacenamiento de objetos.

- Si utiliza una arquitectura de backup ramificada, los siguientes ajustes deben configurarse en el sistema de almacenamiento *primary*.
- Cuando se utiliza una arquitectura de copia de seguridad en cascada, los siguientes ajustes deben configurarse en el sistema de almacenamiento *secondary*.

Se necesitan los siguientes requisitos de red de clúster de ONTAP:

- El clúster de ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario desde la LIF del interconexión de clústeres al nodo de puerta de enlace StorageGRID para las operaciones de backup y restauración. El puerto se puede configurar durante la configuración de copia de seguridad.

ONTAP lee y escribe datos en y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, solo responde.

- ONTAP requiere una conexión entrante desde el conector hasta la LIF de administración del clúster. El conector debe residir en sus instalaciones.
- Se requiere una LIF de interconexión de clústeres en cada nodo ONTAP donde se alojan los volúmenes en los que se desea incluir. La LIF debe estar asociada al *IPspace* que ONTAP debería utilizar para conectarse al almacenamiento de objetos. ["Obtenga más información acerca de los espacios IP"](#).

Al configurar el backup y la recuperación de BlueXP, se le pedirá que utilice el espacio IP. Debe elegir el espacio IP al que está asociada cada LIF. Puede ser el espacio IP «predeterminado» o un espacio IP personalizado que haya creado.

- Las LIF de interconexión de clústeres de los nodos pueden acceder al almacén de objetos (no es necesario cuando se instala el conector en un sitio «oscuro»).
- Los servidores DNS se configuraron para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Descubra cómo ["Configure los servicios DNS para la SVM"](#).
- Si utiliza un espacio IP diferente al predeterminado, es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones del servicio de backup y recuperación de BlueXP desde ONTAP al almacenamiento de objetos a través del puerto que especificó (normalmente con el puerto 443) y el tráfico de resolución de nombres de la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).

## Compruebe los requisitos de red de ONTAP para replicar volúmenes

Si planeas crear volúmenes replicados en un sistema ONTAP secundario mediante el backup y la recuperación de datos de BlueXP, asegúrese de que los sistemas de origen y destino cumplan los siguientes requisitos de red.

### Requisitos de red de ONTAP en las instalaciones

- Si el clúster se encuentra en sus instalaciones, debe tener una conexión entre la red corporativa y la red virtual en el proveedor de cloud. Normalmente se trata de una conexión VPN.
- Los clústeres de ONTAP deben cumplir con requisitos adicionales de subred, puerto, firewall y clúster.

Al poder replicar en Cloud Volumes ONTAP o en sistemas en las instalaciones, revise los requisitos de los pares de los sistemas de ONTAP en las instalaciones. ["Ver requisitos previos para la relación de clústeres entre iguales en la documentación de ONTAP"](#).

### Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida necesarias: Específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas se incluyen en el grupo de seguridad predefinido.

## Preparar StorageGRID como destino de backup

StorageGRID debe cumplir con los siguientes requisitos. Consulte ["Documentación de StorageGRID"](#) si quiere más información.

Para obtener más información sobre los requisitos de bloqueo de datos y protección contra ransomware para StorageGRID, consulte ["Opciones de políticas de backup en objeto"](#).

## Versiones de StorageGRID compatibles

Se admite StorageGRID 10.3 y versiones posteriores.

Para usar la protección DataLock & Ransomware para sus copias de seguridad, sus sistemas StorageGRID deben ejecutar la versión 11.6.0.3 o posterior.

Para organizar los backups antiguos en niveles en el almacenamiento de archivado en cloud, los sistemas StorageGRID deben ejecutar la versión 11.3 o posterior. Además, debes descubrir tus sistemas StorageGRID en BlueXP Canvas.

Para el almacenamiento de archivos del usuario, se necesita acceso a la IP del nodo de administrador.

Siempre es necesario el acceso a IP de puerta de enlace.

## Credenciales de S3

Debe haber creado una cuenta de inquilino de S3 para controlar el acceso al almacenamiento de StorageGRID. ["Consulte los documentos de StorageGRID para obtener más información"](#).

Al configurar un backup en StorageGRID, el asistente de backup le solicita una clave de acceso de S3 y una clave secreta para una cuenta de inquilino. La cuenta de inquilino permite el backup y la recuperación de BlueXP para autenticar y acceder a los bloques de StorageGRID que se utilizan para almacenar backups. Las claves son necesarias para que StorageGRID sepa quién está haciendo la solicitud.

Estas claves de acceso deben estar asociadas a un usuario que tenga los siguientes permisos:

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

## Control de versiones de objetos

No debe habilitar manualmente el control de versiones de objetos StorageGRID en el bloque de almacenamiento de objetos.

## Prepárese para archivar archivos de backup antiguos en almacenamiento en cloud público

Organizar en niveles los archivos de backup antiguos en el almacenamiento de archivado ahorra dinero al utilizar un tipo de almacenamiento más económico para backups que quizás no necesite. StorageGRID es una solución en las instalaciones (cloud privado) que no ofrece almacenamiento de archivado, pero puede mover archivos de backup antiguos a un almacenamiento de archivado en el cloud público. Cuando se utilizan de esta forma, los datos organizados en niveles en el almacenamiento cloud o restaurados a partir del almacenamiento en cloud pasan entre StorageGRID y el almacenamiento cloud - BlueXP no está implicado en esta transferencia de datos.

El soporte actual le permite archivar backups en el almacenamiento AWS S3 *Glacier*/S3 *Glacier Deep Archive* o *Azure Archive*.

## Requisitos de ONTAP

- El clúster debe utilizar ONTAP 9.12.1 o superior.

### Requisitos de StorageGRID

- Su StorageGRID debe utilizar 11,4 o superior.
- Su StorageGRID debe estar ["Descubierto y disponible en BlueXP Canvas"](#).

### Requisitos de Amazon S3

- Tendrá que registrarse en una cuenta de Amazon S3 para conocer el espacio de almacenamiento donde se ubicarán sus backups archivados.
- Puede elegir entre organizar los backups en niveles en el almacenamiento de AWS S3 Glacier o S3 Glacier Deep Archive. ["Obtenga más información acerca de los niveles de archivado de AWS"](#).
- StorageGRID debe tener acceso de control total al cucharón (s3: \*); sin embargo, si esto no es posible, la directiva bucket debe conceder los siguientes permisos S3 a StorageGRID:
  - s3:AbortMultipartUpload
  - s3:DeleteObject
  - s3:GetObject
  - s3:ListBucket
  - s3:ListBucketMultipartUploads
  - s3:ListMultipartUploadParts
  - s3:PutObject
  - s3:RestoreObject

### Requisitos de Azure Blob

- Tendrá que inscribirse en una suscripción de Azure para disfrutar del espacio de almacenamiento donde se ubicar los backups archivados.
- El asistente de activación permite utilizar un grupo de recursos existente para administrar el contenedor Blob que almacenará las copias de seguridad o crear un nuevo grupo de recursos.

A la hora de definir la configuración de archivado para la política de backup del clúster, debe introducir las credenciales del proveedor de cloud y seleccionar la clase de almacenamiento que desea utilizar. El backup y la recuperación de datos de BlueXP crea el bloque de cloud cuando activas el backup para el clúster. A continuación se muestra la información necesaria para el almacenamiento de archivado de AWS y Azure.

| AWS                                                                                             | Azure                                                                                             |
|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Tier Backups to Archive<br>Cloud Provider<br><div>AWS</div> | <input checked="" type="checkbox"/> Tier Backups to Archive<br>Cloud Provider<br><div>AZURE</div> |
| Account<br><div>Select Account</div>                                                            | Azure Subscription<br><div>Select Account</div>                                                   |
| Region<br><div>Select Region</div>                                                              | Region<br><div>Select Region</div>                                                                |
| AWS Access Key<br><div>Enter AWS Access Key</div>                                               | Resource Group Type<br><div>Select an Existing Resource Group</div>                               |
| AWS Secret Key<br><div>Enter AWS Secret Key</div>                                               | Resource Group<br><div>Select Resource Group</div>                                                |
| Archive After (Days)<br><div>(1-999)</div>                                                      | Archive After (Days)<br><div>(1-999)</div>                                                        |
| Storage Class<br><div>S3 Glacier</div>                                                          | Storage Class<br><div>Azure Archive</div>                                                         |

La configuración de la política de archivado que seleccione generará una política de gestión del ciclo de vida de la información (ILM) en StorageGRID y añadirá la configuración como "reglas".

- Si ya existe una política activa de ILM, se añadirán nuevas reglas a la política de ILM para mover los datos al nivel de archivado.
- Si ya existe una política de ILM en el estado "propuesta", no será posible la creación y activación de una nueva política de ILM. ["Obtenga más información acerca de las reglas y políticas de ILM de StorageGRID"](#).

## Active backups en sus ONTAP Volumes

Active los backups en cualquier momento directamente desde su entorno de trabajo local.

Un asistente le llevará por los siguientes pasos principales:

- [Seleccione los volúmenes de los que desea realizar el backup](#)
- [Defina la estrategia de backup](#)
- [Revise las selecciones](#)

También puede hacerlo [Muestra los comandos de la API](#) en el paso de revisión, puede copiar el código para automatizar la activación de la copia de seguridad para entornos de trabajo futuros.

### Inicie el asistente

#### Pasos

1. Acceda al asistente Activar copia de seguridad y recuperación de una de las siguientes maneras:
  - En el lienzo de BlueXP, selecciona el entorno de trabajo y selecciona **Habilitar > Volúmenes de copia de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.
  - Si el destino de sus backups existe como entorno de trabajo en el Canvas, puede arrastrar el clúster de ONTAP al almacenamiento de objetos.
  - Seleccione **Volúmenes** en la barra Copia de seguridad y recuperación. En la pestaña Volúmenes, seleccione la opción **Acciones (...)** y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tenga la replicación o copia de seguridad en el almacenamiento de objetos ya habilitados).

La página Introducción del asistente muestra las opciones de protección, incluidas las instantáneas locales, la replicación y las copias de seguridad. Si realizó la segunda opción en este paso, aparecerá la

página Definir estrategia de copia de seguridad con un volumen seleccionado.

2. Continúe con las siguientes opciones:

- Si ya tienes un conector BlueXP, ya lo tendrás todo. Solo tienes que seleccionar **Siguiente**.
- Si aún no tienes un conector BlueXP, aparece la opción **Add a Connector**. Consulte [Prepare el conector BlueXP](#).

## Seleccione los volúmenes de los que desea realizar el backup

Elija los volúmenes que desea proteger. Un volumen protegido es uno que tiene uno o varios de los siguientes: Política de Snapshot, política de replicación, backup en política de objetos.

Puede optar por proteger los volúmenes de FlexVol o FlexGroup; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar el backup para un entorno de trabajo. Descubra cómo ["active el backup para volúmenes adicionales en el entorno de trabajo"](#) (FlexVol o FlexGroup) después de configurar el backup de los volúmenes iniciales.



- Puede activar un backup solo en un único volumen de FlexGroup a la vez.
- Los volúmenes que seleccione deben tener la misma configuración de SnapLock. Todos los volúmenes deben tener SnapLock Enterprise habilitado o SnapLock deshabilitado.

## Pasos

Tenga en cuenta que si los volúmenes que elija ya tienen aplicadas políticas de Snapshot o de replicación, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Select Volumes, seleccione el o los volúmenes que desea proteger.

- Opcionalmente, filtre las filas para mostrar solo los volúmenes con ciertos tipos de volumen, estilos y más para facilitar la selección.
- Después de seleccionar el primer volumen, puede seleccionar All FlexVol Volumes (los volúmenes de FlexGroup se pueden seleccionar de uno por vez solo). Para realizar un backup de todos los volúmenes FlexVol existentes, active primero un volumen y, a continuación, marque la casilla en la fila del título. (☒ Volume Name).
- Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume\_1).

2. Seleccione **Siguiente**.

## Defina la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Tanto si desea una como todas las opciones de backup: Copias Snapshot locales, replicación y backup en el almacenamiento de objetos
- Arquitectura
- Política de Snapshot local
- Objetivo y política de replicación



Si los volúmenes seleccionados tienen distintas políticas de Snapshot y de replicación a las políticas seleccionadas en este paso, se sobrescribirán las políticas existentes.

- Backup en la información de almacenamiento de objetos (proveedor, cifrado, conexión a redes, política de backup y opciones de exportación).

## Pasos

1. En la página Definir estrategia de copia de seguridad, seleccione una o todas las siguientes opciones. Los tres están seleccionados de forma predeterminada:
  - **Instantáneas locales:** Si está realizando una replicación o una copia de seguridad en el almacenamiento de objetos, se deben crear instantáneas locales.
  - **Replicación:** Crea volúmenes replicados en otro sistema de almacenamiento ONTAP.
  - **Backup:** Realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si elige tanto la replicación como la copia de seguridad, elija uno de los siguientes flujos de información:
  - **Cascading:** La información fluye desde el primario al secundario, y luego desde el secundario al almacenamiento de objetos.
  - **Fan Out:** La información fluye del primario al secundario *and* del almacenamiento primario al objeto.

Para obtener información detallada sobre estas arquitecturas, consulte ["Planifica tu proceso de protección"](#).

3. **Instantánea local:** Elija una política de Snapshot existente o cree una nueva.



Para crear una política personalizada antes de activar la instantánea, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

4. **Replicación:** Establezca las siguientes opciones:

- **Objetivo de replicación:** Seleccione el entorno de trabajo de destino y SVM. De manera opcional, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregará al nombre del volumen replicado.
- **Política de replicación:** Elija una política de replicación existente o cree una.



Para crear una política personalizada antes de activar la replicación, consulte ["Crear una política"](#).

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.

5. **Copia de seguridad en Object:** Si seleccionaste **Copia de seguridad**, establece las siguientes opciones:

- **Proveedor:** Selecciona **StorageGRID**.
- **Configuración del proveedor:** Ingrese los detalles FQDN del nodo de la puerta de enlace del

proveedor, el puerto, la clave de acceso y la clave secreta.

La clave de acceso y la clave secreta son las del usuario de IAM que se creó para otorgar al clúster de ONTAP acceso al bloque.

- **\* Redes\***: Elija el espacio IP en el clúster de ONTAP donde residen los volúmenes de los que desea realizar una copia de seguridad. Las LIF entre clústeres de este espacio IP deben tener acceso saliente a Internet (no es necesario cuando el conector se instala en un sitio «oscuro»).



Al seleccionar el espacio IP correcto, se garantiza que el backup y la recuperación de BlueXP puedan configurar una conexión desde ONTAP a tu almacenamiento de objetos de StorageGRID.

- **Política de copia de seguridad**: Seleccione una política existente de copia de seguridad para almacenamiento de objetos o cree una.



Para crear una política personalizada antes de activar el backup, consulte "[Crear una política](#)".

Para crear una política, selecciona **Crear nueva política** y haz lo siguiente:

- Introduzca el nombre de la política.
- Seleccione hasta 5 horarios, normalmente de diferentes frecuencias.
- En el caso de políticas de backup a objeto, se deben establecer los ajustes de DataLock y Ransomware Protection. Para obtener más información sobre DataLock y Protección contra ransomware, consulte "[Configuración de políticas de backup en objeto](#)".

Si su clúster utiliza ONTAP 9.11.1 o superior, puede optar por proteger sus backups de ataques de eliminación y ransomware configurando *DataLock* y *Protección de ransomware*. *DataLock* protege sus archivos de copia de seguridad de ser modificados o eliminados, y *Ransomware Protection* analiza sus archivos de copia de seguridad para buscar pruebas de un ataque de ransomware en sus archivos de copia de seguridad.

- Seleccione **Crear**.

Si el clúster utiliza ONTAP 9.12.1 o posterior y el sistema StorageGRID utiliza la versión 11.4 o posterior, puede optar por organizar en niveles los backups antiguos en niveles de archivado en cloud público después de un determinado número de días. Actualmente es compatible con los niveles de almacenamiento de AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. [Vea cómo configurar sus sistemas para esta funcionalidad](#).

- **Copia de seguridad de nivel en la nube pública**: Seleccione el proveedor de nube al que desea organizar las copias de seguridad en niveles e introduzca los detalles del proveedor.

Seleccione o cree un clúster de StorageGRID nuevo. Para obtener más detalles sobre la creación de un clúster de StorageGRID para que BlueXP pueda detectarlo, consulte "[Documentación de StorageGRID](#)".

- **Exporte las copias Snapshot existentes al almacenamiento de objetos como copias de seguridad**: Si hay alguna copia Snapshot local para volúmenes en este entorno de trabajo que coincida con la etiqueta de programación de copia de seguridad que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que se copien todas las copias Snapshot históricas en el almacenamiento de objetos como archivos de backup a fin de garantizar la protección más completa de los volúmenes.



## 6. Seleccione **Siguiente**.

### Revise las selecciones

Esta es la oportunidad de revisar sus selecciones y hacer ajustes, si es necesario.

#### Pasos

1. En la página Review, revise las selecciones.
2. Opcionalmente marque la casilla para **sincronizar automáticamente las etiquetas de la política de Snapshot con las etiquetas de la política de replicación y copia de seguridad**. De este modo, se crea Snapshot con una etiqueta que coincide con las etiquetas de las políticas de replicación y backup.
3. Seleccione **Activar copia de seguridad**.

#### Resultado

El backup y la recuperación de datos de BlueXP comienzan a realizar los backups iniciales de tus volúmenes. La transferencia básica del volumen replicado y el archivo de backup incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos del almacenamiento primario contenidos en las copias Snapshot.

Se crea un volumen replicado en el clúster de destino que se sincronizará con el volumen de almacenamiento principal.

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta que ha introducido, y los archivos de copia de seguridad se almacenan allí.

La consola de backup de volumen se muestra para poder supervisar el estado de los backups.

También es posible supervisar el estado de los trabajos de backup y restauración mediante la ["Panel de control de trabajos"](#).

### Muestra los comandos de la API

Puede ser conveniente mostrar y copiar, opcionalmente, los comandos API que se utilizan en el asistente Activar backup y recuperación. Se recomienda hacer esto para automatizar la activación del backup en entornos de trabajo futuros.

#### Pasos

1. En el asistente Activar copia de seguridad y recuperación, seleccione **Ver solicitud de API**.
2. Para copiar los comandos en el portapapeles, seleccione el icono **Copiar**.

### El futuro

- Puede hacerlo ["gestione los archivos de copia de seguridad y las políticas de copia de seguridad"](#). Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copia de seguridad, etc.
- Puede hacerlo ["gestione la configuración de backup en el nivel del clúster"](#). Esto incluye cambiar el ancho de banda de red disponible para cargar backups en el almacenamiento de objetos, cambiar la configuración de backup automático para volúmenes futuros, etc.
- También puede hacerlo ["restaure volúmenes, carpetas o archivos individuales desde un archivo de backup"](#) En un sistema ONTAP en las instalaciones.

# Migre volúmenes usando SnapMirror a Cloud Resync con respaldo y recuperación de BlueXP

La función SnapMirror to Cloud Resync en la copia de seguridad y recuperación de BlueXP optimiza la protección y la continuidad de los datos durante las migraciones de volumen en entornos NetApp. Cuando se migra un volumen con la replicación lógica de SnapMirror (LRSE), desde una puesta en marcha de NetApp en las instalaciones a otra o a una solución basada en el cloud, como Cloud Volumes ONTAP o Cloud Volumes Service, SnapMirror a Cloud Resync garantiza que los backups existentes en el cloud permanecen intactos y operativos.

Esta función elimina la necesidad de una operación de nueva base que requiere mucho tiempo y requiere muchos recursos, lo que permite que las operaciones de backup continúen tras la migración. Esta función es muy útil en escenarios de migración de cargas de trabajo, compatible tanto con FlexVols como con FlexGroups y está disponible a partir de la versión 9.16.1 de ONTAP.

Al mantener la continuidad del backup entre entornos, SnapMirror a Cloud Resync mejora la eficiencia operativa y reduce la complejidad de la gestión de datos híbrida y multicloud.

## Funcionamiento del backup y recuperación de datos SnapMirror de BlueXP para la resincronización en el cloud

Si completa una actualización técnica o migra volúmenes de un clúster de ONTAP a otro, es importante que los backups sigan funcionando sin interrupciones. El backup y recuperación de datos de BlueXP SnapMirror to Cloud Resync ayuda a hacerlo al garantizar que los backups en la nube permanecen consistentes incluso después de una migración de volumen.

Veamos un ejemplo:

Imagine que tiene un volumen en las instalaciones llamado Vol1a. Este volumen tiene tres copias de Snapshot: S1, S2 y S3. Estas copias Snapshot son como puntos de restauración. Ya se está haciendo un backup de VOL1 en un extremo de almacén de objetos de cloud mediante SnapMirror en el cloud (SM-C). Sin embargo, hasta el momento, solo se han realizado backups de S1 y S2 en un almacén de objetos.

Ahora se desea migrar VOL1 a otro clúster de ONTAP. Para ello, crea una relación de replicación lógica de SnapMirror (LRSE) con un nuevo volumen de cloud denominado Vol1b. Esto transfiere las tres copias Snapshot (S1, S2 y S3) de Vol1a a Vol1b.

Una vez finalizada la migración, tendrá la siguiente configuración:

- Se elimina la relación SM-C original (almacén de objetos de Vol1a →).
- La relación LRSE (Vol1a → Vol1b) también se elimina.
- Vol1b ahora es su volumen activo.

Llegado a este punto, quiere seguir realizando un backup de Vol1b en el mismo extremo de cloud. Sin embargo, en lugar de empezar un backup completo desde cero (que requeriría tiempo y recursos), usas SnapMirror para la resincronización de cloud.

Así es como funciona la resincronización:

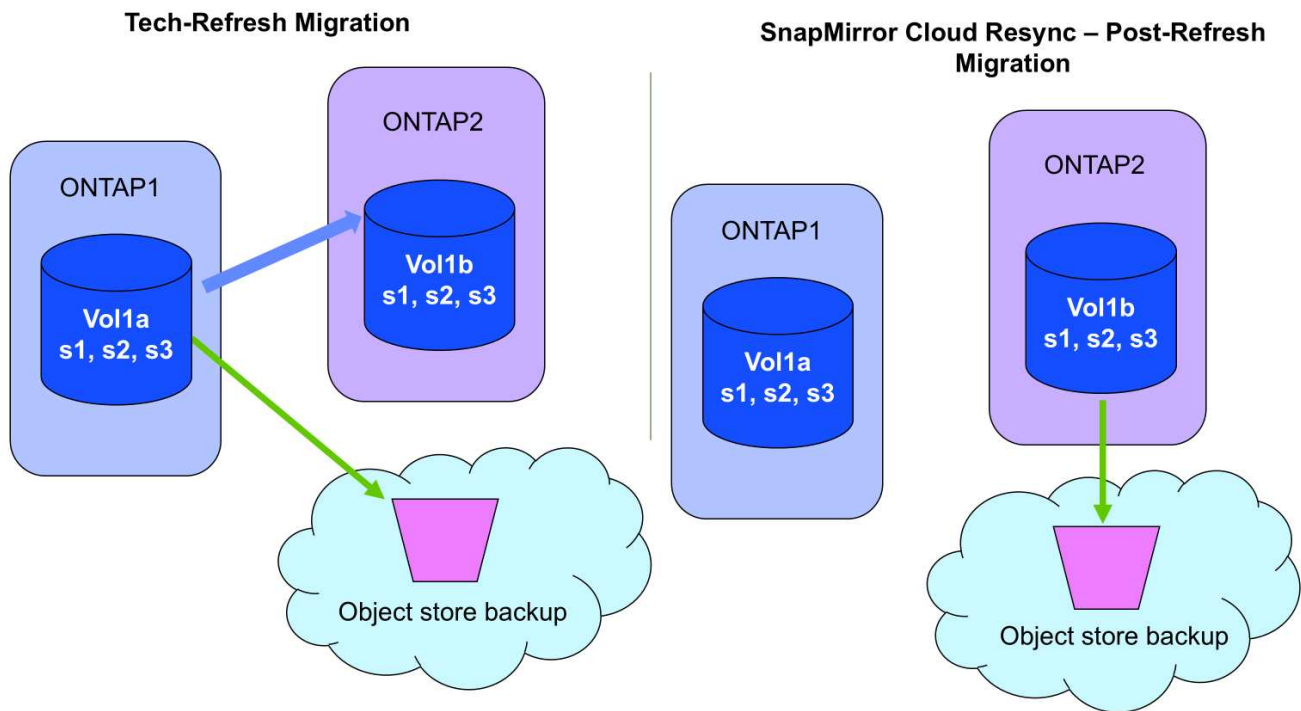
- El sistema comprueba si hay una snapshot común entre Vol1a y el almacén de objetos. En este caso,

ambos tienen S2.

