Referencia

Cloud Backup

NetApp
March 13, 2023

Tabla de Contenido

Referencia

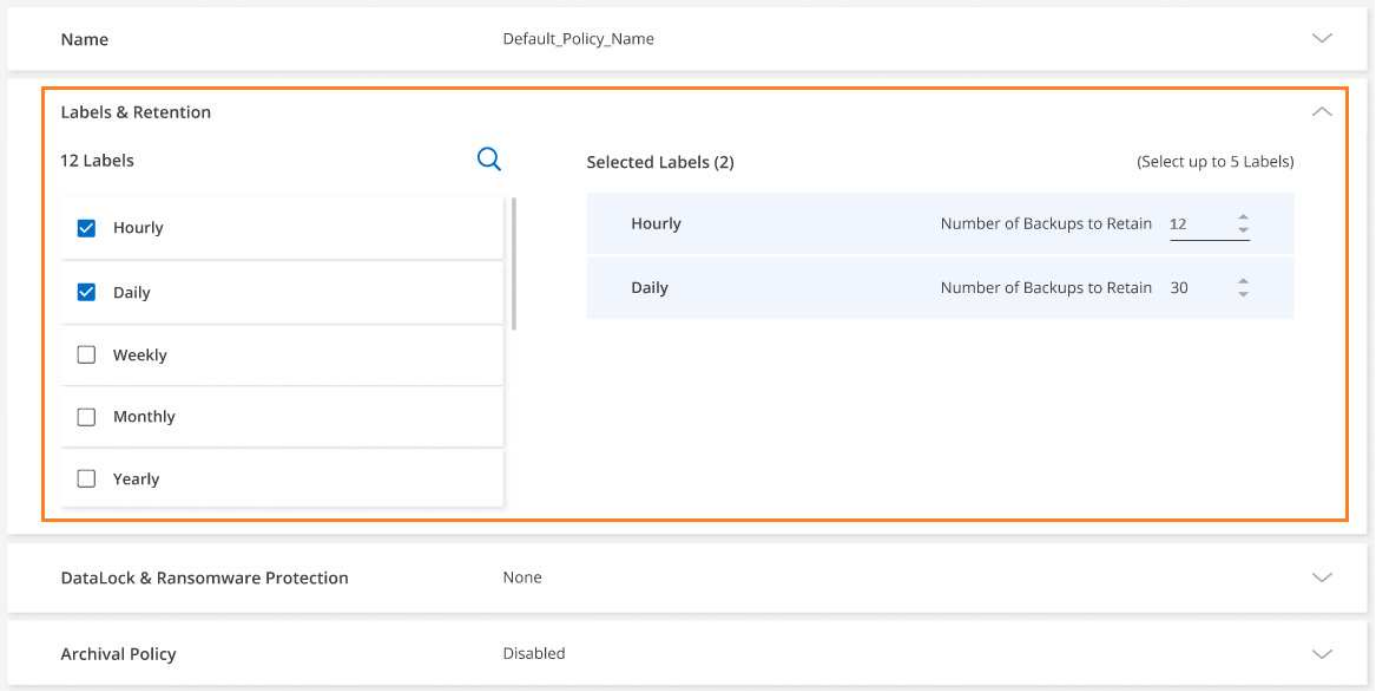
Opciones de configuración de la política de Cloud Backup

Este documento describe las opciones de configuración de políticas de backup para sistemas ONTAP en las instalaciones y sistemas Cloud Volumes ONTAP cuando se utiliza Cloud Backup Service.

Programaciones de backup

Cloud Backup permite crear varias políticas de backup con programaciones únicas para cada entorno de trabajo (clúster). Es posible asignar diferentes políticas de backup a volúmenes con diferentes objetivos de punto de recuperación (RPO).

Cada directiva de copia de seguridad proporciona una sección para *Labels & Retention* que puede aplicar a sus archivos de copia de seguridad.



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

- **Label** define la frecuencia con la que se crea (o actualiza) un archivo de copia de seguridad desde el volumen. Puede seleccionar entre los siguientes tipos de etiquetas:
  - Puede elegir uno o una combinación de, **cada hora**, **diario**, **semanal**, **mensual**, y **anualmente** plazos.
  - Puede seleccionar una de las políticas definidas por el sistema que proporcione backup y retención durante 3 meses, 1 año o 7 años.
  - Si creó políticas de protección de backup personalizadas en el clúster mediante ONTAP System Manager o la CLI de ONTAP, puede seleccionar una de esas políticas.
- El valor **Retention** define cuántos archivos de copia de seguridad se conservan para cada etiqueta (intervalo de tiempo). Una vez alcanzado el número máximo de backups en una categoría o intervalo, se eliminan los backups más antiguos de modo que siempre habrá los backups más recientes. Esto también

ahorra costes de almacenamiento ya que los backups obsoletos no continúan ocupar espacio en el cloud.

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

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

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

Protección de DataLock y ransomware

Cloud Backup ofrece compatibilidad con la protección de DataLock y Ransomware para los backups de volúmenes. Estas funciones le permiten bloquear los archivos de backup y analizarlos para detectar posibles ransomware en los archivos de backup. Este es un ajuste opcional que se puede definir en las políticas de backup cuando se desea contar con protección adicional para los backups de volúmenes para un clúster de.

Ambas funciones protegen sus archivos de backup de forma que siempre tendrá un archivo de backup válido para recuperar los datos desde un ataque de ransomware en sus datos de origen. También resulta útil satisfacer ciertos requisitos normativos en los que los backups deben bloquearse y conservarse durante un cierto período de tiempo. Cuando se habilita la protección de DataLock y ransomware, el bloque de cloud que se aprovisiona como parte de la activación de Cloud Backup tendrá habilitado el bloqueo de objetos y el control de versiones de objetos.

"Consulte el blog de protección de DataLock y Ransomware para obtener más información".

Esta función no ofrece protección para los volúmenes de origen, solo para los backups de esos volúmenes de origen. Utilice NetApp "Cloud Insights y Cloud Secure", o alguna de las "Protecciones contra el ransomware proporcionadas por ONTAP" para proteger los volúmenes de origen.

- Si tiene previsto utilizar la protección DataLock y Ransomware, debe habilitarla cuando cree su primera política de backup y active Cloud Backup para ese clúster.
- La protección de DataLock y Ransomware no se puede deshabilitar para un clúster una vez que se ha configurado. No habilite esta función en un clúster para probarlo.

Qué es DataLock

DataLock protege sus archivos de copia de seguridad de ser modificados o eliminados durante un período de tiempo determinado. Esta funcionalidad utiliza la tecnología del proveedor de almacenamiento de objetos para "bloqueo de objetos". El período de tiempo durante el que el archivo de copia de seguridad está bloqueado (y retenido) se denomina período de retención de DataLock. Se basa en la programación de la política de backup y la configuración de retención que haya definido, más un búfer de 14 días. Cualquier política de retención de DataLock que sea inferior a 30 días se redondea a un mínimo de 30 días.

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

Veamos algunos ejemplos de cómo funciona:

- Si crea una programación de backup mensual con 12 retentions, cada backup queda bloqueado durante 12 meses (más 14 días) antes de eliminarlo.
- Si crea una política de backup que crea 30 backups diarios, 7 semanales y 12 mensuales, habrá tres periodos de retención bloqueados. Los backups «30 diarios» se conservarían durante 44 días (30 días más 14 días de búfer), los backups «7 semanales» se conservarían durante 9 semanas (7 semanas más 14 días) y los backups «12 mensuales» se conservarían durante 12 meses (más 14 días).
- Si crea una programación de backup horaria con 24 retentions, puede pensar que los backups están bloqueados durante 24 horas. Sin embargo, dado que es inferior al mínimo de 30 días, cada backup se bloqueará y conservará durante 44 días (30 días más 14 días de búfer).

  En este último caso, puede comprobar que si cada archivo de copia de seguridad está bloqueado durante 44 días, tendrá muchos más archivos de copia de seguridad de los que se tendrían normalmente con una normativa de repetición por hora/24. Normalmente, cuando Cloud Backup crea el archivo de backup 25, se elimina el backup más antiguo para mantener las retentions máximas en 24 (según la política). En este caso, la configuración de retención de DataLock anula la configuración de retención de directivas de la política de copia de seguridad. Esto podría afectar a los costes de almacenamiento, ya que los archivos de backup se guardarán en el almacén de objetos durante un periodo de tiempo más largo.

