



Proteger las cargas de trabajo de volumen de ONTAP

NetApp Backup and Recovery

NetApp
March 09, 2026

Tabla de contenidos

Proteger las cargas de trabajo de volumen de ONTAP	1
Proteja sus datos de volumen ONTAP con NetApp Backup and Recovery	1
Funciones	2
Sistemas compatibles para operaciones de copia de seguridad y restauración	3
Volúmenes admitidos	4
Costo	4
Licencias	5
Cómo funciona NetApp Backup and Recovery	6
Consideraciones sobre la política de niveles de FabricPool	10
Planifique su proceso de protección con NetApp Backup and Recovery	10
¿Qué funciones de protección utilizarás?	11
¿Qué arquitectura de respaldo utilizarás?	12
¿Utilizará las políticas predeterminadas para instantáneas, replicaciones y copias de seguridad?	14
¿Dónde residen mis políticas?	15
¿Quieres crear tu propio contenedor de almacenamiento de objetos?	16
¿Qué modo de implementación del agente de consola estás utilizando?	17
Administre políticas de respaldo para volúmenes ONTAP con NetApp Backup and Recovery	18
Ver políticas para un sistema	19
Crear políticas	19
Editar una política	21
Eliminar una política	21
Encuentra más información	22
Opciones de política de copia de seguridad a objeto en NetApp Backup and Recovery	22
Opciones de programación de copias de seguridad	22
Opciones de protección contra DataLock y Ransomware	23
Opciones de almacenamiento de archivos	29
Administrar las opciones de almacenamiento de copia de seguridad en objetos en la configuración avanzada de NetApp Backup and Recovery	31
Ver la configuración de copia de seguridad a nivel de clúster	31
Cambiar el ancho de banda de red disponible para cargar copias de seguridad al almacenamiento de objetos	32
Cambiar si las instantáneas históricas se exportan como archivos de copia de seguridad	32
Cambiar si las instantáneas "anuales" se eliminan del sistema de origen	33
Habilitar o deshabilitar los análisis de ransomware	33
Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3 con NetApp Backup and Recovery	34
Verificar la compatibilidad con su configuración	34
Verificar los requisitos de la licencia	35
Prepare su agente de consola	36
Verificar los requisitos de red de ONTAP para replicar volúmenes	39
Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP	39
Activar copias de seguridad en sus volúmenes ONTAP	40
Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob Storage con	

NetApp Backup and Recovery	44
Verificar la compatibilidad con su configuración	45
Verificar los requisitos de la licencia	46
Prepare su agente de consola	46
Verificar los requisitos de red de ONTAP para replicar volúmenes	49
Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP	49
Activar copias de seguridad en sus volúmenes ONTAP	50
¿Que sigue?	55
Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con NetApp Backup and Recovery	55
Verificar la compatibilidad con su configuración	55
Verificar los requisitos de la licencia	56
Prepare su agente de consola	57
Verificar los requisitos de red de ONTAP para replicar volúmenes	58
Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP	59
Prepare Google Cloud Storage como su destino de respaldo	60
Activar copias de seguridad en sus volúmenes ONTAP	62
¿Que sigue?	66
Realice copias de seguridad de los datos locales de ONTAP en Amazon S3 con NetApp Backup and Recovery	66
Identificar el método de conexión	66
Prepare su agente de consola	68
Verificar los requisitos de la licencia	69
Prepare sus clústeres de ONTAP	69
Prepare Amazon S3 como su destino de respaldo	71
Activar copias de seguridad en sus volúmenes ONTAP	76
Realice una copia de seguridad de los datos locales de ONTAP en Azure Blob Storage con NetApp Backup and Recovery	80
Identificar el método de conexión	80
Prepare su agente de consola	82
Verificar los requisitos de la licencia	85
Prepare sus clústeres de ONTAP	85
Prepare Azure Blob como destino de copia de seguridad	87
Activar copias de seguridad en sus volúmenes ONTAP	87
Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con NetApp Backup and Recovery	92
Identificar el método de conexión	92
Prepare su agente de consola	94
Preparar la red para el agente de consola	95
Verificar los requisitos de la licencia	96
Prepare sus clústeres de ONTAP	96
Prepare Google Cloud Storage como su destino de respaldo	98
Activar copias de seguridad en sus volúmenes ONTAP	100
Realice una copia de seguridad de los datos locales de ONTAP en ONTAP S3 con NetApp Backup and Recovery	104

Identificar el método de conexión	104
Prepare su agente de consola	106
Verificar los requisitos de la licencia	107
Prepare sus clústeres de ONTAP	107
Prepare ONTAP S3 como su destino de respaldo	109
Activar copias de seguridad en sus volúmenes ONTAP	110
Realice copias de seguridad de los datos locales de ONTAP en StorageGRID con NetApp Backup and Recovery	114
Identificar el método de conexión	114
Prepare su agente de consola	115
Verificar los requisitos de la licencia	116
Prepare sus clústeres de ONTAP	116
Prepare StorageGRID como su destino de respaldo	118
Activar copias de seguridad en sus volúmenes ONTAP	121
Migrar volúmenes mediante SnapMirror a Cloud Resync en NetApp Backup and Recovery	125
Cómo funciona la resincronización de SnapMirror to Cloud de NetApp Backup and Recovery	126
Notas de procedimiento	127
Cómo migrar volúmenes usando SnapMirror a Cloud Resync	127
Restaurar datos de configuración de NetApp Backup and Recovery en un sitio oscuro	130
Restaurar datos de NetApp Backup and Recovery a un nuevo agente de consola	130
Administre copias de seguridad de sus sistemas ONTAP con NetApp Backup and Recovery	135
Ver el estado de la copia de seguridad de los volúmenes en sus sistemas	136
Activar la copia de seguridad en volúmenes adicionales en un sistema	136
Cambiar la configuración de copia de seguridad asignada a los volúmenes existentes	137
Cree una copia de seguridad de volumen manual en cualquier momento	138
Ver la lista de copias de seguridad de cada volumen	139
Ejecutar un análisis de ransomware en una copia de seguridad de volumen en el almacenamiento de objetos	139
Administrar la relación de replicación con el volumen de origen	139
Editar una política de copia de seguridad en la nube existente	140
Agregar una nueva política de copia de seguridad en la nube	141
Eliminar copias de seguridad	142
Eliminar relaciones de copia de seguridad de volumen	144
Desactivar NetApp Backup and Recovery para un sistema	145
Anular el registro de NetApp Backup and Recovery para un sistema	145
Restaurar desde copias de seguridad de ONTAP	145
Restaurar datos de ONTAP desde archivos de respaldo con NetApp Backup and Recovery	146
Restaurar desde copias de seguridad de ONTAP mediante la función Buscar y restaurar	147
Restaurar datos de ONTAP mediante Explorar y restaurar	155

Proteger las cargas de trabajo de volumen de ONTAP

Proteja sus datos de volumen ONTAP con NetApp Backup and Recovery

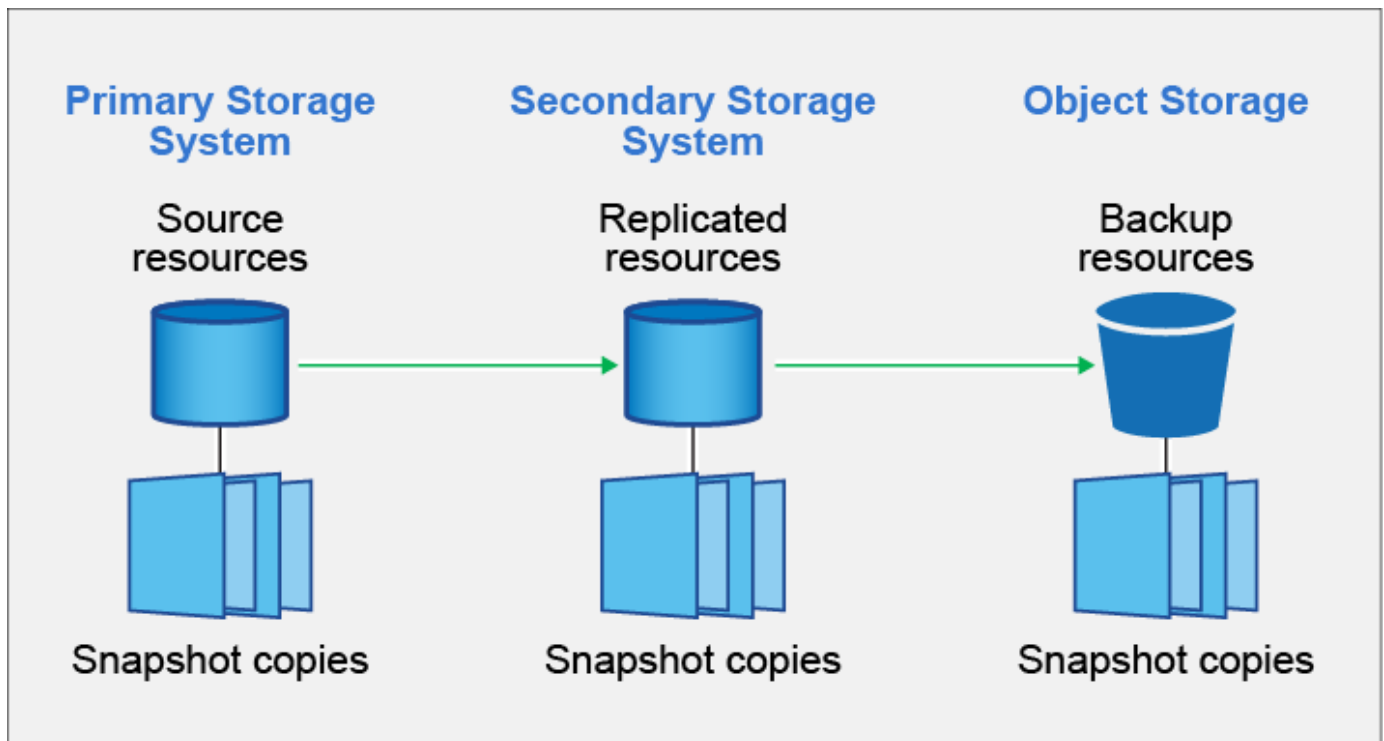
NetApp Backup and Recovery ofrece capacidades de respaldo y restauración para la protección y el archivo a largo plazo de sus datos de volumen ONTAP . Puede implementar una estrategia 3-2-1 donde tenga 3 copias de sus datos de origen en 2 sistemas de almacenamiento diferentes junto con 1 copia en la nube.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

Después de la activación, la copia de seguridad y la recuperación crean copias de seguridad incrementales a nivel de bloque y permanentes que se almacenan en otro clúster de ONTAP y en el almacenamiento de objetos en la nube. Además de tu volumen de origen, tendrás:

- Instantánea del volumen en el sistema de origen
- Volumen replicado en un sistema de almacenamiento diferente
- Copia de seguridad del volumen en el almacenamiento de objetos



NetApp Backup and Recovery aprovecha la tecnología de replicación de datos SnapMirror de NetApp para garantizar que todas las copias de seguridad estén completamente sincronizadas mediante la creación de instantáneas y su transferencia a las ubicaciones de copia de seguridad.

Los beneficios del enfoque 3-2-1 incluyen:

- Múltiples copias de datos protegen contra amenazas cibernéticas internas y externas.
- El uso de diferentes tipos de medios le ayudará a recuperarse si uno de ellos falla.
- Puede restaurar rápidamente desde la copia local y utilizar las copias externas si la copia local se ve comprometida.

Cuando sea necesario, puede restaurar un *volumen* completo, una *carpeta* o uno o más *archivos*, desde cualquiera de las copias de seguridad al mismo sistema o a uno diferente.

Funciones

Características de replicación:

- Replique datos entre sistemas de almacenamiento ONTAP para respaldar la copia de seguridad y la recuperación ante desastres.
- Garantice la confiabilidad de su entorno de DR con alta disponibilidad.
- Cifrado en vuelo ONTAP nativo configurado a través de una clave precompartida (PSK) entre los dos sistemas.
- Los datos copiados son inmutables hasta que los haga escribibles y estén listos para usar.
- La replicación se autocura en caso de falla de transferencia.
- En comparación con ["NetApp Replication"](#) La replicación en NetApp Backup and Recovery incluye las siguientes características:
 - Replica varios volúmenes FlexVol a la vez en un sistema secundario.
 - Restaure un volumen replicado en el sistema de origen o en un sistema diferente mediante la interfaz de usuario.

Ver ["Limitaciones de replicación para volúmenes ONTAP"](#) para obtener una lista de las funciones de replicación que no están disponibles con NetApp Backup and Recovery para volúmenes ONTAP .

Funciones de copia de seguridad en objeto:

- Realice copias de seguridad independientes de sus volúmenes de datos en un almacenamiento de objetos de bajo costo.
- Aplique una única política de respaldo a todos los volúmenes de un clúster o asigne diferentes políticas de respaldo a volúmenes que tengan objetivos de punto de recuperación únicos.
- Cree una política de respaldo que se aplicará a todos los volúmenes futuros creados en el clúster.
- Realice copias de seguridad inmutables de los archivos para que estén bloqueados y protegidos durante el período de retención.
- Escanee los archivos de respaldo para detectar posibles ataques de ransomware y elimine o reemplace las copias de seguridad infectadas automáticamente.
- Guarde los archivos de respaldo más antiguos en un almacenamiento de archivo para ahorrar costos.
- Elimine la relación de respaldo para poder archivar volúmenes de origen innecesarios y conservar las copias de seguridad de volúmenes.
- Realice copias de seguridad de nube a nube y de sistemas locales a nubes públicas o privadas.
- Los datos de respaldo están protegidos con cifrado AES de 256 bits en reposo y conexiones HTTPS TLS 1.2 en tránsito.
- Utilice sus propias claves administradas por el cliente para el cifrado de datos en lugar de utilizar las

claves de cifrado predeterminadas de su proveedor de nube.

- Admite hasta 4000 copias de seguridad de un solo volumen.

Funciones de restauración:

- Restaura datos desde un punto específico en el tiempo a partir de instantáneas locales, volúmenes replicados o volúmenes de copia de seguridad en almacenamiento de objetos.
- Restaurar un volumen, una carpeta o archivos individuales en el sistema de origen o en un sistema diferente.
- Restaurar datos en un sistema que utilice una suscripción/cuenta diferente o que esté en una región diferente.
- Realice una *restauración rápida* de un volumen desde el almacenamiento en la nube a un sistema Cloud Volumes ONTAP o a un sistema local; perfecto para situaciones de recuperación ante desastres donde necesita proporcionar acceso a un volumen lo antes posible.
- Restaure datos a nivel de bloque, colocando los datos directamente en la ubicación que especifique y conservando las ACL originales.
- Examine y busque catálogos de archivos para seleccionar fácilmente carpetas y archivos individuales para restaurar un solo archivo.

Sistemas compatibles para operaciones de copia de seguridad y restauración

NetApp Backup and Recovery es compatible con sistemas ONTAP y proveedores de nube públicos y privados.

Regiones compatibles

NetApp Backup and Recovery es compatible con Cloud Volumes ONTAP en muchas regiones de Amazon Web Services, Microsoft Azure y Google Cloud.

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

Destinos de copia de seguridad admitidos

NetApp Backup and Recovery le permite realizar copias de seguridad de volúmenes ONTAP desde los siguientes sistemas de origen a los siguientes sistemas secundarios y almacenamiento de objetos en proveedores de nube pública y privada. Las instantáneas residen en el sistema de origen.

Sistema fuente	Sistema secundario (Replicación)	Almacén de objetos de destino (copia de seguridad)
Cloud Volumes ONTAP en AWS	Cloud Volumes ONTAP en el sistema ONTAP local de AWS	Amazon S3
Cloud Volumes ONTAP en Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure	Blob de Azure
Cloud Volumes ONTAP en Google	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP	Almacenamiento en la nube de Google
Sistema ONTAP local	Cloud Volumes ONTAP Sistema ONTAP local	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

Destinos de restauración admitidos

Puede restaurar datos de ONTAP desde un archivo de copia de seguridad que reside en un sistema secundario (un volumen replicado) o en almacenamiento de objetos (un archivo de copia de seguridad) en los siguientes sistemas. Las instantáneas residen en el sistema de origen y solo se pueden restaurar en ese mismo sistema.

Ubicación del archivo de respaldo		Sistema de destino
Almacén de objetos (copia de seguridad)	Sistema secundario (replicación)	
Amazon S3	Cloud Volumes ONTAP en el sistema ONTAP local de AWS	Cloud Volumes ONTAP en el sistema ONTAP local de AWS
Blob de Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure
Almacenamiento en la nube de Google	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP
StorageGRID en NetApp	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local
ONTAP S3	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local

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

Volúmenes admitidos

NetApp Backup and Recovery admite los siguientes tipos de volúmenes:

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



NetApp Backup and Recovery no admite copias de seguridad de volúmenes FlexCache .

Ver las secciones sobre "[Limitaciones de copia de seguridad y restauración para volúmenes ONTAP](#)" para requisitos y limitaciones adicionales.

Costo

Hay dos tipos de costos asociados con el uso de NetApp Backup and Recovery con sistemas ONTAP : cargos por recursos y cargos por servicio. Ambos cargos corresponden a la parte de respaldo del objeto del servicio.

No se cobra ninguna tarifa por crear instantáneas o volúmenes replicados, aparte del espacio en disco necesario para almacenar las instantáneas y los volúmenes replicados.

Cargos por recursos

Los cargos por recursos se pagan al proveedor de la nube por la capacidad de almacenamiento de objetos y por escribir y leer archivos de respaldo en la nube.

- Para realizar copias de seguridad en almacenamiento de objetos, usted paga a su proveedor de nube los costos de almacenamiento de objetos.

Dado que NetApp Backup and Recovery preserva las eficiencias de almacenamiento del volumen de origen, usted paga al proveedor de la nube los costos de almacenamiento de objetos por los datos *después* de las eficiencias de ONTAP (para la menor cantidad de datos después de que se hayan aplicado la deduplicación y la compresión).

- Para restaurar datos mediante Búsqueda y restauración, su proveedor de nube proporciona ciertos recursos y existe un costo por TiB asociado con la cantidad de datos escaneados por sus solicitudes de búsqueda. (Estos recursos no son necesarios para Explorar y restaurar).
 - En AWS, "[Amazona Atenea](#)" y "[Pegamento de AWS](#)" Los recursos se implementan en un nuevo bucket S3.
 - En Azure, un "[Área de trabajo de Azure Synapse](#)" y "[Almacenamiento de Azure Data Lake](#)" Se aprovisionan en su cuenta de almacenamiento para almacenar y analizar sus datos.
 - En Google, se implementa un nuevo depósito y el "[Servicios de Google Cloud BigQuery](#)" se aprovisionan a nivel de cuenta/proyecto.
- Si planea restaurar datos de volumen desde un archivo de respaldo que se ha movido al almacenamiento de objetos de archivo, entonces hay una tarifa de recuperación adicional por GiB y una tarifa por solicitud del proveedor de la nube.
- Si planea escanear un archivo de respaldo en busca de ransomware durante el proceso de restauración de datos de volumen (si ha habilitado DataLock y Ransomware Resilience para sus copias de seguridad en la nube), también incurrirá en costos de salida adicionales de su proveedor de la nube.

Cargos por servicio

Los cargos por servicio se pagan a NetApp y cubren tanto el costo de *crear* copias de seguridad en el almacenamiento de objetos como de *restaurar* volúmenes o archivos a partir de esas copias de seguridad. Usted paga solo por los datos que protege en el almacenamiento de objetos, calculados según la capacidad lógica utilizada de origen (antes de las eficiencias de ONTAP) de los volúmenes de ONTAP que se respaldan en el almacenamiento de objetos. Esta capacidad también se conoce como Front-End Terabytes (FETB).

Hay tres formas de pagar el servicio de Backup. La primera opción es suscribirse a través de su proveedor de nube, lo que le permite pagar por mes. La segunda opción es obtener un contrato anual. La tercera opción es comprar licencias directamente de NetApp.

Licencias

NetApp Backup and Recovery está disponible con los siguientes modelos de consumo:

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

Se requiere una licencia de respaldo solo para realizar copias de seguridad y restaurar desde el almacenamiento de objetos. La creación de instantáneas y volúmenes replicados no requiere licencia.

Traiga su propia licencia

BYOL se basa en el plazo (1, 2 o 3 años) y en la capacidad en incrementos de 1 TiB. Usted paga a NetApp para usar el servicio durante un período de tiempo, digamos 1 año, y por una capacidad máxima, digamos 10 TiB.

Recibirá un número de serie que deberá ingresar en la NetApp Console para habilitar el servicio. Cuando se alcance cualquiera de los límites, deberá renovar la licencia. La licencia de Backup BYOL se aplica a todos los sistemas de origen asociados con su organización o cuenta de NetApp Console .

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

Suscripción de pago por uso

NetApp Backup and Recovery ofrece licencias basadas en el consumo en un modelo de pago por uso. Después de suscribirse a través del mercado de su proveedor de nube, usted paga por GiB por los datos respaldados (no hay pago inicial). Su proveedor de nube le facturará a través de su factura mensual.

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

Tenga en cuenta que hay una prueba gratuita de 30 días disponible cuando se registra inicialmente con una suscripción PAYGO.

Contrato anual

Cuando utiliza AWS, hay dos contratos anuales disponibles por períodos de 1, 2 o 3 años:

- Un plan de "Copia de seguridad en la nube" que le permite realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos de ONTAP locales.
- Un plan "CVO Professional" que le permite combinar Cloud Volumes ONTAP y NetApp Backup and Recovery. Esto incluye copias de seguridad ilimitadas para los volúmenes Cloud Volumes ONTAP cargados contra esta licencia (la capacidad de copia de seguridad no se cuenta contra la licencia).

Cuando utiliza Azure, hay dos contratos anuales disponibles por períodos de 1, 2 o 3 años:

- Un plan de "Copia de seguridad en la nube" que le permite realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos de ONTAP locales.
- Un plan "CVO Professional" que le permite combinar Cloud Volumes ONTAP y NetApp Backup and Recovery. Esto incluye copias de seguridad ilimitadas para los volúmenes Cloud Volumes ONTAP cargados contra esta licencia (la capacidad de copia de seguridad no se cuenta contra la licencia).

Cuando usa GCP, puede solicitar una oferta privada de NetApp y luego seleccionar el plan cuando se suscriba desde Google Cloud Marketplace durante la activación de NetApp Backup and Recovery .

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

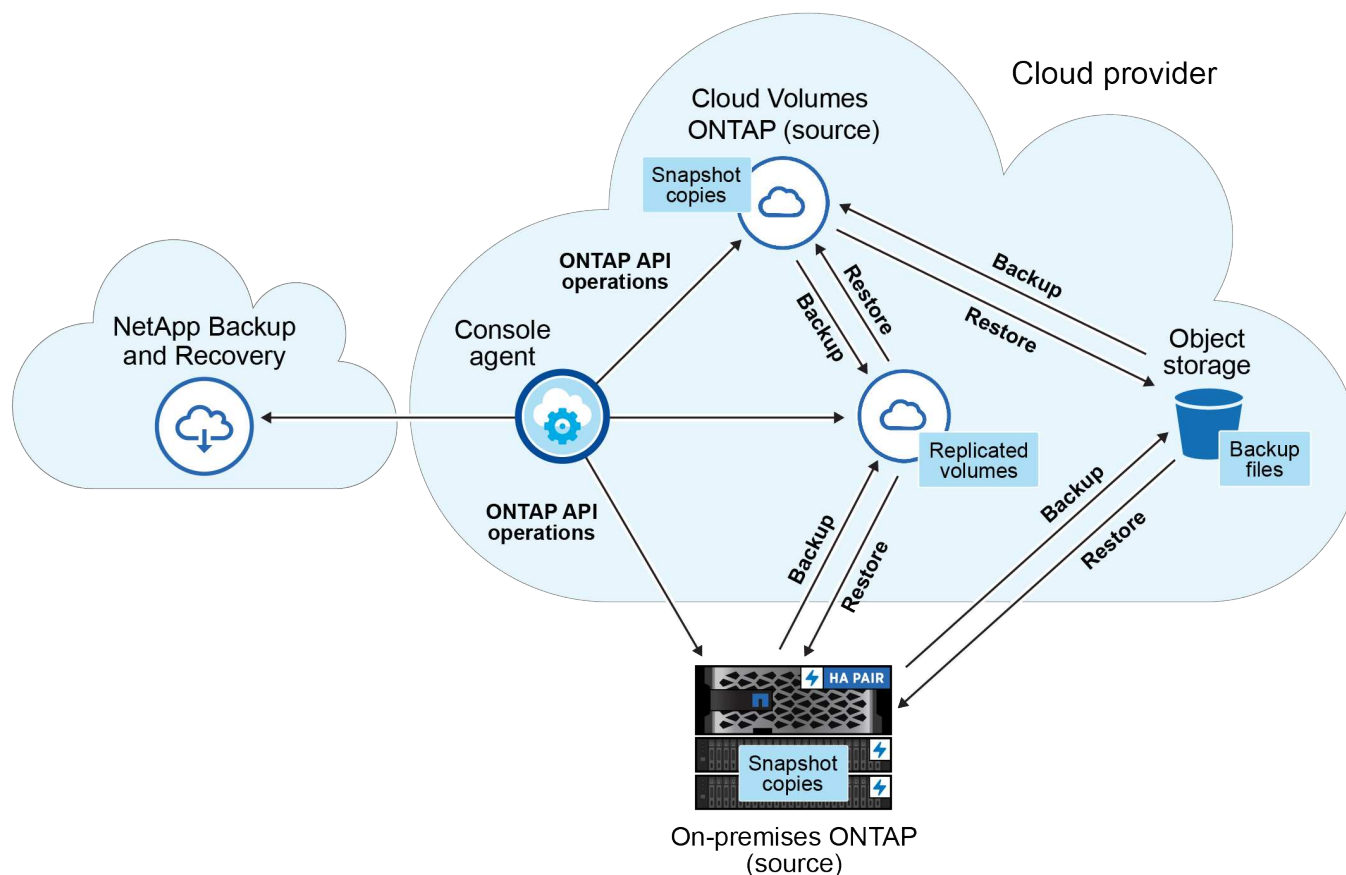
Cómo funciona NetApp Backup and Recovery

Cuando habilita NetApp Backup and Recovery en un sistema Cloud Volumes ONTAP o ONTAP local, el servicio realiza una copia de seguridad completa de sus datos. Después de la copia de seguridad inicial, todas las copias de seguridad adicionales son incrementales, lo que significa que solo se respaldan los bloques modificados y los bloques nuevos. Esto mantiene el tráfico de red al mínimo. La copia de seguridad en el almacenamiento de objetos se basa en ["Tecnología NetApp SnapMirror Cloud"](#) .



Cualquier acción realizada directamente desde el entorno de su proveedor de nube para administrar o cambiar archivos de respaldo en la nube puede dañar los archivos y generar una configuración no compatible.

La siguiente imagen muestra la relación entre cada componente:



Este diagrama muestra volúmenes que se replican en un sistema Cloud Volumes ONTAP, pero los volúmenes también podrían replicarse en un sistema ONTAP local.

Dónde residen las copias de seguridad

Las copias de seguridad residen en diferentes ubicaciones según el tipo de copia de seguridad:

- Las *instantáneas* residen en el volumen de origen del sistema de origen.
- Los *volúmenes replicados* residen en el sistema de almacenamiento secundario: un Cloud Volumes ONTAP o un sistema ONTAP local.
- Las *copias de seguridad* se almacenan en un almacén de objetos que la consola crea en su cuenta en la nube. Hay un almacén de objetos por clúster/sistema, y la consola nombra el almacén de objetos de la siguiente manera: "netapp-backup-clusteruuid". Asegúrese de no eliminar este almacén de objetos.
 - En AWS, la consola permite "[Función de acceso público bloqueado de Amazon S3](#)" en el bucket S3.
 - En Azure, la consola usa un grupo de recursos nuevo o existente con una cuenta de almacenamiento para el contenedor de blobs. La consola "[bloquea el acceso público a sus datos de blobs](#)" por defecto.
 - En GCP, la consola usa un proyecto nuevo o existente con una cuenta de almacenamiento para el depósito de Google Cloud Storage.

- En StorageGRID, la consola utiliza una cuenta de inquilino existente para el depósito S3.
- En ONTAP S3, la consola utiliza una cuenta de usuario existente para el bucket S3.

Si desea cambiar el almacén de objetos de destino para un clúster en el futuro, deberá ["Cancelar el registro de NetApp Backup and Recovery para el sistema"](#) y luego habilite NetApp Backup and Recovery usando la nueva información del proveedor de nube.

Programación de copias de seguridad personalizable y configuraciones de retención

Cuando habilita NetApp Backup and Recovery para un sistema, se realiza un respaldo de todos los volúmenes que seleccione inicialmente utilizando las políticas que seleccione. Puede seleccionar políticas independientes para instantáneas, volúmenes replicados y archivos de copia de seguridad. Si desea asignar diferentes políticas de respaldo a determinados volúmenes que tienen diferentes objetivos de punto de recuperación (RPO), puede crear políticas adicionales para ese clúster y asignar esas políticas a los otros volúmenes después de que se active NetApp Backup and Recovery .

Puede elegir una combinación de copias de seguridad por hora, diarias, semanales, mensuales y anuales de todos los volúmenes. Para realizar copias de seguridad de objetos, también puede seleccionar una de las políticas definidas por el sistema que proporcionan copias de seguridad y retención durante 3 meses, 1 año y 7 años. Las políticas de protección de respaldo que haya creado en el clúster mediante ONTAP System Manager o la CLI de ONTAP también aparecerán como selecciones. Esto incluye políticas creadas utilizando etiquetas SnapMirror personalizadas.



La política de instantáneas aplicada al volumen debe tener una de las etiquetas que está utilizando en su política de replicación y en su política de copia de seguridad de objetos. Si no se encuentran etiquetas coincidentes, no se crearán archivos de respaldo. Por ejemplo, si desea crear volúmenes replicados y archivos de copia de seguridad "semanales", debe utilizar una política de instantáneas que cree instantáneas "semanales".

Una vez que se alcanza el número máximo de copias de seguridad para una categoría o intervalo, se eliminan las copias de seguridad más antiguas para que siempre tenga las copias de seguridad más actuales (y así las copias de seguridad obsoletas no sigan ocupando espacio).



El período de retención de las copias de seguridad de los volúmenes de protección de datos es el mismo que el definido en la relación SnapMirror de origen. Puedes cambiar esto si lo deseas utilizando la API.

Configuración de protección de archivos de respaldo

Si su clúster usa ONTAP 9.11.1 o superior, puede proteger sus copias de seguridad en el almacenamiento de objetos contra ataques de eliminación y ransomware. Cada política de respaldo proporciona una sección para *DataLock y Resiliencia ante ransomware* que se puede aplicar a sus archivos de respaldo durante un período de tiempo específico: el *período de retención*.

- *DataLock* protege sus archivos de respaldo para que no sean modificados ni eliminados.
- La *protección contra ransomware* escanea sus archivos de respaldo para buscar evidencia de un ataque de ransomware cuando se crea un archivo de respaldo y cuando se restauran los datos de un archivo de respaldo.

Los análisis programados de protección contra ransomware están habilitados de forma predeterminada. La configuración predeterminada para la frecuencia de escaneo es de 7 días. El escaneo ocurre solo en la última instantánea. Los análisis programados se pueden desactivar para reducir sus costos. Puede activar o desactivar los análisis programados de ransomware en la última instantánea mediante la opción

correspondiente en la página de Configuración avanzada. Si lo habilita, los análisis se realizan semanalmente de forma predeterminada. Puedes cambiar ese horario a días o semanas o desactivarlo, ahorrando costos.

El período de retención de la copia de seguridad es el mismo que el período de retención del programa de copia de seguridad, más un margen máximo de 31 días. Por ejemplo, las copias de seguridad *semanales* con 5 copias conservadas bloquearán cada archivo de copia de seguridad durante 5 semanas. Las copias de seguridad *mensuales* con 6 copias conservadas bloquearán cada archivo de copia de seguridad durante 6 meses.

Actualmente, el soporte está disponible cuando el destino de su respaldo es Amazon S3, Azure Blob o NetApp StorageGRID. Se agregarán otros destinos de proveedores de almacenamiento en futuras versiones.

Para más detalles consulte esta información:

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



DataLock no se puede habilitar si está organizando copias de seguridad en niveles de almacenamiento de archivo.

Almacenamiento de archivo para archivos de respaldo antiguos

Al utilizar determinados tipos de almacenamiento en la nube, puede mover archivos de respaldo más antiguos a una clase de almacenamiento/nivel de acceso menos costoso después de una cierta cantidad de días. También puede optar por enviar sus archivos de respaldo al almacenamiento de archivo inmediatamente sin escribirlos en el almacenamiento en la nube estándar. Tenga en cuenta que el almacenamiento de archivo no se puede utilizar si ha habilitado DataLock.

- En AWS, las copias de seguridad comienzan en la clase de almacenamiento *Estándar* y pasan a la clase de almacenamiento *Estándar-Acceso infrecuente* después de 30 días.

Si su clúster usa ONTAP 9.10.1 o superior, puede optar por organizar las copias de seguridad más antiguas en almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive* en la interfaz de usuario de NetApp Backup and Recovery después de una cierta cantidad de días para optimizar aún más los costos. ["Obtenga más información sobre el almacenamiento de archivos de AWS"](#).

- En Azure, las copias de seguridad están asociadas con el nivel de acceso *Cool*.

Si su clúster usa ONTAP 9.10.1 o superior, puede optar por organizar en niveles las copias de seguridad más antiguas en el almacenamiento *Azure Archive* en la interfaz de usuario de NetApp Backup and Recovery después de una cierta cantidad de días para optimizar aún más los costos. ["Obtenga más información sobre el almacenamiento de archivo de Azure"](#).

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

Si su clúster usa ONTAP 9.12.1 o superior, puede elegir organizar en niveles las copias de seguridad más antiguas en el almacenamiento *Archivo* en la interfaz de usuario de NetApp Backup and Recovery después de una cierta cantidad de días para optimizar aún más los costos. ["Obtenga más información sobre el almacenamiento de archivos de Google"](#).

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

Si su clúster local usa ONTAP 9.12.1 o superior, y su sistema StorageGRID usa 11.4 o superior, puede archivar archivos de respaldo más antiguos en el almacenamiento de archivo en la nube pública después

de una cierta cantidad de días. El soporte actual es para niveles de almacenamiento de AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. ["Obtenga más información sobre cómo archivar archivos de respaldo desde StorageGRID"](#).

Consulte el enlace:[prev-ontap-policy-object-options.html](#)] para obtener detalles sobre cómo archivar archivos de respaldo más antiguos.

Consideraciones sobre la política de niveles de FabricPool

Hay ciertas cosas que debe tener en cuenta cuando el volumen que está respaldando reside en un agregado de FabricPool y tiene una política de niveles asignada distinta a `none` :

- La primera copia de seguridad de un volumen en niveles de FabricPool requiere leer todos los datos locales y en niveles (desde el almacén de objetos). Una operación de respaldo no "recalienta" los datos fríos almacenados en el almacenamiento de objetos.

Esta operación podría ocasionar un aumento único en el costo de lectura de los datos de su proveedor de nube.

- Las copias de seguridad posteriores son incrementales y no tienen este efecto.
- Si la política de niveles se asigna al volumen cuando se crea inicialmente, no verá este problema.
- Considere el impacto de las copias de seguridad antes de asignarlas a `all` Política de niveles según volúmenes. Debido a que los datos se organizan en niveles de forma inmediata, NetApp Backup and Recovery leerá los datos desde el nivel de la nube en lugar de desde el nivel local. Debido a que las operaciones de respaldo simultáneas comparten el enlace de red con el almacén de objetos en la nube, podría producirse una degradación del rendimiento si los recursos de red se saturan. En este caso, es posible que desee configurar de forma proactiva múltiples interfaces de red (LIF) para disminuir este tipo de saturación de la red.

Planifique su proceso de protección con NetApp Backup and Recovery

NetApp Backup and Recovery le permite crear hasta tres copias de sus volúmenes de origen para proteger sus datos. Hay muchas opciones que puede seleccionar al habilitar la Copia de seguridad y recuperación en sus volúmenes, por lo que debe revisar sus opciones para estar preparado.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Repasaremos las siguientes opciones:

- ¿Qué funciones de protección utilizará: instantáneas, volúmenes replicados o copias de seguridad en la nube?
- ¿Qué arquitectura de respaldo utilizará: una copia de seguridad en cascada o en abanico de sus volúmenes?
- ¿Utilizará las políticas de respaldo predeterminadas o necesitará crear políticas personalizadas?
- ¿Quieres que el servicio cree los depósitos en la nube para ti o quieres crear tus propios contenedores de almacenamiento de objetos antes de comenzar?

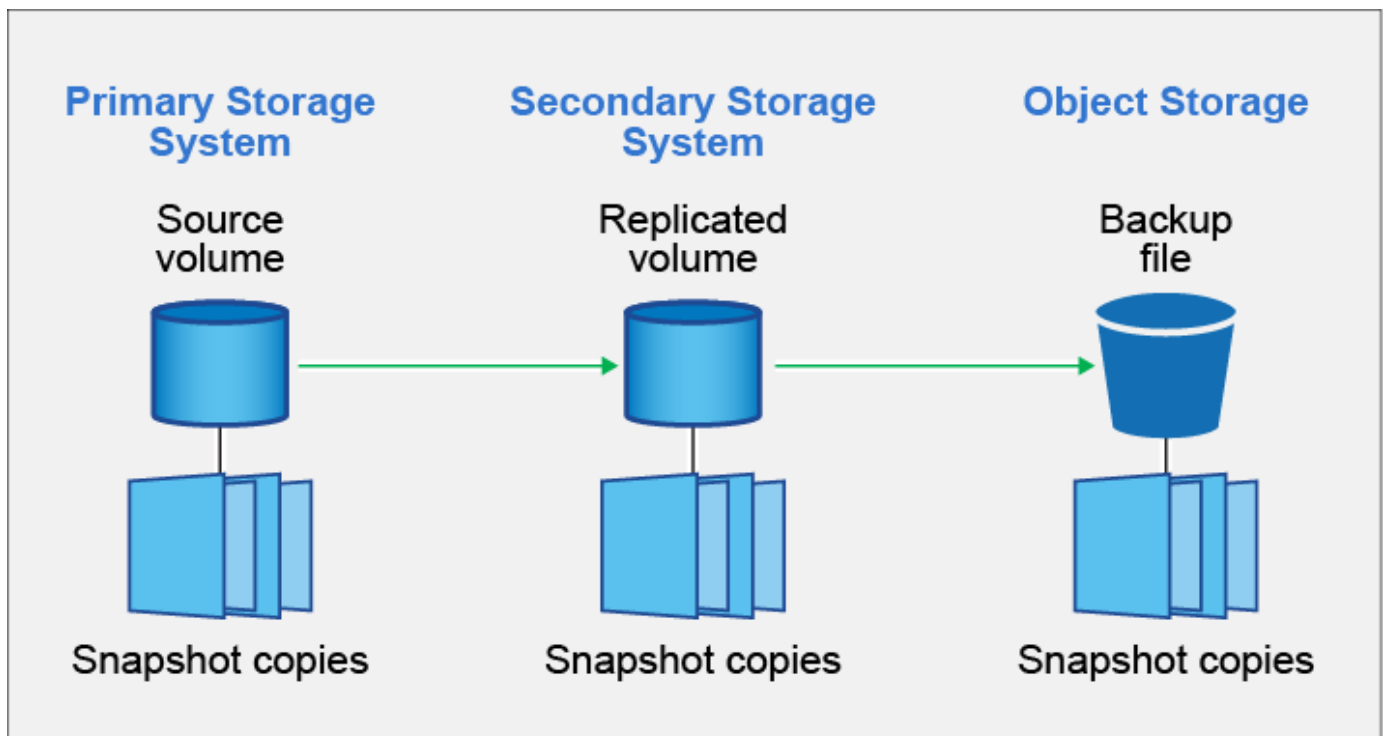
- ¿Qué modo de implementación del agente de consola estás utilizando (modo estándar, restringido o privado)?

¿Qué funciones de protección utilizarás?

Antes de seleccionar las funciones que utilizará, aquí le ofrecemos una breve explicación de lo que hace cada función y qué tipo de protección proporciona.

Tipo de copia de seguridad	Descripción
Snapshot	Crea una imagen de solo lectura y puntual de un volumen dentro del volumen de origen como una instantánea. Puede utilizar la instantánea para recuperar archivos individuales o para restaurar todo el contenido de un volumen.
Replicación	Crea una copia secundaria de sus datos en otro sistema de almacenamiento ONTAP y actualiza continuamente los datos secundarios. Sus datos se mantienen actualizados y permanecen disponibles siempre que los necesite.
Copia de seguridad en la nube	Crea copias de seguridad de sus datos en la nube para su protección y con fines de archivo a largo plazo. Si es necesario, puede restaurar un volumen, una carpeta o archivos individuales desde la copia de seguridad al mismo sistema o a uno diferente.

Las instantáneas son la base de todos los métodos de copia de seguridad y son necesarias para utilizar el servicio de copia de seguridad y recuperación. Una instantánea es una imagen de un volumen, de solo lectura y en un punto determinado del tiempo. La imagen consume un espacio de almacenamiento mínimo y genera una sobrecarga de rendimiento insignificante porque solo registra los cambios realizados en los archivos desde que se tomó la última instantánea. La instantánea que se crea en su volumen se utiliza para mantener sincronizados el volumen replicado y el archivo de copia de seguridad con los cambios realizados en el volumen de origen, como se muestra en la figura.



Puede optar por crear volúmenes replicados en otro sistema de almacenamiento ONTAP y realizar copias de seguridad de los archivos en la nube. O puede elegir simplemente crear volúmenes replicados o archivos de respaldo: es su elección.

Para resumir, estos son los flujos de protección válidos que puede crear para los volúmenes en su sistema ONTAP :

- Volumen de origen → Instantánea → Volumen replicado → Archivo de copia de seguridad
- Volumen de origen → Instantánea → Archivo de copia de seguridad
- Volumen de origen → Instantánea → Volumen replicado



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

Comparación de los diferentes métodos de backup

La siguiente tabla muestra una comparación generalizada de los tres métodos de copia de seguridad. Si bien el espacio de almacenamiento de objetos suele ser menos costoso que su almacenamiento en disco local, si cree que puede restaurar datos de la nube con frecuencia, las tarifas de salida de los proveedores de la nube pueden reducir parte de sus ahorros. Necesitará identificar con qué frecuencia necesita restaurar datos de los archivos de respaldo en la nube.

