



Realice backups y restauraciones de datos de ONTAP

Cloud Backup

NetApp
March 13, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-backup-restore/aws/concept-ontap-backup-to-cloud.html> on March 13, 2023. Always check docs.netapp.com for the latest.

Tabla de Contenido

- Realice backups y restauraciones de datos de ONTAP 1
 - Proteja los datos de su clúster de ONTAP mediante Cloud Backup 1
 - Realizar backups de los datos de Cloud Volumes ONTAP en Amazon S3 9
 - Realizar backups de datos de ONTAP en las instalaciones en Amazon S3 19
 - Realización de backups de datos de ONTAP en las instalaciones en StorageGRID 33
 - Administrar backups para sus sistemas ONTAP 43
 - Gestión de la configuración de backup en el nivel del clúster 63
 - Restaurar datos ONTAP a partir de archivos de backup 68

Realice backups y restauraciones de datos de ONTAP

Proteja los datos de su clúster de ONTAP mediante Cloud Backup

Cloud Backup proporciona funcionalidades de backup y restauración para protección y archivado a largo plazo de sus datos de clúster de ONTAP. Los backups se generan y almacenan automáticamente en un almacén de objetos en su cuenta de cloud público o privado, independientemente de las copias Snapshot de volumen que se utilicen para la recuperación o el clonado a corto plazo.

Cuando sea necesario, puede restaurar un *volume* completo, un *folder* o uno o más *files*, desde una copia de seguridad en el mismo entorno de trabajo o en un entorno de trabajo diferente.

Funciones

Funciones de backup:

- 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.
- En el caso de los sistemas Cloud Volumes ONTAP, los backups pueden residir en una suscripción/cuenta diferente o en una región diferente.
- 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.

Funciones de restauración:

- Restaure los datos de un momento específico.
- 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.
- Los datos se restauran en el nivel de bloque, colocando los datos directamente en la ubicación especificada, siempre que se conservan las ACL originales.
- Catálogos de archivos que se pueden examinar y realizar búsquedas para seleccionar fácilmente carpetas y archivos individuales para restaurar un solo archivo.

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

Cloud Backup le permite realizar backups de ONTAP Volumes desde los siguientes entornos laborales en el almacenamiento de objetos en los siguientes proveedores de cloud público y privado:

Entorno de trabajo de fuente	Destino de archivo de copia de seguridad ifdef::aws[]
Cloud Volumes ONTAP en AWS	Endif de Amazon S3::aws[] ifdef::Azure[]
Cloud Volumes ONTAP en Azure	Endif de Azure Blob::Azure[] ifdef::gcp[]
Cloud Volumes ONTAP en Google	Fin de Google Cloud Storage::gcp[]
Sistema ONTAP en las instalaciones	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::Azure[] endif de Azure Blob::Azure[] ifdef::gcp[] Google Cloud Storage endif::gcp[] NetApp StorageGRID

Es posible restaurar un volumen, una carpeta o archivos individuales, desde un archivo de backup de ONTAP a los siguientes entornos de trabajo:

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino ifdef::aws[]
Amazon S3	Cloud Volumes ONTAP en la endif del sistema ONTAP en las instalaciones de AWS::aws[] ifdef::Azure[]
Azure Blob	Cloud Volumes ONTAP en Azure on-premises ONTAP system endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Cloud Volumes ONTAP en Google on-local ONTAP system endif::gcp[]
StorageGRID de NetApp	Sistema ONTAP en las instalaciones

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

Compatibilidad con sitios sin conectividad a Internet

Cloud Backup se puede utilizar en un sitio sin conectividad a Internet (también conocido como sitio "sin conexión" o "oscuro") para realizar backups de datos de volumen. Esta configuración también admite tanto la restauración de volúmenes como de archivos. En este caso, deberá desplegar el conector BlueXP en el sitio oscuro.

- Puede realizar backups de datos de sistemas ONTAP locales en las instalaciones en sistemas StorageGRID de NetApp locales. Consulte ["Realización de backups de datos de ONTAP en las instalaciones en StorageGRID"](#) para obtener más detalles.

- Puede realizar backups de los datos de sistemas Cloud Volumes ONTAP instalados en regiones comerciales de AWS y Azure en Amazon S3 o Azure Blob. Consulte ["Realizar backups de los datos de Cloud Volumes ONTAP en Amazon S3"](#) y.. ["Realizar backups de los datos de Cloud Volumes ONTAP en Azure Blob"](#).

Volúmenes compatibles

Cloud Backup admite los siguientes tipos de volúmenes:

- Volúmenes FlexVol de lectura y escritura
- Volúmenes de destino de protección de datos (DP) de SnapMirror
- SnapLock Enterprise Volumes (requiere ONTAP 9.11.1 o posterior)
 - Actualmente, los volúmenes de SnapLock Compliance no son compatibles.
- FlexGroup Volumes (requiere ONTAP 9.12.1 o posterior)

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

Coste

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

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, paga a su proveedor de cloud por los costes de almacenamiento de objetos.

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

- 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.
- Si necesita restaurar datos de volumen de un archivo de backup que se haya movido a almacenamiento de archivado, hay una tasa de recuperación adicional por GIB y una cuota por solicitud del proveedor de cloud.

cargos por servicio

NetApp cobra costes de servicio, por lo que cubre tanto el coste de crear_ backups como los volúmenes o archivos de *restore* de dichos backups. Solo paga por los datos que protege, calculados por la capacidad lógica utilizada de origen (*antes* eficiencia de ONTAP) de los volúmenes de ONTAP de los que se realiza un backup 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

Cloud Backup está disponible 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.



Si adquiere una licencia de BYOL de NetApp, también tendrá que suscribirse a la oferta PAYGO del mercado de su proveedor de cloud. La licencia siempre se cargará primero, pero se cargará a partir de la tarifa por horas en el mercado en estos casos:

- Si supera la capacidad de la licencia
- Si el período de su licencia caduca

Si tiene un contrato anual desde un mercado, se le cobrará todo el consumo de Cloud Backup con relación a dicho contrato. No se puede mezclar y combinar un contrato anual de mercado con una licencia propia.

Con su propia licencia

BYOL se basa en el plazo (12, 24 o 36 meses) 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.

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

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

Suscripción de pago por uso

Cloud Backup ofrece licencias basadas en consumo en un modelo de pago por uso. Después de suscribirse a través del mercado de su proveedor de 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 se utiliza AWS, hay dos contratos anuales disponibles para períodos de 12, 24 o 36 meses:

- 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 le permite agrupar Cloud Volumes ONTAP y Cloud Backup. Esto incluye backups ilimitados de volúmenes de Cloud Volumes ONTAP cargados con esta licencia (la capacidad de backup no se cuenta con la licencia).

"Aprenda a establecer contratos anuales".

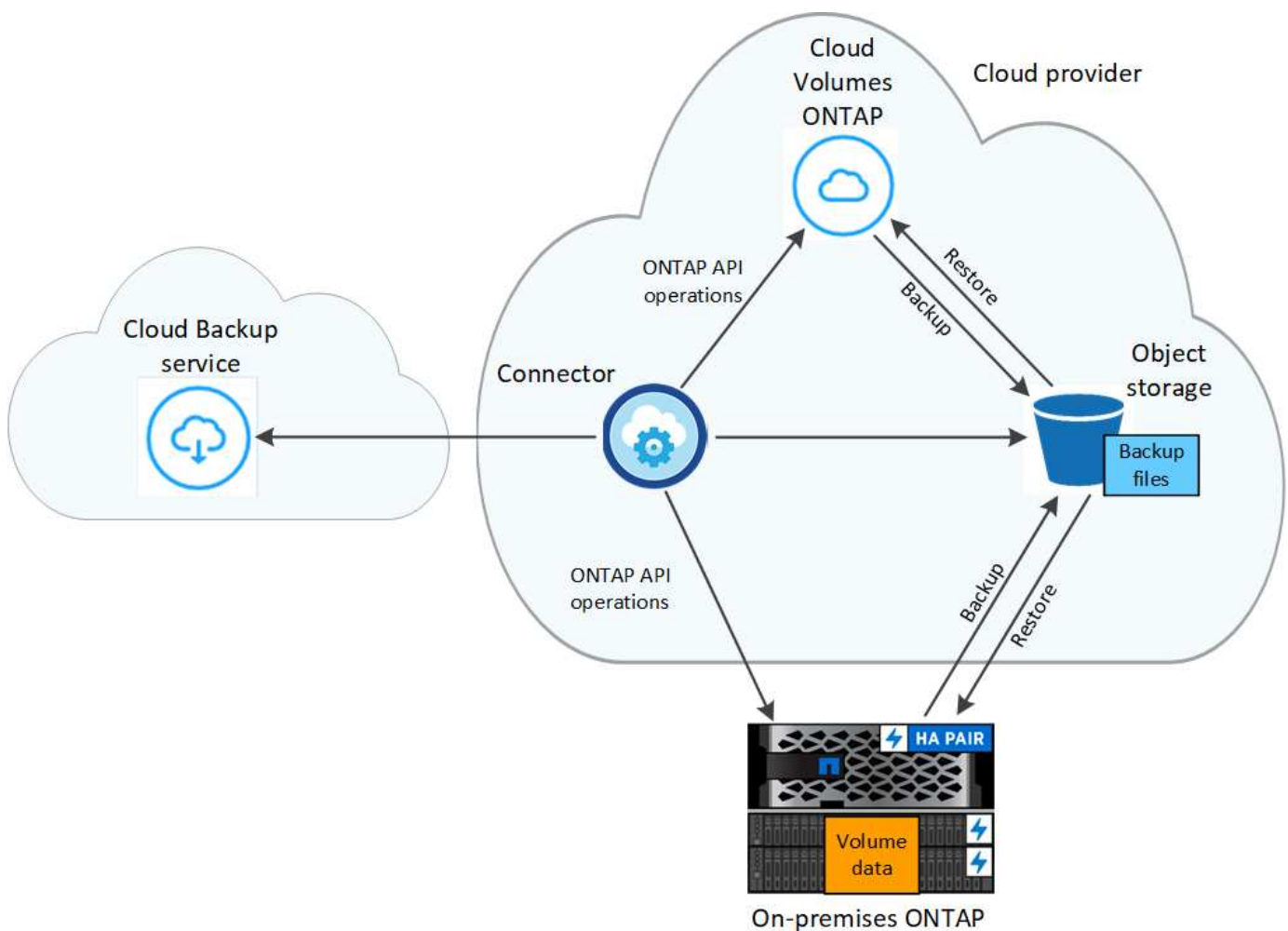
Cómo funciona Cloud Backup

Cuando habilita Cloud Backup en un sistema Cloud Volumes ONTAP o ONTAP en las instalaciones, el servicio realiza un backup completo de los datos. Las snapshots de volúmenes no están incluidas en la imagen de backup. 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. Cloud Backup se basa en la ["Tecnología SnapMirror Cloud de NetApp"](#).



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

La siguiente imagen muestra la relación entre cada componente:



La ubicación de los backups

Las copias de seguridad se almacenan en un almacén de objetos que BlueXP crea en su 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 habilita la ["Función de acceso público en bloque de Amazon S3"](#) En el bloque de S3.

- En StorageGRID, BlueXP utiliza una cuenta de almacenamiento existente para el bloque de almacenamiento de objetos.

Si desea cambiar el almacén de objetos de destino de un clúster en el futuro, tendrá que hacerlo ["Cancele el registro de Cloud Backup para el entorno de trabajo"](#)Y, a continuación, active Cloud Backup con la información del nuevo proveedor de cloud.

Programación de copia de seguridad y configuración de retención personalizables

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

Se puede elegir una combinación de backups por hora, diarios, semanales, mensuales y anuales de todos los volúmenes. También puede seleccionar una de las políticas definidas por el sistema que proporcione backups y retención durante 3 meses, 1 año y 7 años. Estas políticas son:

Nombre de la política de backup	Backups por intervalo...			Capacidad Completos
	Diario	Semanal	mensual	
Netapp3MonthsRetention	30	13	3	46
Netapp1YearRetention	30	13	12	55
Retención de Netapp7YearsRetention	30	53	84	167

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.

Una vez que haya alcanzado la cantidad máxima de backups para una categoría o intervalo, los backups más antiguos se eliminan de modo que siempre tendrá los backups más actuales (y, por lo tanto, los backups obsoletos no continúan ocupar espacio en el cloud).

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 superior, puede proteger sus backups de ataques de ransomware y eliminación. 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.

El período de retención de backup es igual al período de retención de programa de backup; más 14 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.

Consulte "[Protección de DataLock y ransomware](#)" Para obtener más detalles sobre cómo funciona la protección DataLock y Ransomware.



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. 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 su clúster utiliza ONTAP 9.10.1 o superior, puede optar por organizar en niveles los backups más antiguos en el almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive* en la interfaz de usuario de Cloud Backup tras un determinado número de días para obtener una mayor optimización de los costes. "[Obtenga más información acerca del almacenamiento de archivado de AWS](#)".

- 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 ciertas cosas que debe tener en cuenta cuando el volumen del cual se está realizando el backup reside en un agregado de FabricPool y tiene una política asignada, excepto en `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. Dado que los datos se organizan en niveles inmediatamente, Cloud Backup leerá los datos del nivel de cloud en lugar 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.

Limitaciones

Limitaciones de backup

- La posibilidad de organizar en niveles archivos de backup antiguos en el almacenamiento de datos archivados requiere que el clúster ejecute ONTAP 9.10.1 o posterior. Para restaurar volúmenes a partir de archivos de backup que residen en un almacenamiento de archivado, el clúster de destino tiene que ejecutar ONTAP 9.10.1 o posterior.
- Cuando se crea o edita una política de backup cuando no se asignan volúmenes a la política, el número de backups retenidos puede ser un máximo de 1018. Como solución alternativa, puede reducir el número de copias de seguridad para crear la directiva. Luego, se puede editar la política para crear hasta 4000 backups después de asignar volúmenes a la política.
- Cuando se realiza un backup de volúmenes de protección de datos (DP):
 - Relaciones con las etiquetas de SnapMirror `app_consistent` y `all_source_snapshot` no se realizarán backups en el cloud.
 - Si crea copias locales de Snapshot en el volumen de destino de SnapMirror (independientemente de las etiquetas de SnapMirror utilizadas), estas Snapshots no se moverán al cloud como backups. En este momento, deberá crear una política de Snapshot con las etiquetas que desee en el volumen de DP de origen para que Cloud Backup los realice backups.
- Los backups de volúmenes de FlexGroup no se pueden mover a un almacenamiento de archivado ni tampoco se puede usar la protección de DataLock y Ransomware.
- Se admite el backup de volúmenes de SVM-DR con las siguientes restricciones:
 - Los backups solo son compatibles desde el almacenamiento secundario de ONTAP.
 - La política de Snapshot aplicada al volumen debe ser una de las políticas reconocidas por Cloud Backup, que incluye diario, semanal, mensual, etc. No se reconoce la política predeterminada `"sm_creado"` (utilizada para **Mirror All Snapshots**) y el volumen DP no aparecerá en la lista de volúmenes de los que se puede hacer copia de seguridad.
- Soporte de MetroCluster:
 - Cuando se utiliza ONTAP 9.12.1 GA o superior, el backup es compatible cuando se conecta al sistema primario. Toda la configuración de backup se transfiere al sistema secundario de forma que los backups al cloud continúan automáticamente tras la conmutación. No es necesario configurar el backup en el sistema secundario (de hecho, ya no se tiene la restricción de hacerlo).
 - Cuando se utiliza ONTAP 9.12.0 y versiones anteriores, el backup solo es compatible desde el sistema secundario ONTAP.
 - Por el momento no se admiten backups de volúmenes de FlexGroup.
- La copia de seguridad de volumen ad-hoc con el botón **Backup Now** no se admite en los volúmenes de protección de datos.

- No se admiten las configuraciones de SM-BC.
- ONTAP no admite relaciones de SnapMirror entre fan-out de un único volumen y varios almacenes de objetos; por lo tanto, Cloud Backup no admite esta configuración.
- En este momento, EL modo WORM y cumplimiento de normativas en un almacén de objetos es compatible con Amazon S3, Azure y StorageGRID. Esto se conoce como función DataLock y debe gestionarse mediante la configuración Cloud Backup, no mediante la interfaz del proveedor de cloud.

Limitaciones de la restauración

Estas limitaciones se aplican tanto a los métodos de restauración de archivos y carpetas como a los métodos de búsqueda y restauración, a menos que se especifique lo contrario.

- Browse & Restore permite restaurar hasta 100 archivos individuales a la vez.
- Search & Restore puede restaurar 1 fichero cada vez.
- Al utilizar ONTAP 9.13.0 o superior, Browse & Restore y Search & Restore pueden restaurar una carpeta junto con todos los archivos y subcarpetas del mismo.

Cuando se utiliza una versión de ONTAP superior a 9.11.1 pero anterior a la 9.13.0, la operación de restauración solo puede restaurar la carpeta seleccionada y los archivos de esa carpeta; no se restauran ninguna subcarpeta ni los archivos de las subcarpetas.

Si se utiliza una versión de ONTAP anterior a la 9.11.1, no se admite la restauración de carpetas.

- Actualmente, la restauración de directorio/carpeta no es compatible con los volúmenes de FlexGroup.
- No puede restaurar carpetas individuales si el archivo de backup reside en el almacenamiento de archivado.
- No se admite la restauración de volúmenes de FlexGroup a volúmenes de FlexVol o volúmenes de FlexVol a volúmenes de FlexGroup.
- El archivo que se va a restaurar debe estar utilizando el mismo idioma que el del volumen de destino. Recibirá un mensaje de error si los idiomas no son los mismos.
- La prioridad de restauración *High* no se admite al restaurar datos desde el almacenamiento de archivado de Azure a los sistemas StorageGRID.

Realizar backups de los datos de Cloud Volumes ONTAP en Amazon S3

Complete unos pasos para empezar a realizar backups de datos desde 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.



Verifique la compatibilidad con la configuración

- Ejecuta Cloud Volumes ONTAP 9.7P5 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 Cloud Backup de NetApp.
- Tiene un conector instalado en AWS.
 - El conector se puede instalar en un sitio con o sin acceso a Internet.
 - La función IAM que proporciona el conector BlueXP con permisos incluye permisos S3 de la última versión "[Política de BlueXP](#)".

2

Habilite Cloud Backup en su sistema nuevo o existente

- Nuevos sistemas: Cloud Backup está habilitado de forma predeterminada en el asistente del entorno de trabajo. Asegúrese de mantener la opción habilitada.
- Sistemas existentes: Seleccione el entorno de trabajo y haga clic en **Activar** junto al servicio copia de seguridad y recuperación del panel derecho y, a continuación, siga el asistente de configuración.



3

Introduzca los detalles del proveedor

Seleccione la cuenta de AWS y la región donde desea crear los backups. También puede elegir su propia clave gestionada por el cliente para el cifrado de datos en lugar de utilizar la clave de cifrado predeterminada de Amazon S3.

4

Defina la política de backup predeterminada

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

Los backups se almacenan de forma predeterminada en el almacenamiento estándar S3. Si el clúster utiliza ONTAP 9.10.1 o superior, puede optar por colocar los backups en niveles en el almacenamiento S3 Glacier o S3 Glacier Deep Archive después de un determinado número de días para aumentar la optimización de los costes.

De manera opcional, al usar ONTAP 9.11.1 y versiones posteriores, puede optar por proteger sus backups de ataques de eliminación y ransomware configurando una de las configuraciones *DataLock* y *Protección de ransomware*. ["Obtenga más información acerca de las opciones de configuración de la política de Cloud Backup disponibles"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

i Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	<p>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.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archive</p> <p>Archive After (Days) <input type="text" value="30"/> Storage Class <input type="text" value="S3 Glacier"/></p>	

5

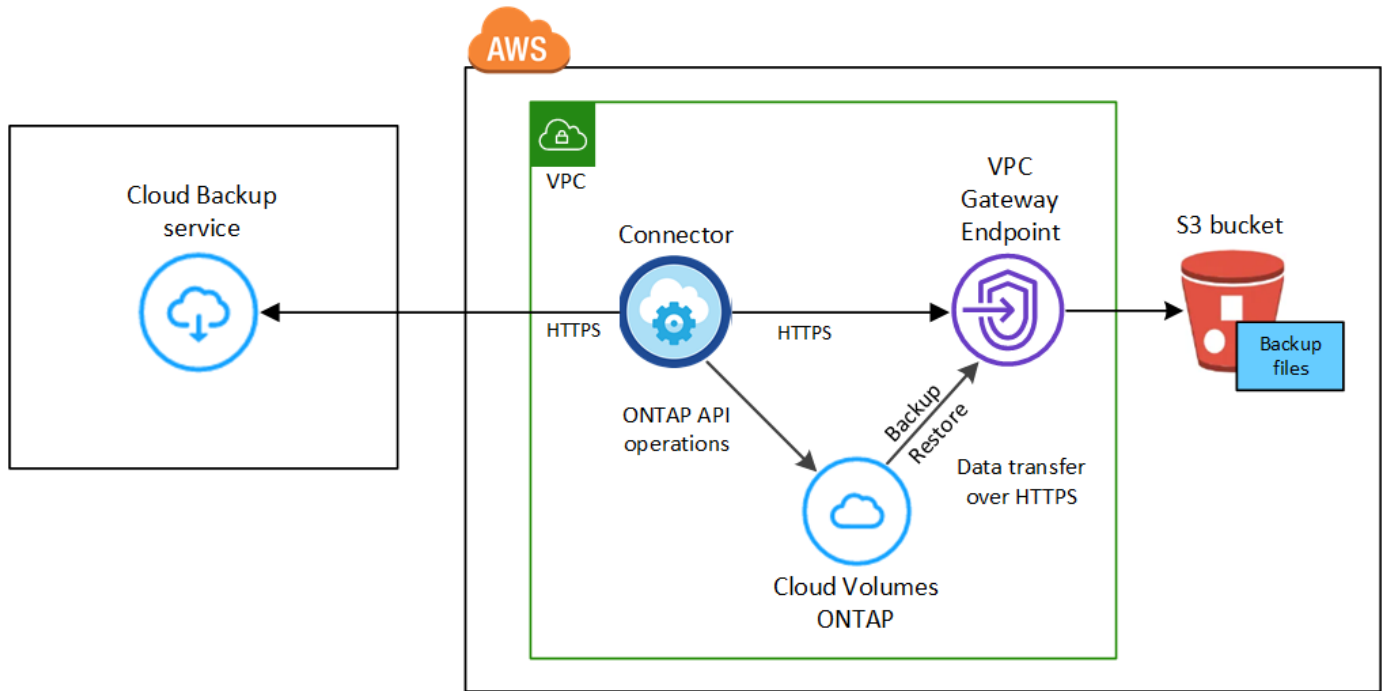
Seleccione los volúmenes de los que desea realizar el backup

Identifique los volúmenes para los que se desea realizar el backup con la política de backup predeterminada en la página Select Volumes. Si desea asignar diferentes políticas de backup a ciertos volúmenes, puede crear políticas adicionales y aplicarlas más adelante.

Requisitos

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:



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 9.7P5; ONTAP 9.8P13 y posterior.

Requisitos de licencia

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

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

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

Para las licencias BYOL de Cloud Backup, necesita el número de serie de NetApp que le permite usar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a gestionar sus licencias BYOL"](#). La licencia de BYOL se debe usar 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.

Regiones admitidas de AWS

Cloud Backup es compatible en todas las regiones de AWS ["Donde se admite Cloud Volumes ONTAP"](#); Incluidas las regiones de AWS GovCloud.

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"](#).