Qué es la protección contra Ransomware

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

Los análisis de ransomware se producen en 3 puntos del proceso de backup y restauración:

- Cuando se crea un archivo de copia de seguridad

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

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

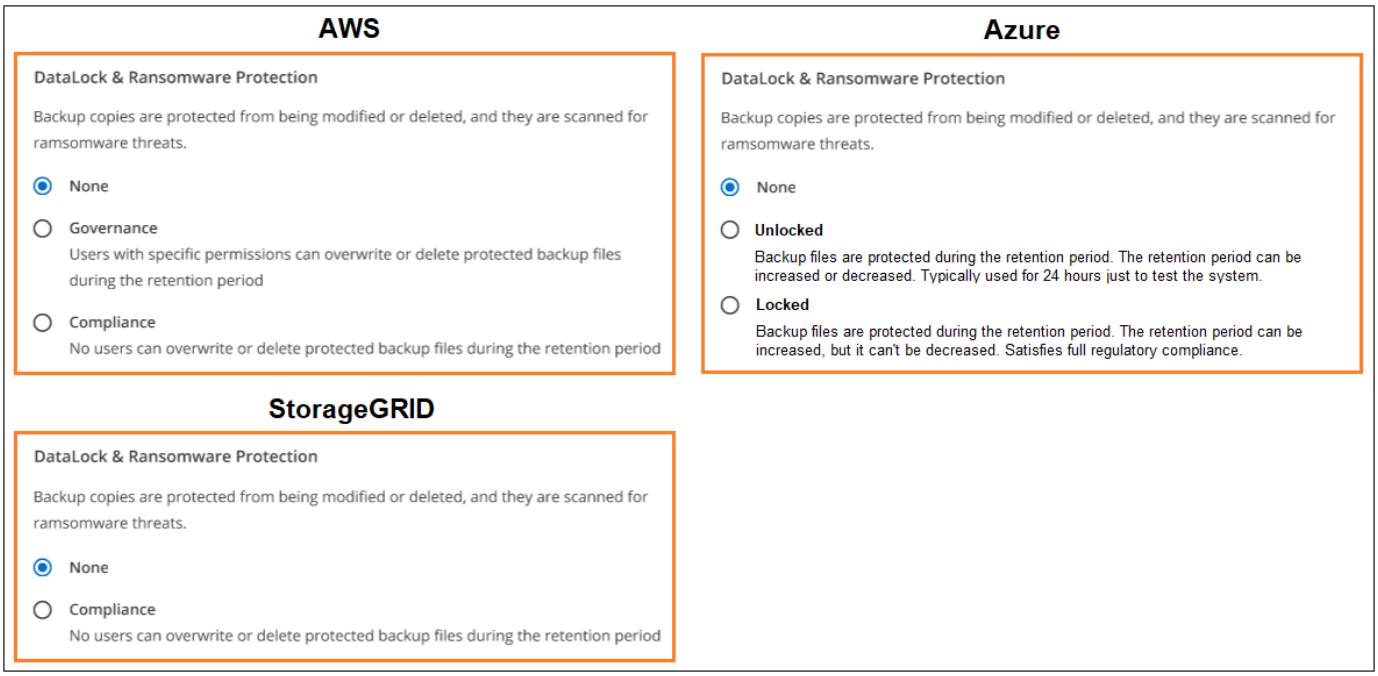
  Puede elegir ejecutar un análisis antes de restaurar datos de un archivo de copia de seguridad o omitir este análisis.

- Manualmente

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

Configuración de protección de DataLock y Ransomware

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



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

AWS

- **Ninguno** (predeterminado)

  La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Gobierno**

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

- **Cumplimiento**

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

Azure

- **Ninguno** (predeterminado)

  La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Desbloqueado**

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

- **Bloqueado**

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

StorageGRID

- **Ninguno** (predeterminado)

  La protección DataLock y la protección contra ransomware están deshabilitadas.

- **Cumplimiento**

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

Entornos de trabajo y proveedores de almacenamiento de objetos compatibles

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

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

Requisitos

- Sus clústeres deben ejecutar ONTAP 9.11.1 o superior (9.12.1 en el caso de Azure).
- Debe utilizar BlueXP 3.9.21 o superior
- Para AWS:
  - El conector puede ponerse en marcha en el cloud o en sus instalaciones
  - Los siguientes permisos S3 deben formar parte del rol IAM que proporciona el conector con permisos. Residen en la sección "backupS3Policy" para el recurso "arn:aws:s3::netapp-backup-*":
    - s3:GetObjectVersionTagging
    - s3:GetBucketObjectLockConfiguration
    - s3:GetObjectVersionAcl
    - s3:PutObjectEtiquetado
    - s3:DeleteObject
    - s3:DeleteObjectTagging
    - s3:GetObjectRetention
    - s3:DeleteObjectVersionTagging
    - s3:PutObject
    - s3:GetObject
    - s3:PutBucketObjectLockConfiguration
    - s3:GetLifecycleConfiguration
    - s3:ListBucketByTags
    - s3:GetBucketTagging
    - s3:DeleteObjectVersion
    - s3:ListBucketVersions
    - s3:ListBucket
    - s3:PutBucketEtiquetado
    - s3:GetObjectTagging
    - s3:PutBucketVersioning
    - s3:PutObjectVersionEtiquetado
    - s3:GetBucketVersioning

        - s3:GetBucketAcl
        - s3:BypassGovernanceRetention
        - s3:PutObjectRetention
        - s3:GetBucketLocation
        - s3:GetObjectVersion

          "Vea el formato JSON completo para la directiva donde puede copiar y pegar los permisos necesarios".

- Para Azure:
    - El conector puede ponerse en marcha en el cloud o en sus instalaciones
- Para StorageGRID:
    - Se requiere StorageGRID 11.6.0.3 y superior para una compatibilidad total con las funciones de DataLock
    - El conector debe estar desplegado en sus instalaciones (se puede instalar en un sitio con o sin acceso a Internet)
    - Los siguientes permisos S3 deben formar parte del rol IAM que proporciona el conector permisos:
        - s3:GetObjectVersionTagging
        - s3:GetBucketObjectLockConfiguration
        - s3:GetObjectVersionAcl
        - s3:PutObjectEtiquetado
        - s3:DeleteObject
        - s3:DeleteObjectTagging
        - s3:GetObjectRetention
        - s3:DeleteObjectVersionTagging
        - s3:PutObject
        - s3:GetObject
        - s3:PutBucketObjectLockConfiguration
        - s3:GetLifecycleConfiguration
        - s3:ListBucketByTags
        - s3:GetBucketTagging
        - s3:DeleteObjectVersion
        - s3:ListBucketVersions
        - s3:ListBucket
        - s3:PutBucketEtiquetado
        - s3:GetObjectTagging
        - s3:PutBucketVersioning
        - s3:PutObjectVersionEtiquetado
        - s3:GetBucketVersioning

- s3:GetBucketAcl
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Restricciones

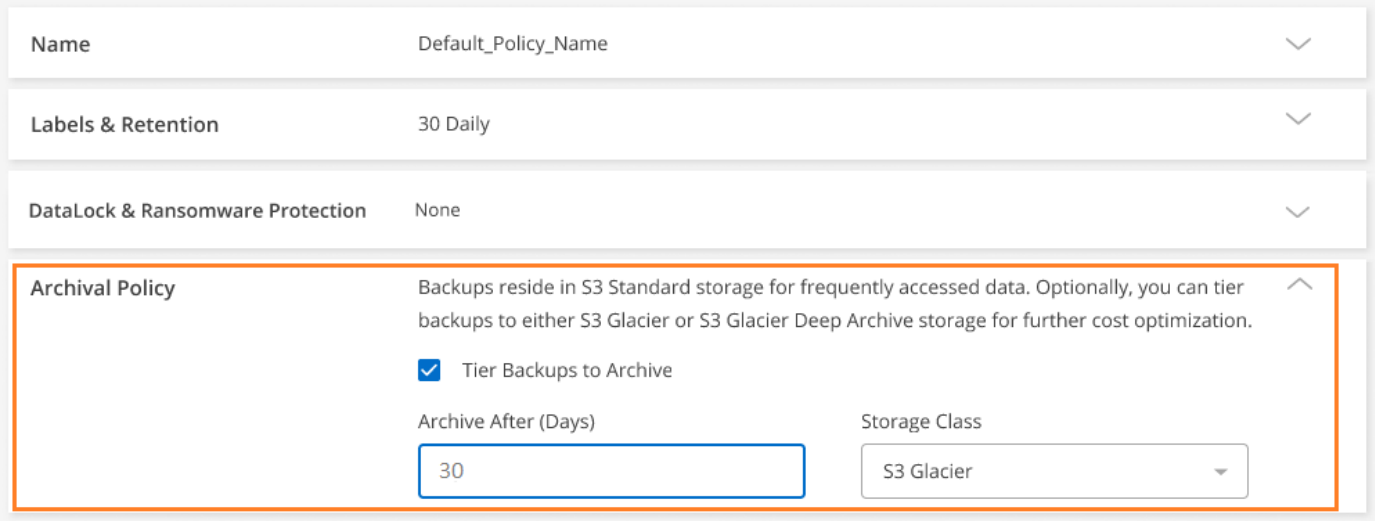
- La protección de DataLock y Ransomware no está disponible si ha configurado el almacenamiento de archivado en la normativa de backup.
- La opción DataLock que seleccione al activar Cloud Backup debe utilizarse para todas las políticas de backup del clúster.
- No se pueden utilizar ambos modos DataLock en un solo clúster.
- Si activa DataLock, se bloquearán todas las copias de seguridad de los volúmenes. No se pueden mezclar backups de volúmenes bloqueados y no bloqueados para un solo clúster.
- La protección de DataLock y ransomware se aplica a backups de volúmenes nuevos con una política de backup con protección de datos Lock y ransomware habilitada. No se puede habilitar esta función después de activar Cloud Backup.