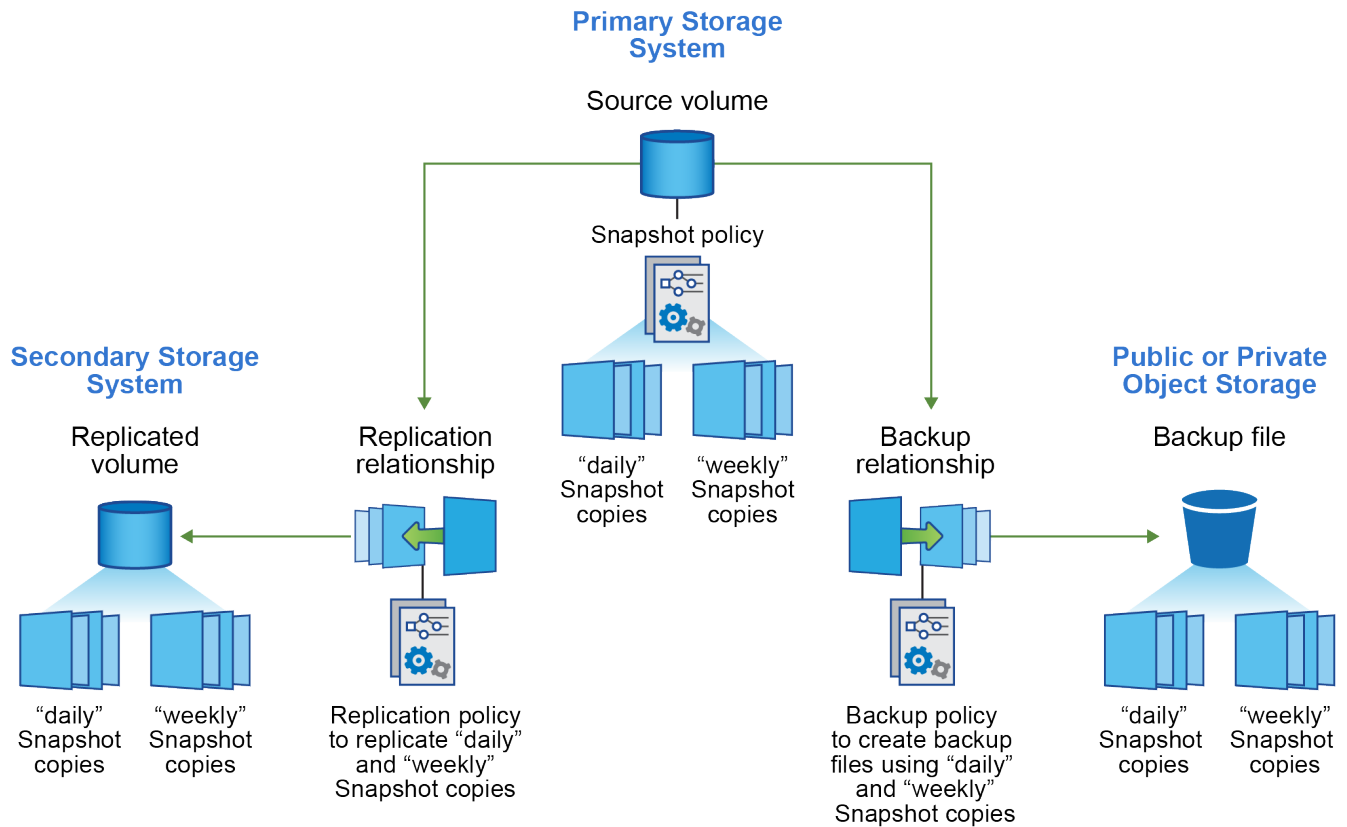
Además de este criterio, el almacenamiento en la nube ofrece opciones de seguridad adicionales si utiliza la función DataLock y Ransomware Resilience, y ahorros de costos adicionales al seleccionar clases de almacenamiento de archivo para archivos de respaldo más antiguos. ["Obtenga más información sobre la protección contra DataLock y Ransomware y la configuración de almacenamiento de archivos."](#)

Tipo de copia de seguridad	Velocidad de respaldo	Costo de respaldo	Restaurar velocidad	Costo de restauración
Instantánea	Alto	Bajo (espacio en disco)	Alto	Bajo
Replicación	Medio	Medio (espacio en disco)	Medio	Medio (red)
Copia de seguridad en la nube	Bajo	Bajo (espacio de objeto)	Bajo	Altas (tarifas del proveedor)

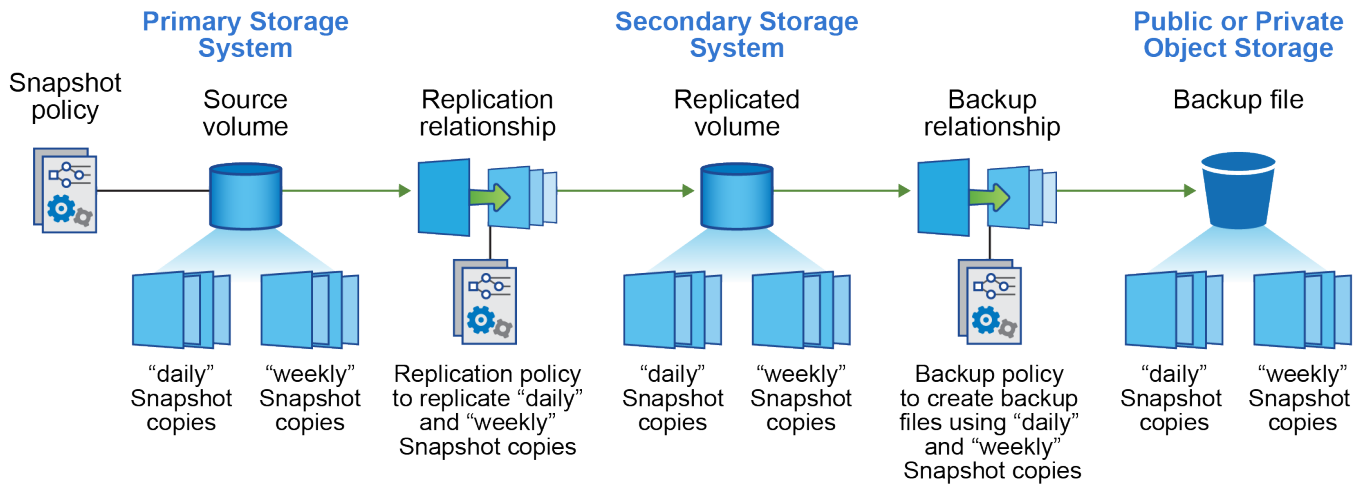
¿Qué arquitectura de respaldo utilizarás?

Al crear volúmenes replicados y archivos de respaldo, puede elegir una arquitectura en cascada o en abanico para realizar el respaldo de sus volúmenes.

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



Una arquitectura **en cascada** transfiere primero la instantánea al sistema de almacenamiento de destino, y luego ese sistema transfiere la copia al objeto de copia de seguridad en la nube.



Comparación de las diferentes opciones de arquitectura

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

Abanico	Cascada
El impacto en el rendimiento del sistema fuente es mínimo debido al envío de instantáneas a dos sistemas distintos.	Menor impacto en el rendimiento del sistema de almacenamiento de origen, ya que la instantánea se envía solo una vez.

Abanico	Cascada
Más fácil de configurar porque todas las políticas, redes y configuraciones de ONTAP se realizan en el sistema de origen	Requiere que también se realicen algunas configuraciones de red y ONTAP desde el sistema secundario.

¿Utilizará las políticas predeterminadas para instantáneas, replicaciones y copias de seguridad?

Puede utilizar las políticas predeterminadas proporcionadas por NetApp para crear sus copias de seguridad o puede crear políticas personalizadas. Cuando utiliza el asistente de activación para habilitar el servicio de respaldo y recuperación para sus volúmenes, puede seleccionar entre las políticas predeterminadas y cualquier otra política que ya exista en el sistema (Cloud Volumes ONTAP o sistema ONTAP local). Si desea utilizar una política diferente a las existentes, puede crear la política antes de comenzar o mientras usa el asistente de activación.

- La política de instantáneas predeterminada crea instantáneas horarias, diarias y semanales, conservando 6 instantáneas horarias, 2 diarias y 2 semanales.
- La política de replicación predeterminada replica instantáneas diarias y semanales, conservando 7 instantáneas diarias y 52 semanales.
- La política de copia de seguridad predeterminada replica instantáneas diarias y semanales, conservando 7 instantáneas diarias y 52 semanales.

Si crea políticas personalizadas para replicación o copia de seguridad, las etiquetas de las políticas (por ejemplo, "diaria" o "semanal") deben coincidir con las etiquetas que existen en sus políticas de instantáneas o volúmenes replicados y no se crearán archivos de copia de seguridad.

Puede crear políticas de instantáneas, replicación y copia de seguridad en almacenamiento de objetos en la interfaz de usuario de NetApp Backup and Recovery . Vea la sección para ["agregar una nueva política de respaldo"](#) Para más detalles.

Además de utilizar NetApp Backup and Recovery para crear políticas personalizadas, puede utilizar System Manager o la interfaz de línea de comandos (CLI) de ONTAP :

- ["Cree una política de instantáneas mediante el Administrador del sistema o la CLI de ONTAP"](#)
- ["Cree una política de replicación mediante el Administrador del sistema o la CLI de ONTAP"](#)

Nota: Al utilizar el Administrador del sistema, seleccione **Asincrónico** como el tipo de política para las políticas de replicación, y seleccione **Asincrónico** y **Copia de seguridad en la nube** para las políticas de copia de seguridad en objetos.

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

Descripción de la política	Comando
Política de instantáneas simples	<code>snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly</code>

Descripción de la política	Comando
Copia de seguridad sencilla en la nube	<pre> snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>
Copia de seguridad en la nube con DataLock y protección contra ransomware	<pre> snapmirror policy create -policy CloudBackupService- Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name> snapmirror policy add-rule -policy CloudBackupService- Enterprise -retention-period 30days </pre>
Copia de seguridad en la nube con clase de almacenamiento de archivo	<pre> snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>
Replicación simple a otro sistema de almacenamiento	<pre> snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name> snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep </pre>



Solo se pueden usar políticas de bóveda para realizar copias de seguridad en las relaciones en la nube.

¿Dónde residen mis políticas?

Las políticas de respaldo residen en diferentes ubicaciones según la arquitectura de respaldo que planea utilizar: en abanico o en cascada. Las políticas de replicación y las políticas de respaldo no están diseñadas de la misma manera porque las replications emparejan dos sistemas de almacenamiento ONTAP y la copia de seguridad en un objeto utiliza un proveedor de almacenamiento como destino.

- Las políticas de instantáneas siempre residen en el sistema de almacenamiento principal.
- Las políticas de replicación siempre residen en el sistema de almacenamiento secundario.
- Las políticas de copia de seguridad a objeto se crean en el sistema donde reside el volumen de origen: este es el clúster principal para configuraciones de distribución y el clúster secundario para configuraciones en cascada.

Estas diferencias se muestran en la tabla.

Arquitectura	Política de instantáneas	Política de replicación	Política de respaldo
Abanico	Primario	Secundario	Primario
Cascada	Primario	Secundario	Secundario

Entonces, si planea crear políticas personalizadas al usar la arquitectura en cascada, necesitará crear las

políticas de replicación y copia de seguridad de objetos en el sistema secundario donde se crearán los volúmenes replicados. Si planea crear políticas personalizadas al usar la arquitectura de distribución, deberá crear las políticas de replicación en el sistema secundario donde se crearán los volúmenes replicados y las políticas de copia de seguridad de objetos en el sistema principal.

Si está utilizando las políticas predeterminadas que existen en todos los sistemas ONTAP , entonces está todo listo.

¿Quieres crear tu propio contenedor de almacenamiento de objetos?

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

Puede crear el contenedor usted mismo en la cuenta del proveedor de objetos si desea utilizar un prefijo determinado o asignar propiedades especiales. Si desea crear su propio contenedor, debe crearlo antes de iniciar el asistente de activación. NetApp Backup and Recovery puede usar cualquier bucket y compartir buckets. El asistente de activación de respaldo descubrirá automáticamente los contenedores aprovisionados para la cuenta y las credenciales seleccionadas para que pueda seleccionar la que desee usar.

Puedes crear el depósito desde la consola o desde tu proveedor de nube.

- ["Crear buckets de Amazon S3 desde la consola"](#)
- ["Crear cuentas de almacenamiento de blobs de Azure desde la consola"](#)
- ["Crear depósitos de Google Cloud Storage desde la consola"](#)

Si planea utilizar un prefijo de depósito diferente a "netapp-backup-xxxxxx", deberá modificar los permisos de S3 para el rol de IAM del agente de consola.

Configuración avanzada del depósito

Si planea mover archivos de respaldo antiguos al almacenamiento de archivo, o si planea habilitar DataLock y la protección contra ransomware para bloquear sus archivos de respaldo y escanearlos en busca de posible ransomware, deberá crear el contenedor con ciertas configuraciones:

- En este momento, el almacenamiento de archivos en sus propios buckets es compatible con el almacenamiento AWS S3 cuando utiliza el software ONTAP 9.10.1 o posterior en sus clústeres. De forma predeterminada, las copias de seguridad comienzan en la clase de almacenamiento *Standard* de S3. Asegúrese de crear el depósito con las reglas de ciclo de vida adecuadas:
 - Mueva los objetos en todo el alcance del bucket a S3 *Standard-IA* después de 30 días.
 - Mueva los objetos con la etiqueta "smc_push_to_archive: true" a *Glacier Flexible Retrieval* (anteriormente S3 Glacier)
- La protección contra ransomware y DataLock es compatible con el almacenamiento de AWS cuando se usa el software ONTAP 9.11.1 o posterior en sus clústeres, y con el almacenamiento de Azure cuando se usa el software ONTAP 9.12.1 o posterior.
 - Para AWS, debe habilitar el bloqueo de objetos en el depósito utilizando un período de retención de 30 días.
 - Para Azure, debe crear la clase de almacenamiento con soporte de inmutabilidad a nivel de versión.

¿Qué modo de implementación del agente de consola estás utilizando?

Si ya está utilizando la consola para administrar su almacenamiento, entonces ya se ha instalado un agente de consola. Si planea utilizar el mismo agente de consola con NetApp Backup and Recovery, entonces está todo listo. Si necesita utilizar un agente de consola diferente, deberá instalarlo antes de comenzar la implementación de copia de seguridad y recuperación.

La NetApp Console ofrece múltiples modos de implementación que le permiten usar la consola de una manera que satisfaga sus requisitos comerciales y de seguridad. El *modo estándar* aprovecha la capa SaaS de la consola para proporcionar una funcionalidad completa, mientras que el *modo restringido* y el *modo privado* están disponibles para organizaciones que tienen restricciones de conectividad.

["Obtenga más información sobre los modos de implementación de la NetApp Console".](#)

Soporte para sitios con conectividad completa a Internet

Cuando se utiliza NetApp Backup and Recovery en un sitio con conectividad completa a Internet (también conocido como *modo estándar* o *modo SaaS*), puede crear volúmenes replicados en cualquier sistema ONTAP local o Cloud Volumes ONTAP administrado por la consola, y puede crear archivos de respaldo en el almacenamiento de objetos en cualquiera de los proveedores de nube compatibles. ["Consulte la lista completa de destinos de copia de seguridad compatibles"](#).

Para obtener una lista de ubicaciones válidas del agente de consola, consulte uno de los siguientes procedimientos de respaldo para el proveedor de nube donde planea crear archivos de respaldo. Existen algunas restricciones donde el agente de consola debe instalarse manualmente en una máquina Linux o implementarse en un proveedor de nube específico.

- ["Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3"](#)
- ["Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob"](#)
- ["Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud"](#)
- ["Realice una copia de seguridad de los datos locales de ONTAP en Amazon S3"](#)
- ["Realice una copia de seguridad de los datos de ONTAP locales en Azure Blob"](#)
- ["Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud"](#)
- ["Realice una copia de seguridad de los datos locales de ONTAP en StorageGRID"](#)
- ["Realizar copias de seguridad de ONTAP local en ONTAP S3"](#)

Soporte para sitios con conectividad a Internet limitada

NetApp Backup and Recovery se puede utilizar en un sitio con conectividad a Internet limitada (también conocido como *modo restringido*) para realizar copias de seguridad de datos de volumen. En este caso, necesitará implementar el agente de consola en la región de nube de destino.

- Puede realizar copias de seguridad de datos de sistemas ONTAP locales o de sistemas Cloud Volumes ONTAP instalados en regiones comerciales de AWS en Amazon S3. ["Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3"](#).
- Puede realizar copias de seguridad de datos de sistemas ONTAP locales o de sistemas Cloud Volumes ONTAP instalados en regiones comerciales de Azure en Azure Blob. ["Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob"](#).

Soporte para sitios sin conexión a Internet

NetApp Backup and Recovery se puede utilizar en un sitio sin conectividad a Internet (también conocidos como sitios *modo privado* o *oscuros*) para realizar copias de seguridad de datos de volumen. En este caso, necesitarás implementar el agente de consola en un host Linux en el mismo sitio.



El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada. Para obtener documentación del modo privado en la interfaz heredada de BlueXP, consulte la ["Documentación en PDF para el modo privado de BlueXP"](#).

- Puede realizar copias de seguridad de datos desde sistemas ONTAP locales a sistemas NetApp StorageGRID locales. ["Realice una copia de seguridad de los datos locales de ONTAP en StorageGRID"](#).
- Puede realizar copias de seguridad de datos desde sistemas ONTAP locales a sistemas ONTAP locales o sistemas Cloud Volumes ONTAP configurados para el almacenamiento de objetos S3. ["Realice una copia de seguridad de los datos locales de ONTAP en ONTAP S3"](#).

Administre políticas de respaldo para volúmenes ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery, utilice las políticas de respaldo predeterminadas proporcionadas por NetApp para crear sus copias de seguridad o cree políticas personalizadas. Las políticas rigen la frecuencia de las copias de seguridad, el momento en que se realizan y la cantidad de archivos de copia de seguridad que se conservan.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery, consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#).

Cuando utiliza el asistente de activación para habilitar el servicio de respaldo y recuperación para sus volúmenes, puede seleccionar entre las políticas predeterminadas y cualquier otra política que ya exista en el sistema (Cloud Volumes ONTAP o sistema ONTAP local). Si desea utilizar una política diferente a las existentes, puede crear la política antes o mientras utiliza el asistente de activación.

Para obtener más información sobre las políticas de respaldo predeterminadas proporcionadas, consulte ["Planifique su viaje de protección"](#).

NetApp Backup and Recovery ofrece tres tipos de copias de seguridad de datos de ONTAP: instantáneas, replicaciones y copias de seguridad en almacenamiento de objetos. Sus políticas residen en diferentes ubicaciones según la arquitectura que utilice y el tipo de copia de seguridad:

Arquitectura	Ubicación de almacenamiento de la política de instantáneas	Ubicación de almacenamiento de la política de replicación	Copia de seguridad en la ubicación de almacenamiento de la política de objetos
Abanico	Primario	Secundario	Primario
Cascada	Primario	Secundario	Secundario

Cree políticas de respaldo utilizando las siguientes herramientas según su entorno, sus preferencias y el tipo

de protección:

- UI de NetApp Console
- Interfaz de usuario del administrador del sistema
- Interfaz de línea de comandos de ONTAP



Al utilizar el Administrador del sistema, seleccione **Asincrónico** como tipo de política para las políticas de replicación, y seleccione **Asincrónico y Hacer copia de seguridad en la nube** para las políticas de copia de seguridad en objetos.

Ver políticas para un sistema

1. En la interfaz de usuario de la consola, seleccione **Volúmenes > Configuración de copia de seguridad**.
2. Desde la página Configuración de copia de seguridad, seleccione el sistema, seleccione **Acciones***  **icono y seleccione *Administración de políticas**.

Aparece la página de administración de políticas. Las políticas de instantáneas se muestran de forma predeterminada.

3. Para ver otras políticas que existen en el sistema, seleccione **Políticas de replicación** o **Políticas de copia de seguridad**. Si las políticas existentes se pueden utilizar para sus planes de respaldo, ya está todo listo. Si necesitas tener una política con características diferentes, puedes crear nuevas políticas desde esta página.

Crear políticas

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

- [Cree una política de instantáneas antes de iniciar la instantánea](#)
- [Cree una política de replicación antes de iniciar la replicación](#)
- [Cree una política de copia de seguridad en almacenamiento de objetos antes de iniciar la copia de seguridad](#)

Cree una política de instantáneas antes de iniciar la instantánea

Parte de su estrategia 3-2-1 implica crear una instantánea del volumen en el sistema de almacenamiento **primario**.

Parte del proceso de creación de políticas implica identificar etiquetas de instantáneas y SnapMirror que indican la programación y la retención. Puedes utilizar etiquetas predefinidas o crear las tuyas propias.

Pasos

1. En la interfaz de usuario de la consola, seleccione **Volúmenes > Configuración de copia de seguridad**.
2. Desde la página Configuración de copia de seguridad, seleccione el sistema, seleccione **Acciones***  **icono y seleccione *Administración de políticas**.

Aparece la página de administración de políticas.

3. En la página Políticas, seleccione **Crear política > Crear política de instantánea**.

4. Especifique el nombre de la política.
5. Seleccione el o los horarios de las instantáneas. Puedes tener un máximo de 5 etiquetas. O bien, crea un horario.
6. Si decide crear un horario:
 - a. Seleccione la frecuencia: horaria, diaria, semanal, mensual o anual.
 - b. Especifique las etiquetas de instantáneas que indican la programación y la retención.
 - c. Introduzca cuándo y con qué frecuencia se tomará la instantánea.
 - d. Retención: Ingrese la cantidad de instantáneas que desea conservar.
7. Seleccione **Crear**.

Ejemplo de política de instantáneas utilizando arquitectura en cascada

Este ejemplo crea una política de instantáneas con dos clústeres:

1. Grupo 1:
 - a. Seleccione el Clúster 1 en la página de políticas.
 - b. Ignore las secciones de políticas de replicación y copia de seguridad en objeto.
 - c. Crear la política de instantáneas.
2. Grupo 2:
 - a. Seleccione el Clúster 2 en la página Política.
 - b. Ignore la sección de política de instantáneas.
 - c. Configurar las políticas de replicación y copia de seguridad de objetos.

Cree una política de replicación antes de iniciar la replicación

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

Pasos

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

Cree una política de copia de seguridad en almacenamiento de objetos antes de iniciar la copia de seguridad

Su estrategia 3-2-1 podría incluir realizar una copia de seguridad de un volumen en un almacenamiento de objetos.

Esta política de almacenamiento reside en diferentes ubicaciones del sistema de almacenamiento según la arquitectura de respaldo:

- Fan-out: Sistema de almacenamiento primario

- Cascada: sistema de almacenamiento secundario

Pasos

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

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

6. (Opcional) Para proteger sus copias de seguridad y evitar que se modifiquen o eliminen, seleccione la opción **Protección contra DataLock y Ransomware**.

Si su clúster utiliza ONTAP 9.11.1 o superior, puede optar por proteger sus copias de seguridad contra eliminación configurando *DataLock* y *Ransomware protection*.

["Obtenga más información sobre las configuraciones de DataLock disponibles"](#).

7. Seleccione **Crear**.

Editar una política

Puede editar una instantánea personalizada, una política de replicación o de respaldo.

Cambiar la política de respaldo afecta a todos los volúmenes que utilizan esa política.

Pasos

1. En la página de administración de políticas, seleccione la política, seleccione **Acciones***  **icono y seleccione *Editar política**.



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

2. En la página Editar política, realice los cambios.
3. Seleccione **Guardar**.

Eliminar una política

Puede eliminar políticas que no estén asociadas a ningún volumen.

Si una política está asociada a un volumen y desea eliminarla, primero debe eliminarla del volumen.

Pasos

1. En la página de administración de políticas, seleccione la política, seleccione **Acciones***  **icono y seleccione *Eliminar política de instantáneas**.
2. Seleccione **Eliminar**.

Encuentra más información

Para obtener instrucciones sobre cómo crear políticas mediante el Administrador del sistema o la CLI de ONTAP , consulte lo siguiente:

["Crear una política de instantáneas mediante el Administrador del sistema"](#) ["Cree una política de instantáneas mediante la CLI de ONTAP"](#) ["Crear una política de replicación mediante el Administrador del sistema"](#) ["Cree una política de replicación mediante la CLI de ONTAP"](#) ["Crear una copia de seguridad de una política de almacenamiento de objetos mediante el Administrador del sistema"](#) ["Cree una copia de seguridad de una política de almacenamiento de objetos mediante la CLI de ONTAP"](#)

Opciones de política de copia de seguridad a objeto en NetApp Backup and Recovery

NetApp Backup and Recovery le permite crear políticas de respaldo con una variedad de configuraciones para sus sistemas ONTAP locales y Cloud Volumes ONTAP .



Estas configuraciones de políticas son relevantes únicamente para el almacenamiento de copias de seguridad en objetos. Ninguna de estas configuraciones afecta sus políticas de instantáneas o replicación.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Opciones de programación de copias de seguridad

NetApp Backup and Recovery le permite crear múltiples políticas de respaldo con programaciones únicas para cada sistema (clúster). Puede asignar diferentes políticas de respaldo a volúmenes que tengan diferentes objetivos de punto de recuperación (RPO).

Cada política de respaldo proporciona una sección para *Etiquetas y retención* que puede aplicar a sus archivos de respaldo. Tenga en cuenta que la política de instantáneas aplicada al volumen debe ser una de las políticas reconocidas por NetApp Backup and Recovery o no se crearán archivos de respaldo.

El programa consta de dos partes: la etiqueta y el valor de retención:

- La **etiqueta** define con qué frecuencia se crea (o actualiza) un archivo de respaldo desde el volumen. Puede seleccionar entre los siguientes tipos de etiquetas:
 - Puede elegir uno o una combinación de períodos de tiempo **por hora, diarios, semanales, mensuales y anuales**.
 - Puede seleccionar una de las políticas definidas por el sistema que brindan respaldo y retención durante 3 meses, 1 año o 7 años.
 - Si ha creado políticas de protección de respaldo personalizadas en el clúster mediante ONTAP System Manager o la CLI de ONTAP , puede seleccionar una de esas políticas.
- El valor **retención** define cuántos archivos de respaldo se conservan para cada etiqueta (período de tiempo). Una vez que se alcanza el número máximo de copias de seguridad en una categoría o intervalo, se eliminan las copias de seguridad más antiguas para que siempre tenga las copias de seguridad más actuales. Esto también le ahorra costos de almacenamiento porque las copias de seguridad obsoletas no continúan ocupando espacio en la nube.

Por ejemplo, supongamos que crea una política de respaldo que crea 7 copias de seguridad **semanales** y 12 **mensuales**:

- Cada semana y cada mes se crea un archivo de respaldo para el volumen
- En la octava semana, se elimina la primera copia de seguridad semanal y se agrega la nueva copia de seguridad semanal de la octava semana (manteniendo un máximo de 7 copias de seguridad semanales)
- En el mes 13, se elimina la primera copia de seguridad mensual y se agrega la nueva copia de seguridad mensual del mes 13 (manteniendo un máximo de 12 copias de seguridad mensuales)

Las copias de seguridad anuales se eliminan automáticamente del sistema de origen después de transferirse al almacenamiento de objetos. Este comportamiento predeterminado se puede cambiar en la página de Configuración avanzada del sistema.

Opciones de protección contra DataLock y Ransomware

NetApp Backup and Recovery brinda soporte para DataLock y protección contra ransomware para sus copias de seguridad de volumen. Estas funciones le permiten bloquear sus archivos de respaldo y escanearlos para detectar posible ransomware en ellos. Esta es una configuración opcional que puede definir en sus políticas de respaldo cuando desee protección adicional para sus copias de seguridad de volumen para un clúster.

Ambas funciones protegen sus archivos de respaldo para que siempre tenga un archivo de respaldo válido para recuperar datos en caso de un intento de ataque de ransomware en sus copias de seguridad. También es útil cumplir con ciertos requisitos reglamentarios donde las copias de seguridad deben bloquearse y conservarse durante un período de tiempo determinado. Cuando la opción DataLock y Ransomware Resilience está habilitada, el depósito de nube que se aprovisiona como parte de la activación de NetApp Backup and Recovery tendrá habilitado el bloqueo y el control de versiones de objetos.

Esta función no proporciona protección para los volúmenes de origen; solo para las copias de seguridad de esos volúmenes de origen. Utilice algunos de los ["Protecciones anti-ransomware proporcionadas por ONTAP"](#) para proteger sus volúmenes de origen.



- Si planea utilizar DataLock y protección contra ransomware, puede habilitarlo al crear su primera política de respaldo y activar NetApp Backup and Recovery para ese clúster. Posteriormente puede habilitar o deshabilitar el escaneo de ransomware mediante la Configuración avanzada de NetApp Backup and Recovery .
- Cuando la consola escanea un archivo de respaldo en busca de ransomware al restaurar datos de volumen, incurrirá en costos de salida adicionales de su proveedor de nube para acceder al contenido del archivo de respaldo.

¿Qué es DataLock?

Con esta función, puede bloquear las instantáneas en la nube replicadas a través de SnapMirror en la nube y también habilitar la función para detectar un ataque de ransomware y recuperar una copia consistente de la instantánea en el almacén de objetos. Esta función es compatible con AWS, Azure, Google Cloud Platform y StorageGRID.

DataLock protege sus archivos de respaldo para que no se modifiquen ni eliminen durante un período de tiempo determinado, también llamado *almacenamiento inmutable*. Esta funcionalidad utiliza tecnología del proveedor de almacenamiento de objetos para el "bloqueo de objetos".

Los proveedores de nube utilizan una fecha de retención hasta (RUD), que se calcula en función del período de retención de instantáneas. El período de retención de instantáneas se calcula en función de la etiqueta y el recuento de retención definidos en la política de respaldo.

El período mínimo de retención de instantáneas es de 30 días. Veamos algunos ejemplos de cómo funciona esto:

- Si elige la etiqueta **Diario** con un recuento de retención de 20, el período de retención de instantáneas será de 20 días, que por defecto es el mínimo de 30 días.
- Si elige la etiqueta **Semanal** con recuento de retención 4, el período de retención de instantáneas es de 28 días, que es el mínimo predeterminado de 30 días.
- Si elige la etiqueta **Mensual** con recuento de retención 3, el período de retención de instantáneas es de 90 días.
- Si elige la etiqueta **Anual** con recuento de retención 1, el período de retención de instantáneas es de 365 días.

¿Qué es la Retención hasta la Fecha (RUD) y cómo se calcula?

La fecha de retención hasta (RUD) se determina en función del período de retención de instantáneas. La fecha de retención hasta se calcula sumando el período de retención de instantáneas y un búfer.

- Buffer es el Buffer para el Tiempo de Transferencia (3 días) + Buffer para Optimización de Costos (28 días), lo que suma un total de 31 días.
- La fecha mínima de retención hasta es de 30 días + 31 días de margen = 61 días.

A continuación se muestran algunos ejemplos:

- Si crea un programa de copia de seguridad mensual con 12 retenciones, sus copias de seguridad se bloquean durante 12 meses (más 31 días) antes de eliminarse (reemplazarse por el próximo archivo de copia de seguridad).
- Si crea una política de respaldo que crea 30 copias de seguridad diarias, 7 semanales y 12 mensuales, hay tres períodos de retención bloqueados:
 - Las copias de seguridad "30 diarias" se conservan durante 61 días (30 días más 31 días de búfer).
 - Las copias de seguridad "7 semanales" se conservan durante 11 semanas (7 semanas más 31 días) y
 - Las copias de seguridad "12 mensuales" se conservan durante 12 meses (más 31 días).
- Si crea una programación de copias de seguridad por hora con 24 retenciones, podría pensar que las copias de seguridad están bloqueadas durante 24 horas. Sin embargo, dado que esto es menos que el mínimo de 30 días, cada copia de seguridad se bloqueará y se conservará durante 61 días (30 días más 31 días de margen).



Las copias de seguridad antiguas se eliminan una vez que expira el período de retención de DataLock, no después del período de retención de la política de copia de seguridad.

La configuración de retención de DataLock anula la configuración de retención de políticas de su política de respaldo. Esto podría afectar sus costos de almacenamiento ya que sus archivos de respaldo se guardarán en el almacén de objetos durante un período de tiempo más largo.

Habilitar DataLock y la protección contra ransomware

Puede habilitar la protección contra DataLock y Ransomware al crear una política. No se puede habilitar, modificar ni deshabilitar esto una vez creada la política.

1. Cuando cree una política, expanda la sección **DataLock y resiliencia ante ransomware**.

2. Elija una de las siguientes opciones:

- **Ninguno:** La protección DataLock y la resiliencia frente a ransomware están deshabilitadas.
- **Desbloqueado:** La protección DataLock y la resiliencia contra ransomware están habilitadas. Los usuarios con permisos específicos pueden sobrescribir o eliminar archivos de respaldo protegidos durante el período de retención.
- **Bloqueado:** la protección DataLock y la resiliencia frente a ransomware están habilitadas. Ningún usuario puede sobrescribir o eliminar archivos de respaldo protegidos durante el período de retención. Esto satisface el pleno cumplimiento normativo.

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

¿Qué es la protección contra ransomware?

La protección contra ransomware escanea sus archivos de respaldo para buscar evidencia de un ataque de ransomware. La detección de ataques de ransomware se realiza mediante una comparación de suma de comprobación. Si se identifica un posible ransomware en un nuevo archivo de respaldo en comparación con el archivo de respaldo anterior, ese archivo de respaldo más nuevo se reemplaza por el archivo de respaldo más reciente que no muestra ningún signo de un ataque de ransomware. (El archivo que fue identificado como víctima de un ataque de ransomware se elimina 1 día después de haber sido reemplazado).

Los escaneos ocurren en estas situaciones:

- Los escaneos de objetos de respaldo en la nube se inician poco después de que se transfieren al almacenamiento de objetos en la nube. El escaneo no se realiza en el archivo de respaldo cuando se escribe por primera vez en el almacenamiento en la nube, sino cuando se escribe el siguiente archivo de respaldo.
- Los análisis de ransomware se pueden iniciar cuando se selecciona la copia de seguridad para el proceso de restauración.
- Los escaneos se pueden realizar a pedido en cualquier momento.

¿Cómo funciona el proceso de recuperación?

Cuando se detecta un ataque de ransomware, el servicio utiliza la API REST del verificador de integridad del agente Active Data Console para iniciar el proceso de recuperación. La versión más antigua de los objetos de datos es la fuente de la verdad y se convierte en la versión actual como parte del proceso de recuperación.

Veamos cómo funciona esto:

- En caso de un ataque de ransomware, el servicio intenta sobrescribir o eliminar el objeto en el depósito.
- Debido a que el almacenamiento en la nube cuenta con control de versiones, crea automáticamente una nueva versión del objeto de respaldo. Si se elimina un objeto con el control de versiones activado, se marca como eliminado pero aún se puede recuperar. Si se sobrescribe un objeto, se almacenan y marcan las versiones anteriores.
- Cuando se inicia un análisis de ransomware, se validan las sumas de comprobación para ambas versiones del objeto y se comparan. Si las sumas de comprobación son inconsistentes, se ha detectado un posible ransomware.
- El proceso de recuperación implica volver a la última copia buena conocida.

Sistemas compatibles y proveedores de almacenamiento de objetos

Puede habilitar la protección contra DataLock y Ransomware en los volúmenes ONTAP de los siguientes sistemas al utilizar almacenamiento de objetos en los siguientes proveedores de nube pública y privada.

Sistema fuente	Destino del archivo de respaldo
Cloud Volumes ONTAP en AWS	Amazon S3
Cloud Volumes ONTAP en Azure	Blob de Azure
Cloud Volumes ONTAP en Google Cloud	Google Cloud
Sistema ONTAP local	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

Requisitos

- Para AWS:
 - Sus clústeres deben ejecutar ONTAP 9.11.1 o superior
 - El agente de consola se puede implementar en la nube o en sus instalaciones.
 - Los siguientes permisos de S3 deben ser parte de la función de IAM que proporciona permisos al agente de la consola. Se encuentran en la sección "backupS3Policy" del recurso "arn:aws:s3:::netapp-backup-*".

Permisos de AWS S3

- s3: Obtener etiquetado de versión de objeto
- s3:Configuración de bloqueo de objeto de depósito
- s3:ObtenerAcl de versión de objeto
- s3:Etiquetado de objetos de colocación
- s3:EliminarObjeto
- s3:EliminarEtiquetadoDeObjeto
- s3:ObtenerRetenciónDeObjeto
- s3: Eliminar etiquetado de versión de objeto
- s3:PonerObjeto
- s3:Obtener objeto
- s3:Configuración de bloqueo de objeto PutBucket
- s3:Obtener configuración del ciclo de vida
- s3: Obtener etiquetado de cubo
- s3:EliminarVersiónDeObjeto
- s3:ListBucketVersions
- s3:ListBucket
- s3:Etiquetado de cubo de colocación
- s3:Obtener etiquetado de objeto
- s3:Versión de PutBucket
- s3:Etiquetado de versión de objeto de colocación
- s3: Obtener versiones de Bucket
- s3:ObtenerAcl del depósito
- s3: Retención de gobernanza de bypass
- s3:PonerRetenciónDeObjeto
- s3: Obtener ubicación del depósito
- s3:ObtenerVersiónDeObjeto

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

- Para Azure:
 - Sus clústeres deben ejecutar ONTAP 9.12.1 o superior
 - El agente de consola se puede implementar en la nube o en sus instalaciones.
- Para Google Cloud:
 - Sus clústeres deben ejecutar ONTAP 9.17.1 o superior
 - El agente de consola se puede implementar en la nube o en sus instalaciones.
- Para StorageGRID:

- Sus clústeres deben ejecutar ONTAP 9.11.1 o superior
- Sus sistemas StorageGRID deben ejecutar 11.6.0.3 o superior
- El agente de consola debe implementarse en sus instalaciones (se puede instalar en un sitio con o sin acceso a Internet)
- Los siguientes permisos de S3 deben ser parte de la función de IAM que proporciona permisos al agente de la consola:

Permisos de StorageGRID S3

- s3: Obtener etiquetado de versión de objeto
- s3:Configuración de bloqueo de objeto de depósito
- s3:ObtenerAcl de versión de objeto
- s3:Etiquetado de objetos de colocación
- s3:EliminarObjeto
- s3:EliminarEtiquetadoDeObjeto
- s3:ObtenerRetenciónDeObjeto
- s3: Eliminar etiquetado de versión de objeto
- s3:PonerObjeto
- s3:Obtener objeto
- s3:Configuración de bloqueo de objeto PutBucket
- s3:Obtener configuración del ciclo de vida
- s3: Obtener etiquetado de cubo
- s3:EliminarVersiónDeObjeto
- s3:ListBucketVersions
- s3:ListBucket
- s3:Etiquetado de cubo de colocación
- s3:Obtener etiquetado de objeto
- s3:Versión de PutBucket
- s3:Etiquetado de versión de objeto de colocación
- s3: Obtener versiones de Bucket
- s3:ObtenerAcl del depósito
- s3:PonerRetenciónDeObjeto
- s3: Obtener ubicación del depósito
- s3:ObtenerVersiónDeObjeto

Restricciones

- La función de protección DataLock y Ransomware no está disponible si ha configurado el almacenamiento de archivo en la política de respaldo.
- La opción DataLock que seleccione al activar NetApp Backup and Recovery debe usarse para todas las

políticas de respaldo de ese clúster.

- No se pueden utilizar varios modos DataLock en un solo clúster.
- Si habilita DataLock, se bloquearán todas las copias de seguridad de volumen. No se pueden combinar copias de seguridad de volúmenes bloqueados y no bloqueados para un solo clúster.
- La protección DataLock y contra ransomware se aplica a nuevas copias de seguridad de volumen que utilicen una política de copia de seguridad con la protección DataLock y contra ransomware habilitada. Posteriormente podrá habilitar o deshabilitar estas funciones mediante la opción Configuración avanzada.
- Los volúmenes FlexGroup pueden usar protección DataLock y Ransomware solo cuando se usa ONTAP 9.13.1 o superior.

Consejos sobre cómo mitigar los costos de DataLock

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

Incluso si los análisis de ransomware programados están deshabilitados, aún puede realizar análisis a pedido cuando sea necesario.

Puedes elegir diferentes niveles de protección:

- **DataLock sin análisis de ransomware:** brinda protección para los datos de respaldo en el almacenamiento de destino que puede estar en modo de gobernanza o de cumplimiento.
 - **Modo de gobernanza:** ofrece flexibilidad a los administradores para sobrescribir o eliminar datos protegidos.
 - **Modo de cumplimiento:** proporciona indelebilidad completa hasta que expire el período de retención. Esto ayuda a cumplir con los requisitos de seguridad de datos más estrictos de entornos altamente regulados. Los datos no se pueden sobrescribir ni modificar durante su ciclo de vida, lo que proporciona el mayor nivel de protección para sus copias de seguridad.



Microsoft Azure utiliza un modo de bloqueo y desbloqueo.

- **DataLock con análisis de ransomware:** proporciona una capa adicional de seguridad para sus datos. Esta función ayuda a detectar cualquier intento de cambiar las copias de seguridad. Si se realiza algún intento, se crea discretamente una nueva versión de los datos. La frecuencia de escaneo se puede cambiar a 1, 2, 3, 4, 5, 6 o 7 días. Si los análisis se configuran cada 7 días, los costos disminuyen significativamente.

Para obtener más consejos para mitigar los costos de DataLock, consulte <https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475>

Además, puede obtener estimaciones del costo asociado con DataLock visitando el sitio web "[Calculadora del coste total de propiedad \(TCO\) de NetApp Backup and Recovery](#)".

Opciones de almacenamiento de archivos

Al usar el almacenamiento en la nube de AWS, Azure o Google, puede mover archivos de respaldo más antiguos a una clase de almacenamiento de archivo o nivel de acceso menos costoso después de una cierta cantidad de días. También puede optar por enviar sus archivos de respaldo al almacenamiento de archivo inmediatamente sin escribirlos en el almacenamiento en la nube estándar. Simplemente ingrese **0** como

"Archivar después de días" para enviar su archivo de respaldo directamente al almacenamiento de archivo. Esto puede ser especialmente útil para usuarios que rara vez necesitan acceder a datos de copias de seguridad en la nube o para usuarios que están reemplazando una solución de copia de seguridad en cinta.