- Debido a esta instantánea compartida, el sistema solo necesita transferir los cambios incrementales entre S2 y S3.

Esto significa que solo se añaden los nuevos datos después de que S2 se envía al almacén de objetos, no al volumen completo.

Este proceso evita volver a enviar datos de los que ya se ha realizado una copia de seguridad, ahorra ancho de banda y garantiza que la cadena de copia de seguridad continúe sin problemas después de la migración.



NetApp

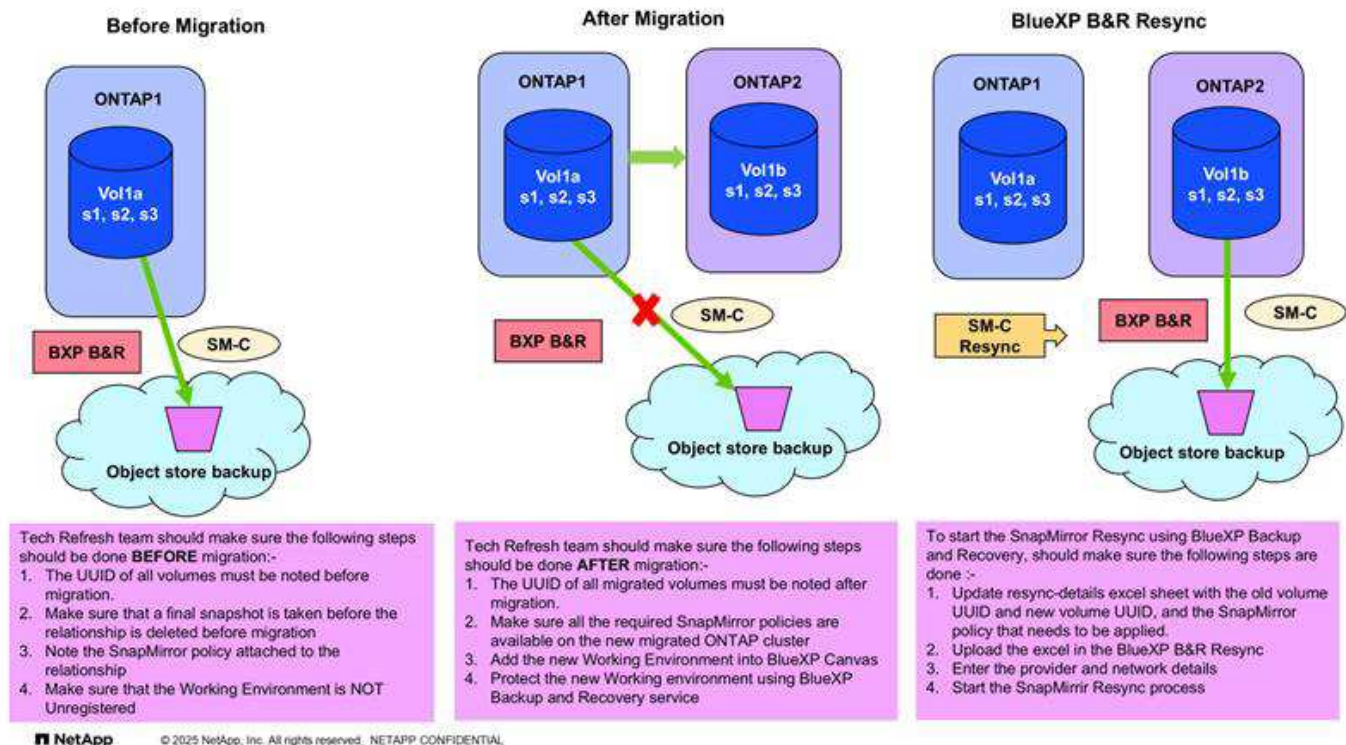
## Notas de procedimiento

- El clúster de ONTAP de destino debe ejecutar ONTAP versión 9.16.1 o posterior.
- El clúster de ONTAP de origen anterior debe protegerse mediante backup y recuperación de datos de BlueXP.
- Las migraciones y las actualizaciones tecnológicas no se realizan con el backup y la recuperación de datos de BlueXP. Las debe llevar a cabo un equipo de servicios profesionales o un administrador de almacenamiento cualificado.
- Un equipo de migración de NetApp es responsable de crear la relación de SnapMirror entre los clústeres de ONTAP de origen y de destino para facilitar la migración de volúmenes.
- Comprobar que la migración durante una actualización tecnológica se basa en la migración basada en SnapMirror.
- Actualmente no se admiten la resincronización de SnapMirror a cloud después de las migraciones con los métodos SVM-Migrate, SVM-DR o Head Swap.

## Cómo migrar volúmenes mediante SnapMirror para resincronizar con la nube

La migración de volúmenes mediante SnapMirror a la resincronización en el cloud implica los siguientes pasos principales, cada uno de los cuales se describe con más detalle a continuación:

- **Siga una lista de comprobación previa a la migración:** Antes de iniciar la migración, un equipo de actualización tecnológica de NetApp garantiza que se cumplan los siguientes requisitos previos para evitar la pérdida de datos y garantizar un proceso de migración sin problemas.
- **Siga una lista de comprobación posterior a la migración:** Después de la migración, un equipo de actualización técnica de NetApp se asegura de que se completen los siguientes pasos para establecer la protección y prepararse para la resincronización.
- **Realiza una resincronización de SnapMirror a la nube:** Después de la migración, un equipo de Actualización de tecnología de NetApp realiza una operación de resincronización de SnapMirror a la nube para reanudar las copias de seguridad en la nube de los volúmenes recién migrados.



### Siga una lista de comprobación previa a la migración

Antes de iniciar la migración, un equipo de actualización tecnológica de NetApp se encarga de cumplir los siguientes requisitos previos para evitar la pérdida de datos y garantizar que el proceso de migración se realice sin problemas.

1. Asegúrese de que todos los volúmenes que se vayan a migrar estén protegidos mediante el backup y la recuperación de datos de BlueXP .
2. Registre los UUID de instancia del volumen. Escriba los UUID de instancia de todos los volúmenes antes de iniciar la migración. Estos identificadores son cruciales para las operaciones de asignación y resincronización más adelante.
3. Realice una snapshot final de cada volumen para conservar el estado más reciente antes de eliminar ninguna relación de SnapMirror.

4. Documentar las políticas de SnapMirror. Registre la política de SnapMirror actualmente adjunta a la relación de cada volumen. Esto lo necesitará más adelante durante el proceso de resincronización del SnapMirror al cloud.
5. Elimine las relaciones de cloud de SnapMirror con el almacén de objetos.
6. Cree una relación estándar de SnapMirror con el nuevo clúster de ONTAP para migrar el volumen al nuevo clúster de ONTAP de destino.

### Siga una lista de comprobación posterior a la migración

Después de la migración, un equipo de actualización tecnológica de NetApp se asegura de que se completen los pasos siguientes para establecer la protección y prepararse para la resincronización.

1. Registre nuevos UUID de instancia de volumen de todos los volúmenes migrados en el clúster de ONTAP de destino.
2. Confirmar que todas las políticas de SnapMirror necesarias disponibles en el clúster de ONTAP antiguo se han configurado correctamente en el nuevo clúster de ONTAP.
3. Agregue el nuevo clúster de ONTAP como entorno de trabajo en el lienzo de BlueXP .

### Realiza una resincronización de SnapMirror a Cloud

Después de la migración, un equipo de actualización tecnológica de NetApp ejecuta una operación de resincronización de SnapMirror al cloud para reanudar los backups en el cloud de los volúmenes recién migrados.

1. Agregue el nuevo clúster de ONTAP como entorno de trabajo en el lienzo de BlueXP .
2. Consulte la página Volúmenes de copia de seguridad y recuperación de BlueXP para asegurarse de que los detalles del entorno de trabajo de origen antiguo están disponibles.
3. En la página Volúmenes de copia de seguridad y recuperación de BlueXP , selecciona **Configuración de copia de seguridad**.
4. En el menú, seleccione **Resync backup**.
5. En la página Resync Working Environment, realice lo siguiente:
  - a. **Nuevo entorno de trabajo de origen:** Entra en el nuevo cluster ONTAP donde se han migrado los volúmenes.
  - b. **Almacén de objetos objetivo existente:** Seleccione el almacén de objetos objetivo que contiene las copias de seguridad del antiguo entorno de trabajo de origen.
6. Seleccione **Descargar plantilla CSV** para descargar la hoja de Excel Detalles de Resync. Utilice esta hoja para introducir los detalles de los volúmenes que se migrarán. En el archivo CSV, introduzca los siguientes detalles:
  - El UUID de la instancia de volumen antiguo del clúster de origen
  - El UUID de instancia de volumen nuevo del clúster de destino
  - La política de SnapMirror que se aplicará a la nueva relación.
7. Seleccione **Cargar** en **Cargar detalles de asignación de volumen** para cargar la hoja CSV completada en la interfaz de usuario de copia de seguridad y recuperación de BlueXP .
8. Introduzca la información de configuración del proveedor y de red necesaria para la operación de resincronización.
9. Seleccione **Enviar** para iniciar el proceso de validación.

El backup y la recuperación de datos de BlueXP validan que cada volumen seleccionado para la resincronización tiene al menos una Snapshot común. Esto garantiza que los volúmenes estén listos para la operación de resincronización de SnapMirror en el cloud.

10. Revise los resultados de validación, incluidos los nombres de los volúmenes de origen nuevos y el estado de resincronización de cada volumen.
11. Compruebe la idoneidad del volumen. El sistema comprueba si los volúmenes son aptos para la resincronización. Si un volumen no es elegible, significa que no se encontró ninguna instantánea común.



Para garantizar que los volúmenes sigan siendo aptos para la operación de resincronización de SnapMirror a cloud, cree una snapshot final de cada volumen antes de eliminar cualquier relación de SnapMirror durante la fase previa a la migración. Esto conserva el estado más reciente de los datos.

12. Seleccione **Resync** para iniciar la operación de resincronización. El sistema utiliza la instantánea común para transferir solo los cambios incrementales, garantizando la continuidad de la copia de seguridad.
13. Supervise el proceso resyn en la página Monitor de trabajos.

## Administre copias de seguridad de sus sistemas ONTAP con BlueXP Backup and Recovery

Con la copia de seguridad y recuperación de BlueXP, administre las copias de seguridad de sus Cloud Volumes ONTAP y los sistemas ONTAP locales cambiando el programa de copia de seguridad, habilitando o deshabilitando las copias de seguridad de volúmenes, pausando las copias de seguridad, eliminando las copias de seguridad y más. Esto incluye todos los tipos de backups, incluidas las copias Snapshot, los volúmenes replicados y los archivos de backup en el almacenamiento de objetos.



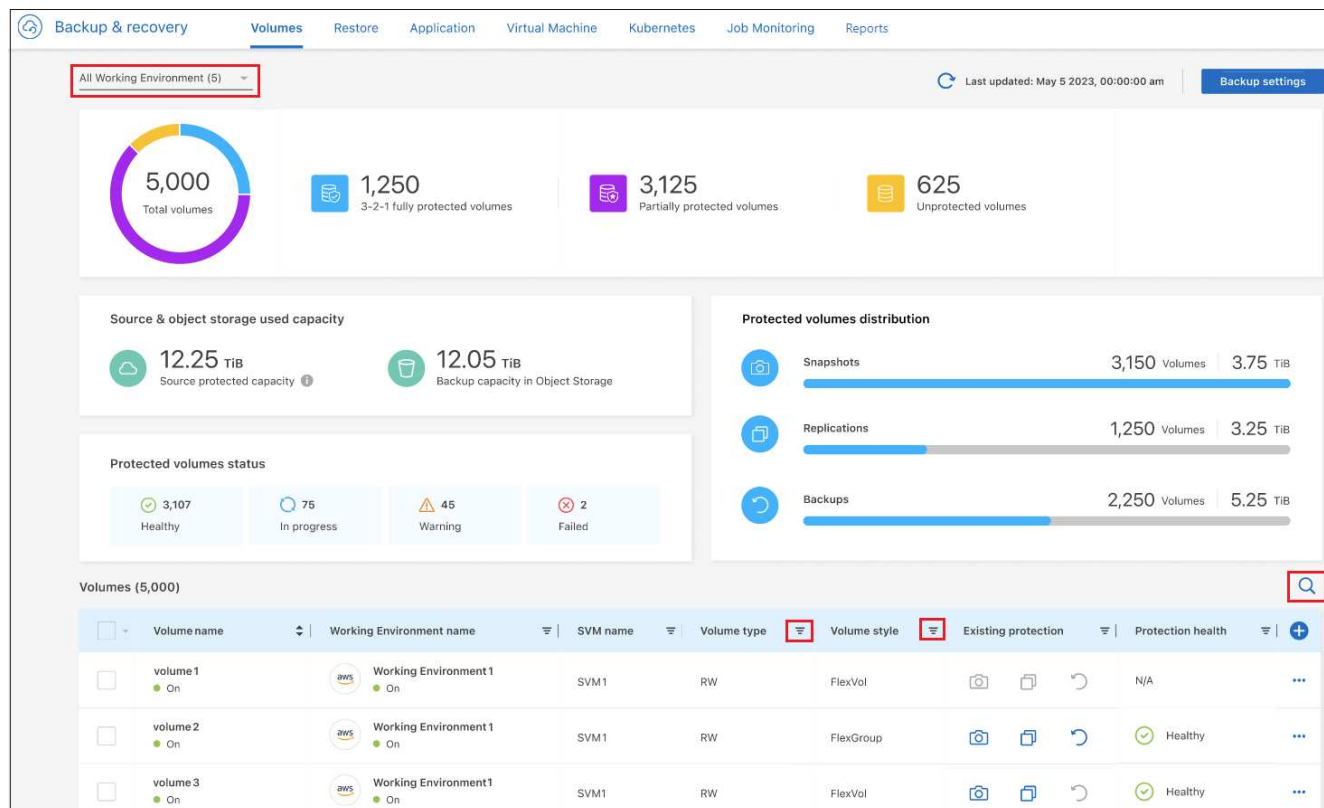
No gestione ni modifique los archivos de backup directamente en sus sistemas de almacenamiento ni desde su entorno de proveedor de cloud. Esto puede dañar los archivos y dar como resultado una configuración no compatible.

### Vea el estado de backup de los volúmenes en sus entornos de trabajo

Es posible ver una lista de todos los volúmenes de los que se están respaldando en la consola de backup de volúmenes. Esto incluye todos los tipos de backups, incluidas las copias Snapshot, los volúmenes replicados y los archivos de backup en el almacenamiento de objetos. También puede ver los volúmenes en aquellos entornos de trabajo de los que no se esté realizando un backup actualmente.

#### Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la pestaña **Volúmenes** para ver la lista de los volúmenes de los que se ha realizado una copia de seguridad de sus sistemas Cloud Volumes ONTAP y ONTAP locales.



- Si está buscando volúmenes específicos en determinados entornos de trabajo, puede refinar la lista por entorno de trabajo y volumen. También puede usar el filtro de búsqueda u ordenar las columnas según el estilo de volumen (FlexVol o FlexGroup), tipo de volumen y más.

Para mostrar columnas adicionales (agregados, estilo de seguridad (Windows o UNIX), política de Snapshot, política de replicación y política de backup), seleccione .

- Revise el estado de las opciones de protección en la columna Protección existente. Los 3 iconos significan «copias Snapshot locales», «volúmenes replicados» y «backups en almacenamiento de objetos».



Cada icono es azul cuando ese tipo de copia de seguridad está activado, y es gris cuando el tipo de copia de seguridad está inactivo. Es posible pasar el cursor sobre cada icono para ver la política de backup que se está utilizando, así como otra información pertinente de cada tipo de backup.

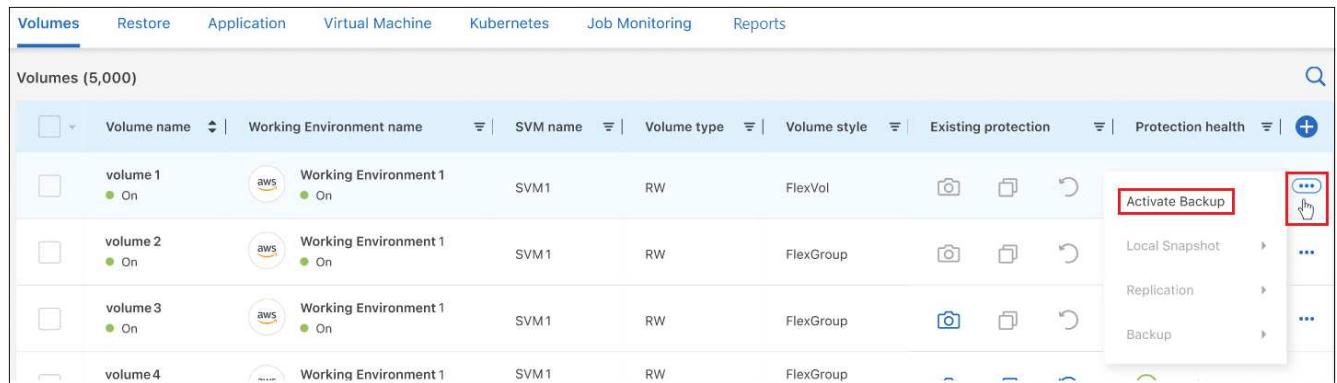
## Activar backup en volúmenes adicionales en un entorno de trabajo

Si activaste el backup solo en algunos de los volúmenes de un entorno de trabajo cuando habilitaste el backup y la recuperación de BlueXP por primera vez, puedes activar backups en volúmenes adicionales más adelante.

### Pasos

- En la pestaña **Volúmenes**, identifique el volumen en el que desea activar las copias de seguridad, seleccione el menú Acciones  Al final de la fila, y seleccione **Activar copia de seguridad**.





- En la página *Definir estrategia de backup*, seleccione la arquitectura de backup y, a continuación, defina las políticas y otros detalles para Local Snapshot copies, los volúmenes replicados y los archivos de backup. Consulte los detalles de las opciones de backup en los volúmenes iniciales que activó en este entorno de trabajo. A continuación, haga clic en **Siguiente**.
- Revise la configuración de copia de seguridad de este volumen y luego haga clic en **Activar copia de seguridad**.

Si desea activar el backup en varios volúmenes al mismo tiempo con configuraciones de backup idénticas, consulte [Editar la configuración de backup en varios volúmenes](#) para obtener más detalles.

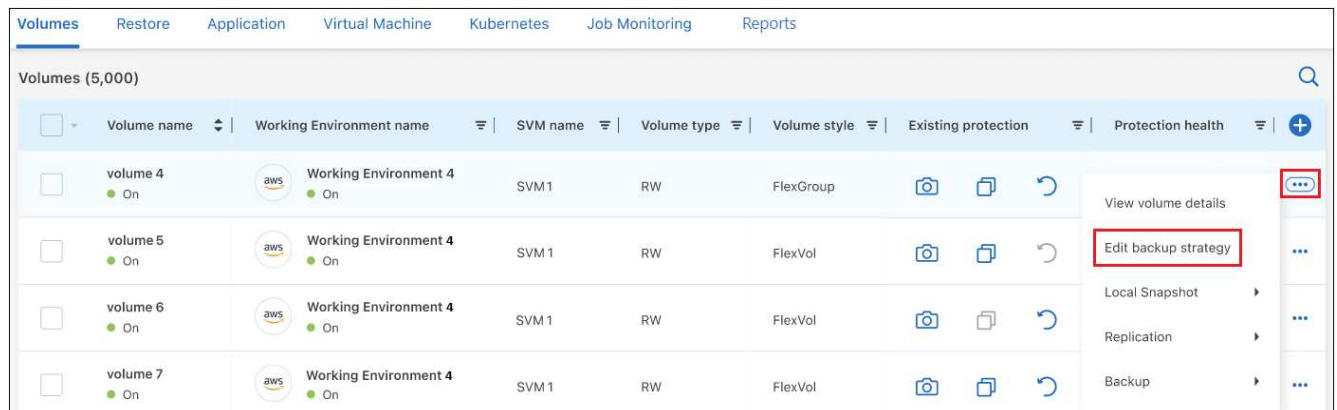
## Cambie la configuración de backup asignada a los volúmenes existentes

Es posible cambiar las políticas de backup asignadas a los volúmenes existentes que tienen políticas asignadas. Puede cambiar las políticas de sus copias snapshot locales, volúmenes replicados y archivos de backup. Cualquier nueva política de Snapshot, replicación o backup que desee aplicar a los volúmenes debe existir ya.

### Edite la configuración de backup en un único volumen

#### Pasos

- En la pestaña **Volúmenes**, identifique el volumen que desea realizar cambios en la política, seleccione el menú Acciones **...** Al final de la fila, y seleccione **Editar estrategia de copia de seguridad**.



- En la página *Editar estrategia de copia de seguridad*, realice cambios en las políticas de copia de seguridad existentes para copias Snapshot locales, volúmenes replicados y archivos de copia de seguridad y haga clic en **Siguiente**.

Si habilitó *DataLock* y *Ransomware Protection* para backups en el cloud en la política de backup inicial al



activar el backup y la recuperación de BlueXP para este clúster, solo verá otras políticas que se hayan configurado con DataLock. Y si no activaste *DataLock* y *Ransomware Protection* al activar el backup y la recuperación de BlueXP, solo verá otras políticas de backup en la nube que no tengan DataLock configurado.

- 3. Revise la configuración de copia de seguridad de este volumen y luego haga clic en **Activar copia de seguridad**.

**Editar la configuración de backup en varios volúmenes**

Si desea usar la misma configuración de backup en varios volúmenes, puede activar o editar la configuración de backup en varios volúmenes al mismo tiempo. Puede seleccionar volúmenes que no tengan configuración de backup, solo configuración de Snapshot, solo backup en configuración de cloud, etc., y realizar cambios masivos en todos esos volúmenes con configuraciones de backup diversas.

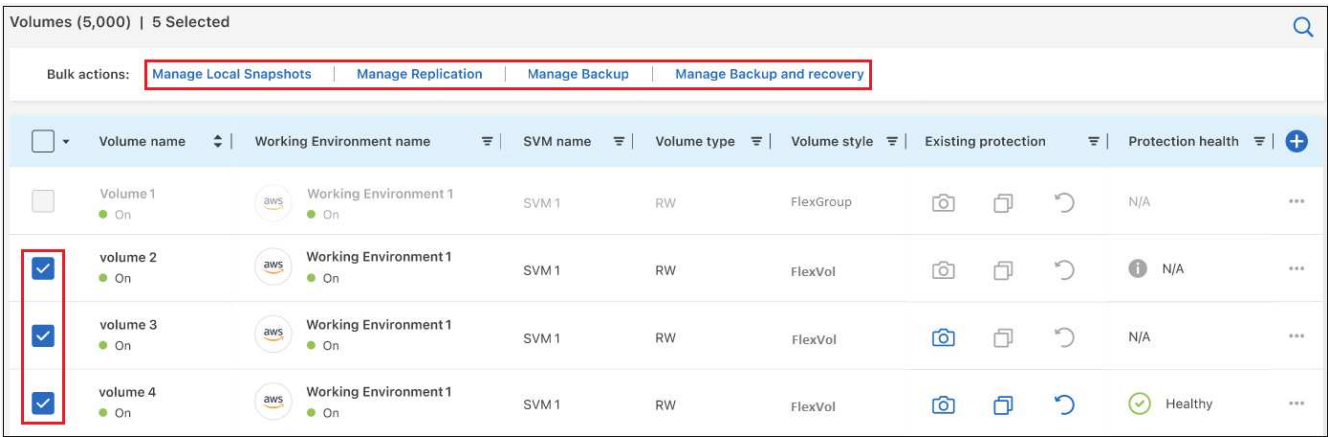
Al trabajar con varios volúmenes, todos los volúmenes deben tener las siguientes características comunes:

- el mismo entorno de trabajo
- Mismo estilo (volumen de FlexVol o FlexGroup)
- Mismo tipo (volumen de lectura-escritura o protección de datos)

Cuando se habilitan más de cinco volúmenes para el backup, el backup y recuperación de datos de BlueXP inicializa únicamente cinco volúmenes a la vez. Una vez finalizados, crea el siguiente lote de cinco subtrabajos para iniciar el siguiente conjunto y continúa hasta que se inicializan todos los volúmenes.