Configuración de almacenamiento de archivado

Al usar cierto almacenamiento en cloud, se pueden mover los archivos de backup antiguos a un nivel de acceso/clase de almacenamiento más económico tras un determinado número de días. Tenga en cuenta que el almacenamiento de archivado no se puede utilizar si ha habilitado DataLock.

No se puede acceder inmediatamente a los datos en el nivel de archivado cuando sea necesario y exige un mayor coste de recuperación, por lo que debe plantearse la frecuencia con la que es necesario restaurar datos desde ficheros de backup archivados.

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



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

  Si el clúster utiliza ONTAP 9.10.1 o superior, puede organizar en niveles los backups antiguos en el

almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive*. "Obtenga más información acerca del almacenamiento de archivado de AWS".

Tenga en cuenta que si elige *S3 Glacier* o *S3 Glacier Deep Archive* en la primera política de backup al activar Cloud Backup, ese nivel será el único nivel de archivado disponible para futuras políticas de backup para ese clúster. Si selecciona ningún nivel de archivado en su primera política de copia de seguridad, *S3 Glacier* será la única opción de archivado para futuras políticas.

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

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

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

  Si su clúster local utiliza ONTAP 9.12.1 o más, puede optar por organizar los backups antiguos en el almacenamiento *Archive* en la interfaz de usuario de backup en el cloud tras un determinado número de días para obtener mayor optimización de los costes. "Más información sobre el almacenamiento de archivos de Google".

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

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

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

+ ** para Azure, puede organizar en niveles los backups antiguos para el almacenamiento *Azure Archive*. "Obtenga más información sobre el almacenamiento de archivado de Azure".

+"Obtenga más información sobre el archivado de archivos de backup desde StorageGRID".

Clases de almacenamiento de archivado y tiempos de recuperación de restauraciones de AWS S3

Cloud Backup admite dos clases de almacenamiento de archivado S3 y la mayoría de regiones.

Clases de almacenamiento de archivado S3 compatibles para Cloud Backup

Cuando los archivos de copia de seguridad se crean inicialmente, se almacenan en almacenamiento S3 *Standard*. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia, pero esto también permite acceder a ellos de forma inmediata. Tras 30 días, los backups realizan la transición a la clase de almacenamiento S3 *Standard-Infrecuente Access* y se ahorran en costes.

Si los clústeres de origen ejecutan ONTAP 9.10.1 o superior, puede optar por organizar los backups en niveles en el almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive* tras un determinado número de días (normalmente más de 30 días) para obtener una mayor optimización de los costes. No se puede acceder inmediatamente a los datos de estos niveles cuando sea necesario y exige un mayor coste de recuperación, por lo que debe plantearse la frecuencia con la que es necesario restaurar los datos de estos ficheros de backup archivados. Consulte la sección Acerca de restaurar datos desde el almacenamiento de archivado.

Si elige *S3 Glacier* o *S3 Glacier Deep Archive* en la primera política de backup al activar Cloud Backup, ese nivel será el único nivel de archivado disponible para las futuras políticas de backup para ese clúster. Si selecciona ningún nivel de archivado en su primera política de copia de seguridad, *S3 Glacier* será la única opción de archivado para futuras políticas.

Tenga en cuenta que, al configurar Cloud Backup con este tipo de regla de ciclo de vida, no debe configurar ninguna regla del ciclo de vida al configurar el bloque en su cuenta de AWS.

"Obtenga información acerca de las clases de almacenamiento S3".

Restaurar datos desde el almacenamiento de archivado

A pesar de que el almacenamiento de ficheros de backup antiguos en un almacenamiento de archivado es mucho más barato que en los sistemas estándar o estándar, el acceso a los datos desde un archivo de backup del almacenamiento de archivado para las operaciones de restauración requiere más tiempo y supondrá un coste mayor.

¿Cuánto cuesta restaurar datos desde los profundos archivos Amazon S3 Glacier y Amazon S3 Glacier?

Puede elegir entre 3 prioridades de restauración al recuperar datos de Amazon S3 Glacier y 2 prioridades de restauración al recuperar datos de Amazon S3 Glacier Deep Archive. El archivo profundo de Glacier S3 es más caro que S3 Glacier:

Nivel de archivado	Prioridad y coste de la restauración		
	Alto	**Estándar**	**Baja**
Glaciar S3	Recuperación más rápida, mayor coste	Recuperación más lenta, menos coste	La recuperación más lenta, el coste más bajo
S3 Glacier Deep Archive		Recuperación más rápida, mayor coste	Recuperación más lenta, menor coste

Cada método tiene una tarifa de recuperación por GB diferente y una tarifa por solicitud. Para obtener información detallada sobre los precios de S3 Glacier por región de AWS, visite la "Página de precios de Amazon S3".

¿Cuánto tiempo tardaría en restaurar los objetos archivados en Amazon S3 Glacier?

Hay dos partes que componen el tiempo total de restauración:

- **Tiempo de recuperación**: El tiempo para recuperar el archivo de copia de seguridad del archivo y colocarlo en almacenamiento estándar. A esto se le llama a veces el tiempo de "rehidratación". El tiempo de recuperación varía según la prioridad de restauración seleccionada.

Nivel de archivado	Restaurar prioridad y tiempo de recuperación		
	Alto	**Estándar**	**Baja**
Glaciar S3	3-5 minutos	3-5 horas	5-12 horas
S3 Glacier Deep Archive		12 horas	48 horas

- **Tiempo de restauración**: Tiempo para restaurar los datos del archivo de copia de seguridad en almacenamiento estándar. Esta vez no difiere de la operación de restauración típica directamente del almacenamiento estándar cuando no se utiliza un nivel de archivado.

Para obtener más información sobre las opciones de recuperación de Amazon S3 Glacier y S3 Glacier Deep Archive, consulte "Preguntas frecuentes de Amazon sobre estas clases de almacenamiento".

Niveles de archivado y tiempos de recuperación de restauraciones de Azure

Cloud Backup admite un nivel de acceso de archivado de Azure y la mayoría de las regiones.

Niveles de acceso de Azure Blob compatibles para Cloud Backup

Cuando los archivos de copia de seguridad se crean inicialmente, se almacenan en el nivel de acceso *Cool*. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia; sin embargo, cuando sea necesario, es posible acceder de forma inmediata.

Si sus clústeres de origen ejecutan ONTAP 9.10.1 o más, puede optar por colocar en niveles los backups del almacenamiento *Cool* to *Azure Archive* tras un determinado número de días (normalmente más de 30 días) para obtener una mayor optimización de los costes. No se puede acceder inmediatamente a los datos de este nivel cuando sea necesario y exige un mayor coste de recuperación, por lo que debe plantearse la frecuencia con la que es necesario restaurar los datos de estos ficheros de backup archivados. Consulte la siguiente sección acerca de restaurar datos desde el almacenamiento de archivado.

Tenga en cuenta que al configurar Cloud Backup con este tipo de regla de ciclo de vida, no debe configurar ninguna regla de ciclo de vida al configurar el contenedor en su cuenta de Azure.

"Obtenga más información acerca de los niveles de acceso de Azure Blob".

Restaurar datos desde el almacenamiento de archivado

A pesar de que almacenar archivos de backup antiguos en un almacenamiento de archivado es mucho más barato que Cool Storage, el acceso a los datos desde un archivo de backup en Azure Archive para las operaciones de restauración tardará más tiempo y costará más dinero.

¿Cuánto cuesta restaurar los datos desde Azure Archive?

Puede elegir entre dos prioridades de restauración al recuperar datos de Azure Archive:

- **Alta**: Recuperación más rápida, mayor costo
- **Estándar**: Recuperación más lenta, menor costo

Cada método tiene una tarifa de recuperación por GB diferente y una tarifa por solicitud. Para obtener información detallada sobre los precios de Azure Archive por región de Azure, visite la "Página de precios de Azure".

> La prioridad alta no es compatible cuando se restauran datos desde Azure a sistemas StorageGRID.

¿Cuánto tiempo tardaría en restaurar mis datos archivados en Azure Archive?

Hay dos partes que componen el tiempo de restauración:

- **Retrieval Time**: El tiempo para recuperar el archivo de copia de seguridad archivado de Azure Archive y colocarlo en almacenamiento Cool. A esto se le llama a veces el tiempo de "rehidratación". El tiempo de recuperación varía en función de la prioridad de restauración que se elija:

- **Alta**: < 1 hora
- **Estándar**: < 15 horas

- **Tiempo de restauración**: El tiempo para restaurar los datos del archivo de copia de seguridad en almacenamiento fresco. Esta vez no difiere de la operación de restauración típica directamente del almacenamiento Cool, cuando no se utiliza un nivel de archivado.

Para obtener más información sobre las opciones de recuperación de Azure Archive, consulte "Estas preguntas frecuentes de Azure".