No se puede acceder a los datos en niveles de archivo inmediatamente cuando se los necesita y requerirán un mayor costo de recuperación, por lo que deberá considerar con qué frecuencia necesitará restaurar datos de los archivos de respaldo antes de decidir archivar sus archivos de respaldo.



- Incluso si selecciona "0" para enviar todos los bloques de datos al almacenamiento en la nube de archivo, los bloques de metadatos siempre se escriben en el almacenamiento en la nube estándar.
- No se puede utilizar el almacenamiento de archivo si ha habilitado DataLock.
- No puedes cambiar la política de archivo después de seleccionar **0** días (archivar inmediatamente).

Cada política de respaldo proporciona una sección para *Política de archivo* que puede aplicar a sus archivos de respaldo.

- En AWS, las copias de seguridad comienzan en la clase de almacenamiento *Estándar* y pasan a la clase de almacenamiento *Estándar-Acceso infrecuente* después de 30 días.

Si su clúster usa ONTAP 9.10.1 o superior, puede organizar las copias de seguridad más antiguas en almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive*. ["Obtenga más información sobre el almacenamiento de archivos de AWS"](#).

- Si no selecciona ningún nivel de archivo en su primera política de respaldo al activar NetApp Backup and Recovery, entonces *S3 Glacier* será su única opción de archivo para políticas futuras.
 - Si selecciona *S3 Glacier* en su primera política de respaldo, podrá cambiar al nivel *S3 Glacier Deep Archive* para futuras políticas de respaldo para ese clúster.
 - Si selecciona *S3 Glacier Deep Archive* en su primera política de respaldo, ese nivel será el único nivel de archivo disponible para futuras políticas de respaldo para ese clúster.
- En Azure, las copias de seguridad están asociadas con el nivel de acceso *Cool*.

Si su clúster usa ONTAP 9.10.1 o una versión superior, puede organizar en niveles las copias de seguridad más antiguas en el almacenamiento *Azure Archive*. ["Obtenga más información sobre el almacenamiento de archivo de Azure"](#).

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

Si su clúster local usa ONTAP 9.12.1 o superior, puede optar por organizar en niveles las copias de seguridad más antiguas en el almacenamiento *Archivo* en la interfaz de usuario de NetApp Backup and Recovery después de una cierta cantidad de días para optimizar aún más los costos. ["Obtenga más información sobre el almacenamiento de archivos de Google"](#).

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

Si su clúster local usa ONTAP 9.12.1 o superior, y su sistema StorageGRID usa 11.4 o superior, puede archivar archivos de respaldo más antiguos en un almacenamiento de archivo en la nube pública.

- Para AWS, puede organizar las copias de seguridad en niveles de almacenamiento AWS *S3 Glacier* o *S3 Glacier Deep Archive*. ["Obtenga más información sobre el almacenamiento de archivos de AWS"](#).
- En el caso de Azure, puede organizar en niveles las copias de seguridad más antiguas en el

Administrar las opciones de almacenamiento de copia de seguridad en objetos en la configuración avanzada de NetApp Backup and Recovery

Puede cambiar la configuración de almacenamiento de respaldo a objeto a nivel de clúster que configure al activar NetApp Backup and Recovery para cada sistema ONTAP mediante la página Configuración avanzada. También puede modificar algunas configuraciones que se aplican como configuraciones de copia de seguridad "predeterminadas". Esto incluye cambiar la velocidad de transferencia de las copias de seguridad al almacenamiento de objetos, si las instantáneas históricas se exportan como archivos de copia de seguridad y habilitar o deshabilitar los análisis de ransomware para un sistema.



Estas configuraciones solo están disponibles para el almacenamiento de copias de seguridad en objetos. Ninguna de estas configuraciones afecta su configuración de instantánea o replicación.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Puede cambiar las siguientes opciones en la página Configuración avanzada:

- Cambiar las claves de almacenamiento que le dan a su sistema ONTAP permiso para acceder al almacenamiento de objetos
- Cambiar el espacio IP de ONTAP que está conectado al almacenamiento de objetos
- Cambiar el ancho de banda de red asignado para cargar copias de seguridad al almacenamiento de objetos mediante la opción Velocidad máxima de transferencia
- Cambiar si las instantáneas históricas se exportan como archivos de copia de seguridad y se incluyen en los archivos de copia de seguridad de referencia iniciales para volúmenes futuros.
- Cambiar si las instantáneas "anuales" se eliminan del sistema de origen
- Habilitar o deshabilitar análisis de ransomware para un sistema, incluidos los análisis programados

Ver la configuración de copia de seguridad a nivel de clúster

Puede ver la configuración del sistema a nivel de clúster y la configuración del proveedor para cada sistema.

Pasos

1. Desde el menú Consola, seleccione **Protección > Copia de seguridad y recuperación**.
2. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
3. Desde la página *Configuración de copia de seguridad*, seleccione la **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del sistema** para ver los ajustes del sistema y **Configurar ajustes avanzados > Ajustes del proveedor** para ver los ajustes del proveedor.

La página resultante muestra la configuración actual de ese sistema. Al visualizar la configuración del proveedor, las configuraciones del proveedor que se muestran son relevantes para el depósito que seleccione en la parte superior de la página.

Tenga en cuenta que algunas opciones no están disponibles según la versión de ONTAP en el clúster de origen y el destino del proveedor de nube donde residen las copias de seguridad.

Cambiar el ancho de banda de red disponible para cargar copias de seguridad al almacenamiento de objetos

Cuando activa NetApp Backup and Recovery para un sistema, de manera predeterminada, ONTAP puede usar una cantidad ilimitada de ancho de banda para transferir los datos de respaldo desde los volúmenes del sistema al almacenamiento de objetos. Si nota que el tráfico de respaldo está afectando las cargas de trabajo normales de los usuarios, puede limitar la cantidad de ancho de banda de red que se utiliza durante la transferencia utilizando la opción Velocidad de transferencia máxima en la página Configuración avanzada.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, haga clic en **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del sistema**.
3. En la página Configuración avanzada, expanda la sección **Tasa máxima de transferencia**.
4. Elija un valor entre 1 y 1.000 Mbps como velocidad de transferencia máxima.
5. Seleccione el botón de opción **Limitado** e ingrese el ancho de banda máximo que se puede usar, o seleccione **Ilimitado** para indicar que no hay límite.
6. Seleccione **Aplicar**.

Esta configuración no afecta el ancho de banda asignado a cualquier otra relación de replicación que pueda configurarse para los volúmenes del sistema.

Cambiar si las instantáneas históricas se exportan como archivos de copia de seguridad

Si existen instantáneas locales de volúmenes que coincidan con la etiqueta de programación de copias de seguridad que está utilizando en este sistema (por ejemplo, diaria, semanal, etc.), puede exportar esas instantáneas históricas al almacenamiento de objetos como archivos de copia de seguridad. Esto le permite inicializar tus copias de seguridad en la nube moviendo instantáneas antiguas a la copia de seguridad de referencia.

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

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, haga clic en **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del sistema**.
3. En la página Configuración avanzada, expanda la sección **Exportar copias de instantáneas existentes**.
4. Seleccione si desea exportar las instantáneas existentes.
5. Seleccione **Aplicar**.

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

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

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, haga clic en **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del sistema**.
3. En la página Configuración avanzada, expanda la sección **Eliminación de instantáneas anuales**.
4. Seleccione **Deshabilitado** para conservar las instantáneas anuales en el sistema de origen.
5. Seleccione **Aplicar**.

Habilitar o deshabilitar los análisis de ransomware

Los análisis de protección contra ransomware están habilitados de forma predeterminada. La configuración predeterminada para la frecuencia de escaneo es de 7 días. El escaneo ocurre solo en la última instantánea.

Para obtener detalles sobre las opciones de DataLock y Ransomware Resilience, consulte ["Opciones de DataLock y resiliencia ante ransomware"](#).

Puedes cambiar ese horario a días o semanas o desactivarlo, ahorrando costos.



Habilitar análisis de ransomware generará cargos adicionales según el proveedor de la nube.

Si los análisis de ransomware programados están deshabilitados, aún puede realizar análisis a pedido y el análisis durante una operación de restauración se seguirá realizando.

Referirse a ["Administrar políticas"](#) para obtener detalles sobre la gestión de políticas que implementan la detección de ransomware.

Habilitar o deshabilitar los análisis de ransomware para un sistema

Puede habilitar o deshabilitar los análisis de ransomware para un clúster.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, haga clic en **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del sistema**.
3. En la página resultante, expanda la sección **Análisis de ransomware**.
4. Habilitar o deshabilitar **Análisis de ransomware**.
5. Seleccione **Análisis de ransomware programado**.
6. Opcionalmente, cambie el escaneo predeterminado de cada semana a días o semanas.
7. Establezca la frecuencia en días o semanas con la que se debe ejecutar el análisis.
8. Seleccione **Aplicar**.

Habilitar o deshabilitar los análisis de ransomware para un proveedor

Puede habilitar o deshabilitar los análisis de ransomware a nivel de proveedor utilizando la página de configuración del proveedor. Las configuraciones de la página son relevantes para el depósito que seleccione en la parte superior de la página.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, haga clic en **...** para el sistema y seleccione **Configurar ajustes avanzados > Ajustes del proveedor**.
3. En la parte superior de la página resultante, seleccione el depósito cuya configuración necesita cambiar.
4. Expande la sección **Análisis de ransomware**.
5. Habilitar o deshabilitar **Análisis de ransomware**.
6. Seleccione **Análisis de ransomware programado**.
7. Opcionalmente, cambie el escaneo predeterminado de cada semana a días o semanas.
8. Establezca la frecuencia en días o semanas con la que se debe ejecutar el análisis.
9. Seleccione **Aplicar**.

Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Amazon S3 con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en Amazon S3.



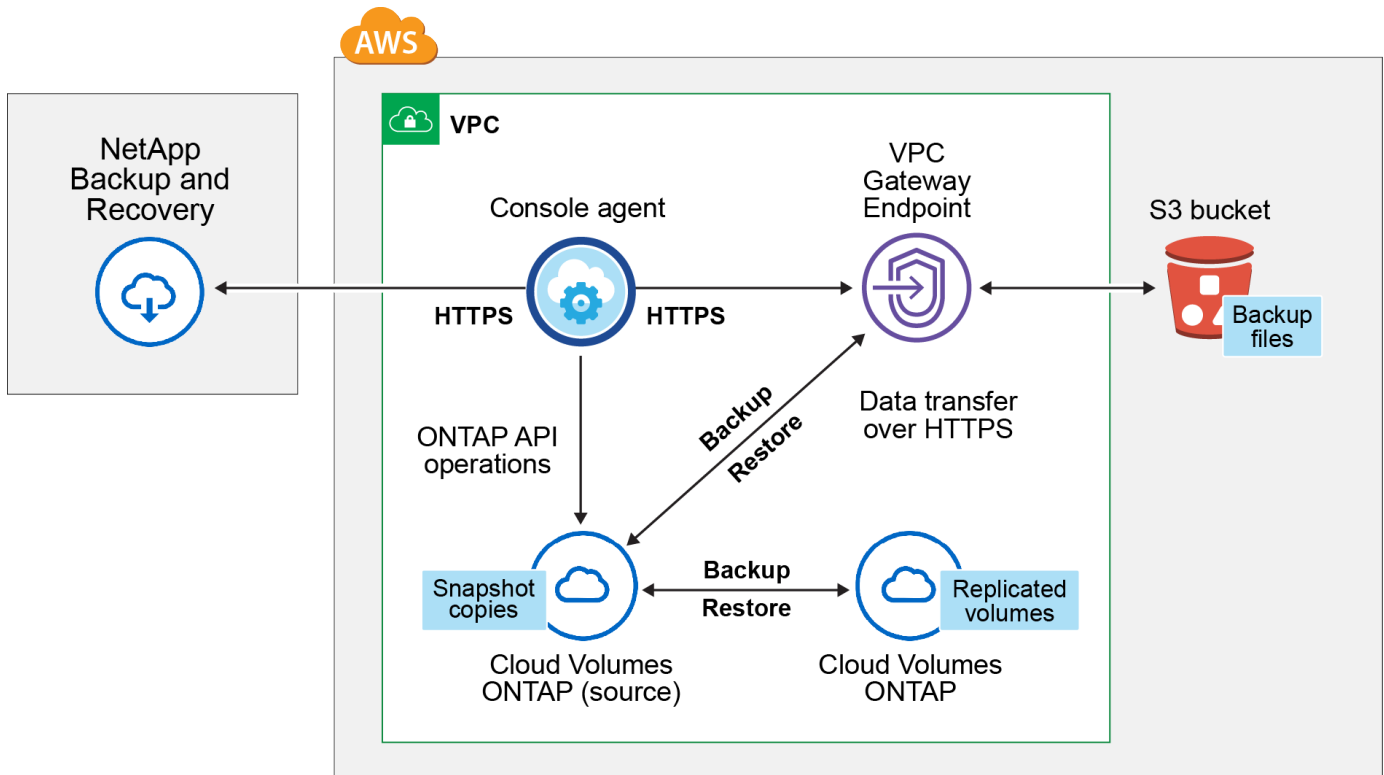
Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

Verificar la compatibilidad con su configuración

Lea los siguientes requisitos para asegurarse de tener una configuración compatible antes de comenzar a realizar copias de seguridad de volúmenes en S3.

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

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



El punto final de la puerta de enlace de VPC ya debe existir en su VPC. ["Obtenga más información sobre los puntos finales de la puerta de enlace"](#) .

Versiones de ONTAP compatibles

Mínimo de ONTAP 9.8; se recomienda ONTAP 9.8P13 y posterior.

Información necesaria para utilizar claves administradas por el cliente para el cifrado de datos

Puede elegir sus propias claves administradas 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 necesitarás tener las claves de cifrado administradas ya configuradas. ["Vea cómo utilizar sus propias llaves"](#) .

Verificar los requisitos de la licencia

Para las licencias PAYGO de NetApp Backup and Recovery , hay una suscripción de consola disponible en AWS Marketplace que permite implementaciones de Cloud Volumes ONTAP y NetApp Backup and Recovery. Necesitas ["Suscríbete a esta suscripción de NetApp Console"](#) antes de habilitar NetApp Backup and Recovery. La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción.

Para obtener un contrato anual que le permita realizar copias de seguridad de los datos de Cloud Volumes ONTAP y de los datos locales de ONTAP , debe suscribirse desde ["Página de AWS Marketplace"](#) y luego ["asociar la suscripción con sus credenciales de AWS"](#) .

Para obtener un contrato anual que le permita combinar Cloud Volumes ONTAP y NetApp Backup and Recovery, debe configurar el contrato anual cuando cree un sistema Cloud Volumes ONTAP . Esta opción no le permite realizar copias de seguridad de datos locales.

Para obtener una licencia BYOL de NetApp Backup and Recovery , necesita el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#). Debe utilizar una licencia BYOL cuando el agente de consola y el sistema Cloud Volumes ONTAP se implementan en un sitio oscuro.

Y necesitas tener una cuenta de AWS para el espacio de almacenamiento donde se ubicarán tus copias de seguridad.

Prepare su agente de consola

El agente de consola debe instalarse en una región de AWS con acceso a Internet completo o limitado (modo "estándar" o "restringido"). ["Consulte los modos de implementación de la NetApp Console para obtener más detalles"](#) .

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Implementar un agente de consola en AWS en modo estándar \(acceso completo a Internet\)"](#)
- ["Instalar el agente de consola en modo restringido \(acceso saliente limitado\)"](#)

Verificar o agregar permisos al agente de la consola

El rol de IAM que proporciona permisos a la consola debe incluir permisos S3 de la última versión. ["Política de consola"](#) . Si la política no contiene todos estos permisos, consulte la ["Documentación de AWS: Edición de políticas de IAM"](#) .

A continuación se muestran los permisos específicos de la política:


```

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

```

```

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

```



Al crear copias de seguridad en las regiones de AWS China, debe cambiar el nombre del recurso de AWS "arn" en todas las secciones *Resource* en las políticas de IAM de "aws" a "aws-cn"; por ejemplo `arn:aws-cn:s3:::netapp-backup-*` .

Permisos necesarios de AWS Cloud Volumes ONTAP

Cuando su sistema Cloud Volumes ONTAP ejecuta el software ONTAP 9.12.1 o posterior, la función IAM que proporciona permisos a ese sistema debe incluir un nuevo conjunto de permisos S3 específicamente para NetApp Backup and Recovery de la última versión. ["Política de Cloud Volumes ONTAP"](#) .

Si creó el sistema Cloud Volumes ONTAP con la versión de consola 3.9.23 o superior, estos permisos ya deberían ser parte de la función de IAM. De lo contrario, necesitará agregar los permisos faltantes.

Regiones de AWS compatibles

NetApp Backup and Recovery es compatible con todas las regiones de AWS, incluidas las regiones de AWS GovCloud.

Configuración necesaria para crear copias de seguridad en una cuenta de AWS diferente

De forma predeterminada, las copias de seguridad se crean utilizando la misma cuenta que la utilizada para su sistema Cloud Volumes ONTAP . Si desea utilizar una cuenta de AWS diferente para sus copias de seguridad, debe:

- Verifique que los permisos "s3:PutBucketPolicy" y "s3:PutBucketOwnershipControls" sean parte del rol de IAM que proporciona permisos al agente de la consola.
- Agregue las credenciales de la cuenta de AWS de destino en la consola. ["Vea cómo hacer esto"](#) .
- Agregue los siguientes permisos en las credenciales de usuario en la segunda cuenta:

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

Crea tus propios cubos

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

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

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#).

Requisitos de red de Cloud Volumes ONTAP

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

Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP

Habilitar NetApp Backup and Recovery es fácil. Los pasos varían levemente dependiendo de si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

Habilitar NetApp Backup and Recovery en un nuevo sistema

NetApp Backup and Recovery está habilitado de forma predeterminada en el asistente del sistema. Asegúrese

de mantener la opción habilitada.

Ver "[Lanzamiento de Cloud Volumes ONTAP en AWS](#)" para conocer los requisitos y detalles para crear su sistema Cloud Volumes ONTAP .

Pasos

1. Desde la página **Sistemas** de la consola, seleccione **Agregar sistema**, elija el proveedor de nube y seleccione **Agregar nuevo**. Seleccione **Crear Cloud Volumes ONTAP**.
2. Seleccione **Amazon Web Services** como proveedor de nube y luego elija un solo nodo o un sistema HA.
3. Complete la página de Detalles y Credenciales.
4. En la página Servicios, deje el servicio habilitado y seleccione **Continuar**.
5. Complete las páginas del asistente para implementar el sistema.

Resultado

NetApp Backup and Recovery está habilitado en el sistema. Después de haber creado volúmenes en estos sistemas Cloud Volumes ONTAP , inicie NetApp Backup and Recovery y "[Activar la copia de seguridad en cada volumen que desee proteger](#)" .

Habilitar NetApp Backup and Recovery en un sistema existente

Habilite NetApp Backup and Recovery en un sistema existente en cualquier momento directamente desde la consola.

Pasos

1. Desde la página **Sistemas** de la Consola, seleccione el clúster y seleccione **Habilitar** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Amazon S3 para sus copias de seguridad existe como un clúster en la página **Sistemas**, puede arrastrar el clúster al sistema Amazon S3 para iniciar el asistente de configuración.

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:
 - Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de AWS para sus copias de seguridad existe como un sistema en la página **Sistemas** de la consola, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de AWS.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones** ➤ opción de icono y seleccione **Activar protección 3-2-1** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo "[Activar la copia de seguridad para volúmenes adicionales en el sistema](#)" (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

Si los volúmenes que elige ya tienen políticas de instantáneas o replicación aplicadas, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos

- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos. Al seleccionar depósitos existentes o configurar depósitos nuevos, puede realizar copias de seguridad de volúmenes en hasta seis depósitos por clúster.
2. **Arquitectura:** Si eligió replicación y copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** la información fluye desde el sistema de almacenamiento primario al secundario, y desde el secundario al almacenamiento de objetos.
 - **Distribución en abanico:** la información fluye desde el sistema de almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- a. Introduzca el nombre de la política.
- b. Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- c. Seleccione **Crear**.

4. **Replicación:** Establezca las siguientes opciones:
 - **Objetivo de replicación:** seleccione el sistema de destino y la máquina virtual de almacenamiento. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.
 - **Política de replicación:** elija una política de replicación existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- i. Introduzca el nombre de la póliza.
- ii. Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- iii. Seleccione **Crear**.

5. **Copia de seguridad:** Establezca las siguientes opciones:

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

Ingrese la cuenta de AWS utilizada para almacenar las copias de seguridad. Esta puede ser una cuenta diferente a aquella donde reside el sistema Cloud Volumes ONTAP .

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

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

Cree un nuevo depósito o seleccione uno existente.

- **Cifrado:** Si creó un nuevo depósito, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Elija si utilizará las claves de cifrado de AWS predeterminadas o elegirá sus propias claves administradas por el cliente desde su cuenta de AWS para administrar el cifrado de sus datos. ("[Vea cómo utilizar sus propias claves de cifrado](#)").

Si elige utilizar sus propias claves administradas por el cliente, ingrese al almacén de claves y a la información de la clave.



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

- **Redes:** configure las opciones de red para este proveedor.
- **Política de respaldo:** seleccione una política de almacenamiento de respaldo a objetos existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- i. Introduzca el nombre de la póliza.
 - ii. Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
 - iii. Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte "[Configuración de la política de copia de seguridad en objeto](#)" .
 - iv. Seleccione **Crear**.
- **Exportar instantánea existente:** si hay instantáneas locales para volúmenes en este sistema que coinciden con la etiqueta de programación de respaldo que acaba de seleccionar para este sistema

(por ejemplo, diaria, semanal, etc.), se muestra este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Reparar automáticamente las etiquetas no coincidentes en la instantánea local, la replicación y la copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de instantáneas, replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las instantáneas.

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

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta ingresada, y los archivos de respaldo se almacenan allí.

Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página de seguimiento de trabajos"](#).

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob Storage con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en

el almacenamiento de blobs de Azure.



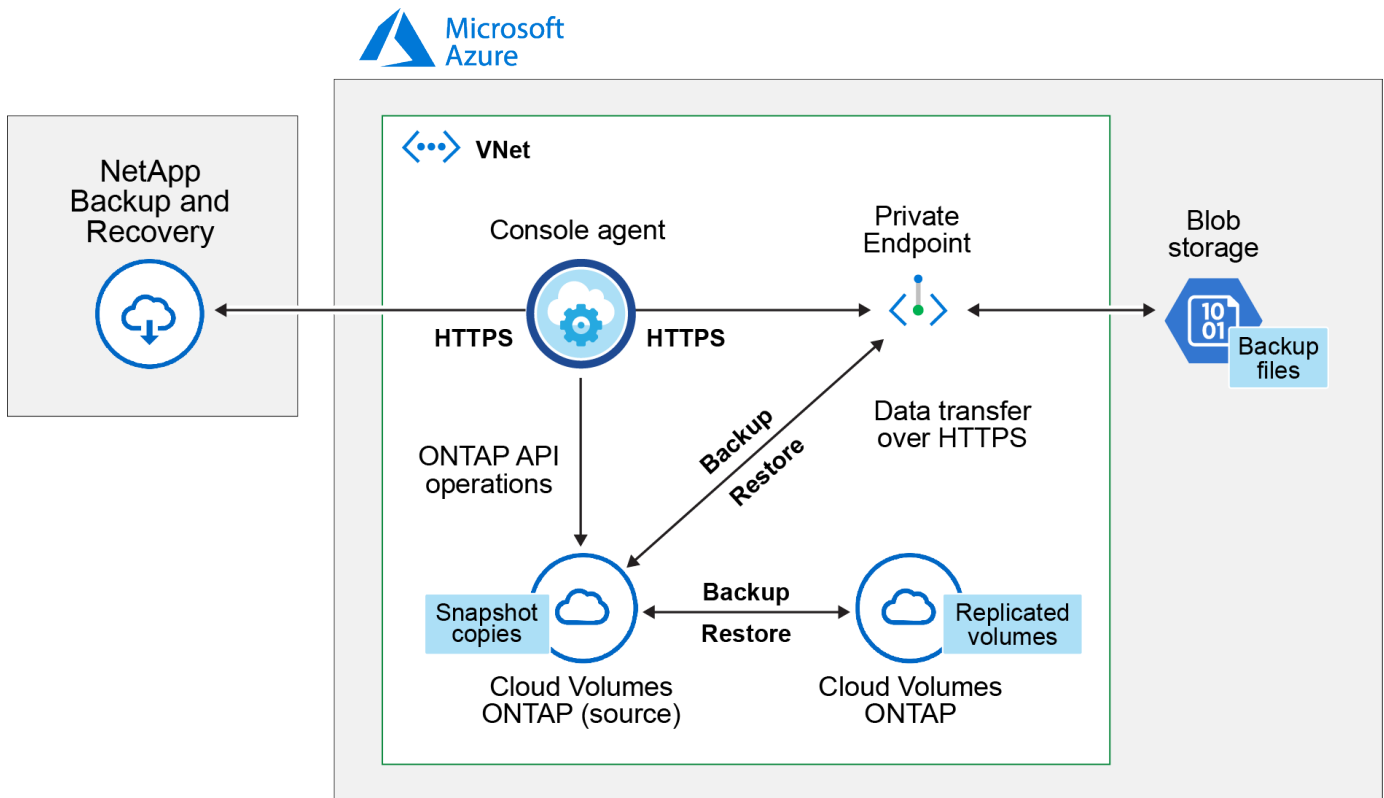
Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Verificar la compatibilidad con su configuración

Lea los siguientes requisitos para asegurarse de tener una configuración compatible antes de comenzar a realizar copias de seguridad de volúmenes en Azure Blob Storage.

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

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



Versiones de ONTAP compatibles

Mínimo de ONTAP 9.8; se recomienda ONTAP 9.8P13 y posterior.

Regiones de Azure compatibles

NetApp Backup and Recovery es compatible con todas las regiones de Azure, incluidas las regiones de Azure Government.

De forma predeterminada, NetApp Backup and Recovery aprovisiona el contenedor Blob con redundancia local (LRS) para optimizar costos. Puede cambiar esta configuración a Redundancia de zona (ZRS) después de que se haya activado NetApp Backup and Recovery si desea asegurarse de que sus datos se repliquen entre diferentes zonas. Consulte las instrucciones de Microsoft para ["Cambiar la forma en que se replica su cuenta de almacenamiento"](#) .

Configuración necesaria para crear copias de seguridad en una suscripción de Azure diferente

De forma predeterminada, las copias de seguridad se crean utilizando la misma suscripción que la utilizada para su sistema Cloud Volumes ONTAP .

Verificar los requisitos de la licencia

Para obtener una licencia PAYGO de NetApp Backup and Recovery , se requiere una suscripción a través de Azure Marketplace antes de habilitar NetApp Backup and Recovery. La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción. ["Puede suscribirse desde la página Detalles y Credenciales del asistente del sistema"](#) .

Para obtener una licencia BYOL de NetApp Backup and Recovery , necesita el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#) . Debe utilizar una licencia BYOL cuando el agente de consola y el sistema Cloud Volumes ONTAP se implementan en un sitio oscuro ("modo privado").

Y necesita tener una suscripción a Microsoft Azure para el espacio de almacenamiento donde se ubicarán sus copias de seguridad.

Prepare su agente de consola

El agente de consola se puede instalar en una región de Azure con acceso a Internet completo o limitado (modo "estándar" o "restringido"). ["Consulte los modos de implementación de la NetApp Console para obtener más detalles"](#) .

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Implementar un agente de consola en Azure en modo estándar \(acceso completo a Internet\)"](#)
- ["Instalar el agente de consola en modo restringido \(acceso saliente limitado\)"](#)

Verificar o agregar permisos al agente de la consola

Para utilizar la funcionalidad de búsqueda y restauración de NetApp Backup and Recovery , debe tener permisos específicos en el rol del agente de consola para que pueda acceder al área de trabajo de Azure Synapse y a la cuenta de almacenamiento de Data Lake. Vea los permisos a continuación y siga los pasos si necesita modificar la política.

Antes de empezar

- Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") con su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#) . Debe ser el **Propietario** o **Colaborador** de la suscripción para registrar al proveedor de recursos.
- El puerto 1433 debe estar abierto para la comunicación entre el agente de la consola y los servicios SQL de Azure Synapse.

Pasos

1. Identifique el rol asignado a la máquina virtual del agente de consola:
 - a. En el portal de Azure, abra el servicio de máquinas virtuales.
 - b. Seleccione la máquina virtual del agente de consola.
 - c. En Configuración, seleccione **Identidad**.
 - d. Seleccione **Asignaciones de roles de Azure**.

- e. Tome nota de la función personalizada asignada a la máquina virtual del agente de consola.
2. Actualizar el rol personalizado:
- a. En el portal de Azure, abra su suscripción de Azure.
 - b. Seleccione **Control de acceso (IAM) > Roles**.
 - c. Seleccione los puntos suspensivos (...) para el rol personalizado y luego seleccione **Editar**.
 - d. Seleccione **JSON** y agregue los siguientes permisos:

```

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

```

["Ver el formato JSON completo de la política"](#)

e. Seleccione **Revisar + actualizar** y luego seleccione **Actualizar**.

Información necesaria para utilizar claves administradas por el cliente para el cifrado de datos

Puede utilizar sus propias claves administradas por el cliente para el cifrado de datos en el asistente de activación en lugar de utilizar las claves de cifrado administradas por Microsoft predeterminadas. En este caso, necesitará tener la suscripción de Azure, el nombre de Key Vault y la clave. "[Vea cómo utilizar sus propias llaves](#)".

NetApp Backup and Recovery admite las *políticas de acceso de Azure*, el modelo de permisos de *control de acceso basado en roles de Azure* (Azure RBAC) y el *modelo de seguridad de hardware administrado* (HSM) (consulte "[¿Qué es Azure Key Vault Managed HSM?](#)").

Cree su cuenta de almacenamiento de blobs de Azure

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

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

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. "[Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP](#)".

Requisitos de red de Cloud Volumes ONTAP

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

Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP

Habilitar NetApp Backup and Recovery es fácil. Los pasos varían levemente dependiendo de si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

Habilitar NetApp Backup and Recovery en un nuevo sistema

NetApp Backup and Recovery está habilitado de forma predeterminada en el asistente del sistema. Asegúrese de mantener la opción habilitada.

Ver "[Lanzamiento de Cloud Volumes ONTAP en Azure](#)" para conocer los requisitos y detalles para crear su

sistema Cloud Volumes ONTAP .



Si desea elegir el nombre del grupo de recursos, **deshabilite** NetApp Backup and Recovery al implementar Cloud Volumes ONTAP.

Pasos

1. Desde la página **Sistemas** de la consola, seleccione **Agregar sistema**, elija el proveedor de nube y seleccione **Agregar nuevo**. Seleccione **Crear Cloud Volumes ONTAP**.
2. Seleccione **Microsoft Azure** como proveedor de nube y luego elija un solo nodo o un sistema HA.
3. En la página Definir credenciales de Azure, ingrese el nombre de las credenciales, el ID del cliente, el secreto del cliente y el ID del directorio, y seleccione **Continuar**.
4. Complete la página Detalles y credenciales y asegúrese de tener una suscripción a Azure Marketplace y seleccione **Continuar**.
5. En la página Servicios, deje el servicio habilitado y seleccione **Continuar**.
6. Complete las páginas del asistente para implementar el sistema.

Resultado

NetApp Backup and Recovery está habilitado en el sistema. Después de haber creado volúmenes en estos sistemas Cloud Volumes ONTAP , inicie NetApp Backup and Recovery y ["Activar la copia de seguridad en cada volumen que desee proteger"](#) .

Habilitar NetApp Backup and Recovery en un sistema existente

Habilite NetApp Backup and Recovery en cualquier momento directamente desde el sistema.

Pasos

1. Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Azure Blob para sus copias de seguridad existe como un sistema en la página **Sistemas** de la consola, puede arrastrar el clúster al sistema de Azure Blob para iniciar el asistente de configuración.

2. Complete las páginas del asistente para implementar NetApp Backup and Recovery.
3. Cuando desee iniciar copias de seguridad, continúe con [Activar copias de seguridad en sus volúmenes ONTAP](#) .

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:

- Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Azure para sus copias de seguridad existe como un sistema en la página **Sistemas**, puede arrastrar el clúster ONTAP al almacenamiento de objetos Blob de Azure.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones***  **y seleccione *Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes características: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo ["Activar la copia de seguridad para volúmenes adicionales en el sistema"](#) (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

Si los volúmenes que elige ya tienen políticas de instantáneas o replicación aplicadas, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, podrá seleccionar todos los volúmenes FlexVol . (Los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.

- Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.

2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si eligió replicación y copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** la información fluye desde el sistema de almacenamiento primario al secundario, y desde el secundario al almacenamiento de objetos.
 - **Distribución en abanico:** la información fluye desde el sistema de almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

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

- **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen

replicado.

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



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

- **Proveedor:** Seleccione **Microsoft Azure**.
- **Configuración del proveedor:** Ingrese los detalles del proveedor.

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

Cree una nueva cuenta de almacenamiento o seleccione una existente.

Ingrese la suscripción de Azure utilizada para almacenar las copias de seguridad. Esta puede ser una suscripción diferente a la que se encuentra en el sistema Cloud Volumes ONTAP.

Cree su propio grupo de recursos que administre el contenedor de Blobs o seleccione el tipo de grupo de recursos y el grupo.



Si desea proteger sus archivos de respaldo para que no se modifiquen ni eliminen, asegúrese de que la cuenta de almacenamiento se haya creado con el almacenamiento inmutable habilitado utilizando un período de retención de 30 días.

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

Si elige utilizar sus propias claves administradas por el cliente, ingrese al almacén de claves y a la información de la clave. "[Aprende a usar tus propias llaves](#)".



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

- **Redes:** elija el espacio IP y si utilizará un punto final privado. El punto final privado está deshabilitado de forma predeterminada.
 - i. El espacio IP en el clúster ONTAP donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
 - ii. De manera opcional, elija si utilizará un punto de conexión privado de Azure que haya configurado previamente. "[Obtenga información sobre el uso de un punto de conexión privado de Azure](#)".
- **Política de respaldo:** seleccione una política de almacenamiento de respaldo a objetos existente.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte ["Configuración de la política de copia de seguridad en objeto"](#).
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos de almacenamiento primario contenidos en las instantáneas.

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

Se crea un contenedor de almacenamiento de blobs en el grupo de recursos ingresado y los archivos de respaldo se almacenan allí.

De forma predeterminada, NetApp Backup and Recovery aprovisiona el contenedor Blob con redundancia local (LRS) para optimizar costos. Puede cambiar esta configuración a Redundancia de zona (ZRS) si desea asegurarse de que sus datos se repliquen entre diferentes zonas. Consulte las instrucciones de Microsoft para ["Cambiar la forma en que se replica su cuenta de almacenamiento"](#).

Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página](#)

[de seguimiento de trabajos](#) .

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

¿Que sigue?

- Puede ["Administrar sus archivos de respaldo y políticas de respaldo"](#) . Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copias de seguridad, y más.
- Puede ["Administrar la configuración de copias de seguridad a nivel de clúster"](#) . Esto incluye cambiar las claves de almacenamiento que ONTAP usa para acceder al almacenamiento en la nube, cambiar el ancho de banda de red disponible para cargar copias de seguridad al almacenamiento de objetos, cambiar la configuración de copia de seguridad automática para volúmenes futuros y más.
- También puedes ["restaurar volúmenes, carpetas o archivos individuales desde un archivo de respaldo"](#) a un sistema Cloud Volumes ONTAP en AWS o a un sistema ONTAP local.

Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas Cloud Volumes ONTAP en Google Cloud Storage.



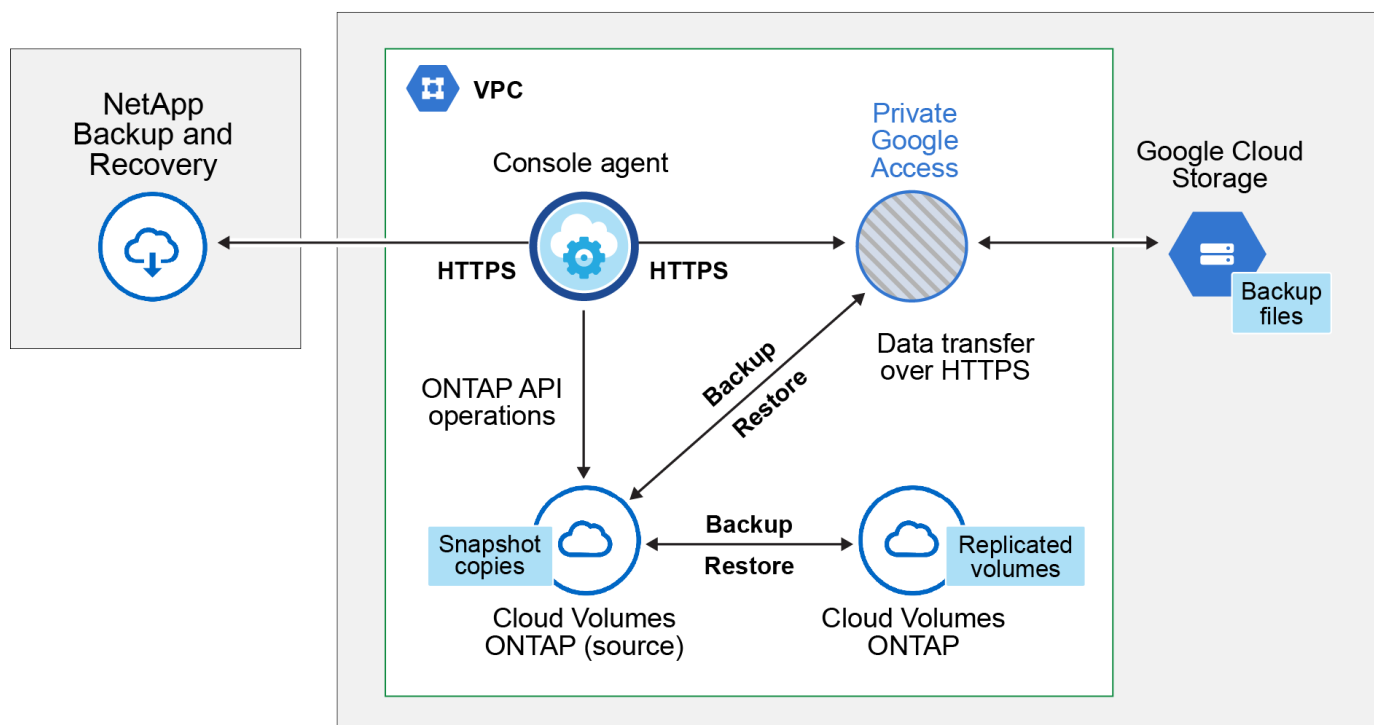
Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Verificar la compatibilidad con su configuración

Lea los siguientes requisitos para asegurarse de tener una configuración compatible antes de comenzar a realizar copias de seguridad de volúmenes en Google Cloud Storage.

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

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



Versiones de ONTAP compatibles

Mínimo de ONTAP 9.8; se recomienda ONTAP 9.8P13 y posterior.

Regiones de GCP compatibles

NetApp Backup and Recovery es compatible en todas las regiones de GCP.

Cuenta de servicio de GCP

Debe tener una cuenta de servicio en su proyecto de Google Cloud que tenga el rol personalizado.

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



El rol de administrador de almacenamiento ya no es necesario para la cuenta de servicio que permite que NetApp Backup and Recovery acceda a los depósitos de Google Cloud Storage.

Verificar los requisitos de la licencia

Para las licencias PAYGO de NetApp Backup and Recovery , hay una suscripción de consola disponible en Google Marketplace que permite implementaciones de Cloud Volumes ONTAP y NetApp Backup and Recovery. Necesitas ["Suscríbete a esta suscripción de consola"](#) antes de habilitar NetApp Backup and Recovery. La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción. ["Puede suscribirse desde la página Detalles y Credenciales del asistente del sistema"](#) .

Para obtener una licencia BYOL de NetApp Backup and Recovery , necesita el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#) .

Además, es necesario tener una suscripción a Google para el espacio de almacenamiento donde se ubicarán las copias de seguridad.

Prepare su agente de consola

El agente de consola debe instalarse en una región de Google con acceso a Internet.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Implementar un agente de consola en Google Cloud"](#)

Verificar o agregar permisos al agente de la consola

Para utilizar la funcionalidad "Buscar y restaurar" de NetApp Backup and Recovery , debe tener permisos específicos en el rol del agente de consola para que pueda acceder al servicio Google Cloud BigQuery. Vea los permisos a continuación y siga los pasos si necesita modificar la política.

Pasos

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

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

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

Información necesaria para utilizar claves de cifrado administradas por el cliente (CMEK)

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

- Necesitarás tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado administradas por el cliente"](#) .
- Deberá verificar que estos permisos requeridos estén incluidos en la función del agente de consola:

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

- Deberá verificar que la API "Cloud Key Management Service (KMS)" de Google esté habilitada en su proyecto. Ver el ["Documentación de Google Cloud: Habilitación de API"](#) Para más detalles.

Consideraciones sobre CMEK:

- Se admiten claves generadas por software y HSM (respaldadas por hardware).
- Se admiten claves Cloud KMS recién creadas o importadas.
- Sólo se admiten claves regionales; no se admiten claves globales.
- Actualmente, solo se admite el propósito de "Cifrado/descifrado simétrico".
- NetApp Backup and Recovery asigna el rol de IAM "CryptoKey Encrypter/Decrypter" (roles/cloudkms.cryptoKeyEncrypterDecrypter)" al agente de servicio asociado con la cuenta de almacenamiento.

Crea tus propios cubos

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

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

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#).

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo

de seguridad predefinido.

- Para replicar datos entre dos sistemas Cloud Volumes ONTAP en diferentes subredes, las subredes deben enrutarse juntas (esta es la configuración predeterminada).

Habilitar NetApp Backup and Recovery en Cloud Volumes ONTAP

Los pasos para habilitar NetApp Backup and Recovery difieren levemente según si tiene un sistema Cloud Volumes ONTAP existente o uno nuevo.

Habilitar NetApp Backup and Recovery en un nuevo sistema

NetApp Backup and Recovery se puede habilitar cuando completa el asistente del sistema para crear un nuevo sistema Cloud Volumes ONTAP .