Requisitos del conector

El conector se puede instalar en una región de AWS con o sin acceso a Internet. En este momento, sólo los sitios comerciales de AWS son compatibles con sitios sin acceso a Internet.

- ["Más información sobre conectores"](#)
- ["Ponga en marcha un conector en AWS"](#)
- ["Instalación del conector en un host Linux en una región AWS sin acceso a Internet"](#)



La funcionalidad de copia de seguridad en la nube está integrada en el conector BlueXP. Cuando esté instalado en un sitio sin conectividad a Internet, deberá actualizar periódicamente el software Connector para obtener acceso a nuevas funciones. Compruebe la ["Novedades sobre el backup en el cloud"](#) Para ver las nuevas funciones en cada versión de Cloud Backup y, a continuación, puede seguir los pasos a ["Actualice el software del conector"](#) cuando desee utilizar nuevas funciones.

Le recomendamos encarecidamente que cree copias de seguridad locales de los datos de configuración de Cloud Backup de forma periódica cuando el conector esté instalado en un sitio sin conectividad a Internet. ["Descubra cómo realizar backups de datos de Cloud Backup en un sitio oscuro"](#).

Permisos necesarios de AWS Connector

La función IAM que proporciona permisos BlueXP debe incluir permisos S3 de la última versión ["Política de BlueXP"](#).

A continuación se muestran los permisos específicos de 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:ListBucketByTags",
"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-*"
]
}

```

Si ha implementado el conector con la versión 3.9.21 o superior, estos permisos ya deben formar parte del rol IAM. De lo contrario, tendrá que agregar los permisos que faltan. Específicamente los permisos "athena" y "glue", ya que son necesarios para Buscar y restaurar.

Permisos necesarios de AWS Cloud Volumes ONTAP

Si el sistema Cloud Volumes ONTAP ejecuta software ONTAP 9.12.1 o posterior, la función IAM que proporciona ese entorno de trabajo con permisos debe incluir un nuevo conjunto de permisos S3 específicamente para Cloud Backup desde el último ["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.

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"
```

Activación de Cloud Backup en un nuevo sistema

Cloud Backup está habilitado de forma predeterminada en el asistente de 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. Haga clic en **Crear Cloud Volumes ONTAP**.
2. Seleccione Amazon Web Services como proveedor de cloud 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 activado y haga clic en **continuar**.



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

Resultado

Cloud Backup está habilitado en el sistema y realiza backups de volúmenes cada día y retiene las 30 copias de backup más recientes.

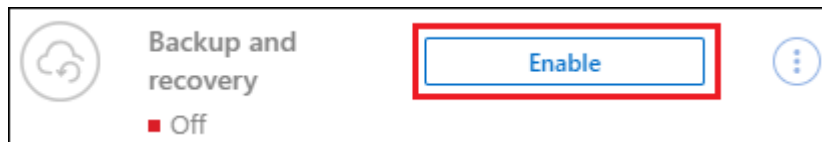
Habilitar Cloud Backup en un sistema existente

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

Pasos

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

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

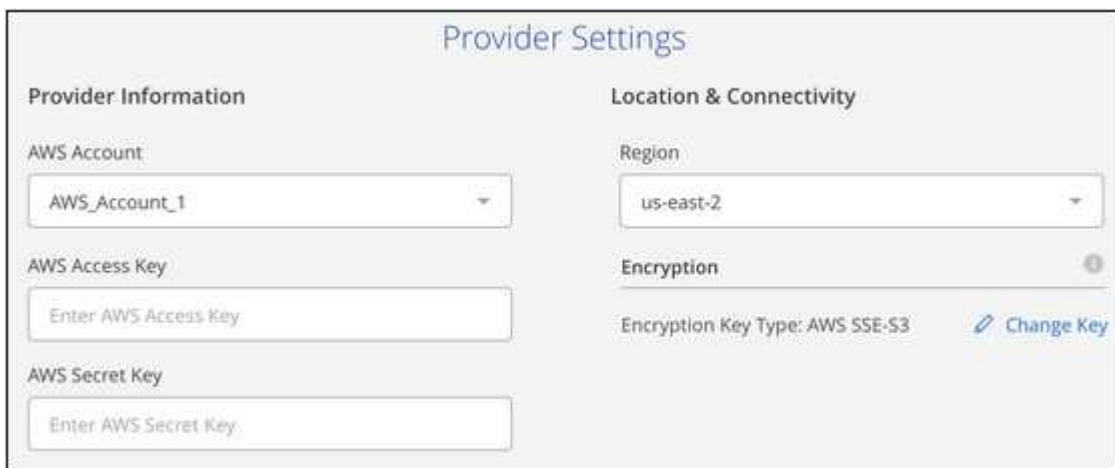


2. Seleccione los detalles del proveedor y haga clic en **Siguiente**.

- a. La cuenta de AWS que se usa 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.

- b. 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.
- c. Tanto si va a usar las claves de cifrado predeterminadas de Amazon S3 como si elige sus propias claves gestionadas por el cliente desde su cuenta de AWS para gestionar el cifrado de sus datos. (["Vea cómo usar sus propias claves de cifrado"](#)).

A screenshot of a "Provider Settings" form. The form is divided into two main sections: "Provider Information" on the left and "Location & Connectivity" on the right. Under "Provider Information", there are three input fields: "AWS Account" (a dropdown menu showing "AWS_Account_1"), "AWS Access Key" (a text input field with placeholder text "Enter AWS Access Key"), and "AWS Secret Key" (a text input field with placeholder text "Enter AWS Secret Key"). Under "Location & Connectivity", there is a "Region" dropdown menu showing "us-east-2". Below this, there is an "Encryption" section with a sub-label "Encryption Key Type: AWS SSE-S3" and a blue link labeled "Change Key".

3. Introduzca los detalles de la política de copia de seguridad que se utilizarán para su directiva predeterminada y haga clic en **Siguiente**. Puede seleccionar una política existente o crear una nueva

introduciendo sus selecciones en cada sección:

- a. Escriba el nombre de la política predeterminada. No es necesario cambiar el nombre.
- b. Defina la programación de backup y elija la cantidad de backups que se retendrán. ["Consulte la lista de políticas existentes que puede elegir"](#).
- c. De manera opcional, al usar ONTAP 9.11.1 y versiones posteriores, puede optar por proteger sus backups de ataques de eliminación y ransomware configurando una de las configuraciones *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 evidencia de un ataque de ransomware en sus archivos de copia de seguridad. ["Obtenga más información acerca de los ajustes de DataLock disponibles"](#).
- d. Opcionalmente, al utilizar ONTAP 9.10.1 y superior, se puede optar por organizar los backups en niveles en el almacenamiento S3 Glacier o en el almacenamiento S3 Glacier Deep Archive al cabo de un determinado número de días para una mayor optimización de los costes. Esta función no está disponible cuando se implementa en sitios oscuros. ["Obtenga más información sobre el uso de niveles de archivado"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

i Cloud Backup will create the S3 bucket after you complete the wizard

Policy Type ☒ Create a new Policy ☐ Select an existing Policy

Name Default_Policy_Name

Labels & Retention 30 Daily

DataLock & Ransomware Protection None

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.

☒ Tier Backups to Archive

Archive After (Days) 30 Storage Class S3 Glacier

Importante: Si planea utilizar DataLock, debe activarlo en su primera directiva al activar Cloud Backup.

4. Seleccione los volúmenes de los que desea realizar un backup mediante la política de backup definida en la página Select Volumes. Si desea asignar diferentes políticas de backup a ciertos volúmenes, puede crear políticas adicionales y aplicarlas más adelante.
 - Para realizar un backup de todos los volúmenes existentes y cualquier volumen añadido en el futuro, active la casilla "realizar backup de todos los volúmenes existentes y futuros...". Recomendamos esta opción para que se haga un backup de todos los volúmenes y que nunca tendrá que recordar para habilitar los backups para volúmenes nuevos.
 - Para realizar un backup solo de los volúmenes existentes, active la casilla de la fila de título (☒ Volume Name).
 - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy
☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes
🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100
< 1 >

Previous
Activate Backup

- Si hay copias Snapshot locales para volúmenes de lectura/escritura en este entorno de trabajo que coincidan con la etiqueta de programación de backup que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se mostrará un mensaje adicional "Exportar copias Snapshot existentes a almacenamiento de objetos como copias de backup". Marque esta casilla si desea que todas las Snapshots históricas se copien al almacenamiento de objetos como archivos de backup para garantizar la protección más completa para los volúmenes.

5. Haga clic en **Activar copia de seguridad** y Cloud Backup comenzará a realizar las copias de seguridad iniciales de cada volumen seleccionado.

Resultado

Un bloque de S3 se crea automáticamente en la cuenta de servicio indicada por la clave de acceso de S3 y la clave secreta introducida; además, se almacenan allí los archivos de backup. 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"](#).

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.

Realizar backups de datos de ONTAP en las instalaciones en Amazon S3

Realice algunos pasos para empezar a realizar backups de datos desde sus sistemas ONTAP locales al almacenamiento Amazon S3.

Cabe destacar que "sistemas ONTAP en las instalaciones" incluyen 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

Identifique el método de configuración que utilizará

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.

[Consulte los métodos de conexión disponibles.](#)

2

Prepare el conector BlueXP

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

[Consulte cómo crear un conector y cómo definir los ajustes de red necesarios.](#)

3

Prepare su clúster de ONTAP en las instalaciones

Descubra su clúster de ONTAP en BlueXP, compruebe que cumple los requisitos mínimos y personalice la configuración de red para que el clúster se pueda conectar a AWS S3.

[Descubra cómo preparar su clúster ONTAP local.](#)

4

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. [Descubra cómo conseguir que su entorno AWS S3 esté listo para recibir backups de ONTAP.](#)

5

Habilite Cloud Backup en el sistema

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. Después, siga el asistente de configuración para definir la política de backup predeterminada y la cantidad de backups que se retendrán, y seleccione los volúmenes que desea realizar el backup.

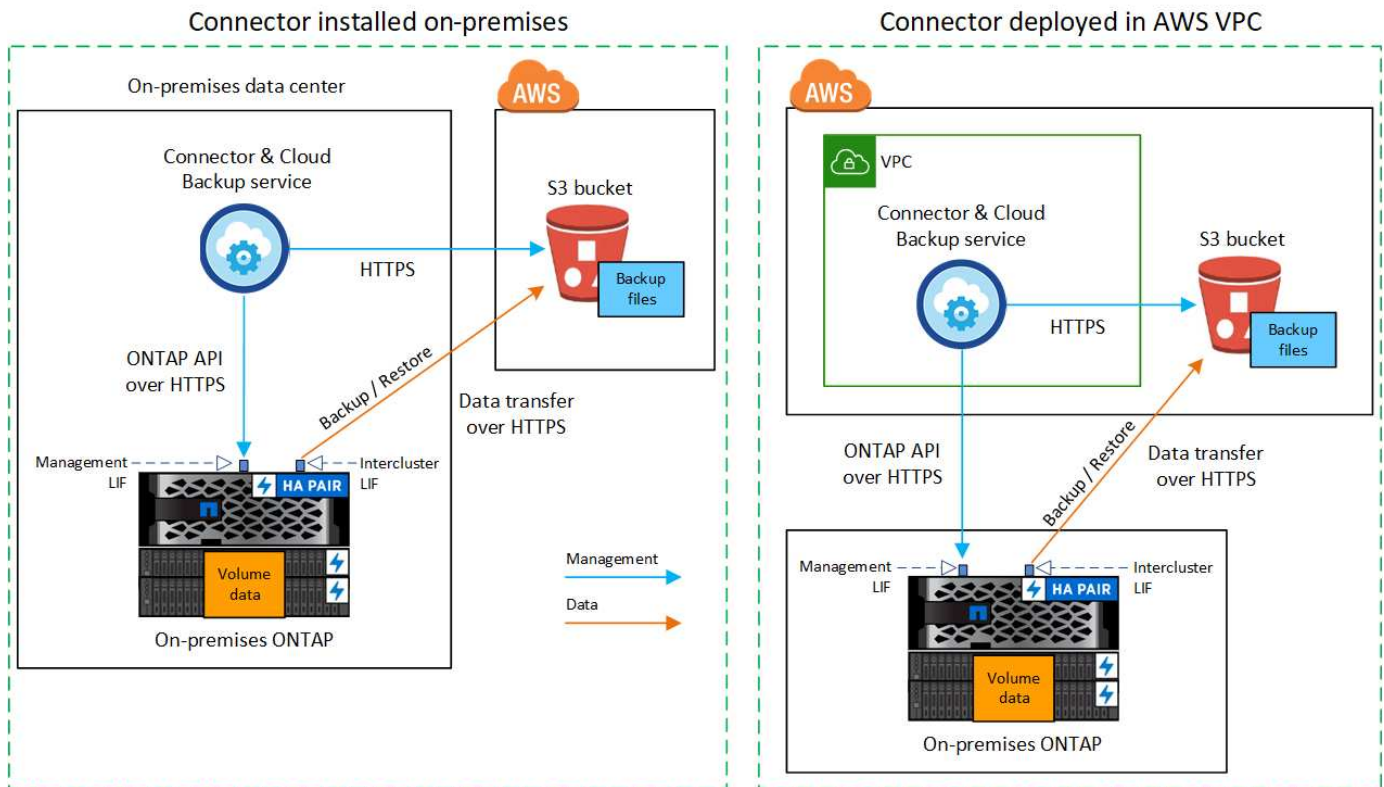
[Vea cómo activar Cloud Backup en sus volúmenes.](#)

Diagramas de red para las opciones de conexión

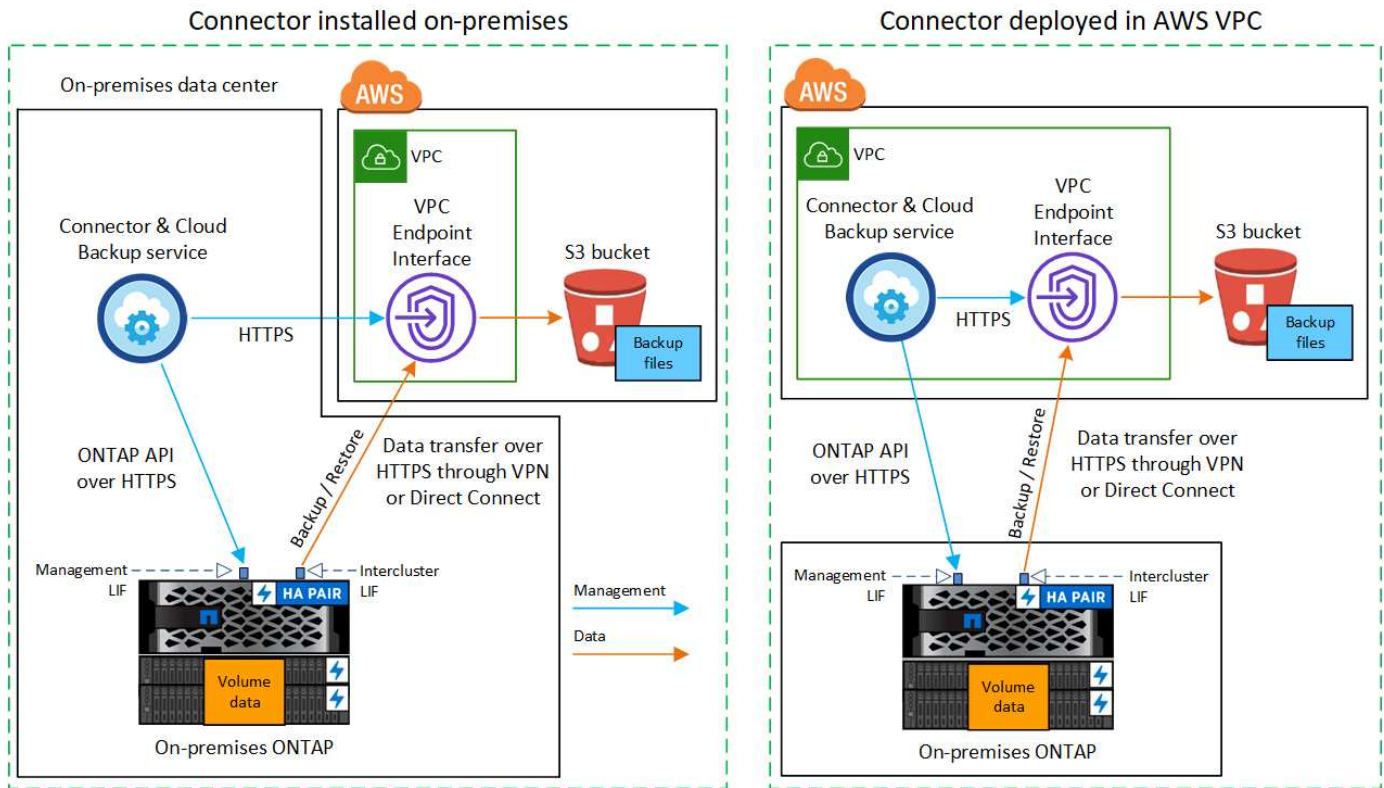
Existen dos métodos de conexión que se pueden utilizar al configurar backups de sistemas ONTAP en las instalaciones a AWS S3.

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

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.

Creación o conmutación de conectores

Si ya tiene un conector puesto en marcha en AWS VPC o en sus instalaciones, todo estará configurado. De lo contrario, necesitará crear un conector en cualquiera de esas ubicaciones para realizar backups de los datos de ONTAP en un almacenamiento AWS S3. No puede utilizar un conector puesto en marcha en otro proveedor de cloud.

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

Cloud Backup es compatible en regiones GovCloud cuando el conector se ha puesto en marcha en el cloud, no es cuando está instalado en sus 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.

Requisitos de conexión a redes 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 a Cloud Backup Service 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](#).

Prepare el clúster ONTAP

Descubra su clúster de ONTAP en BlueXP

Debe detectar un clúster de ONTAP en las instalaciones de BlueXP para poder empezar a realizar backups de datos de volumen. 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"](#).

Requisitos de ONTAP

- Se recomienda un mínimo de ONTAP 9.7P5; 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 Cloud Backup.

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

- La hora y la zona horaria están configuradas correctamente.

Descubra cómo ["configure la hora del clúster"](#).

Requisitos para la red de clúster

- 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"](#).

Cuando configura Cloud Backup, se le solicita 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 conexiones de Cloud Backup desde ONTAP al almacenamiento de objetos a través del puerto 443 y el tráfico de resolución de nombres desde la VM 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"](#).

Verifique los requisitos de licencia

- Antes de poder activar Cloud Backup para su clúster, tendrá que suscribirse a una oferta de pago por uso (PAYGO) BlueXP Marketplace de AWS o comprar y activar una licencia BYOL de Cloud Backup de NetApp. Estas licencias son para su cuenta y se pueden utilizar en varios sistemas.
 - Para las licencias de Cloud Backup PAYGO, necesitará una suscripción a ["Oferta AWS BlueXP Marketplace"](#) Para usar Cloud Backup. La facturación de Cloud Backup se realiza mediante esta suscripción.
 - Para las licencias BYOL de Cloud Backup, 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.

Es posible crear backups desde sistemas locales hasta Amazon S3 en todas las regiones ["Donde se admite Cloud Volumes ONTAP"](#); Incluidas las regiones de AWS GovCloud. Especifique la región en la que se almacenarán las copias de seguridad al configurar el servicio.

Prepare el entorno AWS

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. Confirme que los siguientes permisos de S3 (desde el más reciente "Política de BlueXP") Forman parte de la función IAM que proporciona al conector permisos.

```
{
  "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:ListBucketByTags",
    "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-*"
    ]
},

```

Si ha implementado el conector con la versión 3.9.21 o superior, estos permisos ya deben formar parte del rol IAM. De lo contrario, tendrá que agregar los permisos que faltan. Específicamente los permisos "athena" y "glue", ya que son necesarios para Buscar y restaurar. Consulte ["Documentación de AWS: Editar políticas de IAM"](#).

2. Al activar el servicio, el asistente de backup 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:

```

{
  "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"
    }
  ]
}
{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "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"
}
]
}

```

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

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 desea utilizar sus propias claves gestionadas por el cliente para el cifrado de datos en lugar de utilizar las claves predeterminadas, deberá tener configuradas las claves gestionadas por el cifrado antes de iniciar el asistente de Cloud Backup. ["Vea cómo usar sus propias claves"](#).

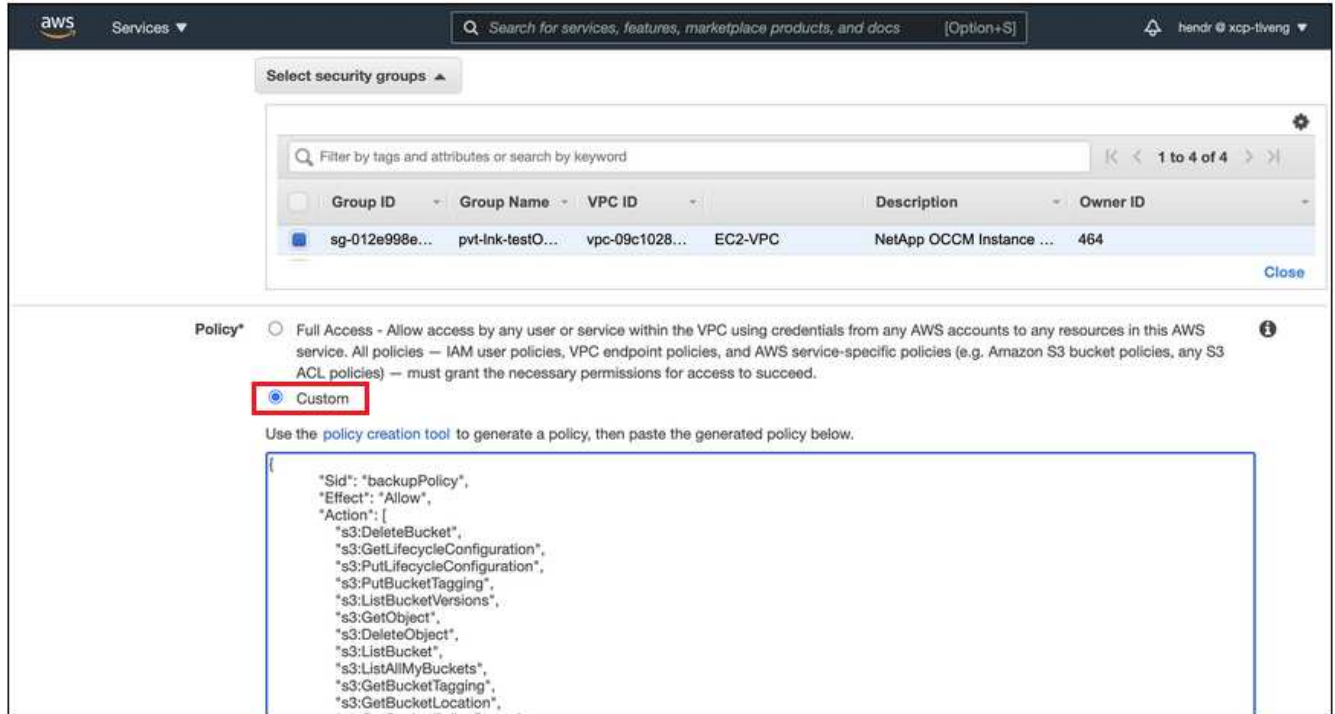
Configure el sistema para una conexión privada mediante una interfaz de extremo VPC

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".

