Referencia

NetApp Backup and Recovery

NetApp
February 10, 2026

Tabla de contenidos

Referencia

Políticas en SnapCenter comparadas con las de NetApp Backup and Recovery

Existen algunas diferencias entre las políticas utilizadas en SnapCenter y las utilizadas en NetApp Backup and Recovery que podrían afectar lo que ve después de importar recursos y políticas desde SnapCenter.

Niveles de programación

SnapCenter utiliza los siguientes niveles de programación:

- **Por hora**: Varias horas y minutos con cualquier hora (0-23) y cualquier minuto (0-60).
- **Diario**: Opción para repetir cada un número determinado de días, por ejemplo, cada 3 días.
- **Semanal**: de domingo a lunes, con la opción de realizar una instantánea el día 1 de la semana o en varios días de la semana.
- **Mensual**: De enero a diciembre, con opción de actuar en días específicos o múltiples cada mes, por ejemplo, el 7.

NetApp Backup and Recovery utiliza los siguientes niveles de programación, que son ligeramente diferentes:

- **Cada hora**: realiza instantáneas solo en intervalos de 15 minutos, por ejemplo, 1 hora o intervalos de 15 minutos menores a 60.
- **Diario**: Horas del día (0-23) con hora de inicio por ejemplo a las 10:00 AM con opción a realizarse cada cierta cantidad de horas.
- **Semanal**: Día de la semana (domingo a lunes) con opción de actuar en 1 día o en varios días. Esto es lo mismo que SnapCenter.
- **Mensual**: Fechas del mes (0-30) con una hora de inicio en múltiples fechas del mes.
- **Anual**: Mensual. Esto coincide con el mensual de SnapCenter.

Varias políticas en SnapCenter con el mismo nivel de programación

Puede asignar varias políticas con el mismo nivel de programación a un recurso en SnapCenter. Sin embargo, NetApp Backup and Recovery no admite múltiples políticas en un recurso que utiliza el mismo nivel de programación.

Ejemplo: Si utiliza tres políticas (para Datos, Registro y Registro de instantáneas) en SnapCenter, después de la migración desde SnapCenter, NetApp Backup and Recovery utiliza una sola política en lugar de las tres.

Programaciones diarias de SnapCenter importadas

NetApp Backup and Recovery ajusta las programaciones de SnapCenter de la siguiente manera:

- Si la programación de SnapCenter está configurada en menos o igual a 7 días, NetApp Backup and Recovery configura la programación en semanal. Se omiten algunas instantáneas durante la semana.

  Ejemplo: Si tiene una política diaria de SnapCenter con un intervalo de repetición de cada 3 días a partir

del lunes, NetApp Backup and Recovery establece la programación en semanal los lunes, jueves y domingos. Se saltarán algunos días porque no es exactamente cada 3 días.

- Si la programación de SnapCenter está configurada para más de 7 días, NetApp Backup and Recovery configura la programación para que sea mensual. Se omitirán algunas instantáneas durante el mes.

  Ejemplo: Si tiene una política diaria de SnapCenter con un intervalo de repetición de cada 10 días a partir del día 2 de cada mes, NetApp Backup and Recovery, después de la migración, establece la programación en mensual los días 2, 12 y 22 del mes. NetApp Backup and Recovery omitirá algunos días el próximo mes.

Horarios por hora de SnapCenter importados

Las políticas por hora de SnapCenter con intervalos de repetición superiores a una hora se convierten en una política diaria en NetApp Backup and Recovery.

Cualquier política horaria con intervalos de repetición que no sean un factor de 24 (por ejemplo, 5, 7, etc.) omitirá algunas instantáneas en un día.

Ejemplo: Si tiene una política horaria de SnapCenter con un intervalo de repetición cada 5 horas a partir de la 1:00 a. m., NetApp Backup and Recovery (después de la migración) establecerá la programación en diaria con intervalos de 5 horas a la 1:00 a. m., 6:00 a. m., 11:00 a. m., 4:00 p. m. y 9:00 p. m. Se saltarán algunas horas, después de las 9:00 PM debería ser las 2:00 AM para repetir después de cada 5 horas, pero siempre será la 1:00 AM.