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

Ver "[Lanzamiento de Cloud Volumes ONTAP en GCP](#)" para conocer los requisitos y detalles para crear su sistema Cloud Volumes ONTAP .

Pasos

1. Desde la página **Sistemas** de la consola, seleccione **Agregar sistema**, elija el proveedor de nube y seleccione **Agregar nuevo**. Seleccione **Crear Cloud Volumes ONTAP**.
2. **Elija una ubicación:** seleccione **Google Cloud Platform**.
3. **Elegir tipo:** Seleccione * Cloud Volumes ONTAP* (nodo único o alta disponibilidad).
4. **Detalles y credenciales:** Ingrese la siguiente información:
 - a. Haga clic en **Editar proyecto** y seleccione un nuevo proyecto si el que desea utilizar es diferente del proyecto predeterminado (donde reside el agente de la consola).
 - b. Especifique el nombre del clúster.
 - c. Habilite el interruptor **Cuenta de servicio** y seleccione la Cuenta de servicio que tenga el rol de Administrador de almacenamiento predefinido. Esto es necesario para habilitar las copias de seguridad y la organización en niveles.
 - d. Especifique las credenciales.

Asegúrese de tener una suscripción a GCP Marketplace.

5. **Servicios:** Deje NetApp Backup and Recovery habilitado y haga clic en **Continuar**.
6. Complete las páginas del asistente para implementar el sistema como se describe en "[Lanzamiento de Cloud Volumes ONTAP en GCP](#)" .

Resultado

NetApp Backup and Recovery está habilitado en el sistema. Después de haber creado volúmenes en estos sistemas Cloud Volumes ONTAP , inicie NetApp Backup and Recovery y "[Activar la copia de seguridad en cada volumen que desee proteger](#)" .

Habilitar NetApp Backup and Recovery en un sistema existente

Puede habilitar NetApp Backup and Recovery en cualquier momento directamente desde el sistema.

Pasos

1. Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Google Cloud Storage para sus copias de seguridad existe como un sistema en la página **Sistemas** de la Consola, puede arrastrar el clúster al sistema de Google Cloud Storage para iniciar el asistente de configuración.

Prepare Google Cloud Storage como su destino de respaldo

Para preparar Google Cloud Storage como destino de respaldo, siga estos pasos:

- Configurar permisos.
- (Opcional) Crea tus propios buckets. (El servicio creará depósitos para usted si lo desea).
- (Opcional) Configure claves administradas por el cliente para el cifrado de datos

Configurar permisos

Debe proporcionar claves de acceso de almacenamiento para una cuenta de servicio que tenga permisos específicos mediante un rol personalizado. Una cuenta de servicio permite que NetApp Backup and Recovery autentique y acceda a los depósitos de Cloud Storage que se utilizan para almacenar copias de seguridad. Las claves son necesarias para que Google Cloud Storage sepa quién realiza la solicitud.

Pasos

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

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

3. En la consola de Google Cloud, "[Vaya a la página de Cuentas de servicio](#)" .
4. Seleccione su proyecto en la nube.
5. Seleccione **Crear cuenta de servicio** y proporcione la información requerida:
 - a. **Detalles de la cuenta de servicio:** Ingrese un nombre y una descripción.
 - b. **Otorgar a esta cuenta de servicio acceso al proyecto:** seleccione el rol personalizado que acaba de crear.

c. Seleccione **Listo**.

6. Ir a ["Configuración de almacenamiento de GCP"](#) y crear claves de acceso para la cuenta de servicio:

- a. Seleccione un proyecto y seleccione **Interoperabilidad**. Si aún no lo ha hecho, seleccione **Habilitar acceso de interoperabilidad**.
- b. En **Claves de acceso para cuentas de servicio**, seleccione **Crear una clave para una cuenta de servicio**, seleccione la cuenta de servicio que acaba de crear y haga clic en **Crear clave**.

Necesitará ingresar las claves en NetApp Backup and Recovery más adelante cuando configure el servicio de respaldo.

Crea tus propios cubos

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

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

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

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

Si planea utilizar sus propias claves administradas por el cliente:

- Necesitarás tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado administradas por el cliente"](#).
- Deberá verificar que estos permisos requeridos estén incluidos en la función del agente de consola:

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

- Deberá verificar que la API "Cloud Key Management Service (KMS)" de Google esté habilitada en su proyecto. Ver el ["Documentación de Google Cloud: Habilitación de API"](#) Para más detalles.

Consideraciones sobre CMEK:

- Se admiten claves generadas por software y HSM (respaldadas por hardware).
- Se admiten claves Cloud KMS recién creadas o importadas.
- Solo se admiten claves regionales, no claves globales.

- Actualmente, solo se admite el propósito de "Cifrado/descifrado simétrico".
- NetApp Backup and Recovery asigna el rol de IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" al agente de servicio asociado con la cuenta de almacenamiento.

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:

- Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de GCP para sus copias de seguridad existe como un sistema en la página **Sistemas** de la consola, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de GCP.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones***  **y seleccione *Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo ["Activar la copia de seguridad para volúmenes adicionales en el sistema"](#) (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

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

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales**: si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación**: crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad**: realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura**: Si eligió replicación y copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada**: la información fluye desde el sistema de almacenamiento primario al secundario, y desde el secundario al almacenamiento de objetos.
 - **Distribución en abanico**: la información fluye desde el sistema de almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Para las políticas de copia de seguridad a objeto, configure Datalock y Ransomware Resilience. Para obtener más detalles sobre Datalock y Ransomware Resilience, consulte ["Configuración de la política de copia de seguridad en objeto"](#) .
- Seleccione **Crear**.

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

- **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.
- **Política de replicación:** elija una política de replicación existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

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

Cree un nuevo depósito o seleccione uno existente.

- **Clave de cifrado:** si creó un nuevo depósito de Google, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Elija si utilizará las claves de cifrado predeterminadas de Google Cloud o elegirá sus propias claves administradas por el cliente desde su cuenta de Google para administrar el cifrado de sus datos.

Si elige utilizar sus propias claves administradas por el cliente, ingrese al almacén de claves y a la información de la clave.



Si seleccionó un depósito de Google Cloud existente, la información de cifrado ya está disponible, por lo que no necesita ingresarla ahora.

- **Política de respaldo:** seleccione una política de almacenamiento de respaldo a objetos existente o

cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las instantáneas.

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

Se crea un depósito de Google Cloud Storage en la cuenta de servicio indicada por la clave de acceso de Google y la clave secreta ingresada, y los archivos de respaldo se almacenan allí.

Las copias de seguridad están asociadas con la clase de almacenamiento *Estándar* de forma predeterminada. Puede utilizar las clases de almacenamiento *Nearline*, *Coldline* o *Archive*, de menor costo. Sin embargo, la clase de almacenamiento se configura a través de Google, no a través de la interfaz de usuario de NetApp Backup and Recovery. Ver el tema de Google "[Cambiar la clase de almacenamiento predeterminada de un bucket](#)" Para más detalles.

Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página de seguimiento de trabajos"](#) .

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

¿Que sigue?

- Puede ["Administrar sus archivos de respaldo y políticas de respaldo"](#) . Esto incluye iniciar y detener copias de seguridad, eliminar copias de seguridad, agregar y cambiar la programación de copias de seguridad, y más.
- Puede ["Administrar la configuración de copias de seguridad a nivel de clúster"](#) . Esto incluye cambiar las claves de almacenamiento que ONTAP usa para acceder al almacenamiento en la nube, cambiar el ancho de banda de red disponible para cargar copias de seguridad al almacenamiento de objetos, cambiar la configuración de copia de seguridad automática para volúmenes futuros y más.
- También puedes ["restaurar volúmenes, carpetas o archivos individuales desde un archivo de respaldo"](#) a un sistema Cloud Volumes ONTAP en AWS o a un sistema ONTAP local.

Realice copias de seguridad de los datos locales de ONTAP en Amazon S3 con NetApp Backup and Recovery

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



Los "sistemas ONTAP locales" incluyen los sistemas FAS, AFF y ONTAP Select .



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

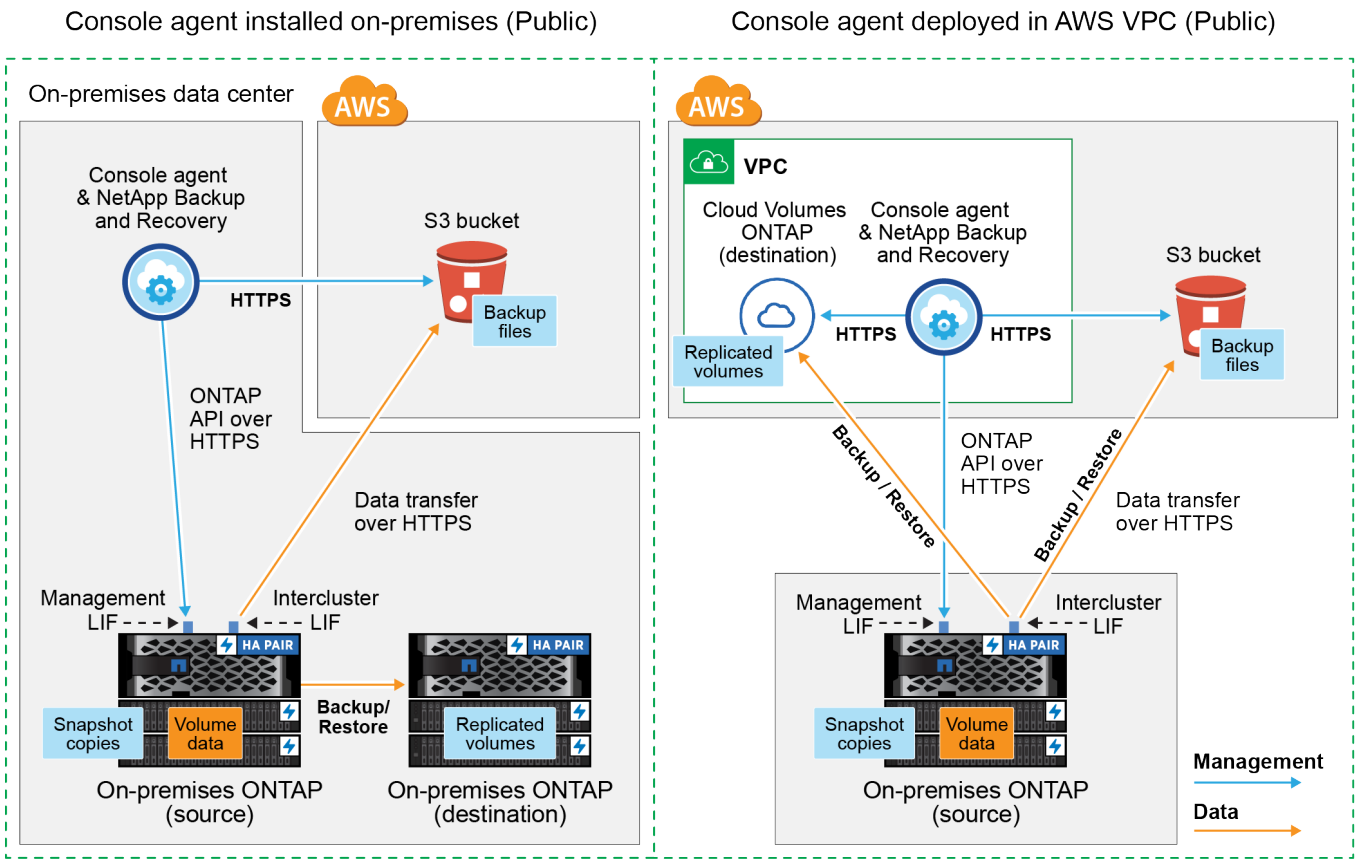
Identificar el método de conexión

Elija cuál de los dos métodos de conexión utilizará al configurar copias de seguridad de los sistemas ONTAP locales a AWS S3.

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

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

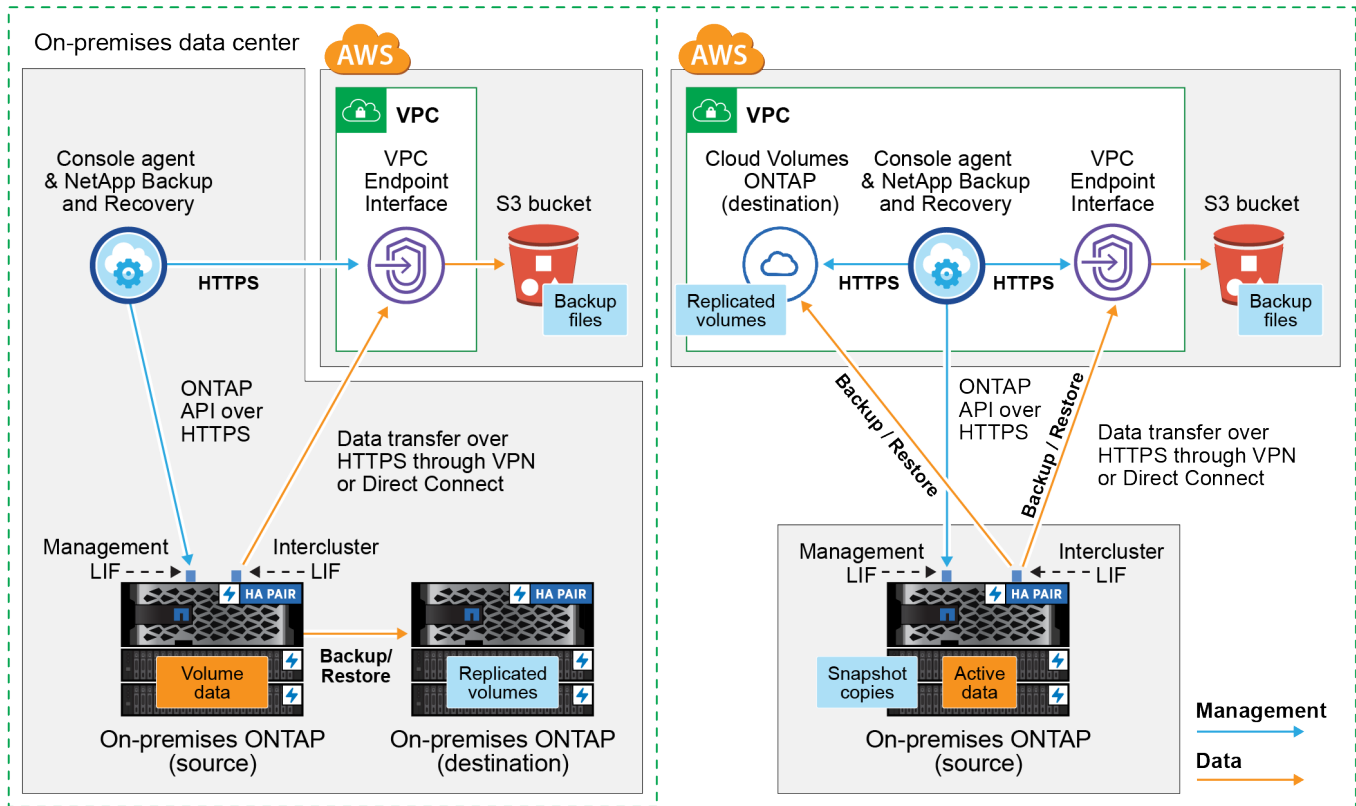
El siguiente diagrama muestra el método de **conexión pública** y las conexiones que debe preparar entre los componentes. Puede utilizar un agente de consola que haya instalado en sus instalaciones o un agente de consola que haya implementado en AWS VPC.



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

Console agent installed on-premises (Private)

Console agent deployed in AWS VPC (Private)



Prepare su agente de consola

El agente de consola es el software principal para la funcionalidad de la NetApp Console . Se requiere un agente de consola para realizar copias de seguridad y restaurar sus datos de ONTAP .

Crear o cambiar agentes de consola

Si ya tiene un agente de consola implementado en su VPC de AWS o en sus instalaciones, entonces está todo listo.

De lo contrario, deberá crear un agente de consola en una de esas ubicaciones para realizar una copia de seguridad de los datos de ONTAP en el almacenamiento de AWS S3. No puedes usar un agente de consola que esté implementado en otro proveedor de nube.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Instalar un agente de consola en AWS"](#)
- ["Instale un agente de consola en sus instalaciones"](#)
- ["Instalar un agente de consola en una región de AWS GovCloud"](#)

NetApp Backup and Recovery es compatible con las regiones GovCloud cuando el agente de consola se implementa en la nube, no cuando se instala en sus instalaciones. Además, debe implementar el agente de consola desde AWS Marketplace. No es posible implementar el agente de la consola en una región gubernamental desde el sitio web de NetApp Console SaaS.

Preparar los requisitos de red del agente de consola

Asegúrese de que se cumplan los siguientes requisitos de red:

- Asegúrese de que la red donde está instalado el agente de consola permita las siguientes conexiones:
 - Una conexión HTTPS a través del puerto 443 a NetApp Backup and Recovery y a su almacenamiento de objetos S3(["ver la lista de puntos finales"](#))
 - Una conexión HTTPS a través del puerto 443 a su LIF de administración de clúster ONTAP
 - Se requieren reglas de grupo de seguridad entrantes y salientes adicionales para las implementaciones de AWS y AWS GovCloud. Ver ["Reglas para el agente de consola en AWS"](#) Para más detalles.
- Si tiene una conexión directa o VPN desde su clúster ONTAP a la VPC, y desea que la comunicación entre el agente de la consola y S3 permanezca en su red interna de AWS (una conexión **privada**), deberá habilitar una interfaz de punto final de VPC a S3. [Configure su sistema para una conexión privada mediante una interfaz de punto final de VPC.](#)

Verificar los requisitos de la licencia

Deberá verificar los requisitos de licencia tanto para AWS como para la NetApp Console:

- Antes de poder activar NetApp Backup and Recovery para su clúster, deberá suscribirse a una oferta de NetApp Console Marketplace de pago por uso (PAYGO) de AWS o comprar y activar una licencia BYOL de NetApp Backup and Recovery de NetApp. Estas licencias son para su cuenta y se pueden usar en múltiples sistemas.
 - Para obtener la licencia PAYGO de NetApp Backup and Recovery , necesitará una suscripción a ["Oferta de NetApp Console desde AWS Marketplace"](#) . La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción.
 - Para obtener una licencia BYOL de NetApp Backup and Recovery , necesitará el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia.
- Necesita tener una suscripción a AWS para el espacio de almacenamiento de objetos donde se ubicarán sus copias de seguridad.

Regiones compatibles

Puede crear copias de seguridad desde sistemas locales a Amazon S3 en todas las regiones, incluidas las regiones de AWS GovCloud. Usted especifica la región donde se almacenarán las copias de seguridad cuando configura el servicio.

Prepare sus clústeres de ONTAP

Prepare su sistema local de origen ONTAP y cualquier sistema local secundario ONTAP o Cloud Volumes ONTAP .

La preparación de sus clústeres ONTAP implica los siguientes pasos:

- Descubra sus sistemas ONTAP en NetApp Console
- Verificar los requisitos del sistema ONTAP
- Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos
- Verificar los requisitos de red de ONTAP para replicar volúmenes

Descubra sus sistemas ONTAP en NetApp Console

Tanto su sistema ONTAP local de origen como cualquier sistema ONTAP local secundario o sistemas Cloud Volumes ONTAP deben estar disponibles en la página **Sistemas** de la NetApp Console .

Necesitará saber la dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para agregar el clúster. "[Aprenda a descubrir un clúster](#)".

Verificar los requisitos del sistema ONTAP

Asegúrese de que su sistema ONTAP cumpla con los siguientes requisitos:

- Mínimo de ONTAP 9.8; se recomienda 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 NetApp Backup and Recovery.

Aprenda cómo "[Administrar sus licencias de clúster](#)".

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo "[Configurar el tiempo de su clúster](#)".
- Si replica datos, verifique que los sistemas de origen y destino ejecuten versiones de ONTAP compatibles.

"[Ver versiones de ONTAP compatibles con las relaciones de SnapMirror](#)".

Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos

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

- Para una arquitectura de respaldo en abanico, configure los siguientes ajustes en el sistema *principal*.
- Para una arquitectura de respaldo en cascada, configure los siguientes ajustes en el sistema *secundario*.

Se necesitan los siguientes requisitos de red del clúster ONTAP :

- El clúster requiere una conexión HTTPS entrante desde el agente de la consola al LIF de administración del clúster.
- Se requiere un LIF entre clústeres en cada nodo de ONTAP que aloje los volúmenes que desea respaldar. Estos LIF entre clústeres deben poder acceder al almacén de objetos.

El clúster inicia una conexión HTTPS saliente a través del puerto 443 desde los LIF entre clústeres al almacenamiento de Amazon S3 para operaciones de respaldo y restauración. ONTAP lee y escribe datos hacia y desde el almacenamiento de objetos: el almacenamiento de objetos nunca se inicia, solo responde.

- Los LIF entre clústeres deben estar asociados con el *IPspace* que ONTAP debe usar para conectarse al almacenamiento de objetos. "[Obtenga más información sobre IPspaces](#)".

Cuando configura NetApp Backup and Recovery, se le solicita el espacio IP que desea utilizar. Debes elegir el espacio IP con el que están asociados estos LIF. Ese podría ser el espacio IP "predeterminado" o un espacio IP personalizado que usted creó.

Si utiliza un espacio IP diferente al "Predeterminado", es posible que necesite crear una ruta estática para obtener acceso al almacenamiento de objetos.

Todos los LIF entre clústeres dentro del espacio IP deben tener acceso al almacén de objetos. Si no puede configurar esto para el espacio IP actual, entonces necesitará crear un espacio IP dedicado donde todos los LIF entre clústeres tengan acceso al almacén de objetos.

- Los servidores DNS deben haber sido configurados para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Vea cómo ["Configurar servicios DNS para la SVM"](#) .
- Actualice las reglas de firewall, si es necesario, para permitir conexiones de NetApp Backup and Recovery desde ONTAP al almacenamiento de objetos a través del puerto 443 y tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).
- Si está utilizando un punto final de interfaz de VPC privada en AWS para la conexión S3, entonces para poder utilizar HTTPS/443, deberá cargar el certificado del punto final S3 en el clúster de ONTAP . [Configure su sistema para una conexión privada mediante una interfaz de punto final de VPC](#).
- Asegúrese de que su clúster ONTAP tenga permisos para acceder al bucket S3.

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#) .

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo de seguridad predefinido.

Prepare Amazon S3 como su destino de respaldo

La preparación de Amazon S3 como destino de respaldo implica los siguientes pasos:

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

Configurar permisos S3

Necesitarás configurar dos conjuntos de permisos:

- Permisos para que el agente de la consola cree y administre el depósito S3.
- Permisos para el clúster ONTAP local para que pueda leer y escribir datos en el depósito S3.

Pasos

1. Asegúrese de que el agente de la consola tenga los permisos necesarios. Para más detalles, consulte ["Permisos de políticas de la NetApp Console"](#) .



Al crear copias de seguridad en las regiones de AWS China, debe cambiar el nombre del recurso de AWS "arn" en todas las secciones *Resource* en las políticas de IAM de "aws" a "aws-cn"; por ejemplo `arn:aws-cn:s3:::netapp-backup-*` .

2. Cuando active el servicio, el asistente de copia de seguridad le solicitará que ingrese una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda realizar copias de seguridad y restaurar datos en el depósito S3. Para ello, necesitarás crear un usuario IAM con los siguientes permisos.

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

```

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

```

Crea tus propios cubos

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

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

Si crea sus propios depósitos, debe utilizar el nombre de depósito "netapp-backup". Si necesitas usar un nombre personalizado, edita el `ontapcloud-instance-policy-netapp-backup` IAMRole para los CVO existentes y agregue el siguiente bloque JSON a los permisos de S3 `Statement` formación. Necesitas incluir `"Resource": "arn:aws:s3:::*"` y asignar todos los permisos necesarios que deben asociarse con el depósito.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "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:::*"
  }
]
```

Configurar claves de AWS administradas 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 depósito S3, entonces está todo listo porque la instalación predeterminada usa ese

tipo de cifrado.

Si, en cambio, desea utilizar sus propias claves administradas por el cliente para el cifrado de datos en lugar de utilizar las claves predeterminadas, deberá tener las claves administradas de cifrado ya configuradas antes de iniciar el asistente de NetApp Backup and Recovery .

["Consulte cómo utilizar sus propias claves de cifrado de Amazon con Cloud Volumes ONTAP"](#).

["Consulte cómo utilizar sus propias claves de cifrado de Amazon con NetApp Backup and Recovery"](#).

Configure su sistema para una conexión privada mediante una interfaz de punto final de VPC

Si desea utilizar una conexión a Internet pública estándar, todos los permisos los establece el agente de la consola y no es necesario hacer nada más.

Si desea tener una conexión más segura a Internet desde su centro de datos local a la VPC, hay una opción para seleccionar una conexión AWS PrivateLink en el asistente de activación de Backup. Es necesario si planea usar una VPN o AWS Direct Connect para conectar su sistema local a través de una interfaz de punto final de VPC que usa una dirección IP privada.

Pasos

1. Cree una configuración de punto final de interfaz mediante la consola de Amazon VPC o la línea de comandos. ["Consulte los detalles sobre el uso de AWS PrivateLink para Amazon S3"](#) .
2. Modifique la configuración del grupo de seguridad asociado con el agente de consola. Debe cambiar la política a "Personalizada" (de "Acceso completo") y debe [Agregar los permisos S3 desde la política de respaldo](#) como se mostró anteriormente.

Si está utilizando el puerto 80 (HTTP) para comunicarse con el punto final privado, ya está todo listo. Ahora puede habilitar NetApp Backup and Recovery en el clúster.

Si está utilizando el puerto 443 (HTTPS) para comunicarse con el punto final privado, debe copiar el certificado del punto final S3 de VPC y agregarlo a su clúster ONTAP , como se muestra en los siguientes 4 pasos.

3. Obtenga el nombre DNS del punto final desde la consola de AWS.
4. Obtenga el certificado del punto final S3 de VPC. Esto lo hace mediante ["Iniciar sesión en la máquina virtual que aloja el agente de consola"](#) y ejecutando el siguiente comando. Al ingresar el nombre DNS del punto final, agregue "bucket" al comienzo, reemplazando el "***":

```
openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

5. Desde la salida de este comando, copie los datos del certificado S3 (todos los datos entre las etiquetas BEGIN / END CERTIFICATE, incluidas estas):

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvboZ/oO2NWLLFCqI+xmKLCmiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

6. Inicie sesión en la CLI del clúster ONTAP y aplique el certificado que copió usando el siguiente comando (sustituya el nombre de su propia máquina virtual de almacenamiento):

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

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:
 - Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Amazon S3 para sus copias de seguridad existe como un sistema en la página **Sistemas** de la consola, puede arrastrar el clúster ONTAP al almacenamiento de objetos de Amazon S3.

 - Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones***  **icono y seleccione *Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo "[Activar la copia de seguridad para volúmenes adicionales en el sistema](#)" (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

Si los volúmenes que elige ya tienen políticas de instantáneas o replicación aplicadas, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si eligió replicación y copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** la información fluye desde el almacenamiento primario al secundario, al almacenamiento de objetos, y desde el secundario al almacenamiento de objetos.
 - **Distribución en abanico:** la información fluye desde el almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantánea existente o cree una política.



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

4. Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:
 - Introduzca el nombre de la póliza.
 - Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
 - Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte ["Configuración de la política de copia de seguridad en objeto"](#) .
 - Seleccione **Crear**.
5. **Replicación:** Establezca las siguientes opciones:
 - **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.
 - **Política de replicación:** elija una política de replicación existente o cree una política.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

6. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

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

La clave de acceso y la clave secreta son para el usuario de IAM que creó para otorgarle al clúster ONTAP acceso al depósito S3.

- **Bucket:** elija un bucket S3 existente o cree uno nuevo. Referirse a ["Agregar depósitos S3"](#).
- **Clave de cifrado:** si creó un nuevo depósito S3, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Elija si utilizará las claves de cifrado predeterminadas de Amazon S3 o elegirá sus propias claves administradas por el cliente desde su cuenta de AWS para administrar el cifrado de sus datos.



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

- **Redes:** elija el espacio IP y si utilizará un punto final privado. El punto final privado está deshabilitado de forma predeterminada.
 - i. El espacio IP en el clúster ONTAP donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
 - ii. Opcionalmente, elija si utilizará un AWS PrivateLink que haya configurado previamente. ["Consulte los detalles sobre el uso de AWS PrivateLink para Amazon S3"](#).
- **Política de respaldo:** seleccione una política de respaldo existente o cree una política.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

7. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de

seguridad.

3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos primarios contenidos en las instantáneas.

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

El depósito S3 se crea en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta ingresada, y los archivos de respaldo se almacenan allí. Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página de seguimiento de trabajos"](#).

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Realice una copia de seguridad de los datos locales de ONTAP en Azure Blob Storage con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP locales a un sistema de almacenamiento secundario y al almacenamiento de blobs de Azure.



Los "sistemas ONTAP locales" incluyen los sistemas FAS, AFF y ONTAP Select .



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Identificar el método de conexión

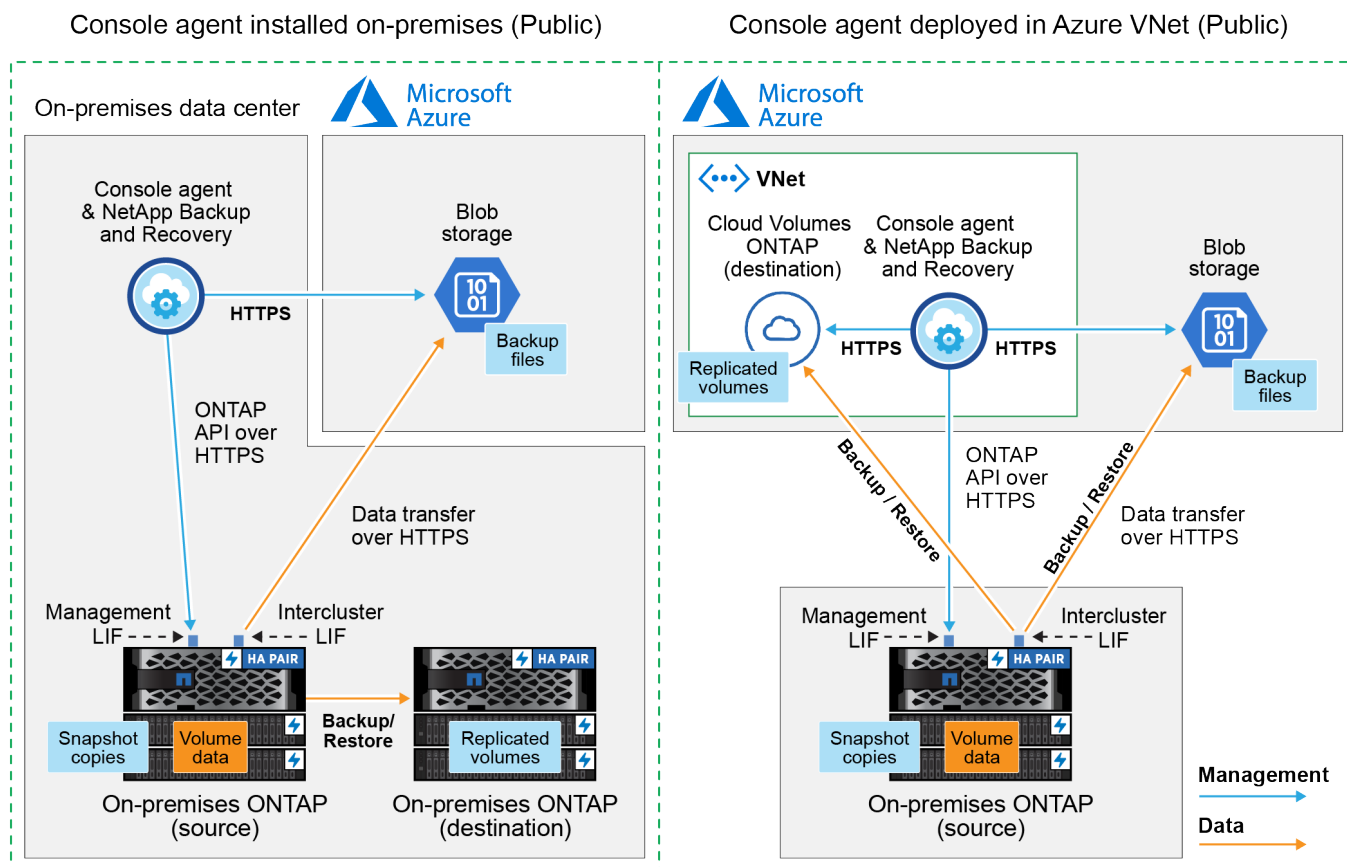
Elija cuál de los dos métodos de conexión usará al configurar copias de seguridad de sistemas ONTAP locales a Azure Blob.

- **Conexión pública:** conecte directamente el sistema ONTAP al almacenamiento de blobs de Azure mediante un punto de conexión público de Azure.

- **Conexión privada:** utilice una VPN o ExpressRoute y enrute el tráfico a través de un punto final privado de VNet que use una dirección IP privada.

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

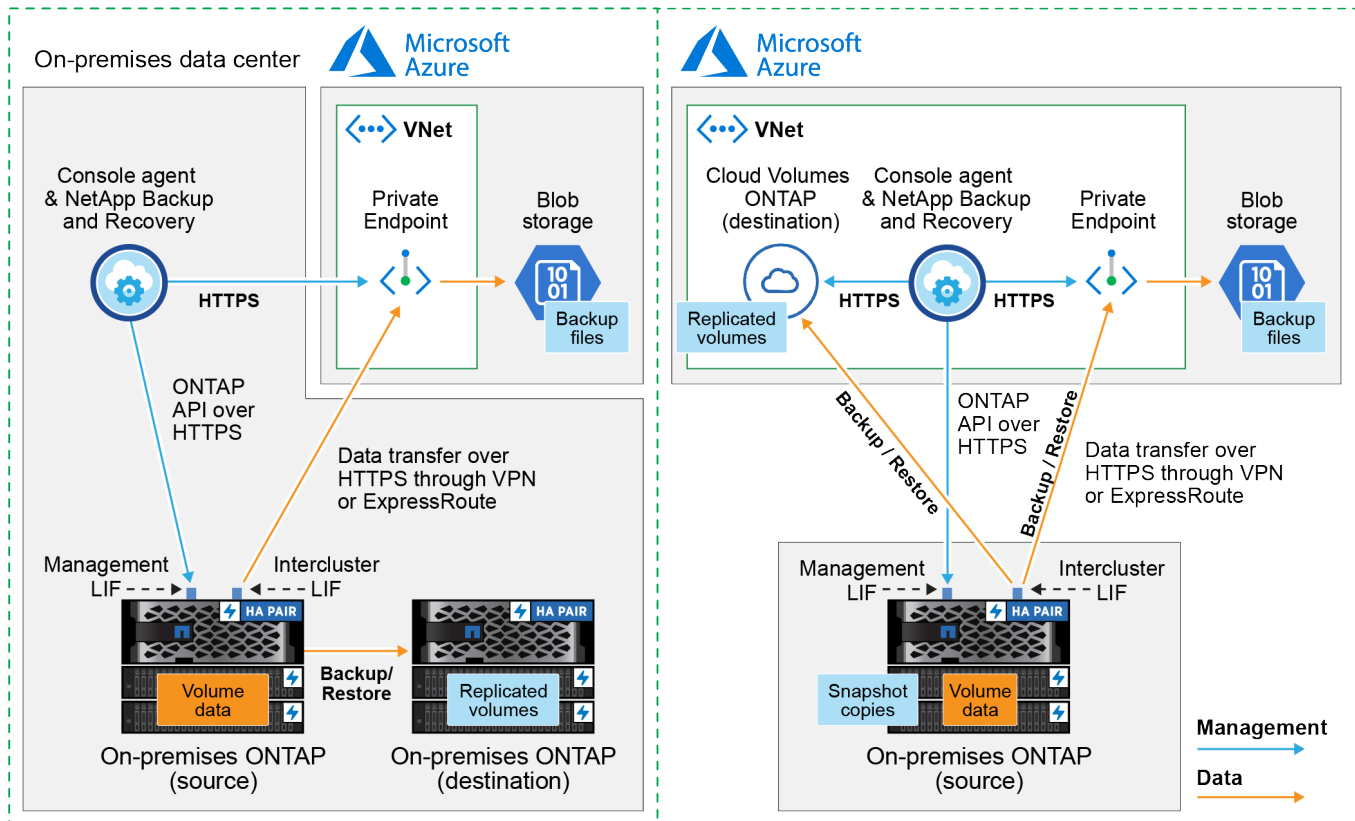
El siguiente diagrama muestra el método de **conexión pública** y las conexiones que debe preparar entre los componentes. Puede usar un agente de consola que haya instalado en sus instalaciones o un agente de consola que haya implementado en la red virtual de Azure.



El siguiente diagrama muestra el método de **conexión privada** y las conexiones que debe preparar entre los componentes. Puede usar un agente de consola que haya instalado en sus instalaciones o un agente de consola que haya implementado en la red virtual de Azure.

Console agent installed on-premises (Private)

Console agent deployed in Azure VNet (Private)



Prepare su agente de consola

El agente de consola es el software principal para la funcionalidad de la NetApp Console . Se requiere un agente de consola para realizar copias de seguridad y restaurar sus datos de ONTAP .

Crear o cambiar agentes de consola

Si ya tiene un agente de consola implementado en su red virtual de Azure o en sus instalaciones, entonces está todo listo.

De lo contrario, deberá crear un agente de consola en una de esas ubicaciones para realizar una copia de seguridad de los datos de ONTAP en el almacenamiento de blobs de Azure. No puedes usar un agente de consola que esté implementado en otro proveedor de nube.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Instalar un agente de consola en Azure"](#)
- ["Instale un agente de consola en sus instalaciones"](#)
- ["Instalar un agente de consola en una región de Azure Government"](#)

NetApp Backup and Recovery es compatible con las regiones de Azure Government cuando el agente de consola se implementa en la nube, no cuando se instala en sus instalaciones. Además, debe implementar el agente de consola desde Azure Marketplace. No es posible implementar el agente de la consola en una región gubernamental desde el sitio web de Console SaaS.

Preparar la red para el agente de consola

Asegúrese de que el agente de consola tenga las conexiones de red necesarias.

Pasos

1. Asegúrese de que la red donde está instalado el agente de consola permita las siguientes conexiones:
 - Una conexión HTTPS a través del puerto 443 a NetApp Backup and Recovery y a su almacenamiento de objetos Blob(["ver la lista de puntos finales"](#))
 - Una conexión HTTPS a través del puerto 443 a su LIF de administración de clúster ONTAP
 - Para que la funcionalidad de búsqueda y restauración de NetApp Backup and Recovery funcione, el puerto 1433 debe estar abierto para la comunicación entre el agente de la consola y los servicios SQL de Azure Synapse.
 - Se requieren reglas de grupo de seguridad entrante adicionales para las implementaciones de Azure y Azure Government. Ver ["Reglas para el agente de consola en Azure"](#) Para más detalles.
2. Habilite un punto de conexión privado de VNet para el almacenamiento de Azure. Esto es necesario si tiene una conexión ExpressRoute o VPN desde su clúster ONTAP a la VNet y desea que la comunicación entre el agente de la consola y el almacenamiento de blobs permanezca en su red privada virtual (una conexión **privada**).

Verificar o agregar permisos al agente de la consola

Para utilizar la funcionalidad de búsqueda y restauración de NetApp Backup and Recovery , debe tener permisos específicos en el rol del agente de consola para que pueda acceder al área de trabajo de Azure Synapse y a la cuenta de almacenamiento de Data Lake. Vea los permisos a continuación y siga los pasos si necesita modificar la política.

Antes de empezar

Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") con su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#) . Debe ser el **Propietario o Colaborador** de la suscripción para registrar al proveedor de recursos.

Pasos

1. Identifique el rol asignado a la máquina virtual del agente de consola:
 - a. En el portal de Azure, abra el servicio Máquinas virtuales.
 - b. Seleccione la máquina virtual del agente de consola.
 - c. En **Configuración**, seleccione **Identidad**.
 - d. Seleccione **Asignaciones de roles de Azure**.
 - e. Tome nota de la función personalizada asignada a la máquina virtual del agente de consola.
2. Actualizar el rol personalizado:
 - a. En el portal de Azure, abra su suscripción de Azure.
 - b. Seleccione **Control de acceso (IAM) > Roles**.
 - c. Seleccione los puntos suspensivos (...) para el rol personalizado y luego seleccione **Editar**.
 - d. Seleccione **JSON** y agregue los siguientes permisos:

```

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

```

["Ver el formato JSON completo de la política"](#)

e. Seleccione **Revisar + actualizar** y luego seleccione **Actualizar**.

Verificar los requisitos de la licencia

Necesitará verificar los requisitos de licencia tanto para Azure como para la consola:

- Antes de poder activar NetApp Backup and Recovery para su clúster, deberá suscribirse a una oferta de Console Marketplace de pago por uso (PAYGO) de Azure o comprar y activar una licencia BYOL de NetApp Backup and Recovery de NetApp. Estas licencias son para su cuenta y se pueden usar en múltiples sistemas.
 - Para obtener la licencia PAYGO de NetApp Backup and Recovery , necesitará una suscripción a ["Oferta de NetApp Console de Azure Marketplace"](#) . La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción.
 - Para obtener una licencia BYOL de NetApp Backup and Recovery , necesitará el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#).
- Necesita tener una suscripción de Azure para el espacio de almacenamiento de objetos donde se ubicarán sus copias de seguridad.

Regiones compatibles

Puede crear copias de seguridad desde sistemas locales a Azure Blob en todas las regiones, incluidas las regiones de Azure Government. Usted especifica la región donde se almacenarán las copias de seguridad cuando configura el servicio.

Prepare sus clústeres de ONTAP

Prepare su sistema local de origen ONTAP y cualquier sistema local secundario ONTAP o Cloud Volumes ONTAP .

La preparación de sus clústeres ONTAP implica los siguientes pasos:

- Descubra sus sistemas ONTAP en NetApp Console
- Verificar los requisitos del sistema ONTAP
- Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos
- Verificar los requisitos de red de ONTAP para replicar volúmenes

Descubra sus sistemas ONTAP en NetApp Console

Tanto su sistema ONTAP local de origen como cualquier sistema ONTAP local secundario o sistemas Cloud Volumes ONTAP deben estar disponibles en la página **Sistemas** de la NetApp Console .