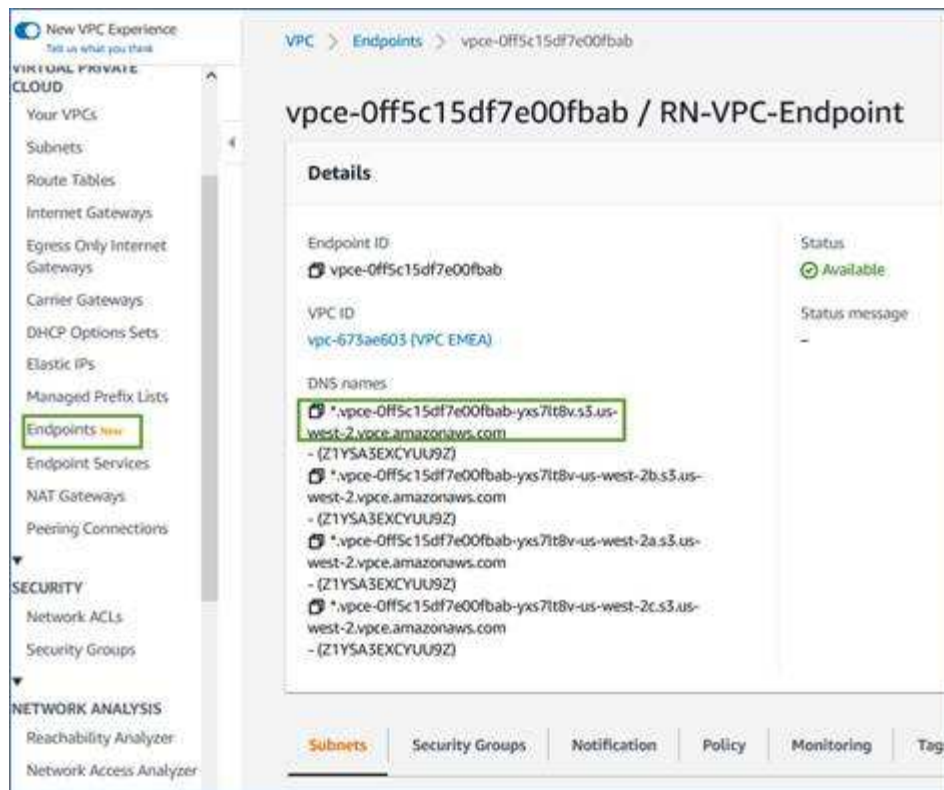
1. Cree una configuración de extremo de interfaz mediante la consola de Amazon VPC o la línea de comandos. "[Consulte detalles sobre el uso de AWS PrivateLink para Amazon S3](#)".
2. Modifique la configuración del grupo de seguridad asociada al conector BlueXP. Debe cambiar la política a "personalizada" (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. Ahora puede habilitar Cloud Backup en el clúster.