Clases de almacenamiento de archivado y tiempos de recuperación de restauración de Google

Cloud Backup admite una clase de almacenamiento de archivado de Google y la mayoría de regiones.

Clases de almacenamiento de archivado compatibles con Google para Cloud Backup

Cuando los archivos de copia de seguridad se crean inicialmente, se almacenan en almacenamiento *Standard*. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia, pero esto también permite acceder a ellos de forma inmediata.

Si su clúster local utiliza ONTAP 9.12.1 o más, puede optar por organizar en niveles los backups antiguos en el almacenamiento *Archive* en la interfaz de usuario de backup en cloud tras un determinado número de días (normalmente más de 30 días) para obtener una mayor optimización de los costes. Los datos de este nivel requerirán un mayor coste de recuperación, por lo que debe considerar la frecuencia con la que puede que necesite restaurar datos de estos ficheros de backup archivados. Consulte la sección Acerca de restaurar datos desde el almacenamiento de archivado.

Tenga en cuenta que al configurar Cloud Backup con este tipo de regla de ciclo de vida, no debe configurar ninguna regla de ciclo de vida al configurar el bloque en su cuenta de Google.

"Obtenga información sobre las clases de almacenamiento de Google".

Restaurar datos desde el almacenamiento de archivado

A pesar de que el almacenamiento de archivos de backup antiguos en el almacenamiento de archivado es mucho más barato que en el almacenamiento estándar, el acceso a los datos desde un archivo de backup en el almacenamiento de archivado para las operaciones de restauración tardará un poco más tiempo y supondrá un coste mayor.

¿Cuánto cuesta la restauración de datos desde Google Archive?

Para obtener información detallada sobre los precios de Google Cloud Storage por región, visite la "Página de precios de Google Cloud Storage".

¿Cuánto tiempo tardaría en restaurar los objetos archivados en Google Archive?

Hay dos partes que componen el tiempo total de restauración:

- **Retrieval time**: El tiempo para recuperar el archivo de copia de seguridad de Archive y colocarlo en almacenamiento estándar. A esto se le llama a veces el tiempo de "rehidratación". A diferencia de las soluciones de almacenamiento "más frías" que ofrecen otros proveedores de cloud, se puede acceder

a los datos en milisegundos.

- **Tiempo de restauración**: Tiempo para restaurar los datos del archivo de copia de seguridad en almacenamiento estándar. Esta vez no difiere de la operación de restauración típica directamente del almacenamiento estándar cuando no se utiliza un nivel de archivado.

Realice backups y restauraciones de datos de Cloud Backup en un sitio oscuro

Cuando utilice Cloud Backup en un sitio sin acceso a Internet, deberá realizar una copia de seguridad periódica de los archivos críticos de Cloud Backup en caso de que tenga un problema con el sistema host de BlueXP Connector. Esto le permitirá implementar un nuevo conector y restaurar los datos críticos de Cloud Backup.

Cuando utiliza Cloud Backup en un entorno SaaS en el que BlueXP Connector se pone en marcha en su proveedor de cloud o en su propio sistema host que tiene acceso a Internet, se hace un backup de todos los datos de configuración importantes de Cloud Backup y se almacenan en la nube. Cuando utiliza Cloud Backup en un sitio sin acceso a Internet, también conocido como "sitio oscuro", esta información de Cloud Backup se almacena únicamente en el sistema conector local.

En este tema se describe cómo realizar backups de datos críticos de Cloud Backup en el sistema StorageGRID conectado. También describe cómo restaurar los datos en un conector nuevo cuando sea necesario.

Realice backups de datos cruciales de Cloud Backup

Hay dos tipos de datos para los que es necesario realizar una copia de seguridad:

- Base de datos de Cloud Backup
- Archivos de catálogo indexados (utilizados para la función de búsqueda y restauración)

Debería planificar periódicamente realizar un backup de estos datos de Cloud Backup para que siempre tenga acceso a los datos más recientes.

Tenga en cuenta que nunca se incluyen datos de volumen en la base de datos de Cloud Backup o los archivos del catálogo indexado.

Realice un backup de la base de datos de Cloud Backup

La base de datos de Cloud Backup contiene un listado de todos los volúmenes, los archivos de backup, las políticas de backup y la información de configuración.

Pasos

1. Inicie sesión en el sistema host de Connector con las credenciales adecuadas.
2. Introduzca el shell del contenedor de MySQL introduciendo el siguiente comando:

```
docker exec -it ds_mysql_1 sh
```

3. En el shell del contenedor, despliegue "env".

4. Necesitará la contraseña de MySQL DB, así que copie el valor de la clave "MYSQL_ROOT_PASSWORD".
5. Haga un backup de la base de datos MySQL de Cloud Backup introduciendo el comando siguiente:

```
mysqldump --user root --password -p cloud_backup --result
-file=mysql.dump.cloud_backup.sql
```

6. Copie el backup de la base de datos MySQL del contenedor MySQL Docker introduciendo el comando siguiente:

```
docker cp ds_mysql_1:/mysql.dump.cloud_backup.sql .
```

7. Copie las copias de seguridad en una ubicación segura de la red. Se puede utilizar un sistema StorageGRID local si se crean backups de volúmenes ONTAP en esa ubicación.

Realice una copia de seguridad de los archivos del catálogo indexado

El catálogo indexado se utiliza para la funcionalidad de búsqueda y restauración. Contiene información sobre cada volumen y cada archivo de backup, lo que hace que las búsquedas sean muy rápidas y eficientes cuando se buscan datos de volumen que desea restaurar.

1. En el sistema host del conector, cambie el directorio a "/tmp".
2. Busque la carpeta Index Catalog. Comienza con la cadena **catálogo**.
3. Zip la carpeta "catalog<_xxxxxx_>" introduciendo el siguiente comando:

```
zip -r catalogxxxxxx.zip catalogxxxxxx
```

4. Copie la copia de seguridad comprimida en una ubicación segura de la red.

Restaure datos de Cloud Backup en un conector nuevo

Si su conector local tiene un fallo catastrófico, deberá instalar un conector nuevo y, a continuación, restaurar los datos de Cloud Backup en el nuevo conector.

Tendrá que realizar 4 tareas para devolver su sistema Cloud Backup a un estado de trabajo:

- Instale un conector BlueXP nuevo
- Restaure la base de datos de Cloud Backup
- Restaurar los archivos de catálogo indexado
- Redescubra todos sus sistemas ONTAP y StorageGRID en las instalaciones a la interfaz de usuario de BlueXP

Una vez que compruebe que su sistema está en un orden de funcionamiento, le recomendamos que cree nuevos archivos de copia de seguridad.

Instale un nuevo conector en un nuevo host Linux local

Al instalar un nuevo conector BlueXP, asegúrese de descargar la misma versión de software que había instalado en el conector original. Los cambios periódicos en la estructura de la base de datos de Cloud Backup pueden hacer que las versiones de software más nuevas sean incompatibles con los backups de la base de datos original. Puede hacerlo "Actualice el software Connector a la versión más reciente después de restaurar la base de datos de copia de seguridad".

1. "Instale el conector BlueXP en un nuevo host Linux local"
2. Inicie sesión en BlueXP con las credenciales de usuario administrador que acaba de crear.

Restaure la base de datos de Cloud Backup

1. Copie los backups de MySQL de la ubicación segura en el nuevo host de Connector.
2. Copie el backup en el contenedor MySQL Docker con el siguiente comando:

```
docker cp mysql.dump.cloud_backup.sql ds_mysql_1:/.
```

3. Introduzca el shell del contenedor de MySQL mediante el siguiente comando:

```
docker exec -it ds_mysql_1 sh
```

4. En el shell del contenedor, despliegue "env".
5. Necesitará la contraseña de MySQL DB, así que copie el valor de la clave "MYSQL_ROOT_PASSWORD".
6. Restaure la base de datos MySQL de Cloud Backup con el siguiente comando:

```
mysql -u root -p cloud_backup < mysql.dump.cloud_backup.sql
```

7. Compruebe que la base de datos MySQL de Cloud Backup se haya restaurado correctamente con los siguientes comandos de SQL:

```
# mysql -u root -p cloud_backup
```

Introduzca la contraseña.

```
mysql> show tables;
mysql> select * from volume;
```

Compruebe si los volúmenes que se muestran son los mismos que los existentes en el entorno original.

Restaurar los archivos de catálogo indexado

1. Copie el archivo zip de copia de seguridad del catálogo indexado desde la ubicación segura al nuevo host

de Connector de la carpeta "/tmp".

2. Descomprima el archivo "Catalogxxxxxx.zip" mediante el siguiente comando:

```
unzip catalogxxxxxx.zip
```

3. Ejecute el comando **ls** para asegurarse de que la carpeta "Catalogxxxxxx" se ha creado con las subcarpetas "Changes" y "snapshots" debajo.

Detectar los clústeres de ONTAP y los sistemas StorageGRID

1. "Descubra todos los entornos de trabajo de ONTAP en las instalaciones" disponibles en el entorno anterior.
2. "Descubra sus sistemas StorageGRID".

