Proteja los buckets con SnapMirror S3

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Proteja los buckets con SnapMirror S3

Obtenga más información sobre ONTAP SnapMirror S3

A partir de ONTAP 9.10.1, puede proteger buckets en almacenes de objetos de ONTAP S3 mediante mirroring de SnapMirror y funcionalidad de backup. A diferencia de SnapMirror estándar, SnapMirror S3 permite el mirroring y los backups en destinos que no son de NetApp, como AWS S3.

SnapMirror S3 admite mirroring activo y niveles de backup de buckets S3 de ONTAP en los destinos siguientes:

Destino	¿Admite los reflejos activos y la toma de control?	¿Compatible con backup y restauración?
ONTAP S3 • Bloques en la misma SVM • Los bloques de diferentes SVM en el mismo clúster • Bloques en SVM en clústeres diferentes	Sí	Sí
StorageGRID	No	Sí
AWS S3	No	Sí
Cloud Volumes ONTAP para Azure	Sí	Sí
Cloud Volumes ONTAP para AWS	Sí	Sí
Cloud Volumes ONTAP para Google Cloud	Sí	Sí

Puede proteger bloques existentes en servidores ONTAP S3 o puede crear nuevos bloques con protección de datos habilitada de inmediato.

Requisitos de SnapMirror S3

- Versión de ONTAP

  ONTAP 9.10.1 o una versión posterior debe ejecutarse en clústeres de origen y de destino.

  SnapMirror S3 no es compatible con las configuraciones de MetroCluster.

- Licencia

  Las siguientes licencias están disponibles en "ONTAP One"la suite de software y son necesarias en los sistemas de origen y destino de ONTAP para ofrecer acceso a:

  - Protocolo y almacenamiento ONTAP S3
  - SnapMirror S3 para dirigirse a otros destinos de almacén de objetos NetApp (ONTAP S3,

StorageGRID y Cloud Volumes ONTAP)

- SnapMirror S3 para dirigirse a almacenes de objetos de terceros, incluido AWS S3 (disponible en "Paquete de compatibilidad de ONTAP One")
- Si el clúster ejecuta ONTAP 9.10.1, se necesita un"Licencia de FabricPool".

- ONTAP S3
  - Los servidores ONTAP S3 deben ejecutar SVM de origen y de destino.
  - Se recomienda, pero no es obligatorio, que los certificados de CA para el acceso TLS estén instalados en sistemas que alojan servidores S3.
    - Los certificados de CA utilizados para firmar los certificados de los servidores S3 deben instalarse en la máquina virtual de almacenamiento de administración de los clústeres que alojan servidores S3.
    - Es posible usar un certificado de CA autofirmado o un certificado firmado por un proveedor de CA externo.
    - Si las máquinas virtuales de almacenamiento de origen o de destino no escuchan con HTTPS, no es necesario instalar certificados de CA.
- Relaciones entre iguales (para destinos de ONTAP S3)
  - Las LIF de interconexión de clústeres deben configurarse (para destinos ONTAP remotos) y las LIF de interconexión de clústeres del clúster de origen y de destino pueden conectarse a las LIF de datos de servidor S3 de origen y de destino.
  - Los clústeres de origen y destino tienen una relación entre iguales (para destinos de ONTAP remotos).
  - Las máquinas virtuales de almacenamiento de origen y de destino tienen una relación entre iguales (para todos los destinos ONTAP).
- Política de SnapMirror
  - Se requiere una política de SnapMirror específica de S3 para todas las relaciones de SnapMirror S3, pero puede usar la misma política para varias relaciones.
  - Puede crear su propia directiva o aceptar la predeterminada **continua**, que incluye los siguientes valores:
    - Acelerador (límite superior de rendimiento/ancho de banda): Ilimitado.
    - Tiempo objetivo de punto de recuperación: 1 hora (3600 segundos).

> Debe tener en cuenta que, cuando hay dos buckets S3 en una relación de SnapMirror, si hay políticas de ciclo de vida configuradas de forma que la versión actual de un objeto caduque (se elimina), se replica la misma acción en el bloque del partner. Esto es así incluso si el bloque de partners es de solo lectura o pasivo.

- Claves de usuario raíz Se requieren claves de acceso de usuario raíz de la máquina virtual de almacenamiento para las relaciones de SnapMirror S3; ONTAP no las asigna de forma predeterminada. La primera vez que crea una relación SnapMirror S3, debe verificar que las claves existan en las máquinas virtuales de almacenamiento de origen y destino y regenerarlas si no es así. Si necesita volver a regenerarlos, debe asegurarse de que todos los clientes y todas las configuraciones del almacén de objetos de SnapMirror que utilicen el par de claves secreta y de acceso se actualicen con las nuevas claves.

Para obtener información sobre la configuración del servidor S3, consulte los temas siguientes:

- "Habilite un servidor S3 en una máquina virtual de almacenamiento"

- "Acerca del proceso de configuración de ONTAP S3"

Para obtener información acerca de la relación entre iguales de clústeres y máquinas virtuales de almacenamiento, consulte el tema siguiente:

- "Preparación del mirroring y el almacenamiento (System Manager, pasos 1 a 6)"
- "Relaciones entre iguales de clústeres y SVM (CLI)"

Relaciones de SnapMirror admitidas

SnapMirror S3 admite relaciones en cascada y de abanico. Para obtener una descripción general, consulte "Puestas en marcha de protección de datos en cascada y distribución ramificada" .

SnapMirror S3 no admite puestas en marcha ramificadas (relaciones de protección de datos entre varios bloques de origen y un único bloque de destino). SnapMirror S3 puede admitir varios duplicados de bloque de varios clústeres en un único clúster secundario, pero cada bloque de origen debe tener su propio bloque de destino en el clúster secundario.

SnapMirror S3 no es compatible con entornos MetroCluster.

Controle el acceso a S3 cucharones

Cuando se crean bloques nuevos, se puede controlar el acceso mediante la creación de usuarios y grupos.

Aunque SnapMirror S3 replica objetos del bloque de origen a un bloque de destino, no replica usuarios, grupos ni políticas del almacén de objetos de origen al almacén de objetos de destino.

Los usuarios, las políticas de grupo, los permisos y los componentes similares deben estar configurados en el almacén de objetos de destino para que los clientes puedan acceder al bloque de destino durante un evento de conmutación por error.

