Referencia

BlueXP backup and recovery

NetApp
October 09, 2024

Tabla de contenidos

Referencia

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

El backup y la recuperación de BlueXP admite dos clases de almacenamiento de archivado S3 y la mayoría de las regiones.

Clases de almacenamiento de archivado S3 admitidas para backup y recuperación de BlueXP

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. Puede establecer esto en “0” o en 1-999 días. Si lo establece en “0” días, no podrá cambiarlo más tarde a 1-999 días.

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 de esta página sobre la restauración de datos desde el almacenamiento de archivado.

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

Tenga en cuenta que al configurar el backup y la recuperación de BlueXP 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 AWS.

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

Restaurar datos del 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

El backup y la recuperación de BlueXP son compatibles con un nivel de acceso de archivado de Azure y la mayoría de las regiones.

Niveles de acceso de Azure Blob compatibles para el backup y recuperación de BlueXP

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 sección de

esta página sobre la restauración de datos desde el almacenamiento de archivado.

Tenga en cuenta que cuando configure el backup y la recuperación de BlueXP 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 del 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

El backup y la recuperación de BlueXP son compatibles con una clase de almacenamiento de archivado de Google y la mayoría de regiones.

Clases de almacenamiento de archivado de Google admitidas para backup y recuperación de BlueXP

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 tu clúster on-premises utiliza ONTAP 9.12.1 o posterior, puedes elegir organizar en niveles los backups antiguos en el almacenamiento *Archive* en la interfaz de usuario de backup y recuperación de BlueXP después de un cierto número de días (normalmente más de 30 días) para mejorar la 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 de esta página sobre la restauración de datos desde el almacenamiento de archivado.

Tenga en cuenta que al configurar el backup y la recuperación de BlueXP 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 del 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.

Configurar el backup para el acceso de cuentas múltiples en Azure

El backup y la recuperación de datos de BlueXP te permite crear archivos de backup en una cuenta de Azure diferente a la de dónde residen los volúmenes de Cloud Volumes ONTAP de origen. Ambas cuentas pueden ser diferentes a la cuenta en la que reside el conector de BlueXP.

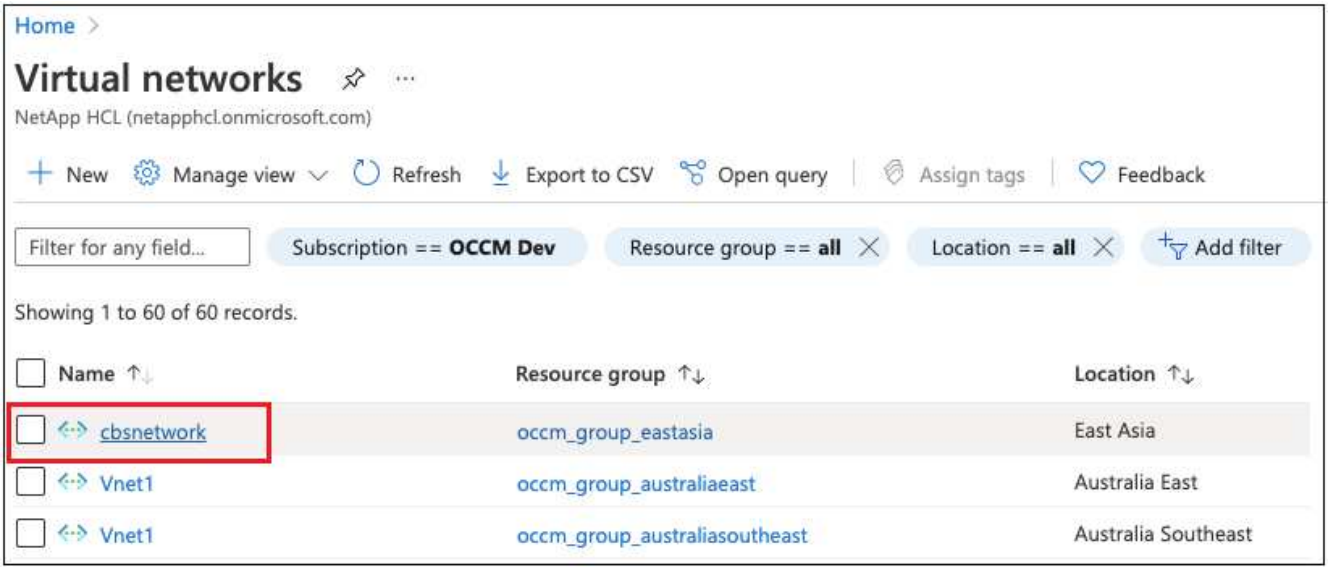
Estos pasos son necesarios solo cuando se encuentre "Realizar backups de los datos de Cloud Volumes ONTAP en un almacenamiento de Azure Blob".