Configurar los detalles del entorno de StorageGRID

Agregue los detalles del sistema StorageGRID asociado a sus entornos de trabajo de ONTAP tal y como se han configurado en la configuración original del conector con la "API de BlueXP".

Tendrá que realizar estos pasos en cada sistema ONTAP que esté realizando una copia de seguridad de los datos en StorageGRID.

1. Extraiga el token de autorización mediante la siguiente API de autenticación/token.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'User-Agent:
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100101 Firefox/108.0'
-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":"pass
word"}
> '
```

Esta API devolverá una respuesta como la siguiente. Puede recuperar el token de autorización como se muestra a continuación.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Extraiga el ID de entorno de trabajo y el ID de X-Agent mediante la API de uso/externo/recurso.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Esta API devolverá una respuesta como la siguiente. El valor bajo "resourceIdentifier" denota el *WorkingEnvironment ID* y el valor bajo "agentId" denota *x-agent-id*.

3. Actualice la base de datos de Cloud Backup con los detalles del sistema StorageGRID asociado con los entornos de trabajo. Asegúrese de introducir el nombre de dominio completo de la 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
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
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" }'
```

Compruebe la configuración de Cloud Backup

1. Seleccione cada entorno de trabajo de ONTAP y haga clic en **Ver copias de seguridad** junto al servicio copia de seguridad y recuperación del panel derecho.

   Es necesario ver todos los backups creados para los volúmenes.

2. En el Panel de restauración, en la sección Buscar y restaurar, haga clic en **Configuración de indexación**.

   Asegúrese de que los entornos de trabajo que tenían activada la catalogación indexada anteriormente permanecen habilitados.

3. Desde la página Buscar y restaurar, ejecute algunas búsquedas de catálogo para confirmar que la restauración de catálogo indexado se ha completado correctamente.

Configurar el backup para el acceso de cuentas múltiples en Azure

Cloud Backup permite la creación de archivos de backup en una cuenta de Azure que difieren del lugar en el que residen los volúmenes de Cloud Volumes ONTAP de origen. Y ambas cuentas pueden ser diferentes a la cuenta en la que reside BlueXP Connector.

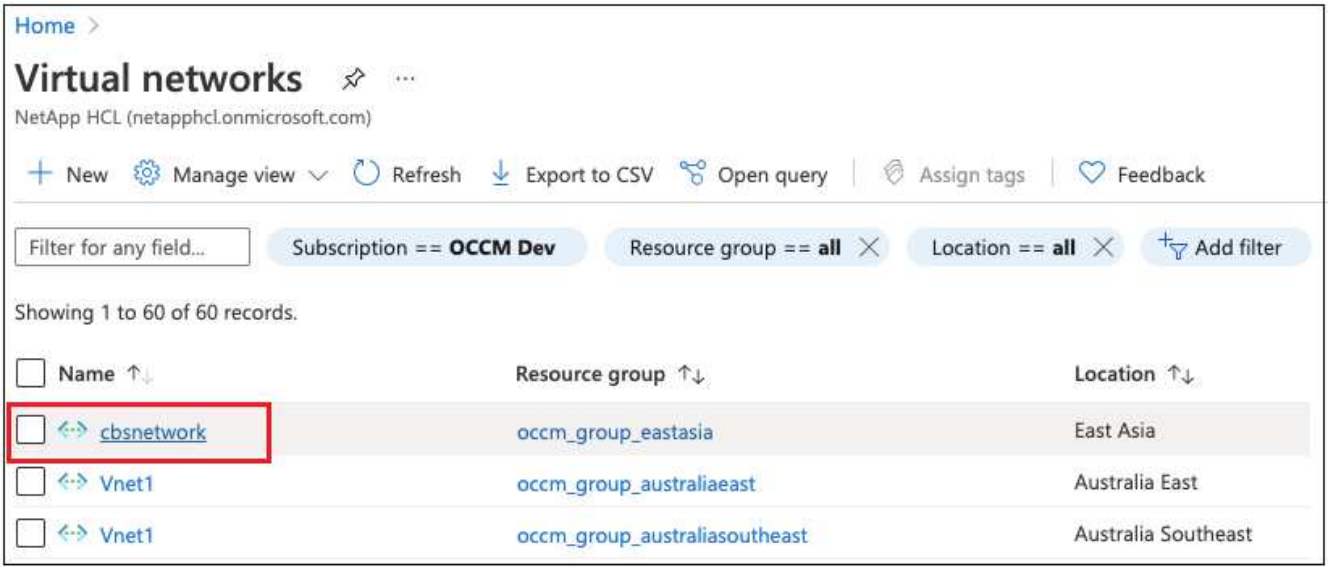
Estos pasos son necesarios solo cuando se encuentre "Realizar backups de los datos de Cloud Volumes ONTAP en un almacenamiento de Azure Blob".

Solo tiene que seguir los pasos que se indican a continuación para configurar su configuración de esta manera.

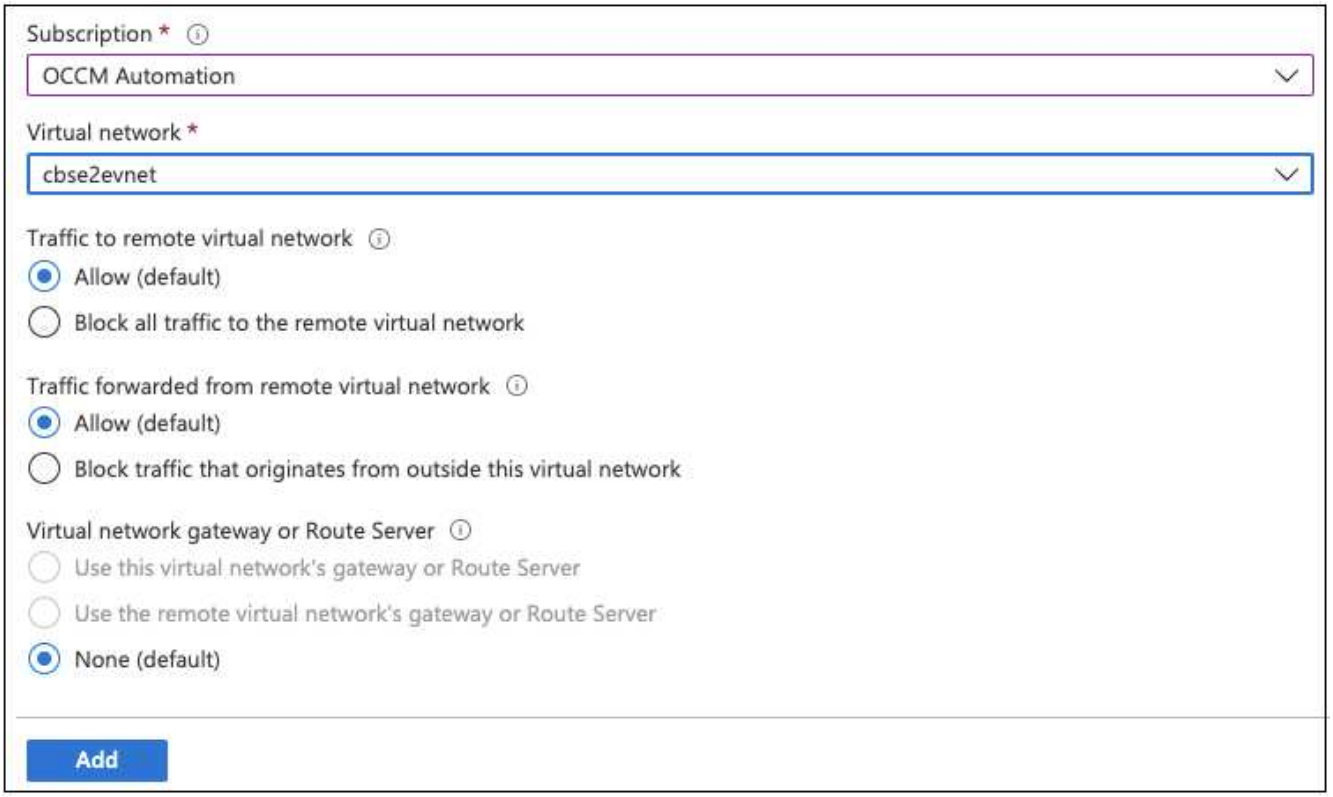
Configure vnet peering entre cuentas

Tenga en cuenta que si desea que BlueXP administre su sistema Cloud Volumes ONTAP en una región o cuenta distinta, debe configurar vnet peering. No se requiere vnet peering para la conectividad de la cuenta de almacenamiento.