**Pasos**

- 1. Desde la pestaña **Volúmenes**, filtra por el entorno de trabajo en el que residen los volúmenes.
- 2. Seleccione todos los volúmenes en los cuales desea gestionar la configuración de backup.
- 3. En función del tipo de acción de copia de seguridad que desee configurar, haga clic en el botón del menú Acciones masivas:



| Acción de copia de seguridad...                                 | Haga clic en este botón...         |
|-----------------------------------------------------------------|------------------------------------|
| Gestionar la configuración de backup de Snapshot                | Administrar instantáneas locales   |
| Gestionar la configuración de copia de seguridad de replicación | Administrar Replicación            |
| Gestione la configuración de backup en el cloud                 | * Administrar copia de seguridad * |

| Acción de copia de seguridad...                                                                                                              | Haga clic en este botón...                        |
|----------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Gestionar varios tipos de configuración de copia de seguridad. Esta opción también le permite cambiar la arquitectura de copia de seguridad. | * Administrar copia de seguridad y recuperación * |

- En la página de copia de seguridad que aparece, realice cambios en las políticas de copia de seguridad existentes para copias Snapshot locales, volúmenes replicados o archivos de copia de seguridad y haga clic en **Guardar**.

Si habilitó *DataLock* y *Ransomware Protection* para backups en el cloud en la política de backup inicial al activar el backup y la recuperación de BlueXP para este clúster, solo verá otras políticas que se hayan configurado con DataLock. Y si no activaste *DataLock* y *Ransomware Protection* al activar el backup y la recuperación de BlueXP, solo verás otras políticas de backup en la nube que no tengan DataLock configurado.

## Crear un backup manual de volúmenes en cualquier momento

Es posible crear un backup bajo demanda en cualquier momento para capturar el estado actual del volumen. Esto puede ser útil si se han realizado cambios muy importantes en un volumen y no debe esperar a que se realice el siguiente backup programado para proteger los datos. Esta funcionalidad también puede usar para crear un backup para un volumen que no se está respaldando actualmente y que desee capturar su estado actual.

Es posible crear una copia Snapshot ad hoc o un backup en un objeto de un volumen. No se puede crear un volumen replicado ad hoc.

El nombre de backup incluye la Marca de hora para poder identificar el backup bajo demanda desde otros backups programados.

Si habilitó *DataLock* y *Ransomware Protection* al activar el backup y la recuperación de BlueXP para este clúster, el backup bajo demanda también se configurará con DataLock, y el período de retención será de 30 días. Los análisis de ransomware no se admiten para backups ad hoc. ["Más información sobre la protección de DataLock y Ransomware"](#).

Es preciso tener en cuenta que al crear un backup ad hoc, se crea una Snapshot en el volumen de origen. Dado que esta instantánea no forma parte de una programación normal de instantánea, no se girará. Puede eliminar manualmente esta snapshot del volumen de origen una vez completado el backup. De este modo, se podrán liberar los bloques relacionados con esta snapshot. El nombre de la snapshot comenzará con `cbs-snapshot-adhoc-`. ["Consulte cómo eliminar una snapshot con la CLI de ONTAP"](#).



No se admite el backup de volúmenes bajo demanda en los volúmenes de protección de datos.

### Pasos

- En la ficha **Volumes**, haga clic en **...** Para el volumen y seleccione **Copia de seguridad > Crear copia de seguridad ad-hoc**.

| Volumes (5,000)          |                |                             |          |             |              |                                                                                                                                                                                                                                                             |                                                                                     |
|--------------------------|----------------|-----------------------------|----------|-------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Volume name    | Working Environment name    | SVM name | Volume type | Volume style | Existing protection                                                                                                                                                                                                                                         | Protection health                                                                   |
| <input type="checkbox"/> | volume 4<br>On | Working Environment 4<br>On | SVM 1    | RW          | FlexGroup    |    |  |
| <input type="checkbox"/> | volume 5<br>On | Working Environment 5<br>On | SVM 1    | RW          | FlexVol      | View Backup                                                                                                                                                                                                                                                 | ...                                                                                 |
| <input type="checkbox"/> | volume 6<br>On | Working Environment 5<br>On | SVM 1    | RW          | FlexVol      | Create Ad-hoc Backup                                                                                                                                                                                                                                        | ...                                                                                 |
| <input type="checkbox"/> | volume 7<br>On | Working Environment 5<br>On | SVM 1    | RW          | FlexVol      | Pause Backup                                                                                                                                                                                                                                                | ...                                                                                 |
| <input type="checkbox"/> |                |                             |          |             |              | Delete relationship                                                                                                                                                                                                                                         | Backup                                                                              |

La columna Backup Status de ese volumen muestra "in progress" hasta que se crea el backup.

## Consulte 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.

### Pasos

1. En la ficha **Volumes**, haga clic en **...** Para el volumen de origen y seleccione **Ver detalles del volumen**.

| Volumes (5,000)          |                             |                                   |             |             |              |                                                                                                                                                                                                                                                                   |                                                                                      |
|--------------------------|-----------------------------|-----------------------------------|-------------|-------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Volumes name                | Working Environment name          | SVM name    | Volume type | Volume style | Existing protection                                                                                                                                                                                                                                               | Protection health                                                                    |
| <input type="checkbox"/> | Source volume name #4<br>On | Working Environment name #4<br>On | SVM name #1 | RW          | FlexGroup    |       |  |
| <input type="checkbox"/> | Source volume name #5<br>On | Working Environment name #5<br>On | SVM name #1 | RW          | FlexVol      |    | ...                                                                                  |
| <input type="checkbox"/> | Source volume name #6<br>On | Working Environment name #6<br>On | SVM name #1 | RW          | FlexVol      |    | ...                                                                                  |
| <input type="checkbox"/> | Source volume name #7<br>On | Working Environment name #7<br>On | SVM name #1 | RW          | FlexVol      |    | ...                                                                                  |

De forma predeterminada, se muestran los detalles del volumen y la lista de copias Snapshot.

Volume name

Volume

Working Environment name

Working Environment

AWS

Location

SVM name

SVM

3-2-1 protection

Healthy

Protection health

Snapshot

Replication

Backup

Local Snapshot Policy

Snapshot policy name

5 Labels

Snapshots (1,200)

Snapshot name

Snapshot size

Date

Snapshot name number 1

2.125 GiB

March 27 2023, 00:00:00 am

Snapshot name number 2

2.125 GiB

March 27 2023, 00:00:00 am

2. Seleccione **Instantánea**, **Replicación** o **Copia de seguridad** para ver la lista de todos los archivos de copia de seguridad para cada tipo de copia de seguridad.



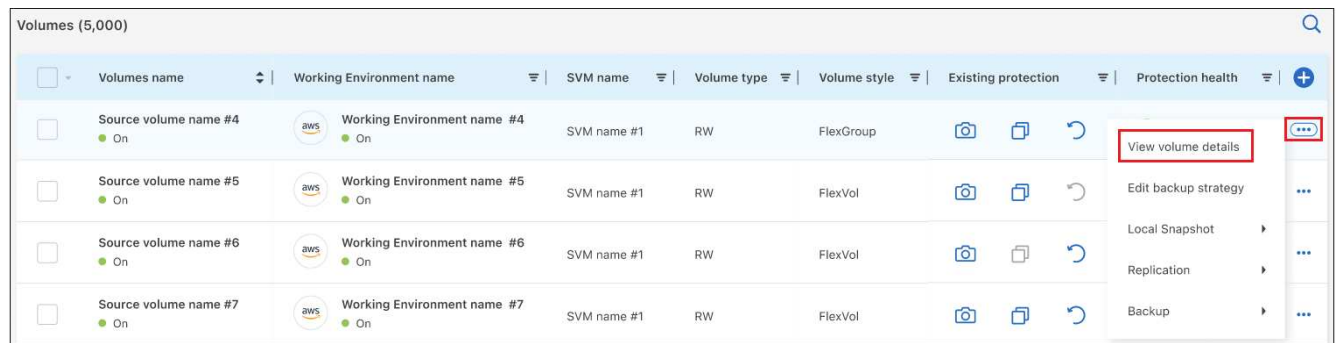
## Ejecuta un análisis de ransomware en un backup de volúmenes en el almacenamiento de objetos

El software de protección frente a ransomware NetApp analiza sus archivos de backup para buscar pruebas de un ataque de ransomware cuando se crea un backup en un archivo de objetos, y cuando se restauran datos de un archivo de backup. También puede ejecutar un análisis de protección frente al ransomware bajo demanda en cualquier momento para comprobar la facilidad de uso de un archivo de backup específico en el almacenamiento de objetos. Esto puede resultar útil si tuvo un problema de ransomware en un volumen en particular y desea verificar que los backups de ese volumen no se vean afectados.

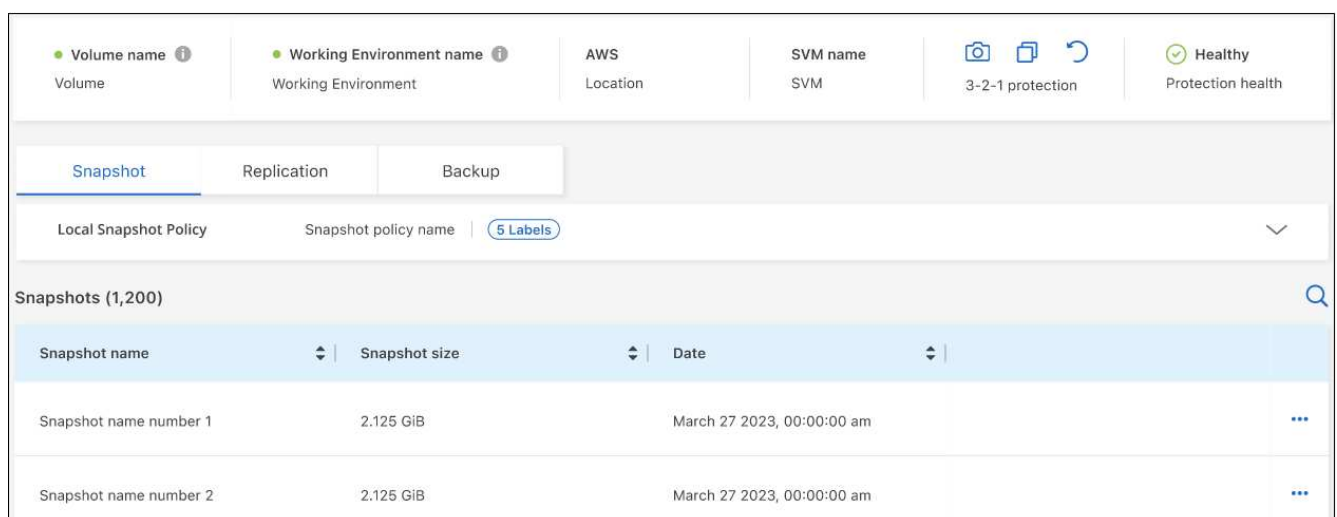
Esta función solo está disponible si el backup del volumen se creó desde un sistema con ONTAP 9.11.1 o superior, y si habilitó *DataLock and Ransomware Protection* en la política de backup en objetos.

### Pasos

1. En la ficha **Volumes**, haga clic en **...** Para el volumen de origen y seleccione **Ver detalles del volumen**.



Se muestran los detalles del volumen.



2. Seleccione **Copia de seguridad** para ver la lista de archivos de copia de seguridad en el almacenamiento de objetos.



3. Haga clic en ... Para el archivo de copia de seguridad del volumen que desea escanear en busca de ransomware y haga clic en **Escanear para Ransomware**.

Backups (1,200)

| Backup name          | Backup size | Date                       | Ransomware protection | Storage class | Snapmirror label |     |
|----------------------|-------------|----------------------------|-----------------------|---------------|------------------|-----|
| Backup Name Number 1 | 2.125 GiB   | March 27 2023, 00:00:00 am | Compliance            | None          |                  | ... |
| Backup name number 2 | 2.125 GiB   | March 27 2023, 00:00:00 am | None                  | None          |                  | ... |
| Backup name number 3 | 2.125 GiB   | March 27 2023, 00:00:00 am | Compliance            | None          |                  | ... |

Scan for Ransomware

Restore

Delete

La columna Ransomware Protection mostrará que el análisis está en curso.

## Gestione la relación de replicación con el volumen de origen

Después de configurar la replicación de datos entre dos sistemas, puede gestionar la relación de replicación de datos.

### Pasos

1. En la ficha **Volumes**, haga clic en ... Para el volumen de origen y seleccione la opción **Replicación**. Puede ver todas las opciones disponibles.
2. Seleccione la acción de replicación que desea realizar.

Volumes (5,000)

|                          | Volume name    | Working Environment name        | SVM name | Volume type | Volume style | Existing protection | Protection health |     |
|--------------------------|----------------|---------------------------------|----------|-------------|--------------|---------------------|-------------------|-----|
| <input type="checkbox"/> | volume 4<br>On | aws Working Environment 4<br>On | SVM 1    | RW          | FlexGroup    |                     | N/A               | ... |
| <input type="checkbox"/> | volume 5<br>On | aws Working Environment 5<br>On | SVM 1    | RW          | FlexVol      |                     |                   | ... |
| <input type="checkbox"/> | volume 6<br>On | aws Working Environment 5<br>On | SVM 1    | RW          | FlexVol      |                     |                   | ... |

View Replications

Update Replication

Pause Replication

Break Replication

Stop Replication

Reverse resync

Delete Relationship

View volume details

Edit backup strategy

Local Snapshot

Replication

Backup

En la siguiente tabla se describen las acciones disponibles:

| Acción                     | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ver replicación            | Muestra detalles sobre la relación de volumen: Información de transferencia, información de la última transferencia, detalles sobre el volumen e información sobre la política de protección asignada a la relación.                                                                                                                                                                                                                                                                                                         |
| Actualizar la replicación  | Inicia una transferencia incremental para actualizar el volumen de destino que se sincronizará con el volumen de origen.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Pausar la replicación      | Ponga en pausa la transferencia incremental de copias Snapshot para actualizar el volumen de destino. Puede reanudar más tarde si desea reiniciar las actualizaciones incrementales.                                                                                                                                                                                                                                                                                                                                         |
| Interrumpir la replicación | <p>Interrumpe la relación entre los volúmenes de origen y destino, y activa el volumen de destino para el acceso a los datos, lo convierte en de lectura y escritura.</p> <p>Esta opción suele utilizarse cuando el volumen de origen no puede servir datos debido a eventos como datos dañados, una eliminación accidental o un estado sin conexión.</p> <p><a href="#">"Aprenda a configurar un volumen de destino para acceder a los datos y reactivar un volumen de origen en la documentación de ONTAP"</a></p>         |
| Aborte la replicación      | Deshabilita los backups de este volumen en el sistema de destino y también deshabilita la capacidad de restaurar un volumen. No se eliminarán los backups existentes. Esto no elimina la relación de protección de datos entre los volúmenes de origen y de destino.                                                                                                                                                                                                                                                         |
| Resincronización inversa   | <p>Revierte los roles de los volúmenes de origen y destino. El contenido del volumen de origen original se sobrescribe con el contenido del volumen de destino. Esto es útil cuando se desea reactivar un volumen de origen que se desconectó.</p> <p>No se conservan todos los datos escritos en el volumen de origen original entre la última replicación de datos y la hora en la que se deshabilitó el volumen de origen.</p>                                                                                            |
| Suprimir relación          | Elimina la relación de protección de datos entre los volúmenes de origen y de destino, lo que significa que ya no se produce la replicación de datos entre los volúmenes. Esta acción no activa el volumen de destino para el acceso a datos, lo que significa que no lo convierte en lectura/escritura. Esta acción también elimina la relación entre iguales de clústeres y la relación entre iguales de máquinas virtuales de almacenamiento (SVM), si no hay otras relaciones de protección de datos entre los sistemas. |

## Resultado

Después de seleccionar una acción, BlueXP actualiza la relación.

## Edite una política de backup en el cloud existente

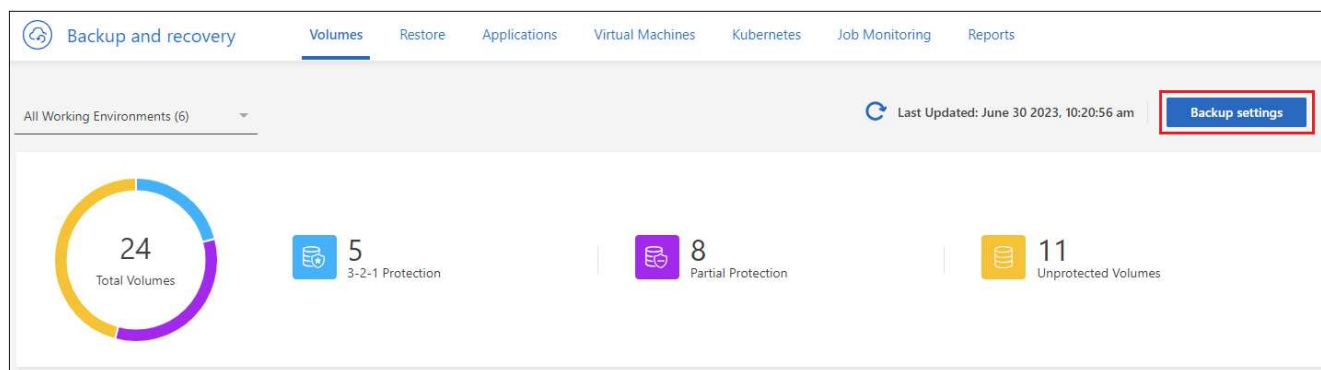
Puede cambiar los atributos de una política de backup que se aplique actualmente a los volúmenes en un entorno de trabajo. Los cambios que se aplican en la política de backup afectan a todos los volúmenes existentes que usan la política.



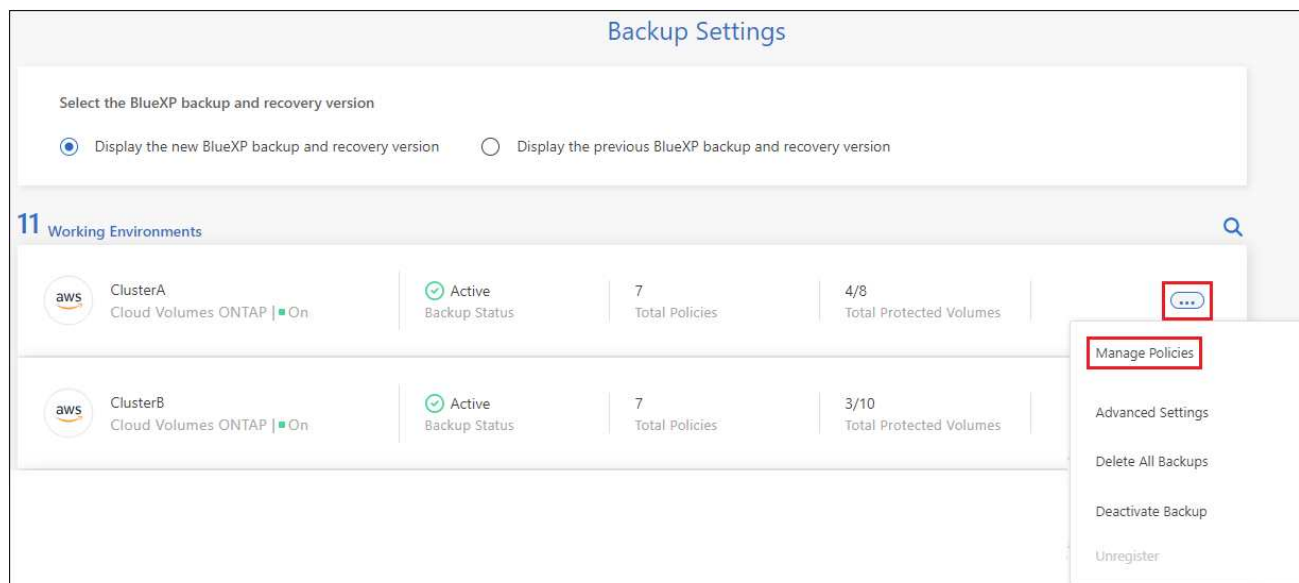
- Si habilitó *DataLock* y *Ransomware Protection* en la política inicial al activar el backup y la recuperación de BlueXP para este clúster, todas las políticas que edite deben configurarse con la misma configuración de DataLock (gobernanza o cumplimiento de normativas). Y si no activaste *DataLock* y *Ransomware Protection* al activar el backup y la recuperación de BlueXP, no puedes habilitar DataLock ahora.
- Al crear backups en AWS, si eligió *S3 Glacier* o *S3 Glacier Deep Archive* en su primera política de backup al activar el backup y la recuperación de BlueXP, ese nivel será el único nivel de archivado disponible al editar las políticas de backup. Si no ha seleccionado ningún nivel de archivado en su primera política de copia de seguridad, *S3 Glacier* será la única opción de archivado al editar una directiva.

## Pasos

1. En la ficha **Volumes**, 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 de la directiva y seleccione **Administrar directivas**.



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



Manage Policies

Add New Policy

Working Environment: ClusterB

Only Custom policies are editable

7 Policies

hourly\_bp

Custom Policy

Edit

2 Labels: Hourly (10), Daily (10)

Labels & Retention

None

DataLock & Ransomware Protection

Not Active

Archival Policy

3 out of 10

Associated Volumes

4. En la página *Edit Policy*, haga clic en  Para ampliar la sección *Labels & Retention* para cambiar la programación y/o la retención de copia de seguridad, y haga clic en **Guardar**.

Edit Policy

Working Environment: ClusterB

|                                  |                                                                                        |   |
|----------------------------------|----------------------------------------------------------------------------------------|---|
| Name                             | hourly_bp                                                                              | ▼ |
| Labels & Retention               | 10 Hourly   10 Daily                                                                   | ▼ |
| DataLock & Ransomware Protection |  None | ▼ |
| Archival Policy                  | Disabled                                                                               | ▼ |

Si el clúster ejecuta ONTAP 9.10.1 o más, también tendrá la opción de habilitar o deshabilitar la clasificación por niveles de los backups en el almacenamiento de archivado después de un cierto número de días.

["Obtenga más información sobre el uso del almacenamiento de archivado de AWS"](#).

["Obtenga más información sobre el uso del almacenamiento de archivado de Azure"](#).

["Obtenga más información sobre el uso del almacenamiento de archivado de Google"](#). (Requiere ONTAP 9.12.1).



**Archival Policy**  
Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

**Azure**

☒ Tier Backups to Archival

Archive after (Days): 30

Access Tier: Azure Archive

---

**Archival Policy**  
Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

**AWS**

☒ Tier Backups to Archival

Archive after (Days): 30

Storage Class: S3 Glacier

S3 Glacier Deep Archive

---

**Archival Policy**  
Backups reside in Google Cloud Standard storage for frequently accessed data. Optionally, you can tier backups to Google Cloud Archive storage for further cost optimization.

**Google**

☒ Tier Backups to Archival

Archive after (Days): 30

Storage Class: Google Cloud Archive

+ tenga en cuenta que todos los archivos de backup organizados en niveles para el almacenamiento de archivado se dejan en ese nivel si se detienen los backups por niveles en el archivado; no se vuelven a transferir automáticamente al nivel estándar. Solo los nuevos backups de volúmenes permanecerán en el nivel estándar.

## Añada una nueva política de backup en el cloud

Al habilitar el backup y la recuperación de BlueXP para un entorno de trabajo, se realiza un backup de todos los volúmenes que seleccionó inicialmente, utilizando la política de backup predeterminada que definió. 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.

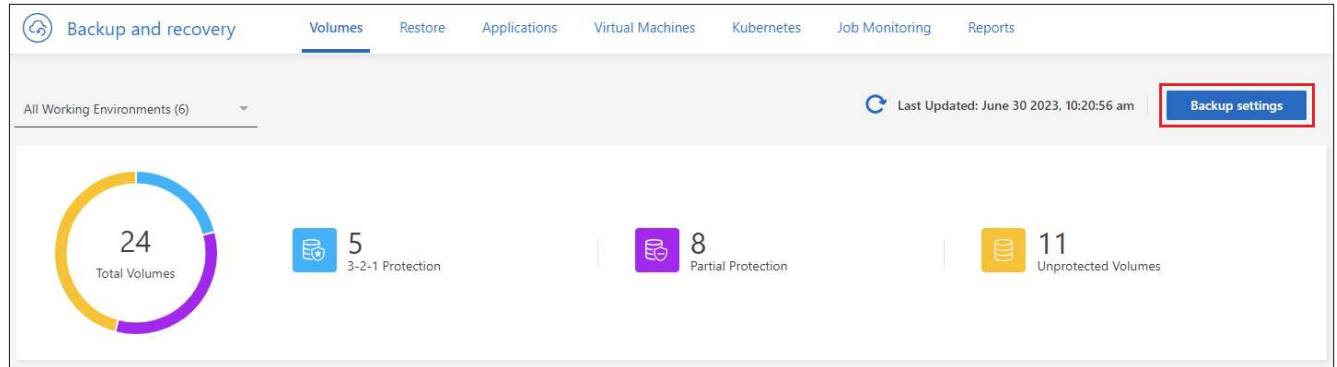
Si desea aplicar una nueva política de backup a ciertos volúmenes en un entorno de trabajo, primero debe añadir la política de backup al entorno de trabajo. Ahora puede [aplique la política a los volúmenes en ese entorno de trabajo](#).