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

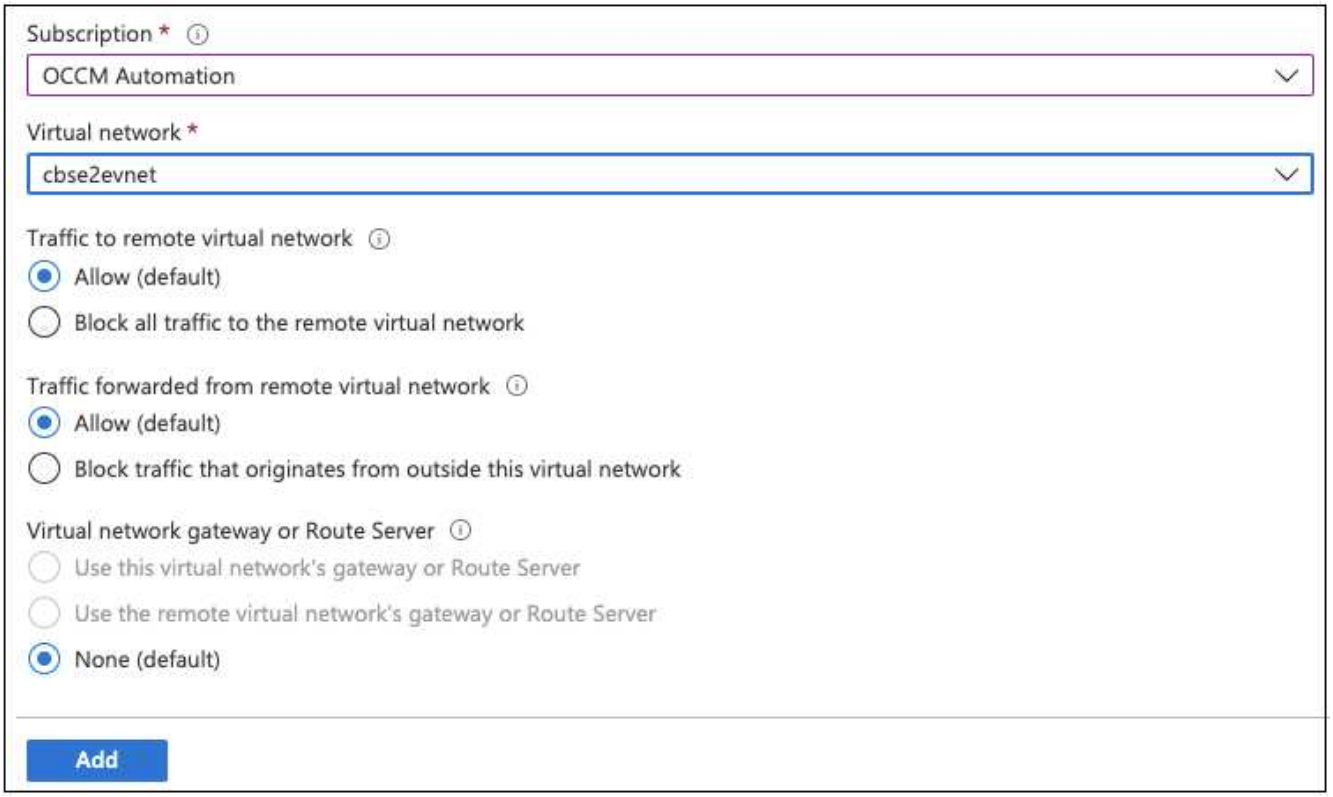
Configure vnet peering entre cuentas

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.

