Gestión del almacenamiento de objetos S3

ONTAP 9

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/es-es/ontap/s3-config/index.html on April 16, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

Gestión del almacenamiento de objetos S3 . . . 1
Conozca el soporte de S3 en ONTAP 9 . . . 1
Planificación . . . 4
Configurar . . . 9
Proteja los bloques con SnapMirror de S3 . . . 59
Auditar eventos S3 . . . 94

Gestión del almacenamiento de objetos S3

Conozca el soporte de S3 en ONTAP 9

Información general de la configuración de S3

A partir de ONTAP 9.8, puede habilitar un servidor de almacenamiento de objetos ONTAP simple Storage Service (S3) en un clúster de ONTAP.

ONTAP es compatible con dos casos prácticos en las instalaciones para dar servicio al almacenamiento de objetos S3:

- Organización en niveles FabricPool para un bloque en el clúster local (nivel a un bloque local) o clúster remoto (nivel de cloud).
- Acceso de aplicación de cliente S3 a un bloque del clúster local o de un clúster remoto.

A partir de ONTAP 9.14.1, puede habilitar un servidor de almacenamiento de objetos S3 en una SVM en un agregado reflejado o no reflejado en configuraciones de IP y FC de MetroCluster.

A partir de ONTAP 9.12.1, se puede habilitar un servidor de almacenamiento de objetos S3 en una SVM en un agregado no reflejado en una configuración IP de MetroCluster. Para obtener más información sobre las limitaciones de los agregados no reflejados en las configuraciones IP de MetroCluster, consulte "Consideraciones sobre los agregados no reflejados".

Debe usar estos procedimientos si desea configurar el almacenamiento de objetos S3 de la siguiente manera:

- Desea proporcionar almacenamiento de objetos S3 desde un clúster existente que ejecuta ONTAP.

  ONTAP S3 es adecuado si se desean funcionalidades de S3 en los clústeres existentes sin necesidad de hardware ni gestión adicionales. Sin embargo, el software NetApp StorageGRID sigue siendo la solución insignia de NetApp para el almacenamiento de objetos. Para obtener más información, consulte "Documentación de StorageGRID".

- Tiene privilegios de administrador de clúster, no de administrador de SVM.

Configuración de S3 con System Manager y la interfaz de línea de comandos de ONTAP

Puede configurar y gestionar ONTAP S3 con System Manager y la interfaz de línea de comandos de ONTAP. Cuando se habilita S3 y se crean bloques con System Manager, ONTAP selecciona los valores predeterminados de prácticas recomendadas para simplificar la configuración. Si es necesario especificar parámetros de configuración, se recomienda usar la CLI de ONTAP. Si configura el servidor y los bloques de S3 desde la CLI, puede seguir gestionarlos con System Manager si lo desea, o viceversa.

Cuando se crea un bloque de S3 con System Manager, ONTAP configura un nivel de servicio de rendimiento predeterminado que es el más alto disponible en el sistema. Por ejemplo, en un sistema AFF, el valor predeterminado sería **extremo**. Los niveles de servicio de rendimiento son grupos de políticas de calidad de servicio (QoS) adaptativas predefinidos. En lugar de uno de los niveles de servicio predeterminados, puede especificar un grupo de políticas de calidad de servicio personalizado o ningún grupo de políticas.

Los grupos de políticas de calidad de servicio adaptativas predefinidos son:

- **Extreme**: Se utiliza para aplicaciones que esperan la latencia más baja y el rendimiento más alto.

- **Rendimiento**: Se utiliza para aplicaciones con necesidades de rendimiento y latencia modestos.
- **Valor**: Se utiliza para aplicaciones para las que el rendimiento y la capacidad son más importantes que la latencia.
- **Personalizado**: Especifique una política de QoS personalizada o ninguna política de QoS.

Si selecciona **usar para clasificación por niveles**, no se seleccionan niveles de servicio de rendimiento y el sistema intenta seleccionar medios de bajo costo con un rendimiento óptimo para los datos organizados por niveles.

Consulte también: "Utilice grupos de políticas de calidad de servicio adaptativos".

ONTAP intenta aprovisionar este bloque en niveles locales que tengan los discos más adecuados para cumplir el nivel de servicio elegido. Sin embargo, si necesita especificar qué discos se incluirán en el bloque, considere la configuración del almacenamiento de objetos S3 desde la CLI especificando los niveles locales (agregado). Si configura el servidor S3 desde la CLI, puede seguir gestionarlo con System Manager si lo desea.

Si desea la capacidad de especificar qué agregados se utilizan para bloques, solo puede hacerlo mediante la CLI.

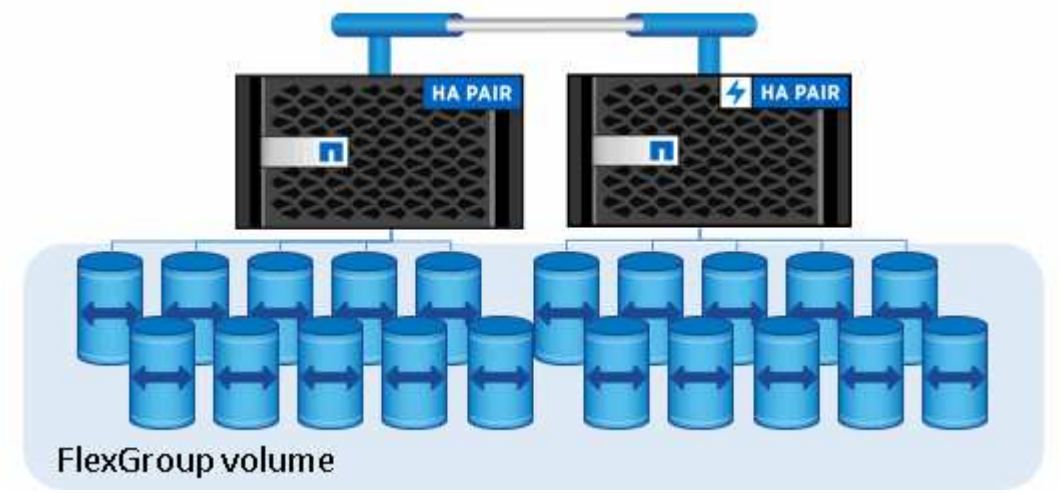
Configuración de bloques de S3 en Cloud Volumes ONTAP

Si desea servir bloques de Cloud Volumes ONTAP, se recomienda encarecidamente seleccionar manualmente los agregados subyacentes para garantizar que solo utilicen un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia. Por lo tanto, en entornos Cloud Volumes ONTAP, debería hacerlo Configure cubos de S3 desde la interfaz de línea de comandos.

De lo contrario, los servidores S3 en Cloud Volumes ONTAP están configurados y mantenidos de la misma forma en Cloud Volumes ONTAP que en entornos locales.

Arquitectura

En ONTAP, la arquitectura subyacente para un bloque es un volumen FlexGroup, un espacio de nombres único que está compuesto por varios volúmenes constituyentes, pero que se gestiona como un único volumen.

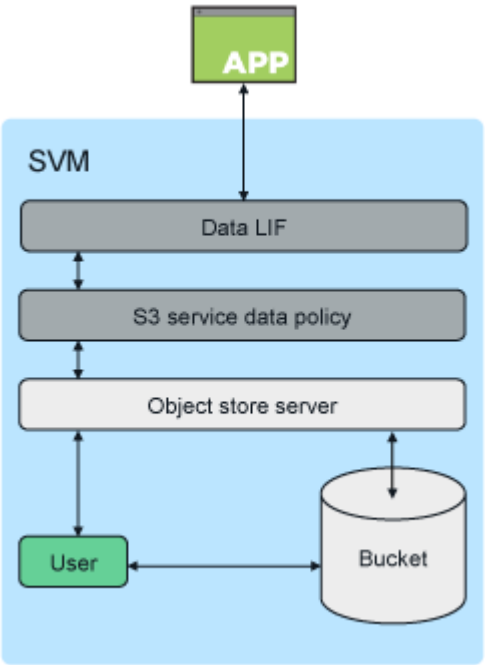


Los bloques solo están limitados por los máximos físicos del hardware subyacente, los máximos

arquitectónicos podrían ser mayores. Los bloques pueden aprovechar el tamaño elástico de FlexGroup para hacer crecer automáticamente un componente de un volumen FlexGroup si se está quedando sin espacio. Existe un límite de 1000 bloques por volumen de FlexGroup, o 1/3 de la capacidad del volumen de FlexGroup (para hacer frente al crecimiento de datos en bloques).

No se permite acceso al protocolo NAS o SAN al volumen FlexGroup que contiene bloques S3.

El acceso al bloque se proporciona a través de usuarios autorizados y aplicaciones cliente.



Casos de uso

Existen tres casos prácticos principales para el acceso de clientes a los servicios ONTAP S3:

- Para sistemas ONTAP que utilizan ONTAP S3 como nivel de capacidad de FabricPool remota (cloud)

  El servidor y el bloque de S3 que contienen el nivel de capacidad (para datos *fríos*) se encuentran en un clúster diferente al nivel de rendimiento (para datos *hot*).

- Para los sistemas ONTAP que usan ONTAP S3 como nivel de FabricPool local

  El servidor y el bloque de S3 que contiene el nivel de capacidad están en el mismo clúster, pero en un par de alta disponibilidad diferente, al nivel de rendimiento.

- Para aplicaciones de cliente S3 externas

  ONTAP S3 da servicio a las aplicaciones cliente S3 que se ejecutan en sistemas que no son de NetApp.

Se recomienda proporcionar acceso a buckets de ONTAP S3 mediante HTTPS. Cuando HTTPS está habilitado, se requieren certificados de seguridad para una integración correcta con SSL/TLS. A continuación, se requieren claves secretas y de acceso de los usuarios clientes para autenticar el usuario con ONTAP S3, así como para autorizar los permisos de acceso de los usuarios para operaciones en ONTAP S3. La aplicación de cliente también debe tener acceso al certificado de CA raíz (el certificado firmado del servidor

ONTAP S3) para poder autenticar el servidor y crear una conexión segura entre el cliente y el servidor.

Los usuarios se crean dentro de la SVM habilitada para S3 y sus permisos de acceso se pueden controlar a nivel de bloque o SVM; es decir, se puede otorgar acceso a uno o más bloques dentro de la SVM.

De forma predeterminada, HTTPS está habilitado en los servidores ONTAP S3. Es posible deshabilitar HTTPS y habilitar HTTP para el acceso de cliente, en cuyo caso no se requiere la autenticación con certificados de CA. Sin embargo, cuando se habilita HTTP y HTTPS está deshabilitado, todas las comunicaciones con el servidor ONTAP S3 se envían por la red en texto sin cifrar.

Para obtener más información, consulte "Informe técnico: S3 en las prácticas recomendadas de ONTAP"

Información relacionada

"Gestión de volúmenes de FlexGroup"

Planificación

Compatibilidad de versiones de ONTAP para el almacenamiento de objetos S3

ONTAP es compatible con el almacenamiento de objetos S3 para entornos locales que comienzan con ONTAP 9.8. Cloud Volumes ONTAP admite el almacenamiento de objetos S3 para entornos cloud que empiezan por ONTAP 9.9.1.

Compatibilidad de S3 con Cloud Volumes ONTAP

ONTAP S3 está configurado y funciona igual en Cloud Volumes ONTAP que en entornos locales, con una excepción:

- Los agregados subyacentes deben ser solo de un nodo. Más información acerca de "Creación de bloques en entornos CVO".

Proveedor de cloud	Versión de ONTAP
Azure	ONTAP 9.9.1 y versiones posteriores
AWS	ONTAP 9.11.0 y versiones posteriores
Google Cloud	ONTAP 9.12.1 y versiones posteriores

Vista previa pública de S3 en ONTAP 9.7

En ONTAP 9.7, el almacenamiento de objetos S3 se introdujo como una vista previa pública. Esta versión no estaba destinada a entornos de producción y ya no se actualizará a partir de ONTAP 9.8. Solo ONTAP 9.8 y las versiones posteriores admiten el almacenamiento de objetos S3 en entornos de producción.

Los bloques de S3 creados con la vista previa pública de 9.7 pueden usarse en ONTAP 9.8 y versiones posteriores, pero no pueden aprovechar las mejoras de funciones. Si ha creado bloques con la vista previa pública de 9.7, debe migrar el contenido de esos bloques a 9.8 bloques para garantizar el soporte de la función, la seguridad y las mejoras de rendimiento.

Acciones compatibles con ONTAP S3

Las acciones de ONTAP S3 son compatibles con las API DE REST estándar de S3

excepto que se indica a continuación. Para obtener más detalles, consulte "Referencia de la API de Amazon S3".

Operaciones de bloques

Las siguientes operaciones son compatibles en ONTAP mediante las API S3 de AWS:

Funcionamiento del cucharón	Soporte de ONTAP empezando por
CreateBucket	ONTAP 9.11.1
DeleteBucket	ONTAP 9.11.1
DeleteBucketPolicy	ONTAP 9.12.1
GetBucketAcl	ONTAP 9,8
GetBucketLifecycleConfiguration	ONTAP 9.13.1 * solo se admiten acciones de caducidad
GetBucketLocation	ONTAP 9.10.1
GetBucketPolicy	ONTAP 9.12.1
Segmento de cabeza	ONTAP 9,8
ListCuchers	ONTAP 9,8
Control de versiones de lista	ONTAP 9.11.1
ListObjectVersions	ONTAP 9.11.1
PutBucket	• ONTAP 9.11.1 • ONTAP 9,8: Solo compatible con API DE REST DE ONTAP
PutBucketLifecycleConfiguration	ONTAP 9.13.1 * solo se admiten acciones de caducidad
Política de PutBucketPolicy	ONTAP 9.12.1

Operaciones de objeto

A partir de ONTAP 9.9.1, ONTAP S3 admite el etiquetado y los metadatos de objetos.

- PutObject y CreateMultipartUpload incluyen pares clave-valor mediante `x-amz-meta-<key>`.

  Por ejemplo: `x-amz-meta-project: ontap_s3`.

- GetObject. Y HeadObject devuelven metadatos definidos por el usuario.
- A diferencia de los metadatos, las etiquetas se pueden leer independientemente de los objetos mediante:
  - PutObjectEtiquetado
  - GetObjectEtiquetado
  - DeleteObjectTagging

A partir de ONTAP 9.11.1, ONTAP S3 admite el control de versiones de objetos y acciones asociadas con

estas API de ONTAP:

- GetBucketVersioning
- ListBucketVersions
- PutBucketVersioning

Operación de objeto	Soporte de ONTAP empezando por
AbortMultipartUpload	ONTAP 9,8
CompleteMultipartUpload	ONTAP 9,8
CopyObject	ONTAP 9.12.1
CreateMultipartUpload	ONTAP 9,8
DeleteObject	ONTAP 9,8
DeleteObjects	ONTAP 9.11.1
DeleteObjectTagging	ONTAP 9.9.1
GetBucketVersioning	ONTAP 9.11.1
GetObject	ONTAP 9,8
GetObjectAcl	ONTAP 9,8
GetObjectRetention	ONTAP 9.14.1
GetObjectEtiquetado	ONTAP 9.9.1
Objeto principal	ONTAP 9,8
ListMultipartUpload	ONTAP 9,8
ListObjects	ONTAP 9,8
ListObjectsV2	ONTAP 9,8
ListBucketVersions	ONTAP 9.11.1
ListParts	ONTAP 9,8
PutBucketVersioning	ONTAP 9.11.1
Objeto de puta	ONTAP 9,8
PutObjectLockConfiguration	ONTAP 9.14.1
PutObjectRetention	ONTAP 9.14.1
PutObjectEtiquetado	ONTAP 9.9.1
UploadPart	ONTAP 9,8
UploadPartCopy	ONTAP 9.12.1

Normativas de grupo

Estas operaciones no son específicas de S3 y generalmente se asocian a procesos de identidad y gestión (IAM). ONTAP admite estos comandos, pero no utiliza las API DE REST del IAM.

- Crear política
- Directiva de AttachGroup

Gestión de usuarios

Estas operaciones no son específicas de S3 y generalmente se asocian con procesos IAM.

- CreateUser
- Deleteuser
- CreateGroup
- DeleteGroup

Interoperabilidad de ONTAP S3

El servidor ONTAP S3 interactúa de manera normal con otras funcionalidades de ONTAP, excepto que se indica en esta tabla.