Necesitará saber la dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para agregar el clúster. ["Aprenda a descubrir un clúster"](#).

Verificar los requisitos del sistema ONTAP

Asegúrese de que su sistema ONTAP cumpla con los siguientes requisitos:

- Mínimo de ONTAP 9.8; se recomienda 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 NetApp Backup and Recovery.

Aprenda cómo ["Administrar sus licencias de clúster"](#) .

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["Configurar el tiempo de su clúster"](#) .
- Si replica datos, verifique que los sistemas de origen y destino ejecuten versiones de ONTAP compatibles.

["Ver versiones de ONTAP compatibles con las relaciones de SnapMirror"](#).

Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos

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

- Para una arquitectura de respaldo en abanico, configure los siguientes ajustes en el sistema *principal*.
- Para una arquitectura de respaldo en cascada, configure los siguientes ajustes en el sistema *secundario*.

Se necesitan los siguientes requisitos de red del clúster ONTAP :

- El clúster ONTAP inicia una conexión HTTPS a través del puerto 443 desde el LIF entre clústeres al almacenamiento de blobs de Azure para operaciones de copia de seguridad y restauración.

ONTAP lee y escribe datos hacia y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, simplemente responde.

- ONTAP requiere una conexión entrante desde el agente de la consola al LIF de administración del clúster. El agente de consola puede residir en una red virtual de Azure.
- Se requiere un LIF entre clústeres en cada nodo de ONTAP que aloje los volúmenes que desea respaldar. El LIF debe estar asociado con el *IPspace* que ONTAP debe usar para conectarse al almacenamiento de objetos. ["Obtenga más información sobre IPspaces"](#) .

Cuando configura NetApp Backup and Recovery, se le solicita el espacio IP que desea utilizar. Debes elegir el espacio IP con el que está asociado cada LIF. Ese podría ser el espacio IP "predeterminado" o un espacio IP personalizado que usted creó.

- Los LIF de los nodos y entre clústeres pueden acceder al almacén de objetos.
- Se han configurado servidores DNS para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Vea cómo ["Configurar servicios DNS para la SVM"](#) .
- Si utiliza un espacio IP diferente al predeterminado, es posible que necesite crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir conexiones del servicio NetApp Backup and Recovery desde ONTAP al almacenamiento de objetos a través del puerto 443 y tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#) .

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo de seguridad predefinido.

Prepare Azure Blob como destino de copia de seguridad

1. Puede utilizar sus propias claves personalizadas administradas para el cifrado de datos en el asistente de activación en lugar de utilizar las claves de cifrado administradas predeterminadas por Microsoft. En este caso, necesitará tener la suscripción de Azure, el nombre de Key Vault y la clave. ["Aprende a usar tus propias llaves"](#) .

Tenga en cuenta que la copia de seguridad y la recuperación admiten *políticas de acceso de Azure* como modelo de permisos. El modelo de permisos de *control de acceso basado en roles de Azure* (Azure RBAC) no es compatible actualmente.

2. Si desea tener una conexión más segura a través de Internet público desde su centro de datos local a la red virtual, existe una opción para configurar un punto de conexión privado de Azure en el asistente de activación. En este caso, necesitará conocer la VNet y la subred para esta conexión. ["Consulte los detalles sobre el uso de un punto final privado"](#) .

Cree su cuenta de almacenamiento de blobs de Azure

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

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

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:

- Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto al servicio de Respaldo y recuperación en el panel derecho.

Si el destino de Azure para sus copias de seguridad existe en la página **Sistemas** de la consola, puede arrastrar el clúster de ONTAP al almacenamiento de objetos Blob de Azure.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones***  **y seleccione *Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo ["Activar la copia de seguridad para volúmenes adicionales en el sistema"](#) (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

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

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.

2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si eligió replicación y copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** la información fluye del almacenamiento primario al secundario y del secundario al de objetos.
 - **Distribución en abanico:** la información fluye desde el almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

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

- **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.

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



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

- **Proveedor:** Seleccione **Microsoft Azure**.
- **Configuración del proveedor:** ingrese los detalles del proveedor y la región donde se almacenarán las copias de seguridad.

Cree una nueva cuenta de almacenamiento o seleccione una existente.

Cree su propio grupo de recursos que administre el contenedor de Blobs o seleccione el tipo de grupo de recursos y el grupo.



Si desea proteger sus archivos de respaldo para que no se modifiquen ni eliminen, asegúrese de que la cuenta de almacenamiento se haya creado con el almacenamiento inmutable habilitado utilizando un período de retención de 30 días.



Si desea organizar en niveles los archivos de respaldo más antiguos en Azure Archive Storage para optimizar aún más los costos, asegúrese de que la cuenta de almacenamiento tenga la regla de ciclo de vida adecuada.



Si seleccionas **Bring your own bucket**, asegúrate de que el contenedor que creas como destino de la copia de seguridad tiene el mismo nombre que la cuenta de almacenamiento Azure.

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

Si elige utilizar sus propias claves administradas por el cliente, ingrese al almacén de claves y a la información de la clave.



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

- **Redes:** elija el espacio IP y si utilizará un punto final privado. El punto final privado está deshabilitado de forma predeterminada.
 - i. El espacio IP en el clúster ONTAP donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.
 - ii. De manera opcional, elija si utilizará un punto de conexión privado de Azure que haya configurado previamente. "[Obtenga información sobre el uso de un punto de conexión privado de Azure](#)".

- **Política de respaldo:** seleccione una política de copia de seguridad en almacenamiento de objetos existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la política.
 - Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
 - Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte ["Configuración de la política de copia de seguridad en objeto"](#).
 - Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las instantáneas.

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

Se crea una cuenta de almacenamiento de Blobs en el grupo de recursos ingresado y los archivos de respaldo se almacenan allí. El panel de control de copias de seguridad de volumen se muestra para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página de seguimiento de trabajos"](#).

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP locales primarios a un sistema de almacenamiento secundario y a Google Cloud Storage.



Los "sistemas ONTAP locales" incluyen los sistemas FAS, AFF y ONTAP Select .



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

Identificar el método de conexión

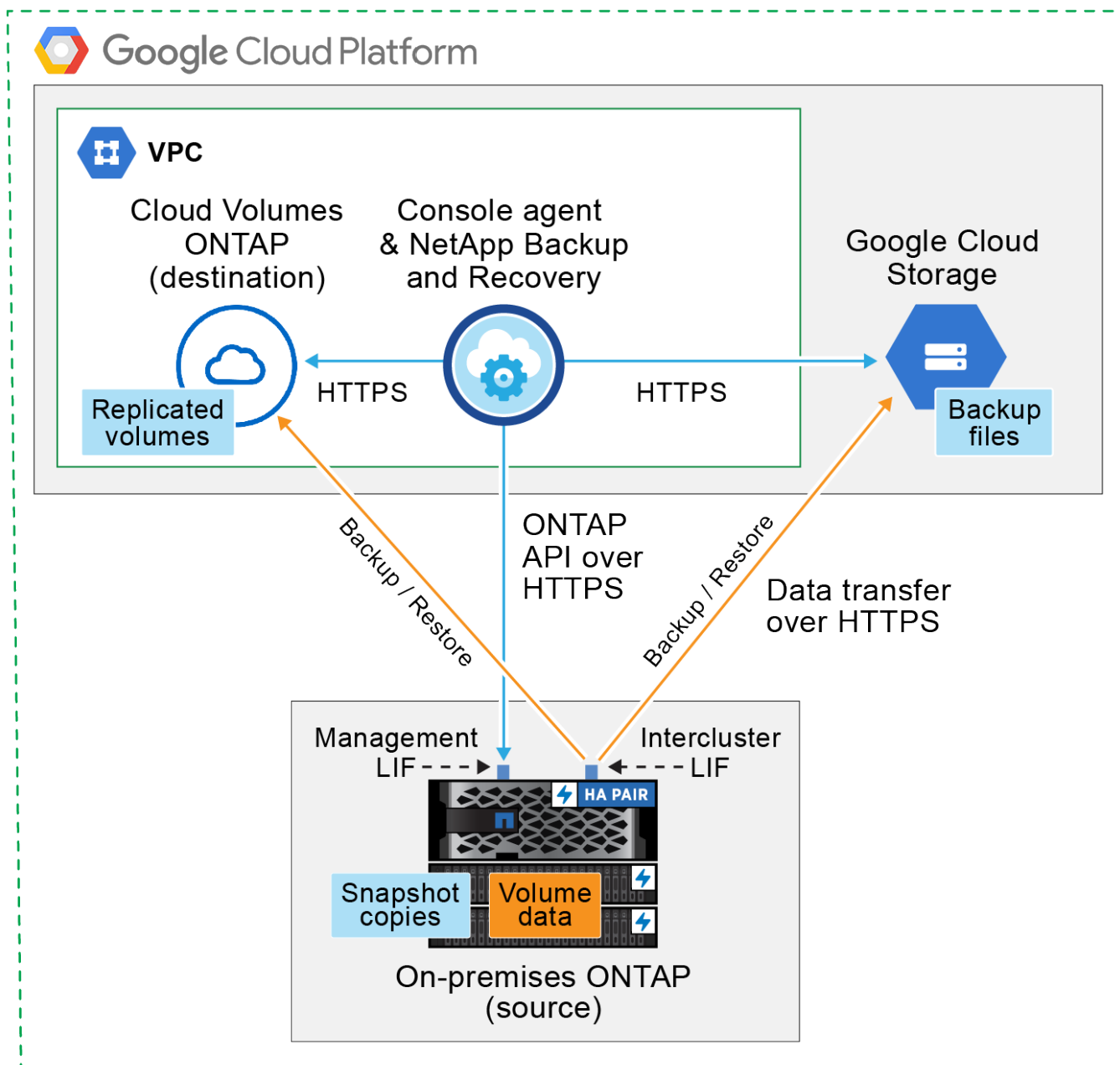
Elija cuál de los dos métodos de conexión utilizará al configurar copias de seguridad de los sistemas ONTAP locales a Google Cloud Storage.

- **Conexión pública:** conecte directamente el sistema ONTAP a Google Cloud Storage mediante un punto final público de Google.
- **Conexión privada:** utilice una VPN o Google Cloud Interconnect y enrute el tráfico a través de una interfaz de acceso privado de Google que utiliza una dirección IP privada.

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

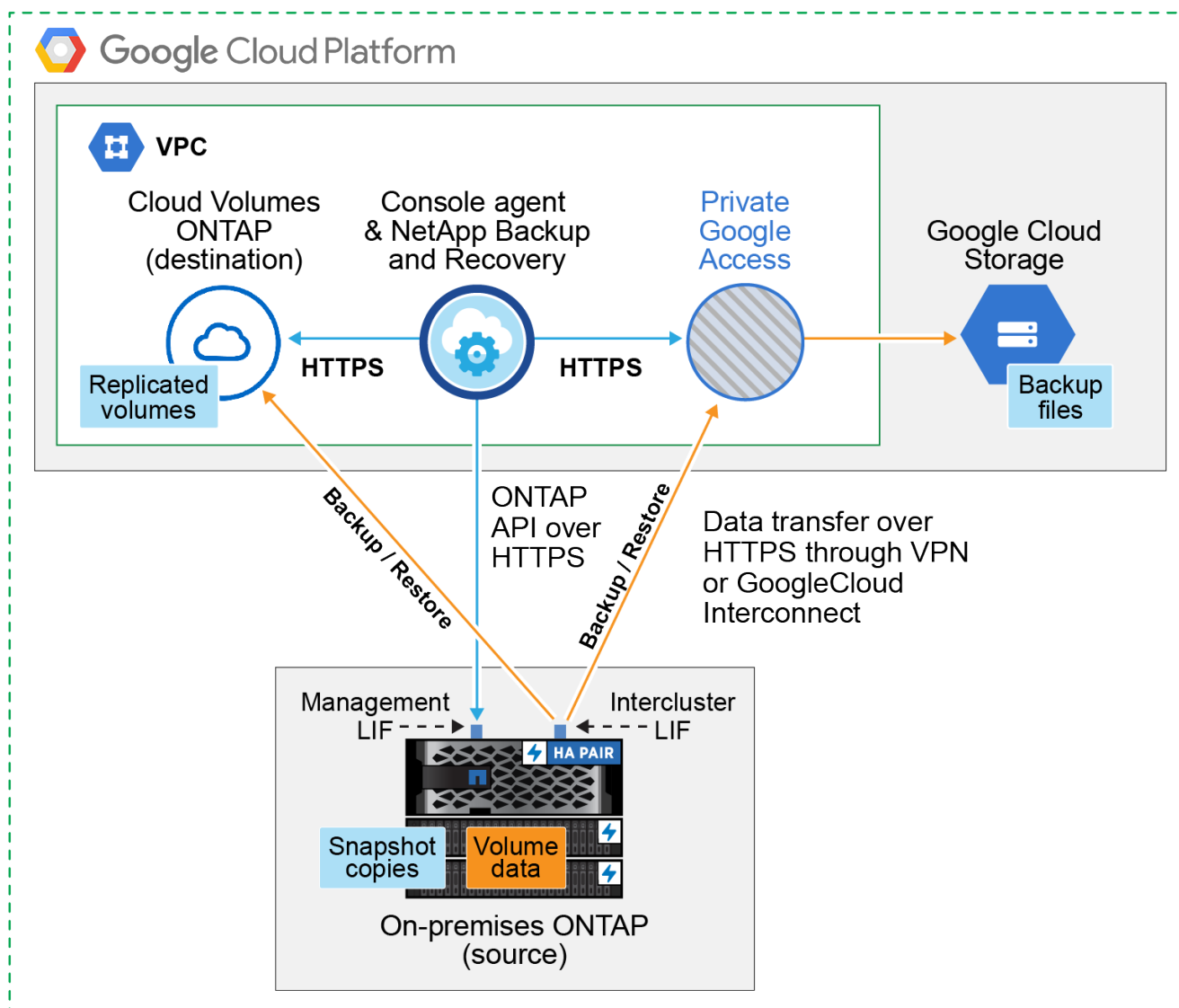
El siguiente diagrama muestra el método de **conexión pública** y las conexiones que debe preparar entre los componentes. El agente de consola debe implementarse en la VPC de Google Cloud Platform.

Console agent deployed in Google Cloud VPC (Public)



El siguiente diagrama muestra el método de **conexión privada** y las conexiones que debe preparar entre los componentes. El agente de consola debe implementarse en la VPC de Google Cloud Platform.

Console agent deployed in Google Cloud VPC (Private)



Prepare su agente de consola

El agente de consola es el software principal para la funcionalidad de la consola. Se requiere un agente de consola para realizar copias de seguridad y restaurar sus datos de ONTAP.

Crear o cambiar agentes de consola

Si ya tienes un agente de consola implementado en tu VPC de Google Cloud Platform, entonces estás listo.

De lo contrario, deberá crear un agente de consola en esa ubicación para realizar una copia de seguridad de los datos de ONTAP en Google Cloud Storage. No puedes usar un agente de consola que esté implementado en otro proveedor de nube o en instalaciones locales.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Instalar un agente de consola en GCP"](#)

Preparar la red para el agente de consola

Asegúrese de que el agente de consola tenga las conexiones de red necesarias.

Pasos

1. Asegúrese de que la red donde está instalado el agente de consola permita las siguientes conexiones:
 - Una conexión HTTPS a través del puerto 443 a NetApp Backup and Recovery y a su almacenamiento de Google Cloud(["ver la lista de puntos finales"](#))
 - Una conexión HTTPS a través del puerto 443 a su LIF de administración de clúster ONTAP
2. Habilite el acceso privado de Google (o la conexión de servicio privada) en la subred donde planea implementar el agente de la consola. ["Acceso privado a Google"](#) o ["Conexión de servicio privado"](#) son necesarios si tiene una conexión directa desde su clúster ONTAP a la VPC y desea que la comunicación entre el agente de la consola y Google Cloud Storage permanezca en su red privada virtual (una conexión **privada**).

Siga las instrucciones de Google para configurar estas opciones de acceso privado. Asegúrese de que sus servidores DNS se hayan configurado para apuntar `www.googleapis.com` y `storage.googleapis.com` a las direcciones IP internas (privadas) correctas.

Verificar o agregar permisos al agente de la consola

Para utilizar la funcionalidad "Buscar y restaurar" de NetApp Backup and Recovery , debe tener permisos específicos en el rol del agente de consola para que pueda acceder al servicio Google Cloud BigQuery. Revise los permisos a continuación y siga los pasos si necesita modificar la política.

Pasos

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

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

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

Verificar los requisitos de la licencia

- Antes de poder activar NetApp Backup and Recovery para su clúster, deberá suscribirse a una oferta de Console Marketplace de pago por uso (PAYGO) de Google o comprar y activar una licencia BYOL de NetApp Backup and Recovery de NetApp. Estas licencias son para su cuenta y se pueden usar en múltiples sistemas.
 - Para obtener la licencia PAYGO de NetApp Backup and Recovery , necesitará una suscripción a ["Oferta de NetApp Console de Google Marketplace"](#) . La facturación de NetApp Backup and Recovery se realiza a través de esta suscripción.
 - Para obtener una licencia BYOL de NetApp Backup and Recovery , necesitará el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#).
- Necesita tener una suscripción a Google para el espacio de almacenamiento de objetos donde se ubicarán sus copias de seguridad.

Regiones compatibles

Puede crear copias de seguridad desde sistemas locales a Google Cloud Storage en todas las regiones. Usted especifica la región donde se almacenarán las copias de seguridad cuando configura el servicio.

Prepare sus clústeres de ONTAP

Prepare su sistema local de origen ONTAP y cualquier sistema local secundario ONTAP o Cloud Volumes ONTAP .

La preparación de sus clústeres ONTAP implica los siguientes pasos:

- Descubra sus sistemas ONTAP en NetApp Console
- Verificar los requisitos del sistema ONTAP
- Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos
- Verificar los requisitos de red de ONTAP para replicar volúmenes

Descubra sus sistemas ONTAP en NetApp Console

Tanto su sistema ONTAP local de origen como cualquier sistema ONTAP local secundario o sistemas Cloud Volumes ONTAP deben estar disponibles en la página **Sistemas** de la NetApp Console .

Necesitará saber la dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para agregar el clúster. ["Aprenda a descubrir un clúster"](#).

Verificar los requisitos del sistema ONTAP

Asegúrese de que su sistema ONTAP cumpla con los siguientes requisitos:

- Mínimo de ONTAP 9.8; se recomienda 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 NetApp Backup and Recovery.

Aprenda cómo ["Administrar sus licencias de clúster"](#) .

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["Configurar el tiempo de su clúster"](#) .
- Si replica datos, verifique que los sistemas de origen y destino ejecuten versiones de ONTAP compatibles.
["Ver versiones de ONTAP compatibles con las relaciones de SnapMirror"](#).

Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos

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

- Para una arquitectura de respaldo en abanico, configure los siguientes ajustes en el sistema *principal*.
- Para una arquitectura de respaldo en cascada, configure los siguientes ajustes en el sistema *secundario*.

Se necesitan los siguientes requisitos de red del clúster ONTAP :

- El clúster ONTAP inicia una conexión HTTPS a través del puerto 443 desde el LIF entre clústeres a Google Cloud Storage para operaciones de respaldo y restauración.

ONTAP lee y escribe datos hacia y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, simplemente responde.

- ONTAP requiere una conexión entrante desde el agente de la consola al LIF de administración del clúster. El agente de la consola puede residir en una VPC de Google Cloud Platform.
- Se requiere un LIF entre clústeres en cada nodo de ONTAP que aloje los volúmenes que desea respaldar. El LIF debe estar asociado con el *IPspace* que ONTAP debe usar para conectarse al almacenamiento de objetos. ["Obtenga más información sobre IPspaces"](#) .

Cuando configura NetApp Backup and Recovery, se le solicita el espacio IP que desea utilizar. Debes elegir el espacio IP con el que está asociado cada LIF. Ese podría ser el espacio IP "predeterminado" o un espacio IP personalizado que usted creó.

- Los LIF entre clústeres de los nodos pueden acceder al almacén de objetos.
- Se han configurado servidores DNS para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Vea cómo ["Configurar servicios DNS para la SVM"](#) .

Si está utilizando Private Google Access o Private Service Connect, asegúrese de que sus servidores DNS estén configurados para apuntar `storage.googleapis.com` a la dirección IP interna (privada) correcta.

- Tenga en cuenta que si utiliza un espacio IP diferente al predeterminado, es posible que necesite crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir conexiones de NetApp Backup and Recovery desde ONTAP al almacenamiento de objetos a través del puerto 443, y tráfico de resolución de nombres desde la máquina virtual de almacenamiento al servidor DNS a través del puerto 53 (TCP/UDP).

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#) .

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo de seguridad predefinido.

Prepare Google Cloud Storage como su destino de respaldo

Para preparar Google Cloud Storage como destino de respaldo, siga estos pasos:

- Configurar permisos.
- (Opcional) Crea tus propios buckets. (El servicio creará depósitos para usted si lo desea).
- (Opcional) Configure claves administradas por el cliente para el cifrado de datos

Configurar permisos

Debe proporcionar claves de acceso de almacenamiento para una cuenta de servicio que tenga permisos específicos mediante un rol personalizado. Una cuenta de servicio permite que NetApp Backup and Recovery autentique y acceda a los depósitos de Cloud Storage que se utilizan para almacenar copias de seguridad. Las claves son necesarias para que Google Cloud Storage sepa quién realiza la solicitud.

Pasos

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

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

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

Necesitará ingresar las claves en NetApp Backup and Recovery más adelante cuando configure el servicio de respaldo.

Crea tus propios cubos

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

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

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

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

Si planea utilizar sus propias claves administradas por el cliente:

- Necesitarás tener el llavero y el nombre de la clave para poder agregar esta información en el asistente de activación. ["Obtenga más información sobre las claves de cifrado administradas por el cliente"](#).
- Deberá verificar que estos permisos requeridos estén incluidos en la función del agente de consola:

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

- Deberá verificar que la API "Cloud Key Management Service (KMS)" de Google esté habilitada en su

proyecto. Ver el ["Documentación de Google Cloud: Habilitación de API"](#) Para más detalles.

Consideraciones sobre CMEK:

- Se admiten claves generadas por software y HSM (respaldadas por hardware).
- Se admiten claves Cloud KMS recién creadas o importadas.
- Solo se admiten claves regionales, no claves globales.
- Actualmente, solo se admite el propósito de "Cifrado/descifrado simétrico".
- NetApp Backup and Recovery asigna el rol de IAM "CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)" al agente de servicio asociado con la cuenta de almacenamiento.

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:

- Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de Google Cloud Storage para sus copias de seguridad existe como en la página **Sistemas** de la consola, puede arrastrar el clúster de ONTAP al almacenamiento de objetos de Google Cloud.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione **Acciones**  **icono y seleccione *Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo "[Activar la copia de seguridad para volúmenes adicionales en el sistema](#)" (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

Si los volúmenes que elige ya tienen políticas de instantáneas o replicación aplicadas, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.

- **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
- **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.

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

- **En cascada:** la información fluye del almacenamiento primario al secundario y del secundario al de objetos.
- **Distribución en abanico:** la información fluye desde el almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

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

- **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.
- **Política de replicación:** elija una política de replicación existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

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

Cree un nuevo depósito o seleccione uno que ya haya creado.



Si desea almacenar archivos de respaldo más antiguos en el almacenamiento de Google Cloud Archive para optimizar aún más los costos, asegúrese de que el depósito tenga la regla de ciclo de vida adecuada.

Introduzca la clave de acceso y la clave secreta de Google Cloud.

- **Clave de cifrado:** si creó una nueva cuenta de almacenamiento de Google Cloud, ingrese la información de la clave de cifrado que le proporcionó el proveedor. Elija si utilizará las claves de

cifrado predeterminadas de Google Cloud o elegirá sus propias claves administradas por el cliente desde su cuenta de Google Cloud para administrar el cifrado de sus datos.



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

Si elige utilizar sus propias claves administradas por el cliente, ingrese el llavero y el nombre de la clave. "[Obtenga más información sobre las claves de cifrado administradas por el cliente](#)".

- **Redes:** Elija el espacio IP.

El espacio IP en el clúster ONTAP donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente.

- **Política de respaldo:** seleccione una política de copia de seguridad en almacenamiento de objetos existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
 - Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
 - Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas en las políticas de replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos del sistema de almacenamiento principal. Las transferencias posteriores contienen copias diferenciales de los datos del sistema de almacenamiento primario contenidos en las instantáneas.

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

Se crea automáticamente un depósito de Google Cloud Storage en la cuenta de servicio indicada por la clave de acceso de Google y la clave secreta ingresadas, y los archivos de respaldo se almacenan allí. Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el "[Página de seguimiento de trabajos](#)".

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Realice una copia de seguridad de los datos locales de ONTAP en ONTAP S3 con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de los datos de volumen de sus sistemas ONTAP locales principales. Puede enviar copias de seguridad a un sistema de almacenamiento ONTAP secundario (un volumen replicado) o a un depósito en un sistema ONTAP configurado como un servidor S3 (un archivo de copia de seguridad), o ambos.

El sistema ONTAP local principal puede ser un sistema FAS, AFF o ONTAP Select . El sistema ONTAP secundario puede ser un ONTAP local o un sistema Cloud Volumes ONTAP . El almacenamiento de objetos puede estar en un sistema ONTAP local o en un sistema Cloud Volumes ONTAP en el que haya habilitado un servidor de almacenamiento de objetos Simple Storage Service (S3).



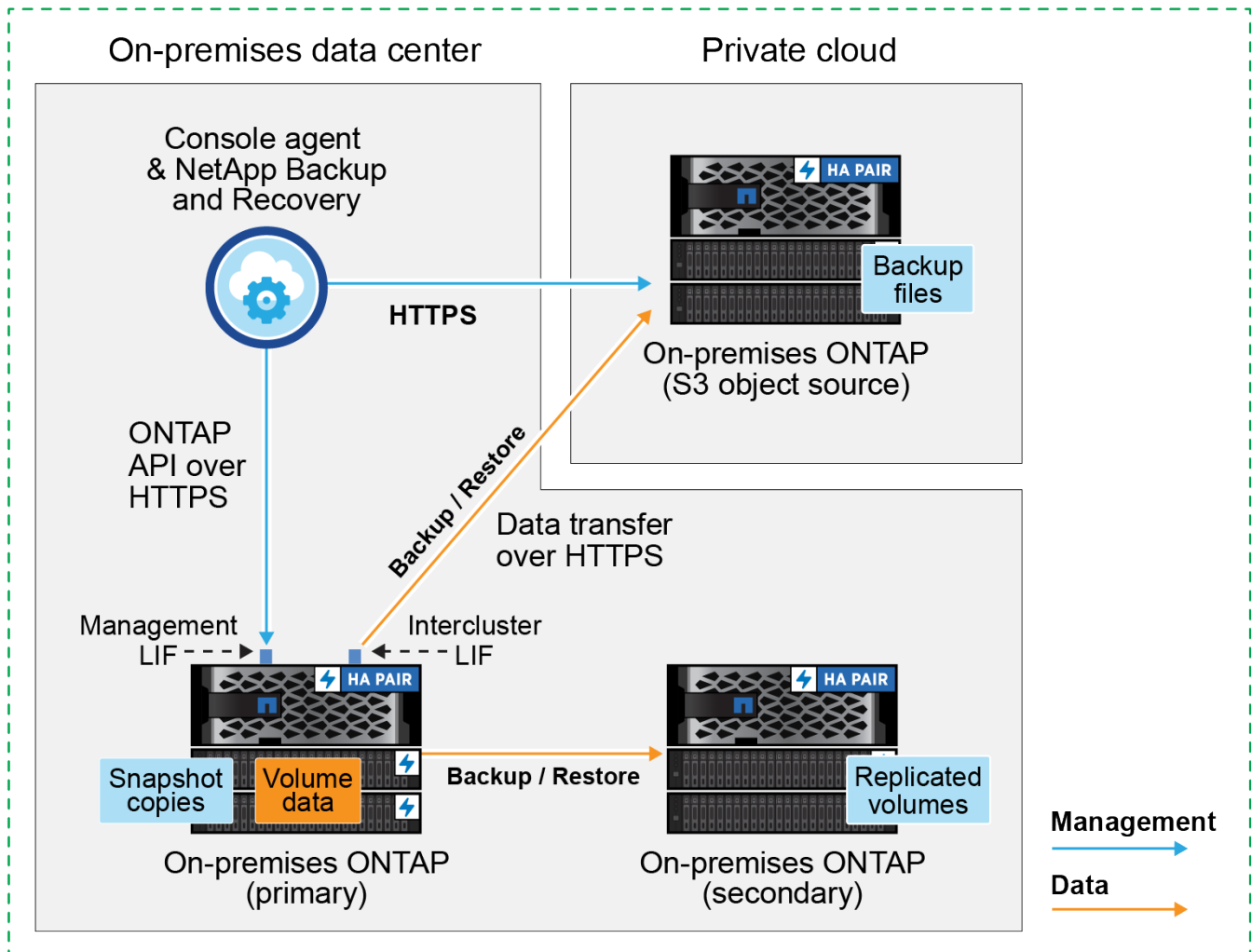
Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

Identificar el método de conexión

Hay muchas configuraciones en las que puedes crear copias de seguridad en un bucket S3 en un sistema ONTAP . A continuación se muestran dos escenarios.

La siguiente imagen muestra cada componente al realizar una copia de seguridad de un sistema ONTAP local principal en un sistema ONTAP local configurado para S3 y las conexiones que debe preparar entre ellos. También muestra una conexión a un sistema ONTAP secundario en la misma ubicación local para replicar volúmenes.

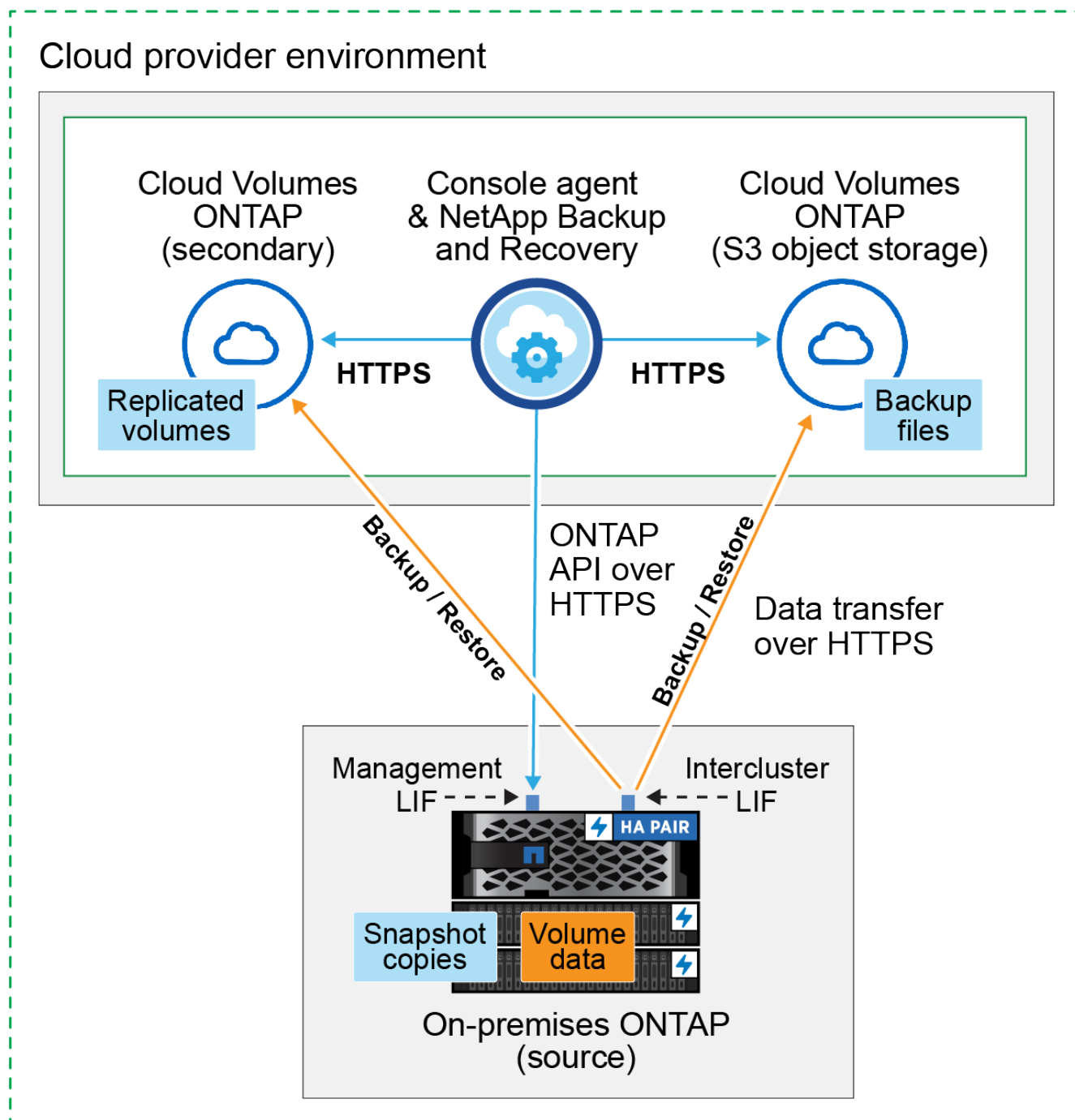
Console agent installed on premises (Public)



Cuando el agente de consola y el sistema ONTAP local principal están instalados en una ubicación local sin acceso a Internet (una implementación en modo "privado"), el sistema ONTAP S3 debe estar ubicado en el mismo centro de datos local.

La siguiente imagen muestra cada componente al realizar una copia de seguridad de un sistema ONTAP local principal en un sistema Cloud Volumes ONTAP configurado para S3 y las conexiones que debe preparar entre ellos. También muestra una conexión a un sistema Cloud Volumes ONTAP secundario en el mismo entorno del proveedor de nube para replicar volúmenes.

Console agent deployed in cloud (Public)



En este escenario, el agente de consola debe implementarse en el mismo entorno del proveedor de nube en el que se implementan los sistemas Cloud Volumes ONTAP .

Prepare su agente de consola

El agente de consola es el software principal para la funcionalidad de la consola. Se requiere un agente de consola para realizar copias de seguridad y restaurar sus datos de ONTAP .

Crear o cambiar agentes de consola

Al realizar una copia de seguridad de los datos en ONTAP S3, debe haber un agente de consola disponible en sus instalaciones o en la nube. Necesitará instalar un nuevo agente de consola o asegurarse de que el agente de consola seleccionado actualmente resida en una de estas ubicaciones. El agente de consola local se puede instalar en un sitio con o sin acceso a Internet.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Instalar el agente de consola en su entorno de nube"](#)
- ["Instalación del agente de consola en un host Linux con acceso a Internet"](#)
- ["Instalación del agente de consola en un host Linux sin acceso a Internet"](#)
- ["Cambiar entre agentes de la consola"](#)

Preparar los requisitos de red del agente de consola

Asegúrese de que la red donde está instalado el agente de consola permita las siguientes conexiones:

- Una conexión HTTPS a través del puerto 443 al servidor ONTAP S3
- Una conexión HTTPS a través del puerto 443 a su LIF de administración del clúster ONTAP de origen
- Una conexión a Internet saliente a través del puerto 443 hacia NetApp Backup and Recovery (no es necesaria cuando el agente de la consola está instalado en un sitio "oscuro")

Consideraciones sobre el modo privado (sitio oscuro)

La funcionalidad de NetApp Backup and Recovery está integrada en el agente de consola. Cuando se instala en modo privado, necesitará actualizar periódicamente el software del agente de la consola para obtener acceso a nuevas funciones. Compruebe el ["Novedades de NetApp Backup and Recovery"](#) para ver las nuevas funciones en cada versión de NetApp Backup and Recovery . Cuando desee utilizar las nuevas funciones, siga los pasos para ["actualizar el software del agente de la consola"](#) .

Cuando utiliza NetApp Backup and Recovery en un entorno SaaS estándar, los datos de configuración de NetApp Backup and Recovery se respaldan en la nube. Cuando utiliza NetApp Backup and Recovery en un sitio sin acceso a Internet, los datos de configuración de NetApp Backup and Recovery se respaldan en el depósito ONTAP S3 donde se almacenan sus copias de seguridad.

Verificar los requisitos de la licencia

Antes de poder activar NetApp Backup and Recovery para su clúster, deberá comprar y activar una licencia BYOL de NetApp Backup and Recovery de NetApp. La licencia es para realizar copias de seguridad y restaurar en almacenamiento de objetos; no se necesita ninguna licencia para crear instantáneas o volúmenes replicados. Esta licencia es para la cuenta y se puede utilizar en múltiples sistemas.

Necesitará el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#).



La licencia PAYGO no es compatible al realizar copias de seguridad de archivos en ONTAP S3.

Prepare sus clústeres de ONTAP

Prepare su sistema local de origen ONTAP y cualquier sistema local secundario ONTAP o Cloud Volumes ONTAP .

La preparación de sus clústeres ONTAP implica los siguientes pasos:

- Descubra sus sistemas ONTAP en NetApp Console
- Verificar los requisitos del sistema ONTAP
- Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos
- Verificar los requisitos de red de ONTAP para replicar volúmenes

Descubra sus sistemas ONTAP en NetApp Console

Tanto su sistema ONTAP local de origen como cualquier sistema ONTAP local secundario o sistemas Cloud Volumes ONTAP deben estar disponibles en la página **Sistemas** de la NetApp Console .

Necesitará saber la dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para agregar el clúster. ["Aprenda a descubrir un clúster"](#).

Verificar los requisitos del sistema ONTAP

Asegúrese de que su sistema ONTAP cumpla con los siguientes requisitos:

- Mínimo de ONTAP 9.8; se recomienda 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 NetApp Backup and Recovery.

Aprenda cómo ["Administrar sus licencias de clúster"](#) .

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo ["Configurar el tiempo de su clúster"](#) .
- Si replica datos, verifique que los sistemas de origen y destino ejecuten versiones de ONTAP compatibles.

["Ver versiones de ONTAP compatibles con las relaciones de SnapMirror"](#).

Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos

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



- Cuando se utiliza una arquitectura de copia de seguridad en abanico, las configuraciones se deben configurar en el sistema de almacenamiento *principal*.
- Cuando se utiliza una arquitectura de copia de seguridad en cascada, las configuraciones se deben configurar en el sistema de almacenamiento *secundario*.

["Obtenga más información sobre los tipos de arquitectura de respaldo"](#).

Se necesitan los siguientes requisitos de red del clúster ONTAP :

- El clúster ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario desde el LIF entre clústeres al servidor ONTAP S3 para operaciones de respaldo y restauración. El puerto se puede

configurar durante la configuración de la copia de seguridad.

ONTAP lee y escribe datos hacia y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, simplemente responde.

- ONTAP requiere una conexión entrante desde el agente de la consola al LIF de administración del clúster.
- Se requiere un LIF entre clústeres en cada nodo de ONTAP que aloje los volúmenes que desea respaldar. El LIF debe estar asociado con el *IPspace* que ONTAP debe usar para conectarse al almacenamiento de objetos. ["Obtenga más información sobre IPspaces"](#) .

Cuando configura NetApp Backup and Recovery, se le solicita el espacio IP que desea utilizar. Debes elegir el espacio IP con el que está asociado cada LIF. Ese podría ser el espacio IP "predeterminado" o un espacio IP personalizado que usted creó.

- Los LIF entre clústeres de los nodos pueden acceder al almacén de objetos (no es necesario cuando el agente de consola está instalado en un sitio "oscuro").
- Se han configurado servidores DNS para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Vea cómo ["Configurar servicios DNS para la SVM"](#) .
- Si utiliza un espacio IP diferente al predeterminado, es posible que necesite crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones del servicio NetApp Backup and Recovery desde ONTAP al almacenamiento de objetos a través del puerto que especificó (normalmente 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).

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#) .

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo de seguridad predefinido.

Prepare ONTAP S3 como su destino de respaldo

Debe habilitar un servidor de almacenamiento de objetos de Servicio de almacenamiento simple (S3) en el clúster de ONTAP que planea usar para las copias de seguridad de almacenamiento de objetos. Ver el ["Documentación de ONTAP S3"](#) Para más detalles.

Nota: Puede agregar este clúster a la página **Sistemas** de la Consola, pero no está identificado como un servidor de almacenamiento de objetos S3 y no puede arrastrar y soltar un sistema de origen en este sistema S3 para iniciar la activación de la copia de seguridad.

Este sistema ONTAP debe cumplir los siguientes requisitos.

Versiones de ONTAP compatibles

Se requiere ONTAP 9.8 y versiones posteriores para los sistemas ONTAP locales. Se requiere ONTAP 9.9.1 y versiones posteriores para los sistemas Cloud Volumes ONTAP .

Credenciales S3

Debe haber creado un usuario S3 para controlar el acceso a su almacenamiento ONTAP S3. ["Consulte la documentación de ONTAP S3 para obtener más detalles."](#) .