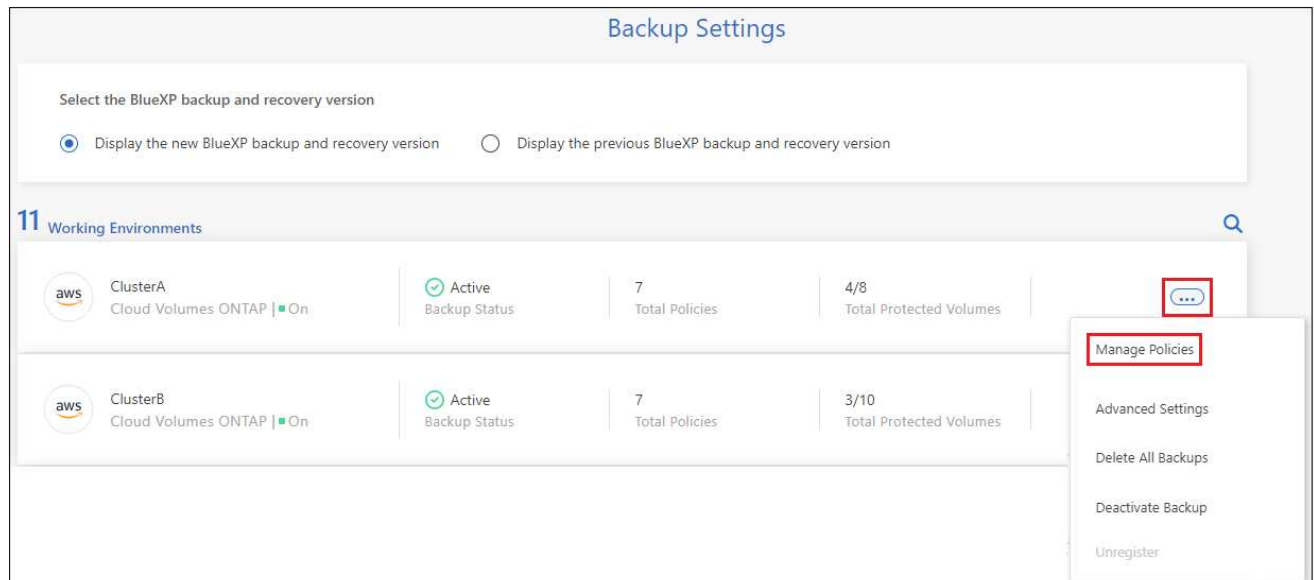
- Si habilitó *DataLock* y *Ransomware Protection* en la política inicial al activar el backup y la recuperación de BlueXP para este clúster, todas las políticas adicionales que cree deberán configurarse con la misma configuración de DataLock (gobernanza o cumplimiento de normativas). Y si no activaste *DataLock* y *Ransomware Protection* al activar el backup y la recuperación de BlueXP, no puedes crear nuevas políticas que utilicen DataLock.
- Al crear backups en AWS, si eligió *S3 Glacier* o *S3 Glacier Deep Archive* en su primera política de backup al activar el backup y la recuperación de BlueXP, ese nivel será el único nivel de archivado disponible para las futuras políticas de backup para ese clúster. Si ha seleccionado ningún nivel de archivado en su primera política de copia de seguridad, *S3 Glacier* será la única opción de archivado para futuras políticas.

## Pasos

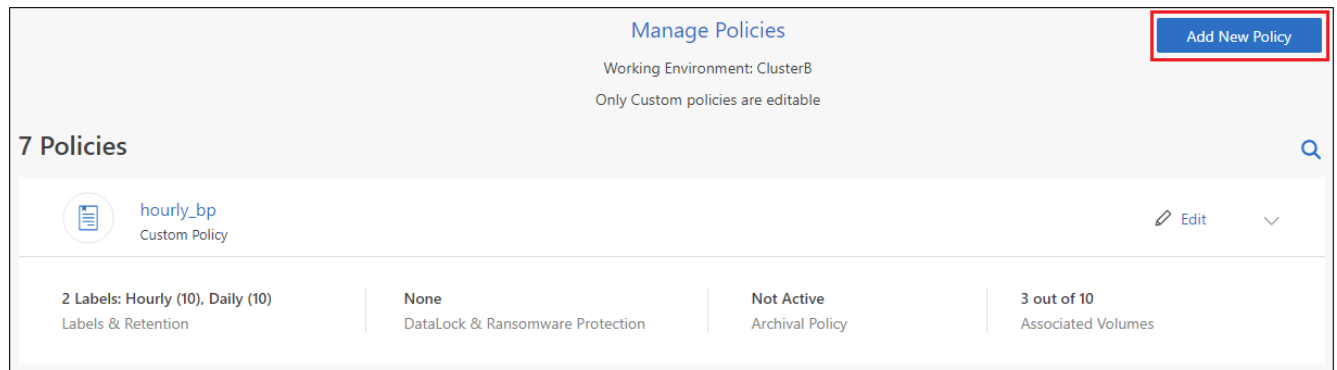
1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ... Para el entorno de trabajo en el que desea agregar la nueva directiva y seleccione **Administrar directivas**.



3. En la página *Manage Policies*, haga clic en **Add New Policy**.



4. En la página *Add New Policy*, haga clic en ▼ Para ampliar la sección *Labels & Retention* para definir la programación y la retención de copias de seguridad, y haga clic en **Guardar**.

| Add New Policy                             |                     |   |
|--------------------------------------------|---------------------|---|
| Working Environment: Working Environment 1 |                     |   |
| Name                                       | Default_Policy_Name | ▼ |
| Labels & Retention                         | 30 Daily            | ▼ |
| DataLock & Ransomware Protection           | None                | ▼ |
| Archival Policy                            | Disabled            | ▼ |

Si el clúster ejecuta ONTAP 9.10.1 o más, también tendrá la opción de habilitar o deshabilitar la clasificación por niveles de los backups en el almacenamiento de archivado después de un cierto número de días.

"Obtenga más información sobre el uso del almacenamiento de archivado de AWS".

"Obtenga más información sobre el uso del almacenamiento de archivado de Azure".

"Obtenga más información sobre el uso del almacenamiento de archivado de Google". (Requiere ONTAP 9.12.1).

Archival Policy

Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.

Azure

☒ Tier Backups to Archival

Archive after (Days)

30

Access Tier

Azure Archive ▼

---

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

AWS

☒ Tier Backups to Archival

Archive after (Days)

30

Storage Class

S3 Glacier ▲
S3 Glacier
S3 Glacier Deep Archive

---

Archival Policy

Backups reside in Google Cloud Standard storage for frequently accessed data. Optionally, you can tier backups to Google Cloud Archive storage for further cost optimization.

Google

☒ Tier Backups to Archival

Archive after (Days)

30

Storage Class

Google Cloud Archive ▼

## Eliminar backups

El backup y la recuperación de BlueXP te permite eliminar un único archivo de backup, eliminar todos los backups de un volumen o eliminar todas las copias de seguridad de todos los volúmenes en un entorno de trabajo. 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.

Tenga en cuenta que no puede eliminar los archivos de copia de seguridad bloqueados mediante la protección DataLock y Ransomware. La opción "Eliminar" no estará disponible en la interfaz de usuario si ha seleccionado uno o más archivos de backup bloqueados.



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. El backup y la recuperación de datos de BlueXP no elimina automáticamente los backups cuando se elimina un sistema y no existe compatibilidad actual en la interfaz de usuario para eliminar los backups después de que el sistema se haya eliminado. Seguirá cobrándose los costes de almacenamiento de objetos por los backups restantes.

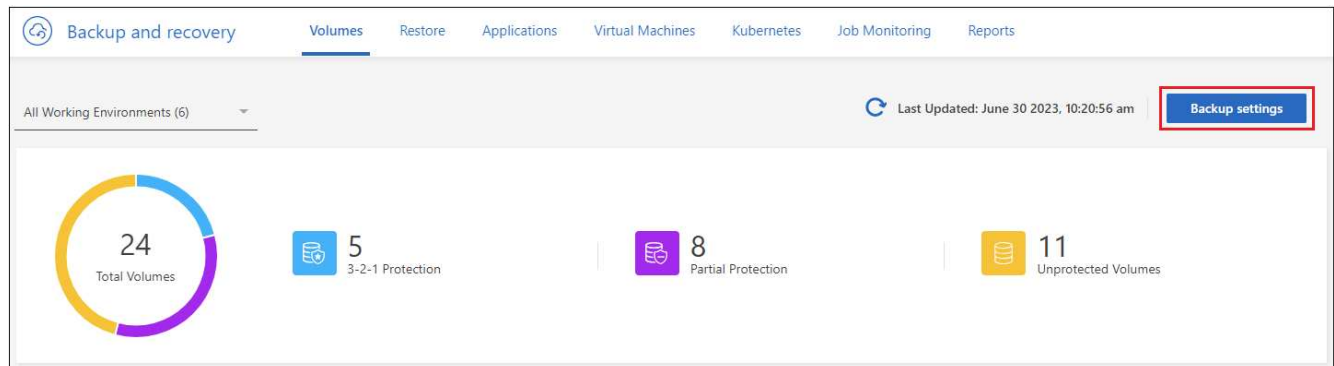
### Suprimir todos los archivos de copia de seguridad de un entorno de trabajo

Eliminar todos los backups del almacenamiento de objetos para un entorno de trabajo no deshabilita los futuros backups de 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](#).

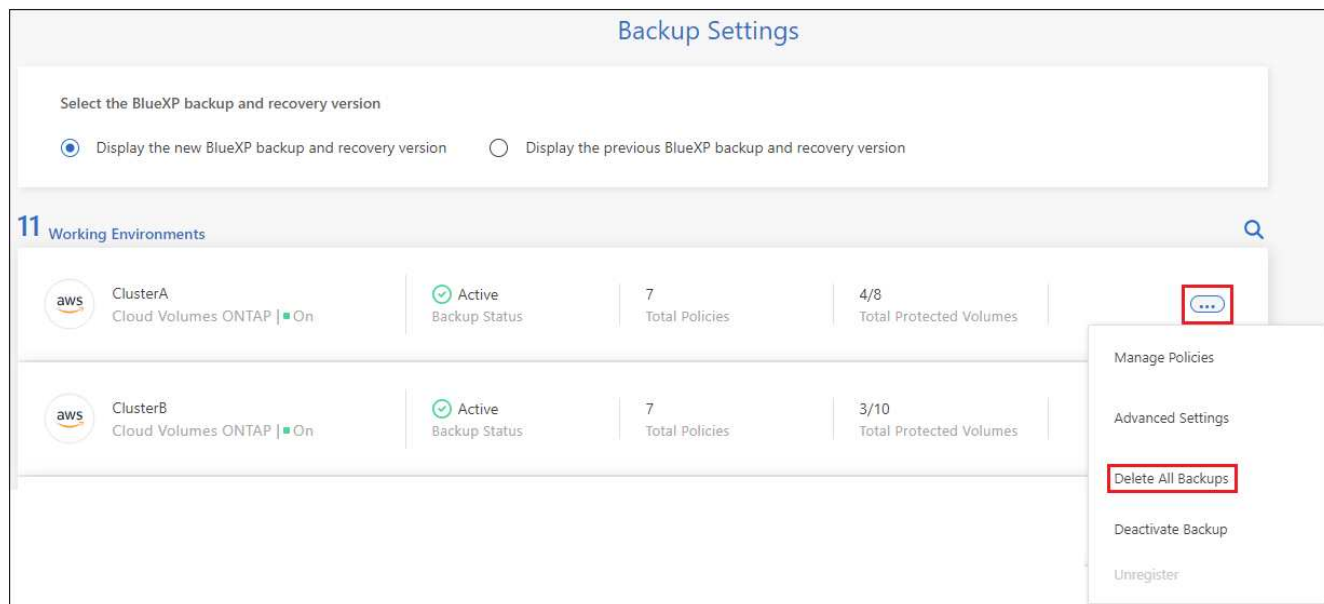
Tenga en cuenta que esta acción no afecta a las copias Snapshot ni a los volúmenes replicados: Estos tipos de archivos de backup no se eliminan.

#### Pasos

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



2. Haga clic en ... Para el entorno de trabajo 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**.

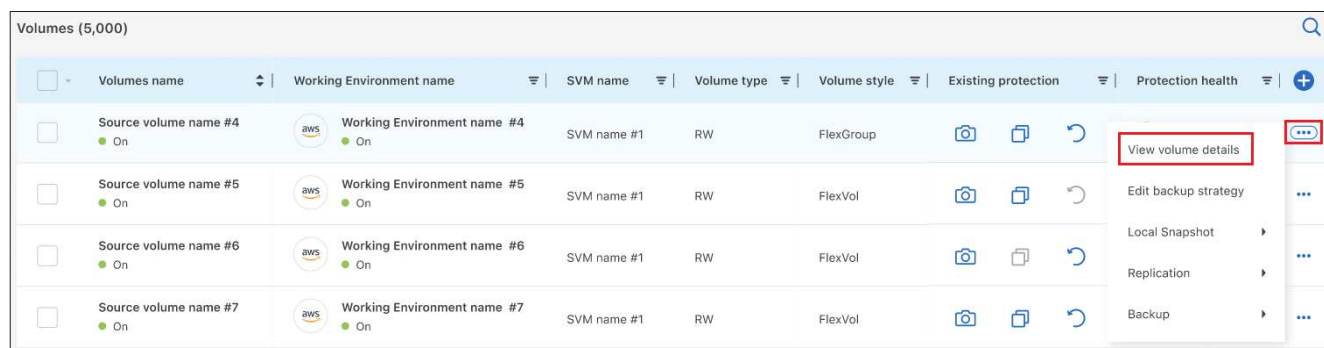
### Elimine un solo archivo de backup para un volumen

Puede eliminar un solo archivo de copia de seguridad si ya no lo necesita. Esto incluye la eliminación de un backup único de una copia Snapshot de volumen o de un backup en almacenamiento de objetos.

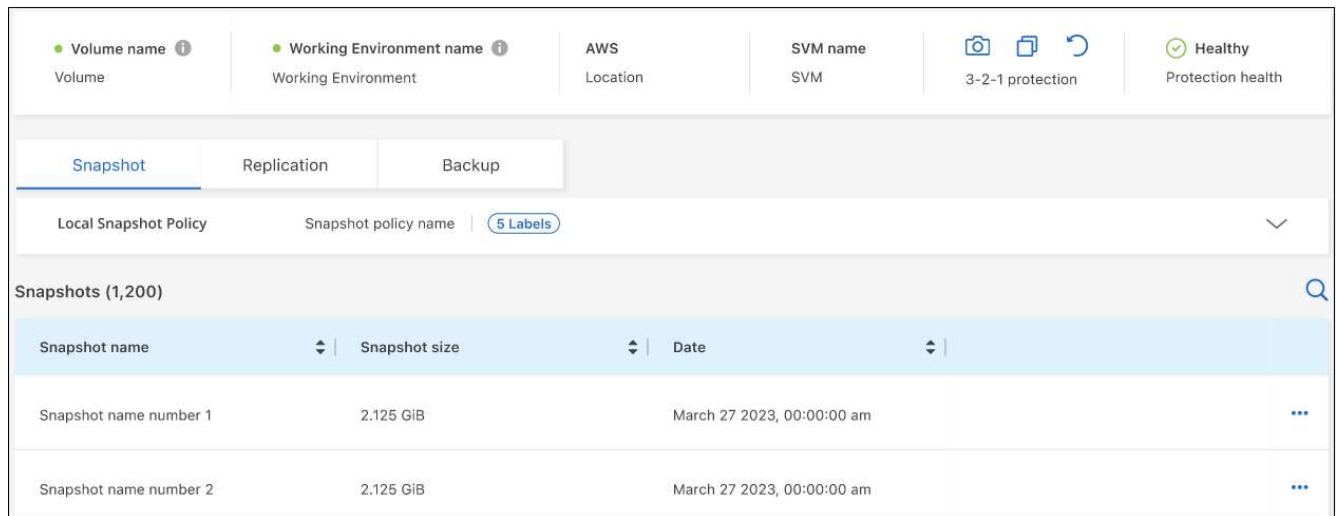
No se pueden eliminar volúmenes replicados (volúmenes de protección de datos).

### Pasos

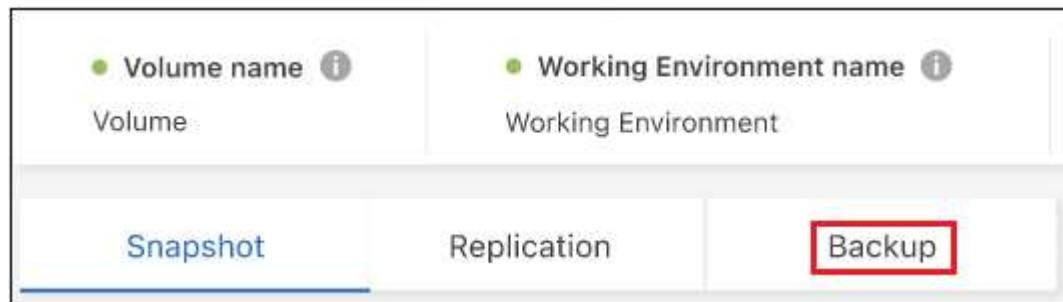
1. En la ficha **Volumes**, haga clic en ... Para el volumen de origen y seleccione **Ver detalles del volumen**.



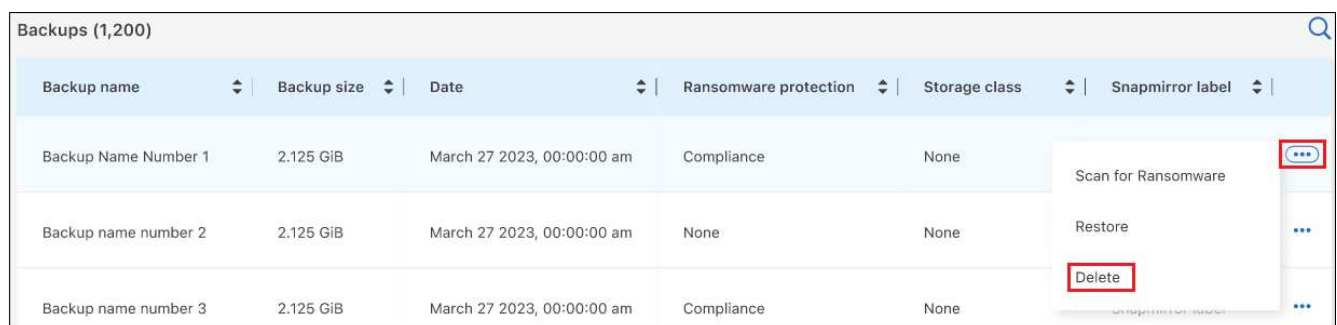
Se muestran los detalles del volumen y puede seleccionar **Instantánea**, **Replicación** o **Copia de seguridad** para ver la lista de todos los archivos de copia de seguridad del volumen. De forma predeterminada, se muestran las copias Snapshot disponibles.



2. Seleccione **Instantánea** o **Copia de seguridad** para ver el tipo de archivos de copia de seguridad que desea eliminar.



3. Haga clic en ... Para el archivo de copia de seguridad de volumen que desea eliminar y haga clic en **Eliminar**. La siguiente captura de pantalla es de un archivo de copia de seguridad en el almacenamiento de objetos.



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

## Elimine las relaciones de backup de volúmenes

Eliminar la relación de backup de un volumen ofrece un mecanismo de archivado si desea detener la creación de nuevos archivos de backup y eliminar el volumen de origen, pero conservar todos los archivos de backup existentes. Esto le permite restaurar el volumen desde el archivo de backup en el futuro, si es necesario, a la vez que se borra espacio del sistema de almacenamiento de origen.

No es necesario eliminar el volumen de origen. Es posible eliminar la relación de backup de un volumen y conservar el volumen de origen. En este caso, es posible "activar" el backup en el volumen más adelante. En

este caso se sigue utilizando la copia de backup base original: No se crea ni exporta una nueva copia de backup de referencia al cloud. Tenga en cuenta que si se reactivará una relación de backup, se asignará el volumen la política de backup predeterminada.

Esta función solo está disponible si el sistema ejecuta ONTAP 9.12.1 o posterior.

No se puede eliminar el volumen de origen desde la interfaz de usuario de backup y recuperación de BlueXP. Sin embargo, puede abrir la página Detalles de volumen en el lienzo y ["elimine el volumen desde allí"](#).



No se pueden eliminar archivos de backup de volúmenes individuales una vez que se ha eliminado la relación. Sin embargo, puede eliminar todos los backups del volumen.

## Pasos

1. En la ficha **Volumes**, haga clic en **...** Para el volumen de origen y seleccione **Copia de seguridad > Eliminar relación**.

| Volume name | Working Environment name | SVM name | Volume type | Volume style | Existing protection  | Protection health |
|-------------|--------------------------|----------|-------------|--------------|----------------------|-------------------|
| volume 4    | Working Environment 4    | SVM 1    | RW          | FlexGroup    |                      |                   |
| volume 5    | Working Environment 5    | SVM 1    | RW          | FlexVol      | View Backups         |                   |
| volume 6    | Working Environment 5    | SVM 1    | RW          | FlexVol      | Create Ad-hoc Backup |                   |
| volume 7    | Working Environment 5    | SVM 1    | RW          | FlexVol      | Pause Backup         |                   |

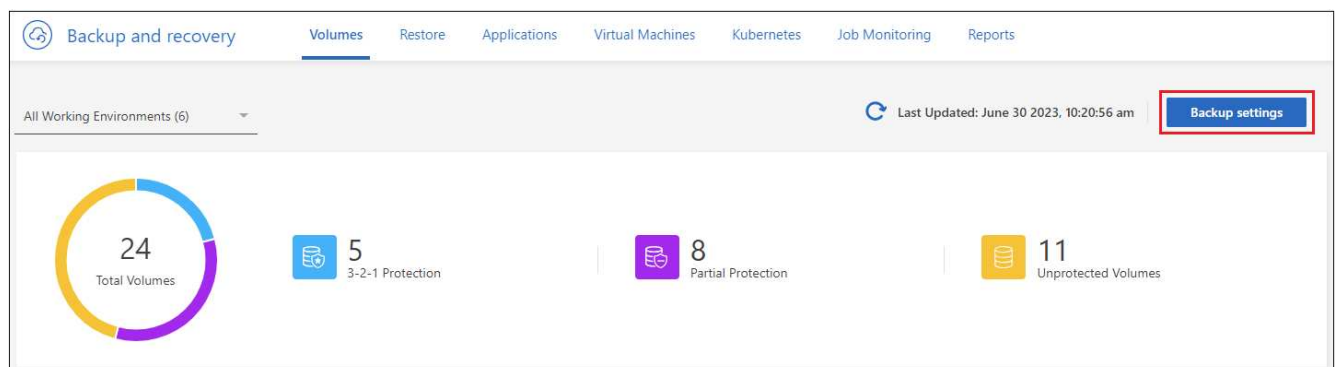
## Desactiva el backup y la recuperación de BlueXP para un entorno de trabajo

Si se desactiva la copia de seguridad y recuperación de BlueXP para un entorno de trabajo, se desactivan las copias de seguridad de cada volumen del sistema y también se deshabilita la capacidad de 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 [elimine los backups](#).

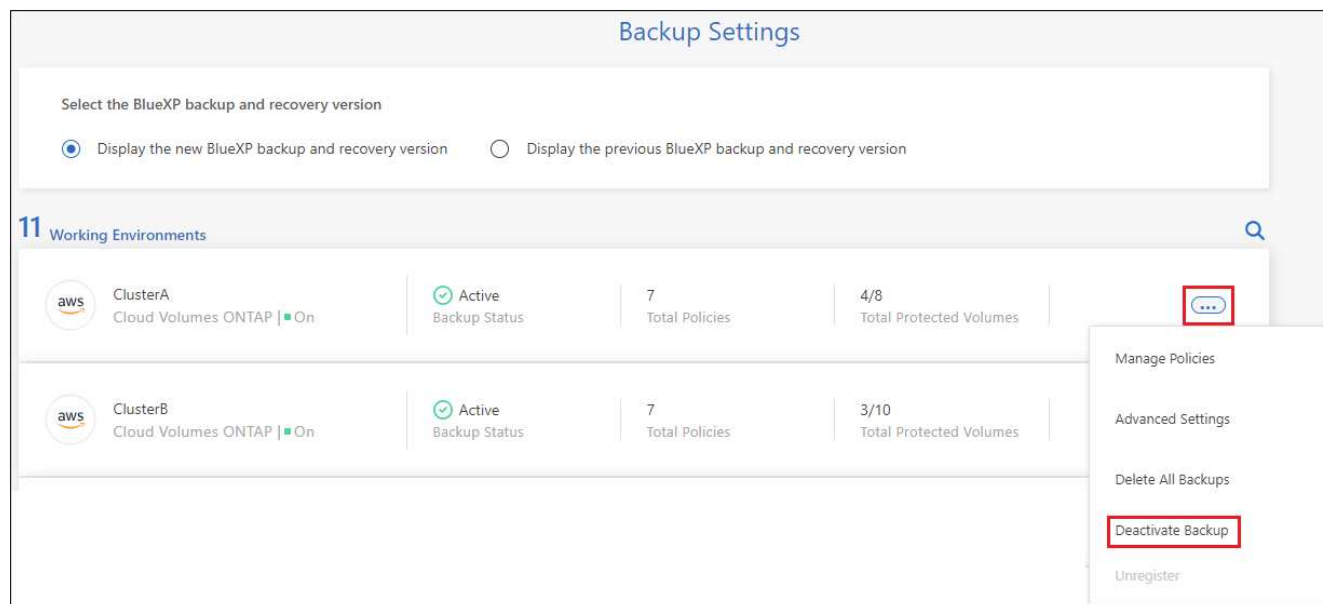
## Pasos

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





2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo en el que desea desactivar las copias de seguridad y seleccione **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.