Área de operación	Compatible	No admitido
Cloud Volumes ONTAP	• Clientes de Azure en ONTAP 9.9.1 y versiones posteriores • Clientes de AWS en ONTAP 9.11.0 y versiones posteriores • Clientes de Google Cloud en ONTAP 9.12.1 y versiones posteriores	• Cloud Volumes ONTAP para cualquier cliente en ONTAP 9.8 y versiones anteriores
Protección de datos	• Cloud Sync • "Control de versiones de objetos" (A partir de ONTAP 9.11.1) • "SnapMirror S3" (A partir de ONTAP 9.10.1) • Configuraciones de IP de MetroCluster (comenzando por ONTAP 9.12.1) • SnapLock (versión inicial de ONTAP 9.14.1) • WORM (a partir de ONTAP 9.14.1)	• Codificación de borrado • Gestión de la vida útil de la información • NDMP • SMTape • SnapMirror Cloud • Recuperación ante desastres de SVM • SyncMirror • Copias Snapshot creadas por el usuario

Área de operación	Compatible	No admitido
Cifrado	• Cifrado de agregados de NetApp (NAE) • Cifrado de volúmenes de NetApp (NVE) • Cifrado en almacenamiento de NetApp (NSE) • TLS/SSL	• ESCORIA
Eficiencia del almacenamiento	• Deduplicación • Compresión • Compactación	• Eficiencias a nivel de agregados • Clon de volumen del volumen de FlexGroup que contiene bloques ONTAP S3
Virtualización del almacenamiento	-	Virtualización FlexArray de NetApp
Calidad de servicio (QoS)	• Máximos de calidad de servicio (techos) • Mínimos de calidad de servicio (pisos)	-
Características adicionales	• "Auditar eventos S3" (A partir de ONTAP 9.10.1)	• Volúmenes de FlexCache • FPolicy • Qtrees • Cuotas

Soluciones de terceros validadas con ONTAP S3

NetApp ha validado las siguientes soluciones de terceros para su uso con ONTAP S3. Si la solución que busca no aparece en la lista, póngase en contacto con su representante de cuentas de NetApp.

Soluciones de terceros validadas en ONTAP S3

NetApp ha probado estas soluciones en colaboración con los partners correspondientes.

- Amazon SageMaker
- Cliente Apache Hadoop S3A
- Apache Kafka
- CommVault (V11)
- Confluente Kafka
- Red Hat Quay

- RUBRIK
- Copo de nieve
- Trino
- Veeam (V12)

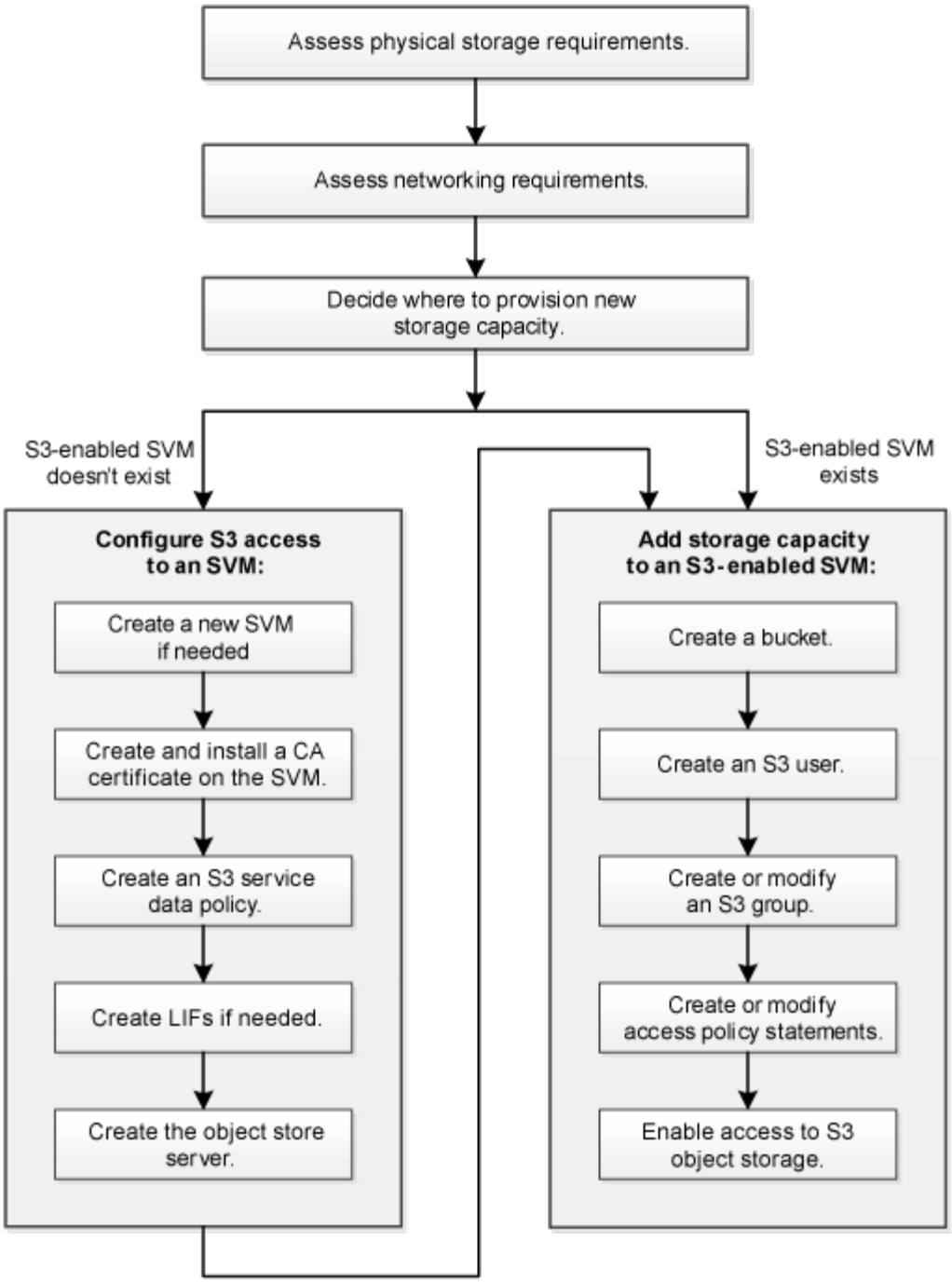
Configurar

Acerca del proceso de configuración de S3

Flujo de trabajo de configuración de S3

La configuración de S3 implica evaluar los requisitos de almacenamiento físico y de red y, a continuación, elegir un flujo de trabajo específico para su objetivo: Configurar el acceso S3 a una SVM nueva o existente, o añadir un bloque y usuarios a una SVM existente que ya esté completamente configurada para acceder a S3.

Cuando configura el acceso S3 a una nueva máquina virtual de almacenamiento mediante System Manager, se le pedirá que introduzca información de certificados y de redes, y que la máquina virtual de almacenamiento y el servidor de almacenamiento de objetos S3 se crean en una única operación.



Evaluar los requisitos de almacenamiento físico

Antes de aprovisionar el almacenamiento S3 para clientes, debe asegurarse de que haya espacio suficiente en los agregados existentes para el nuevo almacén de objetos. Si no lo hay, puede añadir discos a los agregados existentes o crear nuevos agregados del tipo y la ubicación que desee.

Acerca de esta tarea

Cuando se crea un bloque de S3 en una SVM con la función S3 habilitada, se crea automáticamente un volumen FlexGroup para admitir el bloque. Puede dejar a ONTAP Select los agregados y componentes de FlexGroup automáticamente (predeterminado) o puede seleccionar los agregados subyacentes y los componentes de FlexGroup usted mismo.

Si decide especificar los agregados y los componentes de FlexGroup; por ejemplo, si tiene requisitos de rendimiento específicos para los discos subyacentes, debe asegurarse de que la configuración de su agregado sea conforme a las directrices de prácticas recomendadas para aprovisionar un volumen de FlexGroup. Obtenga más información:

- "Gestión de volúmenes de FlexGroup"
- "Informe técnico de NetApp 4571-a: Mejores prácticas para los volúmenes ONTAP FlexGroup de NetApp"

Si está sirviendo bloques de Cloud Volumes ONTAP, se recomienda encarecidamente que seleccione manualmente los agregados subyacentes para garantizar que estén usando solo un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia. Descubra "Creación de bloques para Cloud Volumes ONTAP".

Puede usar el servidor ONTAP S3 para crear un nivel de capacidad FabricPool local, es decir, en el mismo clúster que el nivel de rendimiento. Esto puede resultar útil, por ejemplo, si tiene discos SSD conectados a un par de alta disponibilidad y desea colocar en niveles los datos *fríos* en discos HDD de otro par de alta disponibilidad. En este caso de uso, el servidor de S3 y el bloque que contiene el nivel de capacidad local deben estar, por lo tanto, en un par de alta disponibilidad diferente al nivel de rendimiento. La organización en niveles local no es compatible en clústeres de un nodo ni de dos nodos.

Pasos

1. Mostrar el espacio disponible en los agregados existentes:

   ```
   storage aggregate show
   ```

   Si hay un agregado con espacio suficiente o la ubicación de nodos necesaria, registre su nombre para la configuración de S3.

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. Si no hay agregados con suficiente espacio o la ubicación de nodos necesaria, añada discos a un agregado existente mediante el uso de `storage aggregate add-disks` o cree un nuevo agregado con el `storage aggregate create` comando.

Evaluar los requisitos de red

Antes de proporcionar almacenamiento S3 a los clientes, debe verificar que la red esté correctamente configurada para cumplir los requisitos de aprovisionamiento de S3.

Antes de empezar

Deben configurarse los siguientes objetos de red de clúster:

- Puertos físicos y lógicos
- Dominios de retransmisión
- Subredes (si es necesario)
- Espacios IP (según se requiera, además del espacio IP predeterminado)
- Grupos de conmutación por error (según sea necesario, además del grupo de conmutación por error predeterminado para cada dominio de retransmisión).
- Firewalls externos

Acerca de esta tarea

Para los niveles de capacidad de FabricPool remota (cloud) y los clientes S3 remotos, debe usar una SVM de datos y configurar LIF de datos. Para los niveles de cloud de FabricPool, también se deben configurar las LIF de interconexión de clústeres; no es necesaria la relación de clústeres entre iguales.

Para los niveles de capacidad locales de FabricPool, debe utilizar la SVM del sistema (denominada «'Cluster'»), pero tiene dos opciones para la configuración de LIF:

- Puede usar las LIF de clúster.

  En esta opción, no se necesita ninguna otra configuración de LIF, pero habrá un aumento en el tráfico en los LIF del clúster. Además, el nivel local no será accesible para otros clústeres.

- Se pueden usar LIF de datos e interconexión de clústeres.

  Esta opción requiere una configuración adicional, lo que incluye habilitar las LIF para el protocolo S3, pero también será posible acceder al nivel local como nivel de cloud de FabricPool remoto a otros clústeres.

Pasos

1. Mostrar los puertos físicos y virtuales disponibles:

   ```
   network port show
   ```

   - Cuando sea posible, debe utilizar el puerto con la velocidad más alta para la red de datos.
   - Todos los componentes de la red de datos deben tener la misma configuración de MTU para obtener el mejor rendimiento.

2. Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, compruebe que la subred existe y que tenga suficientes direcciones disponibles:

   ```
   network subnet show
   ```

   Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las subredes se crean mediante la `network subnet create` comando.

3. Mostrar espacios IP disponibles:

   ```
   network ipspace show
   ```

   Puede usar el espacio IP predeterminado o un espacio IP personalizado.

4. Si desea usar direcciones IPv6, compruebe que IPv6 esté habilitado en el clúster:

   ```
   network options ipv6 show
   ```

   Si es necesario, puede habilitar IPv6 con el `network options ipv6 modify` comando.

Decidir dónde aprovisionar la nueva capacidad de almacenamiento S3

Antes de crear un bloque de S3 nuevo, debe decidir si colocarlo en una SVM nueva o existente. Esta decisión determina su flujo de trabajo.

Opciones

- Si desea aprovisionar un bloque en una SVM nueva o una SVM que no esté habilitada para S3, complete los pasos en los temas siguientes.

  "Cree una SVM para S3"

  "Cree un bloque para S3"

  Aunque S3 puede coexistir en una SVM con NFS y SMB, es posible que elija crear una SVM nueva si se cumple alguna de las siguientes afirmaciones:

  - Es la primera vez que habilita S3 en un clúster.
  - Tiene SVM existentes en un clúster en el que no desea habilitar la compatibilidad con S3.
  - Tiene una o varias SVM con la función S3 habilitada en un clúster y desea otro servidor S3 con diferentes características de rendimiento.
    Después de habilitar S3 en la SVM, proceda a aprovisionar un bloque.

- Si desea aprovisionar el bloque inicial o un bloque adicional en una SVM existente habilitada para S3, complete los pasos del siguiente tema.

  "Cree un bloque para S3"

Configure el acceso S3 a una SVM

Cree una SVM para S3

Aunque S3 puede coexistir con otros protocolos en una SVM, es posible que desee crear una SVM nueva para aislar el espacio de nombres y la carga de trabajo.

Acerca de esta tarea

Si solo va a proporcionar almacenamiento de objetos S3 desde una SVM, el servidor S3 no requiere ninguna configuración de DNS. Sin embargo, puede configurar DNS en la SVM si se usan otros protocolos.

Cuando configura el acceso S3 a una nueva máquina virtual de almacenamiento mediante System Manager, se le pedirá que introduzca información de certificados y de redes, y que la máquina virtual de

almacenamiento y el servidor de almacenamiento de objetos S3 se crean en una única operación.

Ejemplo 1. Pasos

System Manager

Debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes usarán para el acceso S3. El FQDN del servidor S3 no debe comenzar por un nombre de bloque.

Debe estar preparado para introducir direcciones IP para los datos de roles de interfaz.

Si utiliza un certificado firmado por una CA externa, se le pedirá que lo introduzca durante este procedimiento, también tendrá la opción de usar un certificado generado por el sistema.

1. Habilite S3 en una máquina virtual de almacenamiento.

   a. Agregue un nuevo equipo virtual de almacenamiento: Haga clic en **almacenamiento > Storage VMs** y, a continuación, haga clic en **Add**.

      Si se trata de un sistema nuevo sin equipos virtuales de almacenamiento existentes: Haga clic en **Panel > Configurar protocolos**.

   Si va a agregar un servidor S3 a un equipo virtual de almacenamiento existente: Haga clic en **almacenamiento > Storage VMs**, seleccione una máquina virtual de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ⚙ En **S3**.

   a. Haga clic en **Activar S3** y, a continuación, introduzca el nombre del servidor S3.
   b. Seleccione el tipo de certificado.

      Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.

   c. Introduzca las interfaces de red.
2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
   - La clave secreta no se volverá a mostrar.
   - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Compruebe que S3 tiene licencia en el clúster:

   ```
   system license show -package s3
   ```

   Si no lo está, póngase en contacto con su representante de ventas.

2. Cree una SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Utilice el valor UNIX del `-rootvolume-security-style` opción.
- Utilice el C.UTF-8 predeterminado `-language` opción.
- La `ipspace` el ajuste es opcional.

3. Compruebe la configuración y el estado de la SVM recién creada:

```
vserver show -vserver <svm_name>
```

La `Vserver Operational State` el campo debe mostrar la `running` estado. Si muestra la `initializing` estado, significa que hubo un error en algunas operaciones intermedias, como la creación del volumen raíz, y que debe eliminarse la SVM y volver a crearla.

Ejemplos

El siguiente comando crea una SVM para acceder a los datos en el espacio IP ipspaceA:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

El siguiente comando muestra que se creó una SVM con un volumen raíz de 1 GB, y se inició automáticamente y está en `running` estado. El volumen raíz tiene una política de exportación predeterminada que no incluye reglas, por lo que el volumen raíz no se exporta tras la creación. De forma predeterminada, la cuenta de usuario de vsadmin se crea y está en la `locked` estado. El rol vsadmin se asigna a la cuenta de usuario de vsadmin predeterminada.

```
cluster-1::> vserver show -vserver svm1.example.com
                                   Vserver: svm1.example.com
                              Vserver Type: data
                           Vserver Subtype: default
                              Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                 NIS Domain: -
                 Root Volume Security Style: unix
                                LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                              Quota Policy: default
                List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                              IPspace Name: ipspaceA
```

Cree e instale un certificado de CA en la SVM

Se requiere un certificado de la entidad de certificación (CA) para habilitar el tráfico HTTPS desde clientes S3 a la SVM habilitada para S3.

Acerca de esta tarea

Aunque es posible configurar un servidor S3 para que use únicamente HTTP y, aunque es posible configurar clientes sin requisitos de certificado de CA, es una práctica recomendada proteger el tráfico HTTPS a servidores ONTAP S3 con un certificado de CA.