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
```

Habilite Cloud Backup

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

Pasos

1. En el lienzo, 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.

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.



2. Seleccione Amazon Web Services como proveedor y haga clic en **Siguiente**.
3. Introduzca los detalles del proveedor y haga clic en **Siguiente**.
 - a. La cuenta de AWS, la clave de acceso de AWS y la clave secreta utilizada para almacenar los backups.

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.

- b. Región de AWS en la que se almacenarán los backups.
- c. Tanto si va a usar las claves de cifrado predeterminadas de Amazon S3 como si elige sus propias claves gestionadas por el cliente desde su cuenta de AWS para gestionar el cifrado de los datos. ("[Vea cómo usar sus propias claves](#)").

4. Si no tiene una licencia de Cloud Backup existente para su cuenta, en este momento se le pedirá que seleccione el tipo de método de carga que desea utilizar. Puede suscribirse a una oferta de pago por uso (PAYGO) BlueXP Marketplace de AWS (o si tiene varias suscripciones, tendrá que seleccionar una), o bien adquirir y activar una licencia BYOL de Cloud Backup de NetApp. ["Descubra cómo configurar la licencia de Cloud Backup."](#)
5. Introduzca los detalles de la red y haga clic en **Siguiente**.
 - a. 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.
 - b. 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"](#).

Name	VPC	Endpoint ID
<input type="radio"/> Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/> Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

6. Introduzca los detalles de la política de copia de seguridad que se utilizarán para su directiva predeterminada y haga clic en **Siguiente**. Puede seleccionar una política existente o crear una nueva introduciendo sus selecciones en cada sección:
 - a. Escriba el nombre de la política predeterminada. No es necesario cambiar el nombre.
 - b. Defina la programación de backup y elija la cantidad de backups que se retendrán. ["Consulte la lista de políticas existentes que puede elegir"](#).
 - c. De manera opcional, al usar ONTAP 9.11.1 y versiones posteriores, puede optar por proteger sus backups de ataques de eliminación y ransomware configurando una de las configuraciones *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 evidencia de un ataque de ransomware en sus archivos de copia de seguridad. ["Obtenga más información acerca de los ajustes de DataLock disponibles"](#).

- d. Opcionalmente, al utilizar ONTAP 9.10.1 y superior, se puede optar por organizar los backups en niveles en el almacenamiento S3 Glacier o en el almacenamiento S3 Glacier Deep Archive al cabo de un determinado número de días para una mayor optimización de los costes. ["Obtenga más información sobre el uso de niveles de archivado"](#).

The screenshot shows the 'Define Policy' wizard in the AWS Backup console. At the top, it says 'Define Policy' and 'This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.' Below this is a note: 'Cloud Backup will create the S3 bucket after you complete the wizard'. The 'Policy Type' section has two radio buttons: 'Create a new Policy' (selected) and 'Select an existing Policy'. The 'Name' field is 'Default_Policy_Name'. The 'Labels & Retention' section shows '30 Daily'. The 'DataLock & Ransomware Protection' section shows 'None'. The 'Archival Policy' section is expanded, showing '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.' There is a checkbox 'Tier Backups to Archive' which is checked. Below this, there are two fields: 'Archive After (Days)' with a value of '30' and 'Storage Class' with a dropdown menu showing 'S3 Glacier'.

Importante: Si planea utilizar DataLock, debe activarlo en su primera directiva al activar Cloud Backup.

7. Seleccione los volúmenes de los que desea realizar un backup mediante la política de backup definida en la página Select Volumes. Si desea asignar diferentes políticas de backup a ciertos volúmenes, puede crear políticas adicionales y aplicarlas más adelante.
- Para realizar un backup de todos los volúmenes existentes y cualquier volumen añadido en el futuro, active la casilla "realizar backup de todos los volúmenes existentes y futuros...". Recomendamos esta opción para que se haga un backup de todos los volúmenes y que nunca tendrá que recordar para habilitar los backups para volúmenes nuevos.
 - Para realizar un backup solo de los volúmenes existentes, active la casilla de la fila de título (☒ Volume Name).
 - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy
☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes
🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100
< 1 >

Previous
Activate Backup

- Si hay copias Snapshot locales para volúmenes de lectura/escritura en este entorno de trabajo que coincidan con la etiqueta de programación de backup que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se mostrará un mensaje adicional "Exportar copias Snapshot existentes a almacenamiento de objetos como copias de backup". Marque esta casilla si desea que todas las Snapshots históricas se copien al almacenamiento de objetos como archivos de backup para garantizar la protección más completa para los volúmenes.

8. Haga clic en **Activar copia de seguridad** y Cloud Backup comenzará a realizar las copias de seguridad iniciales de sus volúmenes.

Resultado

Un bloque de S3 se crea automáticamente en la cuenta de servicio indicada por la clave de acceso de S3 y la clave secreta introducida; además, se almacenan allí los archivos de backup. 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"](#).

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.

Realización de backups de datos de ONTAP en las instalaciones en StorageGRID

Complete algunos pasos para empezar a realizar backups de datos desde sus sistemas ONTAP locales a su almacenamiento de objetos en sus sistemas StorageGRID de NetApp.

Cabe destacar que "sistemas ONTAP en las instalaciones" incluyen sistemas FAS, AFF y ONTAP Select.

Inicio rápido

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

1

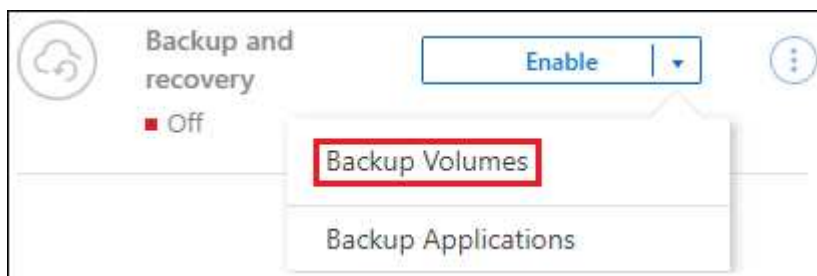
Verifique la compatibilidad con la configuración

- Ha descubierto el clúster en las instalaciones y lo ha añadido a un entorno de trabajo en BlueXP. Consulte ["Detección de clústeres de ONTAP"](#) para obtener más detalles.
 - El clúster ejecuta ONTAP 9.7P5 o una versión posterior.
 - El clúster tiene una licencia de SnapMirror, se incluye como parte del paquete Premium o de Data Protection Bundle.
 - El clúster debe tener conexiones de red necesarias a StorageGRID y conector.
- Tiene un conector instalado en sus instalaciones.
 - El conector se puede instalar en un sitio con o sin acceso a Internet.
 - La conexión a redes para el conector permite una conexión HTTPS de salida al clúster de ONTAP y a StorageGRID.
- Ha comprado ["y activado"](#) Una licencia BYOL de Cloud Backup de NetApp.
- La versión 10.3 de StorageGRID o posterior con claves de acceso que tienen permisos de S3.

2

Habilite Cloud Backup en el sistema

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



3

Introduzca los detalles de la StorageGRID

Seleccione StorageGRID como proveedor y, a continuación, introduzca los detalles de la cuenta de inquilino de S3 y el servidor StorageGRID. También debe especificar el espacio IP del clúster de ONTAP en el que residen los volúmenes.

Storage Settings

Notice : There is no option to change the provider settings after the service has started

Storage Information

StorageGRID Gateway Node FQDN

Port

Access Key

Secret Key

Connectivity

IPspace

Default

4

Defina la política de backup predeterminada

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

Si su clúster utiliza ONTAP 9.12.1 o superior y su sistema StorageGRID utiliza la versión 11.4 o superior, puede optar por organizar en niveles los backups antiguos en niveles de archivado en cloud público después de un determinado número de días para obtener una mayor optimización de los costes. Actualmente es compatible con los niveles de almacenamiento de AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive.

Si su clúster utiliza ONTAP 9.11.1 o superior, puede optar por proteger sus copias de seguridad de ataques de eliminación y ransomware configurando una de las configuraciones *DataLock* y *Protección de ransomware*.

["Obtenga más información acerca de las opciones de configuración de la política de Cloud Backup disponibles"](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type
☒ Create a new Policy
☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	Disabled	▼

5

Seleccione los volúmenes de los que desea realizar el backup

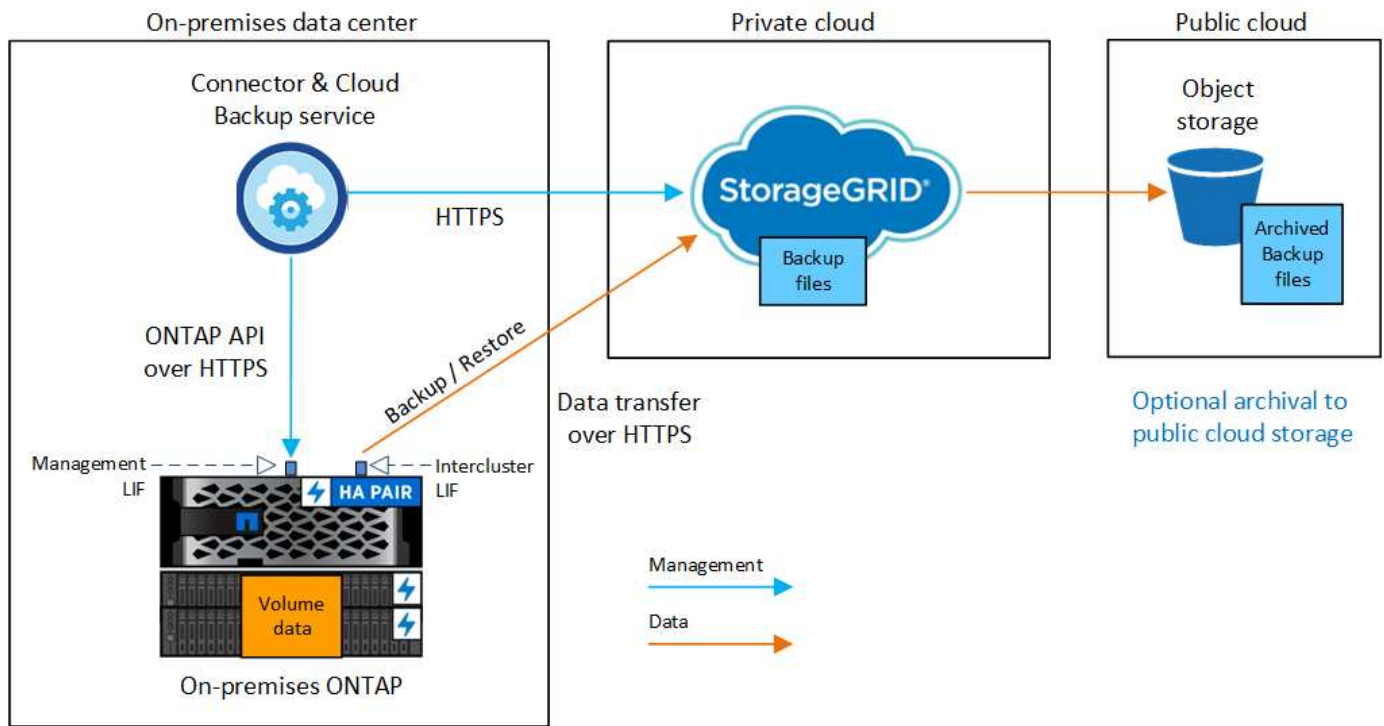
Identifique los volúmenes para los que se desea realizar el backup con la política de backup predeterminada en la página Select Volumes. Si desea asignar diferentes políticas de backup a ciertos volúmenes, puede crear políticas adicionales y aplicarlas más adelante.

Un bloque de S3 se crea automáticamente en StorageGRID, en la cuenta de servicio indicada por la clave de acceso de S3 y la clave secreta introducida; además, se almacenan allí los archivos de backup.

Requisitos

Lea los siguientes requisitos para asegurarse de que tiene una configuración compatible antes de comenzar a realizar el backup de los volúmenes en las instalaciones en StorageGRID.

La siguiente imagen muestra cada componente al realizar una copia de seguridad de un sistema ONTAP en las instalaciones en StorageGRID y de las conexiones que necesita preparar entre ellos.



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.

Preparar los clústeres de ONTAP

Debe detectar los clústeres de ONTAP en las instalaciones en BlueXP para poder empezar a realizar backups de datos de volúmenes.

["Aprenda a detectar un clúster"](#).

Requisitos de ONTAP

- Se recomienda un mínimo de ONTAP 9.7P5; 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 Cloud Backup.

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

- La hora y la zona horaria están configuradas correctamente.

Descubra cómo ["configure la hora del clúster"](#).

Requisitos para la red de clúster

- 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"](#).

Cuando configura Cloud Backup, se le solicita 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"](#).
- 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 conexiones Cloud Backup Service desde ONTAP al almacenamiento de objetos a través del puerto que ha especificado (por lo general, el 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).

Preparando StorageGRID

StorageGRID debe cumplir con los siguientes requisitos. Consulte ["Documentación de StorageGRID"](#) si quiere más información.

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.

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 a Cloud Backup autenticar y acceder a los bloques StorageGRID que se usan 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.

Creación o conmutación de conectores

Al realizar una copia de seguridad de datos en StorageGRID, debe haber un conector disponible en las instalaciones. Tendrá que instalar un conector nuevo 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"](#)



La funcionalidad de copia de seguridad en la nube está integrada en el conector BlueXP. Cuando esté instalado en un sitio sin conectividad a Internet, deberá actualizar periódicamente el software Connector para obtener acceso a nuevas funciones. Compruebe la ["Novedades sobre el backup en el cloud"](#) Para ver las nuevas funciones en cada versión de Cloud Backup y, a continuación, puede seguir los pasos a. ["Actualice el software del conector"](#) cuando desee utilizar nuevas funciones.

Le recomendamos encarecidamente que cree copias de seguridad locales de los datos de configuración de Cloud Backup de forma periódica cuando el conector esté instalado en un sitio sin conectividad a Internet. ["Descubra cómo realizar backups de datos de Cloud Backup en un sitio oscuro"](#).

Preparación de 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 nodo de puerta de enlace StorageGRID
 - Una conexión HTTPS a través del puerto 443 para la LIF de gestión del clúster ONTAP
 - Una conexión de Internet de salida a través del puerto 443 a Cloud Backup (no es necesaria cuando el conector está instalado en un sitio "oscuro")

Preparar el archivado de archivos de backup antiguos en un almacenamiento de 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

- Su clúster debe usar ONTAP 9.12.1 o superior

Requisitos de StorageGRID

- Su StorageGRID debe usar 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. Cloud Backup crea el bucket de cloud cuando activa 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		<input checked="" type="checkbox"/> Tier Backups to Archive	
Cloud Provider		Cloud Provider	
AWS		AZURE	
Account	Region	Azure Subscription	Region
Select Account	Select Region	Select Account	Select Region
AWS Access Key	AWS Secret Key	Resource Group Type	Resource Group
Enter AWS Access Key	Enter AWS Secret Key	Select an Existing Resource Group	Select Resource Group
Archive After (Days)	Storage Class	Archive After (Days)	Storage Class
(1-999)	S3 Glacier	(1-999)	Azure Archive

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"](#).