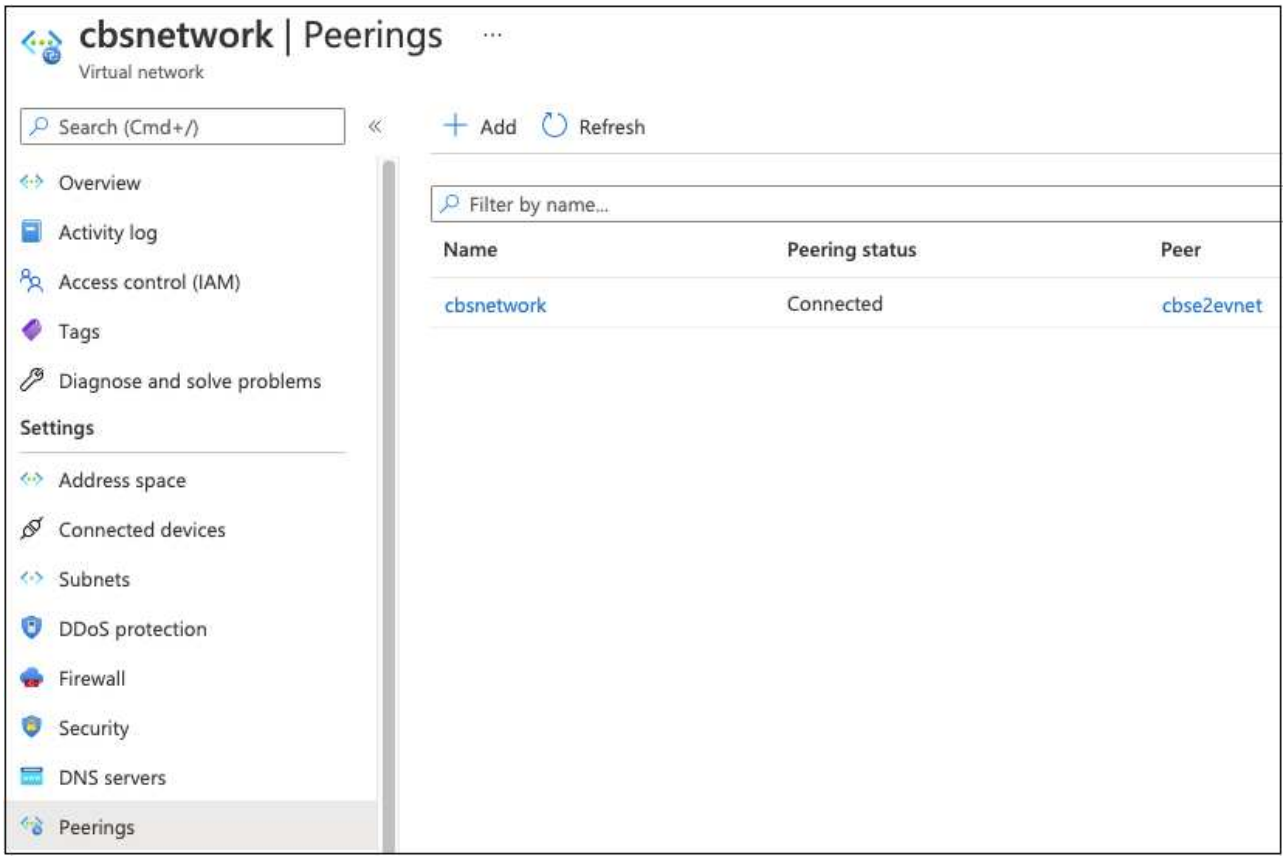
1. Inicie sesión en el portal de Azure y desde casa. Seleccione Virtual Networks.
2. Seleccione la suscripción que está utilizando como suscripción 1 y haga clic en el vnet en el que desea configurar Peering.



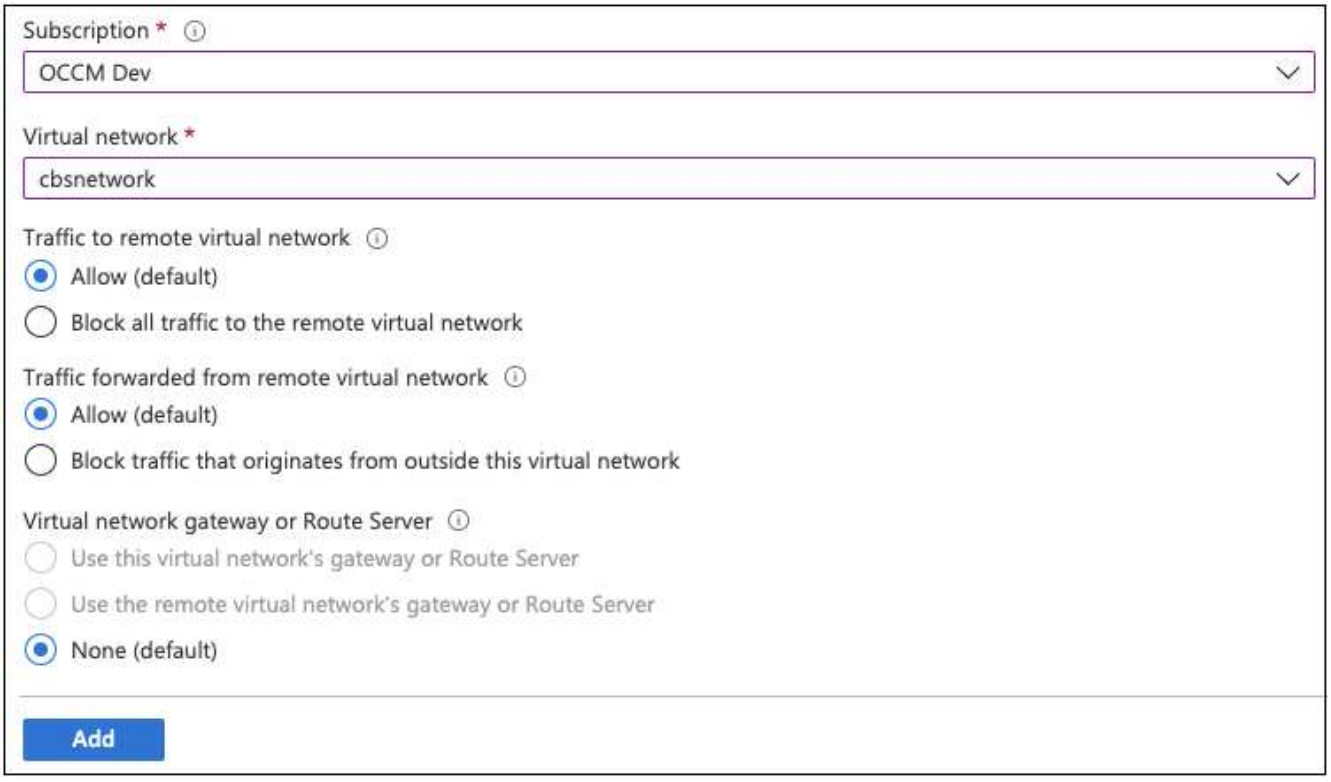
3. Seleccione **cbsnetwork** y, en el panel izquierdo, haga clic en **peerings** y, a continuación, haga clic en **Add**.