Los usuarios de origen y de destino pueden utilizar las mismas claves de acceso y secretas, siempre que las claves de origen se proporcionen manualmente cuando el usuario se crea en el clúster de destino. Por ejemplo:

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

Para obtener más información, consulte los siguientes temas:

- "Añadir usuarios y grupos de S3 (System Manager)"
- "Crear un usuario de S3 (CLI)"
- "Crear o modificar grupos S3 (CLI)"

Utilice el bloqueo de objetos y el control de versiones de S3 con SnapMirror S3

Puede utilizar SnapMirror S3 en bloques de ONTAP habilitados para bloqueo de objetos y control de versiones, con algunas consideraciones:

- Para replicar un depósito de origen con el bloqueo de objetos activado, el bloque de destino también debe tener el bloqueo de objetos activado. Además, tanto el origen como el destino deben tener el control de

versiones activado. De este modo, se evitan los problemas de eliminación de mirroring en el depósito de destino cuando ambos bloques tienen políticas de retención predeterminadas diferentes.

- S3 SnapMirror no replica versiones históricas de los objetos. Sólo se replica la versión actual de un objeto.

Cuando los objetos Object Locked se duplican en un bucket de destino, mantienen su tiempo de retención original. Si se replican los objetos desbloqueados, adoptarán el período de retención predeterminado del depósito de destino. Por ejemplo:

- El período A tiene un período de retención predeterminado de 30 días y el período B tiene un período de retención predeterminado de 60 días. Los objetos replicados del cucharón A al cucharón B mantendrán su período de retención de 30 días, aunque sea inferior al período de retención predeterminado del cucharón B.
- El período A no tiene un período de retención predeterminado y el período B tiene un período de retención predeterminado de 60 días. Cuando los objetos desbloqueados se replican del cucharón A al cucharón B, adoptarán el período de retención de 60 días. Si un objeto se bloquea manualmente en el cucharón A, mantendrá su período de retención original cuando se replique en el cucharón B.
- El período A tiene un período de retención predeterminado de 30 días y el período B no tiene un período de retención predeterminado. Los objetos replicados del bloque A al bloque B mantendrán su período de retención de 30 días.

Refleje y protección de backup en un clúster remoto

Cree una relación de mirroring para un nuevo bloque de ONTAP S3 en el clúster remoto

Cuando crea nuevos buckets S3, puede protegerlos inmediatamente en un destino S3 de SnapMirror en un clúster remoto.

Acerca de esta tarea

Deberá realizar tareas tanto en los sistemas de origen como de destino.

Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre los clústeres de origen y de destino, y existe una relación entre iguales entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación de SnapMirror S3 para esta máquina virtual de almacenamiento, compruebe que existen claves de usuario raíz tanto para máquinas virtuales de almacenamiento de origen como de destino, y vuelva a generarlas si no las cumplen:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la pestaña **Configuración**, haga clic en el mosaico **S3**.
   c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
   d. Si no lo hay, haga clic junto a **root** y luego haga clic en **Regenerar clave**. No vuelva a generar la clave si ya existe.
2. Edite la máquina virtual de almacenamiento para añadir usuarios y añadir usuarios a grupos, tanto en las máquinas virtuales de almacenamiento de origen como de destino:

   Haga clic en **Almacenamiento > VM de almacenamiento**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en S3.

   Consulte "Añada usuarios y grupos de S3" para obtener más información.
3. En el clúster de origen, cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
   b. Haga clic junto a **Políticas de protección** y luego haga clic en **Agregar**.
      - Escriba el nombre de la política y una descripción.
      - Seleccione el alcance de las políticas, el clúster o la SVM
      - Seleccione **Continuo** para las relaciones de SnapMirror S3.
      - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
   b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
   c. En **permisos**, haga clic en **Agregar**.
      - **Principal** y **efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
      - **Acciones**- Asegúrese de que se muestran los siguientes valores:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Utilice los valores predeterminados (*bucketname, bucketname/**) u otros valores que necesite.

        Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre

estos campos.

d. En **Protección**, compruebe **Activar SnapMirror (ONTAP o nube)**. A continuación, introduzca los siguientes valores:

- Destino
  - **OBJETIVO: Sistema ONTAP**
  - **CLUSTER**: Seleccione el cluster remoto.
  - **STORAGE VM**: Seleccione una VM de almacenamiento en el cluster remoto.
  - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *source*.
- Origen
  - **Certificado de CA del SERVIDOR S3:** copie y pegue el contenido del certificado *Destination*.

5. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
6. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
7. Haga clic en **Guardar**. Se crea un nuevo bucket en la máquina virtual de almacenamiento de origen que se refleja en un nuevo bucket que se crea la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener más información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación de SnapMirror S3 para esta SVM, verifique que las claves de usuario raíz existan tanto para las SVM de origen como de destino y vuelva a generarlas si no las tienen:

   ```
   vserver object-store-server user show
   ```

   Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   No vuelva a generar la clave si ya existe.

2. Cree bloques en las SVM de origen y destino:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Añada reglas de acceso a las políticas de bloque predeterminadas tanto en las SVM de origen como de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Ejemplo

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. En el SVM de origen, cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parámetros:

   - Tipo `continuous`: El único tipo de política para las relaciones de SnapMirror S3 (obligatorio).
   - `-rpo` - especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
   - `-throttle` - especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

     Ejemplo

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instale los certificados de servidor de CA en las SVM de administrador de los clústeres de origen y destino:

   a. En el clúster de origen, instale el certificado de CA que firmó el certificado de servidor *DESTINATION* S3:
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. En el clúster de destino, instale el certificado de CA que firmó el certificado de servidor *source* S3:
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

Si utiliza un certificado firmado por un proveedor de CA externo, instale el mismo certificado en la SVM de administrador de origen y de destino.

Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

6. En el SVM de origen, cree una relación SnapMirror S3:

   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name` `-destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   Puede usar una política que haya creado o aceptar la predeterminada.