## Cancela el registro de backup y recuperación de BlueXP para un entorno de trabajo

Puedes cancelar el registro del backup y la recuperación de BlueXP en un entorno de trabajo si ya no quieres utilizar la funcionalidad de backup y quieres dejar de que se te cobren los backups de ese entorno de trabajo. Normalmente, esta función se utiliza cuando se planea eliminar un entorno de trabajo 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 backup y recuperación de BlueXP en el entorno de trabajo, puede habilitar el backup y la recuperación de BlueXP para ese clúster utilizando la nueva información del proveedor de cloud.

Antes de poder cancelar el registro de backup y recuperación de BlueXP, debe realizar los siguientes pasos, en este orden:

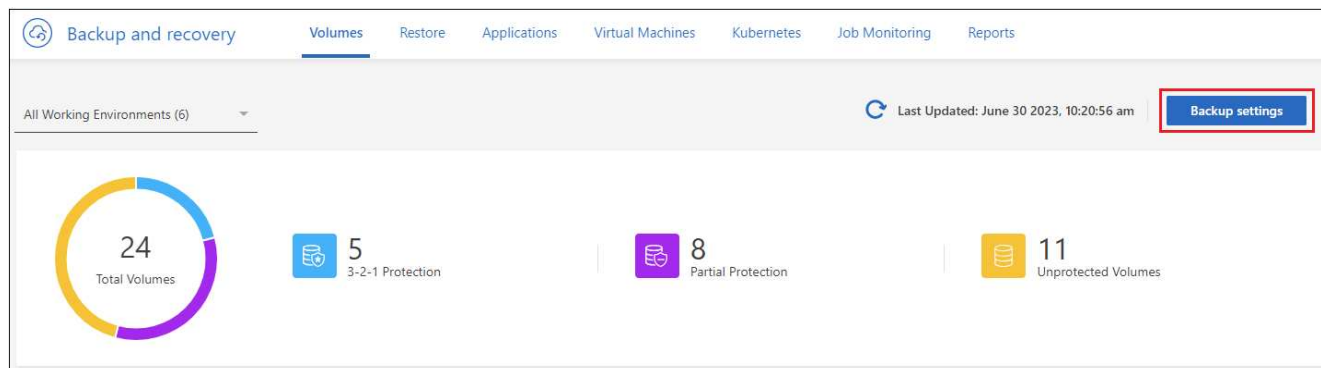
- Desactiva el backup y la recuperación de BlueXP para el entorno de trabajo
- Eliminar todos los backups de ese entorno de trabajo

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

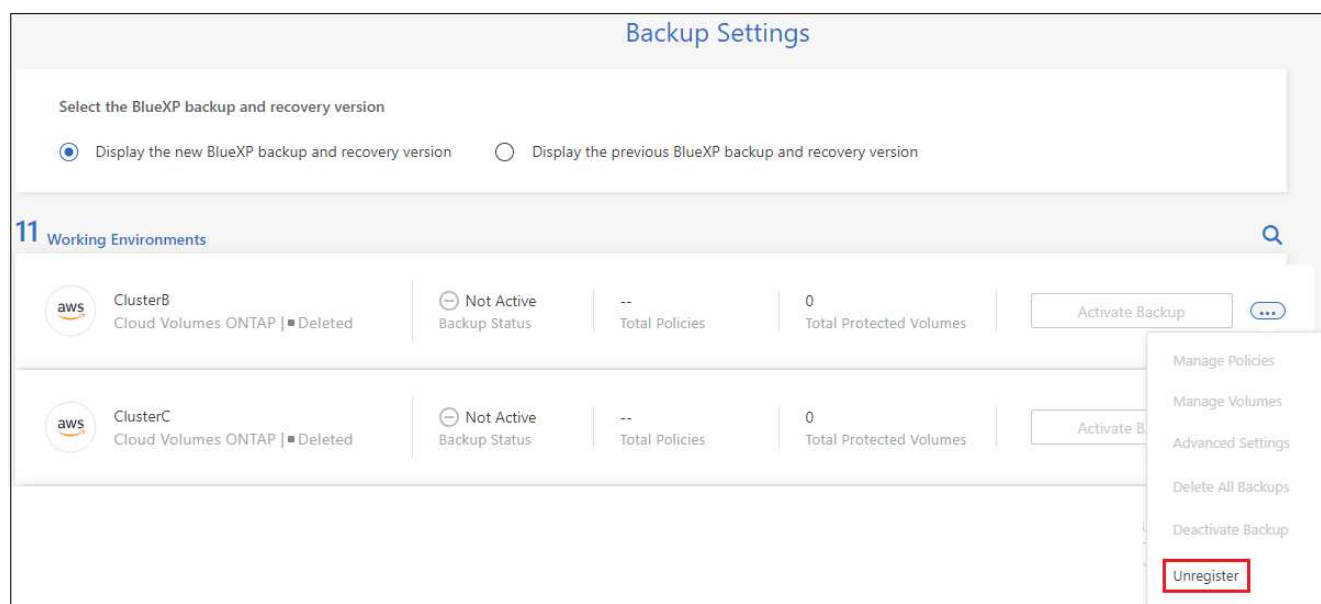
### Pasos

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





2. En la página *Backup Settings*, haga clic en ... Para el entorno de trabajo en el que desea cancelar el registro del servicio de copia de seguridad y seleccionar **Unregister**.



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

## Restaurar datos de ONTAP desde archivos de respaldo con BlueXP Backup and Recovery

Los backups de tus datos de volúmenes de ONTAP están disponibles desde las ubicaciones donde se crearon los backups: Copias Snapshot, volúmenes replicados y backups almacenados en el almacenamiento de objetos. Es posible restaurar datos desde un momento específico desde cualquiera de estas ubicaciones de backups. Con la copia de seguridad y recuperación de BlueXP, restaure un volumen ONTAP completo desde un archivo de copia de seguridad o, si solo necesita restaurar unos pocos archivos, restaure una carpeta o archivos individuales.

- Puede restaurar un **volumen** (como un volumen nuevo) al entorno de trabajo original, a un entorno de trabajo diferente que utiliza la misma cuenta de cloud o a un sistema ONTAP local.
- Puede restaurar una carpeta \*\* en un volumen del entorno de trabajo original, en un volumen de un entorno de trabajo diferente que utiliza la misma cuenta de cloud o en un volumen de un sistema ONTAP local.

- Puede restaurar **archivos** en un volumen del entorno de trabajo original, en un volumen de un entorno de trabajo diferente que utiliza la misma cuenta de cloud o en un volumen de un sistema ONTAP local.

Se requiere una licencia válida de backup y recuperación de BlueXP para restaurar los datos desde los archivos de backup a un sistema de producción.

En resumen, estos son los flujos válidos que se pueden utilizar para restaurar los datos de volúmenes en un entorno de trabajo de ONTAP:

- Archivo de backup → Volumen restaurado
- Volumen replicado → Volumen restaurado
- Copia Snapshot → Volumen restaurado



Si la operación de restauración no se completa, no vuelva a intentar el proceso de restauración hasta que Job Monitor muestre que se produjo un error en la operación de restauración. Si se vuelve a intentar el proceso de restauración antes de que Job Monitor muestre que la operación de restauración falló, la operación de restauración volverá a fallar. Cuando vea el estado de Job Monitor como “Failed”, puede intentar nuevamente el proceso de restauración.



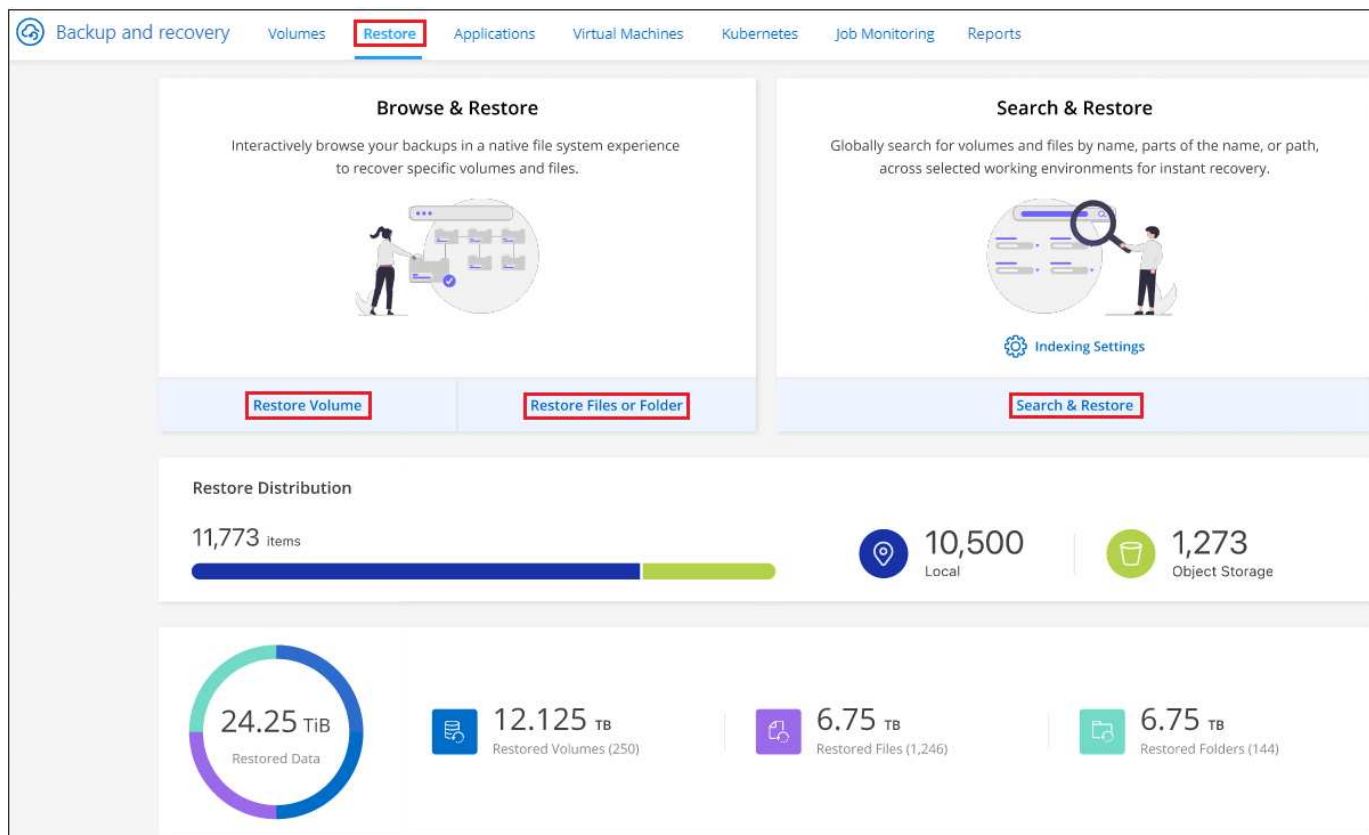
Para conocer las limitaciones relacionadas con la restauración de datos de ONTAP, consulte ["Limitaciones de backup y restauración de los volúmenes de ONTAP"](#).

## La Consola de restauración

Restore Dashboard se utiliza para realizar operaciones de volumen, carpeta y restauración de archivos. Para acceder al Panel de restauración, haga clic en **copia de seguridad y recuperación** en el menú BlueXP y, a continuación, haga clic en la ficha **Restaurar**. También puede hacer clic en > **Ver el Panel de restauración** desde el servicio de copia de seguridad y recuperación desde el panel Servicios.



El backup y la recuperación de BlueXP deben estar activados al menos en un entorno de trabajo y deben existir archivos de copia de seguridad iniciales.



Como puede ver, Restore Dashboard ofrece dos formas diferentes de restaurar datos de archivos de copia de seguridad: **Browse & Restore** y **Search & Restore**.

## Comparación de examinar y restaurar y buscar y restaurar

En términos generales, *Browse & Restore* suele ser mejor cuando necesita restaurar un volumen, carpeta o archivo específico de la última semana o mes, y sabe el nombre y la ubicación del archivo y la fecha en la que estaba en buen estado. *Search & Restore* suele ser mejor cuando necesita restaurar un volumen, una carpeta o un archivo, pero no recuerda el nombre exacto, ni el volumen en el que reside, ni la fecha en la que estaba en buen estado por última vez.

Esta tabla proporciona una comparación de las características de los dos métodos.

| Examinar y restaurar                                                                                                                            | Búsqueda y restauración                                                                                                                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Examine una estructura de estilo de carpeta para encontrar el volumen, la carpeta o el archivo en un único archivo de copia de seguridad.       | Busque un volumen, carpeta o archivo a través de <b>todos los archivos de copia de seguridad</b> por nombre de volumen parcial o completo, nombre de carpeta/archivo parcial o completo, rango de tamaño y filtros de búsqueda adicionales. |
| No gestiona la recuperación de archivos si el archivo se ha eliminado o cambiado de nombre y el usuario no conoce el nombre de archivo original | Controla los directorios recién creados, eliminados y renombrados y los archivos recién creados, eliminados y renombrados                                                                                                                   |
| No se requieren recursos de proveedor de cloud adicionales                                                                                      | Al realizar la restauración desde el cloud, es necesario utilizar el bucket adicional y los recursos de proveedor de cloud público por cuenta.                                                                                              |

| Examinar y restaurar                                 | Búsqueda y restauración                                                                                                               |
|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| No requiere costes de proveedor de cloud adicionales | Al restaurar desde el cloud, se necesitan costes adicionales al analizar los backups y los volúmenes para los resultados de búsqueda. |
| Es compatible con la restauración rápida.            | No se admite la restauración rápida.                                                                                                  |

Esta tabla proporciona una lista de operaciones de restauración válidas en función de la ubicación en la que residen los archivos de copia de seguridad.

| Tipo de backup                       | Examinar y restaurar |                    |                   | Búsqueda y restauración |                    |                   |
|--------------------------------------|----------------------|--------------------|-------------------|-------------------------|--------------------|-------------------|
|                                      | Restaurar volumen    | Restaurar archivos | Restaurar carpeta | Restaurar volumen       | Restaurar archivos | Restaurar carpeta |
| <b>Copia Snapshot</b>                | Sí                   | No                 | No                | Sí                      | Sí                 | Sí                |
| <b>Volumen replicado</b>             | Sí                   | No                 | No                | Sí                      | Sí                 | Sí                |
| <b>Archivo de copia de seguridad</b> | Sí                   | Sí                 | Sí                | Sí                      | Sí                 | Sí                |

Antes de poder utilizar cualquiera de estos métodos de restauración, asegúrese de haber configurado el entorno para los requisitos específicos de recurso. Estos requisitos se describen en las secciones siguientes.

Consulte los requisitos y los pasos de restauración para el tipo de operación de restauración que desea usar:

- <<Restaurar volúmenes mediante la función examinar Restore, Restaurar volúmenes mediante la función examinar Restore
- <<Restaurar carpetas y archivos utilizando examinar Restore, Restaurar carpetas y archivos utilizando examinar Restore
- <<restore-ontap-data-using-search-restore, Restaurar volúmenes, carpetas y archivos mediante la función de restauración de búsqueda

## Restaurar datos de ONTAP mediante Examinar y Restaurar

Antes de empezar a restaurar un volumen, una carpeta o un archivo, debe conocer el nombre del volumen desde el que desea restaurar, el nombre del entorno de trabajo y la SVM donde reside el volumen, así como la fecha aproximada del archivo de backup del que desea restaurar. Es posible restaurar datos de ONTAP desde una copia Snapshot, un volumen replicado o desde backups almacenados en el almacenamiento de objetos.

**Nota:** Si el archivo de copia de seguridad que contiene los datos que desea restaurar reside en el almacenamiento en la nube de archivos (a partir de ONTAP 9.10.1), la operación de restauración tomará más tiempo y incurrirá en un costo. Además, el clúster de destino también debe ejecutar ONTAP 9.10.1 o superior para la restauración de volúmenes, 9.11.1 para la restauración de archivos, 9.12.1 para Google Archive y StorageGRID y 9.13.1 para la restauración de carpetas.

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS".](#)

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de Azure".](#)



La prioridad alta no es compatible cuando se restauran los datos desde el almacenamiento de archivado de Azure en sistemas StorageGRID.

## Examinar y restaurar entornos de trabajo compatibles y proveedores de almacenamiento de objetos

Es posible restaurar datos ONTAP desde un archivo de backup que se encuentra en un entorno de trabajo secundario (un volumen replicado) o en almacenamiento de objetos (un archivo de backup) para los siguientes entornos de trabajo. Las copias Snapshot residen en el entorno de trabajo de origen y se pueden restaurar únicamente en ese mismo sistema.

**Nota:** Puede restaurar un volumen desde cualquier tipo de archivo de copia de seguridad, pero puede restaurar una carpeta o archivos individuales solo desde un archivo de copia de seguridad en el almacenamiento de objetos en este momento.

| Desde Object Store (Backup)                                        | Desde primario (Snapshot)                                                              | Desde el Sistema Secundario (Replicación)                                              | Al entorno de trabajo de destino                                    |
|--------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| Amazon S3                                                          | Cloud Volumes ONTAP en AWS<br>Sistema ONTAP en las instalaciones                       | Cloud Volumes ONTAP en AWS<br>Sistema ONTAP en las instalaciones<br><br>ifdef::azure[] | Azure Blob                                                          |
| Cloud Volumes ONTAP en Azure<br>Sistema ONTAP en las instalaciones | Cloud Volumes ONTAP en Azure<br>Sistema ONTAP en las instalaciones<br><br>ifdef::gcp[] | Google Cloud Storage                                                                   | Cloud Volumes ONTAP en Google<br>Sistema ONTAP en las instalaciones |
| Cloud Volumes ONTAP en Google on-local ONTAP system endif::gcp[]   | StorageGRID de NetApp                                                                  | Sistema ONTAP en las instalaciones                                                     | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           |
| Al sistema ONTAP en las instalaciones                              | ONTAP S3                                                                               | Sistema ONTAP en las instalaciones                                                     | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           |

Para examinar y restaurar, el conector se puede instalar en las siguientes ubicaciones:

- Para Amazon S3, el conector puede ponerse en marcha en AWS o en sus instalaciones
- Para Azure Blob, el conector se puede poner en marcha en Azure o en sus instalaciones
- Para Google Cloud Storage, el conector se debe poner en marcha en su VPC de Google Cloud Platform

- Para StorageGRID, el conector debe estar desplegado en sus instalaciones, con o sin acceso a Internet
- Para ONTAP S3, el conector se puede implementar en sus instalaciones (con o sin acceso a Internet) o en un entorno de proveedor de cloud

Tenga en cuenta que las referencias a "sistemas ONTAP en las instalaciones" incluyen sistemas FAS, AFF y ONTAP Select.



Si la versión de ONTAP de su sistema es inferior a 9.13.1, no podrá restaurar carpetas o archivos si el archivo de copia de seguridad se ha configurado con DataLock & Ransomware. En este caso, es posible restaurar todo el volumen desde el archivo de backup y, a continuación, acceder a los archivos necesarios.

## Restaura volúmenes mediante la función examinar & Restore

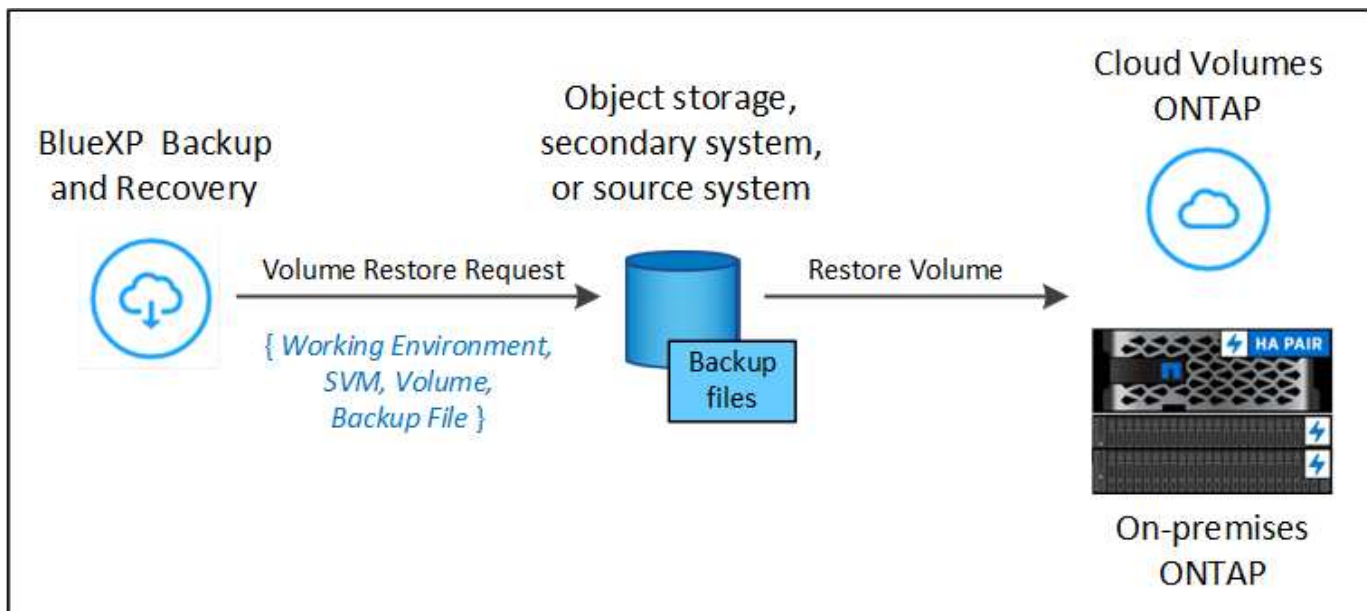
Cuando se restaura un volumen a partir de un archivo de backup, el backup y la recuperación de BlueXP crean un volumen *new* con los datos del backup. Al utilizar un backup a partir del almacenamiento de objetos, es posible restaurar los datos en un volumen en el entorno de trabajo original, en un entorno de trabajo diferente ubicado en la misma cuenta de cloud que el entorno de trabajo de origen o en un sistema ONTAP on-premises.

Al restaurar un backup en el cloud en un sistema Cloud Volumes ONTAP con ONTAP 9.13.0 o posterior o en un sistema ONTAP en las instalaciones que ejecute ONTAP 9.14.1, tendrá la opción de realizar una operación de restauración *rápida*. La restauración rápida es ideal para situaciones de recuperación ante desastres en las que se necesita proporcionar acceso a un volumen lo antes posible. Una restauración rápida restaura los metadatos del archivo de backup a un volumen en lugar de restaurar todo el archivo de backup. No se recomienda la restauración rápida para aplicaciones sensibles al rendimiento ni a la latencia, ni se admite con backups en el almacenamiento archivado.