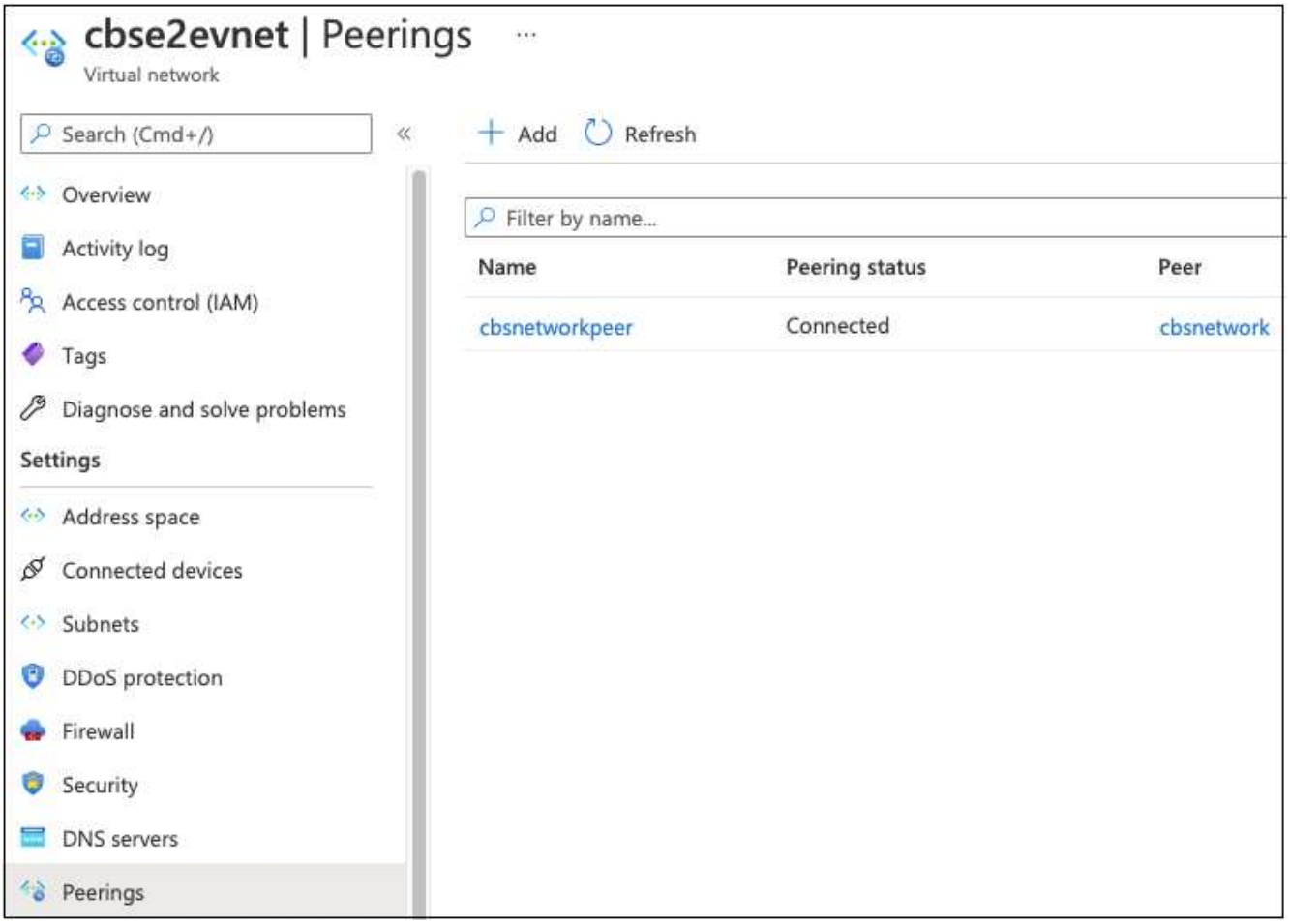
4. Introduzca la siguiente información en la página peering y, a continuación, haga clic en **Add**.
   - Nombre del vínculo de relación de paridad para esta red: Puede asignar cualquier nombre para identificar la conexión de relación de paridad.
   - Nombre de enlace de red virtual remota: Escriba un 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.