   Ejemplo

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy test-policy
   ```

7. Compruebe que el mirroring está activo:
   `snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Cree una relación de mirroring para un bloque de ONTAP S3 existente en el clúster remoto

Puede comenzar a proteger bloques de S3 existentes en cualquier momento; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1.

Acerca de esta tarea

Debe realizar tareas en los clústeres de origen y de destino.

Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre los clústeres de origen y de destino, y existe una relación entre iguales entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

Pasos

Puede crear una relación de mirroring mediante System Manager o la interfaz de línea de comandos de

ONTAP.

System Manager

1. Si esta es la primera relación de SnapMirror S3 para esta máquina virtual de almacenamiento, compruebe que existen claves de usuario raíz tanto para máquinas virtuales de almacenamiento de origen como de destino, y vuelva a generarlas si no las cumplen:
   a. Seleccione **Almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la pestaña **Configuración**, haga clic en el mosaico **S3**.
   c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
   d. Si no lo hay, haga clic en junto a **root**, luego haga clic en **Regenerar clave.** No vuelva a generar la clave si ya existe.
2. Verifique que los usuarios y grupos existentes estén presentes y tengan el acceso correcto tanto en las VM de almacenamiento de origen como en las de destino: Seleccione **Almacenamiento > VM de almacenamiento** y, a continuación, seleccione la VM de almacenamiento y, a continuación, la pestaña **Configuración**. Por último, localice el mosaico **S3**, seleccione y seleccione la pestaña **Usuarios** y luego la pestaña **Grupos** para ver la configuración de acceso de usuarios y grupos.

   Consulte "Añada usuarios y grupos de S3" para obtener más información.
3. En el clúster de origen, cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Seleccione **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
   b. Seleccione junto a **Políticas de protección**, luego haga clic en **Agregar**.
   c. Escriba el nombre de la política y una descripción.
   d. Seleccione el ámbito de la política, clúster o SVM.
   e. Seleccione **Continuo** para las relaciones de SnapMirror S3.
   f. Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliéndose con sus necesidades:
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione el cucharón que desea proteger.
   b. En la pestaña **Permisos**, haz clic en **Editar**, luego haz clic en **Agregar** en **Permisos**.
      - **Principal y efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
      - **Acciones**: Asegúrese de que se muestran los siguientes valores:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos**: Usa los valores predeterminados `(bucketname, bucketname/*)` u otros valores que necesites.

        Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre estos campos.

5. Proteja un bloque existente con la protección SnapMirror S3:
   a. Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
   b. Haga clic en **proteger** e introduzca los siguientes valores:
      - Destino
        - **OBJETIVO**: Sistema ONTAP
        - **CLUSTER**: Seleccione el cluster remoto.
        - **STORAGE VM**: Seleccione una VM de almacenamiento en el cluster remoto.
        - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *source*.
      - Origen
        - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *Destination*.
6. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
7. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
8. Haga clic en **Guardar**. El bloque existente se refleja en un nuevo bloque en la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener más información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación de SnapMirror S3 para esta SVM, verifique que existan las claves de usuario raíz tanto para las SVM de origen como de destino y vuelva a generarlas si no las mantienen: `vserver object-store-server user show` + Verifique que exista una clave de acceso para el usuario raíz. Si no lo hay, introduzca: `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + No vuelva a generar la clave si ya existe una.
2. Crear un bucket en la SVM de destino que sea el destino de mirroring:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Compruebe que las reglas de acceso de las políticas de bloque predeterminadas sean correctas tanto en las SVM de origen como de destino:

   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Ejemplo

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. En el SVM de origen, cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parámetros:

   - `continuous` – El único tipo de política para las relaciones SnapMirror S3 (requerido).
   - `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
   - `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

     Ejemplo

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instale los certificados de CA en las SVM de administrador de los clústeres de origen y destino:

   a. En el clúster de origen, instale el certificado de CA que firmó el certificado de servidor *DESTINATION* S3:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. En el clúster de destino, instale el certificado de CA que firmó el certificado de servidor *source* S3:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` + Si está utilizando un certificado firmado por un proveedor de CA externo, instale el mismo certificado en la SVM de administrador de origen y de destino.

   Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

6. En el SVM de origen, cree una relación SnapMirror S3:

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   Puede usar una política que haya creado o aceptar la predeterminada.

   Ejemplo

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. Compruebe que el mirroring está activo:
   `snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Asuma el control del bucket ONTAP S3 de destino en el clúster remoto

Si los datos de un bloque de origen dejan de estar disponibles, puede romper la relación de SnapMirror para hacer que el bloque de destino sea editable y comenzar a servir datos.

Acerca de esta tarea

Cuando se realiza una operación de toma de control, el bloque de origen se convierte en de solo lectura y el bloque de destino original se convierte en de lectura y escritura, con lo que se invierte la relación de SnapMirror S3.

Cuando el depósito de origen deshabilitado vuelve a estar disponible, SnapMirror S3 vuelve a sincronizar automáticamente el contenido de los dos bloques. No es necesario volver a sincronizar explícitamente la relación, tal y como es necesario en puestas en funcionamiento de SnapMirror para volúmenes.

La operación de toma de control se debe iniciar desde el clúster remoto.

Aunque SnapMirror S3 replica objetos del bloque de origen a un bloque de destino, no replica usuarios, grupos ni políticas del almacén de objetos de origen al almacén de objetos de destino.

Los usuarios, las políticas de grupo, los permisos y los componentes similares deben estar configurados en el almacén de objetos de destino para que los clientes puedan acceder al bloque de destino durante un evento de conmutación por error.

Los usuarios de origen y de destino pueden utilizar las mismas claves de acceso y secretas, siempre que las claves de origen se proporcionen manualmente cuando el usuario se crea en el clúster de destino. Por ejemplo:

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

System Manager

Conmutación por error desde el bloque no disponible y empiece a servir datos:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione **SnapMirror S3**.
2. Haga clic en ⋮, seleccione **Failover** y, a continuación, haga clic en **Failover**.

CLI

1. Inicie una operación de conmutación al nodo de respaldo para el bloque de destino:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Compruebe el estado de la operación de conmutación por error:
   `snapmirror show -fields status`

   Ejemplo

   ```
   dest_cluster::> snapmirror failover start -destination-path
   dest_svm1:/bucket/test-bucket-mirror
   ```

Información relacionada

- "Añadir usuarios y grupos de S3 (System Manager)"
- "Crear un usuario de S3 (CLI)"
- "Crear o modificar grupos S3 (CLI)"
- "inicio de conmutación por error de snapmirror"