Requisitos de licencia

Antes de poder activar Cloud Backup en su clúster, tendrá que adquirir y activar una licencia BYOL de Cloud Backup 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.

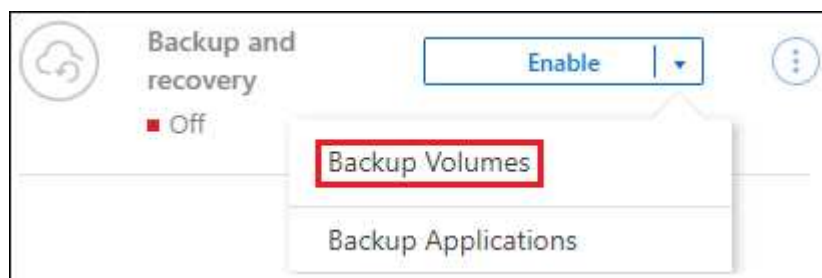
Habilitar Cloud Backup en StorageGRID

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

Pasos

1. En Canvas, selecciona el entorno de trabajo en las instalaciones y haz clic en **Activar > copia de seguridad de volúmenes** junto al servicio copia de seguridad y recuperación del panel derecho.

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



2. Seleccione **StorageGRID** como proveedor, haga clic en **Siguiente** y, a continuación, introduzca los detalles del proveedor:

- a. El FQDN del nodo de puerta de enlace StorageGRID.
- b. El puerto que debe usar ONTAP para la comunicación HTTPS con StorageGRID.
- c. La clave de acceso y la clave secreta utilizadas para acceder al bloque para almacenar backups.
- d. 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 saliente a Internet (no es necesario cuando el conector se instala en un sitio «oscuro»).

Si selecciona el espacio IP correcto, Cloud Backup puede configurar una conexión de ONTAP al almacenamiento de objetos de StorageGRID.

3. Introduzca los detalles de la política de copia de seguridad que se utilizarán para su directiva predeterminada y haga clic en **Siguiente**. Puede seleccionar una política existente o crear una nueva introduciendo sus selecciones en cada sección:
 - a. Escriba el nombre de la política predeterminada. No es necesario cambiar el nombre.
 - b. Defina la programación de backup y elija la cantidad de backups que se retendrán. ["Consulte la lista de políticas existentes que puede elegir"](#).
 - c. 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 evidencia de un ataque de ransomware en sus archivos de copia de seguridad. ["Obtenga más información acerca de los ajustes de DataLock disponibles"](#).
 - d. 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](#).

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy Type
☒ Create a new Policy
 ☐ Select an existing Policy

Name	Default_Policy_Name	▼
Labels & Retention	30 Daily	▼
DataLock & Ransomware Protection	None	▼
Archival Policy	Disabled	▼

Importante: Si planea utilizar DataLock, debe activarlo en su primera directiva al activar Cloud Backup.

4. Seleccione los volúmenes de los que desea realizar un backup mediante la política de backup definida en la página Select Volumes. Si desea asignar diferentes políticas de backup a ciertos volúmenes, puede crear políticas adicionales y aplicarlas más adelante.
 - Para realizar un backup de todos los volúmenes existentes y cualquier volumen añadido en el futuro, active la casilla "realizar backup de todos los volúmenes existentes y futuros...". Recomendamos esta opción para que se haga un backup de todos los volúmenes y que nunca tendrá que recordar para habilitar los backups para volúmenes nuevos.
 - Para realizar un backup solo de los volúmenes existentes, active la casilla de la fila de título (☒ Volume Name).
 - Para realizar un backup de volúmenes individuales, active la casilla de cada volumen (☒ Volume_1).

Select Volumes

☒ Back up all existing and future volumes using the selected Backup policy
☒ Export existing Snapshot copies to object storage as backup files ⓘ

100 Volumes 🔍

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume 1 ● On	RW	SVM_1	12.125 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 2 ● On	RW	SVM_1	1.1 GiB	2 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 3 ● On	RW	SVM_1	15 GiB	25 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 4 ● On	RW	SVM_1	1.125 GiB	5 GiB	⊖ Not Active
<input checked="" type="checkbox"/>	Volume 5 ● On	RW	SVM_1	12 GiB	25 GiB	⊖ Not Active

1 - 50 of 100 < 1 >

Previous
Activate Backup

- Si hay copias Snapshot locales para volúmenes de lectura/escritura en este entorno de trabajo que

coincidan con la etiqueta de programación de backup que acaba de seleccionar para este entorno de trabajo (por ejemplo, diario, semanal, etc.), se mostrará un mensaje adicional "Exportar copias Snapshot existentes a almacenamiento de objetos como copias de backup". Marque esta casilla si desea que todas las Snapshots históricas se copien al almacenamiento de objetos como archivos de backup para garantizar la protección más completa para los volúmenes.

5. Haga clic en **Activar copia de seguridad** y Cloud Backup comenzará a realizar las copias de seguridad iniciales de cada volumen seleccionado.

Resultado

Un bloque de S3 se crea automáticamente en la cuenta de servicio indicada por la clave de acceso de S3 y la clave secreta introducida; además, se almacenan allí los archivos de backup. 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](#)".

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](#)". En un sistema ONTAP en las instalaciones.

Administrar backups para sus sistemas ONTAP

Puede gestionar backups para sus sistemas Cloud Volumes ONTAP y ONTAP en las instalaciones cambiando la programación de backups, creando nuevas políticas de backup, habilitando/deshabilitando backups de volúmenes, haciendo una pausa en los backups, eliminando backups, etc.



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

Ver los volúmenes de los que se está realizando backup

Es posible ver una lista de todos los volúmenes de los que se está haciendo backup en la consola de backup.

Pasos

1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Volumes** para ver la lista de volúmenes de los que se ha realizado una copia de seguridad para sistemas Cloud Volumes ONTAP y ONTAP locales.

Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

All Backed Up Working Environments

Last Updated: June 12 2022, 00:00:00 | Backup Settings

6 Working Environments | 2,011 Protected Volumes | 125.75 TB Total Backup Size

Backup Volumes Status: 1,924 Healthy Backup Volumes | 87 Failed Backup Volumes

2,011 Backed Up Volumes

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup	Backups	Tiering to Archive
Volume 1	Working Environment 1	Source SVM 1	None	Active	June 12 2022	125 Backups	Active
Volume 2	Working Environment 1	Source SVM 2	Governance	Active	June 12 2022	25 Backups	Disabled
Volume 3	Working Environment 1	Source SVM 1	Compliance	Active	June 12 2022	15 Backups	Disabled

Si está buscando volúmenes específicos en ciertos entornos de trabajo, puede refinar la lista según el entorno y el volumen de trabajo, o puede utilizar el filtro de búsqueda.

Habilitar y deshabilitar backups de volúmenes

Puede activar los backups de cualquier volumen nuevo si no se están realizando backups en ese momento. También es posible activar backups para cualquier volumen que haya desactivado previamente.

Es posible desactivar los backups para volúmenes de forma que no se generen backups adicionales. Esto también deshabilita la capacidad para restaurar datos de volúmenes desde un archivo de backup. Esto permite básicamente poner en pausa toda la actividad de backup y restauración durante un periodo de tiempo. Cualquier backup existente no se eliminará, por lo que su proveedor de cloud seguirá cargando en los costes de almacenamiento de objetos de la capacidad que sus backups utilizan, a menos que usted [elimine los backups](#).

Pasos

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

Volumes | Restore | Applications | Virtual Machines | Kubernetes | Job Monitoring

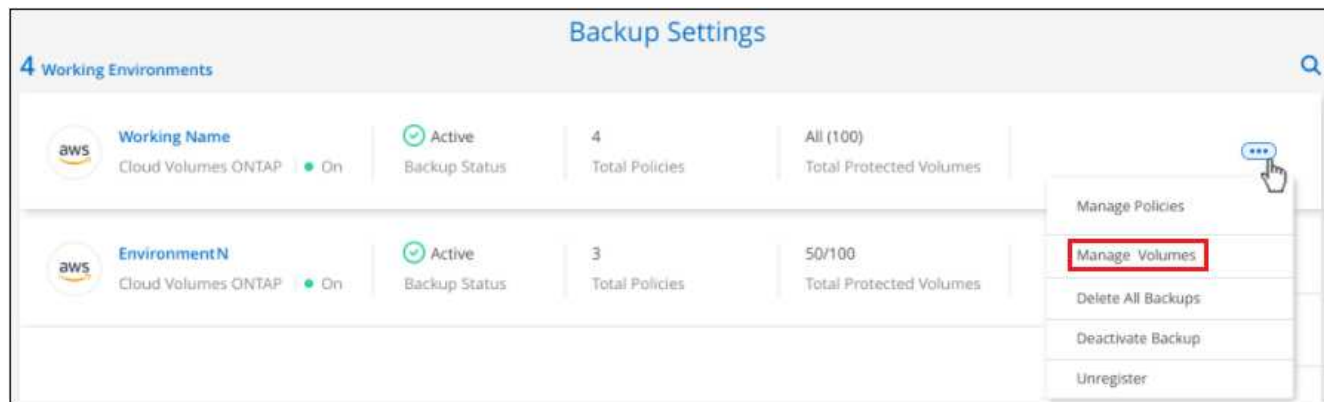
All Backup Working Environments

Backup Settings

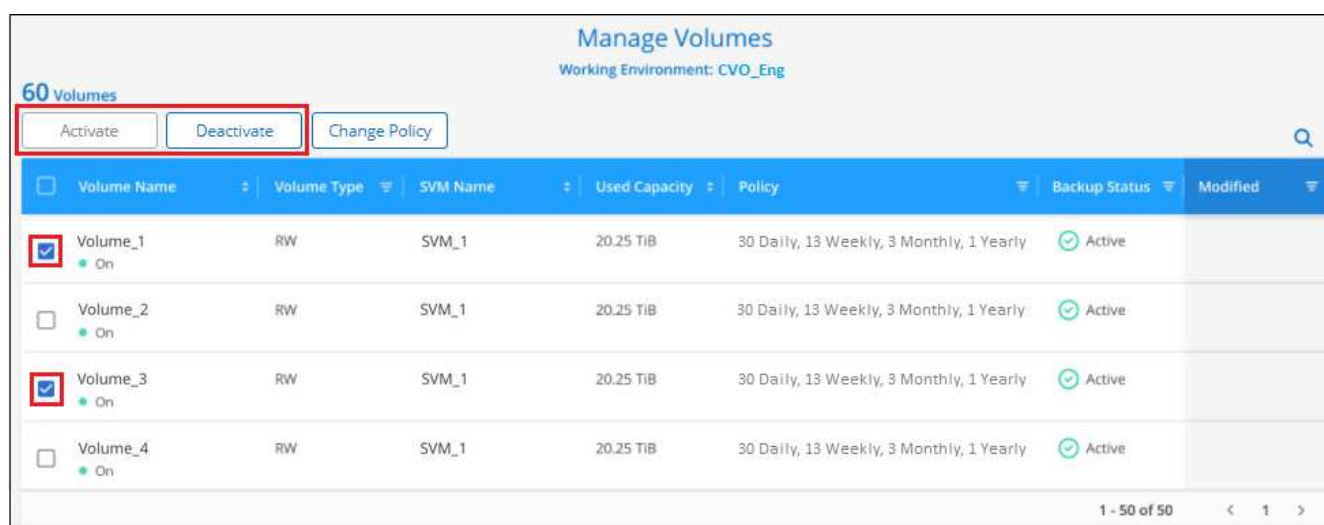
5 Working Environments | 57 Protected Volumes | 15.1 TB Total Backup Size

Protected Volumes Status: 57 Healthy Backups | 0 Failed Backups

2. En la página *Backup Settings*, haga clic en **...** Para el entorno de trabajo y seleccione **gestionar volúmenes**.



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



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

Editar una política de backup existente

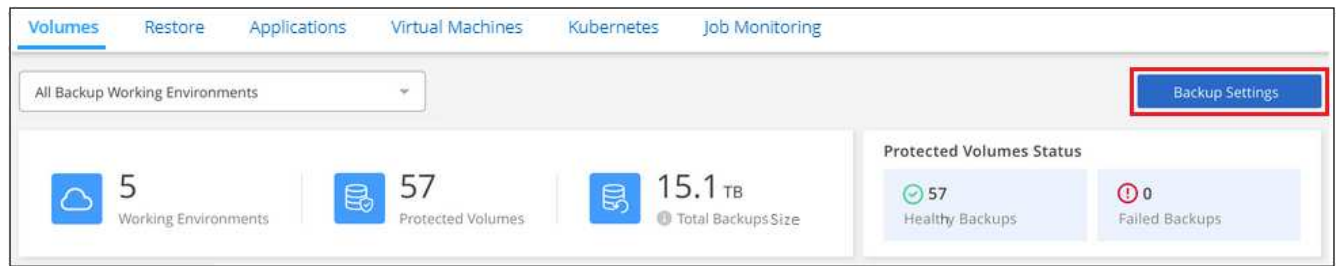
Puede cambiar los atributos de una política de backup que se aplique actualmente a los volúmenes en un entorno de trabajo. Los cambios que se aplican en la política de backup afectan a todos los volúmenes existentes que usan la política.



- Si ha activado *DataLock* y *Protección de ransomware* en la directiva inicial al activar Cloud Backup para este clúster, las directivas que edite deben configurarse con la misma configuración DataLock (Gobierno o cumplimiento). Y si no ha activado *DataLock* y *la protección de ransomware* al activar Cloud Backup, no puede habilitar DataLock ahora.
- Al crear backups en AWS, si eligió *S3 Glacier* o *S3 Glacier Deep Archive* en la primera política de backup al activar Cloud Backup, 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**.

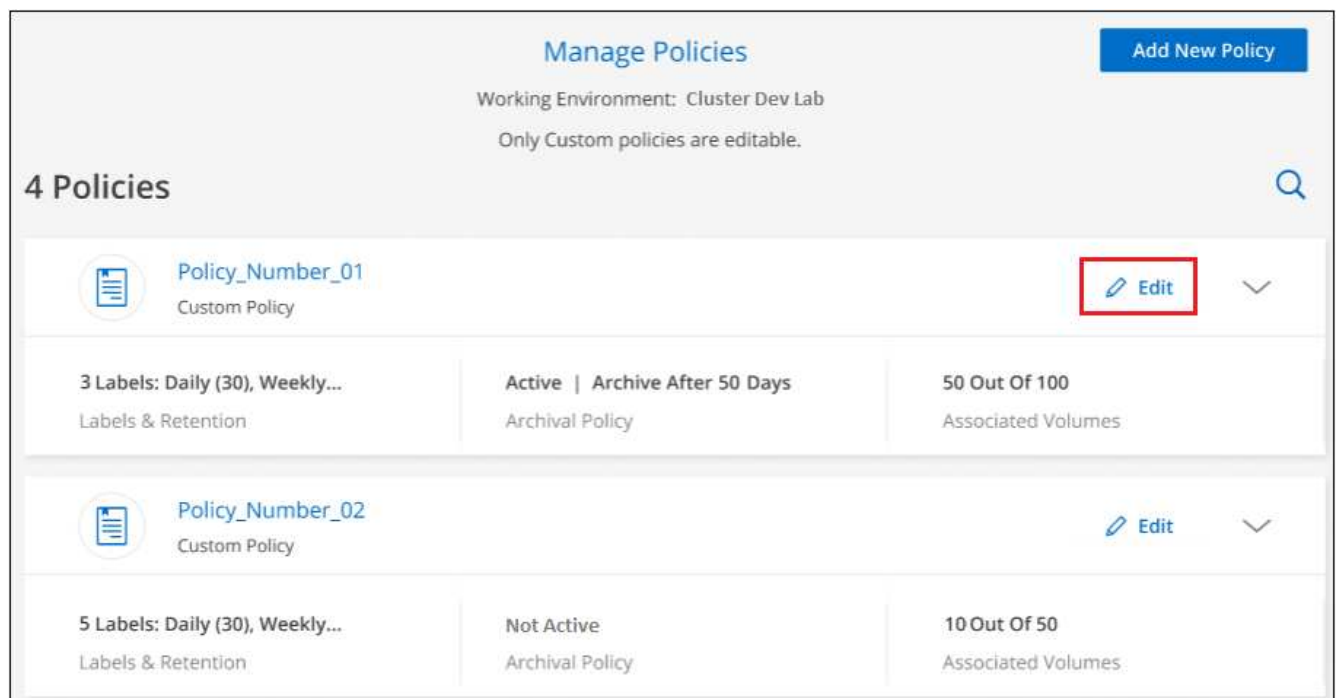


- En la página *Backup Settings*, haga clic en ... Para el entorno de trabajo en el que desea cambiar la configuración de la directiva y seleccione **Administrar directivas**.



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

Nota en la que puede hacer clic ▼ para ver todos los detalles de la política.



- 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: Cluster Dev Lab	
Name	Policy_Number_01
Labels & Retention	30 Daily 2 Weekly 1 Yearly
DataLock & Ransomware Protection	None
Archival Policy	Active Archive After 50 Days

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".

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)

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)

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)

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.

Adición de una nueva política de backup

Al habilitar Cloud Backup para un entorno de trabajo, se realizan backups de todos los volúmenes que

seleccione inicialmente con la política de backup predeterminada que haya definido. Si desea asignar diferentes políticas de backup a ciertos volúmenes que tienen diferentes objetivos de punto de recuperación (RPO), puede crear políticas adicionales para ese clúster y asignar dichas políticas a otros volúmenes.

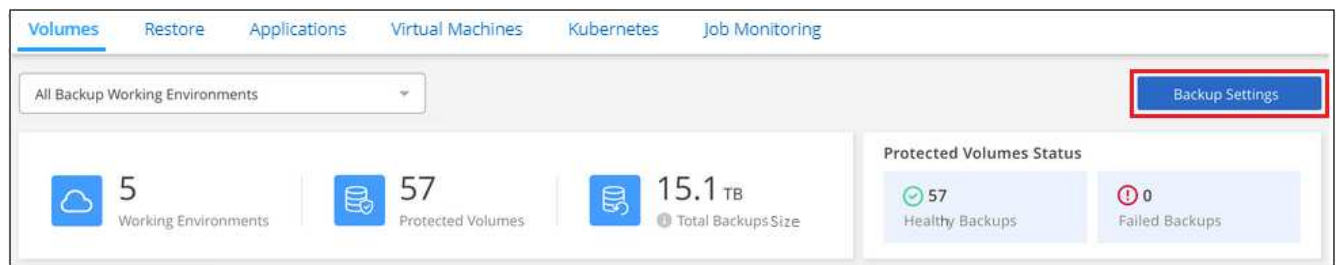
Si desea aplicar una nueva política de backup a ciertos volúmenes en un entorno de trabajo, primero debe añadir la política de backup al entorno de trabajo. Ahora puede [aplique la política a los volúmenes en ese entorno de trabajo](#).



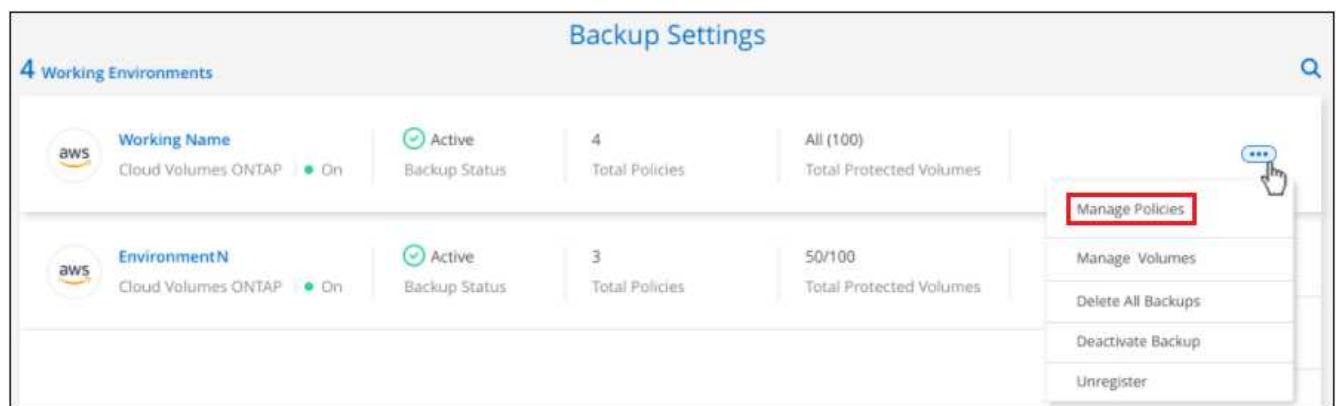
- Si ha activado *DataLock* y *Protección de ransomware* en la directiva inicial al activar Cloud Backup para este clúster, cualquier política adicional que cree debe configurarse con la misma configuración *DataLock* (Gobierno o cumplimiento). Y si no ha activado *DataLock* y *la protección de ransomware* al activar Cloud Backup, no puede crear nuevas políticas que utilicen *DataLock*.
- Al crear backups en AWS, si eligió *S3 Glacier* o *S3 Glacier Deep Archive* en la primera política de backup al activar Cloud Backup, 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**.

Manage Policies

Working Environment: Cluster Dev Lab

Only Custom policies are editable.

Add New Policy

4 Policies

Policy_Number_01

Custom Policy

Edit

3 Labels: Daily (30), Weekly...

Labels & Retention

Active | Archive After 50 Days

Archival Policy

50 Out Of 100

Associated Volumes

Policy_Number_02

Custom Policy

Edit

5 Labels: Daily (30), Weekly...


Labels & Retention

Not Active

Archival Policy





10 Out Of 50

Associated Volumes

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".

<p>Archival Policy</p> <p>Azure</p>	<p>Backups reside in Cool Azure Blob storage for frequently accessed data. Optionally, you can tier backups to Azure Archive storage for further cost optimization.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archival</p> <p>Archive after (Days): <input type="text" value="30"/></p> <p>Access Tier: <input type="text" value="Azure Archive"/></p>
<p>Archival Policy</p> <p>AWS</p>	<p>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.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archival</p> <p>Archive after (Days): <input type="text" value="30"/></p> <p>Storage Class: <input type="text" value="S3 Glacier"/></p> <p><input type="text" value="S3 Glacier"/></p> <p><input type="text" value="S3 Glacier Deep Archive"/></p>
<p>Archival Policy</p> <p>Google</p>	<p>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.</p> <p><input checked="" type="checkbox"/> Tier Backups to Archival</p> <p>Archive after (Days): <input type="text" value="30"/></p> <p>Storage Class: <input type="text" value="Google Cloud Archive"/></p>

Cambiar la política asignada a los volúmenes existentes

Es posible cambiar la política de backup asignada a los volúmenes existentes si se desea cambiar la frecuencia de los backups o si desea cambiar el valor de retención.

Tenga en cuenta que la política que desea aplicar a los volúmenes ya debe existir. [Descubra cómo añadir una nueva normativa de backup para un entorno de trabajo.](#)

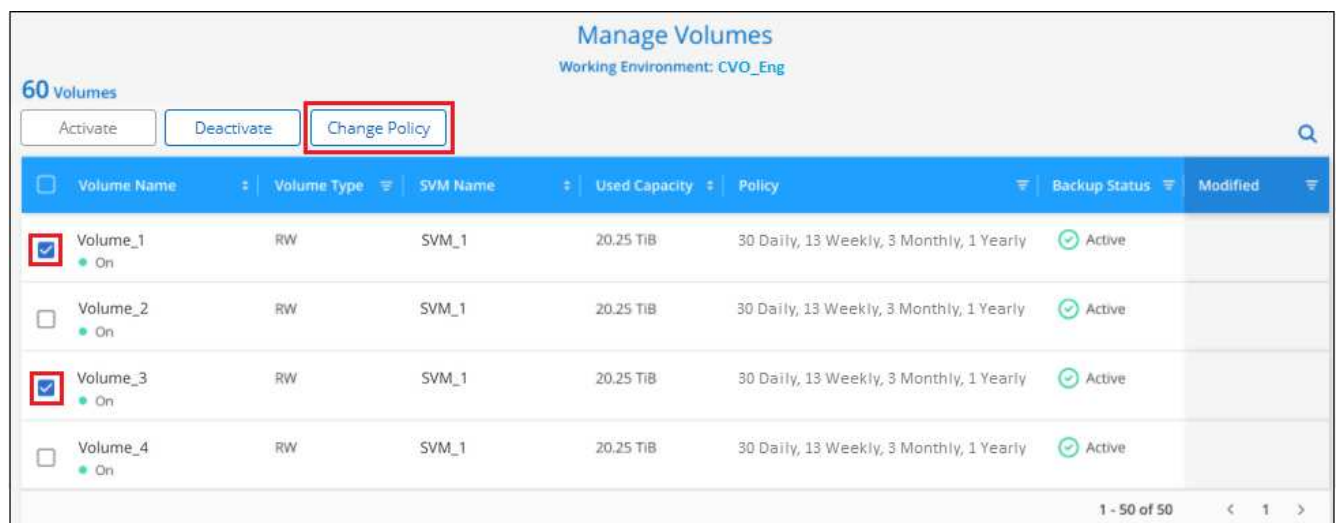
Pasos

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

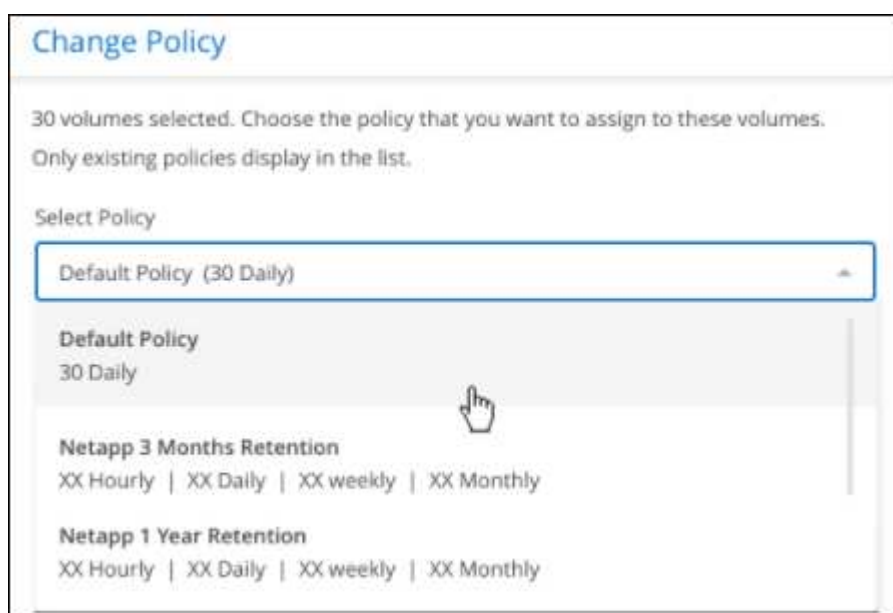
2. En la página *Backup Settings*, haga clic en **Para el entorno de trabajo en el que existen los volúmenes, seleccione **gestionar volúmenes**.**