Retención de registros de las políticas de SnapCenter

Si tiene un recurso en SnapCenter con múltiples políticas, NetApp Backup and Recovery utiliza el siguiente orden de prioridad para asignar el valor de retención de registros:

- Para las políticas de "Copia de seguridad completa con política de copia de seguridad de registros" más "solo registro" en SnapCenter, NetApp Backup and Recovery utiliza el valor de retención de la política de solo registro.
- Para las políticas "Copia de seguridad completa solo con registro" y "Completa y registro" en SnapCenter, NetApp Backup and Recovery utiliza el valor de retención de solo registro.
- Para "Copia de seguridad completa y registro" más "Copia de seguridad completa" en SnapCenter, NetApp Backup and Recovery utiliza el valor de retención "Copia de seguridad completa y registro".
- Si solo tiene una copia de seguridad completa en SnapCenter, NetApp Backup and Recovery no habilita la copia de seguridad del registro.

Retención de copias de seguridad de registros

SnapCenter admite múltiples valores de retención para las políticas de un recurso. NetApp Backup and Recovery solo admite un valor de retención por recurso.

Recuento de retención de las políticas de SnapCenter

Si tiene un recurso con protección secundaria habilitada en SnapCenter con múltiples volúmenes de origen, múltiples volúmenes de destino y múltiples relaciones de SnapMirror , NetApp Backup and Recovery usa solo el recuento de retención de la primera política.

Ejemplo: Si tiene una política de SnapCenter con un recuento de retención de 5 y otra política con un

recuento de retención de 10, NetApp Backup and Recovery usa el recuento de retención de 5.

Etiquetas de SnapMirror de las políticas de SnapCenter

SnapCenter conserva las etiquetas SnapMirror para cada política después de la migración, incluso si cambia el nivel.

Ejemplo: Una política por hora de SnapCenter podría cambiar a diaria en NetApp Backup and Recovery. Sin embargo, las etiquetas de SnapMirror siguen siendo las mismas después de la migración.

Funciones de gestión de identidad y acceso (IAM) de NetApp Backup and Recovery

NetApp Backup and Recovery emplea la gestión de identidad y acceso (IAM) para controlar el acceso que tiene cada usuario a funciones y acciones específicas.

Para obtener más información sobre los roles de IAM específicos de NetApp Backup and Recovery, consulte "Funciones de NetApp Backup and Recovery en la NetApp Console" .

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 "Actualice 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":"pas
sword"}
> '
```

   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":"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 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
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 *WorkingEnvironment Id* y el valor bajo "agentId" denota *x-agent-id*.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

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
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" }'
```

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.

Niveles de almacenamiento de archivos de AWS compatibles con NetApp Backup and Recovery

NetApp Backup and Recovery admite dos clases de almacenamiento de archivo S3 y la mayoría de las regiones.

Para cambiar entre las versiones de la interfaz de usuario de NetApp Backup and Recovery , consulte"Cambiar a la interfaz de usuario anterior de NetApp Backup and Recovery" .

Clases de almacenamiento de archivo S3 compatibles con NetApp Backup and Recovery

Cuando se crean inicialmente los archivos de respaldo, se almacenan en el almacenamiento *estándar* de S3. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia, pero que también permite acceder a ellos de inmediato. Después de 30 días, las copias de seguridad pasan a la clase de almacenamiento S3 *Standard-Infrequent Access* para ahorrar costos.

Si sus clústeres de origen ejecutan ONTAP 9.10.1 o posterior, puede optar por organizar las copias de seguridad en niveles de almacenamiento *S3 Glacier* o *S3 Glacier Deep Archive* después de una cierta cantidad de días (normalmente más de 30 días) para optimizar aún más los costos. Puede establecerlo en "0" o entre 1 y 999 días. Si lo establece en "0" días, no podrá cambiarlo posteriormente a 1-999 días.