- "espectáculo de Snapmirror"

Restaure un bloque de ONTAP S3 desde la SVM de destino en el clúster remoto

Si los datos de un depósito de origen se pierden o se dañan, puede volver a rellenar los datos restaurando objetos desde un bloque de destino.

Acerca de esta tarea

Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El bloque de destino para la operación de restauración debe ser mayor que el espacio utilizado lógico del bucket de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

La operación de restauración debe iniciarse desde el clúster remoto.

System Manager

Restaure los datos de la copia de seguridad:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione **SnapMirror S3**.
2. Haga clic ⋮ y luego seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
   - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
     - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
     - Seleccione el bloque existente.
     - Copie y pegue el contenido del certificado de CA del servidor *destination* S3.
   - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
     - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
     - El nombre, la capacidad y el nivel de servicio de rendimiento del bloque nuevo. Consulte "Los niveles de servicio de almacenamiento" para obtener más información.
     - El contenido del certificado de CA del servidor *Destination* S3.
4. En **destino**, copie y pegue el contenido del certificado de CA del servidor *source* S3.
5. Haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Restaure los cucharones bloqueados

A partir de ONTAP 9.14.1, puede realizar backups de bloques bloqueados y restaurarlos según sea necesario.

Es posible restaurar un bloque de bloqueo de objetos a un bloque nuevo o existente. Puede seleccionar un depósito bloqueado por objeto como destino en las siguientes situaciones:

- **Restaurar a un nuevo cubo**: Cuando se habilita el bloqueo de objetos, un cubo puede restaurarse creando un cubo que también tiene habilitado el bloqueo de objetos. Cuando restaura un bucket bloqueado, se replican el modo de bloqueo de objetos y el periodo de retención del bucket original. También puede definir un período de retención de bloqueo diferente para el nuevo período. Este período de retención se aplica a objetos no bloqueados de otros orígenes.
- **Restaurar a un cubo existente**: Un cubo bloqueado por objeto se puede restaurar a un cubo existente, siempre y cuando el control de versiones y un modo de bloqueo de objetos similar estén habilitados en el cubo existente. Se mantiene la tenencia de retención del cucharón original.
- **Restaurar cubo no bloqueado**: Incluso si el bloqueo de objetos no está habilitado en un cubo, puede restaurarlo en un cubo que tiene el bloqueo de objetos activado y está en el clúster de origen. Al restaurar el bloque, todos los objetos no bloqueados se bloquean, y se aplican el modo de retención y la tenencia del bloque de destino.

CLI

1. Crear el nuevo bloque de destino para la restauración. Para obtener más información, consulte "Cree una relación de backup en el cloud para un nuevo bloque de ONTAP S3".
2. Inicie una operación de restauración para el bloque de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

Ejemplo

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

Obtenga más información sobre `snapmirror restore` en el "Referencia de comandos del ONTAP".

Protección de reflejo y backup en el clúster local

Cree una relación de mirroring para un nuevo bloque de ONTAP S3 en el clúster local

Cuando crea nuevos buckets S3, puede protegerlos inmediatamente en un destino S3 de SnapMirror en el mismo clúster. Puede reflejar datos en un bloque de una máquina virtual de almacenamiento diferente o en la misma máquina virtual de almacenamiento que el origen.

Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación de SnapMirror S3 para esta máquina virtual de almacenamiento, compruebe que existen claves de usuario raíz tanto para máquinas virtuales de almacenamiento de origen como de destino, y vuelva a generarlas si no las cumplen:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la pestaña **Settings**, haga clic en el mosaico S3.
   c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz
   d. Si no lo hay, haga clic junto a **root** y luego haga clic en **Regenerar clave**. No vuelva a generar la clave si ya existe.
2. Edite la VM de almacenamiento para agregar usuarios y para agregar usuarios a grupos, tanto en las VM de almacenamiento de origen como de destino: Haga clic en **Almacenamiento > VM de almacenamiento**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, en S3.

   Consulte "Añada usuarios y grupos de S3" para obtener más información.
3. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
   b. Haga clic junto a **Políticas de protección** y luego haga clic en **Agregar**.
      - Escriba el nombre de la política y una descripción.
      - Seleccione el alcance de las políticas, el clúster o la SVM
      - Seleccione **Continuo** para las relaciones de SnapMirror S3.
      - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
   c. En **permisos**, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
      - **Principal** y **efecto**: Seleccione los valores correspondientes a la configuración del grupo de usuarios o acepte los valores predeterminados.
      - **Acciones** - Asegúrese de que se muestran los siguientes valores:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Utilice los valores predeterminados `(bucketname, bucketname/*)` u otros valores que necesite

        Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre estos campos.

d. En **Protección**, compruebe **Activar SnapMirror (ONTAP o nube)**. A continuación, introduzca los siguientes valores:

- Destino
  - **OBJETIVO**: Sistema ONTAP
  - **CLUSTER**: Seleccione el cluster local.
  - **VM DE ALMACENAMIENTO**: Seleccione una VM de almacenamiento en el clúster local.
  - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado fuente.
- Origen
  - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado de destino.

5. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
6. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
7. Haga clic en **Guardar**. Se crea un nuevo bucket en la máquina virtual de almacenamiento de origen que se refleja en un nuevo bucket que se crea la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener más información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación de SnapMirror S3 para esta SVM, verifique que las claves de usuario raíz existan tanto para las SVM de origen como de destino y vuelva a generarlas si no las tienen:
   `vserver object-store-server user show`

   Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:
   `vserver object-store-server user regenerate-keys -vserver` *`svm_name`* `-user` *`root`*

   No vuelva a generar la clave si ya existe.

2. Cree bloques en las SVM de origen y destino:

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. Añada reglas de acceso a las políticas de bloque predeterminadas tanto en las SVM de origen como de destino:

   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parámetros:

   - `continuous` – El único tipo de política para las relaciones SnapMirror S3 (requerido).
   - `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
   - `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

   Ejemplo

   ```
   src_cluster::> snapmirror policy create -vserver vs0 -type
   continuous -rpo 0 -policy test-policy
   ```

5. Instale los certificados de servidor de CA en la SVM de administrador:

   a. Instale el certificado de CA que firmó el certificado del servidor *source* S3 en la SVM de administración:
      `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. Instale el certificado de CA que firmó el certificado del servidor *DESTINATION* S3 en la SVM de administración
      `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`: + Si está utilizando un certificado firmado por un proveedor de CA externo, solo necesita instalar este certificado en la SVM de administración.

      Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

6. Crear una relación SnapMirror S3:
   `snapmirror create -source-path src_svm_name:/bucket/bucket_name`

`-destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

Puede usar una política que haya creado o aceptar la predeterminada.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror -policy test-policy
```