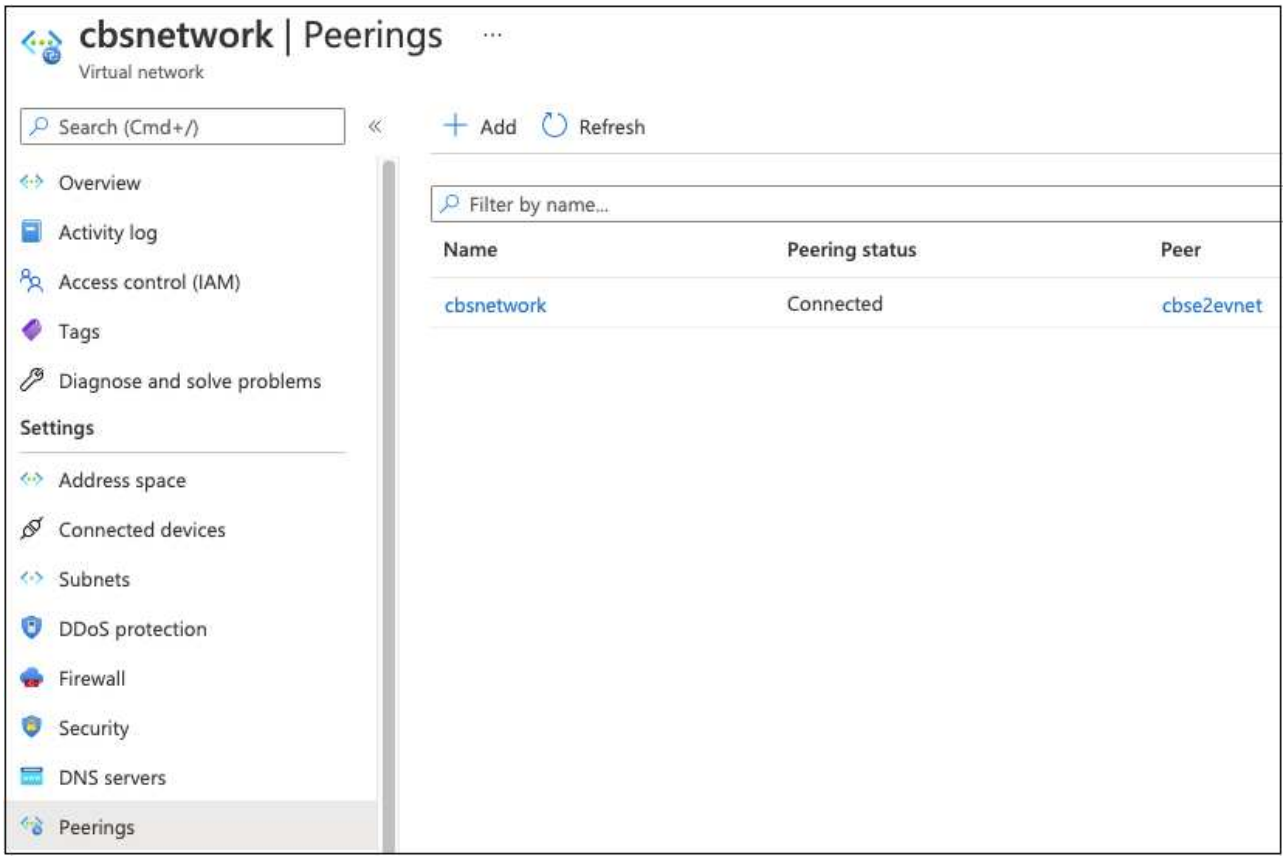
1. Inicie sesión en el portal de Azure y desde casa. Seleccione Virtual Networks.
2. Seleccione la suscripción que está utilizando como suscripción 1 y haga clic en el vnet en el que desea configurar Peering.



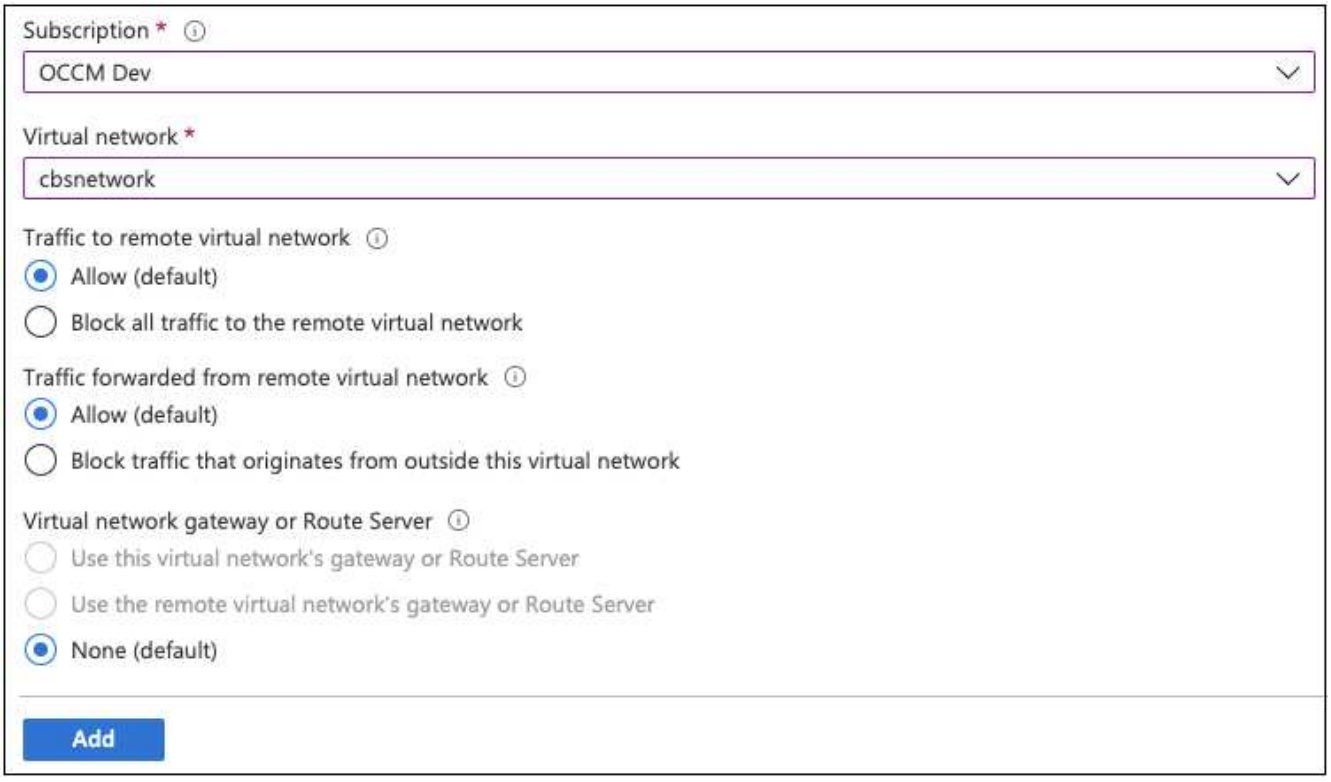
3. Seleccione **cbsnetwork** y, en el panel izquierdo, haga clic en **peerings** y, a continuación, haga clic en **Add**.



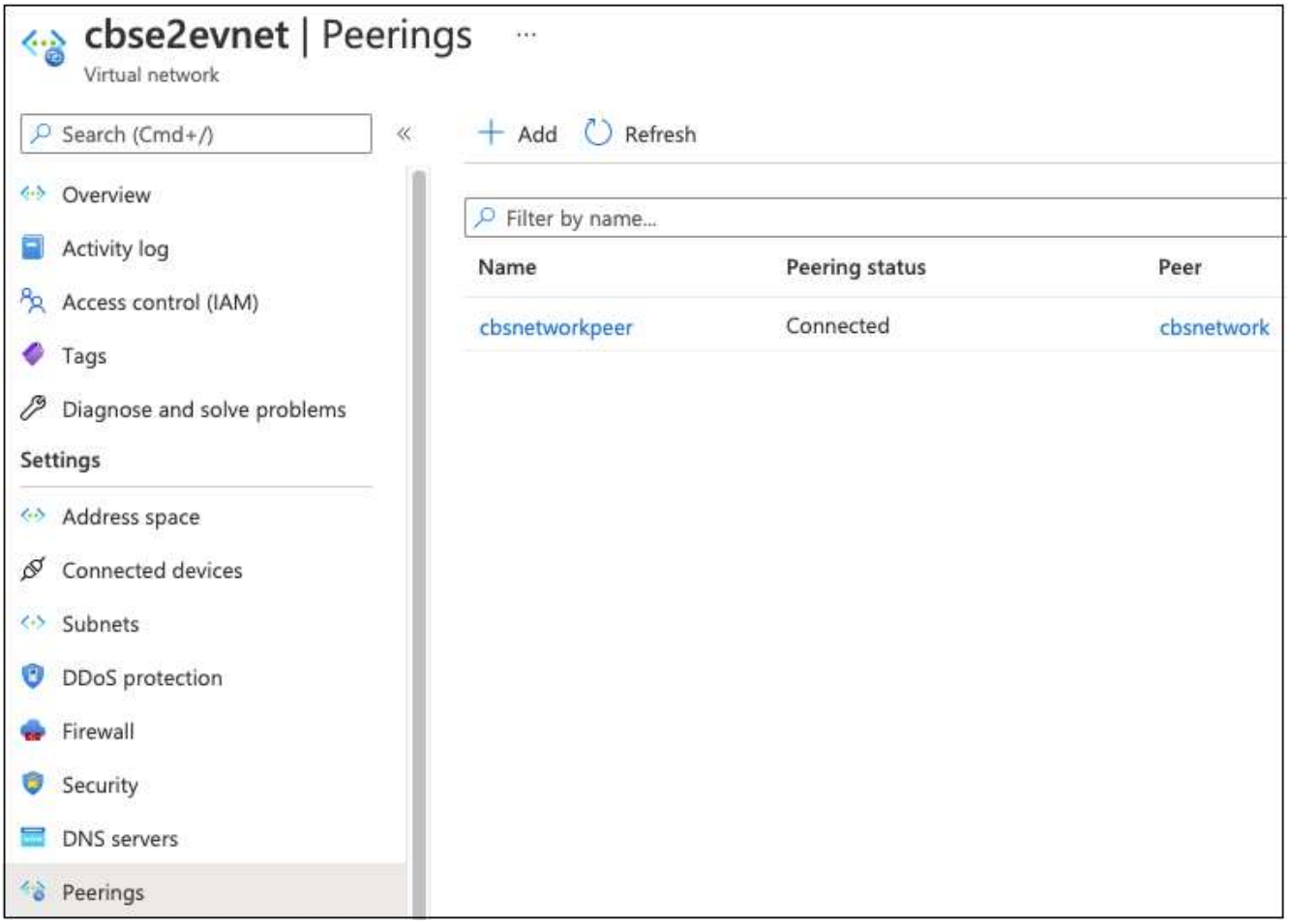
4. Introduzca la siguiente información en la página peering y, a continuación, haga clic en **Add**.
   - Nombre del vínculo de relación de paridad para esta red: Puede asignar cualquier nombre para identificar la conexión de relación de paridad.
   - Nombre de enlace de red virtual remota: Escriba un nombre para identificar la red virtual remota.
   - Mantenga todas las selecciones como valores predeterminados.
   - En subscripción, seleccione la suscripción 2.
   - Red virtual, seleccione la red virtual en la suscripción 2 a la que desea configurar la conexión entre iguales.