Cuando configura la copia de seguridad en ONTAP S3, el asistente de copia de seguridad le solicita una clave de acceso S3 y una clave secreta para una cuenta de usuario. La cuenta de usuario permite que NetApp Backup and Recovery autentique y acceda a los depósitos ONTAP S3 utilizados para almacenar copias de seguridad. Las claves son necesarias para que ONTAP S3 sepa quién está realizando 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",
"s3:GetBucketLocation"
```

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- Seleccione los volúmenes que desea respaldar
- Definir la estrategia y las políticas de backup
- Revise sus selecciones

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:
 - Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes**

de respaldo junto a Copia de seguridad y recuperación en el panel derecho.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione la opción **Acciones (...)** y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si no tiene un agente de consola, aparece la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación y política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo "[Activar la copia de seguridad para volúmenes adicionales en el sistema](#)" (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

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

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Opciones de protección: si desea implementar una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura: si desea utilizar una arquitectura de respaldo en cascada o en abanico

- Política de instantáneas locales
- Objetivo y política de replicación
- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** Crea instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza una copia de seguridad de los volúmenes en un depósito en un sistema ONTAP configurado para S3.
2. **Arquitectura:** Si eligió tanto la replicación como la copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** los datos de respaldo fluyen del sistema principal al secundario y luego del secundario al almacenamiento de objetos.
 - **Distribución en abanico:** los datos de respaldo fluyen desde el sistema principal al secundario y desde el principal al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una nueva.



Si desea crear una política personalizada antes de activar la instantánea, puede usar el Administrador del sistema o la CLI de ONTAP `snapmirror policy create dominio`. Referirse a .



Para crear una política personalizada mediante Copia de seguridad y recuperación, consulte ["Crear una política"](#) .

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la política.
 - Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
 - Seleccione **Crear**.
4. **Replicación:** Si seleccionó **Replicación**, configure las siguientes opciones:
 - **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado de destino (o agregados para volúmenes FlexGroup) y un prefijo o sufijo que se agregará al nombre del volumen replicado.
 - **Política de replicación:** elija una política de replicación existente o cree una nueva.

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

- **Proveedor:** Seleccione * ONTAP S3*.
- **Configuración del proveedor:** ingrese los detalles del FQDN del servidor S3, el puerto y la clave de acceso y la clave secreta de los usuarios.

La clave de acceso y la clave secreta son para el usuario que usted creó para otorgarle al clúster ONTAP acceso al bucket S3.

- **Redes:** elija el espacio IP en el clúster ONTAP de origen donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente (no es necesario cuando el agente de consola está instalado en un sitio "oscuro").



Seleccionar el espacio IP correcto garantiza que NetApp Backup and Recovery pueda configurar una conexión desde ONTAP a su almacenamiento de objetos ONTAP S3.

- **Política de respaldo:** seleccione una política de respaldo existente o cree una nueva.



Puede crear una política con el Administrador del sistema o la CLI de ONTAP . Para crear una política personalizada mediante la CLI de ONTAP `snapmirror policy create` comando, referirse a .



Para crear una política personalizada mediante Copia de seguridad y recuperación, consulte "[Crear una política](#)" .

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte "[Configuración de la política de copia de seguridad en objeto](#)" .
- Seleccione **Crear**.
- **Exportar instantáneas existentes al almacenamiento de objetos como archivos de copia de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de

seguridad. Si las políticas no coinciden, no se crearán copias de seguridad.

3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos de almacenamiento primario contenidos en las instantáneas.

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

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta ingresada, y los archivos de respaldo se almacenan allí.

Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el "[Página de seguimiento de trabajos](#)".

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Realice copias de seguridad de los datos locales de ONTAP en StorageGRID con NetApp Backup and Recovery

Complete algunos pasos en NetApp Backup and Recovery para comenzar a realizar copias de seguridad de datos de volumen desde sus sistemas ONTAP principales locales a un sistema de almacenamiento secundario y al almacenamiento de objetos en sus sistemas NetApp StorageGRID .



Los "sistemas ONTAP locales" incluyen los sistemas FAS, AFF y ONTAP Select .



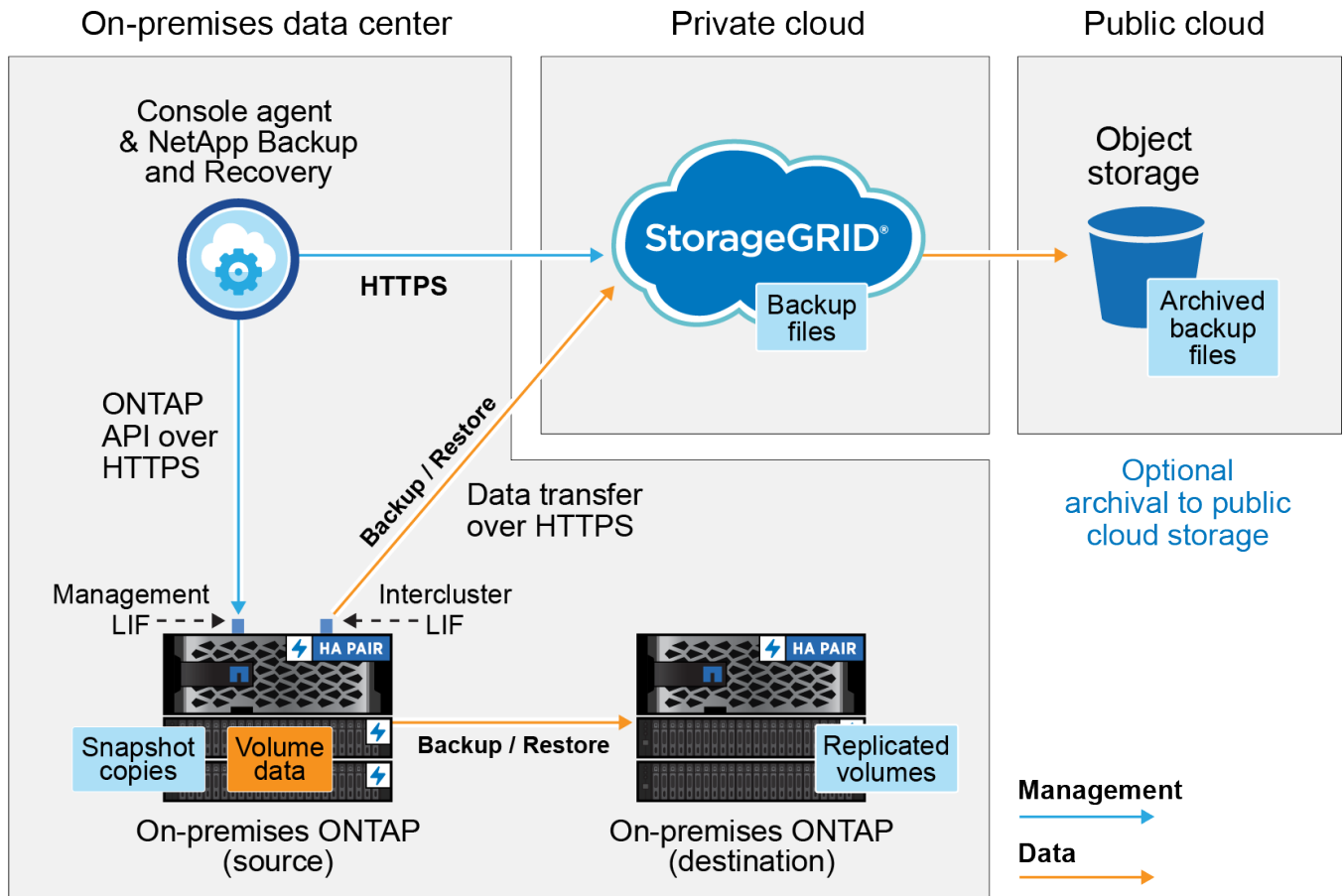
Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

Identificar el método de conexión

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

Opcionalmente, puede conectarse a un sistema ONTAP secundario en la misma ubicación local para replicar

volúmenes.



Cuando el agente de consola y el sistema ONTAP local están instalados en una ubicación local sin acceso a Internet (un "sitio oscuro"), el sistema StorageGRID debe estar ubicado en el mismo centro de datos local. El archivado de archivos de respaldo antiguos en la nube pública no es compatible con configuraciones de sitios oscuros.

Prepare su agente de consola

El agente de consola es el software principal para la funcionalidad de la consola. Se requiere un agente de consola para realizar copias de seguridad y restaurar sus datos de ONTAP .

Crear o cambiar agentes de consola

Al realizar una copia de seguridad de datos en StorageGRID, debe haber un agente de consola disponible en sus instalaciones. Necesitará instalar un nuevo agente de consola o asegurarse de que el agente de consola seleccionado actualmente resida localmente. El agente de consola se puede instalar en un sitio con o sin acceso a Internet.

- ["Obtenga más información sobre los agentes de consola"](#)
- ["Instalación del agente de consola en un host Linux con acceso a Internet"](#)
- ["Instalación del agente de consola en un host Linux sin acceso a Internet"](#)
- ["Cambiar entre agentes de la consola"](#)

Preparar los requisitos de red del agente de consola

Asegúrese de que la red donde está instalado el agente de consola permita las siguientes conexiones:

- Una conexión HTTPS a través del puerto 443 al nodo de puerta de enlace de StorageGRID
- Una conexión HTTPS a través del puerto 443 a su LIF de administración de clúster ONTAP
- Una conexión a Internet saliente a través del puerto 443 hacia NetApp Backup and Recovery (no es necesaria cuando el agente de la consola está instalado en un sitio "oscuro")

Consideraciones sobre el modo privado (sitio oscuro)

- La funcionalidad de NetApp Backup and Recovery está integrada en el agente de consola. Cuando se instala en modo privado, necesitará actualizar periódicamente el software del agente de la consola para obtener acceso a nuevas funciones. Compruebe el ["Novedades de NetApp Backup and Recovery"](#) para ver las nuevas funciones en cada versión de NetApp Backup and Recovery . Cuando desee utilizar las nuevas funciones, siga los pasos para ["actualizar el software del agente de la consola"](#) .

La nueva versión de NetApp Backup and Recovery , que incluye la capacidad de programar y crear instantáneas y volúmenes replicados, además de crear copias de seguridad en almacenamiento de objetos, requiere que utilice la versión 3.9.31 o superior del agente de consola. Por lo tanto, se recomienda que obtenga esta última versión para administrar todas sus copias de seguridad.

- Cuando utiliza NetApp Backup and Recovery en un entorno SaaS, los datos de configuración de NetApp Backup and Recovery se respaldan en la nube. Cuando utiliza NetApp Backup and Recovery en un sitio sin acceso a Internet, los datos de configuración de NetApp Backup and Recovery se respaldan en el depósito StorageGRID donde se almacenan sus copias de seguridad.

Verificar los requisitos de la licencia

Antes de poder activar NetApp Backup and Recovery para su clúster, deberá comprar y activar una licencia BYOL de NetApp Backup and Recovery de NetApp. Esta licencia es para la cuenta y se puede utilizar en múltiples sistemas.

Necesitará el número de serie de NetApp que le permite utilizar el servicio durante la duración y la capacidad de la licencia. ["Aprenda a administrar sus licencias BYOL"](#).



La licencia PAYGO no es compatible al realizar copias de seguridad de archivos en StorageGRID.

Prepare sus clústeres de ONTAP

Prepare su sistema local de origen ONTAP y cualquier sistema local secundario ONTAP o Cloud Volumes ONTAP .

La preparación de sus clústeres ONTAP implica los siguientes pasos:

- Descubra sus sistemas ONTAP en NetApp Console
- Verificar los requisitos del sistema ONTAP
- Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos
- Verificar los requisitos de red de ONTAP para replicar volúmenes

Descubra sus sistemas ONTAP en NetApp Console

Tanto su sistema ONTAP local de origen como cualquier sistema ONTAP local secundario o sistemas Cloud Volumes ONTAP deben estar disponibles en la página **Sistemas** de la NetApp Console .

Necesitará saber la dirección IP de administración del clúster y la contraseña de la cuenta de usuario administrador para agregar el clúster. "[Aprenda a descubrir un clúster](#)".

Verificar los requisitos del sistema ONTAP

Asegúrese de que su sistema ONTAP cumpla con los siguientes requisitos:

- Mínimo de ONTAP 9.8; se recomienda 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 NetApp Backup and Recovery.

Aprenda cómo "[Administrar sus licencias de clúster](#)".

- La hora y la zona horaria están configuradas correctamente. Aprenda cómo "[Configurar el tiempo de su clúster](#)".
- Si replica datos, verifique que los sistemas de origen y destino ejecuten versiones de ONTAP compatibles.

"[Ver versiones de ONTAP compatibles con las relaciones de SnapMirror](#)".

Verificar los requisitos de red de ONTAP para realizar copias de seguridad de datos en el almacenamiento de objetos

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

- Cuando se utiliza una arquitectura de respaldo en abanico, se deben configurar los siguientes ajustes en el sistema de almacenamiento *principal*.
- Cuando se utiliza una arquitectura de copia de seguridad en cascada, se deben configurar los siguientes ajustes en el sistema de almacenamiento *secundario*.

Se necesitan los siguientes requisitos de red del clúster ONTAP :

- El clúster ONTAP inicia una conexión HTTPS a través de un puerto especificado por el usuario desde el LIF entre clústeres al nodo de puerta de enlace de StorageGRID para operaciones de respaldo y restauración. El puerto se puede configurar durante la configuración de la copia de seguridad.

ONTAP lee y escribe datos hacia y desde el almacenamiento de objetos. El almacenamiento de objetos nunca se inicia, simplemente responde.

- ONTAP requiere una conexión entrante desde el agente de la consola al LIF de administración del clúster. El agente de la consola debe residir en sus instalaciones.
- Se requiere un LIF entre clústeres en cada nodo de ONTAP que aloje los volúmenes que desea respaldar. El LIF debe estar asociado con el *IPspace* que ONTAP debe usar para conectarse al almacenamiento de objetos. "[Obtenga más información sobre IPspaces](#)".

Cuando configura NetApp Backup and Recovery, se le solicita el espacio IP que desea utilizar. Debes elegir el espacio IP con el que está asociado cada LIF. Ese podría ser el espacio IP "predeterminado" o un

espacio IP personalizado que usted creó.

- Los LIF entre clústeres de los nodos pueden acceder al almacén de objetos (no es necesario cuando el agente de consola está instalado en un sitio "oscuro").
- Se han configurado servidores DNS para la máquina virtual de almacenamiento donde se encuentran los volúmenes. Vea cómo ["Configurar servicios DNS para la SVM"](#) .
- Si utiliza un espacio IP diferente al predeterminado, es posible que necesite crear una ruta estática para obtener acceso al almacenamiento de objetos.
- Actualice las reglas de firewall, si es necesario, para permitir las conexiones del servicio NetApp Backup and Recovery desde ONTAP al almacenamiento de objetos a través del puerto que especificó (normalmente 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).

Verificar los requisitos de red de ONTAP para replicar volúmenes

Si planea crear volúmenes replicados en un sistema ONTAP secundario mediante NetApp Backup and Recovery, asegúrese de que los sistemas de origen y destino cumplan con los siguientes requisitos de red.

Requisitos de red de ONTAP local

- Si el clúster está local, debe tener una conexión desde su red corporativa a su red virtual en el proveedor de la nube. Normalmente se trata de una conexión VPN.
- Los clústeres ONTAP deben cumplir requisitos adicionales de subred, puerto, firewall y clúster.

Dado que puede replicar en Cloud Volumes ONTAP o en sistemas locales, revise los requisitos de emparejamiento para los sistemas ONTAP locales. ["Consulte los requisitos previos para el peering de clústeres en la documentación de ONTAP"](#) .

Requisitos de red de Cloud Volumes ONTAP

- El grupo de seguridad de la instancia debe incluir las reglas de entrada y salida requeridas: específicamente, reglas para ICMP y los puertos 11104 y 11105. Estas reglas están incluidas en el grupo de seguridad predefinido.

Prepare StorageGRID como su destino de respaldo

StorageGRID debe cumplir los siguientes requisitos. Ver el ["Documentación de StorageGRID"](#) Para más información.

Para obtener detalles sobre los requisitos de DataLock y Ransomware Resilience para StorageGRID, consulte ["Opciones de política de copia de seguridad a objeto"](#) .

Versiones de StorageGRID compatibles

Se admite StorageGRID 10.3 y versiones posteriores.

Para utilizar DataLock y Ransomware Resilience en sus copias de seguridad, sus sistemas StorageGRID deben ejecutar la versión 11.6.0.3 o superior.

Para almacenar copias de seguridad antiguas en un sistema de archivo en la nube, sus sistemas StorageGRID deben ejecutar la versión 11.3 o superior. Además, sus sistemas StorageGRID deben ser detectados en la página **Sistemas** de la consola.

Para el almacenamiento de archivos del usuario, se necesita acceso a la IP del nodo de administrador.

Siempre se necesita acceso a IP de puerta de enlace.

Credenciales S3

Debe haber creado una cuenta de inquilino S3 para controlar el acceso a su almacenamiento StorageGRID . ["Consulte la documentación de StorageGRID para obtener más detalles."](#) .

Cuando configura la copia de seguridad en StorageGRID, el asistente de copia de seguridad le solicita una clave de acceso S3 y una clave secreta para una cuenta de inquilino. La cuenta de inquilino permite que NetApp Backup and Recovery autentique y acceda a los depósitos StorageGRID utilizados para almacenar copias de seguridad. Las claves son necesarias para que StorageGRID sepa quién está realizando 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 depósito de almacenamiento de objetos.

Prepárese para archivar archivos de respaldo antiguos en un almacenamiento en la nube pública

Agrupar los archivos de respaldo más antiguos en un almacenamiento de archivo le permite ahorrar dinero al utilizar una clase de almacenamiento menos costosa para respaldos que quizás no necesite. StorageGRID es una solución local (nube privada) que no proporciona almacenamiento de archivo, pero puede mover archivos de respaldo más antiguos al almacenamiento de archivo en la nube pública. Cuando se usa de esta manera, los datos almacenados en la nube o restaurados desde el almacenamiento en la nube van entre StorageGRID y el almacenamiento en la nube; la consola no participa en esta transferencia de datos.

El soporte actual le permite archivar copias de seguridad en el almacenamiento de AWS *S3 Glacier*/S3 *Glacier Deep Archive* o *Azure Archive*.

*Requisitos de ONTAP *

- Su clúster debe utilizar ONTAP 9.12.1 o superior.
- Requisitos de StorageGRID *
- Su StorageGRID debe utilizar 11.4 o superior.
- Su StorageGRID debe ser ["Descubierto y disponible en la consola"](#) .

Requisitos de Amazon S3

- Necesitará registrarse en una cuenta de Amazon S3 para el espacio de almacenamiento donde se ubicarán sus copias de seguridad archivadas.

- Puede optar por organizar las copias de seguridad en niveles de almacenamiento AWS S3 Glacier o S3 Glacier Deep Archive. ["Obtenga más información sobre los niveles de archivo de AWS"](#).
- StorageGRID debe tener acceso de control total al depósito(s3:*); sin embargo, si esto no es posible, la política del bucket debe otorgar 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

- Necesitará registrarse para obtener una suscripción de Azure para el espacio de almacenamiento donde se ubicarán sus copias de seguridad archivadas.
- El asistente de activación le permite utilizar un grupo de recursos existente para administrar el contenedor de blobs que almacenará las copias de seguridad, o puede crear un nuevo grupo de recursos.

Al definir la configuración de archivo para la política de respaldo de su clúster, ingresará las credenciales de su proveedor de nube y seleccionará la clase de almacenamiento que desea usar. NetApp Backup and Recovery crea el depósito en la nube cuando activa la copia de seguridad para el clúster. La información necesaria para el almacenamiento de archivo de AWS y Azure se muestra a continuación.

AWS	Azure
☒ Tier Backups to Archive Cloud Provider AWS	☒ Tier Backups to Archive Cloud Provider AZURE
Account Select Account	Azure Subscription Select Account
Region Select Region	Region Select Region
AWS Access Key Enter AWS Access Key	Resource Group Type Select an Existing Resource Group
AWS Secret Key Enter AWS Secret Key	Resource Group Select Resource Group
Archive After (Days) (1-999)	Archive After (Days) (1-999)
Storage Class S3 Glacier	Storage Class Azure Archive

Las configuraciones de política de archivo que seleccione generarán una política de administración del ciclo de vida de la información (ILM) en StorageGRID y agregarán las configuraciones como "reglas".

- Si existe una política ILM activa, se agregarán nuevas reglas a la política ILM para mover los datos al nivel de archivo.
- Si existe una política ILM en el estado "propuesto", no será posible crear ni activar una nueva política ILM. ["Obtenga más información sobre las políticas y reglas de StorageGRID ILM"](#).

Activar copias de seguridad en sus volúmenes ONTAP

Active las copias de seguridad en cualquier momento directamente desde su sistema local.

Un asistente lo guiará a través de los siguientes pasos principales:

- [Seleccione los volúmenes que desea respaldar](#)
- [Definir la estrategia de backup](#)
- [Revise sus selecciones](#)

También puedes [Mostrar los comandos API](#) en el paso de revisión, para que pueda copiar el código para automatizar la activación de la copia de seguridad para sistemas futuros.

Iniciar el asistente

Pasos

1. Acceda al asistente para activar copias de seguridad y recuperación mediante una de las siguientes maneras:

- Desde la página **Sistemas** de la Consola, seleccione el sistema y seleccione **Habilitar > Volúmenes de respaldo** junto a Copia de seguridad y recuperación en el panel derecho.

Si el destino de sus copias de seguridad existe como un sistema en la página **Sistemas** de la Consola, puede arrastrar el clúster ONTAP al almacenamiento de objetos.

- Seleccione **Volúmenes** en la barra de Copia de seguridad y recuperación. Desde la pestaña Volúmenes, seleccione la opción **Acciones (...)** y seleccione **Activar copia de seguridad** para un solo volumen (que aún no tenga habilitada la replicación o la copia de seguridad en el almacenamiento de objetos).

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

2. Continúe con las siguientes opciones:

- Si ya tienes un agente de consola, ya estás listo. Simplemente seleccione **Siguiente**.
- Si aún no tiene un agente de consola, aparecerá la opción **Agregar un agente de consola**. Referirse a [Prepare su agente de consola](#).

Seleccione los volúmenes que desea respaldar

Seleccione los volúmenes que desea proteger. Un volumen protegido es aquel que tiene una o más de las siguientes opciones: política de instantáneas, política de replicación, política de copia de seguridad a objeto.

Puede elegir proteger los volúmenes FlexVol o FlexGroup ; sin embargo, no puede seleccionar una combinación de estos volúmenes al activar la copia de seguridad de un sistema. Vea cómo ["Activar la copia de seguridad para volúmenes adicionales en el sistema"](#) (FlexVol o FlexGroup) después de haber configurado la copia de seguridad para los volúmenes iniciales.



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

Pasos

Si los volúmenes que elige ya tienen políticas de instantáneas o replicación aplicadas, las políticas que seleccione más adelante sobrescribirán estas políticas existentes.

1. En la página Seleccionar volúmenes, seleccione el volumen o los volúmenes que desea proteger.
 - Opcionalmente, filtre las filas para mostrar solo volúmenes con determinados tipos de volumen, estilos y más para facilitar la selección.
 - Después de seleccionar el primer volumen, puede seleccionar todos los volúmenes FlexVol (los volúmenes FlexGroup se pueden seleccionar uno a la vez solamente). Para realizar una copia de seguridad de todos los volúmenes FlexVol existentes, marque primero un volumen y luego marque la casilla en la fila del título.
 - Para realizar una copia de seguridad de volúmenes individuales, marque la casilla de cada volumen.
2. Seleccione **Siguiente**.

Definir la estrategia de backup

Definir la estrategia de backup implica configurar las siguientes opciones:

- Ya sea que desee una o todas las opciones de respaldo: instantáneas locales, replicación y respaldo en almacenamiento de objetos
- Arquitectura
- Política de instantáneas locales
- Objetivo y política de replicación



Si los volúmenes que elige tienen políticas de instantáneas y replicación diferentes a las políticas que selecciona en este paso, se sobrescribirán las políticas existentes.

- Realizar copias de seguridad de la información de almacenamiento de objetos (proveedor, cifrado, redes, política de copia de seguridad y opciones de exportación).

Pasos

1. En la página Definir estrategia de respaldo, elija una o todas las siguientes opciones. Los tres están seleccionados por defecto:
 - **Instantáneas locales:** si está realizando una replicación o una copia de seguridad en un almacenamiento de objetos, se deben crear instantáneas locales.
 - **Replicación:** crea volúmenes replicados en otro sistema de almacenamiento ONTAP .
 - **Copia de seguridad:** realiza copias de seguridad de los volúmenes en el almacenamiento de objetos.
2. **Arquitectura:** Si eligió tanto la replicación como la copia de seguridad, elija uno de los siguientes flujos de información:
 - **En cascada:** la información fluye del almacenamiento primario al secundario y luego del secundario al de objetos.
 - **Distribución en abanico:** la información fluye desde el almacenamiento primario al secundario y desde el primario al almacenamiento de objetos.

Para obtener detalles sobre estas arquitecturas, consulte ["Planifique su viaje de protección"](#) .

3. **Instantánea local:** elija una política de instantáneas existente o cree una nueva.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

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

- **Objetivo de replicación:** seleccione el sistema de destino y SVM. Opcionalmente, seleccione el agregado o los agregados de destino y el prefijo o sufijo que se agregarán al nombre del volumen replicado.
- **Política de replicación:** elija una política de replicación existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

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

5. **Copia de seguridad del objeto:** si seleccionó **Copia de seguridad**, configure las siguientes opciones:

- **Proveedor:** Seleccione * StorageGRID*.
- **Configuración del proveedor:** Ingrese los detalles del FQDN del nodo de puerta de enlace del proveedor, el puerto, la clave de acceso y la clave secreta.

La clave de acceso y la clave secreta son para el usuario de IAM que creó para otorgarle al clúster de ONTAP acceso al depósito.

- **Redes:** elija el espacio IP en el clúster ONTAP donde residen los volúmenes que desea respaldar. Los LIF entre clústeres para este espacio IP deben tener acceso a Internet saliente (no es necesario cuando el agente de consola está instalado en un sitio "oscuro").



Seleccionar el espacio IP correcto garantiza que NetApp Backup and Recovery pueda configurar una conexión desde ONTAP a su almacenamiento de objetos StorageGRID .

- **Política de respaldo:** seleccione una política de respaldo en almacenamiento de objetos existente o cree una.



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

Para crear una política, seleccione **Crear nueva política** y haga lo siguiente:

- Introduzca el nombre de la póliza.
- Seleccione hasta cinco horarios, normalmente de diferentes frecuencias.
- Para las políticas de copia de seguridad a objeto, configure las configuraciones DataLock y Ransomware Resilience. Para obtener más detalles sobre DataLock y Ransomware Resilience, consulte ["Configuración de la política de copia de seguridad en objeto"](#) .

Si su clúster utiliza ONTAP 9.11.1 o superior, puede optar por proteger sus copias de seguridad contra eliminación y ataques de ransomware configurando *DataLock* y *Ransomware Resilience*. *DataLock* protege sus archivos de respaldo para que no se modifiquen ni eliminen, y *Ransomware Resilience* escanea sus archivos de respaldo para buscar evidencia de un ataque de ransomware en ellos.

- Seleccione **Crear**.

Si su clúster usa ONTAP 9.12.1 o superior y su sistema StorageGRID usa la versión 11.4 o superior, puede elegir agrupar las copias de seguridad más antiguas en niveles de archivo de nube pública después de una cierta cantidad de días. El soporte actual es para niveles de almacenamiento de AWS S3 Glacier/S3 Glacier Deep Archive o Azure Archive. [Vea cómo configurar sus sistemas para esta funcionalidad](#).

- **Copia de seguridad por niveles en la nube pública:** seleccione el proveedor de la nube al que desea realizar las copias de seguridad por niveles e ingrese los detalles del proveedor.

Seleccione o cree un nuevo clúster StorageGRID . Para obtener detalles sobre cómo crear un clúster StorageGRID para que la consola pueda detectarlo, consulte "[Documentación de StorageGRID](#)".

- **Exportar instantáneas existentes al almacenamiento de objetos como copias de seguridad:** Si existen instantáneas locales para volúmenes en este sistema que coincidan con la etiqueta de programación de copias de seguridad que acaba de seleccionar para este sistema (por ejemplo, diaria, semanal, etc.), se mostrará este mensaje adicional. Marque esta casilla para que todas las instantáneas históricas se copien en el almacenamiento de objetos como archivos de respaldo para garantizar la protección más completa para sus volúmenes.

6. Seleccione **Siguiente**.

Revise sus selecciones

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

Pasos

1. En la página Revisar, revise sus selecciones.
2. Opcionalmente, marque la casilla para **Sincronizar automáticamente las etiquetas de la política de instantáneas con las etiquetas de la política de replicación y copia de seguridad**. Esto crea instantáneas con una etiqueta que coincide con las etiquetas de las políticas de replicación y copia de seguridad.
3. Seleccione **Activar copia de seguridad**.

Resultado

NetApp Backup and Recovery comienza a realizar las copias de seguridad iniciales de sus volúmenes. La transferencia de línea base del volumen replicado y el archivo de respaldo incluye una copia completa de los datos de origen. Las transferencias posteriores contienen copias diferenciales de los datos de almacenamiento primario contenidos en las instantáneas.

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

Se crea un bucket S3 en la cuenta de servicio indicada por la clave de acceso S3 y la clave secreta ingresada, y los archivos de respaldo se almacenan allí.

Se muestra el panel de control de copias de seguridad de volumen para que pueda supervisar el estado de las copias de seguridad.

También puede supervisar el estado de los trabajos de copia de seguridad y restauración mediante el ["Página de seguimiento de trabajos"](#) .

Mostrar los comandos API

Es posible que desee mostrar y, opcionalmente, copiar los comandos API utilizados en el asistente Activar copia de seguridad y recuperación. Es posible que desee hacer esto para automatizar la activación de la copia de seguridad en sistemas futuros.

Pasos

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

Migrar volúmenes mediante SnapMirror a Cloud Resync en NetApp Backup and Recovery

La función SnapMirror to Cloud Resync de NetApp Backup and Recovery optimiza la protección y la continuidad de los datos durante las migraciones de volumen en entornos de NetApp . Cuando se migra un volumen mediante SnapMirror Logical Replication (LRSE) desde una implementación local de NetApp a otra, o a una solución basada en la nube como Cloud Volumes ONTAP, SnapMirror to Cloud Resync garantiza que las copias de seguridad existentes en la nube permanezcan intactas y operativas.

Esta función elimina la necesidad de un proceso de re-línea base y permite que las copias de seguridad continúen después de la migración. Esta característica es valiosa en escenarios de migración de carga de trabajo, ya que admite tanto FlexVols como FlexGroups y está disponible a partir de la versión 9.16.1 de ONTAP .



Esta función está disponible a partir de la versión 4.0.3 de NetApp Backup and Recovery, lanzada en mayo de 2025.

SnapMirror to Cloud Resync mantiene la continuidad de las copias de seguridad en todos los entornos, lo que facilita la gestión de datos en configuraciones híbridas y multi-nube.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Antes de empezar

Asegúrese de que se cumplan estos requisitos previos:

- El clúster ONTAP de destino debe ejecutar ONTAP versión 9.16.1 o posterior.
- El antiguo clúster ONTAP de origen debe protegerse mediante NetApp Backup and Recovery.
- La función de resincronización de SnapMirror a la nube está disponible a partir de la versión 4.0.3 de NetApp Backup and Recovery, lanzada en mayo de 2025.
- Asegúrese de que la copia de seguridad más reciente en el almacenamiento de objetos sea la instantánea común entre la fuente antigua, la fuente nueva y el almacenamiento de objetos. No utilice una instantánea común que sea más antigua que la última instantánea de la que se haya realizado una copia de seguridad en el almacenamiento de objetos.

- Tanto las políticas de instantánea como las de SnapMirror utilizadas en el clúster ONTAP anterior deben crearse en el nuevo clúster ONTAP antes de iniciar la operación de resincronización. Si utiliza alguna política en el proceso de resincronización, también deberá crear esa política. La operación de resincronización no crea políticas.
- Asegúrese de que la política de SnapMirror que se aplica a la relación de SnapMirror del volumen de migración incluya la misma etiqueta que utiliza la relación de nube. Para evitar problemas, utilice la política que rige un reflejo exacto del volumen y todas las instantáneas.



Actualmente no se admite la resincronización de SnapMirror con Cloud después de las migraciones que utilizan los métodos SVM-Migrate, SVM-DR o Head Swap.

Cómo funciona la resincronización de SnapMirror to Cloud de NetApp Backup and Recovery

Si completa una actualización técnica o migra volúmenes de un clúster de ONTAP a otro, es importante que sus copias de seguridad sigan funcionando sin interrupciones. SnapMirror to Cloud Resync de NetApp Backup and Recovery ayuda con esto al garantizar que sus copias de seguridad en la nube se mantengan consistentes incluso después de una migración de volumen.

He aquí un ejemplo:

Imagina que tienes un volumen local llamado Vol1a. Este volumen tiene tres instantáneas: S1, S2 y S3. Estas instantáneas son puntos de restauración. Vol1 tiene una copia de seguridad en la nube mediante SnapMirror to Cloud (SM-C), pero solo S1 y S2 están en el almacenamiento de objetos.

Ahora, desea migrar Vol1 a otro clúster ONTAP. Para ello, crea una relación de replicación lógica de SnapMirror (LRSE) con un nuevo volumen en la nube llamado Vol1b. Esto transfiere las tres instantáneas (S1, S2 y S3) de Vol1a a Vol1b.

Una vez completada la migración, tendrá la siguiente configuración:

- Se elimina la relación SM-C original (Vol1a → Almacén de objetos).
- También se elimina la relación LRSE (Vol1a → Vol1b).
- Vol1b ahora es tu volumen activo.

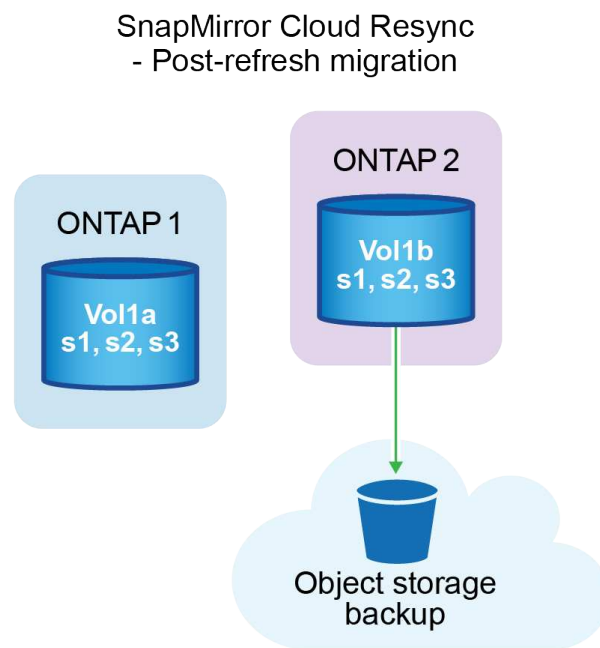
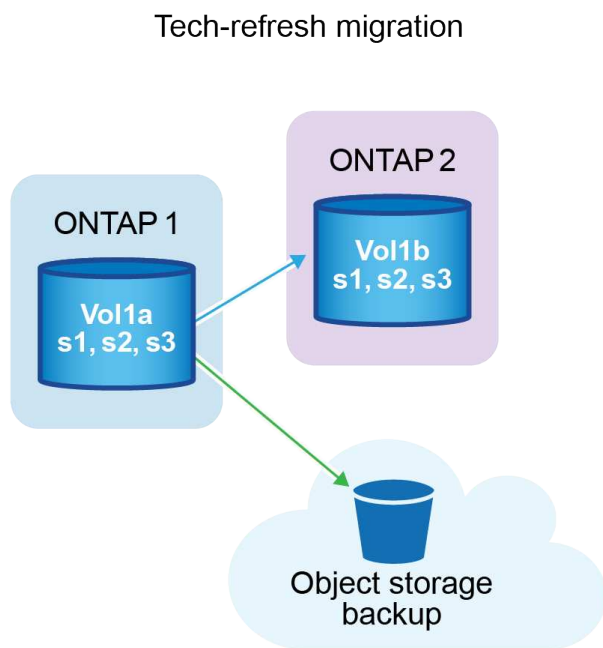
En este punto, desea continuar realizando una copia de seguridad de Vol1b en el mismo punto final de la nube. Pero en lugar de iniciar una copia de seguridad completa desde cero (lo que llevaría tiempo y recursos), utiliza SnapMirror para realizar la resincronización en la nube.

Así es como funciona la resincronización:

- El sistema busca una instantánea común entre Vol1a y el almacén de objetos. En este caso ambos tienen S2.
- Debido a esta instantánea compartida, el sistema necesita transferir solo los cambios incrementales entre S2 y S3.

Esto significa que solo se envían al almacén de objetos los datos nuevos agregados después de S2, no todo el volumen.

Este proceso evita las copias de seguridad duplicadas, ahorra ancho de banda y mantiene las copias de seguridad en funcionamiento después de la migración.



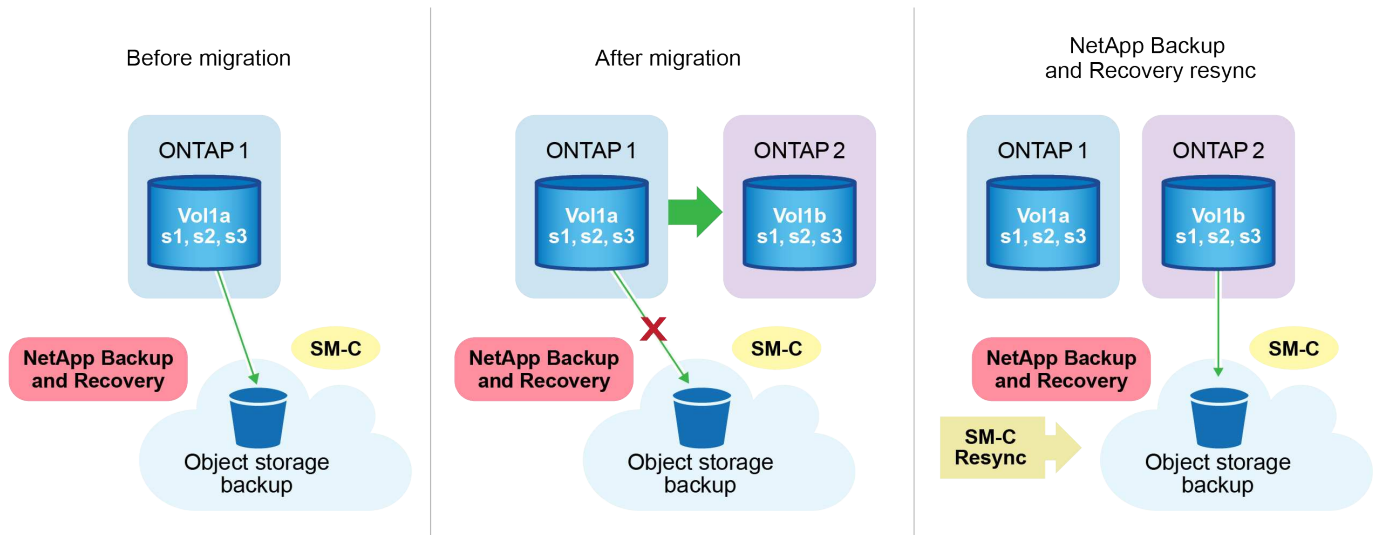
Notas de procedimiento

- Las migraciones y actualizaciones tecnológicas no se realizan mediante NetApp Backup and Recovery. Deben ser realizados por un equipo de servicios profesionales o un administrador de almacenamiento calificado.
- Un equipo de migración de NetApp crea la relación SnapMirror entre los clústeres ONTAP de origen y destino para ayudar a mover los volúmenes.
- Asegúrese de que la migración durante una actualización tecnológica se base en la migración basada en SnapMirror.

Cómo migrar volúmenes usando SnapMirror a Cloud Resync

La migración de volúmenes mediante SnapMirror a Cloud Resync implica los siguientes pasos principales, cada uno descrito con más detalle a continuación:

- **Siga una lista de verificación previa a la migración:** antes de comenzar la migración, un equipo de actualización técnica de NetApp se asegura de que se cumplan los siguientes requisitos previos para evitar la pérdida de datos y garantizar un proceso de migración sin problemas.
- **Siga una lista de verificación posterior a la migración:** después de la migración, un equipo de actualización técnica de NetApp se asegura de que se completen los siguientes pasos para establecer la protección y prepararse para la resincronización.
- **Realizar una resincronización de SnapMirror a la nube:** después de la migración, un equipo de actualización técnica de NetApp realiza una operación de resincronización de SnapMirror a la nube para reanudar las copias de seguridad en la nube desde los volúmenes recientemente migrados.



Siga una lista de verificación previa a la migración

Antes de la migración, el equipo de NetApp Tech Refresh verifica estos requisitos previos para evitar la pérdida de datos y garantizar un proceso sin problemas.

1. Asegúrese de que todos los volúmenes que se van a migrar estén protegidos mediante NetApp Backup and Recovery.
2. Registrar los UUID de las instancias de volumen. Anote los UUID de instancia de todos los volúmenes antes de iniciar la migración. Estos identificadores son cruciales para operaciones de mapeo y resincronización posteriores.
3. Tome una instantánea final de cada volumen para preservar el estado más reciente, antes de eliminar cualquier relación SnapMirror .
4. Documentar las políticas de SnapMirror . Registre la política SnapMirror actualmente asociada a la relación de cada volumen. Esto será necesario más adelante durante el proceso de resincronización de SnapMirror a la nube.
5. Eliminar las relaciones de SnapMirror Cloud con el almacén de objetos.
6. Cree una relación SnapMirror estándar con el nuevo clúster ONTAP para migrar el volumen al nuevo clúster ONTAP de destino.

Siga una lista de verificación posterior a la migración

Después de la migración, un equipo de actualización técnica de NetApp se asegura de que se completen los siguientes pasos para establecer la protección y prepararse para la resincronización.

1. Registre los nuevos UUID de instancia de volumen de todos los volúmenes migrados en el clúster ONTAP de destino.
2. Confirme que todas las políticas de SnapMirror requeridas que estaban disponibles en el antiguo clúster de ONTAP estén configuradas correctamente en el nuevo clúster de ONTAP .
3. Agregue el nuevo clúster ONTAP como un sistema en la página **Sistemas** de la Consola.



Se debe utilizar el UUID de la instancia de volumen, no el ID del volumen. El UUID de la instancia de volumen es un identificador único que permanece constante en todas las migraciones, mientras que el ID del volumen puede cambiar después de la migración.

Realizar una resincronización de SnapMirror a la nube

Después de la migración, un equipo de actualización técnica de NetApp realiza una operación de resincronización de SnapMirror a la nube para reanudar las copias de seguridad en la nube de los volúmenes recién migrados.

1. Agregue el nuevo clúster ONTAP como un sistema en la página **Sistemas** de la Consola.
2. Consulte la página de volúmenes de NetApp Backup and Recovery para asegurarse de que los detalles del sistema de origen antiguo estén disponibles.
3. Desde la página Volúmenes de NetApp Backup and Recovery , seleccione **Configuración de copia de seguridad**.
 - Dentro de la página Configuración de copia de seguridad, seleccione **Ver todo**.
 - Desde el menú Acciones... a la derecha de la *nueva* fuente, seleccione **Resincronizar copia de seguridad**.
4. En la página del sistema Resync, haga lo siguiente:
 - a. **Nuevo sistema de origen**: ingrese el nuevo clúster ONTAP donde se han migrado los volúmenes.
 - b. **Almacén de objetos de destino existente**: seleccione el almacén de objetos de destino que contiene las copias de seguridad del sistema de origen antiguo.
5. Seleccione **Descargar plantilla CSV** para descargar la hoja de Excel de detalles de resincronización. Utilice esta hoja para ingresar los detalles de los volúmenes que se migrarán. En el archivo CSV, ingrese los siguientes detalles:
 - El UUID de la instancia de volumen anterior del clúster de origen
 - El nuevo UUID de la instancia de volumen del clúster de destino
 - La política de SnapMirror que se aplicará a la nueva relación.
6. Seleccione **Cargar** en **Cargar detalles de mapeo de volumen** para cargar la hoja CSV completa en la interfaz de usuario de NetApp Backup and Recovery .



Se debe utilizar el UUID de la instancia de volumen, no el ID del volumen. El UUID de la instancia de volumen es un identificador único que permanece constante en todas las migraciones, mientras que el ID del volumen puede cambiar después de la migración.

7. Ingrese la información de configuración de red y proveedor requerida para la operación de resincronización.
8. Seleccione **Enviar** para iniciar el proceso de validación.

NetApp Backup and Recovery valida que cada volumen seleccionado para resincronizar sea la última instantánea y tenga al menos una instantánea común. Esto garantiza que los volúmenes estén listos para la operación de resincronización de SnapMirror a la nube.
9. Revise los resultados de la validación, incluidos los nuevos nombres de los volúmenes de origen y el estado de resincronización de cada volumen.
10. Verifique la elegibilidad del volumen. El sistema verifica si los volúmenes son elegibles para la resincronización. Si un volumen no es elegible, significa que no es la última instantánea o no se encontró ninguna instantánea común.



Para garantizar que los volúmenes sigan siendo elegibles para la operación de resincronización de SnapMirror a la nube, tome una instantánea final de cada volumen antes de eliminar cualquier relación de SnapMirror durante la fase previa a la migración. Esto conserva el estado más reciente de los datos.

11. Seleccione **Resincronizar** para iniciar la operación de resincronización. El sistema utiliza la instantánea más reciente y común para transferir solo los cambios incrementales, lo que garantiza la continuidad de la copia de seguridad.
12. Supervise el proceso de resincronización en la página Monitor de trabajo.

Restaurar datos de configuración de NetApp Backup and Recovery en un sitio oscuro

Al usar NetApp Backup and Recovery en un sitio sin acceso a Internet, conocido como *modo privado*, los datos de configuración de NetApp Backup and Recovery se respaldan en el depósito StorageGRID o ONTAP S3 donde se almacenan sus copias de seguridad. Si tiene un problema con el sistema host del agente de consola, puede implementar un nuevo agente de consola y restaurar los datos críticos de NetApp Backup and Recovery .



Este procedimiento se aplica únicamente a los datos de volumen de ONTAP .

Cuando utiliza NetApp Backup and Recovery en un entorno SaaS con el agente de consola implementado en su proveedor de nube o en su propio host conectado a Internet, el sistema realiza copias de seguridad y protege todos los datos de configuración importantes en la nube. Si tiene un problema con el agente de consola, cree un nuevo agente de consola y agregue sus sistemas. Los detalles de la copia de seguridad se restauran automáticamente.

Hay dos tipos de datos que se respaldan:

- Base de datos de NetApp Backup and Recovery : contiene una lista de todos los volúmenes, archivos de respaldo, políticas de respaldo e información de configuración.
- Archivos de catálogo indexados: contienen índices detallados que se utilizan para la funcionalidad de búsqueda y restauración que hace que sus búsquedas sean muy rápidas y eficientes cuando busca datos de volumen que desea restaurar.

Se realiza una copia de seguridad de estos datos una vez al día a medianoche y se conserva un máximo de 7 copias de cada archivo. Si el agente de la consola administra varios sistemas ONTAP locales, los archivos de NetApp Backup and Recovery se almacenan en el depósito del sistema que se activó primero.



Nunca se incluyen datos de volumen en la base de datos de NetApp Backup and Recovery ni en los archivos del catálogo indexado.

Restaurar datos de NetApp Backup and Recovery a un nuevo agente de consola

Si su agente de consola local deja de funcionar, deberá instalar un nuevo agente de consola y luego restaurar los datos de NetApp Backup and Recovery en el nuevo agente de consola.

Necesitará realizar las siguientes tareas para que su sistema NetApp Backup and Recovery vuelva a funcionar:

- Instalar un nuevo agente de consola
- Restaurar la base de datos de NetApp Backup and Recovery
- Restaurar los archivos del catálogo indexado
- Redescubre todos tus sistemas ONTAP locales y sistemas StorageGRID en la interfaz de usuario de la NetApp Console

Después de comprobar que su sistema funciona, cree nuevos archivos de respaldo.

Lo que necesitarás

Necesitará acceder a las copias de seguridad de bases de datos e índices más recientes desde el depósito StorageGRID o ONTAP S3 donde se almacenan sus archivos de copia de seguridad:

- Archivo de base de datos MySQL de NetApp Backup and Recovery

Este archivo se encuentra en la siguiente ubicación en el depósito `netapp-backup-<GUID>/mysql_backup/` , y se llama `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Archivo zip de copia de seguridad del catálogo indexado

Este archivo se encuentra en la siguiente ubicación en el depósito `netapp-backup-<GUID>/catalog_backup/` , y se llama `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Instalar un nuevo agente de consola en un nuevo host Linux local

Al instalar un nuevo agente de consola, descargue la misma versión de software que el agente original. Los cambios en la base de datos de NetApp Backup and Recovery pueden provocar que las versiones de software más nuevas no funcionen con copias de seguridad de bases de datos antiguas. Puede ["Actualizar el software del agente de la consola a la versión más actual después de restaurar la base de datos de respaldo"](#) .

1. ["Instalar el agente de consola en un nuevo host Linux local"](#)
2. Inicie sesión en la consola utilizando las credenciales de usuario administrador que acaba de crear.

Restaurar la base de datos de NetApp Backup and Recovery

1. Copie la copia de seguridad de MySQL desde la ubicación de la copia de seguridad al nuevo host del agente de consola. Usaremos el nombre de archivo de ejemplo `"CBS_DB_Backup_23_05_2023.sql"` a continuación.
2. Copie la copia de seguridad en el contenedor Docker de MySQL utilizando uno de los siguientes comandos, dependiendo de si está utilizando un contenedor Docker o Podman:

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Ingrese al shell del contenedor MySQL usando uno de los siguientes comandos, dependiendo de si está usando un contenedor Docker o Podman:


```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. En el shell del contenedor, implemente "env".
5. Necesitará la contraseña de la base de datos MySQL, así que copie el valor de la clave "MYSQL_ROOT_PASSWORD".
6. Restaure la base de datos MySQL de NetApp Backup and Recovery utilizando el siguiente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Verifique que la base de datos MySQL de NetApp Backup and Recovery se haya restaurado correctamente utilizando los siguientes comandos SQL:

```
mysql -u root -p cloud_backup
```

8. Introduzca la contraseña.

```
mysql> show tables;  
mysql> select * from volume;
```

9. Asegúrese de que los volúmenes que se muestran sean los mismos que existían en su entorno original.

Restaurar los archivos del catálogo indexado

1. Copie el archivo zip de respaldo del Catálogo indexado (usaremos el nombre de archivo de ejemplo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip") desde la ubicación de respaldo al nuevo host del agente de consola en la carpeta "/opt/application/netapp/cbs".
2. Descomprima el archivo "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" usando el siguiente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Ejecute el comando **ls** para asegurarse de que se haya creado la carpeta "catalogdb1" con las subcarpetas "cambios" y "instantáneas" debajo.

Descubra sus clústeres ONTAP y sistemas StorageGRID

1. ["Descubra todos los sistemas ONTAP locales"](#) que estaban disponibles en su entorno anterior. Esto incluye el sistema ONTAP que ha utilizado como servidor S3.
2. ["Descubra sus sistemas StorageGRID"](#).

Configurar los detalles del entorno de StorageGRID

Agregue los detalles del sistema StorageGRID asociado con sus sistemas ONTAP tal como se configuraron en la configuración del agente de consola original utilizando el ["API de la NetApp Console"](#) .

La siguiente información se aplica a las instalaciones en modo privado a partir de NetApp Console 3.9.xx. Para versiones anteriores, utilice el siguiente procedimiento: ["Copia de seguridad en la nube de DarkSite: copia de seguridad y restauración de MySQL y catálogo indexado"](#) .

Necesitará realizar estos pasos para cada sistema que esté realizando una copia de seguridad de datos en StorageGRID.

1. Extraiga el token de autorización utilizando la siguiente API oauth/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept: application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '{ "username": "admin@netapp.com", "password": "Netapp@123", "grant_type": "password" }'>
```

Si bien la dirección IP, el nombre de usuario y las contraseñas son valores personalizados, el nombre de la cuenta no lo es. El nombre de la cuenta siempre es "cuenta-DARKSITE1". Además, el nombre de usuario debe utilizar un nombre con formato de correo electrónico.

Esta API devolverá una respuesta como la siguiente. Puede recuperar el token de autorización como se muestra a continuación.

```
{ "expires_in": 21600, "access_token": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoieWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWx1IiwiaWF0IjoxNjc5NzY2MDIzLCJleHAiOiE2NzI3NTc2MjMsImIzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRPRDY23PokyLgl1f67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykODNDmrv5At_f9HHp0-xVMYHqyWZ4nNFalMvAh4xESc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSolIwIeHXZJJV-UsWun9daNgiYd_wX-4WWJVIGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-rxXDOjklSUmumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA" }
```

2. Extraiga el ID del sistema y el X-Agent-Id mediante la API de tenencia/externa/recurso.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiaXVkJjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbnF9uYW11IjoieYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWVpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjcyNzIyNzEzNDQzMjMsImIzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVybBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRdstcFgJLdJHtowweNH2829KsjEGBTtcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Esta API devolverá una respuesta como la siguiente. El valor bajo "resourceIdentifier" denota *WorkingEnvironment Id* y el valor bajo "agentId" denota *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfB1LIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":{"clusterUuid":"2cb6cb4b-dc07-11ec-9114-
d039ea931e09"},"workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfB1LIhqDgIPA0wclients"]}]
```

3. Actualice la base de datos de NetApp Backup and Recovery con los detalles del sistema StorageGRID asociado con los sistemas. Asegúrese de ingresar el nombre de dominio completo de StorageGRID, así como la clave de acceso y la clave de almacenamiento como se muestra a continuación:

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxiwiYXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW11IjoiYWRTaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjc5NzIyNzEzNDQzMtMTsImIzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGfo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRdStcFgJLdJHtowweNH2829KsjEGBTTCBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLihqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Verificar la configuración de NetApp Backup and Recovery

1. Seleccione cada sistema ONTAP y haga clic en **Ver copias de seguridad** junto al servicio de copia de seguridad y recuperación en el panel derecho.

Debería ver todas las copias de seguridad creadas para sus volúmenes.

2. Desde el Panel de restauración, en la sección Buscar y restaurar, haga clic en **Configuración de indexación**.

Asegúrese de que los sistemas que tenían habilitada la catalogación indexada anteriormente permanezcan habilitados.

3. Desde la página Buscar y restaurar, ejecute algunas búsquedas en el catálogo para confirmar que la restauración del catálogo indexado se ha completado correctamente.

Administre copias de seguridad de sus sistemas ONTAP con NetApp Backup and Recovery

Con NetApp Backup and Recovery, administre las copias de seguridad de sus Cloud Volumes ONTAP y sistemas ONTAP locales cambiando la programación de copias de seguridad, habilitando o deshabilitando copias de seguridad de volúmenes, pausando copias de seguridad, eliminando copias de seguridad, forzando la eliminación de copias de seguridad y más. Esto incluye todo tipo de copias de seguridad, incluidas las

instantáneas, los volúmenes replicados y los archivos de copia de seguridad en el almacenamiento de objetos. También puede cancelar el registro de NetApp Backup and Recovery.



No administre ni modifique los archivos de respaldo directamente en sus sistemas de almacenamiento o desde el entorno de su proveedor de nube. Esto puede dañar los archivos y dará como resultado una configuración no compatible.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte ["Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery"](#) .

Ver el estado de la copia de seguridad de los volúmenes en sus sistemas

Puede ver una lista de todos los volúmenes que se están respaldando actualmente en el Panel de respaldo de volúmenes. Esto incluye todo tipo de copias de seguridad, incluidas las instantáneas, los volúmenes replicados y los archivos de copia de seguridad en el almacenamiento de objetos. También puedes ver los volúmenes en aquellos sistemas que actualmente no están siendo respaldados.

Pasos

1. Desde el menú Consola, seleccione **Protección > Copia de seguridad y recuperación**.
2. Seleccione el menú **Volúmenes** para ver la lista de volúmenes respaldados para sus sistemas Cloud Volumes ONTAP y ONTAP locales.
3. Si está buscando volúmenes específicos en determinados sistemas, puede refinar la lista por sistema y volumen. También puede utilizar el filtro de búsqueda o puede ordenar las columnas según el estilo de volumen (FlexVol o FlexGroup), el tipo de volumen y más.

Para mostrar columnas adicionales (agregados, estilo de seguridad (Windows o UNIX), política de instantáneas, política de replicación y política de copia de seguridad), seleccione el signo más.

4. Revise el estado de las opciones de protección en la columna "Protección existente". Los 3 iconos representan "Instantáneas locales", "Volúmenes replicados" y "Copias de seguridad en almacenamiento de objetos".

Cada ícono se ilumina cuando ese tipo de copia de seguridad está activado y es gris cuando el tipo de copia de seguridad está inactivo. Puede pasar el cursor sobre cada ícono para ver la política de respaldo que se está utilizando y otra información pertinente para cada tipo de respaldo.

Activar la copia de seguridad en volúmenes adicionales en un sistema

Si activó la copia de seguridad solo en algunos de los volúmenes de un sistema cuando habilitó por primera vez NetApp Backup and Recovery, puede activar copias de seguridad en volúmenes adicionales más adelante.

Pasos

1. Desde la pestaña **Volúmenes**, identifique el volumen en el que desea activar las copias de seguridad, seleccione el menú Acciones  al final de la fila y seleccione **Activar protección 3-2-1**.
2. En la página *Definir estrategia de copia de seguridad*, seleccione la arquitectura de copia de seguridad y, a continuación, defina las políticas y otros detalles para las instantáneas locales, los volúmenes replicados y los archivos de copia de seguridad. Consulte los detalles de las opciones de respaldo de los volúmenes iniciales que activó en este sistema. Luego, seleccione **Siguiente**.

3. Revise la configuración de respaldo para este volumen y luego seleccione **Activar respaldo**.

Cambiar la configuración de copia de seguridad asignada a los volúmenes existentes

Puede cambiar las políticas de respaldo asignadas a sus volúmenes existentes que tienen políticas asignadas. Puedes cambiar las políticas para tus instantáneas locales, volúmenes replicados y archivos de copia de seguridad. Cualquier nueva instantánea, replicación o política de respaldo que desee aplicar a los volúmenes ya debe existir.

Editar la configuración de copia de seguridad en un solo volumen

Pasos

1. Desde el menú **Volúmenes**, localice el volumen para el cual desea modificar la configuración de política, seleccione el menú Acciones **...** al final de la fila y seleccione **Editar estrategia de respaldo**.
2. En la página *Editar estrategia de copia de seguridad*, realice cambios en las políticas de copia de seguridad existentes para instantáneas locales, volúmenes replicados y archivos de copia de seguridad y seleccione **Siguiente**.

Si habilitó *DataLock* y *Ransomware Resilience* para las copias de seguridad en la nube en la política de copia de seguridad inicial al activar NetApp Backup and Recovery para este clúster, solo verá otras políticas que se hayan configurado con DataLock. Y si no habilitó *DataLock* y *Ransomware Resilience* al activar NetApp Backup and Recovery, solo verá otras políticas de respaldo en la nube que no tengan DataLock configurado.

3. Revise la configuración de respaldo para este volumen y luego seleccione **Activar respaldo**.

Editar la configuración de copia de seguridad en varios volúmenes

Si desea utilizar la misma configuración de respaldo en varios volúmenes, puede activar o editar la configuración de respaldo en varios volúmenes al mismo tiempo. Puede seleccionar volúmenes que no tengan configuraciones de respaldo, solo configuraciones de instantáneas, solo configuraciones de respaldo en la nube, etc., y realizar cambios masivos en todos estos volúmenes con diversas configuraciones de respaldo.

Al trabajar con varios volúmenes, todos ellos deben tener estas características comunes:

- mismo sistema
- mismo estilo (volumen FlexVol o FlexGroup)
- mismo tipo (volumen de lectura-escritura o protección de datos)

Cuando se habilitan más de cinco volúmenes para la copia de seguridad, NetApp Backup and Recovery inicializa solo cinco volúmenes a la vez. Cuando estos están terminados, se continúa en grupos de 5 hasta que se inician todos los volúmenes.

Pasos

1. Desde la pestaña **Volúmenes**, filtre por el sistema en el que residen los volúmenes.
2. Seleccione todos los volúmenes en los que desea administrar la configuración de copia de seguridad.
3. Dependiendo del tipo de acción de respaldo que desee configurar, haga clic en el botón en el menú Acciones masivas:

Acción de respaldo...	Seleccione este botón...
Administrar la configuración de copias de seguridad de instantáneas	Administrar instantáneas locales
Administrar la configuración de la copia de seguridad de replicación	Administrar replicación
Administrar la configuración de la copia de seguridad en la nube	Administrar copia de seguridad
Administrar múltiples tipos de configuraciones de respaldo. Esta opción también le permite cambiar la arquitectura de la copia de seguridad.	Administrar copias de seguridad y recuperación

4. En la página de copia de seguridad que aparece, realice cambios en las políticas de copia de seguridad existentes para instantáneas locales, volúmenes replicados o archivos de copia de seguridad y seleccione **Guardar**.

Si habilitó *DataLock* y *Ransomware Resilience* para las copias de seguridad en la nube en la política de copia de seguridad inicial al activar NetApp Backup and Recovery para este clúster, solo verá otras políticas que se hayan configurado con DataLock. Y si no habilitó *DataLock* y *Ransomware Resilience* al activar NetApp Backup and Recovery, solo verá otras políticas de respaldo en la nube que no tengan DataLock configurado.

Cree una copia de seguridad de volumen manual en cualquier momento

Puede crear una copia de seguridad a pedido en cualquier momento para capturar el estado actual del volumen. Esto puede ser útil si se han realizado cambios muy importantes en un volumen y no desea esperar hasta la próxima copia de seguridad programada para proteger esos datos. También puede utilizar esta funcionalidad para crear una copia de seguridad de un volumen que actualmente no se está respaldando y desea capturar su estado actual.

Puede crear una instantánea ad hoc o una copia de seguridad en el almacén de objetos de un volumen. No se puede crear un volumen replicado ad-hoc.

El nombre de la copia de seguridad incluye la marca de tiempo para que pueda identificar su copia de seguridad a pedido de otras copias de seguridad programadas.

Si habilitó *DataLock* y *Ransomware Resilience* al activar NetApp Backup and Recovery para este clúster, la copia de seguridad a pedido también se configurará con DataLock y el período de retención será de 30 días. Los análisis de ransomware no son compatibles con copias de seguridad ad-hoc. ["Obtenga más información sobre DataLock y la protección contra ransomware"](#).

Cuando se crea una copia de seguridad ad-hoc, se crea una instantánea en el volumen de origen. Debido a que esta instantánea no es parte de una programación de instantáneas normal, no se desactivará. Es posible que desees eliminar manualmente esta instantánea del volumen de origen una vez que se complete la copia de seguridad. Esto permitirá que se liberen los bloques relacionados con esta instantánea. El nombre de la instantánea comenzará con `cbs-snapshot-adhoc-`. ["Vea cómo eliminar una instantánea usando la CLI de ONTAP"](#).



La copia de seguridad de volumen a pedido no se admite en volúmenes de protección de datos.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen y seleccione **Copia de seguridad > Crear**

copia de seguridad ad-hoc.

La columna Estado de la copia de seguridad de ese volumen muestra "En progreso" hasta que se crea la copia de seguridad.

Ver la lista de copias de seguridad de cada volumen

Puede ver la lista de todos los archivos de respaldo que existen para cada volumen. Esta página muestra detalles sobre el volumen de origen, la ubicación de destino y los detalles de la copia de seguridad, como la última copia de seguridad realizada, la política de copia de seguridad actual, el tamaño del archivo de copia de seguridad y más.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen de origen y seleccione **Ver detalles del volumen**.

Se muestran los detalles del volumen y la lista de instantáneas.

2. Seleccione **Instantánea**, **Replicación** o **Copia de seguridad** para ver la lista de todos los archivos de copia de seguridad para cada tipo de copia de seguridad.

Ejecutar un análisis de ransomware en una copia de seguridad de volumen en el almacenamiento de objetos

NetApp Backup and Recovery escanea sus archivos de respaldo para buscar evidencia de un ataque de ransomware cuando se crea un respaldo en un archivo de objeto y cuando se restauran los datos de un archivo de respaldo. También puede ejecutar un análisis a pedido en cualquier momento para verificar la usabilidad de un archivo de respaldo específico en el almacenamiento de objetos. Esto puede ser útil si ha tenido un problema de ransomware en un volumen particular y desea verificar que las copias de seguridad de ese volumen no se vean afectadas.

Esta función solo está disponible si la copia de seguridad del volumen se creó desde un sistema con ONTAP 9.11.1 o superior, y si habilitó *DataLock* y *Ransomware Resilience* en la política de copia de seguridad a objeto.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen de origen y seleccione **Ver detalles del volumen**.

Se muestran los detalles del volumen.

2. Seleccione **Copia de seguridad** para ver la lista de archivos de copia de seguridad en el almacenamiento de objetos.
3. Seleccionar... para el archivo de respaldo de volumen que desea escanear en busca de ransomware y haga clic en **Escanear en busca de ransomware**.

La columna Resiliencia ante ransomware muestra que el análisis está en progreso.

Administrar la relación de replicación con el volumen de origen

Después de configurar la replicación de datos entre dos sistemas, puede administrar la relación de replicación de datos.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen de origen y seleccione la opción **Replicación**. Podrás ver todas las opciones disponibles.
2. Seleccione la acción de replicación que desea realizar.

La siguiente tabla describe las acciones disponibles:

Acción	Descripción
Ver replicación	Muestra detalles sobre la relación de volumen: información de transferencia, información de la última transferencia, detalles sobre el volumen e información sobre la política de protección asignada a la relación.
Actualizar replicación	Inicia una transferencia incremental para actualizar el volumen de destino que se sincronizará con el volumen de origen.
Pausar replicación	Pause la transferencia incremental de instantáneas para actualizar el volumen de destino. Puede reanudar más tarde si desea reiniciar las actualizaciones incrementales.
Romper la replicación	Rompe la relación entre los volúmenes de origen y destino, y activa el volumen de destino para el acceso a los datos (lo hace de lectura y escritura). Esta opción se utiliza normalmente cuando el volumen de origen no puede servir datos debido a eventos como corrupción de datos, eliminación accidental o un estado fuera de línea. https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html ["Aprenda a configurar un volumen de destino para el acceso a datos y reactivar un volumen de origen en la documentación de ONTAP"]
Abortar replicación	Deshabilita las copias de seguridad de este volumen en el sistema de destino y también deshabilita la capacidad de restaurar un volumen. No se eliminarán ninguna copia de seguridad existente. Esto no elimina la relación de protección de datos entre los volúmenes de origen y destino.
Resincronización inversa	Invierte los roles de los volúmenes de origen y destino. El contenido del volumen de origen original se sobrescribe con el contenido del volumen de destino. Esto es útil cuando desea reactivar un volumen de origen que se desconectó. No se conservan los datos escritos en el volumen de origen original entre la última replicación de datos y el momento en que se deshabilitó el volumen de origen.
Eliminar relación	Elimina la relación de protección de datos entre los volúmenes de origen y destino, lo que significa que ya no se produce la replicación de datos entre los volúmenes. Esta acción no activa el volumen de destino para el acceso a los datos, lo que significa que no lo convierte en lectura y escritura. Esta acción también elimina la relación de pares del clúster y la relación de pares de la máquina virtual de almacenamiento (SVM), si no hay otras relaciones de protección de datos entre los sistemas.

Resultado

Después de seleccionar una acción, la consola actualiza la relación.

Editar una política de copia de seguridad en la nube existente

Puede cambiar los atributos de una política de respaldo que se aplica actualmente a los volúmenes de un sistema. Cambiar la política de respaldo afecta a todos los volúmenes existentes que utilizan la política.



- Si habilitó *DataLock* y *Ransomware Resilience* en la política inicial al activar NetApp Backup and Recovery para este clúster, cualquier política que edite debe configurarse con la misma configuración de DataLock (Gobernanza o Cumplimiento). Y si no habilitó *DataLock* y *Ransomware Resilience* al activar NetApp Backup and Recovery, no podrá habilitar DataLock ahora.
- Al crear copias de seguridad en AWS, si elige *S3 Glacier* o *S3 Glacier Deep Archive* en su primera política de copia de seguridad al activar NetApp Backup and Recovery, ese nivel será el único nivel de archivo disponible al editar políticas de copia de seguridad. Y si no seleccionó ningún nivel de archivo en su primera política de respaldo, entonces *S3 Glacier* será su única opción de archivo al editar una política.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, seleccione... para el sistema en el que desea cambiar la configuración de políticas y seleccione **Administrar políticas**.
3. Desde la página *Administrar políticas*, seleccione **Editar** para la política de respaldo que desea cambiar en ese sistema.
4. Desde la página *Editar política*, seleccione la flecha hacia abajo para expandir la sección *Etiquetas y retención* para cambiar la programación o la retención de copias de seguridad y seleccione **Guardar**.

Si su clúster ejecuta ONTAP 9.10.1 o superior, también tiene la opción de habilitar o deshabilitar la organización en niveles de las copias de seguridad en el almacenamiento de archivo después de una cierta cantidad de días.

["Obtenga más información sobre el uso del almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre el uso del almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre el uso del almacenamiento de archivos de Google"](#). (Requiere ONTAP 9.12.1.)

Tenga en cuenta que todos los archivos de respaldo que se hayan organizado en niveles de almacenamiento de archivo se dejarán en ese nivel si deja de organizar en niveles las copias de seguridad en el archivo; no se moverán automáticamente de nuevo al nivel estándar. Sólo las nuevas copias de seguridad de volumen residirán en el nivel estándar.

Agregar una nueva política de copia de seguridad en la nube

Cuando habilita NetApp Backup and Recovery para un sistema, todos los volúmenes que seleccione inicialmente se respaldan utilizando la política de respaldo predeterminada que usted definió. Si desea asignar diferentes políticas de respaldo a determinados volúmenes que tienen diferentes objetivos de punto de recuperación (RPO), puede crear políticas adicionales para ese clúster y asignar esas políticas a otros volúmenes.

Si desea aplicar una nueva política de respaldo a determinados volúmenes de un sistema, primero debe agregar la política de respaldo al sistema. Entonces puedes [aplicar la política a los volúmenes de ese sistema](#).



- Si habilitó *DataLock* y *Ransomware Resilience* en la política inicial al activar NetApp Backup and Recovery para este clúster, cualquier política adicional que cree debe configurarse con la misma configuración de DataLock (Gobernanza o Cumplimiento). Y si no habilitó *DataLock* y *Ransomware Resilience* al activar NetApp Backup and Recovery, no podrá crear nuevas políticas que usen DataLock.
- Al crear copias de seguridad en AWS, si elige *S3 Glacier* o *S3 Glacier Deep Archive* en su primera política de copia de seguridad al activar NetApp Backup and Recovery, ese nivel será el único nivel de archivo disponible para futuras políticas de copia de seguridad para ese clúster. Y si no seleccionó ningún nivel de archivo en su primera política de respaldo, entonces *S3 Glacier* será su única opción de archivo para políticas futuras.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, seleccione... para el sistema donde desea agregar la nueva política y seleccione **Administrar políticas**.
3. Desde la página *Administrar políticas*, seleccione **Agregar nueva política**.
4. Desde la página *Agregar nueva política*, seleccione la flecha hacia abajo para expandir la sección *Etiquetas y retención* para definir la programación y la retención de copias de seguridad, y seleccione **Guardar**.

Si su clúster ejecuta ONTAP 9.10.1 o superior, también tiene la opción de habilitar o deshabilitar la organización en niveles de las copias de seguridad en el almacenamiento de archivo después de una cierta cantidad de días.

["Obtenga más información sobre el uso del almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre el uso del almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre el uso del almacenamiento de archivos de Google"](#). (Requiere ONTAP 9.12.1.)

Eliminar copias de seguridad

NetApp Backup and Recovery le permite eliminar un solo archivo de respaldo, eliminar todos los respaldos de un volumen o eliminar todos los respaldos de todos los volúmenes de un sistema. Es posible que desee eliminar todas las copias de seguridad si ya no las necesita o si eliminó el volumen de origen y desea eliminar todas las copias de seguridad.

No puedes eliminar archivos de respaldo que hayas bloqueado usando DataLock y protección contra ransomware. La opción "Eliminar" no estará disponible en la interfaz de usuario si seleccionó uno o más archivos de respaldo bloqueados.



Si planea eliminar un sistema o clúster que tiene copias de seguridad, debe eliminar las copias de seguridad **antes** de eliminar el sistema. NetApp Backup and Recovery no elimina automáticamente las copias de seguridad cuando se elimina un sistema y no existe soporte actual en la interfaz de usuario para eliminar las copias de seguridad después de que se haya eliminado el sistema. Se le seguirán cobrando los costos de almacenamiento de objetos por cualquier copia de seguridad restante.

Eliminar todos los archivos de respaldo de un sistema

Eliminar todas las copias de seguridad del almacenamiento de objetos de un sistema no deshabilita las futuras copias de seguridad de los volúmenes en este sistema. Si desea dejar de crear copias de seguridad de todos los volúmenes de un sistema, puede desactivar las copias de seguridad [como se describe aquí](#).

Tenga en cuenta que esta acción no afecta a las instantáneas ni a los volúmenes replicados; este tipo de archivos de copia de seguridad no se eliminan.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Seleccionar... para el sistema donde desea eliminar todas las copias de seguridad y seleccione **Eliminar todas las copias de seguridad**.
3. En el cuadro de diálogo de confirmación, ingrese el nombre del sistema.
4. Seleccione **Configuración avanzada**.
5. **Forzar eliminación de copias de seguridad**: indique si desea o no forzar la eliminación de todas las copias de seguridad.

En algunos casos extremos, es posible que desee que NetApp Backup and Recovery ya no tenga acceso a las copias de seguridad. Esto podría suceder, por ejemplo, si el servicio ya no tiene acceso al depósito de copias de seguridad o las copias de seguridad están protegidas por DataLock pero ya no las desea. Anteriormente, no podía eliminarlos usted mismo y necesitaba llamar al soporte de NetApp . Con esta versión, puedes usar la opción para forzar la eliminación de copias de seguridad (a nivel de volumen y sistema).



Utilice esta opción con cuidado y sólo en necesidades de limpieza extremas. NetApp Backup and Recovery ya no tendrá acceso a estas copias de seguridad incluso si no se eliminan del almacenamiento de objetos. Necesitará ir a su proveedor de nube y eliminar manualmente las copias de seguridad.

6. Seleccione **Eliminar**.

Eliminar todos los archivos de respaldo de un volumen

Eliminar todas las copias de seguridad de un volumen también deshabilita las copias de seguridad futuras para ese volumen.

Pasos

1. Desde la pestaña **Volúmenes**, haga clic en... para el volumen de origen y seleccione **Detalles y lista de respaldo**.

Se muestra la lista de todos los archivos de respaldo.
2. Seleccione **Acciones > Eliminar todas las copias de seguridad**.
3. Introduzca el nombre del volumen.
4. Seleccione **Configuración avanzada**.
5. **Forzar eliminación de copias de seguridad**: indique si desea o no forzar la eliminación de todas las copias de seguridad.

En algunos casos extremos, es posible que desee que NetApp Backup and Recovery ya no tenga acceso a las copias de seguridad. Esto podría suceder, por ejemplo, si el servicio ya no tiene acceso al depósito de copias de seguridad o las copias de seguridad están protegidas por DataLock pero ya no las desea. Anteriormente, no podía eliminarlos usted mismo y necesitaba llamar al soporte de NetApp . Con esta versión, puedes usar la opción para forzar la eliminación de copias de seguridad (a nivel de volumen y sistema).



Utilice esta opción con cuidado y sólo en necesidades de limpieza extremas. NetApp Backup and Recovery ya no tendrá acceso a estas copias de seguridad incluso si no se eliminan del almacenamiento de objetos. Necesitará ir a su proveedor de nube y eliminar manualmente las copias de seguridad.

6. Seleccione **Eliminar**.

Eliminar un solo archivo de respaldo para un volumen

Puede eliminar un solo archivo de respaldo si ya no lo necesita. Esto incluye eliminar una única copia de seguridad de una instantánea de volumen o de una copia de seguridad en almacenamiento de objetos.

No se pueden eliminar volúmenes replicados (volúmenes de protección de datos).

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen de origen y seleccione **Ver detalles del volumen**.

Se muestran los detalles del volumen y puede seleccionar **Instantánea**, **Replicación** o **Copia de seguridad** para ver la lista de todos los archivos de copia de seguridad del volumen. Por defecto, se muestran las instantáneas disponibles.

2. Seleccione **Instantánea** o **Copia de seguridad** para ver el tipo de archivos de copia de seguridad que desea eliminar.
3. Seleccionar... para el archivo de respaldo de volumen que desea eliminar y seleccione **Eliminar**.
4. En el cuadro de diálogo de confirmación, seleccione **Eliminar**.

Eliminar relaciones de copia de seguridad de volumen

Eliminar la relación de respaldo de un volumen le proporciona un mecanismo de archivado si desea detener la creación de nuevos archivos de respaldo y eliminar el volumen de origen, pero conservar todos los archivos de respaldo existentes. Esto le brinda la posibilidad de restaurar el volumen desde el archivo de respaldo en el futuro, si es necesario, mientras libera espacio de su sistema de almacenamiento de origen.

No es necesario necesariamente eliminar el volumen de origen. Puede eliminar la relación de respaldo de un volumen y conservar el volumen de origen. En este caso puedes "Activar" la copia de seguridad en el volumen en un momento posterior. En este caso, se sigue utilizando la copia de seguridad de línea base original: no se crea una nueva copia de seguridad de línea base ni se exporta a la nube. Tenga en cuenta que si reactiva una relación de respaldo, al volumen se le asigna la política de respaldo predeterminada.

Esta función solo está disponible si su sistema ejecuta ONTAP 9.12.1 o superior.

No se puede eliminar el volumen de origen desde la interfaz de usuario de NetApp Backup and Recovery . Sin embargo, puede abrir la página Detalles del volumen en la página **Sistemas** de la consola y ["Borra el volumen de ahí"](#) .



No es posible eliminar archivos de respaldo de volúmenes individuales una vez que se haya eliminado la relación. Sin embargo, puedes eliminar todas las copias de seguridad del volumen.

Pasos

1. Desde la pestaña **Volúmenes**, seleccione... para el volumen de origen y seleccione **Copia de seguridad > Eliminar relación**.

Desactivar NetApp Backup and Recovery para un sistema

Al desactivar NetApp Backup and Recovery para un sistema, se deshabilitan las copias de seguridad de cada volumen del sistema y también se deshabilita la capacidad de restaurar un volumen. No se eliminarán ninguna copia de seguridad existente. Esto no anula el registro del servicio de respaldo de este sistema; básicamente, le permite pausar toda la actividad de respaldo y restauración por un período de tiempo.

Tenga en cuenta que su proveedor de nube le seguirá cobrando los costos de almacenamiento de objetos por la capacidad que utilizan sus copias de seguridad a menos que [eliminar las copias de seguridad](#).

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, seleccione... para el sistema en el que desea deshabilitar las copias de seguridad y seleccione **Desactivar copia de seguridad**.
3. En el cuadro de diálogo de confirmación, seleccione **Desactivar**.



Aparece un botón **Activar copia de seguridad** para ese sistema mientras la copia de seguridad está deshabilitada. Puede seleccionar este botón cuando desee volver a habilitar la funcionalidad de copia de seguridad para ese sistema.

Anular el registro de NetApp Backup and Recovery para un sistema

Puede cancelar el registro de NetApp Backup and Recovery para un sistema si ya no desea utilizar la funcionalidad de respaldo y desea dejar de pagar por los respaldos en ese sistema. Normalmente, esta función se utiliza cuando planeas eliminar un sistema y deseas cancelar el servicio de respaldo.

También puede utilizar esta función si desea cambiar el almacén de objetos de destino donde se almacenan las copias de seguridad de su clúster. Después de cancelar el registro de NetApp Backup and Recovery para el sistema, puede habilitar NetApp Backup and Recovery para ese clúster usando la nueva información del proveedor de nube.

Antes de poder cancelar el registro de NetApp Backup and Recovery, debe realizar los siguientes pasos, en este orden:

- Desactivar NetApp Backup and Recovery para el sistema
- Eliminar todas las copias de seguridad de ese sistema

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

Pasos

1. Desde la pestaña **Volúmenes**, seleccione **Configuración de copia de seguridad**.
2. Desde la página *Configuración de copia de seguridad*, seleccione... para el sistema en el que desea anular el registro del servicio de respaldo y seleccione **Anular registro**.
3. En el cuadro de diálogo de confirmación, seleccione **Cancelar registro**.

Restaurar desde copias de seguridad de ONTAP

Restaura datos de ONTAP desde archivos de respaldo con NetApp Backup and Recovery

Las copias de seguridad de los datos de volumen de su ONTAP se almacenan como instantáneas, en volúmenes replicados o en almacenamiento de objetos. Puedes restaurar datos desde cualquiera de estas ubicaciones en un momento específico. Con NetApp Backup and Recovery, puede restaurar un volumen completo, una carpeta o archivos individuales según sea necesario.



Para cambiar hacia y desde las cargas de trabajo de NetApp Backup and Recovery , consulte "[Cambiar a diferentes cargas de trabajo de NetApp Backup and Recovery](#)".

- Puede restaurar un **volumen** (como un nuevo volumen) en el sistema original, en un sistema diferente que use la misma cuenta en la nube o en un sistema ONTAP local.
- Puede restaurar una **carpeta** a un volumen en el sistema original, a un volumen en un sistema diferente que use la misma cuenta en la nube o a un volumen en un sistema ONTAP local.
- Puede restaurar **archivos** a un volumen en el sistema original, a un volumen en un sistema diferente que use la misma cuenta en la nube o a un volumen en un sistema ONTAP local.

Necesitas una licencia válida de NetApp Backup and Recovery para restaurar datos en un sistema de producción.

Para resumir, estos son los flujos válidos que puede utilizar para restaurar datos de volumen en un sistema ONTAP :

- Archivo de respaldo → volumen restaurado
- Volumen replicado → volumen restaurado
- Instantánea → volumen restaurado



Si la operación de restauración no se completa, espere hasta que el Monitor de trabajo muestre "Error" antes de volver a intentar la operación de restauración.



Para conocer las limitaciones relacionadas con la restauración de datos de ONTAP , consulte "[Limitaciones de copia de seguridad y restauración para volúmenes ONTAP](#)".

El panel de restauración

Utilice el Panel de restauración para realizar operaciones de restauración de volúmenes, carpetas y archivos. Para acceder al Panel de Restauración, seleccione **Copia de seguridad y recuperación** en el menú Consola

y, a continuación, seleccione la pestaña **Restaurar**. También puedes seleccionar  > **Consulta el panel de control de restauración** desde el servicio de copia de seguridad y recuperación en el panel de Servicios.



NetApp Backup and Recovery ya debe estar activado para al menos un sistema y deben existir archivos de respaldo iniciales.

El Panel de restauración proporciona dos formas diferentes de restaurar datos de archivos de respaldo: **Explorar y restaurar** y **Buscar y restaurar**.

Comparación entre Explorar y restaurar y Buscar y restaurar

En términos generales, *Explorar y restaurar* suele ser mejor cuando necesita restaurar un volumen, una carpeta o un archivo específico de la última semana o mes (y conoce el nombre y la ubicación del archivo y la fecha en que estuvo en buen estado por última vez). *Buscar y restaurar* 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 se encuentra, ni la fecha en la que estuvo en buen estado por última vez.

Esta tabla proporciona una comparación de las características de los dos métodos.

Explorar y restaurar	Buscar y restaurar
Explore una estructura de estilo de carpeta para encontrar el volumen, la carpeta o el archivo dentro de un solo archivo de respaldo.	Busque un volumen, carpeta o archivo en todos los archivos de respaldo por nombre de volumen parcial o completo, nombre de carpeta/archivo parcial o completo, rango de tamaño y filtros de búsqueda adicionales.
No maneja la recuperación de archivos si el archivo ha sido eliminado o renombrado y el usuario no conoce el nombre del archivo original	Maneja directorios recién creados/eliminados/renombrados y archivos recién creados/eliminados/renombrados
Se admite la restauración rápida.	No se admite la restauración rápida.

Esta tabla proporciona una lista de operaciones de restauración válidas según la ubicación donde residen sus archivos de respaldo.

Tipo de copia de seguridad	Explorar y restaurar			Buscar y restaurar		
	Restaurar volumen	Restaurar archivos	Restaurar carpeta	Restaurar volumen	Restaurar archivos	Restaurar carpeta
Snapshot	Sí	No	No	Sí	Sí	Sí
Volumen replicado	Sí	No	No	Sí	Sí	Sí
Archivo de respaldo	Sí	Sí	Sí	Sí	Sí	Sí

Antes de utilizar cualquiera de los métodos de restauración, configure su entorno para que cumpla con los requisitos de recursos. Consulte las siguientes secciones para obtener más detalles.

Consulte los requisitos y los pasos de restauración para el tipo de operación de restauración que desea utilizar:

- ["Restaurar volúmenes mediante Explorar y restaurar"](#)
- ["Restaurar carpetas y archivos usando Explorar y restaurar"](#)
- ["Restaurar volúmenes, carpetas y archivos mediante Buscar y restaurar"](#)

Restaurar desde copias de seguridad de ONTAP mediante la función Buscar y restaurar

Puede utilizar la función Buscar y restaurar para recuperar volúmenes, carpetas o

archivos de archivos de copia de seguridad de ONTAP . La función Buscar y Restaurar le permite buscar en todas las copias de seguridad (incluidas las instantáneas locales, los volúmenes replicados y el almacenamiento de objetos) sin necesidad de conocer los nombres exactos del sistema, el volumen o los archivos.