7. Compruebe que el mirroring está activo:
`snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Crear una relación de mirroring para un bloque de ONTAP S3 existente en el clúster local

Puede empezar a proteger bloques de S3 existentes en el mismo clúster en cualquier momento; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1. Puede reflejar datos en un bloque de una máquina virtual de almacenamiento diferente o en la misma máquina virtual de almacenamiento que el origen.

Antes de empezar

- Se han completado los requisitos para las versiones de ONTAP, las licencias y la configuración de servidores S3.
- Existe una relación de paridad entre las máquinas virtuales de almacenamiento de origen y de destino.
- Los certificados DE CA se necesitan para las máquinas virtuales de origen y de destino. Puede usar certificados de CA autofirmados o certificados firmados por un proveedor de CA externo.

System Manager

1. Si esta es la primera relación de SnapMirror S3 para esta máquina virtual de almacenamiento, compruebe que existen claves de usuario raíz tanto para máquinas virtuales de almacenamiento de origen como de destino, y vuelva a generarlas si no las cumplen:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la pestaña **Configuración**, haga clic en el mosaico **S3**.
   c. En la ficha **usuarios**, compruebe que hay una clave de acceso para el usuario raíz.
   d. Si no lo hay, haga clic junto a **root** y luego haga clic en **Regenerar clave**. No vuelva a generar la clave si ya existe
2. Verifique que los usuarios y grupos existentes estén presentes y tengan el acceso correcto tanto en las VM de almacenamiento de origen como en las de destino: Seleccione **Almacenamiento > VM de almacenamiento**, luego seleccione la VM de almacenamiento y, a continuación, la pestaña **Configuración**. Por último, localice el mosaico **S3**, seleccione y seleccione la pestaña **Usuarios** y luego la pestaña **Grupos** para ver la configuración de acceso de usuarios y grupos.

   Consulte "Añada usuarios y grupos de S3" para obtener más información.
3. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de directiva local**.
   b. Haga clic junto a **Políticas de protección** y luego haga clic en **Agregar**.
      - Escriba el nombre de la política y una descripción.
      - Seleccione el alcance de las políticas, el clúster o la SVM
      - Seleccione **Continuo** para las relaciones de SnapMirror S3.
      - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliendo con sus necesidades:
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, seleccione el cucharón que desea proteger.
   b. En la pestaña **Permisos**, haz clic en **Editar**, luego haz clic en **Agregar** en **Permisos**.
      - **Principal** y **efecto**: Seleccione los valores correspondientes a la configuración del grupo de usuarios o acepte los valores predeterminados.
      - **Acciones** - Asegúrese de que se muestran los siguientes valores:

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - **Recursos** - Utilice los valores predeterminados *(bucketname, bucketname/*)* u otros valores que necesite.

        Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre estos campos.

5. Proteja un bloque existente con SnapMirror S3:
   a. Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
   b. Haga clic en **proteger** e introduzca los siguientes valores:
      - Destino
        - **OBJETIVO**: Sistema ONTAP
        - **CLUSTER**: Seleccione el cluster local.
        - **STORAGE VM**: Seleccione la misma máquina virtual de almacenamiento o una diferente.
        - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *source*.
      - Origen
        - **Certificado de CA del SERVIDOR S3**: Copie y pegue el contenido del certificado *Destination*.
6. Marque **Utilice el mismo certificado en el destino** si está utilizando un certificado firmado por un proveedor de CA externo.
7. Si hace clic en **Configuración de destino**, también puede introducir sus propios valores en lugar de los valores predeterminados para el nombre del bloque, la capacidad y el nivel de servicio de rendimiento.
8. Haga clic en **Guardar**. El bloque existente se refleja en un nuevo bloque en la máquina virtual de almacenamiento de destino.

Haga retroceder los cucharones bloqueados

A partir de ONTAP 9.14.1, puede crear un backup de bloques S3 bloqueados y restaurarlos según sea necesario.

Al definir la configuración de protección para un bloque nuevo o existente, puede habilitar el bloqueo de objetos en los buckets de destino, siempre y cuando los clústeres de origen y de destino ejecuten ONTAP 9.14.1 o una versión posterior, y que el bloqueo de objetos se habilite en el bloque de origen. El modo de bloqueo de objetos y la tenencia de retención de bloqueos del bloque de origen se aplican a los objetos replicados en el bloque de destino. También puede definir un período de retención de bloqueo diferente para el depósito de destino en la sección **Configuración de destino**. Este período de retención también se aplica a cualquier objeto no bloqueado replicado desde el bloque de origen e interfaces S3.

Para obtener más información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación de SnapMirror S3 para esta SVM, verifique que las claves de usuario raíz existan tanto para las SVM de origen como de destino y vuelva a generarlas si no las tienen:
   `vserver object-store-server user show`

   Compruebe que hay una clave de acceso para el usuario raíz. Si no lo hay, introduzca:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   No vuelva a generar la clave si ya existe.

2. Crear un bucket en la SVM de destino que sea el destino de mirroring:

```
vserver object-store-server bucket create -vserver svm_name -bucket
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Compruebe que las reglas de acceso a las políticas de bloque predeterminadas sean correctas tanto en las SVM de origen como de destino:

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]`
   ```

   Ejemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:

   ```
   snapmirror policy create -vserver svm_name -policy policy_name -type
   continuous [-rpo _integer] [-throttle throttle_type] [-comment text]
   [additional_options]
   ```

   Parámetros:

   - `continuous` – El único tipo de política para las relaciones SnapMirror S3 (requerido).
   - `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional).
   - `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

     Ejemplo

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. Instale los certificados de servidor de CA en la SVM de administrador:

   a. Instale el certificado de CA que firmó el certificado del servidor *source* S3 en la SVM de administración:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. Instale el certificado de CA que firmó el certificado del servidor *DESTINATION* S3 en la SVM de administración
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`: + Si está utilizando un certificado firmado por un proveedor de CA externo, solo necesita instalar este certificado en la SVM de administración.

Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

6. Crear una relación SnapMirror S3:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   Puede usar una política que haya creado o aceptar la predeterminada.