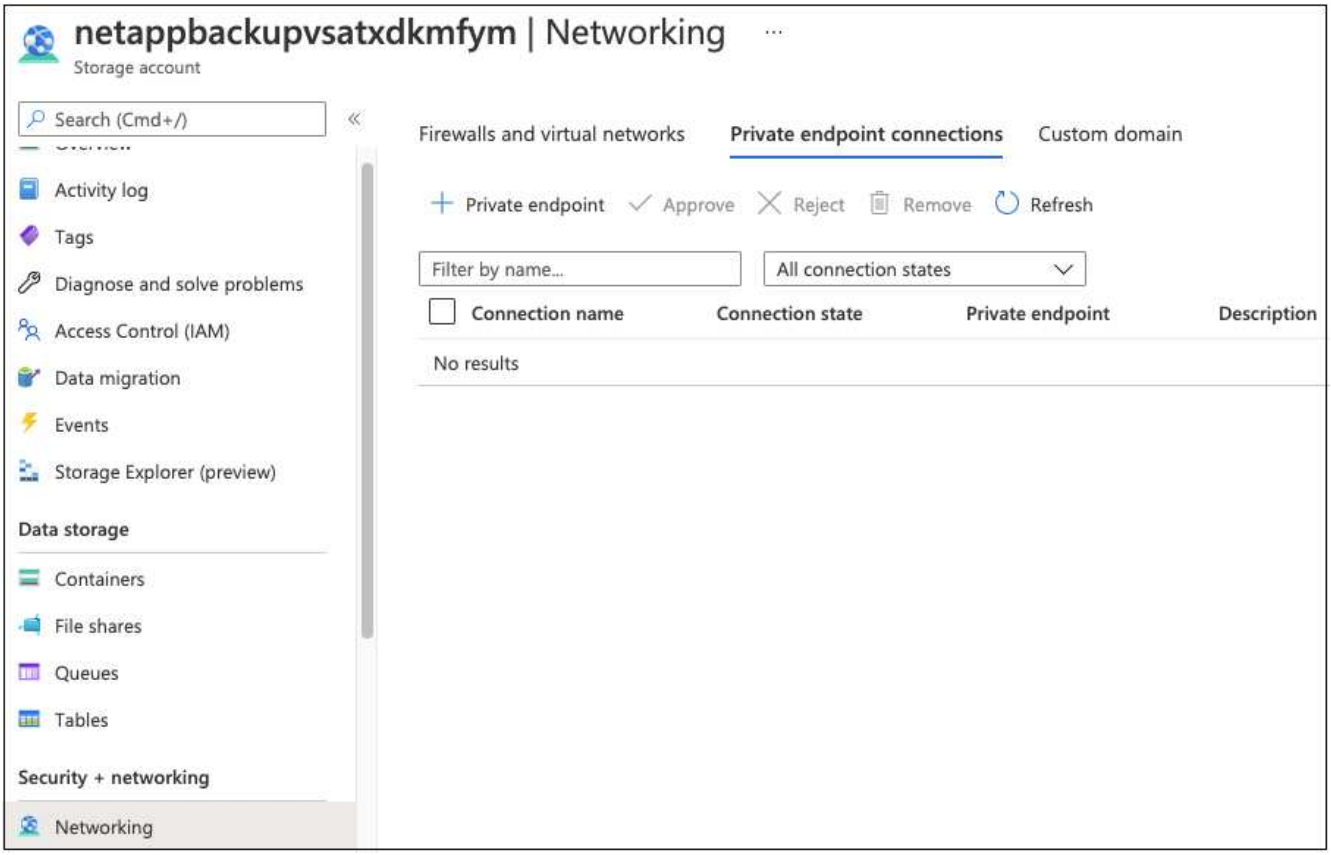
Cree un extremo de privado para la cuenta de almacenamiento

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.

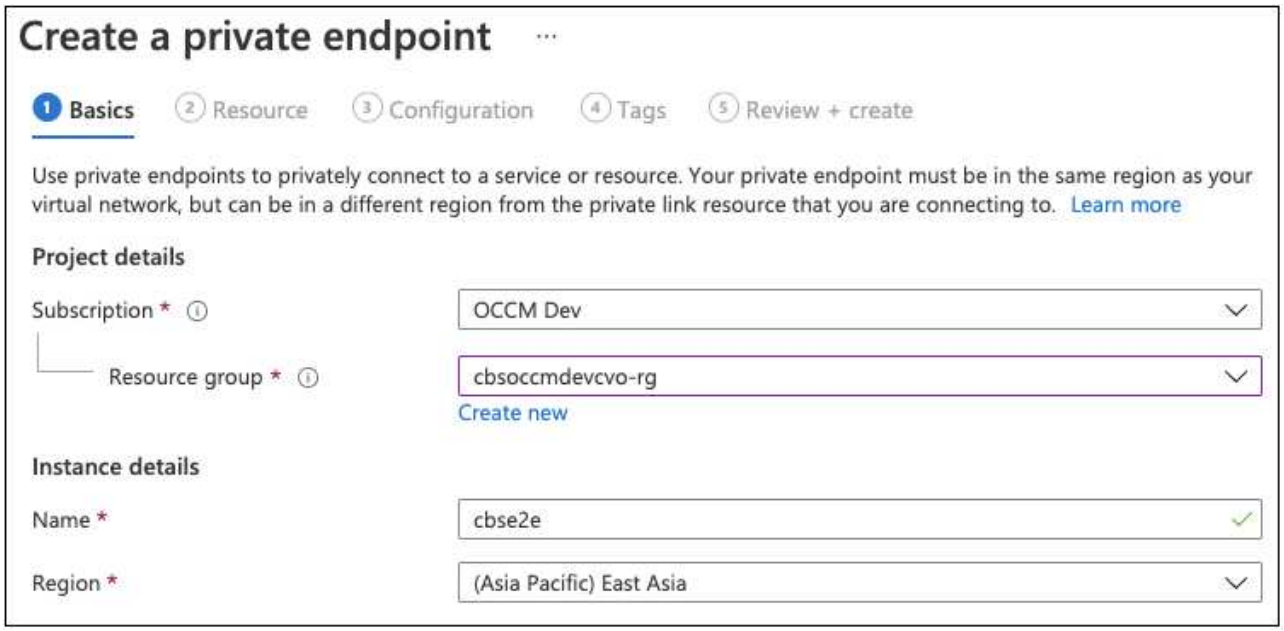
Necesita permiso de colaborador de red para realizar la siguiente acción.

```
{
  "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": []
      }
    ]
  }
}
```