Restaurar desde instantáneas locales o volúmenes replicados suele ser más rápido y menos costoso que restaurar desde almacenamiento de objetos.

Al restaurar un volumen completo, NetApp Backup and Recovery crea un nuevo volumen utilizando los datos de la copia de seguridad. Puede restaurar el sistema original, otro sistema dentro de la misma cuenta en la nube o un sistema ONTAP local. Las carpetas y los archivos se pueden restaurar a su ubicación original, a un volumen diferente en el mismo sistema, a otro sistema en la misma cuenta en la nube o a un sistema local.

Las capacidades de restauración dependen de su versión de ONTAP :

- **Carpetas:** Con ONTAP 9.13.0 o superior, puede restaurar carpetas con todos los archivos y subcarpetas; con versiones anteriores, solo puede restaurar archivos en la carpeta.
- **Almacenamiento de archivo:** La restauración desde el almacenamiento de archivo (disponible con ONTAP 9.10.1 o superior) es más lenta y podría generar costos adicionales.
- **Requisitos del clúster de destino:**
 - Restauración de volumen: ONTAP 9.10.1 o superior
 - Recuperación de archivos: ONTAP 9.11.1 o superior
 - Google Archive y StorageGRID: ONTAP 9.12.1 o superior
 - Restauración de carpetas: ONTAP 9.13.1 o superior

["Obtenga más información sobre la restauración desde el almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre la restauración desde el almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre cómo restaurar desde el almacenamiento de archivo de Google"](#).



- Si el archivo de respaldo en el almacenamiento de objetos se ha configurado con protección DataLock y Ransomware, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o superior. Si está utilizando una versión anterior de ONTAP, puede restaurar todo el volumen desde el archivo de respaldo y luego acceder a la carpeta y los archivos que necesita.
- Si el archivo de respaldo en el almacenamiento de objetos reside en el almacenamiento de archivo, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o superior. Si está utilizando una versión anterior de ONTAP, puede restaurar la carpeta desde un archivo de respaldo más nuevo que no se haya archivado, o puede restaurar el volumen completo desde el respaldo archivado y luego acceder a la carpeta y los archivos que necesita.
- La prioridad de restauración "Alta" no se admite al restaurar datos desde el almacenamiento de archivo de Azure a sistemas StorageGRID .
- Actualmente no se admite la restauración de carpetas desde volúmenes en el almacenamiento de objetos ONTAP S3.

Antes de comenzar, debe tener alguna idea del nombre o la ubicación del volumen o archivo que desea restaurar.

Buscar y restaurar sistemas compatibles y proveedores de almacenamiento de objetos

Puede restaurar datos de ONTAP desde un archivo de respaldo que reside en un sistema secundario (un volumen replicado) o en un almacenamiento de objetos (un archivo de respaldo) en los siguientes sistemas. Las instantáneas residen en el sistema de origen y solo se pueden restaurar en ese mismo sistema.

Nota: Puede restaurar volúmenes y archivos desde cualquier tipo de archivo de respaldo, pero en este momento solo puede restaurar una carpeta desde archivos de respaldo en el almacenamiento de objetos.

Ubicación del archivo de respaldo		Sistema de destino
Almacén de objetos (copia de seguridad)	Sistema secundario (replicación)	
Amazon S3	Cloud Volumes ONTAP en el sistema ONTAP local de AWS	Cloud Volumes ONTAP en el sistema ONTAP local de AWS
Blob de Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure
Almacenamiento en la nube de Google	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP
StorageGRID en NetApp	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local
ONTAP S3	Sistema ONTAP local Cloud Volumes ONTAP	Sistema ONTAP local

Para buscar y restaurar, el agente de consola se puede instalar en las siguientes ubicaciones:

- Para Amazon S3, el agente de consola se puede implementar en AWS o en sus instalaciones
- Para Azure Blob, el agente de consola se puede implementar en Azure o en sus instalaciones.
- Para Google Cloud Storage, el agente de la consola debe implementarse en su VPC de Google Cloud Platform
- Para StorageGRID, el agente de consola debe implementarse en sus instalaciones, con o sin acceso a Internet.
- Para ONTAP S3, el agente de consola se puede implementar en sus instalaciones (con o sin acceso a Internet) o en un entorno de proveedor de nube.

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

Requisitos previos de búsqueda y restauración

Asegúrese de que su entorno cumpla con estos requisitos antes de habilitar Buscar y restaurar:

- 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 un LIF de datos configurado.
 - NFS debe estar habilitado en el volumen (se admiten volúmenes NFS y SMB/CIFS).

- El servidor RPC SnapDiff debe estar activado en la SVM. La consola hace esto automáticamente cuando habilita la indexación en el sistema. (SnapDiff es la tecnología que identifica rápidamente las diferencias de archivos y directorios entre instantáneas).
- NetApp recomienda montar un volumen separado en el agente de consola para aumentar la resiliencia de la función de búsqueda y restauración. Para obtener instrucciones, consulte [Monte el volumen para reindexar el catálogo](#).

Requisitos previos para la búsqueda y restauración heredadas (utilizando el catálogo indexado v1)

Los siguientes son los requisitos para buscar y restaurar cuando se utiliza la indexación heredada:

- Requisitos de AWS:

- Se deben agregar permisos específicos de Amazon Athena, AWS Glue y AWS S3 al rol de usuario que proporciona permisos a la consola. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Tenga en cuenta que si ya estaba usando NetApp Backup and Recovery con un agente de consola que configuró en el pasado, ahora deberá agregar los permisos de Athena y Glue al rol de usuario de consola. Son necesarios para buscar y restaurar.

- Requisitos de Azure:

- Debe registrar el proveedor de recursos de Azure Synapse Analytics (llamado "Microsoft.Synapse") con su suscripción. ["Vea cómo registrar este proveedor de recursos para su suscripción"](#). Debe ser el **Propietario** o **Colaborador** de la suscripción para registrar al proveedor de recursos.
- Se deben agregar permisos específicos de Azure Synapse Workspace y Data Lake Storage Account al rol de usuario que proporciona permisos a la consola. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Tenga en cuenta que si ya estaba usando NetApp Backup and Recovery con un agente de consola que configuró en el pasado, ahora deberá agregar los permisos de Azure Synapse Workspace y Data Lake Storage Account al rol de usuario de consola. Son necesarios para buscar y restaurar.

- El agente de consola debe configurarse **sin** un servidor proxy para la comunicación HTTP a Internet. Si ha configurado un servidor proxy HTTP para su agente de consola, no podrá utilizar la funcionalidad de búsqueda y restauración.

- Requisitos de Google Cloud:

- Se deben agregar permisos específicos de Google BigQuery al rol de usuario que proporciona permisos a la NetApp Console. ["Asegúrese de que todos los permisos estén configurados correctamente"](#).

Si ya estaba usando NetApp Backup and Recovery con un agente de consola que configuró en el pasado, ahora deberá agregar los permisos de BigQuery al rol de usuario de consola. Son necesarios para buscar y restaurar.

- Requisitos de StorageGRID y ONTAP S3:

Dependiendo de su configuración, hay dos formas de implementar la búsqueda y restauración:

- Si no hay credenciales de proveedor de nube en su cuenta, la información del Catálogo indexado se almacena en el agente de la Consola.

Para obtener información sobre el Catálogo indexado v2, consulte la sección a continuación sobre cómo habilitar el Catálogo indexado.

- Si está utilizando un agente de consola en un sitio privado (oscuro), la información del catálogo indexado se almacena en el agente de consola (requiere la versión 3.9.25 o superior del agente de consola).
- Si tienes ["Credenciales de AWS"](#) o ["Credenciales de Azure"](#) en la cuenta, entonces el catálogo indexado se almacena en el proveedor de la nube, al igual que con un agente de consola implementado en la nube. (Si tiene ambas credenciales, AWS estará seleccionado de forma

predeterminada).

Incluso si utiliza un agente de consola local, se deben cumplir los requisitos del proveedor de la nube tanto para los permisos del agente de consola como para los recursos del proveedor de la nube. Consulte los requisitos de AWS y Azure anteriores al utilizar esta implementación.

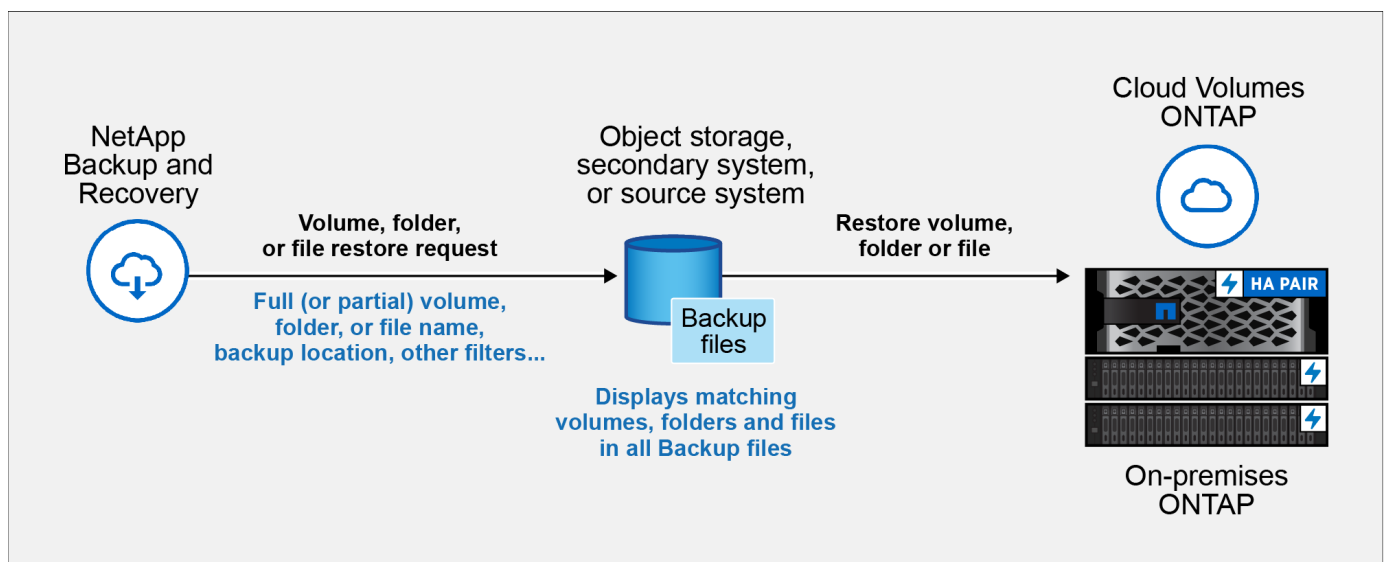
Proceso de búsqueda y restauración

El proceso es así:

1. Antes de poder usar Buscar y restaurar, debe habilitar "Indexación" en cada sistema de origen desde el cual desee restaurar datos de volumen. Esto permite que el Catálogo indexado realice un seguimiento de los archivos de respaldo de cada volumen.
2. Cuando desee restaurar un volumen o archivos desde una copia de seguridad de volumen, en *Buscar y restaurar*, seleccione **Buscar y restaurar**.
3. Ingrese los criterios de búsqueda para un volumen, carpeta o archivo por nombre de volumen parcial o completo, nombre de archivo parcial o completo, ubicación de respaldo, rango de tamaño, rango de fecha de creación, otros filtros de búsqueda y seleccione **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. Seleccione **Ver todas las copias de seguridad** para la ubicación que desea utilizar para restaurar el volumen o archivo y, a continuación, seleccione **Restaurar** en el archivo de copia de seguridad real que desea utilizar.
5. Seleccione la ubicación donde desea que se restaure el volumen, la carpeta o los archivos y seleccione **Restaurar**.
6. Se restauran el volumen, la carpeta o los archivos.



Solo necesitas conocer un nombre parcial y NetApp Backup and Recovery buscará en todos los archivos de copia de seguridad que coincidan con tu búsqueda.

Habilitar el Catálogo Indexado para cada sistema

Antes de poder usar Buscar y restaurar, debe habilitar "Indexación" en cada sistema de origen desde el cual planea restaurar volúmenes o archivos. Esto permite que el Catálogo indexado rastree cada volumen y cada archivo de respaldo, lo que hace que sus búsquedas sean muy rápidas y eficientes.

El catálogo indexado es una base de datos que almacena metadatos sobre todos los volúmenes y archivos de respaldo de su sistema. La función de búsqueda y restauración lo utiliza para encontrar rápidamente los archivos de respaldo que contienen los datos que desea restaurar.

Características del catálogo indexado

NetApp Backup and Recovery no aprovisiona un bucket separado cuando se utiliza el Catálogo indexado. En cambio, para las copias de seguridad almacenadas en AWS, Azure, Google Cloud Platform, StorageGRID u ONTAP S3, el servicio aprovisiona espacio en el agente de la consola o en el entorno del proveedor de la nube.

El catálogo indexado admite lo siguiente:

- Eficiencia de búsqueda global en menos de 3 minutos
- Hasta 5 mil millones de archivos
- Hasta 5000 volúmenes por clúster
- Hasta 100 000 instantáneas por volumen
- El tiempo máximo para la indexación de referencia es inferior a 7 días. El tiempo real variará dependiendo de su entorno.

Pasos para habilitar la indexación de un sistema:

Si la indexación ya está habilitada para su sistema, vaya a la siguiente sección para restaurar sus datos.

Primero deberá montar un volumen separado para almacenar los archivos del catálogo. Esto evita la pérdida de datos si el tamaño de los archivos que contienen las instantáneas se vuelve demasiado grande. Esto no es necesario en todos los clústeres; puede montar cualquier volumen de cualquiera de los clústeres de su entorno. Si no lo hace, es posible que la indexación no funcione correctamente.

Para el volumen montado, utilice la siguiente guía de dimensionamiento:

- Utilice un volumen NetApp NFS.
- Se recomienda almacenamiento AFF con un rendimiento de disco de 300 MB/s. La menor capacidad de procesamiento afectará a las búsquedas y otras operaciones.
- Habilite las instantáneas de NetApp para proteger los metadatos del catálogo, además de los archivos zip de copia de seguridad del catálogo.
- 50 GB por cada mil millones de archivos
- 20 GB para los datos del catálogo, con espacio adicional para la creación de archivos zip y archivos temporales.

Pasos para montar el volumen y reindexar el catálogo

1. Monta el volumen en `/opt/application/netapp/cbs` introduciendo el siguiente comando, donde:

- `volume name` es el volumen del clúster donde se almacenarán los archivos del catálogo
- `/opt/application/netapp/cbs` es el camino por donde se está montando

```
mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
```

Ejemplo:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

Pasos para habilitar el índice

1. Debe realizar una de las siguientes acciones:
 - Si no se han indexado sistemas, en el Panel de restauración, en *Buscar y restaurar*, seleccione **Habilitar indexación para sistemas**.
 - Si ya se ha indexado al menos un sistema, en el Panel de restauración, en *Buscar y restaurar*, seleccione **Configuración de indexación**.
2. Seleccione **Habilitar indexación** para el sistema.

Resultado

Una vez aprovisionados todos los servicios y activado el Catálogo Indexado, el sistema se muestra como "Activo".

Dependiendo del tamaño de los volúmenes en el sistema y la cantidad de archivos de respaldo en las tres ubicaciones de respaldo, el proceso de indexación inicial podría demorar hasta una hora. Después de eso, se actualiza de forma transparente cada hora con cambios incrementales para mantenerse actualizado.

Restaurar volúmenes, carpetas y archivos mediante Buscar y restaurar

Después de que tengas [Habilitó la indexación para su sistema](#), 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 de todos los archivos de respaldo.

Pasos

1. Desde el menú Consola, seleccione **Protección > Copia de seguridad y recuperación**.
2. Seleccione la pestaña **Restaurar** y se mostrará el Panel de restauración.
3. Desde la sección *Buscar y restaurar*, seleccione **Buscar y restaurar**.
4. Desde la sección *Buscar y restaurar*, seleccione **Buscar y restaurar**.
5. Desde la página Buscar y restaurar:
 - a. En la *Barra de búsqueda*, ingrese 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 Todos**.
 - c. En el área *Filtrar por*, seleccione los criterios de filtro. Por ejemplo, puede seleccionar el sistema donde residen los datos y el tipo de archivo, por ejemplo, un archivo .JPEG. O bien, puede seleccionar el tipo de ubicación de copia de seguridad si desea buscar resultados solo dentro de las instantáneas o archivos de copia de seguridad disponibles en el almacenamiento de objetos.
6. Seleccione **Buscar** y el área Resultados de la búsqueda mostrará todos los recursos que tienen un archivo, carpeta o volumen que coincide con su búsqueda.
7. Localice el recurso que tiene los datos que desea restaurar y seleccione **Ver todas las copias de**

seguridad para mostrar todos los archivos de copia de seguridad que contienen el volumen, la carpeta o el archivo correspondiente.

8. Localice el archivo de respaldo que desea utilizar para restaurar los datos y seleccione **Restaurar**.

Tenga en cuenta que los resultados identifican instantáneas de volumen locales y volúmenes replicados remotos que contienen el archivo de su búsqueda. Puede elegir restaurar desde el archivo de copia de seguridad en la nube, desde la instantánea o desde el volumen replicado.

9. Seleccione la ubicación de destino donde desea que se restaure el volumen, la carpeta o los archivos y seleccione **Restaurar**.
 - Para los volúmenes, puede seleccionar el sistema de destino original o puede seleccionar un sistema alternativo. Al restaurar un volumen FlexGroup, deberá elegir varios agregados.
 - Para las carpetas, puede restaurarlas a la ubicación original o puede seleccionar una ubicación alternativa; incluido el sistema, el volumen y la carpeta.
 - Para los archivos, puede restaurarlos a la ubicación original o puede seleccionar una ubicación alternativa; incluido el sistema, el volumen y la carpeta. Al seleccionar la ubicación original, puede optar por sobrescribir los archivos de origen o crear archivos nuevos.

Si selecciona un sistema ONTAP local y aún no ha configurado la conexión del clúster al almacenamiento de objetos, se le solicitará información adicional:

- Al restaurar desde Amazon S3, seleccione el espacio IP en el clúster ONTAP donde residirá el volumen de destino, ingrese la clave de acceso y la clave secreta del usuario que creó para darle al clúster ONTAP acceso al bucket S3 y, opcionalmente, elija un punto final de VPC privado para una transferencia de datos segura. "[Ver detalles sobre estos requisitos](#)".
- Al restaurar desde Azure Blob, seleccione el espacio IP en el clúster ONTAP donde residirá el volumen de destino y, opcionalmente, elija un punto final privado para la transferencia de datos segura seleccionando la red virtual y la subred. "[Ver detalles sobre estos requisitos](#)".
- Al restaurar desde Google Cloud Storage, seleccione el espacio IP en el clúster ONTAP donde residirá el volumen de destino, y la clave de acceso y la clave secreta para acceder al almacenamiento de objetos. "[Ver detalles sobre estos requisitos](#)".
- Al restaurar desde StorageGRID, ingrese el FQDN del servidor StorageGRID y el puerto que ONTAP debe usar para la comunicación HTTPS con StorageGRID, ingrese la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP en el clúster ONTAP donde reside el volumen de destino. "[Ver detalles sobre estos requisitos](#)".
- Al restaurar desde ONTAP S3, ingrese el FQDN del servidor ONTAP S3 y el puerto que ONTAP debe usar para la comunicación HTTPS con ONTAP S3, seleccione la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP en el clúster ONTAP donde residirá el volumen de destino. "[Ver detalles sobre estos requisitos](#)".

Resultados

Se restauran el volumen, la carpeta o los archivos y regresa al Panel de restauración para que pueda revisar el progreso de la operación de restauración. También puede seleccionar la pestaña **Monitoreo de trabajos** para ver el progreso de la restauración. Ver "[Página de monitorización de trabajos](#)".

Restaurar datos de ONTAP mediante Explorar y restaurar

Con NetApp Backup and Recovery, restaure los datos de ONTAP mediante la función Explorar y restaurar. Antes de restaurar, anote el nombre del volumen de origen, el sistema de origen y el SVM, y la fecha del archivo de copia de seguridad. Puede

restaurar datos de ONTAP desde una instantánea, un volumen replicado o desde copias de seguridad almacenadas en almacenamiento de objetos.

Las capacidades de restauración dependen de su versión de ONTAP :

- **Carpetas:** Con ONTAP 9.13.0 o superior, puede restaurar carpetas con todos los archivos y subcarpetas; con versiones anteriores, solo puede restaurar archivos en la carpeta.
- **Almacenamiento de archivo:** La restauración desde el almacenamiento de archivo (disponible con ONTAP 9.10.1 o superior) es más lenta y podría generar costos adicionales.
- **Requisitos del clúster de destino:**
 - Restauración de volumen: ONTAP 9.10.1 o superior
 - Recuperación de archivos: ONTAP 9.11.1 o superior
 - Google Archive y StorageGRID: ONTAP 9.12.1 o superior
 - Restauración de carpetas: ONTAP 9.13.1 o superior

["Obtenga más información sobre la restauración desde el almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre la restauración desde el almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre cómo restaurar desde el almacenamiento de archivo de Google"](#).



La prioridad alta no se admite al restaurar datos desde el almacenamiento de archivo de Azure a sistemas StorageGRID .

Explorar y restaurar sistemas compatibles y proveedores de almacenamiento de objetos

Puede restaurar datos de ONTAP desde un archivo de respaldo que reside en un sistema secundario (un volumen replicado) o en un almacenamiento de objetos (un archivo de respaldo) en los siguientes sistemas. Las instantáneas residen en el sistema de origen y solo se pueden restaurar en ese mismo sistema.

Nota: Puede restaurar un volumen desde cualquier tipo de archivo de respaldo, pero en este momento solo puede restaurar una carpeta o archivos individuales desde un archivo de respaldo en el almacenamiento de objetos.

Desde el almacén de objetos (copia de seguridad)	Desde Primaria (Instantánea)	Desde el sistema secundario (replicación)	Al sistema de destino
Amazon S3	Cloud Volumes ONTAP en el sistema ONTAP local de AWS	Cloud Volumes ONTAP en el sistema ONTAP local de AWS	Blob de Azure
Cloud Volumes ONTAP en el sistema ONTAP local de Azure	Cloud Volumes ONTAP en el sistema ONTAP local de Azure	Almacenamiento en la nube de Google	Cloud Volumes ONTAP en el sistema Google On-premises ONTAP
Cloud Volumes ONTAP en el sistema Google On-premises ONTAP	StorageGRID en NetApp	Sistema ONTAP local	Sistema ONTAP local Cloud Volumes ONTAP
Al sistema ONTAP local	ONTAP S3	Sistema ONTAP local	Sistema ONTAP local Cloud Volumes ONTAP

Para explorar y restaurar, el agente de consola se puede instalar en las siguientes ubicaciones:

- Para Amazon S3, el agente de consola se puede implementar en AWS o en sus instalaciones
- Para Azure Blob, el agente de consola se puede implementar en Azure o en sus instalaciones.
- Para Google Cloud Storage, el agente de la consola debe implementarse en su VPC de Google Cloud Platform
- Para StorageGRID, el agente de consola debe implementarse en sus instalaciones, con o sin acceso a Internet.
- Para ONTAP S3, el agente de consola se puede implementar en sus instalaciones (con o sin acceso a Internet) o en un entorno de proveedor de nube.

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



Si la versión de ONTAP en su sistema es inferior a 9.13.1, no podrá restaurar carpetas o archivos si el archivo de respaldo se ha configurado con DataLock y Ransomware. En este caso, puede restaurar todo el volumen desde el archivo de respaldo y luego acceder a los archivos que necesita.

Restaurar volúmenes mediante Explorar y restaurar

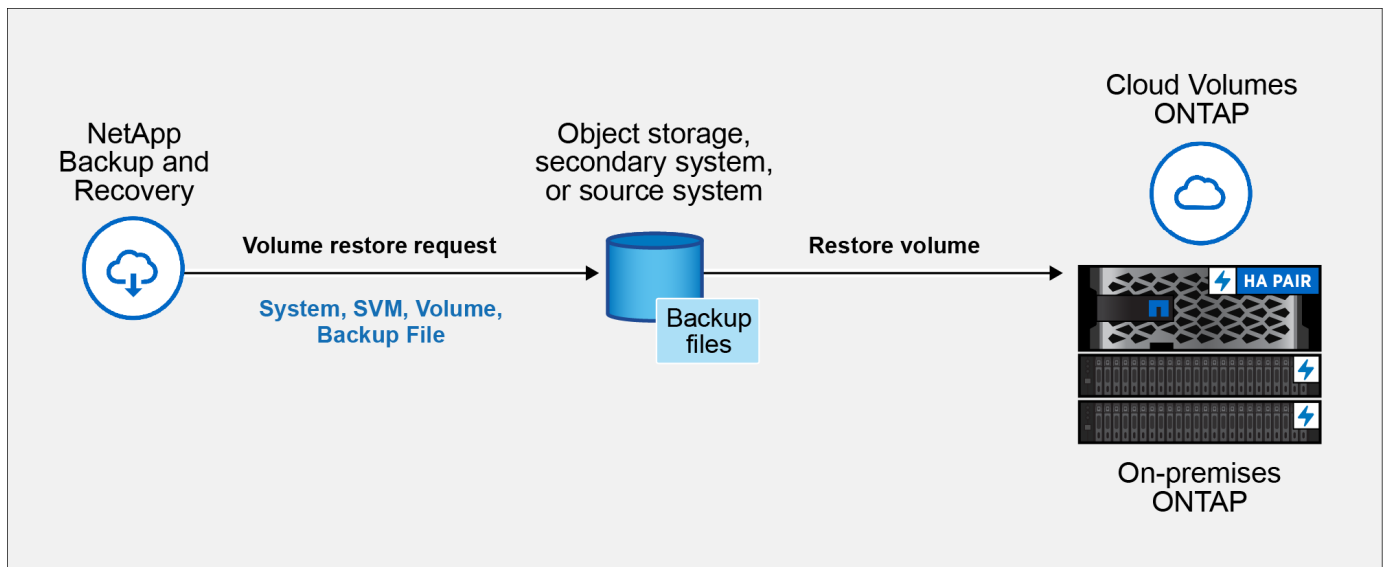
Cuando restaura un volumen desde un archivo de respaldo, NetApp Backup and Recovery crea un *nuevo* volumen usando los datos del respaldo. Al usar una copia de seguridad desde un almacenamiento de objetos, puede restaurar los datos en un volumen en el sistema original, en un sistema diferente ubicado en la misma cuenta en la nube que el sistema de origen o en un sistema ONTAP local.

Al restaurar una copia de seguridad en la nube en un sistema Cloud Volumes ONTAP que utiliza ONTAP 9.13.0 o superior, o en un sistema ONTAP local que ejecuta ONTAP 9.14.1, tendrá la opción de realizar una operación de *restauración rápida*. La restauración rápida es ideal para situaciones de recuperación ante desastres donde necesita proporcionar acceso a un volumen lo antes posible. Una restauración rápida restaura los metadatos del archivo de respaldo a un volumen en lugar de restaurar el archivo de respaldo completo. No se recomienda la restauración rápida para aplicaciones sensibles al rendimiento o a la latencia, y no es compatible con copias de seguridad en almacenamiento archivado.



La restauración rápida solo es compatible con volúmenes FlexGroup si el sistema de origen desde el cual se creó la copia de seguridad en la nube ejecutaba ONTAP 9.12.1 o superior. Y solo es compatible con volúmenes SnapLock si el sistema de origen ejecutaba ONTAP 9.11.0 o superior.

Al restaurar desde un volumen replicado, puede restaurar el volumen al sistema original o a un sistema Cloud Volumes ONTAP o ONTAP local.



Para restaurar un volumen, necesita el nombre del sistema de origen, la máquina virtual de almacenamiento, el nombre del volumen y la fecha del archivo de copia de seguridad.

Pasos

1. Desde el menú Consola, seleccione **Protección > Copia de seguridad y recuperación**.
2. Seleccione la pestaña **Restaurar** y se mostrará el Panel de restauración.
3. Desde la sección *Explorar y restaurar*, seleccione **Restaurar volumen**.
4. En la página *Seleccionar origen*, navegue hasta el archivo de respaldo del volumen que desea restaurar. Seleccione el **sistema**, el **volumen** y el archivo de **copia de seguridad** que tenga la marca de fecha y hora desde el que desea restaurar.

La columna **Ubicación** muestra si el archivo de copia de seguridad (instantánea) es **Local** (una instantánea en el sistema de origen), **Secundario** (un volumen replicado en un sistema ONTAP secundario) o **Almacenamiento de objetos** (un archivo de copia de seguridad en almacenamiento de objetos). Seleccione el archivo que desea restaurar.

5. Seleccione **Siguiente**.

Tenga en cuenta que si selecciona un archivo de respaldo en el almacenamiento de objetos y Ransomware Resilience está activo para ese respaldo (si habilitó DataLock y Ransomware Resilience en la política de respaldo), se le solicitará que ejecute un análisis de ransomware adicional en el archivo de respaldo antes de restaurar los datos. Le recomendamos que escanee el archivo de respaldo en busca de ransomware. (Incurrirá en costos de salida adicionales de su proveedor de nube para acceder al contenido del archivo de respaldo).

6. En la página *Seleccionar destino*, seleccione el **sistema** donde desea restaurar el volumen.
7. Al restaurar un archivo de respaldo desde un almacenamiento de objetos, si selecciona un sistema ONTAP local y aún no ha configurado la conexión del clúster al almacenamiento de objetos, se le solicitará información adicional:
 - Al restaurar desde Amazon S3, seleccione el espacio IP en el clúster ONTAP donde residirá el volumen de destino, ingrese la clave de acceso y la clave secreta del usuario que creó para darle al clúster ONTAP acceso al bucket S3 y, opcionalmente, elija un punto final de VPC privado para una transferencia de datos segura.
 - Al restaurar desde Azure Blob, seleccione el espacio IP en el clúster ONTAP donde residirá el volumen

de destino, seleccione la suscripción de Azure para acceder al almacenamiento de objetos y, opcionalmente, elija un punto final privado para la transferencia segura de datos seleccionando la red virtual y la subred.

- Al restaurar desde Google Cloud Storage, seleccione el proyecto de Google Cloud y la clave de acceso y la clave secreta para acceder al almacenamiento de objetos, la región donde se almacenan las copias de seguridad y el espacio IP en el clúster ONTAP donde residirá el volumen de destino.
- Al restaurar desde StorageGRID, ingrese 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 en el clúster ONTAP donde residirá el volumen de destino.
- Al restaurar desde ONTAP S3, ingrese el FQDN del servidor ONTAP S3 y el puerto que ONTAP debe usar para la comunicación HTTPS con ONTAP S3, seleccione la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP en el clúster ONTAP donde residirá el volumen de destino.

8. Ingrese el nombre que desea utilizar para el volumen restaurado y seleccione la máquina virtual de almacenamiento y el agregado donde residirá el volumen. Al restaurar un volumen FlexGroup, deberá seleccionar varios agregados. De forma predeterminada, se utiliza **<source_volume_name>_restore** como nombre del volumen.

Al restaurar una copia de seguridad desde un almacenamiento de objetos a un sistema Cloud Volumes ONTAP que utiliza ONTAP 9.13.0 o superior, o a un sistema ONTAP local que ejecuta ONTAP 9.14.1, tendrá la opción de realizar una operación de *restauración rápida*.

Y si está restaurando el volumen desde un archivo de respaldo que reside en un nivel de almacenamiento de archivo (disponible a partir de ONTAP 9.10.1), puede seleccionar la Prioridad de restauración.

["Obtenga más información sobre la restauración desde el almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre la restauración desde el almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre cómo restaurar desde el almacenamiento de archivo de Google"](#). Los archivos de respaldo en el nivel de almacenamiento de Google Archive se restauran casi de inmediato y no requieren prioridad de restauración.

9. Seleccione **Siguiente** para elegir si desea realizar un proceso de restauración normal o de restauración rápida:
- **Restauración normal:** utilice la restauración normal en volúmenes que requieran alto rendimiento. Los volúmenes no estarán disponibles hasta que se complete el proceso de restauración.
 - **Restauración rápida:** Los volúmenes y datos restaurados estarán disponibles de inmediato. No utilice esto en volúmenes que requieran alto rendimiento porque durante el proceso de restauración rápida, el acceso a los datos podría ser más lento de lo habitual.
10. Seleccione **Restaurar** y regresará al Panel de restauración para que pueda revisar el progreso de la operación de restauración.

Resultado

NetApp Backup and Recovery crea un nuevo volumen basado en la copia de seguridad que seleccionó.

Tenga en cuenta que restaurar un volumen desde un archivo de respaldo que reside en un almacenamiento de archivo puede demorar muchos minutos u horas según el nivel de archivo y la prioridad de restauración. Puede seleccionar la pestaña **Monitoreo de trabajo** para ver el progreso de la restauración.

Restaurar carpetas y archivos usando Explorar y restaurar

Si necesita restaurar solo unos pocos archivos de una copia de seguridad de volumen ONTAP , puede optar por restaurar una carpeta o archivos individuales en lugar de restaurar el volumen completo. Puede restaurar carpetas y archivos en un volumen existente en el sistema original o en un sistema diferente que utilice la misma cuenta en la nube. También puede restaurar carpetas y archivos a un volumen en un sistema ONTAP local.



En este momento, solo puede restaurar una carpeta o archivos individuales desde un archivo de respaldo en el almacenamiento de objetos. Actualmente no se admite la restauración de archivos y carpetas desde una instantánea local o desde un archivo de copia de seguridad que reside en un sistema secundario (un volumen replicado).

Si selecciona varios archivos, se restaurarán en el mismo volumen de destino. Para restaurar archivos en diferentes volúmenes, ejecute el proceso varias veces.

Al utilizar ONTAP 9.13.0 o superior, puede restaurar una carpeta junto con todos los archivos y subcarpetas que contiene. Al utilizar una versión de ONTAP anterior a 9.13.0, solo se restauran los archivos de esa carpeta; no se restauran las subcarpetas ni los archivos dentro de las subcarpetas.

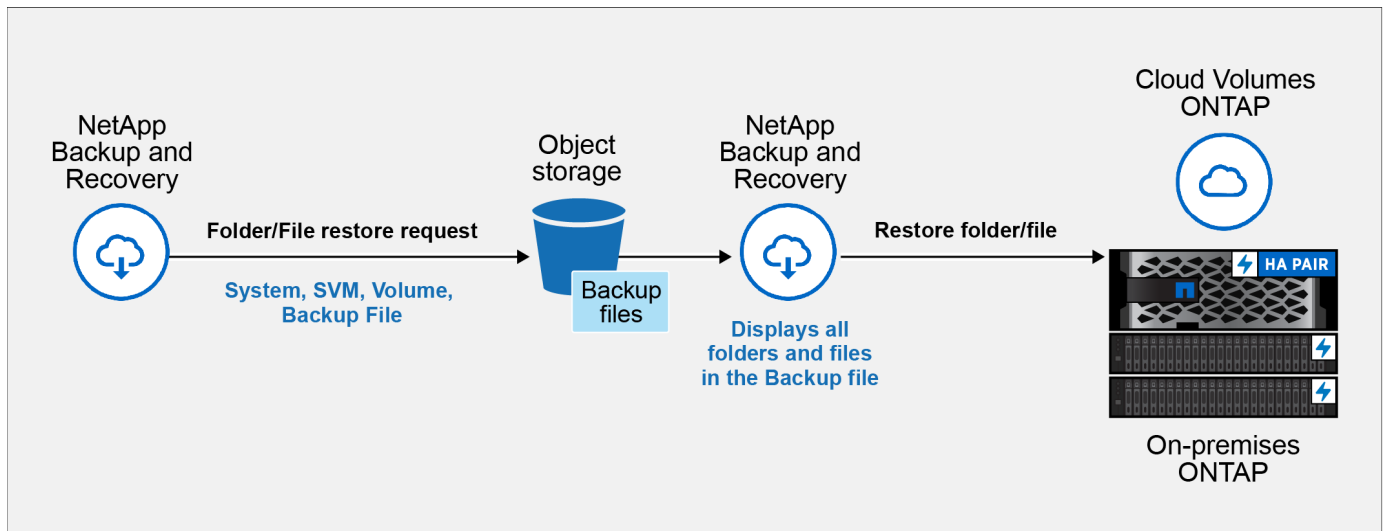


- Si el archivo de respaldo se configuró con protección DataLock y Ransomware, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o superior. Si está utilizando una versión anterior de ONTAP, puede restaurar todo el volumen desde el archivo de respaldo y luego acceder a la carpeta y los archivos que necesita.
- Si el archivo de respaldo reside en el almacenamiento de archivo, la restauración a nivel de carpeta solo se admite si la versión de ONTAP es 9.13.1 o superior. Si está utilizando una versión anterior de ONTAP, puede restaurar la carpeta desde un archivo de respaldo más nuevo que no se haya archivado, o puede restaurar el volumen completo desde el respaldo archivado y luego acceder a la carpeta y los archivos que necesita.
- Con ONTAP 9.15.1, puedes restaurar carpetas de FlexGroup usando la opción "Examinar y restaurar".

Puedes probarlo usando una bandera especial descrita en el ["Blog de la versión de julio de 2024 de NetApp Backup and Recovery"](#) .

Restaurar carpetas y archivos

Siga estos pasos para restaurar carpetas o archivos a un volumen desde una copia de seguridad de volumen ONTAP . Debe saber el nombre del volumen y la fecha del archivo de respaldo que desea utilizar para restaurar la carpeta o los archivos. Esta funcionalidad utiliza la navegación en vivo para que pueda ver la lista de directorios y archivos dentro de cada archivo de respaldo.



Antes de empezar

- La versión de ONTAP debe ser 9.6 o superior para realizar operaciones de restauración de *archivos*.
- La versión de ONTAP debe ser 9.11.1 o superior para realizar operaciones de restauración de *carpeta*. Se requiere la versión 9.13.1 de ONTAP si los datos están en un almacenamiento de archivo o si el archivo de respaldo utiliza protección DataLock y contra ransomware.
- La versión de ONTAP debe ser 9.15.1 p2 o superior para restaurar directorios FlexGroup usando la opción Explorar y restaurar.

Pasos

1. Desde el menú Consola, seleccione **Protección > Copia de seguridad y recuperación**.
2. Seleccione la pestaña **Restaurar** y se mostrará el Panel de restauración.
3. Desde la sección *Explorar y restaurar*, seleccione **Restaurar archivos o carpeta**.
4. En la página *Seleccionar origen*, navegue hasta el archivo de respaldo del volumen que contiene la carpeta o los archivos que desea restaurar. Seleccione el **sistema**, el **volumen** y la **copia de seguridad** que tenga la marca de fecha y hora desde donde desea restaurar los archivos.
5. Seleccione **Siguiente** y se mostrará la lista de carpetas y archivos de la copia de seguridad del volumen.

Si está restaurando carpetas o archivos desde un archivo de respaldo que reside en un nivel de almacenamiento de archivo, puede seleccionar la Prioridad de restauración.

["Obtenga más información sobre la restauración desde el almacenamiento de archivo de AWS"](#). ["Obtenga más información sobre la restauración desde el almacenamiento de archivo de Azure"](#). ["Obtenga más información sobre cómo restaurar desde el almacenamiento de archivo de Google"](#). Los archivos de respaldo en el nivel de almacenamiento de Google Archive se restauran casi de inmediato y no requieren prioridad de restauración.

Y si Ransomware Resilience está activo para el archivo de respaldo (si habilitó DataLock y Ransomware Resilience en la política de respaldo), entonces se le solicitará que ejecute un análisis de ransomware adicional en el archivo de respaldo antes de restaurar los datos. Le recomendamos que escanee el archivo de respaldo en busca de ransomware. (Incurrirá en costos de salida adicionales de su proveedor de nube para acceder al contenido del archivo de respaldo).

6. En la página *Seleccionar elementos*, seleccione la carpeta o los archivos que desea restaurar y seleccione **Continuar**. Para ayudarlo a encontrar el artículo:

- Puede seleccionar la carpeta o el nombre del archivo si lo ve.
- Puede seleccionar el icono de búsqueda e ingresar el nombre de la carpeta o archivo para navegar directamente al elemento.
- Puede navegar hacia abajo en los niveles de las carpetas usando la flecha hacia abajo al final de la fila para encontrar archivos específicos.

A medida que selecciona archivos, estos se agregan al lado izquierdo de la página para que pueda ver los archivos que ya ha elegido. Puede eliminar un archivo de esta lista si es necesario seleccionando la **x** junto al nombre del archivo.

7. En la página *Seleccionar destino*, seleccione el **sistema** donde desea restaurar los elementos.

Si selecciona un clúster local y aún no ha configurado la conexión del clúster al almacenamiento de objetos, se le solicitará información adicional:

- Al restaurar desde Amazon S3, ingrese el espacio IP en el clúster ONTAP donde reside el volumen de destino, y la clave de acceso de AWS y la clave secreta necesarias para acceder al almacenamiento de objetos. También puede seleccionar una configuración de enlace privado para la conexión al clúster.
- Al restaurar desde Azure Blob, ingrese el espacio IP en el clúster ONTAP donde reside el volumen de destino. También puede seleccionar una configuración de punto final privado para la conexión al clúster.
- Al restaurar desde Google Cloud Storage, ingrese el espacio IP en el clúster ONTAP donde residen los volúmenes de destino, y la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos.
- Al restaurar desde StorageGRID, ingrese el FQDN del servidor StorageGRID y el puerto que ONTAP debe usar para la comunicación HTTPS con StorageGRID, ingrese la clave de acceso y la clave secreta necesarias para acceder al almacenamiento de objetos, y el espacio IP en el clúster ONTAP donde reside el volumen de destino.

8. Luego seleccione el **Volumen** y la **Carpeta** donde desea restaurar la carpeta o los archivos.

Tiene algunas 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 cursor sobre una carpeta y hacer clic al final de la fila para explorar las subcarpetas y luego seleccionar una carpeta.
- Si ha seleccionado el mismo sistema de destino y volumen donde se encontraba la carpeta/archivo de origen, puede seleccionar **Mantener ruta de la carpeta de origen** para restaurar la carpeta o los archivos a la misma carpeta donde existían en la estructura de origen. Todas las mismas carpetas y subcarpetas deben existir previamente; no se crean carpetas. Al restaurar archivos a su ubicación original, puede optar por sobrescribir los archivos de origen o crear archivos nuevos.

9. Seleccione **Restaurar** para volver al Panel de Restauración y revisar el progreso de la operación de restauración.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.