   Ejemplo

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy test-policy
   ```

7. Compruebe que el mirroring está activo:
`snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Asuma el control del bucket ONTAP S3 de destino en el clúster local

Si los datos de un bloque de origen dejan de estar disponibles, puede romper la relación de SnapMirror para hacer que el bloque de destino sea editable y comenzar a servir datos.

Acerca de esta tarea

Cuando se realiza una operación de toma de control, el bloque de origen se convierte en de solo lectura y el bloque de destino original se convierte en de lectura y escritura, con lo que se invierte la relación de SnapMirror S3.

Cuando el depósito de origen deshabilitado vuelve a estar disponible, SnapMirror S3 vuelve a sincronizar automáticamente el contenido de los dos bloques. No es necesario resincronizar explícitamente la relación, como es necesario para puestas en funcionamiento de SnapMirror para volúmenes estándar.

Si el bloque de destino se encuentra en un clúster remoto, la operación de toma de control se debe iniciar desde el clúster remoto.

System Manager

Conmutación por error desde el bloque no disponible y empiece a servir datos:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione **SnapMirror S3**.
2. Haga clic en ⋮, seleccione **Failover** y, a continuación, haga clic en **Failover**.

CLI

1. Inicie una operación de conmutación al nodo de respaldo para el bloque de destino:
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Compruebe el estado de la operación de conmutación por error:
   `snapmirror show -fields status`

Ejemplo

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Información relacionada

- "inicio de conmutación por error de snapmirror"
- "espectáculo de Snapmirror"

Restaure un bloque ONTAP S3 a partir de la SVM de destino en el clúster local

Cuando los datos de un depósito de origen se pierden o dañan, puede volver a rellenar los datos restaurando objetos desde un bloque de destino.

Acerca de esta tarea

Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El bloque de destino para la operación de restauración debe ser mayor que el espacio utilizado lógico del bucket de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

La operación de restauración se debe iniciar desde el clúster local.

System Manager

Restaure los datos de backup:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione el bloque.
2. Haga clic ⋮ y luego seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
   - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
     - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
     - Seleccione el bloque existente.
4. Copie y pegue el contenido del certificado de CA del servidor S3 de destino.
   - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
     - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
     - El nombre, la capacidad y el nivel de servicio de rendimiento del bloque nuevo. Consulte "Los niveles de servicio de almacenamiento" para obtener más información.
     - El contenido del certificado de CA de servidor S3 de destino.
5. En **destino**, copie y pegue el contenido del certificado de CA del servidor S3 de origen.
6. Haga clic en **Protección** > Relaciones para supervisar el progreso de la restauración.

Restaure los cucharones bloqueados

A partir de ONTAP 9.14.1, puede realizar backups de bloques bloqueados y restaurarlos según sea necesario.

Es posible restaurar un bloque de bloqueo de objetos a un bloque nuevo o existente. Puede seleccionar un depósito bloqueado por objeto como destino en las siguientes situaciones:

- **Restaurar a un nuevo cubo**: Cuando se habilita el bloqueo de objetos, un cubo puede restaurarse creando un cubo que también tiene habilitado el bloqueo de objetos. Cuando restaura un bucket bloqueado, se replican el modo de bloqueo de objetos y el periodo de retención del bucket original. También puede definir un período de retención de bloqueo diferente para el nuevo período. Este período de retención se aplica a objetos no bloqueados de otros orígenes.
- **Restaurar a un cubo existente**: Un cubo bloqueado por objeto se puede restaurar a un cubo existente, siempre y cuando el control de versiones y un modo de bloqueo de objetos similar estén habilitados en el cubo existente. Se mantiene la tenencia de retención del cucharón original.
- **Restaurar cubo no bloqueado**: Incluso si el bloqueo de objetos no está habilitado en un cubo, puede restaurarlo en un cubo que tiene el bloqueo de objetos activado y está en el clúster de origen. Al restaurar el bloque, todos los objetos no bloqueados se bloquean, y se aplican el modo de retención y la tenencia del bloque de destino.

CLI

1. Si va a restaurar objetos en un bloque nuevo, cree el bloque nuevo. Para obtener más información, consulte "Cree una relación de backup en el cloud para un nuevo bloque de ONTAP S3".
2. Inicie una operación de restauración para el bloque de destino:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

Ejemplo

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Obtenga más información sobre `snapmirror restore` en el "Referencia de comandos del ONTAP".

Protección de backup con destinos cloud

Requisitos para las relaciones objetivo de cloud de ONTAP SnapMirror S3

Asegúrese de que los entornos de origen y destino cumplen los requisitos de la protección de backup de SnapMirror S3 en los destinos cloud.

Debe tener credenciales de cuenta válidas con el proveedor de almacenes de objetos para acceder al bloque de datos.

Las LIF de interconexión de clústeres y un espacio IP se deben configurar en el clúster antes de que el clúster pueda conectarse a un almacén de objetos cloud. Debe crear LIF de interconexión de clústeres en cada nodo para transferir datos sin problemas desde el almacenamiento local al almacén de objetos de cloud.

Para los destinos StorageGRID, debe conocer la siguiente información:

- Nombre del servidor, expresado como un nombre de dominio completo (FQDN) o una dirección IP
- nombre de bloque; el bloque debe existir antes
- clave de acceso
- clave secreta

Además, el certificado de CA utilizado para firmar el certificado del servidor StorageGRID debe instalarse en la máquina virtual de almacenamiento de administración del clúster ONTAP S3 mediante el `security certificate install` dominio. Para obtener más información, consulte "Instalar un certificado de CA" si usa StorageGRID.

Para los destinos AWS S3, debe conocer la siguiente información:

- Nombre del servidor, expresado como un nombre de dominio completo (FQDN) o una dirección IP
- nombre de bloque; el bloque debe existir antes
- clave de acceso
- clave secreta

El servidor DNS de la máquina virtual de almacenamiento de administrador del clúster de ONTAP debe poder resolver FQDN (si se utiliza) a direcciones IP.

Información relacionada

- "instalación del certificado de seguridad"

Cree una relación de backup en el cloud para un nuevo bloque de ONTAP S3

Cuando crea nuevos buckets S3, puede realizar una copia de seguridad de ellos inmediatamente en un bucket de destino S3 de SnapMirror en un proveedor de almacenamiento de objetos, que puede ser un sistema StorageGRID o una implementación de Amazon S3.

Antes de empezar

- Tiene credenciales de cuenta válidas e información de configuración para el proveedor de almacenes de objetos.
- Las interfaces de red entre clústeres y un espacio IP se han configurado en el sistema de origen.
- • La configuración de DNS para el equipo virtual de almacenamiento de origen debe poder resolver el FQDN del destino.

System Manager

1. Edite la máquina virtual de almacenamiento para añadir usuarios y añadir usuarios a los grupos:
   a. Haga clic en **Almacenamiento > VM de almacenamiento**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en **S3**.

      Consulte "Añada usuarios y grupos de S3" para obtener más información.

2. Añada un almacén de objetos cloud en el sistema de origen:
   a. Haga clic en **Protección > Descripción general** y seleccione **almacenamiento de objetos en la nube**.
   b. Haga clic en **Agregar** y, a continuación, seleccione **Amazon S3** o **StorageGRID**.
   c. Introduzca los siguientes valores:
      - Nombre de almacén de objetos en cloud
      - Estilo de URL (ruta o host virtual)
      - Máquina virtual de almacenamiento (habilitada para S3)
      - Nombre del servidor de almacén de objetos (FQDN)
      - Certificado de almacén de objetos
      - Clave de acceso
      - Clave secreta
      - Nombre del contenedor (cubo)
3. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
   b. Haga clic → junto a **Políticas de protección** y luego haga clic en **Agregar**.
      - Escriba el nombre de la política y una descripción.
      - Seleccione el alcance de las políticas, el clúster o la SVM
      - Seleccione **Continuo** para las relaciones de SnapMirror S3.
      - Introduzca los valores **acelerador** y **objetivo de punto de recuperación**.
4. Crear un bloque con la protección SnapMirror:
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione el equipo virtual de almacenamiento, introduzca un tamaño y, a continuación, haga clic en **más opciones**.
   c. En **permisos**, haga clic en **Agregar**. Verificar permisos es opcional pero se recomienda.
      - **Principal** y **Efecto**: Selecciona los valores correspondientes a la configuración de tu grupo de usuarios o acepta los valores predeterminados.
      - **Acciones**: Asegúrate de que se muestren los siguientes valores:

```
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
```

- **Recursos**: Usa los valores predeterminados `_(bucketname, bucketname/*)` u otros valores que necesites.

  Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre estos campos.

d. En **Protección**, marque **Activar SnapMirror (ONTAP o nube)**, seleccione **almacenamiento en nube** y, a continuación, seleccione **almacén de objetos en nube**.

Al hacer clic en **Guardar**, se crea un nuevo bloque en el equipo virtual de almacenamiento de origen y se realiza una copia de seguridad en el almacén de objetos en la nube.

CLI

1. Si esta es la primera relación de SnapMirror S3 para esta SVM, verifique que existan las claves de usuario raíz tanto para las SVM de origen como de destino y vuelva a generarlas si no lo hacen: `vserver object-store-server user show` + Confirme que existe una clave de acceso para el usuario raíz. Si no lo hay, introduzca: `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + No vuelva a generar la clave si ya existe una.
2. Cree un bloque en la SVM de origen: `vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`
3. Añada reglas de acceso a la política de bloques predeterminada: `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   Ejemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada: `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parámetros: * `type continuous`: El único tipo de política para las relaciones de SnapMirror S3 (obligatorio). * `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional). * `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

Ejemplo

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Si el destino es un sistema StorageGRID, instale el certificado de servidor de CA de StorageGRID en la SVM de administrador del clúster de origen:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

6. Defina el almacén de objetos de destino de SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   Parámetros: * `-object-store-name`: El nombre del destino del almacén de objetos en el sistema ONTAP local. * `-usage` – usar `data` para este flujo de trabajo. * `-provider-type` – `AWS_S3` Y `SGWS` los destinos (StorageGRID) son compatibles. * `-server` – El FQDN o la dirección IP del servidor de destino. * `-is-ssl-enabled` –Habilitar SSL es opcional pero recomendado. + Aprenda más sobre `snapmirror object-store config create` en el "Referencia de comandos del ONTAP".

   Ejemplo

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS
   -server sgws.example.com -container-name target-test-bucket -is-ssl
   -enabled true -port 443 -access-key abc123 -secret-password xyz890
   ```

7. Crear una relación SnapMirror S3:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parámetros: * `-destination-path` - El nombre del almacén de objetos que creó en el paso anterior y el valor fijo `objstore`. + puede usar una directiva que ha creado o aceptar el valor predeterminado.