No se puede acceder a los datos en estos niveles inmediatamente cuando se los necesita y requerirán un mayor costo de recuperación, por lo que debe considerar con qué frecuencia necesitará restaurar datos de estos archivos de respaldo archivados. Consulte la sección en esta página sobre cómo restaurar datos desde el almacenamiento de archivo.

- 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.

Tenga en cuenta que cuando configura NetApp Backup and Recovery con este tipo de regla de ciclo de vida, no debe configurar ninguna regla de ciclo de vida al configurar el depósito en su cuenta de AWS.

"Obtenga más información sobre las clases de almacenamiento S3".

Restaurar datos desde el almacenamiento de archivo

Si bien almacenar archivos de respaldo más antiguos en un almacenamiento de archivo es mucho menos costoso que el almacenamiento Estándar o Estándar-IA, acceder a los datos de un archivo de respaldo en un almacenamiento de archivo para operaciones de restauración llevará más tiempo y costará más dinero.

¿Cuánto cuesta restaurar datos de Amazon S3 Glacier y Amazon S3 Glacier Deep Archive?

Hay 3 prioridades de restauración que puede elegir al recuperar datos de Amazon S3 Glacier y 2 prioridades de restauración al recuperar datos de Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive cuesta menos que S3 Glacier:

Nivel de archivo	Restaurar prioridad y costo		
	Alto	Estándar	Bajo
Glaciar S3	Recuperación más rápida, mayor coste	Recuperación más lenta, menor coste	Recuperación más lenta, menor costo

Nivel de archivo	Restaurar prioridad y costo		
Archivo de Glaciar Deep S3		Recuperación más rápida, mayor coste	Recuperación más lenta, menor costo

Cada método tiene una tarifa de recuperación por GB y una tarifa por solicitud diferentes. Para conocer los precios detallados de S3 Glacier por región de AWS, visite "Página de precios de Amazon S3" .

¿Cuánto tiempo tomará restaurar mis objetos archivados en Amazon S3 Glacier?

Hay 2 partes que componen el tiempo total de restauración:

- **Tiempo de recuperación**: el tiempo necesario para recuperar el archivo de respaldo del archivo y colocarlo en el almacenamiento estándar. A esto a veces se le llama el tiempo de "rehidratación". El tiempo de recuperación es diferente según la prioridad de restauración que elija.

Nivel de archivo	Restaurar prioridad y tiempo de recuperación		
	Alto	**Estándar**	**Bajo**
Glaciar S3	3-5 minutos	3-5 horas	5-12 horas
Archivo de Glaciar Deep S3		12 horas	48 horas

- **Tiempo de restauración**: el tiempo para restaurar los datos del archivo de respaldo en el almacenamiento estándar. Esta vez no es diferente a la operación de restauración típica directamente desde el almacenamiento estándar, cuando no se utiliza un nivel de archivo.

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 acceso a archivos de Azure compatibles con NetApp Backup and Recovery

NetApp Backup and Recovery admite un nivel de acceso de archivo de Azure y la mayoría de las regiones.

Para cambiar entre las versiones de la interfaz de usuario de NetApp Backup and Recovery , consulte"Cambiar a la interfaz de usuario anterior de NetApp Backup and Recovery" .

Niveles de acceso de Azure Blob compatibles con NetApp Backup and Recovery

Cuando se crean inicialmente los archivos de respaldo, se almacenan en el nivel de acceso *Cool*. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia, pero a los que se puede acceder de inmediato cuando es necesario.

Si sus clústeres de origen ejecutan ONTAP 9.10.1 o una versión posterior, puede optar por organizar las copias de seguridad en niveles desde el almacenamiento *Cool* al almacenamiento *Azure Archive* después de una cierta cantidad de días (normalmente más de 30 días) para optimizar aún más los costos. No se puede acceder a los datos de este nivel inmediatamente cuando se los necesita y requerirán un mayor costo de

recuperación, por lo que debe considerar con qué frecuencia podría necesitar restaurar datos de estos archivos de respaldo archivados. Consulte la sección en esta página sobre cómo restaurar datos desde el almacenamiento de archivo.

Tenga en cuenta que cuando configura NetApp Backup and Recovery 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 información sobre los niveles de acceso de Azure Blob".