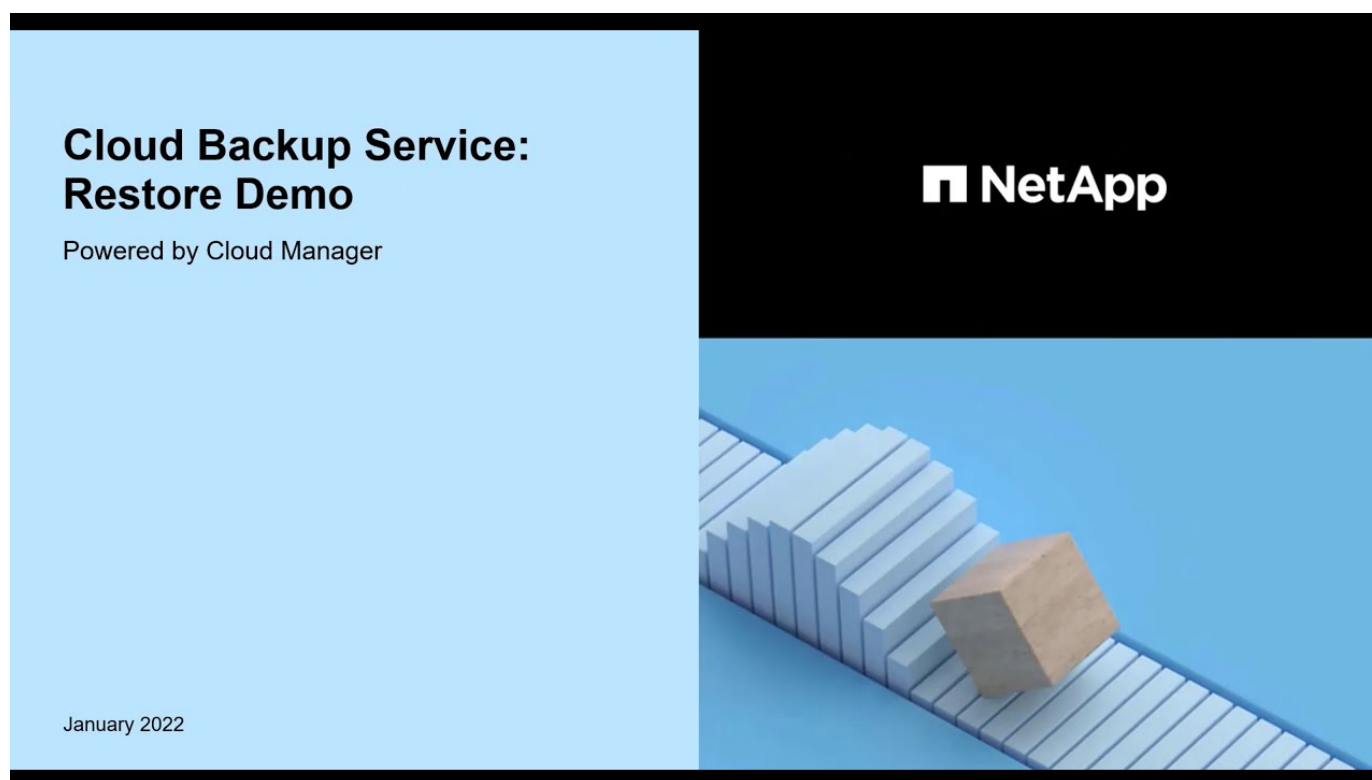
La restauración rápida solo es compatible con los volúmenes de FlexGroup si el sistema de origen desde el cual se creó el backup de cloud ejecutaba ONTAP 9.12.1 o posterior. Y solo se admite para volúmenes de SnapLock si el sistema de origen ejecutaba ONTAP 9.11.0 o posterior.

Al restaurar desde un volumen replicado, puede restaurar el volumen en el entorno de trabajo original o en un sistema Cloud Volumes ONTAP o ONTAP on-premises.



Como puede ver, tendrá que conocer el nombre del entorno de trabajo de origen, la máquina virtual de almacenamiento, el nombre del volumen y la fecha del archivo de backup para realizar una restauración de volumen.

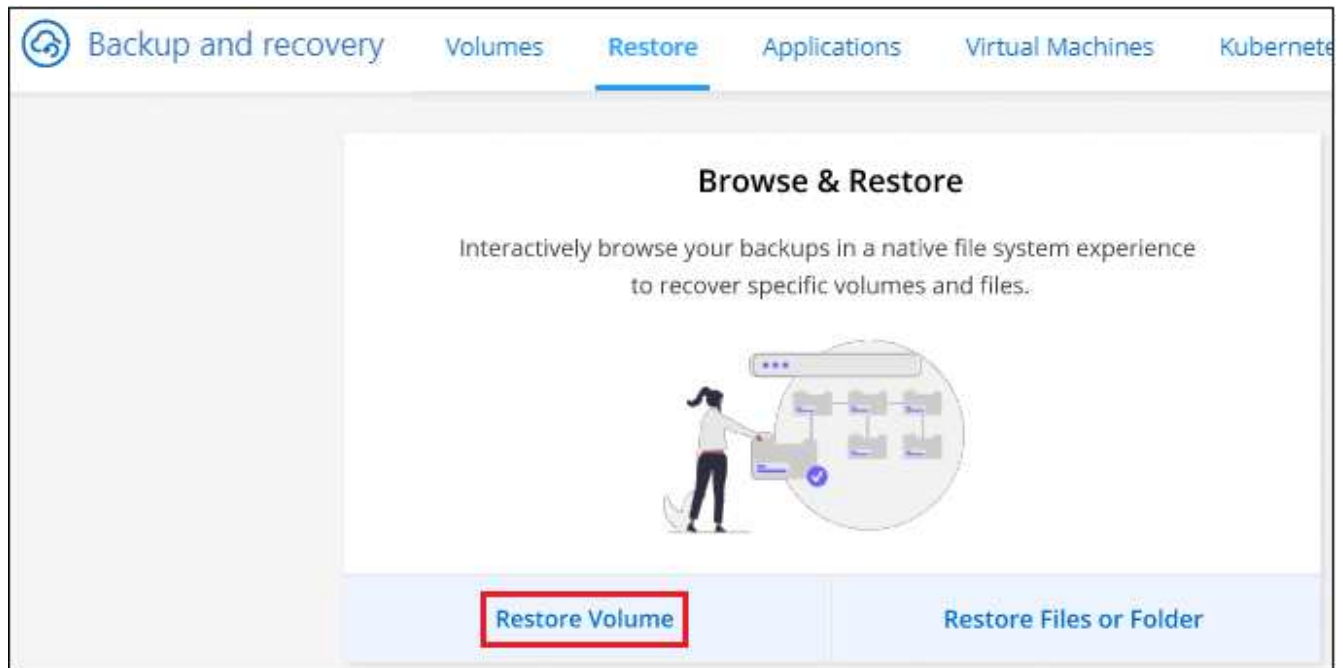
En el siguiente vídeo se muestra un tutorial rápido sobre cómo restaurar un volumen:



## Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Restaurar** y aparecerá el Panel de restauración.
3. En la sección *Browse & Restore*, haga clic en **Restore Volume**.





4. En la página *Select Source*, desplácese hasta el archivo de copia de seguridad del volumen que desea restaurar. Seleccione **entorno de trabajo**, **volumen** y el archivo **copia de seguridad** que tiene la Marca de fecha/hora desde la que desea restaurar.

La columna **Ubicación** muestra si el archivo de copia de seguridad (instantánea) es **Local** (una copia de Snapshot en el sistema de origen), **Secundario** (un volumen replicado en un sistema ONTAP secundario) o **Almacenamiento de objetos** (un archivo de copia de seguridad en el almacenamiento de objetos). Elija el archivo que desea restaurar.

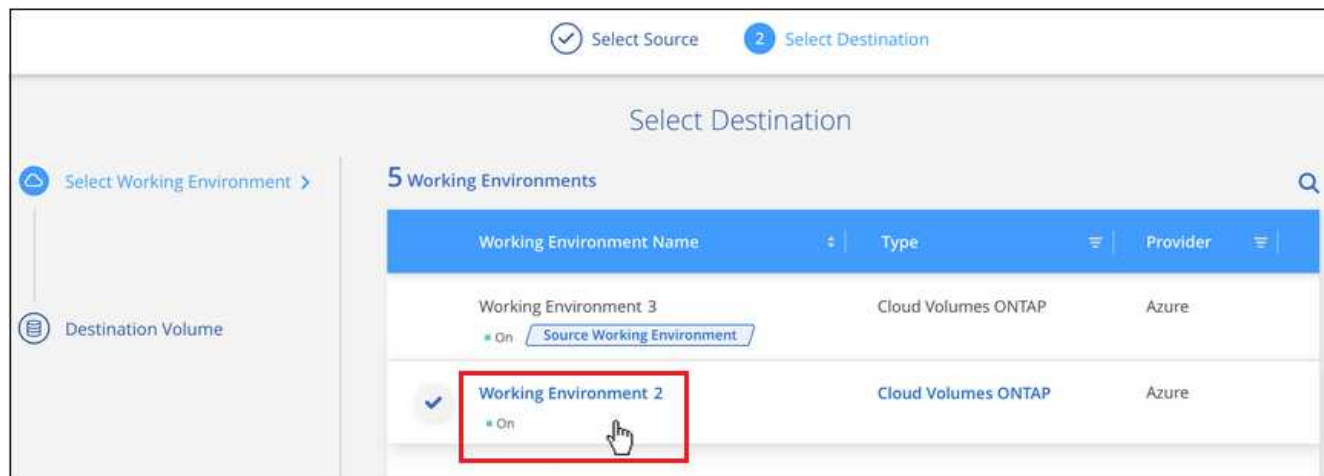
| Snapshot Name   | Location       | Date                   | Size       | Ransomware Scan | Storage Class |
|-----------------|----------------|------------------------|------------|-----------------|---------------|
| Backup 1        | Local          | June 12 2022, 00:00:00 | 12.125 TiB | N/A             | N/A           |
| <b>Backup 2</b> | Local          | June 12 2022, 00:00:00 | 12.125 TiB | N/A             | N/A           |
| Backup 3        | Local          | June 12 2022, 00:00:00 | 12.125 TiB | N/A             | N/A           |
| Backup 4        | Object Storage | June 12 2022, 00:00:00 | 12.125 TiB | Protected       | Standard      |

5. Haga clic en **Siguiente**.

Tenga en cuenta que si selecciona un archivo de backup en el almacenamiento de objetos y la protección contra ransomware está activa para ese backup (si habilitó DataLock y Ransomware Protection en la política de backup), se le pedirá que ejecute un análisis de ransomware adicional en el archivo de backup antes de restaurar los datos. Se recomienda que escanee el archivo de backup como ransomware. (Incurrirá en costes adicionales de salida de su proveedor de cloud para acceder al contenido del archivo de backup).

6. En la página *Select Destination*, seleccione **entorno de trabajo** donde desea restaurar el volumen.





7. Al restaurar un archivo de backup desde el almacenamiento de objetos, si selecciona un sistema ONTAP en las instalaciones y aún no configuró la conexión del clúster con el almacenamiento de objetos, se le pedirá información adicional:
- Al restaurar desde Amazon S3, seleccione el espacio IP del clúster de ONTAP en el que residirá el volumen de destino, introduzca la clave de acceso y la clave secreta del usuario que creó para permitir el acceso del clúster ONTAP al bloque de S3, Y, opcionalmente, elegir un extremo privado VPC para una transferencia de datos segura.
  - Al restaurar desde Azure Blob, seleccione el espacio IP en el clúster de ONTAP donde reside el volumen de destino, seleccione la suscripción de Azure para acceder al almacenamiento de objetos y, opcionalmente, elija un extremo privado para la transferencia de datos segura mediante la selección de la red y la subred.
  - Al restaurar desde Google Cloud Storage, seleccione Google Cloud Project y Access Key y Secret Key para acceder al almacenamiento de objetos, la región donde se almacenan los backups y el espacio IP del clúster de ONTAP donde reside el volumen de destino.
  - Al restaurar desde StorageGRID, introduzca el FQDN del servidor StorageGRID y el puerto que ONTAP debe usar para la comunicación HTTPS con StorageGRID, seleccione la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP del clúster ONTAP donde reside el volumen de destino.
  - Cuando se restaure desde ONTAP S3, introduzca el FQDN del servidor ONTAP S3 y el puerto que ONTAP debe utilizar para la comunicación HTTPS con ONTAP S3, seleccione la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos. y el espacio IP del clúster de ONTAP donde residirá el volumen de destino.
    - a. Introduzca el nombre que desea usar para el volumen restaurado y seleccione la máquina virtual de almacenamiento y el agregado donde reside el volumen. Cuando restaure un volumen de FlexGroup, deberá seleccionar varios agregados. De forma predeterminada, se utiliza **<source\_volume\_name>\_restore** como nombre del volumen.

| Select Destination                                                                                                                                                                                                                                                                                                                                                      |  |                       |                                   |               |               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|-----------------------|-----------------------------------|---------------|---------------|
| <div> <div> <div>✓</div> <div>Selected Working Environment</div> <div>Working Environment Name 2</div> </div> <div> <div>📁</div> <div>Destination Volume &gt;</div> <div>General_restore</div> </div> </div>                                                                                                                                                            |  |                       |                                   |               |               |
| <div> <div> <div>📘</div> <div>A new volume will be created in the working environment based on the backup you selected</div> </div> <div> <div>Volume Name</div> <div>General_restore</div> </div> <div> <div>Storage VM</div> <div>svm1</div> </div> <div> <div>Aggregate</div> <div>aggr2</div> </div> <div> <div>Restore Priority</div> <div>Low</div> </div> </div> |  |                       |                                   |               |               |
| <div> <div>Volume Information</div> <table border="1"> <tr> <td>Volume Size: 50.00 GB</td> </tr> <tr> <td>Backup Policy: CloudBackupService</td> </tr> <tr> <td>Protocol: NFS</td> </tr> <tr> <td>Disk Type: RW</td> </tr> </table> </div>                                                                                                                              |  | Volume Size: 50.00 GB | Backup Policy: CloudBackupService | Protocol: NFS | Disk Type: RW |
| Volume Size: 50.00 GB                                                                                                                                                                                                                                                                                                                                                   |  |                       |                                   |               |               |
| Backup Policy: CloudBackupService                                                                                                                                                                                                                                                                                                                                       |  |                       |                                   |               |               |
| Protocol: NFS                                                                                                                                                                                                                                                                                                                                                           |  |                       |                                   |               |               |
| Disk Type: RW                                                                                                                                                                                                                                                                                                                                                           |  |                       |                                   |               |               |

Al restaurar un backup desde un almacenamiento de objetos a un sistema Cloud Volumes ONTAP mediante ONTAP 9.13.0 o posterior, o a un sistema ONTAP on-premises que ejecuta ONTAP 9.14.1, tendrá la opción de realizar una operación *quick restore*.

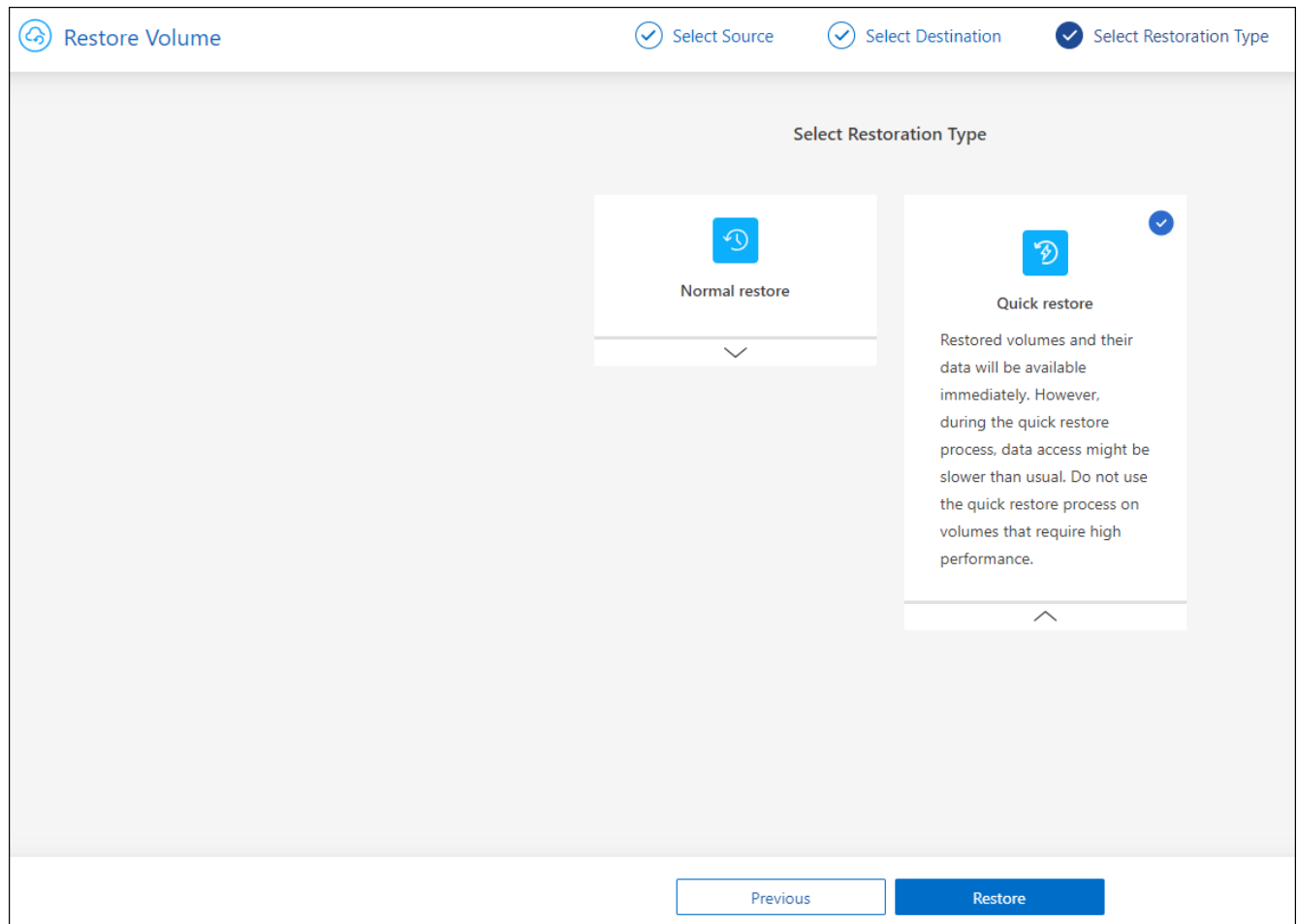
Además, si va a restaurar el volumen a partir de un archivo de backup que reside en un nivel de almacenamiento de archivado (disponible a partir de ONTAP 9.10.1), puede seleccionar la prioridad de restauración.

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS"](#).

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de Azure"](#).

["Más información sobre cómo restaurar a partir del almacenamiento de archivado de Google"](#). Los archivos de copia de seguridad del nivel de almacenamiento de Google Archive se restauran casi inmediatamente y no requieren prioridad de restauración.

1. Haga clic en **Siguiente** para elegir si desea realizar una restauración normal o un proceso de restauración rápida:



- **Restauración normal:** Utilice la restauración normal en volúmenes que requieren un alto rendimiento. Los volúmenes no estarán disponibles hasta que se complete el proceso de restauración.
- **Restauración rápida:** Volúmenes y datos restaurados estarán disponibles inmediatamente. No lo use en volúmenes que requieran un alto rendimiento porque, durante el proceso de restauración rápida, el acceso a los datos puede ser más lento que lo habitual.

2. Haga clic en **Restaurar** y volverá al Panel de restauración para que pueda revisar el progreso de la operación de restauración.

## Resultado

El backup y la recuperación de BlueXP crea un nuevo volumen basado en el backup que has seleccionado.

Tenga en cuenta que la restauración de un volumen a partir de un archivo de backup que reside en el almacenamiento de archivado puede tardar varios minutos u horas, según el nivel de archivado y la prioridad de restauración. Puede hacer clic en la ficha **Supervisión de trabajos** para ver el progreso de la restauración.

## Restaure carpetas y archivos utilizando examinar & Restore

Si necesita restaurar sólo algunos archivos de un backup de volúmenes de ONTAP, puede optar por restaurar una carpeta o archivos individuales en lugar de restaurar el volumen completo. Es posible restaurar carpetas y archivos a un volumen existente en el entorno de trabajo original o a un entorno de trabajo diferente que utilice la misma cuenta de cloud. También puede restaurar carpetas y archivos en un volumen de un sistema ONTAP en las instalaciones.



Puede restaurar una carpeta o archivos individuales solo desde un archivo de backup en el almacenamiento de objetos en este momento. Actualmente, no se admite la restauración de archivos y carpetas desde una copia de instantánea local o desde un archivo de respaldo que reside en un entorno de trabajo secundario (un volumen replicado).

Si selecciona varios archivos, todos los archivos se restauran en el mismo volumen de destino que se elija. Por lo tanto, si desea restaurar archivos en diferentes volúmenes, deberá ejecutar el proceso de restauración varias veces.

Si utiliza ONTAP 9.13.0 o superior, puede restaurar una carpeta junto con todos los archivos y subcarpetas dentro de ella. Cuando se utiliza una versión de ONTAP anterior a la 9.13.0, solo se restauran los archivos de esa carpeta, no se restauran ni las subcarpetas ni los archivos de esas carpetas.



- Si el archivo de backup se configuró con protección DataLock & Ransomware, la restauración en el nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o superior. Si utiliza una versión anterior de ONTAP, puede restaurar el volumen entero desde el archivo de backup y luego acceder a la carpeta y los archivos que necesita.
- Si el archivo de backup reside en un almacenamiento de archivado, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o posterior. Si utiliza una versión anterior de ONTAP, puede restaurar la carpeta desde un archivo de backup más reciente que no se haya archivado, o puede restaurar todo el volumen desde el backup archivado y, a continuación, acceder a la carpeta y los archivos que necesita.
- Con ONTAP 9.15.1, puede restaurar carpetas de FlexGroup utilizando la opción «Examinar y restaurar». Esta función se encuentra en el modo Vista previa de tecnología.

Puede probarlo utilizando un indicador especial descrito en el ["Backup y recuperación de BlueXP Julio 2024 Release blog"](#).

## Requisitos previos

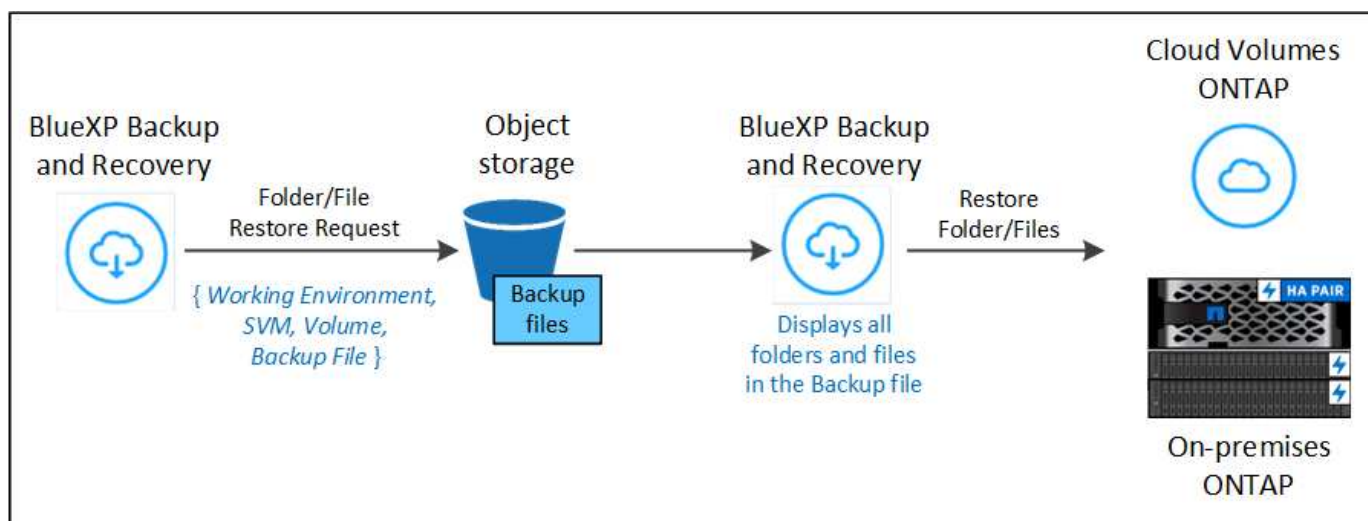
- La versión de ONTAP debe ser 9.6 o superior para realizar operaciones de restauración *File*.
- La versión de ONTAP debe ser 9.11.1 o superior para realizar operaciones de restauración de *folder*. Se requiere ONTAP versión 9.13.1 si los datos se encuentran en el almacenamiento de archivado o si el archivo de copia de seguridad utiliza DataLock y protección contra ransomware.
- La versión de ONTAP debe ser 9.15.1 P2 o superior para restaurar directorios de FlexGroup mediante la opción Examinar y restaurar.

## Proceso de restauración de carpetas y archivos

El proceso va como este:

1. Cuando desee restaurar una carpeta o uno o más archivos desde una copia de seguridad de volumen, haga clic en la ficha **Restaurar** y haga clic en **Restaurar archivos o carpeta** en *Browse & Restore*.
2. Seleccione el entorno de trabajo de origen, el volumen y el archivo de copia de seguridad en el que residen la carpeta o los archivos.
3. La copia de seguridad y recuperación de BlueXP muestra las carpetas y archivos que existen dentro del archivo de copia de seguridad seleccionado.
4. Seleccione la carpeta o los archivos que desea restaurar a partir de esa copia de seguridad.
5. Seleccione la ubicación de destino en la que desea restaurar la carpeta o los archivos (el entorno de trabajo, el volumen y la carpeta) y haga clic en **Restaurar**.