Un certificado de CA no es necesario para un caso de uso de organización en niveles local, donde el tráfico de IP pasa únicamente por las LIF del clúster.

Las instrucciones de este procedimiento crearán e instalarán un certificado autofirmado de ONTAP. También se admiten certificados DE CA de proveedores externos; consulte la documentación de autenticación de administrador para obtener más información.

"Autenticación de administrador y RBAC"

Consulte `security certificate` páginas de manual para opciones de configuración adicionales.

Pasos

1. Cree un certificado digital autofirmado:

   `security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name`

   La `-type root-ca` Opción crea e instala un certificado digital autofirmado para firmar otros certificados actuando como entidad de certificación (CA).

   La `-common-name` La opción crea el nombre de la entidad de certificación (CA) de la SVM y se utilizará al generar el nombre completo del certificado.

   El tamaño predeterminado del certificado es de 2048 bits.

   Ejemplo

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Cuando se muestre el nombre generado del certificado; asegúrese de guardarlo para pasos posteriores de este procedimiento.

2. Genere una solicitud de firma de certificación:

   `security certificate generate-csr -common-name s3_server_name [additional_options]`

   La `-common-name` El parámetro de la solicitud de firma debe ser el nombre del servidor S3 (FQDN).

   Puede proporcionar la ubicación y otra información detallada sobre la SVM si lo desea.

   Se le solicitará que conserve una copia de su solicitud de certificado y la clave privada para futuras consultas.

3. Firme la CSR con SVM_CA para generar el certificado de S3 Server:

   `security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial ca_cert_serial_number [additional_options]`

   Escriba las opciones de comando que ha utilizado en pasos anteriores:

   - `-ca` — el nombre común de la CA que introdujo en el paso 1.
   - `-ca-serial` — el número de serie de CA desde el Paso 1. Por ejemplo, si el nombre del certificado de CA es svm1_CA_159D1587CE21E9D4_svm1_ca, el número de serie es 159D1587CE21E9D4.

     De forma predeterminada, el certificado firmado caducará en 365 días. Puede seleccionar otro valor y especificar otros detalles de firma.

Cuando se le solicite, copie e introduzca la cadena de solicitud de certificado que guardó en el paso 2.

Se muestra un certificado firmado; guárdelo para un uso posterior.

4. Instale el certificado firmado en la SVM habilitada para S3:

   ```
   security certificate install -type server -vserver svm_name
   ```

   Cuando se le solicite, introduzca el certificado y la clave privada.

   Puede introducir certificados intermedios si desea una cadena de certificados.

   Cuando se muestren la clave privada y el certificado digital firmado por CA, guárdelos para referencia futura.

5. Obtenga el certificado de clave pública:

   ```
   security certificate show -vserver svm_name -common-name ca_cert_name -type
   root-ca -instance
   ```

   Guarde el certificado de clave pública para la configuración posterior del cliente.

   Ejemplo

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                         Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                     Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Cree una política de datos de servicio de S3

Puede crear políticas de servicio para los servicios de gestión y datos de S3. Se necesita una política de datos de servicio de S3 para habilitar el tráfico de datos de S3 en las LIF.

Acerca de esta tarea

Es necesaria una política de datos de servicio de S3 si se usan LIF de datos y LIF de interconexión de clústeres. No es necesario si utiliza LIF de clúster para el caso de uso de organización en niveles local.

Cuando se especifica una política de servicio para una LIF, la política se usa para construir un rol predeterminado, una política de conmutación por error y una lista de protocolos de datos para la LIF.

Aunque se pueden configurar varios protocolos para las SVM y LIF, lo mejor es que S3 sea el único protocolo cuando ofrece datos de objetos.

Pasos

1. Cambie la configuración del privilegio a avanzado:

   ```
   set -privilege advanced
   ```

2. Crear una política de datos de servicio:

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   La `data-core` y.. `data-s3-server` Los servicios son los únicos necesarios para habilitar ONTAP S3, aunque se pueden incluir otros servicios según sea necesario.

Cree LIF de datos

Si creó una SVM nueva, las LIF dedicadas que crea para el acceso S3 deberían ser LIF de datos.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador `up` estado.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

  Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante la `network subnet create` comando.

- Debe haber la política de servicio de LIF.

Acerca de esta tarea

- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster mediante el `network interface capacity show` Comando y la capacidad de LIF admitida en cada nodo mediante el `network interface capacity details show` (en el nivel de privilegio avanzado).
- Si va a habilitar la organización en niveles de capacidad de FabricPool remota (cloud), también debe configurar las LIF de interconexión de clústeres.

Pasos

1. Cree una LIF:

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   service_policy_names -home-node node_name -home-port port_name {-address
   IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
   data -auto-revert {true|false}
   ```

   - `-home-node` Es el nodo al que devuelve el LIF cuando el `network interface revert` El comando se ejecuta en la LIF.

     También puede especificar si el LIF debería volver automáticamente al nodo raíz y al puerto raíz con el `-auto-revert` opción.

   - `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando el `network interface revert` El comando se ejecuta en la LIF.
   - Puede especificar una dirección IP con el `-address` y.. `-netmask` o puede habilitar la asignación desde una subred con `-subnet_name` opción.

- Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.
- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. La `network route create` La página man contiene información sobre la creación de una ruta estática dentro de una SVM.
- Para la `-firewall-policy` opción, utilice el mismo valor predeterminado `data` Como el rol de LIF.

  Si lo desea, puede crear y agregar una política de firewall personalizada más adelante.

  > A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

- `-auto-revert` Permite especificar si un LIF de datos se revierte automáticamente a su nodo principal en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o el momento en que se realiza la conexión de red. El valor predeterminado es `false`, pero puede establecerlo en `false` según las políticas de administración de red del entorno.
- La `-service-policy` opción especifica la política de servicios de administración y datos que ha creado y cualquier otra política que necesite.

2. Si desea asignar una dirección IPv6 en el `-address` opción:

   a. Utilice la `network ndp prefix show` Comando para ver la lista de prefijos RA aprendidos en varias interfaces.

      La `network ndp prefix show` el comando está disponible en el nivel de privilegio avanzado.

   b. Utilice el formato `prefix:id` Para construir la dirección IPv6 manualmente.

      `prefix` es el prefijo aprendido en varias interfaces.

   Para obtener la `id`, elija un número hexadecimal aleatorio de 64 bits.

3. Compruebe que la LIF se ha creado correctamente mediante el `network interface show` comando.
4. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	`network ping`
Dirección IPv6	`network ping6`

Ejemplos

El siguiente comando muestra cómo crear una LIF de datos de S3 asignada con el `my-S3-policy` política de servicio:

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

El siguiente comando muestra todas las LIF del clúster-1. Data LIF datalif1 y datalif3 están configurados con direcciones IPv4, y datalif4 está configurado con una dirección IPv6:

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Cree LIF de interconexión de clústeres para la organización en niveles de FabricPool remota

Si va a habilitar la organización en niveles de la capacidad remota de FabricPool (cloud) mediante ONTAP S3, debe configurar las LIF entre clústeres. Las LIF de interconexión

de clústeres se pueden configurar en los puertos compartidos con la red de datos. De este modo, se reduce el número de puertos necesarios para interconectar redes.

Antes de empezar

- El puerto de red físico o lógico subyacente debe haber sido configurado para el administrador `up` estado.
- Debe haber la política de servicio de LIF.

Acerca de esta tarea

Las LIF de interconexión de clústeres no son necesarias para la organización en niveles de los pools de estructura local ni para servir aplicaciones S3 externas.

Pasos

1. Enumere los puertos del clúster:

   ```
   network port show
   ```

   En el siguiente ejemplo se muestran los puertos de red en `cluster01`:

   ```
   cluster01::> network port show
                                                                     Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

2. Crear LIF de interconexión de clústeres en la SVM del sistema:

   ```
   network interface create -vserver Cluster -lif LIF_name -service-policy
   default-intercluster -home-node node -home-port port -address port_IP -netmask
   netmask
   ```

   En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Compruebe que se han creado las LIF de interconexión de clústeres:

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Compruebe que las LIF de interconexión de clústeres son redundantes:

   `network interface show –service-policy default-intercluster -failover`

   El siguiente ejemplo muestra las LIF de interconexión de clústeres `cluster01_icl01` y.. `cluster01_icl02` en la `e0c` el puerto se conmuta al nodo de respaldo `e0d` puerto.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Cree el servidor de almacenamiento de objetos S3

El servidor de almacenamiento de objetos ONTAP gestiona los datos como objetos S3, a diferencia del almacenamiento de archivos o bloques que proporcionan los servidores NAS y SAN de ONTAP.

Antes de empezar

Debe estar preparado para introducir el nombre del servidor S3 como un nombre de dominio completo (FQDN), que los clientes usarán para el acceso S3. El FQDN no debe comenzar por un nombre de bloque.

Debe tener un certificado de CA autofirmado (creado en pasos anteriores) o un certificado firmado por un proveedor de CA externo. Un certificado de CA no es necesario para un caso de uso de organización en niveles local, donde el tráfico de IP pasa únicamente por las LIF del clúster.

Acerca de esta tarea

Cuando se crea un servidor de almacenamiento de objetos, se crea un usuario raíz con UID 0. No se genera ninguna clave de acceso ni clave secreta para este usuario raíz. El administrador de ONTAP debe ejecutar el `object-store-server users regenerate-keys` comando para establecer la clave de acceso y la clave secreta de este usuario.

> Como práctica recomendada por NetApp, no utilice este usuario raíz. Cualquier aplicación cliente que utilice la clave de acceso o la clave secreta del usuario raíz tiene acceso completo a todos los bloques y objetos del almacén de objetos.

Consulte `vserver object-store-server` páginas de manual para opciones de visualización y configuración adicionales.

Ejemplo 2. Pasos

System Manager

Utilice este procedimiento si va a añadir un servidor S3 a una máquina virtual de almacenamiento existente. Para añadir un servidor de S3 a una máquina virtual de almacenamiento nueva, consulte "Cree una SVM de almacenamiento para S3".

Debe estar preparado para introducir direcciones IP para los datos de roles de interfaz.

1. Habilitar S3 en una máquina virtual de almacenamiento existente.
   a. Seleccione la VM de almacenamiento: Haga clic en **almacenamiento > Storage VMs**, seleccione una VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ⚙ En **S3**.
   b. Haga clic en **Activar S3** y, a continuación, introduzca el nombre del servidor S3.
   c. Seleccione el tipo de certificado.

      Tanto si selecciona un certificado generado por el sistema como uno propio, será necesario para el acceso de los clientes.

   d. Introduzca las interfaces de red.
2. Si seleccionó el certificado generado por el sistema, la información del certificado se muestra cuando se confirma la creación de la máquina virtual de almacenamiento nueva. Haga clic en **Descargar** y guárdelo para acceder a los clientes.
   - La clave secreta no se volverá a mostrar.
   - Si necesita de nuevo la información del certificado: Haga clic en **almacenamiento > Storage VMs**, seleccione la VM de almacenamiento y haga clic en **Configuración**.

CLI

1. Cree el servidor S3:

   `vserver object-store-server create -vserver` *`svm_name`* `-object-store-server` *`s3_server_fqdn`* `-certificate-name` *`server_certificate_name`* `-comment` *`text`* `[additional_options]`

   Puede especificar opciones adicionales al crear el servidor S3 o en cualquier momento posterior.

   - Si va a configurar la organización en niveles local, el nombre de la SVM puede ser una SVM de datos o un nombre de System SVM (clúster).
   - El nombre del certificado debe ser el nombre del certificado de servidor (certificado de usuario final o de hoja), no el certificado de CA de servidor (certificado de CA intermedio o raíz).
   - De forma predeterminada, HTTPS está habilitado en el puerto 443. Puede cambiar el número de puerto con el `-secure-listener-port` opción.

     Cuando HTTPS está activado, se necesitan certificados de CA para una correcta integración con SSL/TLS.

   - HTTP está desactivado de forma predeterminada. Cuando está activado, el servidor recibe en el puerto 80. Puede habilitarla mediante el `-is-http-enabled` o cambie el número de puerto con `-listener-port` opción.

Cuando HTTP está activado, la solicitud y las respuestas se envían a través de la red en texto sin cifrar.

2. Compruebe que S3 está configurado:

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

Ejemplo

Este comando verifica los valores de configuración de todos los servidores de almacenamiento de objetos:

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Añadir capacidad de almacenamiento a una SVM habilitada para S3

Crear un bucket

Los objetos S3 se guardan en *buckets*. No se anidan como archivos dentro de un directorio dentro de otros directorios.

Antes de empezar

Debe existir una máquina virtual de almacenamiento que contenga un servidor S3.

Acerca de esta tarea

- A partir de ONTAP 9.14.1, se habilitó el ajuste de tamaño automático en los volúmenes FlexGroup de S3 TB cuando se crean buckets en ellos. De este modo se elimina la asignación de capacidad excesiva durante la creación de bloques en volúmenes de FlexGroup nuevos y existentes. El tamaño de los volúmenes FlexGroup se cambia a un tamaño mínimo requerido según las siguientes directrices. El tamaño mínimo requerido es el tamaño total de todos los bloques de S3 KB de un volumen FlexGroup.
  - A partir de ONTAP 9.14.1, si se crea un volumen de S3 FlexGroup como parte de la creación de un bloque nuevo, el volumen de FlexGroup se creará con el tamaño mínimo requerido.
  - Si se creó un volumen FlexGroup de S3 GB antes de ONTAP 9.14.1, el primer bloque creado o eliminado posteriormente a ONTAP 9.14.1 cambia el tamaño del volumen FlexGroup al tamaño mínimo requerido.
  - Si se creó un volumen FlexGroup de S3 GB anterior a ONTAP 9.14.1 y ya tenía el tamaño mínimo requerido, la creación o eliminación de un bloque posterior a ONTAP 9.14.1 mantendrán el tamaño del

volumen de S3 FlexGroup.

- Los niveles de servicio de almacenamiento son grupos de políticas de calidad de servicio (QoS) adaptativos predefinidos, con niveles *Value*, *Performance* y *Extreme* predeterminados. En lugar de uno de los niveles de servicio de almacenamiento predeterminados, también puede definir un grupo de políticas de calidad de servicio personalizado y aplicarlo a un bloque. Para obtener más información sobre las definiciones de servicios de almacenamiento, consulte "Definiciones de servicios de almacenamiento". Para obtener más información sobre la gestión del rendimiento, consulte "Gestión del rendimiento".
  A partir de ONTAP 9.8, cuando se aprovisiona el almacenamiento, la calidad de servicio se habilita de forma predeterminada. Puede deshabilitar la calidad de servicio o seleccionar una política de calidad de servicio personalizada durante el proceso de aprovisionamiento o más adelante.
- Si va a configurar la organización en niveles de capacidad local, debe crear bloques y usuarios en una máquina virtual de almacenamiento de datos, no en la máquina virtual de almacenamiento del sistema donde está ubicado el servidor S3.
- Para el acceso de cliente remoto, debe configurar buckets en una máquina virtual de almacenamiento habilitada para S3. Si crea un bloque en una máquina virtual de almacenamiento que no tiene la función S3, solo estará disponible para la organización en niveles local.
- A partir de ONTAP 9.14.1, puede hacerlo "Cree un bucket en un agregado reflejado o no reflejado en una configuración de MetroCluster".
- Para la CLI, cuando crea un bloque, tiene dos opciones de aprovisionamiento:
  - Dejar a ONTAP Select los agregados subyacentes y los componentes de FlexGroup (predeterminado)
    - ONTAP crea y configura un volumen de FlexGroup para el primer bloque seleccionando automáticamente los agregados. Seleccionará automáticamente el nivel de servicio más alto disponible para su plataforma, o bien se puede especificar el nivel de servicio de almacenamiento. Todos los bloques adicionales que añada más adelante a la máquina virtual de almacenamiento tendrán el mismo volumen de FlexGroup subyacente.
    - También puede especificar si el bloque se utilizará para la organización en niveles, en cuyo caso ONTAP intentará seleccionar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles.
  - Seleccione los agregados subyacentes y los componentes de FlexGroup (requiere opciones de comandos de privilegios avanzados): Tiene la opción de seleccionar manualmente los agregados donde se debe crear el bloque y el volumen de FlexGroup, y luego especificar la cantidad de componentes en cada agregado. Al añadir cubos adicionales:
    - Si especifica agregados y componentes para un bloque nuevo, se creará una FlexGroup nueva para el bloque nuevo.
    - Si no se especifican agregados y componentes para un bloque nuevo, el nuevo bloque se añadirá a una FlexGroup existente.
      Consulte Gestión de volúmenes de FlexGroup si quiere más información.