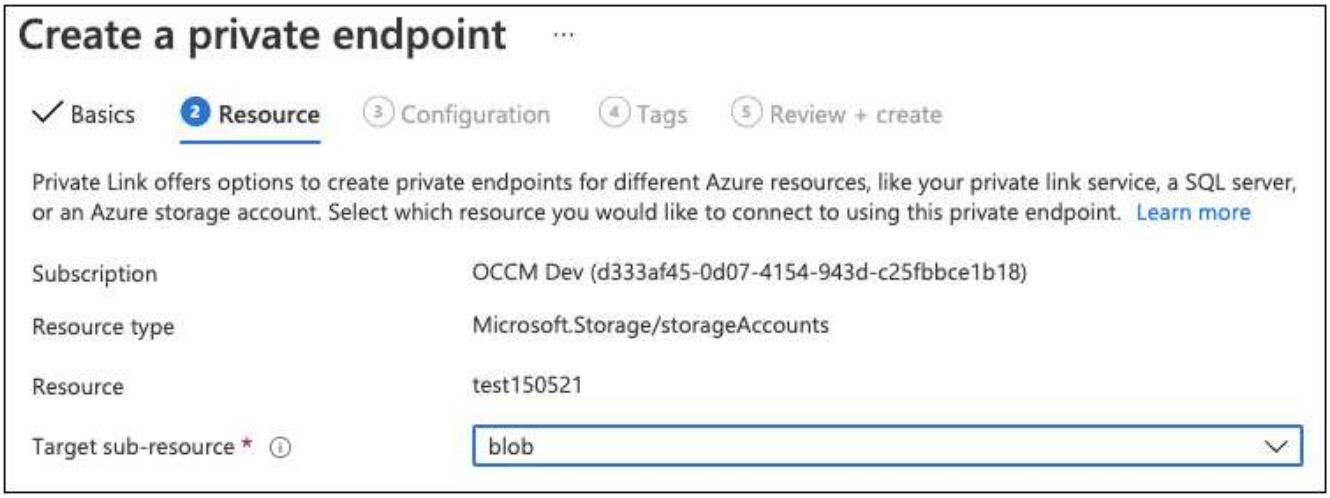
1. Vaya a la cuenta de almacenamiento > Redes > Conexiones de punto final privado y haga clic en **+ Punto final privado**.