5. Realice los mismos pasos en la suscripción 2 vnet y especifique los detalles de suscripción y vnet remoto de la suscripción 1.



La configuración de relaciones entre iguales se agrega.



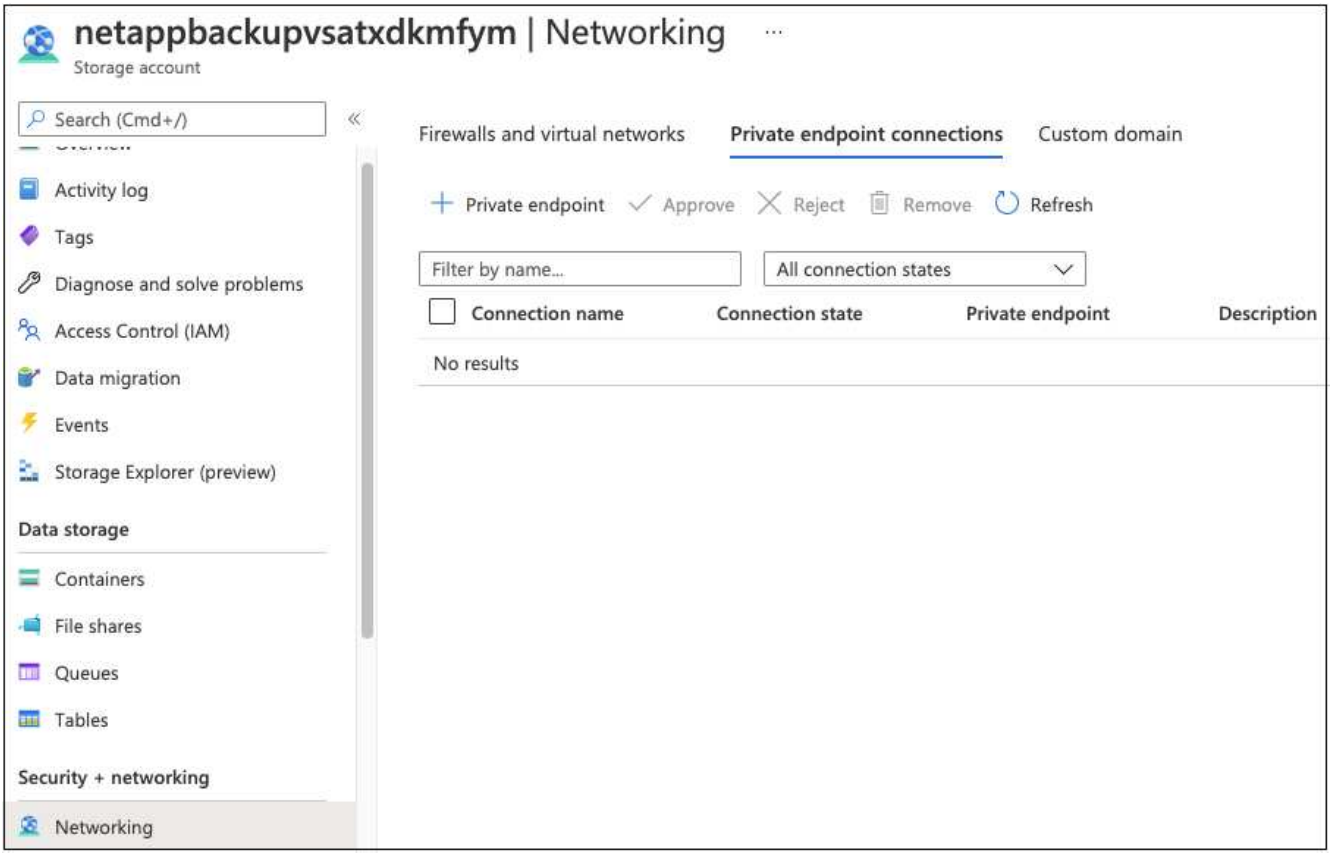
Cree un extremo de privado para la cuenta de almacenamiento

Ahora debe crear un extremo privado para la cuenta de almacenamiento. En este ejemplo, la cuenta de almacenamiento se crea en la suscripción 1 y el sistema Cloud Volumes ONTAP se ejecuta en la suscripción 2.

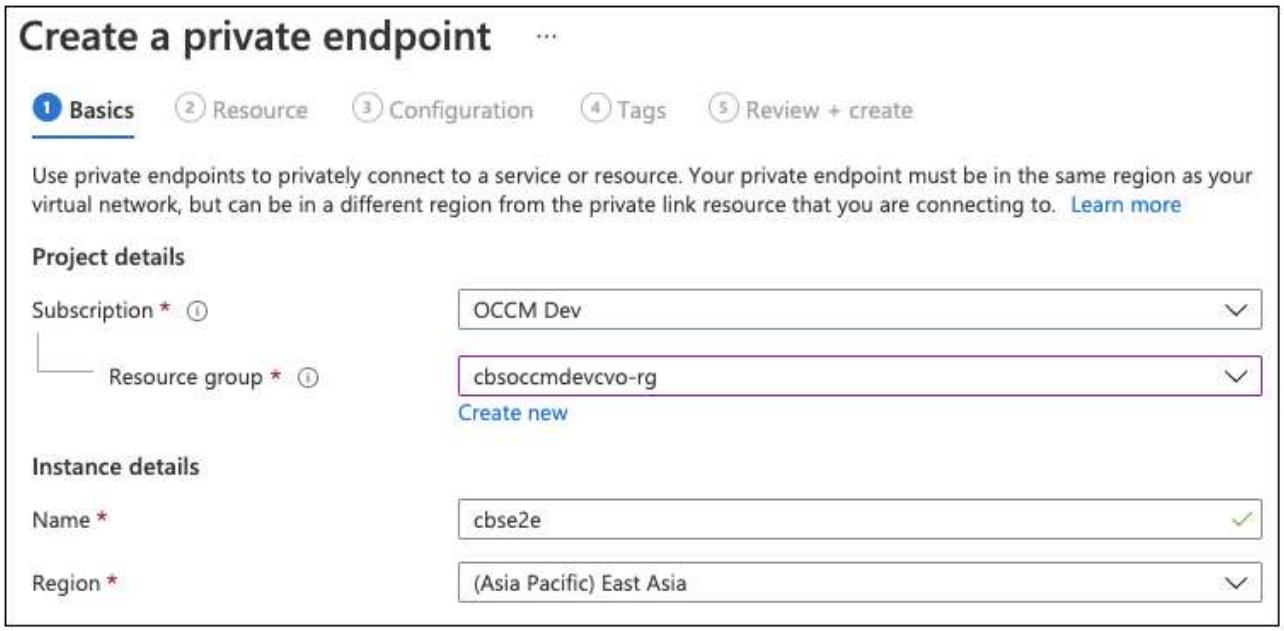
Necesita permiso de colaborador de red para realizar la siguiente acción.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