      Cuando se especifican agregados y componentes al crear un bloque, no se aplican grupos de políticas de calidad de servicio, predeterminados ni personalizados. Puede hacerlo más tarde con el `vserver object-store-server bucket modify` comando.

  Consulte "modificación de bucket object-store-server de vserver" si quiere más información.

Nota: Si está sirviendo cubos de Cloud Volumes ONTAP, debe utilizar el procedimiento CLI. Se recomienda seleccionar manualmente los agregados subyacentes para garantizar que solo utilicen un nodo. El uso de agregados de ambos nodos puede afectar al rendimiento, ya que los nodos se encuentran en zonas de disponibilidad separadas geográficamente y, por lo tanto, pueden estar expuestos a problemas de latencia.

Crear bloques S3 con la interfaz de línea de comandos de ONTAP

1. Si piensa seleccionar agregados y componentes de FlexGroup por su cuenta, establezca el nivel de privilegio en Advanced (de lo contrario, el nivel de privilegio de administrador es suficiente): `set -privilege advanced`
2. Crear un bloque:

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

   El nombre de la máquina virtual de almacenamiento puede ser una máquina virtual de almacenamiento de datos o `Cluster` (El nombre de VM de almacenamiento del sistema) si se va a configurar la organización en niveles local.

   Si no especifica ninguna opción, ONTAP crea un bucket de 800GB con el nivel de servicio definido en el nivel más alto disponible para su sistema.

   Si desea que ONTAP cree un bloque según el rendimiento o el uso, utilice una de las siguientes opciones:

   - nivel de servicio

     Incluya el `-storage-service-level` opción con uno de los siguientes valores: `value`, `performance`, o. `extreme`.

   - Organización en niveles

     Incluya el `-used-as-capacity-tier true` opción.

     Si desea especificar los agregados en los que se creará el volumen de FlexGroup subyacente, utilice las siguientes opciones:

   - La `-aggr-list` El parámetro especifica la lista de agregados que se usarán para los componentes de volumen de FlexGroup.

     Cada entrada de la lista crea un componente en el agregado especificado. Puede especificar un agregado varias veces para que se creen varios componentes en el agregado.

   Para obtener un rendimiento coherente en todo el volumen FlexGroup, todos los agregados deben usar las mismas configuraciones de tipo de disco y grupo RAID.

   - La `-aggr-list-multiplier` parámetro especifica la cantidad de veces que se debe iterar sobre los agregados que se enumeran con el `-aggr-list` Parámetro cuando se crea un volumen de FlexGroup.

     El valor predeterminado de `-aggr-list-multiplier` el parámetro es 4.

3. Añada un grupo de políticas QoS si es necesario:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. Verificar creación de bloques:

```
vserver object-store-server bucket show [-instance]
```

Ejemplo

El siguiente ejemplo crea un bloque para la máquina virtual de almacenamiento `vs1` de tamaño `1TB` y especificando el agregado:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Crear bloques S3 con System Manager

1. Añadir un nuevo bloque en una máquina virtual de almacenamiento habilitada para S3.
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.
      - Si hace clic en **Guardar** en este punto, se crea un bloque con estos valores predeterminados:
        - No se concede acceso a ningún usuario al bloque a menos que ninguna política de grupo esté ya en vigor.

          No se debe usar el usuario raíz de S3 para gestionar el almacenamiento de objetos ONTAP y compartir sus permisos, ya que tiene acceso ilimitado al almacén de objetos. En su lugar, cree un usuario o grupo con privilegios administrativos que asigne.

        - Un nivel de calidad de servicio (rendimiento) que es el más alto disponible para su sistema.
      - Haga clic en **Guardar** para crear un bucket con estos valores predeterminados.

Configurar permisos y restricciones adicionales

Puede hacer clic en **Más opciones** para configurar la configuración de bloqueo de objetos, permisos de usuario y nivel de rendimiento cuando configure el depósito, o puede modificar estos ajustes más adelante.

Si tiene la intención de utilizar el almacén de objetos S3 para la organización en niveles de FabricPool, considere la posibilidad de seleccionar **utilizar para la organización en niveles** (utilizar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles) en lugar de un nivel de servicio de rendimiento.

Si desea habilitar el control de versiones de sus objetos para su posterior recuperación, seleccione **Activar control de versiones**. El control de versiones está activado de forma predeterminada si está activando el bloqueo de objetos en el depósito. Para obtener más información sobre el control de versiones de objetos, consulte "Uso del control de versiones en bloques de S3 para Amazon".

A partir de 9.14.1, el bloqueo de objetos es compatible con bloques de S3. El bloqueo de objetos de S3 GB requiere una licencia estándar de SnapLock. Esta licencia se incluye con "ONTAP One".
Antes de ONTAP One, la licencia de SnapLock se incluía en el paquete de seguridad y cumplimiento de normativas. El paquete de seguridad y cumplimiento ya no se ofrece, pero sigue siendo válido. Aunque actualmente no es obligatorio, los clientes existentes pueden optar por hacerlo "Actualice a ONTAP One".
Si está activando el bloqueo de objetos en un depósito, debe hacerlo "Compruebe que hay instalada una licencia de SnapLock". Si no hay una licencia de SnapLock instalada, debe "instale" antes de poder activar el bloqueo de objetos.

Cuando haya verificado que la licencia de SnapLock está instalada, para evitar que los objetos de su depósito se borren o sobrescriban, seleccione **Habilitar bloqueo de objetos**. El bloqueo se puede habilitar en todas las versiones de objetos o en algunas específicas, y solo cuando se inicializa el reloj de cumplimiento de normativas de SnapLock para los nodos del clúster. Siga estos pasos:

1. Si el reloj de cumplimiento de SnapLock no se inicializa en ningún nodo del clúster, aparece el botón **Inicializar reloj de cumplimiento de SnapLock**. Haga clic en **Inicializar reloj de cumplimiento de SnapLock** para inicializar el reloj de cumplimiento de SnapLock en los nodos del clúster.
2. Seleccione el modo **Gobernanza** para activar un bloqueo basado en el tiempo que permite los permisos *Escribir una vez, leer muchos (WORM)* en los objetos. Incluso en el modo *Governance*, los objetos pueden ser eliminados por los usuarios administradores con permisos específicos.
3. Seleccione el modo **Compliance** si desea asignar reglas más estrictas de eliminación y actualización en los objetos. En este modo de bloqueo de objetos, los objetos solo pueden caducarse al finalizar el período de retención especificado. A menos que se especifique un período de retención, los objetos permanecen bloqueados indefinidamente.
4. Especifique la tenencia de retención del bloqueo en días o años si desea que el bloqueo se aplique durante un período determinado.

> El bloqueo se aplica a los cucharones S3 con versiones y sin versiones. El bloqueo de objetos no se aplica a los objetos NAS.

Puede configurar los ajustes de protección y permisos, así como el nivel de servicio de rendimiento del bloque.

> Debe haber creado usuarios y grupos antes de configurar los permisos.

Para obtener más información, consulte "Crear reflejo para nuevo bloque".

Verifique el acceso al cucharón

En aplicaciones cliente S3 (ya sea ONTAP S3 o una aplicación externa de terceros), puede verificar el acceso al depósito recién creado introduciendo lo siguiente:

- El certificado de CA de servidor S3.
- La clave de acceso y la clave secreta del usuario.
- El nombre FQDN del servidor S3 y el nombre de bloque.

Cree un bucket en un agregado reflejado o no reflejado en una configuración de MetroCluster

A partir de ONTAP 9.14.1, puede aprovisionar un bloque en un agregado reflejado o no reflejado en las configuraciones de IP y FC de MetroCluster.

Acerca de esta tarea

- De forma predeterminada, los buckets se aprovisionan en agregados reflejados.
- Las mismas directrices de provisión descritas en la "Crear un bucket" Aplique para crear un bloque en un entorno MetroCluster.
- Las siguientes funciones de almacenamiento de objetos S3 no son compatibles con entornos MetroCluster:
  - SnapMirror S3

- Gestión del ciclo de vida de los bloques de S3
- Bloqueo de objetos S3 en el modo **Compliance**

  Se admite el bloqueo de objetos S3 en el modo **Gobernanza**.

- Organización en niveles de FabricPool local

Antes de empezar

Debe haber una SVM que contenga un servidor S3.

Proceso para crear cubos

CLI

1. Si piensa seleccionar agregados y componentes de FlexGroup por su cuenta, establezca el nivel de privilegio en Advanced (de lo contrario, el nivel de privilegio de administrador es suficiente): `set -privilege advanced`
2. Crear un bloque:

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates
   true/false]
   ```

   Ajuste la `-use-mirrored-aggregates` opción a. `true` o. `false` según si desea usar un agregado reflejado o no reflejado.

   > De forma predeterminada, la `-use-mirrored-aggregates` opción establecida en `true`.

   - El nombre de la SVM debe ser una SVM de datos.
   - Si no especifica ninguna opción, ONTAP crea un bucket de 800GB con el nivel de servicio definido en el nivel más alto disponible para su sistema.
   - Si desea que ONTAP cree un bloque según el rendimiento o el uso, utilice una de las siguientes opciones:
     - nivel de servicio

       Incluya el `-storage-service-level` opción con uno de los siguientes valores: `value`, `performance`, o. `extreme`.

     - Organización en niveles

       Incluya el `-used-as-capacity-tier true` opción.
   - Si desea especificar los agregados en los que se creará el volumen de FlexGroup subyacente, utilice las siguientes opciones:
     - La `-aggr-list` El parámetro especifica la lista de agregados que se usarán para los componentes de volumen de FlexGroup.

       Cada entrada de la lista crea un componente en el agregado especificado. Puede especificar un agregado varias veces para que se creen varios componentes en el agregado.

   Para obtener un rendimiento coherente en todo el volumen FlexGroup, todos los agregados deben usar las mismas configuraciones de tipo de disco y grupo RAID.

   - La `-aggr-list-multiplier` parámetro especifica la cantidad de veces que se debe iterar sobre los agregados que se enumeran con el `-aggr-list` Parámetro cuando se crea un volumen de FlexGroup.

     El valor predeterminado de `-aggr-list-multiplier` el parámetro es 4.

3. Añada un grupo de políticas QoS si es necesario:

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   ```

```
-group qos_policy_group
```

4. Verificar creación de bloques:

```
vserver object-store-server bucket show [-instance]
```

Ejemplo

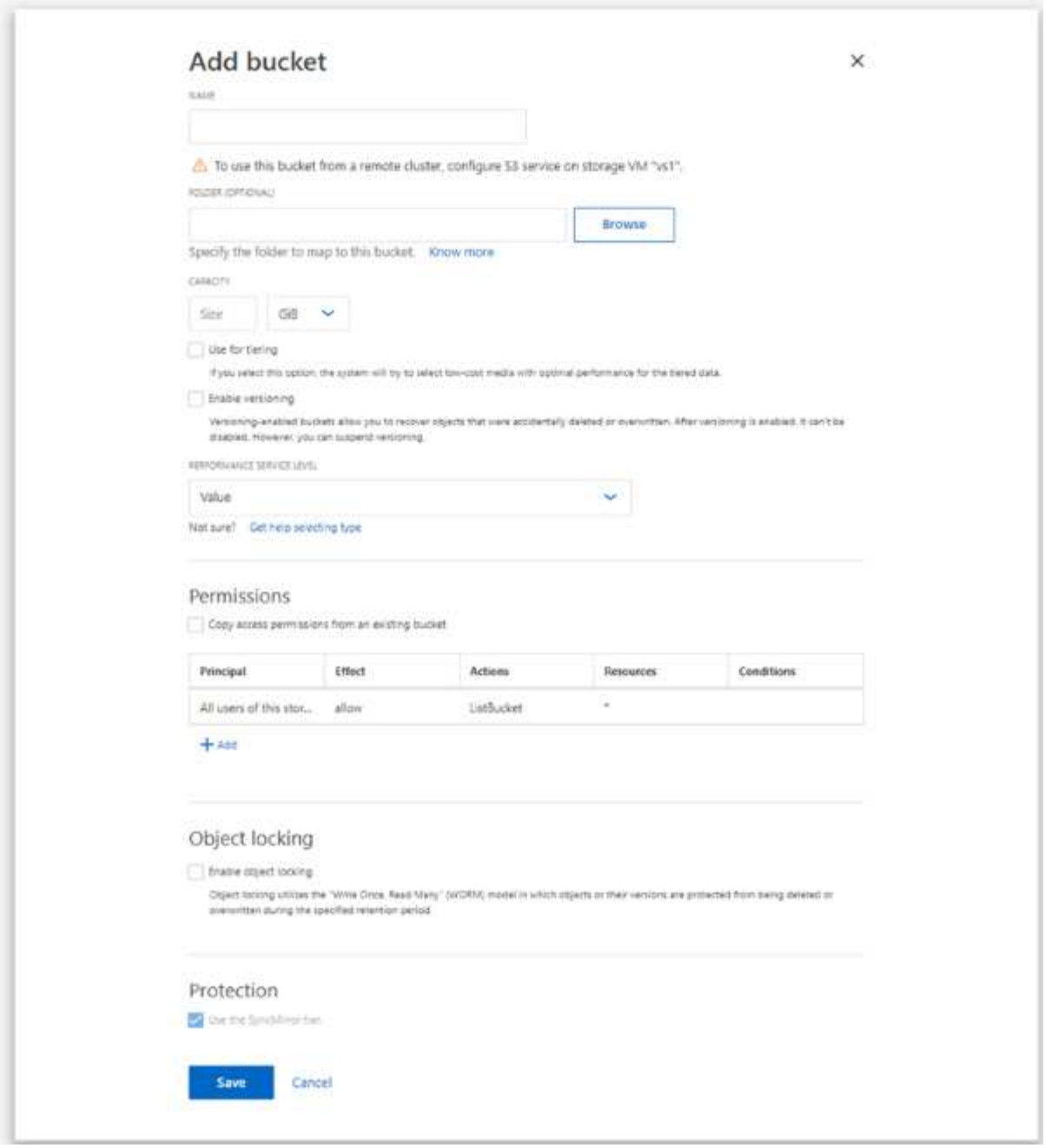
En el ejemplo siguiente se crea un bloque para SVM VS1 de tamaño 1TB en un agregado reflejado:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Añadir un nuevo bloque en una máquina virtual de almacenamiento habilitada para S3.
   a. Haga clic en **almacenamiento > Cuchos** y, a continuación, haga clic en **Agregar**.
   b. Introduzca un nombre, seleccione la máquina virtual de almacenamiento e introduzca un tamaño.

      De forma predeterminada, el bloque se aprovisiona en un agregado reflejado. Si quieres crear un bucket en un agregado no reflejado, selecciona **Más opciones** y desmarca la casilla **Usar el nivel SyncMirror** bajo **Protección** como se muestra en la siguiente imagen:



- Si hace clic en **Guardar** en este punto, se crea un bloque con estos valores predeterminados:
  - No se concede acceso a ningún usuario al bloque a menos que ninguna política de grupo esté ya en vigor.

    > No se debe usar el usuario raíz de S3 para gestionar el almacenamiento de objetos ONTAP y compartir sus permisos, ya que tiene acceso ilimitado al almacén de objetos. En su lugar, cree un usuario o grupo con privilegios administrativos que asigne.

  - Un nivel de calidad de servicio (rendimiento) que es el más alto disponible para su sistema.
- Puede hacer clic en **más opciones** para configurar los permisos de usuario y el nivel de rendimiento al configurar el bloque, o puede modificar esta configuración más tarde.

- Debe haber creado usuarios y grupos antes de utilizar **más opciones** para configurar sus permisos.
- Si tiene la intención de utilizar el almacén de objetos S3 para la organización en niveles de FabricPool, considere la posibilidad de seleccionar **utilizar para la organización en niveles** (utilizar medios de bajo coste con un rendimiento óptimo para los datos organizados en niveles) en lugar de un nivel de servicio de rendimiento.

2. En aplicaciones de cliente S3, otro sistema ONTAP o una aplicación de terceros externa, verifique el acceso al nuevo bloque introduciendo lo siguiente:
   - El certificado de CA de servidor S3.
   - Clave secreta y clave de acceso del usuario.
   - El nombre FQDN del servidor S3 y el nombre de bloque.

Cree una regla de gestión del ciclo de vida del bloque

A partir de ONTAP 9.13.1, puede crear reglas de gestión del ciclo de vida para gestionar los ciclos de vida de los objetos en sus bloques S3. Puede definir reglas de supresión para objetos específicos de un depósito y, a través de estas reglas, caducar esos objetos de cubo. De este modo, se cumplen los requisitos de retención y se gestiona un almacenamiento de objetos S3 general de forma eficiente.

> Si el bloqueo de objetos está activado para los objetos de depósito, las reglas de gestión del ciclo de vida para la caducidad de objetos no se aplicarán a los objetos bloqueados. Para obtener más información sobre el bloqueo de objetos, consulte "Crear un bucket".

Antes de empezar

Debe haber una SVM habilitada para S3 que contenga un servidor S3 y un bloque. Consulte "Cree una SVM para S3" si quiere más información.

Acerca de esta tarea

Al crear las reglas de gestión del ciclo de vida, puede aplicar las siguientes acciones de eliminación a los objetos del depósito:

- Supresión de versiones actuales: Esta acción vence los objetos identificados por la regla. Si el control de versiones está activado en el depósito, S3 hace que todos los objetos caducados no estén disponibles. Si el control de versiones no está activado, esta regla suprime los objetos de forma permanente. La acción de la CLI es `Expiration`.
- Eliminación de versiones no actuales: Esta acción especifica cuándo S3 puede eliminar permanentemente objetos no actuales. La acción de la CLI es `NoncurrentVersionExpiration`.
- Supresión de marcadores de supresión caducados: Esta acción suprime los marcadores de supresión de objetos caducados.
  En los bloques con control de versiones activado, los objetos con marcadores de supresión se convierten en las versiones actuales de los objetos. Los objetos no se eliminan y no se puede realizar ninguna acción en ellos. Estos objetos caducan cuando no hay versiones actuales asociadas a ellos. La acción de la CLI es `Expiration`.
- Eliminación de cargas multiparte incompletas: Esta acción establece un tiempo máximo (en días) en el que desea permitir que las cargas multiparte permanezcan en curso. Después de lo cual, se eliminan. La acción de la CLI es `AbortIncompleteMultipartUpload`.

El procedimiento que siga depende de la interfaz que utilice. Con ONTAP 9.13,1, tiene que utilizar la CLI. A partir de ONTAP 9.14.1, también puede usar System Manager.

Gestione las reglas de gestión del ciclo de vida con la interfaz de línea de comandos

A partir de ONTAP 9.13.1, puede usar la interfaz de línea de comandos de ONTAP para crear reglas de gestión del ciclo de vida para caducar objetos en sus bloques S3.

Antes de empezar

Para la CLI, debe definir los campos necesarios para cada tipo de acción de caducidad al crear una regla de gestión del ciclo de vida del bloque. Estos campos se pueden modificar después de la creación inicial. En la siguiente tabla se muestran los campos únicos para cada tipo de acción.

Tipo de acción	Campos únicos
Caducidad sin CurrentVersionespiración	• `-non-curr-days` - Número de días después de los cuales se eliminarán las versiones no actuales • `-new-non-curr-versions` - Número de últimas versiones no actuales que se conservarán
Caducidad	• `-obj-age-days` - Número de días desde la creación, después de lo cual se puede eliminar la versión actual de los objetos • `-obj-exp-date` - Fecha específica en la que los objetos deben expirar • `-expired-obj-del-markers` - Limpiar objetos borrar marcadores
AbortEncompleteMultipartUpload	• `-after-initiation-days` - Número de días de iniciación, después de los cuales la carga puede ser abortada

Para que la regla de gestión del ciclo de vida del depósito se aplique sólo a un subconjunto específico de objetos, los administradores deben establecer cada filtro al crear la regla. Si estos filtros no se establecen al crear la regla, la regla se aplicará a todos los objetos del depósito.

Todos los filtros se pueden modificar después de la creación inicial *Excepto* para lo siguiente: +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Pasos

1. Utilice la `vserver object-store-server bucket lifecycle-management-rule create` comando con los campos necesarios para el tipo de acción de vencimiento para crear la regla de gestión del ciclo de vida del bloque.

Ejemplo

El siguiente comando crea una regla de gestión del ciclo de vida del bloque NonCurrentVersionExpiration:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Ejemplo

El siguiente comando crea una regla de gestión del ciclo de vida del depósito de vencimiento:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Ejemplo

El siguiente comando crea una regla de gestión del ciclo de vida del bloque AbortIncompleteMultipartUpload:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gestione las reglas de gestión del ciclo de vida con System Manager

A partir de ONTAP 9.14.1, puede caducar objetos de S3 mediante System Manager. Puede agregar, editar y eliminar reglas de gestión del ciclo de vida para los objetos S3. Además, puede importar una regla de ciclo de vida creada para un depósito y utilizarla para los objetos de otro depósito. Puede desactivar una regla activa y habilitarla más tarde.

Agregue una regla de gestión del ciclo de vida

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el período para el que desea especificar la regla de caducidad.
3. Haga clic en la ⋮ Icono y seleccione **Administrar reglas de ciclo de vida**.
4. Haga clic en **Agregar > Regla de ciclo de vida**.
5. En la página Agregar una regla de ciclo de vida, agregue el nombre de la regla.

6. Defina el ámbito de la regla, si desea que se aplique a todos los objetos del depósito o a objetos específicos. Si desea especificar objetos, agregue al menos uno de los siguientes criterios de filtro:
   a. Prefijo: Especifique un prefijo de los nombres de clave de objeto a los que se debe aplicar la regla. Normalmente, es la ruta o carpeta del objeto. Puede introducir un prefijo por regla. A menos que se proporcione un prefijo válido, la regla se aplica a todos los objetos de un depósito.
   b. Etiquetas: Especifique hasta tres pares de clave y valor (etiquetas) para los objetos a los que se debe aplicar la regla. Sólo se utilizan claves válidas para el filtrado. El valor es opcional. Sin embargo, si agrega valores, asegúrese de agregar sólo valores válidos para las claves correspondientes.
   c. Tamaño: Puede limitar el alcance entre los tamaños mínimo y máximo de los objetos. Puede introducir uno o ambos valores. La unidad predeterminada es MIB.
7. Especifique la acción:
   a. **Expire la versión actual de los objetos**: Establezca una regla para que todos los objetos actuales no estén disponibles permanentemente después de un número específico de días desde su creación, o en una fecha específica. Esta opción no está disponible si se selecciona la opción **Eliminar marcadores de eliminación de objetos caducados**.
   b. * Eliminar permanentemente versiones no actuales*: Especifique el número de días después de los cuales la versión se convierte en no actual, y después puede ser eliminado, y el número de versiones a retener.
   c. **Eliminar marcadores de eliminación de objetos caducados**: Seleccione esta acción para eliminar objetos con marcadores de eliminación caducados, es decir, eliminar marcadores sin un objeto actual asociado.

      Esta opción no está disponible cuando selecciona la opción **Expire la versión actual de los objetos** que elimina automáticamente todos los objetos después del período de retención. Esta opción también no está disponible cuando se utilizan etiquetas de objetos para filtrar.

   d. **Eliminar cargas multiparte incompletas**: Establece el número de días después de los cuales las cargas multiparte incompletas deben ser eliminadas. Si las cargas de varias partes que están en curso fallan dentro del período de retención especificado, puede eliminar las cargas incompletas de varias partes. Esta opción no está disponible cuando se utilizan etiquetas de objetos para filtrar.
   e. Haga clic en **Guardar**.

Importar una regla de ciclo de vida

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el período para el que desea importar la regla de caducidad.
3. Haga clic en la ⋮ Icono y seleccione **Administrar reglas de ciclo de vida**.
4. Haga clic en **Agregar > Importar una regla**.
5. Seleccione el depósito desde el que desea importar la regla. Aparecen las reglas de gestión del ciclo de vida definidas para el bloque seleccionado.
6. Seleccione la regla que desea importar. Tiene la opción de seleccionar una regla a la vez, siendo la selección predeterminada la primera regla.
7. Haga clic en **Importar**.

Editar, eliminar o desactivar una regla

Sólo puede editar las acciones de gestión del ciclo de vida asociadas a la regla. Si la regla se filtró con etiquetas de objeto, las opciones **Eliminar marcadores de eliminación de objetos caducados** y **Eliminar cargas incompletas de varias partes** no estarán disponibles.

Al eliminar una regla, dicha regla ya no se aplicará a los objetos asociados anteriormente.

1. Haga clic en **Almacenamiento > Buckets**.
2. Seleccione el depósito para el que desea editar, suprimir o desactivar la regla de gestión del ciclo de vida.
3. Haga clic en la ⋮ Icono y seleccione **Administrar reglas de ciclo de vida**.
4. Seleccione la regla necesaria. Puede editar y desactivar una regla a la vez. Puede eliminar varias reglas a la vez.
5. Seleccione **Editar**, **Eliminar** o **Desactivar** y complete el procedimiento.

Cree un usuario de S3

Se requiere autorización de usuario en todos los almacenes de objetos de ONTAP para restringir la conectividad a los clientes autorizados.

Antes de empezar.

Debe existir una máquina virtual de almacenamiento habilitada para S3.

Acerca de esta tarea

Se puede otorgar acceso a cualquier bloque de una máquina virtual de almacenamiento a un usuario de S3. Cuando crea un usuario S3, también se generan una clave de acceso y una clave secreta para el usuario. Se deben compartir con el usuario junto con el FQDN del almacén de objetos y el nombre del bloque. Se pueden ver las teclas de un usuario de S3 con el `vserver object-store-server user show` comando.

Puede conceder permisos de acceso específicos a usuarios de S3 en una política de bloque o una política de servidor de objetos.

> Al crear un nuevo servidor de almacén de objetos, ONTAP crea un usuario raíz (UID 0), que es un usuario con privilegios con acceso a todos los depósitos. En lugar de administrar ONTAP S3 como usuario raíz, NetApp recomienda crear un rol de usuario administrador con privilegios específicos.

CLI

1. Cree un usuario de S3:
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - Agregar un comentario es opcional.
   - A partir de ONTAP 9.14.1, puede definir el período de tiempo durante el cual la clave será válida en el `-key-time-to-live` parámetro. Puede agregar el período de retención en este formato para indicar el período después del cual caduca la clave de acceso:
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     Por ejemplo, si desea introducir un período de retención de un día, dos horas, tres minutos y cuatro segundos, introduzca el valor como `P1DT2H3M4S`. A menos que se especifique, la clave es válida durante un período de tiempo indefinido.

     El siguiente ejemplo crea un usuario con su nombre `sm_user1` En equipos virtuales de almacenamiento `vs0`, con un período de retención clave de una semana.