6. Se restauran los archivos.

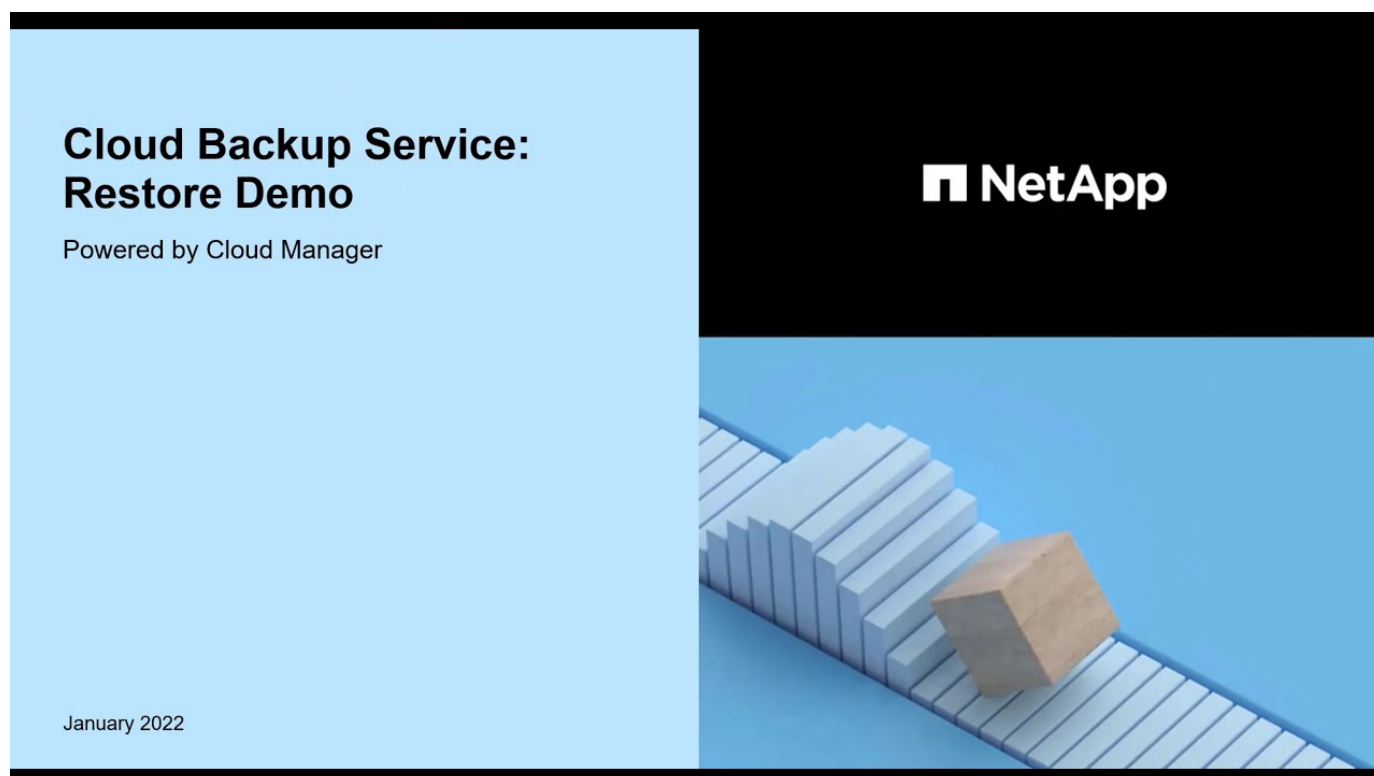


Como puede ver, necesita conocer el nombre del entorno de trabajo, el nombre del volumen, la fecha del archivo de copia de seguridad y el nombre de carpeta/archivo para realizar una restauración de carpetas o archivos.

#### Restaurar carpetas y archivos

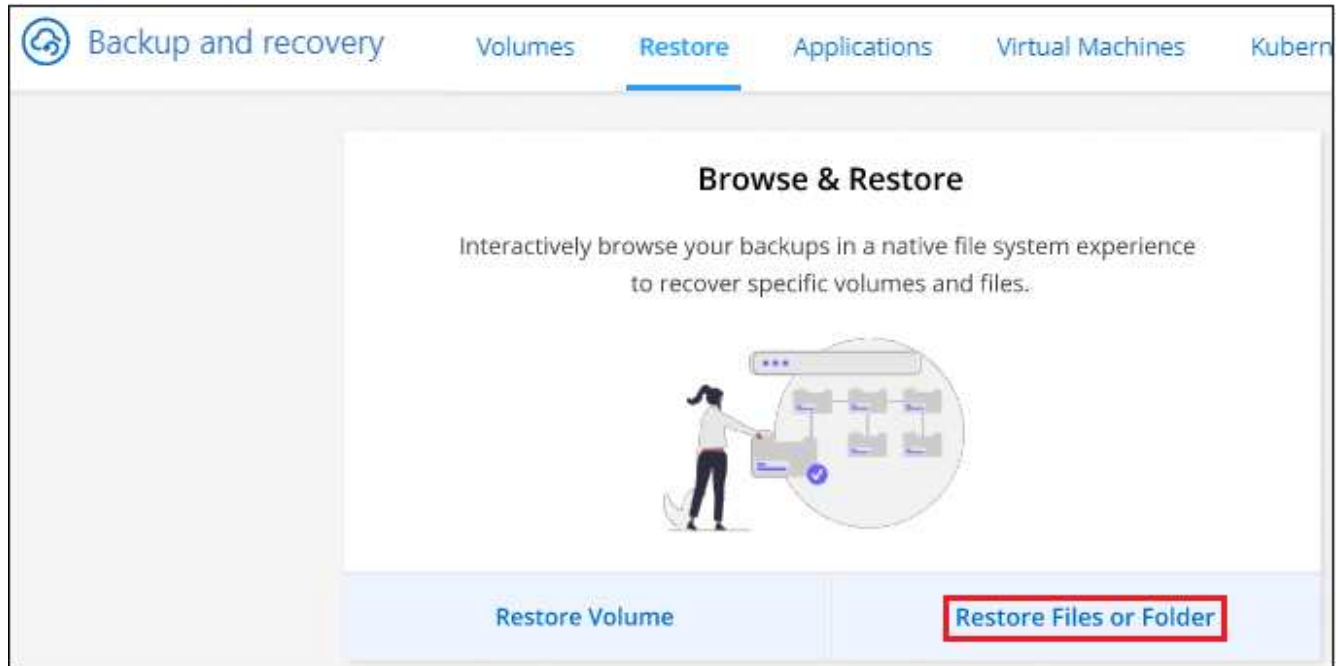
Siga estos pasos para restaurar carpetas o archivos en un volumen a partir de un backup de volumen de ONTAP. Debe conocer el nombre del volumen y la fecha del archivo de backup que desea utilizar para restaurar la carpeta o los archivos. Esta funcionalidad utiliza Live Browsing para que pueda ver la lista de directorios y archivos dentro de cada archivo de copia de seguridad.

El siguiente vídeo muestra un tutorial rápido sobre cómo restaurar un único archivo:

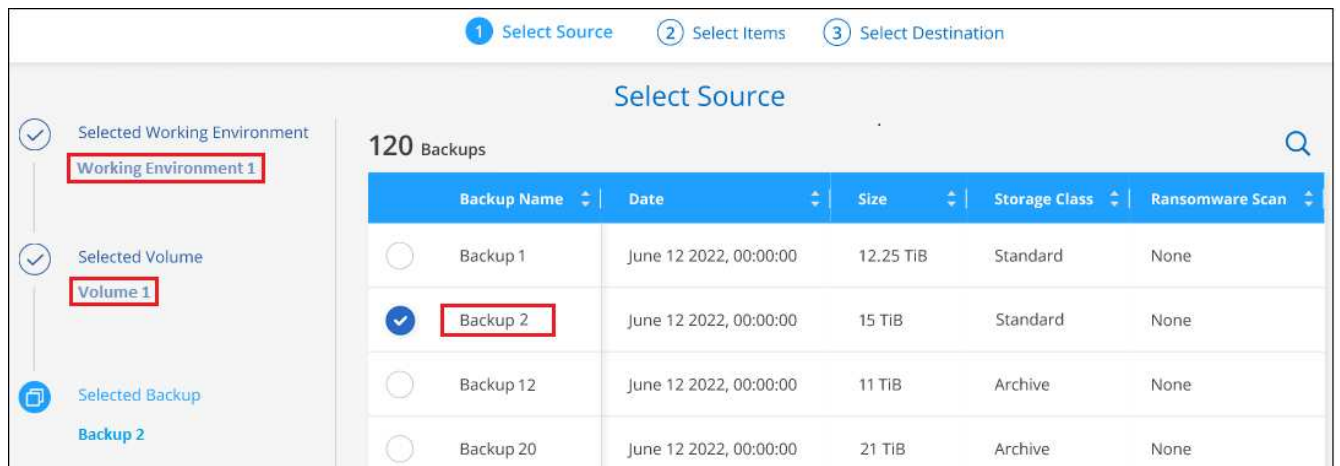


## Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Restaurar** y aparecerá el Panel de restauración.
3. En la sección *Browse & Restore*, haga clic en **Restaurar archivos o carpeta**.



4. En la página *Select Source*, desplácese hasta el archivo de copia de seguridad del volumen que contiene la carpeta o los archivos que desea restaurar. Seleccione **entorno de trabajo, volumen y copia de seguridad** que tenga la Marca de fecha/hora desde la que desea restaurar archivos.



5. Haga clic en **Siguiente** y aparecerá la lista de carpetas y archivos de la copia de seguridad de volumen.

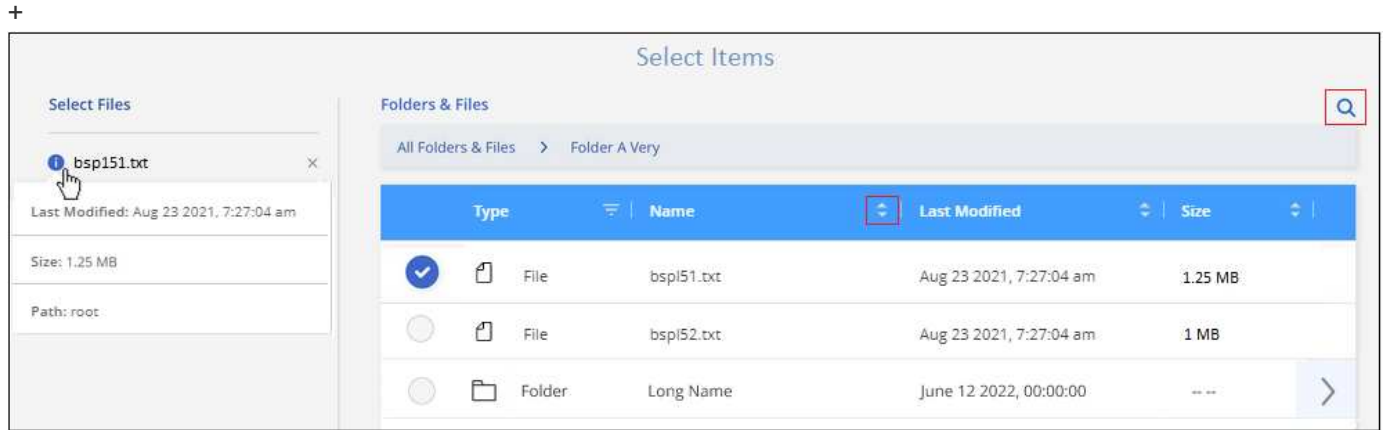
Si va a restaurar carpetas o archivos desde un archivo de copia de seguridad que reside en un nivel de almacenamiento de archivado, puede seleccionar la prioridad de restauración.

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS"](#).

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de Azure"](#).

"[Más información sobre cómo restaurar a partir del almacenamiento de archivado de Google](#)". Los archivos de copia de seguridad del nivel de almacenamiento de Google Archive se restauran casi inmediatamente y no requieren prioridad de restauración.

Y, si la protección contra ransomware está activa para el archivo de backup (si habilitó DataLock y Ransomware Protection en la política de backup), se le pedirá que ejecute un análisis adicional de ransomware en el archivo de backup antes de restaurar los datos. Se recomienda que escanee el archivo de backup como ransomware. (Incurrirá en costes adicionales de salida de su proveedor de cloud para acceder al contenido del archivo de backup).

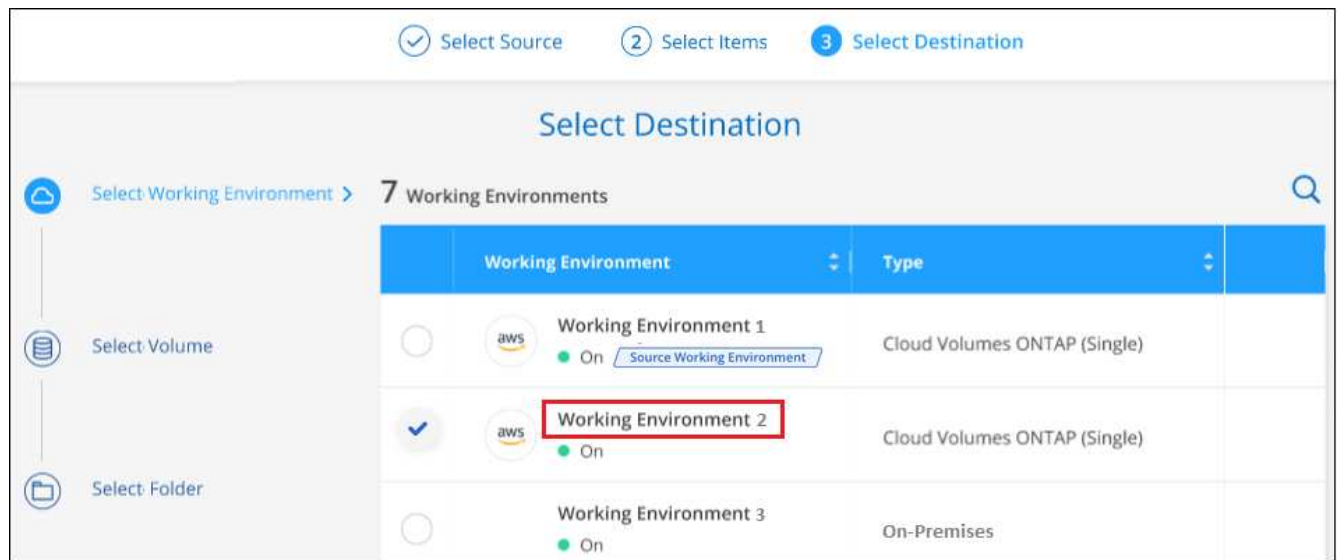


1. En la página *Select ITEMS*, seleccione la carpeta o los archivos que desea restaurar y haga clic en **continuar**. Para ayudarle a encontrar el elemento:
  - Si lo ve, puede hacer clic en la carpeta o en el nombre del archivo.
  - Puede hacer clic en el icono de búsqueda e introducir el nombre de la carpeta o archivo para desplazarse directamente al elemento.
  - Puede desplazarse por los niveles de las carpetas mediante  al final de la fila para buscar archivos específicos.

A medida que seleccione los archivos, se agregarán a la parte izquierda de la página para que pueda ver los archivos que ya ha elegido. Si es necesario, puede eliminar un archivo de esta lista haciendo clic en **x** junto al nombre del archivo.

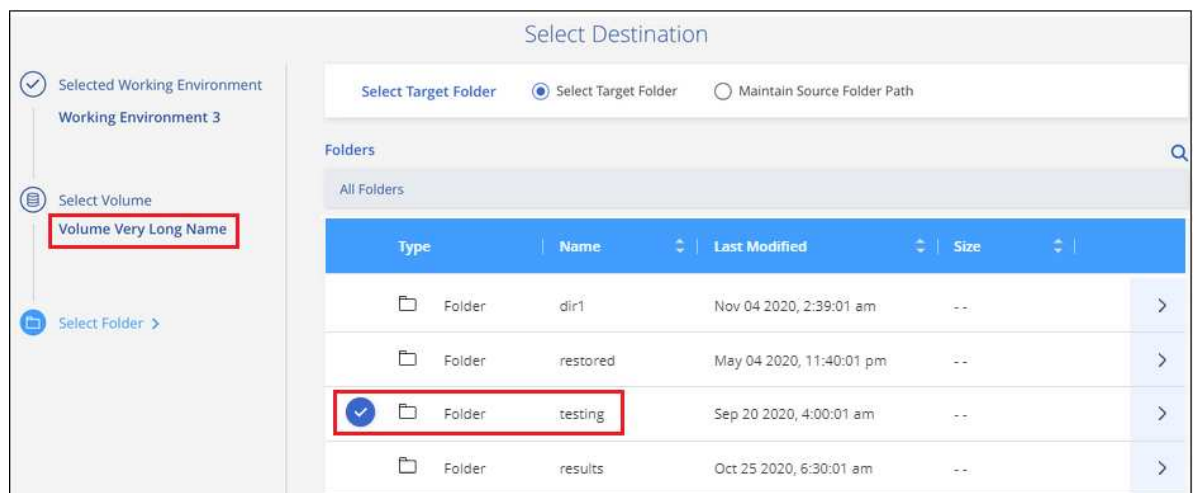
2. En la página *Select Destination*, seleccione **entorno de trabajo** donde desea restaurar los elementos.





Si selecciona un clúster en las instalaciones y no ha configurado todavía la conexión de clúster con el almacenamiento de objetos, se le pedirá información adicional:

- Al restaurar desde Amazon S3, introduzca el espacio IP del clúster de ONTAP donde se encuentra el volumen de destino y la clave secreta y de acceso AWS se necesitan para acceder al almacenamiento de objetos. También puede seleccionar una configuración de vínculo privado para la conexión al clúster.
  - Al restaurar desde Azure Blob, introduzca el espacio IP en el clúster de ONTAP donde reside el volumen de destino. También puede seleccionar una configuración de extremo privado para la conexión con el clúster.
  - Al restaurar desde Google Cloud Storage, introduzca el espacio IP en el clúster de ONTAP en el que residen los volúmenes de destino y la clave secreta y de acceso necesaria para acceder al almacenamiento de objetos.
  - Al restaurar desde StorageGRID, introduzca el FQDN del servidor StorageGRID y el puerto que ONTAP debe usar para la comunicación HTTPS con StorageGRID, introduzca la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP del clúster ONTAP en el que reside el volumen de destino.
- a. A continuación, seleccione **volumen** y **carpeta** donde desea restaurar la carpeta o los archivos.





Tiene varias opciones para la ubicación al restaurar carpetas y archivos.

- Cuando haya elegido **Seleccionar carpeta de destino**, como se muestra arriba:
  - Puede seleccionar cualquier carpeta.
  - Puede pasar el ratón sobre una carpeta y hacer clic en  al final de la fila para explorar subcarpetas y, a continuación, seleccione una carpeta.
- Si ha seleccionado el mismo entorno de trabajo y volumen de destino en el que se encontraba la carpeta/archivo de origen, puede seleccionar **mantener ruta de carpeta de origen** para restaurar la carpeta o archivos a la misma carpeta en la que existían en la estructura de origen. Ya deben existir todas las mismas carpetas y subcarpetas; no se crean las carpetas. Al restaurar los archivos a su ubicación original, puede elegir sobrescribir los archivos de origen o crear nuevos archivos.
  - a. Haga clic en **Restaurar** y volverá al Panel de restauración para que pueda revisar el progreso de la operación de restauración. También puede hacer clic en la ficha **Supervisión de trabajos** para ver el progreso de la restauración.

## Restaura datos de ONTAP con Search & Restore

Es posible restaurar un volumen, una carpeta o archivos desde un archivo de backup de ONTAP mediante Search & Restore. Search & Restore permite buscar un volumen, una carpeta o un archivo específicos de todos los backups y, a continuación, ejecutar una restauración. No es necesario que sepa el nombre exacto del entorno de trabajo, el nombre del volumen o el nombre de archivo; la búsqueda busca a través de todos los archivos de copia de seguridad del volumen.

La operación de búsqueda busca todas las copias Snapshot locales que existen para los volúmenes ONTAP, todos los volúmenes replicados en los sistemas de almacenamiento secundario y todos los archivos de backup existentes en el almacenamiento de objetos. Como restaurar datos desde una copia Snapshot local o un volumen replicado puede ser más rápido y menos costoso que la restauración desde un archivo de backup en un almacenamiento de objetos, quizás desee restaurar datos desde estas otras ubicaciones.

Cuando restaura un *full volume* desde un archivo de backup, el backup y la recuperación de BlueXP crean un volumen *new* con los datos del backup. Puede restaurar los datos como un volumen en el entorno de trabajo original, en un entorno de trabajo diferente ubicado en la misma cuenta de cloud que el entorno de trabajo de origen o en un sistema ONTAP on-premises.

Puede restaurar *carpetas o archivos* a la ubicación del volumen original, a otro volumen en el mismo entorno de trabajo, a un entorno de trabajo diferente que utilice la misma cuenta de cloud o a un volumen en un sistema ONTAP local.

Si utiliza ONTAP 9.13.0 o superior, puede restaurar una carpeta junto con todos los archivos y subcarpetas dentro de ella. Cuando se utiliza una versión de ONTAP anterior a la 9.13.0, solo se restauran los archivos de esa carpeta, no se restauran ni las subcarpetas ni los archivos de esas carpetas.

Si el archivo de backup del volumen que desea restaurar reside en el almacenamiento de archivado (disponible a partir de ONTAP 9.10.1), la operación de restauración tardará más tiempo y generará costes adicionales. Tenga en cuenta que el clúster de destino también debe ejecutar ONTAP 9.10.1 o superior para la restauración de volúmenes, 9.11.1 para la restauración de archivos, 9.12.1 para Google Archive y StorageGRID y 9.13.1 para la restauración de carpetas.

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS".](#)

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de Azure".](#)

["Más información sobre cómo restaurar a partir del almacenamiento de archivado de Google".](#)



- Si el archivo de backup del almacenamiento de objetos se configuró con protección DataLock y Ransomware, la restauración en el nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o posterior. Si utiliza una versión anterior de ONTAP, puede restaurar el volumen entero desde el archivo de backup y luego acceder a la carpeta y los archivos que necesita.
- Si el archivo de backup del almacenamiento de objetos reside en un almacenamiento de archivado, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o posterior. Si utiliza una versión anterior de ONTAP, puede restaurar la carpeta desde un archivo de backup más reciente que no se haya archivado, o puede restaurar todo el volumen desde el backup archivado y, a continuación, acceder a la carpeta y los archivos que necesita.
- La prioridad de restauración «Alta» no se admite al restaurar datos desde el almacenamiento de archivado de Azure en sistemas StorageGRID.
- Actualmente, no se admite la restauración de carpetas desde los volúmenes en el almacenamiento de objetos de ONTAP S3.

Antes de empezar, debe tener idea del nombre o la ubicación del volumen o el archivo que desea restaurar.

El siguiente vídeo muestra un tutorial rápido sobre cómo restaurar un único archivo:



### Entornos de trabajo compatibles con Search & Restore y proveedores de almacenamiento de objetos

Es posible restaurar datos ONTAP desde un archivo de backup que se encuentra en un entorno de trabajo secundario (un volumen replicado) o en almacenamiento de objetos (un archivo de backup) para los siguientes entornos de trabajo. Las copias Snapshot residen en el entorno de trabajo de origen y se pueden restaurar únicamente en ese mismo sistema.