3. Seleccione la casilla de verificación para un volumen o volúmenes para los que desea cambiar la directiva y, a continuación, haga clic en **Política de cambio**.



4. En la página *Change Policy*, seleccione la directiva que desea aplicar a los volúmenes y haga clic en **Change Policy**.





Si ha activado *DataLock* y *Protección de ransomware* en la directiva inicial al activar Cloud Backup para este clúster, solo verá otras directivas que se hayan configurado con DataLock. Y si no ha activado *DataLock* y *Protección de ransomware* al activar Cloud Backup, solo verá otras directivas que no tengan DataLock configurado.

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

Creación de un backup de volumen manual en cualquier momento

Es posible crear un backup bajo demanda en cualquier momento para capturar el estado actual del volumen. Esto puede resultar útil si se han realizado cambios muy importantes en un volumen y no desea esperar a que se realice la siguiente copia de seguridad programada para proteger esos datos, o si actualmente el volumen no se está haciendo copia de seguridad y se desea capturar su estado actual.

El nombre de backup incluye la Marca de hora para poder identificar el backup bajo demanda desde otros backups programados.

Si ha activado *DataLock* y la *protección de ransomware* al activar Cloud Backup para este clúster, la copia de seguridad 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

1. En la ficha **Volumes**, haga clic en **...** Para el volumen y seleccione **copia de seguridad ahora**.

The screenshot displays the 'Volumes' tab in a backup management console. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below these, a dropdown menu shows 'All Backup Working Environments'. A summary section shows 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' box indicates 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, it says '2,011 Backed Up Volumes'. The main table lists three volumes. For 'Volume 2', a dropdown menu is open, showing 'Backup Now' highlighted with a red box.

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	aws Working Environment 1 On	Source SVM 1	None	Active	June 12 2022
Volume 2 On	aws Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	aws Working Environment 1 On	Source SVM 1	Compliance	Active	

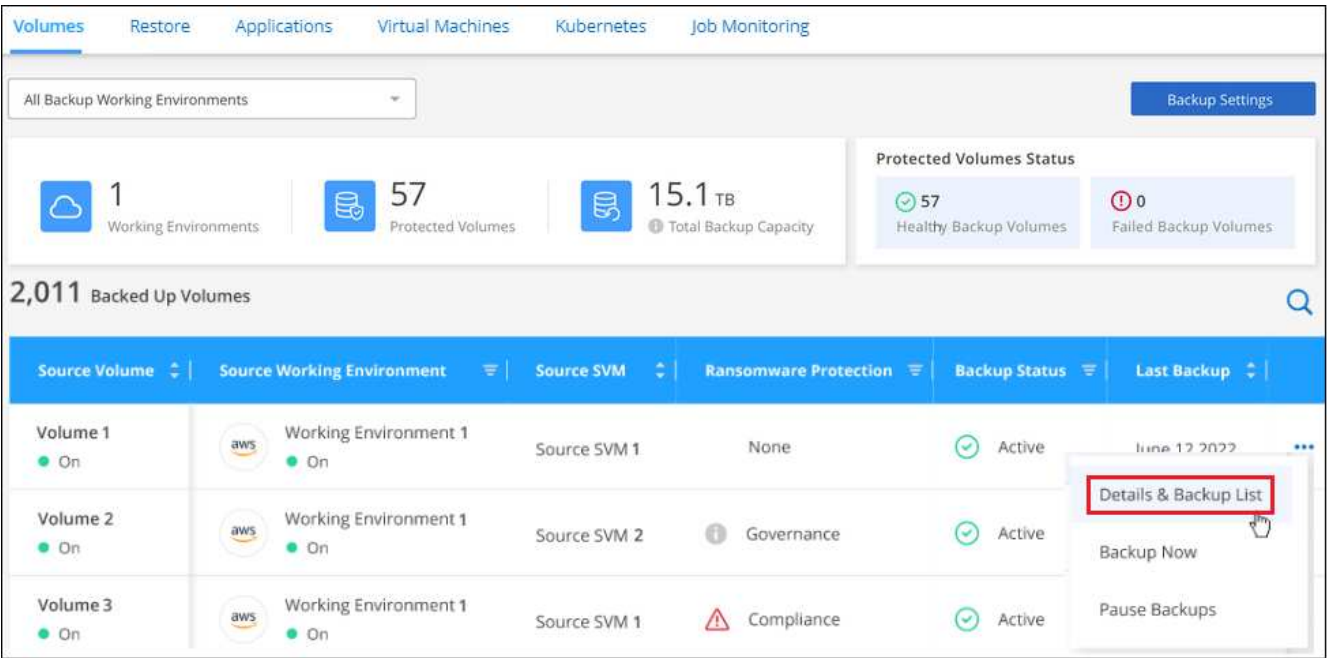
La columna Backup Status de ese volumen muestra "in progress" hasta que se crea el backup.

Ver la lista de backups de cada volumen

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

Pasos

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



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

Source

Volume

Volume Name

Working Environment

Working Environment N...

Type

Cloud Volumes ONTAP (HA)

Provider

AWS

SVM

SVM Name

Destination

Cloud Provider

AWS

Bucket

Backup Bucket Name

Region

US East (N.Virginia)

Account ID

01234567890123456789

Backup Information

Relationship Status

Active

Last Backup

Oct 26 2022, 8:27:34 pm

Lag Duration

1 day ago

Backups

125

Policy Name

My_First_Policy

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

Ejecuta un análisis de ransomware en un backup de volumen

El software de protección ransomware de NetApp analiza sus archivos de backup para buscar pruebas de un ataque de ransomware cuando se crea un archivo de backup y cuando se restauran los datos de un archivo de backup. También puede ejecutar un análisis de protección contra ransomware bajo demanda en cualquier momento para verificar la facilidad de uso 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.

Esta función solo está disponible si el backup de volumen se creó a partir de un sistema con ONTAP 9.11.1 o posterior y si se habilitó *DataLock* y *Protección de ransomware* en la política de backup.

Pasos

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

The screenshot displays the AWS Backup console interface. At the top, there are navigation tabs: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below these, a dropdown menu shows 'All Backup Working Environments'. A summary section indicates 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' box shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. The main section is titled '2,011 Backed Up Volumes'. A table lists volumes with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. A context menu is open for 'Volume 3', showing options: 'Details & Backup List' (highlighted), 'Backup Now', and 'Pause Backups'.

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

- Haga clic en ... Para el archivo de copia de seguridad de volumen que desea analizar y haga clic en **Análisis de ransomware**.

The screenshot displays the AWS Backup console interface for the 'Backups' section. It shows 125 Backups. A table lists backups with columns: Backup Name, Date, Size, Ransomware Scan, and Storage Class. A context menu is open for 'Backup 20', showing options: 'Delete', 'Restore', and 'Ransomware Scan' (highlighted).

La columna Análisis de ransomware mostrará que la exploración está en curso.

Eliminar backups

Cloud Backup le permite eliminar un único archivo de backup, eliminar todos los backups del volumen o eliminar todos los backups 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.



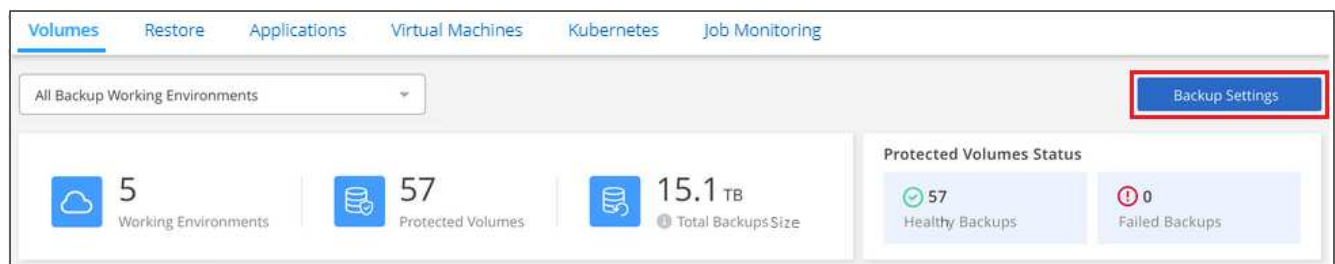
Si piensa eliminar un entorno de trabajo o clúster que tiene copias de seguridad, debe eliminar las copias de seguridad **antes de** eliminando el sistema. Cloud Backup no elimina automáticamente las copias de seguridad cuando se elimina un sistema y no hay compatibilidad actual en la interfaz de usuario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

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

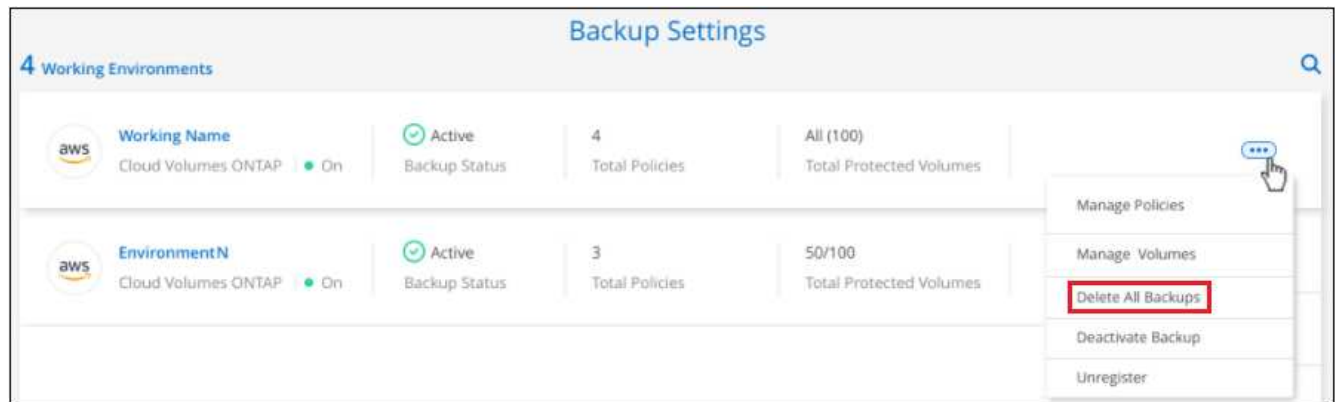
La eliminación de todos los backups de un entorno de trabajo no deshabilita los futuros backups de los volúmenes en este entorno de trabajo. Si desea detener la creación de backups de todos los volúmenes en un entorno de trabajo, puede desactivar los backups [como se describe aquí](#).

Pasos

1. En la ficha **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**.

Eliminación de todos los archivos de backup de un volumen

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

Puede hacerlo [reinicie haciendo backups para el volumen](#) En cualquier momento desde la página Manage backups.

Pasos

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

seguridad.

The screenshot shows the 'Volumes' dashboard with a top navigation bar including 'Volumes', 'Restore', 'Applications', 'Virtual Machines', 'Kubernetes', and 'Job Monitoring'. A dropdown menu is open for 'All Backup Working Environments'. The dashboard displays summary statistics: 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a section for '2,011 Backed Up Volumes' features a table with columns: Source Volume, Source Working Environment, Source SVM, Ransomware Protection, Backup Status, and Last Backup. The table lists three volumes. A dropdown menu is open for 'Volume 2', showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

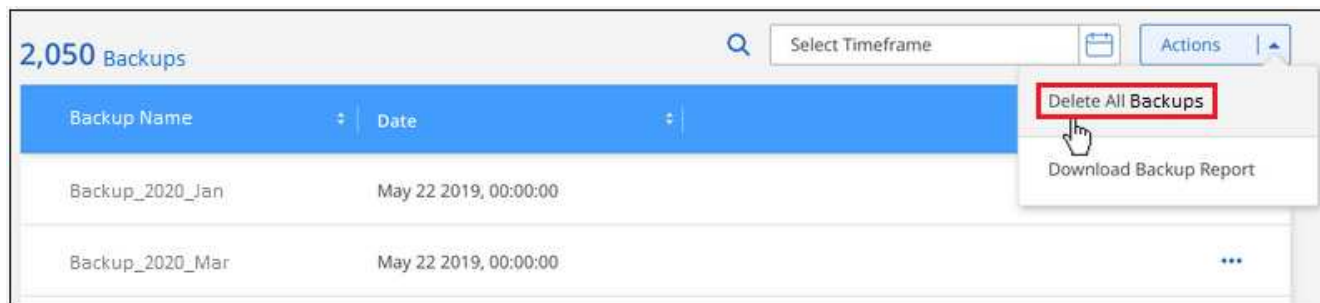
Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	Last Backup
Volume 1 On	Working Environment 1 On	Source SVM 1	None	Active	June 12 2022
Volume 2 On	Working Environment 1 On	Source SVM 2	Governance	Active	
Volume 3 On	Working Environment 1 On	Source SVM 1	Compliance	Active	

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

The screenshot shows the 'Backup details' page. It is divided into three main sections: 'Source', 'Destination', and 'Backup Information'. The 'Source' section lists details for Volume, Working Environment, Type, Provider, and SVM. The 'Destination' section lists details for Cloud Provider, Bucket, Region, and Account ID. The 'Backup Information' section lists details for Relationship Status, Last Backup, Lag Duration, Backups, and Policy Name. Below these sections, a section for '125 Backups' features a table with columns: Backup Name, Date, Size, Ransomware Scan, and Storage Class. The table lists three backups. A dropdown menu is open for 'Backup 2', showing options: 'Details & Backup List' (highlighted with a red box), 'Backup Now', and 'Pause Backups'.

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

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



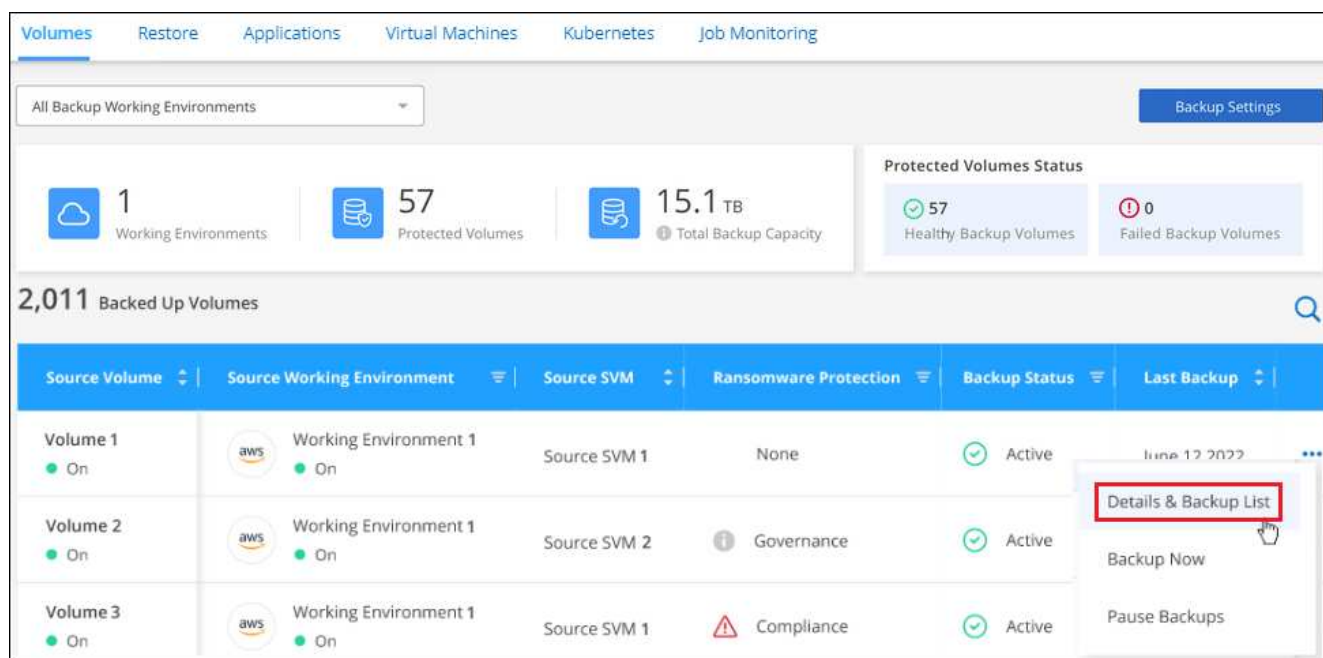
3. En el cuadro de diálogo de confirmación, introduzca el nombre del volumen y haga clic en **Eliminar**.

Eliminar un único archivo de backup para un volumen

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

Pasos

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



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

Source

Volume

Volume Name

Working Environment

Working Environment N...

Type

Cloud Volumes ONTAP (HA)

Provider

AWS

SVM

SVM Name

Destination

Cloud Provider

AWS

Bucket

Backup Bucket Name

Region

US East (N.Virginia)

Account ID

01234567890123456789

Backup Information

Relationship Status

Active

Last Backup

Oct 26 2022, 8:27:34 pm

Lag Duration

1 day ago

Backups

125

Policy Name

My_First_Policy

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 12:00:00	20.12 GiB	Protected	Standard
Backup 2	June 12 2022, 13:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 3	June 12 2022, 14:00:00	20.12 GiB	Protected	Standard

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

125 Backups

Select Timeframe

Actions

Backup Name	Date	Size	Ransomware Scan	Storage Class
Backup 1	June 12 2022, 00:00:00	20.125 GiB	Potential Ransomware identified	Standard
Backup 2	June 12 2022, 00:00:00	2.5 GiB	Protected	Standard
Backup 12	June 12 2022, 00:00:00	20 GiB	Protected	Standard
Backup 20	June 12 2022, 00:00:00	125 GiB	Failed	Standard

Delete

Restore

Ransomware Scan

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

Eliminación de relaciones de backup de volumen

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.

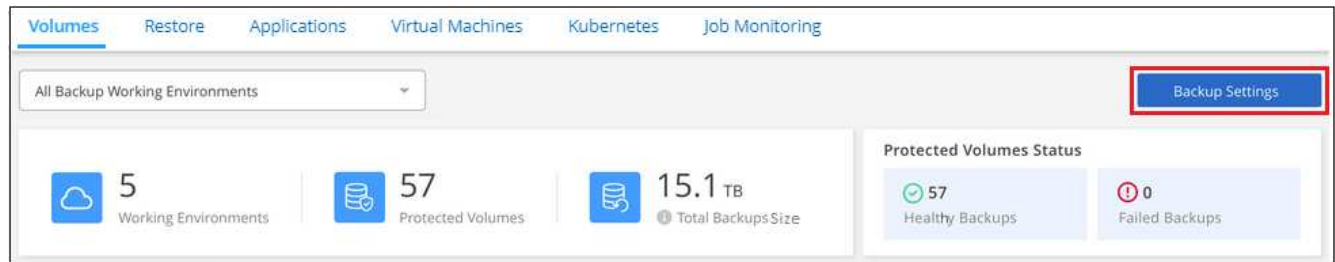
No se puede eliminar el volumen de origen de la interfaz de usuario de Cloud Backup. Sin embargo, puede abrir la página Detalles de volumen en el lienzo y ["elimine el volumen desde allí"](#).



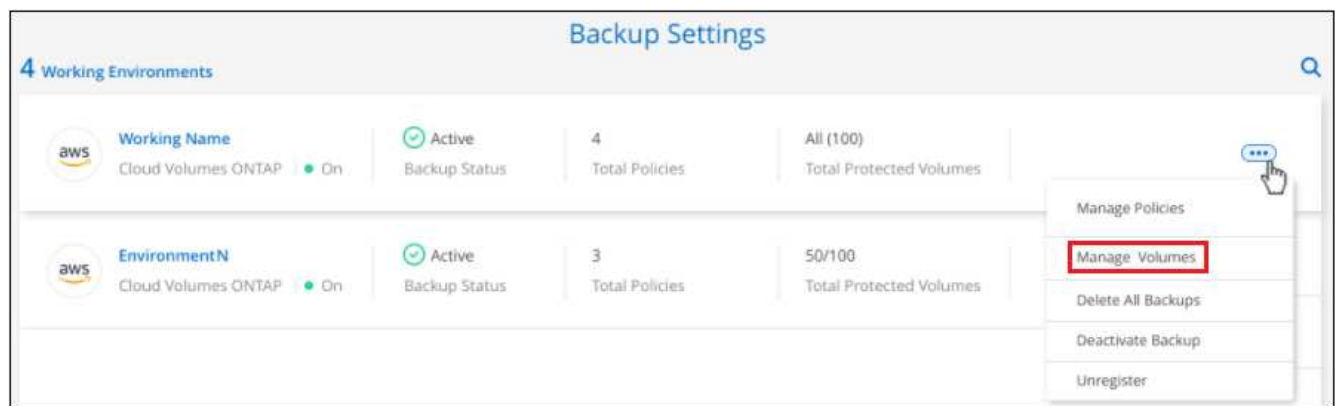
No se pueden eliminar archivos de backup de volúmenes individuales una vez que se ha eliminado la relación. Sin embargo, usted puede "eliminar todos los backups del volumen" si desea quitar todos los archivos de backup.

Pasos

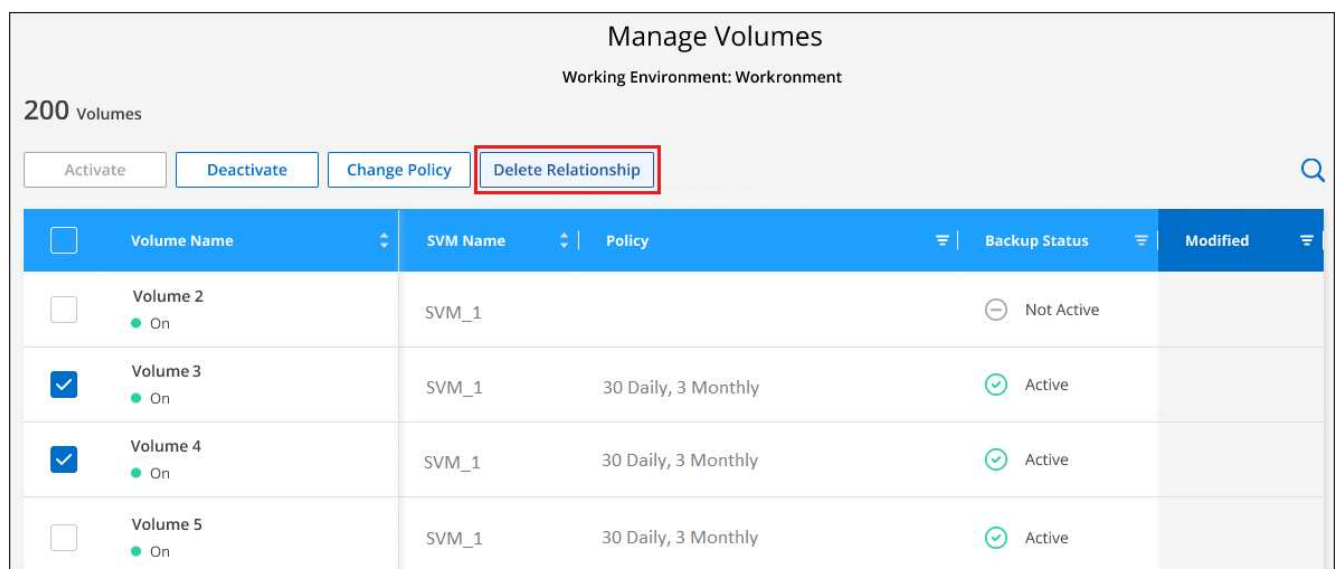
1. En la ficha **Volumes**, seleccione **Configuración de copia de seguridad**.



2. En la página *Backup Settings*, haga clic en ... Para el entorno de trabajo y seleccione **gestionar volúmenes**.



3. Seleccione la casilla de verificación de un volumen o volúmenes que desee eliminar la relación de copia de seguridad y, a continuación, haga clic en **Eliminar relación**.



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

Tenga en cuenta que también puede eliminar la relación de backup para un único volumen de la página Volumes.

2,011 Backed Up Volumes

Source Volume	Source Working Environment	Source SVM	Ransomware Protection	Backup Status	
Volume 1 On	aws Working Env On	SVM-1	Compliance	Active	⋮
Vol 3 On	aws Working Env On	SVM-1		Active	Details & Backup List
Volume 2 On	aws Working Env On	SVM-1	Compliance	Active	Backup Now
					Pause Backups
					Delete Relationship

Cuando vea la lista de copias de seguridad para cada volumen, verá el "Estado de la relación" que aparece como **relación eliminada**.

Source

Volume
Working Environment
Type
Provider
SVM

Volume Name
Working Environment N...
Cloud Volumes ONTAP (HA)
AWS
SVM Name

Destination

Cloud Provider
Bucket
Region
Account ID

AWS
Backup Bucket Name
US East (N.Virginia)
01234567890123456789

Backup Information

Relationship Status
Last Backup
Lag Duration
Backups
Policy Name

Relationship Deleted
Oct 26 2022, 8:27:34 pm

125
My_First_Policy

125 Backups

Backup Name	Date	Size	Ransomware Scan	Storage Class	
Backup 1	June 12 2022, 12:00:00	20.12 GiB	None	Standard	⋮
Backup 2	June 12 2022, 13:00:00	20.125 GiB	None	Standard	⋮
Backup 3	June 12 2022, 14:00:00	20.12 GiB	None	Standard	⋮

Desactivación de Cloud Backup en un entorno de trabajo

Al desactivar Cloud Backup en un entorno en funcionamiento se deshabilitan los backups 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.

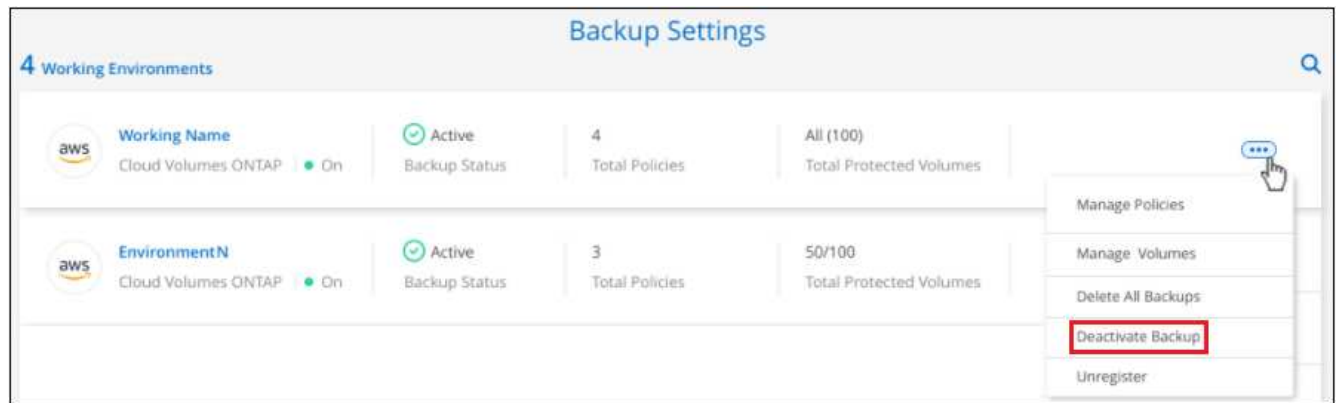
Tenga en cuenta que su proveedor de cloud seguirá facturando los costes del almacenamiento de objetos por la capacidad que utilicen sus backups a menos que usted [eliminar los backups](#).

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.

Cancelación del registro de Cloud Backup para un entorno de trabajo

Es posible cancelar el registro de Cloud Backup para un entorno de trabajo si ya no desea usar la funcionalidad de backup y quiere dejar de estar cargado por backups en ese entorno de trabajo. Normalmente, esta función se 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 Cloud Backup para el entorno laboral, puede habilitar Cloud Backup para ese clúster mediante la nueva información del proveedor de cloud.

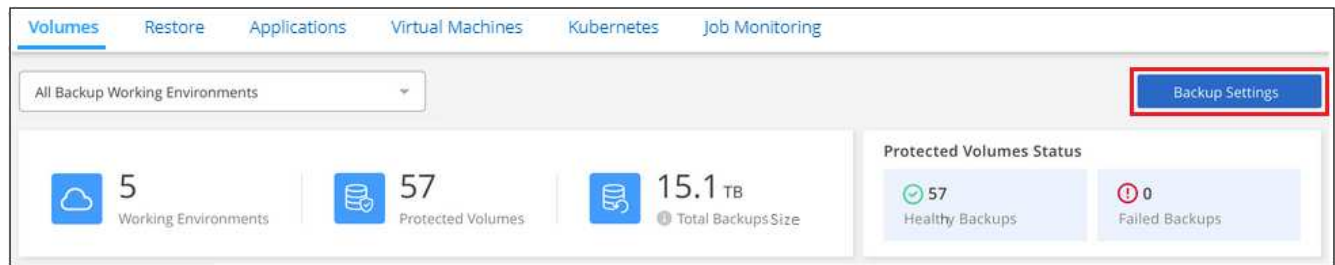
Para poder cancelar el registro de Cloud Backup, debe realizar los siguientes pasos en el siguiente orden:

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

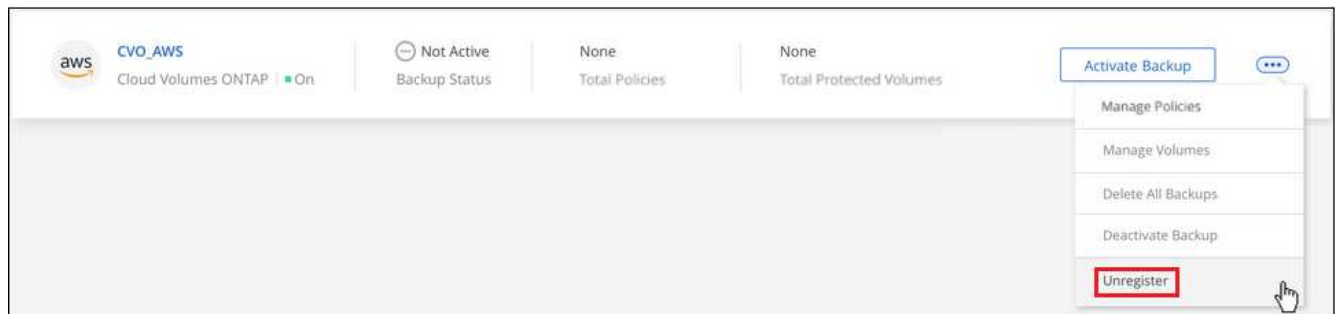