```
vserver object-store-server user create -vserver vs0 -user sm_user1
-key-time-to-live P1W
```

2. Asegúrese de guardar la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

System Manager

1. Haga clic en **almacenamiento > Storage VMs**. Seleccione la VM de almacenamiento a la que necesita agregar un usuario, seleccione **Configuración** y luego haga clic en En S3.
2. Para agregar un usuario, haga clic en **Usuarios > Agregar**.
3. Introduzca un nombre para el usuario.
4. A partir de ONTAP 9.14.1, puede especificar el período de retención de las claves de acceso que se crean para el usuario. Puede especificar el período de retención en días, horas, minutos o segundos, después del cual las claves caducan automáticamente. De forma predeterminada, el valor se establece en `0` esto indica que la clave es válida indefinidamente.
5. Haga clic en **Guardar**. Se crea el usuario y se generan una clave de acceso y una clave secreta para el usuario.
6. Descargue o guarde la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

Siguientes pasos

- Cree o modifique grupos S3

Cree o modifique grupos S3

Puede simplificar el acceso a bloques mediante la creación de grupos de usuarios con las autorizaciones de acceso adecuadas.

Antes de empezar

Los usuarios S3 de una SVM habilitada para S3 ya deben existir.

Acerca de esta tarea

A los usuarios de un grupo de S3 se puede conceder acceso a cualquier bloque de una SVM, pero no a varias SVM. Los permisos de acceso a grupos se pueden configurar de dos formas:

- A nivel de cucharón

  Después de crear un grupo de usuarios S3, debe especificar permisos de grupo en las sentencias de política de bloque y sólo se aplican a ese bloque.

- A nivel de SVM

  Después de crear un grupo de usuarios S3, debe especificar nombres de políticas de servidor de objetos en la definición del grupo. Esas políticas determinan los bloques y el acceso de los miembros del grupo.

System Manager

1. Edite el equipo virtual de almacenamiento: Haga clic en **almacenamiento > equipos virtuales de almacenamiento**, haga clic en el equipo virtual de almacenamiento, seleccione **Configuración** y, a continuación, haga clic en En S3.
2. Agregar un grupo: Seleccione **grupos** y, a continuación, seleccione **Agregar**.
3. Introduzca un nombre de grupo y selecciónelo en una lista de usuarios.
4. Puede seleccionar una política de grupo existente o añadirla ahora, o bien agregar una política más adelante.

CLI

1. Cree un grupo de S3:
   `vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]`
   La `-policies` la opción se puede omitir en configuraciones con un solo bloque en un almacén de objetos; el nombre del grupo se puede agregar a la política de bloque.
   La `-policies` la opción se puede añadir más adelante con la `vserver object-store-server group modify` comando después de crear las políticas de servidor de almacenamiento de objetos.

Regenerar claves y modificar su período de retención

Las claves de acceso y las claves secretas se generan automáticamente durante la creación del usuario para habilitar el acceso de los clientes S3. Puede volver a generar claves para un usuario si una clave ha caducado o está en peligro.

Para obtener más información sobre la generación de claves de acceso, consulte "Cree un usuario de S3".

CLI

1. Vuelva a generar las claves secretas y de acceso para un usuario ejecutando el `vserver object-store-server user regenerate-keys` comando.
2. De forma predeterminada, las claves generadas son válidas indefinidamente. A partir de 9.14.1, puede modificar su período de retención, después del cual las claves caducan automáticamente. Puede agregar el período de retención en este formato:
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   Por ejemplo, si desea introducir un período de retención de un día, dos horas, tres minutos y cuatro segundos, introduzca el valor como `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. Guarde el acceso y las claves secretas. Serán necesarios para el acceso de S3 clientes.

System Manager

1. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
2. En la ficha **Configuración**, haga clic en ✎ En el mosaico **S3**.
3. En la pestaña **Usuarios**, verifique que no haya ninguna clave de acceso o que la clave haya caducado para el usuario.
4. Si necesita volver a generar la clave, haga clic en ⋮ Junto al usuario, luego haga clic en **Regenerar clave**.
5. De forma predeterminada, las claves generadas son válidas durante un período de tiempo indefinido. A partir de 9.14.1, puede modificar su período de retención, después del cual las claves caducan automáticamente. Introduzca el período de retención en días, horas, minutos o segundos.
6. Haga clic en **Guardar**. La clave se regenera. Cualquier cambio en el período de retención de clave se aplica inmediatamente.
7. Descargue o guarde la clave de acceso y la clave secreta. Serán necesarios para el acceso de S3 clientes.

Crear o modificar sentencias de directiva de acceso

Acerca de las políticas de servidor de almacenamiento de objetos y bloques

El acceso de usuario y grupo a recursos S3 está controlado por las políticas de servidores de almacén de objetos y bloques. Si tiene un pequeño número de usuarios o grupos, es probable que sea suficiente controlar el acceso a nivel de bloque, pero si tiene muchos usuarios y grupos, es más fácil controlar el acceso a nivel de servidor del almacén de objetos.

Modificar una política de bloques

Puede agregar reglas de acceso a la política de bloque predeterminada. El ámbito de su control de acceso es el cucharón que contiene, por lo que resulta más adecuado cuando

hay un único cucharón.

Antes de empezar

Debe existir una máquina virtual de almacenamiento habilitada para S3 que contenga un servidor S3 y un bloque.

Debe haber creado usuarios o grupos antes de conceder permisos.

Acerca de esta tarea

Puede agregar nuevas sentencias para usuarios y grupos nuevos o modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server bucket policy` páginas de manual.

Los permisos de usuario y grupo se pueden otorgar cuando se crea el bloque o cuando se necesite más adelante. También puede modificar la asignación de capacidad de los bloques y del grupo de políticas de calidad de servicio.

A partir de ONTAP 9,9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y. `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Pasos

1. Edite la cuchara: Haga clic en **almacenamiento > Cuchos**, haga clic en la cuchara deseada y, a continuación, haga clic en **Editar**.
   Al agregar o modificar permisos, puede especificar los siguientes parámetros:
   - **Principal**: El usuario o grupo al que se concede acceso.
   - **Efecto**: Permite o deniega el acceso a un usuario o grupo.
   - **Acciones**: Acciones permitidas en el cucharón para un usuario o grupo determinado.
   - **Recursos**: Rutas y nombres de objetos dentro del bloque para los cuales se concede o deniega el acceso.

     Los valores predeterminados ***bucketname*** y ***bucketname/**** conceden acceso a todos los objetos del bloque. También puede otorgar acceso a objetos individuales; por ejemplo, ***bucketname/*_readme.txt**.
   - **Condiciones** (opcional): Expresiones que se evalúan cuando se intenta acceder. Por ejemplo, puede especificar una lista de direcciones IP para las que se permitirá o deniega el acceso.

> A partir de ONTAP 9.14.1, puede especificar variables para la política de depósitos en el campo **Recursos**. Estas variables son marcadores de posición que se reemplazan por valores contextuales cuando se evalúa la política. Por ejemplo, If `${aws:username}` se especifica como una variable para una política, a continuación, esta variable se sustituye por el nombre de usuario del contexto de solicitud y la acción de política se puede realizar como se ha configurado para ese usuario.

CLI

Pasos

1. Agregar una sentencia a una política de bloque:

   ```
   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]
   ```

   Los siguientes parámetros definen los permisos de acceso:

`-effect`	La declaración puede permitir o denegar el acceso
`-action`	Puede especificar `*` para indicar todas las acciones, o una lista de una o varias de las siguientes: `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl,GetObjectAcl, ListBucketMultipartUploads,` y.. `ListMultipartUploadParts`.

`-principal`	Una lista de uno o más grupos o usuarios de S3. • Se puede especificar un máximo de 10 usuarios o grupos. • Si se especifica un grupo de S3, debe estar en el formulario `group/group_name`. • `*` se puede especificar que significa acceso público; es decir, acceso sin clave de acceso y clave secreta. • Si no se especifica ningún principal, se concede acceso a todos los usuarios S3 de la máquina virtual de almacenamiento.
`-resource`	El bloque y cualquier objeto que contenga. Los caracteres comodín `*` y.. `?` se puede utilizar para formar una expresión regular para especificar un recurso. En el caso de un recurso, puede especificar variables en una política. Estas son variables de política que son marcadores de posición que se reemplazan por los valores contextuales cuando se evalúa la política.

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

Ejemplos

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento svm1.example.com y bucket1 que especifica el acceso permitido a una carpeta Léame para el usuario de servidor de almacén de objetos user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

En el siguiente ejemplo se crea una sentencia de política de depósito de servidor de almacén de objetos para la máquina virtual de almacenamiento svm1.example.com y bucket1 que especifica el acceso permitido a todos los objetos para el grupo de servidores de almacén de objetos group1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

A partir de ONTAP 9.14.1, puede especificar variables para una política de bloque. En el siguiente ejemplo se crea una sentencia de política de bloque de servidor para la máquina virtual de almacenamiento `svm1` y.. `bucket1`, y especifica `${aws:username}` como variable para un recurso de política. Cuando se evalúa la política, la variable de política se sustituye por el nombre de usuario de contexto de solicitud y la acción de política se puede realizar según se haya configurado para ese usuario. Por ejemplo, cuando se evalúa la siguiente sentencia de política, `${aws:username}` Se sustituye por el usuario que realiza la operación S3. Si es un usuario `user1` realiza la operación a la que

el usuario tiene acceso `bucket1` como `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Cree o modifique una política de servidor de almacenes de objetos

Puede crear políticas que se puedan aplicar a uno o varios bloques de un almacén de objetos. Las políticas de servidores de almacenamiento de objetos pueden conectarse a grupos de usuarios, lo cual simplifica la gestión del acceso a los recursos en varios bloques.

Antes de empezar

Debe haber una SVM habilitada para S3 que contenga un servidor S3 y un bloque.

Acerca de esta tarea

Puede habilitar las políticas de acceso en el nivel de SVM especificando una política predeterminada o personalizada en un grupo de servidores de almacenamiento de objetos. Las directivas no surten efecto hasta que se especifiquen en la definición del grupo.

> Cuando se utilizan directivas de servidor de almacenamiento de objetos, se especifican los principales (es decir, los usuarios y los grupos) en la definición de grupo, no en la propia directiva.

Hay tres políticas predeterminadas de solo lectura para el acceso a los recursos de ONTAP S3:

- Acceso completo
- NoS3Access
- ReadOnlyAccess

También puede crear nuevas directivas personalizadas y, a continuación, agregar nuevas sentencias para nuevos usuarios y grupos, o puede modificar los atributos de las sentencias existentes. Para obtener más opciones, consulte `vserver object-store-server policy` "referencia de comandos".

A partir de ONTAP 9,9.1, si tiene previsto admitir la funcionalidad de etiquetado de objetos de cliente de AWS con el servidor ONTAP S3, las acciones se realizarán `GetObjectTagging`, `PutObjectTagging`, y. `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Edite el equipo virtual de almacenamiento: Haga clic en **almacenamiento > equipos virtuales de almacenamiento**, haga clic en el equipo virtual de almacenamiento, seleccione **Configuración** y, a continuación, haga clic en En S3.
2. Agregar un usuario: Haga clic en **Directivas** y, a continuación, haga clic en **Agregar**.
   a. Introduzca un nombre de política y selecciónelo de una lista de grupos.
   b. Seleccione una política predeterminada existente o agregue una nueva.

      Al agregar o modificar una política de grupo, se pueden especificar los siguientes parámetros:

      - Grupo: Los grupos a los que se concede acceso.
      - Efecto: Permite o deniega el acceso a uno o varios grupos.
      - Acciones: Acciones permitidas en uno o más cucharones para un grupo determinado.
      - Recursos: Rutas y nombres de objetos dentro de uno o más segmentos para los que se concede o deniega el acceso.
        Por ejemplo:
        - ***** Concede acceso a todos los bloques del equipo virtual de almacenamiento.
        - **bucketname** y **bucketname/*** conceden acceso a todos los objetos de un bloque específico.
        - **bucketname/readme.txt** otorga acceso a un objeto en un bloque específico.
   c. Si lo desea, agregue sentencias a las directivas existentes.

CLI

Utilice la CLI para crear o modificar una directiva de servidor de almacén de objetos

Pasos

1. Cree una política de servidor de almacenamiento de objetos:

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Crear una instrucción para la directiva:

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Los siguientes parámetros definen los permisos de acceso:

`-effect`	La declaración puede permitir o denegar el acceso

`-action`	Puede especificar `*` para indicar todas las acciones, o una lista de una o varias de las siguientes: `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, y.. `ListMultipartUploadParts`.
`-resource`	El bloque y cualquier objeto que contenga. Los caracteres comodín `*` y.. `?` se puede utilizar para formar una expresión regular para especificar un recurso.

Opcionalmente, puede especificar una cadena de texto como comentario con el `-sid` opción.

De forma predeterminada, las nuevas sentencias se agregan al final de la lista de sentencias, que se procesan en orden. Cuando agregue o modifique sentencias más tarde, tiene la opción de modificar las sentencias `-index` configuración para cambiar la orden de procesamiento.

Configure el acceso S3 para los servicios de directorio externos

A partir de ONTAP 9.14.1, los servicios para directorios externos se han integrado con el almacenamiento de objetos S3 de ONTAP. Esta integración simplifica la administración de usuarios y accesos a través de servicios de directorio externos.

Puede proporcionar grupos de usuarios que pertenecen a un servicio de directorio externo con acceso al entorno de almacenamiento de objetos de ONTAP. El protocolo ligero de acceso a directorios (LDAP) es una interfaz para la comunicación con servicios de directorio, como Active Directory, que proporcionan una base de datos y servicios para la gestión de identidades y accesos (IAM). Para proporcionar acceso, debe configurar los grupos LDAP en el entorno de ONTAP S3. Después de configurar el acceso, los miembros del grupo tienen permisos para los buckets de ONTAP S3. Para obtener más información sobre LDAP, consulte "Información general sobre cómo usar LDAP".

También puede configurar grupos de usuarios de Active Directory para el modo de enlace rápido, de modo que las credenciales de usuario se puedan validar y las aplicaciones S3 de terceros y de código abierto se puedan autenticar a través de conexiones LDAP.

Antes de empezar

Asegúrese de lo siguiente antes de configurar los grupos LDAP y habilitar el modo de enlace rápido para el acceso de grupos:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte "Cree una SVM para S3".
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte "Crear un bucket".
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte "Configure los servicios DNS".
4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte "Instale el certificado de CA raíz autofirmado en la SVM".

5. Se configura un cliente LDAP con TLS habilitado en la SVM. Consulte "Cree una configuración de cliente LDAP" y.. "Asocie la configuración del cliente LDAP con las SVM para obtener información".

Configure el acceso S3 para los servicios de directorio externos

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Cree una sentencia de política de cubo de almacén de objetos con `principal` Defina el grupo LDAP al que desea otorgar acceso:

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Ejemplo: En el siguiente ejemplo se crea una sentencia de política de bloque para `buck1`. La política permite el acceso al grupo LDAP `group1` al recurso (bloque y sus objetos) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Verifique que un usuario del grupo LDAP `group1` Es capaz de realizar operaciones S3 desde el cliente S3.

Use el modo de enlace rápido LDAP para la autenticación

1. Especifique LDAP como la base de datos del servicio *name* de la SVM para el grupo y la contraseña a LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Asegúrese de que un usuario LDAP que acceda al bloque de S3 tenga permisos definidos en las políticas de bloque. Para obtener más información, consulte "Modificar una política de bloques".
3. Verifique que un usuario del grupo LDAP pueda realizar las siguientes operaciones:
   a. Configure la clave de acceso en el cliente S3 en este formato:
      `"NTAPFASTBIND" + base64-encode(user-name:password)`
      Ejemplo: `"NTAPFASTBIND"` + base64-encode(ldapuser:password), lo que resulta en `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      > Es posible que el cliente S3 solicite una clave secreta. En ausencia de una clave secreta, se puede introducir cualquier contraseña de al menos 16 caracteres.

   b. Realice operaciones S3 básicas desde el cliente S3 para el que el usuario tenga permisos.

Habilite LDAP o usuarios de dominio para generar sus propias claves de acceso S3

A partir de ONTAP 9.14.1, como administrador de ONTAP, puede crear roles personalizados y concederles a grupos de dominio locales o a grupos de protocolo ligero de acceso a directorios (LDAP), de modo que los usuarios que pertenecen a esos grupos puedan generar sus propias claves secretas y de acceso para el acceso de clientes S3.

Debe realizar algunos pasos de configuración en la máquina virtual de almacenamiento, de manera que el rol personalizado se pueda crear y asignar al usuario que llama a la API para la generación de claves de acceso.

Antes de empezar

Asegúrese de lo siguiente:

1. Se creó una máquina virtual de almacenamiento habilitada para S3 que contiene un servidor S3. Consulte "Cree una SVM para S3".
2. Se ha creado un bloque en esa máquina virtual de almacenamiento. Consulte "Crear un bucket".
3. DNS está configurado en la máquina virtual de almacenamiento. Consulte "Configure los servicios DNS".
4. Hay un certificado de entidad de certificación raíz (CA) autofirmado del servidor LDAP instalado en la máquina virtual de almacenamiento. Consulte "Instale el certificado de CA raíz autofirmado en la SVM".
5. Se configura un cliente LDAP con TLS habilitado en la máquina virtual de almacenamiento. Consulte "Cree una configuración de cliente LDAP" y .
6. Asocie la configuración del cliente al Vserver. Consulte "Asocie la configuración del cliente LDAP con las SVM" y.. "creación de ldap de servicio de nombres de servicios vserver".
7. Si utiliza una máquina virtual de almacenamiento de datos, cree una interfaz de red de gestión (LIF) y en la máquina virtual, así como una política de servicio para la LIF. Consulte "se crea la interfaz de red" y.. "interfaz de red service-policy create" comandos.

Configurar usuarios para la generación de claves de acceso

1. Especifique LDAP como la base de datos del servicio *name* de la máquina virtual de almacenamiento para el grupo y la contraseña a LDAP:

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Para obtener más información acerca de este comando, consulte "servicios de vserver servicio de nombres ns-switch modificar" comando.

2. Cree un rol personalizado con acceso al extremo de la API de REST DE S3 usuarios:
   `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
   En este ejemplo, la `s3-role` Se genera el rol para los usuarios en la máquina virtual de almacenamiento `svm-1`, a los que se otorgan todos los derechos de acceso, leer, crear y actualizar.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Para obtener más información acerca de este comando, consulte "creación de rest-role de conexión de seguridad" comando.

3. Cree un grupo de usuarios LDAP con el comando security login y añada el nuevo rol personalizado para acceder al punto final de la API DE REST DE usuarios de S3. Para obtener más información acerca de este comando, consulte "seguridad de inicio de sesión creado" comando.

   ```
   security login create -user-or-group-name <ldap-group-name> -application
   http -authentication-method nsswitch -role <custom-role-name> -is-ns
   -switch-group yes
   ```

   En este ejemplo, el grupo LDAP `ldap-group-1` se crea en `svm-1`, y el rol personalizado `s3role` Se ha añadido a él para acceder al punto final de la API, junto con la habilitación del acceso LDAP en el modo de enlace rápido.

   ```
   security login create -user-or-group-name ldap-group-1 -application http
   -authentication-method nsswitch -role s3role -is-ns-switch-group yes
   -second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
   ```

   Para obtener más información, consulte "Utilice el enlace rápido LDAP para la autenticación nsswitch".

Al agregar el rol personalizado al dominio o grupo LDAP, los usuarios de ese grupo tendrán acceso limitado a la ONTAP `/api/protocols/s3/services/{svm.uuid}/users` extremo. Al invocar la API, los usuarios del grupo de dominio o LDAP pueden generar su propio acceso y claves secretas para acceder al cliente S3.

Pueden generar las claves solo para ellos mismos y no para otros usuarios.

Como usuario S3 o LDAP, genere sus propias claves de acceso

A partir de ONTAP 9.14.1, puede generar sus propias claves de acceso y secretas para acceder a clientes S3, si su administrador le ha otorgado el rol para generar sus propias claves. Puede generar claves únicamente para usted mediante el siguiente extremo de la API REST DE ONTAP.

Método HTTP y punto final

Esta llamada a la API de REST utiliza el siguiente método y extremo. Para obtener información sobre los otros métodos de este punto final, consulte la referencia "Documentación de API".

Método HTTP	Ruta
PUBLICAR	/api/protocols/s3/services/{svm.uid}/usuarios

Ejemplo de curl

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Ejemplo de resultado JSON


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```


Habilite el acceso del cliente al almacenamiento de objetos de S3

Habilite el acceso de ONTAP S3 para la organización remota en niveles de FabricPool

Para que ONTAP S3 se use como nivel de capacidad de FabricPool remota (cloud), el administrador de ONTAP S3 debe proporcionar información acerca de la configuración del servidor S3 al administrador de clústeres de ONTAP remoto.

Acerca de esta tarea

Se necesita la siguiente información del servidor S3 para configurar niveles de cloud FabricPool:

- Nombre del servidor (FQDN)
- nombre del bloque
- Certificado de CA
- clave de acceso
- contraseña (clave de acceso secreta)

Además, se requiere la siguiente configuración de red:

- Debe haber una entrada para el nombre de host del servidor ONTAP S3 remoto en el servidor DNS configurado para la SVM de administrador, incluido el nombre FQDN del servidor S3 y las direcciones IP en sus LIF.

- Las LIF de interconexión de clústeres se deben configurar en el clúster local, aunque no sea necesaria la relación de clústeres entre iguales.

Consulte la documentación de FabricPool sobre cómo configurar ONTAP S3 como nivel de cloud.

"Gestión de niveles de almacenamiento mediante FabricPool"

Habilite el acceso de ONTAP S3 para la organización local de FabricPool Tiering

Para que ONTAP S3 se pueda usar como nivel de capacidad FabricPool local, debe definir un almacén de objetos basado en el bloque que ha creado y, a continuación, adjuntar el almacén de objetos a un agregado de nivel de rendimiento para crear una FabricPool.

Antes de empezar

Debe tener el nombre del servidor ONTAP S3 y un nombre de bloque, y el servidor S3 debe haberse creado mediante las LIF del clúster (con el `-vserver Cluster` parámetro).

Acerca de esta tarea

La configuración del almacén de objetos contiene información sobre el nivel de capacidad local, incluidos los nombres de servidor S3 y bloques, y los requisitos de autenticación.

Una vez creada, la configuración de almacén de objetos no debe volver a asociarse con un almacén de objetos o un bloque diferentes. Es posible crear varios bloques para niveles locales, pero no se pueden crear varios almacenes de objetos en un solo bloque.

No se requiere una licencia de FabricPool para un nivel de capacidad local.

Pasos

1. Cree el almacén de objetos para el nivel de capacidad local:

   `storage aggregate object-store config create -object-store-name` *`store_name`* `-ipspace Cluster -provider-type ONTAP_S3 -server` *`S3_server_name`* `-container -name` *`bucket_name`* `-access-key` *`access_key`* `-secret-password password`

   - La `-container-name` Es el bloque de S3 que ha creado.
   - La `-access-key` El parámetro autoriza las solicitudes al servidor ONTAP S3.
   - La `-secret-password` El parámetro (clave de acceso secreta) autentica las solicitudes en el servidor ONTAP S3.
   - Puede ajustar la `-is-certificate-validation-enabled` parámetro a. `false` Para deshabilitar la comprobación de certificados para ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Mostrar y verificar la información de configuración del almacén de objetos:

```
storage aggregate object-store config show
```

3. Opcional: Para ver cuántos datos de un volumen están inactivos, siga los pasos de "Determinar cuántos datos de un volumen están inactivos mediante la generación de informes de datos inactivos".

   Ver cuántos datos de un volumen están inactivos puede ayudarle a decidir qué agregado usar para la organización en niveles local de FabricPool.

4. Asocie el almacén de objetos a un agregado:

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Puede utilizar el `allow-flexgroup` **`true`** Opción para conectar agregados que contienen componentes de volumen FlexGroup.

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Muestre la información del almacén de objetos y compruebe que el almacén de objetos asociado esté disponible:

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

Habilite el acceso del cliente desde una aplicación de S3

Para que las aplicaciones cliente S3 puedan acceder al servidor ONTAP S3, el administrador de ONTAP S3 debe proporcionar información de configuración al usuario S3.

Antes de empezar

La aplicación cliente S3 debe poder autenticarse con el servidor ONTAP S3 mediante las siguientes versiones de firma AWS:

- Firma Versión 4, ONTAP 9.8 y posterior
- Versión de la firma 2, ONTAP 9.11.1 y posterior

ONTAP S3 no admite otras versiones de firma.

El administrador de ONTAP S3 debe haber creado usuarios de S3 y haberle otorgado permisos de acceso, como usuarios individuales o como miembro de un grupo, en la política de bucket o en la de los servidores de almacenamiento de objetos.

La aplicación cliente S3 debe poder resolver el nombre del servidor ONTAP S3, lo que requiere que el administrador de ONTAP S3 proporcione el nombre del servidor S3 (FQDN) y las direcciones IP para los LIF del servidor S3.

Acerca de esta tarea

Para acceder a un bloque de ONTAP S3, un usuario de la aplicación del cliente de S3 introduce información que proporciona el administrador de ONTAP S3.

A partir de ONTAP 9.9.1, el servidor ONTAP S3 admite la siguiente funcionalidad del cliente AWS:

- metadatos de objetos definidos por el usuario

  Un conjunto de pares de clave-valor se puede asignar a objetos como metadatos cuando se crean usando PUT (o POST). Cuando se realiza una operación GET/HEAD en el objeto, los metadatos definidos por el usuario se devuelven junto con los metadatos del sistema.

- etiquetado de objetos

  Se puede asignar un conjunto separado de pares clave-valor como etiquetas para categorizar objetos. A diferencia de los metadatos, se crean y se leen etiquetas con las API DE REST independientemente del objeto, y se implementan cuando se crean los objetos o en cualquier momento.

> Para permitir que los clientes obtengan y coloquen información sobre el etiquetado, las acciones `GetObjectTagging`, `PutObjectTagging`, y. `DeleteObjectTagging` debe permitirse el uso de las políticas de bloque o grupo.

Para obtener más información, consulte la documentación de AWS S3.

Pasos

1. Autentique la aplicación cliente S3 con el servidor ONTAP S3 introduciendo el nombre del servidor S3 y el certificado de CA.
2. Para autenticar un usuario en la aplicación S3 Client, introduzca la siguiente información:
   - El nombre del servidor S3 (FQDN) y el nombre del bloque
   - clave secreta y clave de acceso del usuario

Definiciones de servicios de almacenamiento

ONTAP incluye servicios de almacenamiento predefinidos que están asignados a factores mínimos de rendimiento correspondientes.

El conjunto real de servicios de almacenamiento disponibles en un clúster o SVM está determinado por el tipo de almacenamiento que compone un agregado en la SVM.

En la siguiente tabla se muestra cómo se asignan los factores mínimos de rendimiento a los servicios de almacenamiento predefinidos:

Servicio de almacenamiento	IOPS (SLA) esperada	Pico de IOPS (SLO)	IOPS de volumen mínimo	Latencia estimada	¿Se espera que las IOPS se apliquen?
valor	128 $ por TB	512 $ por TB	75	17 ms	En AFF: Sí En caso contrario: No
rendimiento	2048 por TB	4096 $ por TB	500	2 ms	Sí
extremo	6144 $ por TB	12288 $ por TB	1000	1 ms	Sí

En la siguiente tabla se define el nivel de servicio de almacenamiento disponible para cada tipo de medios o nodo:

Medios o nodo	Nivel de servicio de almacenamiento disponible
Disco	valor
Disco de máquina virtual	valor
LUN de FlexArray	valor
Híbrido	valor
Flash con optimización de la capacidad	valor
Unidad de estado sólido (SSD): No AFF	valor
Flash optimizado para el rendimiento - SSD (AFF)	extremo, rendimiento, valor

Proteja los bloques con SnapMirror de S3

Información general de SnapMirror de 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 de S3 permite el mirroring y los backups en destinos que no sean de NetApp, como AWS S3.

SnapMirror de S3 admite reflejos activos y niveles de backup desde bloques de ONTAP S3 en los siguientes destinos:

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	✔	✔
StorageGRID		✔
AWS S3		✔
Cloud Volumes ONTAP para Azure	✔	✔
Cloud Volumes ONTAP para AWS	✔	✔
Cloud Volumes ONTAP para Google Cloud	✔	✔

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

Requisitos de SnapMirror de S3

- Versión de ONTAP
  ONTAP 9.10.1 o una versión posterior debe ejecutarse en clústeres de origen y de destino.
- Licencia
  Los siguientes paquetes de licencia se requieren en los sistemas de origen y de destino de ONTAP:
  - Paquete básico
    Para el protocolo y el almacenamiento ONTAP S3.
  - Bundle de protección de datos
    Para SnapMirror de S3 para dirigirse a otros destinos de almacenes de objetos de NetApp (ONTAP S3, StorageGRID y Cloud Volumes ONTAP).
  - Bundle de protección de datos y de cloud híbrido
    Para S3 SnapMirror para apuntar a almacenes de objetos de terceros, incluido AWS S3.
- 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 administrador 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 de ONTAP remotos).
    - 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 para S3 en todas las relaciones de SnapMirror S3, pero se 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).
- Claves de usuario raíz
  Se requieren claves de acceso del usuario raíz de Storage VM para las relaciones de SnapMirror de S3; ONTAP no las asigna de forma predeterminada. La primera vez que crea una relación SnapMirror de S3, debe comprobar que las claves existen tanto en los equipos virtuales de almacenamiento de origen como de destino, y volver a regenerarlas si no lo hacen. 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 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 de S3 admite relaciones de distribución ramificada y en cascada. Para ver información general, consulte "Puestas en marcha de protección de datos en cascada y distribución ramificada".

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

Controle el acceso a S3 cucharones

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

Refleje y protección de backup en un clúster remoto

Crear una relación de mirroring para un bloque nuevo (clúster remoto)

Cuando se crean nuevos bloques S3, se pueden proteger inmediatamente a un destino S3 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 SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la ficha **Configuración**, haga clic en ✎ 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**, 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 > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ✎ En S3.

   Consulte "Añada usuarios y grupos de S3" si quiere más información.
3. En el clúster de origen, cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
   b. Haga clic en → Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:

   ```
   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 la SVM de origen, cree una política de SnapMirror S3 si no tiene una existente y no quiere usar 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 (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 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.

Consulte `security certificate install` manual para más detalles.

6. En la SVM de origen, cree una relación de SnapMirror de 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`

Crear una relación de mirroring para un bloque existente (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 SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
   a. Seleccione **Almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la ficha **Configuración**, haga clic en 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. Compruebe que el acceso de usuario y grupo es correcto tanto en las máquinas virtuales de almacenamiento de origen como de destino:
   Seleccione **Almacenamiento > VM de almacenamiento**, luego seleccione la VM de almacenamiento y luego **Configuración**. Por último, seleccione En **S3**.

   Consulte " Añada usuarios y grupos de S3" si quiere más información.
3. En el clúster de origen, cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Seleccione **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
   b. Seleccione Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 ficha **permisos**, haga clic en **Editar**, luego haz clic en **Agregar** bajo **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**: 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 la protección S3 SnapMirror:
   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 información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:
   `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 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 la SVM de origen, cree una política de SnapMirror de S3 si no tiene una existente y no quiere usar la directiva 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 relaciones SnapMirror de 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 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.

Consulte `security certificate install` manual para más detalles.

6. En la SVM de origen, cree una relación de SnapMirror de 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`

Toma de control y sirve datos desde el bloque de destino (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 bloque de destino original de solo lectura y se convierte en bloque de destino original de lectura y escritura; de este modo, se invierte la relación de SnapMirror de S3.

Una vez que el bloque de origen deshabilitado se vuelva a poner disponible, S3 SnapMirror 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.

System Manager

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

1. Haga clic en **Protección > Relaciones** y seleccione **S3 SnapMirror**.
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
   ```

Restaurar un bloque a partir de la máquina virtual de almacenamiento de destino (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 seleccione **S3 SnapMirror**.
2. Haga clic en ⋮ Y, a continuación, 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" si quiere 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 "Crear una relación de backup para un bloque nuevo (destino cloud)".
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
```

Protección de reflejo y backup en el clúster local

Crear una relación de mirroring para un bloque nuevo (clúster local)

Cuando crea nuevos bloques S3, puede protegerlos inmediatamente a un destino S3 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 SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la ficha **Configuración**, haga clic en ✎ En el icono 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**, 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 > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ✎ En S3.

   Consulte "Añada usuarios y grupos de S3" si quiere más información.
3. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de política local**.
   b. Haga clic en → Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:
   `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 de SnapMirror de S3 si no tiene una existente y no desea usar la directiva 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 relaciones SnapMirror de 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 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 utiliza un certificado firmado por un proveedor de CA externo, solo debe instalar este certificado en la SVM de administrador.

      Consulte `security certificate install` manual para más detalles.

6. Cree una relación de SnapMirror de 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`

Crear una relación de mirroring para un bloque existente (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 SnapMirror de S3 para este equipo virtual de almacenamiento, compruebe que existen claves de usuario raíz para los equipos virtuales de almacenamiento de origen y de destino, y regenlas si no:
   a. Haga clic en **almacenamiento > Storage VMs** y, a continuación, seleccione la VM de almacenamiento.
   b. En la ficha **Configuración**, haga clic en ✎ 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**, haga clic en **regenerar clave**.
   No vuelva a generar la clave si ya existe
2. Compruebe que el acceso de usuario y grupo es correcto tanto en las máquinas virtuales de almacenamiento de origen como de destino:
   - Haga clic en **almacenamiento > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en ✎ En S3.

     Consulte "Añada usuarios y grupos de S3" si quiere más información.
3. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, haga clic en **Configuración de directiva local**.
   b. Haga clic en → Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 ficha **permisos**, haga clic en ✎ **Edición** y, a continuación, haga 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,GetOb
        jectAcl,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 de 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 información sobre cómo activar el bloqueo de objetos en un depósito, consulte "Crear un bucket".

CLI

1. Si esta es la primera relación SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:
   `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 de SnapMirror de S3 si no tiene una existente y no desea usar la directiva 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 relaciones SnapMirror de 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. 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 utiliza un certificado firmado por un proveedor de CA externo, solo debe instalar este certificado en la SVM de administrador.

Consulte `security certificate install` manual para más detalles.

6. Cree una relación de SnapMirror de 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`

Toma de control y sirve datos desde el bloque de destino (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 bloque de destino original de solo lectura y se convierte en bloque de destino original de lectura y escritura; de este modo, se invierte la relación de SnapMirror de S3.

Una vez que el bloque de origen deshabilitado se vuelva a poner disponible, S3 SnapMirror 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 seleccione **S3 SnapMirror**.
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
```

Restaurar un bloque desde la máquina virtual de almacenamiento de destino (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 depósito de destino para la operación de restauración debe ser mayor que el espacio lógico utilizado del cubo 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 en ⋮ Y, a continuación, 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" si quiere 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 "Crear una relación de backup para un bloque nuevo (destino cloud)".
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
```

Protección de backup con destinos cloud

Requisitos para las relaciones objetivo del cloud

Asegúrese de que sus entornos de origen y objetivo 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 interfaces de red entre clústeres y un espacio IP se deben configurar en el clúster antes de que el clúster se pueda conectar a un almacén de objetos en cloud. Debe crear interfaces de red de clúster en cada nodo para transferir datos sin problemas desde el almacenamiento local al almacén de objetos en 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 de servidor StorageGRID debe instalarse en la máquina virtual de almacenamiento de administración del clúster ONTAP S3 mediante el `security certificate install command`. Para obtener más información, consulte "Instalar un certificado de CA" Si utiliza 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 administración del clúster ONTAP debe poder resolver FQDN (si se utiliza) a direcciones IP.

Crear una relación de backup para un bloque nuevo (destino cloud)

Cuando crea nuevos buckets de S3, puede realizar backups inmediatamente en un bloque de destino de SnapMirror S3 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 la máquina virtual de almacenamiento de origen debe ser capaz de 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 > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en En **S3**.

      Consulte "Añada usuarios y grupos de S3" si quiere 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 de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
   b. Haga clic en Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 de su grupo de usuarios o acepte los valores predeterminados.
      - **Acciones** - Asegúrese de que se muestran los siguientes valores:

        ```
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
        bjectAcl,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**, 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 SnapMirror de S3 para esta SVM, compruebe que existen claves de usuario raíz para las SVM de origen y de destino y vuelva a regenerarlas si no:
   `vserver object-store-server user show`

   Confirmar 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.
2. Crear 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. Agregar reglas de acceso a la directiva de bloque 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 de SnapMirror de S3 si no tiene una existente y no desea usar la directiva 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 relaciones SnapMirror de 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 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`*

   Consulte `security certificate install` manual para más detalles.

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 de almacén de objetos en el sistema ONTAP local.
   * `-usage` – uso `data` para este flujo de trabajo.
   * `-provider-type` – `AWS_S3` y.. `SGWS` Se admiten los destinos de (StorageGRID).
   * `-server` – La dirección IP o FQDN del servidor de destino.
   * `-is-ssl-enabled` –La activación de SSL es opcional pero se recomienda.

   Consulte `snapmirror object-store config create` manual para más detalles.

   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. Cree una relación de SnapMirror de 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 política que haya creado o aceptar la predeterminada.

   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`

Crear una relación de backup para un bloque existente (destino cloud)

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 > Storage VMs**, haga clic en la VM de almacenamiento, haga clic en **Configuración** y, a continuación, haga clic en En S3.

   Consulte "Añada usuarios y grupos de S3" si quiere más información.

2. Cree una política de SnapMirror de S3 si no tiene una existente y no desea usar la directiva predeterminada:
   a. Haga clic en **Protección > Descripción general** y, a continuación, en **Configuración de directivas locales**.
   b. Haga clic en Junto a **Directivas de protección**, 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 **Continuous** para las relaciones de SnapMirror de 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 ficha **permisos**, haga clic en **Edición** y, a continuación, haga 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**: 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. Realice un backup del bloque con S3 SnapMirror:
   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 bloque 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 de SnapMirror de S3 si no tiene una existente y no desea usar la directiva 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 relaciones SnapMirror de 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 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`*

   Consulte `security certificate install` manual para más detalles.

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 de almacén de objetos en el sistema ONTAP local.
   * `-usage` – uso `data` para este flujo de trabajo.
   * `-provider-type` – `AWS_S3` y.. `SGWS` Se admiten los destinos de (StorageGRID).
   * `-server` – La dirección IP o FQDN del servidor de destino.
   * `-is-ssl-enabled` –La activación de SSL es opcional pero se recomienda.

   Consulte `snapmirror object-store config create` manual para más detalles.