Restaurar datos desde el almacenamiento de archivo

Si bien almacenar archivos de respaldo más antiguos en un almacenamiento de archivo es mucho menos costoso que el almacenamiento esporádico, acceder a los datos de un archivo de respaldo en Azure Archive para operaciones de restauración llevará más tiempo y costará más dinero.

¿Cuánto cuesta restaurar datos desde Azure Archive?

Hay dos prioridades de restauración que puede elegir al recuperar datos de Azure Archive:

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

Cada método tiene una tarifa de recuperación por GB y una tarifa por solicitud diferentes. Para conocer los precios detallados de Azure Archive por región de Azure, visite el sitio web "Página de precios de Azure" .

La prioridad alta no se admite al restaurar datos de Azure a sistemas StorageGRID .

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

Hay 2 partes que componen el tiempo de restauración:

- **Tiempo de recuperación**: el tiempo necesario para recuperar el archivo de copia de seguridad archivado de Azure Archive y colocarlo en el almacenamiento esporádico. A esto a veces se le llama el tiempo de “rehidratación”. El tiempo de recuperación es diferente según la prioridad de restauración que elija:
  - **Alto**: < 1 hora
  - **Estándar**: < 15 horas
- **Tiempo de restauración**: el tiempo para restaurar los datos del archivo de respaldo en el almacenamiento Cool. Esta vez no es diferente a la operación de restauración típica directamente desde el almacenamiento Cool, cuando no se utiliza un nivel de archivo.

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

Niveles de almacenamiento de archivos de Google compatibles con NetApp Backup and Recovery

NetApp Backup and Recovery admite una clase de almacenamiento de archivo de Google y la mayoría de las regiones.

Para cambiar entre las versiones de la interfaz de usuario de NetApp Backup and Recovery , consulte"Cambiar a la interfaz de usuario anterior de NetApp Backup and Recovery" .

Clases de almacenamiento de archivo de Google compatibles con NetApp Backup and Recovery

Cuando se crean inicialmente los archivos de respaldo, se almacenan en el almacenamiento *Estándar*. Este nivel está optimizado para almacenar datos a los que se accede con poca frecuencia, pero que también permite acceder a ellos de inmediato.

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 (normalmente más de 30 días) para optimizar aún más los costos. Los datos de este nivel requerirán un mayor costo de recuperación, por lo que deberá considerar con qué frecuencia necesitará restaurar datos de estos archivos de respaldo archivados. Consulte la sección en esta página sobre cómo restaurar datos desde el almacenamiento de archivo.

Tenga en cuenta que cuando configura NetApp Backup and Recovery con este tipo de regla de ciclo de vida, no debe configurar ninguna regla de ciclo de vida al configurar el depósito en su cuenta de Google.

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

Restaurar datos desde el almacenamiento de archivo

Si bien almacenar archivos de respaldo antiguos en el almacenamiento de archivo es mucho menos costoso que el almacenamiento estándar, acceder a los datos de un archivo de respaldo en el almacenamiento de archivo para operaciones de restauración tomará un poco más de tiempo y costará más dinero.

¿Cuánto cuesta restaurar datos de Google Archive?

Para conocer los precios detallados de Google Cloud Storage por región, visite "Página de precios de Google Cloud Storage" .

¿Cuánto tiempo tardará en restaurarse mis objetos archivados en Google Archive?

Hay 2 partes que componen el tiempo total de restauración:

- **Tiempo de recuperación**: el tiempo necesario para recuperar el archivo de respaldo del archivo y colocarlo en el almacenamiento estándar. A esto a veces se le llama el tiempo de “rehidratación”. A diferencia de las soluciones de almacenamiento más "frías" que ofrecen otros proveedores de nube, sus datos son accesibles en cuestión de milisegundos.
- **Tiempo de restauración**: el tiempo para restaurar los datos del archivo de respaldo en el almacenamiento estándar. Esta vez no es diferente a la operación de restauración típica directamente desde el almacenamiento estándar, cuando no se utiliza un nivel de archivo.

Información de copyright

Información de la marca comercial