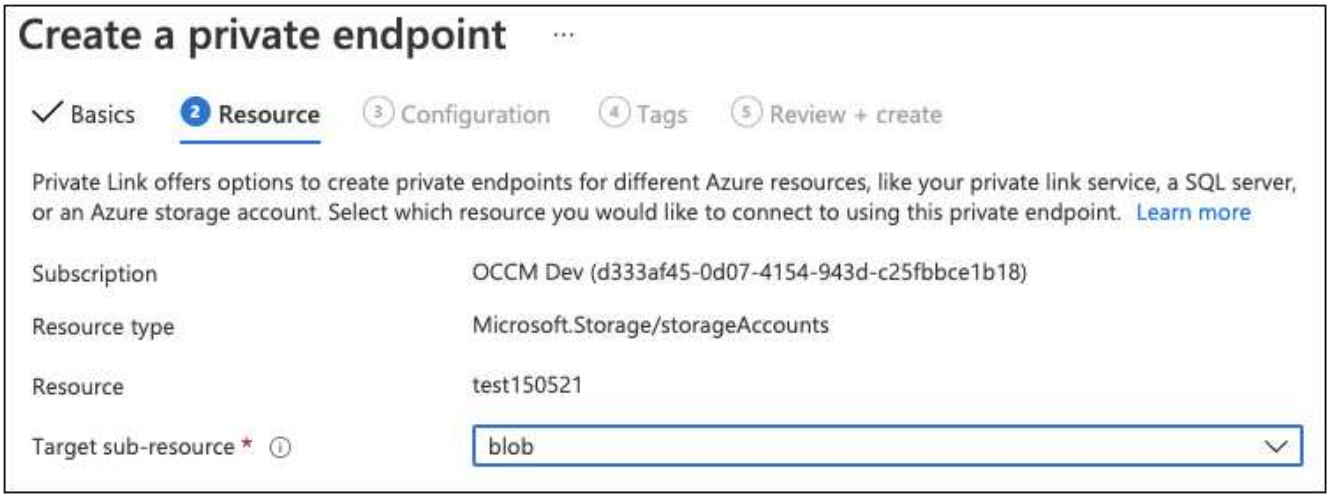
1. Vaya a la cuenta de almacenamiento > redes > conexiones de punto final privado y haga clic en **+ Private Endpoint**.



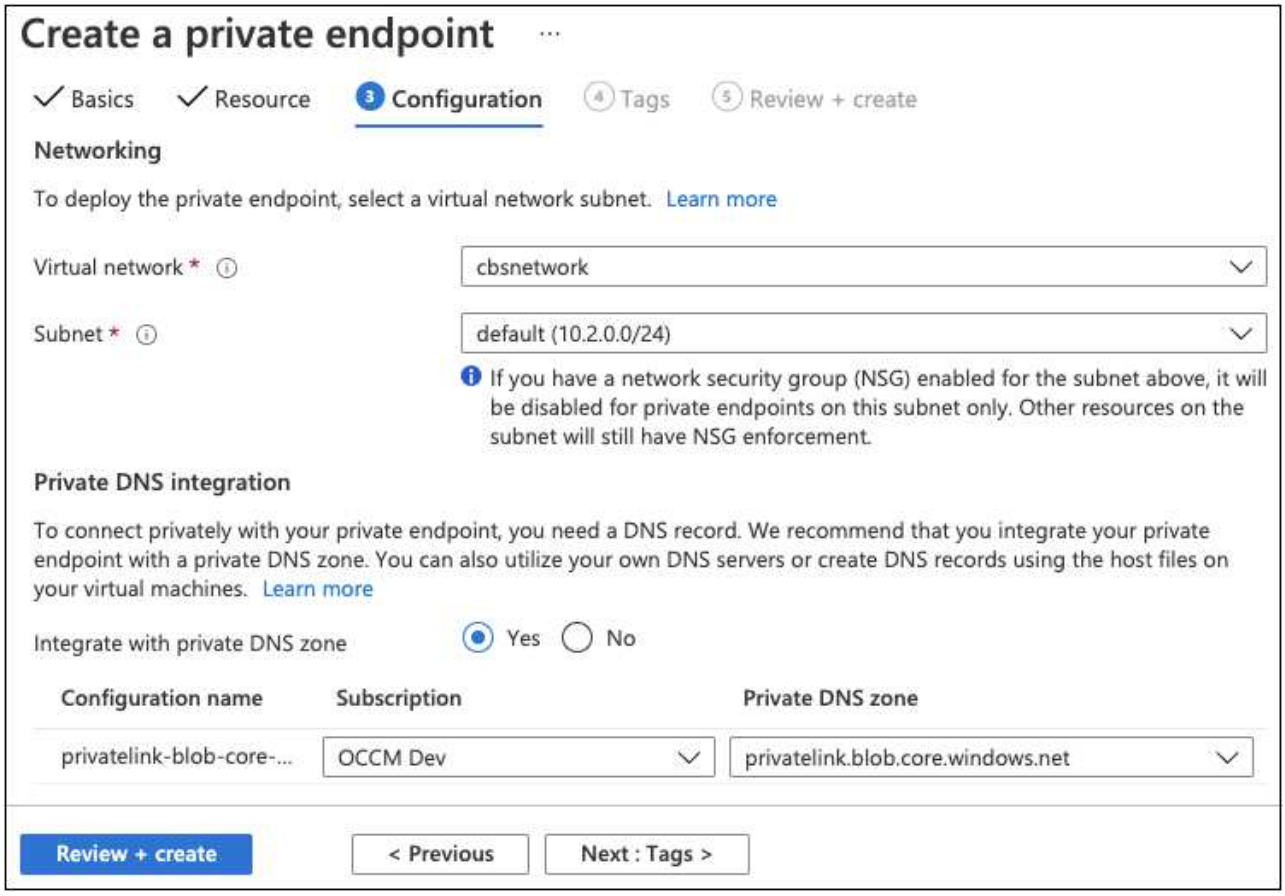
2. En la página Private Endpoint *Basics*:
   - Seleccione la suscripción 2 (donde están implementados el conector BlueXP y el sistema Cloud Volumes ONTAP) y el grupo de recursos.
   - Introduzca un nombre de extremo.
   - Seleccione la región.



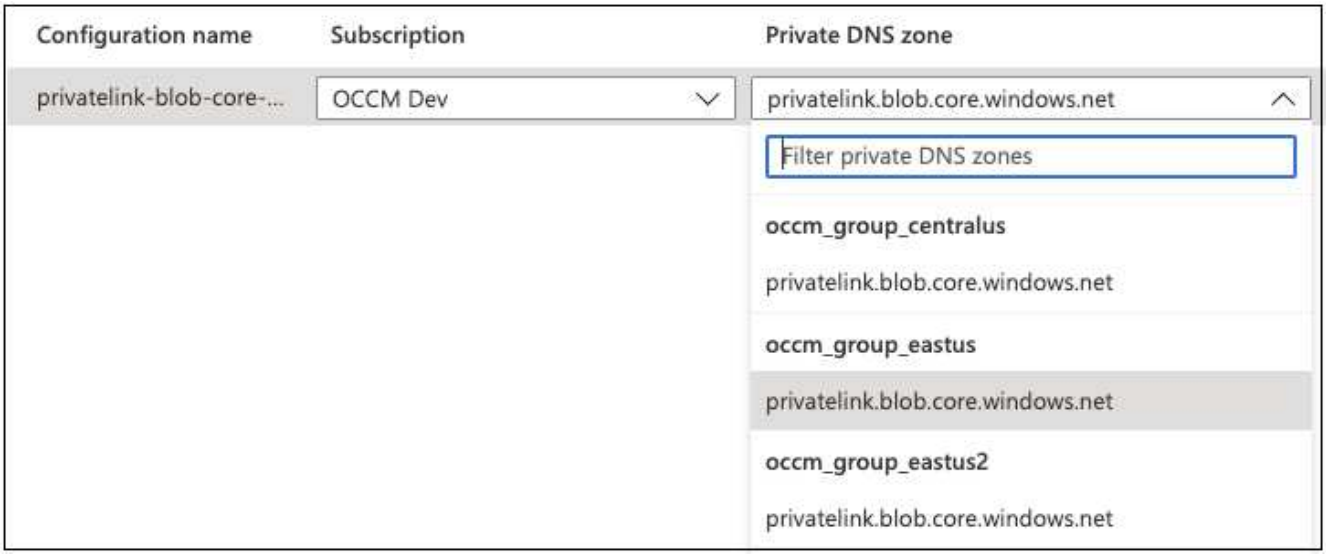
3. En la página *Resource*, seleccione Subrecurso destino como **BLOB**.



4. En la página Configuration:
   - Seleccione la red virtual y la subred.
   - Haga clic en el botón de opción **Sí** para "integrar con la zona DNS privada".



5. En la lista Zona DNS privada, asegúrese de que la Zona privada está seleccionada en la región correcta y haga clic en **revisar + Crear**.



Ahora, la cuenta de almacenamiento (de suscripción 1) tiene acceso al sistema Cloud Volumes ONTAP que se ejecuta en la suscripción 2.

6. Vuelva a intentar habilitar Cloud Backup en el sistema Cloud Volumes ONTAP y esta vez debe realizarse correctamente.

Información de copyright

Información de la marca comercial