   Ejemplo

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path sgws-store:/objstore -policy test-policy
   ```

8. Compruebe que el mirroring está activo:
`snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Cree una relación de backup en cloud para un bloque de ONTAP S3 existente

Puede empezar a realizar en cualquier momento backups de bloques de S3 existentes; por ejemplo, si actualizó una configuración de S3 desde una versión anterior a ONTAP 9.10.1.

Antes de empezar

- Tiene credenciales de cuenta válidas e información de configuración para el proveedor de almacenes de objetos.
- Las interfaces de red entre clústeres y un espacio IP se han configurado en el sistema de origen.
- La configuración de DNS para el equipo virtual de almacenamiento de origen debe poder resolver el FQDN del destino.

System Manager

1. Compruebe que los usuarios y grupos están definidos correctamente: Haga clic en **Almacenamiento > VM de almacenamiento**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, en S3.

   Consulte "Añada usuarios y grupos de S3" para obtener más información.

2. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
   b. Haga clic junto a **Políticas de protección** y luego haga clic en **Agregar**.
   c. Escriba el nombre de la política y una descripción.
   d. Seleccione el alcance de las políticas, el clúster o la SVM
   e. Seleccione **Continuo** para las relaciones de SnapMirror S3.
   f. Introduzca los valores de los objetivos **acelerador** y **punto de recuperación**.
3. Añada un almacén de objetos cloud en el sistema de origen:
   a. Haga clic en **Protección > Descripción general** y seleccione **Tienda de objetos en la nube**.
   b. Haga clic en **Agregar** y, a continuación, seleccione **Amazon S3** o **otros** para StorageGRID Webscale.
   c. Introduzca los siguientes valores:
      - Nombre de almacén de objetos en cloud
      - Estilo de URL (ruta o host virtual)
      - Máquina virtual de almacenamiento (habilitada para S3)
      - Nombre del servidor de almacén de objetos (FQDN)
      - Certificado de almacén de objetos
      - Clave de acceso
      - Clave secreta
      - Nombre del contenedor (cubo)
4. Compruebe que la política de acceso a bloques del bloque existente sigue cumpliéndose con sus necesidades:
   a. Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara que desea proteger.
   b. En la pestaña **Permisos**, haz clic en **Editar**, luego haz clic en **Agregar** en **Permisos**.
      - **Principal** y **efecto**: Seleccione los valores correspondientes a la configuración de su grupo de usuarios o acepte los valores predeterminados.
      - **Acciones** - Asegúrese de que se muestren los siguientes valores: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Recursos** - Utilice los valores predeterminados *`(bucketname, bucketname/*)`* u otros valores que necesite.

Consulte "Gestionar el acceso del usuario a bloques" para obtener más información sobre estos campos.

5. Haga copias de seguridad del bloque con SnapMirror S3:
   a. Haga clic en **almacenamiento** > **Cuchos** y, a continuación, seleccione la cuchara de la que desea realizar la copia de seguridad.
   b. Haga clic en **proteger**, seleccione **almacenamiento en nube** en **objetivo** y, a continuación, seleccione **almacén de objetos en nube**.

Al hacer clic en **Guardar**, se realiza una copia de seguridad del bloque existente en el almacén de objetos en la nube.

CLI

1. Compruebe que las reglas de acceso de la política de depósito predeterminada son correctas:
   `vserver object-store-server bucket policy add-statement -vserver` *`svm_name`*
   `-bucket` *`bucket_name`* `-effect {allow|deny} -action` *`object_store_actions`*
   `-principal` *`user_and_group_names`* `-resource` *`object_store_resources`* `[-sid`
   `text``] [-index` *`integer`*`]`

   Ejemplo

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Cree una política SnapMirror S3 si no tiene una existente y no desea utilizar la política predeterminada:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parámetros: * `type continuous`: El único tipo de política para las relaciones de SnapMirror S3 (obligatorio). * `-rpo` – especifica el tiempo para el objetivo de punto de recuperación, en segundos (opcional). * `-throttle` – especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos (opcional).

   Ejemplo

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. Si el destino es un sistema StorageGRID, instale el certificado de CA de StorageGRID en la SVM de administrador del clúster de origen:
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Obtenga más información sobre `security certificate install` en el "Referencia de comandos del ONTAP".

4. Defina el almacén de objetos de destino de SnapMirror S3:
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

   Parámetros: * `-object-store-name`: El nombre del destino del almacén de objetos en el sistema ONTAP local. * `-usage` – usar `data` para este flujo de trabajo. * `-provider-type` – `AWS_S3` Y `SGWS` los destinos (StorageGRID) son compatibles. * `-server` – El FQDN o la dirección IP del servidor de destino. * `-is-ssl-enabled` –Habilitar SSL es opcional pero recomendado. + Aprenda más sobre `snapmirror object-store config create` en el "Referencia de comandos del ONTAP".

   Ejemplo

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS
   -server sgws.example.com -container-name target-test-bucket -is-ssl
   -enabled true -port 443 -access-key abc123 -secret-password xyz890
   ```

5. Crear una relación SnapMirror S3:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parámetros: * `-destination-path` - El nombre del almacén de objetos que creó en el paso anterior y el valor fijo `objstore`. + puede usar una directiva que ha creado o aceptar el valor predeterminado.

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
   -destination-path sgws-store:/objstore -policy test-policy
   ```

6. Compruebe que el mirroring está activo:
`snapmirror show -policy-type continuous -fields status`

Información relacionada

- "snapmirror create"
- "Crear política de SnapMirror"
- "espectáculo de Snapmirror"

Restaure un bloque S3 de ONTAP desde un destino cloud

Cuando los datos de un bloque de origen se pierden o dañan, puede volver a rellenar los datos mediante la restauración a partir de un bloque de destino.

Acerca de esta tarea

Puede restaurar el bloque de destino en un bloque existente o en un bloque nuevo. El bloque de destino para

la operación de restauración debe ser mayor que el espacio lógico usado del cucharón de destino.

Si utiliza un bloque existente, debe estar vacío al iniciar una operación de restauración. La restauración no "rollback" de un bloque en el tiempo; más bien, rellena un bloque vacío con su contenido anterior.

System Manager

Restaure los datos de backup:

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione **SnapMirror S3**.
2. Haga clic ⋮ y luego seleccione **Restaurar**.
3. En **Fuente**, seleccione **cucharón existente** (predeterminado) o **Nuevo cucharón**.
   - Para restaurar a un **segmento existente** (valor predeterminado), lleve a cabo las siguientes acciones:
     - Seleccione la máquina virtual de almacenamiento y clúster para buscar el bloque existente.
     - Seleccione el bloque existente.
     - Copie y pegue el contenido del certificado de CA del servidor *destination* S3.
   - Para restaurar a un **New Bucket**, introduzca los siguientes valores:
     - El equipo virtual de clúster y almacenamiento para alojar el nuevo bloque.
     - El nombre, la capacidad y el nivel de servicio de rendimiento del nuevo cucharón. Consulte "Los niveles de servicio de almacenamiento" para obtener más información.
     - El contenido del certificado de CA de servidor S3 de destino.
4. En **destino**, copie y pegue el contenido del certificado de CA del servidor *source* S3.
5. Haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

Procedimiento de la CLI

1. Crear el nuevo bloque de destino para la restauración. Para obtener más información, consulte "Crear una relación de backup para un bloque (destino de cloud)".
2. Inicie una operación de restauración para el bloque de destino:
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Ejemplo

   En el siguiente ejemplo se restaura un bucket de destino en un bucket existente.

   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   Obtenga más información sobre `snapmirror restore` en el "Referencia de comandos del ONTAP".

Modifique una política de ONTAP SnapMirror S3

Puede modificar una política de SnapMirror de S3 si desea ajustar los valores de RPO y de acelerador.

System Manager

1. Haga clic en **Protección > Relaciones** y, a continuación, seleccione la política de protección para la relación que desea modificar.
2. Haga clic ⋮ junto al nombre de la política y, a continuación, haga clic en **Editar**.

CLI

Modificar una política de SnapMirror S3:
`snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo <integer>] [-throttle <throttle_type>] [-comment <text>]`

Parámetros:

- `-rpo`: Especifica el tiempo para el objetivo de punto de recuperación, en segundos.
- `-throttle`: Especifica el límite superior de rendimiento/ancho de banda, en kilobytes/segundos.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

Información relacionada

- "modificar la política de SnapMirror"