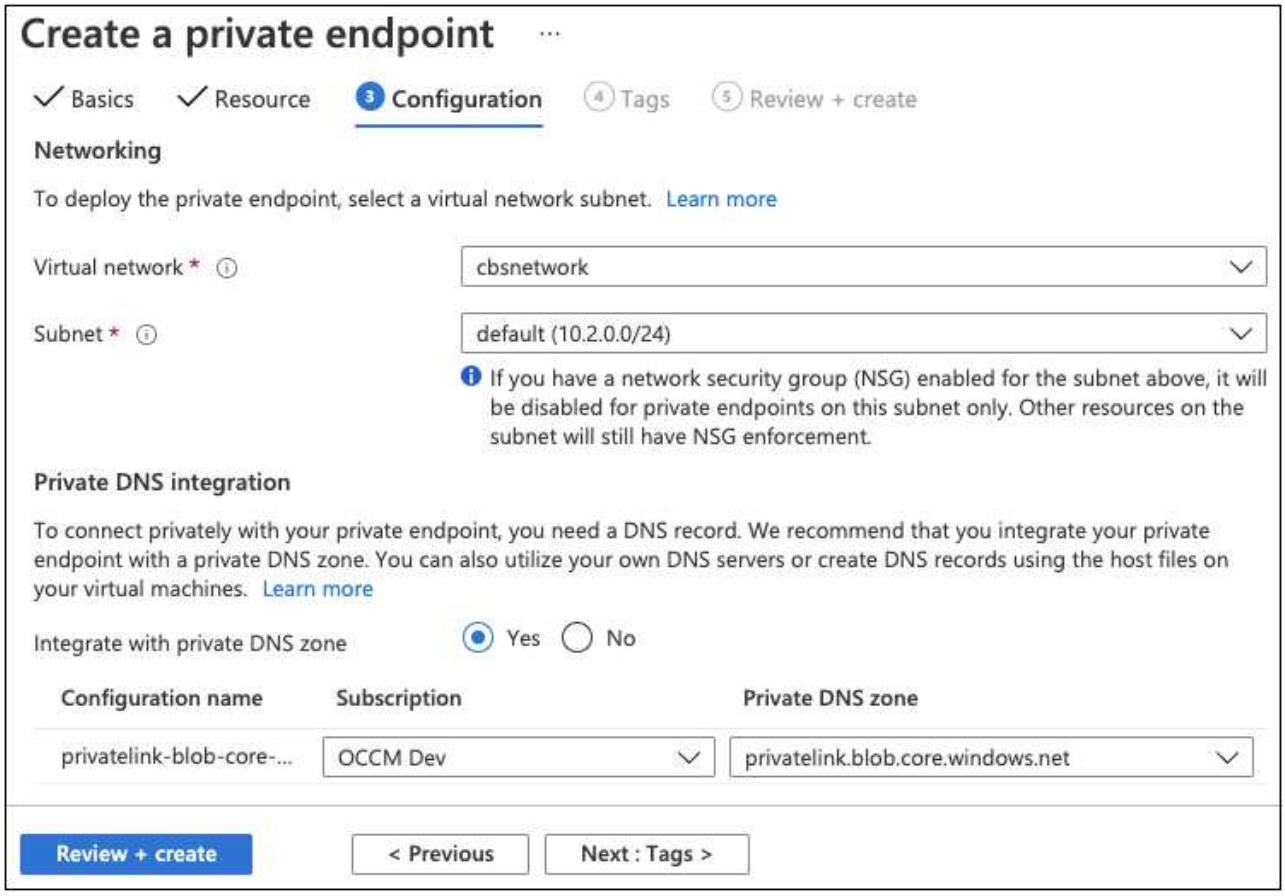
2. En la página Private Endpoint *Basics*:
   - Seleccione la suscripción 2 (donde están implementados el conector BlueXP y el sistema Cloud Volumes ONTAP) y el grupo de recursos.
   - Introduzca un nombre de extremo.
   - Seleccione la región.



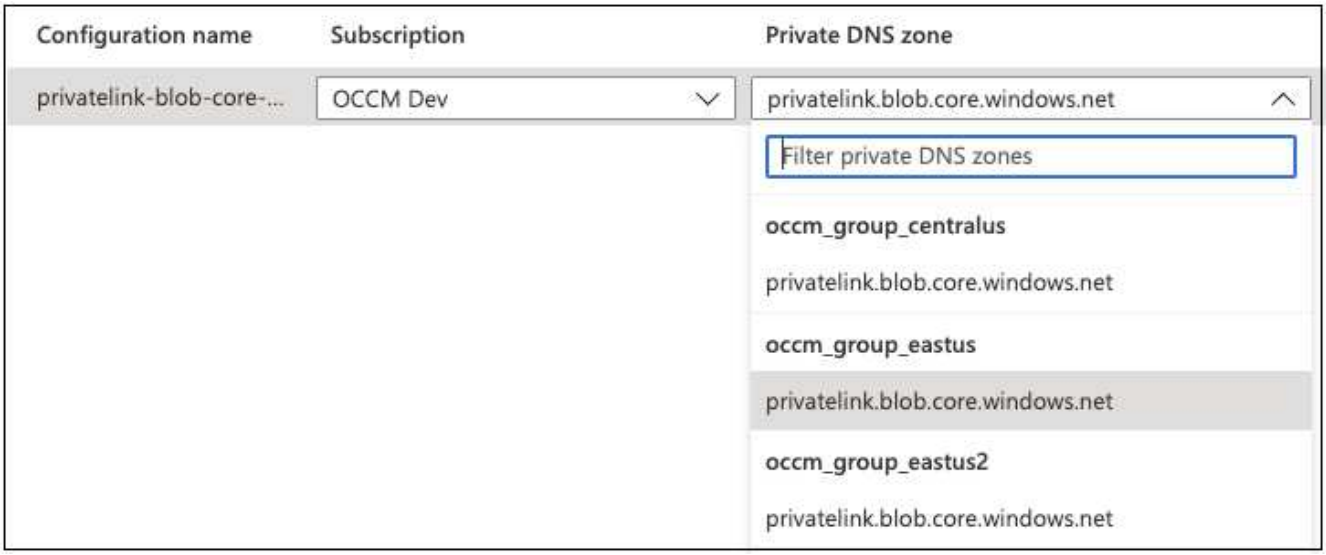
3. En la página *Resource*, seleccione Subrecurso destino como **BLOB**.



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. Intenta habilitar el backup y la recuperación de BlueXP en el sistema Cloud Volumes ONTAP y esta vez debe tener éxito.

Restaurar datos de backup y recuperación de BlueXP en un sitio oscuro

Al utilizar el backup y la recuperación de BlueXP en un sitio sin acceso a Internet, conocido como *modo privado*, los datos de configuración de backup y recuperación de BlueXP se copian en el bloque StorageGRID o ONTAP S3 donde se almacenan los backups. Si tienes un problema con el sistema de host del conector de BlueXP en el futuro, puedes implementar un nuevo conector y restaurar los datos críticos de backup y recuperación de BlueXP.