La opción cancelar el registro no estará disponible hasta que se completen estas dos acciones.

Pasos

1. En la ficha **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**.

Gestión de la configuración de backup en el nivel del clúster

Puede cambiar muchas opciones de configuración de backup en el nivel del clúster que haya establecido al activar Cloud Backup para cada sistema ONTAP. También puede modificar algunos ajustes que se aplican como ajustes de copia de seguridad "predeterminados". Esto incluye cambiar las claves de almacenamiento, la tasa de transferencia de los backups a su almacenamiento de objetos, si las copias Snapshot históricas se exportan como archivos de backup y más.

La configuración de backup a nivel de clúster está disponible en la página *Advanced Settings*.

El conjunto completo de ajustes de copia de seguridad que puede cambiar incluye:

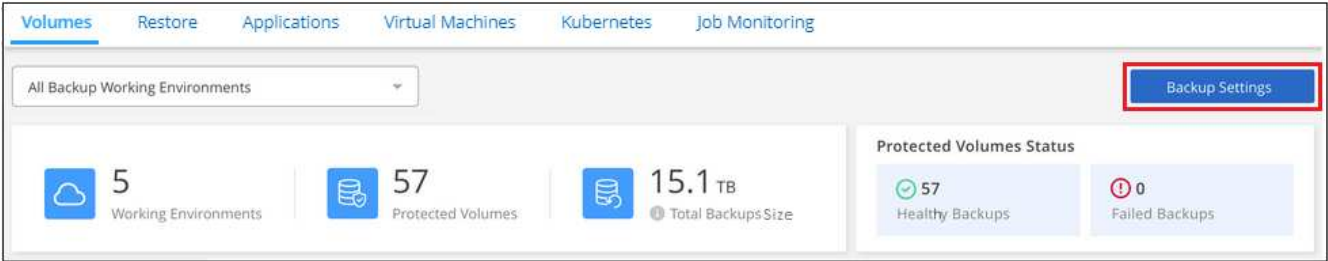
- Cambiar las claves de almacenamiento que otorgan a su sistema ONTAP permiso para acceder al almacenamiento de objetos
- Cambiar el espacio IP de la ONTAP conectado al almacenamiento de objetos
- Cambiar el ancho de banda de red asignado para cargar backups en el almacenamiento de objetos
- Cambiar la clase de almacenamiento de archivado (solo AWS)
- Cambiar la configuración (y la política) automática de backup para volúmenes futuros
- Cambiar si se incluyen las copias snapshot históricas en los archivos de backup de base iniciales para volúmenes futuros
- Cambiar si las copias Snapshot "anuales" se eliminan del sistema de origen

Ver la configuración de backup en el nivel del clúster

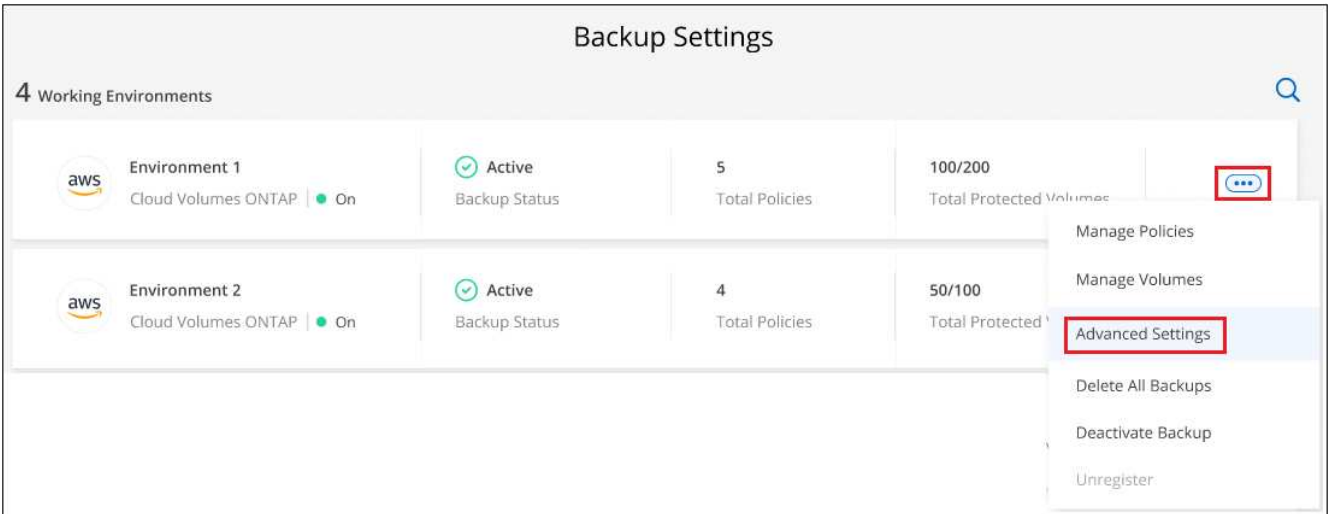
Es posible ver la configuración de backup a nivel de clúster de cada entorno de trabajo.

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.

Advanced Settings		
Working Environment: Environment 4		
Storage Keys	Access Key: 0123456789	▼
IPspace	Default	▼
Max Transfer Rate	Unlimited	▼
Archival Storage Class	S3 Glacier	▼
Automatic Backup	Enabled	▼
Export existing Snapshot copies	Enabled	▼
Yearly Snapshot Deletion	Enabled	▼

Si necesita realizar algún cambio, 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 las claves de almacenamiento para que ONTAP acceda al almacenamiento en cloud

Si tiene una política de empresa que le obliga a rotar periódicamente todas las credenciales, por ejemplo, cada 6 meses o un año, así será como sincronizará la clave de acceso y la clave secreta del proveedor de cloud con su sistema ONTAP. Esto le permite actualizar las credenciales de su proveedor de cloud y cambiar las claves de su sistema de ONTAP para que los dos sistemas sigan comunicándose.

Esta opción solo está disponible para sistemas ONTAP en las instalaciones y solo cuando se almacenan backups en Amazon S3, Google Cloud Storage y StorageGRID.

Storage Keys	Access Key: 0123456789
Access Key	Secret Key
<input type="text" value="1111111111"/>	<input type="password" value="*****"/>
Apply Cancel	

Sólo tiene que introducir la nueva clave de acceso y la clave secreta, y hacer clic en **aplicar**.

Cambie el espacio IP de la ONTAP que está conectado al almacenamiento de objetos

Puede cambiar el espacio IP de la ONTAP que está conectado al almacenamiento de objetos. Esta opción está disponible cuando se realiza un backup de datos solo de sistemas ONTAP en las instalaciones; no está disponible para sistemas Cloud Volumes ONTAP.

Esta opción no se debe utilizar en un sistema que realice backups activos de datos de volumen en un almacenamiento de objetos. Solo se debe utilizar en caso de que se haya seleccionado un espacio IP incorrecto al activar inicialmente el backup en un sistema ONTAP en las instalaciones.

Consulte la documentación de introducción para realizar backups de los datos de los sistemas ONTAP en las instalaciones en su proveedor de cloud específico a fin de asegurarse de que la configuración de ONTAP se ha configurado correctamente para el espacio IP nuevo. Por ejemplo:

- 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 espacio IP que ONTAP debe utilizar para conectarse al almacenamiento de objetos.
- Las LIF de interconexión de clústeres de los nodos deben poder acceder al almacén de objetos.
- Si utiliza un espacio IP diferente al *default*, es posible que deba crear una ruta estática para obtener acceso al almacenamiento de objetos.



The screenshot shows a dialog box titled "IPspace" with a close button in the top right corner. Inside the dialog, there is a label "IPspace" above a dropdown menu that currently displays "Default". At the bottom left of the dialog, there are two buttons: "Apply" (in blue) and "Cancel".

Sólo tiene que seleccionar el nuevo espacio IP y hacer clic en **aplicar**. Tras ello, podrá seleccionar los volúmenes de los que desea realizar copias de seguridad de los agregados en ese espacio IP.

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

Al activar Cloud Backup en un entorno de trabajo, de forma predeterminada, ONTAP puede usar una cantidad ilimitada de ancho de banda para transferir los datos del backup de 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 utilizado durante la transferencia. Puede elegir un valor entre 1 y 1,000 Mbps como la velocidad máxima de transferencia.



The screenshot shows a dialog box titled "Max Transfer Rate" with a close button in the top right corner. Inside the dialog, there are two radio button options: "Unlimited" and "Limited". The "Limited" option is selected. To the right of the "Limited" option is a text field labeled "Limited to:" which contains the value "1-1,000 Mbps". At the bottom left of the dialog, there are two buttons: "Apply" (in blue) and "Cancel".

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.

Cambie la clase de almacenamiento de archivado

Si desea cambiar la clase de almacenamiento de archivado que se utiliza cuando los archivos de copia de seguridad se han almacenado durante un determinado número de días (normalmente más de 30 días), puede realizar el cambio aquí. Todas las normativas de backup que utilizan almacenamiento de archivado han cambiado inmediatamente para utilizar este nuevo tipo de almacenamiento.

Esta opción está disponible para los sistemas ONTAP y Cloud Volumes ONTAP en las instalaciones (con ONTAP 9.10.1 o superior) al escribir archivos de backups en Amazon S3.

Tenga en cuenta que sólo puede cambiar de *S3 Glacier* a *S3 Glacier Deep Archive*. Una vez que haya seleccionado Glacier Deep Archive, no podrá volver a Glacier.



Archival Storage Class

☒ S3 Glacier

☐ S3 Glacier Deep Archive

Apply Cancel

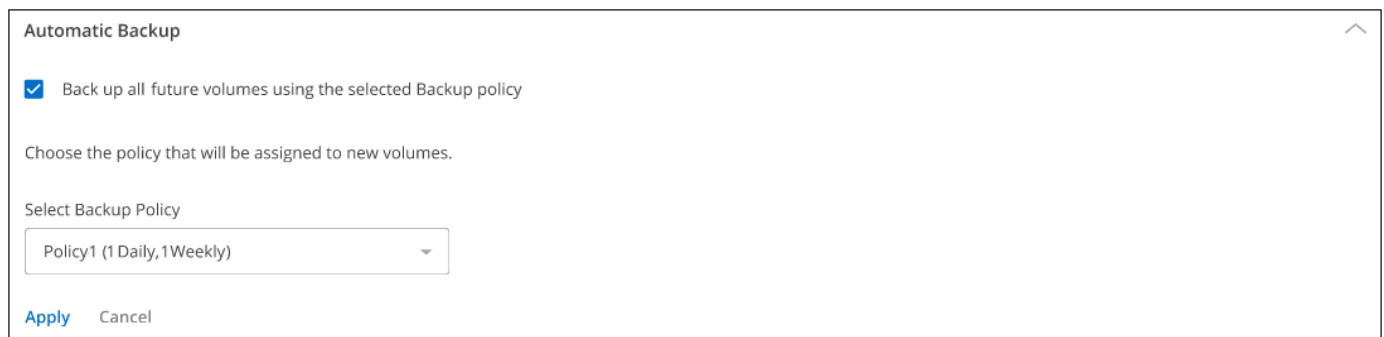
["Obtenga más información sobre la configuración de almacenamiento de archivado"](#). ["Obtenga más información sobre el uso del almacenamiento de archivado de AWS"](#).

Cambie la configuración de backup automático para los volúmenes futuros

Si no habilitó el backup automático de futuros volúmenes al activar Cloud Backup, puede empezar a realizar copias de seguridad automáticas de los volúmenes nuevos en la sección copia de seguridad automática. También puede seleccionar la política de backup que se aplicará a esos nuevos volúmenes. Si se asigna una política de backup a volúmenes recién creados, se garantizan que todos los datos estén protegidos.

Si habilitó el backup automático de volúmenes futuros al activar Cloud Backup, puede cambiar la política de backup que se utilizará para los volúmenes recién creados en la sección Automatic Backup.

Tenga en cuenta que la política que desea aplicar a nuevos volúmenes ya debe existir. ["Descubra cómo crear una nueva normativa de backup para un entorno de trabajo"](#).



Automatic Backup

☒ Back up all future volumes using the selected Backup policy

Choose the policy that will be assigned to new volumes.

Select Backup Policy

Policy1 (1 Daily, 1Weekly)

Apply Cancel

Una vez habilitada, esta normativa de backup se aplicará a los volúmenes nuevos creados en este entorno de trabajo mediante BlueXP, System Manager, la CLI de ONTAP o las API.

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).

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](#)

Sólo tiene que seleccionar si desea exportar las copias Snapshot existentes y hacer clic en **aplicar**.

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

Si selecciona la etiqueta de backup "Anual" para una política de backup para cualquiera de los volúmenes, la copia de Snapshot creada es muy grande. De forma predeterminada, estas snapshots 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.

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](#)

Seleccione **Desactivado** y haga clic en **aplicar** si desea conservar las instantáneas anuales en el sistema de origen.

Restaurar datos ONTAP a partir de archivos de backup

Los backups se almacenan en un almacén de objetos en su cuenta de cloud para que pueda restaurar datos desde un momento específico. Es posible restaurar un volumen completo de ONTAP desde un archivo de backup o si solo es necesario restaurar unos pocos archivos, puede restaurar una carpeta o archivos individuales desde un archivo de backup.


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.

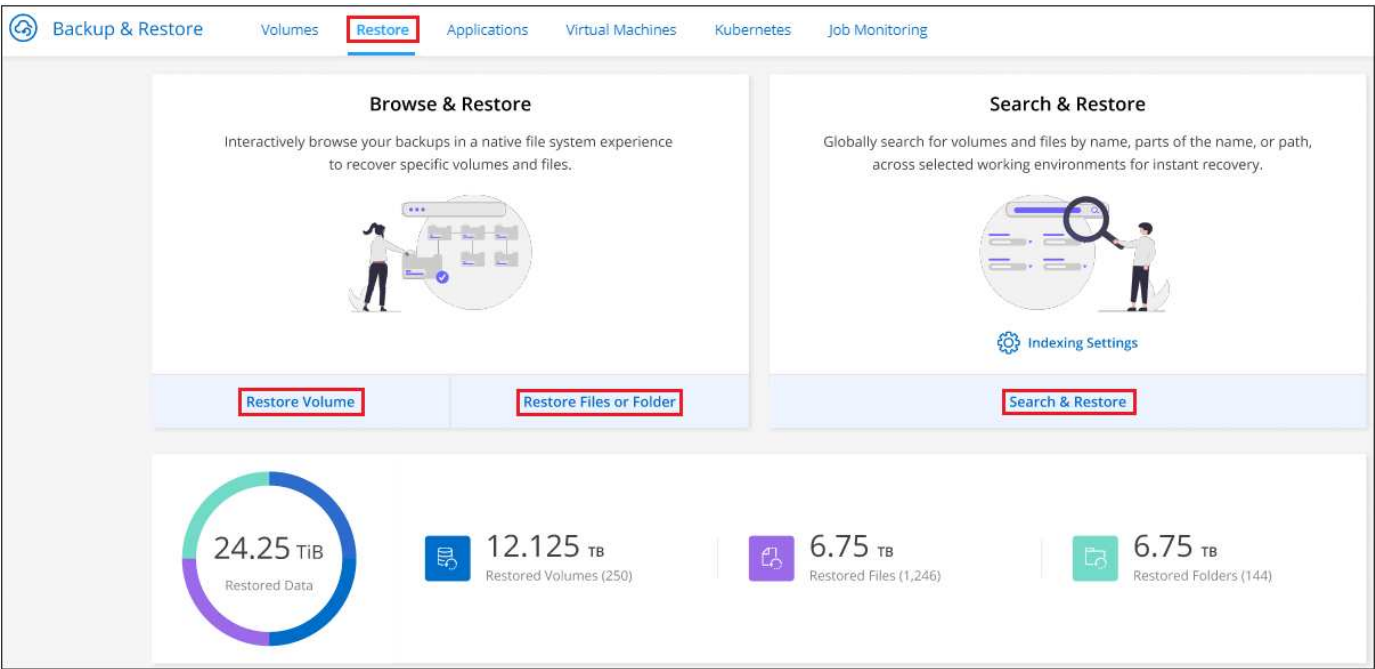
Se necesita una licencia de Cloud Backup válida para restaurar datos de archivos de backup a un sistema de producción.

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.



Cloud Backup debe estar activado como mínimo en un entorno de trabajo y deben existir archivos de backup 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 los 2 métodos.

Examinar y restaurar	Búsqueda y restauración
Examine una estructura de tipo carpeta para buscar el volumen, carpeta o archivo dentro de un único archivo de copia de seguridad	Busque un volumen, carpeta o archivo en todos los archivos de copia de seguridad por nombre de volumen parcial o completo, nombre de carpeta/archivo parcial o completo, intervalo de tamaño y filtros de búsqueda adicionales
La restauración de volúmenes y archivos funciona con archivos de backup almacenados en Amazon S3, Azure Blob, Google Cloud y NetApp StorageGRID	La restauración de volúmenes y archivos funciona con archivos de backup almacenados en Amazon S3, Azure Blob, Google Cloud y NetApp StorageGRID
Restaurar volúmenes, carpetas y archivos desde StorageGRID en sitios sin acceso a Internet	Restaurar volúmenes, carpetas y archivos desde StorageGRID en sitios sin acceso a Internet
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
Busque resultados en clouds públicos y privados	Busque resultados en clouds públicos y copias Snapshot locales
No se requieren recursos de proveedor de cloud adicionales	Se requieren recursos de bloque y proveedor de cloud público adicionales por cuenta
No requiere costes de proveedor de cloud adicionales	Coste asociado con los recursos del proveedor de cloud público al analizar sus backups y volúmenes para obtener resultados de búsqueda

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:

- <<Restoring volumes using Browse & Restore, Restaure volúmenes mediante la función examinar Restore
- <<Restoring folders and files using Browse & Restore, Restaure carpetas y archivos utilizando examinar Restore
- <<Restoring ONTAP data using Search & Restore, Restaure 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.

Nota: Si el archivo de copia de seguridad que contiene los datos que desea restaurar reside en el almacenamiento de archivado (a partir de ONTAP 9.10.1), la operación de restauración tardará 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 y 9.12.1 para Google Archive y StorageGRID.

["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS".](#)



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 un volumen, una carpeta o archivos individuales, desde un archivo de backup de ONTAP a los siguientes entornos de trabajo:

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino <code>ifdef::aws[]</code>
Amazon S3	Cloud Volumes ONTAP en la endif del sistema ONTAP en las instalaciones de AWS::aws[] <code>ifdef::Azure[]</code>
Azure Blob	Cloud Volumes ONTAP en Azure on-premises ONTAP system endif::Azure[] <code>ifdef::gcp[]</code>
Google Cloud Storage	Cloud Volumes ONTAP en Google on-local ONTAP system endif::gcp[]
StorageGRID de NetApp	Sistema ONTAP en las instalaciones

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 StorageGRID, el conector debe estar desplegado en sus instalaciones, con o sin acceso a Internet

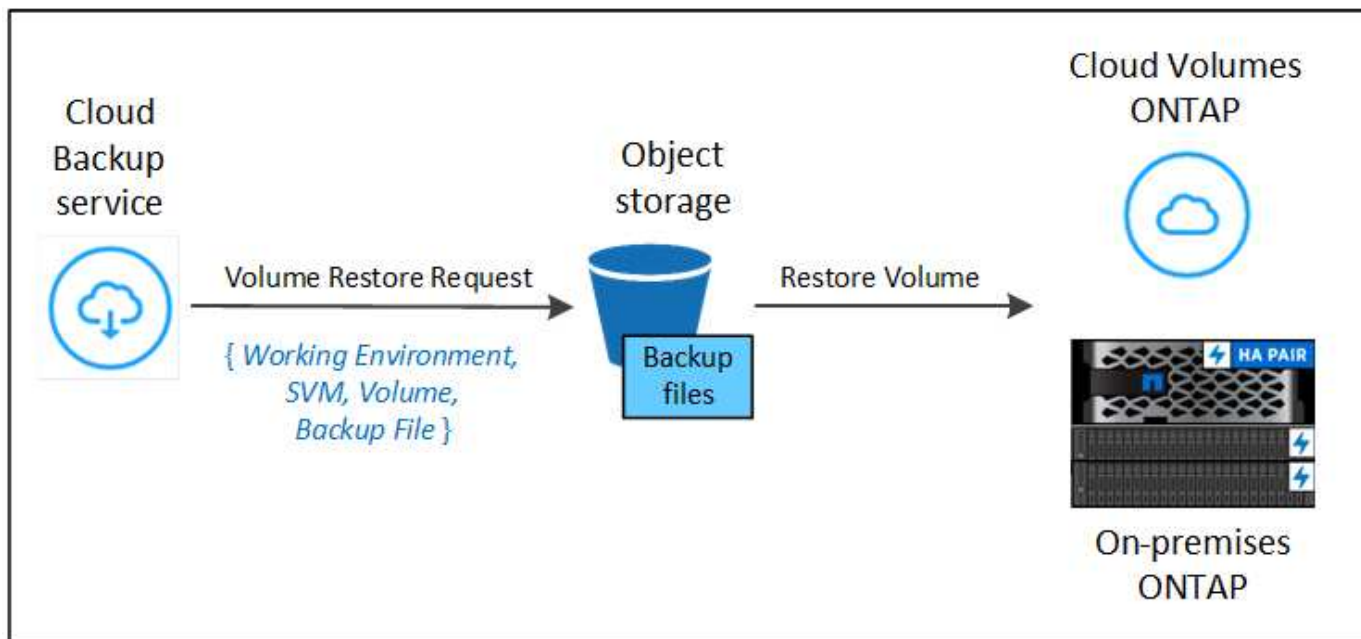
Tenga en cuenta que las referencias a "sistemas ONTAP en las instalaciones" incluyen sistemas FAS, AFF y ONTAP Select.



No se pueden 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.

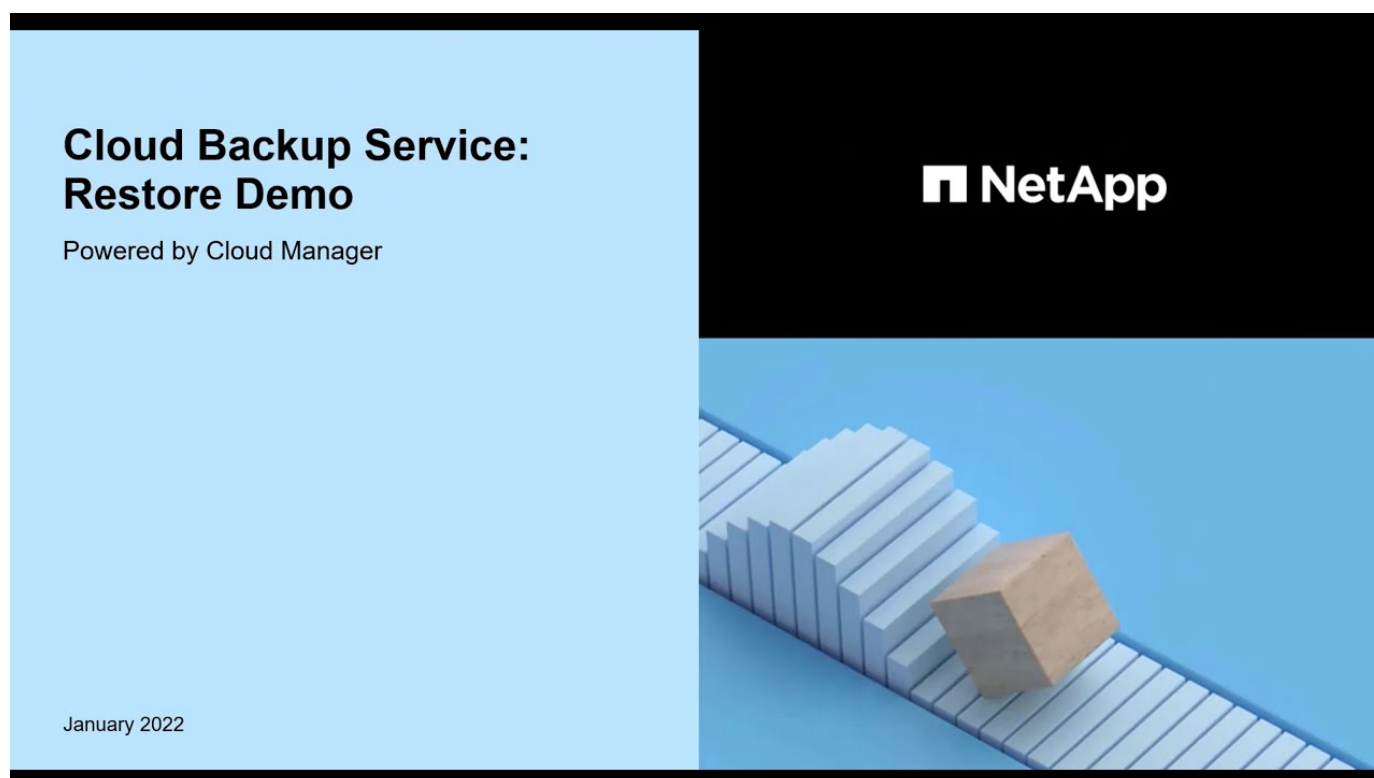
Restaurar volúmenes mediante Browse y Restore

Al restaurar un volumen a partir de un archivo de copia de seguridad, Cloud Backup crea un volumen *new* utilizando los datos de la copia de seguridad. Puede restaurar los datos en un volumen del entorno de trabajo original o en otro entorno de trabajo ubicado en la misma cuenta de cloud que el entorno de trabajo de origen. También es posible restaurar volúmenes en un sistema ONTAP en las instalaciones.



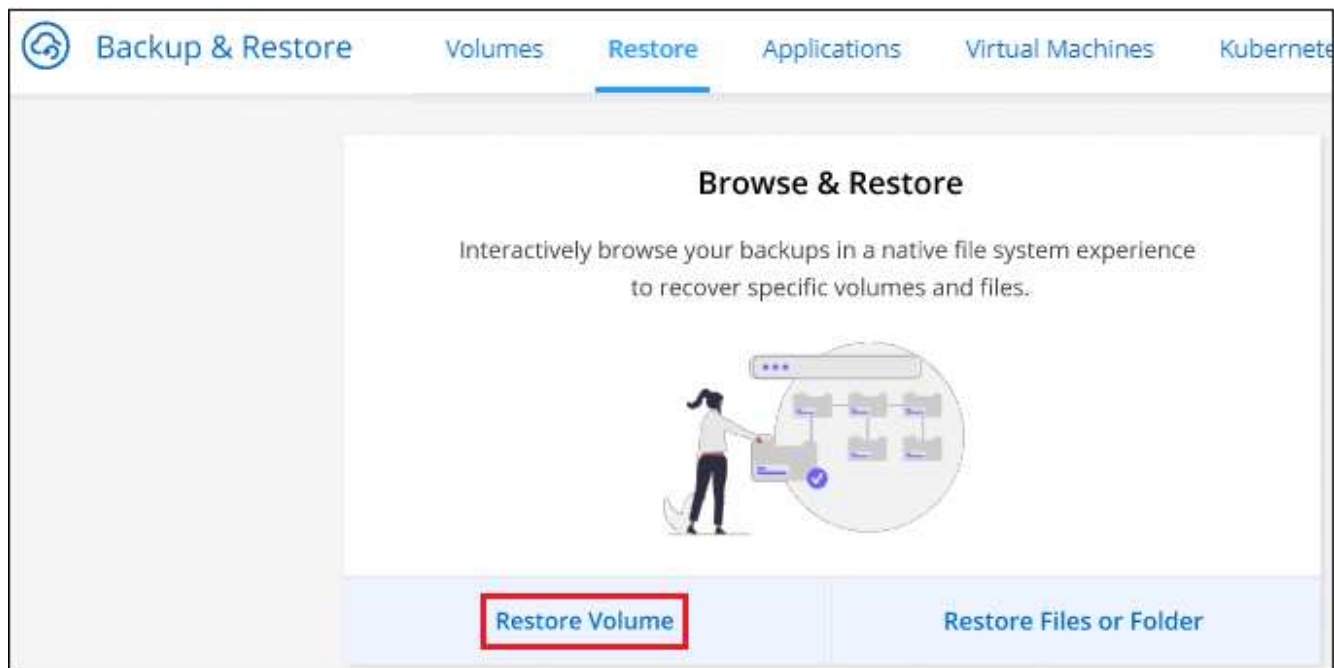
Como puede ver, necesita conocer el nombre del entorno de trabajo, la máquina virtual de almacenamiento, el nombre del volumen y la fecha del archivo de backup para restaurar un volumen.