**Nota:** Puede restaurar volúmenes y archivos de cualquier tipo de archivo de copia de seguridad, pero puede restaurar una carpeta solo desde archivos de copia de seguridad en el almacenamiento de objetos en este

momento.

| Ubicación del archivo de copia de seguridad |                                                                     | Entorno de trabajo de destino                                                                          |
|---------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Almacén de objetos (Backup)                 | Sistema secundario (Replicación)                                    | ifdef::aws[]                                                                                           |
| Amazon S3                                   | Cloud Volumes ONTAP en AWS<br>Sistema ONTAP en las instalaciones    | Cloud Volumes ONTAP en la endif del sistema ONTAP en las instalaciones de AWS::aws[]<br>ifdef::Azure[] |
| Azure Blob                                  | Cloud Volumes ONTAP en Azure<br>Sistema ONTAP en las instalaciones  | Cloud Volumes ONTAP en Azure<br>on-premises ONTAP system<br>endif::Azure[] ifdef::gcp[]                |
| Google Cloud Storage                        | Cloud Volumes ONTAP en Google<br>Sistema ONTAP en las instalaciones | Cloud Volumes ONTAP en Google<br>on-local ONTAP system endif::gcp[]                                    |
| StorageGRID de NetApp                       | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           | Sistema ONTAP en las instalaciones                                                                     |
| ONTAP S3                                    | Sistema ONTAP en las instalaciones<br>Cloud Volumes ONTAP           | Sistema ONTAP en las instalaciones                                                                     |

Para Buscar y restaurar, el conector se puede instalar en las siguientes ubicaciones:

- Para Amazon S3, el conector puede ponerse en marcha en AWS o en sus instalaciones
- Para Azure Blob, el conector se puede poner en marcha en Azure o en sus instalaciones
- Para Google Cloud Storage, el conector se debe poner en marcha en su VPC de Google Cloud Platform
- Para StorageGRID, el conector debe estar desplegado en sus instalaciones, con o sin acceso a Internet
- Para ONTAP S3, el conector se puede implementar en sus instalaciones (con o sin acceso a Internet) o en un entorno de proveedor de cloud

Tenga en cuenta que las referencias a "sistemas ONTAP en las instalaciones" incluyen sistemas FAS, AFF y ONTAP Select.

## Requisitos previos

- Requisitos del clúster:
  - La versión de ONTAP debe ser 9.8 o superior.
  - La máquina virtual de almacenamiento (SVM) en la que reside el volumen debe tener una LIF de datos configurada.
  - Debe habilitarse NFS en el volumen (se admiten los volúmenes NFS y SMB/CIFS).
  - El servidor RPC de SnapDiff debe estar activado en la SVM. BlueXP hace esto automáticamente al activar la indización en el entorno de trabajo. (SnapDiff es la tecnología que identifica rápidamente las diferencias en archivos y directorios entre las copias snapshot).
- Requisitos de AWS:
  - Deben añadirse permisos específicos de Amazon Athena, AWS Glue y AWS S3 a la función de

usuario que proporciona BlueXP con permisos. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Tenga en cuenta que, si ya estaba utilizando la copia de seguridad y la recuperación de BlueXP con un conector que configuró en el pasado, deberá añadir los permisos de Athena y Glue al rol de usuario de BlueXP ahora. Son necesarios para buscar y restaurar.

- Requisitos de Azure:

- Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") en su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#). Debe ser Subscription **Owner** o **Contributor** para registrar el proveedor de recursos.
- Los permisos específicos de cuentas de almacenamiento de áreas de trabajo y lagos de datos de Azure Synapse deben agregarse a la función de usuario que proporciona permisos a BlueXP. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Tenga en cuenta que, si ya estaba utilizando el backup y la recuperación de BlueXP con un conector que configuró en el pasado, deberá añadir los permisos de la cuenta de almacenamiento de lago de datos y espacio de trabajo de Azure Synapse Workspace ahora al rol de usuario de BlueXP. Son necesarios para buscar y restaurar.

- El conector debe configurarse **sin** un servidor proxy para la comunicación HTTP a Internet. Si ha configurado un servidor proxy HTTP para su conector, no podrá utilizar la funcionalidad de búsqueda y restauración.

- Requisitos de Google Cloud:

- Se deben agregar permisos específicos de Google BigQuery a la función de usuario que proporciona permisos a BlueXP. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Ten en cuenta que, si ya utilizabas la copia de seguridad y la recuperación de BlueXP con un conector que configuraste en el pasado, tendrás que añadir los permisos de BigQuery al rol de usuario de BlueXP ahora. Son necesarios para buscar y restaurar.

- Requisitos de StorageGRID y ONTAP S3:

Dependiendo de la configuración, hay dos formas de implementar Search & Restore:

- Si su cuenta no tiene credenciales de proveedor de cloud, la información del catálogo indexado se almacena en el conector.

Para obtener información sobre el catálogo indexado v2, consulte la sección siguiente acerca de cómo activar el catálogo indexado.

- Si utiliza un conector en un sitio privado (oscuro), la información del catálogo indexado se almacena en el conector (requiere la versión 3.9.25 o superior del conector).
- Si lo tiene ["Credenciales de AWS"](#) o ["Credenciales de Azure"](#) En la cuenta, el catálogo indexado se almacena en el proveedor de cloud, al igual que con un conector puesto en marcha en el cloud. (Si tiene ambas credenciales, AWS está seleccionado de forma predeterminada.)

Aunque utilice un conector en las instalaciones, deben cumplir los requisitos del proveedor de cloud tanto para los permisos de Connector como para los recursos del proveedor de cloud. Consulte los requisitos anteriores de AWS y Azure al utilizar esta implementación.

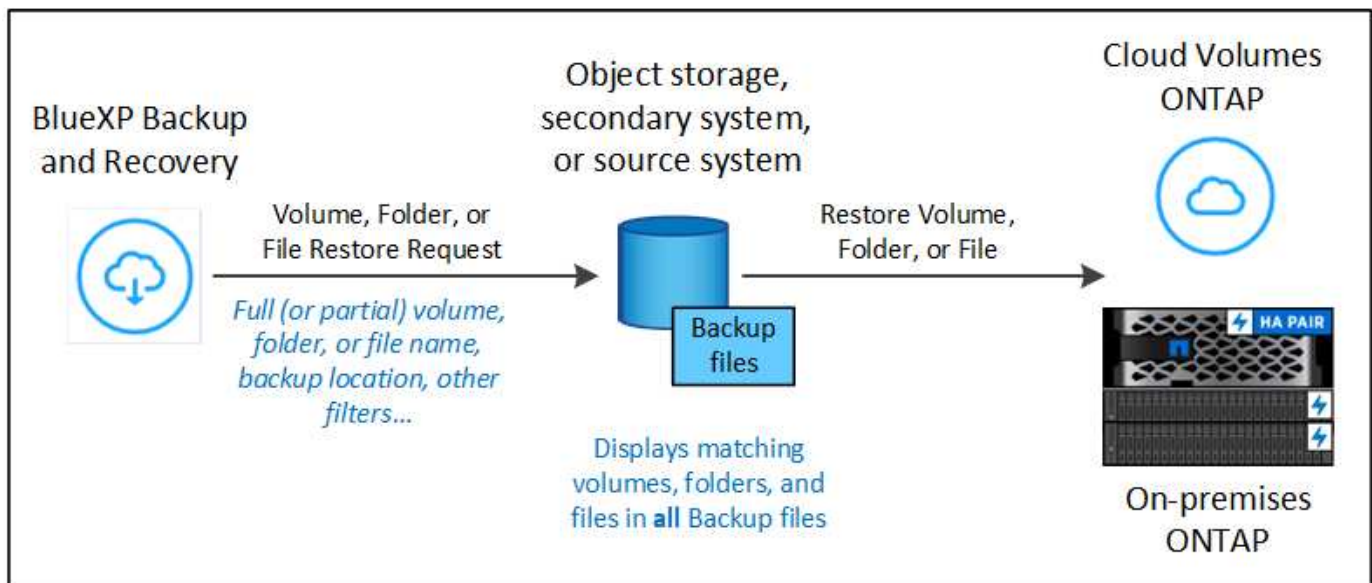
## Proceso de búsqueda y restauración

El proceso va como este:

1. Para poder utilizar Search & Restore, debe habilitar "Indexing" en cada entorno de trabajo de origen desde el que desea restaurar datos de volumen. De este modo, el catálogo indexado puede realizar un seguimiento de los archivos de copia de seguridad de cada volumen.
2. Cuando desee restaurar un volumen o archivos de una copia de seguridad de volumen, en *Search & Restore*, haga clic en **Search & Restore**.
3. Introduzca los criterios de búsqueda para un volumen, carpeta o archivo por nombre de volumen parcial o completo, nombre de archivo parcial o completo, ubicación de backup, rango de tamaños, rango de fechas de creación, otros filtros de búsqueda, Y haga clic en **Buscar**.

La página resultados de la búsqueda muestra todas las ubicaciones que tienen un archivo o volumen que coincide con sus criterios de búsqueda.

4. Haga clic en **Ver todas las copias de seguridad** para la ubicación que desee utilizar para restaurar el volumen o el archivo y, a continuación, haga clic en **Restaurar** en el archivo de copia de seguridad real que desee utilizar.
5. Seleccione la ubicación en la que desea restaurar el volumen, la carpeta o los archivos y haga clic en **Restaurar**.
6. Se restauran el volumen, la carpeta o los archivos.



Como puedes ver, realmente solo necesitas saber un nombre parcial y las búsquedas de backup y recuperación de BlueXP a través de todos los archivos de copia de seguridad que coincidan con tu búsqueda.

### Active el catálogo indexado para cada entorno de trabajo

Antes de poder utilizar Buscar y restaurar, debe habilitar la función "indexación" en cada entorno de trabajo de origen desde el que planea restaurar volúmenes o archivos. Esto permite al catálogo indexado realizar un seguimiento de cada volumen y cada archivo de copia de seguridad, lo que hace que las búsquedas sean muy rápidas y eficaces.

El catálogo indexado es una base de datos que almacena metadatos sobre todos los volúmenes y archivos de copia de seguridad del entorno de trabajo. La función de búsqueda y restauración lo utiliza para encontrar

rápidamente los archivos de copia de seguridad que contienen los datos que desea restaurar.

### Características del catálogo indexado v2

El catálogo indexado v2, lanzado en febrero de 2025, tiene nuevas características que lo hacen más eficiente y fácil de usar. Esta versión tiene una mejora significativa del rendimiento y está habilitada por defecto para todos los nuevos clientes.

Revise las siguientes consideraciones con respecto a v2:

- El catálogo indexado v2 está disponible en modo de vista previa.
- Si ya es cliente y desea utilizar el Catálogo v2, debe volver a indexar completamente su entorno.
- El Catálogo v2 indexa sólo las instantáneas que tienen una etiqueta de instantánea.
- Los backups y las recuperaciones de BlueXP no indexan los snapshots con etiquetas de SnapMirror cada hora. Si desea indexar las instantáneas con la etiqueta SnapMirror "horaria", debe habilitarla manualmente mientras el v2 está en modo de vista previa.
- Las funciones de backup y recuperación de BlueXP indicarán los volúmenes y las instantáneas asociadas a entornos de trabajo protegidos por el backup y la recuperación de BlueXP sólo con el Catálogo v2. Otros entornos de trabajo descubiertos en la plataforma BlueXP no se indexarán.

El catálogo indexado v2 admite lo siguiente:

- Eficacia de la búsqueda global en menos de 3 minutos
- Hasta 5 millones de archivos
- Hasta 5000 volúmenes por clúster
- Hasta 100K snapshots por volumen
- El tiempo máximo para la indexación de línea base es inferior a 7 días. El tiempo real variará según tu entorno.

### Activación del catálogo indexado para un entorno de trabajo

Cuando habilita esta funcionalidad, el backup y recuperación de BlueXP permite utilizar SnapDiff v3 en la SVM para los volúmenes y realiza las siguientes acciones:

- Para los backups almacenados en AWS, aprovisiona un nuevo bloque de S3 y el ["Servicio de consultas interactivas de Amazon Athena"](#) y.. ["Servicio de integración de datos sin servidor de AWS"](#).
- Para los backups almacenados en Azure, aprovisiona un espacio de trabajo Azure Synapse y un sistema de archivos Data Lake como el contenedor donde se almacenan los datos del espacio de trabajo.
- Para los backups almacenados en Google Cloud, aprovisiona un nuevo bloque y el ["Servicios de Google Cloud BigQuery"](#) se aprovisionan en el nivel de cuenta/proyecto.
- Para los backups almacenados en StorageGRID o ONTAP S3, se aprovisiona el espacio en el conector o en el entorno del proveedor de cloud.

Si ya se ha activado la indización para el entorno de trabajo, vaya a la siguiente sección para restaurar los datos.

### Pasos para activar la indexación para un entorno de trabajo:

1. Debe realizar una de las siguientes acciones:
  - Si no se ha indexado ningún entorno de trabajo, en el Panel de restauración en *Search & Restore*, seleccione **Enable Indexing for Working Environments**.

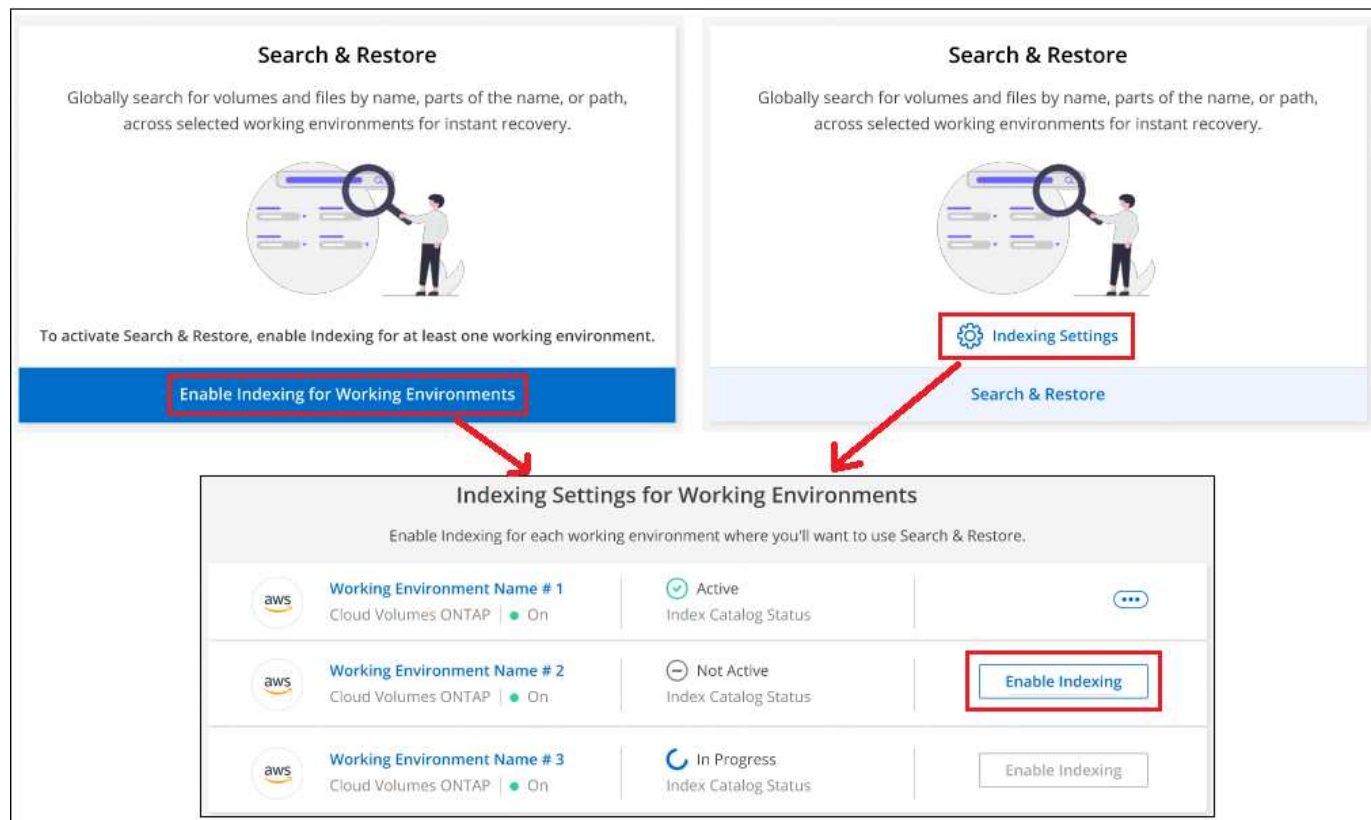


- Si ya se ha indexado al menos un entorno de trabajo, en el Panel de restauración en *Search & Restore*, haga clic en **Configuración de indexación**.

2. Seleccione **Activar indexación** para el entorno de trabajo.

## Resultado

Una vez que se han aprovisionado todos los servicios y se ha activado el catálogo indexado, el entorno de trabajo se muestra como "activo".



Según el tamaño de los volúmenes en el entorno de trabajo y el número de archivos de copia de seguridad en las 3 ubicaciones de copia de seguridad, el proceso inicial de indexación puede tardar hasta una hora. Después, se actualiza de forma transparente cada hora con cambios incrementales para mantenerse al día.

## Restaurar volúmenes, carpetas y archivos mediante la función de restauración de & de búsqueda

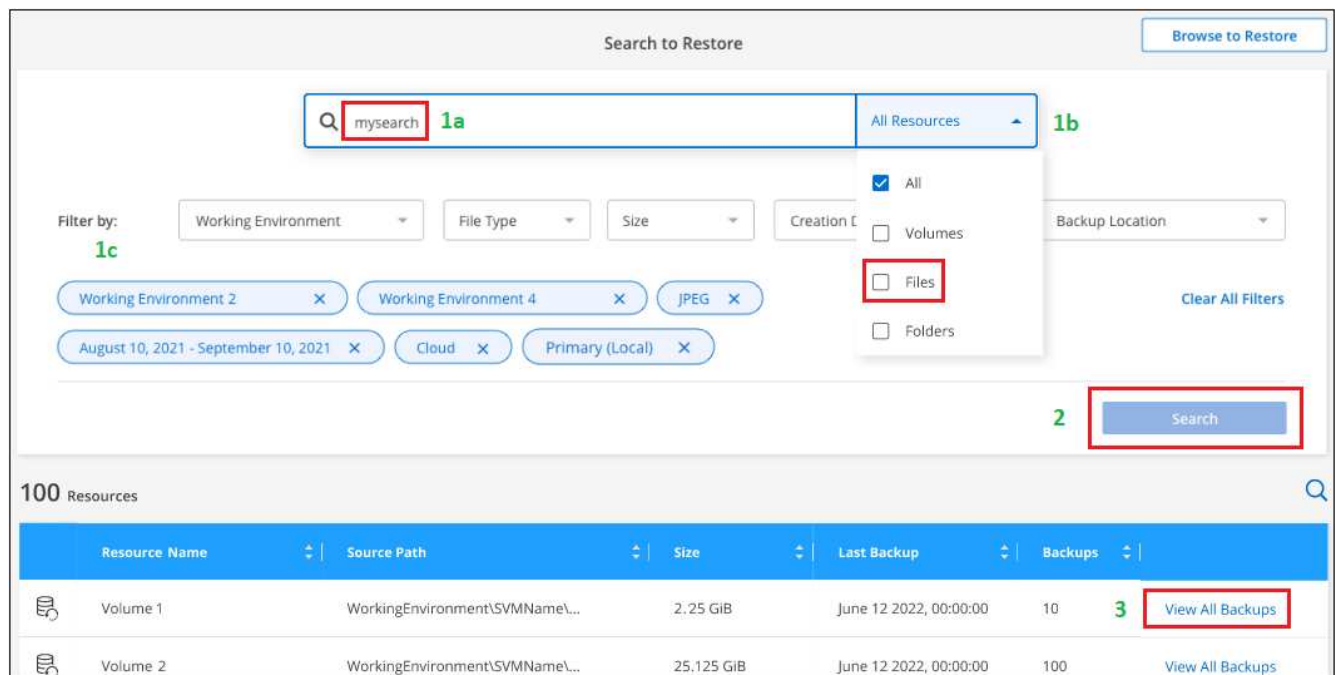
Después de haberlo hecho [Indexación activada para el entorno de trabajo](#), Puede restaurar volúmenes, carpetas y archivos mediante Buscar y restaurar. Esto le permite utilizar una amplia gama de filtros para encontrar el archivo o volumen exacto que desea restaurar desde todos los archivos de copia de seguridad.

## Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Restaurar** y aparecerá el Panel de restauración.
3. En la sección *Search & Restore*, haga clic en **Search & Restore**.

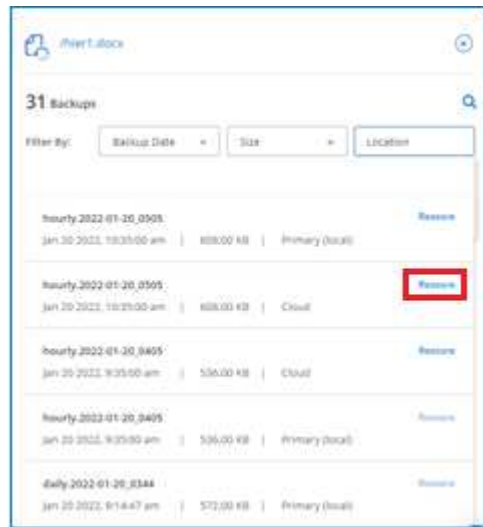


4. Desde la página Buscar en Restaurar:
  - a. En la barra *Search*, introduzca un nombre de volumen completo o parcial, un nombre de carpeta o un nombre de archivo.
  - b. Seleccione el tipo de recurso: **Volúmenes**, **Archivos**, **carpetas** o **todo**.
  - c. En el área *Filter by*, seleccione los criterios de filtro. Por ejemplo, puede seleccionar el entorno de trabajo donde residen los datos y el tipo de archivo, por ejemplo un archivo .JPEG. También puede seleccionar el tipo de Ubicación de backup si desea buscar resultados solo dentro de las copias Snapshot disponibles o los archivos de backup en el almacenamiento de objetos.
5. Haga clic en **Buscar** y el área resultados de la búsqueda mostrará todos los recursos que tengan un archivo, carpeta o volumen que coincida con la búsqueda.



6. Localice el recurso que tiene los datos que desea restaurar y haga clic en **Ver todas las copias de seguridad** para mostrar todos los archivos de copia de seguridad que contienen el volumen, carpeta o archivo coincidentes.





7. Localice el archivo de copia de seguridad que desea utilizar para restaurar los datos y haga clic en **Restaurar**.

Tenga en cuenta que los resultados identifican copias Snapshot de volúmenes locales y volúmenes remotos replicados que contienen el archivo en la búsqueda. Puede elegir restaurar desde el archivo de backup en el cloud, desde la copia Snapshot o desde el volumen replicado.

8. Seleccione la ubicación de destino en la que desea restaurar el volumen, la carpeta o los archivos y haga clic en **Restaurar**.
  - Para los volúmenes, es posible seleccionar el entorno de trabajo de destino original o bien seleccionar un entorno de trabajo alternativo. Cuando restaure un volumen de FlexGroup, debe elegir varios agregados.
  - Para las carpetas, puede restaurar a la ubicación original o seleccionar una ubicación alternativa, incluido el entorno de trabajo, el volumen y la carpeta.
  - Para los archivos, es posible restaurar a la ubicación original o seleccionar una ubicación alternativa, incluido el entorno de trabajo, el volumen y la carpeta. Al seleccionar la ubicación original, puede elegir sobrescribir los archivos de origen o crear archivos nuevos.

Si selecciona un sistema ONTAP en las instalaciones y todavía no ha configurado la conexión de clúster con el almacenamiento de objetos, se le pedirá información adicional:

- Al restaurar desde Amazon S3, seleccione el espacio IP del clúster de ONTAP en el que residirá el volumen de destino, introduzca la clave de acceso y la clave secreta del usuario que creó para permitir el acceso del clúster ONTAP al bloque de S3, Y, opcionalmente, elegir un extremo privado VPC para una transferencia de datos segura. ["Consulte los detalles de estos requisitos"](#).
- Al restaurar desde Azure Blob, seleccione el espacio IP en el clúster de ONTAP donde reside el volumen de destino y, opcionalmente, elija un extremo privado para la transferencia de datos segura mediante la selección de la red y la subred. ["Consulte los detalles de estos requisitos"](#).
- Al restaurar desde Google Cloud Storage, seleccione el espacio IP del clúster de ONTAP en el que residirá el volumen de destino y la clave de acceso y clave secreta para acceder al almacenamiento de objetos. ["Consulte los detalles de estos requisitos"](#).
- Al restaurar desde StorageGRID, introduzca el FQDN del servidor StorageGRID y el puerto que ONTAP debe usar para la comunicación HTTPS con StorageGRID, introduzca la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP del clúster ONTAP en el que reside el volumen de destino. ["Consulte los detalles de estos requisitos"](#).

[requisitos](#)".

- Cuando se restaure desde ONTAP S3, introduzca el FQDN del servidor ONTAP S3 y el puerto que ONTAP debe utilizar para la comunicación HTTPS con ONTAP S3, seleccione la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos. y el espacio IP del clúster de ONTAP donde residirá el volumen de destino. "[Consulte los detalles de estos requisitos](#)".

## Resultados

Se restauran el volumen, la carpeta o los archivos y se devuelve a la consola de restauración para poder revisar el progreso de la operación de restauración. También puede hacer clic en la ficha **Supervisión de trabajos** para ver el progreso de la restauración.

Para los volúmenes restaurados, es posible "[gestione la configuración de backup para este nuevo volumen](#)" según sea necesario.

## Información de copyright

Copyright © 2025 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.