   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. Cree una relación de SnapMirror de 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 política que haya creado o aceptar la predeterminada.

```
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`

Restaurar un bloque a partir de un destino de 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 seleccione **S3 SnapMirror**.
2. Haga clic en ⋮ Y, a continuación, 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" si quiere 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 ejemplo siguiente se restaura un bloque de destino a un bloque existente.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

Modificar una política de mirroring

Es posible que desee modificar una política de reflejo de S3; por ejemplo, si desea ajustar los valores de RPO y acelerador.

System Manager

Si desea ajustar estos valores, puede editar una política de protección existente.

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

CLI

Modifique una política de SnapMirror de 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 capacidad de procesamiento/ancho de banda, en kilobytes/segundos.

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

Auditar eventos S3

Auditar eventos S3

A partir de ONTAP 9.10.1, puede auditar eventos de datos y gestión en entornos ONTAP S3. La funcionalidad de auditoría de S3 es similar a las funcionalidades de auditoría NAS existentes, y la auditoría de S3 y NAS puede coexistir en un clúster.

Cuando se crea y se habilita una configuración de auditoría de S3 en una SVM, los eventos de S3 se registran en un archivo de registro. El puede especificar los siguientes eventos que se registrarán:

- Eventos de acceso a objetos (datos)

  GetObject, PutObject y DeleteObject

- Eventos de gestión

  Cubo de puta y eliminarbloque

El formato del registro es notación de objetos JavaScript (JSON).

El límite combinado para las configuraciones de auditoría de S3 y NFS es de 50 SVM por clúster.

Se requiere el siguiente paquete de licencia:

- Paquete principal, para el protocolo ONTAP S3 y el almacenamiento

Para obtener más información, consulte "Cómo funciona el proceso de auditoría de ONTAP".

Auditoría garantizada

De forma predeterminada, se garantiza la auditoría de S3 y NAS. ONTAP garantiza que se registren todos los eventos de acceso a bloques que pueden someterse a auditorías, incluso si un nodo no está disponible. No se puede completar una operación de bloque solicitada hasta que el registro de auditoría de esa operación se guarde en el volumen provisional en un almacenamiento persistente. Si los registros de auditoría no se pueden guardar en los archivos de almacenamiento provisional, ya sea por falta de espacio o por otros problemas, se deniegan las operaciones de cliente.

Requisitos de espacio para la auditoría

En el sistema de auditoría de ONTAP, los registros de auditoría se almacenan inicialmente en archivos binarios de almacenamiento provisional en nodos individuales. Periódicamente, se consolidan y convierten en registros de eventos legibles por el usuario, que se almacenan en el directorio del registro de eventos de auditoría de la SVM.

Los archivos de almacenamiento provisional se almacenan en un volumen de almacenamiento provisional dedicado, que ONTAP crea cuando se crea la configuración de auditoría. Hay un volumen de almacenamiento provisional por agregado.

Debe planificar el espacio disponible suficiente en la configuración de auditoría:

- Para los volúmenes de almacenamiento provisional en agregados que contienen bloques auditados.
- Para el volumen que contiene el directorio en el que se almacenan los registros de eventos convertidos.

Es posible controlar el número de registros de eventos y, por lo tanto, el espacio disponible en el volumen, mediante uno de los dos métodos al crear la configuración de auditoría de S3:

- Un límite numérico; el `-rotate-limit` parámetro controla la cantidad mínima de archivos de auditoría que se deben conservar.
- Un límite de tiempo; el `-retention-duration` parámetro controla el período máximo que se pueden conservar los archivos.

En ambos parámetros, una vez excedido el valor configurado, se pueden eliminar los archivos de auditoría más antiguos para dejar espacio para otros más nuevos. Para ambos parámetros, el valor es 0, lo que indica que se deben mantener todos los archivos. Para garantizar que haya espacio suficiente, se recomienda, por tanto, establecer uno de los parámetros en un valor distinto de cero.

Debido a la auditoría garantizada, si el espacio disponible para los datos de auditoría se agota antes del límite de rotación, no se pueden crear datos de auditoría más nuevos, lo que provoca errores en el acceso de los clientes a los datos. Por lo tanto, la elección de este valor y del espacio asignado a la auditoría se debe elegir cuidadosamente, y debe responder a las advertencias sobre el espacio disponible del sistema de auditoría.

Para obtener más información, consulte "Conceptos básicos de auditoría".

Planifique una configuración de auditoría de S3

Debe especificar una serie de parámetros para la configuración de auditoría de S3 o aceptar los valores predeterminados. En particular, debe considerar qué parámetros de rotación de log ayudarán a garantizar un espacio libre adecuado.

Consulte **`vserver object-store-server audit create`** man page para detalles de la sintaxis.

Parámetros generales

Hay dos parámetros necesarios que debe especificar al crear la configuración de auditoría. También puede especificar tres parámetros opcionales.

Tipo de información	Opción	Obligatorio
SVM name Nombre de la SVM en la que se creará la configuración de auditoría. La SVM ya debe existir y estar habilitada para S3.	`-verserver` *`svm_name`*	Sí
Ruta de destino del registro Especifica dónde se almacenan los registros de auditoría convertidos. La ruta ya debe existir en la SVM. La ruta puede tener hasta 864 caracteres y debe tener permisos de lectura y escritura. Si la ruta no es válida, el comando de configuración de auditoría falla.	`-destination` *`text`*	Sí
Categorías de eventos para auditar Se pueden auditar las siguientes categorías de eventos: • sql server Eventos GetObject, PutObject y DeleteObject • gestión Eventos PutBucket y DeleteBucket El valor predeterminado es auditar únicamente los eventos de datos.	`-events {data|management}, …`	No

Es posible introducir uno de los siguientes parámetros para controlar la cantidad de archivos de registro de auditoría. Si no se introduce ningún valor, se conservan todos los archivos de registro.

Tipo de información	Opción	Obligatorio

Límite de rotación de los archivos de registro Determina cuántos archivos de registro de auditoría se retendrán antes de rotar el archivo de registro más antiguo. Por ejemplo, si introduce un valor de 5, se conservan los cinco últimos archivos de registro. El valor 0 indica que se conservan todos los archivos de registro. El valor predeterminado es 0.	`-rotate-limit` *`integer`*	No
Límite de duración de los archivos de registro Determina cuánto tiempo se puede retener un archivo de registro antes de eliminarlo. Por ejemplo, si introduce un valor de 5d0h0m, se eliminarán los registros de más de 5 días de antigüedad. El valor 0 indica que se conservan todos los archivos de registro. El valor predeterminado es 0.	`-retention duration` *`integer_time`*	No

Parámetros para la rotación del registro de auditoría

Puede rotar los registros de auditoría en función del tamaño o la programación. El valor predeterminado es girar los registros de auditoría en función del tamaño.

Rotar registros según el tamaño del registro

Si desea utilizar el método de rotación de registro predeterminado y el tamaño de registro predeterminado, no necesita configurar ningún parámetro específico para la rotación de registros. El tamaño predeterminado del registro es 100 MB.

Si no desea utilizar el tamaño predeterminado del registro, puede configurar el `-rotate-size` parámetro para especificar un tamaño de registro personalizado.

Si desea restablecer la rotación basándose únicamente en un tamaño de registro, utilice el siguiente comando para anular la definición del `-rotate-schedule-minute` parámetro:

```
vserver audit modify -vserver svm_name -destination / -rotate-schedule-minute -
```

Rotar registros según un programa

Si opta por rotar los registros de auditoría según una programación, puede programar la rotación del registro utilizando los parámetros de rotación basados en tiempo en cualquier combinación.

- Si utiliza rotación basada en tiempo, el `-rotate-schedule-minute` el parámetro es obligatorio.
- Todos los demás parámetros de rotación basados en el tiempo son opcionales.
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`

- El programa de rotación se calcula utilizando todos los valores relacionados con el tiempo.
  Por ejemplo, si especifica solo el `-rotate-schedule-minute` parámetro, los archivos de registro de auditoría se rotan en función de los minutos especificados en todos los días de la semana, durante todas las horas en todos los meses del año.
- Si especifica solo uno o dos parámetros de rotación basados en la hora (por ejemplo, `-rotate -schedule-month` y.. `-rotate-schedule-minutes`), los archivos de registro se rotan en función de los valores de minutos que haya especificado en todos los días de la semana, durante todas las horas, pero sólo durante los meses especificados.

  Por ejemplo, puede especificar que el registro de auditoría se va a rotar durante los meses de enero, marzo y agosto todos los lunes, miércoles y sábados a las 10:30 a.m.

- Si especifica valores para ambos `-rotate-schedule-dayofweek` y.. `-rotate-schedule-day`, se consideran independientes.

  Por ejemplo, si especifica `-rotate-schedule-dayofweek` Como viernes y. `-rotate-schedule-day` Como 13, los registros de auditoría se girarían cada viernes y el día 13 del mes especificado, no sólo cada viernes 13.

- Si desea restablecer la rotación únicamente según una programación, utilice el siguiente comando para anular la definición del `-rotate-size parameter`:

  ```
  vserver audit modify -vserver svm_name -destination / -rotate-size -
  ```

Rotar registros según el tamaño del registro y el programa

Puede optar por girar los archivos de registro según el tamaño del registro y una programación estableciendo tanto el parámetro -rotate-size como los parámetros de rotación basados en tiempo en cualquier combinación. Por ejemplo: Si `-rotate-size` Se establece en 10 MB y. `-rotate-schedule-minute` Se establece en 15, los archivos de registro giran cuando el tamaño del archivo de registro alcanza 10 MB o en el 15 minuto de cada hora (el evento que ocurra primero).

Cree y habilite una configuración de auditoría de S3

Para implementar la auditoría de S3, primero se debe crear una configuración de auditoría del almacén de objetos persistente en una SVM habilitada para S3 y, luego, habilitar la configuración.

Lo que necesitará

- Una SVM habilitada para S3.
- Espacio suficiente para organizar temporalmente volúmenes en el agregado.

Acerca de esta tarea

Se requiere una configuración de auditoría para cada SVM que contenga bloques de S3 que se desee auditar. Puede habilitar la auditoría de S3 en servidores S3 nuevos o existentes. Las configuraciones de auditoría persisten en un entorno S3 hasta que se elimina mediante el comando **vserver object-store-Server audit delete**.

La configuración de auditoría de S3 se aplica a todos los bloques de la SVM que seleccione para auditoría. Una SVM habilitada para auditoría puede contener bloques auditados y no auditados.

Se recomienda configurar la auditoría de S3 para la rotación automática del registro, determinada por el

tamaño del registro o una programación. Si no configura la rotación automática del registro, todos los archivos de registro se conservan de forma predeterminada. También puede rotar los archivos de registro S3 manualmente mediante el comando **VServer objeto-almacén-auditoría rotate-log**.

Si la SVM es un origen de recuperación ante desastres de SVM, la ruta de destino no puede estar en el volumen raíz.

Procedimiento

1. Cree la configuración de auditoría para rotar los registros de auditoría según el tamaño del registro o un programa.

Si desea rotar registros de auditoría en…	Introduzca…
Tamaño del registro	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination` *`path`* `[[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integer_d][_integer_h][_integer_m][_integers`*`]]} [-rotate-size {`*`integer`*`[KB|MB|GB|TB|PB]}]`
Un programa	`vserver object-store-server audit create -vserver` *`svm_name`* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *`integer`*`] | [-retention-duration [`*`integerd`*`][`*`integerh`*`] [`*`integerm`*`][`*`integers`*`]] } [-rotate-schedule-month` *`chron_month`*`] [-rotate-schedule-dayofweek` *`chron_dayofweek`*`] [-rotate-schedule-day` *`chron_dayofmonth`*`] [-rotate-schedule-hour` *`chron_hour`*`] -rotate-schedule-minute` *`chron_minute`* La `-rotate-schedule-minute` el parámetro es necesario si se configura la rotación del registro de auditoría basado en tiempo.

2. Habilitar auditoría de S3:

   `vserver object-store-server audit enable -vserver` *`svm_name`*

Ejemplos

En el siguiente ejemplo, se crea una configuración de auditoría que audita todos los eventos de S3 (los valores predeterminados) mediante la rotación basada en tamaño. Los registros se almacenan en el directorio /audit_log. El límite de tamaño del archivo de registro es de 200 MB. Los registros se rotan cuando alcanzan los 200 MB de tamaño.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

En el siguiente ejemplo, se crea una configuración de auditoría que audita todos los eventos de S3 (los valores predeterminados) mediante la rotación basada en tamaño. El límite de tamaño del archivo de registro es 100 MB (el valor predeterminado) y los registros se conservan durante 5 días antes de eliminarse.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
```

```
-duration 5d0h0m
```

El siguiente ejemplo crea una configuración de auditoría que audita los eventos de gestión de S3 y eventos de configuración de políticas de acceso central mediante rotación basada en el tiempo. Los registros de auditoría se rotan mensualmente, a las 12:30 p.m. en todos los días de la semana. El límite de rotación del registro es 5.

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

Seleccione bloques para auditoría de S3

Debe especificar qué bloques se van a auditar en una SVM habilitada para auditoría.

Lo que necesitará

- Una SVM habilitada para la auditoría de S3.

Acerca de esta tarea

Las configuraciones de auditoría de S3 se habilitan por SVM, pero debe seleccionar los bloques en SVM que estén habilitadas para auditoría. Si añade bloques a la SVM y desea que se auditen los nuevos bloques, debe seleccionarlos con este procedimiento. También puede tener bloques no auditados en una SVM habilitada para la auditoría de S3.

Las configuraciones de auditoría persisten en los bloques hasta que se eliminan por el `vserver object-store-server audit object-select delete` comando.

Procedimiento

Seleccione un bloque para la auditoría de S3:

```
vserver object-store-server audit event-selector create -vserver svm_name -bucket
bucket_name [[-access] {read-only|write-only|all}] [[-permission] {allow-
only|deny-only|all}]
```

- `-access` - especifica el tipo de acceso a eventos que se va a auditar: `read-only`, `write-only` o. `all` (el valor predeterminado es `all`).
- `-permission` - especifica el tipo de permiso de evento que se va a auditar: `allow-only`, `deny-only` o. `all` (el valor predeterminado es `all`).

Ejemplo

En el siguiente ejemplo se crea una configuración de auditoría de bloques que solo registra los eventos permitidos con acceso de solo lectura:

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

Modifique una configuración de auditoría de S3

Puede modificar los parámetros de auditoría de bloques individuales o la configuración de auditoría de todos los bloques seleccionados para la auditoría en la SVM.

Si desea modificar la configuración de auditoría para…	Introduzca…
Cucharones individuales	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`]` `[`*`parameters to modify`*`]`
Todos los bloques del SVM	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

Ejemplos

En el siguiente ejemplo se modifica una configuración de auditoría de bloque individual para auditar únicamente los eventos de acceso de sólo escritura:

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

En el siguiente ejemplo se modifica la configuración de auditoría de todos los bloques de la SVM para cambiar el límite de tamaño del registro a 10MB y para retener 3 archivos de registro antes de rotar.

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

Muestra configuraciones de auditoría de S3

Después de completar la configuración de auditoría, puede comprobar que la auditoría está configurada correctamente y que está activada. También puede mostrar información sobre todas las configuraciones de auditoría del almacén de objetos en el clúster.

Acerca de esta tarea

Puede mostrar información sobre las configuraciones de auditoría de bloques y SVM.

- Cubos: Utilice la `vserver object-store-server audit event-selector show` comando

  Sin parámetros, el comando muestra la siguiente información sobre los bloques de todas las SVM del clúster con configuraciones de auditoría del almacén de objetos:

  - Nombre de SVM
  - Nombre del bloque
  - Valores de acceso y permisos
- SVM: Utilice `vserver object-store-server audit show` comando

  Sin parámetros, el comando muestra la siguiente información sobre todas las SVM del clúster con configuraciones de auditoría del almacén de objetos:

  - Nombre de SVM

- Estado de auditoría
- Directorio de destino

Puede especificar el `-fields` parámetro para especificar la información de configuración de auditoría que se va a mostrar.

Procedimiento

Mostrar información acerca de las configuraciones de auditoría de S3:

Si desea modificar la configuración para…	Introduzca…
Cucharones	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVM	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

Ejemplos

El siguiente ejemplo muestra información para un solo bloque:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

El siguiente ejemplo muestra información para todos los bloques de una SVM:

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

En el siguiente ejemplo, se muestra el nombre, el estado de auditoría, los tipos de evento, el formato de registro y el directorio objetivo de todas las SVM.

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

En el siguiente ejemplo, se muestran los nombres de las SVM y los detalles sobre el registro de auditoría de todas las SVM.

```
cluster1::> vserver object-store-server audit show -log-save-details

                  Rotation                           Rotation
      Vserver     File Size Rotation Schedule        Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

El siguiente ejemplo muestra de una lista con toda la información de configuración de auditoría acerca de todas las SVM.

```
cluster1::> vserver object-store-server audit show -instance

                             Vserver: vs1
                     Auditing state: true
               Log Destination Path: /audit_log
       Categories of Events to Audit: data
                          Log Format: json
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
           Log Files Rotation Limit: 0
                 Log Retention Time: 0s
```

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.