En el siguiente vídeo se muestra un tutorial rápido sobre cómo restaurar un volumen:

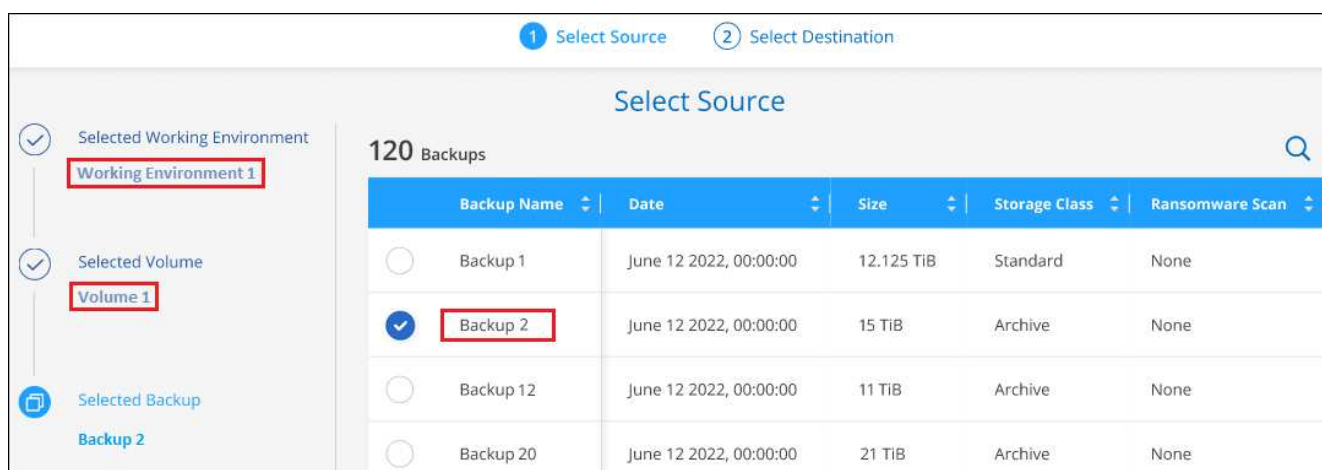


Pasos

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**.



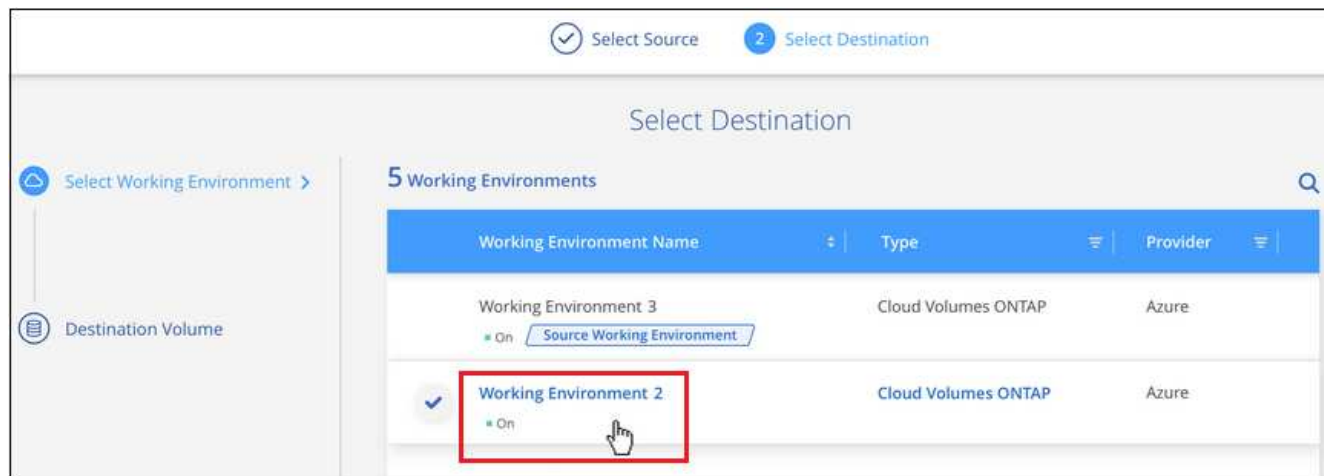
4. En la página *Select Source*, desplácese hasta el archivo de copia de seguridad del volumen que desea restaurar. Seleccione **entorno de trabajo**, **volumen** y el archivo **copia de seguridad** que tiene la Marca de fecha/hora desde la que desea restaurar.



5. Haga clic en **Siguiente**.

Tenga en cuenta que si la protección contra ransomware está activa para el archivo de copia de seguridad (si habilitó DataLock y la protección contra ransomware en la política de copia de seguridad), se le solicitará que ejecute un análisis adicional de ransomware en el archivo de copia de seguridad antes de restaurar los datos. Se recomienda que escanee el archivo de backup como ransomware.

6. En la página *Select Destination*, seleccione **entorno de trabajo** donde desea restaurar el volumen.



7. 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.
 - 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.
 - 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. Al restaurar un volumen de FlexGroup, puede elegir varios agregados. De forma predeterminada, se utiliza **<source_volume_name>_restore** como nombre del volumen.

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".

1. Haga clic en **Restaurar** y volverá al Panel de restauración para que pueda revisar el progreso de la

operación de restauración.

Resultado

Cloud Backup crea un nuevo volumen según el backup seleccionado. Puede hacerlo ["gestione la configuración de backup para este nuevo volumen"](#) según sea necesario.

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.

Restaurar carpetas y archivos mediante Browse & Restore

Si solo necesita restaurar algunos archivos desde un backup de volumen 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.

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.



- Actualmente, no se admite la restauración a nivel de carpeta si el archivo de backup se configuró con DataLock y Ransomware. En este caso, es posible restaurar todo el volumen desde el archivo de backup y, a continuación, acceder a la carpeta y los archivos necesarios.
- Actualmente, no se admite la restauración a nivel de carpeta si el archivo de backup reside en el almacenamiento de archivado. En este caso, puede restaurar la carpeta desde un nuevo archivo de copia de seguridad que no se haya archivado o restaurar todo el volumen desde la copia de seguridad archivada y, a continuación, acceder a la carpeta y los archivos que necesite.

Requisitos previos

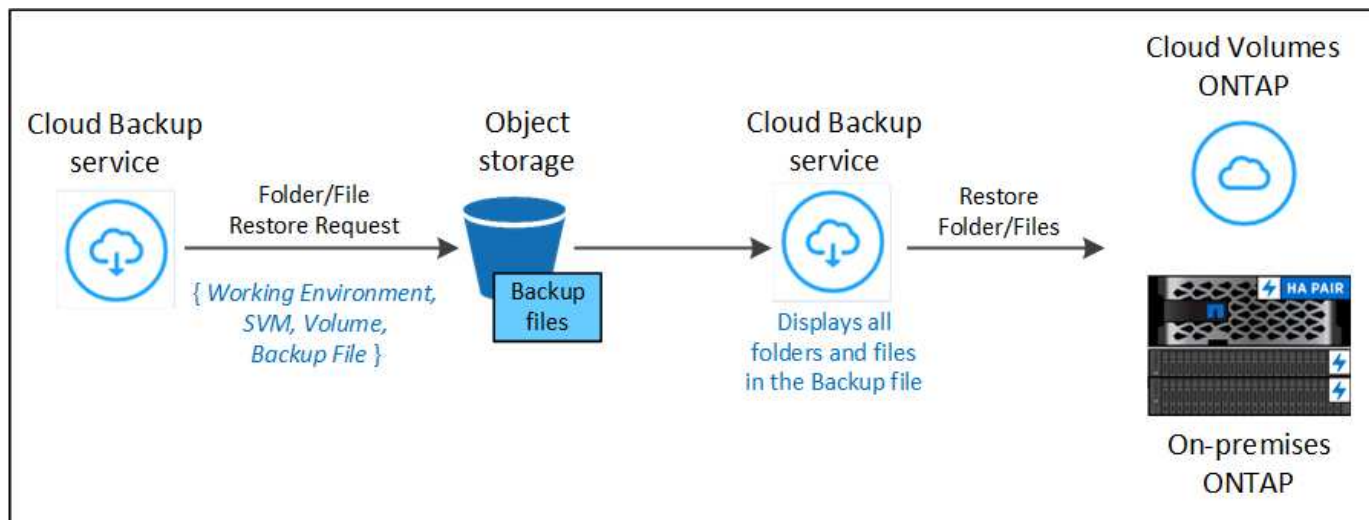
- La versión de ONTAP debe ser 9.6 o superior para realizar operaciones de restauración *File*.
- La versión de ONTAP debe ser 9.11.1 o superior para realizar operaciones de restauración de *folder*.

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. Cloud Backup muestra las carpetas y los 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.

Restauración de 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.

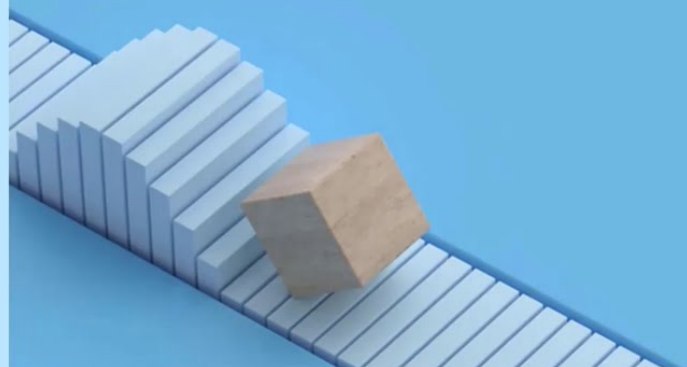
El siguiente vídeo muestra un tutorial rápido sobre cómo restaurar un único archivo:

Cloud Backup Service: Restore Demo

Powered by Cloud Manager

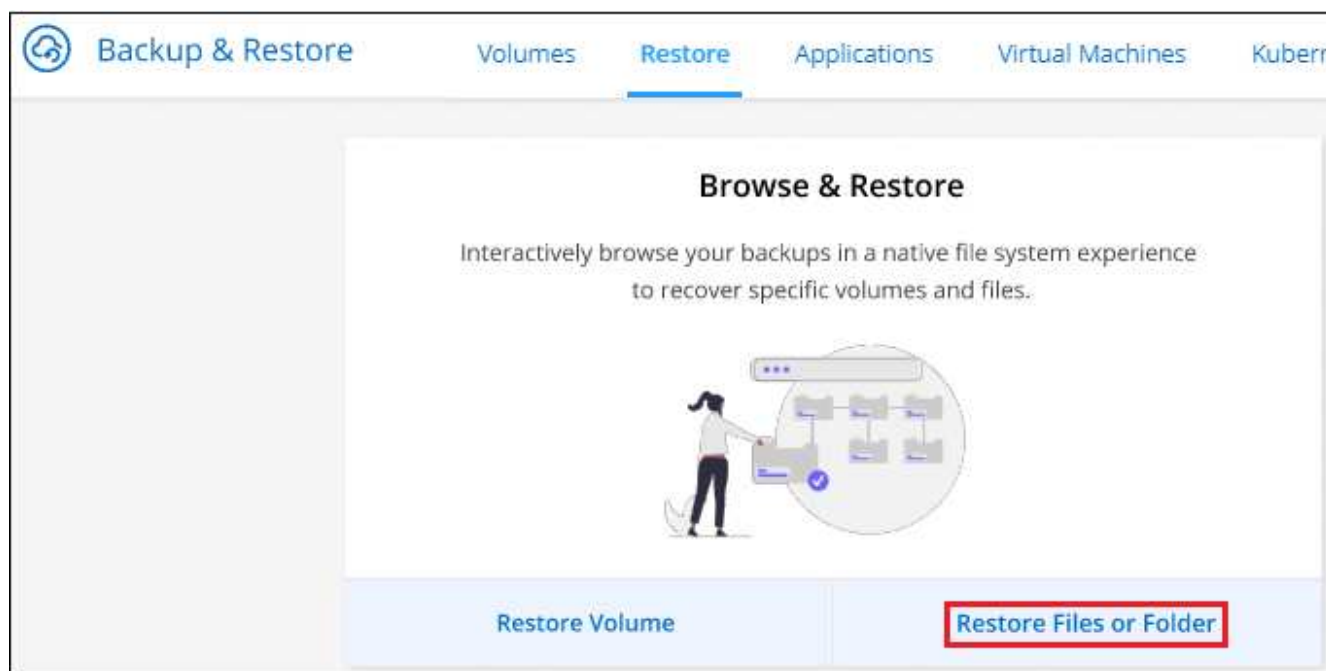
January 2022

 NetApp

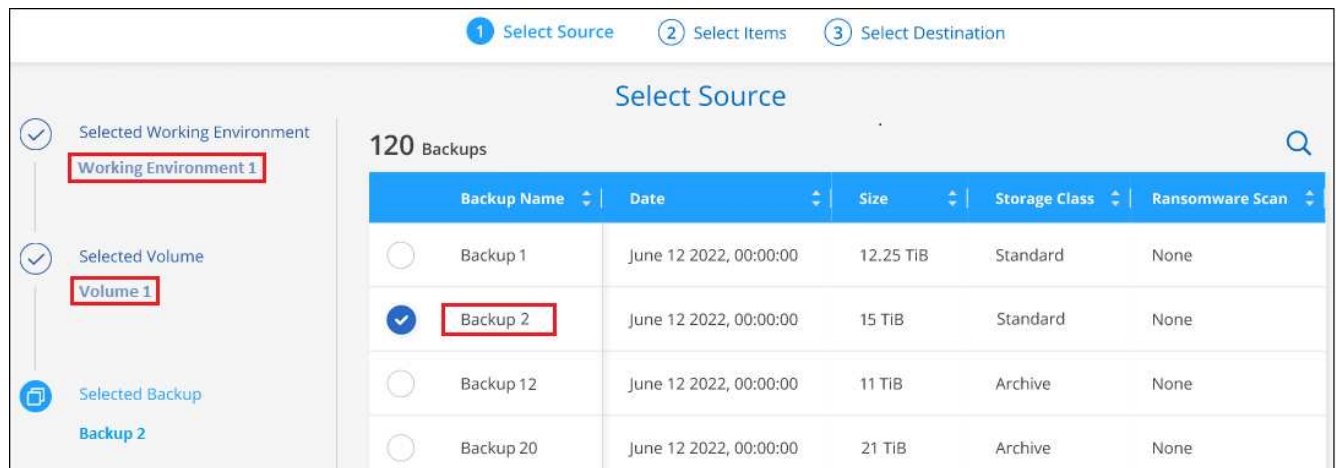


Pasos

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.



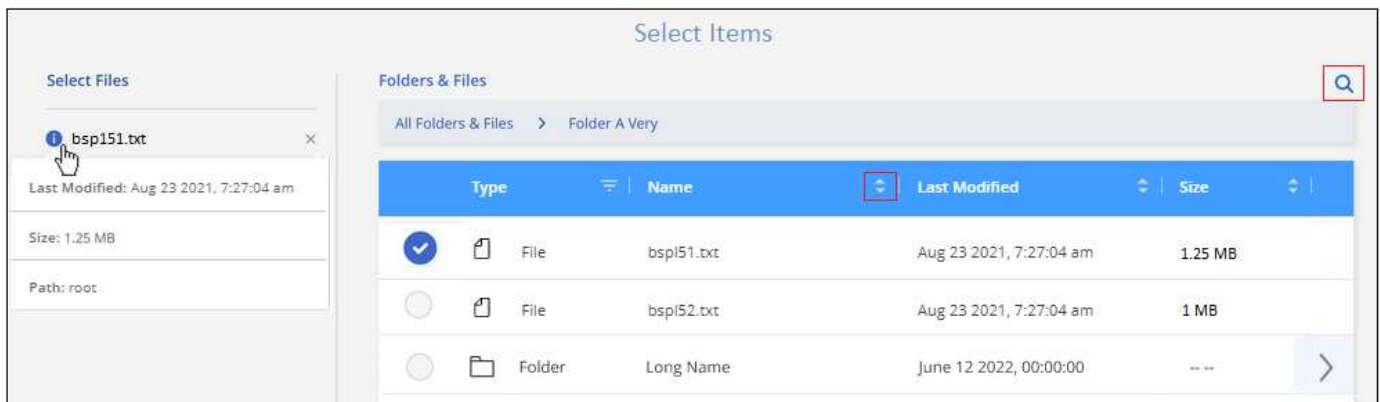
5. Haga clic en **Siguiente** y aparecerá la lista de carpetas y archivos de la copia de seguridad de volumen.

Si va a restaurar carpetas o archivos desde un archivo de copia de seguridad que reside en un nivel de almacenamiento de archivado (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".](#)

+ y si la protección contra ransomware está activa para el archivo de copia de seguridad (si habilitó DataLock y la protección contra ransomware en la política de copia de seguridad), se le solicitará que ejecute un análisis adicional de ransomware en el archivo de copia de seguridad antes de restaurar los datos. Se recomienda que escanee el archivo de backup como ransomware.

+

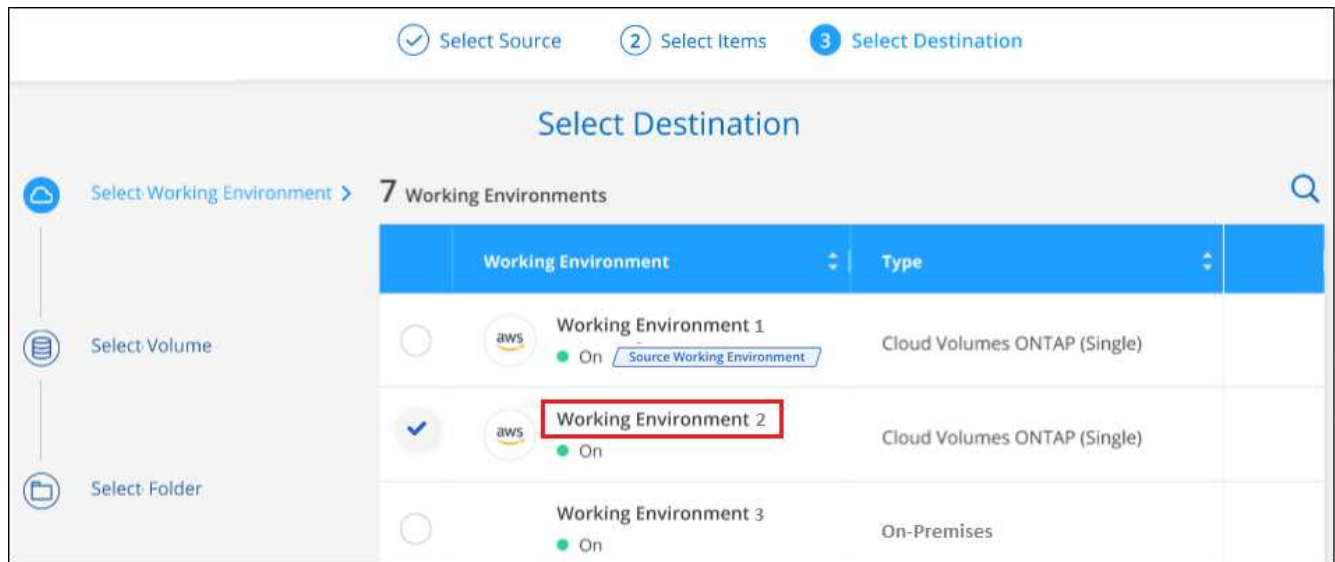


1. En la página **Select ITEMS**, seleccione la carpeta o los archivos que desea restaurar y haga clic en **continuar**. Para ayudarle a encontrar el elemento:

- 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.

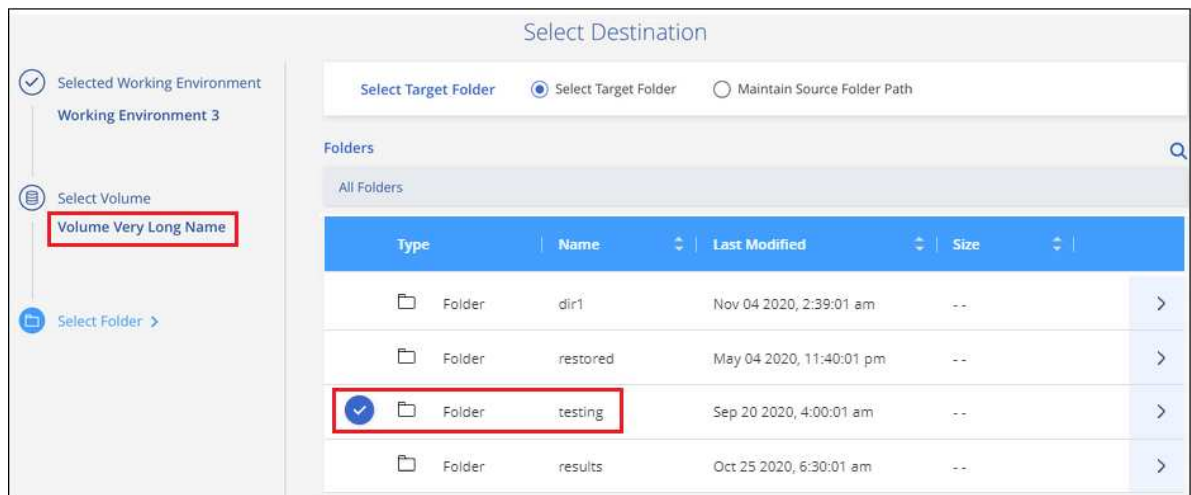
A medida que seleccione los archivos, se agregarán a la parte izquierda de la página para que pueda ver los archivos que ya ha elegido. Si es necesario, puede eliminar un archivo de esta lista haciendo clic en **x** junto al nombre del archivo.

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 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.

Restaurar datos de ONTAP mediante la opción Buscar y restaurar

Es posible restaurar un volumen, una carpeta o archivos desde un archivo de backup de ONTAP mediante Search & Restore. Search & Restore le permite buscar un volumen, una carpeta o un archivo específicos a partir de todos los backups almacenados en el almacenamiento en cloud para un proveedor en concreto y, a continuación, llevar a cabo una restauración. No necesita conocer el nombre exacto del entorno de trabajo o el nombre del volumen; la búsqueda se realiza mediante todos los archivos de backup de volúmenes.

La operación de búsqueda también busca todas las copias Snapshot locales que existen también para los volúmenes ONTAP. Como la restauración de datos de una copia Snapshot local puede ser más rápida y económica que la restauración desde un archivo de respaldo, es posible que desee restaurar datos de la copia Snapshot. Puede restaurar la snapshot como un volumen nuevo "[Desde la página Detalles de volumen del lienzo](#)" (No de Cloud Backup).

Al restaurar un volumen a partir de un archivo de copia de seguridad, Cloud Backup crea un volumen *new* utilizando los datos de la copia de seguridad. Puede restaurar los datos como un volumen en el entorno de trabajo original o a un entorno de trabajo diferente ubicado en la misma cuenta de cloud que el entorno de trabajo de origen. También es posible restaurar volúmenes en un sistema ONTAP en las instalaciones.

Es posible restaurar carpetas o archivos en la ubicación del volumen original, a un volumen diferente del mismo entorno de trabajo 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.

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 y 9.12.1 para Google Archive y StorageGRID.

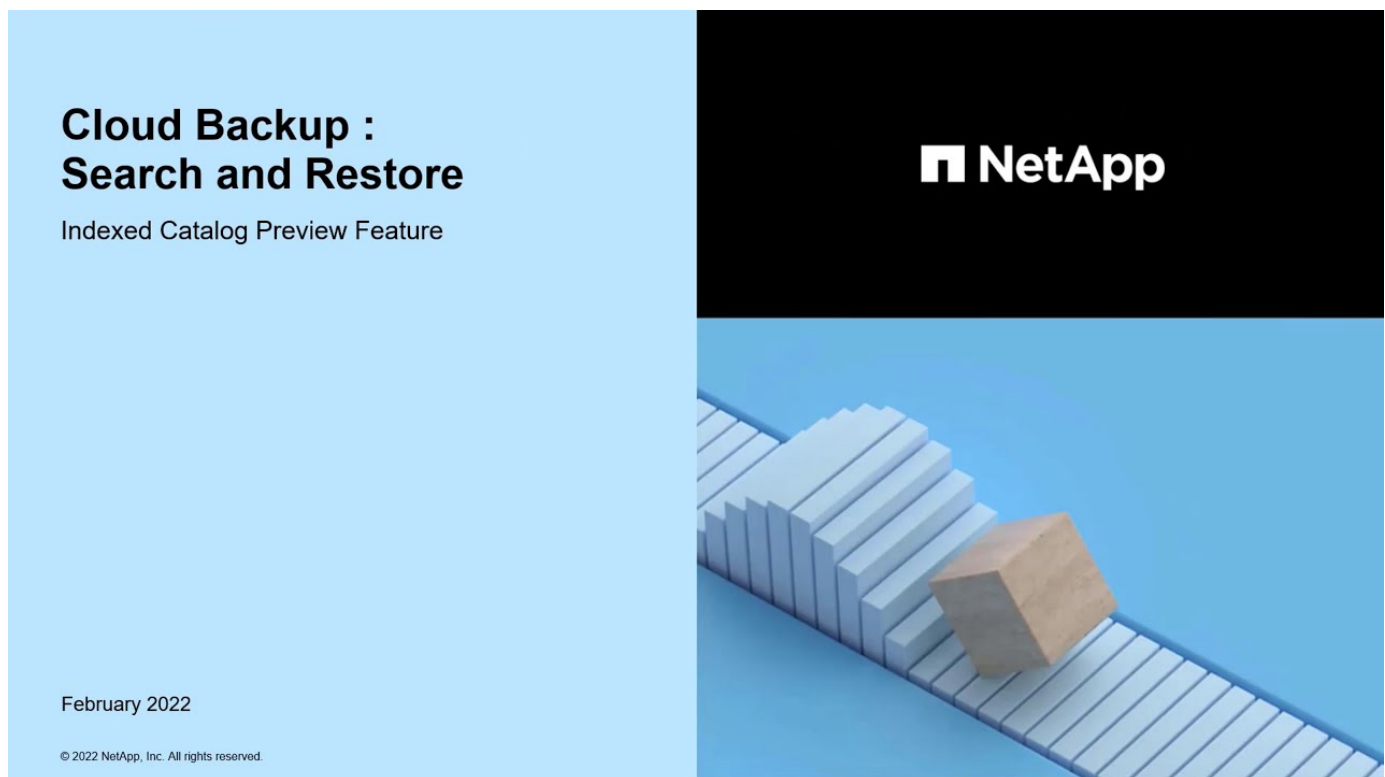
["Obtenga más información sobre la restauración a partir del almacenamiento de archivado de AWS".](#)



- Actualmente, no se admite la restauración a nivel de carpeta si el archivo de backup se configuró con DataLock y Ransomware. En este caso, es posible restaurar todo el volumen desde el archivo de backup y, a continuación, acceder a la carpeta y los archivos necesarios.
- Actualmente, no se admite la restauración a nivel de carpeta si el archivo de backup reside en el almacenamiento de archivado. En este caso, puede restaurar la carpeta desde un nuevo archivo de copia de seguridad que no se haya archivado o restaurar todo el volumen desde la copia de seguridad archivada y, a continuación, acceder a la carpeta y los archivos que necesite.
- La prioridad de restauración alta no es compatible cuando se restauran los datos desde el almacenamiento de archivado de Azure a los sistemas StorageGRID.

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 un volumen, una carpeta o archivos individuales, desde un archivo de backup de ONTAP a los siguientes entornos de trabajo:

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino <code>ifdef::aws[]</code>
Amazon S3	Cloud Volumes ONTAP en la endif del sistema ONTAP en las instalaciones de AWS::aws[] <code>ifdef::Azure[]</code>
Azure Blob	Cloud Volumes ONTAP en Azure on-premises ONTAP system endif::Azure[] <code>ifdef::gcp[]</code>

Ubicación del archivo de copia de seguridad	Entorno de trabajo de destino <code>ifdef::aws[]</code>
Google Cloud Storage	Cloud Volumes ONTAP en Google on-local ONTAP system <code>endif::gcp[]</code>
StorageGRID de NetApp	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 StorageGRID, el conector debe estar desplegado en sus instalaciones, con o sin acceso a Internet

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 entre los ficheros y los directorios entre dos 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 Cloud Backup con un conector configurado anteriormente, tendrá que agregar los permisos Athena y Glue al rol de usuario de BlueXP ahora. Estos son nuevos y se requieren para buscar y restaurar.

- Requisitos de StorageGRID:

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.
- Si está utilizando un conector en un sitio 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.

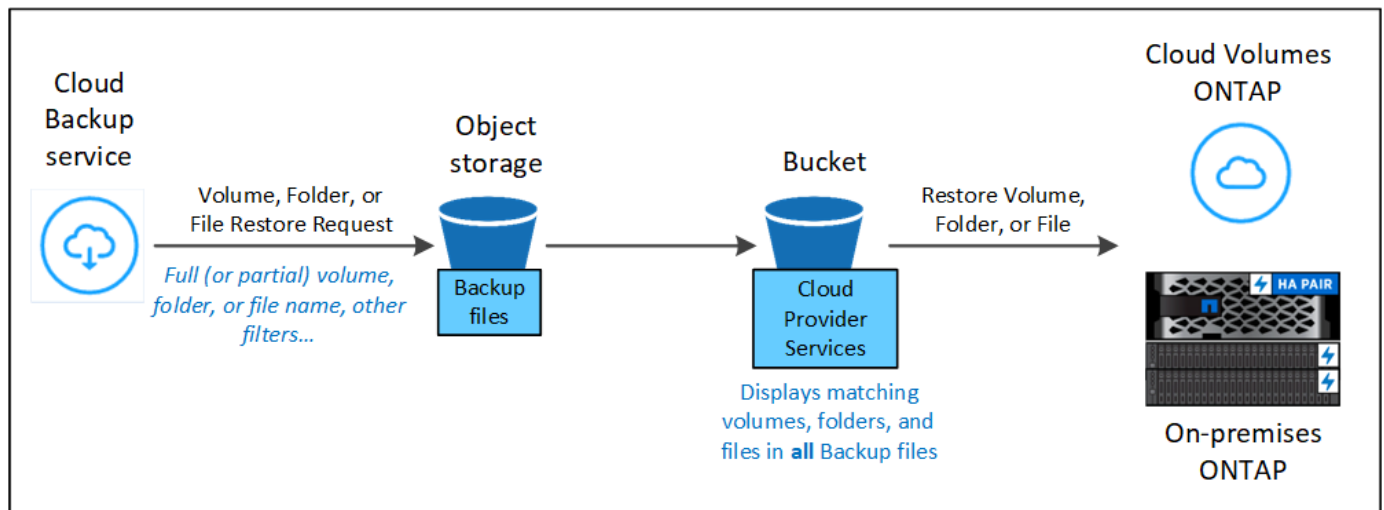
Proceso de búsqueda y restauración

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 parcial o completo, nombre parcial o completo del archivo, intervalo de tamaño, intervalo 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 puede ver, sólo necesita conocer un nombre parcial y las búsquedas de Cloud Backup en todos los archivos de copia de seguridad que coincidan con su búsqueda.

Activación del 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.

Al habilitar esta funcionalidad, Cloud Backup habilita SnapDiff v3 en la SVM para sus 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 backups almacenados en StorageGRID, aprovisiona 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.

Para habilitar la indización para un entorno de trabajo:

- Si no se han indizado los entornos de trabajo, en el Panel de restauración, en *Search & Restore*, haga clic en **Activar indexación para entornos de trabajo** y haga clic en **Activar indexación** para el entorno de trabajo.
- Si ya se ha indizado al menos un entorno de trabajo, en el Panel de restauración, en *Search & Restore*, haga clic en **Configuración de indexación** y haga clic en **Activar indexación** para el entorno de trabajo.

Una vez que se han aprovisionado todos los servicios y se ha activado el catálogo indexado, el entorno de trabajo se muestra como "activo".

The diagram illustrates the process of enabling indexing for working environments. It starts with the 'Search & Restore' panel, which has a button 'Enable Indexing for Working Environments'. This leads to the 'Indexing Settings for Working Environments' panel, which shows a table of working environments. In the table, the 'Enable Indexing' button for 'Working Environment Name # 2' is highlighted.

Indexing Settings for Working Environments		
Enable Indexing for each working environment where you'll want to use Search & Restore.		
	Working Environment Name # 1 Cloud Volumes ONTAP ● On	Active Index Catalog Status
	Working Environment Name # 2 Cloud Volumes ONTAP ● On	Not Active Index Catalog Status Enable Indexing
	Working Environment Name # 3 Cloud Volumes ONTAP ● On	In Progress Index Catalog Status Enable Indexing

En función del tamaño de los volúmenes del entorno de trabajo y del número de archivos de backup en el cloud, el proceso de indexación inicial 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 Search & Restore

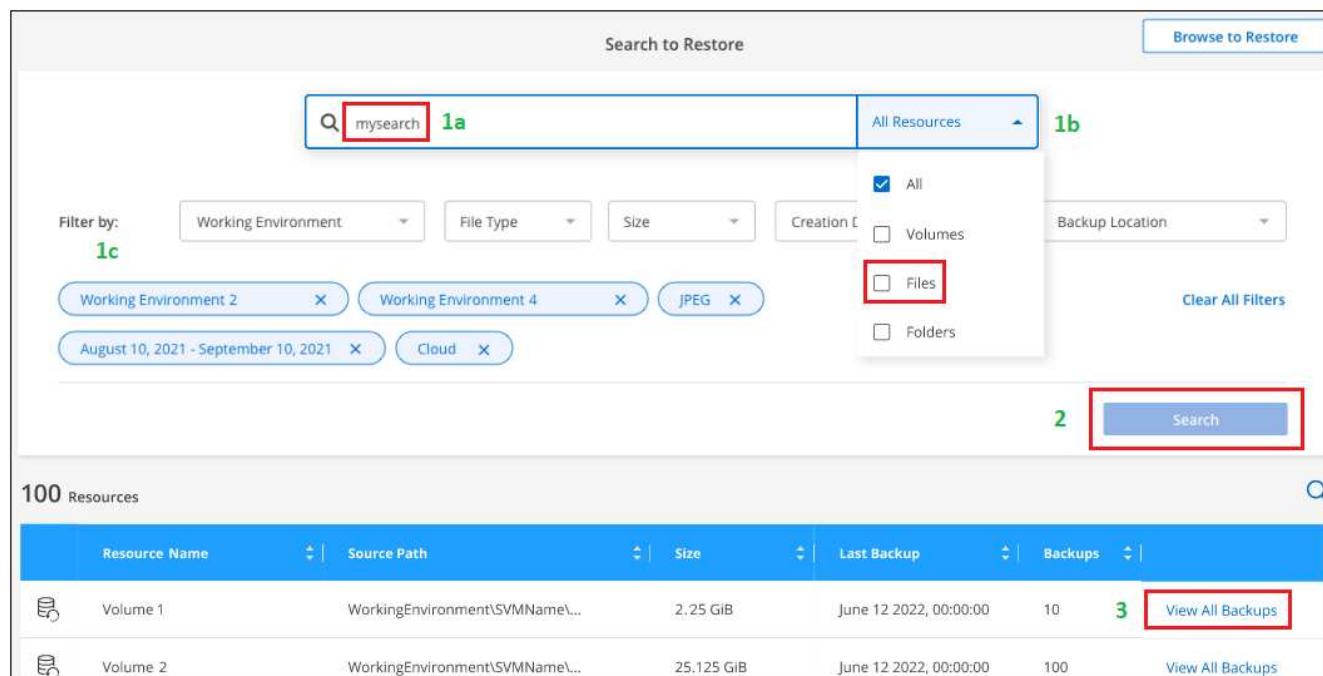
Después de haberlo hecho [Indexación activada para el entorno de trabajo](#), Puede restaurar volúmenes, carpetas y archivos mediante Buscar y restaurar. Esto le permite utilizar una amplia gama de filtros para encontrar el archivo o volumen exacto que desea restaurar desde todos los archivos de copia de seguridad.

Pasos

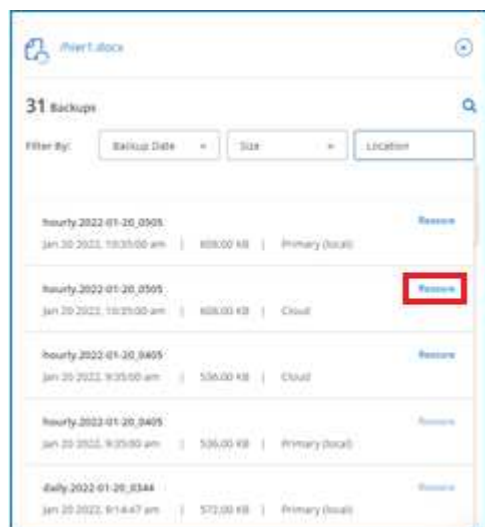
1. En el menú BlueXP, seleccione **Protección > copia de seguridad y recuperación**.
2. Haga clic en la ficha **Restaurar** y aparecerá el Panel de restauración.
3. En la sección *Search & Restore*, haga clic en **Search & Restore**.



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.
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. Haga clic en **Ver todas las copias de seguridad** del recurso que contiene los datos que desea restaurar para mostrar todos los archivos de copia de seguridad que contienen el volumen, carpeta o archivo coincidente.



7. Haga clic en **Restaurar** para el archivo de copia de seguridad que desea utilizar para restaurar el elemento de la nube.

Tenga en cuenta que los resultados también identifican las copias Snapshot de volumen local que contienen el archivo en la búsqueda. El botón **Restaurar** no funciona para instantáneas en este momento, pero si desea restaurar los datos de la copia Snapshot en lugar de hacerlo desde el archivo copia de seguridad, anote el nombre y la ubicación del volumen, abra la página Detalles del volumen en el lienzo, Y utilice la opción **Restaurar desde copia Snapshot**.

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. Al restaurar un volumen de FlexGroup, puede 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 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"](#).

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 © 2023 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.