Tenga en cuenta que cuando utilice el backup y la recuperación de datos de BlueXP en un entorno SaaS donde se implementa el conector BlueXP en su proveedor de cloud o en su propio sistema host que tiene acceso a Internet, todos los datos importantes de configuración de backup y recuperación de BlueXP se copian y se protegen en el cloud. Si tiene un problema con el conector, simplemente cree un nuevo conector y agregue sus entornos de trabajo y los detalles de la copia de seguridad se restaurarán automáticamente.

Existen 2 tipos de datos de los que se realiza una copia de seguridad:

- Base de datos de backup y recuperación de BlueXP: Contiene una lista de todos los volúmenes, archivos de backup, políticas de backup y información de configuración.
- Archivos de catálogo indexados: Contiene índices detallados que se utilizan para la función de búsqueda y restauración que hacen que las búsquedas sean rápidas y eficaces cuando se buscan datos de volumen que se desean 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 conector gestiona varios entornos de trabajo de ONTAP en las instalaciones, los archivos de backup y recuperación de BlueXP se ubicarán en el depósito del entorno de trabajo que se activó primero.

Nunca se incluyen datos de volumen en la base de datos de backup y recuperación de BlueXP o en los archivos de catálogo indexado.

Restaurar los datos de backup y recuperación de BlueXP en un nuevo conector

Si tu conector on-premises tiene un fallo catastrófico, tendrás que instalar un nuevo conector y restaurar los datos de backup y recuperación de BlueXP en el nuevo conector.

Hay 4 tareas que necesitarás realizar para que el sistema de backup y recuperación de BlueXP regrese a un estado de trabajo:

- Instale un conector BlueXP nuevo
- Restaura la base de datos de backup y recuperación de BlueXP
- 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.

Lo que necesitará

Tendrá que acceder a las copias de seguridad de base de datos e índices más recientes desde el bucket de StorageGRID o ONTAP S3 donde se almacenan los archivos de copia de seguridad:

- Archivo de base de datos MySQL de backup y recuperación de BlueXP

  Este archivo se encuentra en la siguiente ubicación del depósito `netapp-backup-<GUID>/mysql_backup/`, y se nombra `CBS_DB_Backup_<day>_<month>_<year>.sql`.

- Archivo zip de copia de seguridad de catálogo indexado

  Este archivo se encuentra en la siguiente ubicación del depósito `netapp-backup-<GUID>/catalog_backup/`, y se nombra `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`.

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 backup y recuperación de BlueXP pueden hacer que las versiones de software más nuevas sean incompatibles con las copias de seguridad de la base de datos originales. 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.

Restaura la base de datos de backup y recuperación de BlueXP

1. Copie el backup de MySQL de la ubicación del backup en el nuevo host Connector. Usaremos el nombre de archivo de ejemplo “CBS_DB_Backup_23_05_2023.sql” a continuación.

2. Copie el backup en el contenedor de Docker de MySQL mediante uno de los siguientes comandos, en función de si utiliza 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. Introduzca el shell de contenedor MySQL mediante uno de los siguientes comandos, dependiendo de si está utilizando 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, 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 backup y recuperación de BlueXP con el siguiente comando:

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Compruebe que la base de datos MySQL de backup y recuperación de BlueXP se ha restaurado correctamente mediante 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 backup del Catálogo indexado (utilizaremos el nombre del archivo de ejemplo «Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip») desde la ubicación del backup al nuevo host de Connector en la carpeta «/opt/application/netapp/cbs».
2. Descomprima el archivo Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip con el siguiente comando:

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Ejecute el comando **ls** para asegurarse de que la carpeta “catalogdb1” ha sido creada con las subcarpetas “Cambios” y “Instantáneas” 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. 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 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. Actualiza la base de datos de backup y recuperación de BlueXP 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" }'
```

Comprueba la configuración de backup y recuperación de BlueXP

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.

Reinicia el servicio de backup y recuperación de BlueXP

Puede haber situaciones en las que tengas que reiniciar el servicio de backup y recuperación de BlueXP.

La funcionalidad de backup y recuperación de BlueXP está integrada en BlueXP Connector. Deberá seguir diferentes pasos iniciales para reiniciar el servicio en función de si ha implementado el conector en la nube o si ha instalado el conector manualmente en un sistema Linux.

Pasos

1. Conéctese al sistema Linux en el que se está ejecutando el conector.

Ubicación del conector	Procedimiento
Puesta en marcha de cloud	Siga las instrucciones para "Conexión a la máquina virtual Connector Linux" en función del proveedor de cloud que utilice.
Instalación manual	Inicie sesión en el sistema Linux.

2. Escriba el comando para reiniciar el servicio.

Ubicación del conector	Comando de Docker	Comando Podman
Puesta en marcha de cloud	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Instalación manual con acceso a Internet	`docker restart cloudmanager_cbs`	`podman restart cloudmanager cbs`
Instalación manual sin acceso a Internet	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`